Topic 19
Quantum Cryptography

Dipan Kumar Ghosh
Indian Institute of Technology Bombay
Powai, Mumbai 400076

April 15, 2017

1 Introduction

We have seen that classical cryptography based on RSA algorithm is reasonably robust because of difficulty in factoring large composite numbers in polynomial time. There is, however, reason to believe that attempts in this direction may become successful and there will be a need to define alternative encryption mechanism. In recent years a group of undergraduate students at the IIT, Kanpur, led by their mentor Professor Manindra Agrawal, showed how to predict, in polynomial time, whether a given number is a prime or not, without factoring the number. This, of course, does not imply that factorization can now be done. However, this certainly indicates that efforts in factoring large composite number will now receive a major impetus. Peter Shor's algorithm for factoring a composite number using a quantum computer has added a new challenge that classical encryption will face once quantum computers become a reality.

Historically, the possibility of using quantum mechanical ideas for coding goes back to Stephen Wiesner, who in his graduate thesis suggested an interesting idea, which came to be known as "quantum money". The idea behind this is the following. In each currency note a sequence of light traps are stored each trap having one of the four polarizations, viz., horizontal (↕), vertical (↔), polarizations state making 45° with the horizontal and a polarization state making 135° with the horizontal. It may be noted that the sequence of polarization being random, if one uses even 20 such light traps, it would result in 4^{20} different configuration, which is a trillion possibilities. A database of currency notes would contain a usual identification number and an enumeration of the state of polarization stored in each bill. In case of a fraud, the identity of the bill can be verified without ambiguity. Duplicating such a bill would be a near impossible task and would cost lot more than what the currency bill is worth.

Cryptography using quantum states is secure because the message that is being sent being an unknown state, it cannot be copied in view of quantum no cloning theorem. In

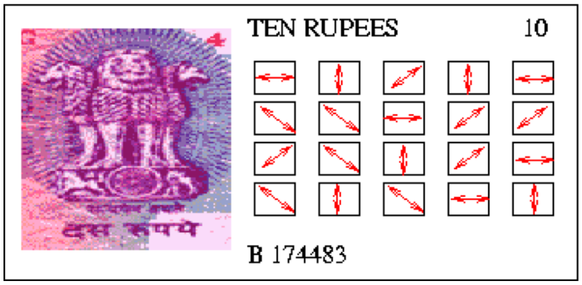

Figure 1: Wiesner Money with light traps of random polarization

addition, since each single qubit is in a linear combination of two states, any attempt to measure the message would disturb the system and what the interceptor would get will make no sense to him . Further, if the interceptor, having measured the message, cannot reconstruct the original message because of irreversible nature of quantum measurement. What we will discuss in this and the next lecture, we will discuss some protocols for sending secure communication.

Recall that Vernam cipher or the one time pad is the only really secure communication. The aim of the protocols that we will discuss to establish a one time pad between a sender and the receiver, in a public but in a way which would ensure the various characteristics of a secured communication.

2 BB-84 Protocol

The purpose of BB-84 and B-92 protocols is to generate a secret key to be shared between a sender (Alice) and receiver (Bob), with a possible eavesdropper (Eve) who attempts to intercept and get at least some of the information in the message. It may be mentioned that the key itself does not contain a message but will be used to encrypt a message and hence the secrecy of the key is as important as the secrecy of the message itself. Experimentally, the quantum key distribution can be performed by using the polarisation states of photons and sent over a channel such an an optical finer. The security of the key sharing over a quantum channel is based on the fact that when Eve intercepts and measures the quantum state sent by Alice, she will make the state collapse into a state determined by her measuring device. She cannot measure and copy the state because of the impossibility of cloning non-orthogonal states. Thus, the presence of Eve can always be detected and the protocol will be aborted if it is believed that an interceptor is gaining substantial information from such interception. Polarizers, such as calcite crystals, can be used to generate photons whose polarisation directions are along specified directions in space. If a single photon polarised along a direction making an angle θ to the horizontal is made to be incident on a second polariser (called an analyser), with its axis parallel to the direction of polarisation, the photon will pass through the analyser. On the other

