Secure Multi-Agent Quantum Communication: Towards the Most Efficient Scheme (A Pedagogical Remark)

Olga Kosheleva and Vladik Kreinovich
University of Texas at El Paso
El Paso, TX 79968, USA
olgak@utep.edu, vladik@utep.edu

Abstract

In many economic and financial applications, it is important to have secure communications. At present, communication security is provided mostly by RSA coding, but the emergent quantum computing can break this encoding, thus making it not secure. One way to make communications absolutely secure is to use quantum encryption. The existing schemes for quantum encryption are aimed at agent-to-agent communications; however, in practice, we often need secure multi-agent communications, where each of the agents has the ability to securely send messages to everyone else. In principle, we can repeat the agent-to-agent scheme for each pair of agents, but this requires a large number of complex preliminary quantum communications. In this paper, we show how to minimize the number of such preliminary communications – without sacrificing reliability of the all-pairs scheme.

1 Need for Secure Group Communications

Need for secure communications. In e-commerce and e-finance, it is important to preserve privacy and confidentiality of all the transactions. In other words, we need to make sure that e-commerce and e-finance are based on a secure communication scheme.

How communications are made secure now. At present, secure communications are based mostly on the RSA algorithm; see, e.g., [1]. In this scheme, the communicator A selects two large prime numbers P_1 and P_2 that he/she keeps private, and releases their product $P = P_1 \cdot P_2$ into the public domain. This public code P can then be used any anyone to encode the messages they send to A. To decode the messages, one needs to know the factors P_1 and P_2. Since A knows these factors, A can decode these messages.

The security of this encoding scheme is provided by the fact that no efficient algorithm is known for factoring large integers – and RSA algorithms use 100-digit and longer factors P_i. In principle, we can factor an integer P by trying all possible prime numbers $p \le \sqrt{P}$. This works for small P, but for a number with 100 decimal digits, testing all prime numbers $\le \sqrt{P}$ requires $\sqrt{10^{100}} = 10^{50}$ computational steps – which make this procedure much longer than the lifetime of the Universe.

Why we need quantum communications. For factoring large integers on the usual computers, no efficient algorithm is known. However, it is known that if we consider quantum computers, then factoring large integers becomes feasible; see, e.g., [4, 5, 6, 8]. At present, we do not yet have quantum computers powerful enough to decode the usual RSA message, but engineers are designing more and more powerful quantum computers, and sooner or later RSA-encoded communications will no longer be secure.

Good news is that the same quantum physics that makes RSA not secure also provides us with a secure way to communicate, known as quantum cryptography; see, e.g., [3, 4, 8]. In contrast to quantum computing, which is mostly the thing of the future, quantum cryptography is a practical scheme, it has been used for decades already.

In this scheme – it is described in some detail in the appendix – two agents that want to communicate in the future exchange quantum signals. By analyzing these signals, they come up with a sequence $s = s_1 s_2 \ldots s_n$ of bits (0s and 1s) s_1, s_2, $\ldots$, s_n which they both know but which is not known to anyone else.

This sequence of 0s and 1s can then be used as *one-time pad*. Namely, if one of the two agents needs to send a message $m = m_1 m_2 \ldots m_n$ consisting of bits $m_1, \ldots, m_n$, then:

- the sender computes and send the encoded signal $e = s \oplus m$, where

$$(s \oplus m)_i \stackrel{\text{def}}{=} s_i \oplus m_i$$

  and $\oplus$ means addition modulo 2 – which differs by the usual addition of bits only when $s_i = m_i = 1$, in which case $1 \oplus 1 = 0$;

- the receiver, after getting the signal, reconstructs the original message as $m = s \oplus e$.

Indeed, for addition modulo 2, we always have $a \oplus a = 0$, hence

$$s \oplus e = s \oplus (s \oplus m) = (s \oplus s) \oplus m = 0 \oplus m = m.$$

Once the message is sent, the pair of agents again perform preliminary quantum communications and generate a new one-time pad, etc.

Need for multi-agent communications. In economic and financial applications, it is often important to have multi-agent communications. Such communications are especially important for decentralized schemes (like blockchain-based

schemes), where each record of financial transactions is stored in many different locations.

In such a scheme, we have several agents. Let us denote the overall number of agents who need to communicate with each other by N. The system should be ready for each of these agents $A_1, \ldots, A_N$ to send communication to everyone else.

