hakin9 EXTRA

Issue 7/2012 (14) ISSN 1733-7186

QUANTUM COMPUTING

RSA ENCRYPTION AND QUANTUM COMPUTING

QUANTUM SECURITY

SHOR'A ALGORITHM AND THE FUTURE OF RSA

WHO'S AFRAID OF QUANTUM COMPUTERS?

PLUS

QUANTUM GAMING

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth* **HDD diagnostics**, **firmware recovery**, **HDD duplication**, and **file recovery**. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch

Atola TECHNOLOGY

Visit atola.com for details

Learn ethical hacking › Become a Pentester™

- Get trained today through our exclusive 7-months hands-on course.
- Gain access to our complex LAB environment exploiting vulnerabilities across many platforms.
- Receive a trainer dedicated to you during the 7 months.
- 10 different hands-on engagements, 2 different certifications levels.

MONTH 1	› Vulnerability Assessment - level 1 › Vulnerability Assessment - level 2 › Vulnerability Assessment - level 3
MONTH 2	› Network Penetration Testing - level 1 › Network Penetration Testing - level 2
MONTH 3	› Network Penetration Testing - level 3
MONTH 4	› Web Application Penetration Testing - level 1 › Web Application Penetration Testing - level 2
MONTH 5	› Web Application Penetration Testing - level 3
MONTH 6	› Certification Exam 1 - Certified Cyber 51 Pentesting Professional - (CC51PP)
MONTH 7	› Certification Exam 2 - Certified Cyber 51 Pentesting Expert - (CC51PE)

~~Regular Price 1260 USD~~

Discounted Price

999 USD

Sign Up Now

www.cyber51.com

Cyber 51

HAKIN9 EXTRA

Managing:
Michał Wiśniewski
m.wisniewski@software.com.pl

Senior Consultant/Publisher:
Paweł Marciniak

Editor in Chief:
Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Art Director:
Marcin Ziółkowski

DTP:
Marcin Ziółkowski
www.gdstudio.pl

Production Director:
Andrzej Kuca
andrzej.kuca@hakin9.org

Marketing Director:
Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Proofreadres:
Dan Dieterle, Michael Munt,
Michał Wiśniewski

Top Betatesters:
Ruggero Rissone, David von Vistauxx,
Dan Dieterle, Johnette Moody,
Nick Baronian, Dan Walsh, Sanjay Bhalerao,
Jonathan Ringler, Arnoud Tijssen,
Patrik Gange

Publisher: Hakin9 Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
www.hakin9.org/en

Dear Readers,

This month's hakin9 extra issue is totally devoted to Quantum Computing. The landscape in the area of personal computers is changing rapidly according to Moore's law. Quantum Computing offers the possibilities that regular PCs can only dream about and as this month's contributor – Ayo Tayo Balogun has written - "Quantum Computing is like classical computing on steroids". Quantum computer can work like millions of regular computers at once – just to paraphrase David Deutsch. We try to keep up to date with recent trends and "hot topics", hence the issue on Quantum Computing. We sincerely believe that the aforementioned technology will change the traditional way of computing forever. In this issue Ayo Tayo Balogun has prepared a detailed introduction to the topic of Quantum Computing. Alastair Kay is going to present you an article on Quantum Computers and RSA Encryption. Faisal Shah Khan will introduce you to Quantum Gaming. According to Henning Dekant, some people are affraid of big, bad Quantum Computer, and he is going to show you why. Joe Fitzimos in his article expatiated on Quantum Changes in the Cryptographic landscape. Next, Ian T. Durham has written on Shor's Algorithm and the Future of RSA. Jeffrey Zhi J. Zheng, Jie-Ao Zhu & Jie Wan are going to present you Variant, Double-Path Simulation and are going to resolve mysteries and Wave-Particle paradoxes in Quantum Interactions.

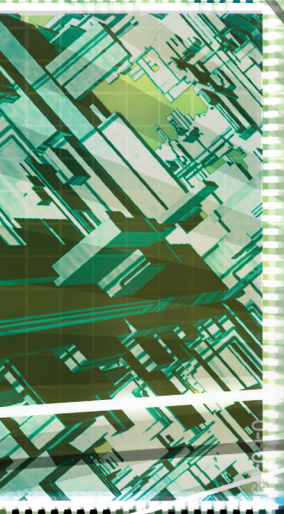
I hope that you will enjoy the reading.

P.S. If you want to learn ethical hacking and become a PenTester, together with Cyber 51 we have prepared a promo course only for hakin9 readers. Do not hesitate and check the link below:

http://www.cyber51.com/affiliates/idevaffiliate.php?id=109

Michał Wiśniewski, hakin9 Extra
m.wisniewski@software.com.pl

Air Freshener?



Printer PSU?
...nope

The Industry's First Commercial Pentesting Drop Box.

THE Pwn Plug.

FEATURES:

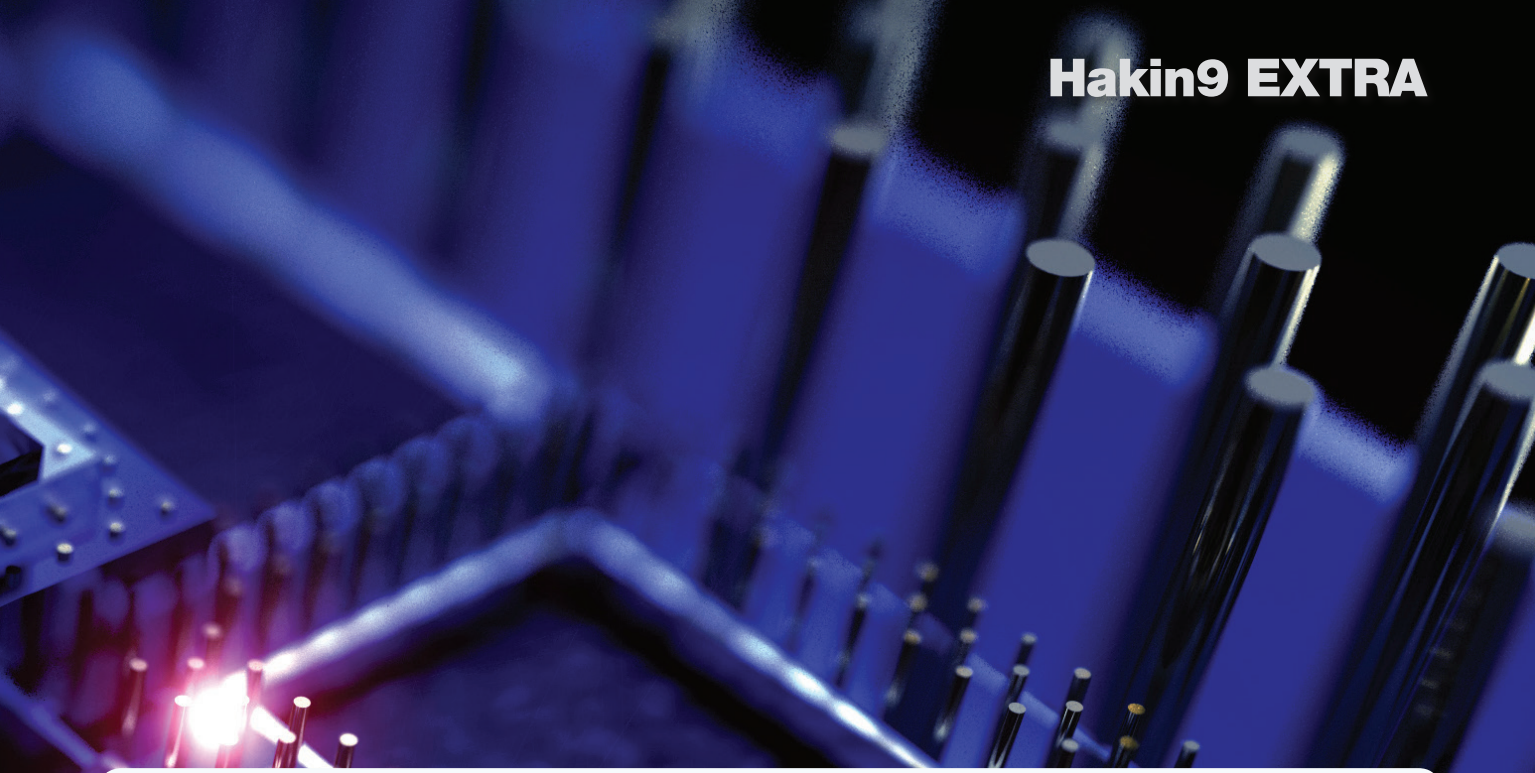
- Covert tunneling
- SSH access over 3G/GSM cell networks
- NAC/802.1x bypass
- and more!

Discover the glory of
Universal Plug & Pwn

PWNIE EXPRESS

@ pwnieexpress.com

t) @pwnieexpress e) info@pwnieexpress.com p) 802.227.2PWN



26. Quantum Changes in the Cryptographic Landscape

By Joseph Fitzsimons

While the above discussion may paint a bleak picture for cryptography in a world where large scale quantum computers are available, all is not lost. As we have seen, certain areas of cryptography, such as symmetric-key ciphers and hashes are not particularly inherently vulnerable to quantum attacks. Indeed, in these areas there do exist information theoretically secure protocols, which are of course invulnerable to quantum attacks. However, quantum attacks cause problems for areas of cryptography where such information theoretically secure classical schemes do not and cannot exist, such as public key ciphers, digital signatures and key exchange protocols.

32. Quantum Computers and Information Security: Shor's Algorithm and the Future of RSA

By Ian T. Durham

All implementations of quantum computing fall into one of four models of quantum computation. The *quantum gate array* implementation most resembles a classical computer in that it uses quantum logic gates that are somewhat analogous to the similar classical gates seen in classical computation. A *one-way* or *cluster-state* quantum computer decomposes the computation into a series of single-qubit measurements made on a highly entangled initial state, i.e. a cluster state. *Adiabatic* quantum computation, as implemented in D-Wave's system, decomposes the computation into a slow, continuous transformation of an operator called a Hamiltonian from an initial state to a final state whose ground state includes the solution. *Topological* quantum computing decomposes the computation into the braiding of particles called anyons that are two-dimensional generalizations of fermions and bosons.and ciphertexts [13].

36. Variant Double-Path Simulation – Resolving Mysteries and Wave-Particle Paradoxes in Quantum Interactions

By Jeffrey Zhi J. Zheng, Jie-Ao Zhu & Jie Wan

Wave-particle paradoxes forced this type of formal discussions and historical Bohr-Einstein debates without a common solution from 1900s and still an open question in modern quantum foundation. Using advanced variant logic and measurement construction, it is feasible to identify complex quantum interactions under multiple/conditional probability into a series of symmetry/anti-symmetry and synchronous/asynchronous conditions.

QUANTUM COMPUTING: WHY WOULD YOU CARE?

AYO-TAYO BALOGUN

The advancements in Information Technology have no doubt made our lives very interesting, and undoubtedly, computers are at the core of information technology advancements. Interestingly, everyone (or almost everyone) now owns a PC. However, your present day PC is not so different from the machine created by Konrad Zuse in 1941 except for the considerable variation in size and the speed at which computations are performed – computers are much smaller now and they process data at much faster rate. At least, this is true for classical computers whose fundamental unit of information is binary in nature. They function by manipulating and interpreting an encoding of binary bits into a useful computational result. A bit, by the way, is a fundamental unit of information, classically represented as a 0 or 1 in your digital (classical) computer.

In quantum computers, quantum effects [1] are exploited to compute in ways that are faster or more efficient than, or even impossible, on conventional computers. Quantum computers use a specific physical implementation to gain a computational advantage over conventional (classical) computers. Our computing needs increase at a very rapid rate, and we require more powerful computers that are not only leaner, but that can do more at a faster pace. To meet this demand, scientists proposed quantum computing. Instead of processing data using bits and bytes in silicon chips, the quantum computing approach uses laser pulses to excite atoms, a process that allows scientists to harness the power of atoms and meet the demand for more complex mathematical computations.

WHAT IS QUANTUM COMPUTING?

If someone says that he can think or talk about quantum physics without becoming dizzy, that shows only that he has not understood anything what(so)ever about it.

– Niels Bohr

Quantum Computing is like Classical Computing on steroids. Quantum computing is a computer design which uses the principles of quantum physics to increase computational power beyond what is attainable by a conventional computer. The term quantum computing is attributed to Richard Feynman (1981) who posited that simulations that inherently include quantum physics from the outset have the potential to tackle those otherwise impossible problems. Like Alan Turing turing machine, computers today work by manipulating bits and exist in one of two distinct states (either 0 or 1 as in a switch off or on). With Quantum computers, the rules have changed. Quantum computers are not limited to two distinct states; they encode information as a series of quantum bits (called qubits) which can exist in superposition – that is - a quantum bit can be in any state within an infinite set of states. Given the fact that quantum computers can perform classical computation simultaneously, which binary systems cannot do, it has the potential to be millions of times more powerful than what we call supercomputers today.

It is obvious therefore, that the properties of quantum computing are very different from classical computing – they have more enormous computational power in comparison to their classical counterparts. What are the elements that differentiate them?

FEATURES OF QUANTUM COMPUTERS

One key element of Quantum Computers is Superpositions – the quality that enables quantum bits to be in any state at the same time unlike the binary states (0 or 1) as we are used to in conventional computers. This superposition attribute gives quantum computers their inherent parallelism. Parallelism, according to physicist David Deutsch, "allows a quantum computer to work on a million computations at once, while your classical PC works on one." A quantum register of *n* quantum bits can be at the same time, in any infinitely many superpositions of basis states.

The essential idea of parallelism is that if an atom can travel through many different routes simultaneously, a computer should be able to use atoms to perform calculations through many different routes simultaneously as well. In other words, quantum computers offer the possibility that multiple calculations can be performed simultaneously.

Thus the parallelism that can be exhibited is striking. Citing an example in an article by Bonsor and Strickland "a 30-qubit quantum computer would equal the processing power of a conventional computer that could run at 10 teraflops (trillions of floating-point operations per second). Today's typical desktop computers run at speeds measured in gigaflops (billions of floating-point operations per second)."

Another key element is entanglement. Entangled states are a hallmark of quantum mechanics and it is an important resource of quantum information processing as it allows scientists to know the value of the qubits without actually looking at them.

According to Michael Nielson (a quantum computer scientist) quantum computers can solve problems that are intractable for conventional computers. That is, it's not just that quantum computers are like regular computers, but smaller and faster, rather, quantum computers work according to principles entirely different than conventional computers, and using those principles can solve problems whose solution will never be feasible on a conventional computer.

It has been shown in theory that a quantum computer will be able to perform any task that a classical computer can, but at a faster pace. For example, atoms (that quantum computer use) change energy states very quickly, much more quickly than even the fastest computer processors. Each qubit can take the place of an entire processor.

Quantum computers will be valuable in factoring large numbers, and therefore extremely useful for working on extremely complex encryption algorithms. Our current methods of encryption are simple compared to the complicated methods possible in quantum computers. Quantum computers could also be used to search large databases in a fraction of the time that it would take a conventional computer.

Quantum computers may also harness the power of atoms and molecules to perform memory and processing tasks at a significantly faster pace than silicon-based binary computer.

IMPLICATION OF QUANTUM COMPUTING

From what we already know, a quantum computer is able to perform the kind of tasks that classical computers can. If however, we run classical algorithms on a quantum computer, the calculation will be performed on the quantum computer as it would have been performed on a classical computer. For us to get the best out of a quantum computer, we need to employ the right algorithms. The kind of algorithms that can exploit the phenomenon of quantum parallelism discussed previously. An example of one such algorithm is the quantum factorization algorithm created by Peter Shor (http://en.wikipedia.org/wiki/Peter_Shor). This algorithm tackles the problem of factorizing large numbers into its prime factors. Using classical computing, the task is ordinarily very difficult to solve; in fact it is so difficult that it forms the basis of RSA encryption, (RSA algorithm is arguably the most popular algorithm for encryption and authentication in recent times). Shor's algorithm cleverly uses the effects of quantum parallelism to give the results of the prime factorization problem in a matter of seconds whereas a classical computer would take about a million years to produce a result!

For organizations, particularly computer manufacturers or power users of computing cycles, the technical aspects and predicted capabilities of quantum computing should be of more than cursory interest. For the rest of us, however, it is the potential of quantum computing to revolutionize how we use computers that should capture our attention. While the development of a full-fledged quantum computer is yet to take place, the discussion of this new technology and the advancement in science and technology allows IT to reflect upon current practices in a number of issues. Some of the questions that readily come to mind are the following:

- How do we currently process data? Have we fully harnessed the processes involved? Have we efficiently utilized our current computational power?
- In terms of security, are we aware of new and emerging threats such as, in time, the possibility of an attack from a quantum computer? According to **Bruce Schneier**, *A quantum computer will reduce the complexity of an attack by a factor of a square root. So it will effectively halve the keyspace*.
- What do users want and expect in the long run? Do they need more computing speed and power? Do they demand and expect more than you are delivering?
- What effect will quantum computers have on artificial intelligence and robotics?

SECURITY IMPLICATIONS

The advancement in quantum computing presents a change that would revolutionize modern technology. The implications of such change will be far reaching, with one of its greatest impacts affecting information security. More specifically, that of modern cryptography

Cracking the most secure codes in existence might require a computer farm covering much of North America to run at full speed for 10 years, even if it did not consume all of the Earth's energy in a single day; that is, using classical computing. In contrast, a future quantum computer the size of a building might only take 16 hours and have about the same power requirements as today's supercomputers. Quantum computers may not replace our computers today, but would be useful in cracking encoded communications by solving the complex encrypted codes.

Research is currently ongoing on quantum communication systems which would allow a sender and receiver to agree on a code for protecting communication. The uncertainty prin-

ciple, (heisenberg's uncertainty principle), ensures that if an eavesdropper tries to monitor the signal in transit it will be disturbed in such a way that the sender and receiver are alerted. Quantum computing holds a whole lot of promise for the world of cryptography. Ironically, it also poses a humongous threat as it presents the capacity to break the most secure of cryptographic algorithms thereby rendering all communication channels exploitable.

The concept of quantum computing may also bring about the introduction of new application frameworks, which may introduce corresponding new vulnerabilities and in turn will require new security architectures (hypothetically speaking). What would be the implication of all these security-related issues to the average non-technology savvy user? The quantum computing technology could make password cracking a lot faster, port-scanning would run at a fraction of their normal time, locating vulnerable systems on the Internet would take much less time. How would these issues impact on the end users?

ARTIFICIAL INTELLIGENCE

The theories of quantum computation suggest that every physical object, even the universe, is in some sense a quantum computer. If this is the case, then according to Turing's work which says that all computers are functionally equivalent, computers should be able to model every physical process. Ultimately this suggests that computers will be capable of simulating conscious rational thought. These theories provoke a minefield of philosophical debate, but maybe the quantum computer will be the key to achieving true artificial intelligence.

A CHRONICLE OF SELECTED RESEARCH/EVENTS IN QUANTUM COMPUTING

- In March 2000, scientists at Los Alamos National Laboratory announced the development of a 7-qubit quantum computer within a single drop of liquid. These particles in positions parallel or counter to the magnetic field allow the quantum computer to mimic the information-encoding of *bits* in digital computers.
- In 2001, Scientists from IBM and Stanford University successfully demonstrated Shor's Algorithm on a quantum computer. Shor's Algorithm is a method for finding the prime factors of numbers (which plays an intrinsic role in cryptography). They used a 7-qubit computer to find the factors of 15. The computer correctly deduced that the prime factors were 3 and 5.
- In 2005, the Institute of Quantum Optics and Quantum Information at the University of Innsbruck announced that scientists had created the first qubyte, or series of 8 qubits, using ion traps.
- In 2006, Scientists in Waterloo and Massachusetts devised methods for quantum control on a 12-qubit system. Quantum control becomes more complex as systems employ more qubits.
- In 2007, Canadian startup company D-Wave demonstrated a 16-qubit quantum computer. The computer solved a Sudoku puzzle and other pattern matching problems.
- In 2012, IBM claimed that its researchers have achieved a major break-through in quantum computing that could help lead to the development of machines able to carry out processing tasks at speeds far beyond those of modern supercomputers.
- In comparison the progress in quantum communications has been somewhat more fruitful. Companies like BT have actually achieved working systems that are able to use quantum effects to detect eavesdropping on a channel.
- 2012: NSA Building A $2 Billion Quantum Computer Artificial Intelligence Spy Center.

CONCLUSION

The future of quantum computing looks really promising and living is likely to become more interesting. Major breakthroughs are expected in Medicine, Engineering and other fields. The desire to consume less power even as we achieve more is also a major driver for quantum computing. As we take the first few quantum computing baby steps, we will need to work on adopting a new paradigm so as to leverage the technology for optimum productivity and effectiveness.

According to *Physics Technology News*, *This is a field of research where progress is increasingly rapid and it is probably too soon to speculate on when the first full-scale quantum computer will be built but recent progress indicates that there is every reason to be optimistic*.

Advocates of quantum computing continue to argue that the shrinkage in microprocessor size presents an opportunity for IT that can be leveraged using quantum computing. This is truly the case as far back as the 90s when the 21st century was tagged the quantum age by Paul Davies.

As the concept of quantum computing begins to take shape therefore, we do not only have to prepare for it, we also have to be mindful about its implications for us. What are the upsides and downsides? Are we ready for the advent of quantum computing? Are we ready for the security implications? When it arrives, will it revolutionalize computing as we hope? These questions and many more are on the verge of being answered as quantum computing arrives eventually.

BIBLIOGRAPHY

- *www.fflch.usp.br/df/opessoa/InfoCog-3.pdf*
- *http://en.wikipedia.org/wiki/Uncertainty_principle*
- *http://en.wikipedia.org/wiki/Quantum_computer,Quantum comuters*
- *http://computer.howstuffworks.com/quantum-computer2.htm*
- *http://blog.alexanderhiggins.com/2012/03/18/nsa-building-a-2-billion-quantum-computer-spy-center-98341/*
- *http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol1/spb3/*
- D. Deutsch, Proc. Roy. Soc. London, Ser. A 400, 97(1985).
- R. P. Feynman, Int. J. Theor. Phys. 21, 467 (1982).
- J. Preskill, "Quantum Computing: Pro and Con," quant- ph/9705032 v3, 26 Aug 1997.

AYO TAYO BALOGUN

is an IT Security Analyst, he graduated with a Bachelor's Degree in Electrical & Computer Engineering from Federal University of Technology Minna (Nigeria) 2000. He has over 10 years professional experience in Information Technology and over 7 years experience in IT Security. Also, he has given a few talks on IT Security and also authored a couple of articles. He's consulted for large financial institutions (through his employer of course), and a couple of smaller firms on IT Security. He tweets IT Security-related stuff using the @ hacksassins handle.

I have a few certifications - CEH, ECSA, EDRP, Project+, Security+, CCNA, MCP, CIW Security Analyst; and I'm currently studying to earn the CHFI. I love to write and hang out with my family.

SeagateDataRecovery.com

Seagate Data Recovery Services work on any disk drive.

Seagate takes the dread out of data mishaps. From accidental file deletions to physical hard disk damage–from any brand–we make it easy to get your files back. With our No Data–No Recovery Charge Guarantee, our skilled professional data recovery technicians use cutting-edge technology to retrieve your data. And for your peace of mind, we also recover data from server applications and virtual technologies. Learn more at www.seagatedatarecovery.com.

Seagate®

RSA ENCRYPTION AND QUANTUM COMPUTERS

ALASTAIR KAY

Public key cryptography is one of the central technologies in securing communications across a myriad of scenarios, but especially through the internet. RSA, named for Rivest, Shamir and Adleman, who first publicly described it in 1978, is the canonical example of a public key crypto system, and is closely related to a number of other protocols such as Diffie-Helman.

Its security is based on two key ingredients; perfect implementation of the pure mathematics that specifies the algorithm (such that no side information is available) and an assumption about the difficulty of performing certain calculations. In fact, the difficulty assumption is already known to be false. At this moment in time, we lack the hardware, a quantum computer, to exploit it, but such a realisation is inevitable. Thus, the security of RSA is rather based on the hope for a slow pace of technological development, which is hardly borne out by recent history. Moreover, it means that any information that is not time sensitive should not be encoded using RSA today.

