Technical Report 2007-542
Key Distribution versus Key Enhancement in Quantum Cryptography *

Naya Nagy, Marius Nagy and Selim G. Akl
School of Computing
Queen's University
Kingston, Ontario K7L 3N6
Canada
Email: {nagy,marius,akl}@cs.queensu.ca

Abstract

It has been said that quantum cryptography in general offers a secure solution to the problem of key enhancement. This means that two parties who *already* share a small secret key, can use quantum protocols to establish a new large secret key. This large secret key can be arbitrarily long and is unbreakable. Thus, to date, the main contribution of quantum cryptography has been believed to be quantum key enhancement. This paper shows that quantum cryptography can do significantly more. The quantum protocol described here distributes an unbreakable secret key to the two parties by relying on *public* information only. This is the first time that quantum cryptography is shown to be able to produce *secret* information using only *public* information. This contribution is also unique for cryptography in general, classical and quantum.

Keywords: quantum key distribution, authentication, entanglement

1 Introduction

Consider two parties, affectionately called Alice and Bob, who want to achieve sharing a secret key value. The key should be of considerable size. In fact

*This research was supported by the Natural Sciences and Engineering Research Council of Canada.

the key should be as long as the message to be encoded, thus providing a one-time pad [7]. In quantum computation such a secret key is developed by Alice and Bob following a quantum protocol, while they have two communication channels available: a quantum channel carrying quantum bits and a classical channel carrying classical binary bits. A remarkable property of these protocols is that the resulting secret key is unbreakable even with arbitrarily large computational power employed in breaking the key.

The drawback in all existing quantum computation algorithms is that for the algorithm to work, the classical channel needs to be authenticated. Authentication of a classical channel can be done using a small secret key. This means that in order to distribute a (larger) secret key between Alice and Bob, a small secret key needs to be used to authenticate the classical channel. This small secret key has to be shared between Alice and Bob prior to the quantum key distribution protocol. Therefore, these protocols are in fact quantum key *enhancement* protocols.

This paper shows that quantum cryptography has more to offer than key enhancement. In fact Alice and Bob can reach a consensus about the value of a secret key without sharing *any* secret information prior to the quantum algorithm that distributes this key. Moreover, the secret key can be arbitrarily large and consequently can be used as a one-time pad. All classical information exchanged between Alice and Bob is intrinsically public. This means that it is accessible to any eavesdropper or masquerader.

Lomonaco [5] describes the basics of classical and quantum cryptography as well as the problems faced by each discipline. He talks of the famous *Catch 22* of classical cryptography, namely:

Catch 22. There are perfectly good ways to communicate in *secret*, provided we can communicate in *secret* ...

Classical cryptography is subject to this catch and according to the literature to date, quantum cryptography falls in the same category. This paper proves however, that quantum cryptography steps out of these limits. Indeed, secret communication using quantum means does not need any prior secret or secure private communication. It only needs *public* communication. This is the strongest requirement, namely, that "some limited" public information is protected. This means that this public information is guaranteed to come from the expected source (e.g., Alice) and that the information is truthful: An eavesdropper Eve could not tamper with the contents of this information and could not masquerade as Alice. These ideas of protected public information are well known in public key cryptosystems and are referred to as the public keys. Alice publishes her public key in a secure, protected place, such as the yellow pages of a telephone book. The key is available to everybody. Eve can see the key but cannot tamper with it. Bob can see/read Alice's

public key and is *absolutely certain* that he now possesses Alice's correct public key. Note that classic cryptographic protocols, the public key cryptosystem for instance, rely on the fact that Alice *is able* to publish her key in this secure way.

The protocol presented in this paper relies on public communication only, therefore weakening the requirements for secret communication. For quantum cryptography, Catch 22 has to be reformulated as:

Quantum Catch 22. There are perfectly good ways to communicate *secretly*, provided we can communicate *publicly* in a protected way ...

The rest of the paper is organized as follows. Section 2 contains a description of entanglement as used in our protocol. Section 3 describes the BB84 key enhancement protocol from the perspective of secret and public information. Section 4 presents the main result of the paper, a quantum protocol that distributes a secret key. Notably, all information exchanged in this protocol is public. The last section, section 5, sums up the paper with some conclusions.

