Generalized Oblivious Transfer Protocols Based on Noisy Channels

Valeri Korjik[1] and Kirill Morozov[2]

[1] Section of Telecommunications, IPN CINVESTAV, AV. IPN No. 2508 ESQ Ticoman, Col. San Pedro, Zacatenco, C.P. 07000, Mexico D.F., Mexico
Fax: 5747-7088, Tel.: 5747-3770
vkorjik@mail.cinvestav.mx

[2] Telecommunications Security Department, State University of Telecommunications, Moika 65, St. Petersburg, 191186, Russia
Fax: 312-10-78, Tel.: 315-83-74
kirill@fem.sut.ru

Abstract. The main cryptographic primitives (Bit Commitment (BC) and Oblivious Transfer (OT) protocols) based on noisy channels have been considered in [1] for asymptotic case. Non-asymptotic behavior of BC protocol has been demonstrated in [2]. The current paper provides stricter asymptotic conditions on Binary Symmetric Channel (BSC) to be feasible OT protocol proposed in [1]. We also generalize this protocol using different encoding and decoding methods that require to regain formulas for Renyi entropy. Non-asymptotic case (finite length of blocks transmitted between parties) is also presented. Some examples are given to demonstrate that these protocols are in fact reliable and information-theoretically secure. We also discuss the problem – how to extend $\binom{2}{1}$-OT protocol to $\binom{L}{1}$-OT protocol and how to arrange BSC connecting parties. Both BC and OT protocols can be used as components of more complex and more important for practice protocols like "Digital cash", "Secure election" or "Distance bounding".

1 Introduction

The simplest of cryptographic protocols that are sufficient to accomplish many complex protocols can be called *cryptographic primitives*. One of such primitives is so called *Oblivious Transfer* ($\binom{2}{1}$-OT). According to this primitive, one party Alice has two secret strings b_0 and b_1, and another party Bob wants to learn b_c, $c = 0, 1$ for a secret bit c of his choice. Alice is willing to collaborate provided that Bob does not learn any information about $b_{\bar{c}}$ and Bob will only participate if Alice cannot obtain information about c. (We note that $\binom{2}{1}$-OT protocol is a particular case of

$\binom{L}{1}$-OT protocol, where Alice has L secret strings and Bob wants to learn only one of them but in a manner to be completely unknown for Alice which of L secrets Bob receives.)

The algorithms to perform $\binom{2}{1}$-OT protocol (OT for brevity) have been considered in [3]. To be secure they require limitation on parties' computing power, so they are *computational secure*. This paper (following the idea of [1]) considers a scenario where both Alice and Bob have no limitation on their computing power. It would be impossible to accomplish this protocol without another assumption. Such an extra assumption we make is that Alice and Bob are connected by *Binary Symmetric Channel* (BSC_φ) with *bit error probability* φ.

In [1] the following OT information-theoretically secure protocol based on BSC_φ connecting parties was proposed. Alice and Bob agree on a binary linear code C that has constructive algorithm to correct maximum possible number of errors. It is also assumed that there exist noiseless channels to exchange messages between Alice and Bob. After this *initialization phase* Alice and Bob have to perform the following *base protocol*:

