# Modelling of Quantum Key Distribution Protocols in Communicating Quantum Processes Language with Verification and Analysis in PRISM

Satya Kuppam
*University of Massachusetts, Amherst, U.S.A.*

Keywords: PRISM, Modelling, Analysis, Verification, Quantum Cryptography, Communicating Quantum Processes, π-calculus.

Abstract: Proof of security of cryptography protocols theoretically establishes the strength of a protocol and the constraints under which it can perform, it does not take into account the overall design of the protocol. In the past model checking has been successfully applied to classical cryptography protocols to weed out design flaws which would have otherwise gone unnoticed. Quantum key distribution protocols differ from their classical counterparts, in their ability to detect the presence of an eavesdropper while exchanging the key. Although unconditional security has been proven for both BB84(Mayers, 2002) and B92(Quan and Chaojing, 2002) key distribution protocols, in this paper we show that identifying an eavesdropper's presence is constrained on the number of qubits exchanged. We first model the protocols in Communicating Quantum Processes (CQP)(Gay and Nagarajan, 2005)(Davidson, 2012) and then explain the mechanism by which we have translated this into a PRISM model and how we analysed the protocols' capabilities. We mainly focus on the protocols' ability to detect an active eavesdropper and the extent to which an eavesdropper can retrieve the shared key without being detected by either party. We then conclude by comparing the performance of the protocols.

## 1 INTRODUCTION

Quantum cryptographic protocols have garnered much acclaim in the last two decades for their ability to provide unconditional security, which is not practically assured by their classical counterparts. Commercial availability of quantum infrastructure in the last decade has placed even more emphasis on developing methodologies to ascertain the reliability of protocols in practice. Even though, protocols are theoretically secure, our experience with classical protocols has shown that security can be compromised during implementation. Since modelling, analysing and verifying classical protocols have worked so well, developing techniques along these lines seems prudent for quantum cryptography protocols as well.

The cornerstone of quantum cryptography protocols is the inherent probabilistic nature. Unlike classical key distribution protocols (KD) which accommodates a passive eavesdropper, wherein the eavesdropper can copy the bits and analyse them later, quantum key-distribution protocols (QKD) mandate an active eavesdropper. This constraint is promulgated by the no-cloning(Bužek and Hillery, 1996) theorem which handicaps the eavesdropper from copying qubits. In trying to extract the bit value from the qubit the eavesdropper will make some 'measurements' which will 'corrupt' the qubits and make her presence known to parties trying to establish a key (section 2). Moreover, quantum protocols also involve both classical and quantum channels. Therefore we need a language that is capable of modelling probabilistic phenomenon and also takes into account both classical and quantum communications.

Communicating Quantum Processes (CQP)(Gay and Nagarajan, 2005) is a language developed with the expert purpose of modelling quantum protocols. CQP uses the communication primitives of pi-calculus(Milner, 1999) and has capabilities for applying unitary operators, performing measurements, and a static type system that differentiates between classical and quantum communications. Hence CQP seems an obvious choice for modelling quantum protocols. PRISM allows us to model probabilistic transitions, as we show later, this allows to seamlessly translate a CQP model into a PRISM model.

Previous work on analysis of BB84 by Papanikolaou (Gay et al., 2005) has reasoned about the probability of detecting an eavesdropper and corroborates the claim made by Mayers in his proof of uncondi-

Kuppam, S.
Modelling of Quantum Key Distribution Protocols in Communicating Quantum Processes Language with Verification and Analysis in PRISM.
DOI: 10.5220/0006834500750082
In *Proceedings of 8th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2018)*, pages 75-82
ISBN: 978-989-758-323-0

tional security of BB84. However, this work does not model BB84 in CQP. We first model BB84 in CQP, convert the CQP model into PRSIM and check the validity of the observations made by Papanikolaou(Gay et al., 2005). We then proceed to show that B92's eavesdropping detection capabilities can be reasoned along the same lines.

To ensure brevity we have refrained from explaining Quantum Mechanical primitives like unitary operators, measurements and no-cloning theorem. One good resource is Nielsen and Chuang's work(Nielsen and Chuang, 2010). Also, we have only provided an elementary introduction to CQP, only to the extent to which we use it in this paper. A better and comprehensive resource would be Thimothy Davidson's(Davidson, 2012) doctoral thesis.

