Efficient Protocols Achieving the Commitment Capacity of Noisy Correlations

Hideki Imai*†, Kirill Morozov†, Anderson C. A. Nascimento‡, Andreas Winter§
* Department of Electrical, Electronic and Communication Engineering,
Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
† National Institute of Advanced Industrial Science and Technology (AIST),
1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan
Email: {h-imai,kirill.morozov}@aist.go.jp
This work is done in part at Institute of Industrial Science, University of Tokyo, Japan
‡ Department of Electrical Engineering, University of Brasilia, 70910-900, Brasilia, DF, Brazil
E-mail: andclay@ene.unb.br
§ Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom
E-mail: a.j.winter@bris.ac.uk

***Abstract*— Bit commitment is an important tool for constructing zero-knowledge proofs and multi-party computation. Unconditionally secure bit commitment can be based, in particular, on noisy channel or correlation where noise considered a valuable resource. Recently, Winter, Nascimento and Imai introduced the concept of commitment capacity, the maximal ratio between the length of a string which the sender commits to and the number of times the noisy channel/correlation is used. They also proved that for any discrete memoryless channel there exists a secure protocol achieving its commitment capacity however, no particular construction was given. Solving their open question, we provide an efficient protocol for achieving the commitment capacity of discrete memoryless systems (noisy channels and correlations).**

I. Introduction

Commitment schemes were introduce by Blum in [3]. A bit commitment (BC) scheme is a tool for transmitting an evidence about a piece of information without revealing the information itself.

Bit commitment scheme consists of two phases *commit* and *reveal* executed by two parties, a sender (or committer) Alice, and a receiver Bob. First, Alice and Bob execute the commit phase that results in Bob holding an evidence of A's input value a. Ideally, the receiver should learn no information about a from this. Later, Alice and Bob may execute the opening phase after which Bob outputs "accept", or "reject". Note that in principle, the opening phase may never happen. Formally, the ideal commitment scheme must satisfy the following properties:

- *Concealing*: If Alice is honest, then committing to a reveals no information about a to Bob.
- *Binding*: If the receiver Bob is honest, then he always accepts with some value which is exactly the same that the honest Alice decides to commit to. Furthermore, Alice cannot open the commitment such that Bob accepts a different value.
- *Soundness*: If both parties behave honestly, then Bob always accepts.

Commitment schemes are essential in the construction of a number of cryptographic protocols. General zero-knowledge proofs and arguments of [10] and [4] as well as multi-party computations of [6] and [11] are based on commitment schemes. In the computational model, it is possible to build the bit commitment schemes which are unconditionally binding and computationally concealing (see, e.g., [15]). At the same time, there also exist the schemes (see, e.g., [6]) which are unconditionally concealing and computationally binding. Computational security involves an assumption that some problem is intractable for adversaries whose computational power is assumed to be polynomial. In the *unconditional* (or *information theoretic*) security model, adversaries are allowed unlimited computing power. We shall demand unconditional security for both Alice and Bob.

However, it is impossible to construct a commitment which is both unconditionally binding and hiding, and based on noiseless communications without any additional assumption. The intuitive reason is the so-called symmetry condition on what participants know about each other's data. Since both parties possess the entire transcript of the conversations that has taken place between them, in a two-party case, Alice can determine *exactly* what Bob knows about Alice's data, and the same holds for Bob. One of the methods to break the symmetry condition was presented by Crépeau and Kilian in [7] and later developed by Crépeau in [5]. Their idea was to construct BC based on noisy channels. In [7], a reduction of oblivious transfer to binary symmetric channel was presented, while oblivious transfer, in turn, implies BC according to [3]. In [5], there was introduced a bit commitment protocol which was based directly on binary symmetric channel. Finally, a BC scheme based on a weaker (and more realistic) assumption of *unfair* noisy channel (where the parties have partial control over the randomness introduced by the channel) was presented by Damgård, Kilian and Salvail in [9]. Recently, Winter, Nascimento and Imai [17] introduced a concept of *commitment capacity*, which is a ratio between the length of the string

1-4244-0504-1/06/$20.00 ©2006 IEEE

Alice commits to and the number of times the noisy channel is used when performing the protocol. Commitment capacity of a discrete memoryless channel appeared to be equal to the equivocation of the channel after its trivial redundancy is removed [17].

