Oblivious Transfer and Bit Commitment from Weak Primitives

Kirill Morozov[3], Joern Mueller-Quade[2], Anderson C. A. Nascimento[1]

[1] Department of Electrical Engineering, University of Brasilia
Campus Universitario Darcy Ribeiro,Brasilia, CEP: 70910-900, Brazil
E-mail: andclay@ene.unb.br
[2] Universitaet Karlsruhe, Institut fuer Algorithmen und Kognitive Systeme
Am Fasanengarten 5, 76128 Karlsruhe, Germany
E-mail: muellerq@ira.uka.de
[3] Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST)
Akihabara Daibiru room 1102
1-18-13 Sotokanda, Chiyoda-ku Tokyo 101-0021, Japan
E-mail: kirill.morozov@aist.go.jp

Abstract. In this paper we survey recent developments in the field of commitment and oblivious transfer based on weak primitives. We also present two original results: a commitment protocol that achieves non-zero rate from any non-trivial unfair binary symmetric channel; and an analysis of the information theoretical composability of oblivious transfer schemes based on two-party primitives.

1 Introduction

Information theoretical security (also known as unconditional security) aims at obtaining protocols that are secure even if unlimited computational power is available to an adversary. Because of its strength, information theoretical security is a highly desirable feature, however it is difficult to obtain.

Physical assumptions (such the availability of trusted sources of noise), also known as weak primitives, came on to the scene as a new hope to obtain practical information theoretical secure protocols and have been being an active area of research for the last decades both in the information theory and cryptographic communities.

In this paper, we survey recent developments in the field of cryptographic primitives based on weak primitives and present some new results. We focus on bit commitment and oblivious transfer due to their importance as fundamental building blocks in more complex protocols [23].

Besides surveying the field, we also present, to the best of our knowledge, the first commitment protocol achieving non-zero rate for any non-trivial unfair binary symmetric channel and the first analysis of statistically secure universal composition of oblivious transfer protocols based on two-party primitives.

This paper is organized as follows: in Section 2 we present some of the physical assumptions used in the literature; in Section 3 we present a survey of results on commitment protocols and our original protocol based on unfair binary symmetric channels; in Section 4 we review the literature of recent results on oblivious transfer based on physical assumptions; in Section 5, we present some results on the universal composability of unconditionally ecure oblivious transfer protocols.

2 Weak Primitives

In this Section, we briefly review the most used physical assumptions (primitives) to obtain information theoretically secure cryptographic protocols.

We always assume there is an unlimited bidirectional noiseless channel available between Alice and Bob. As a noiseless channel is trivial in the sense nothing can be obtained from it, we assume the existence of an additional primitive.

We firstly consider a discrete memoryless noisy channel $W : \mathcal{X} \longrightarrow \mathcal{Z}$ from Alice to Bob, which may be used n times: on input $x^n = x_1 \dots x_n$, the output distribution on $\mathcal{Z}^n$ is $W^n_{x^n} = W_{x_1} \otimes \cdots \otimes W_{x_n}$.

Another possible primitive that can be used to obtain two-party cryptographic protocols is a unidirectional noisy Gaussian channel, connecting the players Alice and Bob. The Gaussian channel is a time discrete channel with continuous input/output symbols belonging to a real alphabet.

The noise T is drawn i.i.d. from a Gaussian distribution with variance ${\sigma_G}^2$. Thus, at time i the output symbol z_i is related to input and noise as follows:

$$z_i = x_i + t_i, \quad t_i \sim \mathcal{N}(0, {\sigma_G}^2).$$

For every word transmitted over the channel, there is also a power constraint:

$$\frac{1}{n} \sum_{i=1}^{n} {x_i}^2 \leq P.$$

Alternatively, we may assume independent, identically distributed (i.i.d.) realisations of a pair of random variables (X, Y) given to Alice and Bob, respectively (range $\mathcal{X} \times \mathcal{Y}$ with distribution P_{XY}, in both cases with finite sets $\mathcal{X}, \mathcal{Y}$).

