Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Is the future of cryptography in qubits

While quantum computer algorithms threaten the future of classical cryptography, One-time pads can still offer security even in the presence of key cracking quantum computers, but the key distribution problem would have to be overcome. In a beautiful irony, quantum computers may break current cryptography but quantum mechanics also offer hope to cryptography in quantum key distribution.

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Is the future of cryptography in qubits

Wayne Redmond

28 September 2002

GIAC Security Essentials Certification (GSEC v1.4b)

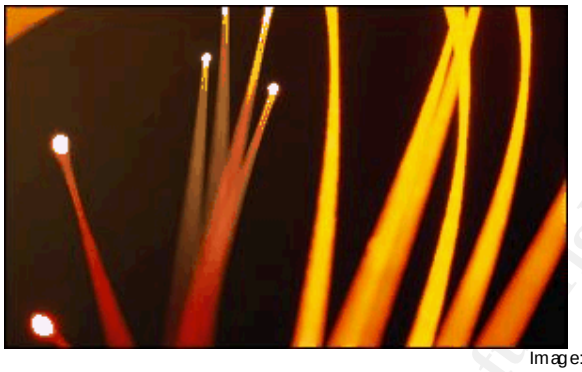


Image: Ivan Noble - BBC-online

Abstract

While quantum computer algorithms threaten the future of classical cryptography, One–time pads can still offer security even in the presence of key cracking quantum computers, but the key distribution problem would have to be over come. In a beautiful irony, quantum computers may break current cryptography but quantum mechanics also offer hope to cryptography in quantum key distribution.

Introduction

For many centuries, cryptography has been, and will continue to be used for protection of information and enabling of secret communications, for both individuals and states.

The earliest forms of cryptography used a simple mono-alphabetic substitution changing a single letter for another for each letter of the alphabet. This simple form of encryption is easily broken by cryptanalysts employing frequency analysis.[1] As cryptographers developed new and stronger methods for encrypting, the time taken to "break" the encryption increased. Cryptography was winning the battle but during the Second World War, development of a "universal Turing machine" (the for-runner of the modern computer) by Alan Turing, at Bletchley Park, and utilising the cryptanalysis work of Pole Marian Rjewski enabled the British to read the German Enigma communications, the battle was over, literally. The next 50 years saw the computer develop into the machine most of us have sitting on our desktops today, each year becoming smaller and faster.[2] The requirement of secure communications now supports, not only governments and individuals, but also a new revolution in commerce, e-commerce. New forms of cryptography have evolved to build this new world of; confidentiality, authentication, non-repudiation, and integrity, but while this work well in the here now, with the advent of the quantum computer on the horizon classical cryptography is threatened.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"In as soon as 10 years, the quantum computer could begin knocking down the increasingly vulnerable public-key systems that today are the security engines of the Internet." – Mark Anderson. [3]

Requirements of cryptography

Cryptography must ensure that, the unaltered content of a communication is exposed only to the intended receiver(s) – integrity and confidentiality.

Some background

In order to appreciate the future of cryptography we need to explore its past, and expose the weaknesses, that have forced the advancement of cryptographic technology.

Symmetric encryption:

Early ciphers substituted each of the letters of the alphabet with another letter, eg. If each letter is shifted by three, a – D, b – E, … s – V… you get the following:

	a simple message
Becomes:	D VLPSOH PHVVDJH

The key to this encrypted message is - the alphabet has been shifted by three letters, and that shifting back by three letters is the key to decrypting the message. Note that the key is the same to encrypt and decrypt and therefore must be secret to both the sender and receiver. Anyone with this knowledge can decrypt the message (confidentiality attack), or encrypt a message (misinformation, integrity attack). This is secret key or symmetric key cryptography, this example of a mono-alphabetic substitution cipher is known as a Caesar shift cipher, used by Julius Caesar in the Gallic wars 58 – 50 B.C.[4]

A stronger form of encryption is a 26-alphabet matrix, the development of, credited to Blaise de Vigenère (born 1523) [4] (Figure 1).
Encrypting the message is achieved by the use of a key word, which must remain secret between the sender and receiver. The key determines which substituted alphabet is used to encrypt that letter, creating a poly-alphabetic cipher text.
The encryption is performed as follows: The key word is written above the plain text repeatedly to cover the entire message, the letters in the key word indicate the cipher row to be used and the intercept of the plain text on this row produces a cipher letter, this process is then repeated for each letter of the key stream. eg. If the secret keyword is SECRET, we get:

