JASS ’05 - Course 1

Alternative Approaches – Quantum Cryptography and Bounded Storage Model

Andreas Würfl

28th March 2005

Abstract

Several encryption algorithms have been discussed in the course of this seminar. This paper will introduce two alternative approaches. A change in the concept of provable security leads to a cipher which is shown to be ”perfect with high probability”. Assuming that the memory capabilities of a potential adversary are limited a strongly-randomized cipher is devised which uses a publicly-accessible string of random bits. In this cipher the secret key is short but the plaintext can be very long.

The second approach is based on quantum physics. Heisenberg’s uncertainty principle guarantees the security of quantum cryptography. The first experiment which demonstrated the practicability of the only known encryption unbreakable by law of nature was conducted in 1989. The physical and technical fundamentals are introduced as well as the Quantum Key Exchange (QKE) protocol. We will demonstrate the effects of attempted eavesdropping and its detection. Finally the rapid development of the last 15 years and the currently available implementations will be presented.

Contents

1 Introduction

Excluding approaches that are based on a generally unrealistic assumption about the enemy's knowledge and resources there are two types of crypto algorithms. Algorithms from the first group are based on the intractability of certain mathematical problems (e.g. factoring). These algorithms rely on the unproven assumption that certain problems are not efficiently solveable. Examples are the algorithms by ElGamal [ElG85] and the RSA Algorithm [RSA78]. The second group contains algorithms which may be provably secure but are impractical in most applications. The most prominent member of the second group is the one-time pad [Ver26].

In this paper we give a short introduction into two alternative approaches introduced by Brassard and Maurer respectively. First we have a look at quantum cryptography. We explain its physical and technical basics and the protocol used. The current state of research and development will be shown as well as the future applications. Second we consider the randomized cipher proposed by Maurer in [Mau92] which – under novel assumptions on the limitations of an attacker – provides provable security.

In the last decade quantum cryptography has seen a rapid developement and has now reached working status. The first commercial realizations[1] have been shiped only 14 years after the first working prototype was presented in [BenBra89]. It is not possible to address the technical problems that had to be solved within a few pages but the theoretical aspects of the only known encryption unbreakable by law of nature will be discussed throughly.

Maurer's randomized cipher has not been implemented for commercial use yet. This is not due to the computational complexity or possible security threads, which are promising, but due to the lack of a widely accessible source of randomness. Provided that there was such a source – which is already technically realizable – the randomized cipher is secure under the assumption that the enemy's memory but not necessarily his computational abilities are limited.

2 Physical and Technical Fundamentals

2.1 Heisenberg's Uncertainty Principle

In 1927 the German physicist Werner Heisenberg published his groundbraeking [Hei27]. This paper became one of the cornerstones of modern quantum physics and the author was awarded a Nobel Prize in 1932. Heisenberg proposed that given a quantum system it is impossible to measure a certain variable without perturbing the system and thus loosing information about the state of the quantum system before the measurement. On application of Heisenberg's Uncertainty Principle is the follwing inequality

$$\Delta p_x \Delta x \geq \frac{h}{2\pi}$$

where Δp_x is the uncertainty about the impulse and Δx is the uncertainty about the place of a given particle, $h \approx 6.6261 \cdot 10^{-31} Js$ is the PLANCK-constant[2]. It describes the highest possible accuracy one can obtain measuring the place and impulse of a particle simultaneously. While the above application is widely known there are a number of pairs of cunjugate variables that suffice this law of nature. For the purposes of quantum cryptography Heisenberg's Uncertainty Principle guarantees that one cannot observe the polarization plain of a photon without disturbing it: The mere choice of polarizer orientations leaves the observed photon with uncertainty about the polarization plain.

[1] Since Nov. '03 the US-company MagiQ Technologies offers a quantum cryptography system called *Navajo Security Gateway*. For 50.000$ customers get two sender/receiver units and 15 km of fibre.