# 2 PRELIMINARIES

The quantum counterparts of the classical bits are called 'qubits'. We can consider bits as being voltages with a high voltage representing a '1' bit and a low voltage representing a '0' bit or vice-versa. Qubits on the other hand represent some quantum mechanical property of a photon, atom or a subatomic particle. For example one can say that in a hydrogen atom if the electron is in the ground state then it encodes a '0' bit, but if it is in an excited state it encodes a '1' bit. It is not necessary that the electron has to reside in either of these two states, it can also reside in a superposition of the ground state and the excited state. One can perform a 'quantum measurement' to determine if the electron is present in the ground state or the excited state.

## 2.1 Quantum Measurement

It is inherent with any quantum mechanical system that any measurement done on the system will induce some irreversible disturbances. We are going to rely on this property of qubits heavily in any quantum cryptographic protocols. Any quantum system can be represented as a vector in an *n* dimensional complex Hilbert space. Measuring this quantum system can only give a set of priviliged results namely those associated with the basis vectors of the state space.
For example, consider a *2-dimensional* complex Hilbert space with $|0\rangle$ and $|1\rangle$ as basis vectors. Lets say the vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ describes the system where $\alpha, \beta \in \mathbb{C}$. If we try to measure the system in the basis $\{0,1\}$, then the system changes to a new state, either $|\psi'\rangle = |0\rangle$ or $|\psi'\rangle = |1\rangle$ permanently. It has a probability $|\alpha|^2$ of changing into $|\psi'\rangle = |0\rangle$ and a probability $|\beta|^2$ of changing into $|\psi'\rangle = |1\rangle$. Also, $|\alpha|^2 + |\beta|^2 = 1$. We can also measure the system in whichever basis that we choose. Lets measure the system in another basis $\{+,-\}$, where
$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, then the quantum state can be represented as $|\psi\rangle = \frac{(\alpha+\beta)}{\sqrt{2}}(|+\rangle) + \frac{(\alpha-\beta)}{\sqrt{2}}(|-\rangle)$.
Measuring this system in the basis $\{+,-\}$ will yield $|+\rangle$ and $|-\rangle$ with probability $\frac{(\alpha+\beta)^2}{2}$ and $\frac{(\alpha-\beta)^2}{2}$ respectively.

## 2.2 BB84 QKD Protocol

A and B want to establish a secret for secure communication. A sends the encoding of some bits in the $+,\times$basis to B on the quantum channel. The $+$basis is called the rectilinear basis and the $\times$basis is called the diagonal basis. B then chooses a random sequences of bases and measures the qubit sent by A in that basis. If the basis of Alice and Bob are equal then the B obtains the classical bit chosen by Alice other wise she randomly gets $\{0,1\}$. A and B then use the classical channel to exchange some of the basis from the random sequence and the corresponding measurements of qubits to decide upon a shared key or to detect the presence of an eavesdropper.

## 2.3 B92 QKD Protocol

Unlike BB84 where each classical bit has two different encoding depending on the basis used, B92 has only one. In other words there is a one to one correspondence between the classical bits and qubits exchanged. If Alice wants to send a classical bit 0 to Bob she sends $\rightarrow$and if she wants to send 1 she sends $\nearrow$. The rest of the steps involved are the same as in BB84.

## 2.4 Eavesdropping Attacker

As mentioned earlier, whenever Eve measures the qubits that are in transit to Bob from Alice, she makes a permanent change to the state of qubits if she doesn't use the same basis as that of Alice. In BB84 protocol if on some qubits both Alice and Bob use the same basis to encode and measure but Bob decodes a classical bit different from what Alice encoded, suggests the presence of Eve. In B92 as well, Alice and Bob should obtain the opposite results when the encoding basis is the same, then an attacker is present. We are assuming the qubit channel shared by all the participants noiseless. The eavesdropping attacker has two capabilities, first of those is *random-substitution* wherein the attacker's main aim is to disrupt the key exchange process by randomly dropping qubits and introducing new ones and the second is called *intercept-resend* wherein the attacker takes a qubit makes an observation and re-sends the qubit to the intended destination. In this type of attack the main motive is to gain information about the key being exchanged. We analyse how the protocols perform in both these settings.

