Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)

GSEC Assignment Version 1.4b

Option 1 – Research on Topics in Information Security

Lawrence H. O'Neill Jr.

Quantum Mechanics and Security

By Lawrence H. O'Neill Jr.

25 July 2003

Abstract

Quantum mechanics both threaten and promise to protect the security of electronic communications. Robust protection appears to be considerably closer than the threat.

Public-key encryption systems, non-existent until the 1970s, are now ubiquitous in secure transactions for which it would be cumbersome and expensive to distribute cryptographic keys, in advance, over physically secure channels. All such systems, for example the familiar RSA (after Rivest, Shamir, and Adleman), depend upon the supposed intractability of inverting certain operations on large integers, which operations are efficient in the forward direction. Since 1994, however, it has been known that inversion of the two operations most commonly used in public-key encryption would not be intractable to a hypothetical quantum computer, that is a computer that relies essentially upon the ability of a quantum-mechanical system to exist simultaneously in a superposition of elementary states until one such state is actually observed.

Quantum computers of very modest capability have actually been realized. There are formidable obstacles to building ones both large enough to be more capable than existing digital computers and robust enough to be useable in practice. Nevertheless, the eventual advent of quantum computers that will overcome presently intractable problems appears very likely, especially since encouraging and surprising insights have been gained into possible ways of making such devices resistant to perturbations from the environment.

An additional threat to the security of public-key communications, which has nothing to do with quantum computers, is worth noting: It has never been rigorously demonstrated that the reversibility problems upon which this security depends are really even intractable in the usual sense. It is obviously very difficult to estimate the seriousness of this threat. The problems have survived three decades of highly-motivated attack by specialists worried about encryption, and undoubtedly many more by pure mathematicians. But Fermat's Last Theorem fell after three centuries.

Methods exploiting quantum mechanics are known that can provide for the secure distribution of cryptographic keys at the speed of light. Some have actually been demonstrated in practice over limited distances. These methods do not prevent the interception of a key, but any such interception will be evident to the authorized users before the key is used. The laws of quantum mechanics guarantee strictly that no amount of delicacy or subtlety in the method of interception can avoid detection.

Keys known to be un-compromised can then be used to encrypt messages using methods that do depend upon the prior distribution of keys. While, strictly speaking, the problem of prior distribution, which motivated the invention of public-key systems, is not avoided, distribution is made sufficiently fast and convenient that it is no longer a practical obstacle.

Even private-key encryption systems may be subject to successful attack by quantum computers. In fact they have sometimes even been broken by regular computers, as a number of well-known war stories make clear. But rapid, electronic distribution of cryptographic keys will make it feasible to use keys that are random bit strings as long as the messages they encrypt. In that case, the "One-Time-Keypad" encryption algorithm can be used. This is the only algorithm rigorously shown to absolutely unbreakable. No computer, quantum or otherwise, no matter how fast, can make any sense out of cipher text produced by this algorithm. An exhaustive trial of all possible keys, even if feasible, simply produces all possible clear texts, whether comprehensible or meaningless, that fit into the given number of bits. There is no way of deciding which one is correct.

Quantum key distribution appears to be far ahead of quantum computing, so that from the point of view of security, the defense will win over the offense almost certainly.

Introduction

Cryptography seems to have arisen gradually among the ancient Egyptians, starting about 3,000 years ago [1]. In spite of its tremendous political, military, and commercial importance for such a long time, it was always taken for granted, almost down to our own time, that there was nothing a recipient could infer from

an encrypted message that a third party who intercepted the message could not also infer, unless the sender and the intended recipient had exchanged some secret information not available to the third party. As a modern web site [2] puts it, this seems like common sense. With no different, a-priori information, the intended addressee and the interceptor would seem to be in the same position.

Thus arises the key-distribution problem. With traditional, secret-key algorithms, cryptographic keys have to be distributed in advance of any communication, through channels that are not just as insecure as the one thought to require encryption in the first place. This tends to be slow, involving couriers with locked briefcases or the like, and it tends to limit the frequency with which keys are changed. Furthermore, until the advent of electronic data processing and magnetic storage media of tremendous capacity, practical considerations made it very advantageous to keep keys short. First, encryption by manual methods is very tedious and error-prone if it involves long keys. Second, physical transportation of very many, very long keys on paper becomes impractical.