1. Alice picks randomly $2n$ bits x_i, $i = 1, 2, \ldots, 2n$, repeats twice each of them and sends $4n$-bit string to Bob over BSC_φ.
2. Bob accepts each received pair if and only if it is either 00 or 11, otherwise he rejects it. The accepted pairs are transformed in $2n$-bit string x'_i, $i = 1, 2, \ldots, 2n$, following the trivial decision rule: $00 \rightarrow 0$, $11 \rightarrow 1$.
3. Bob selects the desired bit string b_c, where $c = 0$ or 1 and picks two disjoint subsets I_0, I_1 of the set $(1, 2, \ldots, 2n)$, satisfying the conditions: $|I_0| = |I_1| = n$, I_c contains only the numbers of positions corresponding to accepted bits in the step 2 of protocol.
4. Bob sends I_0 and I_1 to Alice over noiseless channel.
5. Alice computes the *check strings* (*or syndromes*) s_0, s_1 to original n-bit substrings x_{I_0}, x_{I_1} using the known check matrix of the code C. Then Alice sends these check strings to Bob over noiseless channel.
6. Alice picks random n-bit string m, computes $\hat{b}_0 = b_0 \oplus h_m(x_{I_0})$, $\hat{b}_1 = b_1 \oplus h_m(x_{I_1})$, where "$\oplus$" is bitwise mod 2 addition, $h_m(\ldots)$ is a hash function taken from universal$_2$ class [4] given known m and sends to Bob m, $\hat{b}_0$ and $\hat{b}_1$ over noiseless channel.
7. Bob corrects errors on x'_{I_c} using s_c, recovers x_{I_c} and computes the desired secret $b_c = \hat{b}_c \oplus h_m(x_{I_c})$.

If Alice is honest (that means that she follows to this protocol) and the channel connecting parties is in fact BSC_φ without memory, then Alice has no chances to

distinguish which of two subsets I_0 or I_1 corresponds to c. It is more complex to prove that Bob does not learn any information about $b_{\bar{c}}$ and on the other hand that Bob following honestly to the protocol given above is able to learn b_c with high probability. Solution to these problems will be considered in the next Sections.

The paper is organized as follows. In Section 2 the condition on the bit error probability φ to provide both reliability and security of OT protocol is presented. We also give there an optimization of this parameter to provide more efficient protocol. Section 3 contains several generalizations of the base protocol and a description of their asymptotic behavior. In Section 4 we give the main non-asymptotic formulas to estimate reliability and security of the base protocol and consider also the problem how to optimize its parameters. In Section 5 we summarize the main results and consider possible transformations of $\binom{2}{1}$-OT protocols to $\binom{L}{1}$-OT protocol and discuss an arrangement of BSC_φ between parties.

2 Feasibility of base OT protocol in asymptotic case

First of all we note that if Alice and Bob run the base protocol described above the following probabilities are true:

$P(\text{accept}) = \varepsilon = \varphi^2 + (1-\varphi)^2 =$ (the probability to accept any bit by Bob)

$$P(x' \neq x \mid \text{accept}) = \varphi^2 / \varepsilon = \quad (1)$$

= (the probability to be error in any bit accepted by Bob)

In asymptotic case ($n \to \infty$) we have the following sufficient conditions to get at least n bits accepted by Bob (it allows him to form the subset I_c, $|I_c| = n$) and to correct all errors in x_{I_c} using check string s_c, respectively:

$$\varepsilon \geq 1/2, \quad (2)$$

$$r \sim nH(\varphi^2/\varepsilon), \quad (3)$$

where r is the length of check strings s_0 and s_1, $H(\ldots)$ is the entropy function [5]. (It is easy to see that the inequality (2) is trivial because it has solution $0 \leq \varphi \leq 1/2$).

The main theorem of privacy amplification [6] says that with high probability the amount of Shannon's information I_0, leaking to Bob about the secret string $b_{\bar{c}}$ is bounded by the following inequality

$$I_0 \leq 2^{-(n-l-r-I_c)} / \ln 2, \quad (4)$$

where $l = \alpha n$ $(0 < \alpha < 1)$ is the length of the secret strings b_0 and b_1,

I_c is Renyi (or collision) information obtained by Bob about the string $x_{I_{\bar{c}}}$.

The amount of collision information in any of erased bits is zero, while the amount of collision information containing in the string of accepted bits can be expressed asymptotically as follows [6]:

$$I_c \sim n_a\left(1 - H\left(\varphi^2/\varepsilon\right)\right), \tag{5}$$

where n_a is the number of bits accepted by Bob.

