Partial Key Exposure attack on RSA—Lattice Dimensions

G.Premnath, Dr.A.Nageshwaran
Research scholar CMJ university
Veltech Technical University Chennai

Abstract:

Secure communication without Eavesdropping is a major issue. Though initially Internet and other networks were built for universities , its applications have reached fields like business and e-commerce where sharing of private and critical details like credit card numbers should not exposed to attack of Eavesdropping . In recent times many schemes have been published and implemented like systems involving RSA algorithm for public key encryption which are based on unproven computational difficulty of certain mathematical functions. These schemes have been shown to break progressively over the years , leading to an increase in the complexity of the schemes used to establish a secure communication. The complexity has nowadays reached its limits ,thus hampering communications with regard to the speed . We wish to present quantum cryptography which is seen as uncrackable and a thing of not-so-far future . It relies on the cutting edge laws of physics like quantum properties of some matter (sub atomic particles ,photons) to establish a secure way to share a public key. It is still in the infant stages of development with constraints regarding duplicate channel , photon generation and recognition equipment . So there is lot of scope for study in the field encryption systems with new algorithms to break the existing ones in record time and thus paving way for quantum cryptography as the future.

1.Cryptography - an Overview

Cryptography, a word with greek origins, means “secret writing”**.** Cryptography referred to the encryption and decryption of messages using secret keys. Usually the enciphering of message and generating of the keys will be related to mathematical algebra (i.e number theory, linear algebra, and algebraic structures etc).using those mathematical relations we will change the messge in such a way that it can be again decrypted using some mathematical operations again.

2. Classical Cryptography

Cryptography is the art of devising codes and ciphers, and crypto analysis is the art of breaking themThere are two branches of modern cryptographic techniques: public key encryption and secret key encryption. In PKC, each participant has a "public key" and a "private key"; the former is used by others to encrypt messages, and the latter is used by the participant to decrypt them. One proposed method for solving the key distribution problem is the appointment of a central key distribution server. Every potential communicating party registers with the server and establishes a secret key. The server then relays secure communications between users, but the server itself is vulnerable to attack. Another method is a protocol for agreeing on a secret key based on publicly exchanged large prime numbers, as in the Diffie Hellman key exchange. Its security is based on the assumed difficulty of finding the power of a base that will generate a specified remainder when divided by a very large prime number, but this suffers from the uncertainty that such problems will remain intractable.

3. Breaking the public key

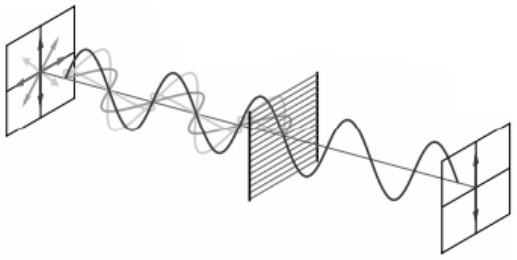
The RSA problem is defined as the task of taking *e*th roots modulo a composite *n*: recovering a value *m* such that $c=m^e \bmod n$, where (*e*, *n*) is an RSA public key and *c* is an RSA ciphertext. Currently the most promising approach to solving the RSA problem is to factor the modulus *n*. With the ability to recover prime factors, an attacker can compute the secret exponent *d (private key)* from a public key (*e*, *n*), then decrypt *c* using the standard procedure. To accomplish this, an attacker factors *n* into *p* and *q*, and computes $(p-1)(q-1)$ which allows the determination of *d* from *e*. When the numbers are very large, no efficient integer factorization algorithm is publicly known; a recent effort which factored a 200 digit number (RSA-200) took eighteen months and used over half a century of computer time. The presumed difficulty of this problem is at the heart of certain algorithms in cryptography such as RSA. Many areas of mathematics and computer science have been brought to bear on the problem, including elliptic curves, algebraic number theory, and quantum computing.

4 History of Quantum Cryptography

The roots of quantum cryptography are in a proposal by Stephen Weisner called ``Conjugate Coding'' from the early 1970s. It was eventually published in 1983 in Sigact News, and by that time Bennett and Brassard, who were familiar with Weisner's ideas, were ready to publish ideas of their own. They produced ``BB84,'' the first quantum cryptography protocol, in 1984, but it was not until 1991 that the first experimental prototype based on this protocol was made operable (over a distance of 32 centimeters). More recent systems have been tested successfully on fiber optic cable over distances in the kilometers.