2 Entangled Qubits

The key distribution algorithm we present in the following sections relies on entangled qubits. Alice and Bob, each possess one of a pair of entangled qubits. If one party, say Alice, measures her qubit, Bob's qubit will collapse to the state compatible with Alice's measurement.

The vast majority of key distribution protocols based on entanglement [2, 1, 6], rely on Bell entangled qubits. The qubit pair is in one of the four Bell states:

$$\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

Suppose Alice and Bob share a pair of entangled qubits described by the first Bell state:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alice has the first qubit and Bob has the second. If Alice measures her qubit and sees a 0, then Bob's qubit has collapsed to $|0\rangle$ as well. Bob will measure a 0 with certainty, that is, with probability 1. Again, if Alice

measures a 1, Bob will measure a 1 as well, with probability 1. The same scenario happens if Bob is the first to measure his qubit.

Note that any measurement on one qubit of this entanglement collapses the other qubit to a *classical* state. This property is specific to all four Bell states and is then exploited by the key enhancement protocols mentioned above: If Alice measures her qubit, she *knows* what value Bob will measure. The entanglement employed by the algorithm proposed in this paper, however, does not have this property directly.

2.1 Entanglement Caused by Phase Incompatibility

Let us look now at an unusual form of entanglement. Consider the following ensemble of two qubits:

$$\phi = \frac{1}{2}(-|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

The ensemble has all four components, $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, in its expression. And yet, this ensemble is entangled.

Consider the following proof. Suppose the ensemble ϕ is not entangled. This means ϕ can be written as a tensor product of two independent qubits:

$$\phi = \frac{1}{2}(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$$

Matching the coefficients from each base vector, we have the following conditions:

1. $\alpha_1\alpha_2 = -1$
2. $\alpha_1\beta_2 = 1$
3. $\alpha_2\beta_1 = 1$
4. $\beta_1\beta_2 = 1$

The multiplication of conditions 1 and 4 yields: $\alpha_1\alpha_2\beta_1\beta_2 = -1$. On the other hand, from conditions 2 and 3, we have: $\alpha_1\alpha_2\beta_1\beta_2 = 1$. This is a contradiction. The product $\alpha_1\alpha_2\beta_1\beta_2$ cannot have two values, both $+1$ and -1. It follows that ϕ cannot be decomposed and thus the two qubits are entangled.

The entanglement of the ensemble is caused by the *signs* in front of the four base vector components. Thus, it is not that some vector is missing in the expression of the ensemble, rather it is the phases of the base vectors that keep the two qubits entangled.

2.2 Measurement

Let us investigate what happens to the ensemble ϕ, when the entanglement is disrupted through measurement.

If the first qubit q_1 is measured and yields $q_1 = |0\rangle = 0$ then the second qubit collapses to $q_2 = \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)$. This is not a classical state, but a simple Hadamard gate transforms q_2 into a classical state. The Hadamard gate is defined by the matrix

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Applying the Hadamard gate to an arbitrary qubit, we have $H(\alpha|0\rangle + \beta|1\rangle) = \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. For our collapsed q_2, we have $H(q_2) = H(\frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)) = -|1\rangle$. This is a classical 1.

The converse happens when qubit q_1 yields 1 through measurement. In this case q_2 collapses to $q_2 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Applying the Hadamard gate transforms q_2 to $H(q_2) = H(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = |0\rangle = 0$. Again this is a classical state 0.

It follows that by using the Hadamard gate, there is a clear correlation between the measured values of the first and second qubit. In particular, they always have opposite values.

A similar scenario can be developed, when the second qubit q_2 is measured first. In this case, the first qubit q_1, transformed by a Hadamard gate, yields the opposite value of q_2.

3 The BB84 protocol - Information on the Classical Channel is Public

Let us recall the well known BB84 key enhancement protocol. Alice and Bob share one classical and one quantum communication channel. The classical channel needs to be authenticated using a small secret key previously known to only Alice and Bob. This is why the protocol is called a key enhancement protocol. On the quantum channel Alice can send quantum bits to Bob. Alice possesses an array of entangled EPR qubit pairs. For each entangled pair, Alice reads (measures) one qubit in one of two orthonormal bases. She then sends the pair of this qubit to Bob, who randomly measures it again in one of the two orthonormal bases. After all the array of entangled qubit pairs is measured pair by pair by Alice and Bob, they start communicating on the classical channel. On the classical channel, they reveal their respective measurement bases and retain only the values of the qubits measured in the same base.

