More Extensions of Weak Oblivious Transfer

Minh-Dung Dang

***Abstract*— *Oblivious Transfer* (OT) is a primitive of asymmetrically distributing information between users, proposed to build Secure Computations. In this letter, we propose an information-theoretical variant of OT that requires weak assumptions and can be therefore more easily implemented with transmission media. We show then that *One-out-of-two Oblivious Transfer* (O-OT), the central version of OT, can be reduced to this Weak OT (WOT) with arbitrary small loss of security, i.e. secure O-OT can be realised from our WOT.**

***Index Terms*— Oblivious transfer, information-theoretic security, reduction between protocols.**

I. Introduction

OBLIVIOUS TRANSFER (OT) is an important cryptographic primitive which is used to build asymmetrical cryptographic protocols such as Coin Tossing, Zero-Knowledge Proofs, ..., or more generally, Multi-party Secure Computations [1].

Informally speaking, the original version, proposed by Rabin and so called *Rabin OT* [2], is a transmission scheme where a partner, named Alice, has an one-bit message b to send to another partner, named Bob, who has only a probability $1/2$ to receive b. At the end of the execution, Bob knows if he has got Alice's message or not and Alice does not know what has happened to Bob. Another fraternal protocol, named chosen One-out-of-two Oblivious Transfer (O-OT), was introduced in [3] where Alice has two bits b_0, b_1 and Bob can choose to get one and only one of them while Alice cannot discover Bob's choice. In spite of their equivalence [4], the chosen O-OT has is more preferred thanks to its determinist nature. It was also generalized to get chosen OTs, for instance *one-out-of-two string OT* where b_0, b_1 are two strings, and *m-out-of-n OT* where Bob chooses to get $m < n$ of n Alice's messages. We call these standard OTs.

Such asymmetrical information transmissions are not evident. Within the scope of Modern Cryptography, OTs can be built upon the asymmetry in the field of computational complexity and their security is based on the *unproven* assumptions of the hardness of some problems, such as the factoring of large integers. The doubt about their *computational security* has been increasing as soon as Shor found an efficient factoring algorithm for quantum machine [5].

There nevertheless exists a provable security, the *unconditional security* based on Shannon's theory of information [6], that withstands attacks even by an adversary with unlimited computational power [7]. Following Shannon, an information appears to a person who is interested in it as a random variable X that can take values in a finite set $\{x_1, .., x_N\}$ with probability $\{p(x_1), .., p(x_N)\}$. The degree of knowledge of that person about the information X, or the *equivocation* of X to the person, is defined as the entropy $H(X) = -\sum_{i=1}^{N} p(x_i)\log(p(x_i))$. We denote here the entropy of a binary variable (bit) X, the function that will be used repeatedly in this article:

$$h_2(p) = -p \times \log(p) - (1-p) \times \log(1-p) \qquad (1)$$

for $p = p(X = 0)$ or $p = p(X = 1)$. If the person "knows" the information X by observing an evidence E, a random variable which would take value in $\{e_1, .., e_M\}$, then the degree of knowledge about X, knowing E, is defined as the conditional entropy

$$\begin{aligned} H(X/E) &= \sum_{i=1}^{M} p(e_i) H(X/e_i) \\ &= -\sum_{i,j} p(x_i, e_j)\log(x_i/e_j) \leq H(X) \end{aligned}$$

A system that protects an information X against a person is unconditionally secure if all evidence E that the system reveals to this person does not influence the equivocation of X, i.e. $H(X/E) = H(X)$ [7].

As the equivocation of information has a subjective sense, i.e. two people can have different degrees of knowledge about the same information, we would so use $h_A(X/f)$ to denote the equivocation of X to a person A given the fact f, and $h_A(X)$ for the equivocation of X to A for implicitly all of the given facts at the speaking moment.

We report here the definitions of the two main versions of OT in the light of Shannon's theory (cf. definitions I.1, I.2).

