Chaotic Quantum Cryptography:
The ultimate for Network Security

Stamatios V. Kartalopoulos, Ph.D.
Williams Professor in Telecommunications Networking
The University of Oklahoma
TCOM Graduate Program
Kartalopoulos@ou.edu

ICETE 2010/SECRYPT
Athens, GR,
July 26-28, 2010

1. INTRODUCTION

Recent events have placed data security and network security at the forefront of research.

As a consequence, a number of cryptosystems and public key distribution protocols have been developed.

The U.S. National Security Agency (NSA) has recommended a set of advanced cryptographic algorithms, known as ***Suite B***. All algorithms in the Suite B are consistent with the National Institute of Standards and Technology (**NIST**) publications.

The **public key protocols** in Suite B are:

- For **key agreement**: The Elliptic Curve Menezes-Qu-Vanstone (**ECMQV**) and the Elliptic Curve Diffie-Hellman (**ECDH**)
- For **authentication**: The Elliptic Curve Digital Signature Algorithm (**ECDSA**)
- For **data encryption**: The Advanced Encryption Standard (**AES**), and
- For **hashing**: The Secure Hash Algorithm (**SHA**).

However,

vulnerabilities or ***insecurities are not absent from many algorithms,*** which one by one are broken; for example, the SHA-1 was broken by a Chinese research team (announced on March 1. 2005, *The Australian*).

Optical fiber is the medium that currently supports **many Tbps** of aggregate data traffic per single fiber using **dense wavelength division multiplexing** (DWDM)+; a cable of several hundred fibers supports many **Pbps** of aggregate traffic.

Part of this **humongous data** is sensitive and vulnerable. **And Mr. Evan, the bad actor, knows how to do it!**

As a result, modern cryptographers are in search of the **"holy grail"** of cryptography; and they search in

- **Quantum theory,** or in
- **Chaos theory.**

In the following we examine both, and particularly how they can be integrated to enhance security.

+ S.V. Kartalopoulos, *DWDM: Networks, Devices and Technology,* IEEE/Wiley, 2003

1. INTRODUCTION
2. QUANTUM CRYPTOGRAPHY BASICS
3. K05 & K08: ADVANCED PROTOCOL S for QC
4. CHAOS FUNCTIONS
5. CHAOTIC QUANTUM CRYPTOGRAPHY
6. CONCLUSION

Quantum Cryptography
Superposition of states -101

Consider a binary system. Classically, this system is in one or in the other state ("1" or "0") .

Quantum theory predicts that an **unprobed system can be in both states simultaneously, with some probability to be in one state and some other in the other. That is,**

the state of the quantum system is a superposition of the two states.

The **superposition of states** defines a **qubit,** which in |ket> notation is:

$$|y\rangle = (1/\sqrt{2})\,(\alpha\,|1\rangle + \beta\,|0\rangle),\ \text{where } \alpha^2+\beta^2=1$$

The "**qubit**" is a key concept of a quantum system. Such system may be based on the two spin eigenstates of a particle, the two polarization states of a photon, or other.

Two eigenstates are associated with the binary logic values "1" and "0" and are mathematically denoted as:

$$|1\rangle \equiv |\uparrow\rangle$$

$$|0\rangle \equiv |\downarrow\rangle$$

Again, a qubit is not defined in one state or the other but in the **superposition of the two**, which is a radical deviation from classical mechanics.

Based on this:

Quantum cryptography (**QC**) claims that a secret key can be established with a sophisticated scheme that is immune to eavesdropping. This secret key is used for encryption/decryption of messages.

The protocol that is used to establish the secret key is known as **quantum key distribution** (**QKD**). The efficiency of QKD may also deduct the presence or absence of an eavesdropper.

All possible **states of polarization** (SoP) of a single photon is better visualized if we consider the Poincaré sphere; on its surface each point S represents a particular SoP.