# 3 FORMALISING IN CQP

A brief overview of CQP calculus is provided and then we proceed to formalise both the protocols in CQP. An example of BB84-Bit Commitment Protocol in CQP(Gay and Nagarajan, 2005) was given by Simon and Gay and our formalisation uses the same techniques.

A protocol at any given point of time has multiple participants, like *Alice* and *Bob* which are legitimate entities involved and also adversaries like Eve. These entities are collectively known as *agents*. Agents communicate with each other via communication channels to exchange information. The working of the agents is encapsulated by *processes*. Every agent has more than one process, and at any given time its possible that more than one process is in action. These processes can be reasonably thought of as *states* in finite state automata and every process transitions to another or terminates. CQP allows us to impose a probabilistic distribution across these transitions. Also processes in CQP can be parameterised.

1. channels are declared by the *new* keyword. For example to declare a new qubit channel, we write (*new qubitChannel*:^[*Qbit*]), where *Qbit* is the data type *qubitChannel* is constrained to and '^' identifies it as a channel.
2. variables can be declared within a process like so, (*qbit* q).
3. *Process Output:* $c![x].P_{i+1}$ to send the data stored by variable $x$ along channel $c$ and then proceed with process $P_{i+1}$.
4. *Process Input:* $c?[x].P_{i+1}$ to receive along channel $c$ and then proceed with process $P_{i+1}$.
5. *Process action:* $e.P_{i+1}$ evaluates expression $e$ and then proceeds with process $P_{i+1}$
6. *Process decision:* *if* $e$ *then*$P_{i+1}$*else*$P_{i+2}$ if the expression $e$ evaluates to *true* then proceed with process $P_{i+1}$ else $P_{i+2}$
7. *Terminate:* $P_i.0$ the process terminates after $P_i$.

## 3.1 Formalising BB84

We identify that *Alice*, *Bob* are the primary agents of the protocol and to analyse the effects of an eavesdropper, *Eve* becomes an agent of the system as well. As described above channels can only transport messages of a particular type. We have *qubitChannel* to transport qubits, *intChannel* for integers and *decisionChannel*, *decisionFlagChannel*, *randomBitChannel* for bits. Technically one bit channel would suffice.

However having two different channels that are used at two different stages in the protocol helps us to convert the CQP-model into PRISM as will be elaborated in the next section. We have also made use of *List* type, with its associated functions of *hd*, *tl*, *[]* and *@* for reading the first element, dropping the first element, an empty list and placing data at the tail of the list respectively. The use of these functions is demonstrated by Gay et al.(Gay and Nagarajan, 2005).

- *System* is parameterised by a *bitList*, which constitutes the classical bits that need to be exchanged between *Alice* and *Bob Random* agent creates a random bit and sends it via the *radomBitChannel* *Alice* first sends the length of the number of bits to be exchanged with *Bob*, i.e the length of *bitList*. Upon sending the length of the bit list, *Alice* continues with the process *AliceSend*. This is a recursive process which terminates after sending all the bits in *bitList*. *AliceSend* first receives a random bit from *randomBitChannel*, if the value received is equal to zero then the *qubit q* is encoded in the rectilinear basis else it is encoded in the diagonal basis. *(qubit q)* creates a new qubit *q* initialised to $|0\rangle$. Hence an operation of $X$ on $q$ to create $|1\rangle$ and $X$ or $X,H$ to convert it into $|+\rangle$ and $|-\rangle$ respectively. *AliceSend* then sends the qubit $q$ via *qubitChannel* to be received by *Bob*. The random bits are stored in *encodeBitList* to be used later when both the entities decide upon the key.
- *Bob* receives the length of the *bitList* and then continues with *BobReceive* process. Like *AliceSend*, this is a recursive process which terminates after receiving all the bits. *BobReceive* then uses a random bit from *randomBitChannel*, if this bit is zero then *Bob* measures the received qubit in the rectilinear basis else in the diagonal basis. We used a list that stores a couplet, where we store the random bit and the corresponding measurement.
- After exchanging the qubits, *Alice* and *Bob* continue with *AliceReveal* and *BobFinal* respectively. *AliceReveal* sends the basis that she used for encoding via the *decisionBitChannel*. *BobFinal* upon

receiving this basis elements checks whether the basis he measured in the same as of that of *Alice* in which case, he sends an acknowledgement via *decisionFlagChannel* to *Alice* and the corresponding bit he measured. *Alice* checks if the measurement that *Bob* made is the same as that of the intended bit. Since we are dealing with channels without any noise, if the measurement *Bob* made does not match, *Alice* straight away confirms the presence of an attacker and sends an *eveDetect* flag to *Bob*.