RSA is an asymmetric system where one person, Alice, creates a public/private key pair, and makes the public component freely available so that anyone wanting to send her a message can encode it. However, only she, making use of her private key, can decode the result. Mathematically, this is based on modular arithmetic, in which we write $a \pmod b = q$ to mean that a is divisible by b with remainder q. There are a variety of techniques, such as the Chinese Remainder Theorem and Euclid's algorithm, that allow one to manipulate these expressions very efficiently. The core of RSA, however, is the use of Fermat's Little Theorem, which enables the decoding process. It states that for a prime P, and an integer $M<P$, $M^{P-1} \pmod P = 1$.

Alice defines the keys by selecting two large primes, P and Q. Subsequently, she finds a value e which is coprime (i.e. has no common factors) with $(P-1)(Q-1)$, and a value d such that $ed \pmod{(P-1)(Q-1)} = 1$. The private key consists of P, Q and d, while the public key is e and PQ. If Bob wants to send Alice a message, he expresses it as an integer $M<PQ$, and calculates $C=M^e \pmod{PQ}$. The idea is that anybody who knows C and the public key should not be able to extract M, whereas Alice, knowing her private key, can calculate $C^d \pmod{PQ} = M^{ed} \pmod{PQ} = M$, where the last step uses the fact that ed is 1+ an integer multiple of $(P-1)(Q-1)$, along with Fermat's Little Theorem. How do we know that nobody else can read the message? We assume that it is impossible to go from the value PQ to P and Q, thereby yielding the entirety of Alice's private key.

Of course, finding the factors is not impossible. Quite the opposite: given enough time, the brute force approach of testing all possible integers is guaranteed to find the solution. The key, however, is that for an n-bit number you would have to test all $2^{n/2}$ numbers of n/2 bits, which grows extremely rapidly with n. For instance, the largest number that has been factored so far was 768 bits, requiring 2 years spread across multiple computers, and estimated as being equivalent to 2000 years compute time on a single 2.2GHz computer. The logical conclusion is that the equivalent computation on the same hardware for an 804 bit integer would take 15 billion years. In other words, the age of the universe! As for a 1024 bit number, "astronomical" doesn't nearly cut it. While this naive

Glossary

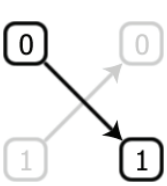
Side Information: Even if the pure mathematics of an algorithm can be proven to be perfectly secure, the translation from that ideal specification into a practical protocol can reveal additional, side, information to an adversary that can be used to break it. For example, the time it takes to perform a certain operation must be the same for all possible inputs otherwise the time required conveys something about the input.

Euclid's Algorithm: When presented with two integers, Euclid's algorithm is a very quick and simple method for finding the largest number that divides into both integers, i.e. it finds the largest common factor.

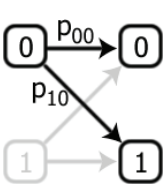
algorithm for finding factors is not the most efficient, the best that is known (the generalised number sieve) still has a near exponential dependence in the number of bits of the integer to factor, permitting size choices that go way beyond anything that can be feasibly computed, and leaving us feeling secure under the proviso that these algorithms are close to the best.

This is where quantum computers come in. While nobody has ever found a better way to factor on a regular computer, such a method has been found on a quantum computer. What makes a quantum computer different to the "classical" computers of our every day experience is, in essence, the software that they can run. Any program that can be written for a classical computer can be expressed in terms of a small number of elementary operations, or gates, with only a relatively modest overhead. The typical example is that of the NAND gate. By wiring up the inputs and outputs of a bunch of these gates, you can replicate any software program. The trick that new, quantum, hardware potentially allows is the addition of an extra gate to its toolkit that cannot be expressed in a nice way by the existing set of gates. Once the hardware that implements this new instruction set is available, the extra gate allows some subroutines to be rewritten in completely novel ways to gain massive speed advantages.

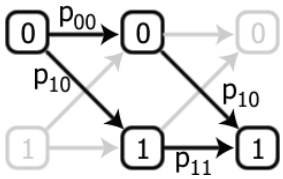
Although NAND gates are sufficient to replicate any classical algorithm, they are not reversible (meaning that you can't, by looking at the output, figure out what the inputs were). This is fairly obvious given that there are 4 possible inputs but only 2 outputs. Now that we're about to delve (superficially) into the world of quantum mechanics, in which every operation (except measurement) is reversible, it's better to think of a different set of gates. Any classical algorithm can be rewritten in a reversible manner, and, having done that, it can be expressed as a circuit of only Toffoli gates[1]. Any quantum computation can similarly be written as a circuit composed of two different types of gate – the Toffoli and the "square root of NOT". The reason why the classical theory of computation seems self-evident, self contained and did not immediately lead to the insights of quantum computation is that one can argue this square root of NOT gate is impossible! To see this, a brief diversion is required. Consider a single bit, which takes values either 0 or 1. A simple operation on this bit is to flip its value, so if it's initially 0, it ends up as 1.



This is the familiar NOT gate. More generally, it would seem reasonable to assume that any operation on this single bit can be described by the set of probabilities p_{ij}, which specify the probability of an input bit j being converted to an output bit i.



The question is the following: is there any such gate that creates the NOT gate by two consecutive applications?



One can calculate, for example, that the probability of converting from an input 0 to an output 1 is $p_{10}(p_{00}+p_{11})$, which we would need to equal 1. There are 3 other conditions, and given that probabilities can't be negative, it is impossible to simultaneously satisfy all four. Hence, it is impossible to build a device which, by acting twice,

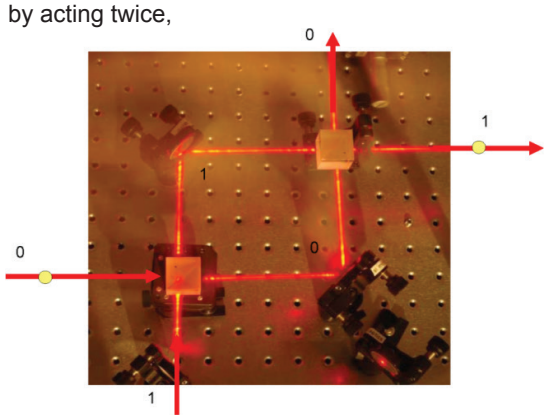
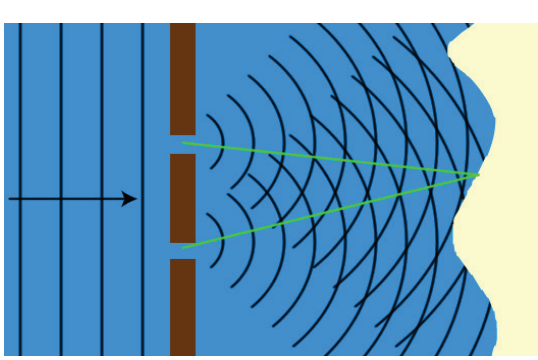


Figure 1. *A pair of partially silvered mirrors (the two pieces of glass bottom left and top right) act so that laser light (even single photons) entering at the bottom (1) leave at the top (0), implementing NOT. Photo courtesy of the Centre for Quantum Technologies, National University of Singapore.*

gives the NOT gate. Since it is impossible to find a satisfying assignment of the probabilities, this gate is said to be logically impossible. The only problem is the inescapable fact that such an operation, which we call the square root of NOT gate, does exist! The resolution is that while the axioms of probability seem obvious from our daily experience, there is no fundamental rule that says they have to be obeyed and, indeed, when one enters the quantum-mechanical regime, the statistics obey a different set of axioms.

How does this contribute towards a new algorithm for factoring numbers? It opens up new avenues of investigation because this square root of NOT gate allows us to (crudely speaking) evaluate a function for many different inputs simultaneously. While we can't just read out all those sets of values any faster, we can ask about some global properties of those values. The simplest example is a one bit function evaluation where you want to know whether $f(0)$ and $f(1)$ are the same or different. Classically, we would have to evaluate both $f(0)$ and $f(1)$ separately, and then compare the two answer bits. Quantumly, however, this is not necessary. If this sounds strange, it's worth realising



that even classical waves exhibit similar properties. Imagine a water wave coming in and hitting a wall, in which there are two holes. From the other side of the wall, this will look like two new waves, one emanating from each hole. The height of the water at any given point is just the sum of the heights of the two waves, so if two peaks coincide, the water is much higher. The maximum height that the water achieves at a given point depends on when the peaks of the two different waves arrive. However, it doesn't depend on the two arrival times independently. Instead, it depends on the difference between their two arrival times, i.e. there is information about the difference in the distance of the point of observation from the two different holes. It's exactly these sorts of differences that we can probe with quantum states (except that different, quantum mechanical, probability axioms apply, meaning that wave heights don't simply add. Sometimes, they can subtract!).

Figure 1 is a photo of an experiment that is composed of two partially reflecting mirrors (bottom left and top right) and two normal mirrors (top left and bottom right). The normal mirrors are just there to help with the routing of the light, and are otherwise irrelevant. Each of the partially reflecting mirrors can be thought of as a logic gate. There are two sides (left, bottom) which are inputs and two which are outputs. We can label the inputs as 0 and 1, and label the outputs such that if light is inputted for a given logical value, and happens to be transmitted, the output site corresponds to the same logical value. With two of these mirrors chained together, the overall output is the NOT gate, so a single mirror is this square root of NOT that is claimed to be impossible. Fire a photon in to 1 input and it always comes out at the 0 output. It helps to think of the light passing through the system as a wave. After passing through the first piece of glass, this wave travels along both possible paths, and then recombines at the second piece of glass. How it recombines depends on the relative positions of the peaks of the two waves. The two paths are exactly the same length, so the only thing that can create a relative shift between the peaks of the two waves are whether those waves were transmitted or reflected on the partially silvered mirrors. In the case where we look at the opposite output to the input (e.g. input 1, output 0), the waves along both paths get reflected once and transmitted once. Thus, they have the same change in peak position, and the peaks arrive together. They combine together so that the photon appears on that output. If the photon appears there, it doesn't appear in the other output.

Without introducing a whole lot of mathematical notation, we're quickly running out of suitable words to describe what's going on, simply because quantum mechanics' operating regime is so far outside our day to day experience. Nevertheless, the idea is simple; there are operations that cannot be described by our usual logic, and by extending the set of available operations we can recode some sub-routines to operate more quickly, particularly if the answers we're after depend on global properties of a function. It's not a magic solution that means everything will run faster, but some specific instances will be able to benefit. It is worth emphasising that while quantum mechanics is famed for its weird probabilistic actions such as a cat being both dead and alive at the same time, quantum computers actually operate (almost) deterministically. While they might go through strange intermediate configurations that are the equivalent of the dead and alive cat (or a single photon passing through both paths at once, evaluating both functions), the whole game of designing quantum algorithms is still to give a definite answer at the output.

Factoring is one instance which benefits from the extended set of operations because it can be cast into an equivalent problem known as order finding, which demands a global property of a function (based on the Fourier Transform). In order to factor the number PQ, start by picking a random number x which is less than PQ. Assuming x is does not share a common factor with PQ (in which case, we'd be done already), then the order, r, of x is defined to be the smallest integer such that $x^r \pmod{PQ}=1$. A little number theory can be used to prove that r is almost certainly even. That means that it can be written as

$$(x^{r/2}-1)(x^{r/2}+1) \pmod{PQ}=0$$

In other words, $(x^{r/2}-1) \pmod{PQ}$ must be a multiple of either P or Q, from which the factors can be extracted[2]. Hence, our only goal is to find r. To do this, it is worth realising that for any integer $k=ar+b$,

$$x^k \pmod{PQ}=(x^r \pmod{PQ})^a(x^b \pmod{PQ})= x^b \pmod{PQ}$$

So, the function $f(k)=x^k \pmod{PQ}$ has a repeating pattern with period r. It is exactly this periodicity that a quantum computer can take advantage of. We can write a quantum sub-routine that evaluates $f(k)$ for all different k, and examines the periodicity, thereby extracting r. In practice, all it extracts is the closest integer to the value $2^L s/r$, where L is a parameter that we specify (it grows linearly with the number of bits of PQ), and s is an unknown integer. Another standard algorithm, known as continued fractions, comes to the rescue and guarantees to extract from this value the numbers s and, most importantly, r. So, the majority of what we do uses standard classical algorithms, simply substituting a new (quantum) subroutine for finding the order in the middle. This is the major step, however, and reduces the running time for factoring an n bit number down to a time that scales with n^3.

RSA in Action

Alice releases two public components, PQ=77 and e=13. She keeps secret the values P=7, Q=11 and d=37. Bob wants to send Alice the number 42 secretly, so he calculates $42^{13} \pmod{77}$=14, and sends that instead. When Alice receives 14, she calculates $14^{37} \pmod{77}$=42, correctly recovering the intended message.

In this instance, it is very obvious what the factors of 77 are. Instead, we proceed by selecting a value which is coprime with 77, such as x=5.

n	1	2		15		29	30	31	32
$5^n \pmod{77}$	5	25	...	34	...	31	1	5	25

From this, we can identify that the sequence repeats with period r=30, which is even. Hence $x^{r/2}-1 \pmod{77}$=33. Via Euclid's algorithm (or inspection), the highest common divisor of 33 and 77 is clearly 11, one of the factors. From this, the other factor, 7, is recovered, and a suitable d is calculated.

It is this reduction in the scaling associated with the factoring algorithm that makes RSA unreliable. It is not the same as a one-off speed boost arising from building a faster processor. Even if we suddenly made a processor 1000 times faster, RSA could simply compensate by using a few more bits. However, with this different scaling, calculating the private key from the public key takes a similar time to all other calculations required in the legitimate application of RSA. Not only is it infeasible to create a sufficiently large key to exclude an eavesdropper on the basis of insufficient computational power, but doing so would also exclude legitimate users from performing the message encoding, decoding etc. because they would have insufficient computational power.

For now, we're safe because the hardware to implement these quantum computations doesn't exist yet. While the theory of what is required of a quantum computer is well developed, experiments are still in their infancy, only operating on a few qubits. Nevertheless, from the moment the first quantum computer is turned on, all messages previously encoded with RSA will be readable. Any secrets that need to remain so after that moment, whether it comes in 10 years or next week, should not trust RSA now. Security based on the assumption of the lack of technological progress hardly constitutes security.

If RSA can't be trusted, what should we use instead? Two natural candidates present themselves. The first is quantum cryptography, which replaces the assumption of computational intractability with one about the physical nature of the Universe, which seems a much more secure footing, but requires hardware working in the quantum mechanical regime. Still, this hardware is much simpler than that required for breaking RSA, and some systems are already available commercially. The second option would be to remain with a classical public key crypto system, but one which we don't believe can be broken by a quantum computer. The logical starting point for this may be to base it on a so-called "NP-complete" problem; the class of the hardest problems for a classical computer to solve for which the solution can be easily verified (the verification step is equivalent to Alice producing the public key from her private key, and solving the problem is equivalent to the eavesdropper trying to produce the private key from the public one). It is not known that quantum computers can efficiently solve these, and it is generally believed that they can't. If true, then this would recover the exponential scaling, and hence place the possibility of reverse engineering the private key from the public one beyond even the scope of quantum computers, but still leaving the basic implementation for legitimate users on a classical computer. No such system exists yet. One of the sticking points seems to be that proving that a problem belongs to this general class is based on the worst case – there only needs to be one instance of a function evaluation that is difficult to compute, while most cases could be easy. In comparison, for a crypto scheme to be reliable, it would have to utilise a subset of instances which are all hard to compute. While this has not been proven for any of these hardest of problems, there are cryptosystems based on finding distances between points of a lattice, which involve functions that are not known to be attackable by quantum computers. This lattice-based cryptography is a strong candidate for an immediate replacement to RSA.

[1] The Toffoli gate is one which acts on 3 bits – two controls and one target. If both controls are input as 1, then the target bit is flipped on output.
[2] Technically, xr/2-1 could be divisible by PQ, but then we just have to try again by picking a different x.

MONITOR STRONY

Innowacyjne e-usługi do monitorowania stron www

SEOmonitor
monitorowanie strony www na potrzeby SEO

SPEEDmonitor
monitorowanie prędkości ładowania strony www

CONTENTmonitor
monitorowanie poprawności językowe treści publikowanych na stronie www

www.monitorstrony.pl

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

DOTACJE NA INNOWACJE
Projekt współfinansowany przez Unię Europejską
z Europejskiego Funduszu Rozwoju Regionalnego

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

CODENAME:
SAMURAI SKILLS COURSE

<< Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time , any where)
- Our Course is Totally Different from Other Courses (new Techniques)

QUANTUM GAMING – A VERY NAÏVE INTRODUCTION

FAISAL SHAH KHAN

The theories of information and computation entered the quantum physical realm in 1965 when Gordon E. Moore asserted that the number of transistors on a microprocessor doubles approximately every two years. This assertion, which has come to be known as Moore's law, roughly predicts that somewhere between the years of 2020 and 2030 (or possibly sooner) circuits on a microprocessor will measure on the atomic scale.

At this scale, quantum mechanical effects will begin to materialize, and virtually every aspect of microprocessor design and engineering will be required to account for these effects. To this end, the theories of *quantum* information and computation study information and its processing under a quantum physical regime. One major goal of these theories is the development of quantum computers that can harness quantum physical phenomenon such as superposition and entanglement for superior information processing capability.

While the study of quantum information and computation is trans-disciplinary in nature, having been cast into perspectives originating in Physics, Chemistry, Computer Science, and Electrical Engineering, here, a relatively new perspective on the subject inspired by non-cooperative game theory will be the focus of discussion. In line with the title of this article, this discussion will be very naïve and cursory, but (hopefully) informative. Starting with a very brief introduction to the notion of information and that of its measure, I will discuss how information is made quantum physical and how the resulting access to the quantum physical feature of entanglement distinguishes quantum information from the original *classical* information.

Further, I will discuss how entanglement has been used as a resource in breaking free of unfavorable Nash equilibrium outcomes in non-cooperative games. Finally, a more general non-cooperative game-theoretic perspective of quantum information processing itself is discussed that seeks optimal processing of quantum information under given constraints.

Information

In a modern mathematical sense due to Claude Shannon [1], information is characterized by randomness. More precisely, it is meaningful to speak of information only after the occurrence of an event, with the informational content of the event quantified in terms of the probability with which the event occurred.

For example, consider the outcomes of a two-headed coin flip. Even before the coin is actually flipped, it is certain that the outcome of the flip will be Heads (H). A fundamental axiom of information theory states that no information is transmitted when this two-headed coin actually lands flat showing the outcome Heads. Next, consider a coin that lands flat showing Heads one out of ten times it is flipped and lands flat showing Tails (T) the other nine out of ten times. When this coin is flipped and lands flat showing Tails, very little information is transmitted since this was the expected outcome. On the other hand, the outcome where this coin lands flat showing Heads carries more information since it is not the expected one.

In short, the probability of the occurrence of an event is inversely related to the amount of information that is received from the event. So the smaller the probability of occurrence of the event is, the higher the informational content of the event, and vice versa. Information theorists express this probabilistic quantification of information more precisely by the equation.

Figure 1. *The probability distribution (p, 1-p).*

$$I(E) = \log\left[\frac{1}{p(E)}\right] \qquad (1)$$

where $I(E)$ denotes the informational content of an event E that occurs with probability $p(E)$. Informational content of complex events such as unions of events and events that are in-

terdependent are quantified via appropriate laws of probability and expectation in the context of equation (1), leading to the notion of *informational entropy* which is of fundamental importance to both information theory and physics. The reader is referred to [2] for a detailed, yet relatively gentle, account of basic concepts of information theory such as entropy.

Information theory enters the quantum physical realm when the notion of probability of occurrence of an event is appropriately generalized. To see how this works, consider first the following more formal approach to probability. We begin by noting that the probability of an event is always positive because an event can never occur a negative number of times out of a positive number of trials of some experiment, and vice versa. Next, note that as soon as an event *E* occurs, the complimentary event "not *E*", henceforth denoted as *–E*, does not. In this case, associate with *E* the maximum possible probability of 1 or absolute certainty of occurrence, and associate with *–E* the least possible probability of 0 or absolute certainty of non-occurrence. This suggests that the relationship between the probability of an event and its complement should satisfy

$$p(E), p(-E) \geq 0$$
$$p(E) + P(-E) = 1.$$

The second equat3ion in (2) suggests that in general, the probability of an event *E* or its complement *–E* originates in the *unit interval* [0,1] which consists of both 0 and 1 and all the numbers in between. For the sake of notational simplicity, let *p(E)=p;* then it follows form the second equation in (2) that *p(–E)=1–p*.

This more formal and geometrically intuitive approach gives rise to the notion of *probability distribution* over two events, that is, an ordered pair of numbers (*p*, 1–*p*) the entries of which split the unit interval into two pieces with the length of the first interval equaling *p* and the length of the second equaling 1– *p*. See Figure 1.

Quantum information

Information is said to be *quantum* when randomization using probability distribution is replaced with the higher order of randomization via quantum superposition followed by measurement. As per by the axioms of quantum physics, quantum superpositions describe the possible states that a quantum object can be in while isolated from its surrounding non-quantum or classical environment. Upon interaction with its classical environment, a quantum object can be in exactly one of

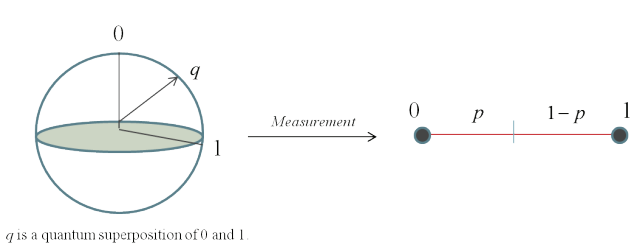


Figure 2. *A quantum superposition q of basis states 0 and 1measures as the probability distribution (p, 1 – p) in the unit interval.*

several possible quantum superpositions called *basis states*. Basis states have a more restricted physical nature than arbitrary quantum superpositions and are viewed as representing the "real" world. When a quantum object takes on a basis state, it is said to have been *measured*. The actual basis state the quantum object takes on after measurement is determined by a probability distribution which is intrinsically related to the quantum superposition the object was originally in. Quantum physical operations other than measurement create quantum superpositions from basis states. Hence, a quantum superposition is always expressible in terms of basis states.

The relationship between a probability distribution and a quantum superposition followed by measurement is reminiscent of the relationship between real numbers and complex numbers and their multiplication. To see this, consider the real number 13 which is a prime number since its only real factors are itself and the number 1. However, if we consider 13 as a special complex number with imaginary part equal to 0, then we can factorize it as

$$(2+3i)(2-3i) = 4+6i-6i+9 = 4+9+0i = 13+0i = 13.$$

Here, introducing the higher order of complex numbers followed by their multiplication produces a new non-trivial factorization of the number 13. This property of complex numbers offers mathematical insight into the notion of a number and can potentially offer insights in the making and breaking of encryption schemes based on factorization of numbers. Similarly, one hopes to observe non-trivial and practically useful properties of higher order randomization via quantum superposition followed by measurement. It turns out that this is indeed the case, as exemplified in the next few sections.

The relationship between quantum superposition and measurement and probability distributions is captured in Figure 2. The "mystical" ball in Figure 2 depicts the more exotic mathematical space of quantum superpositions known as a projective complex Hilbert space. Two basis states labeled 0 and 1 are shown together with an arbitrary quantum superposition *q* of these two basis states. Measurement of *q* maps it to a probability distribution in the unit interval.

Quantum coin flips

Quantum superpositions of two basis states can be viewed as all possible states a *quantum coin* can be in when flipped using quantum physical operations other than measurement. Measurement of the state of a quantum coin produces a probability distribution. A little thought will convince the reader that practically speaking, the flip of a single quantum coin is entirely equivalent to the flip of an ordinary coin! However, when two or more quantum coins are flipped and a measurement is made, an impressive property of quantum information called entanglement becomes apparent. To see how entanglement works, consider first the flip of two classical coins with one coin having an associated probability distribution (*p*,1 –*p*), so that it lands flat showing Heads (H) with probability *p* and lands flat showing Tails (T) with probability 1– *p*. Let the other coin have an associated probability distribution (*q*, 1–*q*). The coins are assumed to be *independent*, that is, the outcome of the flip of one coin does not influence the outcome of the flip of the other. Possible outcomes from flipping two coins are HH, HT, TH, TT, that is both coins land flat showing Heads, or one coin lands flat showing Heads and other lands flat showing Tails, and so forth. The probability distribution associated with the outcomes of the flip of two independent coins is

$$\left(pq, \mathrm{p}(1-q), (1-p)q, (1-p)(1-q)\right) \qquad (3)$$

or the product of the individual probability distributions associated with each coin. Call the probability distribution in (3) *product distribution*.