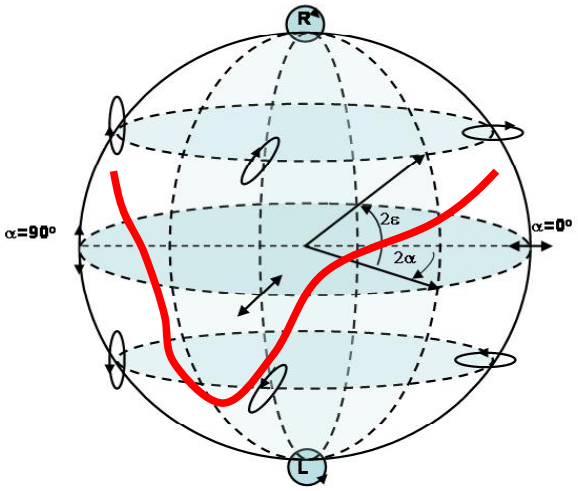
Each SoP is defined in terms of an azimuth α and an ellipticity ε as:

$$\text{SOP} = \begin{vmatrix} 1+\cos(2\alpha)\cos(2\varepsilon) & \\ & \\ \cos(2\alpha)\sin(2\varepsilon)+i\sin(2\alpha) & \end{vmatrix}$$

The SoP changes as the photon travels in a non-linear birefringent medium. This is very critical in Quantum Cryptography, which assumes that ***the SoP of a single photon remains the same for the length of travel, source-destination***.

As the SoP changes, a point S on the ***Poincaré sphere*** moves on its surface defining a trajectory of SoPs.

For now, imagine that this movement is a selective **random walk** on the surface !



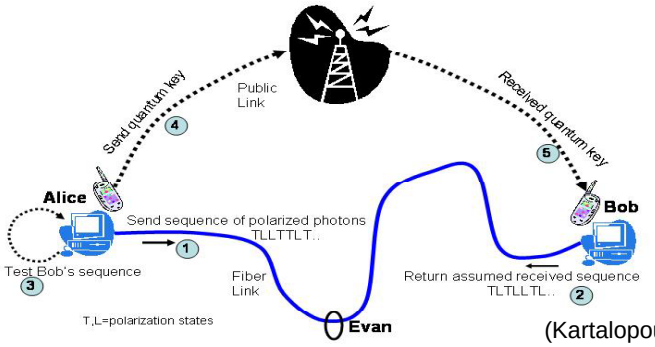
The **effectiveness** of **quantum cryptography (QC)** relies on two propositions:

- **Probing a qubit disturbs its superposition state, and it yields incomplete information.**
  That is, an intruder causes unavoidable disturbance of the qubit, which is detected by the sender and the receiver. Quanto-mechanically, “reading” the value “0” or “1” of a qubit, the superposition state holds no more.

- **A qubit cannot be copied or cloned.**
  That is, any attempt by an intruder to clone or copy a qubit will destroy the qubit state, which will be detected.

So, **how does the quantum key distribution work**?
Assume a transmitter at point A (**Alice**), a receiver at point B (**Bob**), and an eavesdropper between Alice and Bob (called **Evan**).
There are **two separate connecting paths between Alice and Bob**:

- one is the private optical fiber, and
- the other a public channel.



(Kartalopoulos, 2005)

The task at hand is to generate a key such that:

only Alice knows of it,
Bob can use it (but he does not know the details of it), and
Evan cannot understand it even if he has tapped the optical fiber.

OU-Tulsa

1. INTRODUCTION
2. QUANTUM CRYPTOGRAPHY BASICS
3. K05 & K08: ADVANCED PROTOCOL S for QC
4. CHAOS FUNCTIONS
5. CHAOTIC QUANTUM CRYPTOGRAPHY
6. CONCLUSION

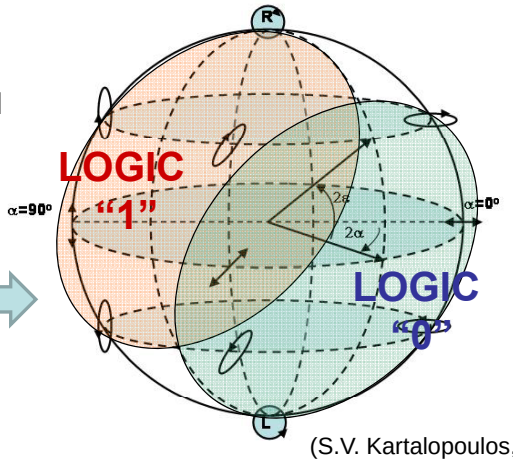
The original BB84 algorithm uses four distinct SoPs, two states per logic symbol with orthogonality as follows:

Logic "1": → **and** ↗

Logic "0": ↑ **and** ↖

Which of the two states per symbol is selected at a given time is determined ***randomly***.