### 3.2 Formalising B92

Since *B*92 and *BB*84 only differ in how they encode the qubits, we can modify the CQP formalisation of *BB*84 for *B*92. *AliceSend* does not encode the qubit in a random basis. If the *bitList* element is equal to zero then she sends $|0\rangle$ else if the element in equal to one then $|+\rangle$ is exchanged. With few modifications to *AliceSend* in BB84, we can adopt it model B92.

## 4 MODELLING AND ANALYSIS IN PRISM

Conversion from CQP to PRISM is a step by step process. This conversion for a subset of commands has been done by Ware in his Master's thesis(Ware, 2008). We are going to use the same procedure. In the previous section we have mentioned that we have used *List* type. Unfortunately a parallel for this type does not exist for *PRISM*. To overcome this handicap we will have to modify the model, in both the protocols the public discussion starts after both the parties have exchanged all the qubits. Instead in the PRISM model after every qubit exchange, both the parties proceed to exchange the encoding basis and measured bit to establish the validity of the qubit. This way we can ensure that the original characteristics of the protocol remain intact.

- all the channels in the CQP model are defined as global variables in the *PRISM* model.
- the *PRISM* model constitutes of three modules representing the different agents in the CQP modelling
- on the *qbitChannel* the messages to be exchanged are limited to [0..3] with 0 representing $|0\rangle$, 1 for $|1\rangle$, 2 for $|+\rangle$ and 3 for $|-\rangle$.
- when Eve is detected, both *Alice* and *Bob* cease to exchange any more qubits and reach their end state.
- like in the CQP model we do not create a module for Random, rather all the parties create their own random bits either zero or one with equal probability.
- after choosing a random basis to measure in there is a one-fourth probability of any of the four outcomes.
- the number of bits to be exchanged is set by *N* the global variable. We check the properties of the model by varying the value of *N*. *Alice* and *Bob* iterate constrained by the value *N* and are synchronised by the label *loop*.
- *Alice* and *Bob* modules terminate either after exchanging *N* qubits or after detecting *Eve* and are synchronised by *stop*.

### 4.1 Analysis of BB84

With the models we have made in *PRISM* we are going to show there is a non zero probability with which the eavesdropper can be detected and how this probability varies with the number of photons exchanged.
*PRISM* is capable of calculating probabilities of the form $P_{\sigma,\Phi} = Pr\{\sigma \models \Phi\}$, i.e, given a *PRISM* model $\sigma$, we can calculate the probability with which the property $\Phi$ holds. $\Phi$ is expressed in **PCTL**. We have two models $\sigma_1$ and $\sigma_2$ for *random-substitution* and *intercept-resend*, respectively. Both these models are parametrised by *N* the number of qubits that both the parties exchange.

Let $P^n_{ED} = Pr\{\sigma_n(N) \models \Phi_1\}$ for $n \in \{1,2\}$, for the probability of eavesdropper detection and $P^n_{CM} = Pr\{\sigma_n(N) \models \Phi_2\}$ for $n \in \{1,2\}$ for the probability of the eavesdropper making correct measurements for more than half of the qubits. $n = 1$ for *random-substitution* and $n = 2$ for intercept resend. We also have $N \in [1,20]$, i.e, we start to find these probabilities starting from one qubit being exchanged to twenty.