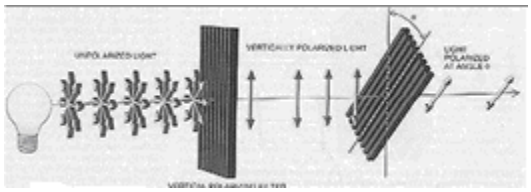
5.Quantum Cryptography Fundamentals

Electromagnetic waves such as light waves can exhibit the phenomenon of polarization, in which the direction of the electric field vibrations is constant or varies in some definite way. A polarization filter is a material that allows only light of a specified polarization direction to pass. If the light is randomly polarized, only half of it will pass a perfect filter.According to quantum theory, light waves are propagated as discrete particles known as photons. A photon is a massless particle, the quantum of the electromagnetic field, carrying energy, momentum, and angular momentum. The polarization of the light is carried by the direction of the angular momentum or spin of the photons. A photon either will or will not pass through a polarization filter, but if it emerges it will be aligned with the filter regardless of its initial state; there are no partial photons. Information about the photon's polarization can be determined by using a photon detector to determine whether it passed through a filter. "Entangled pairs" are pairs of photons generated by certain particle reactions. Each pair contains two photons of different but related polarization. Entanglement affects the randomness of measurements. If we measure a beam of photons E1 with a polarization filter, onehalf of the incident photons will pass the filter, regardless ofits orientation. Whether a particular photon will pass the filter is random. However, if we measure a beam of photons E2 consisting of entangled companions of the E1 beam with a



filter oriented at 90 degrees (deg) to the first filter, then if an E1 photon passes its filter, its E2 companion will also pass itsfilter. Similarly, if an E1 photon does not pass its filter then its E2 companion will not.

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that what direction to measure affects all subsequent measurements. For instance, if one measures the polarization of a photon by noting that it passes through a vertically oriented filter, the photon emerges as vertically polarized regardless of its initial direction of polarization. If one places a second filter oriented at some angle _ to the vertical, there is a certain probability that the photon will pass through the second filter as well, and this probability depends on the angle Θ. AsΘ increases, the probability of the photon passing through the second filter decreases until it reaches 0 at Θ = 90 deg (i.e., the second filter is horizontal). When Θ = 45 deg, thechance of the photon passing through the second filter is precisely 1/2. This is the same result as a stream of randomly



polarized photons impinging on the second filter, so the first filter is said to randomize the measurements of the second.

6.Polarization by a filter

Unpolarized light enters a vertically aligned filter, which absorbs some of the light and polarizes the remainder in the vertical direction. A second filter tilted at some angle Θ absorbs some of the polarized light and transmits the rest, giving it a new polarization. A pair of orthogonal (perpendicular) polarization states used to describe the polarization of photons, such as horizontal /vertical, is referred to as a basis. A pair of bases are said to be conjugate bases if the measurement of the polarization in the first basis completely randomizes the measurement in the second basis, as in the above example with Θ = 45 deg. If a sender, typically designated Alice in the literature, uses a filter in the 0-deg/90-deg basis to give the photon an initial polarization (either horizontal or vertical, but she doesn't reveal which), a receiver Bob can determine this by using a filter aligned to the same basis. However if Bob uses a filter in the 45-deg/135-deg basis to measure the photon, he cannot determine any information about the initial polarization of the photon . These characteristics provide the principles behind quantum cryptography. If an eavesdropper Eve uses a filter aligned with Alice's filter, she can recover the original polarization of the photon. But if she uses a misaligned filter she will not only receive no information, but will have influenced the original photon so that she will be unable to reliably retransmit one with the original polarization. Bob will either receive no message or a garbled one, and in either case will be able to deduce Eve's presence.

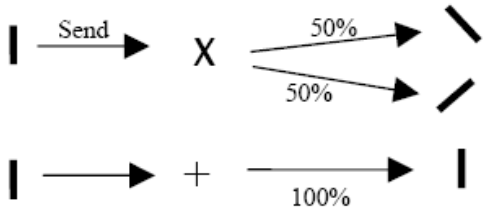
7. Quantum Cryptography Application

Sending a message using photons is straightforward in principle, since one of their quantum properties, namely polarization, can be used to represent a 0 or a 1. Each photon therefore carries one bit of quantum information, which measuring one property prevents the observer from{0,1}(rectilinear) and {+,-}(diagonal) form an orthogonal qubit state. They are indistinguishable from each other. To receive such a qubit, the recipient must determine the photon's polarization, for example by passing it through a filter, a measurement that inevitably alters the photon's properties. This is bad news for eavesdroppers, since the sender and receiver

can easily spot the alterations these measurements cause. Cryptographers cannot exploit this idea to send private messages, but they can determine whether its security was compromised in retrospect The genius of quantum cryptography is that it solves the problem of key distribution.

$$\begin{cases} |0\rangle \\ |1\rangle \\ |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

