HYBRID AUTHENTICATION PROTOCOL TO ADDRESS THE ISSUE OF AUTHENTICATION

Julie Dilip Abraham
Amity School of Computer Sciences
Sec-44 Noida UP INDIA
julie_dilip@hotmail.com

Monika Jena
Amity School of Computer Sciences
Sec-44, Noida UP INDIA
jena_monika@yahoo.com

Abstract: **From National security and counter-terrorism to online retailing and telemedicine, secure communications is now a defining theme of the networking industry. Rapid advances in computing power are leaving traditional approaches to data encryption more and more susceptible to attack. This paper explains the basic principles of quantum cryptography and how these principles apply to quantum key distribution. The major drawbacks of Classical or Traditional Cryptography is discussed followed by full justification as to why it becomes imperative to adopt Quantum Cryptography for communication in the future. Quantum Key Distribution(QKD) has no counter-measure for man-in-the-middle attack i.e. eavesdroppers masquerading as legitimate communicators. This paper specifically deals with different strategies for Authentication in a Quantum Key Distribution System. The different strategies are broadly classified into systems using public-key authentication techniques and systems using pre-established symmetric keys. Finally, an analysis of a Hybrid Authentication Protocol that combines a QKD protocol with Symmetric Cryptography involving one or more trusted servers.**

Keywords: BB84, hybrid authentication protocol, Intrusion detection, Key-validity check, key-exchange sub-system, Photon polarization Public-Key, authentication, Quantum Cryptography, Secret-key Cryptography, symmetric-key authentication, Uncertainty principle.

I. CRYPTOGRAPHY

In the electronic communication networks that facilitate the world's information exchange, privacy and security have always remained important issues to be addressed. This is where Cryptography plays a pivotal role.

Cryptography is the art of encoding and decoding messages. The purpose of Cryptography is to transmit information such that only the intended recipient receives it.

Classical Cryptography encompasses two methods namely Secret-Key and Public-Key Cryptography.

Secret-Key Cryptography requires that users first develop and securely share a secret-key, which is a long string of randomly chosen bits. The users then use complex algorithms to encrypt and decrypt messages. The sender of a message *m* uses the key *k* to produce a ciphertext i.e. c=E(m,k) where E is the encryption algorithm. The receiver of the message uses the key *k* to recover the message i.e. m=D(c,k), where D is the decryption algorithm.

The central problem in Secret-Key Cryptography is the key distribution problem. The key-distribution problem arises from the fact that users must first communicate over a secure channel to establish a secret key before they can communicate in secret over the insecure channel. All classical methods of transmitting the key are subject to eavesdropping that cannot be detected by the users. This is referred to as the Catch-22 of Secret–Key cryptography.

Another drawback of Secret-Key Cryptography is that of Authentication. The user **A** has absolutely no means to determine with certainty that he/she is communication with **B** and not to a hacker masquerading as **B**.

Yet another drawback of Secret-Key Cryptography is that the users have no means for Intrusion Detection. i.e. the users communicating with each other cannot ascertain whether a hacker is eavesdropping/intercepting their messages.

The inherent Catch-22 flaw can be overcome by another classical cryptography method called as **Public-Key** Cryptography, in which encrypting and decrypting keys are different, hence the necessity of securely distributing a key does not arise. The process is as shown below:

$$c = E(m, PK)$$

$$m = D(c, SK)$$

or simply

$$D(E(m, PK), SK) = m$$

Where PK is the Public-key and SK is the Private-key.

The security of public-key cryptography depends on factorization or other difficult mathematical problems. It is easy to compute the product of two large numbers but extremely hard to factor it back into the primes. The popular RSA cipher algorithm, a technology first introduced in 1977 by three MIT researchers, Rivest, Shamir & Adleman, is widely deployed in public-key cryptography.

The problem of Authentication is also solved by Public-Key Cryptography by the concept of Digital Signature, that uses the reciprocity of RSA.