Key	SECRETSECRETSE
Plain text	asimplemessage
Cipher text	SWKDTEWQGJWTYI

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figure 1. A Vigenère square

Both these methods of encrypting are mono-alphabetic the Caesar shift cipher, obviously so but the Vigenère cipher alphabets remain constant during the encryption process also; just different cipher alphabets are used for each letter of the key stream.

The Enigma machine (Figure 2) invented by Arthur Scherbuis and Richard Ritter in 1918 and used by the Germans in the Second World War encrypted messages in a truly poly-alphabetic fashion.

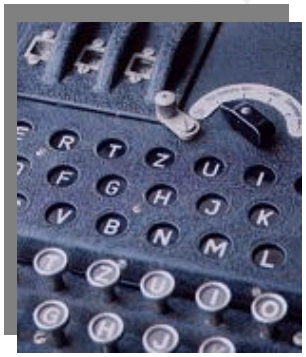


Image - simonsingh

Figure 2. An Enigma machine

The three rotating scramblers (seen at the top of Figure 2) would rotate separately after each keystroke effectively producing another cipher alphabet, the combination of alphabets for the three rotors totalled 26x26x26=17576 alphabet combinations, (later machines used a four rotor encryption mechanism). In addition to the scrambler rotation the location and starting positions of the swappable scramblers, along with the wiring of letter pairs on the plug board is the key for the day's encryptions. These setting were needed at each end of the communication

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

channel, and where distributed in a codebook. Since replicas of the Enigma machines where available to the Allied forces, having a codebook would allow the decryption of the communications.
Can you see where this is going, the strength of the cryptographic system relies on the security of the distributed secret keys not the strength of the actual algorithms or encryption mechanisms. A fundamental assumption in cryptanalysis, first definitively stated by Dutch linguist, Auguste Kerckhoffs von Nieuwenhof in 1883, is that the secrecy must reside entirely in the key. [5]

For more information on cracking of the Enigma see David Kahn's book "Seizing The Enigma ".[6] or for a great Enigma emulator see Andy Carlson's enigma emulator. [7]

Major Joseph Mauborgne and Gilbert Vernam in 1917 invented the one-time pad (Figure 3) a simple method of encrypting messages using a pad of random letters to encrypt the plain text, this is still a symmetrically encryption method, as the one-time pads are the same at both ends of the communication channel, therefore must remain secret. An important cravat of one-time pads is that the random string of key letters must not be repeated or reused, as the Soviets discovered in the 1940s. Due to a manufacturing fault in the production of their one-time pads, 35 000 pages where duplicated enabling the United States cryptanalyst Lt. Richard Hallock from Arlington Hall, Northern Virginia to decrypt Soviet "trade" communications. [8]

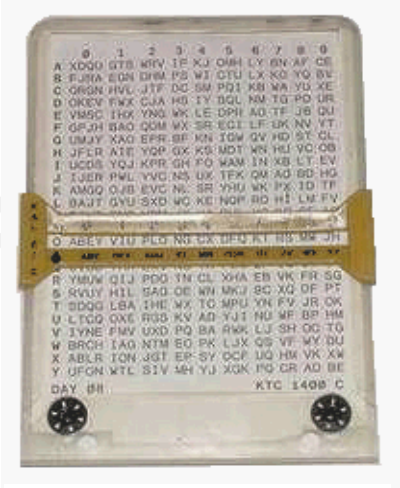


Image - Brooke Clarke

Figure 3. A Vernam One-time pad

Again, the pad must be available to the sender and recipient(s) and the secure distribution of the one-time pads coordinated. This is a huge disadvantage of a one-time pad system, the secret key is just as large is the message, so there is a key distribution problem.