A protocol proposed in [17] is non-interactive, but their scheme is a non-constructive one, that is, only existence of a protocol achieving the commitment capacity was proved. Here, we show that if interaction is permitted in the commit phase then we obtain efficient optimal protocols. In other words, we show a protocol which efficiently achieves the commitment capacity of discrete memoryless systems (channels and correlations). By allowing interaction during the commit phase and using universal hash functions [8], we obtain a protocol with security failure probabilities decreasing exponentially fast in a security parameter which is a number of noisy system invocations. The protocol [5] is also interactive but our possibility result extends to any discrete memoryless system, besides, we point out that universal hash functions are enough, we do not need in addition a random linear code as in [5]. Our protocol is inspired by the scheme proposed in [9], a similar protocol was also sketched in [18] but no analysis was provided.

We use a security model and definitions first introduced in [17]. It is also worth noting that our proof of optimality for the efficient protocol, although going along the lines of [17], is simpler than the former one.

This paper is organized as follows, in Section II we review the security model and basic definitions. Our protocol and its security proof is presented in Section III. A proof of optimality for this protocol is introduced in Section IV. In Section V, we discuss our results and open questions.

II. Model

We review here the model proposed in [17]. The sender Alice wants to commit to a message a from a certain set $\mathcal{A}$. A commitment scheme consists of two stages: first the commit phase, in which Alice (based on a) and Bob exchange messages, according to the protocol. This will leave Bob with a record (usually called a *view*), to be used in the second stage, the reveal phase. This consists of Alice disclosing a and other relevant information to Bob. Bob performs a test on all his recorded data which accepts if Alice followed the protocol and disclosed the correct information in the second stage, and rejects if cheating is discovered.

In order to be useful, such a scheme has to fulfill three aforementioned requirements: it must be concealing, sound and binding. For unconditional security setting, the first property means that after the commit phase Bob has a negligible information about a (i.e., even though Alice has committed herself to something by the communications to Bob, this commitment remains secret), and this has to hold even if Bob does not follow the protocol, while Alice does. From here on, by saying "negligible", we mean exponentially small in some security parameter. At the same time, by saying that something holds "with high probability", we mean that it is true except with probability negligible in some security parameter. Soundness implies that if both parties behave according to the protocol, Bob's test will accept with high probability after the reveal phase. The protocol to be binding means that Bob's test is such that whatever Alice did in the commit phase (with Bob following the rules) there is only at most one a she can "reveal" which passes Bob's test with high probability.

In our present consideration there is an unlimited bidirectional noiseless channel available between Alice and Bob, and in addition a discrete memoryless noisy channel $W : \mathcal{X} \to \mathcal{Z}$ 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 $W_{x^n}^n = W_{x_1} \otimes \cdots \otimes W_{x_n}$.

Definition 1: The channel W is called *non–redundant*, if none of its output distributions is a convex combination of its other output distributions:

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

where $x, y \in \mathcal{X}$, P is a probability distribution. In geometric terms, this means that all distributions W_x are distinct extremal points of the polytope $\mathcal{W} = \operatorname{conv}\{W_x : x \in \mathcal{X}\}$, the convex hull of the output distributions within the probability simplex over $\mathcal{Z}$. Clearly, we can make W into a non–redundant channel $\widetilde{W}$ by removing all input symbols x whose output distribution W_x is not extremal. The old channel can be simulated by the new one, because by feeding it distributions over input symbols one can generate the output distributions of the removed symbols.

The channel W is called *trivial*, if after making it non–redundant its output distributions have mutually disjoint support. This means that from the output one can infer the input with certainty.

With this we can pass to a formal definition of a protocol: this, consisting of the named two stages, involves creation on Alice's side of either messages intended for the noiseless channel, or inputs to the noisy channel, based on previous messages received from Bob via the noiseless channel, which themselves are based on data received before, etc. Both agents may employ probabilistic choices, which we model by Alice and Bob each using a random variable, M and N, respectively. This allows them to use *deterministic* functions in the protocol. Note that this makes all messages sent and received into well-defined random variables, *dependent on* a.