Using pairwise communication scheme for multi-agent communication: a straightforward idea. In principle, we should be ready for communications between each pair of agents. For N agents, there are $\frac{N \cdot (N-1)}{2}$ such pairs. So, a straightforward idea is to repeat the quantum-communication protocol for each pair (A_j, A_k) and thus get $\frac{N \cdot (N-1)}{2}$ one-time pads $s^{(j,k)}$ corresponding to these pairs.

If agent A_j needs to send a message to all the other agents A_1, A_2, $\ldots$ A_{j-1}, A_{j+1}, $\ldots$, A_n, this agent will use a one-time pad $s^{(j,k)}$ to communicate with the k-th agent.

Can we do it more efficiently? The above scheme requires $\frac{N \cdot (N-1)}{2}$ preliminary quantum communications – and preliminary quantum communications are the most complex part of the general quantum communication protocol. Can we have fewer preliminary quantum communications?

We can do it, but at the expense of reliability. One possibility to have a more efficient multi-communication scheme is to select one agent as a hub and set up one-time pads between this selected agent and everyone else. This way, we have a secure communication channel between the hub agent and every other agent.

Then, if an agent A_j wants to transmit a message to everyone else, this agent first sends this message to the hub agent, and then the hub agent sends it to everyone else.

This scheme is efficient – it needs only $N-1$ preliminary quantum communications – but it is not as reliable as the original scheme: indeed, if the hub agent is not functioning well (which happens), then the original scheme still works while the hub scheme does not. So, we arrive at the following question.

Can we have an efficient scheme without decreasing reliability: formulation of the problem and our answer. Can we have an efficient scheme without decreasing reliability?

In this paper, we show that this is indeed possible: namely, we provide a multi-agent communication scheme which is maximally efficient and at the same time as reliable as the all-pairs scheme.

2 Towards the Optimal Multi-Agent Quantum Communication Protocol

Lower bound on the number of preliminary quantum communications. The only way to have secure communications is to have a secure one-time pad provided by preliminary quantum communications. A pair of agents may get a one-time pad either directly from the mutual preliminary quantum communication, or by somehow combining one-time pads provided by other pairs.

Each agent can thus securely communicate only with agents which are either directly connected with this agent by preliminary quantum communications, or connected by a chain in which each agent is connected to the next one by preliminary quantum communications between them.

Since we want each agent to be able to securely communicate with any other agent, every two agents must be connected by such a chain. We start with a single agent. At each point, we have a set of agents that can be thus connected with the agent A_1. Each new preliminary quantum agent-to-agent communication adds may add one agent to this list – if it connects this new agent with one of the agents which are already on this list. Thus, each new comunication adds no more than one new agent to this list. We start with a single agent, so after performing k agent-to-agent preliminary quantum communications, we add no more than k agents to the original list, and thus, we have $\le k+1$ agents connected to A_1. We want to have all N agents connected to A_1, so we must have $N \le k+1$ and thus, $k \ge N-1$.

This is the desired lower bound: to enable each agent to securely communicate with every other agent, we need to perform at least $N-1$ agent-to-agent preliminary quantum communications.

Towards a scheme that implements this lower bound. Let us show that it is possible to have a secure communication protocol that requires exactly $N-1$ agent-to-agent preliminary quantum communications. Due to what we have just shown, this algorithm is the most efficient one – in the sense that it requires the smallest possible number of agent-to-agent preliminary quantum communications.

Let one of the agents – let us denote this agent by A_1 – perform the preliminary step of quantum communication with every other agent $A_1, \ldots, A_m$. As a result, for each $j = 2, 3, \ldots, N$, both A_1 and A_j know a one-time pad $s^{(j)}$ – which no one else knows.

Then, A_1 uses a random number generator to generate a random string s and then sends by an open channel, to each agent A_j, a string $s \oplus s^{(j)}$. Each agent can reconstruct s as $(s \oplus s^{(j)}) \oplus s^{(j)}$. Thus, all N agents now have the same one-time pad s that they can use for the future multi-agent communication.

Acknowledgments

This work was partially supported by the US National Science Foundation via grant HRD-1242122 (Cyber-ShARE Center of Excellence).

References

[1] Th. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, MIT Press, Cambridge, Massachusetts, 2009.

[2] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics*, Addison Wesley, Boston, Massachusetts, 2005.

[3] O. Galindo, V. Kreinovich, and O. Kosheleva, "Current quantum cryptography algorithm is optimal: a proof", *Proceedings of the IEEE Symposium on Computational Intelligence for Engineering Solutions CIES'2018*, Bengaluru, India, November 18–21, 2018.

