ISBN 978-94-007-2487-7

NATO Science for Peace and Security Series - A:
Chemistry and Biology

Technological Innovations in Sensing and Detection of Chemical, Biological, Radiological, Nuclear Threats and Ecological Terrorism

Edited by
Ashok Vaseashta
Eric Braman
Philip Susmann

Springer

NATO OTAN *This publication is supported by:* The NATO Science for Peace and Security Programme

Chapter 36
Quantum Cryptography for Information-Theoretic Security

Quantum Cryptography

Barry Sanders

Abstract This article explains quantum computing and its potential for rendering current encrypted communication via public channels insecure. A review of quantum key distribution is given as a way to ensure secure public-channel communication regardless of the computational power of an adversary, that may possesses a quantum computer. Finally, state-of-the-art quantum key distribution is discussed with an insight into its future.

Keywords Quantum computing • Quantum key distribution • Quantum cryptography • Quantum communication • Information security

36.1 Introduction

For business and pleasure, we need to send secrets through public channels, whether by telephone, fax, telex or the internet. Let us consider the following example. Suppose you wish to make a payment via a web page using your credit card, but you want to ensure that your credit card details are safe from eavesdropping criminals.

This criminal eavesdropper, whom we call "Eve", could be powerful beyond your dreams, for example using devices and mathematics we do not yet imagine. Is our communication protected against such powerful adversaries? Here is one

B. Sanders (✉)
Institute for Quantum Information Science, University of Calgary,
2500 University Drive N.W., Calgary, AB, Canada
e-mail: sandersb@ucalgary.ca

A. Vaseashta et al. (eds.), *Technological Innovations in Sensing and Detection of Chemical, Biological, Radiological, Nuclear Threats and Ecological Terrorism*,
NATO Science for Peace and Security Series A: Chemistry and Biology,
DOI 10.1007/978-94-007-2488-4_36, © Springer Science+Business Media B.V. 2012

way that our communication is kept safe nowadays. Alice, who works for the company waiting for your payment, generates a pair of numbers expressed as strings of binary digits, or “bits”. She sends you one string, which is called the public key, and she keeps the other string for herself, which is called the private key.

The message you plan to send, such as your credit card number, can also be expressed as a binary string. To send the message securely, you compute some function of both your message and Alice’s public key, and then you send her the calculated result. This function is considered to be hard-to-crack – without knowing the private key, inverting the function to reveal the message is believed to be beyond the capability of the eavesdropper’s computers within a reasonable timeframe.

When Alice receives the result of your computation, she uses her private key to decode the message from your result. Because Alice holds the corresponding private key, inverting the function to find the message, i.e. decoding, is easy for her. On the other hand, Eve knows the public key and the result but is unable to decode the message without having access to the private key.

We are prepared to take the risk that Eve could crack the code when making financial transactions, but what about more important information? Could a national secret be transmitted safely via a public channel in this way? There are three reasons not to do so. One reason is that some secrets have to be secrets for a long time, maybe forever. For many years, the power of computers has improved exponentially so Eve could record the message and wait for a more powerful computer to be created that would make cracking the code easy. Another risk is that Eve is so smart she devises a way to invert the function in a way that we have not figured out yet: the difficulty of breaking these codes is not proven but rather just assumed, albeit with strong evidence supporting this assumption.

The third reason to be wary with computationally-secure cryptography is the threat posed by a quantum computer: a scalable quantum computer, meaning a computer that can run quantum algorithms and can be made larger at a cost that grows only as a polynomial function of the computer’s size, renders these coding functions easy-to-crack. Thus, computationally-secure cryptography can be regarded as secure against a non-quantum computer, subject to the provisos above, but insecure against a computer that exploits the full potential of quantum mechanics.

The quantum computer could make today’s methods of cryptography instantly unsafe and thereby threatens public-key cryptography. On the other hand, a technique known as quantum key distribution also uses quantum technology but for the purpose of creating a shared key that is intended to be unbreakable no matter what kind of computer Eve possesses or what algorithms she knows. In other words quantum cryptography, which uses quantum key distribution, is information-theoretically secure – it cannot be broken by computational attacks – in contrast to today’s bounded-computational security where Eve is believed to have limited computational capability.

36.2 The Quantum Computing Threat

36.2.1 What Is a Quantum Computer?

Let us consider what defines a quantum computer [1] Defining the quantum computer is, in fact, rather subtle [2]. As we believe that quantum mechanics underpins all of science, then all computers are quantum, in the same sense that everything around us is quantum. Yet we are safe in regarding most things in the world as non-quantum so a better criterion is needed.