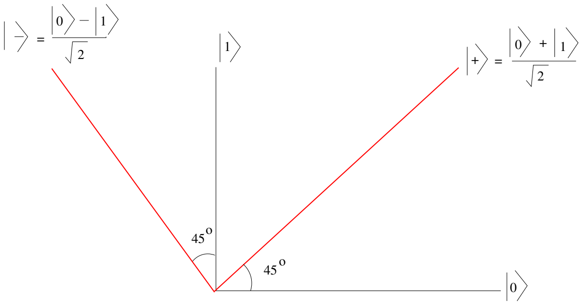
$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$|1\rangle$
$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
45°
45°
$|0\rangle$

Figure 2: Alice and Bob's bases in BB-84 protocol : H/V bases are along the axes, the diagonal bases are shown in red

hand, if it is incident on an analyser whose axis is perpendicular to the direction of polarisation, the photon does not get transmitted. If, however, the axis makes an angle φ with the direction of polarisation, the probability of the photon passing through is $\cos^2\varphi$. An important difference between the classical and the quantum picture may be kept in mind. When a beam of photons polarised along a particular direction is incident on a polariser with an axis making an angle φ with the direction of polarisation, the intensity of transmitted photons is $\cos^2\varphi$ (the law of Malus). This means that a fraction $\cos^2\varphi$ of photons pass through. However, for a single photon, this implies that the probability of passing through is $\cos^2\varphi$, as a single photon cannot be split. In this discussion we assume that Eve has complete knowledge of the protocols used. This is the situation that is most favourable for Eve as it can only become worse for her if she either has no information or a partial knowledge of the protocol. In BB-84 protocol, Alice uses one of the two bases available with her in a random fashion. She could, for instance, toss a coin and if she gets a "head", she will use a horizontal/vertical (H/V) basis, encoding the classical bit 0 as $|\,0\rangle$ and the bit 1 as $|\,1\rangle$, i.e. she uses the computational basis to encode 0 and 1. In practice she would use a single photon polarised along the horizontal direction to code 0 and that polarised along the vertical direction to code the bit 1. If, however, her coin toss results in a 'tail', she will encode the bit 0 by a photon whose direction of polarisation makes an angle of 45° to horizontal, and code the bit 1 by a photon whose polarisation direction makes an angle of 135° to the horizontal. In the later case, we will call the basis as the "Diagonal basis".

(D) and denote the basis vectors as $|\,0'\rangle$ and $|\,1'\rangle$, where, in terms of the computational basis, the corresponding quantum states are given by

$$|\,0'\rangle = \frac{|\,0\rangle + |\,1\rangle}{\sqrt{2}} = |\,+\rangle$$
$$|\,1'\rangle = \frac{|\,0\rangle - |\,1\rangle}{\sqrt{2}} = |\,-\rangle$$

Thus the bit is 0 is encoded as $|\,0\rangle$ with a probability 1/2 and as $|\,+\rangle$ with an equal probability. Likewise, he bit is 1 is encoded as $|\,1\rangle$ with a probability 1/2 and as $|\,-\rangle$

with an equal probability. The density matrix that Alice sends to Bob corresponding to the bit 0 is

$$\rho_0 = \frac{1}{2}(|\, 0\rangle\langle 0 \,| + |\, +\rangle\langle + \,|)$$

and that corresponding to the bit 1 is

$$\rho_1 = \frac{1}{2}(|\, 1\rangle\langle 1 \,| + |\, -\rangle\langle - \,|)$$

has no knowledge of the basis Alice uses to code a particular bit in the sequence of bits that she sends to him. However, he is aware that she uses either the H/V basis or the D basis to code the photons. accordingly, he also uses the same pair of bases to decode the state of polarisation of arriving photons, in a random selection. He could also use the same strategy for selecting a measuring basis as Alice did in selecting the sending basis. Bob could toss a coin and if he gets a 'head', he will use H/V basis to decode the bit and if he gets a tail, he will use D basis to decode. If both Alice and Bob happen to use the same basis for a particular bit, Bob will measure the polarisation state of the photon correctly and his interpretation of the bit received will be identical to what Alice sent, assuming of course, that there is no Eve intercepting the transmission. If, however, Alice and Bob use dissimilar bases, Bob's measurement will still lead to a correct interpretation of the bit half the time, probabilistically, because the two bases are inclined at 45° with each other. Thus Bob's interpretation of Alice's bits will be the same as that sent by Alice, 75% of time, half of them because they used the same bases and a quarter because of probabilistic reasons.