Definition I.1 Rabin OT

Alice has an one-bit message b and sends to Bob. The execution e of the protocol appears as a random binary evidence that takes two schemas $1, 0$ with equal probability. At the end, Bob gets a message b' and knows which schema e has taken value, i.e. $h_B(e) = 0$:

- if $e = 1$, Bob knows that he has received b, i.e. $h_B(b/b', e = 1) = 0$.
- if $e = 0$, Bob knows that he did not receive b, i.e. $h_B(b/b', e = 0) = 1$.

While Alice does not, i.e. $h_A(e) = 1$.

However, we cannot build information-theoretically secure OTs from scratch. Researchers look for reducing it to variants of OT that could be achieved by hypothetical asymmetries in transmission, such as imperfect media or *noisy channels*. There ergo exists a family of variants of OTs. The reductions between them are based on information theory and the realization of one of them implies the others without or with negligible

Ecole Nationale Supérieure des Télécommunications de Paris. Addr: 46 rue Barrault, 75013 Paris, France. Email: dang@infres.enst.fr

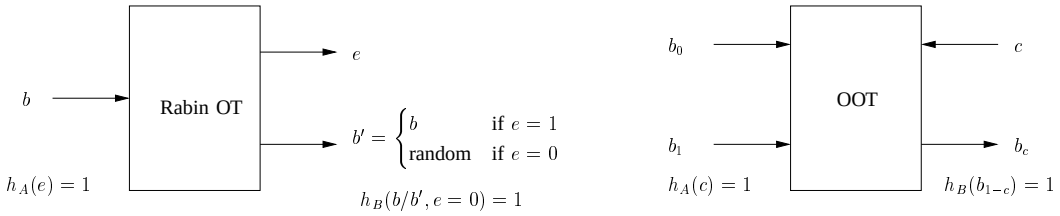

Fig. 1. Rabin's oblivious transfer and One-out-of-two bit oblivious transfer

Definition I.2 O-OT

Alice has two one-bit messages b_0, b_1 that she sends to Bob. Bob has a selection bit $c \in \{0,1\}$ to choose to receive b_c. The execution e has only one schema:

- Bob gets the bit b_c but cannot get b_{1-c}, i.e; $h_B(b_c/e) = 0$ and $h_B(b_{1-c}/e) = 1$.
- Alice does not know the choice c of Bob, i.e. $h_A(c/e) = 1$.

loss of security [4], [8]–[13]. This helps to build OTs, when an hypothetical transmission medium is realized, with the provable unconditional security.

This paper aims at contributing to this movement. The idea is to adjust new members into the family of OTs with weaker assumptions which could match real physical media.

The remaining of the paper is organized as follows. In Section II, we extend Crépeau's OT protocol [4], which is a generalized variant of Rabin OT, to a more general case. We show then, in Section III, that the standard OTs can be reduced to this variant by building a secure O-OT protocol upon it. Some concluding discussions will be exposed in Section IV.

II. A WEAK OT PROTOCOL (WOT)

We introduce here a Weak OT (WOT), that is a variant of Rabin OT, such as the execution e of WOT protocol takes value 1 with probability $\beta \in]0,1[$ and if $e = 0$ then Bob knows that he gets a non-zero equivocation $\alpha \in]0,1[$ of Alice's message. The particular case with $\alpha = 1$ has been studied by Crépeau [4]. Our WOT is thus parameterized by α, β (cf. Definition II.1).

Definition II.1 (α, β)WOT

Alice has an one-bit message b that she sends to Bob. The execution e of the protocol is a random binary variable with $p(e = 1) = \beta$. At the end of the protocol, Bob receives a message b', the value that e has taken and knows:

- $h_B(b/b', e = 1) = 0$
- $h_B(b/b', e = 0) = \alpha$

While Alice gets no more information: $h_A(e) = h_2(\beta)$.

This WOT is a case of asymmetrical transmission, which is more general than Crepeau's instance and Rabin OT and requires weaker assumptions, is obviously more easily realizable.

III. BUILDING O-OT FROM (α, β) WOT

Due to the equivalence of standard OTs, we can reduce these to our variant by only doing it on one of them. We show here that our WOT is suited for building secure One-out-of-two Oblivious Transfer (O-OT) protocol. The construction of O-OT from WOT can be described as in Protocol III.1.