It is possible to conceive of probability distributions over the four outcomes of the flip of two coins that cannot be expressed as a product distribution. For example, consider the probability distribution

$$\left(\frac{1}{2},0,0,\frac{1}{2}\right) \qquad (4)$$

so that the outcomes HH and TT occur half the time while HT and TH never occur. The dramatic observation here is that both coins *always* land flat showing the same side! This observation becomes even more dramatic if the coins are assumed to be flipped in two different geographical locations, for then it appears to be the case that the coins, although outwardly two different entities, are somehow intrinsically connected. Einstein famously referred to this intrinsic connection as *spooky action at a distance*.

But the flip of two independent classical coins will never exhibit spooky action at distance. This assertion can be checked easily by setting the entries of the probability distributions in (3) and (4) equal to each other and attempting to solve them for *p* and *q*.Try it!

The flip of two independent quantum coins on the other hand can exhibit spooky action at a distance. The trick is to perform on the quantum coins certain physical operations, only available in the quantum realm, and put the coins in a quantum superposition that measures exactly as the probability distribution in (4). A quantum superposition that results in spooky action at a distance is referred to as an *entanglement* to reflect the idea of some intrinsic connection between the quantum coins that is not outwardly obvious. Entanglement has proven to be a resource that can offer practical advantages in the realm of quantum computation. Examples and more detailed theoretical discussions on entanglement and its practical uses can be found in [3,4]. In the remaining discussion, I will focus on the use of entanglement as a resource to break free from unfavorable equilibrium outcomes in non-cooperative games.

Non-cooperative games

Non-cooperative multiplayer game theory is the mathematical study of conflict between interacting individuals. Call the interaction a *game*, the individuals, *players*, and the ability of a player to interact with others his *pure strategies*. Suppose as well that each player has stakes in the game called *payoffs* and that each player is rational, that is, each player will seek to maximize her payoff in a manner consistent with her preferences over all possible payoffs.

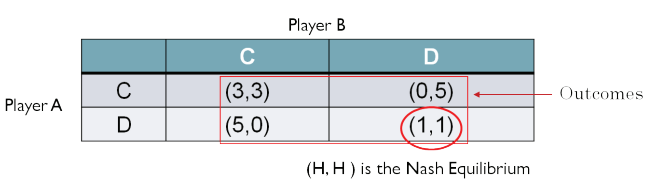


Figure 3. *The game Prisoners' Dilemma.*

A *play* of the game entails a choice of a pure strategy by each player. A play of the game is equivalent to a collection of pure strategies, one per player, called a *pure strategy profile* that determines an *outcome* of the game. From an outcome, appropriate payoffs to each player are computed. The notion of a game is mathematically formalized as a function taking a pure strategy profile to an outcome.

Rational players will seek out a play in which each pure strategy is a *best reply* to all others. Such a play of the game is called *Nash equilibrium* and is considered to be a fundamental solution concept in non-cooperative game theory. Another way to characterize Nash equilibrium is to say that in a Nash equilibrium, no player will unilaterally deviate from his choice of pure strategy (since this will lead to a payoff to him that is less than before).

While the discussion above captures the fundamentals of non-cooperative game theory, it far from being complete. Indeed, professional applications of game theory to real life problems involve many more game-theoretic concepts which are beyond the scope here. Readers are referred to [5] for further exploration. However, this brief discussion is enough to be able to explore simple toy model games such as the popular game called Prisoners' Dilemma, represented in tabular form for easier analysis in Figure 3.

In Figure 3, the pure strategies of both Player A and Player B are Co-operate (C) and Defect (D). The pure strategies of Player A are laid out as rows of the table in Figure 3 while those of Player B are laid out as columns of the table. A play of the game results in an intersection of a row and a column of the table and the payoffs to the players are read off from the ordered pair of numbers in the intersection, the first number in the ordered pair being the payoff to Player A and the second being the payoff to Player B. For instance, the play (C, C) in Prisoners' Dilemma gives a payoff of 3 to each player.

Note however that the play (C, C) is not a Nash equilibrium as C is not a best reply to C on part of either player. Each player can in fact earn a payoff of 5 (better than 3) by unilaterally deviating to D. But this reasoning produces the play (D, D) which in fact is the Nash equilibrium in the game as no player can do better by unilaterally deviating to C.

Mixed Game

As Prisoners' Dilemma exhibits, Nash equilibrium is not necessarily the most favorable outcome of a game in terms of the players' payoffs. A real life example of this situation can be found in history in the form of the Mutually Assured Destruction (MAD) doctrine of the cold war. Even though MAD constituted a Nash equilibrium in the Cold War game between the United States and the Soviet Union, it was

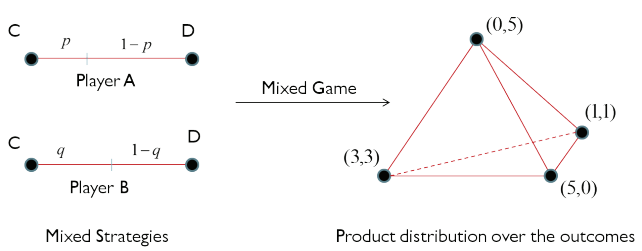


Figure 4. *Extending Prisoners' Dilemma to the corresponding mixed game. The tetrahedron on the right is the geometric representation of the set of all probability distributions over four outcomes such as the outcomes of the flip of two classical coins.*

hardly a favorable outcome. Situations can sometimes be even worse when Nash equilibria don't even exist! In such unfavorable situations, game theorists call upon the players to enlarge the game so as to gain some "breathing room", but insist that any such enlargement *does not change the game*. This process of enlarging a game without changing it is referred to as extending the game.

Players have extended games to avoid unfavorable Nash equilibrium outcomes since time immemorial by randomizing their choice of pure strategies via probability distributions. A probability distribution over pure strategies is called a *mixed strategy*. The new extended game is called the *mixed* game and is defined as the function that takes a mixed strategy profile to the corresponding product distribution over the outcomes of the original game.

It is a worthwhile exercise to check that the mixed game restricts to the original game. Payoff to each player in the mixed is calculated as expected payoff using the product distribution. Geometrically, extending to the mixed game amounts to identifying the players' pure strategies with the endpoints of unit intervals and the outcomes of the game

with the corners of a generalization of the unit interval know as a simplex. This procedure is captured in Figure 4 for Prisoners' Dilemma.

The merit of extending to the mixed game is made explicit by Nash's famous theorem [6] of game theory which uses Kakutani's fixed point theorem to show that there exists at least one Nash equilibrium in the mixed game. Moreover, it is often the case that the mixed game Nash equilibria are more favorable to the players than those available in the original game. However, Nash's theorem offers no guarantee that a mixed game Nash equilibrium will always be more favorable. Indeed, sometimes mixed game Nash equilibria coincide with those available in the original game, a situation that occurs in Prisoners' Dilemma.

Quantized Games

An extension of games that reaches into the quantum physical realm is also possible. A game can be extended into the quantum realm by factoring players' mixed strategies (probability distributions over the pure strategies) as quantum superposition and measurement. The resulting quantum superpositions of their pure strategies are called the players' *pure quantum strategies* and are equivalent to the players using quantum coins to randomize. The new extended game is called a *quantized* game and is defined as any physical operation available within the quantum realm as long as it restricts to the mixed (and therefore the original) game. Since infinitely many physical operations are possible in the quantum realm, it is only possible to speak of a quantized game, a situation very different than that of *the* mixed game.

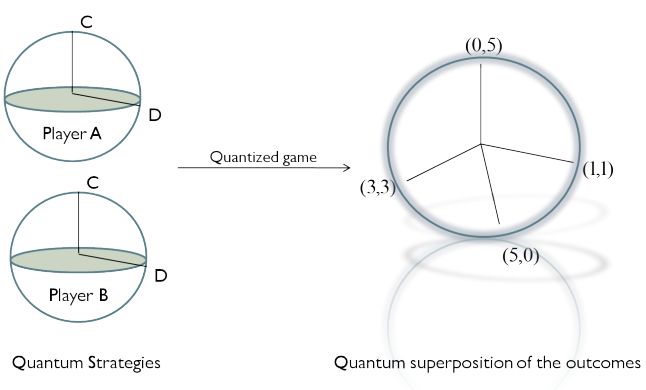


Figure 5. *A quantization of the game Prisoners' Dilemma were players can form quantum superpositions of their pure strategies. The figure on the right hand side represents the space of quantum superpositions of four basis states.*

A quantized game takes a pure quantum strategy profile to a quantum superposition of the outcomes of the original game. Measurement of this quantum superposition can produce probability distributions over the outcomes of the original game that need not be product distributions. These probability distributions resulting from measurement are used to compute expected payoffs to the players. Figure 5 shows the general framework of quantizing Prisoners' Dilemma.

The merit of game quantization lies in its ability to allow players access to entanglement and therefore probability distributions that are not product distributions. Non-product probability distributions, when used to compute expected payoffs, can sometimes lead to the players breaking free from unfavorable Nash equilibrium outcomes. This happens in a quantization of Prisoner's Dilemma due to Eisert, Wilkens, and Lewenstein [7] in which access to entanglement leads to a Nash equilibrium outcome with a payoff of 3 to each player.

There is no equivalent of Nash's theorem for quantum strategies. Quite the opposite, a theorem due to Meyer [8] states that Nash equilibrium in quantum strategies need not even exist! Note that this theorem does not *prove* the non-existence of Nash equilibrium in quantized games, with the Eisert et al. quantization clearly being a counter-example.

Gaming the Quantum

While game quantization looks for enhanced game-theoretic results such as more favorable Nash equilibrium by applying quantum physics to game theory, a more general perspective applies game theory to quantum physics and is referred to as "gaming the quantum".

Consider two players who engage in a non-cooperative *quantum* game, that is, a function representing any physical operation accessible in the quantum realm that takes a pure quantum strategy profile and maps it to a quantum superposition. Unlike quantized games however, a quantum game is not assumed to be an extension into the quantum realm of some underlying game. As such, being a more general game-theoretic construct, it captures the philosophy of applying game theory to quantum physical systems with the goal of gaining insights into their equilibrium behavior more accurately than quantized games.

But whereas a quantized game inherits the notion of players' preferences over payoff from its underlying game, a quantum game enjoys no such privilege and notions of both players' payoffs, and their preferences over these payoffs, in terms of quantum superpositions need declaration. One way to declare such notions is via basis states. Consider for example four possible basis states. For each player, associate numeric values, not all equal, with each of these four basis states so that a player prefers more the basis state with the larger numeric value over another of lesser numeric value.

Next, consider the following property of a quantum superposition *Q*: the *closer Q* (in a particular well-defined sense beyond the scope of the discussion here) it is to a basis state, the *higher the probability* that it will measure as *that* basis state. A player will therefore prefer *Q* over another quantum superposition *P* if *Q* is closer to his most preferred basis state than *P* is (Why?). Finally, a quantum game takes a pure quantum strategy profile to a quantum superposition.

Nash equilibrium in quantum games can be characterized in terms of the notion of closeness of quantum superpositions to basis states. More precisely, a pure quantum strategy profile is a Nash equilibrium if the quantum superposition it is mapped to by the quantum game is *simultaneously* closest to the most preferred outcomes of each player [9]. Gaming the quantum carries the potential for an insightful game theory inspired study of equilibrium behavior of quantum information systems such as quantum algorithms and control of quantum informational systems.

Finally, I conclude with a following natural question: how do quantized games fit into the more general setting of quantum games?

References

- [1] C. Shannon, *A Mathematical Theory of Communication,* The Bell System Technical Journal, Volume 27, 1948.
- [2] R. Hamming, *Coding and Information Theory*, Prentice Hall, 1986.
- [3] M. Nielson and I. Chuang, *Quantum Computation and Quantum Information,* Cambridge University Press, 2004.
- [4] D. Marinescu and G. Marinescu, *Approaching Quantum Computing*, Prentice Hall, 2004.
- [5] K. Binmore, *Fun and Games, A Text Book on Game Theory,* D. C. Heath, 1992.
- [6] J. Nash, *Equilibrium points in n-person games,* Proceedings of the National Academy of Sciences, 1950.
- [7] J. Eisert, M. Wilkens, and M. Lewenstein, *Quantum Games and Quantum Strategies,* Physical Review Letters, 1999.
- [8] D. Meyer, *Quantum Strategies*, Physics Review Letters, 1999.
- [9] F. S. Khan & Simon J. D. Phoenix, *Gaming the Quantum,* preprint available at *http://arxiv.org/abs/1202.1142*

WHO'S AFRAID OF THE BIG BAD QUANTUM COMPUTER?

HENNING DEKANT

Be afraid; be very afraid, as the next fundamental transition in computing technology will obliterate all your encryption protection.

If there is any awareness of quantum computing in the wider IT community then odds are it is this phobia that is driving it. Probably Peter Shore didn't realize that he was about to pigeonhole the entire research field when he published his work on what is now the best known quantum algorithm. But once the news spread that he uncovered a method that could potentially speed up RSA decryption, the fear factor made it spread far and wide. Undoubtedly, if it wasn't for the press coverage that this news received, quantum information technology research would still be widely considered to be just another academic curiosity.

So how realistic is this fear, and is breaking code the only thing a quantum computer is good for? This article is an attempt to separate fact from fiction.

First let's review how key exchange protocols that underlie most modern public key encryption schemes accomplish their task. A good analogy that illustrates the key attribute that quantum computing jeopardizes is shown in the following diagram (image courtesy of Wikipedia) (Figure 1).

Let's assume we want to establish a common secret color shared by two individuals, Alice and Bob[1] – in this example this may not be a primary color but one that can be produced as a mix of three other ones. The scheme assumes that there exists a common first paint component that our odd couple already agreed on. The next component is a secret private color. This color is not shared with anybody. What happens next is the stroke of genius, the secret sauce that makes public key exchange possible. In our toy example it corresponds to the mixing of the secret, private color with the public one. As everybody probably as early as kindergarten learned it's easy to mix colors, but not so easy-try practically impossible-to revert it. From a physics standpoint the underlying issue is that entropy massively increases when the colors are mixed. Nature drives the process towards the mixed state, but makes it very costly to reverse the process. Hence, in thermodynamics, these processes are called "irreversible".

This descent into the physics of our toy example may seem a rather pointless digression, but we will see later that in the context of quantum information processing, this will actually become very relevant.

But first let's get back to Alice and Bob. They can now publicly exchange their mix-color, safe in the knowledge that there are myriads of ways to get to this particular shade of paint, and that nobody has much of a chance of guessing their particular components. Since in the world of this example nobody has any concept of chromatics, even if a potential eavesdropper were to discover the common color, they'd still be unable to discern the secret ones as they cannot unmix the publicly exchanged color shades.

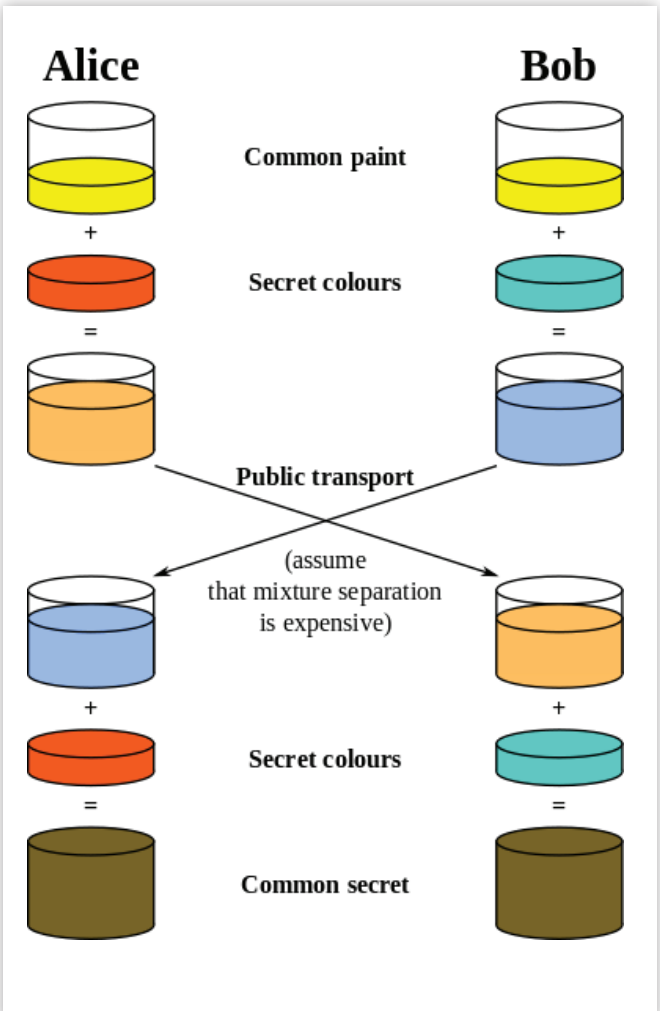


Figure 1.

In the final step, Alice and Bob recover a common color by adding their private secret component. This is a secret that they now share to the exclusion of everybody else.

So how does this relate to the actual public key exchange protocol? We get there by substituting the colors with numbers, say x and y for the common and Alice's secret color. The mixing of colors corresponds to a mathematical function G(x,y). Usually the private secret numbers are picked from the set of prime numbers and the function G is simply a multiplication, exploiting the fact that integer factorization of large numbers is a very costly process. The next diagram depicts the exact same process, just mapped on numbers in this way (Figure 2).

If this simple method is used with sufficiently large prime numbers then the Shared Key is indeed quite safe as there is no known efficient classical algorithm that allows for a reasonably fast integer factorization. Of course "reasonably fast" is a very fuzzy term, so let's be a bit more specific: There is no known classical algorithm that scales polynomially with the size of the integer. So for instance, an effort to crack a 232-digit number (RSA-768) that concluded in 2009 took the combined CPU power of hundreds of machines (Intel Core2 equivalents) **over two years** to accomplish.

And this is where the quantum computing bogeyman comes into the picture, and the aforementioned Peter Shor. This affable MIT researcher formulated a quantum algorithm almost twenty years ago that can factorize integers in polynomial time

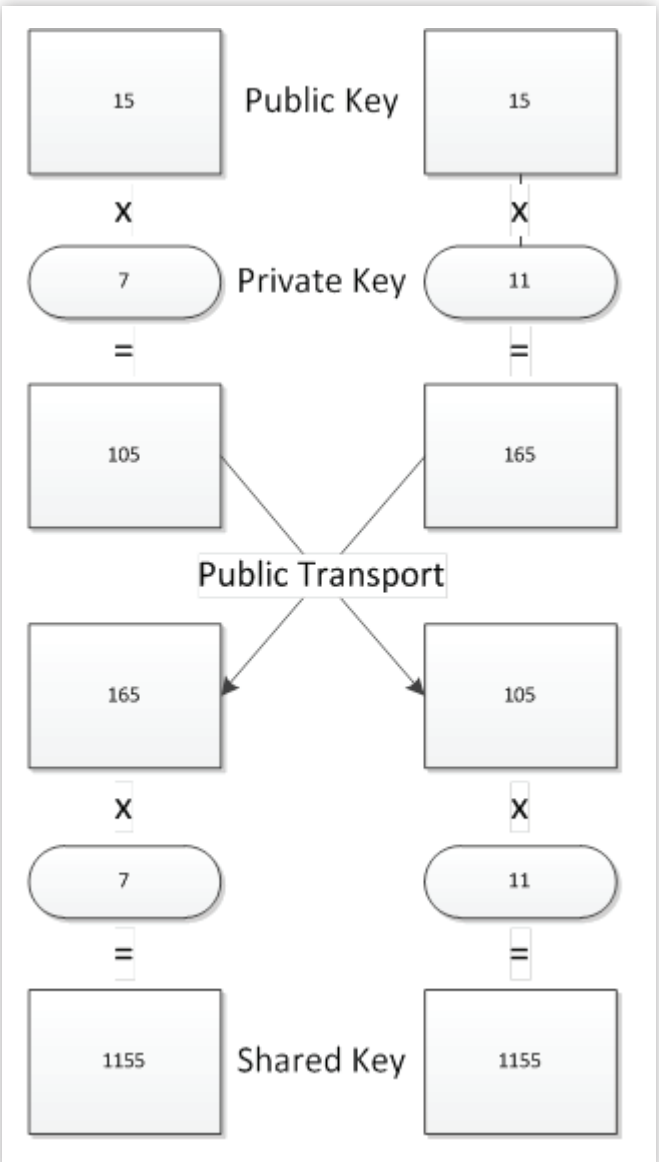


Figure 2.

on the, as of yet elusive, quantum hardware. So what difference would that actually make? The following graph puts this into perspective (Figure 3).

Z encodes stands for the logarithmic value of the size of the integer. The purple curve appears as almost vertical on this scale because the necessary steps in this classic algorithm grow explosively with the size of the integer. Shor's algorithm, in comparison, shows a fairly well behaved slope with increas-

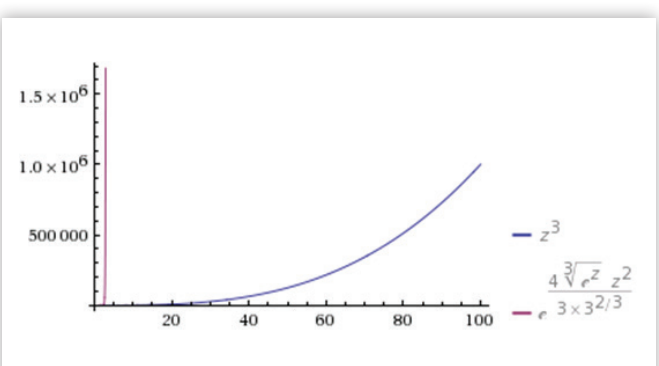


Figure 3.

ing integer sizes, making it theoretically a practical method for factorizing large integers.

And that is why common encryptions such as RSA could not protect against a deciphering attack if a suitable quantum computer was to be utilized. So now that commercial quantum computing devices such as the D-Wave One are on the market, where does that leave our cryptographic security?

First off: Not all quantum computers are created equal. There are universal gate-based ones, which are theoretically probably the best understood, and a textbook on the matter will usually start introducing the subject matter from this vantage point. But then there are also quantum simulators, topological design and adiabatic ones (I will forgo quantum cellular automatons in this article). The only commercially available machine, i.e. D-Wave's One, belongs to the latter category but is not a universal machine, in that it cannot simulate any arbitrary Hamiltonian (this term describes the energy function that governs a quantum system). Essentially this machine is a super-fast and accurate solver for only one class of equations. This kind of equation was first written out for describing solid state magnets according to what it now called the Ising model.

But fear not: The D-Wave machine is not suitable for Shor's algorithm. The latter requires a gate programmable device (or universal adiabatic machine) that provides plenty of qbits. The D-Wave one falls short on both ends. It has a special purpose adiabatic quantum chip with 128 qbits. Even if the architecture were compatible with Shor's algorithm, the amount of qbits falls far short: If N is the number we want to factorize then we need a bit more than the square of that number in terms of qbits. Since the integers we are interested in are pretty large, this is far outside anything that can be realized at this point. For instance, for the RSA-768 challenge mentioned earlier, more than 232^2=53824 qbits are required.

So you may wonder, what good is this vanguard of the coming quantum revolution if it can't even handle the most famous quantum algorithm? To answer this let's step back and look at what motivated the research into quantum computing to begin with. It wasn't the hunt for new, more powerful algorithms but rather the insight, first formulated by Richard Feynman, that quantum mechanical systems cannot be efficiently simulated on classical hardware. This is, of course, a serious impediment as our entire science driven civilization depends on exploiting quantum mechanical effects. I am not even referring to the obvious culprits such as semiconductor based electronics, laser technology etc. but the more mundane chemical industry. Everybody will probably recall the Styrofoam models of orbitals and simple molecules such as benzene C6H6 (Figure 4).

As the graphic illustrates, we know that sp2 orbitals facilitate the binding with the hydrogen, and that there is a delocalized π electron cloud formed from the overlapping p2 orbitals. Yet, these insights are inferred (and now thanks to raster electron microscopy also measured) but they don't flow from an exact solution of the corresponding Schrödinger equations that govern the physics of these kinds of molecules. Granted, multibody problems don't have an exact solution in the classical realm either, but the corresponding equations are well behaved when it comes to numerical simulations. The Schrödinger equation that rules quantum mechanical systems, on the other hand, is not. Simple scenarios are still within reach for classical computing, but not so larger molecules (i.e. the kind that biological processes typically employ). Things get even worse when one wants to go even further and model electrodynamics on the quantum level. Quantum field theories require a summation over an infinite regime of interaction paths – something that will bring any classical computer to its knees quickly. Not a *quantum* computer, though. Just recently a paper was published in the XXXX that showed conclusively that for this new breed of machine a polynomial scaling of these notorious calculations is indeed possible. (As for String theory simulations, the jury is still out on that – but it has been suggested that maybe it should be considered as an indication of an unphysical theory if a particular flavor of a String theory cannot be efficiently simulated on a quantum computer).