But the drawback of Intrusion Detection still remains.

There are some inherent problems with basing security on the assumed difficulty of mathematical problems. The first problem is that the difficulty of mathematical problems is assumed not proven. All security will vanish if efficient factoring algorithms are discovered.

The advent of "Quantum Information Science", which blends Quantum Mechanics and Information Theory, is inevitable. The ultimate technology to emerge from this science is a "Quantum Computer". The capability of Quantum Computers to rapidly perform challenging factorizations may actually lead to the eventual demise of RSA.

Hence, Classical Cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one-way functions such as that of factoring large integers.

Quantum Cryptography has satisfactorily dealt with the above mentioned fundamental issues plaguing Classical Cryptography namely secure distribution of secret keys that is independent of future developments in computing and code-breaking and in addition, also provide Intrusion Detection.

II. CRYPTOGRAPHY BASED ON QUANTUM MECHANICS

Quantum Cryptography is based on the fundamental principles of Quantum Mechanics.

Quantum Cryptography makes use of the Heisenberg Uncertainty Principle. According to the principle, ***"Knowing or measuring the value of one quantum observable implies an intrinsic uncertainty about the values of some other observables i.e. obtaining some information about an unknown quantum system generally causes a disturbance to the quantum state of that system "***. The security of Quantum Cryptography relies on this trade-off.
When a photon is on the move, it vibrates, and the angle of vibration is called its polarization. The two chosen bases of polarization and the possible results of a measurement according to the bases are: *rectilinear* polarizations: up/down ("|") & left/right ("—")and *diagonal* polarizations: diagonal left ("\") and diagonal right ("/").

The photon polarization principle describes how light photons can be oriented or polarized in specific directions. A polarized photon can only be detected by a photon filter with the correct polarization or else the photon will be destroyed.

This forms the basis for the in-built intrusion detection i.e. users can ascertain with certainty if a hacker is eavesdropping or has intercepted the message. The users can also determine if the message has been communicated without any interception.

According to Classical Physics, if a photon with an up/down polarization ("|") is sent towards an up/down Polaroid ("|"), the photon will pass through the filter. But if a left/right photon ("—") is sent towards an up/down Polaroid ("|"), the filter will block it.

In Quantum Physics, photons behave in a very erratic manner. If a diagonal photon is sent towards a rectilinear Polaroid, the filter will block the photon some of the time and other times, the photon will pass through and when it does pass through, its polarization changes. The rectilinear filter turns the diagonal photon into a rectilinear photon. The same phenomenon takes place when a rectilinear photon is sent towards a diagonal filter.

If a photon with an unknown polarization is sent to a user, there's no way to determine what that polarization is. If the user holds up an up/down filter ("|") and it passes through, it could be an up/down photon ("|"), but it may also be one of the diagonal photons ("\" or "/"). If it's blocked, it could be a left/right photon ("—"), but it may be a diagonal photon in this case as well.

Hence, Quantum Cryptography is based on the following principle:

“Every ***measurement of the unknown state of a Quantum System irreversibly perturbs the original state of the system, except if the system was prepared in a state that is compatible with the measurement.*** **“**

III. QUANTUM CRYPTOGRAPHY IN ACTION

Quantum Key Distribution (QKD) systems are used to achieve secure communication. The keys generated and disseminated using QKD systems have proved to be absolutely random and secure.

Brassard & Bennett, pioneers in Quantum Cryptography, employed individual photons of light as their very small particles and suggested the first protocol **“BB84”** for establishing a secret key using quantum transmission.