[2] Max Planck, German physicist, discovered the constant in the context of radiant heat in 1894. He was awarded a Nobel Prize in 1918.

2.2 Polarization of Light

Photons are transverse electromagnetic waves. This means that the electric and the magnetic fields are perpendicular to the direction in which they propagate. Moreover, the electric and magnetic fields are perpendicular to each other. Thus, in the usual three dimensional coordinate system with mutually perpendicular $x-$, $y-$ and $z-$axes, if a photon is propagating in the positive z-direction, the electric and magnetic fields will oscillate in the $x-z$ plane and the $y-z$ plane, respectively.

The photon property we are interested in is called *polarization* and refers to the bias of the electric field in the electromagnetic field of the photon. *Linear* polarization means that as the photon propagates the electric field stays in the same plane. In *circularly* polarized light the electric field rotates at a certain frequency as the photon propagates. Quantum cryptography can be implemented with linearly polarized light, circularly polarized light, or a combination of the two. However, we restrict our discussions to implementations using linearly polarized light only as this is a little simpler to explain.

In order to encode a bit in the direction of polarization of a photon, it is necessary to place a photon in a particular polarization state. This amounts to creating a photon whose electric field is oscillating in a desired plane. One way to do this is simply to pass the photn through a polarizer whose polarization axis is set at the desired angle[3].

According to quantum theory, one of two things can happen to a single photon passing through a polarizer: either it will emerge with its electric field oscillating in the desired plane or else it will not emerge at all. In the latter case, the photon is absorbed by the polarizer and its energy reemitted later in the form of heat.

If the axis of the polarizer makes an angle of θ with the plane of the electric field of the photon fed into the polarizer, there is a probability of $\cos^2\theta$ that the photon will emerge with its polarization set at the desired angle and a probability of $1-\cos^2\theta$ that it will be absorbed.

$$P(E|\theta) = \cos^2\theta \tag{1}$$

We now define two different sets of polarizer orientations. We call a polarizer ”rectilinear” if its axis makes an angle of either 0° or 90° to some reference line and ”diagonal” if its axis makes an angle of 45° or 135° respectively. We use photons polarized at angles of 0° and 45° to encode the binary value 0 and those polarized at angles of 90° and 135° to encode the binary value 1.

According to this agreement we use a sequence of bits to control the orientation of the polarizer and convert the sequence of bits into a sequence of polarized photons. These may then be fed into some communication channel, such as an optical fiber.

In order to recover the bits encoded in the polarization orientation of a stream of photons, it is necessary for the recipient to measure the polarizations. This can easily be done by a combination of a set of polarizers and a photo detector. By choosing either the rectilinear or the diagonal polarizer the photo detector behind the polarizer determines weather the photon’s electric field was in the plane of the polarizer orientation (a photon is detected) or the photon’s electric field was orthogonal to the polarizer orientation (no photon is detected). Using the output of the photo detector the sequence of polarized photons is converted back to a sequence of bits. For the rest of this introduction we assume that the conversion as well as the transmission are error free.

[3] For a relyable source of polarized photons sophisticated technology is needed. Building a quantum cryptography system the generation is in fact a major problem.

3 The Quantum Key Exchange Protocol

3.1 Quantum Cryptography in the Absence of Eavesdropping

In this chapter we want to concentrate on the mathematical properties of the quantum key exchange protocol. Thus we neglect the technical problems an assume that we are able to generate single photons with the desired polarization orientation and that the transmission and detection are error free. Our goal is to establish a secure connection between two parties named Alice and Bob which is capable of transfering an unlimited amount of information while restricting the probability of a successful attack by an eavesdropper to any given upper bound. We assume that Alice and Bob both have access to perfect local randomizers.
The quantum key exchange consists of the following five steps:

1. Generating a random Bit-Sequence and random Polarizer Orientations
2. Measuring the Photons using random Polarizer Orientations
3. Comparing the used Polarizer Orientations and a Subset of Bits
4. Retrieving the common Secret Key

Generating a random Bit-Sequence and random Polarizer Orientations

In the initial step Alice generates a random bit-sequence of length n and a random sequence of polarizer orientations (i.e. rectilinear or diagonal) with the same length n. n depends on two variables: the desired length k of the secret key Alice and Bob want to exchange and the highest tolerable probability ϵ an eavesdropper may remain undetected. The exact formula for n will be discussed in Section 3.2. Alice denotes both random sequences. She uses the polarizer orientations to encode the corresponding bits into photons and sends them to Bob.