Quantum Computing has, therefore, the potential to usher in a new era for chemical and nano-scale engineering, putting an end to the still common practice of having to blindly test thousands of substances for pharmaceutical purposes, and finally realizing the vision of designing smart drugs that specifically match targeted receptor proteins. Of course, even if you can model protein structures, you still need to know which isomer is actually the biologically relevant one. Fortunately, a new technology deploying electron holography is expected to unlock a cornucopia of protein structure data. But this data will remain stale if you cannot understand how these proteins can fold. The latter is going to be key for understanding the function of a protein within the living organism. Unfortunately, simulating protein folding has been shown to be an NP hard problem. Quantum computing is once again coming to the rescue, allowing for a polynomial speed-up of these kinds of calculations. It is not an exaggeration to expect that in the not too distant future lifesaving drug development will be facilitated this way.

This is just one tiny sliver of the fields that quantum computing will impact. Just as with the unexpected applications that ever-increasing conventional computing power enabled, it is

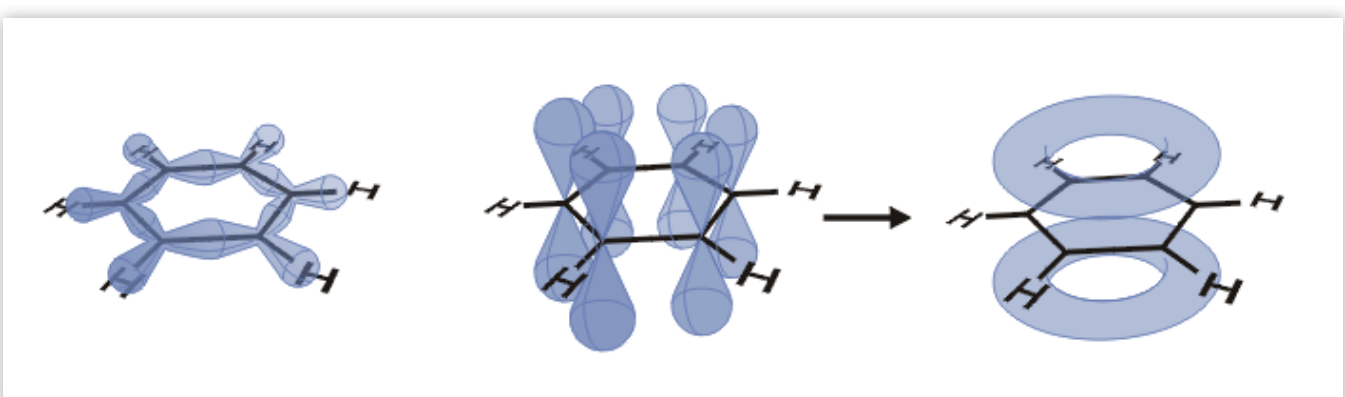


Figure 4.

safe to say that we, in all likelihood, cannot fully anticipate how this technological revolution will impact our lives. But we can certainly identify some more areas that will immediately benefit from it: Artificial Intelligence, graph theory, operational research (and its business applications), database design etc. One could easily file another article on each of these topics while only scratching the surface, so the following observations have to be understood as extremely compressed.

It shouldn't come as a surprise that quantum computing will prove fruitful for artificial intelligence. After all, one other major strand that arguably ignited the entire research field was contemplations on the nature of the human mind. The prominent mathematician and physicist Roger Penrose, for instance, argued vehemently that the human mind cannot be understood as a classical computer i.e. he is convinced (almost religious in his certainty) that a Turing machine in principle cannot emulate a human mind. Since it is not very practical to try to put a human brain into a state of controlled quantum superposition, the next best thing is to think this through for a computer. This is exactly the kind of thought experiment that David Deutsch discussed in his landmark paper on the topic. (It was also for the first time that a quantum algorithm was introduced, albeit not a very useful one, demonstrating that the imagined machine can do some things better than a classical Turing machine). So it is only fitting that one of the first demonstrations of D-Wave's technology concerned the training of an artificial neural net. This particular application maps nicely onto the structure of their system, as the training is mathematically already expressed as the search for a global minimum of an energy function that depends on several free parameters. To the extent that an optimization problem can be recast in this way, it becomes a potential candidate to benefit from D-Wave's quantum computer. There are many applicable use cases for this in operational research (i.e. logistics, supply chain etc.) and business intelligence.

While this is all very exciting, a skeptic will rightfully point out that just knowing a certain tool can help with a task does not tell us how well it will stack up to conventional methods. Given the price tag of $10 million, it had better be good. There are unfortunately not a lot of benchmarks available, but a brute force search method implemented to find some obscure numbers from graph theory (Ramsey numbers) gives an indication that this machine can substitute for some considerable conventional computing horsepower i.e. about 55 MIPS, or the equivalent of a cluster of more than 300 of Intel's fastest commercially available chips. Another fascinating aspect that will factor into the all-important TCO (Total Cost of Ownership) considerations is that a quantum computer will actually require far less energy to achieve this kind of performance (its energy consumption will also only vary minimally under load). Earlier I described a particular architecture as adiabatic, and it is this term that describes this counterintuitive energy characteristic. It is a word that originated in thermodynamics and describes when a process progresses without heat exchange. I.e. throughout most of the QC processing there is no heat-producing entropy increase. At first glance, the huge cooling apparatus that accompanies a quantum computer seems to belie this assertion, but the reason for this considerable cooling technology is not a required continuous protection of the machines from over-heating (like in conventional data centers) but because most QC implementations require an environment that is considerably colder than even the coldest temperature that can be found anywhere in space (the surface of Pluto would be outright balmy in comparison). Amazingly, these days commercially available Helium cooling systems can readily achieve these temperatures close to absolute zero. After cooling down, the entire remaining cooling effort is only employed to counteract thermal flow that even the best high vacuum insulated environments will experience. The quantum system itself will only dissipate a minimal amount of heat when the final result of an algorithm is read out. That is why the system just pulls 15 KWatt in total. This is considerably less than what our hypothetical 300 CPU cluster would consume under load i.e. >100KW per node, more than double D-Wave's power consumption. And the best part: The cooling system, and hence power consumption, will remain the same for each new iteration of chips - D-Wave recently introduced their new 512 qbits RAINER chip, and so far steadily followed their own version of Moor's law, doubling integration about every 18 months.

So although D-Wave's currently available quantum computing technology cannot implement Shore's algorithm, or the second most famous one, Grover's search over an unstructured list, the capabilities it delivers are nothing to scoff at. With heavyweights like IBM pouring considerable R&D resources into this technology, fully universal quantum processors will hit the market much earlier than most IT analysts (such as Gartner) currently project. Recently IBM demoed a 4 qbit universal chip (interestingly using the same superconducting foundry approach as D-Wave). If they also were to manage a doubling of their integration density every 18 months then we'd be looking at 256 qbit chips within three years.

While at this point current RSA implementation will not be in jeopardy, this key exchange protocol is slowly reaching its end-of-life cycle. So how best to mitigate against future quantum computing attacks on the key exchange? The most straightforward approach is simply to use a different "color-mixing" function than integer multiplication i.e. a function that even a quantum computer cannot unravel within a polynomial time frame. This is an active field of research, but so far no consensus for a suitable post-quantum key exchange function has evolved. At least it is well established that most current symmetric crypto (cyphers and hash functions) can be considered secure from the looming threat.

As to key exchange, the ultimate solution can also be provided by quantum mechanics in the form of quantum cryptography that in principle allows to transfer a key in such a manner that any eavesdropping will be detectable. To prove that this technology can be scaled for global intercontinental communication, the current record holder for the longest distance of quantum teleportation, the Chinese physicist Juan Yin[2], plans to repeat this feat in space, opening up the prospect for ultra secure communication around the world[3]. Welcome to the future.

- [1] Don't ask why they are called Alice and Bob – it's just traditional. But if you really need to know Wikipedia has an entry.
- [2] *http://www.technologyreview.com/view/427910/chinese-physicists-smash-distance-record-for/*
- [3] *http://sciencegate.wordpress.com/2012/05/14/chinese-physicists-breaks-down-teleport-records/*

The author can be reached at his blog wavewatching.net where he regular writes about quantum computing.

QUANTUM CHANGES IN THE CRYPTOGRAPHIC LANDSCAPE

JOSEPH FITZSIMONS

The discovery of quantum information processing techniques has enormous consequences for the field of cryptography. The advent of large scale quantum computers would compromise the security of many of todays most widely used cryptosystems, yet quantum techniques can also be exploited to help keep information secret. Here we discuss how the impending quantum revolution changes the balance of power between cryptographer and cryptanalyst.

The histories of cryptography and its cousin steganography stretch back thousands of years, and in that time an enormous variety of techniques have been proposed and used in an attempt *to* keep secret any information not meant for prying eyes. Some of these techniques amounted to abstract manipulations of information, for example substituting or transposing the letters of a message, while others relied on properties of the medium carrying the message, as in the case of invisible ink. Most of these methods were extremely ad hoc, and it was not until the 19th century that a systematic approach to cryptography began to emerge. This approach abstracted away the underlying physical system and began to treat cryptography in a purely mathematical way. By the 20th century, mathematicians had successfully formalised notions of computation and information, and in the process brought about a revolution in how we think about cryptography.

In formalising what is meant by information, and information processing, assumptions about physics play an important but understated role. If one is to define what information is in general, then one needs a definition which can be applied equally to any possible representation of that information. For example, the information content of this article should not depend on the medium on which you receive it: on a computer screen or printed on paper. Any sensible information theory must be agnostic to these matters. However, if we wish for a theory which allows us to successfully abstract information from any physical representation, it is necessary that the theory allows for the full variety of physical states and processes. Similarly, if we wish for a theory of efficient computation, independent of implementation, then we must be careful to account for all physical processes which can happen in a given period of time. Thus any such theories must make assumptions about the underlying physics which governs all physical systems, and hence all possible representations and manipulations of information.

The usual notions of information and efficient computation which we encounter are no exception to this. While it may not be obvious, they are deeply rooted in the physics of the 19th century. Inbuilt is an assumption that the state of a system must necessarily be distinguishable from any other state of the system, and that all processes should map a state to another state or a probabilistic distribution over such states. Indeed, this was an accurate description of nature as we knew it, right up until the early 20th century. However, the discovery of quantum mechanics brought about a revolution in physics, completely transforming our understanding of physical states and processes. The transformation in our physical understanding of nature has been so great that we

now use the term 'classical' to refer to notions of physics prior to this quantum revolution.

The fields of quantum information theory and quantum computation are based on the realisation that quantum mechanics allows for a wider variety of states and processes than can be accounted for classically. Quantum systems are not restricted to distinguishable states, but can also exist in superpositions of such states. This is a form of generalised probabilistic distribution over distinguishable states, in which each such state is associated with a complex amplitude. These complex amplitudes are similar to probabilities, in that they do determine the probability of finding the system in a particular state if measured, but they also contain additional information in the form of a phase. The phase term allows quantum systems to exhibit wavelike behaviour: if a final state can be reached with equal probability via two different computational paths, then, depending on their relative phase, these can either add together to increase the total probability of reaching that final state, or can cancel to result in zero probability of reaching the state. As a result, both the state space and the processes available to a quantum computer are much richer than are available to a classical computer.

While the computers we use today rely on quantum mechanical effects within their CPU to implement logic gates, they represent and process information in an inherantly classical way. Such computers were never designed to protect the delicate phases present at a quantum mechanical level, and have no way to produce the superpositions necessary to exploit the power of quantum computation. However, it is possible, both in principle and increasingly in practice, to build devices which can maintain and manipulate quantum superpositions. Such quantum computers can exploit quantum effects such as interference to aid in computation and communications tasks, and open the door to a variety of new algorithms and communications protocols. As we shall see, these have a significant impact on the cryptographic landscape. The existence of efficient quantum algorithms for the abelian hidden subgroup problem undermines the security of many of the most commonly used public-key cryptosystems. On the other hand, the impossibility of distinguishing certain quantum states allows for novel cryptographic protocols which are provably secure against all attacks, both classical and quantum.

QUANTUM ATTACKS

In cryptography, there are a number of notions of what it means for a cryptosystem to be secure. The ideal case, of course, is for a cryptosystem to reveal nothing about the encoded information independent of the computational resources of an adversary. This notion of security which is independent of the computational capabilities is generally referred to as information theoretic security, since the security of the system can be proved with arguments based on information theory alone. While there exist some classical cryptographic protocols which are indeed information theoretically secure, the use of such systems is often either impractical or impossible. For example, symmetric ciphers where both the sender and receiver are assumed to share a pre-agreed random bit-string, can be constructed which are information theoretically secure, leaking nothing other than the message length provided that the shared key is at least as long as the message to be sent, and is never reused. The classical one time pad is an example of such a cipher. In practice, however, the use of such ciphers is limited by the difficulty of distributing the necessary keys. On the other hand, public-key ciphers, in which a publicly announced key is used to encrypt the message, can never be constructed without relying on computational assumptions. This is because an adversary can simply encode all possible messages using the public key and compare the result to the ciphertext until they have found the original message. The security of public key cryptography, therefore, relies on the assumption that there exist invertible mathematical functions which can be efficiently computed, but which are computationally intractable to invert. Proving that such one-way functions exist would amount to solving the famously open problem of P vs NP of theoretical computer science. While without resolving the P vs NP problem we cannot know for sure whether true one-way functions exist, current public key cryptosystems are based on certain functions which are believed, but not proved, to be hard to invert. Such computational assumptions form the basis for much of modern cryptography.

The advent of quantum computing complicates the picture somewhat. Even for cryptosystems which cannot be efficiently broken by a classical computer there may exist quantum attacks. Indeed, one of the driving forces behind the development of quantum computing has been the discovery of quantum algorithms for factoring integers and searching disordered databases, each of which have important consequences for the security of current cryptosystems.

Hidden subgroup problems

Perhaps the most celebrated of all results in quantum algorithms was the discovery by Peter Shor, in 1994, of an efficient algorithm for integer factorization [1]. This discovery sparked a significant increase in interest in quantum computing, due in part to the central role the difficulty of the integer factorization problem plays in the RSA cryptosystem. In RSA, the public key is an integer which is the result of multiplying together two prime numbers. These numbers must be kept secret, since the private key can easily be calculated from them. The security of RSA therefore depends entirely on the difficulty of factoring integers. For years, factoring had been considered a good candidate one-way function, having been studied for centuries by mathematicians as illustrious as Fermat and Euler. While there has been significant progress in discovering novel classical algorithms for integer factorization, there is as yet no subexponential time algorithm, and many believe that no such algorithm exists. Shor's discovery, therefore, was enormously important both in terms of showing that quantum computers could provide significant speed-ups over known classical algorithms for real world problems beyond the few fairly contrived examples already known then, and in showing that computational assumptions used in constructing cryptosystems may not survive quantum attacks.

While the factoring result is widely known both inside and outside the quantum computing community, another result contained within the same paper has garnered less attention outside of the research community. Shor also presented a quantum algorithm for solving the discrete logarithm problem: the problem of computing an integer solution for $\log_b(a)$ modulo n. This result, too, has important implications for public-key cryptography. A wide variety of cryptosystems derive their security from the hardness of the discrete logarithm problem, including ElGamal, the Digital Signature Algorithm, and the Diffie-Hellman key exchange protocol.

Both integer factorization and finding discrete logarithms are instances of a more general problem, known as the hidden subgroup problem. The definition of the hidden subgroup problem is rather mathematical in nature, however we give it here for completeness. Given a group G, a set S, and a function f which maps G onto S with the property that $f(g_1)=f(g_2)$ for any g_1 and g_2 in G if and only if $g_1H = g_2H$ for some subgroup H of G, the hidden subgroup problem is then to identify H. A wide variety of problems in theoretical computer science can be reduced to some form of the hidden subgroup problem, and it has played a central role in quantum algorithms research. Many cryptosystems derive their security from the assumption that the hidden subgroup problem is hard for specific choices of the group G, and so the hardness of this problem is an important question in determining whether or not such cryptosystems are secure. At present, our knowledge is incomplete, but we do know that there exist efficient quantum algorithms for a number of commonly used groups. A general quantum algorithm exists for solving the hidden subgroup problem over finite abelian groups [2], which includes factorization and discrete logarithms as special cases. Quantum algorithms also exist for certain finite non-abelian groups [3,4], however the general case of non-abelian groups remains open.

The net result of this is that few classical public-key cryptosystems are robust against quantum attacks. RSA, Rabin-Williams, DSA, ECDSA, Diffie-Hellman and eliptic curve cryptography all fall foul of hidden subgroup attacks.

Grover's algorithm

Another area in which quantum computers have an advantage over their classical counterparts is when it comes to searching a disordered database. In 1996, Lov Grover showed that it is possible to search an unstructured database of N entries with only $O(N^{½})$ queries [5], a substantial improvement over the expected N/2 queries required by any classical algorithm. The importance of this algorithm extends beyond searching actual databases, as it can be used in the context of algorithms to search for a specific input to a function which satisfies some specified criteria. If the best classical approach is simply to try evaluating the function for various inputs until a suitable choice is found, then Grover's algorithm provides a way to find a solution with only the square root of the number of queries required classically.

In the context of cryptography, this approach can be used to solve any number of problems. For example, if you wish to find text which results in a particular hash, or to find an encryption key which decodes a given ciphertext to a plaintext with certain statistical properties, Grover's algorithm can be used. It is truely one of the most versatile tricks to come out of quantum computation, but in the context of cryptography it is not all powerful. As the speed-up produced by the algorithm is only polynomial, the advantage to such attacks is limited. If the size of the search space is squared, then the advantage of Grover's algorithm disappears. In the context of searching for the key for some symmetric cipher, for instance, this amounts to simply increasing the key length by a factor of two, while in the case of a hash function, this generally corresponds to a similar increase in the length of the hash.

Importantly, Grover's algorithm is known to be optimal for searching unstructured data, and so there is no danger that an improved quantum algorithm will be discovered which improves the viability of such black-box attacks. Any quantum attacks which provide a better speed-up must necessarily make use of the structure of the particular cryptosystem being attacked. For many cryptosystems, then, all that is required to achieve a level of security against such black-box quantum attacks comparable to their current security against classical attacks is at most a doubling of the size of the relevant key, which is unlikely to impose unmanagable computational overhead.

Finding collisions

Aside from the sort of brute force searches discussed in the previous section, there is another area where quantum search algorithms can potentially increase the efficiency of attacks. Classically, if one wishes to find two inputs for a function which result in the same output, for example if searching for two messages which hash to the same value, then it is only necessary to try a number of random inputs which scales as the square root of the number of possible values of the function before a collision is found. Such an approach is known as a birthday attack because it corresponds to the birthday paradox in probability theory. Here too quantum computation can provide an advantage. A quantum algorithm exists for the collision problem which requires a number of evaluations of the function that scales only as the cubic root of the number of possible values of the function [6]. As in the case of Grover's algorithm, the collision algorithm is known to be optimal to within a constant factor. Thus increasing the search space by a constant factor removes any quantum advantage.

Post-quantum cryptography

While the above discussion may paint a bleak picture for cryptography in a world where large scale quantum computers are available, all is not lost. As we have seen, certain areas of cryptography, such as symmetric-key ciphers and hashes, are not particularly inherently vulnerable to quantum attacks. Indeed, in these areas there do exist information theoretically secure protocols, which are of course invulnerable to quantum attacks. However, quantum attacks cause problems for areas of cryptography where such information theoretically secure classical schemes do not and cannot exist, such as public key ciphers, digital signatures and key exchange protocols. Nonetheless, there exist some public-key schemes which are not currently known to be vulnerable to quantum attacks. There is increasing interest in the area of public-key schemes robust against quantum adversaries under the heading of post-quantum cryptography [7].

Thus far, the most prominant examples of post-quantum cryptography include code-based systems, such as the McEliece cryptosystem, and schemes based on lattice problems, such as NTRU. In the realm of digital signatures, Lamport signatures are believed to be resistant to quantum attacks. However, while these schemes are currently believed to be secure against quantum adversaries, the evidence for this largely amounts to lack of progress on relevant quantum algorithms.

As we shall see in the next section, however, quantum mechanics offers us reason for hope ... at least in some areas.

QUANTUM CRYPTOGRAPHY

Thus far we have considered the advantages that quantum mechanics offers over classical computation in terms of computational ability. However, this is not the full story of quantum information. Quantum mechanics also imposes restrictions not present in classical theories. In particular, our inability to perfectly distinguish quantum states means that if given a copy

of an unknown quantum state we are unable to determine a full classical description of the state. Indeed, a result known as Holevo's theorem tells us that we can at most recover one classical bit per qubit (the basic unit of quantum information) we receive. This restriction on the information that can be learned from a quantum state also limits our ability to copy an unknown quantum state.

Quantum key distribution (QKD)

Even before it was realised that quantum computers brought into question the security of public-key cryptography, scientists had already realised that quantum mechanics could be used to achieve even more secure methods of communication. In 1984, Charles Bennett and Gilles Brassard proposed a scheme which, like Diffie-Hellman, allowed to remote parties to agree on a shared secret key [8]. Unlike Diffie-Hellman, however, the scheme (now known as BB84) derived its security not from computational assumptions, but rather from physics. They noticed that if, rather than exchanging classical bitstrings, the two parties exchanged quantum states, then an eavesdropper could not intercept a message without altering the quantum state of the message in a way that would be detectable to the users of the protocol.

Another quantum mechanical approach to the key distribution problem was put forth by Artur Ekert in 1991 [9]. Ekert's approach differed somewhat from the BB84 protocol, in that it exploited a phenomenon known as entanglement. Entanglement is a form of quantum correlation that occurs in states which are in any superposition over the classical states of two systems such that the state of the system as a whole cannot be factored into separate states of the two subsystems. A previous result, due to Bell, had shown that there existed inequalities on the statistics of measurement outcomes which could only be violated by measurements for which the results which were not predetermined [10]. Importantly, entangled quantum states can violate Bell's inequality. Ekert's protocol made use of this fact, by distributing entangled particles between parties, to ensure that the result of the measurements must be unknowable to an eavesdropper: if a third party could learn the outcome of the measurements by intercepting the entangled particles in advance of the measurements, then the results would be predetermined and hence unable to violate Bell's inequality.

Both protocols are information theoretically secure, so even a computationally unbounded adversary cannot successfully eavesdrop. While these two protocols appear to take very different approaches to the same problem, a deeper look reveals striking similarities. If the measurement step made by one of the parties in the second protocol is moved earlier, prior to the distribution of the particles, it results in a remarkably BB84-like protocol, with no mathematical difference to the functioning of the protocol. However, such entanglement-based protocols do offer one substantial advantage over the alternative, which has only recently been realised. As the security relies only on the classical statistics of the measurement results, and not on the specific operation of the device, it is possible to verify security without trusting the device itself. This means that no trust in the manufacturer of the device is required: provided that the measurement results sufficiently violate Bell's inequality, it is impossible that they can have been known to an eavesdropper [11,12]. Such results only apply to the process of agreeing a key, and of course cannot ensure security after the key has been agreed. Thus, it is still necessary for the users to ensure the end points are secure. Nonetheless, this new notion of device independent security has become a hot topic in quantum cryptography research in recent years.

Quantum key distribution is perhaps the first technology based on quantum information processing to have reached the level of a commercial product. Currently a number of QKD systems are commercially available, though as yet device independent setups remain at the proof of concept stage.

Secure random number generation

For many cryptographic tasks it is necessary to produce randomness, and cryptographically secure pseudo-random number generators are an important element of classical cryptography. Quantum mechanics, however, allows for true randomness to be generated, and currently it is possible to buy quantum random number generators. The current generation of devices, however, essentially require the user to trust that they are correctly functioning, or to dismantle the device to verify each component works as advertised. Even then, the security is contingent on our current understanding of the dimensionality of the state space for particular physical systems. However, as we have seen in the previous section, the violation of Bell's inequality allows for a way to certify that measurement results cannot have been predetermined and hence are necessarily random, independent of the underlying physical system. Thus similar techniques to those which allow for device independent quantum key distribution also allow for the creation of random number generators for which a user can verify that the numbers produced are indeed truely random [13].