In order to check for the existence of an intruder Eve to the protocol, Alice and Bob have to check the values of some of their correctly measured qubits. These qubits will be discarded from the final key. Eve will be detected if she has measured some qubits or has replaced some qubits with qubits of her choice. It is important to note here that the classical channel is essentially public. Eve is allowed to listen to the classical channel. The information exchanged on the classical channel does not reveal any information about the value of the secret key. This is specific for quantum key enhancement protocols.

We said that the classical channel needs to be authenticated. If it were not authenticated, Eve could masquerade on both channels such that Alice *never* speaks to Bob, but only to Eve. In the same way Bob is only connected to Eve and *never* speaks to Alice. In this case both Alice and Bob have no way to detect the masquerader Eve. Therefore, the classical channel, if authenticated, prevents this situation from happening. Now here is the interesting characteristic of this algorithm. It authenticates *public* information and public information only. In this, the quantum key enhancement protocols are unique.

It follows that public information does not need a communication channel. Public information does not need to be authenticated by authenticating the communication channel. The problem of a certain public information reliably belonging to a certain source (say Alice) is not a problem of authentication any more. It is reduced to *protecting* the public information published by Alice. Normally, under commercially viable circumstances, this is accepted to be possible. As an example, publishing a telephone number in a telephone book, is accepted to provide accurate information, for which the telephone company is responsible. "Eve" cannot masquerade as someone else in a telephone book. It is therefore reasonable to consider that there are means to publishing *protected* public information, and these means are available to Alice and Bob.

4 A True Quantum Key*Distribution* Algorithm

We are ready to describe now an algorithm that truly distributes a secret key rather than enhances an already existing small secret key. The algorithm is closely related to those presented in [3, 4]. It does not need a small secret key shared by Alice and Bob in advance, because it does not authenticate any classical channel. In fact, there is no classical channel at all that would allow Alice and Bob to communicate classical binary information. The classical

information is public and therefore is published protectedly. Moreover, both Alice and Bob are allowed to publish protected public information exactly once. We will call this unique binary classical information a *public posting*. The size of the public information is similar to the size of the secret key to be established. Alice, at some point in the algorithm, will publish *her* posting and likewise Bob will publish *his* posting. Remember that these postings replace the classical communication channel of previous quantum key enhancement algorithms, and thus they will contain useful information pertaining to the protocol. Alice's posting is denoted pp_A and Bob's public posting is denoted pp_B. The two postings are independent, both in value and in time. Alice and Bob use these postings for authentication. Being protected public information, the postings define the owner.

There is a concept in classical cryptography that has characteristics in common with our public postings. The public key cryptosystem uses a private and a public key to communicate securely. Bob uses Alice's public key to encode his message and Alice decodes the message using her private secret key. The private key is known only to Alice and therefore its secrecy is ensured. The case of the public key is more interesting. Alice publishes her public key to be seen by everyone. Bob can see the public key and also Eve. The key has to be published *protectedly*, meaning Eve cannot tamper with or replace the key (i.e., masquerade as Alice). This quality of protectedness is required of Alice's public key, otherwise the system does not work.

The exact same property applies to the public postings in our algorithm. They also have to have the same property of protectedness, in which Eve cannot interfere. Some differences can be noted here. In the public key cryptosystem, Alice's public key can be used for an arbitrary number of messages sent by Bob. In our algorithm, the public postings are unique for one session of quantum key distribution. The content of the public posting naturally varies from one key distribution session to another. Also, Alice's public key is known prior to any message communication between Bob and Alice, whereas the content of the public postings are developed during the key distribution protocol.

4.1 Formal Steps

The secret key *secret* to be distributed consists of n bits, $secret = b_1 b_2 ... b_n$. The quantum communication channel consists of an array of entangled qubits. The array has length l, it consists of l qubit pairs denoted (q_{1A}, q_{1B}), (q_{2A}, q_{2B}) , ..., (q_{lA}, q_{lB}). The array is split between Alice and Bob. Alice receives the first qubit of each entangled qubit pair, namely $q_{1A}, q_{2A}, ..., q_{lA}$, and Bob receives the second half of the qubit pairs, $q_{1B}, q_{2B}, ..., q_{lB}$. The entanglement of a qubit pair is of the type described earlier, namely, phase incompatibility.