Measuring the Photons using random Polarizer Orientations

Bob also generates a random sequence of polarizer orientations. He uses the sequence to measure the incoming photons and doing so he decodes the message into binary values. Bob denotes the polarizer orientations he used and the binary values he measured.

Comparing the used Polarizer Orientations and a Subset of Bits

In the next step Alice uses a public insecure channel to tell Bob which polarizer orientations she used for encoding. Bob compares the orientations with his own. He marks those polarizer orientations/bits Alice used the same polarizer orientations and randomly chooses l of those bits where l depends on the tolerable probability of undetected eavesdropping (→ Section 3.2). Also using the public, insecure channel he tells Alice to send him the l bits he chose. On receipt of those bits he compares the bits Alice sent with his own observation. Obviously, if the connection is secure all l bits have to match.

Retrieving the common Secret Key

Provided that the connection is secure Alice and Bob take the remaining bits they used the same polarizer orientations on as their common secret key. This key is randomly distributed and thus can be used as a one-time pad. Alice and Bob can use their common secret key to encrypt messages they exchange over a public, insecure connection.

3.2 Quantum Cryptography in the Presence of Eavesdropping

In this section we will demonstrate what effect eavesdropping has on the communication between Alice and Bob and how likely they are to detect eavesdropping. We suppose the eavesdropper (Eve) has access to the stream of polarized photons and to the public insecure channel but no information about the random sequences of polarizer orientations and bits Alice and Bob use. Thus a possible (and in fact the only possible) attack consists of the following steps:

1. Intercepting the Photons and Measuring the Photons with a (random) Sequence of Polarizer Orientations
2. Sending the intercepted Message on to Bob in an Effort to cover Eavesdropping

Intercepting the Photons and Measuring the Photons with a (random) Sequence of Polarizer Orientations

Eve has no information about the random sequence of polarizer orientations Alice used to encode her bits. Thus Eve has probability of $\frac{1}{2}$ to chose the right polarizer orientation for a single bit no matter which strategy she uses. We assume Eve uses a random sequence just like Bob would have done. She denotes the orientations and the decoded message. Note that Heisenberg's Uncertainty Principle prevents Eve from obtaining exact information about the polarization of the photons. Further note that in those cases Eve used the wrong polarizer orientation she measured a random value since the angle between her polarizer and the plane of the magnetic field of the measured photon was $\theta = 45°$ and therefore the probability for both binary values is $\frac{1}{2}$ (Equation 1).

Sending the intercepted Message on to Bob to cover Eavesdropping

In an effort to cover her tracks Eve has to pass a message on to Bob. As she has no information about the sequence of polarizer orientations Alice used her best strategy is to encode the message she intercepted using her own sequence of polarizer orientations. Doing this she will use another polarizer orientation than Alice did (e.g. rectilinear instead of diagonal) with probability of $\frac{1}{2}$ for every single bit.

Detecting Eve

Now we will focus on the detection of eavesdropping. There are three potential ways to manipulate the communication between Alice and Bob. The changes that occur by intercepting the photons, the transfer of the polarizer orientations and the transfer of the encoded bits. While Eve has control over her changing the latter two she necessarily changes the intercepted photons randomly.