The result is that encrypted messages tend to be sent rapidly via electronic media, then decrypted using short, infrequently changed keys. The ratio of message bits to key bits consumed in decrypting the messages tends to be very large. This was not uniformly so. In 1918, Gilbert S. Vernam of AT&T and Major Joseph O. Mauborgne of the US Army Signal Corps, developed what is now known as the “Vernam” or “One-Time Keypad,” or simply “One-Time Pad” algorithm [3]. It had the feature that the key included as many bits as the message. It was not widely used because of the cumbersomeness of distributing the keys. The “pad” refers to a literal pad of paper that an agent would have to carry around. A string of key information would be taken from one page, which then had to be destroyed to make sure it was never used again.

The significance of these circumstances was not clearly appreciated until after the Second World War. It turns out that any message or set of messages having more bits than the key bits consumed in encrypting it will always leave some trace of the original clear text in the encrypted text. That means that an adversary possessing the cipher text can at least infer more about the probabilities of all the possible clear text messages than he can know a priori. This was proved by C.E. Shannon of Bell Laboratories, but not until 1949 [4]. Shannon also showed ([4] page 682) that the Vernam code does realize what he called “perfect secrecy.” That is for any possible, intercepted cipher text, the probability of any given clear text is the same as it was a-priori. With the cipher text but without the key, the interceptor knows absolutely nothing more about which clear text message, of all the ones possible, is likely to have been sent than he would know without the cipher text.

This does not mean that codes with keys much shorter than the message are actually feasible to break. Shannon’s results do not mean that actually calculating the probabilities of the possible clear texts is tractable. (Typically, as more cipher

text is obtained, the probability of the correct clear text rises to near unity and the sum total probability of the other possibilities rapidly approaches zero. This is the basis of cryptanalysis. One wants the one message actually sent, not a spectrum of probabilities.) Indeed, the modern Data Encryption Standard (DES) [5] has served well for many years with the startling short key of fifty-six (56) independent bits. It has been broken, albeit with tremendous resources [6], and is now being superseded by Advanced Encryption Standard (AES) [7], which can accommodate keys of various lengths as the desired level of security may require.

On the other hand, some famous codes have turned out to have subtle flaws that revealed the correct clear text very rapidly. The most famous of these is undoubtedly the German "Enigma" of the Second World War. Several accounts of the successful British effort to defeat this system have been published [8].

Public Key Systems

The old insight that the intended recipient of an encrypted message must have some more information than an interceptor is actually correct, but, by the 1970s, several investigators had realized that the extra information possessed by the addressee need not be known to the sender. In 1976, Diffie and Hellman [9], referencing originally independent work by Ralph Merkle published a method that would in principle allow two parties to arrive at a common, secret key which had itself never been sent from one to the other. Nor could a third party feasibly infer what the secret key is from anything that is sent. The method depends upon the fact that certain operations on large integers are efficient to carry out in one direction but apparently intractable in the other.

The Diffie-Hellman method allows secure communications with one other party but provides no method of assuring that that party is who he claims to be. Thus it is vulnerable to the so-called "Man in the Middle" attack.

Rivest, Shamir, and Adelman at MIT became interested in Diffie, Hellman, and Merkle's work and developed a practical implementation based upon the difficulty of factoring a composite integer with two very large prime factors. RSA also provided for digital signatures that a "Man in the Middle" could not reproduce. After some struggle with the US National Security Agency (NSA) [2], Rivest, Shamir, and Adleman published their results in 1978 [10]. Their algorithm has become a cornerstone of Internet commerce.

While no algorithm is know that efficiently factors large composite integers, there is no proof that none exists [11]. ("Algorithm" is used here in the sense of a procedure that would run on a conventional, digital computer. "Efficiently" is used here in the usual computer-science sense: The amount of time required by an efficient algorithm would grow no faster than some polynomial in the length of the composite integer.) If such an algorithm were to be found, RSA would fall.

Furthermore, even if the factorization problem is in fact intractable, there is no proof that some algorithm other than factorization would not defeat RSA. In contrast, the Blum Blum Shub random number generator [12], which can also be used in public-key cryptography [13], has been shown to be exactly as hard as the factorization problem [11], so that if the latter is in fact intractable, Blum Blum Shub is secure against conventional algorithms.

In 1994, however, Peter Shor [14] showed that a so-called "Quantum Computer" could in fact solve the factorization problem "in polynomial time," meaning that the time taken to solve the problem would be bounded by a polynomial in the size of the problem, in this case the length of the composite integer. An updated version of his original work is available at [15].

