Potential and Limitations of Quantum Key Distribution

An Introduction

Dr Nick Papanikolaou

Research Fellow, e-Security Group
International Digital Laboratory
University of Warwick
http://go.warwick.ac.uk/nikos

Seminar on The Future of Cryptography
The British Computer Society
17 September 2009

Outline

Introduction

Key Ideas and Connections

Quantum Information Processing: Setting the Context

Background

On the Security of QKD

Limitations and Open Questions

Overcoming Weaknesses of QKD

Formal Methods for Design and Analysis of QKD Systems

Future Directions

About Me

- Nikolaos Papanikolaou, BSc, MSc, PhD (Warwick)
- Working in **e-Security Group** led by **Professor Sadie Creese** at Digital Lab, WMG, University of Warwick
- Developed model checking tools and techniques for quantum systems [was supervised by **Rajagopal Nagarajan**]
  - Supported by EPSRC grants and EU project **SECOQC**.
- For more information see `http://go.warwick.ac.uk/nikos`.

Outline

Outline

Quantum Computing and Quantum Information

Quantum computing and quantum information is an emerging discipline that has been developing steadily over the past 25 years.

- Usable quantum computers are 10–20 years away...
- **but** technologies involving quantum information are practical and commercially available today!
  - **Quantum key distribution systems** by MagiQ, ID Quantique, NEC, Toshiba, ...
  - there are strong security results with no classical analogue [Mayers '00]

Quantum Information Processing

- Quantum Information Processing (QIP) is the discipline dealing with **the storage, manipulation and transmission of information using quantum phenomena.**
- QIP is divided into two interrelated areas:
  - Quantum Computation
  - Quantum Information Theory
- QIP has important applications in cryptology.

Quantum Information Processing

- There exist efficient **quantum algorithms**, with no classical analogue, for solving difficult computational problems.
  - **prime factoring** and **discrete logarithm** (Peter Shor)
  - unstructured database search (Lov Grover)
- The implementation of quantum algorithms requires large–scale **quantum computers**.
- Quantum computers will clearly threaten the security of popular current–day cryptosystems (e.g. RSA, ElGamal).

Quantum Protocols

Practical systems implement protocols involving characteristic quantum phenomena:

- **superposition** of quantum states
- **quantum entanglement**
- the **probabilistic nature** of quantum measurement

Using these phenomena:

- the presence of an eavesdropper is detected in quantum key distribution [Bennett & Brassard 84]
- anonymity, commitment in untrusted settings, and other security goals can be achieved [Bouda 07, ...]
- one can devise quantum schemes for common cryptographic tasks, including **oblivious transfer**, **bit commitment** etc.

Fundamental Issues

A classical computing device **cannot efficiently simulate a quantum computer** [Feynman 82]. The possibility of quantum computing gives rise to **new complexity classes** and challenges the strong version of the Church–Turing thesis.

However:

- **Quantum protocols** are simpler to implement in practice and do not require the full power of a quantum computer.
- In fact, several protocols are efficiently simulable on current hardware.

Real Considerations

Practical quantum technologies **combine manipulation of quantum and classical bits**.
Typical setups described by the QRAM model [Knill 97]:

classical hardware & software	+	quantum resource

- The interaction of a quantum system with a classical computing device is a **potential source of flaws and vulnerabilities.**
- Even if an arbitrary quantum protocol (exploiting the full power of quantum computation) cannot be efficiently implemented, it is possible today to have technology comprising **combined quantum–classical systems.**

How to use QKD in a real system

Key Point What I intend to emphasize is that the "quantum" part of quantum cryptography is but a piece of a bigger puzzle.

I will reveal parts of the puzzle one by one, so that the limitations of the purely "quantum" part are addressed in order.

The Security Results for QKD refer to a full system, which comprises a combination of quantum and classical processes.

- **Key distribution** is the process of establishing a common secret

  $$k \in \{0,1\}^N$$

  known as the **key**, between two users ("Alice" and "Bob"), so that they may subsequently exchange secret messages.
- Unconditionally secure key distribution in a classical (i.e. non–quantum) setting is impossible; classical key distribution is, at best, **computationally secure**.
- Strong known security result:
  - **QKD is unconditionally secure against all attacks permitted by quantum mechanics (Mayers, 1996).**

- QKD solves the `Catch-22' known as the *key distribution problem*.
- A **private-key cryptosystem** can be used with the key that is established to exchange secret messages.
- **Public-key cryptography** was designed to solve the same problem: in this setting users use different keys for encryption and decryption of messages.

