2016/2500M-0054

ISSN 1797-3457 (verkkojulkaisu)
ISBN (PDF) 978-951-25-2850-9

SUMMARY REPORT

APPLICATIONS OF THE QUANTUM KEY DISTRIBUTION (QKD) METHOD

Ilkka Tittonen, professor,
Department of Micro- and Nanosciences (MNT), Aalto University,
Tietotie 3, 02150 Espoo, ilkka.tittonen@aalto.fi
Iikka Elonsalo (MNT)
Teemu Manninen (MNT)
Olav Tirkkonen, professor,
Department of Communications and Networking (COMNET), Aalto University
Jari Lietzen (COMNET),
Dr. Ülo Parts (COMNET)
Mikko Kiviranta (VTT)

Abstract Horizon 2020 defined Quantum Technologies (QT) by the FET (Future and Emerging Technologies). This involves the control and manipulation of quantum systems to achieve results not possible with classical matter. However, Quantum Technologies give much more than this and represent a completely new paradigm, as they bring technological applications to a different physical framework where devices are described by quantum laws. With the advent of quantum computers, traditional methods of cryptography become vulnerable. The only method to ensure security against any eavesdropping in a world with quantum computers is to use quantum-based cryptographic methods. In the proposed second year of the project, Quantum Key Distribution (QKD) will be further investigated based on the experience obtained during the first year. An open platform for QKD will be used to build know-how in the applicability of QKD for encryption of messages transmitted over extended distances. Classical error correcting coding will be explored for quantum key distillation.

1 Introduction

With the advent of quantum computers, traditional methods of cryptography become vulnerable. The only method to ensure security against any eavesdropping in a world with quantum computers is to use quantum-based cryptographic methods. Quantum key distribution (QKD) has been under investigation in the current project. QKD systems will remain secure regardless of computational power available to an adversary. An open platform Clavis2 has been useful to acquire know-how, perform various performance tests, and gather data for current and future research.

2 Research objectives and accomplishment plan

One of the key objectives of the research was to build know-how in quantum key distribution (QKD) and to evaluate the performance of a QKD system as a function of communication distance. Another target was to characterize the main sources of losses in QKD.

The work was done by utilizing Clavis2, a commercial device from ID Quantique. The plan was

implemented as two-fold approach. Actual measurements in various conditions were done to characterize the capabilities of existing devices. During that phase real data bits of quantum channel were gathered for processing in the second task of the project.

3 Materials and methods

ID Quantique's quantum key distribution (QKD) Clavis2 devices have been used in the research. The apparatus suits well for research purposes. It can be utilized for gathering actual data from the quantum channel. Real channel data is unique from the research point of view as it provides opportunities to study communications engineering aspects in laboratory circumstances. We have gathered channel data for different lengths of optical fiber up to 54 km.

There are several steps in quantum key distribution: Alice sends the raw bits to Bob. Bob receives a fraction of those. The next phase is called sifting, when only those bits are accepted which have the same basis. Those bits still contain errors, which are corrected using the Cascade method, where the parity information is exchanged via classical channel. That information is available to the eavesdropper. Therefore privacy amplification is used. The system also stores the data after each step of quantum key generation. The number of bits per each step for 25 km is shown in the table below.

Alice's raw key	$5.14 \cdot 10^8$	100 %
Bob's raw key	$4.00 \cdot 10^6$	0.778 %
Sifted key	$9.95 \cdot 10^5$	0.194 %
Disclosed bits	$2.74 \cdot 10^5$	0.0534 %
Secret key	$2.39 \cdot 10^5$	0.0466 %

Quantum key generation efficiency decreases as a function of communication distance. For the current Clavis2 system, the efficiency decreases rapidly close to the distance of 50 km.

The table shows that there is significant loss also from the error correction process. In the current project, we studied the influence of a simple adaptive method. The method consists of the following steps:

1. Alice and Bob are comparing first 1024 bits from received raw bits (after sifting) and estimate initial bit error rate (BER).
2. BER is used to select initial block size. The target is to select a block size, where there is 1 error only with high probability.
3. Alice and Bob are comparing parities of the blocks with determined size. If the parity is different, the block is just discarded
4. Parity comparison is taken into account on quality counters.
5. If the number of successful comparisons exceeds certain threshold value, the block size is increased
6. If the number of unsuccessful comparisons exceeds certain threshold value, the block size is decreased

In order to ensure that the key is the same for Alice and Bob, they calculate after several thousands of bits a cryptographic hash. If the hashes are not the same, the key is either discarded, or the errors are searched once again by selecting e.g. different block size or different composition of blocks. In our study we found that the amount of errors that are are left is about 0.3 % from total bits. These are detected using the hash.

