Basic Quantum Cryptography

Version 0.9

Gerald Scharitzer

Vienna University of Technology

Institute of Automation

Table of Contents

1 BASICS

Quantum Cryptography is based upon conventional cryptographic methods and extends these through the use of quantum effects. The two major advantages of quantum cryptography over conventional cryptography are true random secret key generation and eavesdropping detection.

1.1 Key Generation

Key generation is performed by communication through quantum channels which make use of elemental sub-atomic particles as medium for the transport of information. This way of communication has the ability to create true random and secret raw key material, which can then be used as seeds to conventional cryptographic methods for the generation of suitable keys.

1.2 Eavesdropping Detection

Any eavesdropper listening on the quantum channel influences the particles he is observing. Thus even the application of intercept and resend methods on the quantum channel induces measurable effects on the data received.

1.3 Vocabulary

For Quantum Informatics the smallest unit of information is the qubit [BBS02 page 196], which is a generalized form of the classical bit. In topics of quantum based communication the sender is called Alice, the receiver is called Bob and the eavesdropper is called Eve. The quantum channel or quantum link is the communications channel performing the transmission of the qubits.

2 BB84 PROTOCOL

The first quantum cryptographic protocol was introduced in 1984 by Charles H. Bennet of IBM New York and Gilles Brassard of the Universtiy of Montreal. In opposition to public key systems this protocol is based upon the generation of random secret (private) encryption and decryption keys. This can be implemented in several different technologies including the following:

- single photon polarization
- single photon self interference phase modulation
- two photon entanglement

2.1 Principle

First Alice transmits a random sequence of qubits over the quantum channel to Bob. She generates this sequence by repeatedly encoding a randomly selected bit value (0 or 1) into an also randomly selected base from 2 different bases. This results in yet another random sequence of 4 different quantum states, which she sends to Bob via the quantum link. Alice records the base-value-combinations she used during generation for later use.

The 2 bases are applied for encoding and also for decoding. Furthermore they must fulfill the requirement of yielding the correct result when aligned and producing an indeterministic result when they are not aligned.

2.1.1 Key Generation

When not intercepted Bob receives the Qubits directly from Alice. Since Alice transmitted only the Qubits without any further information, the only way for Bob to derive any information from the incoming qubits is to measure them against a randomly selected sequence of bases of his own. If he selects the same base, which was used for encoding, then the result is determined to be correct. When the bases are different, then the result of this measurement is indeterministic. Bob records both his own sequence of bases and the results he measured.

After that Alice and Bob communicate via conventional means to compare their sequences of applied bases. They keep only those values, where both used the same base for encoding and decoding. The other bits are discarded from the sequence of values. This remaining sequence is a purely random private raw key and is called the sifted key. Since this raw key may not be suitable for encryption and decryption it can still be used as seed to generate such a key as long as Alice and Bob apply the same cryptographic algorithms.

The actual encryption, transmission and decryption of content is performed by conventional means over standard communication lines as long as secret key protocols are implemented. Optimum privacy can be achieved by generating an encryption key, which is as long as the document to be secured. This way, every single byte of data can be encrypted with its own randomly generated byte of the whole key. Such encrypted data contains no patterns of itself anymore, which could otherwise be used as basis for attempts of code breaking.

2.1.2 Eavesdropping Detection

When Eve listens on the quantum channel she intercepts the qubits sent by Alice and performs her observations before resending her results to Bob. Since Eve has to follow same physical laws as Bob does the only way for Eve to get any information out of the qubits sent by Alice is to apply her own sequence of bases when measuring them. The results obtained by Eve also obey the rules of determinism and indeterminism when being measured. Thus all the bits measured by Eve with a different base than Alice have a maximum probability of 50 % of being wrong.

2.2 Single Photon Polarization

The 4 basis and value states are encoded in the polarization angles of single photons as in [Gei01].

basis	value	angle	pol
⊕	0	0	→
⊕	1	π/2	↑
⊗	0	π/4	↗
⊗	1	3π/4	↖

Table 1: Basis & Value Encoding

2.2.1 Qubit Combinations

The following table shows the possible qubit combinations which can occur in an error free and undisturbed quantum channel.

	combination	01	02	03	04	05	06	07	08	09	10	11	12
Alice	basis	⊕	⊕	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗
	value	0	0	0	1	1	1	0	0	0	1	1	1
	polarization	→	→	→	↑	↑	↑	↗	↗	↗	↖	↖	↖
Bob	basis	⊕	⊗	⊗	⊕	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊕
	polarization	→	↗	↖	↑	↗	↖	↗	→	↑	↖	→	↑
	value	0	0	1	1	0	1	0	0	1	1	0	1
	correct	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✓

Table 2: Qubit Combinations

The combinations 1, 4, 7 and 10 use the same basis for encoding and decoding, so the value sent by Alice yields the same value measured by Bob. These bits will be used as raw key material.

