

A Probabilistic Quantum Key Transfer Protocol

Abhishek Parakh

Nebraska University Center for Information Assurance

University of Nebraska at Omaha

Omaha, NE 68182

Email: aparakh@unomaha.edu

August 9, 2012

Abstract

We propose a protocol to transfer a one-time-pad (in a probabilistic manner) from Alice to Bob, over a public channel. The proposed protocol is unique because Bob merely acts as the receiver of the pad (secret key), i.e. Bob does not need to send any message back to Alice unless he detects eavesdropping. Such a secure transfer of one-time-pad, over public channel, is not possible in classical cryptography and in quantum cryptography all previous protocols require Bob to send almost as many messages back to Alice as she does to Bob, to establish a key.

1 Introduction

Quantum key agreement protocols provide perfect security using laws of quantum physics [10]. This is of great advantage when all the classical key agreement techniques over public channels have been based on unproven mathematical assumptions [7]. A quantum key agreement protocol was first proposed by Bennett and Brassard [2] (BB84). In BB84, Alice generates a random string of bits and sends each bit to Bob as a photon in a randomly chosen basis (rectilinear or diagonal). Bob, not knowing which of the two

bases each photon is in, measures them randomly in rectilinear or diagonal basis. After measuring all the photons, Bob discloses his choice of bases of measurement to Alice and she tells Bob which of their bases agree. The final key is made up of bits that were received by Bob in the matching bases. A subset of these bits are used to check if there was any eavesdropping. Here disclosure of bases is done over a classical communication channel.

Eavesdropping is detected in BB84 because Eve not knowing the original bases of the photons, like Bob, measures them in random bases. This will make 75% of the photons collapse randomly at Bob's end. However, Bob expects 50% of this random bases to agree with Alice's and hence see only 50% of the photons collapse randomly. After all the measurements are done, Alice and Bob randomly select a subset of the bits received by Bob in the correctly aligned bases and check for errors. If Eve has made measurements, they would expect to see disagreements in some of the bit values.

Ekert [4] proposed the use of entangled photons measured randomly in three coplanar axes. While Ekert's protocol used Bell's inequality to demonstrate its security against eavesdropping, Bennett, Brassard and Mermin [3] proposed a protocol that used entangled pairs and did not depend on Bell's inequality for detection of eavesdropping. Bennett [1] in another scheme showed that any two non-orthogonal states suffice for key agreement. A protocol by Katalopoulus [6] used two quantum channels for key agreement in conjunction with a classical channel. In his protocol, Alice sends same information on both the quantum channels and Bob measures the photons on these channels, randomly, in complementary bases (rectilinear on one and diagonal on other). They compare their chosen bases publicly and Bob retrieves the key.

Almost all quantum key distribution protocols have a similar concept behind them in which photons are first measured in random bases and then the chosen bases are compared publicly. Consequently, the final key to be used cannot be decided in advance and depends on Bob's measurements as well. Further, all the protocols require Bob to actively send messages back to Alice in a back and forth communication.

A somewhat different three-stage quantum key agreement protocol based on the idea of commuting transformations was proposed in [5], similar to classical commutative cryptography [9]. However, it requires Bob to choose rotation basis of his own and thus a two-way exchange of messages for the key agreement process. A protocol that uses repeated transmission and measurement of photons in both directions is proposed in [11]. In contrast, although

the protocol proposed here uses repeated transmission of photons, we only send messages in one direction, making it at least twice as efficient as that proposed in [11].

Therefore, the contributions of the proposed protocol is as follows:

1. It enables Alice to transfer a secretly chosen one-time-pad to Bob over a public channel. The key is entirely chosen by Alice.
2. Probabilistic nature of transfer: the one-time-pad is transferred to Bob correctly with a very high probability (a parameter chosen by the participants).
3. Bob sends a message back to Alice only if he detects eavesdropping and does not need to disclose his bases of measurement. Consequently, unlike previous protocols, there is no two-way exchange of messages to establish a key.
4. Unlike other protocols, where only Alice can detect eavesdropping because only she knows the original values of the bits she sent, in the proposed protocol Bob is able to detect eavesdropping.
5. The probability of detection of eavesdropper is higher than that in BB84.

Further, we assume that Alice and Bob have agreed on bases of measurements and encoding of photons long before Alice decides to transmit a one-time-pad to Bob. Such arrangements can be a part of global standards that communicating parties follow. Also, assume that Alice has quantum systems capable of producing single photons in desired polarization and there is no loss of photons during transmission or elsewhere.

