An Automated Analysis of the Security of Quantum Key Distribution

Rajagopal Nagarajan [1,3]

Department of Computer Science
University of Warwick
United Kingdom

Nikolaos Papanikolaou [1,4]

Department of Computer Science
University of Warwick
United Kingdom

Garry Bowen [2,5]

Centre for Quantum Computation
University of Cambridge
United Kingdom

Simon Gay [6]

Department of Computing Science
University of Glasgow
United Kingdom

Abstract

This paper discusses the use of computer–aided verification as a practical means for analysing quantum information systems; specifically, the BB84 protocol for quantum key distribution is examined using this method. This protocol has been shown to be unconditionally secure against all attacks in an information–theoretic setting, but the relevant security proof requires a thorough understanding of the formalism of quantum mechanics and is not easily adaptable to practical scenarios. Our approach is based on *probabilistic model–checking;* we have used the PRISM model–checker to show that, as the number of qubits transmitted in BB84 is increased, the amount of valid information held by an eavesdropper about the transmitted key decreases exponentially. We have also shown that the probability of detecting the presence of an eavesdropper increases exponentially with the number of qubits. We do not purport to provide a complete security proof of any kind; our model is a simple one, and it does not take into account the phases of secret–key reconciliation

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: `www.elsevier.nl/locate/entcs`

and privacy amplification. The results presented here demonstrate the use of the model–checking approach in the context of quantum systems.

Key words: quantum cryptography, quantum information, security proof, probabilistic model checking, PRISM

1 Introduction

That quantum–mechanical phenomena can be effectively exploited for the storage, manipulation and exchange of information is now a widely recognised fact. The whole field of quantum information poses new challenges for the information theory community and involves several novel applications, especially with respect to cryptology.

Recent interest in quantum cryptography has been stimulated by the observation that quantum algorithms, such as Shor's algorithms for integer factorization and discrete logarithm [21], threaten the security of classical cryptosystems. A wide range of quantum cryptographic protocols for key distribution, bit commitment, oblivious transfer and other problems [3] has been introduced in the last decade or so. Furthermore, the implementation of quantum cryptographic protocols has turned out to be significantly easier than the implementation of quantum algorithms: although practical quantum computers are still some way in the future, quantum cryptography has already been demonstrated in non-laboratory settings [19] and is well on the way to becoming an important practical technology.

Quantum cryptographic protocols are designed with the intention that their security is guaranteed by the laws of quantum physics. Naturally it is necessary to prove, for any given protocol, that this is indeed the case. The most notable result in this area is Mayers' proof [13] of the unconditional security of the quantum key distribution protocol "BB84" [2]. This proof guarantees the security of BB84 in the presence of an attacker who can perform any operation allowed by quantum physics; hence the security of the protocol will not be compromised by future developments in quantum computing.

Mayers' result, and others of the same kind [11,4,12], are extremely important contributions to the study of quantum cryptography. However, a mathematical proof of security of a *protocol* does not in itself guarantee the security of an implemented *system* which relies on the protocol. Experience of classical cryptography has shown that, during the progression from an idealised protocol to an implementation, many security weaknesses can arise. For example: the system might not correctly implement the desired protocol; there might be security flaws which only appear at the implementation level and which are not visible at the level of abstraction used in proofs; problems can also arise at boundaries between systems

[1] The work of R. Nagarajan and N. Papanikolaou is partially supported by EPSRC grant GR/S34090 and the EU Sixth Framework Programme (Project SecoQC: *Development of a Global Network for Secure Communication based on Quantum Cryptography*).
[2] The work of G. Bowen is partially supported by EPSRC grant GR/S92816.
[3] Email: biju@dcs.warwick.ac.uk
[4] Email: nikos@dcs.warwick.ac.uk
[5] Email: gab30@cam.ac.uk
[6] Email: simon@dcs.gla.ac.uk

and between components which have different execution models or data representations. We therefore argue that it is worth analysing quantum cryptographic systems at a level of detail which is closer to a practical implementation.

Computer scientists have developed a range of techniques and tools for the analysis and verification of communication systems and protocols. Those particularly relevant to security analysis are surveyed by Ryan *et al.* in [20]. This approach has two key features. The first is the use of formal languages to precisely specify the behaviour of the system and the properties which it is meant to satisfy. The second is the use of automated software tools to either verify that a system satisfies a specification or to discover flaws. These features provide a high degree of confidence in the validity of systems, and the ability to analyse variations and modifications of a system very easily.