We now introduce the concept of redundancy that turned out to be vital in the characterization of the usefulness of noisy resources for obtaining two-party cryptographic primitives.

The channel W is called *non–redundant*, if none of its output distributions is a convex combination of its other output distributions:

$$\forall y \forall P \text{ s.t. } P(y) = 0 \quad W_y \neq \sum_x P(x) W_x.$$

It is easy to observe that, we can make W into a non–redundant channel by removing all redundant input symbols x. Also, observe that redundant symbols can be simulated by non-redundant ones.

The same concept can be extended to pre-distributed correlated randomness.

The pair X, Y of random variables with joint distribution $P(X, Y)$ is called *non–redundant*, if for any two distinct symbols $x_1, x_1 \in \mathcal{X}$,

$$\Pr\{Y|X = x_1\} \neq \Pr\{Y|X = x_2\},$$

and symmetrically for symbols from $\mathcal{Y}$. If there is redundancy, one can change the variables in a unique way to make them non–redundant by collapsing x_1 and x_2 which fail the above inequation. A similar reasoning applies to redundant symbols y_1 and y_2.

One should note that discrete memoryless channels are not a very realistic model for dealing with real world channels. In real implementations of noisy channels an adversary can always control, to some degree, the level of noise in the channel, for instance by buying a better antenna in the case of a wireless link. Also, note that an adversary performing this attack can always hide the fact that he has made the channel less noisy by introducing errors by himself in the messages which are sent to the other player.

In order to deal with this situation, Damgard, Kilian and Salvail introduced in [19] the notion of an *unfair noisy channel* (UNC). A $[\gamma; \delta] - UNC$ is a binary symmetric channel where dishonest players can reduce its error probability from δ to γ, where $0 < \gamma < \delta < 1/2$.

Cryptogates are boxes that receive inputs x from Alice, y from Bob and return z to Alice and w to Bob according to a certain joint probability distribution $p(x, y, z, w)$. They are one of the most general for studying weak primitives. Several results for classification of trivial and non-trivial cryptogates are listed in [24].

3 Commitment Protocols

Commitment protocols were introduced by Blum [10] and are important building blocks in theoretical cryptography. They are the digital equivalent of a sealed envelope. A commitment protocol is composed of two phases: a commit and an opening phase. During the commit phase sender (Alice) and receiver (Bob) exchange messages over the noisy and noiseless channels. During the opening phase, Alice sends some message over the noiseless channel to Bob. After performing some test based on the data available to him, Bob decides if he accepts Alice's commitment or not. Informally, the protocol is said to be secure against an dishonest sender (binding) if Alice is unable (with high probability) to successfully open two different commitments (messages). It is secure against a dishonest receiver (concealing) if Bob is unable to obtain significant knowledge on the message Alice commits to before the opening phase. The protocol is correct if the probability it fails for honest sender and receiver is negligible.

Crepeau and Kilian in [15] were the first ones to show that commitment schemes can be obtained from a source of trusted noise. In their case, they assumed a binary symmetric channel connecting the players. The efficiency of these results was later improved in [14] by using privacy amplification.

A characterization of which noisy resource (pre-distributed randomness and discrete memoryless channels) are useful for obtaining commitment was presented in [29]. There, it was proved that after redundancy is removed from a certain channel or distribution and the resulting random resource possess positive equivocation, then commitment schemes are possible. [29] also introduced the question of computing the so called *commitment capacity* of a discrete memoryless system. The commitment capacity is defined as the maximum ratio of a securely committed string k and the number of times a noisy system is used n. It measures how efficiently a certain resource can be used for implementing string commitment in the same way Shannon capacity measures the maximum efficiency of reliably information transmission over a noisy channel. [29] proved that, after redundancy is removed, the commitment capacity is given by the equivocation of the noisy resource.

