**Improving cyber security using quantum computing**

***Abstract –*** The aim of this paper is to describe a new possible encryption algorithm which proposes to combine the facilities provided by quantum computing with the implementation of hash functions, symmetric and asymmetric-key algorithms as a result of quantum super positioning, as well as introduce readers to key aspects of quantum computing and elucidate its implications in present cryptography. In particular the reader can delve into the following subjects: present cryptographic schemes (symmetric and asymmetric), differences between quantum and classical computing, challenges in quantum computing, quantum algorithms (Shor’s and Grover’s), public key encryption schemes affected, symmetric schemes affected, the impact on hash functions, and post quantum cryptography. The experiments taken on the available data show a possible improvement compared to other related work due to a lower value of the Quantum Bit Error Rate, which is a metric for measuring how efficient and reliable a quantum algorithm is.

***ACM and AMS classifications:***

**AMS:**

81-XX Quantum theory

81Pxx Foundations, quantum information and its processing, quantum axioms, and philosophy

81P40 Quantum coherence, entanglement, quantum correlations

68-XX Computer science {For papers containing software, source code, etc. in a specific mathematical area, see the classification number -04 in that area}

68Mxx Computer system organization

68M25 Computer security

97-XX Mathematics education

97Pxx Computer science (educational aspects)

97P20 Theoretical computer science (educational aspects)

**ACM**:

* [D.](http://www.acm.org/about/class/ccs98-html#D.): Software
  + [D.4](http://www.acm.org/about/class/ccs98-html#D.4): OPERATING SYSTEMS
    - [D.4.6](http://www.acm.org/about/class/ccs98-html#D.4.6): Security and Protection
* [E.](http://www.acm.org/about/class/ccs98-html#E.): Data
  + [E.3](http://www.acm.org/about/class/ccs98-html#E.3): DATA ENCRYPTION
* [F.](http://www.acm.org/about/class/ccs98-html#F.): Theory of Computation
  + [F.m](http://www.acm.org/about/class/ccs98-html#F.m): MISCELLANEOUS

* [I.](http://www.acm.org/about/class/ccs98-html#I.): Computing Methodologies
  + [I.m](http://www.acm.org/about/class/ccs98-html#I.m): MISCELLANEOUS

**Table of contents**

1. Introduction
2. Original approach
3. Existing Work
4. Research Methodology
5. Results
6. Discussion
7. Conclusion

**1. Introduction**

Quantum computing theory firstly introduced as a concept in 1982 by Richard Feynman, has been researched extensively and is considered the destructor of the present modern asymmetric cryptography. In addition, it is a fact that symmetric cryptography can also be affected by specific quantum algorithms; however, its security can be increased with the use of larger key spaces. Furthermore, algorithms that can break the present asymmetric cryptoschemes whose security is based on the difficulty of factorizing large prime numbers and the discrete logarithm problem have been introduced. It appears that even elliptic curve cryptography which is considered presently the most secure and efficient scheme is weak against quantum computers. Consequently, a need for cryptographic algorithms robust to quantum computations arose.

Quantum mechanics changes our view of information processing: the ability to access, operate and transmit data according to the laws of quantum physics opens the doors to a vast realm of possible applications. Cryptography is one of the areas that is most seriously impacted by the potential of quantum information processing, since the security of most cryptographic primitives in use today relies on the hardness of computational problems that are easily broken by adversaries having access to a quantum computer.

While the impact of quantum computers on cryptanalysis is tremendous, quantum mechanics itself predicts physical phenomena that can be exploited in order to achieve new levels of security. These advantages were already mentioned in the late 1970’s in pioneering work of Wiesner and have led to the very successful theory of quantum key distribution (QKD), which has already seen real-world applications. QKD achieves information-theoretically secure key expansion, and has the advantage of relatively simple hardware requirements (notwithstanding a long history of successful attacks to QKD at the implementation level).

The cryptographic possibilities of quantum information go well beyond QKD. Indeed, quantum copy-protection, quantum money and revocable time-release encryption are just some examples where properties unique to quantum data enable new cryptographic constructions. Thanks in part to these tremendous cryptographic opportunities, we envisage an increasing need for an information infrastructure that enables quantum information. Such an infrastructure will be required to support:

– Quantum functionality: honest parties can store, exchange, and compute on quantum data;

– Quantum security: quantum functionality is protected against quantum adversaries.