"Because the key has to be as long as the message, it doesn't solve the security problem. One way to look at encryption is that it takes very long secrets – the message – and turns them into very short secrets: the key." - Bruce Schneier.[9]

The advantage of a one-time pad, over a shorter keyword, is the provable security of the encryption method due to the unicity distance. Claude Shannon's 1949 paper "Communication Theory of Secrecy Systems" [10] explains the concept of unicity distance, the relationship between key length and unconditional security, i.e. Security of cryptosystems when there is no bound placed on the amount of computation. As the key length approaches the message length, the unicity distance increases. The unicity distance defines the amount of cipher text required such that there is only one

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

reasonable plain text.[9] The unicity distance for a one-time pad encryption system is infinite, therefore, for a one-time pad encryption system, the cipher text will resolve to all possible plain texts, therein lies the security.

"Given any cipher text, the probability that it matches any particular message is the same, and given any plain text, the probability that it matches any particular cipher text is the same." - David Evans [11]

One prerequisite of obtaining unconditional security is the randomness, or more correctly, the unpredictability, of the character strings in the one-time pads.

Key distribution options

The key distribution problem is mitigated in two ways:

1. By avoiding it with an asymmetric key or public key system, as the name suggests two keys are involved in this system and they are not symmetric. A public key is used to encrypt the message(s) and the private key is used to decrypt the message(s). Examples of this type of cryptographic system are RSA (Rivest, Shamir and Adleman), and ECC (Eliptic Curve Cryptography) These systems are well proven and have not been publicly acknowledged as having been "broken", due to the intractability of the mathematics involved in the algorithms; factoring large integers (RSA) and the discrete logarithm problem (ECC). The time required to "brake" the encryption classically is very long, with the typical key lengths in use.
Although there is no key distribution problems, from a security point of view, as the public key is distributed to public databases like a phone book. These systems are not as fast as the symmetric systems and are usually implemented for the distribution of one-off symmetric keys to be used in the main communications, as with the Diffie-Hellman system. As eluded to above a brute force attack can be mounted against the cipher text and the encryption is not provably secure its just, currently too hard to "break".

2. By solving it, there is an irony in the fact that quantum computers may be the downfall of current cryptography but on the other hand, quantum mechanics offers the solution, in quantum cryptography, or more correctly, quantum key distribution (QKD). QKD has advantages over classical cryptography in the key distribution, enabling, an exchanged of, an unpredictable string of binary bits, and any eavesdropping to be detected. Only the non-interfered with bits of the binary sequence are used in a one-time pad which is, as eluded too earlier, provably secure.

Asymmetric cryptography:
Algorithms such as RSA and ECC use a two key system, one key for encryption (public) and another key for decryption (private). They can also be used in "reverse" for authentication – but I will not pursue this here.
Asymmetric cryptography or public key cryptography solves the problem of key distribution very nicely. It is a slower method of encryption than say tripleDES (Data Encryption Standard) and key lengths required offering similar strengths to symmetric systems are much longer. (Table 1)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Symmetric Key Length	Public Key Length
128bit	2304

Table 1. A comparison of key lengths offering similar resistance to brute force attacks. [12]

The threat

Different algorithms offer different degrees of security, it comes down to the cost in time, and or, the cost in money quantum mechanics changes this, well may be just the time cost. In 1994, Peter Shor of AT&T Laboratories showed that efficient algorithms for prime factorization and discrete logarithms are possible on a quantum computer.[13] The state of a quantum computer is a superposition of exponentially many basis states, each of which corresponds to a state of a classical computer. A quantum computer can perform in a reasonable time some tasks that would take ridiculously long on a classical computer. Shor's discovery propelled the then obscure subject of quantum computing into a dynamic and rapidly developing field, and stimulated scores of experiments and proposals aimed toward building of quantum computers.

Lov Grover of Bell Laboratories, Lucent Technologies, [14] who in 1996 invented a quantum -searching algorithm showed that to find one particular object "O" among a number of objects "N" requires checking O(N) items classically but with Grover's algorithm, a quantum computer need only look up items O($\sqrt{N}$) times. It can be used to radically speed up the brute force attack of DES (that is, trying all 2^{128} possibilities, of a 128 bit key. Although on average, only half of the possible keys will need tried). Similar attacks on RSA, ECC and other cryptographic systems utilising intractable mathematical problems are also possible. It looks like classical cryptography's intractable mathematics may be about to become tractable.