We assume Alice and Bob agreed on l bits to check for possible eavesdropping. Thus in step 3 of the quantum key exchange Bob will request l binary values from Alice over the public channel. Bob supposes he and Alice used the same polarizer orientations for the corresponding l photons. If Eve (involuntarily) changed the polarizer orientation on a certain bit by measuring it or by manipulating the communication over the public channel Bob used another polarizer orientation then Alice to measure this bit. As a consequence Bob will decode the wrong value with probability of $\frac{1}{2}$ (Equation 1). If Bob does so he imideateely detects eavesdropping since the only possible reason for different values is Eve's interference. Eve uses the wrong polarizer orientation with probability of $\frac{1}{2}$ and in this case Bob detects a value different from the expected value Alice sent with probability of $\frac{1}{2}$. Thus the probability to detect a difference is $\frac{1}{4}$ for every single bit. As a difference only occure in the presence of eavesdropping Alice and

Bob have the following probability to detect Eve (D):

$$P(D) = \left(1 - \frac{1}{4}\right)^l = \left(\frac{3}{4}\right)^l \tag{2}$$

Now we can estimate the necessary number of bits n to generate a secret key with length k while limiting the probability of undetected eavesdropping to a given ϵ. Let l be the smallest integer satisfying $\left(\frac{3}{4}\right)^l \leq \epsilon \Rightarrow l = \left\lfloor \frac{\log \epsilon}{\log 3/4} \right\rfloor$. Thus we need $l + k$ bits measured with the same polarizer orientation. The overall number of bits necessary is approximately:

$$n \approx 2 \cdot (l + k) = 2 \cdot \left(\left\lfloor \frac{\log \epsilon}{\log 3/4} \right\rfloor + k \right) \tag{3}$$

By repeating steps 1-5 consecutively Alice and Bob can exchange a common secret key with any desired length n.

Note that there is no strategy for Eve to avoid perturbing the checkbits since these are selected randomly for every session. Furthermore it is use for Eve to manipulate the message containing the initial bits from Alice. Obviously the probability for detecting her remains the same if she changes the values or positions of the checkbits.

Concluding one can say that the probability of undetected eavesdropping can easily be limited to any reasonable bound with little overhead. The fraction of bits used for the private key converges to $\frac{1}{2}$ for $n \to \infty$.

3.3 Practical Relevance of Quantum Cryptography

In [PPS04] Paterson, Piper and Schack point out that quantum cryptography is strongly vulnerable to *man-in-the-middle attacks*. Without *additional authentication* an attacker who has access to the physical connection (i.e. the fiber) can easily intercept the communication without leaving any clues about his presence.

Possible authentication-methods can be divided into two groups: those which provide unconditional security and those which do not. RSA and symmetric key algorithms belong to the second group. Although a combination of QKE and an authentication using complexity cryptography does not provide unconditional security it may still offer some security advantages over traditional (i.e. non QKE-based) approaches. In any successful attack on such a system the public key authentication mechansim would have to be broken before or during the execution of the QKE protocol. This is in contrast to a system using only classical information and traditional key-establishment techniques, where the messages exchanged in order to establish a key can be stored by the adversary and analyzed at some point in the future, possibly using more advanced cryptanalytic techniques than available at the time of key establishment. The only encryption algorithm that provides unconditional security is the one-time pad. Thus a system belonging to the first group requires a pre-established common secret key. As many key bits as there are message bits must be established by the QKE protocol. This may be a problem in some practical applications, as the key bit rats of current QKE systems are relatively small. In a traditional one-time pad system (not making use of QKE), the pre-established key must be at least as long as the data to be communicated. A QKE system has an advantage here in that the pre-established key can be relatively short, as it is used only to authenticate an initial run of the QKE protocol, with part of the keying material exchanged in that run being used to authenticate subsequent runs. However, QKE loses much of its appeal in these settings, as the overall system security is no longer guaranteed by the laws of quantum physics alone. To obtain an overall communication system with unconditional security, an unconditionally secure key exchange sub-system is required. A pre-established secret key is required to obtain such a sub-system. For practical purposes the advantages of QKE over conventional encryption has to compared to the additional technical effort.