Protocol III.1 *O-OT*$(b_0, b_1)(c)$ from (α, β)*WOT*

1) Alice and Bob agree on security parameter K.
2) Alice chooses at random K bits $m_1, \ldots, m_K$.
3) For $i = 1$ to K: Alice uses a $(\alpha, \beta)WOT$ protocol to send m_i to Bob who gets m'_i and the execution $e[i] \in \{0,1\}$ of i^{th} WOT.
4) Bob selects two subsets $I_0 = \{i_1, ..., i_\gamma\}$ and $I_1 = \{i_{\gamma+1}, ..., i_{2\gamma}\}$ of $\{1, 2, \ldots, K\}$ such that $I_0 \cap I_1 = \emptyset$ and $\forall i \in I_0, e[i] = 1$, where $\gamma = min\{\lfloor 2.K.\beta/3 \rfloor, \lfloor K/2 \rfloor\}$
5) Bob sends (I_c, I_{1-c}) to Alice.
6) Alice receives (I_c, I_{1-c}), computes $\hat{b}_0 = b_0 \oplus \bigoplus_{i \in I_c} m_i$ and $\hat{b}_1 = b_1 \oplus \bigoplus_{i \in I_{1-c}} m_i$, and sends $(\hat{b}_0, \hat{b}_1)$ to Bob.
7) Bob receives $(\hat{b}_0, \hat{b}_1)$ and computes $b_c = \hat{b}_c \oplus \bigoplus_{i \in I_0} m'_i$.

As a cryptographic protocol, the scheme should guarantee its privacy and correctness. The correctness means that the protocol works correctly when all users respect the protocol's instructions and the privacy of the protocol is analyzed in the sense that one dishonest user tries to cheat the other user who is honest.

- *Correctness:* Bob gets the selected bit b_c if Alice and Bob follow the protocol.
- *Privacy:*
  - *At Alice's side:* Alice gains no information about Bob's choice.
  - *At Bob's side:* Bob gets no more than one bit of $\{b_0, b_1\}$.

A. Correctness and Privacy at Bob's side

Now, the execution of WOT rounds can be expressed as a random variable $e = (e[1], ..e[K]) \in \{0,1\}^K$, and as $e[i]$ are independent each of the other, $h_B(m_i/e) = h_B(m_i/e[i])$ knowing m'_i. Let $k_0 = \bigoplus_{i \in I_0} m_i$ and $k_1 = \bigoplus_{i \in I_1} m_i$, then $\hat{b}_c = b_c \oplus k_0$ and $\hat{b}_{1-c} = b_{1-c} \oplus k_1$. At the end of Protocol III.1, Bob receives $\hat{b}_c$ and $\hat{b}_{1-c}$ and has the equivocations

Annex III.1 Privacy amplification via entropy accumulation

Let $V = \bigoplus_{i=1..a} v_i$ where the v_i are random binary variables (bits) with entropy α and $p_\alpha \in]0, 1/2]$ is the probability associated with binary entropy α: i.e. $\alpha = H(v_i) = h_2(p_\alpha)$. We assume without loss of generality that p_α is the probability that each v_i takes the value 1. V takes the value 1 if an odd number of the v_i takes the value 1. Thus:

$$\begin{aligned} p_1 &= p(V=1) = C_a^1 p_\alpha (1-p_\alpha)^{a-1} + ... + C_a^{2n+1} p_\alpha^{2n+1} (1-p_\alpha)^{a-2n-1} + ... \\ p_0 &= p(V=0) = C_a^0 (1-p_\alpha)^a + ... + C_a^{2n} p_\alpha^{2n} (1-p_\alpha)^{a-2n} + ... \end{aligned}$$