The array of qubits is unprotected. There is no guarantee that the qubits of a pair are indeed entangled; indeed, Eve may have disrupted the entanglement. Also, Eve may have masqueraded as either Alice or Bob, modifying the entangled qubits, such that Alice's qubit is actually entangled with a qubit in Eve's possession rather than Bob's, and the same holds for Bob. In case Eve has disrupted the entanglement or has masqueraded, any result of the algorithm is discarded and the key distribution is attempted all over again, from the beginning.

The size n of the secret key is less than half of the length l of the initial qubit array, $n < \frac{l}{2}$. Indeed, $\frac{l}{2}$ qubits, that is half of the qubits, are discarded because the bases in which Alice and Bob measure are inconsistent 50% of the time. From the remaining half of qubits a further arbitrary number is sacrificed for security checking. The number of qubits thus sacrificed depends on the desired degree of security.

The key distribution algorithm, like all quantum key distribution algorithms, develops the value of the secret key during the computation. Implicitly, the values of the public postings as well are developed *during* the computation. There exists no knowledge whatsoever about the values of the secret key and public postings prior to running the algorithm.

Both Alice and Bob follow the same steps briefly denoted below:

1. **Measure your entangled qubits**
2. **Compute your own public key and post it**
3. **Read your partner's key and check for eavesdropping**
4. **Construct the value of the secret key**

A detailed description of the algorithm follows.

Step 1

Alice works with the array of qubits q_{1A}, q_{2A}, ..., q_{lA}. Binary information is rendered by the results of measuring. All measurements are performed in the standard computational basis. Alice has two options for processing her qubits. She either measures a qubit directly, or she transforms the qubit by a Hadamard gate and measures afterwards. For each qubit, q_{iA}, Alice decides randomly on one of the two processing options. Notably, there is no communication with Bob at this stage. To look at a concrete example, suppose Alice has 10 qubits q_{1A}, q_{2A}, ..., q_{10A}. Qubits q_{iA} transformed by the Hadamard gate are denoted Hq_{iA}; for those measured directly the notation is unchanged. Suppose that by random choice, Alice has processed her qubits as follows:

$$q_{1A}, Hq_{2A}, Hq_{3A}, q_{4A}, q_{5A}, q_{6A}, Hq_{7A}, Hq_{8A}, q_{9A}, q_{10A},$$

and suppose again, she has measured the following binary values:

$$1, 1, 1, 0, 0, 0, 0, 1, 1, 1$$

In the meantime, Bob processes his qubits q_{1B}, q_{2B}, ..., q_{10B} following the same policy. He too, has a random choice on each qubit: to measure directly or to measure after a Hadamard transformation. Suppose again, that by random choice, Bob has obtained the following array:

$$Hq_{1B}, Hq_{2B}, q_{3B}, Hq_{4B}, q_{5B}, q_{6B}, q_{7B}, Hq_{8B}, Hq_{9B}, q_{10B},$$

with the values

$$0, 1, 0, 1, 1, 0, 1, 0, 0, 1$$

We have seen in the previous section that two entangled qubits $q_{iA}q_{iB} = \frac{1}{2}(-|00\rangle+|01\rangle+|10\rangle+|11\rangle)$, consistently render opposite classical bit measurements, if and only if exactly one qubit is measured directly and the other is measured after a Hadamard transformation. It is of no consequence whether the first qubit is Hadamard transformed or the second. The order of the qubits is irrelevant, the important issue is that exactly one of the qubits is passing a Hadamard gate. Thus, there are two "valid" measurement options:

1. q_{iA}, Hq_{iB} and
2. Hq_{iA}, q_{iB}

These measurement scenarios are valid in the sense that they, and only they, yield opposite classical bits after measurement. Each of Alice and Bob knows with certainty the value the other person has measured. Such qubits are considered valid by Alice and Bob and will be used to form the secret key and to check for eavesdropping.

Measurements of the form

3. q_{iA}, q_{iB} and
4. Hq_{iA}, Hq_{iB}

cannot be used by Alice and Bob. For any value measured by Alice, the value measured by Bob is still determined probabilistically. Qubits measured according to these scenarios, will unfortunately have to be discarded. As the

scenarios 1, 2, 3, 4 are equally likely, 50% of the initial qubits will be discarded because of probabilistically inconsistent measurements.