The sequence of steps involved in developing a key using the above concepts is as follows:

1. Alice (by convention the sender) sends Bob (by convention the receiver) a random sequence of photons. These photon transmissions are done on a quantum channel such as optical fiber. The quantum states are used to encode information i.e. the polarizations of the photons are oriented to represent a binary number. The convention that is followed is both “up/down (“|”)”polarization and “diagonal left polarizations (“\”)” represent **1** and both left-right (“---“) and diagonal right (“/”)” polarizations represent **0.**

2. The receiver Bob awaits with two filters: rectilinear and diagonal. As each photon reaches, Bob randomly chooses one of his filters and holds it up. Only if Bob is holding the correct filter, then and only then, the correct value would be read.

3. The above can be explained with two instances.

Alice – sends a up down photon.

Bob can either hold rectilinear filter or diagonal filter.

Case 1 : Bob chooses up-down filter, If photon passes, Bob reads it as up-down photon and if it doesn’t, reads it as left-right photon. Either way, Bob ends up reading the correct value.

Case 2: Bob chooses a diagonal filter (either left-diagonal or right-diagonal). The photon may or may not pass. If the photon passes through a right-diagonal filter, photon’s polarization also changes to right-diagonal and Bob ends up reading it as binary **0**.

4. After sending the entire sequence of photons, Alice tells Bob only the correct basis (rectilinear or diagonal) for each photon without divulging their exact polarizations. This communication is done on a classical channel, highly susceptible to eavesdropping.

5. Bob knows exactly which photons have been read correctly. This information is communicated back to Alice, again on a classical channel. Alice & Bob translate the valid polarization data into a string of bits according to the association of polarization states with the binary digits **0** and **1**. This translated string of bits forms the **key** between Alice & Bob.

6. The sender & receiver encrypt their message using the standard encryption technique **– "one time pad"**, which is a standard example of a perfect or unconditionally secure cryptosystem. A new key is generated for each transmission.

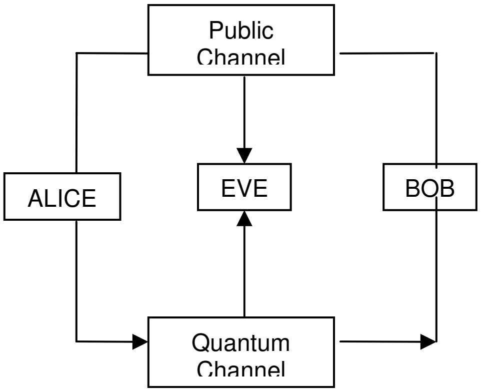

Figure.1 A Quantum Cryptographic Communication System

Table1. Illustration of BB84 Protocol

Message	0	0	0	1	1	0
Alice sends to Bob:	/	—	—	|	\	—
Bob measures with:	+	+	X	+	X	X
Bob's Results:	—	—	\	|	\	/
Valid Data:		—		|	\	
Key:		0		1	1	

+ indicates rectilinear basis

x indicates diagonal basis

IV. QUANTUM CRYPTOGRAPHY TACKLES EAVESDROPPING

The only information that takes place on a classical channel, such as telephone or email, is the exchange of basis used by Alice & Bob for measurement of photons. This information is of no consequence to the interceptor since the exact polarizations are not divulged.

The different possibilities of compromising information by Eve (by convention the interceptor) and the principles of Quantum Cryptography that aid in thwarting these attempts are described below:

1. From the burst of photons sent by the source, Eve skims some photons. Now, she has photons that are identical in polarization to those received by Bob. Eve also has to randomly choose the correct basis for measurement. Eve ends up choosing a different basis than Bob, approximately 50% of the time. Even if Eve chooses the correct basis and Bob uses the incorrect basis for measurement, the result is of no consequence to Eve, since Alice & Bob would eventually not use this particular photon for the final key. Either way, Eve does not end up with the correct key.