- The security of QKD relies on the probabilistic and destructive nature of quantum measurement, as well as the **no–cloning theorem** for quantum states.
  - Quantum channels cannot be monitored without causing noticeable disturbances.
  - Quantum states cannot be cloned.
- Several protocols have been proposed for QKD:
  - **BB84 (Bennett and Brassard, 1984)**
  - B92 (Bennett, 1992)
  - E91 (Ekert, 1991)
- These **basic protocols** only allow the establishment of a **raw key** in such a way that an **enemy's presence can be detected**.
- Further **classical** processing is necessary to produce a final, secret key.

Background

BB84 With No Eavesdropping

- In ⊞–basis, 0 is represented by $|0\rangle$ and 1 by $|1\rangle$.
- In ⊠–basis, 0 is represented by $|+\rangle$ and 1 by $|-\rangle$.
- Phase 1. Alice $\longrightarrow$ Bob.

1.	Alice picks a random bit sequence.	**0**	**1**	**0**	**1**	**0**	**1**	**0**
2.	Alice picks an encoding basis.	⊞	⊞	⊠	⊞	⊠	⊠	⊞
3a.	Alice prepares and sends qubits.	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$

- Phase 2. Bob.

3b.	Bob receives qubits.	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$
4.	Bob picks a decoding basis.	⊠	⊞	⊞	⊠	⊠	⊞	⊞
5.	Bob measures with dec. basis.	0 or 1	**1**	0 or 1	0 or 1	**0**	0 or 1	**0**

- Phase 3. Alice and Bob compare bases and discard errors. Result = **100**

Background

BB84 with Eavesdropping

- Typical...**woman–in–the–middle** attack.
- **Eve** intercepts and measures qubits. She places the results of her measurements back onto the channel.
- Passive eavesdropping impossible (no–cloning!).

	Original bit sequence:	**0**	**1**	**0**	**1**	**0**	**1**	**0**
	Alice's encoding bases:	⊞	⊞	⊠	⊞	⊠	⊠	⊞
3b.	Eve intercepts qubits.	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$
4.	Eve picks a decoding basis.	⊞	⊞	⊞	⊞	⊞	⊞	⊠
5.	Eve measures with basis.	**0**	**1**	0 or 1	**1**	0 or 1	0 or 1	0 or 1
6.	Bob picks a decoding basis.	⊠	⊞	⊞	⊠	⊠	⊞	⊞
7.	Bob measures with basis.	0 or 1	**1**	0 or 1	0 or 1	0 or 1	0 or 1	0 or 1
						↑ detected		↑ detected

Detecting an Eavesdropper

- The eavesdropper, "Eve," will try to perform a "woman–in–the–middle" attack by trying to intercept and measure the qubit states sent by Alice.
- In order to make a measurement, Eve chooses a measurement basis at random.
  - If Eve uses the correct basis to measure the *i*th qubit, she will leave that qubit undisturbed.
  - **If Eve uses the incorrect basis** to measure the *i*th qubit, **she will destroy the original state of the qubit and collapse it to one of that basis' states.** Furthermore, she will have to send Bob a new qubit (no–cloning theorem).

Detection

As soon as Alice and Bob find a bit position i for which $b_i' = b_i$ but $d_i' \neq d_i$, they know an eavesdropper is present.

Detecting an Eavesdropper

- Eve necessarily causes a disturbance to a qubit whenever she chooses the wrong basis. In this case, if Bob subsequently tries to measure the qubit correctly, **his** result will be random! (incorrect 50% of the time)

Detection

As soon as Alice and Bob find a bit position i for which $b_i' = b_i$ but $d_i' \neq d_i$, they know an eavesdropper is present.

Attacking BB84

- What about **impersonation**?
  - **Unconditionally secure user authentication** is possible **classically** using hash functions (Wegman–Carter, 1979).
- What if Eve has a **quantum memory**?
  - No cloning theorem: She has to create **substitute states** to send to Bob, or she will be easily detected.
- What if there is **noise** on the channel?
  - the **upper bound** on errors induced by the channel is exceeded when an eavesdropper is present.
- What happens when an eavesdropper is detected?
  - A secret key can be established, using **privacy amplification** (which can be done **classically**).

The Meaning of Unconditional Security

Unconditional security often refers to the property of an ideal cryptosystem, as defined by Shannon (1949). He preferred the term **perfect secrecy**.