Quantum Computers

A quantum computer [16] exploits the deeply-counterintuitive fact that the same quantum mechanical system can exist simultaneously in a superposition of all the states it is capable of occupying. When a measurement is made to determine what state it is in, it jumps to just one. Which one is not determined, but each has a probability controlled by the original state, before the observation. This has the consequence that an operation, such as the application of a radio-frequency pulse to the system, in effect operates on all the simultaneous states at the same time. This in turn enables a massively parallel mode of computation.

The difficulties of practical implementation are formidable, particularly because a quantum system is easily disturbed by interaction with its environment. Nevertheless, great insights are being achieved into ways of stabilizing quantum computers by spreading the information they contain across multiple components of the system. This makes the information much more robust than it would be if it resided in, say, the angular momentum of individual atomic nuclei.

Memories of quantum computers are sized in "qubits," as the coined term has it. A "qubit" is the amount of information that can be contained in a quantum mechanical system that can be observed in either of two discrete states. In sharp contrast to a classical switch, the quantum system can exist simultaneously in a superposition of the two states. When a measurement is made to determine which state, the system jumps to one or another of the states, with statistical probabilities that depend upon how the system was set up before the measurement. The choice of the two alternative states is not unique. For example, a photon's polarization can be measured to determine whether it is horizontal or vertical. If that is the nature of the measurement, it will always appear unambiguously in one or the other of those polarization states. But the choice could have been made in advance to measure whether the photon was in one or the other of the two diagonally polarized states. In that case, the photon will be measured as being unambiguously in one or the other of the diagonal states. This is wholly counterintuitive and different from anything in classical

physics. It accounts for the fact that quantum computers can in effect operate simultaneously on a huge number of arrays of numbers.

Quantum computers to threaten the factorization problem, or anything else now intractable, seem to be far away. They would have to be machines with hundreds or thousands of qubits [17]. The largest quantum computer made so far has seven [18], and the method used to achieve this will not scale to much larger numbers. One estimate, made this year (2003) by the aforementioned Peter Shor, is that a thirty-qubit machine is ten years off. Another estimate from this year from the National Institutes of Standards and Technology (NIST) is in rough agreement: A fifty-qubit system should be ten or twenty years away [19]. Obviously no one can rule out a startling breakthrough. On the other hand, no one can be sure that quantum computers will not become a nuclear-fusion-like problem, and remain frustrating for many decades.

Quantum Encryption

By contrast, encryption methods that employ the features of quantum mechanics are in some reasonable sense already here. Quantum encryption works by setting up quantum mechanical systems, say photons, in certain states, such as horizontal or vertical polarization, so that the systems carry information. Horizontal = 0; vertical = 1, for example. But, as mentioned above, the choice of such basic states is not unique. In the case of a photon, the choice might be diagonally polarized one or the other way, or left-circularly versus right-circularly polarized. If a sender does not announce in advance which choice he is making for a particular system, photon or whatever, an interceptor detecting the system will not know what type of measurement to make on it. Neither will the intended recipient, but this problem can be repaired as well shall see. Suppose the sender transmits a long string of bits intended for subsequent use as a cryptographic key. At random he chooses whether to encode the bits as horizontally-polarized photon = 0; vertically-polarized photon = 1, or lower left to upper right =0; upper left to lower right = 1. Anyone receiving the photon can only guess which type of measurement to make. The Heisenberg Uncertainty Principle, which is fundamental to quantum mechanics, strictly precludes his making both measurements at the same time, and in any sequential pair of measurements, the earlier one will ruin the reliability of the later. If he guesses wrongly and makes, say, a diagonal measurement when the photon has been launched in a rectilinear (horizontal or vertical) state, he will observe the two diagonal polarizations randomly, with 50/50 probability, no matter whether the sender created a horizontally or vertically polarized photon. To cover his tracks, he must then send out a photon in the polarization state he has observed. But if the intended receiver is making the correct measurement – we come in a moment to how this is arranged – he will get the two possible results of his measurement with 50/50 probability, irrespective of what the sender sent or the interceptor re-sent. If the interceptor made the wrong guess every time, the intended receiver

would get a bit error 50% of the time. If, more plausibly, the interceptor guesses randomly and is wrong half the time, the receiver has a net bit-error rate of 25%.