In this paper we present the results of applying the above methodology to the basic BB84 quantum key distribution protocol. We have carried out an analysis using PRISM [7], a probabilistic model-checking system. Our results confirm some of the properties which arise from Mayers' security proof; more significantly, they demonstrate the effectiveness of the model-checking approach and the ease with which parameters of the system can be varied. It should be emphasized at the outset that our analysis does not take into account important aspects of the full BB84 protocol such as secret–key reconciliation and privacy amplification. Our objective here is only to demonstrate how the model–checking approach can be applied in the quantum setting. Also, we are restricting the analysis to a specific type of attack (intercept–resend), assuming noiseless quantum channels. The attacker in our model *does* obtain partial information about the final key produced by the protocol, with a certain probability; we show that this information is negligible, in particular, it decreases exponentially with the number of qubits transmitted (N). We also show that the probability that the eavesdropper's presence is detected (and the protocol aborted) increases exponentially with N.

Acknowledgements.

We would like to thank the organisers of SecCo'05, Michael Backes and Andre Scedrov, for giving us the opportunity to present this work. We are very grateful to the anonymous reviewers whose comments have been invaluable and have led to numerous improvements to the content and accuracy of this paper.

2 Quantum Key Distribution and Security Criteria

The objective of *key distribution* is to enable two communicating parties, Alice and Bob, to agree on a common secret key $\boldsymbol{k} \in \{0,1\}^N$, $N > 0$, without sharing any information initially. Once a common secret key has been established, Alice and Bob can use a symmetric cryptosystem to exchange messages privately. In a classical (i.e. non–quantum) setting, it is quite impossible to perform key distribution securely unless assumptions are made about the enemy's computational power [8].

[7] See http://www.cs.bham.ac.uk/~dxp/prism.

The use of quantum channels, which cannot be tapped or monitored without causing a noticeable disturbance, makes unconditionally secure key distribution possible. The presence of an enemy is made manifest to the users of such channels through an unusually high error rate. We will now describe the BB84 scheme for quantum key distribution [2], which uses polarised photons as information carriers. Note that the basic concepts and notation associated with quantum information are presented briefly in Appendix A.

BB84 assumes that the two legitimate users are linked by two specific channels, which the enemy also has access to:

(i) a classical, possibly public channel, which may be passively monitored but not tampered with by the enemy;

(ii) a quantum channel which may be tampered with by an enemy. By its very nature, this channel prevents passive monitoring.

The first phase of BB84 involves transmissions over the quantum channel, while the second phase takes place over the classical channel.

Notation 1 *The pair of quantum states* $\{|0\rangle, |1\rangle\}$ *is the* rectilinear basis *of the Hilbert space* $\mathscr{H}_2$*, and is denoted by* $\boxplus$*.*

Notation 2 *The pair of quantum states* $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ *is the* diagonal basis *of the Hilbert space* $\mathscr{H}_2$*, and is denoted by* $\boxtimes$*.*

Definition 2.1 The encoding function $f_{\mathrm{BB84}} : D \times B \mapsto \mathscr{H}_2$ where $D = \{0, 1\}$, $B = \{\boxplus, \boxtimes\}$ is defined as follows:

$$f_{\mathrm{BB84}}(0, \boxplus) = |0\rangle \tag{1}$$
$$f_{\mathrm{BB84}}(1, \boxplus) = |1\rangle \tag{2}$$
$$f_{\mathrm{BB84}}(0, \boxtimes) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{3}$$
$$f_{\mathrm{BB84}}(1, \boxtimes) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4}$$

The basic BB84 protocol can be summarised as follows:

(i) First Phase (Quantum Transmissions)
  (a) Alice generates a random string of bits $\boldsymbol{d} \in \{0, 1\}^n$, and a random string of bases $\boldsymbol{b} \in \{\boxplus, \boxtimes\}^n$, where $n > N$.
  (b) Alice places a photon in quantum state $|\psi_i\rangle = f_{\mathrm{BB84}}(d_i, b_i)$ for each bit d_i in $\boldsymbol{d}$ and b_i in $\boldsymbol{b}$, and sends it to Bob over the quantum channel.
  (c) Bob measures each $|\psi_i\rangle$ received, with respect to either $\boxplus$ or $\boxtimes$, chosen at random. Bob's measurements produce a string $\overrightarrow{d'} \in \{0, 1\}^n$, while his choices of bases form $\overrightarrow{b'} \in \{\boxplus, \boxtimes\}^n$.

(ii) Second Phase (Public Discussion)
  (a) For each bit d_i in $\boldsymbol{d}$:
    Alice sends the value of b_i to Bob over the classical channel.
    Bob responds by stating whether he used the same basis for measurement. If

$b'_i \neq b_i$, both d_i and d'_i are discarded.

(b) Alice chooses a subset of the remaining bits in $\boldsymbol{d}$ and discloses their values to Bob over the classical channel. If the result of Bob's measurements for any of these bits do not match the values disclosed, eavesdropping is detected and communication is aborted.