$\Phi_1$ and $\Phi_2$ are to be expressed in PCTL. $\Phi_1$ is the PCTL formula corresponding to when the eavesdropper is detected. From the PRISM model for BB84, whenever an eavesdropper is detected *Alice* is in *aliceState=15* and *Bob* is in state *bobState=10*. The corresponding expression for $\Phi_1$ and their property expression in PRISM:

$$\Phi_1 = \{(aliceState = 15) \wedge (bobState = 10)\} \quad (1)$$

*P=?[F(aliceState=15)&(bobState=10)]* (2)

Similarly for $\Phi_2$ which gives the probability of eavesdropper measuring more than half of the exchanged qubits correctly is

$$\Phi_2 = \mathbf{true} \quad \mathcal{U} \quad (correctMeasurement > N/2) \quad (3)$$

$$P{=}?[F(correctMeasurement{>}\ \frac{N}{2})] \quad (4)$$

Table 1: Probability of detecting eavesdropper for BB84-QKD.

| N | $P^1_{ED}$ | $P^2_{ED}$ |
|---|---|---|
| 5 | 0.822 | 0.5512 |
| 10 | 0.9577 | 0.7698 |
| 15 | 0.9899 | 0.8819 |
| 20 | 0.9976 | 0.9394 |

TABLE I and TABLE II have probabilities that are observed from *PRISM*. Using the Curve Fitting tool of MATLAB, and using the Marquardt-Levenberg nonlinear least squares algorithm for curve-fitting we have come up with the equation that best fits these probabilities.

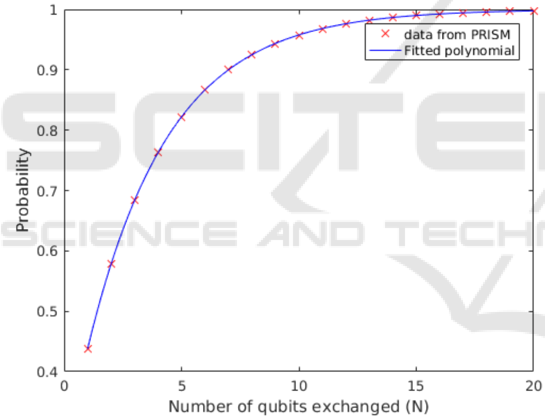

Figure 1: Probability of detecting eavesdropper for BB84 Random Substitution.

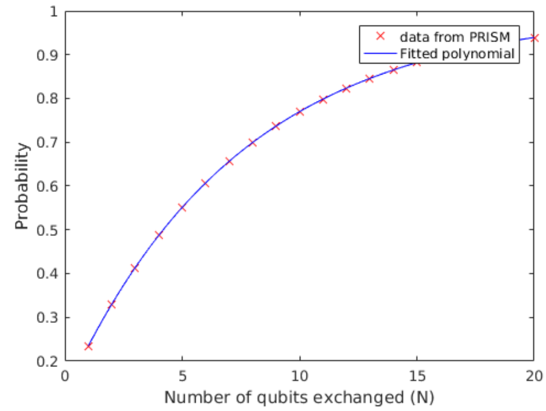

Figure 2: Probability of detecting eavesdropper for BB84 Intercept Resend.

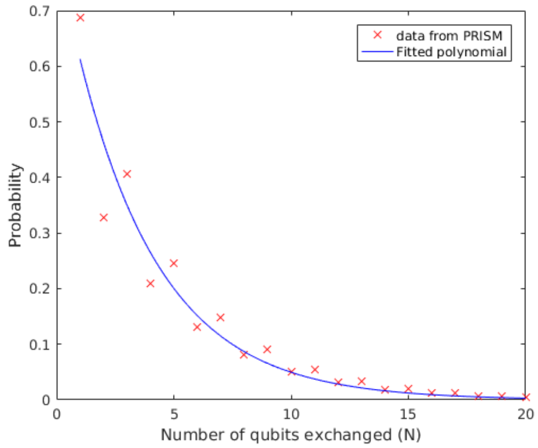

Figure 3: Probability of measuring more than $\frac{N}{2}$ qubits correctly for BB84 Random Substitution.

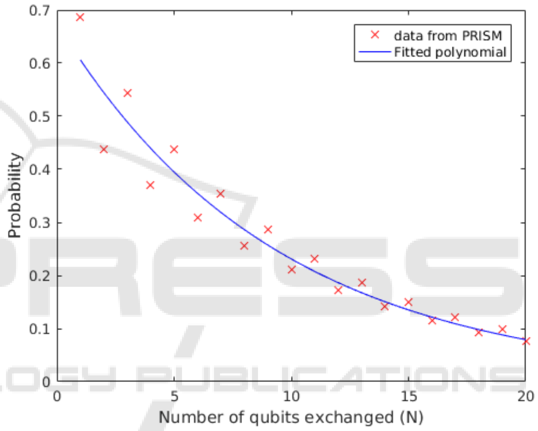

Figure 4: Probability of measuring more than $\frac{N}{2}$ qubits correctly for BB84 Intercept Resend.