The solution

With respect to classical computing the basic unit of information is the binary bit and can exist as either 0 or 1, in quantum computing the basic unit of information is known as a quantum bit or qubit[15] and can exist in both states at once, or in supposition. Further more the, Heisenberg uncertainty principle dictates that it is fundamentally impossible to know the exact values of complementary variables such as a particles' momentum and its position. So how does this achieve the distribution of an unpredictable key of the desired length (the message length, for a one time pad), and have the ability to detect an eavesdropper.

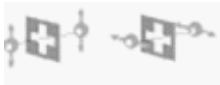
Stephen Wiesner [16] came up with an idea in the 1960 that utilised the uncertainty of polarised light photons. He realized that photons could be polarised in a plane of a known angle, but that the angle of the polarisation plane could not be measured with certainty by an observer.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Consider this. Given a single photon in one of four possible polarisations:

0º 90º 45º 135º

Is its polarisation able to be measured with certainty?
Surprisingly, the answer is, No.
The rectilinear basis,



and the diagonal basis,

are incompatible, so the Heisenberg uncertainty principle forbids us from simultaneously measuring both. Uncertainty allows a diagonally polarised

photon to be detected by the both the correct diagonal basis detection filter and the incorrect rectilinear basis detection filter, but the photon will not pass through a filter 90º to the original polarisation (Table 2).

Lets run through it, Alice wants to send a secret message to Bob in the possible presence of an eavesdropper, Eve. First they need a protocol Charles Bennett and Gilles Brassard proposed a quantum key distribution (QKD) scheme, known as BB84, [17] in which, Alice sends Bob a sequence of photons, each independently prepared in one of four polarisations and assigned these binary values (Figure 4).

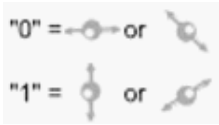
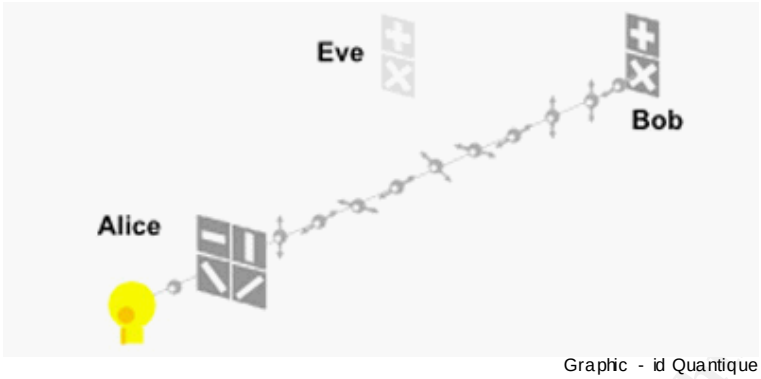


Figure 4. Photon polarisation values

For each photon, Bob randomly picks one of the two detection filters,

rectilinear or diagonal to perform a measurement (Figure 5).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Graphic - id Quantique

Figure 5. Representation of QKD

How is Bob going to know what basis (filter) to use to detect the photons? He will not, but the Heisenberg uncertainty principle will allow detection of the polarised photons as (Table 2) below explains.

Alice's scheme	Alice's bit	Alice sends	Bob's detector	Correct detector?	Bob detects	Bob's bit	Is Bob's bit correct?
Rectilinear	1		+	Yes		1	Yes
			x	No		1	Yes
						0	No
	0		+	Yes		0	Yes
			x	No		1	No
						0	Yes
Diagonal	1		+	No		1	Yes
						0	No
			x	Yes		1	Yes
	0		+	No		1	No
						0	Yes
			x	Yes		0	Yes

Table 2. Possibilities of polarised photon exchange. [4]

He keeps the measurement outcome secret. Now Alice and Bob publicly compare their bases this could be done over a standard phone line, but Alice and Bob must share some authentication information to begin with; otherwise, Bob has no way to know that the person on the phone is really Alice, and not a clever mimic. They keep only the polarisation data for which they measured in the same basis. In the absence of errors and eavesdropping by Eve, these

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

data should agree. As seen in table 3 Bob will guess right with a probability of 50%, if Eve was also measuring (and not interfering with the quantum state) she would also detect right 50% of the time, but this would on average only match 50% of Bobs right detections, so Eve would actually only get a 25% sample of the key. It is even more elegant than that; the very act of Eve measuring will affect the quantum state of the photons and therefore, Bob's results producing errors between Alice and Bob.
Alice and Bob have now produced a stream of unpredictable bits known only to them (table 3).