Table 1 summarizes the relationship between the sifted key and the final secret key. QBER is the quantum bit error rate calculated from the actual key material and efficiency describes how much sifted key material is present in the final key. The efficiencies are calculated from equal length samples taken from measurements at different distances. The adaptive method was forced to use fixed block size in the error detection phase.

Table 1. Comparison of current error correction method and the proposed adaptive method

Distance [km]	QBER (Calculated)	Efficiency	
		Current	Adaptive
0	1.79 %	31.0 %	43.3 %
33	3.58 %	23.8 %	37.4 %
37	4.19 %	23.0 %	35.5 %
50	7.32 %	6.4 %	27.2 %
52	8.76 %	0.0 %	24.0 %
54	11.79 %	0.0 %	18.4 %

The result of adaptive method for 37 km fiber is shown in Table 2. The measured BER was 4.18 %. The program used to implement the adaptive method keeps statistics of the block lengths. Undetected bit errors in Table 2 are bit errors that were not detected by using the parity check method. Therefore an additional step is needed to ensure the integrity of the final key.

Alice and Bob are using a classical channel for communications during the key distillation process. It should be assumed that there is an eavesdropper on line. Therefore they are using One Time Pad (OTP) for securing the communication. In the proposed adaptive method distributed secure key is used to secure the communication over the classical channel. Therefore it is assumed that half of secure key is used for that purpose. It is taken into account when calculating the quantum key rate or key generation efficiency numbers. That assumption is actually pessimistic in comparison with the needed length of OTP.

Table 2. Example results from adaptive method with 37 km distance.

Sifted bits	Key bits	Parity checks	Detected bit erros	Undetected bit errors
263 265 088	215 909 476	62 244 567	9 500 759	734 922
Block size in bits				
4	8	16	32	64
60 278 770	1 202 014	716 742	46 342	699

The results are obtained through simulations, which is implemented in the C programming language. The C-language is also used for implementing supporting software.

4 Results and discussion

In the current work, we have identified that in the process of secure key generation an adaptive error correction method improves the overall performance. That is in the best way expressed in Figure 1 where the secure key rate in bits/s is plotted as a function of the communication distance. The blue curve represents the performance measured in the Matine project in Otaniemi with Clavis2 devices. The curve is with good accordance with similar data presented in the literature. The important property of the curve is that at a certain distance, when the QBER becomes large enough, the secure key rate decreases rapidly.