Taking into account that asymptotically $n_a \sim n\varepsilon$ and substituting (3) and (5) into (4) we obtain the following sufficient condition to be exponential decreasing of information about $b_{\bar{c}}$, as $n \to \infty$:

$$f_\alpha(\varphi) = 1 - \alpha - H\left(\varphi^2/\varepsilon\right) - \varepsilon\left(1 - H\left(\varphi^2/\varepsilon\right)\right) > 0 \tag{6}$$

In a particular case of one-bit secret strings b_0 and b_1 ($\alpha = 0$), we get from (6) the following condition to be secure OT protocol

$$f_0(\varphi) = 1 - H\left(\varphi^2/\varepsilon\right) - \varepsilon\left(1 - H\left(\varphi^2/\varepsilon\right)\right) > 0 \tag{7}$$

The solution to the last inequality with respect to φ shows that it will be true for every φ within the interval (0, 1/2). In [1] only the case $l = 1$ has been considered and one of the open questions mentioned there was to find an efficient algorithm for $\binom{2}{1}$-OT using BSC_φ for values φ above 0.1982. We have proved it for the same as in [1] algorithm but taking into account the collision information in accepted bits of the string $x_{I_{\bar{c}}}$. The intervals for possible bit error probabilities φ providing the secure OT protocol for different secret rates α are presented in Table 1.

Table 1. The intervals of bit error probabilities φ providing the secure OT protocol

α	0	10^{-3}	$5\cdot10^{-3}$	10^{-2}	0.05	0.1	0.2	0.215
φ	< 0.5	< 0.487 > 0.0005	< 0.470 >0.003	< 0.458 > 0.006	< 0.403 > 0.026	< 0.355 > 0.054	< 0.248 > 0.142	< 0.211 > 0.176

It is worth noting that for $\alpha > 10^{-3}$ the bit error probability has to be sensibly restricted not only from above but also from below. OT protocol does not work at all for BSC_φ, $0 \le \varphi \le 1/2$ if $\alpha > 0.217$.

We can see from (4) and (6) that the more is the function $f_\alpha(\varphi)$, the more efficient is OT protocol. Thus if the parties can establish BSC_φ with different bit error probabilities φ, they can optimize φ to provide a maximum of $f_\alpha(\varphi)$. For example, if $\alpha = 0$, then $f_0(\varphi)$ reaches the maximum for $\varphi \approx 0.2$.

3 Generalizations of base OT protocol

The algorithm to accomplish OT protocol proposed in [1] and described in Section 1 is very natural but not the only one possible to solve the same problem. Let us consider some possible generalizations of it.

3.1 Algorithm with a-multiple repetition of bits x_i, $i = 1, 2, \ldots, 2n$.

It is very natural to generalize algorithm given in [1] if Alice repeats a times each of $2n$ random chosen bits x_i, $i = 1, 2, \ldots, 2n$ and sends them to Bob over BSC_φ. Bob accepts each received a-bit string if and only if the number of zeroes or ones in this string is at least b, $b < a$. This algorithm results in changing the probabilities (1) in the following manner

$$P(\text{accept}) = \varepsilon' = \sum_{\substack{i \in (0, a-b) \\ i \in (b, a)}} \binom{a}{i} \varphi^i (1-\varphi)^{a-i} \tag{8}$$

$$P(x' \neq x \mid \text{accept}) = \frac{1}{\varepsilon'} \sum_{i=b}^{a} \binom{a}{i} \varphi^i (1-\varphi)^{a-i} \tag{9}$$

In asymptotic case this algorithm results in the following sufficient conditions to receive by Bob at least n accepted bits in the string x_i', $i = 1, 2, \ldots, 2n$

$$\varepsilon' \geq 1/2 \tag{10}$$

and to correct all errors in x_{I_c} using the check string s_c

$$r \sim nH\left(\frac{1}{\varepsilon'} \sum_{i=b}^{a} \binom{a}{i} \varphi^i (1-\varphi)^{a-i} \right) \tag{11}$$

