Technical Report 2008-551
Sensor Networks with Quantum Memories*

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

This paper brings together two seemingly unrelated areas of unconventional computation, namely, quantum computing and wireless sensor networks. We show that by endowing each sensor node with a quantum memory, and through the use of a quantum cryptographic scheme, a level of security protection is achieved that is unprecendented, not only in the particular case of sensor networks, but also in more general situations involving secrecy and authentication. Specifically, our scheme completely eliminates the problem of identity theft, an ever growing threat to safety and security in today's society.

The quantum cryptographic solution presented here also comes with the advantages of quantum cryptography: higher security levels and protection from a larger range of attacks. The keys used for encryption are effectively unbreakable and used only once (one time pads).

Keywords: sensor networks, security in sensor networks, quantum cryptography, cryptology, entanglement transfer.

1 Introduction

For the purpose of this paper, we will call *classical cryptography*, any cryptographic scheme that does not make use of quantum bits or quantum com-

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

putation methods. That is to say, classical cryptography uses regular binary bits for computation.

Our concern here is to provide cryptographic security in a network of sensors. Each sensor monitors an area surrounding it and communicates with other sensors via radio signals. The cryptographic entities for the sensor network deviate slightly from the common definitions. The cryptographic problem is customarily formulated as follows. Two parties Alice and Bob want to communicate secretly. Bob and Alice are equivalent entities, whereas in sensor networks, as described in section 3, one entity is considerably more vulnerable to attacks than the other. Alice and Bob protect the contents of their messages through encryption and decryption with secret keys. The method used for encryption and decryption as well as how the secret key is established define a specific security scheme. All security measures have the aim to protect the communication content from a third malevolent party Eve.

Eve attempts any possible attack to gather information about the keys and the messages:

1. Eve may listen to the communication channel and read the encrypted messages. This is eavesdropping.

2. Eve may try to break the keys to be able to both encrypt and decrypt messages any time.

3. Eve may tamper with some message. For example, consider a message, as a string of bits, sent from Bob to Alice. Eve deletes a substring from the message and/or inserts a substring of her own to the message string.

4. Eve may masquerade as Bob and send messages to Alice, pretending she were Bob.

The aim of a security system is to provide an environment in which these attacks from Eve cannot succeed, or at least that Eve's actions are detected and exposed. The security system has to provide the means for Alice and Bob to communicate *secretly* and *trustworthily*.

Depending on the particular security setting, the three main characters of the cryptographic play, Alice, Bob, and Eve, personify different entities: humans, computers, some other device, or maybe even an abstract person. The straitforward simple definitions given for Alice, Bob, and Eve are satisfactory for most practical settings. As will be seen in the next sections, the above definitions are positively insufficient for wireless sensor networks.

In particular, Bob will be associated with a sensor node, yet his identity is not trivial both to define and to protect. The paper shows a clear distinction between the capabilities of classical versus quantum cryptography. The identity of Bob in classical cryptography will inherently remain fuzzy from the point of view of the cryptographic system. Classically, the identity of Bob can be fully defined only *outside* the system. *A judge* who seeks to decide unequivocally whether some entity is Bob or not (maybe Eve) has to step out of the system and make a decision that is not based on cryptographic protocols. On the other hand, the contribution of quantum memories, as described in this paper, is to make the full identification of Bob possible from inside the system. With quantum security Eve *cannot* steal Bob's identity without being caught. This paper is the first to achieve full protection from identity theft. Protection from identity theft is unprecedented in cryptography in general. Our scheme totally eliminates the problem of identity theft, which threatens security and safety in many areas of society.

Full and unequivocal identification of Bob is offered through the cryptographic protocol itself. The link between Bob's identity and Bob's identifying signature is *ensured* through the protocol itself. When Eve attempts to steal Bob's signature, she is implicitly destroying Bob's identity as well. Bob ceases to exist. And Alice can detect the disappearance of Bob. This entire process is possible *only* with quantum cryptography, as classical cryptography does not have any means, even theoretically, to offer this feature. Classically, it is not possible to make the link between the signature and the identity of Bob within the cryptographic system.

The paper defines and proposes a solution to the problem of protecting Bob, the node, in a strongly adverse environment. Section 2 makes the distinction between a cryptographic entity and its identification. Section 3 defines the sensor network and the security issues that arise in its specific environment. Section 4 defines entangled qubits and section 5 shows how this entanglement can be verified. Section 6 describes a technique of swapping the entanglement that will be used to establish a secret key. Sections 7 and 8 present the sensor network with its particular quantum characteristics and processes. Section 9 proposes a way of providing a unique quantum identification of a sensor node, wherein lies the main contribution of the paper. Section 10 describes the secret key distribution and section 11 concludes the paper.

2 The Identification versus the Identity of Bob

It has been said that the aim of a security scheme is to provide *secret* and *trustworthy* communication.

1. **Secret Communication**. The communication is secret, if Eve cannot read and understand the message. Suppose Bob sends a message to Alice. The message is encrypted and only Alice has the decryption key. She is able to read the message. As long as Eve cannot get the decryption key or cannot compute and break the decryption key, the message remains secret.

2. **Trustworthy Communication**. When Alice gets a message, she wants to be sure that the contents of the message represents the intention of the sender, and the sender is known. Here, the sender means the person that Alice knows has sent the message, namely Bob. Trustworthiness refers to both the *content of the message* and also very importantly to *the identity of the sender*. This means the content of the message has not been touched by Eve, but also the sender is indeed Bob. We will see that only quantum cryptographic means provide unequivocal identification of Bob.