The following table shows sample transmission of 16 bits of data sent by Alice to Bob in the absence of an interceptor. In the following table the basis H/V is abbreviated as H)

Bit	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1	1
Alice's Basis	H	D	H	D	D	D	H	D	H	H	D	D	D	H	D	H
Bob's Basis	H	D	D	D	H	D	H	H	H	D	H	D	D	D	H	H
Bob's Result	0	1	0	0	0	1	0	1	1	1	1	0	0	0	1	1
status	✓	✓	R	✓	×	✓	✓	×	✓	R	×	✓	✓	×	R	✓

Here, × is the case where the two bases and the interpretations do not agree whereas R indicates the case where even though the bases are different, the result is the same because of random nature of the result.

In the next lecture, we will see how the protocol is affected due to presence of an eavesdropper (Eve) in the channel.

3 Eve's Interception

Brief summary of BB-84 protocol above is as follows. Both Alice and Bob randomly select a base (H/V or D) and communicate to each other. Assuming that they used the same basis, the bit received by Bob will be the same as that sent by Alice half the time. For the remaining half, on an average another 50% will agree randomly. Thus Bob will receive the same bits as Alice sent 75% of the time. However, other than the case where their bases agree, the remaining agreement is accidental and will be later discarded. Let us now suppose there is an interceptor Eve in the channel, who will intercept every bit sent by Alice and like Bob, not being aware of the base Alice had used (but having known that Alice used one of the two alternatives), Eve will randomly select a basis and measure the bit and resend it to Bob. If Eve intercepts every bit and resends to Bob, she will use bases as random selection. In such a case, the results would be correct when Alice, Eve and Bob used the same bases and would be correct half the time when either Eve or Bob used the wrong basis. Thus out of 8 transmissions, only in two cases (when each one of them choose with H/V or D bases), their results would agree and of the remaining six cases Bob's result would agree with Alice's on three occasions. Thus Alice's and Bob's interpretation would be the same for 2+3=5 bits out of 8, i.e a probability of 5/8.

The way the protocol is implemented is as follows:

1. Alice chooses $4n + \delta$ number of random bits and generates a string of these bits, encoding the individual bits either in H/V basis or in D basis and sends them to Bob.

2. Bob receives these $4n + \delta$ bits and measures each of them in a random basis, either H/V or D.

3. Alice would then, over a public channel, announce the sequence of bases that she used to encode the bits. She, however, does not announce the actual bits.

4. As Bob's selection of the measuring bases is also random, their bases would agree about half of the time, so that it is conceivable that for at least $2n$ bits out of the original $4n+\delta$, Bob would have used the same bases as Alice had used for encoding them. (The additional δ number of bits is to take care of the fact that in practice, the actual number of cases where their bases agree could be somewhat less than 50%.)

5. Bob discards those bits for which their bases were not identical, irrespective of the fact that in the discarded lot, on an average about 50% of the bits would still have been the same as what Alice sent (those cases marked with R in the table above).

6. Bob now announces, once again over a public channel, the locations (not the content - i.e. the bits) of the bits for which their bases agree and Alice and Bob will now keep 2n bits of such data and renumber the string.

7. With the remaining 2n bits, they would perform some checks to determine if there is an eavesdropper in the channel.

8. Alice picks up n random bits (the check bits) out of the above 2n and, once again over a public channel, announces both the location and the content (i.e. the bit) she had sent.

9. Ideally, in such cases, since they had used the same bases, the string should agree, except for an acceptable error due to a lossy channel. If the error is found to be high, the protocol is aborted and they would try it at a later time. In case the error is small, they would do a privacy amplification and keep the n bit string as the shared key which becomes a one time pad.

10. In the above it is assumed that Eve cannot corrupt a public channel and intercept public announcement, change them and resend whatever she wishes to.