We have extended the BB84 and included many SoPs per symbol; we thus define two regions on the Poincaré sphere, each with several SoPs; we have called this protocol **K05**.



(S.V. Kartalopoulos, 2005)

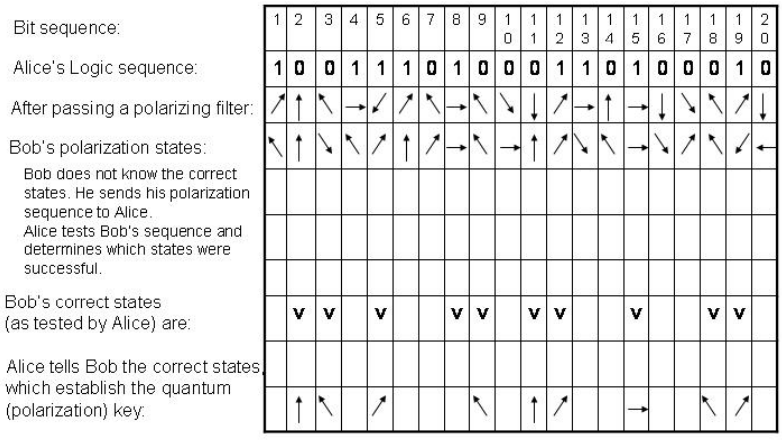
Which regions, which SoPs in a region are used and when they are used during the cryptographic process it is determined **secretly** and **randomly**.

K05: A straightforward protocol:

1. Alice passes a sequence of binary bits through a randomly polarization filter, which is transformed to a sequence of polarization states. One subset of SoPs is associated with logic "1" and another with logic "0"; the two subsets may be visualized as two regions on the Poincaré sphere. **The association of SoPs with logic "1" and "0" are known to Alice only and unknown to anyone else, including Bob**.
2. Bob receives the sequence of polarized photons, which he passes through his *independently* randomly varying polarization filter, but **Bob does not know the association of logic values and SoPs**.
3. The random polarization states of Bob's filter pass or reject the received randomly polarized photons. That is, a new sequence of logic "1s" and "0s" is generated in which some bits (statistically speaking and over a long string of bits) have the correct logic value that Alice sent **but not all**.
4. Assume that Bob's randomly varying polarization filter generates the sequence 010110101001 from the sequence received from Alice. Although ***this sequence is not what Alice transmitted***, ***the common bits between the two sequences are important here***. However, up to this step, neither Alice nor Bob know which bits are common.

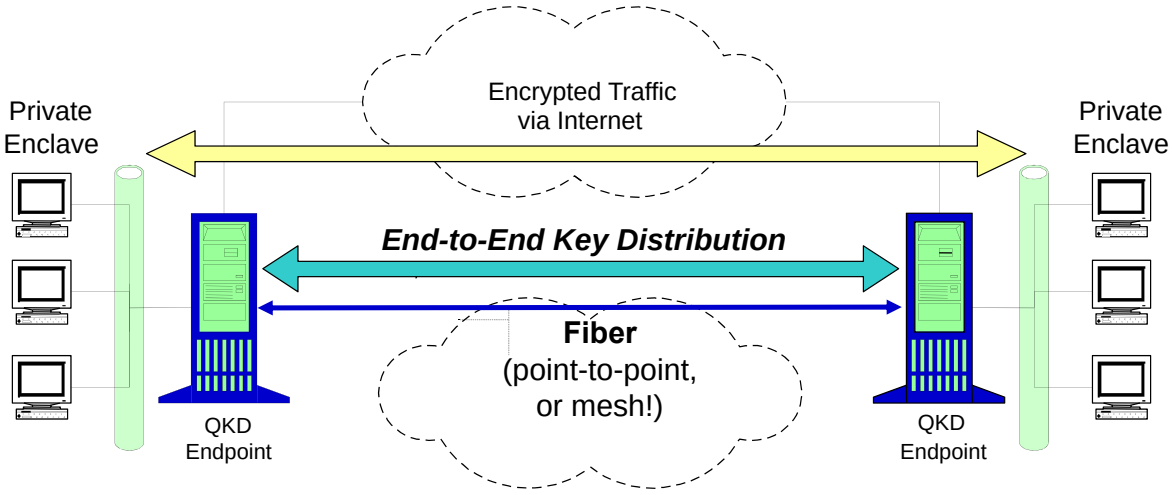
The next steps in quantum cryptography are unconventional and crucial.