Suppose now, that Bob sends a message to Alice and signs it with his name "Bob", so that Alice knows who wrote the message. The message is encrypted by some encryption key and Bob's name is also encrypted.

If the content of the message is able to consistently reach Alice without any changes, this means the message is trustworthy. Eve has not tampered with the content of the message. Eve has not added or deleted parts of the message. As long as Eve does not know the encryption key, she cannot add to the message information encrypted properly.

If Alice can consistently be sure that the messages signed with the name of "Bob" are coming from Bob, this means the messages are *authenticated*. The signature of Bob must be highly discriminant, meaning that it is very unlikely to be produced by chance. The signature must also be impossible to copy or to falsify. Usually Bob's name is encrypted using Bob's secret encryption key. As long as Eve does not know Bob's encryption key, Eve cannot sign messages with Bob's name. This protection prevents Eve from masquerading, that is, sending messages to Alice while pretending she is Bob.

Another application of Bob's signature is to *certify* a message coming from Bob. The practical application of this is electronic signatures. A document signed with Bob's electronic signature is binding for Bob. Bob cannot legally retract the validity of the document signed by him.

We see that Bob's authenticated signature has a double role: it assures Alice that the message comes from Bob, and it binds Bob to his word. From the point of view of the cryptographic system, Bob's signature identifies Bob.

In fact, this is the only way to identify Bob, namely, through his signature. His signature, by convention, is usually the encrypted version of his name. He uses his secret key, the encryption key, to encrypt his name. Behind the identifying signature of Bob stands "Bob himself". Bob's identity and identification are closely linked. Yet, there is a clear distinction between the identification signature and the identity behind the signature. If Eve steals the secret key, she steal Bob's identity. The identity behind the secret key is now Eve. To anticipate our result in sensor networks: classical cryptography is not able to "ensure" the unique correspondence between signature and identity, whereas our quantum security scheme does guarantee this correspondence. Eve cannot steal Bob's identity, she cannot become Bob without being caught.

The unique identification of Bob by his signature comes from the secrecy of the encryption key. Bob's encryption key is known only to Bob and should be again highly discriminant. The latter means that it is unlikely to find a copy of his encryption key by chance. Therefore, Bob's identification, from the point of view of the cryptographic system, is done by his secret encryption key. Actually, Bob is *cryptographically identical* to his secret key.

From the point of view of the cryptographic system, there is no distinction between Bob and his secret key. They are one and the same cryptographic entity. Note here, the important distinction between Bob as a "legal person", or the "actual person", and Bob as a "cryptographic entity". Bob as a "legal person" is a human and different from his secret key, whereas Bob as a cryptographic entity *is* his secret key. Moreover in our real world, Bob, the "legal person", is directly responsible to protect his secret key. Furthermore, Bob has to perform this protection outside of the cryptographic system. Let us illustrate this concept by a story-example:

> *Alice and Bob are two real-life people. Their professional task is to communicate secretly on some arbitrary subject. Bob has to authenticate his messages using his personal private key. This key is secret and is known only to Bob. Yet, Bob is only human ... he does not fully trust his own memory. To say nothing of the fact that keys and passwords get longer by the day. Bob has written his private key in his personal notebook. Eve can do two things:*
>
> 1. *Eve can use her huge computational power and compute / break Bob's private key, or*
>
> 2. *Eve can cunningly enter Bob's office when he is not there and copy his private key from his notebook.*

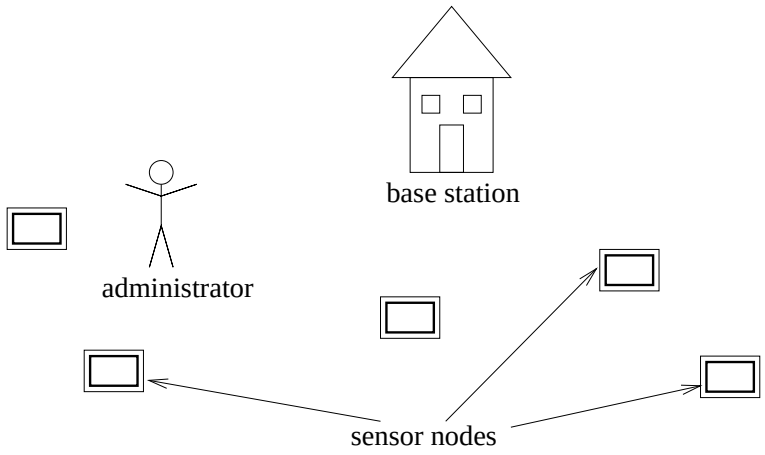

Figure 1: A network of sensor nodes with the administrator walking in the field.

The first attack is an attack **inside** the cryptographic system. If Eve manages to break the key using an inside attack, then the cryptographic system has **failed**. A good cryptographic system should be able to withstand an attack of this kind.

The second attack is **outside** the cryptographic system. If Eve manages to get Bob's private key by this method, it is not the fault of the cryptographic system. The cryptographic system **was not broken**. Yet, the cryptographic system has **failed** in that it did not cover this situation. "Bob's" cryptographic identity is now carried by two legal persons: Bob and Eve, both humans. This responsibility of protecting Bob's key pertained to "Bob" the legal person. The cryptographic system was not intended to offer protection from this second type of attack. The cryptographic scheme described in this paper will prove to be superior to the scheme described in our story in that attacks outside of the system are not possible.