All other combinations use different bases and thus have a 50 % probability of yielding either the same (2, 5, 8, and 11) or the other (3, 6, 9 and 12) value. The bits aquired through these combinations will not be used for key generation.

2.2.2 Intercept and Resend by Eve

	combination	01	02	03	04	05	06	07	08	09	10	11	12
Alice	basis	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
	value	0	0	0	0	0	0	0	0	0	1	1	1
	polarization	→	→	→	→	→	→	→	→	→	↑	↑	↑
Eve	basis	⊕	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕
	polarization	→	→	→	↗	↗	↗	↖	↖	↖	↑	↑	↑
	value	0	0	0	0	0	0	1	1	1	1	1	1
Bob	basis	⊕	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊕	⊕	⊗	⊗
	polarization	→	↗	↖	↗	→	↑	↖	→	↑	↑	↗	↖
	value	0	0	1	0	0	1	1	0	1	1	0	1
	correct	✓	✓	×	✓	✓	×	×	✓	×	✓	×	✓

	combination	13	14	15	16	17	18	19	20	21	22	23	24
Alice	basis	⊕	⊕	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗
	value	1	1	1	1	1	1	0	0	0	0	0	0
	polarization	↑	↑	↑	↑	↑	↑	↗	↗	↗	↗	↗	↗
Eve	basis	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕
	polarization	↗	↗	↗	↖	↖	↖	↗	↗	↗	→	→	→
	value	0	0	0	1	1	1	0	0	0	0	0	0
Bob	basis	⊗	⊕	⊕	⊗	⊕	⊕	⊗	⊕	⊕	⊕	⊗	⊗
	polarization	↗	→	↑	↖	→	↑	↗	→	↑	→	↗	↖
	value	0	0	1	1	0	1	0	0	1	0	0	1
	correct	×	×	✓	✓	×	✓	✓	✓	×	✓	✓	×

	combination	25	26	27	28	29	30	31	32	33	34	35	36
Alice	basis	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
	value	0	0	0	1	1	1	1	1	1	1	1	1
	polarization	↗	↗	↗	↖	↖	↖	↖	↖	↖	↖	↖	↖
Eve	basis	⊕	⊕	⊕	⊗	⊗	⊗	⊕	⊕	⊕	⊕	⊕	⊕
	polarization	↑	↑	↑	↖	↖	↖	→	→	→	↑	↑	↑
	value	1	1	1	1	1	1	0	0	0	1	1	1
Bob	basis	⊕	⊗	⊗	⊗	⊕	⊕	⊕	⊗	⊗	⊕	⊗	⊗
	polarization	↑	↗	↖	↖	→	↑	→	↗	↖	↑	↗	↖
	value	1	0	1	1	0	1	0	0	1	1	0	1
	correct	×	✓	×	✓	×	✓	×	×	✓	✓	×	✓

Table 3: Intercepted Qubit Combinations

The combinations where all three participants select the same basis will all deliver the value encoded by Alice to both Eve and Bob. These are the bits from the raw key which will be known to Eve.

The combinations where Alice and Bob selected different bases have a 50 % probability of yielding different values measured by Bob, regardless of Eve's interception. These values will be discarded instead of being used as raw key material.

The emphasized combinations where Alice and Bob selected the same basis, but Eve selected the other one will cause 50 % of the values measured by Bob to differ from Alice. This induces an error rate of 25 %, which can be detected, when Alice and Bob compare parts of their sifted key. Since the key comparison occurs over the conventional communications channel it is virtually public to everyone, so these bits will also be discared instead of being used as raw key material.

2.2.3 Key Generation

The first and main objective of quantum cryptography is to generate true random secret raw key material. This is performed by the following steps.

2.2.3.1 Alice sends Random Qubit Sequence

Alice encodes her part of the key with a random sequence of bases and by this generates a random sequence of qubits, which is transmitted over the quantum channel.

basis	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗
value	0	1	0	1	0	0	1	1	0	0	1	1
polarization	→	↑	↗	↖	→	→	↑	↑	↗	↗	↖	↖

Table 4: Qubits sent by Alice

2.2.3.2 Bob measures incoming Qubits

Bob measures the incoming qubits against his own random sequence of bases and records the received values. If Bob selected the same base as Alice then he will measure exactliy the same value, which was originally encoded by Alice. Otherwise the polarization of the incoming photon is unaligned with equal distance to the 2 possible polarizations of the applied base.