The procedure is for the transmission to take place with no announcement of how the sender is initializing the systems he is sending, rectilinear or diagonal for example. The intended receiver guesses at random which type of measurement to make. After the transmission is complete, the intended receiver announces, over an unencrypted channel, bit-by-bit, which measurement he has made, but not the result. For example, for bit 28,874, he states that he has made the rectilinear measurement but not the fact that the result was vertically polarized, that is bit-value 1. The sender and receiver then both discard the bits for which the wrong measurement has been made.

If anyone has been intercepting the traffic, no matter how delicate or subtle his technique, the fundamental rules of quantum mechanics ensure that the intended receiver will have a large fraction of wrong bits. The sender and the intended receiver can then apply various statistical tests, such as parity checks on blocks, to exclude this possibility, at the cost of having to discard a small fraction of the data. For example, if a parity check is done on a block, the last bit of the block can be discarded. This destroys the utility of the parity result to anyone listening in. All this checking can be done in the clear over an unencrypted channel. It is worth noting that the intended receiver must still be authenticated in order to exclude the interceptor from being the "Man in the Middle." Methods for doing interception detection, and also handling innocent errors that arise from noise in the transmission channel, bits that are simply lost due to attenuation, dark noise in the detector, and so on, are discussed in somewhat more detail in [20].

There appear to be three fundamental ideas for doing quantum cryptography [21]. The first, called "BB84" because it was proposed by the Bennett and Brassard of [20] in 1984, is what has just been described. The second is based upon the Einstein-Poldosky-Rosen (EPR) effect in quantum mechanics. It makes use of the fact that two quantum systems can be interdependent, so that if a measurement is made with a certain result on one, the result of a similar measurement on the other is instantly predetermined, even though the systems may by then be far apart. If, for example, an atom with no angular momentum drops to a lower quantum energy level and sends out two photons, they must have opposite polarizations. The photons may fly far apart. The polarization of either is random, equally likely to be vertical or horizontal. But as soon is one is observed to be vertical, it is certain that a measurement on the other, if the rectilinear measurement is made, will be horizontal. This so even if the photons are by this time a kilometer apart and are detected simultaneously, so that there is no time, even at the speed of light, for information from one measurement to reach the site of the other. This is very counter-intuitive and hard to reconcile with classical ideas about causality. It refutes the classical idea that each photon must "really" be polarized one way or the other before a measurement on it is made, while the measurement does nothing more than remove the observer's

ignorance. It ties into the fact that a quantum system can exist simultaneously in superimposed, classically incompatible, states until a measurement is made on which state it is in. In this case, the system is the set of both photons.

In the EPR encryption scheme, the sender generates photon pairs as just described. He stores one – very hard in practice – and sends the other one to the intended receiver, who stores it – equally hard. Sender and receiver make immediate polarization measurements, randomly choosing rectilinear or diagonal, and detect interception in the same general way as in BB84. EPR has the advantage that the rest of the photons, still stored, remain correlated. This has the effect that, should an adversary manage to detect even the stored information, after it has arrived, this too would be detectable. EPR is not yet feasible in practice because of the difficulty of bouncing photons back and fourth between reflectors without loss for more than a tiny fraction of a second.

A third, conceptual, method of quantum cryptography has been proposed by the Bennett of BB84 [22]. In this approach, the sender prepares some quantum system to be transmitted in one of two states. This is fairly abstractly described in [22]. It is shown that the user can contrive to make two kinds of measurement, each of which yields a signal on one state and simply nothing on the other. The sender constructs the two states at random and the receiver makes the two types of measurements at random. In contrast to BB84 and EPR, in which the wrong type of measurement yields random results, here the wrong type of measurement yields no result. The receiver communicates to the sender, in the clear, for which bits he has obtained a result, but not which measurement he made. The sender discards the other bits. For the remaining bits, the sender knows which state he sent and the receiver knows which measurement he made, and hence which state was sent. The two versions of the key are identical, unless there has been eavesdropping. As in BB84 and EPR, any observation by a third party will cause some of the systems arriving at the receiver to be in a different superposition of states from what was transmitted. This will sometimes result in the receiver making a positive but incorrect measurement. This can be detected by doing error checking in the clear, in a way generally similar to what is done for the other two schemes. The last scheme is in a sense simpler than the first two because the system being transmitted is only initialized in one of two states, not four, such as vertical, horizontal, lower left to upper right, upper left to lower right.

