An Automated Analysis of Quantum Key Distribution

R. Nagarajan[1] **N. Papanikolaou**[1] G. Bowen[2] S. Gay[3]

[1]Department of Computer Science
University of Warwick

[2]Centre for Quantum Computation
University of Cambridge

[3]Department of Computing Science
University of Glasgow

3rd Int'l Workshop on Security Issues in Concurrency

Outline

Outline

1. Introduction
   - Quantum Information Processing
   - Motivation
   - Background
2. Quantum Key Distribution (QKD)
   - The BB84 Protocol
   - The Security of QKD
3. Model Checking
4. Analysis of BB84 Using PRISM
5. Discussion
   - Limitations
   - Current and Future Work
   - Summary and Conclusion

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 (2)

- 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 Information Processing (3)

- There are several known quantum techniques for usual cryptographic tasks, including **oblivious transfer**, **bit commitment** and **key distribution**.
- We will focus on **quantum key distribution (QKD)** here.
- Strong known security result:
  - **QKD is unconditionally secure against all attacks permitted by quantum mechanics (Mayers, 1996).**
  - Unconditionally secure quantum bit commitment is impossible (Mayers, 1997).

Motivation

- Practical systems for QKD are already available commercially (viz. `www.magiqtech.com`, `www.idquantique.com`).
- The unconditional security proof of QKD holds for an **ideal** implementation and relies on complex information–theoretic arguments.
- We are in favour of a more practical approach, which is at a closer level to implementation: **probabilistic model–checking**.
- We will demonstrate this approach with an elementary analysis of the BB84 protocol for QKD.

Background
Key Distribution

- 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”).
- Unconditionally secure key distribution in a classical (i.e. non–quantum) setting is impossible; classical key distribution is, at best, **computationally secure**.

Background

Quantum Bits

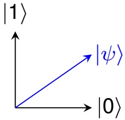
- The state of a 2–level quantum system, such as a polarised photon or a spin–$\frac{1}{2}$ particle, corresponds to a quantum bit or **qubit**.
- A qubit is a vector $|\psi\rangle$ in a 2–D complex vector space $\mathcal{H}_2$.
- The **unit length**, **orthogonal** vectors $|0\rangle$ and $|1\rangle$ form a **basis** of $\mathcal{H}_2$.
- The general state of a qubit is a linear combination

$$|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle, \qquad \alpha, \beta \in \mathbb{C}$$

Background

Measuring qubits (1)

- Measurements are made with respect to a given basis.
- If the qubit state $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$, is measured w.r.t $\boxplus = \{|0\rangle, |1\rangle\}$, then the state collapses into:
  - **either** $|0\rangle$, with probability $||\alpha||^2$,
  - **or** $|1\rangle$, with probability $||\beta||^2$.



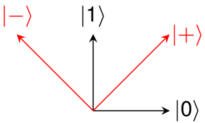
Quantum measurement is **probabilistic** and **destructive**.

Background

Measuring qubits (2)

- Consider the so–called **Hadamard basis**, which is a rotation of the computational basis by 90°. It is written $\boxtimes = \{|+\rangle, |-\rangle\}$ where:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



- Measuring a qubit in state $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ w.r.t. $\{|+\rangle, |-\rangle\}$ will collapse its state into:
  - **either** $|+\rangle$, with probability $||\frac{\alpha+\beta}{\sqrt{2}}||^2$,
  - **or** $|-\rangle$, with probability $||\frac{\alpha-\beta}{\sqrt{2}}||^2$.

Outline

Quantum Key Distribution (QKD)

- The security of QKD relies on the probabilistic and destructive nature of quantum measurement, as well as the **no–cloning theorem** for quantum states.
- Several protocols have been proposed for QKD:
  - **BB84 (Bennett and Brassard, 1984)**
  - B92 (Bennett, 1992)
  - E91 (Ekert, 1991)

BB84 With No Eavesdropping

- In $\boxplus$–basis, "0" is represented by $|0\rangle$ and "1" by $|1\rangle$.
- In $\boxtimes$–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.	$\boxplus$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxplus$
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.	$\boxtimes$	$\boxplus$	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxplus$	$\boxplus$
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**