Beyond QKD

The utility of quantum mechanics in constructing secure cryptographic schemes is not limited to key distribution. Over the years, quantum techniques have been applied to a variety of cryptographic tasks. Some of these schemes amount to extending classical results to the quantum realm, as for example in the case of quantum secret sharing schemes [14] and protocols for secure multi-party quantum computation [15,16]. Others utilise quantum tricks to achieve information theoretic security, as in the case of quantum digital signatures [17] and quantum schemes for anonymous communication [18]. The area of distributed computing, in particular, has seen many novel quantum cryptographic protocols. These include information theoretically secure protocols for performing remote computations in which an even an eavesdropper with access to the remote computer cannot learn which computation has been performed [19-22], and protocols for querying remote databases in such a way that any attempt to learn which query was performed, even by the computer storing the database, will be detected with high probability [23].

CONCLUSIONS

The existence of large scale quantum computers would significantly alter the balance of power between cryptographer and eavesdropper. As we have seen, many commonly used cryptosystems are vulnerable to quantum attacks. However quantum mechanics also allows for new cryptographic protocols, replacing some but not all of the infrastructure threatened by quantum computers, and providing secure protocols for tasks which could not previously be achieved.

Some tasks remain beyond the reach even of quantum computers. It is known that it is impossible to construct information theoretically secure schemes for important cryptographic

primitives such as bit commitment and oblivious transfer. Yet even here, relativity, the other great pillar of modern physics, may offers us hope [24,25].

One thing is for sure, the advent of quantum computers brings about a definite shift in the cryptographic landscape.

DR JOSEPH FITZSIMONS

is currently a senior research fellow at the Centre for Quantum Technologies (CQT), at the National University of Singapore. He received his DPhil from the from the University of Oxford in 2007. Prior to joining CQT, he spent 3 years as a Junior Research Fellow at Merton College, Oxford, and as a visiting researcher at the Institute for Quantum Computing and the department of Combinatorics and Optimization at the University of Waterloo.

REFERENCES

- [1] Peter W. Shor. Algorithms for quantum computation: Discrete log and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science , pages 124-134, 1994.
- [2] D. Boneh and R. Lipton. Quantum cryptanalysis of hidden linear functions. Advances in Cryptology (CRYPTO95), pages 424-437, 1995.
- [3] S. Hallgren, A. Russell, and A. Ta-Shma. Normal sub-group reconstruction and quantum computation using group representations. Proceedings of the 37th Annual ACM Symposium on Theory of Computing, pages 627-635. ACM, 2000.
- [4] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. Proceedings of the 13th Annual ACM Symposium on Parallel Algorithms and Architectures, pages 263-270. ACM, 2001.
- [5] Lov K. Grover. A fast quantum mechanical algorithm for database search. Proceedings of the 28th annual ACM Symposium on Theory of Computing, pages 212-219, 1996.
- [6] G. Brassard, P. Høyer, and A. Tapp. Quantum cryptanalysis of hash and claw-free functions. LATIN'98: Theoretical Informatics, pages 163-169, 1998.
- [7] D.J. Bernstein. Introduction to postquantum cryptography. Post--Quantum Cryptography, pages 1-14, 2009.
- [8] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175-179, 1984.
- [9] Artur K. Ekert. Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6):661-663, 1991.
- [10] John S. Bell. On the Einstein-Podolsky-Rosen paradox. Physics, 1:195-200, 1964.
- [11] A. Acín, N. Gisin, and L. Masanes. From Bell's theorem to secure quantum key distribution. Physical Review Letters, 97(12):120405, 2006.
- [12] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. Physical Review Letters, 98(23):230501, 2007.
- [13] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D Hayes, L. Luo, T.A. Manning, and C. Monroe. Random numbers certied by Bell's theorem. Nature, 464:1021-1024, 2010.
- [14] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. Physical Review A, 59(3):1829, 1999.
- [15] C. Crépeau, D. Gottesman, and A. Smith. Secure multiparty quantum computation. Proceedings of the 34th Annual ACM Symposium on Theory of Computing, pages 643-652. ACM, 2002.
- [16] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science, pages 249-260. IEEE, 2006.
- [17] D. Gottesman and I. Chuang. Quantum digital signatures. quantph/0105032, 2001.
- [18] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp. Anonymous quantum communication. Proceedings of the Advances in Cryptology 13th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT '07), pages 460-473. Springer-Verlag, 2007.
- [19] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, pages 517-526. IEEE, 2009.
- [20] J.F. Fitzsimons and E. Kashefi. Unconditionally verifiable blind computation. arXiv:1203.5217, 2012.
- [21] D. Aharonov, M. Ben-Or, and E. Eban. Interactive proofs for quantum computations. Proceedings of Innovations in Computer Science (ICS 2010), pages 453-469, 2010.
- [22] A.M. Childs. Secure assisted quantum computation. Quantum Information & Computation, 5(6):456-466, 2005.
- [23] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum private queries. arXiv:0708.2992, 2007.
- [24] A. Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. arXiv:1108.2879, 2011.
- [25] J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner. Secure bit commitment from relativistic constraints. arXiv:1206.1740, 2012.

Develop for the Next Big Platform!

Attend the Windows Phone Developer Conference and get the best developer training!

WP DevCon

The Windows Phone Developer Conference

October 22-24, 2012
Hyatt Regency
Burlingame, CA
www.WPDevCon.net

Learn from the top experts at the Windows Phone Developer Conference, including 12 Microsoft MVPs!


Darrin Bishop


Michael Cummings


Nick Landry


Jose Luis Latorre


Chris Love


Colin Melia


Walt Ritscher


Lino Tadros


Kelly White


Shawn Wildermuth


Chris Williams

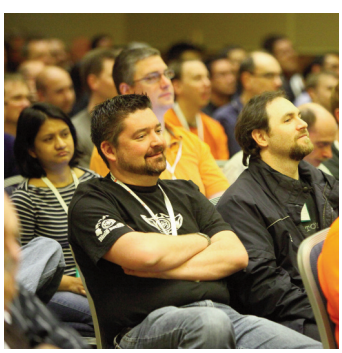

Chris Woodruff

50+ Classes and Workshops

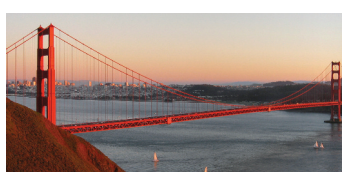
focus on a variety of important topics:

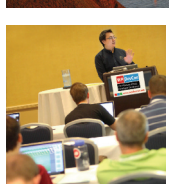
- Design implementation
- Location intelligence services
- Rich data visualization and implementation
- Cloud-based mobile solutions
- Development leveraging HTML5
- User experience
- Application design
- HTTP protocol
- Building reusable components
- Microsoft push notification service
- Creating custom animation
- and many more!

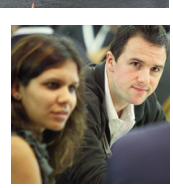
Visit WPDevCon.net for a full list of speakers, bios, classes, workshops, and special events!



Learn, network, and seize the **opportunities** that Windows Phone represents.







Register Early for the **biggest discounts!** at www.WPDevCon.net

Produced by BZ Media SD Times @WPDevCon

QUANTUM COMPUTERS AND INFORMATION SECURITY:

SHOR'S ALGORITHM AND THE FUTURE OF RSA

IAN T. DURHAM

The backbone of information security in the digital age is cryptography. Originally restricted to military purposes, the advent of ATMS and the increasing ubiquity of computers in business led to the development of the first public cryptosystem standard in the 1970s. The Data Encryption Standard (DES) was developed by the United States' National Bureau of Standards (now the National Institutes of Standards and Technology or NIST), modified behind the scenes by the US National Security Agency (NSA), and published in 1975. DES was ultimately cracked by the Electronic Frontier Foundation (EFF) in 1998 and has since been replaced by the Advanced Encryption Standard (AES) also developed by what is now NIST.

In both DES and AES, the receiver and sender must share a secret key. It is the sharing of this secret key that presented one of the greatest hurdles to implementation. How could two parties, who had never met, agree on a secret key without tipping off anyone else? An electronic version of a one-time pad would be ideal but difficult to implement. In 1976 recent MIT graduate Whitfield Diffie and Stanford professor Martin Hellman developed a solution. The Diffie-Hellman public key exchange was based on the idea that the two communicating parties would *split* the key. Mathematically they employed modular exponentiation in such a way that breaking the key would require solving what is known as the *discrete log problem*. The two communicating parties would choose two prime numbers, *p* and *g*, that combine in such a way that an eavesdropper would be overwhelmed by the number of possible solutions to the discrete log problem. In other words, Diffie-Hellman public key exchange had something in common with simple combination locks - the security of the system was based on the enormous number of possible solutions, i.e. brute force.

Seeking a different approach, Ron Rivest, Len Adleman, and Adi Shamir of the MIT computer science department, were seeking a function that was easy to compute but hard to "undo." They hit upon the idea of multiplying two large prime numbers, of roughly the same size, together to get an even larger integer; the integer is easy to obtain but factoring it into a product of two large, roughly equal primes is quite difficult. The RSA approach (whose letters stand for the developers' surnames) was developed in 1977 and included the first instance of the now-standard terminology of Alice, Bob, and Eve for the two communicating parties and eavesdropper respec-

tively. In comparison to the Diffie-Hellman approach, the RSA approach relies on two mathematically difficult procedures: factoring a large integer into two large, roughly equal primes and what is now known as the RSA problem in which one must find the roots of an arbitrary number, modulo *N* where *N* is large[1].

Over the years, numerous attacks have been waged against RSA, some of them successful, but the overall security remains high, particularly when augmentations are included to fight some of these specific attacks. Nevertheless, it is thought that only partial decryption is possible and various padding schemes have been developed to protect against these. Part of the reason RSA is so secure is that no algorithm is known to exist for classical computers that can factor a large integer into two large, roughly equal prime numbers in *polynomial time*. The best known classical algorithm, the general number field sieve (GNFS), is not even *quasi*-polynomial in time (it is, in fact, sub-exponential).

In 1994, however, MIT's Peter Shor discovered that a *quantum* computer *could* solve the integer factorization problem in polynomial time. The reason for this is due to something known as *quantum parallelism*. In classical computers, data is, of course, stored in bits (binary digits) that can have values of 0 or 1. Quantum mechanics, however, allows for the existence of *superpositional* states. As such, *quantum* bits - qubits, as they are called[2] – can have not only the values 0 and 1 but also a simultaneous combination (superposition) of 0 and 1. It is possible to interpret this as saying that a qubit can have values of both 0 and 1 at the same time, but it should be noted that when one *measures* a qubit in order to determine its value, the result is always *either* a 0 *or* a 1, never both. The difference is that the measurement of qubits is a *probabilistic* process. So, for instance, the general state of a qubit, prior to measurement, can be written as

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle$$

where the symbol $|\cdot\rangle$ represents a state and c_n represents a complex number whose square gives the probability of the associated state. This tells us that, upon measurement, we will get $|0\rangle$with a probability of $(c_1)^2$ % and $|1\rangle$ with a probability of $(c_2)^2$ %. Some people also interpret this as telling us that, prior to measurement, the qubit is in a state that consists of $(c_1)^2$ % $|0\rangle$ and $(c_2)^2$ % $|1\rangle$.

In other words, imagine we have a box and in that box could be either a man or a bull with some probability. When we open the box, we either see either a man or a bull and the outcome of the experiment (opening the box) depends on the associated probabilities of the two states - man and bull. Some people, however, interpret this as saying that, before the box is opened, the state is actually something resembling a centaur, the mythic half-man, half-bull, that then becomes either a man or a bull when the box is opened. At any rate, whatever one's beliefs about the state of the qubit, this superposition is not quite what is meant by quantum parallelism, however.

It turns out that in quantum mechanics, quantum objects can be correlated in non classical ways. So, imagine we have a bag that contains two marbles and suppose one is red and the other is blue. If Alice reaches in and pulls out one marble, but doesn't look at it, and Bob does the same, regardless of when either one of them looks at their marbles, if Alice sees that hers is red, Bob instantly knows his is blue. There is nothing terribly mysterious about this. An analogous quantum experiment, however, would be that the marbles do not actually possess a color and Alice and Bob may choose to *either* "measure" red/blue *or* black/yellow. If Alice and Bob happen to choose the same measurement, they are guaranteed to get opposite results (i.e. they can't both find a blue marble). In quantum mechanics these marbles would be said to be "entangled." *This* is quantum parallelism and it basically means you can do a lot more with a qubit than you can with a classical bit, but you pay the price for it in the fact that the operations are probabilistic.

So what does all this mean in terms of Shor's algorithm and RSA? Shor's algorithm makes use of a clever mathematical approach to factoring that arises in modular arithmetic. Suppose the number we wish to factor is *M*. We can, at random, choose an integer *a* such that $1 < a < M$. Now consider a function,

$$f(x)=a^x \bmod M$$

for $x = 1,2,..$ that has a period of $r \leq M$. It turns out that if one can find the period, *r*, one can successfully factor *M* into two, roughly equal prime numbers. As previously noted, no classical algorithm is known to exist that could solve this problem in polynomial time. But here's how Shor's algorithm and the power of quantum computing can do it.

Through a series of operations, a quantum computer can be brought into a superposition of many distinct quantum states where each state expresses both a value of *x* and the corresponding value of $f(x)$. In other words, a quantum computer can *simultaneously* hold numerous values of *x* and $f(x)$. Think of the examples with the marbles. In a classical computer, only one type of measurement can be made at a time. So, for instance, if it is a red/blue measurement and Alice finds a red marble, Bob can *only* find a blue marble. But if the marbles were quantum, Bob could choose to measure black/yellow while Alice measures red/blue.

Now, once the quantum computer is in this superposition, a quantum Fourier transform is performed that allows for the extraction of information regarding the period, *r*. In order to maximize the probability that we can obtain the period in this manner, we must compute the value of $f(x)$ over many periods. Since a quantum computer can be in a superposition of many values of *x* and $f(x)$, it can do this for many periods *simultaneously*. Incidentally, it turns out that a sufficiently high success rate can be achieved if we choose the maximum value of *x* to be approximately M^2.

The actual steps carried out in the execution of the algorithm are fairly complex and implementation can depend on the type of quantum computer being used. Classical computers are fairly standard in their form. Certainly the various internal aspects of the microchips and circuit boards may be a little different, but the point is that they're all built from the same parts - resistors, wires, capacitors, transistors, etc. In short, classical bits are almost universally manifested as some sort of voltage difference. Quantum bits can be lots of things.

A discussion of the various implementations of quantum computers is worthy of an article unto itself. What's important for the information security community is to know how close we are to achieving a large-scale quantum computer. Shor's algorithm itself was first implemented by a group at IBM in 2001 on a quantum computer with 7 qubits, though it was only able to factor the number 15 into 3 and 5. This implementation utilized nuclear magnetic resonance (NMR) technology at its core. Several groups utilizing different imple- mentation techniques have reproduced these results. In 2011 a group

from the University of Bristol managed to factor the number 21 using an optical approach. While these numbers may be too small for practical purposes, many of the implementations have merely been proof-of-concept.

The first commercially available quantum computer is D-Wave's One system, a 128-qubit quantum computer that utilizes an approach known as adiabatic quantum computing[3]. D-Wave's system, however, demonstrates just how different quantum computing is from classical computing. As a machine, it is really best used for machine-learning tasks. In fact, Google used D-Wave's system to improve aspects of Street-View in recent years. But, given the way the computer operates, it is less ideal for implementations of something such as Shor's algorithm. In other words, quantum computers are somewhat contextual in their design in that, though powerful, they may not (yet) prove to be terribly versatile.

All implementations of quantum computing fall into one of four models of quantum computation. The *quantum gate array* implementation most resembles a classical computer in that it uses quantum logic gates that are somewhat analogous to the similar classical gates seen in classical computation. A *one-way* or *cluster-state* quantum computer decomposes the computation into a series of single-qubit measurements made on a highly entangled initial state, i.e. a cluster state. *Adiabatic* quantum computation, as implemented in D-Wave's system, decomposes the computation into a slow, continuous transformation of an operator called a Hamiltonian from an initial state to a final state whose ground state includes the solution. *Topological* quantum computing decomposes the computation into the braiding of particles called anyons that are two-dimensional generalizations of fermions and bosons.

The question for the information security community, then, is what happens to algorithms such as RSA when quantum computing reaches maturity (it is a very young field at this point)? Luckily quantum mechanics provides an answer to that as well via quantum cryptography which, though still in its nascent stages, already provides commercially available products. Quantum cryptography relies on the fact that making a measurement in quantum mechanics necessarily disturbs the system. Thus an eavesdropper can be identified in a fairly straightforward manner, though all the results still must be turned into classical results (since our perception of them is classical) and this leaves room for some loopholes that are slowly being patched up. Nevertheless, it is at least reassuring that quantum mechanics is providing both the problem and its solution generally together.

Further reading:

- *Protecting Information: From Classical Error Correction to Quantum Cryptography* by Susan Loepp and William K. Wootters, Cambridge University Press, 2006.
- *Quantum Computer Science: An Introduction* by N. David Mermin, Cambridge University Press, 2007.
- *Quantum Processes, Systems, & Information* by Benjamin Schumacher and Michael Westmoreland, Cambridge University Press, 2010.
- *Quantiki*, an on-line encyclopedia (Wiki) of quantum information: *http://www.quantiki.org/wiki/Main Page*
- *Qunet Wiki: Quantum Computation and Quantum Error Prevention*, an on-line resource for quantum computing and error correction: *http://qunet.physics.siu.edu/wiki/index.php5/Quantum_Computation_and_Quantum_Error_Prevention*

---

[1] It can be shown mathematically that RSA is actually a generalization of the Diffie-Hellman approach.

[2] Ben Schumacher of Kenyon College coined the term during a somewhat light-hearted discussion with Bill Wootters of Williams College on a drive to the airport. The name stuck. Cornell University's David Mermin has argued that it should more properly be written 'Q-bit' and not 'qubit' but the former has not gained traction.

[3] There has been considerable debate over D-Wave's system over the years. Many have claimed it is not a true quantum computer. However, it is presently being independently tested at UCLA in a project funded by the Lockheed-Martin Corporation who purchased one. Preliminary results seem to indicate that it is, indeed, operating under quantum conditions.


University of Advancing Technology
UAT
Learn. Experience. Innovate.
UAT's coveted Bachelor of Science degree in Network Security is a vital national resource
One of the most prestigious Network Security programs in the country
We will teach you the concepts of security by design, and layered security to protect against exploitation of networks and data
UAT has been designated as a Center for Academic Excellence in Information Systems Security Education by the US National Security Agency
THEY SELDOM SMILE AT THE NSA. CAN YOU MAKE THEM GRIN?
Learn how to synthesize and apply these vital skills and leadership ability to succeed in the fast moving field of Network Security.
Bachelor of Science
Network Engineering
Network Security
Technology Forensics
Master of Science
Information Assurance
Program accreditations, affiliations and certifications:
ACCREDITED
The Higher Learning Commission
MEMBER
For more information: www.ncahlc.org
CLUSTERGEEK WITH CAUTION
LEARN, EXPERIENCE AND INNOVATE WITH THE FOLLOWING DEGREE STUDENTS: Advancing Computer Science, Artificial Life Programming, Digital Media, Digital Video, Enterprise Software Development, Game Art and Animation, Game Design, Game Programming, Human-Computer Interaction, Open Source Technologies, Robotics and Embedded Systems, Serious Game and Simulation, Strategic Technology Development, Technology Product Design, Technology Studies, Virtual Modeling and Design, Web and Social Media Technologies
Prepare to Defend!
www.uat.edu
877.828.4335
GEEK 411 AD
PLEASE SEE WWW.UAT.EDU/FASTFACTS FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS.

VARIANT DOUBLE PATH SIMULATION

– RESOLVING MYSTERIES & WAVE-PARTICLE PARADOXES IN QUANTUM INTERACTIONS

JEFFREY ZHI J. ZHENG, JIE-AO ZHU & JIE WAN

Abstract – It is a top intelligent challenge to explain quantum interactive behaviors consistently using experimental evidences. Wave-particle paradoxes forced this type of formal discussions and historical Bohr-Einstein debates without a common solution from 1900s and still an open question in modern quantum foundation. Using advanced variant logic and measurement construction, it is feasible to identify complex quantum interactions under multiple/conditional probability into a series of symmetry/anti-symmetry and synchronous/asynchronous conditions. In addition to theoretical analysis and explorations, an online prototype *http://vdps.sinaapp.com/single/* focus on simulation of single function has established to illustrate controllable combinations among possible parameters to generate interactive results with a total of 7680 configurations. Main principles and architectures of the simulation prototype are discussed and key components and modules are illustrated. Sample interactive results from two polarized/separated paths and either double path for particles or double path for waves are organized into four groups of results for both single functions and global matrix representations.

Introduction

From 1900, Planck proposed quanta to explain black body radiation using a discrete approach [2,11,12]. During successful developments and applications over a century, modern Quantum Mechanics are still faced severe challenges on foundation from theories and experiments [2,11-17]. In addition to Heisenberg Uncertain Principle and Bohr Complementary for quantum foundation [14-16,19], how to explain particle and/or wave behaviors in quantum interactions are key clues from theoretical and experimental aspects [10-17,19].

People implemented many experiments to distinguish quantum interactive behaviors as particles and/or waves can be trace back to Newton time [15,16]. Isaac Newton (1642-1727) used particle concepts to explain his optical theory and experiments to simulate light as small dusts [14-16]. Thomas Young (1773-1829) proposed Double Slit Experiment DSE to illustrate wave interactive behaviors in interference patterns [14-16].

After Planck historical discovery on quanta, Einstein in 1905 proposed photo-electric effects using the quanta model. This is a

strengthen effort on wave particle paradoxes for quantum foundation [14-16]. In 1923, de Broglie proposed Wave-Particle duality [6], Heisenberg and Schrödinger developed Matrix Mechanics and Wave Functions for Quantum Mechanics [14-17]. After advanced developments and applications for a century [15-17,19], it is interesting to notice that even through great debates between Bohr and Einstein [4,5,7,14-17] both classical problems in quantum foundation and various interpretations on evidences from supporting experiments are still in open questions [2,15,16,20].

In relation to Wave-particle issue, neither precise experiments nor refined simulation devices are available to generate consistent results conveniently to separate two distinct aspects into a series of identified controllable conditions [2,15-17].

Since Thomas Young and other classical DSEs are extremely important in this direction [2,10,11,15-17], it is necessary for us to discuss relevant modern DSE versions in further details.

Mach-Zehnder Device

Using optical fiber and Laser devices, classical DSEs have a modern representative as Mach-Zehnder Double Path Device DPD [2,14-16] shown in Figure 1. Physical device is shown in Fig. 1(a) and its description model is shown in Fig.1(b).

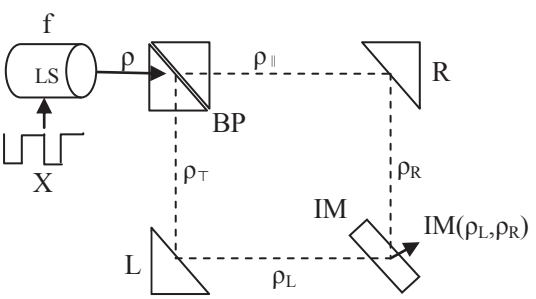
Interaction of Mach-Zehnder DPD can be described as follows.

Light Source (Laser) LS with function f using electric pulse X makes LS output photon flow ρ. This flow passes Bi-Prism BP, two polarized flows $\rho_{\parallel}$ and $\rho_{\top}$ are separated as BP output. Mirrors L and R reflect flows via Left and Right paths to generate two controllable path flows ρ_L and ρ_R respectively. Both controllable flows are merged by IM as Interactive Measurements to form the final output of the DPD.

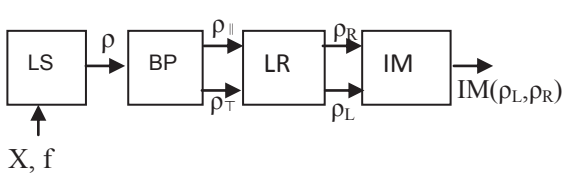
Similar language expression can be used to describe flows using description model. They have equivalent properties in principle.

Feynman models for quantum interactions

Richard Feynman proposed his idea experiments for quantum interactions in 1940s and expressed models well in his popular books [8] in 1965.