[4] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[5] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, New Mexico, November 20–22, 1994.

[6] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Sci. Statist. Comput.*, 1997, Vol. 26, pp. 1484-ff.

[7] K. S. Thorne and R. D. Blandford, *Modern Classical Physics: Optics, Fluids, Plasmas, Elasticity, Relativity, and Statistical Physics*, Princeton University Press, Princeton, New Jersey, 2017

[8] C. P. Williams and S. H. Clearwater, *Ultimate Zero and One*, Copernicus, New York, 2000.

A Quantum Communication: A Brief Reminder

Quantum background: a brief reminder. In quantum mechanics (see, e.g., [2, 7]) each bit, in addition to the usual two states 0 and 1 (which are denoted by $|0\rangle$ and $|1\rangle$), it is also possible to have a superposition $c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$, where c_i are complex numbers for which $|c_0|^2 + |c_1|^2 = 1$. If in this state, we try to find out whether we have 0 or 1, we get 0 with probability $|c_0|^2$ and 1 with probability $|c_1|^2$.

In particular, the standard quantum communication algorithm uses the following two states:

$$|0'\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$$

and

$$|1'\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle.$$

To reconstruct the state, we need to use a measuring instrument. A measuring instrument can be tuned:

- either to detect the usual states $|0\rangle$ and $|1\rangle$ (we will denote this by $+$)
- or to detect the quantum states $|0'\rangle$ and $|1'\rangle$ (we will denote this tuning by $\times$).

In this case:

- If the measuring instrument's tuning matches the signal – e.g., if the signal is $|0\rangle$ or $|1\rangle$ and the instrument is tuned on $|0\rangle$ or $|1\rangle$ – then the instrument reconstructs the original signal.
- On the other hand, if there is a mismatch between the instrument's tuning and the signal – e.g., if the signal is $|0'\rangle$ or $|1'\rangle$ while the instrument is tuned on $|0\rangle$ or $|1\rangle$ – then, irrespective of the signal, the instrument returns 0 or 1 equal with probability 1/2, and the original signal is lost.

The actual quantum communication scheme. The sending agent A runs, several times, a random number generator that generates 0 or 1 with equal probability 1/2. As a result, we get a multi-bit sequence $r_1 \ldots r_c$. Then, A runs the same random number generator n more times, generating c more bits $t_1 \ldots t_c$. For each i:

- if $t_i = 0$, then A uses the $+$ tuning to send the signal t_i, i.e., sends $|0\rangle$ if $r_i = 0$ and sends $|1\rangle$ if $r_i = 1$;
- if $t_i = 0$, then A uses the $\times$ tuning to send the signal t_i, i.e., sends $|0'\rangle$ if $r_i = 0$ and sends $|1'\rangle$ if $r_i = 1$.

The receiving agent B also runs its own random random number generator, generating yet another sequence $b_1, \ldots, b_c$ of c bits. Then, for each i:

- if $b_i = 0$, then B uses the $+$ tuning to measure the received signal, and
- if $b_i = 1$, then B uses the $\times$ tuning to measure the received signal.

For those bits for which there is a match between the signal and the tuning, i.e., for which $t_i = b_i$, B gets exactly the original signal r_i. For every other index i, the result of B's measurements is 0 or 1 with probability 1/2 – and the original signal r_i is lost.

Now, A openly sends, to B, all the bits t_i. In half of the cases, b_i coincides with t_i. The agent B sends, to A, the list of such i's. For these i's – and there are $c/2$ such i's – both agents know the value r_i. The sequence of all these common values is the desired one-time pad of length $n \approx c/2$ that A and B can now use to securely communicate.

Why is this scheme secure. The security of this scheme is based on the fact that an eavesdropped does not know which tuning was used for each bit i. If the eavesdropper tries to measure the signal, it will thus, in half of the cases, use the wrong tuning, and thus, the original signal will be lost – i.e., replaced with a random bit.

As a result, even for some of the bits for which $t_i = b_i$, due to this replacement, the bits measured by B will be, in general, different from r_i. To detect eavesdropping, A also sends to B, by open channel, some of the bits r_i corresponding to the cases when $t_i = b_i$.

- If for some i, B measured a bit different from r_i, this means that there was an eavesdropper.
- If all the test-bits r_i are reproduced by B exactly – this means that the channel was secure, there was no eavesdropping.