The current state-of-the-art is lacking even the most basic cryptographic concepts in the context of quantum functionality and quantum adversaries. In particular, the study of encryption of quantum data (which is arguably one of the most fundamental building blocks) has so far been almost exclusively limited to the quantum one-time pad and other aspects of the informationtheoretic setting (one notable exception being). The achievability of other basic primitives such as public-key encryption has not been thoroughly investigated for the case of fully quantum cryptography. This situation leaves many open questions about what can be achieved in the quantum world.

In this paper I’m going to first show an analysis of symmetric cryptography, asymmetric cryptography and hash functions. Following is an introduction to quantum mechanics and the challenge of building a true quantum computer. Furthermore, I introduce two important quantum algorithms that can have a huge impact in asymmetric cryptography and less in symmetric, namely Shor’s algorithm and Grover’s algorithm respectively. Last but not least, I present my take on an algorithm, experiments, I talk about Quantum Bit Error Rate, Polarization entanglement, Energy-time entanglement, how the algorithm performs compared to other algorithms and conclusions about what the data shows us together with trying to respond to the following research questions:

* Can data encryption be safer using a quantum encryption algorithm together with nowadays algorithms?
* How will the proposed algorithm respond to the problem of quantum adversaries?

**Related work**

The group of Anton Zeilinger, then at the University of Innsbruck, demonstrated such a crypto-system, including error correction, over a distance of 360 meters (Jennewein et al. 2000b). Inspired by a test of Bell inequalities performed with the same set-up a year earlier (Weihs et al., 1998), the two-photon source was located near the center between the two analyzers. Special optical fibers, designed for guiding only a single mode at 700 nm, were used to transmit the photons to the two analyzers. The results of the remote measurements were recorded locally and the processes of key sifting and of error correction implemented at a later stage, long after the distribution of the qubits. Two different protocols were implemented: one based on Wigner’s inequality (a special form of Bell inequalities), and the other one following BB84.

The group of Paul Kwiat then at Los Alamos National Laboratory, demonstrated the Ekert protocol (Naik et al. 2000). This experiment was a table-top realization with the source and the analyzers only separated by a few meters. The quantum channel consisted of a short free space distance. In addition to performing QC, the researchers simulated different eavesdropping strategies as well. As predicted by the theory, they observed a rise of the QBER with an increase of the information obtained by the eavesdropper. Moreover, they also recently implemented the six-state protocol described in paragraph II D 2, and observed the predicted QBER increase to 33% (Enzer et al. 2001).

The main advantage of polarization entanglement is the fact that analyzers are simple and efficient. It is therefore relatively easy to obtain high contrast. Naik and co-workers, for example, measured a polarization 32 extinction of 97%, mainly limited by electronic imperfections of the fast modulators. This amounts to a QBERopt contribution of only 1.5%.

In spite of their qualities, it would be difficult to reproduce these experiments on distances of more than a few kilometers of optical fiber. As mentioned in the introduction to this chapter, polarization is indeed not robust enough to decoherence in optical fibers. In addition, the polarization state transformation induced by an installed fiber frequently fluctuates, making an active alignment system absolutely necessary. Nevertheless, these experiments are very interesting in the context of free space QC.

**Original approach**

**A) Quantum Bit Error Rate**

The QBER is defined as the number of wrong bits to the total number of received bits and is normally in the order of a few percent. In the following I will use it expressed as a function of rates:

Text

Description automatically generated with low confidence,

where the sifted key corresponds to the cases in which Alice and Bob made compatible choices of bases, hence its rate is half that of the raw key. The raw rate is essentially the product of the pulse rate frep, the mean number of photon per pulse µ, the probability tlink of a photon to arrive at the analyzer and the probability η of the photon being detected:

Text

Description automatically generated with medium confidence

The factor q (q≤1, typically 1 or 1 2 ) must be introduced for some phase-coding setups in order to correct for noninterfering path combinations.

One can distinguish three different contributions to Rerror. The first one arises because of photons ending up in the wrong detector, due to unperfect interference or polarization contrast. The rate Ropt is given by the product of the sifted key rate and the probability popt of a photon going in the wrong detector:

Text

Description automatically generated

This contribution can be considered, for a given set-up, as an intrinsic error rate indicating the suitability to use it for QC. We will discuss it below in the case of each particular system.

The second contribution, Rdet, arises from the detector dark counts (or from remaining environmental stray light in free space setups). This rate is independent of the bit rate. Of course, only dark counts falling in a short time window when a photon is expected give rise to errors.

Text

Description automatically generated with medium confidence,

where pdark is the probability of registering a dark count per time-window and per detector, and n is the number of detectors. The two 1 2 -factors are related to the fact that a dark count has a 50% chance to happen with Alice and Bob having chosen incompatible bases (thus eliminated during sifting) and a 50% chance to arise in the correct detector.