The amount of collision information in any bit received by Bob depends on the Hamming weight of a-bit string corresponding to this bit. It can be shown that the average collision information obtained by Bob about the string $x_{I_{\bar{c}}}$ in asymptotic case is the following

$$I_c \sim n\left(1 - \frac{1}{2} \sum_{i=0}^{a} \binom{a}{i} \left(\varphi^i (1-\varphi)^{a-i} + \varphi^{a-i} (1-\varphi)^i\right) \cdot H\left(\frac{\varphi^i (1-\varphi)^{a-i}}{\varphi^i (1-\varphi)^{a-i} + \varphi^{a-i} (1-\varphi)^i} \right)\right) \tag{12}$$

Now if we substitute (11) and (12) for r and I_c in (4), respectively, we can find the optimal bit error probability φ that maximizes the exponent in (4) or functions $f_\alpha(\varphi)$ and $f_0(\varphi)$ similar to those given in (6), (7), respectively. Unfortunately, the inequality (10) is not as trivial as it was for (2). So we have to maximize $f_\alpha(\varphi)$, $f_0(\varphi)$ over the set φ satisfying (10).

The numerical calculations show that the function $f_0(\varphi)$ by (7) reaches the maximum 0.21 for $\varphi = 0.2$, while similar function for generalized algorithm ($a > 2$, $b < a$) reaches the maximum 0.285 for $\varphi = 0.327$, if $a = 8$, $b = 6$, that is a slightly better result.

3.2 Algorithm with arbitrary linear binary (N, K)-code ($K < n$) used to send K-bit substrings of the string x_i, $i = 1, 2, \ldots, 2n$.

Next step to generalize the base OT protocol is to replace a-multiple repetition of bits x_i, $i = 1, 2, \ldots, 2n$ by the use of some binary linear (N, K) code V known for both parties and having maximum possible minimum code distance D.

Without the loss of generality let us take $n = K\beta$, where β is some integer. Alice and Bob also agree on $q = 2^K$-ary ($\widetilde{N}$, $\widetilde{K}$)-Reed Solomon (RS) code, where $\widetilde{K} = \beta$. Then the base OT protocol has to be changed to the following one:

1. Alice picks at random $2n$ bits x_i, $i = 1, 2, \ldots, 2n$, encodes this string by blocks of (N, K)-code and sends these blocks y_j, $j = 1, 2, \ldots, 2\beta$ over BSC_φ.
2. Bob receives the noisy versions of all blocks, corrects at most $t < [(D - 1)/2]$ errors on every block and detects errors using (N, K)-code. He accepts blocks with undetected errors and rejects blocks with detected errors.
3. Bob selects the desired bit string b_c, where $c = 0$ or 1 and picks two disjoint subsets I_0, I_1 of the set $(1, 2, \ldots, 2\beta)$, satisfying the conditions: $|I_0| = |I_1| = \beta$, I_c – contains only the numbers of blocks accepted by Bob.
4. Bob sends both I_0 and I_1 to Alice over noiseless channel.
5. Alice computes the q-ary check strings s_0 and s_1 to y_{I_0}, y_{I_1} respectively using ($\widetilde{N}$, $\widetilde{K}$)-RS code. She sends then both s_0 and s_1 to Bob over noiseless channel.
6. Alice picks random n-bit string m, computes $\hat{b}_0 = b_0 \oplus h_m(x_{I_0})$, $\hat{b}_1 = b_1 \oplus h_m(x_{I_1})$, where x_{I_0}, x_{I_1} are the information symbols of blocks corresponding to subsets I_0 and I_1 respectively and sends $\hat{b}_0$, $\hat{b}_1$, and m to Bob over noiseless channel.
7. Bob corrects errors on x'_{I_c} using s_c, recovers x_{I_c} and computes the desired secret $b_c = \hat{b}_c \oplus h_m(x_{I_c})$.

