Oblivious Transfer in the Bounded Storage Model

Yan Zong Ding

DEAS, Harvard University, Cambridge MA 02138, USA
zong@deas.harvard.edu

Abstract. Building on a previous important work of Cachin, Crépeau, and Marcil [15], we present a provably secure and more efficient protocol for $\binom{2}{1}$-Oblivious Transfer with a *storage-bounded* receiver. A public random string of n bits long is employed, and the protocol is secure against any receiver who can store γn bits, $\gamma < 1$. Our work improves the work of CCM [15] in two ways. First, the CCM protocol requires the sender and receiver to store $O(n^c)$ bits, $c \sim 2/3$. We give a similar but more efficient protocol that just requires the sender and receiver to store $O(\sqrt{kn})$ bits, where k is a security parameter. Second, the basic CCM Protocol was proved in [15] to guarantee that a dishonest receiver who can store $O(n)$ bits succeeds with probability at most $O(n^{-d})$, $d \sim 1/3$, although repitition of the protocol can make this probability of cheating exponentially small [20]. Combining the methodologies of [24] and [15], we prove that in our protocol, a dishonest storage-bounded receiver succeeds with probability only $2^{-O(k)}$, without repitition of the protocol. Our results answer an open problem raised by CCM in the affirmative.

1 Introduction

Oblivious Transfer (OT) was introduced by Rabin [47] in 1981, and has since then become one of the most fundamental and powerful tools in cryptography. An important generalization, known as one-out-of-two oblivious transfer and denoted $\binom{2}{1}$-OT, was introduced by Even, Goldreich, and Lempel [28] in 1982. Informally speaking, in a $\binom{2}{1}$-OT, a sender Alice has two secret bits $M_0, M_1 \in \{0,1\}$, and a receiver Bob has a secret bit $\delta \in \{0,1\}$. Alice sends M_0, M_1 in such a way that Bob receives M_δ, but does not learn both M_0 and M_1, and Alice learns nothing about δ. Crépeau proved in 1987 that OT and $\binom{2}{1}$-OT are equivalent [19]. In 1988, Kilian proved that every secure two-party and multiparty computation can be reduced to OT [33].

Traditionally, protocols for OT have been based on unproven complexity assumptions that certains problems, such as integer factorization, are computationally hard, or that trapdoor permutations exist. The solutions so obtained, although significant, have a drawback. Namely, they do not guarantee *everlasting security.* A dishonest player can store the entire conversation during the protocol, and attempt to subvert the security of the protocol later, when enabled by breakthroughs in computing technology and/or code-breaking algorithms. While

J. Kilian (Ed.): CRYPTO 2001, LNCS 2139, pp. 155–170, 2001.

determining the computational complexity of factorization, or proving the existence of trapdoor permutations, is still beyond the reach of complexity theory, continuing advances in factoring algorithms will jeopardize the security of protocols based on factoring. In addition, these protocols will become insecure if quantum computers become available [50]. Similar threats exist for protocols based on other hardness assumptions. We thus seek protocols that are provably secure in face of any future advances in algorithms and computing technology.

The ground breaking work of Cachin, Crépeau, and Marcil [15] in 1998 gave the first provably secure protocol for $\binom{2}{1}$-OT in the *Bounded Storage Model*, without any complexity assumption. The bounded storage model, introduced by Maurer [37], imposes a bound B on the adversary's *storage* capacity only. A public random string of n bits long, $n > B$, is employed in order to defeat the adversary. Although a trusted third party is not necessary in principle, in a practical implementation, the string α may be one in a steady flow of random strings $\alpha_1, \alpha_2, \ldots$, each of length n, broadcast from a satellite at a very high rate, and available to all. When α is broadcast, the adversary is allowed to compute an *arbitrary* function f on α, provided that the length $|f(\alpha)| \leq B$.