However the technical realization of QKE systems has seen rapid progress: After 15 years quantum cryptography is slowly emerging from research laboratories. In 1989 Bennett and Brassard constructed the first working prototype [BenBra89]. They started a rapid developement. While the first prototype worked over a distance of 30 centimeters and with negligigble transfer-rates todays systems can transfer data over 150 kilometers and reach transfer-rates up to 1 Mbit/s. Although there is no large-scale use of quantum cryptography at the moment a number of aspiring projects have made the technology commercially available.

Although there definitely is a vast field of possible application in the highest security sector (a few examples in the financial and military sector are already working) quantum cryptography will not replace currently wide spread encryption technology in the near future. Many technological problems remain to be solved. Especially bandwidth and range are limiting factors. Nevertheless quantum cryptography will be the solution of choice for highest security in the future. Should the quantum computer be realized someday perhaps the only choice.

4 The Bounded Storage Model

Almost all modern ciphers are based on the intractability of certain mathematical problems. Two prominent examples are the algorithm by ElGamal [ElG85] and the RSA algorithm [RSA78]. Both are considered secure since no adversary is able to break them – with recent technology that is. But will those algorithms still be secure in 40 years? What happens if computing power increases dramatically or some non-standard computation models (e.g. quantum computers) will be implemented or a computational[4] task turns out to be easier then expected. The adversary could simply store transcripts and decode them decades later[5].

In [Mau92] an encryption algorithm was proposed that is secure under the realistic assumption that an attacker's memory capacity and not necessarily his computational capacity are limited. This algorithm is a special randomized cipher using a public source of randomness to generate an amount of date which exceeds the adversary's capabilities.

4.1 Description of the Randomized Cipher

For this section random variables are denoted with capital letters, whereas the corresponding small letters denote specific values that can be taken on by theses random variables. Underlined capital letters or superscripted capital letters denote random vectors; a superscript indicates the number of components. The model of the discussed strongly-randomized cipher is as follows. The communicating parties share a short randomly-selected secret key. The randomizer $\underline{R}$ is a binary random string of length L, which is publicly accessible. The cryptogram is a deterministic function of the plaintext, the secret key and the randomizer. The goal of the design of a randomized cipher is to devise an encryption transformation such that the cryptogram depends on only a few randomizer bits whose positions in turn depend on the secret key in such a manner that without the secret key it is impossible to obtain any information about the plaintext without examining a very large number of randomizer bits.

The cipher is a binary additive stream cipher in which the plaintext $\underline{X} = [X_1, \ldots, X_N]$, the cryptogram $\underline{Y} = [Y_1, \ldots, Y_N]$ and the keystream $\underline{W} = [W_1, \ldots, W_N]$ are binary sequences of length N. The cryptogram $\underline{Y}$ is obtained by adding $\underline{X}$ and $\underline{W}$ bitwise modulo 2:

$$Y_n = X_n \oplus W_n \quad \text{for } 1 \leq n \leq N. \tag{4}$$

The publicly-accessible binary random string $\underline{R}$ consists of K blocks of length T and thus has total length $L = KT$ bits. These blocks are denoted by $R[k, 0], \ldots, R[k, T-1]$ for $1 \leq k \leq K$,

[4] Although it seems likely there is still no prove that $n = np$ does not hold.

[5] VENONA Project: From 1942 to 1946 Americans read and stored a large number of Soviet cryptograms. Some were decrypted in the late 80s

i.e., the randomizer can be viewed as a two-dimensional array of binary random variables. The secret key $\underline{Z} = [Z_1, \ldots, Z_K]$, where $Z_k \in \{0, \ldots, T-1\}$ for $1 \leq k \leq K$, specifies a position within each block of $\underline{R}$, and is chosen to be unifomly distributed over the key space $S_{\underline{Z}} = \{0, \ldots, T-1\}^K$. Thus the number of bits needed to represent the key is $K \log_2 T$.