2 The Proposed Protocol

Assume that Alice wishes to send Bob, over a public channel, a random bit string of length n to be used as a one-time-pad. We assume that Alice and Bob have, long before the start of the protocol agreed to use polarized photons for communication and two bases for measurements. For example, photons in states $|0\rangle$ and $|1\rangle$ are implemented using photons polarized at 0 degrees (\rightarrow) and 90 degrees (\uparrow), respectively, and are said to represent 0

and 1 in rectilinear basis (+). Similarly, photons in states $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ are implemented using photons polarized at 45 degrees (\nearrow) and 135 degrees (\nwarrow), respectively, and are said to represent 0 and 1 in diagonal basis (\times). Further, a photon that is in diagonal basis, when measured by a detector aligned in rectilinear basis randomly collapses to 0 or 1 with a probability of one-half, and vice versa [8].

The protocol proceeds as follows:

1. Alice chooses a random sequence of polarization basis (rectilinear or diagonal) and sends Bob a stream of photons representing one bit of the key in the basis chosen for that bit position.
2. Bob upon receiving the stream of photons, randomly and independently measures each photon in rectilinear or diagonal basis.
3. Alice re-encodes her key as a stream of photons in the same sequence of bases as before and sends it to Bob again.
4. Bob measures the stream of photons in the same sequence of bases that he chose in the previous iteration.
5. Alice and Bob repeat steps 3 and 4, $k - 1$ number of times.
6. Alice sends one final copy of the key as a stream of photons to Bob.

At this point Alice has sent $k + 1$ copies of the key as polarized photons to Bob.

- For the first k iterations, Bob keeps his sequence of bases constant and notes all the measurements for all the iterations in a table.
- If for photon i the measured value changes at least once over k iterations, then Bob concludes that his measurement basis for that photon is not the same as that of Alice's and changes his basis of measurement for that photon to the complementary basis.
- Bob receives the $(k + 1)^{th}$ transmission in the realigned bases.
- Alice then sends to Bob all the original sequence of bases for her photons.
- Bob checks for eavesdropping:

- If eavesdropping is detected - Bob sends an abort signal to Alice.
- Else Alice sends the encrypted message to Bob.

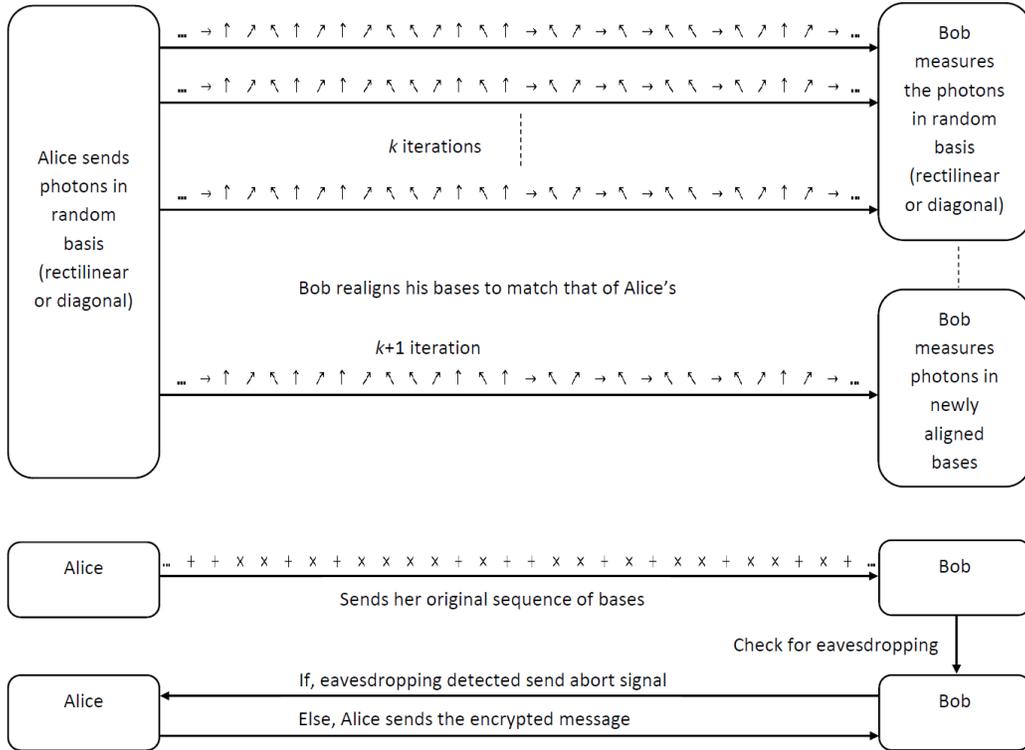


Figure 1. Illustration of the flow of the proposed protocol.