Table 2: Probability of eavesdropper measuring more than half of the qubits correct for BB84-QKD.

| N | $P^1_{CM}$ | $P^2_{CM}$ |
|---|---|---|
| 5 | 0.2458 | 0.4370 |
| 10 | 0.0501 | 0.2111 |
| 15 | 0.0188 | 0.1510 |
| 20 | 0.00425 | 0.0756 |

We observed that

$$P^1_{ED} \approx Pr\{\sigma_1(N) \models \Phi_1\} = 1 - (0.75)e^{-0.2877N} \quad (5)$$

$$P^2_{ED} \approx Pr\{\sigma_2(N) \models \Phi_1\} = 1 - (0.8750)e^{-0.1335N} \quad (6)$$

and

$$P^1_{CM} \approx Pr\{\sigma_1(N) \models \Phi_2\} = (0.8108)e^{-0.2795N} \quad (7)$$

$$P^2_{CM} \approx Pr\{\sigma_2(N) \models \Phi_2\} = (0.6750)e^{-0.1072N} \quad (8)$$

Since $P^1_{ED} > P^2_{ED}$, the probability of eavesdropper getting detected is higher when the eavesdropper resorts to random-substitution.

Also it has to be noted that:

$$\lim_{N\to\infty} P^1_{ED} = \lim_{N\to\infty} P^2_{ED} = 1 \quad (9)$$

which suggests as the number of qubits exchanged increases so does the chances of detecting an eavesdropper.

$$\lim_{N\to\infty} P^1_{CM} = \lim_{N\to\infty} P^2_{CM} = 0 \quad (10)$$

reaffirms the theoretical results obtained by Mayers(Mayers, 2002), wherein he states *"amount of Shannon's information available to Eve must decrease exponentially fast as N increases."*. Both these observations reaffirm the results obtained by Papanikolaou(Gay et al., 2005).

## 4.2 Analysis of B92

We use the same notations as in the previous subsection. The only change being the PCTL expressions. Referring to PRISM model for B92, eavesdropper is detected when *aliceState=11* and *bobState=10*.

$$\Phi_1 = \{(aliceState = 11) \wedge (bobState = 10)\} \quad (11)$$

$$\textit{P=?[F(aliceState=15)\&(bobState=10)]} \quad (12)$$

$$\phi_2 = \textbf{true} \quad \mathcal{U} \quad (correctMeasurement > N/2) \quad (13)$$

$$\textit{P=?[F(correctMeasurement}> \frac{N}{2}\textit{)]} \quad (14)$$

Table 3: Probability of detecting eavesdropper for B92-QKD.

| N | $P^1_{ED}$ | $P^2_{ED}$ |
|---|---|---|
| 5 | 0.8665 | 0.7123 |
| 10 | 0.9683 | 0.89812 |
| 15 | 0.9924 | 0.96392 |
| 20 | 0.9976 | 0.98722 |

Table 4: Probability of eavesdropper measuring more than half of the qubits correct for BB84-QKD.

| N | $P^1_{CM}$ | $P^2_{CM}$ |
|---|---|---|
| 5 | 0.2458 | 0.3345 |
| 10 | 0.0501 | 0.1083 |
| 15 | 0.0201 | 0.0592 |
| 20 | 0.0042 | 0.0199 |

After using the curve fitting algorithm to approximate the results to an equation we have:

$$P^1_{ED} \approx Pr\{\sigma_1(N) \models \Phi_1\} = (1-(0.75)e^{-0.2877N}) \quad (15)$$

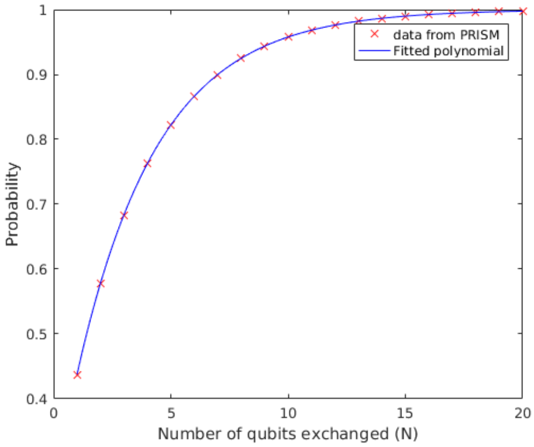

Figure 5: Probability of detecting eavesdropper for B92 Random Substitution.