5. **Bob communicates with Alice over a public unsecured channel** and he tells Alice the polarization sequence that he used while receiving Alice's polarized photons. However, **Bob does not reveal the logic sequence that he generated**.
6. Based on Bob's response, **Alice performs an experiment**. She passes the logic sequence that she sent to Bob through Bob's polarization sequence. Then, Alice compares the initial bit string with the one generated from the experiment and **she identifies the bits that are common in the two bit strings**.
7. Alice tells Bob which of his filter polarization states in the sequence were used correctly, but **without telling him their association** with logic "1" and "0". **The polarization states that were used correctly constitute the quantum key**.
8. When all this is done, Alice encrypts her message with the established key using a modulo-2 operation bit-by-bit) and transmits the encrypted message to Bob, who deciphers it using the same encryption key.



Alice determines a random association of polarization states and logic states "1" and "0".
Bob, uses a random polarization filter to pass the arriving polarized photons. Some successfully pass and some do not.
Bob, not knowing the successes and failures, tells Alice the sequence of polarization directions he used.
Alice passes her original "1" and "0" sequence and determines the ones passing through Bob's filter. She then tells Bob which polarizations were successful; this new sequence determines the quantum key.

The Quantum Network

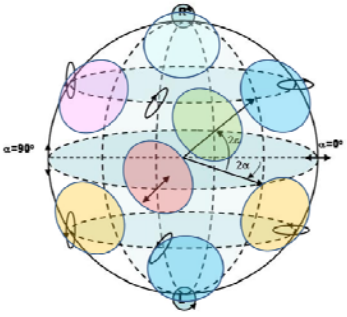


K08: An m-ary generalized protocol

The K08 subdivides the Poincare sphere in 2^m areas to define a m-ary quantum system, and a {m times n} test key length for n correct polarization states.

That is, the K08 uses an alphabet of 2^m symbols.

For example: for m=2, K08 defines four areas of polarizations on the Poincaré sphere and four symbols in binary notation (11, 01, 10, 00} or in symbolic {A, B, C, D}. Each area corresponds to one of the four. This example represents a quantum quaternary protocol, and polarizations in the defined areas are uniquely associated with one of the four symbols.



(Kartalopoulos, SCN, 2008)

Based on this, with n correct polarization states between Alice and Bob a key length for the equivalent bit string $n2^2$ is established. In a more general case m areas are defined. In this case, a n cipher key length corresponds to a $n2^m$ equivalent (binary) string or to a (n times m) symbolic alphabet.

Alternatively, for a fixed length message, the key length is greatly compressed.

QC and **QKD** use a sequence of **randomly polarized photons** and a binary system and it is based on:

- **the principle of superposition of states, and**
- **the no-cloning/no-copying of photon quantum-state principle.**

In a quantum optical network, Alice defines the encryption **quantum key** which is made known in an encrypted manner to Bob. If Evan is present, the efficiency of the QKD drops and this is understood by Bob and by Alice.

Thus, the secrecy of this method and the encryption algorithm promises a secure communications channel.

However, the method depends on the random selection of two states (BB84) or of many states (K05).

Therefore:

The randomness of states and the process that generates random states reproducibly is extremely important.

Chaotic processes satisfy the latter.