We remember that an $[\gamma;\delta]-UNC$ is a binary symmetric channel where dishonest players can reduce its error probability from δ to γ, where $0<\gamma<\delta<1/2$. In [19] it was proved that if $\delta \geq 2\gamma(1-\gamma)$ the UNC is trivial, in the sense that neither bit commitment nor oblivious transfer can be based upon its existence. A protocol implementing bit commitment which works for any $[\gamma;\delta]-UNC$, given that $\delta<2\gamma(1-\gamma)$, was also presented in [19], thus showing the tightness of their bound $\delta \geq 2\gamma(1-\gamma)$. Their protocol is interactive. A non-interactive construction was presented in [22]. [22] shows that, given $\delta < \gamma(3/2-\gamma)$ non-interactive commitment schemes are possible. Moreover, assuming a weaker adversary (one which behaves according the protocol during the commit phase but is fully malicious later on, non-interactive commitments can be based on any non-trivial $[\gamma;\delta]-UNC$.

In [8] the first commitment protocol based on the existence of a continuous channel was proposed. Assuming the existence of an additive white Gaussian noise (AWGN) channel, untamperable and of known characteristics, connecting the sender and the recipient of the commitment, [8] proves that the optimal rate at which an AWGN channel can be used for commitment, *i.e.* its commitment capacity is infinite, even with power constraints.

3.1 Efficient Protocols Achieving the Commitment Capacity of Unfair BSCs

One can see the unfair binary symmetric noisy channel $[\gamma;\delta]-UNC$ defined in [19] as a concatenation of two channels W_1 and W_2 defined as follows:

$$W_1=\begin{pmatrix} 1-\frac{\delta-\gamma}{1-2\gamma} & \frac{\delta-\gamma}{1-2\gamma} \\ \frac{\delta-\gamma}{1-2\gamma} & 1-\frac{\delta-\gamma}{1-2\gamma} \end{pmatrix}, W_2=\begin{pmatrix} 1-\gamma & \gamma \\ \gamma & 1-\gamma \end{pmatrix}. \qquad (1)$$

In the case of a cheating sender, she can remove the channel W_1 from the concatenation and turn the channel connecting her to Bob into W_2, thus reducing its noise level. The same happens for a cheating Bob, he can decrease the level of noise by removing W_1. Honest players are connected by a channel with a noise level between that of the concatenation W_1W_2 and W_2, but unknown to them.

We propose here a protocol that obtains commitments from any non-trivial unfair binary symmetric channel and achieves a rate equals to $h(\gamma) - h(\frac{\delta-\gamma}{1-2\gamma})$, $h()$ being the binary entropy function.

Protocol 1 - Commit Phase

1. Alice chooses a random binary string $r_1, \ldots, r_n$ of dimension n and sends it to Bob over the $[\gamma;\delta] - UNC$.
2. After receiving the string $r'_1, \ldots, r'_n$, Bob chooses at random a two universal hash function $V_1 : \{0,1\}^n \rightarrow \{0,1\}^{n(h(\frac{\delta-\gamma}{1-2\gamma})+\eta)}$,$\eta > 0$, where ηn is an integer. Bob then sends the description of V_1 to Alice over the noiseless channel.
3. Alice computes and sends $V_1(r_1, \ldots, r_n)$ to Bob over the noiseless channel.
4. Alice selects a two-universal hash function $V_2 : \{0,1\}^n \rightarrow \{0,1\}^{n(h(\gamma)-h(\frac{\delta-\gamma}{1-2\gamma})-\epsilon')}$, $\epsilon' > \eta > 0$;and computes $com(a) = a \oplus V_2(r_1, \ldots, r_n)$ where a is the string Alice commits to and "$\oplus$" is a bitwise XOR. Then Alice announces $V_2, com(a)$ to Bob over the noiseless channel.

Protocol 1 - Reveal Phase

1. Alice announces $r_1, \ldots, r_n$ to Bob over the noiseless channel.
2. Bob checks:
   a) if $r_1, \ldots, r_n$ and $r'_1, \ldots, r'_n$ posses hamming distance less or equal to $(\gamma - \epsilon)n, \epsilon > 0$, and if $V_1(r_1, \ldots, r_n)$ equals what he received in the commit phase, otherwise rejects.
   b) If all tests pass successfully then Bob accepts and outputs $a = V_2(r_1, \ldots, r_n) \oplus com(a)$.

We briefly argue about the protocol security.