Finally error counts can arise from uncorrelated photons, because of imperfect photon sources:

.

This factor appears only in systems based on entangled photons, where the photons belonging to different pairs but arriving in the same time window are not necessarily in the same state. The quantity pacc is the probability to find a second pair within the time window, knowing that a first one was created.

The QBER can now be expressed as follows:

Text, letter

Description automatically generated

**B) Polarization entanglement**

A first class of experiments takes advantage of polarization-entangled photon pairs. The setup, depicted in Fig. 21, is similar to the scheme used for polarization coding based on faint pulses.

Diagram

Description automatically generated

**Experiment:**

A two-photon source emits pairs of entangled photons flying back to back towards Alice and Bob. Each photon is analyzed with a polarizing beamsplitter whose orientation with respect to a common reference system can be changed rapidly. Two experiments, have been reported in the spring of 2000 (Jennewein et al. 2000b, Naik et al. 2000). Both used photon pairs at a wavelength of 700 nm, which were detected with commercial single photon detectors based on Silicon APD’s. To create the photon pairs, both groups took advantage of parametric downconversion in one or two BBO crystals pumped by an argon-ion laser. The analyzers consisted of fast modulators, used to rotate the polarization state of the photons, in front of polarizing beamsplitters.

**C) Energy-time entanglement**

*1. Phase-coding*

The other class of experiments takes advantage of energy-time entangled photon pairs. The idea originates from an arrangement proposed by Franson in 1989 to test Bell inequalities. As we will see below, it is comparable to the double Mach-Zehnder configuration discussed in section IV C 1. A source emits pairs of energycorrelated photons with both particles created at exactly the same, however uncertain time (see Fig. 22).

This can be achieved by pumping a non-linear crystal with a pump of large coherence time. The pairs of downconverted photons are then split, and one photon is sent to each party down quantum channels. Both Alice and Bob possess a widely, but identically unbalanced MachZehnder interferometer, with photon counting detectors connected to the outputs. Locally, if Alice or Bob change the phase of their interferometer, no effect on the count rates is observed, since the imbalancement prevents any single-photon interference. Looking at the detection-time at Bob’s with respect to the arrival time at Alice’s, three different values are possible for each combination of detectors.

The different possibilities in a time spectrum are shown in Fig. 22. First, both photons can propagate through the short arms of the interferometers. Next, one can take the long arm at Alice’s, while the other one takes the short one at Bob’s. The opposite is also possible. Finally, both photons can propagate through the long arms. When the path differences of the interferometers are matched within a fraction of the coherence length of the down-converted photons, the short-short and the long-long processes are indistinguishable, provided that the coherence length of the pump photon is larger than the path-length difference.

Conditioning detection only on the central time peak, one observes two-photon interferences which depends on the sum of the relative phases in Alice’s and Bob’s interferometer – non-local quantum correlation (Franson 1989) – see Fig. 22. The phase in the interferometers at Alice’s and Bob’s can, for example, be adjusted so that both photons always emerge from the same output port. It is then possible to exchange bits by associating values to the two ports. This is, however, not sufficient. A second measurement basis must be implemented, to ensure security against eavesdropping attempts.

This can be done for example by adding a second interferometer to the systems (see Fig. 23). In the latter case, when reaching an analyzer, a photon chooses randomly to go to one or the other interferometer. The second set of interferometers can be adjusted to also yield perfect correlations between output ports. The relative phase between their arms should however be chosen so that when the photons go to interferometers not associated, the outcomes are completely uncorrelated.

Such a system features a passive state preparation by Alice, yielding security against multiphoton splitting attacks (see section VI J). In addition, it also features a passive basis choice by Bob, which constitutes an elegant solution: neither a random number generator, nor an active modulator are necessary. It is nevertheless clear that QBERdet and QBERacc (defined in eq. (33)) are doubled since the number of activated detectors is twice as high. This disadvantage is however not as important as it first appears since the alternative, a fast modulator, introduces losses close to 3dB, also resulting in an increase of these error contributions. The striking similarity between this scheme and the double Mach-Zehnder arrangement discussed in the context of faint laser pulses in section IV C 1 is obvious when comparing Fig. 24 and Fig. 16! Diagram