The idea behind privacy amplification is the following. It is presumed that Eve has some information about the secret string of n bits talked about in the above, but not excessively large amount of information. Let us call this string S. Alice picks up m random subsets of these strings (some of the subsets may be partially overlapping). Let us indicate them by S1, S2, ... They compute the parity of each of the subsets (i.e. the number of 1s in the subset) and it is the parity (0 for even number and 1 for odd number of 1s in the subsets) which becomes the new secret string. The new string so generated is much less in size but is completely confidential. This is because even though Eve may know some of the bits of S, she cannot calculate the parity of each subset unless she knows each one of the bits. One of the ways of achieving the privacy amplification could be to use a random binary matrix (with elements 0 and 1) M of dimension m n and obtain the string of size m from the matrix multiplication MV where V is a column vector containing the n bits of S.

4 B-92 Protocol

B-92 protocol, due to Charles Bennet, is a simpler version of BB-84 protocol. In this case, Alice uses two nonorthogonal bases for encoding her bits in a predetermined way, i.e., unlike in BB-84 protocol, she does not use a coin toss. She would encode the bit 0 using a computational basis as a state $| 0\rangle$ (i.e. she represents the bit 0 by a horizontally polarized photon) and encode the bit 1 as $| 1'\rangle$ (i.e. a photon with polarization along any arbitrary angle θ , not orthogonal to the horizontal direction). Taking the special case of $\theta = 45°$, Alice's encoding gives rise to a state $| \psi\rangle$, given by

$$| \psi\rangle = \begin{cases} | 0\rangle & \text{if bit } \ a = 0 \\ \dfrac{| 0\rangle + | 1\rangle}{\sqrt{2}} & \text{if bit } \ a = 1 \end{cases}$$

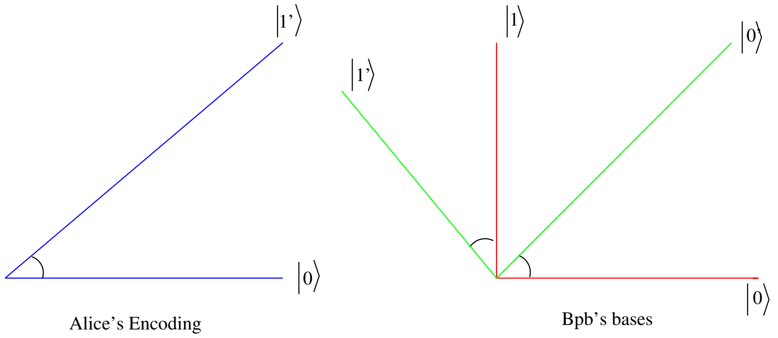

Figure 3: The bases used by Alice and Bob in B-92 Protocol

Bob's decoding measurement will use a coin toss and if the result of such a toss is 'head' (i.e. if $a' = 0$), he will use a computational basis $(|\ 0\rangle, |\ 1\rangle)$ to measure the incoming photon. If the result of the coin toss is a 'tail', Bob will use the diagonal basis $(|\ \pm\rangle)$. Note that a' is a random bit generated from a coin toss which has a value 0 if he gets a head and 1 if he gets a tail. Unlike a, the result of the toss a' is not a bit but may be assigned the value 0 if the coin toss gives a 'head' and 1 if coin toss results in a tail. Consider now the following possible results.

1. $a' = 0$: In this case Bob uses H/V basis. In this basis, it if Bob measures 1, Alice could not have sent 0 because their basis are the same, and Alice's $|\ 0\rangle$ is orthogonal to Bob's $|\ 1\rangle$. Thus Alice must have sent $|\ 1'\rangle$ using the 45° polarized photon $(a = 1)$, which has a probability of being measured along the $|\ 1\rangle$ of the H/V basis. If, on the other hand, Bob meares 0 in H/V basis, no conclusion can be made as to what Alice sent because both $|\ 0\rangle$ and $|\ 1'\rangle$ of Alice have components along Bob's $|\ 0\rangle$.

2. $(a' = 1)$: In this case Bob uses the D-basis for measurement. In this basis if Bob measures 1 (i.e. his state $|\ 1'\rangle$, Alice could not have sent $|\ 1'\rangle$ because Alice's $|\ 1'\rangle$ is orthogonal to Bob's $|\ 1'\rangle$. Hence Alice must have sent $|\ 0\rangle$ in the computational basis, i.e. $a = 0$. If Bob measures 0 in this basis, no conclusion can be drawn.