(c) The common secret key, $\overrightarrow{k} \in \{0,1\}^N$, is the string of bits remaining in $\boldsymbol{d}$ once the bits disclosed in step *2(b)* are removed.

There are two points to note in order to understand BB84 properly. Firstly, measuring with the incorrect basis yields a random result, as predicted by quantum theory. Thus, if Bob chooses the $\boxtimes$ basis to measure a photon in state $|1\rangle$, the classical outcome will be either 0 or 1 with equal probability; if the $\boxplus$ basis was chosen instead, the classical outcome would be 1 with certainty. Secondly, in step *2b)* of the protocol, Alice and Bob perform a test for eavesdropping. The idea is that, wherever Alice and Bob's bases are identical (i.e. $b'_i = b_i$), the corresponding bits should match (i.e. $d'_i = d_i$). If not, an external disturbance has occurred, and on a noiseless channel this can only be attributed to the presence of an eavesdropper. For more details, the reader is referred to [8,15].

We turn now to the formal security requirements for BB84. Among other things, a protocol such as BB84 must ensure that an enemy's presence is always made manifest to the legitimate users and that, if a key does result from the procedure, it is unpredictable and common to both users. But most importantly, the protocol must ensure *privacy:* an enemy must not be able to learn the *full* content of the key. Moreover, even if an enemy *is* able to obtain a certain quantity of information $\boldsymbol{v}$ by trying to monitor the classical channel, that quantity has to be minimal; meanwhile, the enemy's uncertainty about the key, $\mathrm{H}(\boldsymbol{k}|\boldsymbol{v})$, must be maximized.

Note that the enemy may obtain certain bits of the final key successfully in this simplified version of the protocol, and go undetected. For our purposes, partial information gained by the enemy about the key is considered to be of no use. We have limited our model to the case where a small number of bits are transmitted by Alice to Bob; increasing the key length (and hence the number of bits transmitted) increases the probability of detecting the enemy, as we will show later. If the enemy is indeed detected, the protocol is aborted and the key is completely discarded. Therefore, the version of the protocol we have described does not always succeed in producing a final key.

Definition 2.2 The conditional entropy of the key $\boldsymbol{k}$ (of length N) given the "view" $\boldsymbol{v}$ is defined as:

$$\mathrm{H}_N(\boldsymbol{k}|\boldsymbol{v}) = -\frac{1}{\Pr\{N\}} \sum_k \sum_v \Pr\{k, v\} \log\left(\Pr\{k|v\}\right)$$

Formal security requirements are usually expressed in terms of *security parameters*. For quantum key distribution, the security parameters are written n and $\boldsymbol{\epsilon}$. The parameter n is the number of quantum states transmitted, while $\boldsymbol{\epsilon}$ denotes collectively the tolerated error rate, the number of bits used to test for eavesdropping, and related quantities [13]. We use the parameter n instead of the key length N, as these are assumed to be linearly related. For instance, the value of $\mathrm{H}(\boldsymbol{k}|\boldsymbol{v})$ is some function of n and $\boldsymbol{\epsilon}$: $\mathrm{H}(\boldsymbol{k}|\boldsymbol{v}) = \varphi(n, \boldsymbol{\epsilon})$. The proof

[13] stipulates that $\mathrm{H}(\boldsymbol{k}|\boldsymbol{v})$ should be exponentially small in n and $\boldsymbol{\epsilon}$. Formally,

$$\varphi(n, \boldsymbol{\epsilon}) \leqslant c \cdot \mathrm{e}^{-gn} \tag{5}$$

$$\lim_{n\to\infty} \varphi(n, \boldsymbol{\epsilon}) = 0 \tag{6}$$

noting that the choice of n over N as the parameter only changes the value of the constant g, and not the functional relationship. We will demonstrate later for BB84 that, the probability that an enemy succeeds in obtaining more than $\frac{n}{2}$ key bits correctly is a function of the form (5).

Mayers' security proof of BB84 formalises the notion of privacy by defining a quantum key distribution protocol as "f–private," if, for every strategy adopted by an enemy, the average of the quantity $N - H(\boldsymbol{k}|\boldsymbol{v})$ is less than or equal to some constant f. This definition of privacy merely requires the key to be uniformly distributed, when the key length N is known. A more conventional privacy definition would have required that the mutual information $\mathrm{I}(\boldsymbol{k}, \boldsymbol{v})$ be less than or equal to κ, but this is not entirely satisfactory [13].