A user can suggest a key by sending a series of photons with random polarizations. This sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail.Alice and Bob are equipped with two polarizers each, one aligned with the rectilinear 0-deg/90-deg (or +) basis that will emit - or | polarized photons and one aligned with the diagonal 45-deg/135-deg (or X) basis that will emit \ or / polarized photons. Alice and Bob can communicate via a quantum channel over which Alice can send photons, and a public channel over which they can discuss results. An eavesdropper Eve is assumed to have unlimited computing power and access to both these channels, though she cannot alter messages on the public channel (see below for discussion of this). Alice begins to send photons to Bob, each one polarized at random in one of the four directions: 0, 45, 90, or 135 deg. As Bob receives each photon, he measures it with one of his polarizers chosen at random. Since he does not know which direction Alice chose for her polarizer, his choice may not match hers. If it does match the basis, Bob will measure the same polarization as Alice sent, but if it doesn't match, Bob's measurement will be completely random. For instance, if Alice sends a photon | and Bob measures with his + polarizer oriented either - or |, he will correctly deduce Alice sent a | photon, but if he measures with his X polarizer, he will deduce (with equal probability) either \ or /, neither of which is what Alice actually sent. Furthermore, his measurement will have destroyed the original polarization. To eliminate the false measurements from the sequence, Alice and Bob begin a public discussion after the entire sequence of photons has been sent. Bob tells Alice which basis he used to measure each photon, and Alice tells him whether or not it was the correct one. Neither Alice nor Bob announces the actual measurements, only the bases in which they were made. They discard all data for which their polarizers didn't match, leaving (in theory) two perfectly matching strings. They can then convert these into bit strings by agreeing on which photon directions should be 0 and which should be 1. This provides a way for Alice and Bob to arrive at a shared key without publicly announcing any of the bits.

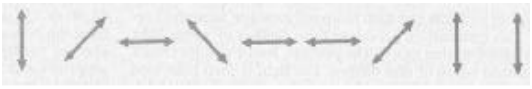


If an eavesdropper Eve tries to gain information about the key by intercepting the photons as they are transmitted from Alice to Bob, measuring their polarization, and then resending them so Bob does receive a message, then since Eve, like Bob, has no idea which basis Alice uses to transmit each photon, she too must choose bases at random for her measurements. If she chooses the correct basis, and then sends Bob a photon matching the one she measures, all is well. However, if she chooses the wrong basis, she

will then see a photon in one of the two directions she is measuring, and send it toBob. If Bob's basis matches Alice's (and thus is different from Eve's), he is equally likely to measure either direction for the photon. However, if Eve had not interfered, he would have been guaranteed the same measurement as Alice. In fact, in this intercept/resend scenario, Eve will corrupt 25 percent of the bits. So if Alice and Bob publicly compare some of the bits in their key that should have been correctly measured and find no discrepancies, they can conclude that Eve has learned nothing about the remaining bits, which can be used as the secret key. Alternatively, Alice and Bob can agree publicly on a random subset of their bits, and compare the parities. The parities will differ in 50 percent of the cases if the bits have been intercepted. By doing 20 parity checks, Alice and Bob can reduce the probability of an eavesdropper remaining undetected to less than one in a million.

An Illustration of Quantum Key Distribution

A quantum cryptography system allows two people, say Alice and Bob, to exchange a secret key. Alice uses a transmitter to send photons in one of four polarizations: 0, 45, 90 or 135 degrees. Bob uses a receiver to measure each polarization in either the rectilinear basis (0 and 90) or the diagonal basis (45 and 135); according to the laws of quantum mechanics he



cannot simultaneously make both measurements.(heisenberg's uncertainity principle)The key distribution requires several steps. Alice sends photons with one of the four polarizations, which she chooses at random.

For each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (X).Bob records the result of his measurements but keeps it a secret. After the transmission, Bob tells Alice the measurement types he used (but not his results) and Alice tells him which were correct for the photons she sent. This exchange may be overheard. Alice and Bob keep all cases in which Bob should have measured the correct polarization. These cases are then translated into bits (1s and 0s) to define the key.

8. Quantum Privacy Attacks

Quantum cryptography obtains its fundamental security from the fact that each qubit of information is carried by a single photon, and that each photon will be altered as soon as it is read once. This foils attempts to intercept message bits without being detected. Quantum cryptographic techniques provide no protection against the classic bucket brigade attack. In this scheme, an eavesdropper Eve is assumed to have the capacity to monitor the communications channel and insert and remove messages without inaccuracy or delay. When Alice attempts to establish a secret key with Bob, Eve intercepts and responds to messages in both directions, fooling both Alice and Bob into believing she is the other. Once the keys are established, Eve receives, copies, and resends messages so as to allow Alice and Bob to communicate. Assuming that processing time and accuracy are not difficulties, Eve will be able to retrieve the entire secret key, and thus the entire plaintext of every message sent between Alice and Bob, without any detectable signs of eavesdropping. Even if Eve does not practice interference of this kind, there are other methods she can still attempt to use. Because of the difficulty of using single photons for transmissions, most systems use small bursts of coherent light instead. By observing these photons.she might gain information about the information transmitted from Alice to Bob. A confounding factor in detecting attacks is the presence of noise on the quantum communication channel. Eavesdropping and noise are indistinguishable to the communicating parties, and so either can cause a secure quantum exchange to fail. This

leads to two potential problems: a malicious eavesdropper could prevent communication from occurring, and attempts to operate in the expectation of noise might make eavesdropping attempts more feasible.