Then, we have:

$$\begin{aligned} |p_0 - p_1| = & \Big| C_a^0 (1-p_\alpha)^a + ... + C_a^{2n} p_\alpha^{2n} (1-p_\alpha)^{a-2n} + .. \\ & - C_a^1 p_\alpha (1-p_\alpha)^{a-1} - ... - C_a^{2n+1} p_\alpha^{2n+1} (1-p)^{a-2n-1} - ... \Big| \\ = & \left| \sum_{i=0}^{a-1} C_a^i (-p_\alpha)^i (1-p_\alpha)^{a-i} \right| = |(1-p_\alpha) - p_\alpha|^a = |1-2p_\alpha|^a = (1-2p_\alpha)^a \end{aligned}$$

and the entropy of V is $H_{V,\alpha}(a) = h_2(p_0) = h_2(p_1)$. Thus, given $\alpha \in]0, 1[$, $H_{V,\alpha}$ is an increasing function of a, i.e $\frac{\partial H_{V,\alpha}}{\partial a} > 0$. We can define the reversed $H_{V,\alpha}^{-1}$ as $H_{V,\alpha}^{-1}(x) = l - 1$ where $l = min\{a | H_{V,\alpha}(a) \geq x\}$, for $x \in]0, 1[$. We can say $H_{V,\alpha}(a) < x$ if and only if $a \leq H_{V,\alpha}^{-1}(x)$. When ϵ is very small, we can estimate $H_{V,\alpha}^{-1}(1-\epsilon)$ as $F^{-1}(1-\epsilon)$ where $F(a) = 1 - (1-2p_\alpha)^a$ and then $H_{V,\alpha}^{-1}(1-\epsilon) \approx a$ where $(1-2p_\alpha)^a \lessapprox \epsilon$.

$h_B(b_c) = h_B(k_0), \quad h_B(b_{1-c}) = h_B(k_1)$ depending on his setting of I_0, I_1 [7]. The analyses of equivocation of k_0, k_1 are exposed in Annex III-A.

We define two variables $\mathcal{C}, \mathcal{P}_\epsilon : \{0,1\}^K \mapsto \{0,1\}$ representing the correctness and the privacy of the protocol. For each execution $e \in \{0,1\}^K$ of WOT rounds, $\mathcal{C}(e) = 1$ if Bob receives enough bits m_i to honestly set up I_0 sharing k_0 with Alice; and $\mathcal{P}_\epsilon(e) = 1$ if Bob cannot has enough m_i with $h_B(m_i) = 0$ to reduce the entropies of both k_0, k_1 below a privacy threshold $1-\epsilon$, i.e. $max\{h_B(k_0), h_B(k_1)\} \geq 1-\epsilon$ whatever his repartition of I_0, I_1 .

We recall here Bernshtein's Law of Large Numbers that will be used in our security demonstrations.

Annex III.2 Bernshtein's Law of Large Numbers

Let $X_1, X_2, ..., X_n$ be independent random variables following a Bernoulli distribution with p as the probability parameter. Then for any $0 < \mu < p(1-p)$,

$$p\left(\left| \frac{\sum_{i=1}^n X_i}{n} - p \right| \geq \mu \right) \leq 2e^{-n\mu^2}$$

From this law of large numbers, we can assume with a signification probability that, after K rounds of WOT, the number of m_i successfully received by Bob, i.e. $e[i] = 1$, is sufficient to set up γ indexes in I_0 and not sufficient to set up 2γ indexes in both I_0, I_1 (cf. Figure III-A).

We consider $p(\mathcal{C} = 1)$ the probability that after the execution of WOT rounds the honest Bob gets b_c, and $p(\mathcal{P}_\epsilon = 0)$ the probability that after the execution of WOT rounds, a dishonest Bob can set up I_0, I_1 reducing both the equivocations of two bits b_c and b_{1-c} below $1-\epsilon$.

Theorem 1: Let constant $s \geq 1$, we can choose K such that
1) $p(\mathcal{C} = 1) \geq 1 - e^{-s}$.
2) given $\epsilon > 0$, $p(\mathcal{P}_\epsilon = 0) \leq e^{-s}$.