R[1,0]	R[1,1]	...	R[1,T-1]
R[2,0]	R[2,1]	...	R[2,T-1]
⋮	⋮		⋮
R[K,0]	R[K,1]	...	R[K,T-1]

Table 1: The randomizer $\underline{R}$, viewed as a two-dimensional array.

The keystream $\underline{W}$, which is a function of the secret key $\underline{Z}$ and the randomizer $\underline{R}$, is the bitwise modulo 2 sum of the K subsequences of length N within the randomizer starting at the positions specified by the key, where each block (row) of $\underline{R}$ is considered to be extended cyclically, i.e., the second index is reduced modulo T:

$$W_n = \sum_{k=1}^{K} R[k, (n-1+Z_k) mod T] \tag{5}$$

for $1 \leq n \leq N$, where the summation is modulo 2. The sub-array of the randomizer that determines $\underline{W}$ is denoted by $R^{\underline{Z}}$ and is depicted in 4.1.

$R[1, Z_1]$	$R[1, Z_1 + 1]$	...	$R[1, Z_1 + N - 1]$
$R[2, Z_2]$	$R[2, Z_2 + 1]$	...	$R[2, Z_2 + N - 1]$
⋮	⋮		⋮
$R[K, Z_K]$	$R[K, Z_K + 1]$	...	$R[K, Z_K + N - 1]$

Table 2: The sub-array $R^{\underline{Z}}$ of the randomizer $\underline{R}$.

The sub-array $R^{\underline{Z}}$ of the randomizer $\underline{R}$ is selected by the secret key $\underline{Z}$. All second indies are to be reduced modulo T. The keystream $\underline{W} = [W_1, \ldots, W_N]$ is formed by adding the K rows of $R^{\underline{Z}}$ bitwise modulo 2.

4.2 Resistence against possible Attacks

The model of the eavesdropper's attack is described in the sequel. We suppose the eavesdropper has access to the cryptogram $\underline{Y}$, the randomizer $\underline{R}$ and some other *a priori* information about the plaintext. We allow the eavesdropper to use an arbitrary, possibly probabilistic, sequential strategy for selecting the positions of the randomizer bits that he examines. At each step of the attack, the eavesdropper can make use of the entire available information, i.e., the cryptogram $\underline{Y}$, the side-information V, and the positions and values of the bits observed so far. Let $E_i = [A_i, B_i]$ denote the address of the i-th randomizer bit examined by the eavesdropper, where A_i and B_i satisfy $1 \leq A_i \leq K$ and $0 \leq B_i \leq T-1$ for $i = 1, 2, \ldots$. Let further $O_i = R(E_i) = R[A_i, B_i]$ denote the observed value of the randomizer bit at position E_i that is axamined by the eavesdropper at the i-th step of his attack. We use the notation $E^m = [E_1, \ldots, E_m]$ and $O^m = [O_1, \ldots, O_m]$ for all $m \geq 1$. For a particular sequence $e^m = [e_1, \ldots, e_m]$ of m bit positions, where $e_i = [a_i, b_i]$ with $1 \leq a_i \leq K$ and $0 \leq b_i \leq T-1$ for $1 \leq i \leq m4$, $R(e^m) = [R(e_1), \ldots, R(e_m)]$ denotes the corresponding sequence of randomizer bits. Correspondingly, we have $O^m = R(E^m)$ for $m \geq 1$.

Theorem: *There exists an event ϵ such that, for all joint probability distributions $P_{\underline{X}V}$ and for all (possibly probabilistic) strategies for examining bits $O_1, \ldots, O_M$ of $\underline{R}$ at adresses $E_1, \ldots, E_M$,*

$$I\left(\underline{X}; \underline{Y}E^M O^M | V, \epsilon\right) = 0 \text{ and } P(\epsilon) \geq 1 - N\delta^K,$$

where $\delta = M/KT$ is the fraction of randomizer bits examined by the eavesdropper.

