QUANTUM COMPUTING 9.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

November 17, 2002

9. QUANTUM CRYPTOGRAPHIC PROTOCOLS

A variety of quantum cryptographic protocols have already been developed for basic cryptographic tasks. They will be presented in this section.

The key issue is whether for basic cryptographic tasks there exist unconditionally secure quantum cryptographic protocols.

BASIC CRYPTOGRAPIC PROTOCOLS

Cryptographic protocols are specifications how two parties, Alice and Bob, should prepare themselves for a communication and how they should behave during a communication in order to achieve their goal and be protected against an adversary.

In **coin-flipping protocols** Alice and Bob can flip a coin over a distance in such a way that neither of them can determine the outcome of the flip, but both can agree on the outcome in spite of the fact that they do not trust each other.

In **bit commitment protocols** Alice can choose a bit and get committed to it in the following sense: Bob has no way of learning Alice's commitment and Alice has no way of changing her commitment.

Alice commits herself to a bit x using a *commit*(x) procedure, and reveals her commitment, if needed, using *open*(x) procedure.

In **1-out-2 oblivius transfer protocols** Alice transmits two messages m_1 and m_2 to Bob who can chose whether to receive m_1 or m_2, but cannot learn both, and Alice has no idea which of them Bob has received.

In **standard oblivious transfer protocols** Alice can send a message to Bob in such a way that Bob receives the message with probability $\frac{1}{2}$ and a garbage with probability $\frac{1}{2}$. Moreover, at the end Bob knows whether he got a message or a garbage, but Alice has no idea which of them Bob has received.

CLASSICAL COIN-FLIPPING (BY PHONE) PROTOCOL

The history of cryptographic protocols started with the following Blum's coin-flipping protocol (1981):

Protocol 0.1 (Coin-flipping by telephone)

1. *Alice chooses two large primes p, q, sends Bob $n = pq$, and keeps p, q secret.*
2. *Bob chooses a random number $y \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ and sends Alice $x = y^2 \bmod n$.*
3. *Alice computes four square roots $(x_1, n - x_1)$ and $(x_2, n - x_2)$ of x. (Alice can compute them because she knows p and q.)*

   Let $x'_1 = \min\{x_1, n - x_1\}$, $x'_2 = \min\{x_2, n - x_2\}$. Since $y \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor)\}$, either $y = x'_1$ or $y = x'_2$.

   Alice then guesses whether $y = x'_1$ or $y = x'_2$ and tells Bob her choice (for example, by reporting the position and the value of the leftmost bit in which x'_1 and x'_2 differ).
4. *Bob tells Alice whether her guess was correct (head) or not correct (tail).*

Later, if necessary, Alice can reveal p and q, and Bob can reveal y.

QUANTUM COIN-FLIPPING PROTOCOL

Alice's random bits	1	0	1	1	0	1	1	0	0	1	1
Alice polarization choice						rectilinear					
photons sent	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
Bob's observable	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$
Bob's table for $\mathcal{B}$	1			1			1		0	1	
Bob's table for $\mathcal{D}$		1	1					0			0
Bob's guess of Alice's pol.						rectilinear					
Alice's message						you WON					
Alice's original bits	1	0	1	1	0	1	1	0	0	1	1
comparison with $\mathcal{B}$	Y			Y			Y		Y	Y	
comparison with $\mathcal{D}$		N	Y					Y			N

Figure 1: Illustration of a quantum coin-flipping protocol

1. Alice randomly chooses a sequence of bits (for example 1000) and a polarization (rectilinear or diagonal—standard or dual). Finally, Alice sends the resulting sequence of the polarized photons to Bob.
2. Bob chooses, for each received photon, randomly, an observable, $\mathcal{B}$ or $\mathcal{D}$, and measures the incoming photon. He records the result into two tables—one for observable $\mathcal{B}$ and the second for observable $\mathcal{D}$. Since some photons can get lost during the transmissions, there can be holes in both tables. At the end of all transmissions, Bob makes a guess whether Alice chosed rectilinear or diagonal polarization and announces his guess to Alice. He is to win if the guess is correct; to lose otherwise.
3. Alice tells Bob whether he won or lost by telling him the polarization she choosed. She can certify her claim by sending Bob the random sequence of bits she choosed at Step 1.
4. Bob verifies Alice's claim by comparing his records in the table for the basis she claims to choose. There should be a perfect agreement with the entries in that table and no correlation with the other table.