The reader will have noted that each of the three schemes just discussed merely detects interception of the signal; none of them prevents it. For this reason, these methods are suitable for transmission of the encryption key, not the message itself. Only after transmission of the key is complete and the integrity of the data is verified can the actual message be sent. Now that both parties have the same, secret key, the message can be encrypted by conventional means and sent over a regular communications channel.

Electronic transmission of encryption keys offers the possibility that this distribution could be effected rapidly and efficiently. That in turn would solve the age-old key-distribution problem and reduce dependence upon public-key systems, the reliability of which, as we have seen, will probably eventually disappear.

If reasonably high data rates can be achieved for quantum key distribution, the advantages of keeping keys short will also become much less persuasive. This means that the absolutely and provably secure Vernam system can be much more widely adopted. Vernam is safe even against quantum computers, or any computer, no matter how fast.

Practical Problems

The main practical obstacle to quantum key distribution is the problem of preserving the delicate quantum states of the particles being transmitted when transmission takes place over great distances. Optical fibers attenuate light, and photons sent through them eventually disappear. Impressive progress has been made nevertheless. Researchers in Switzerland have recently effected quantum key exchange over a distance of sixty-seven (67) kilometers, using the fiber-optic infrastructure of the Swiss telecommuncations network [23].

In principle, the distance problem could be overcome by periodically placing regenerators. Each adjacent pair would establish a secure key, then hand it on as in a bucket brigade. The present author has encountered only a vague reference to this idea [24]. Unlike the links among them, the regenerators themselves would have to be physically tamper-proof. There is probably no way to bomb-proof them, but it should not be too difficult to arrange that they fail safe, that is simply erase volatile memory and stop working as soon as they are opened.

If eventually the EPR scheme can be made to work, perhaps just to detect interception, not reading of the stored key, the distance problem may be attacked in a more straightforward way by linear amplification. According to the American Institute of Physics [25], laser-like amplification of correlated, “entangled” in the usual jargon, particles has been demonstrated. It is not immediately obvious how this would work. As Bennett et al. [20] point out, the BB84 scheme will not work with a big pulse of coherent photons. An interceptor can just split out a small fraction of them and measure the polarization classically. The interceptor would not have to retransmit any photons to cover his tracks. However, if this were done with EPR, whether the interceptor retransmitted or not, the polarizations of some of the photons retained by the sender would still be entailed in the results of the interceptor’s measurement. This is in principle detectable. (In this scenario, the sender is not retaining photons for seconds, but only for as long as it takes the sent photons to propagate through the communications channel, which might actually be feasible.) This explanation of how coherent amplification might work

with EPR is based solely upon the present author's reasoning and is not given or supported by [25].

An approach that would overcome the material absorption of light in glass would be to send keys through air and space via satellites. The physical security of the satellite should not be much of a concern unless the adversary is enormously capable, and even then, tampering would not go undetected. Surprisingly, British researchers have already done a conceptual design and performance analysis on such a system [26]. They believe that secure key distribution rates on the order of 1000 bits/second are feasible, only at night, and using a low-orbit, not a geostationary satellite. Thus one must not only wait for night but also for a satellite that is more or less overhead. Satellites immediately open the prospect of key distribution worldwide. Although the rates seem modest, keys could be accumulated at remote points whenever possible, then consumed in large bursts when big files have to be transferred.

If quantum-key distribution rates are limited, such distribution still offers an attractive compromise: Use the quantum channel to update keys for conventional algorithms, such as AES, not so fast as the data rate, but very much faster than otherwise feasible. According to Shannon's fundamental results [4], this makes cryptanalysis essentially harder, if not necessarily fundamentally impossible. In fact, the Swiss experiment mentioned above was carrying out just such a scheme [27].

Researchers from Northwestern University have demonstrated a prototype quantum system, running at 250 Mbits/s, that encrypts not the key but the data themselves [27]. The reader will note that the foregoing discussion has explained why such a scheme will not work. An explanation of how this system nevertheless does work is beyond the scope of the present paper. (That means that the author does not know.) The same researchers are forecasting a quantum-encryption system running an order of magnitude faster, 2.5 Gbits/s, within five years. This would be typical of the speeds of single optical carriers on the Internet backbone. The scheme would use not four but 4,096 different polarization angles. The present author infers from [27] that it would also require some kind of secret key exchange between sender and intended recipient.