Thus, a definite conclusion can be reached whenever Bob measures 1. In such a case if Bob used $a' = 0$,Alice must have used $a = 1$ and if Bob used $a' = 1$, Alice had used $a = 0$. Both these cases correspond to Bob measuring bit 1. Thus the final key is the bases Alice and Bob used (and not the bits which alice generated or Bob measured). Alice's a corresponds to Bob's $a' - 1$.

5 Ekert Protocol using EPR pairs (E-91)

In this protocol, instead of Alice preparing the particles and sending them to Bob, a third person, say Charlie, prepares EPR pairs and sends one particle of the pair to alice and

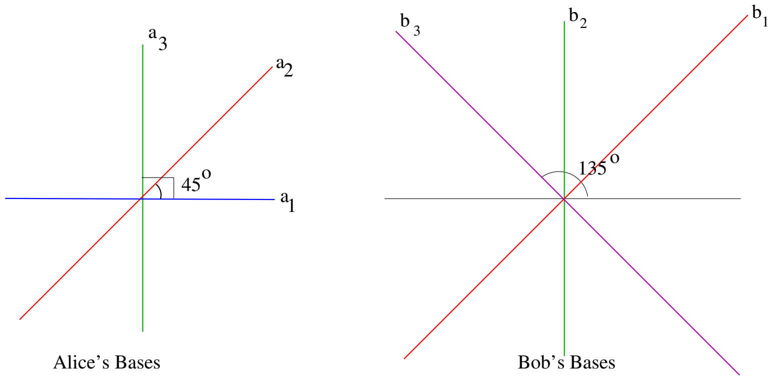

Figure 4: Bases used in Eckert- 91 protocol

sends its correlated entangled partner to Bob. He chooses an EPR singlet of spins

$$\mid \psi\rangle = \frac{1}{\sqrt{2}}\left(\alpha(1)\beta(2) - \alpha(2)\beta(1)\right)$$

where $\alpha(i)$ and $\beta(i)$ stand respectively for the spin up and the spin down states of particle numbered i. The analyzer in this case would be a Stern-Gerlach measuring apparatus with a specified direction of the magnetic field to measure the spin states of the particle. Alice and Bob define three coplanar axes to measure the spin of the particle that is coming towards them. Assuming the particles to travel along the z-direction, the plane of the axes will be the x-y plane. We take the axes for Alice to be a_1, a_2 and a_3 and those for Bob to be b_1, b_2 and b_3. In the figure, the axes a_1, a_2, a_3 have been taken, respectively, to make $0°, 45°$ and $90°$ with respect to the x-axis while b_1, b_2, b_3 have been taken to make $45°, 90°$ and $135°$ respectively.

Clearly, the probability that Alice and Bob choose compatible bases (shown with the same colour in the figure) to measure the spin of their particles is 1/3. When such is the case, if Alice finds her particle to be in spin up state, Bob will find his particle to be in spin down state and vice versa. Thus after the measurements have been made, Alice and Bob announce the axes they used for measurement and keep the corresponding bits as forming their shared key. For instance if Alice used a_2 while Bob used b_1 or when Alice used a_3 and Bob used b_2, Alice could generate a string 0011010111 while Bob would find his string to be 1100101000, where we have used bit 0 to represent a spin up and bit 1 to represent spin down. The measurements which were not used in the key generation are those for which the axes were incompatible. These consisted of base pairs $(a_1, b_1), (a_1, b_3), (a_3, b_1)$ and (a_3, b_3). These can be used to detect the presence of Eve. It may be observed that if Eve intercepts the particles and makes measurements, she would provide local realism to the measurement process and Bell's inequality would be satisfied. Denoting the measured spin up as $+1$ and spin down as -1, we define,

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$$

where $E(a_i, b_j)$ is the expectation value of the measured values of spin when Alice uses a_i and Bob uses b_j axes. With local realism, S would satisfy Bell's inequality $\mid S \mid \leq 2$ whereas for quantum mechanics to be valid $\mid S \mid > 2$.