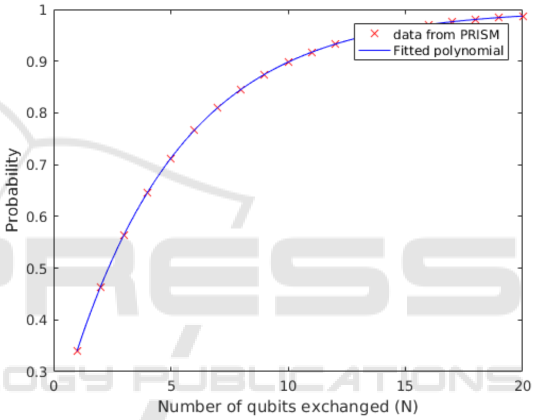

Figure 6: Probability of detecting eavesdropper for B92 Intercept Resend.

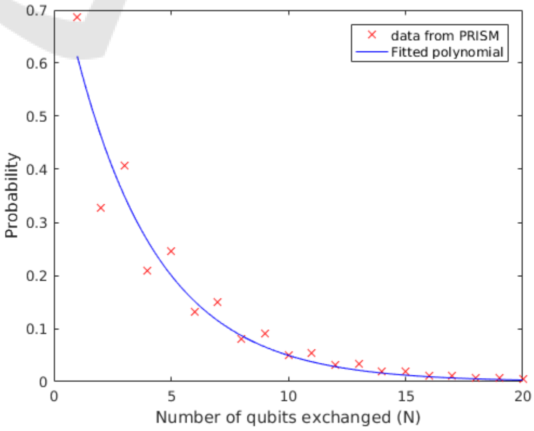

Figure 7: Probability of measuring more than $\frac{N}{2}$ qubits correctly for B92 Random Substitution.

$$P^2_{ED} \approx Pr\{\sigma_2(N) \models \Phi_1\} = (1-(0.8125)e^{-0.2795N}) \quad (16)$$

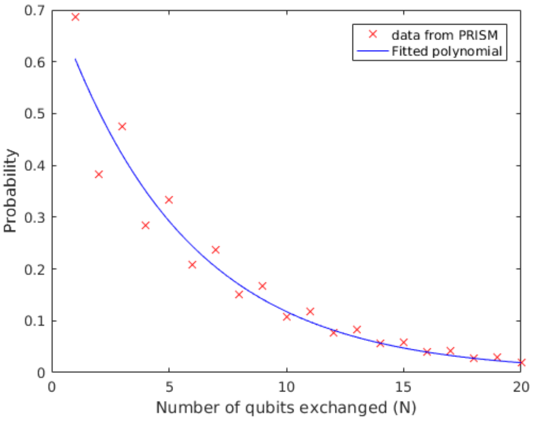

Figure 8: Probability of measuring more than $\frac{N}{2}$ qubits correctly for B92 Intercept Resend.

and

$$P^1_{CM} \approx Pr\{\sigma_1(N) \models \Phi_2\} = (0.8108)e^{-0.2795N} \quad (17)$$

$$P^2_{CM} \approx Pr\{\sigma_2(N) \models \Phi_2\} = (0.7272)e^{-0.1821N} \quad (18)$$

We make the following observations:

$$\lim_{N\to\infty} P^1_{ED} = \lim_{N\to\infty} P^2_{ED} = 1 \quad (19)$$

$$\lim_{N\to\infty} P^1_{CM} = \lim_{N\to\infty} P^2_{CM} = 0 \quad (20)$$

Like the inferences made for BB84, the chances of detecting an eavesdropper increases with the number of qubits exchanged and also the number of correct measurements that an eavesdropper can make decreases exponentially with the number of qubits exchanged. But unlike in BB84, for B92 we have $P^1_{ED} < P^2_{ED}$, hence the probability of eavesdropper detection is higher during intercept-resend than in random substitution.