Alice sends:										
	1	0	0	0	0	1	1	1	0	0
Bob's detector:	+	x	x	+	x	x	+	+	+	x
Bob measures:	0	0	0	0	0	0	1	1	0	0
Retained bits:	-	0	-	0	0	-	-	1	0	0

Table 3. QKD bit exchange between Alice and Bob.

To decide if Eve has tampered with the quantum states, they now choose a random subset of the polarisation data, which they can publicly announce, and chose not use as part of the key, from there, they can compute the error rate (that is, the fraction of data for which their values disagree). If the error rate is unreasonably high –above, say, 10% --they throw away all the data (and perhaps try again later. If no signs of eavesdropping are found, they have a shared key that is guaranteed to be secret. The key generated by QKD can subsequently be used for both encryption and authentication, thus achieving two major goals in cryptography. The random string of binary shared between Alice and Bob can now be used to encrypt their secret message through an XOR (⊕) gate (0⊕0=0, 1⊕1=0, 0⊕1=1 and 1⊕0=1). eg.

Encryption mechanism	
Key:	0 0 0 1 0 0
XOR gate:	⊕⊕⊕⊕⊕⊕
Alice's plain text:	1 0 1 0 1 0
Cipher text:	1 0 1 1 1 0
Decryption mechanism	
Cipher text:	1 0 1 1 1 0
XOR gate:	⊕⊕⊕⊕⊕⊕
Key:	0 0 0 1 0 0
Bob's plain text	1 0 1 0 1 0

Other QKD schemes have, been proposed. For example, Artur Ekert of the University of Oxford [18] suggested one based on quantum mechanically correlated (that is, entangled) photons, using Bell inequalities as a check of security. In 1992, Charles Bennett of IBM proposed another QKD scheme, called B92, [19] that uses only two polarisation states (45º and 90º) not the four polarisation states (0º, 45º, 90º and 135º) of the BB84 protocol. If a bit is detected by Bob he must have chosen the correct detector and a comparison of basis over an open channel does not even need to be preformed, although Alice needs to be informed of detection or no detection. The B92 protocol has

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

advantages in the eavesdropping detection but requirement of authentication of Alice and Bob is clearly necessary.

Is it practical?

Various groups around the world are currently undertaking the practicalities of a QKD scheme. Recently a world record was set of a quantum key exchange over 67 kilometres of Swisscom fiber-optic telephone network by a research group in Switzerland,[20] and Richard Hughes team from Los Alamos[21] are achieving atmospheric quantum key exchanges of 30 kilometres. As of February 2002, you can now buy a Plug and Play QKD system from a Swiss company[20] offering key exchange speeds of 4000Bit s^{-1} over 10 kilometres. The technology is there now and is usable over reasonable distances, there will be limitations, and I will leave this open for a future researcher to explore.

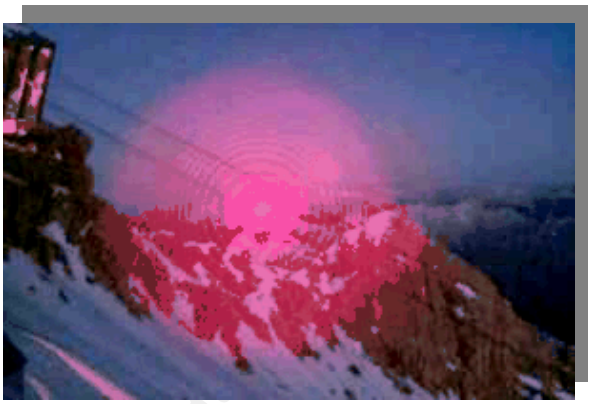


Image: Harald Weinfurter, Christian Kurtsiefer and Patrick Zarda

Figure 6. Alignment laser.