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.	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$
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

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**).
- Two attacks of interest:
  - **Intercept–Resend** attack
  - **Random Substitute** attack

The Security Proof of BB84

- BB84 is unconditionally secure if, after the basic protocol is complete:
  - **Error correction** 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

Model Checking

- **Model checking** is a method of automated verification.
- It consists in **mechanically proving that a model**, σ, expressed in a suitable modelling language, **satisfies a temporal logic formula** ϕ. For given σ and ϕ, a **model checker** whether

$$\sigma \models \phi$$

- Classical **security protocols** are frequently verified using model checking.
  - **Gavin Lowe** used a model checker to detect a subtle security flaw in the Needham Schroeder public key protocol.

Probabilistic Model Checking

- A **probabilistic model checker** is designed to allow the verification of concurrent systems with probabilistic behaviour.
  - **PRISM (Kwiatkowska et al., 2001)**
  - ProbVerus (Clarke et al., 1999)
  - ProbUSM (Baier et al., 2005)
- For a given model σ and temporal formula ϕ, PRISM computes $\Pr(\sigma \models \phi)$.
- We have used PRISM to create a model of the basic BB84 protocol. With PRISM we have computed:
  - the probability P_{det} of detecting an eavesdropper when N qubits are transmitted; and
  - the probability $P_{>1/2}$ that the eavesdropper obtains more than half the originally transmitted bit values by measurement.

Outline

PRISM Models of BB84

- PRISM models can contain **parameters.** Models can be automatically verified for different values of these parameters.
- We have **two PRISM models of BB84**, one for each type of eavesdropping.
- Both models have a single parameter, the number N of qubits transmitted by Alice to Bob over the quantum channel.
- We have computed the probabilities P_{det} and $P_{>1/2}$ for N ranging from 5 to 30.

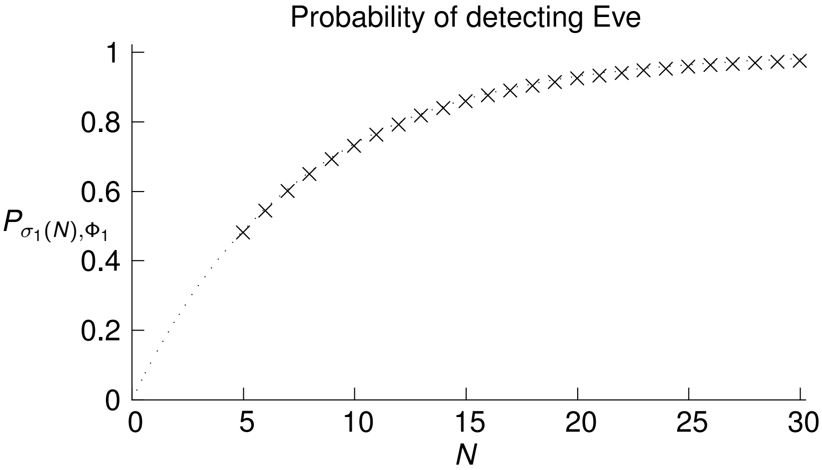
Legend for Graphs

The crosses indicate data points produced by PRISM, while the dotted curve is a nonlinear least squares fit* to these points.