## 4.3 Comparison between BB84 and B92

Quite strangely we observe that with respect to random substitution type of attack, both the protocols perform identically. This is substantiated by the equations

$$P^1_{CM} \approx Pr\{\sigma_1(N) \models \Phi_2\} = (0.8108)e^{-0.2795N} \quad (21)$$

and

$$P^1_{ED} \approx Pr\{\sigma_1(N) \models \Phi_1\} = (1-(0.75)e^{-0.2877N}) \quad (22)$$

However with respect to intercept resend style attacks they differ markedly, as evidenced by Fig. 12 and Fig. 13.

B92 performs better in terms of eavesdropper detection as the probability approaches unity faster than B92 and in terms of decreased number of correct measurements that can be made by the eavesdropper.

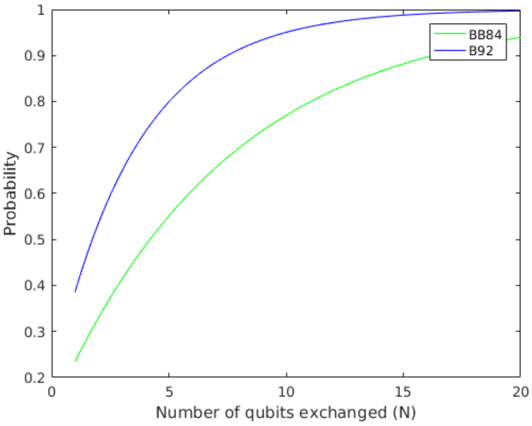

Figure 9: BB84 and B92 Comparison for Intercept Resend eavesdropper detection.

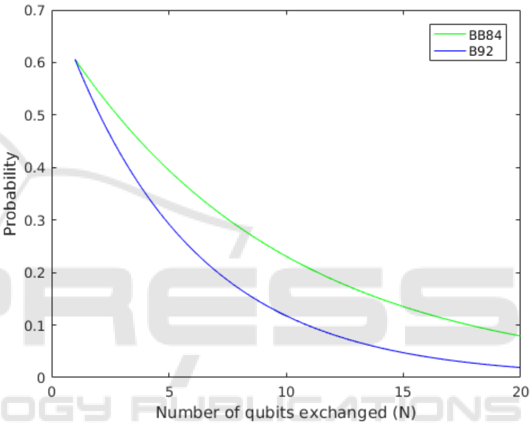

Figure 10: BB84 and B92 comparison for Intercept Resend correct measurements by eavesdropper.

# 5 CONCLUSION

We have successfully modelled BB84 protocol in CQP, showed the process in which we have created PRISM models from the CQP models and analysed the properties using PCTL. We also corroborate the theoretical observations made in earlier research with our analysis, namely the probability of correctly ascertaining the presence of an eavesdropper increases with the number of qubits exchanged. We also compared the performance of BB84 and B92 and infer that B92 is more resilient against an eavesdropper, with its ability to take fewer qubits than BB84 in identifying an eavesdropper and then potentially reducing the number of correct measurements the eavesdropper can make. Hence in practise B92 seems to be a more viable protocol than BB84 because it is less complex to implement and performs better.

## REFERENCES

Bužek, V. and Hillery, M. (1996). Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844.

Davidson, T. A. (2012). *Formal verification techniques using quantum process calculus*. PhD thesis, University of Warwick.

Gay, S., Nagarajan, R., and Papanikolaou, N. (2005). Probabilistic model–checking of quantum protocols. *arXiv preprint quant-ph/0504007*.

Gay, S. J. and Nagarajan, R. (2005). Communicating quantum processes. In *ACM SIGPLAN Notices*, volume 40, pages 145–157. ACM.

Mayers, D. (2002). Shor and preskill's and mayers's security proof for the bb84 quantum key distribution protocol. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 18(2):161–170.

Milner, R. (1999). *Communicating and mobile systems: the pi calculus*. Cambridge university press.

Nielsen, M. A. and Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.

Quan, Z. and Chaojing, T. (2002). Simple proof of the unconditional security of the bennett 1992 quantum key distribution protocol. *Physical Review A*, 65(6):062301.

Ware, C. J. (2008). *Modeling and analysis of quantum cryptographic protocols*. PhD thesis.