The notion of privacy adopted by Mayers is stronger than ours, since for our purposes we consider the protocol to be secure *even* if some (exponentially small) valid information about the final key is leaked to the enemy. This is far from what is required for a *fully general* security proof (whose feasibility clearly depends on which notion of "privacy" or "security" is adopted), and the version of BB84 we are modelling here is a simplified one. Indeed, the version we are considering here fails to produce a secret key when an enemy is detected. If secret–key reconciliation and privacy amplification procedures are added to the protocol being considered here, then the protocol will be capable of producing a secret key even in the presence of a detected enemy.

3 Model Checking Techniques and the PRISM Tool

The theoretical proof of BB84's security is a significant and valuable result. However, to prove a similar result for a different scheme or cryptographic task is far from trivial and is likely to involve new, ever more specialised derivations. A more flexible approach for analyzing the security of quantum cryptographic protocols is clearly desirable. Manufacturers of commercial quantum cryptographic systems [14], for instance, require efficient and rigorous methods for design and testing. A suitable approach should allow for modelling implementation–level details and even minor protocol variations with relative ease. We believe that *model–checking* is such an approach, and we will demonstrate its application to BB84.

PRISM (an acronym for *probabilistic symbolic model checker*) is a tool designed for modelling and validating systems which exhibit probabilistic behaviour. Whereas a logical model–checker, such as SPIN [9], only states whether a system model σ satisfies a temporal formula Φ, a tool such as PRISM computes the probability with which such a formula is satisfied, i.e. the value of $\mathrm{P}_{\sigma,\Phi} = \Pr\{\sigma \models \Phi\}$ for given σ and Φ. The models catered for by PRISM may incorporate specific probabilities for various behaviors and so may the formulas used for verification. Probabilistic models and PRISM–like tools find applications in numerous areas of computer science where random behaviour is involved. Oft–cited

applications are randomized algorithms, real–time systems and Monte Carlo simulation. The application of probabilistic model–checking to quantum systems is entirely appropriate, since quantum phenomena are inherently described by random processes; to reason about such phenomena one must account for this.

PRISM allows models to be parameterised: $\sigma = \sigma(u_1, \ldots, u_k)$. Thus the probability $\Pr\{\sigma \models \Phi\}$ may be computed for different values of $u_1, \ldots, u_k$; this is termed an *experiment*. By varying one parameter at a time, it is possible to produce a meaningful plot of this quantity's variation.

PRISM uses a built–in specification language based on Alur and Henzinger's *Reactive Modules* formalism (see [10,18]). Using this language the user can describe probabilistic behaviour. Internally, a PRISM model is represented by a *probabilistic transition system.* In such a system, each step in a computation is represented by a *move,* or *transition,* from a particular state s to a distribution π of successor states [18].

The probabilistic temporal logic PCTL [5] is used as the principal means for defining properties of systems modelled in PRISM. It suffices for our purposes to remind the reader of the meaning of the operator $\mathscr{U}$, known as "unbounded until". The formula $\Phi_1 \mathscr{U} \Phi_2$ expresses the fact that Φ_1 holds continuously from the current state onward, *until eventually* Φ_2 becomes **true**. The PRISM property $\mathrm{P} \geqslant 1[\Phi_1 \mathscr{U} \Phi_2]$ states that the formula $\Phi_1 \mathscr{U} \Phi_2$ is true with certainty, i.e. with a probability of unity; we use PRISM to check whether such a property holds in a given model.

4 Analysis of BB84 using PRISM

We have built a model of BB84 for use with PRISM. It is not possible to present the source code for this model here, due to space limitations; however, the full source code is available online [8], and is discussed extensively in [17].

A system description for PRISM contains definitions of *modules,* each module representing a component of the system. In our description of BB84, there is a module for each party involved in the protocol, and a module representing the quantum channel. Each module has a set of local variables and a sequence of actions to perform; an action typically takes one of the following two forms:

$$[s] \quad g \quad \rightarrow \quad (v_1 := \mathrm{val}_1); \tag{7}$$

$$[s] \quad g \quad \rightarrow 0.5 : (v_1 := \mathrm{val}_1) + 0.5 : (v_1 := \mathrm{val}_2); \tag{8}$$

In (7), the variable v_1 is assigned the value val_1; in (8), v_1 is assigned either the value val_1 or val_2 with equal probability. Part of the expressive power of PRISM comes from the ability to specify arbitrary probabilities for actions; for example, one could model a bias in Alice's choice of polarisation basis, in BB84, with an action such as:

[8] See http://go.warwick.ac.uk/nikos/research/publications/index.html .

$$[choosebasis]\ \mathbf{true} \rightarrow 0.7 : (al\_basis := \boxplus) \\ +0.3 : (al\_basis := \boxtimes); \tag{9}$$

In this example, Alice is biased towards choosing the rectilinear basis. Knowledge of this syntax is sufficient for an understanding of the PRISM description of BB84. In what follows, we will discuss the properties which we have been able to investigate.