We know that the Heisenberg uncertainty principle [3] and entanglement [4], which are two of the distinguishing features of quantum mechanics, are negligible in our macroscopic world. Therefore, we could think of a quantum computer as a computing machine that exhibits quantum properties whereas existing computers do not. The problem with this definition is that modern computers use transistors, and transistors operate on quantum principles.

Perhaps the best definition of a quantum computer is as a computing machine that is described by quantum mechanics and can perform computations that a device built entirely out of non-quantum components could not do. This definition gets around the problem of a modern computer using a transistor: although we use transistors that operate on quantum principles, we could equally well build the computer out of billiard balls and achieve the same computational power, albeit more bulky, fragile and expensive. More technically, a quantum computer is a computing machine that can run any quantum algorithm.

36.2.2 What Will the Quantum Computer Look Like?

In the early days of computers, logical elements were built from different media: vacuum tubes, germanium or silicon. Similarly, various quantum computer media are available, and we are figuring out which one is the best.

One type of quantum computer technology uses light [5]. Light is quite versatile. Its degrees of freedom include polarization of the field, path of the beam, time of the pulse and more. One polarization state can be the logical zero state and the other polarization state the logical one, or a beam can take two possible paths labeled zero and one. Alternatively the pulse can be created early to make a zero or late to make a one. In this way, the state of the light field can encode a bit, and a quantum field can encode a superposition of zeros and ones, hence encode quantum information.

The electromagnetic field can be processed with passive optical elements, linear and parametric amplifiers, nonlinear phase modulations and photon counting with feedback to enable universal transformations of the field state. In this way, a quantum computer can be realized with light by exploiting one or more of light's degrees of freedom.

Electronic states of atoms provide another promising quantum information medium. A lower energy state can be a zero and an upper energy state a one, with other energy levels available for helping to prepare, control and read the state. The atoms can be neutral or ionized, with each case offering its own advantages and disadvantages. The electronic state can even be coupled with the nuclear state to take advantage of the long nuclear lifetimes for storage and memory [6].

Each approach and each medium has advantages and disadvantages. One medium may be better at storage, another better at effecting quantum gates and another better at readout. At this stage of research, we do not know which media will be winners and which will be losers. More investigation is required.

36.2.3 Hybridizing the Technology

We will probably find it easier not to overcome the disadvantages of one medium but, rather, combine several media to take advantage of the positives and avoid the negatives. To make such a hybrid device we need to transfer quantum information between media at opportune times. As mentioned above, coupling the electronic and nuclear degrees of freedom enables the quantum computer to exploit the advantages of both degrees of freedom. We can generalize this idea of combining the advantages of various media.

For example we could couple electronic and light degrees of freedom, which presents the advantage that light is the favored medium for communicating long distances and electrons are natural quantum information media in solid-state systems so may work well with existing computer chips. Another exciting possibility is using superconducting junctions in conjunction with microwave fields and using molecules to couple microwave and optical fields together to deliver scalable quantum information processing [7].

36.2.4 Scaling Up

The goal of scalability is to make a quantum computer work on a small scale – dozens of qubits and dozens of gate operations – and then to increase the size and number of operations efficiently. By ‘efficiently’ the increasing size and complexity should come at a cost that is no worse than a polynomial function of the size of the problem to be solved. This mathematical characterization of ‘efficiency’ is germane to the computer science notions of efficient *vs* hard problems.

Although quantum computer technology is improving steadily, we are still wrestling with getting small systems to work. Fortunately we do not have to make quantum computers as big as today’s computers to make quantum computers outperform today’s computers. For example, it might take the storage capacity of thousands of laptops in a network to break existing encryption algorithms in a few years, whereas storage capacity of only a 100 quantum kilobytes would break existing encryption algorithm in less than a second.

In a similar vein, a laptop computer operates at gigahertz speeds that completes billions of operations per second, but the quantum computer could operate as fast and complete the calculation in a few thousand cycles, namely in a millionth of a second. The important message is that, for certain problems, a quantum computer is so powerful that even a small prototype is more threatening to information security than combining thousands of the most powerful computers in existence today, if we continue to use the same means for encryption.

36.3 Quantum Cryptography to the Rescue

The quantum computer dashes our hope of information security using existing encryption schemes, but two alternatives restore this hope: new encryption schemes or using quantum cryptography [8]. Here we consider the second possibility, especially as the technology is viable now whereas quantum computing is still a futuristic technology.