Description automatically generatedDiagram

Description automatically generatedDiagram

Description automatically generated Diagram

Description automatically generated

This scheme has been realized in the first half of 2000 by our group at Geneva University (Ribordy et al., 2001). It constitutes the first experiment in which an asymmetric setup, optimized for QC was used instead of a system designed for tests of Bell inequality and having a source located in the center between Alice and Bob (see Fig. 25). The two-photon source (a KNbO3 crystal pumped by a doubled Nd-YAG laser) provides energy-time entangled photons at non-degenerate wavelengths – one around 810 nm, the other one centered at 1550 nm. This choice allows to use high efficiency silicon based single photon counters featuring low noise to detect the photons of the lower wavelength. To avoid the high transmission losses at this wavelength in optical fibers, the distance between the source and the corresponding analyzer is very short, of the order of a few meters. The other photon, at the wavelength where fiber losses are minimal, is sent via an optical fiber to Bob’s interferometer and is then detected by InGaAs APD’s. The decoherence induced by chromatic dispersion is limited by the use of dispersionshifted optical fiber (see section III B 3).

*2. Phase-time coding*

We have mentioned in section IV C that states generated by two-paths interferometers are two-levels quantum systems. They can also be represented on a Poincar´e sphere. The four-states used for phase coding in the previous section would lie on the equator of the sphere, equally distributed. The coupling ratio of the beamsplitter is indeed 50%, and they differ only by a phase difference introduced between the components propagating through either arm. In principle, the four-state protocol can be equally well implemented with only two states on the equator and the two other ones on the poles. In this section, we present a system exploiting such a set of states. Proposed by our group in 1999 (Brendel et al., 1999), the scheme follows in principle the Franson configuration described in the context of phase coding. However, it is based on a pulsed source emitting entangled photons in so-called energy-time Bell states (Tittel et al. 2000). The emission time of the photon pair is therefore given by a superposition of only two discrete terms, instead of a wide and continuous range bounded only by the large coherence length of the pump laser (see paragraph V B 1). Diagram, engineering drawing

Description automatically generated

Consider Fig. 26. If Alice registers the arrival times of the photons with respect to the emission time of the pump pulse t0, she finds the photons in one of three time slots (note that she has two detectors to take into account). For instance, detection of a photon in the first slot corresponds to “pump photon having traveled via the short arm and downconverted photon via the short arm”. To keep it short, we refer to this process , where P stands for the pump- and A for Alice’s photon46. However, the characterization of the complete photon pair is still ambiguous, since, at this point, the path of the photon having traveled to Bob (short or long in his interferometer) is unknown to Alice. Figure 26 illustrates all processes leading to a detection in the different time slots both at Alice’s and at Bob’s detector. Obviously, this reasoning holds for any combination of two detectors. In order to build up the secret key, Alice and Bob now publicly agree about the events where both detected a photon in one of the satellite peaks – without revealing in which one – or both in the central peak – without revealing the detector. This procedure corresponds to key-sifting. For instance, in the example discussed above, if Bob tells Alice that he also detected his photon in a satellite peak, she knows that it must have been the left peak as well. This is due to the fact that the pump photon has traveled via the short arm – hence Bob can detect his photon either in the left satellite or in the central peak. The same holds for Bob who now knows that Alice’s photon traveled via the short arm in her interferometer. Therefore, in case of joint detection in a satellite peak, Alice and Bob must have correlated detection times. Assigning a bit value to each side peak, Alice and Bob can exchange a sequence of correlated bits

*3. Quantum secret sharing*

In addition to QC using phase-time coding, we used the setup depicted in Fig. 26 for the first proof-of-principle demonstration of quantum secret sharing – the generalization of quantum key distribution to more than two parties (Tittel et al., 2001). In this new application of quantum communication, Alice distributes a secret key to two other users, Bob and Charlie, in a way that neither Bob nor Charlie alone have any information about the key, but that together they have full information. Like with traditional QC, an eavesdropper trying to get some information about the key creates errors in the transmission data and thus reveals her presence. The motivation behind quantum secret sharing is to guarantee that Bob and Charlie cooperate – one of them might be dishonest – in order to obtain a given piece of information. In contrast with previous proposals using three-particle GHZ states (Zukowski ˙ et al.,1998, and Hillery et al., 1999), pairs of entangled photons in so-called energy-time Bell states were used to mimic the necessary quantum correlation of three entangled qubits, albeit only two photons exist at the same time. This is possible because of the symmetry between the preparation device acting on the pump pulse and the devices analyzing the downconverted photons. Therefore, the emission of a pump pulse can be considered as the detection of a photon with 100% efficiency, and the scheme features a much higher coincidence rate than that expected with the initially proposed “triple-photon” schemes.