* Levenberg–Marquardt fitting algorithm

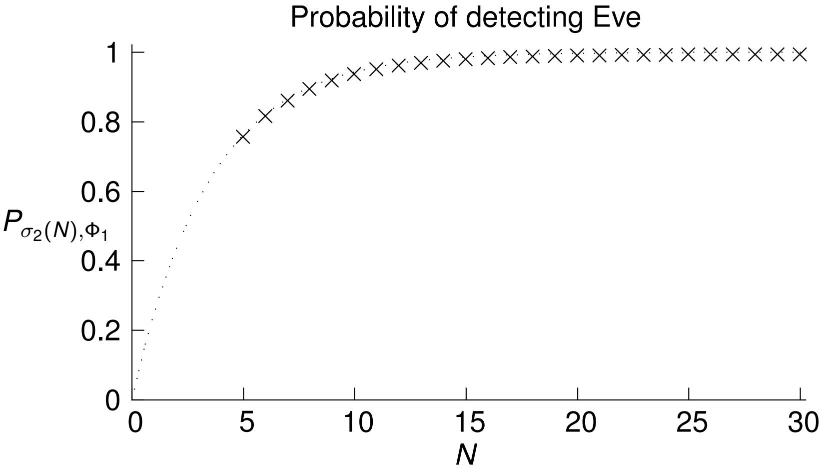
PRISM Models of BB84

Intercept–Resend Eavesdropping: P_{det}



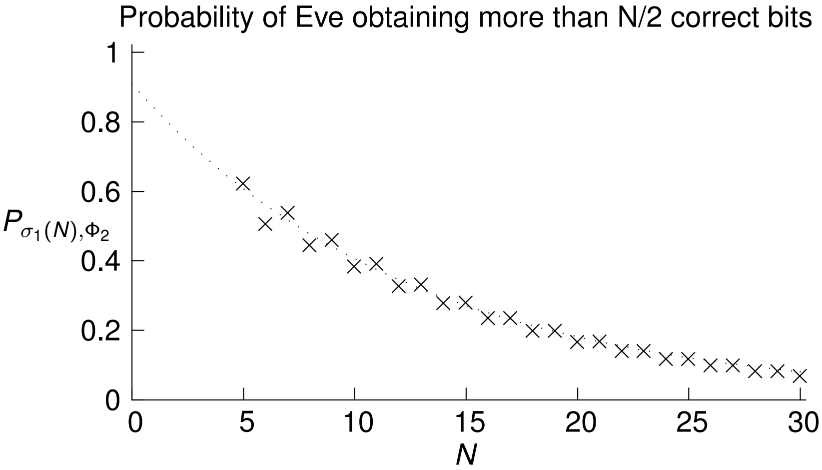
PRISM Models of BB84

Random Substitute Eavesdropping: P_{det}



PRISM Models of BB84

For both types of attack: $P_{>1/2}$



Summary of Results

- As the number of transmitted qubits in a trial of BB84 is increased, **the probability of detecting the eavesdropper asymptotically tends to 1.**
- As the number of transmitted qubits in a trial of BB84 is increased, **the chance that an eavesdropper obtains more than half the correct key values asymptotically tends to 0.**
- **The eavesdropper is detected much sooner** when a **random substitute** attack is performed.
- These results are in agreement with the theoretical predictions.

Outline

Limitations

- Only **finite** systems can be modelled in PRISM.
  - Protocols can only be verified for finite values of their security parameters.
- PRISM input language is too **low–level**.
  - Difficult to construct a useful **representation** of data, and difficult to model **protocol primitives**.
- PRISM struggles with large system models.
- PRISM is still under development.
- In general, quantum phenomena cannot be simulated efficiently on classical computers.
  - But **there exists a class of quantum operations** (those typically arising in quantum protocols) **which can be simulated efficiently**.

Current and Future Work

- Our programme is **to develop a general, high–level framework** for modelling and analysing quantum protocols using model checking.
- We are developing a **code generation tool**, PRISMGEN, which generates finite models for this purpose.
- We aim to combine our formal verification framework with a high–level specification language, in particular **CQP** (Gay and Nagarajan, 2005).

Summary and Conclusion

- We have presented the **BB84 protocol for QKD.**
- We have considered briefly the **security of QKD.**
- We have conducted a **proof–of–concept analysis** of the basic BB84 protocol using probabilistic model checking.
- We have discussed the **limitations** of the approach and **directions for future work.**
- There is much to be done!

For Further Reading

- PAPANIKOLAOU, N.
  Techniques for design and validation of quantum protocols.
  Master's thesis, Department of Computer Science, University of Warwick, 2005.

- GAY, S., NAGARAJAN, R., AND PAPANIKOLAOU, N.
  Probabilistic model–checking of quantum protocols.
  Quantum Physics Repository Preprint quant-ph/0504007, available at `www.arxiv.org`.

- GAY, S. AND NAGARAJAN, R.
  Communicating quantum processes.
  In *POPL '05: Proceedings of the 32nd ACM Symposium on Principles of Programming Languages, Long Beach, California*, January 2005.