In both attacks described above, if the attack is successful, then Eve has achieved her goal: the cryptographic identity of Bob, namely, his secret key, has been stolen. There is no longer an unequivocal link between Bob and his secret key. In the scheme described in this paper, both types of attacks, inside and outside of the system, are impossible. Eve is caught in both cases. Eve cannot break Bob's private key and she cannot attack "outside" of the cryptosystem. There is no identity for Bob outside the cryptographic system.

3 The Sensor Network and Its Security

A sensor network performs a monitoring task over a geographic area. For definiteness, consider the sensor nodes to be monitoring a set of environmental parameters. The administrator of the network is a mobile agent (possibly a person) moving among the sensor nodes in the field (see Fig. 1). The administrator is interested to gather information about any point in the field directly through the network, without having to move to that point. For example, the administrator wants information about a possible danger in some place, *before* moving there. From the point of view of the network, the administrator will be querying arbitrary sensor nodes. Also, if an unexpected event is sensed in the environment of some node, that node should signal to the administrator the unusual situation.

The environment in which the sensor network operates is considered to be hostile. The intruder can take any of the following actions: listen to the environment to intercept messages; send spurious messages in the environment; capture a node (read its content and reprogram its behavior).

The administrator is associated with Alice. Alice is in a position of authority over the network and implicitly over Bob. This is different from standard settings, where Alice and Bob are equivalent cryptographic entities. Alice decides when communication with a sensor node is going to take place. Also, Alice is the ultimate authority to decide whether the intruder, Eve, has meddled in the communication. The administrator's communication partner is any arbitrary sensor node. Thus, Bob is associated with the sensor node.

To defy the intruder's schemes, the network will be equipped with quantum bits and quantum computation gates. The quantum security scheme will offer effectively unbreakable secret keys, intrusion detection, and protection from identity theft. These three qualities of the quantum scheme are absent in classical existing schemes.

4 Qubits and Entangled Qubits

Qubits, or quantum bits, are the basic information unit in quantum computation. They may be in a logical state of 0 or 1 common to regular binary bits. In addition, qubits can be in a superposition of 0 and 1. Their state is 0 and 1 at the same time with a certain probability. In general, an arbitrary qubit can be written as a linear combination of 0 and 1:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

Many quantum key distribution algorithms rely on entangled qubits [6], [3], [11]. Two qubits that are entangled are described by a single quantum state [1]. Consider an entangled qubit pair: Alice holds the first qubit and Bob holds the second qubit. 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, rely on Bell entangled qubits [9]. The qubit pair is in one of the four Bell states:

$$\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2}$$

$$\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{3}$$

$$\Psi^+ = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{4}$$

$$\Psi^- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{5}$$

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

$$\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{6}$$

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 key distribution protocols: If Alice measures her qubit, she *knows* what value Bob will measure.

5 Entanglement Verification

When Eve reads one qubit q_B of an entangled qubit pair (q_A, q_B), she destroys the entanglement. Henceforth, q_A and q_B become independent qubits. Suppose q_A belongs to Alice and q_B belongs to Bob. Alice and Bob can test whether q_A and q_B are still entangled or the entanglement has been disrupted by a third party. The entanglement test is statistical, there is a probability (less than 100 %) that Eve's intervention is revealed. Also, after the test,

the state of (q_A, q_B) is collapsed to the measured values and can therefore no longer be used in the secret communication protocol. Qubits that are tested for entanglement have to be discarded from the rest of the protocol.

The first experiment to test for entanglement was based on Bell's inequality [6] and is not used here. A test for entanglement that does not use Bell's inequality is presented in [3]. The method proposed here is an abstract version of [3] as given in [8]. Consider the same qubits q_A and q_B, generated by a source of entangled qubits and then sent to Alice and Bob. Assume that $(q_A, q_B) = \Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are entangled in the first Bell state. Without prior agreement, Alice randomly decides to measure her qubit q_A either directly (in the computational basis) or after applying a Hadamard gate to it. Bob, without knowing Alice's decision, also randomly measures q_B either directly or after applying a Hadamard gate to q_B. This would mean a measurement in the computational basis (direct measurement) or in a Hadamard basis (measurement after a Hadamard gate).

If Alice and Bob measure in the same measurement basis, there is a correlation between the measured bit values. This happens when Alice and Bob both measure in the computational basis or in the Hadamard basis:

$$(I \otimes I)|\Phi^+\rangle = |\Phi^+\rangle. \tag{7}$$

$$\begin{aligned}(H \otimes H)|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(H|0\rangle \otimes H|0\rangle + H|1\rangle \otimes H|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle. \end{aligned} \tag{8}$$

In both cases, Alice and Bob measure the same bit value: both measure 0 or both measure 1.

If Alice and Bob have measured in different bases, there is no correlation between the measured values:

$$\begin{aligned}(H \otimes I)|\Phi^+\rangle &= (I \otimes H)|\Phi^+\rangle \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle). \end{aligned} \tag{9}$$

This state is still entangled, but as it is spread over all four states, Alice and Bob may measure either equal or different qubit values with the same probability.

Therefore, whenever Alice and Bob have measured in the same basis, q_A and q_B have to yield the same binary value, otherwise q_A and q_B were not entangled to begin with. There is no possible non-entangled ensemble

(q_A, q_B) that consistently yields the same bit value when measured in the same basis. For example, if $q_A q_B = |00\rangle$, there is a 25% chance of measuring different values.