As discussed in Section 2, there are two security requirements of interest for BB84:

(i) *an enemy's presence must not go unnoticed;* if the legitimate users know that an enemy is trying to eavesdrop, they can agree to use privacy amplification techniques [20] and/or temporarily abort the key establishment process.

(ii) *any quantity of valid information which the enemy is able to obtain through eavesdropping must be minimal.*

We can use our model of BB84, denoted henceforth by σ_{BB84}, to compute the probability

$$\Pr\{\sigma_{\mathrm{BB84}} \models \Phi_i\} \tag{10}$$

where Φ_i is a given PCTL property–formula. Therefore, in order to verify that BB84 satisfies the security requirements just mentioned, we have to reformulate these requirements in terms of probability.

Firstly, we should be able to compute exactly what the probability of detecting an enemy is. In our PRISM model, we can vary n, the number of photons transmitted in a trial of BB84, and so this probability is a function of n. Let us write the probability of detecting an enemy as

$$P_{\mathrm{det}}(n) = \Pr\{\sigma_{\mathrm{BB84}} \models \Phi_{\mathrm{det}}\} \tag{11}$$

In (11), Φ_{det} represents the PCTL formula whose boolean value is `true` when an enemy is detected. Before we give the definition of Φ_{det}, we should state the random event $\mathscr{E}$ that occurs when an enemy is detected; this will allow us to write $P_{\mathrm{det}}(n)$ as a classical probability $\Pr(\mathscr{E})$.

In BB84, an enemy, Eve, is detected as a result of the disturbance inevitably caused by some of her measurements. Just as Bob, Eve does not know which polarisation bases were used to encode the bits in Alice's original bit string. Eve has to make a random choice of basis, denoted b_i'', which may or may not match Alice's original choice, b_i. If $b_i'' = b_i$, Eve is guaranteed to measure the i-th photon correctly; otherwise, quantum theory predicts that her measurement result will only be correct with probability 0.5.

In a so–called *intercept–resend attack,* Eve receives each photon on the quantum channel, measures it with her basis b_i'', obtaining bit value d_i'', and then transmits to Bob a new photon, which represents d_i'' in the b_i'' basis. If Eve's basis choice is incorrect, her presence is bound to be detected. But for detection to occur, Bob must choose the correct basis for his measurement. Whenever Bob obtains an incorrect bit value despite having used the correct basis, this is because an enemy has caused a disturbance. Note that we are assuming a

perfect quantum channel here; an imperfect channel would produce noise, causing additional disturbances.

Remember that there is always the possibility that Eve's measurement produces the correct bit value $d_i'' = d_i$. This may arise even if her choice of measurement basis b_i'' is incompatible with Alice's. If Eve's choice of measurement basis matches that of Alice for a particular bit, and for this bit Bob also uses the same basis (i.e. if $b_i = b_i'' = b_i'$), then Eve's presence will *not* be detected from that measurement. In other words, there is clearly a given probability p with which Eve may obtain the entire key being established by Alice and Bob; it is necessary to show that p is negligible.

So, to summarise, an enemy's presence is made manifest as soon as the following event occurs:

$$(b_i'' \neq b_i) \wedge (b_i' = b_i) \text{ for some } i \leqslant n$$

or equivalently, as soon as:

$$\mathscr{E} \equiv (b_i' = b_i) \wedge (d_i' \neq d_i) \text{ for some } i \leqslant n \tag{12}$$

Therefore, the probability of detecting an enemy's presence in BB84 may be written:

$$\begin{aligned} P_{\text{det}}(n) &= \Pr\{\mathscr{E}\} \\ &= \Pr\{(b_i' = b_i) \wedge (d_i' \neq d_i) \text{ for some } i \leqslant n\} \end{aligned}$$

The corresponding PCTL formula for PRISM is:

$$\Phi_{\text{det}} \equiv \{\texttt{true}\ \mathcal{U}\ (b_i' = b_i) \wedge (d_i' \neq d_i)\}$$

The PRISM model of BB84 uses elaborate variable names, e.g. `bob_basis` instead of b_i', and `alice_bit` instead of d_i.

The value of $P_{\text{det}}(n)$ for $5 \leqslant n \leqslant 30$ has been calculated with PRISM, which computes (11); the result is shown in Figure 1.

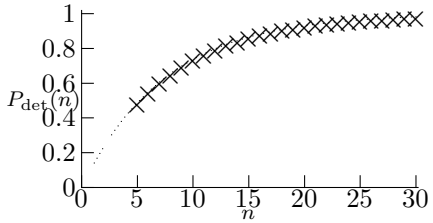

Fig. 1. The probability that Eve is detected in the BB84 Protocol while performing an intercept–resend attack, as a function of the security parameter n. The crosses indicate data points produced by PRISM, while the dotted curve is a non–linear least–squares fit to these points.