CAN BOB OR ALICE CHEAT?

1. Bob is not able to cheat.

   Bob would be able to "cheat" only would he be able to guess with probability $> \frac{1}{2}$, on the base of photons he received, which basis (polarization) Alice has chosen (what contradicts physical laws).

2. Alice could potentially cheat only in Step 1 or in Step 3.

   - **Alice cannot cheat in Step 3**

     In order to cheat she would need to send sequence of bits matching the entries of Bob's table for two possible bases (polarizarions). The probability she keeps making correct guess about Bob's measurement goes fast to 0.

   - **Alice CAN CHEAT at Step 1 by making a clever use of entanglement!**

     In Step 1, instead of sending a sequence of isolated photons, polarized in one of two ways, she produces pairs of photons, each in the state

     $$\frac{1}{2}(|01\rangle + |10\rangle),$$

     she sends to Bob one photon of each pair and stores the other one.

     After Bob's guess, in Step 2, she measures her photon in the opposite basis as was Bob's guess. By that she receives a sequence of bits perfectly correlated with Bob's table corresponding to the basis he did not choose as his guess in Step 2. Alice then announces her sequence in Step 3.

QUANTUM GAMBLING

The question whether there is (unconditionally) secure quantum coin tossing protocol remains open.

The existence of unconditionally secure protocol has been shown for the so-called **quantum gambling** problem.

Quantum gambling — the rules of gambling

Alice and Bob are gamblers. Alice has a particle and two boxes, A and B, to store the particle. Let $|a\rangle$ ($|b\rangle$) denote the quantum state for the particle to be in the box A (B).

Step 1 Alice prepares the particle in some state $|\psi\rangle$ and sends the box B to Bob.

Step 2 Bob has two choices:

1. To open the box B. If he finds there the particle, Alice should pay him a coin; otherwise Bob pays Alice a coin.
2. To ask Alice to send him also the box A. Bob then checks whether
$$|\psi\rangle = |\psi_0\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle).$$
If yes, Bob pays Alice a coin; otherwise Alice pays him R coins. (R is here a "security parameter". For the case $R = 1$ we have a coin tossing protocol.)

Quantum gambling — a protocol

Alice's strategy: To prepare $|\psi\rangle$ as $|\psi_0\rangle$ — as defined above.

Bob's strategy: After receiving the box B, he performs the unitary mapping

$$|b\rangle \rightarrow \sqrt{1-\theta(R)}|b\rangle + \sqrt{\theta(R)}|b'\rangle = |\psi'\rangle,$$

where $\langle b \,|\, b'\rangle = 0$ and $\theta(R)$ is a "splitting parameter", to be specified later.

Afterwards, Bob performs the projection measurement on $|\psi'\rangle$, with respect to the basis $\{|b\rangle, |b'\rangle\}$. If he finds, by doing that, that the particle is in the box B, he then asks Alice to pay him a coin; otherwise he asks her for the box A and verifies whether she prepared the state $|\psi_0\rangle$. If yes, he pays a coin; otherwise Alice pays him R coins.

Quantum gambling — security

Since this is a zero-sum game, and an expectation value of Alice's gain is clearly nonnegative (independently of Bob's strategy), the expectation value of Bob's gain, G_B, has to be nonpositive (independently of Alice's strategy).

It has been shown that at a proper choice of $\theta(R)$ (roughly $\frac{1}{\sqrt{2R}}$), $G_B \geq \delta(R)$, (with $\delta(R)$ approximately $-\sqrt{\frac{2}{R}}$), where $\lim_{R\rightarrow\infty} \delta(R) = 0$.

QUANTUM BIT COMMITMENT PROTOCOLS

In 1993, Brassard, Crépeau, Jozsa and Langlois develop a quantum bit commitment protocol, the so-called BCJL-protocol and provided a proof that it is unconditionally secure.