basis	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕	⊕
polarization	→	↑	↗	↖	↗	↖	↗	↖	→	↑	→	↑
value	0	1	0	1	0	1	0	1	0	1	0	1

Table 5: Bits measured by Bob

2.2.3.3 Alice and Bob compare Bases

Alice and Bob compare the sequences of their applied bases. The bits which were sent and received using the same base yield the same value and can be used as raw key material. On the other side there are the bits, where they used different bases, which are discarded, because they have a 50 % chance of being wrong. The following Table shows, that whenever the bases are aligned the result is correct.

aligned	✓	✓	✓	✓	×	×	×	×	×	×	×	×
correct	✓	✓	✓	✓	✓	×	×	✓	✓	×	×	✓
sifted key	0	0	0	1								

Table 6: Sifted Key

2.2.3.4 Alice and Bob generate True Random Secret Key

Since Alice and Bob select random sequences of bases independently of each other the resulting sequence of corresponding bases is purely random. Due to the indeterminism of qubits measured with unaligned bases Eve has no indication whether her values are right or wrong.

2.2.4 Eavesdropping Detection

The Goal of Eve is to obtain the actual content, which is transmitted without being detected doing so. To achieve this she applies an intercept and resend technique on both the conventional and the quantum channel. This means she listens on the communication channels and intercepts any signals sent by Alice. Then she may try to perform copy or read operations before she resends the signal to Bob. However, in quantum cryptography all these actions by Eve result in permanent quantum effects on the transmitted signals.

2.2.4.1 Alice sends Random Qubit Sequence

Alice generates her random qubit seqence and transmits it via the quantum channel to Bob in the same way, whether this transmission is being listened upon or not.

basis	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗
value	0	1	0	1	0	0	1	1	0	0	1	1
polarization	→	↑	↗	↖	→	→	↑	↑	↗	↗	↖	↖

Table 7: Qubits sent by Alice

2.2.4.2 Eve performs intercept & resend eavesdropping

Eve now intercepts the photons from Alice and may perform the following actions. When cloning the photon the no cloning theorem inhibits the clone froem being an exact copy of the original state. Thus at least one photon is modified by the process and will cause errors, whether it is resent to Bob or kept by Eve.

If Eve decides to perform her measurements on the original photon before resending it to Bob the following situation occurs. By measuring the polarization of a photon the particle adopts exactly the same polorization which was measured. This is asserted by the 5th axiom of quantum theory which causes every measurement to have an effect on the measured object. Thus again the photon resent to Bob will cause detectable errors. Even worse for Eve her measurements also follow the same indeterminism, that holds for Bob.

basis	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕	⊕
polarization	→	↑	↗	↖	↗	↖	↗	↖	→	↑	→	↑
value	0	1	0	1	0	1	0	1	0	1	0	1

Table 8: Bits measured by Eve and resent to Bob

2.2.4.3 Bob measures incoming Qubits

Bob also receives and measures the incoming qubits in the same manner, regardless of possible eavesdropping by Eve. Even though the eavesdropping attempts by Eve caused

an error rate of approximately 25 % this is not yet obvious to Bob. This time the alignment between Eve's and Bob's bases decide over determinism or indeterminism.

basis	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗
polarization	→	↑	↗	↖	→	↑	→	↑	↗	↖	↗	↖
value	0	1	0	1	0	1	1	0	0	1	1	0

Table 9: Bits measured by Bob

2.2.4.4 Alice and Bob compare Bases

This part of the protocol also performs in exactly the same way, as if not intercepted. Eve may listen on the conventional channel and obtain all the information shared by Alice and Bob, which is transmitted over this line. Thus Eve can also compare her own random sequence of bases with both the sequences of Alice and Bob. This also reveals to Eve, which of her measurements yielded the right result. The privacy is kept by the fact that Alice and Bob perform a different pattern matching than Eve and thus obtain a secret key, which is not known to Eve. In the following table it is shown that in this case situations exist, where Alice and Bob have aligned bases but Bob's values are not correct.

aligned	✓	✓	✓	✓	×	×	×	×	✓	✓	✓	✓
correct	✓	✓	✓	✓	✓	×	✓	×	✓	×	✓	×
sifted key	0	0	0	1					0	1	1	0

Table 10: Sifted but intercepted Key

2.2.4.5 Alice and Bob compare Sample of Values

To maintain security Alice and Bob will also compare small portions of their raw keys. The interception by Eve shifted the polarization of those photons, which were measured by her using a different base than Alice. These shifted photons cause the result of Bob's measurement to be indeterminate even if his base is aligned with Alice's base. When performing error correction according to standard methods, Alice and Bob will detect an above average error rate.