The first requirement for BB84, namely that it should be possible to detect an enemy's presence, clearly is satisfied. As we can see from Figure 1, as the number of photons transmitted is increased, the probability of detection tends toward 1, i.e. we conclude that

$$\lim_{n\to\infty} P_{\text{det}}(n) = 1$$

We will now consider the second security requirement. Let $\mathscr{C}_i$ denote the event in which Eve measures the i-th photon transmitted correctly. The probability that Eve measures all photons correctly, and hence is able to obtain the secret key, is the product

$$P_{\text{all}} = \prod_{0<i\leqslant n} \Pr\{\mathscr{C}_i\} = \Pr\{\mathscr{C}_1\} \Pr\{\mathscr{C}_2\} \times \cdots \times \Pr\{\mathscr{C}_n\}$$

We will examine the variation of a quantity proportional to P_{all}, namely the probability $P_{>1/2}(n)$ that Eve measures *more than half* the photons transmitted correctly.

According to the second security requirement for BB84, the amount of valid information obtained by an enemy must be minimised; we will investigate the variation of the probability

$$P_{>1/2}(n) = \Pr\{\sigma_{\text{BB84}} \models \Phi_{>1/2}\}$$

as a function of the number of photons transmitted. We expect this quantity to grow smaller and smaller with n.

The PRISM model of BB84 includes a counter variable, `nc`, whose value is the number of times that Eve makes a correct measurement. The formula $\Phi_{>1/2}$ may be written in terms of this variable:

$$\Phi_{>1/2} = \left\{ \texttt{true}\ \mathcal{U}\ \left(\texttt{nc} > \frac{n}{2}\right) \right\}$$

Given σ_{BB84} and $\Phi_{>1/2}$, PRISM produces the plot shown in Figure 2; it can be seen from the figure that $P_{>1/2}(n)$ decays exponentially with n.

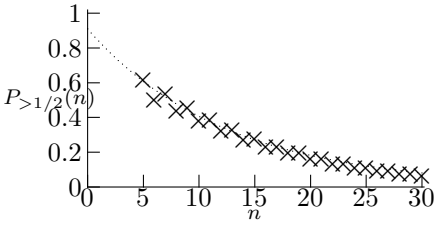

Fig. 2. The probability that Eve, by performing an intercept–resend attack, makes more than $\frac{n}{2}$ correct measurements in BB84, versus the security parameter n.

Figures 1 and 2 each contain two superimposed plots: the data points marked with crosses are actual values produced by PRISM, and the dotted curves are nonlinear functions to which the data points have been fitted. We have used the Levenberg–Marquardt nonlinear fitting algorithm to compute values c_1, c_2, c_3 and c_4 such that:

$$P_{\text{det}}(n) \approx 1 - c_1 \exp[-c_2 n]$$
$$P_{>1/2}(n) \approx c_3 \exp[-c_4 n]$$

In particular, the values obtained are (to three decimal places): $c_1 = 1$, $c_2 = 0.134$, $c_3 = 0.909$, and $c_4 = 0.081$. It is evident that, increasing the number of photons transmitted, or equivalently, the length of the bit sequence generated by Alice, increases BB84's capability

to avert an enemy: the probability of detecting the enemy increases exponentially, while the amount of valid information the enemy has about the key decreases exponentially.

These results are in agreement with Mayers' claim (see [13]), that "in an information–theoretic setting, which is our case, a quantity f_N such as the amount of Shannon's information available to Eve must decrease exponentially fast as N increases." Remember, we have assumed that the number of transmissions, n, is linearly related to N.

Variations in the protocol can be accommodated easily by modifying the PRISM model. For example, in [1] a bias in Alice's choice of basis is introduced, and this can be described by a PRISM action such as (9). This influences the performance of BB84; it alters the variation of both $P_{\text{det}}(n)$ and $P_{>1/2}(n)$.

It should be noted that the results presented here are not as general as Mayers'. For instance, we have assumed that a noiseless channel is being used, and we have only considered a finite number of cases (namely, where $5 \leqslant n \leqslant 30$). Related techniques which are better suited for a full proof of unconditional security include automated theorem proving [6]; we will leave this for future work. This technique is not restricted to finite scenarios, and therefore can provide the generality needed for a more extensive analysis.