If Alice and Bob share a set of entangled qubits, they have to sacrifice a number of qubits for this checking. The more qubits they sacrifice, the higher the probability to catch the intruder, Eve. In fact, this probability can be made arbitrarily high. Consider for example that Alice and Bob check ten qubits. On each qubit checked, Eve has a probability of $75\% = \frac{3}{4}$ to escape being caught. Over ten qubits, Eve escapes with probability $(\frac{3}{4})^{10} = 0.0563$. This means, Eve is caught with probability $p = 1 - (\frac{3}{4})^{10} = 1 - 0.0563 = 0.943 = 94.3\%$.

6 Quantum Teleportation and Entanglement Swapping

Quantum teleportation was defined in [2], [12]. It refers to the transfer of an *unknown* quantum state from one geographical source location to another destination location. This state transfer does not involve any transfer of matter from the source to the destination. It needs an entangled qubit pair, with the first qubit located at the source and the second qubit located at the destination. The second qubit will receive the desired unknown state. In transferring the state to the destination, it disappears from the source, in agreement with the "no cloning" theorem [13].

To obtain the desired teleported state at the destination, two bits of classical information need to be sent from the source to the destination. Depending on this information, the destination qubit needs to be transformed by a simple gate. This property complies with the principle that information cannot be transmitted at a speed greater than the speed of light.

A variant of quantum teleportation is entanglement swapping. Note that, in teleportation, the quantum state of the source qubit q_{source} disappears from the source location and reappears in the destination qubit $q_{destination}$ as exactly the same state. If the original state q_{source} was entangled with some other qubit q_{other}, this entanglement will be transferred to the destination qubit $q_{destination}$, causing the latter to be entangled with q_{other}. This scenario is called entanglement swapping and has been demonstrated in practice [7].

Entanglement swapping will be described in detail in section 8 for the particular setting of our sensor network. Entanglement swapping is the basic step towards private communication between the administrator and some sensor node.

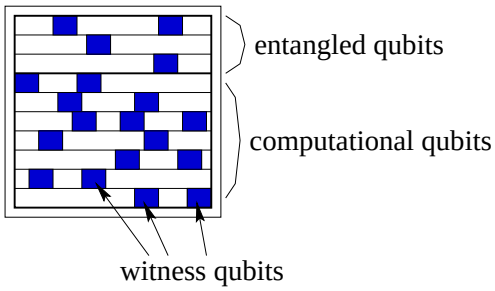

Figure 2: The structure of a node's memory. The whole memory consists of qubits.

7 Quantum Characteristics of the Sensor Network

All the quantum properties of the network will be used to provide security / secrecy of the monitoring and querying. Qubits are not inherently necessary to the monitoring task, classical bits would work just as well.

Every **node** has a local memory made of qubits (see Fig. 2). It is a quantum memory. In fact, the node does not use *any* classical bits. It is well known, that qubits subsume classical bits, meaning that everything that classical bits can compute, qubits can compute identically.

Thus nodes can work in the expected classical way, having the additional advantage of quantum based security protocols.

Qubits of a node's memory perform different tasks. In fact, there are three types of qubit utilization:

1. **Entangled qubits** are used for establishing secret keys. The key generation qubits, $qKey_1$, $qKey_2$, ..., $qKey_n$, are destined to help the key distribution protocol. As a result of the protocol, the administrator and the node will share a secret key. Qubits of this kind are entangled pairwise with qubits from the base station.

2. **Witness qubits** signal the presence of an intruder. The witness qubits, $qWit_1$, $qWit_2$, ..., $qWit_m$, are spread out over the whole memory of the node. Their role is to show the existence of an intruder. They can be hidden as part of the node's program or may be dedicated witnesses. The state of the witness qubits is different depending on whether an intruder has touched the node through reading or the node has remained untouched from the outset. Only reading of the qubits is enough to change their state, the intruder does not need to attempt writing the memory of the node. Reading a witness qubit leaves an unmistakable mark of the act on the state of the qubit.

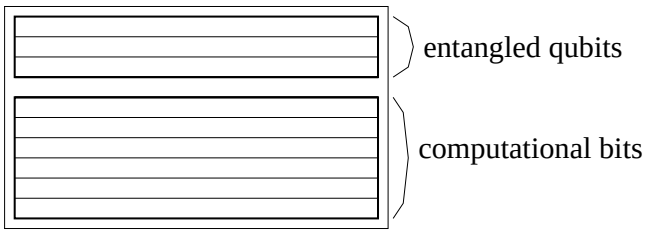

Figure 3: The structure of the administrator's memory. The two parts are structurally different: the entangled qubits are a quantum memory whereas the computational bits form an ordinary binary memory.

The witness qubits are spread out over the memory in a random way, such that an intruder will have to read witness qubits with high probability, even if the intruder reads only a fraction of the memory.

3. **Worker qubits** perform the regular job of the node. The worker qubits, $qWork_1$, $qWork_2$, ..., $qWork_p$, contain programs to be used by the node and data collected from the environment. Transit packets are also stored in this part of the memory.

An arbitrary qubit of the memory can belong to exactly one of the three categories. Every qubit maintains its category from the deployment of the sensor node, throughout the node's lifetime.

The **administrator** does not need protection from the intruder. Therefore, most of its memory consists of classical bits (see Fig. 3). Nevertheless, qubits are necessary to establish a secret key with a node. Thus, the administrator's memory consists of two types of bits/qubits.

1. **Entangled qubits** will provide secret keys for all communications with nodes of the network. The qubits $qAKey_1$, $qAKey_2$, ..., $qAKey_{nA}$, are entangled pairwise with qubits from the base station. The number of entangled qubits nA that the administrator has is considerably larger than the number of entangled qubits n of any sensor node, $nA >> n$.