Commit Phase: The protocol goes for r rounds of Alice–to–Bob and Bob–to–Alice noiseless communications U_j and V_j. After round r_i ($r_1 \leq \ldots \leq r_n \leq r$) Alice will also send a symbol X_i down the noisy channel W, which Bob receives as Z_i. Setting $r_0 = 0$ and $r_{n+1} = r$:
Round $r_i + k$ ($1 \leq k \leq r_{i+1} - r_i$): Alice sends $U^{r_i+k} = f_{r_i+k}\big(a, M, V^{r_i+k-1}\big)$ noiselessly. Bob answers $V_{r_i+k} = g_{r_i+k}\big(Z^i, N, U^{r_i+k}\big)$, also noiselessly. After round r_i and before round $r_i + 1$ ($1 \leq i \leq n$), Alice sends $X_i = F_i\big(a, M, V^{r_i}\big)$, which Bob receives as $Z_i = W(X_i)$.

Reveal Phase: A similar procedure as the commit phase, but without the noisy channel uses, including Alice's sending a to Bob. At the end of the exchange, Bob performs a test as to whether to accept Alice's behavior or not. It is easy to see that this procedure can be simulated by Alice simply telling Bob a and M, after which Bob performs his test $\beta\big(Z^n, N, U^r; a, M\big) \in \{\mathrm{ACC}, \mathrm{REJ}\}$, i.e., requiring Alice to reveal M and a makes cheating for her only more difficult.

Now, the mathematical form of the conditions for concealing as well as for soundness and binding is the following: we call the above protocol ϵ–*concealing* if for any two messages $a, a' \in \mathcal{A}$ and any behavior of Bob during the commit phase,

$$\frac{1}{2}\big\|\mathrm{Distr}_a(Z^n NU^r) - \mathrm{Distr}_{a'}(Z^n NU^r)\big\|_1 \leq \epsilon, \qquad \text{(A)}$$

where $\mathrm{Distr}_a(Z^n NU^r)$ is the distribution of the random variables $Z^n NU^r$ after completion of the commit phase which Alice entered with the message a and the randomness M, and with the ℓ_1–norm $\|\cdot\|_1$; the left side of the above inequality is in fact identical to the total variational distance between the distributions. This is certainly the strongest requirement one could wish for: it says that no statistical test of Bob immediately after the commit phase can distinguish between a and a' with probability larger than ϵ. Note that V^r is a function of $Z^n NU^r$, and hence could be left out in Equation (A). Assuming any probability distribution on the messages, a is the value of a random variable A, and it is jointly distributed with all other variables of the protocol. Then for $\epsilon \leq 1/4$ and any possible Bob's strategy,

$$I\big(A; Z^n NU^r\big) \leq \epsilon' = 2H(2\epsilon, 1-2\epsilon) + 8\epsilon \log|\mathcal{A}|, \qquad \text{(A')}$$

where $I(X;Y) = H(X) + H(Y) - H(XY)$ is the mutual information between X and Y, $H(X)$ is the entropy of X, and $H(p, 1-p)$ is a binary entropy, $0 \leq p \leq 1$ [16]. Equation A' follows from Equation A according to [1]. All exponents and logarithms in this paper are always to basis 2 unless otherwise stated.

We call the protocol δ–*sound and* –*binding* (δ–*binding* for short), if for Alice and Bob following the protocol, for all $a \in \mathcal{A}$,

$$\Pr\big\{\beta\big(Z^n NU^r; aM\big) = \mathrm{ACC}\big\} \geq 1 - \delta, \qquad \text{(B1)}$$

and, whatever Alice does during the commit phase, governed by a random variable S with values σ (which determines the distribution of $Z^n NU^r$), for all $A = a(S, V^r)$, $A' = a'(S, V^r)$, $\widetilde{M} = \mu(S, V^r)$ and $\widetilde{M}' = \mu'(S, V^r)$ such that $A \neq A'$ with probability 1,

$$\Pr\Big\{\beta\big(Z^n NU^r; A\widetilde{M}\big) = \mathrm{ACC} \ \wedge \ \beta\big(Z^n NU^r; A'\widetilde{M}'\big) = \mathrm{ACC}\Big\} \leq \delta. \qquad \text{(B2)}$$

Note that by convexity the cheating attempt of Alice is w.l.o.g. *deterministic*, which is to say that S takes on only one value σ with non-zero probability, hence $\Pr\{S = \sigma\} = 1$.