In 1995 a flaw in the proof of unconditional security of the BCJL-protocol was discovered.

In 1996 two proofs were given that there is no unconditionally secure quantum bit commitment protocol.

The point is that a variant of cheating strategy demonstrated for our quantum coin tossing protocol, a clever misuse of entanglement by Alice, can be always used, in a modified form.

The fact that there is no unconditionally secure quantum bit protocol can be seen as a bad news because bit commitment is a primitive on which many cryptographic protocols can be built.

BCJL — PROTOCOL

Let $\varepsilon > 0$ (be an upper bound on error rate of quantum channel).

Protocol 0.2 (commit (x)**)**

1. Bob chooses a generator matrix G of a binary linear (n, k, d)-code C such that $\frac{d}{n} > 10\varepsilon$ and $\frac{k}{n} = 0.52$ and announces it to Alice.
2. Alice chooses:
   - 2.1. a random string r of length n and announces it to Bob;
   - 2.2. a random k-bit vector s, such that $r \cdot c = x$, where $c = sG$;
   - 2.3. a random sequence b of length n of the polarizations, $\mathcal{B}$ or $\mathcal{D}$, and sends to Bob a sequence of n photons with the polarization of the ith photon $P_{b_i}(c_i)$, where $P_0(0) = 0°$, $P_0(1) = 90°$ and $P_1(0) = 45°$, $P_1(1) = 135°$.
3. Bob chooses a random string b' of n bits and measures the ith photon according to the basis $M(b'_i)$, where $M(0) = \mathcal{B}$ and $M(1) = \mathcal{D}$. Let c' be the n-bit vector where c'_i is the result of the measurement of the ith photon.

Alice keeps the bit x and vectors c and b secret, until the opening takes place, and Bob keeps vectors b' and c' secret.

Protocol 0.3 (open (c, b, x, c', b')**)**

1. Alice sends c, b and x to Bob.
2. Bob verifies that c is a codeword of C and computes $B = \Sigma_{\{i \,|\, b'_i = b_i\}} \frac{c_i \oplus c'_i}{n/2}$, in order to verify that the error rate is under the limit of those pairs of outgoing and measured bits that were polarized/measured by the same basis.
3. if $B < 1.4\varepsilon$ and $x = r \cdot c$, then Bob accepts, otherwise Bob rejects.

QUANTUM OBLIVIOUS TRANSFER PROTOCOLS I

It is easy to design a simple and perfectly secure QOTP provided transmissions and detectors are perfect and no party cheats.

Protocol 0.4 (Ideal one-photon standard QOTP)

1. Alice chooses a bit b and sends it to Bob through one photon encoded using a randomly chosen basis—standard or dual.
2. Bob measures the photon with respect to a randomly chosen basis—standard or dual.
3. Alice lets Bob know the basis she chosed.

At the end Bob has a 50% chance to know b for sure and he knows whether he knows b for sure. Alice has no information whether Bob knows the bit for sure.

Problems with this protocol.

1. Imperfect devices (Alice's source, a noisy channel, or Bob's detector) could much affect the probability of success of Bob's measurement.
2. Bob could "cheat" by making his measurement in the so called Breidbart basis

$$\mathcal{B}_0 = \{\theta_0, \theta_1\},$$

where

$$\theta_0 = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle; \quad \theta_1 = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$$

This way he could learn b with large probability $\cos^2\frac{\pi}{8} \approx 0.85$.

1-out-of-2 QOTP

Parameter agreeing phase

Alice and Bob agree during a communication on parameters:

ε — the expected error rate;

α — the fraction of photons Bob detects successfully;

n — the security parameter; number of photons to be transmitted;

C — a binary linear error-correcting code capable of correcting, well, n-bit words transmitted with the expected error rate ε.

Transmission phase

Alice chooses a random binary string of length $\frac{2n}{\alpha}$ and sends each of the bits through a polarized photon using randomly either the standard or dual polarization basis.

Measurement phase

Bob measures each incoming photon by a randomly chosen basis ($\mathcal{B}$ or $\mathcal{D}$) and records the basis chosen and the results of the measurements into tables.