2. **Worker bits** form a regular memory. The administrator uses this memory for regular computing and storage of data. This memory is of considerable size and can be viewed as the memory of a computer.

The two types of memory are used for their specific tasks only. This means that entangled qubits, for example, will not be used for regular computations.

The **base station** has the largest computational power. From the point of view of the security scheme, the base station possesses pairs of *all* entangled qubits from the field nodes and from the administrator (see Fig. 4). The set

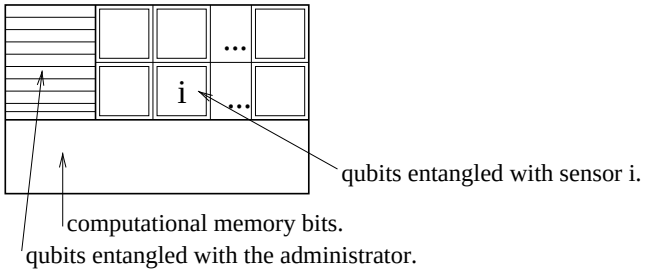

Figure 4: The structure of base station's memory.

corresponding to the administrator is $qAKey'_1$, $qAKey'_2$, ..., $qAKey'_{nA}$. For each node, the base station has a set of corresponding qubits $qKey'_1$, $qKey'_2$, ..., $qKey'_n$. The qubits are entangled in the expected way:

$$qAKey_1 \; with \; qAKey'_1; \quad qAKey_2 \; with \; qAKey'_2; \quad ...; \\ qAKey_{nA} \; with \; qAKey'_{nA}. \tag{10}$$

and

$$qKey_1 \; with \; qKey'_1; \quad qKey_2 \; with \; qKey'_2; \quad ...; \quad qKey_n \; with \; qKey'_n. \tag{11}$$

8 Entanglement Swapping in the Sensor Network

Consider some qubit of the administrator q_{ai} entangled with its base station companion qubit q'_{ai}. The administrator intends to communicate secretly with node s. The node's qubit offered for this entanglement swapping may be q_{sj} entangled with the base station's qubit q'_{sj} (see Fig. 5). These four qubits form an ensemble

$$ensemble = q_{ai} q'_{ai} q'_{sj} q_{sj}. \tag{12}$$

Note that the first qubit of the ensemble belongs to the administrator. The second and third qubits belong to the base station and the fourth qubit belongs to the sensor node. This order has been chosen so that the transformations applied by the base station are easier to see. As both the administrator's qubit pair (q_{ai}, q'_{ai}) and the sensor node's qubit pair (q_{sj}, q'_{sj}) are entangled in the Φ^+ Bell state, the ensemble can be rewritten as

$$\begin{aligned} ensemble &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle). \end{aligned} \tag{13}$$

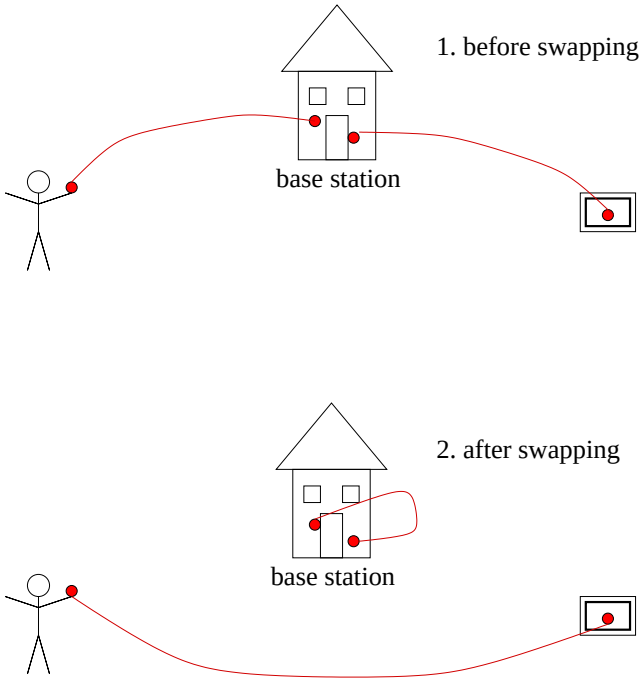

Figure 5: Entanglement swapping.

The following formula rewrites the base station's two qubits (namely, q'_{ai} and q'_{sj}) highlighting the Bell basis

$$\begin{aligned} ensemble &= \frac{1}{2}(|0\rangle \otimes \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) \otimes |0\rangle + \\ &\quad |0\rangle \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \otimes |1\rangle + \\ &\quad |1\rangle \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) \otimes |0\rangle + \\ &\quad |1\rangle \otimes \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle) \otimes |1\rangle) \\ &= \frac{1}{2\sqrt{2}}(|0\rangle \otimes |\Phi^+\rangle \otimes |0\rangle + |1\rangle \otimes |\Phi^+\rangle \otimes |1\rangle + \\ &\quad |0\rangle \otimes |\Phi^-\rangle \otimes |0\rangle - |1\rangle \otimes |\Phi^-\rangle \otimes |1\rangle + \\ &\quad |0\rangle \otimes |\Psi^+\rangle \otimes |1\rangle + |1\rangle \otimes |\Psi^+\rangle \otimes |0\rangle + \\ &\quad |0\rangle \otimes |\Psi^-\rangle \otimes |1\rangle - |1\rangle \otimes |\Psi^-\rangle \otimes |0\rangle). \end{aligned} \tag{14}$$

The base station now measures qubits two and three (namely, q'_{ai} and q'_{sj}), located at the station. The qubits are measured in the Bell basis (Φ^+, Φ^-, Ψ^+, Ψ^-).