2. Another possibility that Eve could use to eavesdrop on the Quantum Channel is to intercept photons, measure them and send them on to Bob. However, when Eve chooses a different basis for measurement than Alice had used for preparation, she will change the photon's polarization through the act of measurement, causing Bob to receive a photon that does not have the same polarization as that sent by Alice. This definitely introduces errors into Bob's final string of bits. Alice & Bob can detect these errors when they run a "**key validity check**". This check, performed over a classical channel, involves comparing a large random subset of their string of bits, assuming that if these match up, then the others that they are not comparing also match up & can be used as the key, with the bits used for comparison being discarded. Although, Bob has chosen the correct basis, the outcome of measurement does not match the original bit encoded by Alice, hence, detecting the presence of an intruder. Therefore, the eavesdropper can't copy/read the photon or the information encoded on it without modifying it, which makes it possible to detect the security breach.

V. QUANTUM AUTHENTICATION

Now, it has been established that Quantum Key Distribution has the potential of absolutely secure communication that cannot be compromised by any eavesdropping technique. At the same time, the interceptor Eve can easily mount a "man-in-the-middle" attack, wherein, both the quantum & the public channels are cut

& subsequently Eve communicates to Alice masquerading as Bob & to Bob, pretending to be Alice. The interceptor would thus share two independent keys with the two legitimate parties and have complete control over any encrypted information that the sender and the receiver might want to send to each other.

The only way to offset this attack would be to somehow incorporate an Authentication mechanism into the whole system. The combination of Authentication mechanism & QKD protocol is referred to as the ***key exchange sub-system.***

A perfect cryptographic system would be an unconditionally secure QKD protocol (to establish the secret keys) combined with an unconditionally secure Authentication and an unconditionally secure cryptosystem.

There are two possibilities: Systems using Public-key authentication and systems using pre-established symmetric keys for authentication.

Authentication based on Public-key cryptography e.g. Digital-signature is used to provide the authentic channel needed for QKD. The security of the key-exchange system is directly dependent on the security of the public-key authentication mechanism. Hence, if RSA digital signature is used, then such a system would not offer unconditional security.

A key-exchange system using QKD and symmetric key authentication has basically two requirements: First, it requires a quantum channel between the communicating parties and secondly it requires the initial establishment and management of secret keys between the communicating parties. All the existing symmetric key message authentication methods are similar to Wegman and Carter and have based their approach on strongly universal functions.

D. Richard Kuhn proposed a Hybrid Authentication Protocol using Quantum entanglement and Symmetric Cryptography. The basic principle involves one or more trusted servers that distributes streams of entangled photons to the two communicating parties. It is assumed that both the sender & the receiver share a previously distributed secret key with the trusted server and that the two parties can communicate with the server using both classical and quantum channels. The sender & the receiver do not share secret keys with each other but make use of Third-Party Authentication.

A. Hybrid Authentication Protocol Description

On the classical channel, Alice sends a message to the trusted server, Tr. This message is encrypted with Alice's secret key and specifies the receiver Bob. Authentication between Alice and the trusted server is also required.

Using the secret keys shared with Alice and Bob, the trusted server Tr sends to Alice and Bob the location, basis, and polarization of tamper detection bits.

On the quantum channels, Tr sends a stream of k pairs of authentication key bits along with d pairs of randomly interspersed tamper detection bits. Each key bit is one half of a entangled pair of photons.

One photon of each pair goes to Alice and its twin to Bob. The tamper detection bit pairs are polarized randomly, according to a sequence of randomly selected bases. Each photon in a pair is polarized in the same direction as the other.

Alice and Bob measure key photons according to a pre-determined basis, known to all communicating parties and tamper detection photons according to the sequence of bases received from Tr, producing a sequence of authentication key bits and tamper detection bits.

Since the key bits are entangled, Bob will observe the same measurement seen by Alice. With zero transmission loss and perfect detection, the tamper detection bits will match Tr's message with 100% accuracy.

If an eavesdropper, Eve, has read the message the error rate for tamper detection bits will be 25%, since she has a 50% chance of guessing the correct basis, and a 50% chance that Alice and Bob will measure the correct polarization even if Eve chooses the wrong basis. In a practical implementation, the error threshold for tamper detection bits should be set as close to 0 as practical. If the error rate for tamper detection bits exceeds the error threshold, the protocol is restarted.