Bob keeps track of all measurements he makes and notes them as shown in the tables. When Bob's basis of measurement matches with Alice's chosen basis for a photon, Bob retrieves the same exact result for that bit in all the k iterations. However, if Bob's basis differs from that of Alice's, Bob will lose all information about that bit (photon will randomly collapse to 0 or 1 with probability one-half).

Since both Alice and Bob are choosing their measurement bases randomly and independently, Bob expects to see 50% of his bases agree with Alice's. Consequently, Bob will see the other 50% of the photons collapse to a random value. This is shown in table 2.

After k iterations Bob will have determined with a very high probability which of his bases align with Alice's and which don't align. For the bases

that don't align with Alice's he changes them to the complementary bases. When Alice sends the $(k + 1)^{th}$ transmission of photons, Bob measures it in his newly aligned basis to determine the secret key.

3 The Value of k

Bob's aim is to determine which of his basis align with Alice's. If, for a given photon, Bob's basis is not aligned with Alice's basis then Bob will see a random collapse of the photon. The probability that Bob's basis is wrongly aligned and yet he sees that photon collapse to the exact same value over k iterations is $\frac{1}{2^{k-1}}$. If $k = 12$, Bob is more than 99.9% confident of his basis for a photon for which his measured value remained constant over k iterations.

Raw key bit stream generated by Alice	0	1	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0	1	0	1	1	0	1	0	1	0	0	
Step 1: Alice randomly chooses bases and encodes key as stream of photons	+	+	x	x	+	x	+	x	x	x	+	x	+	+	x	x	+	x	+	x	x	+	x	x	+	x	+	+	
	→	↑	↗	↖	↑	↗	↑	↗	↖	↖	↗	↑	↖	↑	→	↖	↗	→	↖	→	↖	↖	→	↖	↗	↑	↗	→	
Alice sends the stream of photons to Bob																													
Step 2: Bob's randomly chooses bases for measurement	+	x	+	x	+	x	x	+	x	+	x	+	x	x	+	+	x	x	+	x	x	x	x	x	+	x	+	+	
Bob measures the received photon in the basis chosen for that bit position																													
Bob receives	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	1	/	/	1	1	0	/	/	1	/	0	1	1	/	0	/	0	/	/	/	/	1	1	/	1	/	/	/	0
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Step 3: Alice resends another copy of the key as a stream of photons in the exactly same bases as before																													
Step 4: Bob measures the new stream of photons received in exactly the same bases as before																													
Step 5: Repeat $k-1$ times: Steps 3 and 4																													
Step 6: Alice sends one final copy of the key as stream of photons to Bob																													
At this point Alice has sent $k+1$ copies of the key encoded as stream of photons to Bob																													

Table 1. Sample execution of the proposed protocol.

4 Probabilistic Nature of Key Transfer

It is clear from the above description that the key transfer is probabilistic in the sense that Bob has a residual probability of error for the final key. This is because Alice discloses her bases only after Bob has made all the measurements. Therefore, bits that did not change their value in k iterations

	Bob's observations over 13 iterations for example shown in table 1																														
Iteration 1	0	1	1	1	1	0	0	1	1	0	0	1	1	1	0	1	0	1	0	0	1	1	0	1	0	1	0	0			
Iteration 2	0	1	0	1	1	0	0	1	1	1	0	1	1	0	0	1	0	1	1	0	1	1	0	1	1	1	0	0			
Iteration 3	0	0	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0	0	1	1	1	1	1	1	1	0	1	1	0		
Iteration 4	0	1	1	1	1	0	0	1	1	1	0	1	1	1	0	0	0	0	0	1	1	1	0	1	0	0	0	1	0		
Iteration 5	0	0	0	1	1	0	1	0	1	0	0	1	1	1	0	0	0	1	0	0	1	1	0	1	0	0	0	0	0		
Iteration 6	0	0	1	1	1	0	1	1	1	1	0	1	1	1	0	1	0	0	0	0	1	1	1	1	0	0	0	0	0		
Iteration 7	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	1	0	1	0	1	0	1	1	1	1	1	0	0	1	0	
Iteration 8	0	1	0	1	1	0	1	0	1	0	0	1	1	1	0	1	0	1	0	0	1	1	1	1	1	1	1	1	1	0	
Iteration 9	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	
Iteration 10	0	1	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	0
Iteration 11	0	1	0	1	1	0	1	1	1	1	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	
Iteration 12	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	1	0	
	Bob realigns the bases to match those of Alice's																														
Iteration 13	0	1	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0	1	0	1	1	0	1	0	1	0	0	0		

