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

Fifth International Workshop on Automated Verification of Critical Systems

Outline

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.

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**.

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.**
- Strong known security result:
  - **QKD is unconditionally secure against all attacks permitted by quantum mechanics (Mayers, 1996).**

Background

Quantum Bits

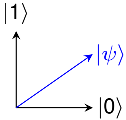
- The state of a 2–level quantum system, such as a polarised photon or a spin–$\frac{1}{2}$ particle, corresponds to a quantum bit or **qubit**.
- A qubit is a vector $|\psi\rangle$ in a 2–D complex vector space $\mathcal{H}_2$.
- The **unit length**, **orthogonal** vectors $|0\rangle$ and $|1\rangle$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

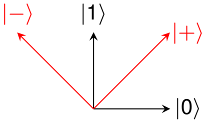


Quantum measurement is **probabilistic** and **destructive**.

Background
Measuring qubits (2)

- Consider the so–called **Hadamard basis**, which is a rotation of the computational basis by 45°. 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 $||\frac{\alpha-\beta}{\sqrt{2}}||^2$.

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.
  - 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)

The BB84 Protocol for QKD

1. **Alice** picks a **random bit** and a **random basis**. She encodes the bit as a qubit expressed w.r.t. the chosen basis and sends the qubit to Bob.
2. **Bob** picks a **random basis** with which to measure; he measures the qubit and stores the result.
3. **Alice** tells **Bob** which basis she used. All bits for which the wrong basis was used by Bob are discarded.

Incorrect basis:

If the incorrect basis is used for measurement, Bob obtains a random result.

Eavesdropping:

If an eavesdropper is present, there will arise cases in which both Alice and Bob used the same basis, but got a different result.

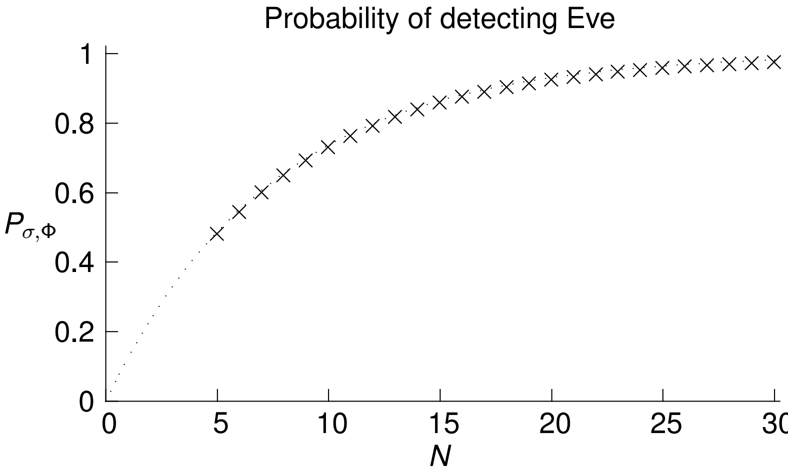
Probabilistic Model Checking

- 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 $\Pr(\sigma \models \phi)$.

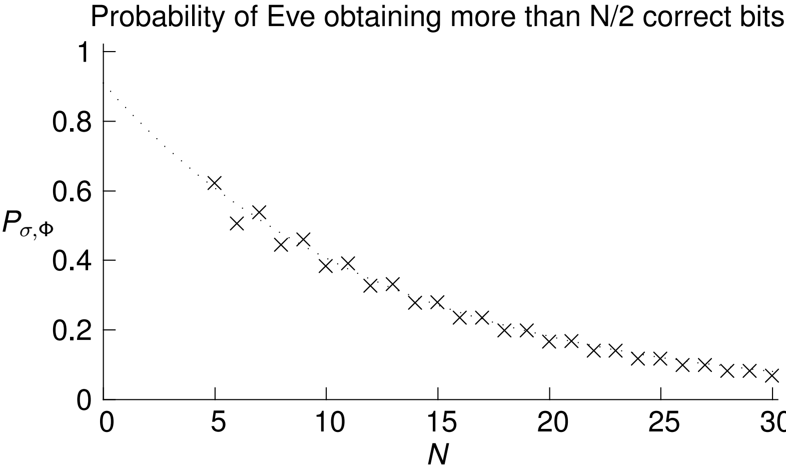
PRISM Models of BB84

- 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.
- The model has 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.

Intercept–Resend Eavesdropping: P_{det}



Intercept–Resend Eavesdropping: $P_{>1/2}$



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).

Review

- We have presented the **BB84 protocol for QKD**.
- We have conducted and discussed a **proof–of–concept analysis** of the basic BB84 protocol using probabilistic model checking.
- 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.