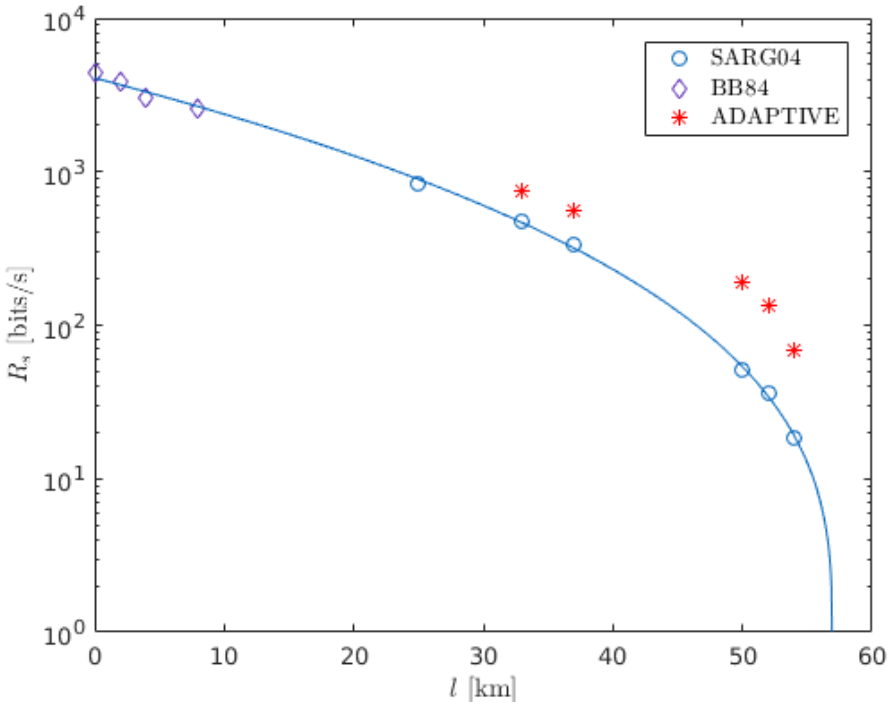

Figure 1: Secure key rate (bit/s) as a function of distance. The circles are measurements with Clavis2 systems. The red stars represent the simulation results with adaptive decoding method.

Red stars in the figure show the key rate with the adaptive bit distillation method. As it is visible from Figure 1, some gain is achievable at large distances when the basic curve turns sharply downward. The gain in this region measured in the secure key rate is significantly larger than at distances 20-30 km.

At the moment, the speed of generating secure keys is not sufficient for real time high data rate applications even at short distances. The problem could be solved with using parallel channels and systems. The other limiting factor is that Clavis2 is using a single optical fiber for communications. Therefore, the quantum bits are transmitted in bursty mode. Some of these limitations will be solved in the next generation systems of ID Quantique, where the target is to achieve the secure key rate over 1 Mbits/s.

At larger distances, the error correction process may be started only when a large enough number of bits have been received. That introduces delays in secure key generation. When using the proposed adaptive method, such delays will be avoided and the process will start with a smaller buffer.

5 Conclusions

In the current projects, we have shown that the error correction protocol has a clear impact on the overall performance of the system measured as a larger secure key rate. In addition the proposed adaptive method represents faster protocol with smaller requirements to the classical communication channel.

The performance of the used system is limited but may be sufficient in specific applications and services with extra high security requirements. It is not suitable for high capacity Internet traffic. Systems with higher performance are under development. Those systems tackle the improvement of optical communication protocols as well as error corrections.

For that purposes we have performed background research, which is clearly extra work compared with the project plan and targets. That part is especially important to road map future development directions, which could bring Finland to the leading position when resourced properly.

The background research revealed that the research field is currently under heavy change. The main motor behind it is the fast development of the technology needed for quantum key exchange. This progress is not only making old things faster and more practical, but is opening completely new ways of taking benefit of quantum phenomena in key exchange.

At the moment it is quite uncertain, which type of technology or protocols will be used even in the near future in quantum key exchange. Theoretical work on such fast progressing topic would have possibility for a breakthrough theoretical work, but would also allow us to collect the practical know-how of the strengths and weaknesses of different QKD solutions.

The preliminary research we have performed have opened several research directions. One of the key problems of the now studied Cascade-based reconciliation is that it is slow. During recent years, this problem has been tried to overcome by protocols that are based on classical error correcting codes (TURBO, Polar, LDPC). These are faster, but they are functional only when QBER is less than 11 percent and they need very large blocks of raw key to begin the reconciliation process. The need for small QBER is common for all protocols that are based on one-way communication using the classical channel. However, it is known that if both Bob and Eve are allowed to communicate through the classical channel, key exchange is possible even when QBER is 20 percent. The preliminary research we have performed now suggest that we could combine some simple two-way post processing method and fast classical coding to create robust QKD protocol that would work also with small amounts of raw key.

In all the previously discussed key exchange protocols the basic assumption is that the quantum information is carried on two dimensional quantum systems (QBIT). However, such as-

sumption is not needed and in fact it is known that in theory using higher dimensional quantum systems (QBITS), would allow higher key rate secure communication. Such protocols have been studied both theoretically and experimentally to a very great degree, but practical applications have appeared rather distant. However, recently several groups have reported very promising implementations of such protocols. If this technology is now turning into reality, designing tailor-made protocols for using higher dimensional key exchange would be a very timely topic.

6 Scientific publishing and other reports produced by the research project

The project has been short effort with goal to get hands on experience with the current state of the art equipment. Results are initial and more research is needed to finalize those as scientific publications.