To authenticate her identity to Bob, Alice sends to Bob the result of measuring the key bit sequence to provide authentication that the message is from Alice. The authentication key effectively serves as a session password. Alice may send only a portion of the key bit sequence, sufficient to authenticate her identity, while retaining the rest to be used as a shared secret key. That is, the protocol can incorporate key distribution as well as authentication.

Bob compares his measurement of the photon stream received from Tr with the result sent by Alice. A perfect match authenticates Alice. The next step would be using the rest of the key in a conventional encryption algorithm.

Alice and Bob share a bit sequence resulting from their measurement of the key photons and even Tr cannot know the bit sequence for the bits that were measured because the measurement result is not transmitted.

B. Security Analysis of the Hybrid Authentication Protocol

1. The most obvious security breach is for Eve to intercept the photons, measure & then resend them. Eve would guess correctly the tamper detection bits interspersed randomly by Tr, 50% of the time. The photons which have been measured incorrectly would now have different polarizations. Alice & Bob would quickly detect the presence of the eavesdropper while comparing the tamper detection bits, having an error rate of 0.25. If there had been no eavesdropper, the tamper detection bits would have matched with an error rate of 0.

2. Eve can make an attempt to guess the tamper detection bits so as to avoid measuring them & hence detection. The chances of Eve correctly guessing the k bits, out of k+d bits (where k is the number of authentication bits & d is the number of tamper detection bits)is $\binom{k+d}{k}^{1}$ which is extremely small for reasonable values of k and d.

3. If Eve can distinguish the tamper detection bits, then she can avoid detection by not measuring them at all in the first place. However, the location of the tamper detection bits is protected using the symmetric keys shared by Tr and the two communicating parties. Eve would need to decrypt this information in real-time for it to be useful, because it is of no value after Alice & Bob have completed their measurements.

4. There is another issue of establishing symmetric keys with the Trusted Server. If the security of the Trusted Server is compromised, then the whole Authentication Mechanism collapses.

5. The entire Hybrid Authentication Mechanism is based on the assumption that channels are only observable and cannot be jammed or disconnected.

VI. CONCLUSION

Quantum Cryptography provides a solution that is fundamentally secure and therefore independent of the relentless advance in computing power. The technique is not only future-proof but also provides a method for key-distribution and management that allows companies and organizations to build self-reliant secure networks.

Cracking today's toughest encryption may be tough, but it is possible. With Quantum Cryptography, **forever** is not too strong a word.

The Hybrid Authentication Protocol relies on idealized properties and practical implementations may face constraints on transmission efficiency.

REFERENCES

[1] Bennett, C. H. & Brassard, G. (1984). Quantum Cryptography: Public key distribution and coin tossing. In *Proceedings of International Conference on Computers, Systems and Signal Processing*, New York.

[2] H. Barnum. "Quantum Secure Identification Using Entanglement and Catalysis." LANL archive *quantph/*9910072.

[3] C.H. Bennett and G. Brassard. Advances in Cryptology:Proceedings of Crypto '84, Springer-Verlag, pp. 475– 480.

[4] [J.G. Jensen and R. Schack. "Quantum Authentication and Key Distrubution Using Catalysis", *quant-ph*/0003104, 13 June 2000.

[5] K.G. Paterson, F.Piper and R.Schack,"Why Quantum Cryptography?",quant-ph/0406147

[6] Gary Stix. Best-Kept Secrets. *Scientific American .Com.* Feb, 03, 2005

[7] Bradford C. Bartlett. Securing Key Distribution with Quantum Cryptography. *GSEC Practical Assignment @SANS Institute.* June 30,2004

[8] Collins, G. 1992. Quantum Cryptography defies eavesdropping. *Physics Today*, November 1992