(a) Mach-Zehnder Double Path Device



(b) Description Model

X	Pulsed Input	f	Control Function
LS	Light Source	BP	Bi-Prism
ρ	Photon Flow	L,R	Left, Right Path
ρ_l, ρ_r	Polarized Flows		
ρ_L, ρ_R	Left, Right Path Flow		
IM	Interactive Measurements		
$IM(\rho_L,\rho_R)$	Results		

(c) Notations

Figure. 1 Double Path Model (a) Mach-Zehnder Double Path Model (b) Description Model (c) Symbol Notations

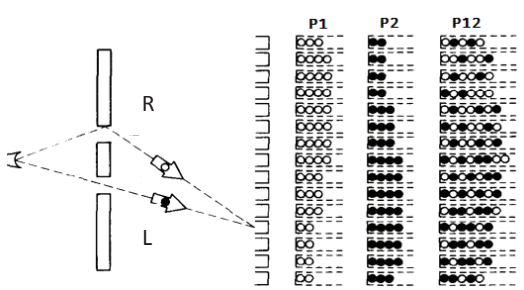
From a visual viewpoint, Hey and Walter's book "The New Quantum Universe" [11] described two Feynman models in interesting forms shown in Figure 2(a-b). Output probability measurements in Fig. 2(a) claim particle properties to satisfy P12 = P1+P2;

however output probability measurements in Fig. 2(b) show wave properties with P12 ≠ P1+P2.

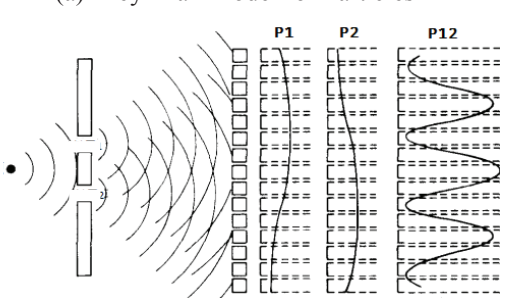
Feynman models provide statistically significant characteristics [1,10-17,20] to distinct two types of distributions corresponding to either particles or waves interactions under DSE environments.

Variant Logic and Measurement Construction

Early version of variant construction developed as the conjugate classification and transformation from 1990s using balanced approaches to handle state classification and transformation on binary images on plane lattices [26]. In 2010, two vector operations: permutation and complementary are expanded into state spaces to make two operations on bit vector with 2^{2^n} elements. Under this extension, variant logic construction has being proposed [26,29,30]. To apply variant logic on different applications, it is natural to use this new approach to simulate various quantum interactions, a list of theoretical and simulation results published [21-28].



(a) Feynman Model for Particles



(b) Feynman Model for Waves

Figure 2 Feynman Interactive Models (a) Particles (b) Waves

Target of this paper

It is difficult for most people to manipulate abstract construction via a list of boring definitions from foundation [3,9,18]. For easier understanding on variant construction, a simulation prototype is proposed for an online version http://vdps.sinaapp.com/single/ to let more people make their selections themselves to observe interference results conveniently. Under this consideration, briefly samples and descriptions are discussed on architecture and key component levels for the prototype. Following given samples and procedures, users with limited skills could control this type of online versions without difficulties. For advanced researchers and academic scholars with sufficient theoretical & methodical background, this prototype could provide a useful simulator for them to observe each controllable interaction in accurate details to separate complex operation as a series of combinations to explore top intelligent challenges and historical mysteries on quantum interactive behaviors under variant simulation mechanism.

In consequent sections, simulation architecture and procedure are described in Section II, Simulation principles are discussed in Section III, Typical selections are illustrated in section IV and further descriptions are discussed in Section V.

Simulation Architecture and Procedure

Architecture

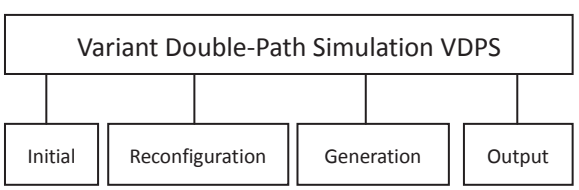
The architecture of Variant Double Path Simulation VDPS is composed of four components: Initial, Reconfiguration, Generation and Output shown in Figure 3(a-c) respectively.

Initial

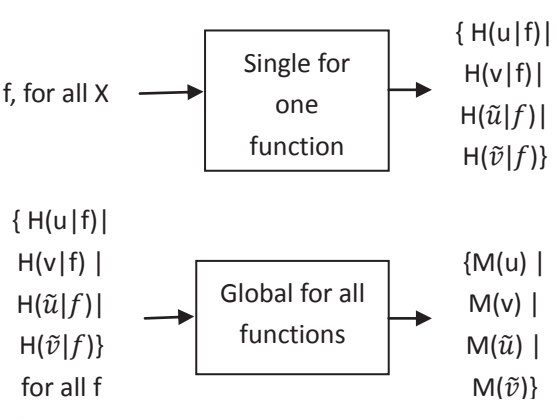
Initial component provides a default configuration for prototype as an initial condition of an entry point.

Reconfiguration

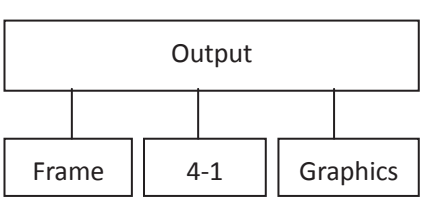
Reconfiguration component provides all feasible parameters for variation to make a certain selection as a set of legal control parameters. When relevant parameters are selected, enabled Process button can be pressed, new configuration could be recreated and their distributions are outputted and organized via Generation and Output components.



(a) Architecture



(b) Generation Component



(c) Output component

Figure 3. VDPS Architecture & Key Components (a) Architecture (b) Generation Component (c) Output Component

Generation

Generation component is composed of two modules: Single and Global. It is the core part of the simulation system to use parameters prepared in either Initial or Reconfiguration component. Single module in Figure 3(b) works for single function f and its N bit vector X exhausted all 2^N elements as input. Under either Symmetry or Anti-symmetry condition, four sets of vector distributions {H(u|f) | H(v|f) | H($\tilde{u}|f$) | H($\tilde{v}|f$)} under either multiple {H(u|f) | H(v|f)} or conditional {H($\tilde{u}|f$) | H($\tilde{v}|f$)} probability to indicate Left Path L-P, Right Path R-P, Double Path for Particles D-P and Double Path for Waves D-W respectively as output results. For a given set of conditions, four distributions of {L-P, R-P, D-P, D-W} are generated as a group. Four groups of 16 distributions can be separated by Interaction: Multiple or Conditional and Parity: Symmetry or Anti-symmetry respectively.

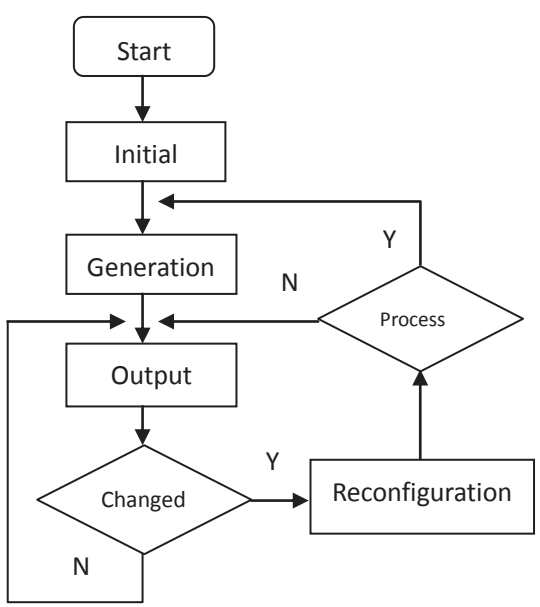


Figure 4. Procedure of VDPS

Under Global module in Figure 3(b), distributions of {H(u|f) | H(v|f) | H($\tilde{u}|f$) | H($\tilde{v}|f$)} for all functions are provided as input, for a given FC, four matrices can be illustrated as SL, W, F and C schemes to show all 16 function's distributions exhaustive generated

four groups of {M(u) | M(v) | M($\tilde{u}$) | M($\tilde{v}$)} as 4x4 matrices in L-P, R-P D-P and D-W forms respectively. Under this organization, a list of Symmetry /Anti-symmetry, Multiple /Conditional probability distributions on relevant matrices can be identified.

Results of either a single function or a selected global configuration will be organized by Output component for visualization.

Output

Output component is shown in Figure 3(c) to be composed of three modules: Frame, 4-1 and Graphics to support people to illustrate either one distribution or four distributions in one frame for either a single function or one of four global configurations, in addition to some Graphics features for output control.

Procedure of VDPS

The procedure of VDPS is shown in Figure 4. In this procedure, the first output is based on initial condition via Generation and Output components to represent results. If there is any change on any parameter, control of the Procedure will pass to Reconfiguration to enable Process button. Then it is necessary for user to press the Process button to push parameters into Generation and Output components for the selected configuration. Under normal environment, this procedure will be continued for the user to support explorations on various selections online.

Simulation Principles

Using variant principle described in the following subsections, for a N bit 0-1 vector X and a given logic function f, all N bit vectors are exhausted and variant measures generate four groups of histograms [21-30]. The main principles of Generation in variant simulation prototype shown in Figure 3(b) needs to be discussed in further details.

In Fig 3(b), Single module is composed of three stages: Pre-process, Interaction and Post-process. At the pre-process stage, a N bit 0-1 vector X and a function f feed into output two signals $\rho(\tilde{\rho})$. After an interactive process, four groups of signal vectors are identified: $u(\tilde{u})$ for symmetry group and $v(\tilde{v})$ for anti-symmetry group. In the post-process stage, all N bit vectors are processed by pre-processing and interactive stages until all of the 2^N data set has been processed to transform symmetry and anti-symmetry signals into a total of 16 histograms: eight for symmetry distributions and another eight for anti-symmetry distributions respectively.

In the interaction stage, input two signals $\rho(\tilde{\rho})$ processed by BP to generate four signals $\{\rho_-,\rho_+\}(\{\tilde{\rho}_-,\tilde{\rho}_+\})$. LR output eight signals

$$\{\rho_-,(1-\rho_-)/2,\rho_+,(1+\rho_+)/2\}$$
$$\left(\{\tilde{\rho}_-,(1-\tilde{\rho}_-)/2,\tilde{\rho}_+,(1+\tilde{\rho}_+)/2\}\right)$$

though IM to generate four groups of signals $u(\tilde{u})$ and $v(\tilde{v})$ respectively.

Variant Principle

The variant principle is based on n-variable logic functions [26,29,30]. For any n -variables, $x = x_{n-1}...x_i...x_0$, $0 \le i < n$, $x_i \in \{0,1\} = B_2$. Let a position j be the selected bit $0 \le j < n$, $x_j \in B_2$ be the selected variable. Let output variable y and n -variable function $f, y = f(x)$, $y \in B$ $x \in B$ For all states of x, a set $S(n)$ composed of the 2^n states can be divided into two sets: $S_0^j(n)$ and $S_1^j(n)$.

$$\begin{cases} S_0^j(n)=\{x \mid x_j=0, \forall x \in B_2^n\} \\ S_1^j(n)=\{x \mid x_j=1, \forall x \in B_2^n\} \\ S(n)=\{S_0^j(n), S_1^j(n)\} \end{cases}$$

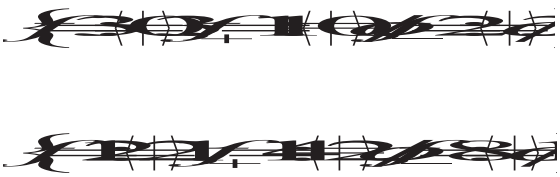
For a given logic function f, there are input and output pair relationships to define four meta-logic functions $\{f_\perp, f_+, f_-, f_T\}$:

$$\begin{cases} f_\perp(x)=\{f(x) \mid x \in S_0^j(n), y=0\} \\ f_+(x)=\{f(x) \mid x \in S_0^j(n), y=1\} \\ f_-(x)=\{f(x) \mid x \in S_1^j(n), y=0\} \\ f_T(x)=\{f(x) \mid x \in S_1^j(n), y=1\} \end{cases}$$

Two logic canonical expressions: AND-OR form is selected by $\{f_+(x), f_T(x)\}$ as y = 1 items, and OR-AND form is selected from $\{f_-(x), f_\perp(x)\}$ as y = 0 items. Considering $\{f_T(x), f_\perp(x)\}$, $x_j = y$ items, they are invariant themselves.

To select $\{f_+(x), f_-(x)\}$; $x_j \neq y$ forming variant logic expression. Let $f(x)=\langle f_+ \mid x \mid f_- \rangle$ be a variant logic expression. Any logic function can be expressed as a variant logic form. In $\langle f_+ \mid x \mid f_- \rangle$ structure, f_+ selected 1 items in $S_0^j(n)$ as same as the AND-OR standard expression, and f_- selecting relevant parts the same as OR-AND expression 0 items in $S_1^j(n)$. For a convenient understanding of variant representation, 2-variable logic structures are illustrated for all 16 functions in Table 1.

E.g. Checking two functions f = 3 and f = 12 :



Variant Measures

Let Δ be variant measure function [21-27].

Let

$$x^v=\begin{cases} \perp, & x=0, y=0; \\ +, & x=0, y=1; \\ -, & x=1, y=0; \\ \mathrm{T}, & x=1, y=1. \end{cases}$$

$$x^\delta=\begin{cases} x, & \delta=1; \\ \bar{x}, & \delta=0. \end{cases}$$

It is convenient to transfer n=2 logic functions into their variant forms in Table 1 to list four meta functions for each partition respectively.

For any given n-variable state there is one position in $\Delta f(x)$ to be 1 and the other 3 positions are 0.

For any N bit 0-1 vector X;

$$X=X_{N-1}...X_J...X_0, 0 \le J < N, X_J \in B_2, X \in B_2^N$$

under n-variable function f, n bit 0-1 output vector Y,

$$Y=f(X)=\langle f_+ \mid X \mid f_- \rangle, \quad Y=Y_{N-1}...Y_J...Y_0,$$

$$0 \le \mathrm{J} < N,\ Y_\mathrm{j} \in B_2,\ Y \in B_2^N.$$

For the J-th position be $x^{\mathrm{J}} = [...X_{\mathrm{J}}...] \in B_2^n$ to form $Y_{\mathrm{J}} = f(x^{\mathrm{J}}) = \langle f_+ \mid x^{\mathrm{J}} \mid f_- \rangle$, let N bit positions be cyclic linked. Variant measures of $f(X)$ can be decomposed

$$\Delta\langle X:Y\rangle = \Delta f(X) = \sum_{J=0}^{N-1} \Delta f(x^J) = \langle N_\perp, N_+, N_-, N_T \rangle$$

as a quaternion $\langle N_\perp, N_+, N_-, N_T \rangle$.

E.g. $N = 10$, given f, $Y = f(\mathrm{X})$.

X	=	0	1	1	0	0	1	1	1	0	0
Y	=	1	0	1	0	1	0	1	0	1	0
Δ(X :Y)	=	+	-	⊤	⊥	+	-	⊤	-	+	⊥

$$\Delta f(X) = \langle N_\perp, N_+, N_-, N_T \rangle = \langle 2,3,3,2 \rangle, N = 10$$

Input and output pairs are 0-1 variables with four combinations. For any given function f, the quantitative relationship of $\{\perp, +, -, T\}$ is determined directly from input/output sequences.

Measurement Equations

Using variant quaternion, signals are calculated by the following equations. For any N bit 0-1 vector X, function f, under Δ measurement: $\Delta f(x) = \langle N_\perp, N_+, N_-, N_T \rangle$,

$N = N_\perp + N_+ + N_- + N_T$.

Equations for Multiple Probability Measurements

Multiple probability Signal ρ is defined as follows [21,24,25].

Using $\{\rho_{\mathrm{L}}, \rho_R\}, \rho_{\mathrm{L}} \neq \rho_R; \rho_{\mathrm{L}}, \rho_R \in \{\rho_\perp, \rho_+, \rho_-, \rho_T\}$, it is feasible to select two signals for both Left and Right Paths. There are six configurations noted as {L0:R1, L0:R2, L0:R3, L1:R2, L1:R3, L2:R3} respectively.

Each pair has following correspondence:

L0:R1= $\{\rho_\perp, \rho_+\}$, L0:R2= $\{\rho_\perp, \rho_-\}$,

L0:R3= $\{\rho_\perp, \rho_T\}$, L1:R2= $\{\rho_+, \rho_-\}$,

L1:R3= $\{\rho_+, \rho_T\}$, L2:R3= $\{\rho_-, \rho_T\}$

Under such condition from a pair of selected multiple probability signals, a pair of interactive signals $\{u, v\}$ with either symmetry or anti-symmetry property can be formulated:

$$\begin{cases} u = \langle u_L, u_R, u_0, u_1 \rangle = \{u_\beta\} \\ v = \langle v_L, v_R, v_0, v_1 \rangle = \{v_\beta\} \end{cases}$$

Symbol $\beta \in \{L, R, 0, 1\}$ indicates four different output results on L: Left Path L-P, R: Right Path R-P, 0: Double Path for Particles D-P and 1: Double Path for Waves D-W respectively.

$$\begin{cases} u_L = \rho_L \\ u_R = \rho_R \\ u_0 = u_L \oplus u_R \\ u_1 = u_L + u_R \\ v_L = (1 + \rho_L)/2 \\ v_R = (1 - \rho_R)/2 \\ v_0 = v_L \oplus v_R \\ v_1 = v_L + v_R - 0.5 \end{cases}$$

Where $0 \le u_\beta, v_\beta \le 1$, $\beta \in \{L, R, 0, 1\}$, $\oplus$: Asynchronous addition, {+, -}: Synchronous addition and subtraction operations.

Using $\{u, v\}$ signals, each u_β (v_β) determines a fixed position in relevant histogram to make vector X on a position.

After completing 2^N data sequences, eight symmetry/anti-symmetry histograms of $\{H(u_\beta \mid f)\}$ $(\{H(v_\beta \mid f)\})$ $\beta \in \{L,R,0,1\}$ are generated.

Equations for Conditional Probability Measurements

Conditional probability Signal $\tilde{\rho}$ is defined as follows [22,23,27]. Different from multiple probability measurements, two separated measures for either 0 or 1 number are required.

$$N_0 = N_\perp + N_+, N_1 = N_- + N_T$$

$$\tilde{\rho} = \langle \tilde{\rho}_\perp, \tilde{\rho}_+, \tilde{\rho}_-, \tilde{\rho}_T \rangle = \left\langle \frac{N_\perp}{N_0}, \frac{N_+}{N_0}, \frac{N_-}{N_1}, \frac{N_T}{N_1} \right\rangle$$

Where $\tilde{\rho}_\alpha, 0 \le \tilde{\rho}_\alpha \le 1,$ $\alpha \in \{\perp, +, -, T\}$

Using

$\{\tilde{\rho}_L, \tilde{\rho}_R\}, \tilde{\rho}_L \ne \tilde{\rho}_R; \tilde{\rho}_L, \tilde{\rho}_R \in \{\tilde{\rho}_\perp, \tilde{\rho}_+, \tilde{\rho}_-, \tilde{\rho}_T\}$, it is feasible to select two signals for both Left and Right Paths. In this condition, there are four configurations noted as {L0:R2, L0:R3, L1:R2, L1:R3} respectively.

Each pair has following correspondence:

L0:R2=$\{\tilde{\rho}_\perp, \tilde{\rho}_-\}$, L0:R3=$\{\tilde{\rho}_\perp, \tilde{\rho}_T\}$,

L1:R2=$\{\tilde{\rho}_+, \tilde{\rho}_-\}$, L1:R3=$\{\tilde{\rho}_+, \tilde{\rho}_T\}$

Under such condition from a pair of selected multiple probability signals, a pair of interactive signals $\{\tilde{u}, \tilde{v}\}$ with either symmetry or anti-symmetry property can be formulated:

$$\begin{cases} \tilde{u} = \langle \tilde{u}_L, \tilde{u}_R, \tilde{u}_0, \tilde{u}_1 \rangle = \{\tilde{u}_\beta\} \\ \tilde{v} = \langle \tilde{v}_L, \tilde{v}_R, \tilde{v}_0, \tilde{v}_1 \rangle = \{\tilde{v}_\beta\} \end{cases}$$

Symbol $\beta \in \{L,R,0,1\}$ indicates four different output results on Left Path L-P, Right Path R-P, Double Path for Particles D-P and Double Path for Waves D-W respectively.

$$\begin{cases} \tilde{u}_L = \tilde{\rho}_L \\ \tilde{u}_R = \tilde{\rho}_R \\ \tilde{u}_0 = \tilde{u}_L \oplus \tilde{u}_R \\ \tilde{u}_1 = (\tilde{u}_L + \tilde{u}_R)/2 \\ \tilde{v}_L = (1 + \tilde{\rho}_L)/2 \\ \tilde{v}_R = (1 - \tilde{\rho}_R)/2 \\ \tilde{v}_0 = \tilde{v}_L \oplus \tilde{v}_R \\ \tilde{v}_1 = \tilde{v}_L + \tilde{v}_R - 0.5 \end{cases}$$

Where $0 \le \tilde{u}_\beta, \tilde{v}_\beta \le 1$, $\beta \in \{L,R,0,1\}$, $\oplus$: Asynchronous addition, {+, -}: Synchronous addition and subtraction operations.

Using $\{\tilde{u}, \tilde{v}\}$ signals, each $\tilde{u}_\beta$ ($\tilde{v}_\beta$) determines a fixed position in relevant histogram to make vector X on a position. After completing 2^N data sequences, eight symmetry/anti-symmetry histograms of $\{H(\tilde{u}_\beta \mid f)\}$ $(\{H(\tilde{v}_\beta \mid f)\})$ $\beta \in \{L,R,0,1\}$ are generated.

Different Statistical Histograms

For a function f, all measurement signals are collected and the relevant histogram represents a complete statistical distribution [21,22]. Using $\{u, v, \tilde{u}, \tilde{v}\}$ signals, each signal selected from $\{u_\beta, v_\beta, \tilde{u}_\beta, \tilde{v}_\beta\}$ determines a fixed position in the relevant histogram to make vector X on a position. After completing 2^N data sequences, a total of sixteen symmetry /anti-symmetry with multiple/conditional probability histograms of $\{H(u_\beta|f), H(v_\beta|f), H(\tilde{u}_\beta|f), H(\tilde{v}_\beta|f)\}$ could be generated as follows.

For a function $f, \beta \in \{L, R, 0, 1\}$

$$\begin{cases} H(u_\beta|f) = \sum_{\forall X \in B_2^N} H(u_\beta|f(X)) \\ H(v_\beta|f) = \sum_{\forall X \in B_2^N} H(v_\beta|f(X)) \\ H(\tilde{u}_\beta|f) = \sum_{\forall X \in B_2^N} H(\tilde{u}_\beta|f(X)) \\ H(\tilde{v}_\beta|f) = \sum_{\forall X \in B_2^N} H(\tilde{v}_\beta|f(X)) \end{cases}$$

Global Matrix Representations

After local interactive measurements and statistical process are undertaken for a given function f, 16 histograms are generated. The Global Matrix Representation in the Generation component performs its operations into two stages. In the first stage, exhausting all possible 16 functions for each distinct selection to generate eight sets, each set contains 16 elements and each element is a histogram.

In the second stage, following FC information arranging all 16 elements generated as a 4x4 matrix by one of the four SL, W, F and C code schemes. Under different coding schemes, it is feasible to observe selected Left and/or Right path signals to be polarized into Horizontal and Vertical relationships respectively.

Matrix and Its Elements

For a given coding scheme, let $f = \langle f^1 | f^0 \rangle$, each element

$$\begin{cases} M_{\langle f^1|f^0\rangle}(u_\beta|f) = H(u_\beta|f) \\ M_{\langle f^1|f^0\rangle}(v_\beta|f) = H(v_\beta|f) \\ M_{\langle f^1|f^0\rangle}(\tilde{u}_\beta|f) = H(\tilde{u}_\beta|f) \\ M_{\langle f^1|f^0\rangle}(\tilde{v}_\beta|f) = H(\tilde{v}_\beta|f) \end{cases}$$

Under this correspondence, 16 functions are located in relevant positions.

