MTAT.07.006 Research Seminar in Cryptography
Attacking Practical Quantum Key Distribution Systems: Review

Katharina Kahrs

October 22, 2008

1 Introduction

The survey "Attacking Practical Quantum Key Distribution Systems" by Mihkel Kree[1] focuses on time shift attacks on quantum key distribution systems. Kree first describes the BB84 protocol for quantum key distribution (QDK). He then briefly describes the intercept-resend eavesdropping strategy and gives a detailed description of the intercept-resend strategy, which is a special case of time shift attacks. The opponent reviewed sections 1 to 3.1 of the survey. This is an update which reviews the updated survey as published on Helger Lipmaa's webpage on 21 Oct 2008. This will be done in accordance with the review form on Helger Lipmaa's MTAT.07.006 webpage.

2 General comments

The paper is well readable: rather yes than no
The survey is quite readable. There are many small examples. This improves readability. In some places, more paragraphs could improve readability further. In one place, there is a contradiction, and in some places Kree is too vague, unclear or imprecise.

Language used in the paper is correct: rather yes than no
There are some typos and grammar mistakes.

The paper is logical and well structured: yes

The general typeset of the paper is correct: yes

The paper was interesting to read: yes
The survey is interesting to read. It is accessible to readers without a background in quantum physics or quantum cryptography.

The paper gives a good overview of the topic:
The opponent is otherwise unfamiliar with the topic. It would be interesting to read more about the current implementations of QKD systems and the impact of time shift attacks on those implementations.

The material in the paper is mathematically correct: yes

References to the external sources are presented correctly: yes

All the relevant references are present: yes

The formulae are typed correctly:
There are no obvious misprints or mistakes.

3 Specific comments

3.1 Abstract

There are several grammar mistakes:

- "description of one possible attack" - this should be "a description of one possible attack".
- "in fields like financial industry as well as government and defence sector" - this should rather be "in fields like financial industry, government, and defence" or "in the financial industry, the government, and the defence sectors".

How many percent of key distribution systems today are QKD systems, and how many are conventional key distribution systems?

3.2 Section 1

Kree introduces three general properties of quantum systems. The first and third property are introduced in more detail in the subsections of section 1, and their relevance for QDK and time shift attacks is clear. The relevance of the second property, however, is unclear. Also, it is unclear what is meant by "complementary properties". Why are position and momentum complementary properties?

It is in the opponent's opinion better to split the sentence "Although there are many equivalent mathematical formulations of QM, we will use the most common one, developed by Paul Dirac." into two sentences: "There are many equivalent mathematical formulations of QM." and "We will use the most common one, developed by Paul Dirac." There is no contradiction between the two parts of the sentence.

"In that formalism" should rather be "In that formulation". A formalism is not the same as a formulation.

There is a contradiction in the second paragraph of section 1.1: "However, in general, QM does not assign values to observables (...) as it is the case in classical mechanics." and "and simultaneously assigns the corresponding eigenvalue to the observable" contradict each other. The opponent suggests to leave out the sentence "However, in general, QM does not assign values to observables (...) as it is the case in classical mechanics." The sentence "In fact, the observables are associated with..." could then instead be: "The observables (e.g. momentum, position, energy of a particle) are associated with...". After this sentence, there should be a paragraph.

"(self-adjoint matrix)" should be left out. After the sentence "...of the corresponding operator", there should be a paragraph.

"Gives as output a combined state" should rather be "It gives as output a combined state".

3.3 Section 3

There are several grammar mistakes and typos:

- "and, conversely, that at time t_1" is better than "and, conversely, at time t_1".
- "she randomly chooses basis": this should be "she randomly chooses a basis".
- "she then encodes the photon": this should be "She then encodes the photon".
- "where Alice and Bob chose different basis": this should be "where Alice and Bob chose different bases".
- "Eve can compromise the sequrity of the system": "this should be "Eve can compromise the security of the system".

It is not clear that α is larger than β. This is, however, essential for the time shift attack. The opponent suggests the following: "Suppose that at time t_0, the efficiency of detecting bit "0" is α and the efficiency of detecting bit "1" is β, and conversely, that at time t_1 the efficiency of detecting bit "0" is β and the efficiency of detecting bit "1" is α, with $\alpha > \beta$.". For clarity the opponent also suggests "$\eta = \frac{\beta}{\alpha} < 1$" instead of just "$\eta = \frac{\beta}{\alpha}$".

The sentence "In addition, she adjusts the arrival time of the photon at Bob's detector to be t_0 or t_1 depending on whether her measured bit value was "0" or "1"." is a bit unclear. This might be better: "In addition, she adjusts the arrival time of the photon at Bob's detector to be t_0 if her measured bit value was "0", or t_1 if her measured bit value was "1".".

Further, Kree clearly explains what Eve does in both the intercept-resend time shift attack and the simple time shift attack. He does not explain, however, why Eve does this rather than the intercept-resend eavesdropping attack.

The key point is that the error rate due to Eve's attack is lower in the time shift attack than in the eavesdropping attack. An example of the intercept-resend eavesdropping attack, the intercept-resend time shift attack, and the simple time shift attack on a fixed instance of the BB84 protocol between Alice and Bob might clarify this. It should be emphasized that $1-\beta$ is large, that $1-\frac{\alpha}{2}-\frac{\beta}{2}$ is small, and that $\frac{\alpha}{2}$ is larger than $\frac{\beta}{2}$.

4 Conclusion

In general, the opponent is of the opinion that this is a good survey.

References

[1] M. Kree. Attacking Practical Quantum Key Distribution Systems