Bob expects to receive $2n$ photons. If he gets more, he ignores additional bits. if less, he adds randomly chosen bits.

At the end Bob reports to Alice arrival times of all $2n$ photons , but neither the bases nor the results of his measurements.

Bases-revealing phase.

Alice tells Bob, through a public channel, the bases she used to encode her random sequence of bits.

Design of good and bad sequences phase.

Bob partitions his $2n$ bits into two sequences, each of length n.

Into the "good" sequence he puts as much as possible of bits he obtained when he used the correct basis for measurements.

The "bad" sequence contains as much as possible of other bits.

Bob then tells Alice indices of bits of both sequences, but not which one is "good" and which is " bad".

At this point Bob shares with Alice a binary word of his good sequence (with respect to an expected error rate not greater than ε). Concerning the bad sequence, Bob shares almost nothing with Alice.

Of course, the above process is not ideal. There can be some errors introduced by the fact that Bob did not use exactly n times the correct basis for his measurement . However, the number of errors introduced this way should be negligible, with respect to the expected noise in the transmissions.

Error-correction phase.

Using the code C, Alice computes syndromes of her words corresponding to the good and bad sequence of Bob, and sends syndromes to Bob, who uses them to perform error correction on his good and bad sequences.

Privacy amplification phase.

Alice chooses randomly two subsets of bits, one from her "good" and one from her "bad" sequence and computes their parities. She let Bob know the "addresses" of bits she chose, but not their values.

This way Bob can compute the parity of the corresponding subset of his good sequence, but he will have no idea about the parity Alice obtained for the subset of bits corresponding to his bad sequence. Alice knows she has no idea which one Bob knows.

Let x_0, x_1 be parity bits Alice knows and $\bar{c}$ be the parity bit Bob knows.

Oblivious transfer phase

1. Bob tells Alice whether or not $c = \bar{c}$.
2. If $c = \bar{c}$, then Alice sends Bob bits $x_0 \oplus b_0$ and $x_1 \oplus b_1$, in this order. If $c \neq \bar{c}$, Alice sends Bob bits $x_0 \oplus b_1$ and $x_1 \oplus b_0$, again in the given order.
3. Bob computes b_c out of two bits he got from Alice.

QUANTUM SECRET SHARING

There is a simple method how Alice can teleport a (secret) qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob and Charles in such a way that they have to cooperate in order to have $|\phi\rangle$.

The basic idea is that Alice couples a given particle P in the state $|\phi\rangle$ with the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ of three particles P_a, P_b and P_c she shares with Bob and Charles and then performs a measurement on the state of particles P and P_a, with respect to the Bell basis $\{\Phi^{\pm}, \Psi^{\pm}\}$. Since

$$\begin{aligned}|\phi\rangle|\psi\rangle \;=\; & \frac{1}{2}(|\Phi^+\rangle(\alpha|00\rangle + \beta|11\rangle) + |\Phi^-\rangle(\alpha|00\rangle - \beta|11\rangle) \\ & +|\Psi^+\rangle(\beta|00\rangle + \alpha|11\rangle) + |\Psi^-\rangle(-\beta|00\rangle + \alpha|11\rangle)),\end{aligned}$$

the outcome of the measurement is that particles P_b and P_c get into one of the states

$$\frac{1}{\sqrt{2}}(\alpha|00\rangle+\beta|11\rangle), \frac{1}{\sqrt{2}}(\alpha|00\rangle-\beta|11\rangle), \frac{1}{\sqrt{2}}(\beta|00\rangle+\alpha|11\rangle), \frac{1}{\sqrt{2}}(-\beta|00\rangle+\alpha|11\rangle)$$

and Alice gets two bits to tell her about which of these four cases happened. However, neither Bob nor Charles has information about which of these four states their particles are in.

Bob now performs a measurement of his particle with respect to the dual basis. He gets out of it one bit of information and Charles's particle P_c gets into one of 8 possible states , which is uniquely determined by bits both Alice and Bob got as the results of their measurements , and which can be transformed into the state $|\phi\rangle$ using one or two applications of Pauli matrices.