The correctness follows straightforwardly from the Chernoff bound [13].

Privacy against Bob follows from the privacy amplification theorem [9] and from the fact that the information Alice sends Bob over the noiseless channel decreases the uncertainty on $r_1, \ldots, r_n$ by at most $nh(\frac{\delta-\gamma}{1-2\gamma}) + \eta)$ bits.

To prove bindingness, first note that we may assume, wlog, that dishonest Alice uses W_2 when sending noisy information to Bob during the commit phase. Let $z_1, \ldots, z_n$ denote the string sent by cheating Alice during the commit phase. Honest Bob has to accept any opening information $r_1, \ldots, r_n$ that is consistent with any channel in between the concatenation W_1W_2 and W_2, Alice can play the role of the channel W_1 and modify $z_1, \ldots, z_n$ producing a jointly typical sequence $r_1, \ldots, r_n$ with respect to W_1 and this sequence must be accepted by Bob if $V_1(r_1, \ldots, r_n)$ is consistent with what he received in the commit phase. Thus, she succeeds in cheating if she finds two sequences $r_1, \ldots, r_n$ that pass the jointly typicality test performed by Bob and are mapped into the same output by the two universal hash function V_1. The number of jointly typical sequences $r_1, \ldots, r_n$ is upper bounded by $2^{h(\frac{\delta-\gamma}{1-2\gamma}+\epsilon)n}, \epsilon > 0$. By the definition of two universal hash functions, the number of jointly typical sequences producing the same output for a random V_1 is at most $2^{h(\frac{\delta-\gamma}{1-2\gamma}+\epsilon)n}/|V_!| = 2^{(\epsilon-\eta)n}$. By choosing an appropriate η we can make the probability that Alice finds two such values negligible.

4 Oblivious Transfer Protocols

We briefly survey some important results in oblivious transfer protocols based on weak primitives. Oblivious transfer was introduced by Rabin in [26]. Originally it was defined as a protocol where Alice sends a bit b to Bob. The protocol is secure if he receives the bit with probability 1/2, otherwise receiving an erasure symbol and if Alice has no information on whether Bob received the bit or not. Variants of oblivious transfer were also introduced in [21, 28], but all those flavors turned out to be equivalent [12, 16, 11, 14, 27].

Crepeau and Kilian [15] proved that a binary symmetric channel yields oblivious transfer. Those results being improved in [14] in terms of uses of the noisy channel. Kilian characterized all the cryptogates and channels which can be used for obtaining oblivious transfer in [24] in the case of passive adversaries.

In [17],and independently in [25] a characterization of non-trivial noisy channels in the case of active adversaries was presented. Additionally, [25] presented a characterization of non-trivial correlated pre-distributed randomness.

The problem of computing the *oblivious transfer capacity* (a measure of how efficient noisy resources can be used to obtain oblivious transfer) was introduced in [25]. Lower bounds in the case of honest-but-curious players were also obtained. The results of [25] were extended in [18].

Oblivious transfer was proven symmetrical in [30].

Preliminary results about oblivious transfer based on unfair noisy channels were proven in [19] and [20] and later corrected and extended in [31]. However, a complete characterization of which unfair noisy resources give us oblivious transfer is still an open question.

5 Information-Theoretically Secure Oblivious Transfer and Composability

Oblivious transfer is one of the most important building blocks in cryptography and, as such, mostly used within larger protocols. Hence it is an important question if a given protocol remains secure if an idealized oblivious transfer primitive is replaced by some concrete realization. Oblivious transfer protocols which are secure in the Universal Composability Framework [2] (or the framework of reactive simulatability [7]) give strong garantees in that respect: A universally composable realisation of oblivious transfer can replace an ideal oblivious transfer functionality in any cryptographic protocol without lowering the security of this protocol. Furthermore, universally composable protocols are also concurrently composable, i.e., many instances can run concurrently and are still at least as secure as many ideal functionalites in parallel. These two properties together constitute the composition theorem of the Universal Composability framework according to which a polynomial number of ideal functionalities in a larger application can simultaneously be replaced by secure realisations without lowering the security of the overall application. With this theorem a modular design of provably secure protocols becomes possible.