As mentioned, half of the l qubits are discarded because of incompatible measurement bases. The size n of the secret key is therefore $n < \frac{l}{2}$. From the remaining qubits, depending on the desired security level, some other qubits are sacrificed for checking.

For the example of the 10 qubits given above, there are five valid qubit-pairs:

$$(q_{1A}, Hq_{1B}), (Hq_{3A}, q_{3B}), (q_{4A}, Hq_{4B}), (Hq_{7A}, q_{7B}), (q_{9A}, Hq_{9B}),$$

carrying the values

$$(1,0), (1,0), (0,1), (0,1), (1,0)$$

Step 2

At this point Alice has no idea what measuring option Bob has employed on his qubits. She does not know that qubits 1, 3, 4, 7, and 9 are valid. Bob is in the same situation.

Therefore, Alice will publish her measuring strategy as part of her public posting. Alice has measured $l = 10$ qubits. As such, the first l bits to be published explain which qubits have been Hadamard transformed and which were measured directly. If Alice has applied the Hadamard gate on qubit q_{iA} then the i-th qubit of the posting is set to 1, $pp_A(i) = 1$. Otherwise, if q_{iA} has been measured directly, then the i-th qubit is 0, $pp_A(i) = 0$. For the example of 10 qubits, the first ten bits of Alice's posting are

$$pp_A(1..10) = 0110001100$$

The second part of Alice's posting is used for security checking. A certain fraction f, for example $f = 40\%$, of the original qubits are made public for Bob to check for eavesdropping. Alice chooses randomly 40% of her l qubits. For each chosen qubit, Alice publishes the index of the qubit and the binary value she has measured. To continue our example, Alice chooses randomly the indices 1, 2, 9, 10. She will publish index 1 with value 1, index 2 with value 1, index 9 with value 1 and index 10 with value 1. Translated in binary this is

$$(0001)1(0010)1(1001)1(1010)1$$

Alice's final posting is the concatenation of the measuring (Hadamard / no Hadamard) information and the qubit checking information:

$$pp_A = 0110001100 \quad 0001\ 1 \ \ 0010\ 1 \ \ 1001\ 1 \ \ 1010\ 1$$

The length of the posting depends on the length l of the qubit array and also on the desired security level given by the fraction f. The following formula computes the length of the posting:

$$length(pp_A) = l + f(1 + \log l)l$$

Here, l, the first term in the sum, refers to the measuring strategy; the second term, $f(1 + \log l)l$, represents the part that publishes the qubits for eavesdropping checking.

Bob creates his posting following exactly the same steps. Bob's measuring strategy is encoded at the beginning of his public key. For our example, this means

$$pp_B(1..10) = 1101000110$$

Suppose Bob sacrifices qubits 1, 5, 7, 8 for checking. In his public posting he will publish (0001)0(0101)1(0111)1(1000)0. Thus, Bob's final posting, the one that Alice and indeed everybody can see, is:

$$pp_B = 1101000110 \quad 0001 \quad 0 \quad 0101 \quad 1 \quad 0111 \quad 1 \quad 1000 \quad 0$$

Both Alice's and Bob's keys, pp_A and pp_B are made public and are available to everybody, including Eve.

Step 3

At this stage, Alice and Bob, in full knowledge of and consensus on each other's postings, will proceed to check for eavesdropping. Alice is looking at Bob's public posting pp_B and learns the values Bob has measured on the randomly sacrificed $f = 40\%$ of his qubits, here qubits 1, 5, 7, 8. Because of the various measuring options, only half of the $f = 40\%$ qubits will be useful. In our example, qubits 1 and 7 are measured with correct options, namely exactly one Hadamard gate applied to an entangled pair. Alice can find out the valid qubits by XOR-ing the measuring strategy of Bob with her own:

$$(0110001100)XOR(1101000110) = (1011001010)$$

which means qubits 1, 3, 4, 7, 9 have been measured well. Alice is left only to compare the values of qubits 1 and 7 she has measured with the values posted by Bob. With no malevolent interference, the binary values are opposite. Thus, if these values are opposite, Alice concludes that the protocol was

not influenced by Eve. Otherwise, Alice discards all information and starts all over again. Bob performs the same checking. He will find the valid qubits posted by Alice 1 and 9 and will compare Alice's binary measured values with his own. Thus Bob makes his own independent decision concerning eavesdropping. For reasonably large qubit arrays and a resonably large number of qubits checked, Alice and Bob will reach the same conclusion concerning the validity of the measured binary data. This conclusion effectively implies the absence of eavesdropping/masquerading (assuming, of course, that the qubits were initially entangled).