It is easy to show that in asymptotic case ($n \to \infty$) the following sufficient condition has to be hold for the number $\widetilde{R} = \widetilde{N} - \widetilde{K}$ of q-ary check symbols of ($\widetilde{N}$, $\widetilde{K}$)-RS code transmitted over noiseless channel to correct all errors in the string x_{I_c}

$$\widetilde{R} \sim -\beta \left(P_{ue} \log_2 \frac{P_{ue}}{q-1} + (1-P_{ue}) \log_2 (1-P_{ue}) \right) \Big/ \log_2 q \,, \qquad (\mathbf{13})$$

where P_{ue} is the probability of undetected error obtained after a completion of error correcting and detecting procedures by (N, K)-linear binary code V. Because each of q-ary symbols can be represented by $K = \log_2 q$ binary symbols we automatically get the following number of binary check bits

$$R \sim -K\widetilde{K} \left(P_{ue} \log_2 \frac{P_{ue}}{q-1} + (1-P_{ue}) \log_2 (1-P_{ue}) \right) \Big/ \log_2 q =$$

$$= -\widetilde{K} \left(P_{ue} \log_2 \frac{P_{ue}}{q-1} + (1-P_{ue}) \log_2 (1-P_{ue}) \right) \qquad (\mathbf{14})$$

The sufficient condition to receive by Bob at least β accepted (without detected errors) code blocks of (N, K)-code among all 2β code blocks can be expressed as follows

$$\sum_{i=0}^{t} \binom{N}{i} \varphi^i (1-\varphi)^{N-i} > 1/2$$

The bottleneck of this algorithm is the finding the collision information obtained by Bob about the string $x_{I_{\bar{c}}}$ taking into account that this substring has been transmitted by code blocks of the code V.

If we assume that the amount of collision information coincides with the amount of Shannon information in asymptotic case with large probability, then we can use the results of [7] to express I_c as follows

$$I_c \sim \beta \left(K - NH(\varphi) - \sum_{j=1}^{2^{N-K}} P(G_j) \log_2 P(G_j) \right), \qquad (\mathbf{15})$$

where $H(\ldots)$ is the entropy function,

$P(G_j) = \sum_{i=0}^{n} A_{ij} \varphi^i (1-\varphi)^{n-i}$,

A_{ij} – is the number of words of weight i in the j-th coset of the standard decompositions V_N / V (weight distribution of cosets).

Substituting (14) for r and (15) for I_c into exponent of (4) and dividing the result by n we get the following function (similar to (6)) that should be maximized over $\varphi \in (0,1/2)$

$$f_\alpha(\varphi) = 1 - \alpha - \frac{1}{K}\left[\left(P_{ue}\log_2\frac{P_{ue}}{q-1} + (1-P_{ue})\log_2(1-P_{ue})\right) - \right.$$

$$\left. - \left(K - NH(\varphi) - \sum_{j=1}^{2^{N-K}} P(G_j)\log_2 P(G_j)\right)\right] \qquad (16)$$

We note that the probability P_{ue} can be found for the chosen (N, K)-code as follows [8]

$$P_{ue} = (1-\varphi)^N \left\{ A_c^{(t)}\left(\frac{\varphi}{1-\varphi}\right)\right\} \qquad (17)$$

where $A_c^{(t)}(z) = \sum_{j=D-t}^{N} A_{t,j} z^j$,

$$A_{t,j} = \sum_{i=j-t}^{j+t} A_i N_t(i,j),$$

t is the multiplicity of errors correcting by the code V, providing $t \le [(D-1)/2]$, where D is the minimum distance of the code V,

$$N_t(i,j) = \sum_{\gamma=\max(0,i-j)}^{[(t+i-j)/2]} \binom{N-i}{\gamma+j-i}\binom{i}{\gamma},$$

A_i is the number of code words of weight i (weight distribution function) of the code V. We note that $A_i = A_{i1}$.

It is seen from (16) and (17) that OT protocol optimization requires the knowledge of weight distribution of cosets for chosen code V. Unfortunately this distribution is known only for a limited classes of linear binary codes [8].