The Last Mile

Should a highly secure Internet backbone in fact come into being, it will need to be borne in mind that the security chain is as strong as its weakest link. It seems likely that very sophisticated security systems will become cost-effective at major nodes of the Internet, but not at the residence or even enterprise. If RSA and similar techniques do fall, it will be urgent to consider the problem of securing the so-called "Last Mile," a chronically troublesome component of the Internet. The author would like to suggest that pending fiber-to-the-home systems would inherently reduce vulnerability by drastically reducing electromagnetic fringe

fields. The mechanical fragility of glass fiber makes it difficult to tap. Perhaps the difficulty of eavesdropping on the last mile, and the more limited economic utility of doing so, may provide sufficient protection to such things as routine credit-card purchases.

Another idea is that mass data-storage devices of very low cost could be physically distributed from time to time by Internet service providers. These would not need to contain enough key bits to cover all traffic. They could just be consulted when a secure transaction was taking place. They would effect a Vernam encryption to and from some suitable node in the provider's network, beyond which quantum methods would take over. Distribution could simply be through the mail. Digital signatures by the customer's computer would defeat "Man in the Middle" attacks should the device be stolen on the way to the customer.

Summary

Quantum mechanics both threaten and protect the security of modern, electronic communications. On present evidence, the defense seems far ahead of the offense, and we may be a decade or so away from universal, provably secure communications, at least for those transactions where such is reasonably needed.

References:

1. The Code Breakers, David Kahn, Scribner, New York (1996), in particular, page 72.
2. http://livinginternet.com/?i/is_crypt_pkc_inv.htm
3. Quantum Cryptography, Paul Lofthouse. http://216.239.39.104/search?q=cache:EviqnG-JFukJ:www.qmechanics.supanet.com/quantum%2520cryptography.doc+Gilbert+S.+Vernam&hl=en&ie=UTF-8
4. Claude E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal,* vol 28-4, page 656 – 715, 1949. Available online at: http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf
5. *http://www.itl.nist.gov/fipspubs/fip46-2.htm*
6. *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html*
7. *http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html*
8. The present author found G. Welshman, *The Hut Six Story: Breaking the Enigma Codes*, McGraw-Hill; (March 1982) to be enlightening.
9. W. Diffie and M.E. Hellman, *New directions in cryptography, IEEE Transactions on Information Theory* **22** (1976), 644-654.

10. Rivest, R.; Shamir, A.; & Adelman, L. (1978). “A Method for Obtaining Digital Signatures and Public Key Cryptosystems.” Communications of the ACM, February 1978. Online at: http://citeseer.nj.nec.com/cache/papers/cs/517/http:zSzzSztheory.lcs.mit.eduzSz~ciszSzpubszSzrivestzSzrsapaper.pdf/rivest78method.pdf
11. http://www.wikipedia.org/wiki/Integer_factorization
12. http://www.wikipedia.org/wiki/Blum_Blum_Shub
13. http://engr.oregonstate.edu/~mundle/ECE679/mundle-gawande.pdf
14. http://www.research.att.com/~shor/papers/index.html
15. http://www.research.att.com/~shor/papers/QCjournal.pdf
16. http://www.cs.caltech.edu/~westside/quantum-intro.html
17. http://www.msnbc.com/news/269473.asp#BODY
18. http://www.abc.net.au/science/news/stories/s796909.htm
19. http://www.trnmag.com/Stories/2003/022603/Quantum_computing_catches_the_bus_022603.html
20. C.H. Bennett, G. Brassard, and A.K. Ekert, “*Quantum Cryptography*”, Scientific American, October 1992, p. 50
21. http://www.qubit.org/library/intros/crypt.html
22. Charles H. Bennett, “*Quantum Cryptography Using Any Two Nonorthogonal States*”, Physical Review Letters, Vol. 68, No. 21, 25 May 1992, p. 3121. Online at: http://www.research.ibm.com/people/b/bennetc/qc2nos.pdf
23. http://physics.iop.org/IOP/Press/PR5802.html
24. http://www.nsf.gov/pubs/2000/nsf00101/nsf00101.htm#c4
25. http://sci.newsfactor.com/perl/story/13468.html
26. http://www.iop.org/EJ/article/1367-2630/4/1/382/nj2182.html
27. http://www.eetimes.com/at/news/OEG20021111S0036

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event