9. State of Quantum Cryptography Technologies

Experimental implementations of quantum cryptography have existed since 1990, and today quantum cryptography is performed over distances of 30-40 kilometers using optical fibers. Essentially, two technologies make quantum key distribution possible: the equipment for creating single photons and that for detecting them. The ideal source is a so-called photon gun that fires a single photon on demand. That substitution creates a vacancy similar to a hole in a p-type semiconductor, which emits single photons when excited by a laser. Many groups are also working on ways of making single ions emit single photons. None of these technologies, however, is mature enough to be used in current quantum cryptography experiments.Most common is the practice of reducing the intensity of a pulsed laser beam to such a level that, on average, each pulse contains only a single photon. The problem here is the small but significant probability that the pulse contains more than one photon. This extra photon is advantageous for Eve, who can exploit the information it contains without Alice and Bob being any the wiser. Single-photon detection is tricky too. The most common method exploits avalanche photodiodes. These devices operate beyond the diode's breakdown voltage, in what is called Geiger mode. At that point, the energy from a single absorbed photon is enough to cause an electron avalanche, an easily detectable flood of current. To detect another photon, the current through the diode must be quenched and the device reset, a time-consuming process. Furthermore, silicon's best detection wavelength is 800 nanometers (nm, where 1 nm = one one-billionth of a meter), and it is not sensitive to wavelengths above 1100 nm, well short of the 1300- and 1550-nm standards for telecommunication. At telecommunications wavelengths, germanium (Ge) or indium-gallium-arsenide (InGaAs) detectors must be used, even though they are far less efficient and must be cooled well below room temperature. While commercial single-photon detectors at telecommunications wavelengths are beginning to appear on the market, they still lack the efficiencies useful for quantum cryptography. The distance that the key can be transmitted is also an important technical limitation. Beyond about 80 km of cable, too few photons make it from Alice to Bob. The range could be extended by devices that strengthen the signal as it passes by, like those used to send telephone conversations over long distances. However, unlike telephone repeaters, quantum versions would have to bolster the signal without measuring the photons. Scientists have shown that creating a repeater that doesn't measure is feasible in principle, but the technology to building one is a long way off. Satellites could provide an alternative means of achieving long-distance transmission.

10. Conclusion

Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry.

11. References

Basili V.R, and Perricone B.T. Software errors and complexity: an empirical investigation 0, Communications of the ACM (1984). 27-1, pp. 42 – 52.

Bhatkar S, DuVarney D. C, and Sekar R. Address obfuscation: an efficient approach to combat a broad range of memory error exploits. 12th USENIX Security Symposium, August 2003.

Canetti R, Dodis Y, Halevi S, Kushilevitz E and Sahai A. Exposure-resilient functions and all-or-nothing transforms, in Advances in Cryptology – EUROCRYPT, 2000, pp. 453-469.

Durden T. Bypassing PaX ASLR Protection. Phrack Inc., 2002 Available from URL http://www.phrack.org/issues.html?issue=59&id=9#article

Eichin M and Rochlis J. With microscope and tweezers: an analysis of the internet virus of november 1988. Proceedings of the IEEE Symposium on Security and Privacy, pages 326–343, May 1989.

Forrest S, Somayaji A, and Ackley D.H. Building diverse computer systems. HOTOS ’97: Proceedings of the 6th Workshop on Hot Topics in Operating Systems (HotOS-VI), pages 67–72, May 1997.

Foster J, Osipov V, Bhalla N, and Heinen N. Buffer Overflow Attacks: Detect, Expolit, Prevent. Syngress, 2005.

Garay J.A and Huelsbergen L. Software integrity using Timed excutable agents, in: Proceedings of the 2006 ACM Symposium on Information, computer and communications security (2006), pp. 189 – 200.

Garfinkel T, Pfaff B, Chow J, Rosenblum M, Boneh D. Terra: A virtual machine-based platform for trusted computing, ACM SIGOPS Operating Systems Review, pages 193 – 206, 2003

Goldman K, Perez R, and Sailer R. Linking remote attestation to secure tunnel endpoints, STC '06: Proceedings of the first ACM workshop on Scalable trusted computing, pages 21 - 24, 2006.

Harrison K. Protecting Cryptographic Keys from Memory Disclosure Attacks. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 137-143, 2007.