Definition 2: We call $\frac{1}{n}\log|\mathcal{A}|$ the *(commitment) rate* of the protocol. A rate R is said to be *achievable* if there exist commitment protocols for every n with rates converging to R, which are ϵ-concealing and δ–binding with $\epsilon, \delta \to 0$ as $n \to \infty$. Observe that our definitions are such that with a rate R any smaller rate is also achievable. The *commitment capacity* $C_{\mathrm{com}}(W)$ of W is the supremum of all achievable rates.

III. Main Result

We present here our protocol and argue its security.

Commit Phase

1) Alice chooses a random string $r_1, \ldots, r_n$ of dimension n belonging to the input alphabet of the channel and sends it to Bob over the noisy channel W.
2) After receiving the string $r'_1, \ldots, r'_n$, where $r'_i = W(r_i)$, Bob chooses a set S at random, $S \subset \{1, 2, \ldots, n\}$, $|S| = \eta n, \eta > 0$, s.t. ηn is an integer and all the elements of S are distinct. Bob then sends the set S to Alice over the noiseless channel.
3) Denote the jth element of S by $S(j)$. After receiving S, Alice computes the row vector $\bar{r} = [r_{S(1)}, \ldots, r_{S(\eta n)}]$. She sends $\bar{r}$ to Bob over the noiseless channel.
4) Alice selects a two-universal hash function $V : \mathcal{X} \to \{0,1\}^{n(H(X|Z) - \epsilon' - \eta)}$, where $H(X|Z)$ is the equivocation of W and ϵ' is some positive constant less than 1; an 1-to-1 invertible mapping π: $\mathcal{A} \to \{0,1\}^{n(H(X|Z) - \epsilon' - \eta)}$ and computes $com(a) = \pi(a) \oplus V(r_1, \ldots, r_n)$ where $a \in \mathcal{A}$ is the string she wants to commit to and "$\oplus$" is a bitwise XOR. Then Alice announces $V, \pi, com(a)$ to Bob over the noiseless channel.

Reveal Phase

1) Alice announces $r_1, \ldots, r_n$ to Bob over the noiseless channel. The Bob checks:
   a) if $r_1, \ldots, r_n$ and $r'_1, \ldots, r'_n$ are jointly typical w.r.t. $W^n_{r_1, \ldots, r_n}$,
   b) if for all $i \in S : \bar{r}(i) = r_i$ and,
   c) if $a = \pi^{-1}\big(com(a) \oplus V(r_1, \ldots, r_n)\big)$.
   If all tests pass successfully then Bob accepts and outputs a, otherwise rejects.

Remark 3: Note that this protocol achieves the rate $H(X|Z)$ according to Definition 2 as the size of $\mathcal{A}$ could be at most $n(H(X|Z) - \epsilon' - \eta)$ due to the conditions in Step 4 of the commit phase, but ϵ and η are constants independent of n.

Remark 4: This protocol can be easily generalized to be based on noisy correlations using methods similar to the ones presented in [17]. The details on this will appear in the full version of this paper.

Let us now argue the security of our protocol.

Proposition 5: The above commitment scheme is ϵ-concealing and δ- sound and binding with ϵ and δ negligible in n.

Proof sketch. Soundness follows straightforwardly from the Chernoff bound by the argument similar to the proof of Proposition 7 in [17].

The concealing property follows from the privacy amplification result of [2] (known in the theory of computation as left-over hash lemma [12]). We shall use the formulation of this result taken from [14]:

Lemma 6: Let X be a random variable with range $\mathcal{X}$, and let V be the random variable corresponding to the random choice according to the uniform distribution, of a function out of a universal class of functions mapping $\mathcal{X}$ to $\{0,1\}^m$. Then $H(V(X)|X) \geq m - 2^{m-H_2(X)/\ln 2}$, where $H_2(\cdot)$ denotes Rényi entropy.