5 Conclusions

In this paper we have analysed the security of the BB84 protocol for quantum key distribution by applying formal verification techniques. In particular, a probabilistic model–checking tool, PRISM, was used to obtain results which corroborate Mayers' unconditional security proof of the protocol. The model checking approach allows us to analyse composite systems, which include both classical and quantum–mechanical components. We are not only able to model abstract protocols — as presented here — but concrete implementations as well. We hope to be able to extend our techniques to accommodate other quantum protocols and also more powerful models of attacker. This is likely to require going beyond the functionality provided by the PRISM tool, but we believe that the use of this tool is an important first step.

References

[1] Ardehali, M., G. Brassard, H. F. Chau and H. K. Lo, *Efficient quantum key distribution*, Quantum Physics Archive: arXiv: quant-ph/9803007 (1998).

[2] Bennett, C. H. and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in: *Proceedings of International Conference on Computers, Systems and Signal Processing*, 1984.

[3] Brassard, G. and C. Crépeau, *Quantum bit commitment and coin tossing protocols*, in: A. Menezes and S. Vanstone, editors, *Advances in Cryptology — CRYPTO '90* (1991), pp. 49—61, volume 537 of *Lecture Notes in Computer Science*.

[4] Christandl, M., R. Renner and A. Ekert, *A generic security proof for quantum key distribution*, Quantum Physics Archive: arXiv:quant-ph/0402131 (2004).

[5] Ciesinski, F. and M. Größer, *On Probabilistic Computation Tree Logic* (2004), to appear.

[6] Clarke, E. M., O. Grumberg and D. A. Peled, "Model Checking," MIT Press, 2000.

[7] Gay, S. and R. Nagarajan, *Communicating quantum processes*, in: *POPL '05: Proceedings of the 32nd ACM Symposium on Principles of Programming Languages, Long Beach, California*, 2005.

[8] Gruska, J., "Quantum Computing," McGraw–Hill International, 1999.

[9] Holzmann, G., "The SPIN Model Checker: Primer and Reference Manual," Pearson Education, 2003.

[10] Kwiatkowska, M., G. Norman and D. Parker, *Modelling and verification of probabilistic systems*, in: P. Panangaden and F. V. Breugel, editors, *Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems*, American Mathematical Society, 2004 Volume 23 of CRM Monograph Series.

[11] Lo, H.-K. and H. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances*, Science **283** (1999), p. 2050.

[12] Mayers, D., *Unconditionally secure quantum bit commitment is impossible*, in: *Fourth Workshop on Physics and Computation — PhysComp '96* (1996).

[13] Mayers, D., *Unconditional security in quantum cryptography*, Journal of the ACM **48** (2001), pp. 351—406.

[14] Muller, A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin, *'Plug and Play' systems for quantum cryptography*, App. Phys. Lett. **70** (1997), see also http://www.idquantique.com.

[15] Nielsen, M. A. and I. L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, 2000.

[16] Papanikolaou, N., *Introduction to quantum cryptography*, ACM Crossroads Magazine **11.3** (2005), pp. 10—16.

[17] Papanikolaou, N., "Techniques for Design and Validation of Quantum Protocols," Master's thesis, Department of Computer Science, University of Warwick (2005), also available as Research Report CS-RR-413.

[18] Parker, D., G. Norman and M. Kwiatkowska, *PRISM 2.0 users' guide* (2004).

[19] Poppe, A., A. Fedrizzi, T. Loruenser, O. Maurhardt, R. Ursin, H. Boehm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein and A. Zeilinger, *Practical quantum key distribution with polarization entangled photons*, Quantum Physics Archive: arXiv:quant-ph/0404115 (2004).

[20] Ryan, P., S. Schneider, M. Goldsmith, G. Lowe and B. Roscoe, "Modelling and Analysis of Security Protocols," Addison-Wesley, 2001.

[21] Shor, P., *Algorithms for quantum computation: discrete logarithms and factoring*, in: *Proceedings of 35th Annual Symposium on Foundations of Computer Science* (1994).

A Basic Concepts of Quantum Information

Here, we briefly describe those aspects of quantum theory relevant to quantum protocols.

A *quantum bit* or *qubit* is a physical system which has two basis states, conventionally written $|0\rangle$ and $|1\rangle$, corresponding to one-bit classical values. These could be, for example, spin states of a particle or polarization states of a photon, but we do not consider physical details. According to quantum theory, a general state of a quantum system is a *superposition* or linear combination of basis states. A qubit has state $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$; states which differ only by a (complex) scalar factor with modulus 1 are indistinguishable. States can be represented by column vectors: $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right] = \alpha|0\rangle + \beta|1\rangle$. Formally, a quantum state is a unit vector in a Hilbert space, i.e. a complex vector space equipped with an inner product satisfying certain axioms. In this paper we restrict attention to collections of qubits.