It is interesting to see what happens to the state of the other two qubits after this measurement. The base station will have to communicate the result of the measurement to the administrator. This is done via the insecure classical channel. If the station's measurement was:

1. Φ^+. The remaining qubits have collapsed to

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{15}$$

   This is a Bell Φ^+ entanglement. The administrator and the field node are now entangled. The administrator knows that the measured valued of its qubit q_{ai} will coincide with the measured value of the node's qubit q_{sj}.

2. Φ^-. The remaining qubits have collapsed to

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{16}$$

   This is not quite a Φ^+ entanglement, as the phase is rotated. Still, the values measured for the qubits coincide, and that is sufficient to have a consensus on the measured values of the two qubits.

3. Ψ^+. The remaining qubits have collapsed to

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{17}$$

   In this case, the administrator has a qubit in which the bit values ($|0\rangle$ and $|1\rangle$) compared to the field node are reversed. After measuring its qubit, the administrator has to take the complement of the resulting bit.

4. Ψ^-. The remaining qubits have collapsed to

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{18}$$

   Now the administrator's qubit has both the bit values reversed and the phase is also rotated. After measuring its qubit, the administrator has to take the complement of the resulting bit.

The administrator has to communicate with the base station by telephone line in order to know the value measured by the base station: Φ^+, Φ^-, Ψ^+, or Ψ^-. If the base station has measured Φ^+ or Φ^- then the administrator simply measures its qubit and has the same binary value as the node. If the base station has measured Ψ^+ or Ψ^- then the administrator has to measure its qubit and then complement the resulting binary value in order to obtain the value measured by the node. Thus, there are two possible options for the administrator. The base station has to send just one bit of information to discriminate among the two options.

Note that if the administrator wants to have a known entanglement with the field qubit, the administrator will have to discriminate among all four of the base station's measurement outcomes. In this case two bits of information would need to be sent by the base station to the administrator.

After the communication step, the administrator and the field node will be able to have a consensus on the value of a bit without having ever met.

9 A New Problem in Cryptography: Who Is Bob?

You look like an angel, walk like an angel, talk like an angel
But ... you're the devil in disguise
Elvis Presley, Devil in Disguise

The cryptographic problem as defined above has some inherent assumptions. They are rather obvious so that often they are not even stated: *Alice and Bob are trusted*. All cryptographic schemes aim to safely *transfer* a message from Alice to Bob or vice-versa. Alice and Bob, the end-points of the message transfer, are supposed to exist from the beginning to the end and their intention is consistently the same and trustworthy: to communicate with each other truthfully and secretly. It is against "common cryptographic sense" to consider that Bob *changes his mind* and becomes more like evil Eve. A more palatable way to describe this scenario is that Bob dies and out of "his ashes" appears a new communication partner with the personality of Eve. As outlandish as these descriptions may seem, secure wireless sensor networks *have* to deal with scenarios of exactly this kind. The intruder can physically capture a node, then read it and change its contents. The node is thus reprogrammed to work according to the intruder's intention. This is equivalent to Bob's death and then Eve's appearance in exactly the same place. The cryptographic problem here becomes for Alice to be able to detect the change of persons from Bob to Eve.

This problem is totally new and is impossible to even address classically except with certain assumptions:

1. It takes time to reprogram a node [10].
2. Attacks follow certain geographical distributions: a node close to a corrupted node is likely to be corrupted in the future [5], [4].
3. Eve misbehaves and does not stay hidden. For example, she floods the network with spurious virus messages.

But in principle, classical cryptography has absolutely no means to *sign* one entity with the name of Bob such that Eve cannot fully copy the signature without any difference. This is also the contribution of using quantum computation.

Note here that in the original cryptographic setting, Eve may attempt to masquerade. She pretends to be Bob and sends a message to Alice signed Bob. There is a similarity between masquerading and Bob's replacement with Eve. In both cases, *full* messages come from the wrong person. Nevertheless, the similarity stops here. The difference remains fundamental. When Eve masquerades as Bob, Alice receives messages from the wrong source. Alice's job is to discern the authenticity of the message. Alice's verdict refers to the message only, and every message has to be analyzed for itself. Communication with Bob may still be attempted. In the case of wireless sensor networks, when a node is physically captured, Bob no longer exists. Eve sends messages using all the physical resources of Bob. Communication with Bob is no longer possible. Alice can no longer perform a handshake with Bob. The problem of Alice is now to clearly establish the *identity* of her communication partner: *Is Bob still the person with the intended characteristics?*

9.1 Previous Solutions to Node Capturing

As previously defined, a node is captured when Eve physically seizes the node and takes full control of its functioning. Such a node is then called *compromised*. Node capturing means that Eve first reads the contents of the node and then reprograms the node to a behavior in accordance with her own plans.

In the literature, there are several approaches to dealing with this situation.

From the early days of algorithms that deal with network reliability, various designs exist to avoid using a faulty node. The idea is to locate a node that is behaving erratically or is non-responsive and then logically eliminate the node from the network. This also implies rerouting paths for packets

that were previously using the node. As such, any rerouting algorithms may be effective in the task of eliminating a node that has been malevolently captured by Eve and thus rendered unusable for the network.