OU-Tulsa

Chaotic Systems - basics

In scientific terms, **chaos is the behavior of a mathematically described complex nonlinear function, which has an unpredictable behavior in the following sense**:

The system is extremely sensitive to initial conditions: ***it produces an extremely large output that resembles random noise for a very small perturbation to the initial condition, and a different output for different perturbation and for different initial condition.***

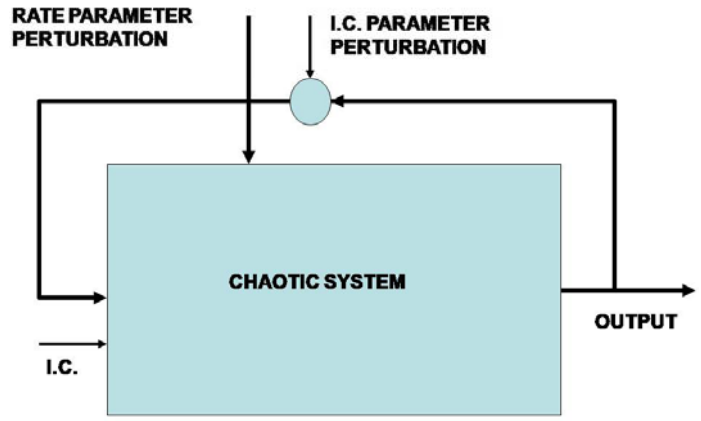


Fig 1

Chaotic System basics

Because of complexity, **chaos functions are applicable to cryptography**.

Among the mostly used functions are:

- the Lorenz/Ulam **X'=AX(1-X)**, also known as the *logistic* equation, and
- the non-linear function **$f(x,a) = (a + 1/x)^{(x/a)}$**.

In this part:

- We review chaos functions as RNGs.
- We describe chaos functions in quantum key establishment, and
- We describe a method that requires substantially fewer random bits in the stream to establish the key and it is also faster.

Consider the non-linear iterative equation $X_{n+1}=AX_n(1-X_n)$ with initial conditions A=2, and X=0.2. Making a small perturbation during the calculation process it produces different results.

Plotting A versus X then at about A=3 the graph forks in two prongs, and, at some value between 3 and 4 each prong forks again. At A=3.7 there are 32 prongs and for A>3.7 the system becomes chaotic; this is known as the ***chaotic regime*** and equations with such behavior are called ***chaos functions***.