Proof: We denote a random variable $X_i = \sum_{j=1}^i e[j]$ that represents the number of bits m_i known by Bob after the execution e. We can write

$$p(\mathcal{C} = 1) = p(X_K \geq \gamma) = 1 - p(X_K < \gamma) \tag{2}$$

Given an occurrence of e, we define $one_e(I_j) = \sum_{i \in I_j} e[i]$ and $zero_e(I_j) = \gamma - one_e(I_j)$ for any partition I_0, I_1 of Bob. As $h_B(k_j) = h_B(\bigoplus_{i \in I_j \wedge e[i]=0} m_i) = H_{V,\alpha}(zero_e(I_j))$ and $max\{zero_e(I_0), zero_e(I_1)\} \geq \lceil (2\gamma - X_K)/2 \rceil$, we have $max\{h_B(k_0), h_B(k_1)\} \geq H_{V,\alpha}(\lceil (2\gamma - X_K)/2 \rceil)$. Therefore

$$\begin{aligned} p(\mathcal{P}_\epsilon = 0) &\leq p\left(\left\lceil \frac{2\gamma - X_K}{2} \right\rceil \leq H_{V,\alpha}^{-1}(1-\epsilon) \right) \\ &\leq p\left(\frac{2\gamma - X_K}{2} \leq H_{V,\alpha}^{-1}(1-\epsilon) \right) \\ &= p\left(2\gamma - X_K \leq 2H_{V,\alpha}^{-1}(1-\epsilon) \right) \end{aligned} \tag{3}$$

We consider the two different cases of γ as follows.

a) Case 1: $\gamma = \lfloor \mathbf{2.K}.\beta/\mathbf{3} \rfloor$ **when** $\beta \leq \mathbf{3/4}$
Following Bernshtein's Law of Large Numbers, we choose $\mu = \frac{\beta}{4}$ and have

$$p\left(\left| \frac{X_K}{K} - \beta \right| \geq \frac{\beta}{4} \right) \leq 2e^{-K\beta^2/16} \leq e^{-s}$$

for $K \geq 16(ln(2) + s)/\beta^2$. We can rewrite (2) as

$$\begin{aligned} p(\mathcal{C} = 1) &= 1 - p\left(X_K < \left\lfloor \frac{2.K.\beta}{3} \right\rfloor \right) \\ &\geq 1 - p\left(X_K \leq \frac{2.K.\beta}{3} \right) \\ &= 1 - p\left(\beta - \frac{X_K}{K} \geq \frac{\beta}{3} \right) \\ &\geq 1 - p\left(\beta - \frac{X_K}{K} \geq \frac{\beta}{4} \right) \end{aligned}$$

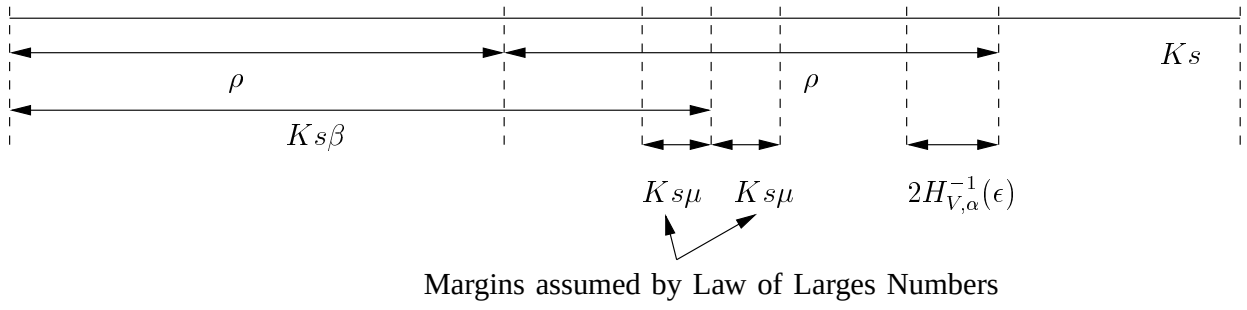

Fig. 2. Correctness and Privacy at Bob's side assumed by Law of Large Numbers

With $K \geq 16(ln(2)+s)/\beta^2$, we assume

$$p(\mathcal{C}=1) \geq 1 - p\left(\left|\beta - \frac{X_K}{K}\right| \geq \frac{\beta}{4}\right) \geq 1 - e^{-s}$$