2.2.4.6 Alice and Bob detect Eavesdropping

After Alice and Bob detected the eavesdropping attempt by Eve they can discard the whole raw key and postpone their communication to a point when the are not listened upon any more. If this is not an option they still have the opportunity to amplify their privacy by discarding only those bits, which were communicated for error correction. The remaining sifted key can then be further modified to decrease the ratio of information available to Eve. Again all bit values revealed over the conventional must not be included in the final key. This way Alice and Bob receive a shortened but truly secret key.

2.3 Single Photon Self Interference Phase Modulation

The first quantum link technology implemented in the DARPA Quantum VPN Network [EPT03] relies on the wave-particle-dualism. The wave-aspect of particles allows self interference while the particle aspect acts as discriminator for the adoption of only single values. These values are encoded in the phase of self interference, where aligned bases

cause amplification or annihilation of the interference. In case of unaligned bases the interference results in partial amplification and annihilation, which causes the required indeterminism for quantum cryptography.

3 PHYSICS

The implementations of quantum cryptography basically rely on a few fundamental laws of quantum physics. These quantum effects describe the behaviour of sub-atomic elemental particles like photons and electrons.

3.1 Binary Quantum States

The qubit represents a binary quantum state, which is a generalization of the classical bit. [BBS02 page 196] The value of a qubit is its probability of being 1. So the highest indeterminism is achieved by a qubit with the probability of 50 % for being 1 which also implies the same probabiliy of 50 % for being 0 (the complement).

3.2 Wave Particle Dualism & Decoherence

In the microcosmos the behavior of single particles can also be described like waves. As soon as these waves interact with other particles their wave functions collapse and they behave like conventional particles. This is why a single photon can only be detected by a single detector or can only take one path through double refracting material.

3.3 Heisenberg's Uncertainty Relation

This effect leads to the 5th axiom of the quantum theory [Sch98 page 368 top]:

If the measurement of observable A yields the result a,
then the original state changes to a.

There is always an interaction between the observer and the observed. Thus every observation influences the object being observed. Thus the measurement of any of the particle's properties will affect the particle that has been measured.

3.4 No Cloning Theorem

According to this theorem it is not possible to clone (non-orthogonal) pure quantum states. [Joz02]

The existence of any physical operation,
which creates an exact copy of single quantum states
is inhibited by the laws of quantum physics.

Through this it is not possible to perform multiple observations of a single particle in its original state since this state can not be copied exactly to perform measurement on multiple copies.

The specific no cloning theorem for qubits is defined by the description of the possible operations on quantum bits. This shows that no such operation, capable of duplicating qubits can exist. [BBS02 page 200 bottom]

4 CONCLUSION

Quantum Cryptography can be performed independently of the availability of quantum computers since the qubits are only transmitted and received, without performing any quantum operations on single qubits or even sequences of qubits (quantum registers).

Communication via the quantum channel is only required during the phase of key generation to provide the desired privacy for key exchange. The actual transmisson of encrypted data occurs on convetional communication lines and application of conventional secret key cryptographic methods.

The Defense Advanced Research Projects Agency (DARPA) is currently building and testing a Virtual Private Network (VPN) implementing Quantum Key Distribution (QKD). Current scientific reports and experiments show that quantum encrypted communication can even be performed in networks and behaves according to it's theoretical background. Efforts are currently made to improve the performance and reliability of the implemented technologies. The progress of research in this field allows the anticipation of quantum cryptography to be available outside of laboratories within the next few years.

5 REFERENCES

[BBS02] Johann Blieberger, Bernd Burgstaller, Gerhard-Helge Schildt; Informatik Grundlagen 4. Auflage; Springer Wien New York, 2002; ISBN 3-211-83710-8

[EPT03] Chip Elliot, David Pearson, Gregory Troxel; Quantum Cryptography in Practice; http://arxiv.org/abs/quant-ph/0307049

[Gei01] Stefan Geirhofer; Einführung in die Quantenkryptographie; http://www.ict.tuwien.ac.at/skripten/krypto/Quanten_Krypto_Geirhofer.pdf

[Joz02] Richard Jozsa; A stronger no-cloning theorem; http://arxiv.org/abs/quant-ph/0204153

[Kie02] Claus Kiefer; Quantentheorie; Fischer Verlag, Frankfurt am Main, Oktober 2002, ISBN 3-596-15356-5

[Sch98] Franz Schwabl; Quantenmechanik 5. Auflage; Springer-Verlag, Berlin Heidelberg New York, 1998; ISBN 3-540-63779-6

[TE02] Hans Tompits, Uwe Egly; VO Quantencomputing SS 2002 Skriptum; http://www.kr.tuwien.ac.at/courses/ss2002/vo_quanten.html