Representation Patterns of Matrices

Using n = 2, four given coding schemes are SL P(3210), W P(2103), F P(3201), C P (3102) conditions [21,22,26,29,30], each code case contains sixteen histograms arranged as a 4x4 matrix as follows.

$$\text{SL P}(3210) = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{pmatrix},$$

$$\text{W P}(2103) = \begin{pmatrix} 0 & 8 & 1 & 9 \\ 2 & 10 & 3 & 11 \\ 4 & 12 & 5 & 13 \\ 6 & 14 & 7 & 15 \end{pmatrix},$$

$$\text{F P}(3201) = \begin{pmatrix} 0 & 2 & 1 & 3 \\ 4 & 6 & 5 & 7 \\ 8 & 10 & 9 & 11 \\ 12 & 14 & 13 & 15 \end{pmatrix},$$

$$\text{C P}(3102) = \begin{pmatrix} 0 & 4 & 1 & 5 \\ 2 & 6 & 3 & 7 \\ 8 & 12 & 9 & 13 \\ 10 & 14 & 11 & 15 \end{pmatrix},$$

All matrices in this prototype use this set of four configurations for matrix patterns to represent their elements to show their global properties.

Typical Selections

Using http://vdps.sinaapp.com/single/ online prototype, it is feasible to try various selections in exploration. In convenient for users, it is useful to describe typical samples of possible configurations as follows. Current online version mainly supports single function in simulation with limited restrictions & refined versions will be provided to enhance prototype systems in future developments.

Legal selections

When any user makes a selection, six groups of legal parameters could be available for the prototype.

1. Vector length := N in {5-10};
2. Frame := {Single | Global};
   Single := a single function f in {0-15},
   Global := four code schemes {SL, W, F, C} , each one contains 16 functions;
3. Interaction := one of ten cases from {Multiple(L0:R1, L0:R2, L0:R3, L1:R2, L1:R3, L2:R3) | Conditional(L0:R2, L0:R3, L1:R2, L1:R3)};
4. Parity := {Symmetry | Anti-symmetry};
5. Output := {L-P, R-P, D-P, D-W, 4-1};

L-P := a frame for Left Path,
R-P := a frame for Right Path,
D-P := a frame for Double Path for Particles,
D-W := a frame for Double Path for Waves,
4-1 := a 2x2 matrix composed of $\begin{pmatrix} \text{L-P} & \text{R-P} \\ \text{D-P} & \text{D-W} \end{pmatrix}$ in one frame.

6. Graphics := $\{Color, Height\}$;
Color :={L-P, R-P, D-W},
$\{\text{L-P, R-P, D-W}\}_{\text{Color}}$:= {yellow, red, green, black, orange, blue, grey};
Height := {L-P, R-P, D-P, D-W};
$\{\text{L-P, R-P, D-P, D-W}\}_{\text{Height}}$:= {10-1000};

Selections of Frame=Global on C code scheme

It is difficult for people to understand four coding schemes without visual assistances. Relevant symbol representations are listed in Table 2 and six possible selections of {L0:R1, L0:R2, L0:R3, L1:R2, L1:R3, L2:R3} are used in this section to help users to illustrate various partitions and combinations in this prototype. Eight symbols {a={Φ}, b={0}, c={2}, d={2,0}} and { A={Φ}, B={3}, C={1}, D={3,1}} are used to represent corresponding eight sets of variant state combinations shown in Table 2. Since same projected function must have the same symbol representative corresponding to the same shape of a certain histogram distribution, this property could help users observe projected functions easily from L-P, R-P and D-P expressions in symbol expressions.

Using matrices of C code scheme, the matrix of P(3102) can be represented as follows.

$$M_C = \begin{pmatrix} 0 & 4 & 1 & 5 \\ 2 & 6 & 3 & 7 \\ 8 & 12 & 9 & 13 \\ 10 & 14 & 11 & 15 \end{pmatrix}$$

Using symbol expressions, four projected matrices are symbolized as follows.

$$(f_{\perp})_C = \begin{pmatrix} d & b & c & a \\ d & b & c & a \\ d & b & c & a \\ d & b & c & a \end{pmatrix}$$

$$(f_{+})_C = \begin{pmatrix} a & c & b & d \\ a & c & b & d \\ a & c & b & d \\ a & c & b & d \end{pmatrix}$$

$$(f_{-})_C = \begin{pmatrix} D & D & D & D \\ B & B & B & B \\ C & C & C & C \\ A & A & A & A \end{pmatrix}$$

$$(f_{T})_C = \begin{pmatrix} A & A & A & A \\ C & C & C & C \\ B & B & B & B \\ D & D & D & D \end{pmatrix}$$

It is interesting to notice that the first and second matrices are arranged within four symbols in vertical distributions and the third and fourth matrices within four symbols in horizontal distributions. This type of direct arrangements are only appeared in C code scheme and other SL, W and F code schemes cannot have such the simplest structure. Since numbers of complicated calculations are involved, users are suggested to manipulate this prototype initially to select N=5 or 6 first to reduce waiting time in generation. Many other selections are available in the prototype, it is convenient for users to do further explorations on other code schemes.

Using this set of four symbol matrices, six cases of symbol matrix combinations can be expressed as follows.

Case 1.

$$(\text{L0:R1})_C$$

$$= \left(\text{L0(f)}\right)_C \left| \left(\text{R1(f)}\right)_C \right. = (f_{\perp})_C \left| (f_{+})_C \right.$$

$$= \begin{pmatrix} d & b & c & a \\ d & b & c & a \\ d & b & c & a \\ d & b & c & a \end{pmatrix} \left| \begin{pmatrix} a & c & b & d \\ a & c & b & d \\ a & c & b & d \\ a & c & b & d \end{pmatrix} \right.$$

Case 2:

$$(\mathrm{L0:R2})_C$$

$$= \big(\mathrm{L0(f)}\big)_C \Big| \big(\mathrm{R2(f)}\big)_C = (f_{\perp})_C \Big| (f_{-})_C$$

$$= \begin{pmatrix} d & b & c & a \\ d & b & c & a \\ d & b & c & a \\ d & b & c & a \end{pmatrix} \Big| \begin{pmatrix} D & D & D & D \\ B & B & B & B \\ C & C & C & C \\ A & A & A & A \end{pmatrix}$$

Case 3:

$$(\mathrm{L0:R3})_C$$

$$= \big(\mathrm{L0(f)}\big)_C \Big| \big(\mathrm{R3(f)}\big)_C = (f_{\perp})_C \Big| (f_{T})_C$$

$$= \begin{pmatrix} d & b & c & a \\ d & b & c & a \\ d & b & c & a \\ d & b & c & a \end{pmatrix} \Big| \begin{pmatrix} A & A & A & A \\ C & C & C & C \\ B & B & B & B \\ D & D & D & D \end{pmatrix}$$

Case 4:

$$(\mathrm{L1:R2})_C$$

$$= \big(\mathrm{L1(f)}\big)_C \Big| \big(\mathrm{R2(f)}\big)_C = (f_{+})_C \Big| (f_{-})_C$$

$$= \begin{pmatrix} a & c & b & d \\ a & c & b & d \\ a & c & b & d \\ a & c & b & d \end{pmatrix} \Big| \begin{pmatrix} D & D & D & D \\ B & B & B & B \\ C & C & C & C \\ A & A & A & A \end{pmatrix}$$

Case 5:

$$(\mathrm{L1:R3})_C$$

$$= \big(\mathrm{L1(f)}\big)_C \Big| \big(\mathrm{R3(f)}\big)_C = (f_{+})_C \Big| (f_{T})_C$$

$$= \begin{pmatrix} a & c & b & d \\ a & c & b & d \\ a & c & b & d \\ a & c & b & d \end{pmatrix} \Big| \begin{pmatrix} A & A & A & A \\ C & C & C & C \\ B & B & B & B \\ D & D & D & D \end{pmatrix}$$

Case 6:

$$(\mathrm{L2:R3})_C$$

$$= \big(\mathrm{L2(f)}\big)_C \Big| \big(\mathrm{R3(f)}\big)_C = (f_{-})_C \Big| (f_{T})_C$$

$$= \begin{pmatrix} D & D & D & D \\ B & B & B & B \\ C & C & C & C \\ A & A & A & A \end{pmatrix} \Big| \begin{pmatrix} A & A & A & A \\ C & C & C & C \\ B & B & B & B \\ D & D & D & D \end{pmatrix}$$

In multiple probability conditions, all six cases are possible to generate six sets of distinct matrices and each set contains eight matrices to illustrate their global distributions in symmetry /anti-symmetry and synchronous /asynchronous conditions respectively.

However, in conditional probability conditions, four cases (Case 2 – Case 5) are satisfied essential conditions in listed equations for conditional interactions to generate four sets of distinct matrices and each set contains eight matrices to illustrate their global distributions in symmetry /anti-symmetry and synchronous /asynchronous conditions respectively.

Two cases of Case 1 and Case 6 need to be ignored for a pair of dependent measurements involved.

From a symbol representative review point, no different relationship between Multiple and Conditional can be observed, but under real interactive conditions, there are significant differences between two types of probability selections. Such differences are much easier for users to try the prototype on various selections observing significantly intrinsic differences.

Four groups in C coding scheme for N=12 are selected for four groups of matrices shown in Figure 5 (I-IV).

Group I.

N=12, Frame=Global, Interaction = Multiple(L1:R2), Parity=Symmetry, Output=4-1 in Figure 5(I).

Group II.

N=12, Frame=Global, Interaction = Multiple(L1:R2), Parity=Anti-symmetry, Output=4-1 in Figure 5(II).

Group III.

N=12, Frame=Global, Interaction = Conditional(L1:R2), Parity=Symmetry, Output=4-1 in Figure 5(III).

Group IV.

N=12, Frame=Global, Interaction = Conditional (L1:R2), Parity=Anti-symmetry, Output=4-1 in Figure 5(IV).

Four global selections are illustrated for people to show relevant global distribution characteristics as guide maps in exploration.

Typical selections on Frame=Single

Under this condition, more selections are available for users to control the prototype in detailed configurations.

Three groups with special pair properties can be identified from a 4x4 C code matrix and each group contains different members with overlap as follows.

1. Six Symmetry pairs: {0:15, 1:7, 2:11, 4:13, 6:9, 8:14}
2. Six Anti-symmetry pairs: {1:8, 2:4, 3:12, 5:10, 6:8, 7:14, 11:13}
3. Four special pairs: {0:15, 3:12, 5:10, 6:9}

Four groups of f=12 are selected and their 16 output results are shown in Figure 6(I-IV).

Group I.

N=8, Frame=Single, f=12, Interaction = Multiple (L1:R2), Parity=Symmetry, L-P_{color} = red, R-P_{Color} = blue, D-W_{Color} = black, {L-P, R-P, D-P, D-W}$_{Height}$ = 300, Output=4-1 in Figure 6(I).

Group II.

N=8, Frame=Single, f=12, Interaction = Multiple (L1:R2), Parity=Anti-symmetry, L-P_{color} = red, R-P_{Color} = blue, D-W_{Color} = black, {L-P, R-P, D-P, D-W}$_{Height}$ = 300, Output=4-1 in Figure 6(II).

Group III.

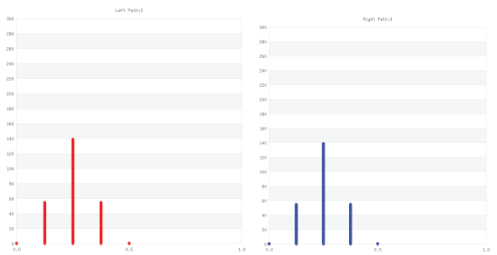
N=8, Frame=Single, f=12, Interaction = Conditional (L1:R2), Parity=Symmetry, L-P_{color} = red, R-P_{Color} = blue, D-W_{Color} = black, {L-P, R-P, D-P, D-W}$_{Height}$ = 300, Output=4-1 in Figure 6(III).

Group IV.

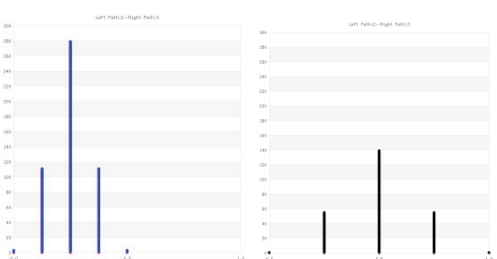
N=8, Frame=Single, f=12, Interaction = Conditional (L1:R2), Parity=Anti-symmetry, L-P_{color} = red, R-P_{Color} = blue, D-W_{Color} = black, {L-P, R-P, D-P, D-W}$_{Height}$ = 300, Output=4-1 in Figure 6(IV).

For four groups, a selection changes from either Multiple to Conditional or Symmetry to Anti-symmetry, output results have significantly visual differences.

After making a proper selection, user can press Process button to start generation under selected parameters. When the generation has complete, the Process button turns to be disable.

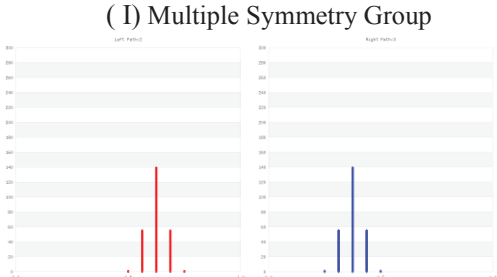


(L-P) (R-P)

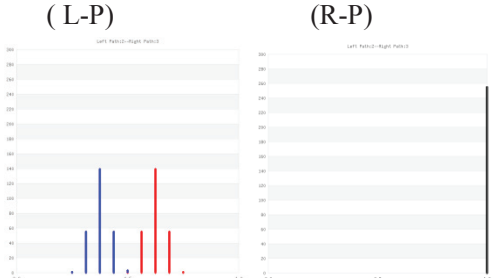


(D-P) (D-W)

(I) Multiple Symmetry Group

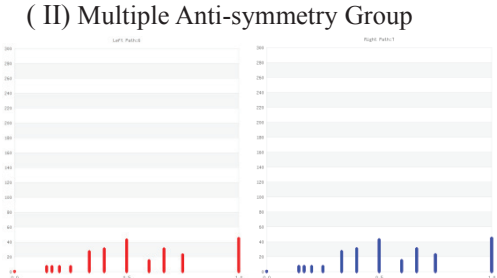


(L-P) (R-P)

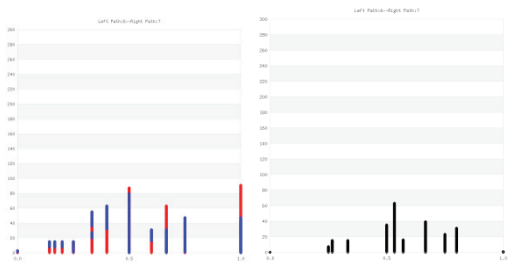


(D-P) (D-W)

(II) Multiple Anti-symmetry Group

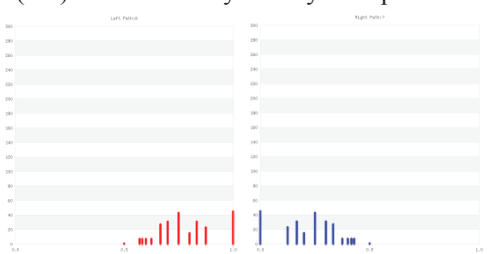


(L-P) (R-P)

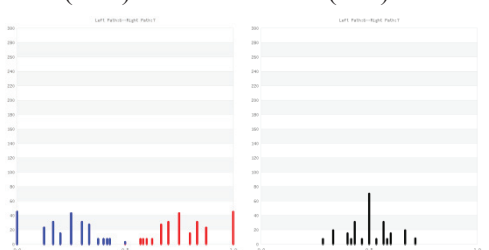


(D-P) (D-W)

(III) Conditional Symmetry Group



(L-P) (R-P)



(D-P) (D-W)

(IV) Conditional Anti-symmetry Group

Figure 6. (I-IV) Four Groups of 16 distributions for a single function. N=8, Frame=Single, f=12, L-P_{color} = red, R-P_{Color} = blue, D-W_{Color} = black, {L-P, R-P, D-P, D-W}$_{Height}$ = 300, Output=4-1; (I,II) Interaction=Multiple (L1:R2), (III,IV) Interaction= Conditional (L1:R2); (I,III) Parity=Symmetry, (II,IV) Parity=Anti-symmetry.

Discussion

Global Cases

Initially M_C matrix itself does not show having special hidden features to organize its elements. Under variant projection, four symbol matrices are represented for their distinct characteristics under symbol representations. Four symbols {a, b, c, d} determine $\{(f_{\perp})_C, (f_{+})_C\}$ matrices to provide four values in vertical directions and another four symbols {A, B, C, D} are in $\{(f_{-})_C, (f_{T})_C\}$ matrices to provide four values in horizontal directions. The six interactive cases provide all possible 2-2 interactive combinations among four matrices.

Due to intrinsic dependent properties in each meta matrix, output matrices of both Case 1 and Case 6 are degenerated and four output matrices of Case 2 – Case 5 can be expressed as one matrix under four rotational operations on 90 degrees. Visual characteristics can be easily observed via relevant histogram distribution matrices.

Four groups of 16 matrices in C code scheme illustrate global properties on horizontal and vertical polarized distributions under variant matrix partition. Significant differences on distributions can be observed to change parameters from either Interaction = Multiple /Conditional or Parity = Symmetry /Anti-symmetry conditions. Four matrices in each group illustrate four distributions with D-P = L-P + R-P and D-W $\neq$ L-P + R-P properties.

i.e. *The simulated results can satisfy two critical conditions of Feynman models to explain wave-particle interactive behaviors.*

Single Cases

Under selected interaction, it is possible to reconfigure other parameters via online interface. One important parameter is Parity that provides either Symmetry or Anti-symmetry characteristics. Another key parameter is Interaction that includes 10 different selections, six cases for Multiple probability interactions and four cases for Conditional probability interactions.

From an analogy viewpoint, this set of parameters provides core links corresponding to deep historical mysteries in foundation of quantum mechanics. Using graphic color control parameters, it is convenient to observe randomness in D-P distributions as separated

color segments with different lengths in some cases. Since wave interactions cannot generate new objects, it is impossible to distinguish each output recorder to be linked to their original resources. Under such condition, only one color could be resigned. It is interesting to see users in further exploration finding new results.

Similar to global characteristics, it is feasible to find refined properties via various detailed selections on controllable parameters. In the prototype, it is convenient for user to click on one picture in 4-1 frame to get a zoom distribution for superior information. Users can use this type of tools to check each interactive result in finer details.

Feasible Configurations

In this prototype, a total number of configurations can be calculated as follows.

For a single function in n=2, possible selections are based on six vector lengths, two parities, four interactive projections, 16 functions, ten interactions. A total of 7680 configurations ($6\times2\times4\times16\times10 = 48\times160$) are available for all controllable selections on the prototype.

Conclusion

It is essential to design an online prototype properly for various implementations. The architecture and core components of VDPS in the paper are only a brief outline to guide further versions of VDPS to meet wider user's requirements. Applying online simulation mechanism on Web, it is more convenient for people to apply VDPS facilities as computer assistant tools in future explorations and observations.

This prototype provides a larger space as controllable configurations for the simulation to visualize various detailed distributions.

In addition to single functions, different configurations on global coding schemes will be designed and implemented in near future to provide more powerful capacities of simulation mechanism to resolve historical mysteries and paradoxes in quantum interactions.

Both theoretical and experimental solutions are expected in quantum foundation and practical applications consequently. To follow VDPS systematical guide maps, it is encouraged to resolve more historical problems and emerging practical challenges in natural world on either theoretical or experimental levels in near future.

Acknowledgements Thanks The School of Software Engineering, Yunnan University, The Key Laboratory of Yunnan Software Engineering and The Yunnan Advanced Overseas Scholar project (W8110305) for financial supports to the Information Security research projects (2010EI02, 2010KS06).

References

[1] R. B. Ash & C. A. Doléans-Dade (2000). *Probability & Measure Theory*, Elsevier.

[2] J. D. Barrow, P. C. W. Davies & J. E. Charles L. Harper (2004). *SCIENCE AND ULTIMATE REALITY: Quantum Theory, Cosmology and Complexity*, Cambridge University Press.

[3] E.A. Bender (2000). *An Introduction to Mathematical Modeling*, Dover, New York.

[4] N. Bohr (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review* 48. 696-702.

[5] N. Bohr (1949). *Discussion with Einstein on Epistemological Problems in Atomic Physics*, Evanston. 200-241.

[6] L. de Broglie; Translated by H.C. Shen (2012). *Selected Works of de Broglie*. in Chinese, Peking University Press.

[7] Einstein, A., Podolsky, B.&Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review* 47. 770-780.

[8] Feynman, R., Leighton, R. & Sands, M. (1965,1989). *The Feynman Lectures on Physics*, Vol. 3, Addison-Wesley, Reading, Mass.

[9] N. Gershenfeld (1998). *The Nature of Mathematical Modeling*, Cambridge Uni. Press.

[10] R. Healey & G. Hellman Edited. (1998). *Quantum Measurement: Beyond Paradox*, Uni. Minnesota Press.

[11] T. Hey & P. Walters (2003). *The New Quantum Universe*, Cambridge University Press.

[12] J.N.P. Hume (1974). *Physics in two volums, Vol. 2 Relativity, Electromagnetism and Quantum Physics*, The Ronald Press Company, New York.

[13] D.G. Ivey (1974). *Physics in two volums, Vol. 1 Classical Mechanics and Introductory Statistical Mechanics,* The Ronald Press Company, New York.

[14] M. Jammer (1974). *The Philosophy of Quantum Mechanics*, Wiley-Interscience Publication.

[15] M. Kumar (2008). *Quantum: Einstein, Bohr and the great debate about the nature of reality*, Icon Books Limited.

[16] J.P. McEvoy & O. Zarate (2007). *Quantum Theory: A Graphic Guide*, Icon Books Ltd.

[17] R. Penrose (2004). *The Road to Reality*, Vintage Books, London.

[18] M.J. Pring (2002). *Breaking the Black Box*, McGraw-Hill.

[19] J. von Neumann (1932,1996). *Mathematical Foundations of Quantum Mechanics*, Princeton Univ. Press.

[20] H. D. Zeh (1970). On the interpretation of measurement in quantum theory, *Foundation of Physics* 1. 69-76.