We are in the scenario of Lemma 6 with $m = n(H(X|Z) - \epsilon' - \eta)$ where X and Z are random variables describing $r_1, \ldots, r_n$ and $r'_1, \ldots, r'_n$, respectively. In the paper, we consider only asymptotic case: $n \to \infty$, therefore $H_2(X) \geq H(X)$. By observing that from Bob's point of view before the open phase take place, $H(X) = n(H(X|Y) - \eta)$, we conclude that the protocol is indeed concealing. Namely, the information that Bob receives before the revealing phase in exponentially small in n, and therefore Bob's probability ϵ to learn a before the reveal phase is negligible in n.

The binding property can be shown using Lemma 2 from the Appendix of [17]. This interpretation of the Chernoff bound implies the following: suppose that Alice sends a word x^n down a discrete memoryless channel and Bob receives y^n but later Alice reveals the word z^n such that $d_H(x^n, z^n) \geq \sigma n$, $\sigma > 0$. Then, the probability that y^n and z^n are jointly typical is negligible in n. This lemma also implies that in order to cheat successfully with a non-negligible probability, Alice must reveal a word belonging to the n-dimensional Hamming sphere centered in x^n with a radius proportional to $\sqrt{n}$, then she can pass the test (a) in the revealing phase. At the same time, she must also be consistent with the string $\bar{r}$ in order to pass the test (b). However, her probability δ to succeed is negligible as it is the probability that in such Hamming sphere, there exist two sequences with same ηn randomly chosen symbols. Clearly this probability is proportional to $2^{O(\sqrt{n})}/2^{O(n)}$ which is negligible in n. □

Remark 7: Note that our protocol is efficient in the sense that, first, it requires only $O(n)$ invocations of the noisy channel and, second, honest players perform computation which complexity is linear in n.

For the sake of being precise, we also note that our protocol requires $O(n^2)$ communication complexity when counting together with noiseless communications as this is the size of the description of the used universal hash functions. However, as we pointed in the introduction, we consider only the genuine noise as an valuable resource, we only caring about the noisy channel usage.

IV. Upper bounding the achievable rate

Here, we present a simpler (compared to [17]) proof of the fact that the commitment capacity of a noisy channel/correlation is essentially equal to its equivocation.

We assume that W is non–redundant. We shall prove the following assertion, assuming a uniformly distributed variable A taking values on the set $\mathcal{A}$ of messages.

Proposition 8: Consider an ϵ–concealing and δ–binding commitment protocol with n uses of W. Then, for $\delta \leq 1/6$ and $\epsilon \leq 1/4$,

$$(1 - 3\delta - 8\epsilon)\log|\mathcal{A}| \leq 3 + n\max\{H(X|Z) : \mathrm{Distr}(Z|X) = W\} \quad (1)$$

The key, as it turns out, of its proof, is the insight that in the commitment protocol, should it be concealing and binding, X^n together with Bob's view of the commit phase (essentially) determine A. In the more general formulation we permitted in Section II, we prove:

$$H(A|Z^n NU^r X^n) \leq \delta' = H(3\delta, 1-3\delta) + 3\delta\log|\mathcal{A}|. \quad \text{(B')}$$

Intuitively, this means that with the items Alice entered into the commit phase of the protocol and those which are accessible to Bob, not too many values of A should be consistent — otherwise Alice had a way to cheat. In a sense this is just the symmetry condition: with only a noiseless channel, any binding commitment cannot be concealing at all. More rigorously, consider the following simulation of the general commitment protocol using the noisy channel by only noiseless communication, and with an honest but curious Bob: whenever the channel W has to be used, Alice sends the input X_i via the noiseless channel, and Bob simulates the effect of W by local randomness. If the original protocol resulted in a δ–binding commitment, the modified one must have the same property. But since the latter uses only noiseless communication, it must be almost non–concealing. Namely, we have

Proposition 9: Consider a δ–binding commitment of uniform $A \in \mathcal{A}$ based only on noiseless message exchange: formally, let $\widetilde{U}$ be Alice's communication, $\widetilde{V}$ Bob's and M, N Alice's and Bob's private randomness such that all their actions in the multi–round interactive commit phase depend deterministically on their private randomness and all previous communications.

Then Bob has an estimator $\widehat{A} = \widehat{A}(\widetilde{U}N\widetilde{V})$ with the property that $\Pr\{A \neq \widehat{A}\} \leq 3\delta$.