Aside, we have

$$\begin{aligned} p(\mathcal{P}_\epsilon = 0) &\leq p\left(2\left\lfloor\frac{2.K.\beta}{3}\right\rfloor - X_K \leq 2H_{V,\alpha}^{-1}(1-\epsilon)\right) \\ &\leq p\left(2\frac{2.K.\beta}{3} - 2 - X_K \leq 2H_{V,\alpha}^{-1}(1-\epsilon)\right) \\ &= p\left(\frac{X_K}{K} - \beta \geq \frac{\beta}{3} - \frac{2(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{K}\right) \end{aligned}$$

If we choose $K \geq \frac{24(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{\beta}$ such that $\frac{2(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{K} \leq \frac{12}{\beta}$ then

$$p(\mathcal{P}_\epsilon = 0) \leq p\left(\frac{X_K}{K} - \beta \geq \frac{\beta}{4}\right) \leq p\left(\left|\frac{X_K}{K} - \beta\right| \geq \frac{\beta}{4}\right) \leq e^{-s}$$

for $K \geq \frac{16(ln(2)+s)}{\beta^2}$. Therefore, we can assume $p(\mathcal{C}=1) \geq 1-e^{-s}$ and $p(\mathcal{P}_\epsilon = 0) \leq e^{-s}$ by choosing

$$K \geq max\left\{\frac{16(ln(2)+s)}{\beta^2}, \frac{24(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{\beta}\right\} \quad (4)$$

b) Case 2: $\gamma = \lfloor \mathbf{K/2} \rfloor$ **when** $\beta > \mathbf{3/4}$

(2) can be rewritten as

$$\begin{aligned} p(\mathcal{C}=1) &= 1 - p\left(X_K < \left\lfloor\frac{K}{2}\right\rfloor\right) \\ &\geq 1 - p\left(X_K \leq \frac{K}{2} \Big/ \beta = \frac{3}{4}\right) \\ &\geq 1 - e^{-s} \quad \text{for } K \geq \frac{16(ln(2)+s)}{(3/4)^2} \end{aligned}$$

We should rewrite (3) as

$$\begin{aligned} p(\mathcal{P}_\epsilon = 0) &\leq p\left(2\left\lfloor\frac{K}{2}\right\rfloor - X_K \leq 2H_{V,\alpha}^{-1}(1-\epsilon)\right) \\ &\leq p\left(K - 2 - X_K \leq 2H_{V,\alpha}^{-1}(1-\epsilon)\right) \\ &= p\left(\frac{X_K}{K} - \beta \geq 1 - \beta - \frac{2(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{K}\right) \end{aligned}$$

Following Bernshtein's Law of Large Numbers, we can choose $\mu = \frac{3(1-\beta)}{4}$ and have

$$p\left(\left|\frac{X_K}{K} - \beta\right| \geq \frac{3(1-\beta)}{4}\right) \leq 2e^{-K9(1-\beta)^2/16} \leq e^{-s}$$

for $K \geq \frac{16(ln(2)+s)}{9(1-\beta)^2}$. If we choose $K \geq \frac{8(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{(1-\beta)}$ such that $\frac{2(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{K} \leq \frac{1-\beta}{4}$, then

$$\begin{aligned} p(\mathcal{P}_\epsilon = 0) &\leq p\left(\frac{X_K}{K} - \beta \geq \frac{3(1-\beta)}{4}\right) \\ &\leq p\left(\left|\frac{X_K}{K} - \beta\right| \geq \frac{3(1-\beta)}{4}\right) \leq e^{-s} \end{aligned}$$

for $K \geq \frac{16(ln(2)+s)}{9(1-\beta)^2} \geq \frac{16(ln(2)+s)}{(3/4)^2}$, when $\gamma > 3/4$. Therefore, we can assume $p(\mathcal{C}=1) \geq 1-e^{-s}$ and $p(\mathcal{P}_\epsilon = 0) \leq e^{-s}$ by choosing

$$K \geq \left\{\frac{16(ln(2)+s)}{9(1-\beta)^2}, \frac{8(H_{V,\alpha}^{-1}(1-\epsilon)+1)}{(1-\beta)}\right\} \quad (5)$$

In conclusion, we can choose K to assume $p(\mathcal{C}=1) \geq 1-e^{-s}$ and $p(\mathcal{P}_\epsilon = 0) \leq e^{-s}$ as shown in (4) and (5). ■

B. Privacy at Alice's side

Theorem 2: Protocol III.1 is unconditionally secure at Alice's side.