Table 2. Bob's observations over 13 iterations for the example shown in table 1.

have a probability of $\frac{1}{2^{k-1}}$ of being measured in the wrong basis and hence Bob does not gain any information about them.

When Alice sends Bob her original bases of encoding, Bob can check if any of his basis were wrongly aligned. For a large k , the addition of a one bit error correcting checksum to the end of the transmitted key would suffice.

5 Eavesdropping

We assume that an eavesdropper has same capabilities as that in BB84 [2], in which case the probability of detection of eavesdropper is greater than that in BB84. Here the eavesdropper, Eve, can only make measurements on the photons that are being sent to Bob. Consequently, not knowing the bases of the photons, Eve will make measurements in random bases before sending the photons to Bob and hence introduce errors in Bob's measurements. The difference from previous protocols is that Bob himself will be able to detect these errors as compared to sending a subset (or a function of the subset) of the bits to Alice for verification.

Irrespective of whether Eve eavesdrops on all the k iterations or just one iteration (or any number in between), Eve measurements will force 75% of the photons to collapse randomly (at Bob's end), whereas Bob is expecting to see only 50% of the photons to collapse randomly. In other words, since Alice later sends Bob the correct bases of the photons, he can go back and check

his table for the bits whose values were supposed to stay constant through all the k iterations. Eve's interference will make half of the photons that were supposed to remain constant (through k iterations) collapse randomly, i.e. 12.5% of all photons.

We say that probability of detection of eavesdropper is higher than BB84 because instead of just using a subset of bits received in the correct bases, Bob is able to check all the bits (expected $\frac{n}{2}$) that he received in correct bases. Consequently, the probability that an Eavesdropper escapes detection is much lower $(\frac{1}{2})^{\frac{n}{8}}$, where a typical $n = 1024$.

6 Conclusions

In this article we have presented a protocol, based on quantum mechanics, that can be used to transfer a one-time-pad over a public channel. The proposed protocol is not intended to replace the existing quantum key distribution protocols, but to demonstrate phenomenon that is not possible in classical communication and has not been discussed previously in quantum cryptography. For example, unlike previous protocols, Bob's communication back to Alice is minimum (only an abort signal upon detection of eavesdropping). Also, in the proposed protocol Bob is able to detect eavesdropping whereas in all previous protocols, Alice detected eavesdropping as she is the one who knows the original bit values that were sent. The security of the protocol remains the same as that of BB84 and the transfer is probabilistic in nature. Bob's confidence in the final key can be made arbitrarily high. Also, Alice chooses the entire key that is to be used.

With a small modification of the protocol one can eliminate the requirement of Alice's classical communication (to Bob) thus making the protocol an all quantum protocol where no bases need to be disclosed. The proposed protocol, like other key exchange protocols, is vulnerable to man-in-the-middle attack and required authenticated channels for communication.

References

- [1] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

- [2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984. IEEE Press.
- [3] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell’s theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.
- [4] A. K. Ekert. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.
- [5] S. Kak. A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, 19:293–296, 2006.
- [6] S. V. Kartalopoulos. K08: a generalized bb84/b92 protocol in quantum cryptography. *Security and Communication Networks*, 2(6):686–693, 2009.
- [7] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.
- [8] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.
- [9] A. Shamir. On the power of commutativity in cryptography. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, pages 582–595, London, UK, UK, 1980. Springer-Verlag.
- [10] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.
- [11] F. Zamani and P. Verma. A qkd protocol with a two-way quantum channel. In *Advanced Networks and Telecommunication Systems (ANTS), 2011 IEEE 5th International Conference on*, pages 1 –6, dec. 2011.