The security definition in the Universal Composability framework is a simulation based notion of security. Securiy is defined by comparing a *real model* with an *ideal model* which is considered to be secure by definition. If every attack in the real model can also be performed in the ideal model by an ideal adversary with very limited control over corrupted parties then this protocol is said to be a secure realization of the ideal functionality which was used in the ideal model. In comparison to other (*stand-alone*) simulation based notions of security [5] an additional machine, the *environment*, is used in the formalization. This environment machine interacts either with the real protocol and the real adversary in the real model or it interacts with an ideal functionality and an ideal adversary. If the environment machine cannot distinguish between the real model and the ideal model the protocol is said to be a secure realization of the ideal functionality. Intuitively the strong composability guarantees arise, because the environment machine can mimic surrounding protocols while trying to distinguish the real from the ideal model.

For this section information-theoretical security is of concern and for this reason the environment machine and the real and the ideal adversary have to be unlimited in time. For details about this variant of the Universal Composability framework (more precisely for the reactive simulatability definition of security) see [6].

Unfortunately the security property Universal Composability is very difficult to achieve. For computational security additional security assumptions and very involved protocols are needed to obtain universally composable protocols. Bit commitment or oblivious transfer are, even with computational assumptions, impossible from scratch and additional assumptions like a trusted *common reference string* are necessary [3, 4].

¿From this point of view it is especially astonishing that for a large class of information-theoretically secure oblivious transfer protocols Universal Composability is already implied by stand alone security.

For a security parameter k we say that an oblivious transfer protocol has a concrete bound $\epsilon(k)$ for the knowledge of a corrupted receiver if the probability that a corrupted receiver learns more information than $\epsilon(k)$ bits about both input bits of the sender is negligible.

Theorem 1. *Let Π be an information-theoretically stand-alone secure oblivious transfer protocol based on a two party primitive. Let Π have a concrete bound $\epsilon(k)$ for the knowledge of a corrupted receiver for a computable negligible function ϵ, then the protocol Π is universally composable.*

Proof. If no party is corrupted the ideal adversary will simulate a real protocol with two honest parties (with input $b_0 = b_1 = c = 0$) and a real adversary. All messages from the environment to the adversary will be given to this simulated real adversary and all messages the simulated adversary wants to send to the environment machine are forwarded to the environment. If the protocol terminates successfully (the receiver generates output) the ideal adversary will schedule the input to the ideal functionality and schedule the output to the ideal receiver.

If the sender S is corrupted, then the ideal adversary will simulate an uncorrupted receiver with input $c = 0$ connected to a simulated real adversary. Messages exchanged between the environment and the adversary will be forwarded to (and from) the simulated real adversary. If the simulated real protocol aborts then the ideal adversary aborts the ideal protocol. Else the ideal adversary sets a variable b_0 to the output of simulated receiver in the simulated protocol run. Next the ideal adversary enumerates all random tapes[4] for which the receiver's view of the interaction between the simulated real adversary and an uncorrupted receiver with input $c = 1$ is identical to the interaction observed with input $c = 0$ in the first simulated real protocol. As the protocol is stand-alone secure any real adversary should be able to learn the input c of the receiver (by a likelyhood estimation) only with negligible probability. Hence with overwhelming probability the following holds: The number of random tapes which yield the specific interaction between adversary and receiver as observed with input $c = 0$ equals (up to a negligible fraction) the number of random tapes yielding this interaction with input $c = 1$. Furthermore if we restrict to random tapes which yield this specific interaction and output on the receiver's side then the two sets still must be of approximately equal size. Otherwise a real adversary could obtain information on the input c by observing if the honest receiver aborts in some larger application using the oblivious transfer protocol.

The set of random tapes yielding this interaction with input $c = 1$ and output on the receiver's side is empty only with negligible probability as it is approximately of the same size as the corresponding set with input $c = 0$ and from this set we sampled one element at random (in the first simulation) and this simulation had output. From this set of random tapes yielding this interaction with input $c = 1$ and output on the receiver's side we take one tape at random and set b_1 to be the output of the simulated uncorrupted receiver in the simulation with this random tape.