Step 4

At this stage, the possibility of eavesdropping has already been eliminated. The qubits that have not been published by Alice or Bob in their public keys continue to be unknown to everybody else. These unpublished qubits form the secret key *secret*, that is, *secret* will be formed from Alice's recorded values, and Bob's complementary values. In our ten qubit example, valid unpublished qubits are qubits 4 and 9. Therefore, the secret key will be Alice's qubits 4 and 9:

$$secret = 01$$

Bob has to complement his qubits to reach the same value as Alice.

The size (length) n of the secret key depends on the initial length of the qubit array l, as well as the fraction of discarded qubits f. Alice and Bob have decided randomly which qubits to publish. In the worst case, the set of qubits published by Alice is disjoint from the set published by Bob. Thus, the fraction of unpublished qubits is $1-2f$. From these unpublished qubits, only half (50%) are measured correctly. The length of the secret key is given by the formula

$$n = (1-2f)\frac{1}{2}l$$

For our example

$$n = (1-2\frac{40}{100})\frac{1}{2}10 = 1$$

The length of the secret key is 1 in the worst case. For our particular example we could use 2 bits.

5 Security Evaluation or Catching the Evil Eavesdropper

Let us consider the algorithm described in the previous section, from the point of view of the eavesdropper Eve. Eve wants to ideally gather knowledge about the value of the secret key without being noticed by either Alice or Bob. It is well known that an entangled qubit pair reveals no information whatsoever unless the qubits are measured and the entangled state collapses. Even so, the algorithm presented in this paper supposes that the entanglement is not protected, only the public postings are protected. This means that the qubits are not guaranteed to be entangled. Eve may masquerade and distribute qubit arrays of her own choice. It is of no advantage to Eve to distribute entangled qubits, as she gains no knowledge about the future secret key from unmeasured entangled qubits. The best choice for Eve is to distribute classical bits, or independent qubits in a known state.

The best Eve can do is to give Alice an array of classical 0s:

$$q_{1A}q_{2A}...q_{lA} = 00...0$$

and to Bob an array of $H1$:

$$q_{1B}q_{2B}...q_{lB} = H1\,H1...H1$$

All other possible arrays Eve could send to Alice and Bob are equivalent or less advantageous than the arrays above. In particular, Eve will want to send any pair (q_{iA}, q_{iB}) that *can* be measured correctly : $(0, H1)$, $(H0, 1)$, $(1, H0)$, or $(H1, 0)$. Any such pair is equally advantageous. For simplicity we will discuss the arrays of 0s and $H1$s, respectively. For a pair $(0, H1)$, Alice and Bob apply randomly one of the four measurement options. The first correct measurement option (q_{iA}, Hq_{iB}) consistently yields complementary correct results, namely $(0, 1)$. The second correct measurement option (Hq_{iA}, q_{iB}) yields all four possible classical bit combinations $(0, 0)$, $(0, 1)$, $(1, 0)$, and $(1, 1)$. Moreover, these combinations are equally likely. In one-half of the cases, measurements will be $(0, 0)$ or $(1, 1)$. This cannot happen, if the qubits are entangled and untouched. This situation reveals the intervention of Eve. Thus, on any qubit checked for eavesdropping, there is a $\frac{1}{4} \times \frac{1}{2} = \frac{1}{8}$ chance of detecting Eve.

As Alice and Bob respectively check a fraction f of the original array, the expected number of times Eve is detected, that is, the *expected detection rate*, is

$$expected\_detection\_rate = \frac{1}{8} \times f \times l$$

For our example, the expected detection rate is

$$expected\_detection\_rate = \frac{1}{8} \times \frac{40}{100} \times 10 = \frac{1}{2} = 50\%$$

Eve is caught 50% of the time. This expected detection rate is rather low given the toy example we have considered, but of course it can be increased arbitrarily by increasing f and/or l.

Suppose we have an array of 1024 qubits and work with the same fraction $f = \frac{40}{100}$. In this case, the length of the final key is

$$n = (1 - 2\frac{40}{100})\frac{1}{2}1024 \approx 100$$

This is a length that can be used in practice.