How to determine that a node is compromised comes down to judging its behavior. This doesn't seem to be directly a problem of cryptography and depends heavily on the particular application. If a node behaves erratically or is not trustworthy, it is concluded that the node is compromised. Let us discuss now the characteristics of Eve. If Eve behaves exactly like Bob, the node will behave correctly and will not be eliminated from the network. If Eve behaves largely differently from Bob, it will be easy for Alice to detect the compromised node. Here, Eve has the option to remain undetected as long as she behaves like Bob. In fact, classically, Eve will be indistinguishable from Bob. Of course, Eve prefers to remain undetected and she has good chances to remain so, while behaving even only approximately like Bob, or behaving like Bob most of the time. After all, a good lie is one that contains much truth in it. Eve may surely try to outwit Alice and lie cleverly and only sometimes. But then again, Alice will try to outwit Eve and design traps to catch her even if Eve is lying sparingly or intelligently. Alice and Eve thus start a race over who is able to outwit the other. Basically, Alice's scheme is succesfull if she is able to outwit Eve, or in more technical terms, if Alice's computational power is sufficiently superior to that of Eve. If Eve has unbounded computational power, she is not likely to be caught. The success of Alice's scheme relies on a weakness of Eve.

9.2 Bob's Quantum Signature

We are ready to describe how the identity of Bob is uniquely protected in our security scheme. Bob is associated with a sensor node. The administrator wants to be able to detect whether an intruder has "touched" the sensor node. The action of the intruder reading the memory of a node will leave an unmistakable mark on the node. The unavoidable mark or change of the node will then be detectable by the administrator, Alice. Bob's witness qubits, as defined in section 7, serve this purpose.

Suppose a witness qubit $qWit_i$ is in the state $qWit_i = H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. When Eve reads this qubit, $qWit_i$ will collapse to either $|0\rangle$ or $|1\rangle$ with equal probability. After Eve has read $qWits_i$, the state of the qubit is changed. Alice can check the state of $qWit_i$. Measuring $qWit_i$ directly will not offer any information, as Alice would just measure the same value as Eve. So Alice first applies a Hadamard gate to $qWit_i$.

If Eve has not touched the qubit then

$$H\ qWit_i = H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |0\rangle. \quad (19)$$

If Eve has previously read $qWit_i$ then one of the following two possibilities will happen:

$$H\ qWit_i = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (20)$$

$$H\ qWit_i = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (21)$$

If Eve has not read $qWit_i$ then Alice, after applying the Hadamard gate, will consistently measure a $|0\rangle$. Otherwise, Alice will measure a $|0\rangle$ or $|1\rangle$ with equal probability. Thus, Alice catches Eve with 50 % probability.

A similar scenario happens for a witness qubit $qWit_j$ in the state $qWit_j = H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. In this case, Alice would expect to read $H\ qWit_j = H\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |1\rangle$, which is consistently a binary 1. If Eve has read the qubit before, then Alice will read again a $|0\rangle$ or $|1\rangle$ with equal probability.

The witness qubits of each node are set to $H|0\rangle$, $H|1\rangle$, $|0\rangle$, or $|1\rangle$ before the node's deployment. The plain $|0\rangle$ and $|1\rangle$ are added so that Eve cannot consistently apply a Hadamard gate to obtain correct results. Each node's witness qubits are set to a different sequence of $H|0\rangle$, $H|1\rangle$, $|0\rangle$, and $|1\rangle$. The particular sequence for some node k is unique and determines the node. Suppose the witness qubits are set to $qWit_1\ qWit_2\ qWit_3\ qWit_4 ... = H|0\rangle\ |0\rangle\ |1\rangle\ H|0\rangle ...$. This sequence is the node's signature. The signature of every node is known before deployment and is communicated to the administrator. The administrator has a map of all the node's identifiers with their signatures. Interesting is that the node, although carrying its signature, does not know its value, nor does the node need to know where its witness qubits are in the memory. It is enough if the internal programs of the node do not touch any witness qubits.

When the administrator wants to check the node for intrusion, it has to measure some witness qubits. Depending on the capabilities of the sensor network, the administrator might need to move geographically beside the node to obtain the quantum state of the witness qubits to be measured. If the network allows the transfer of quantum states, for example optically, then the node just needs to send the witness qubits to the administrator via the network. The administrator will be able to determine the intrusion, but the qubits used for checking will be destroyed.

Whenever Eve reads the memory of a node, she destroys the node's signature. Eve does not know the position of the witness qubits, nor does she

know the signature. Note that, it is only Alice, the administrator, that knows this information. Not even Bob, that is, the node, is informed about the position and value of the witness qubits. This is a clear advantage, as Bob is most vulnerable to the intruder.

With this setting, the identity of Bob is very easy to define. It is the node's quantum signature. Whoever carries this particular quantum signature *is* Bob. From the point of view of the security scheme Bob's quantum signature is his identity. The really beautiful part of this definition is that even *outside* of the security scheme, Bob can be identified as his quantum signature. When Eve corrupts a node, she destroys the quantum signature, thus destroying the identity of Bob. Bob no longer exists, the node has a new identity, namely, the identity of Eve. Note that, even if Eve is smart and tries to behave like Bob, her presence is detected from the signature, that is, from the identity change. Eve cannot hide by behaving like Bob.

Also, because of the no-cloning theorem, Eve cannot make a copy of Bob's signature. If Eve could make a copy of Bob's signature, she would gather information about the key from the copy, while preserving the original. This cannot be done with quantum bits.

10 Secret Key Distribution

The protocol that distributes the secret key between the administrator (Alice) and a sensor node (Bob) follows the steps below. Consider the node to be numbered i and positioned at (x, y).