Next the ideal adversary calls the ideal oblivious transfer functionality with input (b_0, b_1).

If the input of the receiver in the ideal model is $c = 0$ then the real and the ideal model are clearly indistinguishable. As the sizes of the sets of random tapes yielding the same interaction are approximately equal this interaction is equally likely for input $c = 1$ and the ideal model and the real model are indistinguishable for this case, too.

Now let the receiver be corrupted. In this case the ideal adversary connects a simulated real adversary to a simulated honest sender (with input b_0, b_1 chosen at random). All messages from the environment to the adversary are given to the simulated real adversary and all messages the simulated adversary wants to send to the environment are forwarded to the environment.

For each messages sent to the real adversary during the simulation the simulator calculates the number $j_{b_0=0}$ of random tapes consistent with this message

[4] this is possible because.honest parties can be considered to have have a strict runtime bound and hence there exists a concrete bound for the number of bits read from the random tape.

and all messages sent so far and input bit $b_0 = 0$. Further let $j_{b_0=1}$ denote the number of random tapes consistent with this message and all messages sent so far and input bit $b_0 = 1$ and let $j_{b_1=0}$ and $j_{b_1=1}$ be defined analogously. Denote by s the sum of these four numbers and let m denote the first message for which one of the following two numbers is larger than $\epsilon(k)$:

$$\frac{j_{b_0=0}}{s}\log(\frac{j_{b_0=0}}{s}) + \frac{j_{b_0=1}}{s}\log(\frac{j_{b_0=1}}{s}),$$

$$\frac{j_{b_1=0}}{s}\log(\frac{j_{b_1=0}}{s}) + \frac{j_{b_1=1}}{s}\log(\frac{j_{b_1=1}}{s}).$$

Due to the concrete security of the oblivious transfer protocol only one of the two numbers can be greater than $\epsilon(k)$ and this information fixes which of the two bits b_0, b_1 cannot be learnt by the attacker. If the bit which can be learnt by the attacker (in the following called b_c) equals the corresponding bit in the simulation then the message m is sent and the simulation is carried on. If however these bits differ, then a new random tape is randomly chosen for which for input b_c yields the same communication as observed by the attacker. Instead of the message m (which cannot be consisten with input b_c) a new message m' is calculated with the new random tape and the simulation is carried on with the new random tape.

It is an open problem if the nice property that stand-alone security already implies universal composability holds for all information theoretically secure oblivious transfer protocols built on two-party primitives.

However, in the case of oblivious transfer protocols in the bounded storage model [1] the protocols need not be universally composable[5]. In the protocols given in [1] the input of the receiver cannot be extracted from the communication observed and the ideal adversary cannot learn what to enter into the ideal oblivious transfer functionality.

References

1. C. Cachin, C. Crepeau, and S. Marcil. Oblivious transfer with a memory bounded receiver. In *Proc. of 39th FOCS*, 1998.
2. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *IEEE Symposium on Foundations of Computer Science*, pages 136–145, 2001.
3. Ran Canetti and Marc Fischlin. Universally composable commitments. *Lecture Notes in Computer Science*, 2139, 2001.
4. Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *J. Cryptol.*, 19(2):135–167, 2006.

[5] In the literature no formal definition for Universal Composability in the bounded storage model is given and here we assume the sum of the memories of adversary and environment machine to be bounded.