Conclusions

Quantum computers are being developed but clearly, a lot of work lies ahead. Quantum algorithms will be capable of solving currently intractable mathematical problems exposing classical cryptography; QKD is here now and will be used by some organizations wanting unconditional security. QKD is useable and offers provable security, but it has not had the exposure of the global community attacking the system, and we, as security professionals are all taught security is a process not a product. So QKD may be provably secure but wether QKD is secure is yet to be proven.

Additional research

- Background interference and error correction.
- Limitations.
- Privacy amplification.
- Authentication of both; sender and receiver.
- Denial of service attacks on QKD.
- Eavesdropping.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. al-Kinidí, Abú A Manuscript on Decrypting Cryptographic Messages. (9th Century)
2. Moore, Gordon (1965) online: "Moore's Law." available:< http://www.webopedia.com/TERM/M/Moores_Law.html > (October 2002)
3. Anderson, Mark K. (2001) online: "Quantum Crypto to the Rescue." available:< http://www.wired.com/news/infostructure/0,1377,46610,00.html > (October 2002)
4. Singh, Simon The Code Book. Fourth Estate Limited, LONDON, ISBN 1-85702-889-9, (1999).
5. Kerckhoffs von Nieuwenhof, Auguste La Cryptographie militaire. (1883)
6. Kahn, David Seizing The Enigma. Houghton Mifflin, NEW YORK, (1991).
7. Carlson, Andy (2002) online: "enigma emulator.", available:< http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html > (October 2002)
8. Central Intelligence Agency – director of Central Intelligence < http://www.odci.gov/ > online: "Venona: Soviet Espionage and the American Response, 1939-1957" the section "What made Venona possible?" available: < http://www.odci.gov/csi/books/venona/preface.htm > (October 2002)
9. Schneier, Bruce Secrets and Lies: digital security in a networked world. John Wiley & Sons Inc., NEW YORK, ISBN 0-471-25311-1, (2000).
10. Shannon, Claude Communication Theory of Secrecy Systems. (1949)
11. Evans, David (2001) online: "Lecture 2 perfect ciphers." available:< http://www.cs.virginia.edu/~evans/cs588/lectures/lecture2.pdf > (October 2002)
12. Schneier, Bruce Applied Cryptography 2nd Edition. John Wiley & Sons Inc., NEW YORK, ISBN 0-471-11709-9, (1995).
13. Shor, Peter (1997) online: " Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." available:< http://www.research.att.com/~shor/papers/ > (October 2002)
14. Grover, Lov (1998) online: "Annual ACM Symposium on the Theory of Computing (STOC)." available:< http://www1.bell-labs.com/user/lkgrover/ > (October 2002)
15. Clark, Robert (2000) online: " University of New South Wales team producing quantum computer breakthrough." available:< http://www.unsw.edu.au/news/22_08_00_computer_news.html > (October 2002)
16. Wiesner, Stephen SIGACT News. 15, 78 (1983)
17. Bennett, Charles and Brassard, Gilles IEEE International Conference on Computers, Systems, and Signal Processing.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IEEE Press, LOS ALAMITOS, p. 175. (1984), The first paper on quantum cryptography was written by Stephen Wiesner around 1970, but it remained unpublished until 1983: Wiesner, Stephen SIGACT News. 15, 78 (1983)
18. Ekert, Artur (2000) online: "Top secret." available:< http://www.nature.com/nsu/000504/000504-6.html > (October 2002)
19. Bennett, Charles Quantum Cryptography: Uncertainty in the Service of Privacy Science 257, p. 752-3 (1992)
20. id Quantique. 10 rue Cingria, 1205 Genève, Switzerland. available: < http://idquantique.com > (October 2002)
21. Hughes, Richard (2002) online:" Practical free-space quantum key distribution over 10 km in daylight and at night." available:< http://www.iop.org/EJ/S/UNREG/abstract/1367-2630/4/1/343/ > (October 2002)

Graphics credits

- Optic fibres mage: Ivan Noble -BBC-online
- Figure 2.An Enigma machine. Simon Singh
- Figure 3. A Vernam one-time pad. Brooke Clarke
- Figure 4. and 5 graphics. id Quantique
- Figure 6. Alignment laser. Harald Weinfurter, Christian Kurtsiefer and Patrick Zarda

© SANS Institute 2003, Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**