1. Communication Request. The communication request is initiated by the administrator that has the intention to communicate with some sensor node i. The administrator informs the base station via the telephone line about its intention together with the node's number. The base station knows now that the administrator will communicate with node i.

The telephone line is authenticated, but public. The intruder is able to learn that the node i will be queried. Nevertheless, the intruder does not know who this node is. The number i does not reveal the position of the node (x, y).

2. Entanglement Swapping. The base station performs an entanglement swapping between a set of k qubits of the administrator and of the node. This has been described in section 8. The base station combines pairwise the administrator's qubits with the node's qubits and measures each pair in the Bell basis. The result of the measurement is sent to the administrator via the telephone line.

3. Entanglement Verification. The administrator verifies the entanglement directly with the node, as described in section 5. Communication

with the node is done via the sensor network. The verified entangled qubits are discarded.

4. Secret Key Measurement. Both the administrator and the node measure the remaining entangled qubits. This is **the secret key**.

5. Identity Checking of Bob. This is optional. Once the key is established, the administrator checks the node's identity to protect the communication from a masquerader. As described in section 9.2, the administrator checks the node's quantum signature. This checking may be done also at the end of all communication. This validates the entire communication in terms of the genuineness of the node.

11 Conclusion

Our paper connects two domains thus far considered unrelated, namely, quantum computing and wireless sensor networks. By adding quantum memories to each sensor node, the security of the network reaches levels never before attained in any other general purpose cryptographic scheme. Our scheme completely solves the problem of identity theft. Identity theft has never been solved satisfactorily in any cryptographic setting, be it general purpose or for wireless sensor networks. This stands in sharp contrast to the need for identity protection, as today's weak identity management poses a real threat to many security sensitive transactions in our society. Our paper clearly shows that quantum memories is the answer to the issue of identity theft.

Normally, Alice and Bob are cryptographic entities with equal power. Classical cryptographic schemes are usually symmetric. In sensor networks with an administrator, this is not the case. Bob, the sensor node, is a weak entity. Bob is more susceptible to attacks from Eve. Every imaginable attack is easily effected on Bob, including the pervasive identity theft. Alice, the administrator of the network, is a powerful computational entity; the administrator has authority over the sensor node. Cryptographically, Alice "knows" Bob's identification code, his quantum signature. She is the only one to know Bob's identification code. Not even Bob knows his own quantum signature. This is a new paradigm: Alice trusts Bob, but trusts him "weakly". Bob is very susceptible to being corrupted and destroyed.

The cryptographic scheme described in this paper has some unique features. Bob's quantum signature always refers to the intended cryptographic identity, that is the functional sensor node. Eve cannot steal Bob's signature and masquerade as Bob. This property results directly from quantum features. If Eve reads the quantum signature, the superposition collapses and the signature is destroyed. Thus, together with the signature, Bob's identity is destroyed also. The destruction of the signature is easily detectable by

Alice. Therefore, Bob's quantum signature and his identity are totally protected, due to the weird properties of quantum laws. This level of identity protection has never been achieved previously.

In addition, our quantum scheme inherits all advantages of quantum cryptography, in particular the secret keys are effectively unbreakable. Any messages traveling in the network during the secret key distribution protocol reveal nothing about the value of the secret key. For the eavesdropper, any bit of the secret key still has a 50% chance of being either 0 or 1. Also, any secret key is used exactly once and is afterwards discarded. It is a one time pad.

Thus, the system designed in this paper protects the network from a huge variety of attacks. The eavesdropper does not profit from listening to the environment. Eve cannot corrupt a sensor node without being caught. Just reading the contents of a sensor node leaves an unmistakable mark on the node, which can be detected by the administrator. The security level of our scheme does not depend on Eve's computational power, nor on Eve's smart behavior. Even if Eve has an unbounded computational power, the system is equally safe.

This paper exploits directly the counterintuitive, weird properties of quantum mechanics. We believe that this is a beginning, and that quantum properties have much more to say in terms of cryptographic protocols. In this paper, secret messages are still encrypted with a classical binary secret key, albeit quantum generated. Whether a secret communication can be conceived to be fully quantum, with quantum keys and quantum messages, requires an unconventional approach to cryptography in general, still waiting to be initiated.

References

[1] Amir D. Aczel. *Entanglement.* Raincoast Books, Vancouver, 2002.

[2] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

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

[4] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. Node compromise distribution modeling under soft attacks in sensor network security.

[5] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. Attack distribution modeling and its applications in sensor network security. *EURASIP Journal on Wireless Communications and Networking*, 2008:11, 2008.

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

[7] Matthus Halder, Alexios Beveratos, Nicolas Gisin, Valerio Scarani, Christoph Simon, and Hugo Zbinden. Entangling independent photons by time measurement. *Nature Physics*, 3:659–692, 2007.

[8] Marius Nagy and Selim G. Akl. Entanglement verification with application to key distribution protocols. In *Proceedings of the 2008 International Conference on Information Theory and Statistical Learning (ITSL'08, part of WORLDCOMP'08)*, Las Vegas, Nevada, July 2008.

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[10] Adrian Perrig, Robert Szewczyk, Victor Wen, David E. Culler, and J. D. Tygar. SPINS: security protocols for sensor networks. In *Mobile Computing and Networking*, pages 189–199, 2001.

[11] 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.

[12] Lev Vaidman. Teleportation of quantum states. *Phys. Rev. A*, 49(2):1473–1476, Feb 1994.

[13] William K. Wootters and Wojceich H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, October 1982.