Here $I(\underline{X}; \underline{Y}E^M O^M | V, \epsilon)$ denotes the (mutual) information that $\underline{Y}$, E^M and O^M together give about $\underline{X}$, given that V is known and given that the event ϵ occurs. The theorem states that if the event ϵ occurs, then the eavesdropper's total observation $[\underline{Y}, E^M, O^M]$ gives no information about the plaintext $\underline{X}$ beyond the information already provided by V.

Maurer proofs this theorem specifying a certain event ϵ. The proof is in fact stronger than the theorem since it shows that if ϵ occurs, then the eavesdropper would have no information about the plaintext even if he were given the secret key. For details on the proof and the event ϵ regard [Mau92]. We omitte the prove since it is technical and rather lengthy.

The theorem states that it is impossible for an eavesdropper to obtain any additional knowledge about the plaintext unless he stores a substantial fraction (e.g. 2/3) of the entire randomizer. Unfortunately the prove is valid only under the unrealistic assumption that the adversary stores the randomizer and not a cleverly chosen boolean function of it. In [DziMau02] the stronger result was proven that the Bounded Storage Model is secure against any memory-bounded attacker. Since the adversary has to store large parts of the randomizer to break the cipher it is provable secure under the assumption that the communicating parties use a randomizer which exceeds the memory capacities of every possible adversary.

Example

Assume that $K = 50, T = 10^{20}$ and let the plaintext be one gigabit, i.e., $N = 2^{30} \approx 10^9$. The keysize of this cipher is $50 \cdot \log_2 10^{20} \approx 3320$ bits. The legitimate users need to examine only 50 randomizer bits per plaintext bit. An eavesdropper, however, even if he used an optimal strategy for examining a fraction $\delta = 1/4$ of all bits, i.e., $M = KT/4 = 1.25 \cdot 10^{21}$ bits in total, would have a chance of obtaining any new information about the plaintext not greater than $2^{30} \cdot (1/4)^{50} < 10^{-21}$.

4.3 Practical Relevance of the Bounded Storage Model

The last technological hurdle is the generation and distribution of large amounts of random data. At the current state of technology the effort to generate a random bit is of the same order as that required to examine one. Maurer points out that this task could be done by a satelite broadcasting random sequences generated by an astronomical phenomenon[6]. The Bounded Storage Model is of high theoretical interest and a number of publications conerning it are published every year but there are no recent plans to install the hardware necessary for the protocol.

References

[Ver26] Vernam, G. S. *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, J. American Inst. Elec. Eng., vol. 55, pp. 109-115, (1926)

[Hei27] Heisenberg, Werner. *The Actual Content of Quantum Theoretical Kinematics and Mechanics*, Zeitschrift fur Physik, vol. 43, pp. 172-198, (1927)

[RSA78] Rivest, Shamir, Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Communications of the ACM, (1978)

[6] e.g. the surface of the moon or a deep-space radio source

[ElG85] ElGamal, T. *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, (1985)

[BenBra89] Bennett, Brassard. *The dawn of a new era for quantum cryptography: The experimental prototype is working!*. Sigact News, vol. 20, no. 4, pp. 78 - 82, (1989)

[Mau92] Maurer, Ueli. *Conditionally Perfect Secrecy and a Provably-Secure Randomized Cipher*. Journal of Crypotlogy, vol. 5, no. 1, pp. 53-66, (1992)

[Bra94] Brassard, Gilles. *A Bibliography of Quantum Cryptography*, provided by Edith Stoeveken, (1994)

[WilCle98] Williams, Clearwater. *Exploratrions in Quantum Computing*. Springer Verlag, pp. 163-181, (1998)

[DziMau02] Dziembowski, Maurer *Tight security proofs for the bounded-storage model*, STOC, (2002)

[Dzi04] Dziembowski, Stefan. *Bounded Storage Model*, Institute of Informatics, (2004)

[PPS04] Paterson, Piper, Schack *Why Quantum Cryptography?*, (2004)

[Sti05] Stix, Gary. *Best-Kept Secrets*, Scientific American, vol. 292, no. 1, pp. 78-83, (2005)