Proof: All information that Alice has are the probability distribution D of the execution e of WOT rounds, with $p(e[i]=1) = \beta$ and the pair (I_c, I_{1-c}) returned from Bob. She can so guess c with

$$p(c=0/(I_c, I_{1-c}), D) = \frac{p((I_c = I_0), (I_{1-c} = I_1)/D)p(c=0)}{p(I_c, I_{1-c}/D)}$$
$$p(c=1/(I_c, I_{1-c}), D) = \frac{p((I_c = I_1), (I_{1-c} = I_0)/D)p(c=1)}{p(I_c, I_{1-c}/D)}$$

where $p(I_c, I_{1-c}/D)$ is the probability that Bob returns (I_c, I_{1-c}) to Alice, given D. We suppose that honest Bob randomly selects I_0 as any subset of γ members from $\{i \mid e[i]=1\}$ when he receives an occurrence of the execution e of WOT rounds, and I_1 is randomly chosen from the

remaining indexes. The above equations can be rewritten as

$$p(c = 0/(I_c, I_{1-c}), D) = \frac{p(I_c = I_0/D)^2}{2p(I_c, I_{1-c}/D)C^{\gamma}_{K-\gamma}}$$

$$p(c = 1/(I_c, I_{1-c}), D) = \frac{p(I_{1-c} = I_0/D)^2}{2p(I_c, I_{1-c}/D)C^{\gamma}_{K-\gamma}}$$

For $a \geq \gamma$, we use e^a to denote any occurrence of e such that $\sum_i e[i] = a$ and, for each $I \subset \{1, .., K\}$ with $|I| = \gamma$, we define e^a_I as any e^a with $\forall i \in I, e^a[i] = 1$. We state that the distribution D is "bit-sum" uniform, i.e. all occurrence e with the same bit-sum are assigned a same probability: $p(e^a/D) = \beta^a(1-\beta)^{K-a}$. As Bob selects I in a random manner, we have $p(I = I_0/e^a_I) = \frac{1}{C^{\gamma}_a}$ meanwhile $p(I = I_0/e^a) = 0$ if e^a is not a e^a_I. We have

$$\begin{aligned} p(I = I_0/D) &= \sum_{K \geq a \geq \gamma} \sum_{e^a_I} p(e^a_I/D) p(I = I_0/e^a_I) \\ &= \sum_{K \geq a \geq \gamma} \frac{1}{C^{\gamma}_a} \beta^a (1-\beta)^{K-a} \end{aligned}$$

which is constant for any I with $|I| = \gamma$. Therefore $\forall I_c, I_{1-c}, p(I_c = I_0/D) = p(I_{1-c} = I_0/D)$ and so $p(c = 0/(I_c, I_{1-c}), D) = p(c = 1/(I_c, I_{1-c}), D)$. We conclude that after the execution E of the protocol, if Alice receives (I_c, I_{1-c}) then the equivocation of Bob's choice $h_A(c) = h_2(c/(I_c, I_{1-c}), D) = 1$. We say that the protocol is secure against Alice whatever received (I_c, I_{1-c}). ■

IV. More Extensions and Concluding Remarks

In a WOT as described in Definition II.1, the equivocation of Alice's message is fixed to α when Bob does not receive the message. We can remark that the reduction in Protocol III.1 remains secure for more general cases of WOT. For example, suppose that with the WOT, the honest Bob has a chance β to get Alice's bit while any dishonest Bob must get an equivocation $\alpha \geq \alpha_0 > 0$ of Alice's bit with probability $\beta' \geq (1 - \frac{4\beta}{3}) + \epsilon$. With this new extended WOT, the O-OT protocol is secure because we can assume that honest Bob can get enough bits m_i to set up γ indexes in I_0 while dishonest Bob can not set up 2γ indexes in both I_0, I_1 with zero equivocation.