[21] J. Zheng, C. Zheng & T. Kunii (2012). From Local Interactive Measurements to Global Matrix Representations on Variant Construction - A Particle Model of Quantum Interactions for Double Path Experiments, *Advanced Topics in Measurements*, edited by: Z. Haq 371-400. URL: http://www.intechopen.com/books/advanced-topics-in-measurements

[22] J. Zheng, C. Zheng, & T. Kunii (2012). From Conditional Probability Measurements to Global Matrix Representations on Variant Construction ´- A Particle Model of Intrinsic Quantum Waves for Double Path Experiments, *Advanced Topics in Measurements*, edited by: Z. Haq 337-370. URL: http://www.intechopen.com/books/advanced-topics-in-measurements

[23] J. Zheng (2012). Multiple and Conditional Probabilities and Their Statistical Distributions for Variant Measures, *Laser & Optoelectronics*

Progress 49(4): 042701. URL: http://www.opticsjournal.net/abstract.htm?aid=OJ120119000021MjPlSo

[24] J. Zheng (2011). Synchronous properties in quantum interferences, *Journal of Computations & Modelling*, International Scientific Press 1(1). 73-90. URL: http://www.scienpress.com/upload/JCM/Vol%201_1_6.pdf

[25] J. Zheng & C. Zheng (2011). Variant measures and visualized statistical distributions, *Acta Photonica Sinica*, Science Press 40(9). 1397-1404. URL: http://www.photon.ac.cn/CN/article/downloadArticleFile.do?attachType=PDF&id=15668

[26] J. Zheng, C. Zheng & T. Kunii, (2011). A framework of variant-logic construction for cellular automata, *Cellular Automata - Innovative Modelling for Science and Engineering* edited Dr. A. Salcido, InTech Press. 325-352. URL: http://www.intechopen.com/articles/show/title/a-framework-of-variant-logic-construction-for-cellular-automata

[27] J. Zheng (2011). Conditional Probability Statistical Distributions in Variant Measurement Simulations, *Acta Photonica Sinica,* Science Press 40(11): 1662-1666. URL: http://www.opticsjournal.net/viewFull.htm?aid=OJ1112120000332y5B8D

[28] J. Zheng & C. Zheng (2011). Variant simulation system using quaternion structures, *Journal of Modern Optics*, Taylor & Francis Group 59(5): 484-492. URL: http://www.tandfonline.com/doi/abs/10.1080/09500340.2011.636152

[29] J. Zheng (2011). Two Dimensional Symmetry Properties of Global Coding Family on Configuration Function Spaces of Variant Logic , *Journal of Chengdu University of Information Technology* Dec. 2011. URL: http://www.cnki.net/kcms/detail/51.1625.TN.20111227.1043.001.html

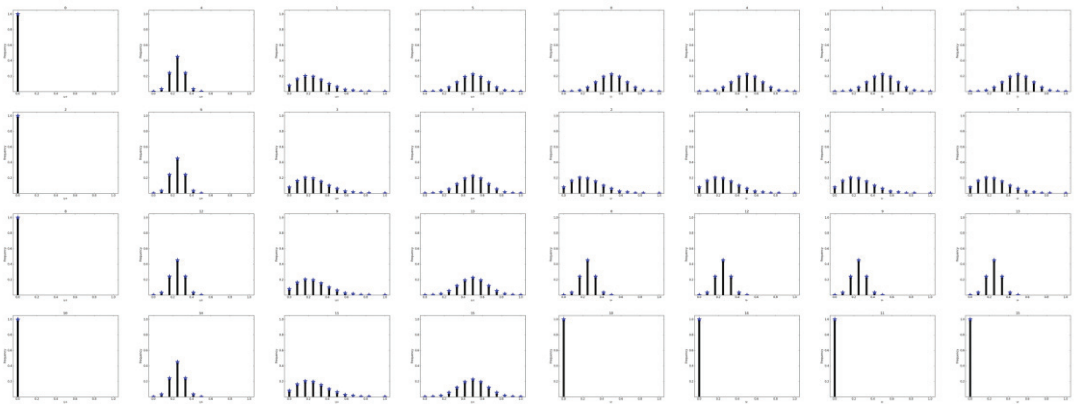
[30] J. Zheng & C. Zheng (2010). A framework to express variant and invariant functional spaces for binary logic, *Frontiers of Electrical and Electronic Engineering in China*, Higher Education Press and Springer 5(2): 163–172. URL: http://www.springerlink.com/content/91474403127n446u/

Authors

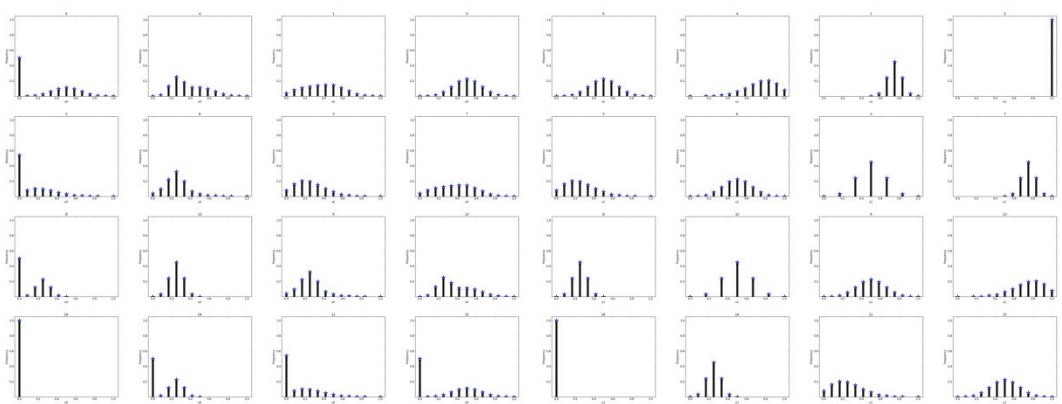
Dr. Jeffrey ZHENG, received ME and PhD degrees from USTC (1981) and Monash Uni. (1994) respectively. Dr. Zheng worked in Institute of Computing Technology, Academia Sinica as an assistant research professor in 1981-1987; Institute of Systems Sciences, NUS as a visiting scientist in 1987-1990; Victoria University of Technology as a research fellow in 1994-1997; CSRIO Division of Manufacturing Science & Technology as a senior software engineering in 1998-2002 and from 2004, Dr. Zheng is the director of Department of Information Security, School of Software, Yunnan University as a Professor. Dr. Zheng worked in parallel architecture & algorithm, image analysis and processing, content-based image retrieval, knowledge representation and higher performance of hierarchical modeling. In recent years, Dr. Zheng has focused his attention on variant logic construction and key applications on Variant Double Path Simulation to resolve historic mysteries of quantum foundation and wave-particle paradoxes.

Mr. Jie-Ao ZHU received a Bachelor degree in software engineering from Yunnan University in 2012 with the thesis: "Design & Implementation Prototype on Variant Double Path Simulation" selected as one of the Best Bachelor Thesis 2012 in Yunnan University supervised by Professor Jeffrey Zheng. He worked in JIKE.com as an IT Architect and Engineer to develop a Collaborative Filtering (CF) personalized recommendation system in 2011 and has published several research papers in national and International conferences on Information Management System and Simulation of Quantum Interactions. He was interested in Data Mining on development of CF information retrieval systems, especially on Recommender System for E-commerce applications. He has being involved in variant R&D from 2010 and has focus attention on using variant logic schemes associated with Professor Zheng to do various data mining on mass data sets and other applications in advanced CF information retrieval.

Mr. Jie WAN received a Bachelor degree in software engineer from Yunnan University in 2011 with the thesis: "Global Classification on Variant Logic Framework" selected as one of the Best Bachelor Thesis 2011 in Yunnan University supervised by Professor Jeffrey Zheng. From 2011, Mr. Wan is a postgraduate student on System Analysis and Integration in School of Software, Yunnan University supervised by Professor Zheng. He is interested in complex recursive data structures using combination and permutation analysis and process approaches. He has being involved in variant R&D from 2009 and has published several research papers in International Journal, national and International conferences on Random number generation and global classification on variant logic construction for Cellular Automata. Recently, Mr. Wan puts his attention to the data visualization on complex multiple measurements for Variant Double Path Simulation on variant phase space.

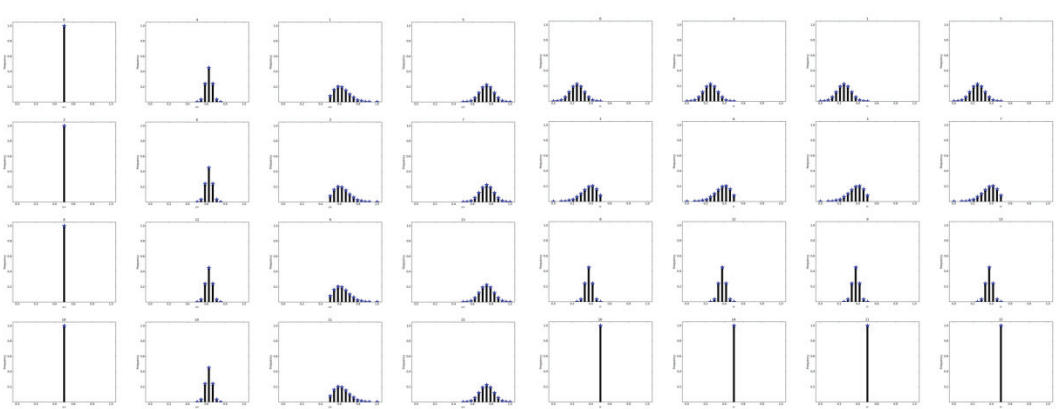


(L-P) (R-P)

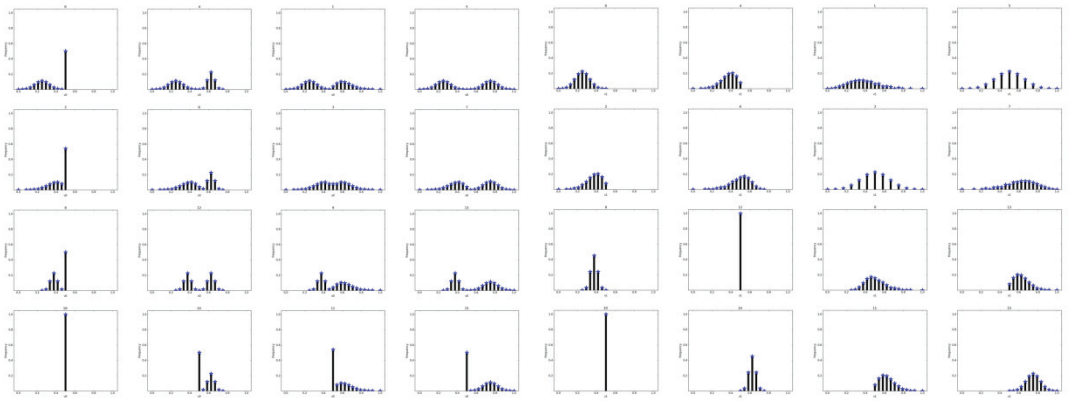


(D-P) (D-W)

(I) Multiple Symmetry Group

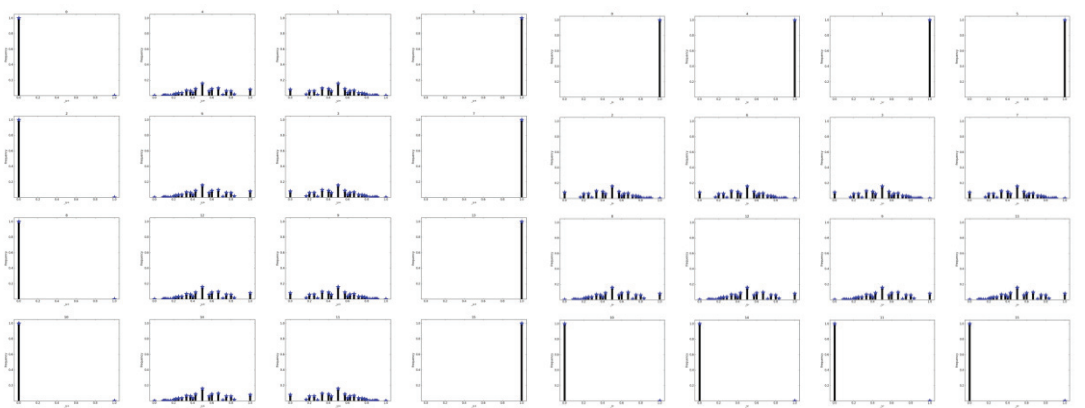


(L-P) (R-P)

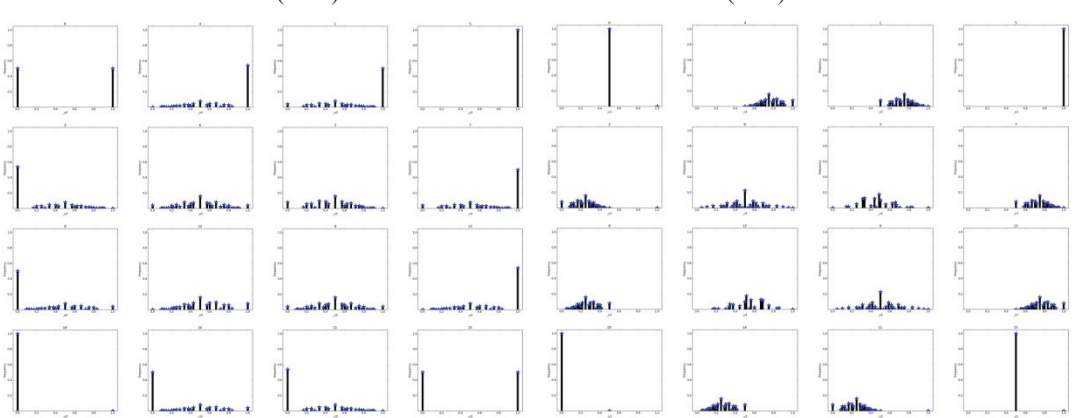


(D-P) (D-W)

(II) Multiple Anti-symmetry Group



(L-P) (R-P)



(D-P) (D-W)

(III) Conditional Symmetry Group

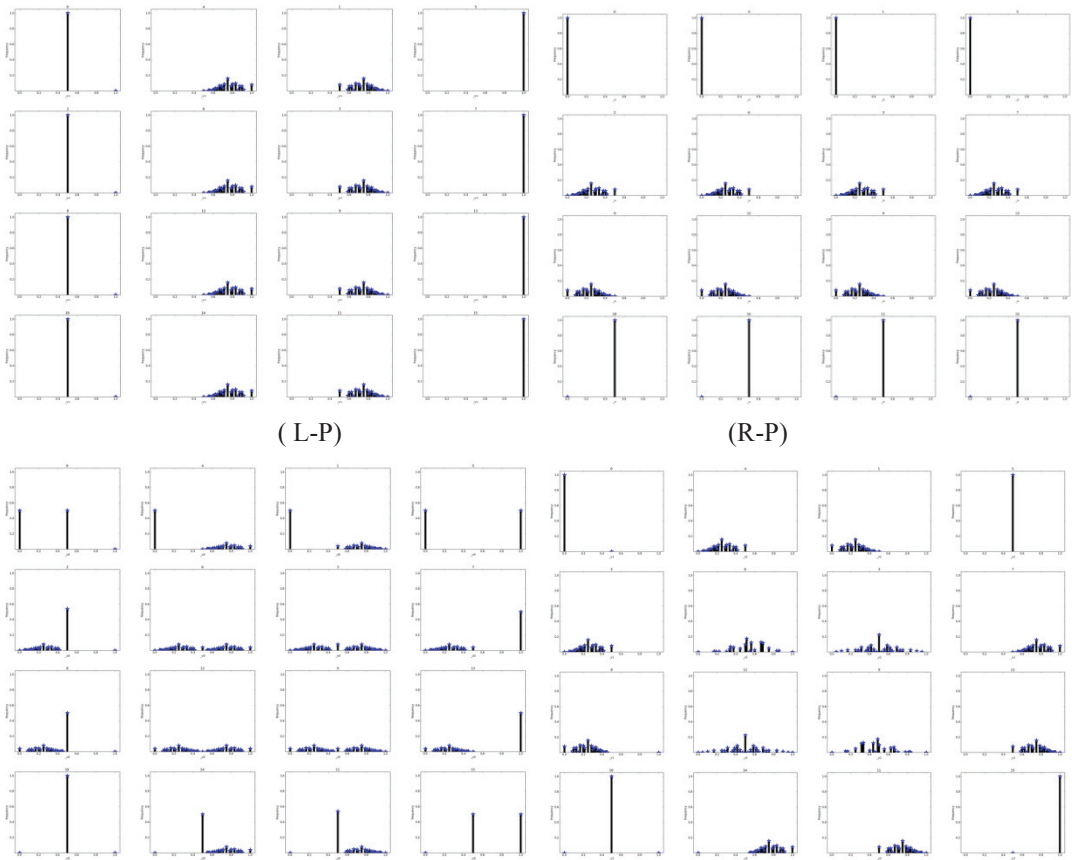


Figure 5. Four Groups of Global Matrices, N=8, Frame=Global, Output=4-1, (I, II) Interaction =Multiple(L1:R2); (III, IV) Interaction = Conditional (L1:R2); (I,III) Parity=Symmetry; (II, IV) Parity=Anti-symmetry

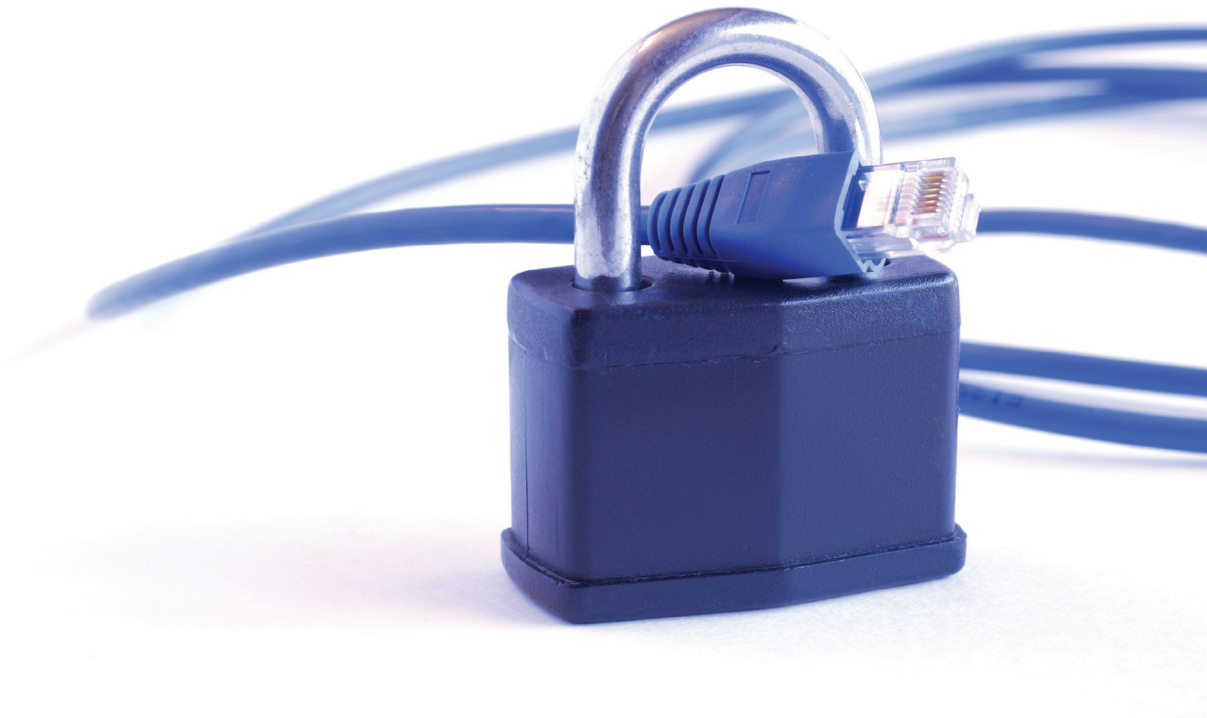
Table 1. Two Variable Logic Functions and Variable Logic Representation (n=2, j=0)

f No.	$f \in S(2)$	3 11	2 10	1 01	0 00	$3^{\vee}$ $11^{\vee}$	$2^{\vee}$ $10^{\vee}$	$1^{\vee}$ $01^{\vee}$	$0^{\vee}$ $00^{\vee}$	$f_{\perp} \in S_0^0(2)$	$f_{+} \in S_0^0(2)$	$f_{-} \in S_1^0(2)$	$f_{\mathrm{T}} \in S_0^0(2)$
0	{Φ}	0	0	0	0	−	⊥	−	⊥	{2,0}	{Φ}	{3,1}	{Φ}
1	{0}	0	0	0	1	−	⊥	−	+	{2}	{0}	{3,1}	{Φ}
2	{1}	0	0	1	0	−	⊥	⊤	⊥	{2,0}	{Φ}	{3}	{1}
3	{1,0}	0	0	1	1	−	⊥	⊤	+	{2}	{0}	{3}	{1}
4	{2}	0	1	0	0	−	+	−	⊥	{0}	{2}	{3,1}	{Φ}
5	{2,0}	0	1	0	1	−	+	−	+	{Φ}	{2,0}	{3,1}	{Φ}
6	{2,1}	0	1	1	0	−	+	⊤	⊥	{0}	{2}	{3}	{1}
7	{2,1,0}	0	1	1	1	−	+	⊤	+	{Φ}	{2,0}	{3}	{1}
8	{3}	1	0	0	0	⊤	⊥	−	⊥	{2,0}	{Φ}	{1}	{3}
9	{3,0}	1	0	0	1	⊤	⊥	−	+	{2}	{0}	{1}	{3}
10	{3,1}	1	0	1	0	⊤	⊥	⊤	⊥	{2,0}	{Φ}	{Φ}	{3,1}
11	{3,1,0}	1	0	1	1	⊤	⊥	⊤	+	{2}	{0}	{Φ}	{3,1}
12	{3,2}	1	1	0	0	⊤	+	−	⊥	{0}	{2}	{1}	{3}
13	{3,2,0}	1	1	0	1	⊤	+	−	+	{Φ}	{2.0}	{1}	{3}
14	{3,2,1}	1	1	1	0	⊤	+	⊤	⊥	{0}	{2}	{Φ}	{3,1}
15	{3,2,1,0}	1	1	1	1	⊤	+	⊤	+	{Φ}	{2,0}	{Φ}	{3,1}

Table 2. Two Variable Logic Functions and Their Symbol Representations (n=2, j=0)

f No.	$f \in S(2)$	3 11	2 10	1 01	0 00	$3^{\vee}$ $11^{\vee}$	$2^{\vee}$ $10^{\vee}$	$1^{\vee}$ $01^{\vee}$	$0^{\vee}$ $00^{\vee}$	$f_{\perp} \in S_0^0(2)$	$f_{+} \in S_0^0(2)$	$f_{-} \in S_1^0(2)$	$f_{\top} \in S_0^0(2)$
0	{Φ}	0	0	0	0	−	⊥	−	⊥	d	a	D	A
1	{0}	0	0	0	1	−	⊥	−	+	c	b	D	A
2	{1}	0	0	1	0	−	⊥	⊤	⊥	d	a	B	C
3	{1,0}	0	0	1	1	−	⊥	⊤	+	c	b	B	C
4	{2}	0	1	0	0	−	+	−	⊥	b	c	D	A
5	{2,0}	0	1	0	1	−	+	−	+	a	d	D	A
6	{2,1}	0	1	1	0	−	+	⊤	⊥	b	c	B	C
7	{2,1,0}	0	1	1	1	−	+	⊤	+	a	d	B	C
8	{3}	1	0	0	0	⊤	⊥	−	⊥	d	a	C	B
9	{3,0}	1	0	0	1	⊤	⊥	−	+	c	b	C	B
10	{3,1}	1	0	1	0	⊤	⊥	⊤	⊥	d	a	A	D
11	{3,1,0}	1	0	1	1	⊤	⊥	⊤	+	c	b	A	D
12	{3,2}	1	1	0	0	⊤	+	−	⊥	b	c	C	B
13	{3,2,0}	1	1	0	1	⊤	+	−	+	a	d	C	B
14	{3,2,1}	1	1	1	0	⊤	+	⊤	⊥	b	c	A	D
15	{3,2,1,0}	1	1	1	1	⊤	+	⊤	+	a	d	A	D

Where eight symbols {a={Φ}, b={0}, c={2}, d={2,0}} and { A={Φ}, B={3}, C={1}, D={3,1}} are used to represent corresponding eight sets of variant state combinations respectively.



Fortune 1000 Open Targets For Flame-Style Attacks

Announcing Venafi MD5 Certificate Assessor™
Identify Your Open Security Doors—For Free

Extinguish the risks of copycat FLAMES by eliminating MD5 certificates

Survey data indicates that nearly all Fortune 1000 organizations rely on the now-compromised MD5 certificates—for security and authentication. These weak, proven "hackable" instruments leave major security doors open. It's critical that all organizations eliminate the use of MD5 in their environments as soon as possible. Yet finding MD5 certificates across your enterprise can be a daunting task. To aid in your efforts, leverage MD5 Certificate Assessor™, which provides a free and easy to deploy assessment of your network to determine MD5 security risks. You will:

- Identify all certificates on your network, including self-signed and wildcard certificates
- Determine the location of all of your network-based MD5 certificates
- See which encryption keys are out of compliance and assess their strengths
- Determine which certificate validity periods are creating the greatest risk

In today's atmosphere of increasingly frequent cyber attacks and regulatory mandates, Venafi provides security best practices and Enterprise Key and Certificate Management solutions to the market.

Learn more at www.Venafi.com/AssessorMD5.

VENAFI™

SecureBlackbox
software components for developers

ELDOS
Feel safer

Download free evaluation at http://eldos.com

PACKAGES are units of licensing.
Combined packages let you save money by purchasing of sets of related components:

- Professional
- Standard
- Data Security
- Transports

Individual packages give you support of particular functionality:

- EDIBlackbox
- LDAPBlackbox
- MailBlackbox
- CloudBlackbox
- SFTPBlackbox
- SSHBlackbox
- SSLBlackbox
- HTTPBlackbox
- FTPSBlackbox
- WebDAVBlackbox
- OfficeBlackbox
- OpenPGPBlackbox
- ZIPBlackbox
- PDFBlackbox
- XMLBlackbox
- PKIBlackbox
- MIMEBlackbox

Distributed Cryptography add-on offers client-side signing of data stored on the server.

EDITIONS define what development tools you are going to use with SecureBlackbox:

- .NET
- VCL
- Active X
- Java
- Library

SUPPORT is provided during evaluation and after licensing via:

- Forums (public support)
- HelpDesk (individual support)
- KnowledgeBase
- LiveChat (sales-related nontechnical questions).

PLATFORMS on which you can use SecureBlackbox:

- Windows (native and .NET)
- Linux (native and Mono)
- MacOS X
- Windows Phone 7
- Web browser (Silverlight)
- Java
- Android
- iOS

LICENSING types are offered for every model of business:

- In-House (applications and web services for your internal needs)
- Vendor (applications and web services for further distribution)
- Ultimate (all above and more)
- Middleware (distribution as a part of your library)

Extra options are also available.