5. Oded Goldreich. *Foundations of Cryptography – II Basic Applications*, volume 2. Cambridge University Press, 2004.
6. Dennis Hofheinz and Dominique Unruh. On the notion of statistical security in simulatability definitions. In *Information Security, Proceedings of ISC'05*, Lecture Notes in Computer Science. Springer, September 2005. Preprint on IACR ePrint 2005/032.
7. Birgit Pfitzmann and Michael Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *Proc. of 2001 IEEE Symp. on Security and Privacy*, 2001.
8. J. Barros, H. Imai, A. Nascimento, S. Skludarek, "Bit Commitment over Gaussian Channels.", In: 2006 IEEE International Symposium on Information Theory, 2006, Seatlle.
9. C. H. Bennett, G. Brassard, C. Crépeau, U. Maurer, "Generalized Privacy Amplification", IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, 1995.
10. M. Blum, "Coin fipping by telephone: a protocol for solving impossible problems", Proc. IEEE Computer Conference, pp. 133–137, 1982.
11. G. Brassard, C. Crépeau, J.-M. Robert, "Information theoretic reductions among disclosure problems", Proc. 27th FOCS, pp. 168–173, IEEE, 1986.
12. C. Cachin, "On the foundations of oblivious transfer", Proc. EUROCRYPT '98, LNCS 1403, pp. 361–374, Springer Verlag, 1998.
13. H. Chernoff, "A measure of asymptotic eciency for tests of a hypothesis based on the sum of observations", Ann. Math. Statistics, vol. 23, pp. 493–507, 1952.
14. C. Crépeau, "Efficient Cryptographic Protocols Based on Noisy Channels", Advances in Cryptology: Proc. EUROCRYPT 1997 , pp. 306–317, Springer 1997.
15. C. Crépeau, J. Kilian, "Achieving oblivious transfer using weakened security assumptions", Proc. 29^{th} FOCS, pp. 42–52. IEEE, 1988.
16. C. Crépeau, "Equivalence between two flavours of oblivious transfers", Proc. CRYPTO '87 , LNCS 293, pp. 350–354, Springer Verlag, 1988.
17. C. Crépeau, K. Morozov, S. Wolf: "Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel," SCN 2004: 47-59
18. R. Ahlswede and I. Csiszar, "On Oblivious Transfer Capacity," in Proc. IEEE ISIT 2007, Nice, France, June, 2007.
19. I. B. Damgård, J. Kilian, L. Salvail, "On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions", Advances in Cryptology: EUROCRYPT 1999, pp. 56–73, Springer 1999.
20. I. B. Damgard, S. Fehr, K. Morozov, L. Salvail, "Unfair Noisy Channels and Oblivious Transfer", TCC 2004: 355-373
21. S. Even, O. Goldreich, A. Lempel, "A Randomized Protocol for Signing Contracts", Comm. ACM vol. 28, no. 6, pp. 637–647, 1985.
22. H. Imai, A. Nascimento, J. Mueller-Quade, A. Winter, "Non-Interactive Commitments based on Unfair Noisy Channels", In: International Symposium on Information Theory and its Applications, 2004, Parma.
23. J. Kilian: "Founding Cryptography on Oblivious Transfer," STOC 1988: 20-31, 1988.
24. J. Kilian: "More general completeness theorems for secure two-party computation," STOC 2000: 316-324
25. A. Nascimento, A. Winter, "On the Oblivious Transfer Capacity of Noisy Correlations", In: 2006 IEEE International Symposium on Information Theory, 2006, Seattle.
26. M. O. Rabin, "How to exchange secrets by oblivious transfer", Technical Memo TR–81, Aiken Computation Laboratory, Harvard University, 1981.

27. D. Stebila, S. Wolf, “Efficient oblivious transfer from any non-trivial binary-symmetric channel”, Proc. ISIT 2002 (Lausanne), p. 293, IEEE, 2002.
28. S. Wiesner, ”Conjugate coding”, Sigact News, vol. 15, no. 1, 1983, pp. 78–88; original manuscript written circa 1970.
29. A. Winter, A. C. A. Nascimento, H. Imai, “Commitment Capacity of Discrete Memoryless Channels”, Proc. 9th IMA International Conference on Cryptography and Coding (Cirencester, 16–18 December 2003), LNCS 2898, pp. 35–51, Springer Verlag, 2003.
30. S. Wolf, J. Wullschleger, “Oblivious transfer is symmetric” Advances in Cryptology - EUROCRYPT ’06, Lecture Notes in Computer Science, Springer-Verlag, 2006.
31. J. Wullschleger, “Oblivious transfer amplification”, Ph.D. Thesis available from http://arxiv.org/abs/cs.CR/0608076