36.3.1 Encryption Mechanism

Existing public-key encryption works by having sender Alice transmit to receiver Bob a public key and keeping her own private key. The goal of quantum key distribution is to have Alice and Bob generate an identical key: at the end of the generation process, Alice and Bob would each hold identical strings of bits using a public channel in such a way that omnipotent Eve is denied enough knowledge of this key so that she is incapable of learning anything about the messages encoded by this key using a ‘one-time pad’. Secret keys used with one-time pads are information-theoretically secure.

Sounds impossible? The uncertainty principle [3] traps Eve: if she wants to learn the shared random keys, her observation disturbs the system, and Alice and Bob can learn of her intrusion before they make the mistake of using the key to construct messages. Alice and Bob discuss publicly the noise in their keys and use a technique known as ‘privacy amplification’ to circumvent Eve from using a little knowledge to crack the codes.

There are four important catches though. One is that Alice and Bob need to authenticate the channel in advance; otherwise Eve could impersonate them. So far the only information-theoretically secure way to authenticate is to use a private channel. As information-theoretically secure authentication through a public channel has not been achieved, quantum key distribution is actually a key amplification scheme whereby the initial authentication key is amplified, but here we use the standard terminology of “distribution” rather than amplification and bear in mind the authentication problem.

The second catch is that Eve could just disrupt the communication by a denial-of-service attack whereby Alice and Bob do not have a working communication channel: Alice and Bob do not reveal their secrets but unfortunately also fail to communicate secrets with each other. Thus, security is maintained at the expense of not communicating at all.

The third catch is that current quantum key distribution technology is limited to distances of hundreds of kilometers. In principle, efficient quantum communication over any length scale is possible using quantum repeaters, but quantum repeaters are almost as hard to build as quantum computers.

The fourth catch is that equipment does not work perfectly, and Eve may know weaknesses that Alice and Bob do not. She thereby exploits a hidden weakness to learn the key without Alice and Bob realizing that weakness is exploited. Recently, though, entanglement-based quantum key distribution has been shown to offer another stunning advantage. Alice and Bob can check quantum correlations between their received quantum signals and thereby rule out attacks based on imperfect devices [9]. This kind of "device-independent security" is not possible in non-quantum cryptography.

36.3.2 State of the Art

Quantum key distribution works and is even available as a commercial technology, but its performance is not yet competitive with other key distribution technologies. This statement needs some qualification, though.

If existing key distribution is regarded as insecure, for any of the reasons given in Sect. 36.1, then even a poorly-performing but secure quantum key distribution system is infinitely better than a better-performing but insecure key distribution based on today's computationally-secure protocols. However, quantum key distribution needs to reach comparable levels of performance to existing schemes, i.e. achieve high levels of key generation rates, if quantum key distribution is to be regarded as viable in the sense that it can step in and replace existing key distributions with a small price to pay in terms of secure-bit distribution rates.

Due to loss, the key generation rate is sensitive to distance. Let us consider a 10-km distance, commensurate with urban-scale security. A rate of two million pulses of light generated per second is reasonable. For security, the average energy per pulse corresponds to one photon per five pulses. Yes, this means that most pulses are effectively empty (no energy), but which ones are empty is random.

Avalanche photodiodes are typically used as detectors, although better detectors are on the horizon. These photodiodes operate with a quantum efficiency of 0.1, a dark-count probability of 0.00001 and a gate time of 2 ns. The gate time is not reducible without causing deleterious after-pulses. With this technology, and after sifting, error correction, privacy amplification and authentication of the raw key, the resultant key rate is around 10 kHz.

This rate of 10 kHz is significantly slower than existing key distribution rates but can be dramatically improved by new detector technology and eventually faster software and integrating the processors on a single chip. New protocols and faster encoding on the pulses will also help to enhance performance.

36.3.3 Symmetric Encryption

For quantum key distribution to deliver information-theoretic security that is impervious to non-quantum computational attacks, the key should be employed in a Vernam cipher, or one-time pad. In practice, the Vernam cipher is off-putting because the length of the shared key needs to be as long as the message.

In practice, the key is used much more efficiently when employed in a symmetric encryption scheme such as the Advanced Encryption Standard, or AES, based on a substitution permutation network. As this method of encryption can be broken, the key is changed frequently; this is known as refreshing the key. Quantum key distribution can be used to generate the key for AES. Then the key rate is important because the length of the key per refresh and the rate of refreshing determines the level of communication security attained.