4 Non-asymptotic case

Let us consider the base protocol [1]. The requirement that the number of accepted bits in the string x_i', $i = 1, 2, \ldots, 2n$ has to be at least n is not necessary for Bob to receive the desired secret b_c because he can correct both errors and erasures in the chosen substring x_{I_c} of length n using check string s_c of the code C. If the minimum

code distance of this code is d then it is capable to correct both t errors and t' erasures when the following condition holds [9]

$$2t + t' \le d - 1 \tag{18}$$

It is easy to show that if Bob corrects both erasures and errors in some n-bit substring x'_{I_c} of $2n$-bit string x'_i, $i = 1, 2, \ldots, 2n$, then the probability to recover x_{I_c} correctly can be upper bounded as follows

$$P_c \ge \sum_{i=n-d+1}^{n-1} \binom{2n}{i} \varepsilon^i (1-\varepsilon)^{2n-i} \sum_{j=0}^{[(d-1-(n-i))/2]} \binom{i}{j} \left(\frac{\varphi^2}{\varepsilon}\right)^j \left(1-\frac{\varphi^2}{\varepsilon}\right)^{i-j} +$$

$$+ \sum_{i=n}^{2n} \binom{2n}{i} \varepsilon^i (1-\varepsilon)^{2n-i} \sum_{j=0}^{[(d-1)/2]} \binom{n}{j} \left(\frac{\varphi^2}{\varepsilon}\right)^j \left(1-\frac{\varphi^2}{\varepsilon}\right)^{n-j} \tag{19}$$

The inequality (4) can be used to estimate the amount of Shannon's information I_0 leaking to Bob about the string $b_{\bar{c}}$, where $I_c = \gamma I_{c_1}$, γ is the number of accepted bits in $x_{I_{\bar{c}}}$ and I_{c_1} is the amount of collision information obtained by Bob about each of these accepted bits. Because the execution of the base protocol results for Bob in $BSC_{\varphi'}$ with $\varphi' = \varphi^2/\varepsilon$ we get for I_{c_1} [6]

$$I_{c_1} = 1 + \log_2\left(\left(1-\varphi^2/\varepsilon\right)^{\left(1-\varphi^2/\varepsilon\right)} + \left(\varphi^2/\varepsilon\right)^{\left(\varphi^2/\varepsilon\right)}\right) \tag{20}$$

To provide the guaranteed security of OT protocol we have to design it under the conservative assumption that Bob can be a dishonest party and distribute the accepted (non-erased) bits equally between substrings $x'_{I_c}, x'_{I_{\bar{c}}}$ thinking to extract at least some information from both secrets b_0 and b_1. If we want to prevent this attack then one can find I_c from (4) for given value I_0, where r is the number of check symbols for chosen $(n + r, n)$-code C and estimate the probability of risk to be accepted by Bob at least 2γ bits on the string x'_i, $i = 1, 2, \ldots, 2n$, where $\gamma = I_c / I_{c_1}$, as follows

$$P_r = \sum_{i=2\gamma}^{2n} \binom{2n}{i} \varepsilon^i (1-\varepsilon)^{2n-i} \tag{21}$$

The problem how to select the main parameters of OT base protocol in non-asymptotic case can be solved by the following algorithm:

1. Fix P_r, $\widetilde{I}_0$, P_c, n, l, and φ.
2. Find d from (19) satisfying P_c in the point 1 given φ and n.
3. Find r using the bound for BCH codes given n and d.
4. Find γ from (21) given n, φ and P_r.
5. Find I_{c_1} from (20) and then $I_c = \gamma I_{c_1}$.

6. Find I_0 from (4) given n, l, r, and I_c.
7. If I_0 that was found in the point 6 occurs at most equal to $\widetilde{I}_0$ given in the point 1, then decrease n and repeat the points 2-6. Otherwise optimize φ to provide a positive result. In the case if no one φ gives $I_0 \le \widetilde{I}_0$ then increase n and repeat the points 2-6.