Perfect secrecy

A cryptosystem has perfect secrecy if

$$H(M|C) = H(M)$$

- Unconditional security is independent of the computational power of the attacker (as opposed to *computational security*).
- In quantum information processing we specifically stipulate that a system/protocol must be secure **against all attacks permitted by the laws of Quantum Mechanics**.

Unconditional Security of Quantum Key Distribution (Mayers, 1998)

- BB84 is unconditionally secure if, after the basic protocol is complete:
  - **Secret-key reconciliation** is performed to reconcile Alice and Bob's binary sequences.
  - **Privacy amplification** is performed to extract a secret subset of the reconciled key.
- If the above hold, **BB84 guarantees the eventual establishment of a common secret key,** in the presence of an eavesdropper.
- This is true **even if there is noise** on the quantum channel.
- The security proof determines a **lower bound** on the number of qubits which must be transmitted to guarantee a final key of given length.

Outline

Basic QKD Protocols In Isolation

A protocol such as BB84, by itself, is intended to make the presence of an eavesdropper manifest to the users of a quantum channel.

The presence of an eavesdropper is associated with a **disturbance** (noise) on the channel.

If the channel is inherently noisy, **how to distinguish between channel noise and errors induced by eavesdropping?**

How to minimize/eliminate information about the key released to the eavesdropper?
How to establish a key even in his/her presence?

Secret Key Reconciliation

Alice and Bob compare their bases over a public channel, which the eavesdropper has control over.

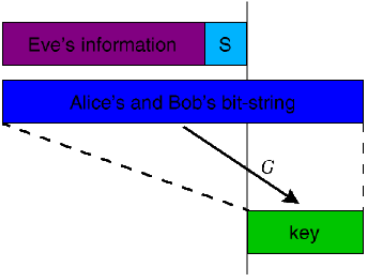
They will exchange actual bit values for some of these, thus revealing information about the key.

Reconciliation protocols allow Alice and Bob to correct errors due to channel noise while releasing a **minimum amount** of information to the eavesdropper.

Secret–Key Reconciliation was proposed by Louis Salvail (1994) and is essentially a form of error correction. (Rather than exchanging bits, **parities** of subsequences of the key are exchanged)

Privacy Amplification

Privacy amplification is a process that allows Alice and Bob to **distill a secret key** from a bit sequence that an eavesdropper has partial information about. The point is to **eliminate** those parts of the key for which the eavesdropper has partial information.



Authentication

Authentication is a process which provides assurance to users of a channel that they are, in fact, communicating with whom they think.

Thus, authentication addresses the possibility of an **impersonation** attack.

Wegman and Carter (late 1970s) proposed a scheme for authentication that has been proven to be **unconditionally secure** - it is a classical protocol which involves applying certain **hash functions** to parts of Alice's and Bob's keys.

BUT: their method ultimately requires some pre-shared bits.

Putting it all together: A Full System

[pre-shared bits?]

↓

Authentication

↓

QKD Protocol

↓

Secret-Key Reconciliation

↓

Privacy Amplification

↓

FINAL KEY

Outline

Research in Theoretical Computer Science

- Measurement-based quantum computing - measurement calculus [Edinburgh]
- Quantum process algebras [Glasgow/Warwick, Grenoble, ...]
- Categorical quantum mechanics [Oxford]
- Simulation of quantum systems [many places]

Outline

Review and Conclusions

- We discussed the processes that make up a **complete QKD system**
- Key point was to show that **unconditional security** is achieved only through a **combination** of features of QM and classical CS results.
- Hopefully given an insight into how these systems work and what sort of attacks they need to resist.
- Pointed out **theoretical limit** - pre-shared information is still needed for unconditionally secure authentication!

Making QKD a part of UK/EU infrastructure

Computer scientists should develop tools and formalisms for understanding these processes and for designing **provably correct implementations**.

It is up to the physicists to do the really difficult part!

For Further Reading

- Gay, S. and I. Mackie, eds.
  Semantics of Quantum Computation.
  Cambridge University Press, 2010.
- Papanikolaou, N.
  Model Checking Quantum Protocols.
  PhD thesis, Department of Computer Science, University of Warwick, 2008.
- Gay, S., Nagarajan, R., and Papanikolaou, N.
  QMC: A Model Checker for Quantum Systems.
  Proceedings of Conference on Computer Aided Verification (CAV'08), Princeton, USA.

See `http://go.warwick.ac.uk/nikos`.