The basis $\{|0\rangle, |1\rangle\}$ is known as the *standard* basis. Other bases are sometimes of interest, especially the *diagonal* (or *dual*, or *Hadamard*) basis consisting of the vectors

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

Evolution of a closed quantum system can be described by a *unitary transformation*. If the state of a qubit is represented by a column vector then a unitary transformation U can be represented by a complex-valued matrix (u_{ij}) such that $U^{-1} = U^*$, where U^* is the conjugate-transpose of U (i.e. element ij of U^* is $\bar{u}_{ji}$). U acts by matrix multiplication:

$$\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix} = \begin{bmatrix}u_{00} & u_{01}\\ u_{10} & u_{11}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

A unitary transformation can also be defined by its effect on basis states, which is extended linearly to the whole space. For example, the *Hadamard* operator is defined by

$$|0\rangle \mapsto |+\rangle = \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \mapsto |-\rangle = \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle$$

which corresponds to the matrix $\mathsf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$. The *Pauli* operators, denoted by $\sigma_0, \sigma_1, \sigma_2, \sigma_3$, are defined by

$$\sigma_0 = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \quad \sigma_1 = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \quad \sigma_2 = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \quad \sigma_3 = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

Measurement plays a key role in quantum physics. If a qubit is in state $\alpha|0\rangle + \beta|1\rangle$ then measuring its value gives the result 0 with probability $|\alpha|^2$ (leaving it in state $|0\rangle$) and the result 1 with probability $|\beta|^2$ (leaving it in state $|1\rangle$). For example, if a qubit is in state $|+\rangle$ then a measurement (with respect to the standard basis) gives result 0 (and state $|0\rangle$) with

probability $\frac{1}{2}$, and result 1 (and state $|1\rangle$) with probability $\frac{1}{2}$. If a qubit is in state $|0\rangle$ then a measurement gives result 0 (and state $|0\rangle$) with probability 1.

To go beyond single-qubit systems, we consider tensor products of spaces (in contrast to the cartesian products used in classical systems). If spaces U and V have bases $\{u_i\}$ and $\{v_j\}$ then $U \otimes V$ has basis $\{u_i \otimes v_j\}$. In particular, a system consisting of n qubits has a 2^n-dimensional space whose standard basis is $|00\ldots0\rangle \ldots |11\ldots1\rangle$. We can now consider measurements of single qubits or collective measurements of multiple qubits. For example, a 2-qubit system has basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ and a general state is $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Measuring the first qubit gives result 0 with probability $|\alpha|^2 + |\beta|^2$ (leaving the system in state $\frac{1}{\sqrt{|\alpha|^2+|\beta|^2}}(\alpha|00\rangle + \beta|01\rangle)$) and result 1 with probability $|\gamma|^2+|\delta|^2$ (leaving the system in state $\frac{1}{\sqrt{|\gamma|^2+|\delta|^2}}(\gamma|10\rangle+\delta|11\rangle)$); in each case we renormalize the state by multiplying by a suitable scalar factor. Measuring both qubits simultaneously gives result 0 with probability $|\alpha|^2$ (leaving the system in state $|00\rangle$), result 1 with probability $|\beta|^2$ (leaving the system in state $|01\rangle$) and so on; the association of basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ with results $0, 1, 2, 3$ is just a conventional choice. The power of quantum computing, in an algorithmic sense, results from calculating with superpositions of states; all of the states in the superposition are transformed simultaneously (*quantum parallelism*) and the effect increases exponentially with the dimension of the state space. The challenge in quantum algorithm design is to make measurements which enable this parallelism to be exploited; in general this is very difficult.

The *controlled not* (CNot) operator on pairs of qubits performs the mapping $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |11\rangle$, $|11\rangle \mapsto |10\rangle$, which can be understood as inverting the second qubit (the *target*) if and only if the first qubit (the *control*) is set. The action on general states is obtained by linearity.

Systems of two or more qubits may be in *entangled* states, meaning that the states of the qubits are correlated. For example, consider a measurement of the first qubit of the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The result is 0 (and the resulting state is $|00\rangle$) with probability $\frac{1}{2}$, or 1 (and the resulting state is $|11\rangle$) with probability $\frac{1}{2}$. In either case, a subsequent measurement of the second qubit gives a definite, non–probabilistic result which is identical to the result of the first measurement. This is true even if the entangled qubits are physically separated. Entanglement illustrates the key difference between the use of the tensor product (in quantum systems) and the cartesian product (in classical systems): an entangled state of two qubits is one which cannot be expressed as a tensor product of single-qubit states. The Hadamard and CNot operators can be combined to create entangled states: $\mathsf{CNot}((\mathsf{H} \otimes I)|00\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.