36.3.4 Long Distance

Because of losses of light during transmission, the secure key rate falls precipitously with increasing distance. Rather than send through optical fiber or free space over the earth, an alternative method is to use satellites to communicate. The great advantage of satellites is their long reach, on a planetary scale, without too much intervening air, which induces losses and scattering of the light. The effective distances, taking into account air density, is much shorter for satellite communication than for over-earth communication although the actual distances can be much larger.

Another strategy to beat the distance limit is to plug in quantum repeaters [10] along the path. Quantum repeaters are much harder to make than existing repeaters used in communication networks. The quantum repeater exploits entanglement-swapping processing of the resultant quantum states to deliver a fixed key rate at a cost that is only a polynomial function of overall distance, hence “efficient” in computer-science parlance. Much effort is now directed to quantum memories [11], which will store and release quantum states on demand, and are required for managing a quantum communication network with quantum repeaters.

36.4 Conclusions

Quantum cryptography is a rapidly developing technology that aims to deliver information-theoretically secure communication. In other words, quantum cryptography's goal is to circumvent the weakness of today's methods: an adversary with a sufficiently strong computer, obtained by recording and breaking the code in the future or by possessing a computer more powerful than envisaged or by building a quantum computer, could break the code. Quantum cryptography would eliminate the computational bound assumption built into today's belief in security.

Development of a quantum computer is slow but steady. Challenges exist in each of the candidate media for realizing quantum computation, but clever ways are being found to surmount the challenges such as hybridizing the media. Hybridization enables quantum information to be prepared or processed or read in various media depending on their strengths and transferred to another medium that is more suitable for one of the tasks. The outlook for quantum computing would be described as optimistic, but patience is required.

Quantum cryptography is a prudent tool to protect against quantum computing. Although the quantum computer will take a long time to build, quantum cryptography also requires a long time to bring its performance up to today's standards for non-quantum key distribution, including high key rates, developing an appropriate authentication protocol, and breaking the current distance barrier. Therefore, quantum cryptography needs to be studied and developed as a long-term strategic effort to protect communication against future communication-security threats.

Acknowledgements BCS has benefitted enormously from valuable discussions with W. Tittel and pedagogical feedback from L. Moore. This work is supported by Alberta's Informatics Circle of Research Excellence (*i*CORE), Canada's Natural Science and Engineering Research Council (NSERC), General Dynamics Canada, Canada's Networks of Centers of Excellence for the Mathematics of Information Technology and Complex Systems (MITACS), the Pacific Institute for Mathematical Sciences (PIMS), and the United States Army Research Office (ARO). BCS is a Fellow of the Canadian Institute for Advanced Research (CIFAR).

References

1. Knill E (2010) Physics: quantum computing. Nature 463:441–443
2. Bartlett SD, Sanders BC (2003) Requirement for quantum computation. J Mod Opt 50(15–17):2331–2340
3. Heisenberg W (1927) Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Phys 43:172–198. English translation; Wheeler JA, Zurek H (1983) Quantum theory and measurement. Princeton University Press, Princeton, pp 62–84
4. Schrödinger E (1935) Discussion of probability relations between separated systems. Proc Camb Philos Soc 31:555–563; (1936) 32:446–451
5. O'Brien JL (2007) Optical quantum computing. Science 318(5856):1567–1570
6. Childress L, Gurudev Dutt MV, Taylor JM, Zibrov AS, Jelezko F, Wrachtrup J, Hemmer PR, Lukin MD (2006) Coherent dynamics of coupled electron and nuclear spin qubits in diamond. Science 314(5797):281–285

7. André A, DeMille D, Doyle JM, Lukin MD, Maxwell SE, Rabl P, Schoelkopf RJ, Zoller P (2006) A coherent all-electrical interface between polar molecules and mesoscopic superconducting resonators. Nat Phys 2:636–642
8. Gisin N, Ribordy G, Tittel W, Zbinden H (2002) Quantum cryptography. Rev Mod Phys 74(1):145–195. doi:dx.doi.org
9. Acin A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V (2007) Device-independent security of quantum cryptography against collective attacks. Phys Rev Lett 98:230501–230505
10. Briegel HJ, Dür W, Cirac JI, Zoller P (1998) Quantum repeaters: the role of imperfect local operations in quantum communication. Phys Rev Lett 81:5932–5935
11. Lvovsky AI, Sanders BC, Tittel W (2009) Quantum optical memory. Nat Photonics 3(12): 706–714