Example. Let us take $l = 20$, $P_c = 0.9999$, $P_r = 10^{-4}$, $I_0 = 10^{-10}$ bit. Then we can evaluate (following algorithm above) the minimal possible $n = 3840$ that results in $r = 255$, $d = 43$ and optimal chosen $\varphi = 0.0453$.

We can see from this example that OT protocol "works", in fact, because it provides both reliability ($P_c \ge 0.9999$) and security ($I_0 \le 10^{-10}$, $P_r \le 10^{-4}$). Unfortunately the length of the string x has to be significant ($n = 3840$) but this is the feature of this base OT algorithm.

5 Discussion of the main results and some open problems

Our contribution (in comparison with paper [1]) is the following:
- extension of OT protocol to multibit secret strings,
- tighter bounds on the bit error probabilities that makes the base OT protocol more feasible,
- generalizations of base OT protocol,
- performance evaluation of OT protocol in a non-asymptotic case.

We showed that base OT protocol practically "works" (in non-asymptotic case), although it requires a significant bit string to be sent over BSC_φ. This protocol is the remarkable example of the combination of both codes and cryptography. In fact, on the one hand OT protocol does not work without the use of error correcting codes and on the other hand OT based on noisy channel is typical cryptographic protocol that is in addition information-theoretically secure.

We do not consider in the current paper how to prevent attacks on OT protocol, that can be initiated by dishonest Alice, who deviates from base OT protocol to find out which of two secrets Bob wants. (The solution to this problem was given in [1] and it also holds for our extensions.)

To extend $\binom{2}{1}$-OT protocol to the case $\binom{L}{1}$-OT protocol, there exist different possibilities to proceed. The simplest way is to arrange a special *dichotomous procedure* that reduces several $\binom{2}{1}$-OT protocols to one $\binom{L}{1}$-protocol. (The complexity of such $\binom{L}{1}$-OT protocol is $(L - 1)$ times more than complexity of $\binom{2}{1}$-OT protocol). Next way is to use base protocol [1] for L secret strings initially. It results in harder conditions than (6) and (7) to be feasible $\binom{L}{1}$-OT protocol in BSC_φ. We are

going to publish these results later and to specify which of $\binom{L}{1}$-protocol versions is the best.

Finally the main problem that has to be solved for practical implementation of OT-protocol (as well as for other protocols based on noisy channels) is an arrangement of BSC_{φ} between parties. This problem has already been discussed in [2]. We can add only that there is some progress in our investigations to arrange BSC_{φ} as quantum channel with low intensity of random polarized photons.

References

1. C. Crepeau, Efficient Cryptographic Protocols Based on Noisy Channels. *Proc. Eurocrypt'97*, Lecture Notes in Computer Science, N 1233, pp. 306–317.
2. V. Korjik, K. Morozov, Non-asymptotic bit commitment protocol based on noisy channels, 20 Biennal Symposium on Communications Department of Electrical and Computing Engineering Queen's University, Proc. pp. 74-78, Kingston, Canada, 2000.
3. B. Schneier, Applied Cryptography, *John Wiley*, 1996.
4. D.R. Stinson, Universal hashing and authentication codes, *Advances in Cryptology, Proc. of Crypto' 91* (Lecture Notes in Computer Science, vol. 576, 1999, pp.74-85.
5. A. Feinstein, Foundations of information theory, New-York, *McGraw Hill*, 1958.
6. C. Bennett, G. Brassard, C. Crepeau and U.M. Maurer, Generalized privacy amplification, *IEEE Trans. on IT*, vol. 41, N 6, Nov. 1995, pp. 1915-1923.
7. V. Korjik, V. Yakovlev, Capacity of communication channel with inner random coding, *Problems of Information Transmission*, vol. 28, no. 4, 1992, pp. 317-325.
8. T. Klove, V. Korjik, Error Detecting Codes, Kluwer, 1995.
9. F.J. Mac Williams and N.J.A. Sloan, The theory of error-correcting codes, New-York: North-Holland, 1977.