The above extended WOT can be simulated by a quantum transmission where Alice is honest as follows. Alice prepares one of two non-orthogonal quantum states to encode her bit and sends to Bob who freely chooses any measurement to discover Alice's message. Due to the *quantum uncertainty principle*, the honest Bob can successfully get Alice's message with a maximally bounded probability while any dishonest Bob has always a minimally bounded probability to get a non-zero equivocation. This constrained quantum WOT is suited for the reduction described in Protocol III.1 [14]. Unfortunately, in the case where Alice is dishonest, she can control the probability distribution at Bob's side and get information about c, based on returned I_c, I_{1-c} (see [14] for more details). Moreover, the insecurity of such a quantum O-OT is confirmed by the theorems on the insecurity of general Quantum Bitcommitment and Quantum Secure Computations [15]–[17].

In conclusion, inspired from contributions to reducing between variants of Oblivious Transfer, notably from [4], [12], we have proposed a new variant to extend the OT family by showing that existing variants can be reduced to it. This would make OTs be near, or even match, mathematical and physical realizations (cf. figure 3).

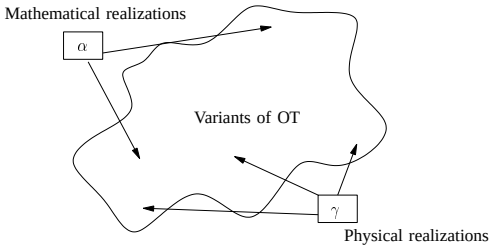

Fig. 3. Realizations of OTs

References

[1] J. Kilian, "Founding cryptography on oblivious transfer," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, 1988, pp. 20 – 31.

[2] M. O. Rabin, "How to exchange secrets by oblivious transfer," technical report TR-81, Aiken Computation Laboratory, Harvard University, Tech. Rep., 1981.

[3] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Communications of the ACM*, vol. 28, no. 6, pp. 637 – 647, 1985.

[4] C. Crepeau, "Equivalence between two flavours of oblivious transfers," in *Proceedings of Advances in Cryptography - Crypto'87*, vol. 293, 1988, pp. 350 – 354.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484 – 1509, 1994.

[6] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.

[7] ——, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28-4, pp. 656–715, 1949.

[8] C. Crepeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions," in *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, 1988, pp. 42 – 52.

[9] C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *Proceedings of Advances in Cryptology - EUROCRYPT'97*, 1997, pp. 306–317.

[10] C. Cachin, "On the foundations of oblivious transfer," in *Proceedings of Advances in Cryptology - EUROCRYPT'98*, 1998, pp. 361– 374.

[11] V. Korjik and K. Morozov, "Generalized oblivious transfer protocols based on noisy channels," in *Proceedings of the International Workshop on Information Assurance in Computer Networks - MMM-ACNS '01*. London, UK: Springer-Verlag, 2001, pp. 219–229.

[12] G. Brassard, C. Crepeau, and S. Wolf, "Oblivious transfers and privacy amplification," *Journal of Cryptology*, vol. 16, no. 4, pp. 219–237, 2003.

[13] C. Crepeau, K. Morozov, and S. Wolf, "Efficient unconditional oblivious transfer from almost any noisy channel," in *Proceedings of Fourth Conference on Security in Communication Networks - SCN'04*, 2004, pp. 47–59.

[14] M.-D. Dang, "Variations on quantum oblivious transfer," 2005, e-print: quant-ph/0506033.

[15] H. Lo and H. Chau, "Is quantum bit commitment really possible ?" *Phys. Rev. Lett.*, vol. 78, pp. 3410 – 3413, 1997.

[16] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Phys. Rev. Lett.*, vol. 78, pp. 3414 – 3417, 1997.

[17] H. K. Lo, "Insecurity of quantum secure computations," *Phys. Rev. A*, vol. 56, no. 2, pp. 1154–1162, 1997, e-print: quant-ph/9512026.