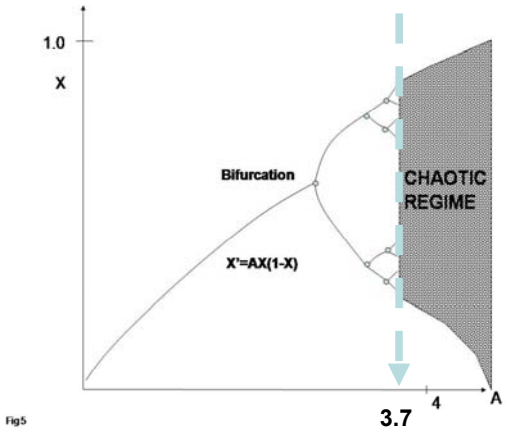


Fig5

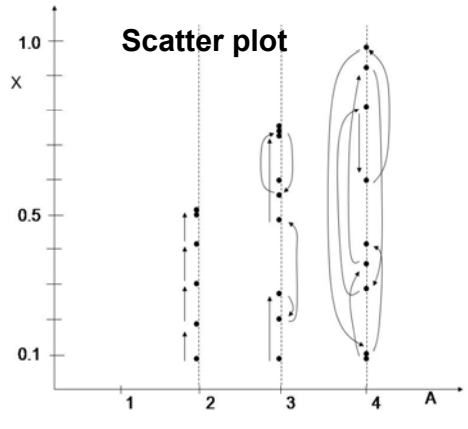


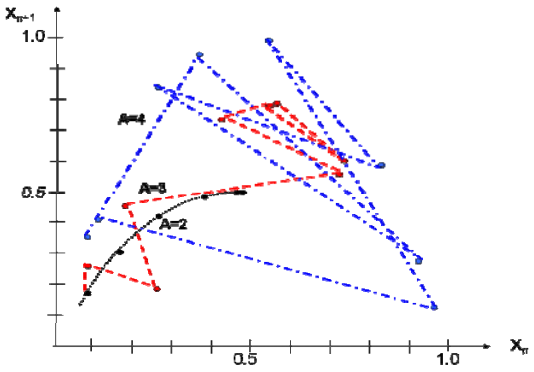
Fig2

TABLE 1

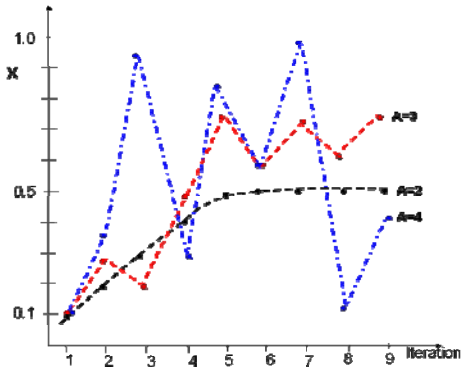
For A=2 and IC X=0.1 Xn is monotonic. For A=3, it oscillates between two prongs, and for A=4 it is chaotic.

A=2	X_{n+1}	A=3	X_{n+1}	A=4	X_{n+1}
	X_0=0.1		X_0=0.1		X_0=0.1
	0.180000000		0.270000000		0.360000000
	0.295200000		0.197100000		0.921600000
	0.416113920		0.474754770		0.289013760
	0.485926251		0.748088035		0.821939226
	0.499603859		0.565356980		0.585420538
	0.499999686		0.737185909		0.970813325
	0.500000000		0.581229671		0.113339251
	0.500000000		0.730705221		0.401973860

When a chaos function enters the chaotic regime it generates ***several random numbers of different lengths*** and **for different iteration ranges**.



Scatter plots for A=2, 3 and 4.



Graphs of iteration values for A=2, 3 and 4.

However, because ***the random process can be repeated for the same function and for the same initial conditions,***

random numbers are selectable and reproducible.

It is this ***selectability*** and ***reproducibility*** that add value to cryptographic processes, such as QC.

Thus, if both ends of a channel know the function parameters, the initial conditions, and the starting/ending points of the random sequence then they can **independently** generate the very same random numbers.

Thus, ***the random numbers generated with a chaos function can be one of the secret keys of a cryptographic algorithm***.

1. INTRODUCTION
2. QUANTUM CRYPTOGRAPHY BASICS
3. K05 & K08: ADVANCED PROTOCOL S for QC
4. CHAOS FUNCTIONS
5. CHAOTIC QUANTUM CRYPTOGRAPHY
6. CONCLUSION

This brings us to the last part of this presentation, whereby **quantum cryptography and chaos functions are integrated**.

Based on the description of chaos functions, and the random processes in quantum cryptography, a chaos function and its initial condition define random numbers, one of which is selected to determine the random process of photon SoPs at Alice and/or at Bob.

According to it, a first key is established using two random processes at Alice and/or Bob, as already described. If both use the same RN, then the key establishment or QKD is greatly expedited (faster and more reliable) and the key may be as 100% long.

During any QKD session, **Alice and Bob may change (dynamically) to different chaos function parameters and initial conditions**. This adds immensely to the security of the method.

The chaotic process may also determine the basis for the next QKD session between Alice and Bob.

Since **both ends use the same chaotic process**, the next key establishment:

- **requires a much shorter bit stream, or it generates a longer key,**
- **makes the process much faster,**
- **it greatly improves the efficiency (~100%),**
- **it detects intrusion faster.**

Thus, **chaos functions can be integrated with quantum cryptographic processes to improve both efficiency and speed of the cryptographic process**.

OU-Tulsa

We **reviewed quantum cryptography**, an extension to the BB84 protocol, K05, and how random numbers are used in the photon polarization process during the quantum key establishment.

We **reviewed chaos functions** and the conditions that enter the chaotic regime.

We explained the **random number generation with chaos functions** and their **applicability to quantum cryptography**.

We finally **integrated these concepts** and developed a quantum key establishment process that incorporates chaos functions so that the bit stream necessary to establish a key is much shorter and much faster. Thus, we believe that we have made a step closer to the **"holy grail"** in cryptography.

Our **research continuous** to identify optimum conditions for both the shortest key, or the fastest key, and also possible vulnerabilities.