The number of qubits checked by Alice (and also by Bob) is

$$checked\_qubits = \frac{1}{2} \times \frac{40}{100} \times 1024 = 204.8$$

On each qubit, Eve can escape being caught with probability $\frac{3}{4}$. Thus Eve can escape with probability $\frac{3}{4}^{204.8} = 3.25 \times 10^{-26}$. This probability is infinitesimal for any practical purposes.

6 Conclusion

The algorithm presented above shows clearly that quantum computation has the means of producing secret information (a secret key) using public information only. This is a major difference compared to existing quantum protocols and also to classical cryptography. In our algorithm a true secret key is developed such that the eavesdropper has no knowledge whatsoever of the value of the key. In fact, Alice and Bob use only an insecure quantum channel and protected public information.

In a more general sense, in cryptography, Alice and Bob want to share a secret key to subsequently encode/decode messages. If the key is indeed secret, then messages can be indeed exchanged secretly. Secrecy of the message is ensured as long as the secret key remains totally secret and unbreakable. If Alice and Bob meet in advance to exchange a secret key this subsequent secret communication is easily achieved. If they want to communicate in secret without a prior meeting, the secrecy is much more difficult to achieve. Classical solutions with good practical results are offered by public key cryptosystems. Alice has both a private and a public key. The public key is used by Bob to encrypt a message that can be decoded only by Alice's secret key.

The encryption function is a one-way function, for which it is not feasible to compute the inverse, and hence the secret key. It is accepted though that with enough computational power such an inverse can be obtained. This means that the public key *reveals* some information about the decoding method. The secret key becomes potentially breakable.

In quantum cryptography, to date, key enhancement assures that the secret key obtained through enhancement protocols is unbreakable. Communication between Alice and Bob does not reveal any information about the secret key. But, as stated in the beginning, quantum key enhancement only obtains a longer key from a shorter one.

This paper presents, for the first time, an algorithm that develops a secret key and overcomes both disadvantages of classical cryptography and previous quantum cryptography. The following are the properties of the secret key produced by our algorithm.

1. The secret key is obtained without using a shorter secret key. This is a major improvement over the previous quantum key enhancement protocols.

2. The secret key is unbreakable. This is common to all previous quantum protocols. The public postings of Alice and Bob do not reveal anything about the value of the key. For Eve, any bit of the secret key still has a 50% chance of being 0 or 1.

The main new idea of the protocol presented in this paper is to use public postings to communicate rather than a classical channel. This idea has a more general applicability. In fact *all* quantum key enhancement protocols to date can be reformulated to work with public postings rather than classical communication channels. And this applies to quantum protocols using entanglement as well as protocols without entanglement. This is important, as it shows the general capability of quantum cryptography to generate secret information from public information. Protocols reformulated to use public postings instead of classical channels, would not need the small secret key for authentication and thus would become true quantum key distribution protocols similar to the one presented here.

If entangled qubits are easily available, the secret key established by the protocol can be arbitrarily long. Our algorithm thus allows Alice and Bob to share a one-time pad without prior meeting. To use one time pads, traditionally, Alice and Bob meet in secret and exchange a long list of keys, each as long as the message it is supposed to encrypt, and each to be used exactly once.

References

[1] Charles H. Bennett, Gilles Brassard, and David N. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557–559, February 1992.

[2] Artur Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[3] Naya Nagy and Selim G. Akl. Authenticated quantum key distribution without classical communication. *Parallel Processing Letters*, 17:323–335, 2007.

[4] Naya Nagy and Selim G. Akl. Quantum authenticated key distribution. In *Proceedings of International Conference on Unconventional Computation. Lecture Notes in Computer Science 4618*, pages 127–136. Springer-Verlag, Heidelberg, 2007.

[5] Jr. Samuel J. Lomonaco. A Talk on Quantum Cryptography or How Alice Outwits Eve. In *Proceedings of Symposia in Applied Mathematics*, volume 58, pages 237–264, Washington, DC, January 2002.

[6] Bao-Sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, and Guang-Can Guo. Quantum key distribution and quantum authentication based on entangled states. *Physics Letters A*, 281(2-3):83–87, 2001.

[7] Serge Vaudenay. *A Classical Introduction to Cryptography: Applications for Communications Security.* Springer, 2006.