With Fano's inequality, this immediately proves eq. (B').

Proof sketch of Proposition 9. First, consider the following cheating attempt by Alice: she behaves exactly according to the protocol in the commit phase, which leaves her and Bob with the random variables $AM\widetilde{U}$ and $N\widetilde{V}$, respectively. Then, in the reveal phase, she generates a sample N' from the distribution $N|AM\widetilde{U}\widetilde{V}$ (i.e., of Bob's private randomness conditioned on all the other data, which are indeed available to Alice). Then she picks $\widehat{A}\widehat{M}$ maximizing

$$\Pr_{N'}\{\beta(N'\widetilde{U}; \widehat{A}\widehat{M}) = \mathrm{ACC}\},$$

breaking ties in some arbitrarily determined way. By its definition,

$$\Pr\{\beta(N\widetilde{U}; \widehat{A}\widehat{M}) = \mathrm{ACC}\} \geq 1 - \delta, \quad (2)$$

since one could choose $\widehat{A}\widehat{M} = AM$, and noting that the distribution of $AM\widetilde{U}N\widetilde{V}$ equals that of $AM\widetilde{U}N'V$.

Of course, this $\widehat{A}$ may coincide with A occasionally, so let us define

$$\widetilde{A} := \begin{cases} \widehat{A} & \text{if } \widehat{A} \neq A, \\ A' & \text{if } \widehat{A} = A, \end{cases}$$

where A' is different from A with probability 1. Note that this modification makes also $\widetilde{A} \neq A$ with probability 1.

Now, we get from eqs. (2) and (B1) on the one hand, and (B2) on the other,

$$\Pr\{\beta(N\widetilde{U}; \widehat{A}\widehat{M}) = \mathrm{ACC} \ \&\ \beta(N\widetilde{U}; AM) = \mathrm{ACC}\} \geq 1 - 2\delta,$$
$$\Pr\{\beta(N\widetilde{U}; \widetilde{A}\widehat{M}) = \mathrm{ACC} \ \&\ \beta(N\widetilde{U}; AM) = \mathrm{ACC}\} \leq \delta.$$

This of course can only mean that

$$\Pr\{\hat{A} = A\} = \Pr\{\hat{A} \neq \widetilde{A}\} \geq 1 - 3\delta.$$

Now only observe that $\widehat{A}\widehat{M}$ can be sampled by Bob: he, seeing $\widetilde{U}N\widetilde{V}$ in the commit phase, can pick $\widehat{A}\widehat{M}$ such as to maximize

$$\Pr_N\{\beta(N\widetilde{U}; \widehat{A}\widehat{M}) = \mathrm{ACC}\}.$$

By the above arguments, this maximum likelihood decoder will yield $\widehat{A} = A$ with probability at least $1 - 3\delta$. □

Armed with eq. (B'), we can proceed to the

Proof sketch of Proposition 8. We can successively estimate,

$$\begin{aligned} H(X^n|Z^n) &\geq H(X^n|Z^nNU^r) \\ &= H(AX^n|Z^nNU^r) - H(A|Z^nNU^r\,X^n) \\ &\geq H(A|Z^nNU^r) - H(A|Z^nNU^r\,X^n) \\ &\geq H(A|Z^nNU^r) - \delta' \\ &= H(A) - I(A \wedge Z^nNU^r) - \delta' \\ &\geq H(A) - \epsilon' - \delta', \end{aligned}$$

using eq. (B') in the fourth, eq. (A') in the sixth line. On the other hand, subadditivity and the conditioning inequality imply

$$H(X^n|Z^n) \leq \sum_{k=1}^{n} H(X_k|Z_k),$$

yielding the claim, because $H(A) = \log|\mathcal{A}|$ and recalling $\epsilon' \leq 2 + 8\epsilon \log|\mathcal{A}|$, by eq. (A'), and $\delta' \leq 1 + 3\delta \log|\mathcal{A}|$, by eq. (B'). □

Note that for the proofs of the above propositions we considered only a very weak attempt of Alice to cheat: she behaves according to the protocol during the commit phase, and only at the reveal stage she tries to be inconsistent. Similarly, our concealingness condition considered only passive attempts to cheat by Bob, i.e., he follows exactly the protocol, and tries to extract information about A only by looking at his view of the exchange.

Thus, even in the model of *passive cheating* of Alice during the commit phase, which is less restrictive than our definition in Section II, we obtain the upper bound of proposition 8.

Now, Proposition 5, Remarks 3, 4 and 7 and Proposition 8 yield the following.

Corollary 10: The protocol of Section III provides us with a family of efficient bit commitment schemes achieving the commitment capacity of discrete memoryless channels and correlations.

V. Conclusion

We have shown that allowing interaction permits us to build an efficient bit commitment scheme achieving the commitment capacity from an i.i.d. samples of a non-trivial discrete memoryless system (noisy channel or correlation). In the full version of this paper, we will attack the problem of obtaining a commitment scheme from general correlations, not necessarily i.i.d. Constructing an efficient bit commitment from a continuous channel (e.g., the Gaussian channel) remains still open.

References

[1] R. Alicki and M. Fannes, "Continuity of Quantum Conditional Information," *J. Phys. A: Math. Gen.*, vol. 37, no. 5, pp. L55–L57, 2004.

[2] C. H. Bennett, G. Brassard, C. Crépeau, U. Maurer, "Generalized Privacy Amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[3] M. Blum, "Coin flipping by telephone: a protocol for solving impossible problems," *Proc. IEEE Computer Conference*, pp. 133–137, 1982.

[4] G. Brassard, D. Chaum, C. Crépeau, "Minimum disclosure proofs of knowledge," *J. Computer Syst. Sci.*, vol. 37, pp. 156–189, 1988.

[5] C. Crépeau, "Efficient Cryptographic Protocols Based on Noisy Channels," *Proc. EUROCRYPT '97*, LNCS, vol. 1233, pp. 306–317, 1997.

[6] D. Chaum, I. Damgård, and J. van de Graaf, "Multi-party Computations Ensuring Privacy of Each Party's Input and Correctness of the Result," *Proc. CRYPTO '87*, LNCS, vol. 293, pp. 87–119, 1988.

[7] C. Crépeau, J. Kilian, "Achieving oblivious transfer using weakened security assumptions," *Proc. 29th FOCS, IEEE*, pp. 42–52, 1988.

[8] J.L. Carter, M.N. Wegman, "Universal Classes of hash functions," *J. of Computer and Syst. Sci.*, vol. 18, pp. 143–154, 1979.

[9] I. B. Damgård, J. Kilian, L. Salvail, "On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions", *Proc. EUROCRYPT '99*, LNCS, vol. 1592, pp. 56–73, 1999.

[10] O. Goldreich, S. Micali, A. Wigderson, "Proofs that Yield Nothing but the Validity of the Assertion, and the Methodology of Cryptographic Protocol Design," *Proc. 27th IEEE FOCS*, pp. 174–187, 1986.

[11] O. Goldreich, S. Micali, A. Wigderson, "How to Play Any Mental Game, or: A completeness theorem for protocols with honest majority," *Proc. 19th ACM STOC*, pp. 218–229, 1987.

[12] J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby, "A Pseudorandom Generator from any one-way function," *SIAM J. on Comp.*, vol. 28, no. 4., pp. 1364–1396, 1999.

[13] H. Imai, J. Müller-Quade, A. C. A. Nascimento, A. Winter, "Rates for Bit Commitment and Coin Tossing from Noisy Correlation," *Proc. IEEE ISIT '04*, p. 47, 2004.

[14] U. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," *Proc. EUROCRYPT '00*, LNCS, vol. 1807, pp. 351–368, 2000.

[15] M. Naor, "Bit commitment using pseudo–randomness", *J. Cryptology*, vol. 2, no. 2, pp. 151–158, 1991.

[16] C. E. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, vol. 27, pp. 379–423 and 623–656, 1948.

[17] A. Winter, A. C. A. Nascimento, H. Imai, "Commitment Capacity of Discrete Memoryless Channels", *Proc. 9th IMA International Conf. on Cryptography and Coding*, LNCS, vol. 2898, pp. 35–51, 2003.

[18] S. Wolf, J. Wullschleger, "Zero-error information and applications in cryptography", *Proc. IEEE ITW '04*, 2004.