In the context of OT, the storage bound is placed on one of the two parties, WLOG say the receiver. By the reversibility of OT [21], the case where the storage bound is placed on the sender, is equivalent. The CCM protocol [15] guarantees provable security against any dishonest sender who is unbounded in every way, and against any *computationally unbounded* dishonest receiver who stores no more than $B = \gamma n$ bits, $\gamma < 1$. Furthermore, the security against a dishonest receiver is preserved regardless of future increases in storage capacity. Together with the completeness of OT [33], a fundamental implication of [15] is that every information-theoretically secure two-party and multi-party computation, in principle, is feasible in the bounded storage model.

The work of CCM [15], however, has two undesirable aspects. First, while providing security against a dishonest receiver who stores $B = O(n)$ bits, the CCM protocol also requires honest sender and receiver to store $O(n^c)$ bits, $c \sim 2/3$. Since n is very large, this requirement could be rather excessive. Second, the CCM protocol was proved in [15] to guarantee that a receiver who stores $O(n)$ bits succeeds with probability at most $O(n^{-d})$, $d \sim 1/3$. Note that this probability is usually not as small as desired. Of course, repitition of the protocol can make this probability of cheating exponentially small [20].

Our Results. Building on the work of Cachin, Crépeau, and Marcil [15], we give a similar but more efficient protocol for $\binom{2}{1}$-OT in the bounded storage model. The major difference between our protocol and the CCM Protocol is that the CCM Protocol uses an extra distillation step, which involves many bits divided into polynomially large blocks, and the extraction of a nearly random bit from each block. Getting rid of this distillation step, we reduce the storage requirement to $O(\sqrt{kn})$, where k is a security parameter. Combining the methodologies of [24] and [15], we prove that in our protocol, any dishonest receiver who stores $O(n)$ bits succeeds with probability at most $2^{-O(k)}$, without repetition of the protocol. Our results answer positively an open problem raised in [15].

1.1 Related Work

OT and $\binom{2}{1}$-OT were introduced by Rabin [47] and Even *et al* [28] respectively. Their equivalence was established by Crépeau [19]. There is a vast literature on the relationships between OT and other cryptographic primitives, and between OT variants. OT can be used to construct protocols for secret key agreement [47], [8], [52], contract signing [28], bit commitment and zero-knowledge proof [33], and general secure multi-party computation [52], [30], [31], [33], [32], [35], [36], [22]. It was proved by Kilian that every secure two-party and multi-party computation reduces to OT [33]. Information-theoretic reductions between OT variants were studied in [10], [11], [19], [20], [21], [12], [9], [14], [25].

In traditional cryptography, protocols for OT have been designed under the assumptions that factoring is hard [47], discret log is hard [6], and trapdoor permutations exist [28], [52], [30], [31]. OT has also been studied in the quantum model [7], and the noisy channel model [20]. Recently OT has been extended to various distributed and concurrent settings [5], [49], [29], [44], and these protocols are either based on complexity assumption, or information-theoretically secure using private channels and auxilliary servers. Cachin, Crépeau, and Marcil [15] gave the first secure two-party protocol for $\binom{2}{1}$-OT in the bounded storage and public random string model, without any complexity assumption, and without private channels or auxilliary servers.

The public random string model was introduced by Rabin [48]. The bounded storage model was introduced by Maurer [37]. Secure encryption in the bounded storage model was first studied in [37], [16], but later significantly stronger results appeared in [1], [2], [24]. Information-theoretically secure key agreement was investigated in [38], [39], [16], [40], [41], [42].

The bounded *space* model for zero-knowledge proof was studied in [18], [17], [34], [23], [26], [27], [3]. Pseudorandomness in the bounded space model was studied in [45], [46]. However, note the important difference between the bounded space model and the bounded storage model: the bounded *space* model imposes a bound on the computation space of the adversary, whereas in the bounded *storage* model the adversary can compute an function with arbitrarily high complexity, provided that the length of the output is bounded.

2 Preliminaries

This section provides the building blocks for our protocol and analysis. Throughout the paper, k is a security parameter, n is the length of a public random string, and $B = \gamma n$, $\gamma < 1$, is the storage bound on the receiver Bob. For simplicity and WLOG, we consider $B = n/6$ (i.e. $\gamma = 1/6$). Similar results hold for any $\gamma < 1$.

Definition 1. *Denote* $[n] = \{1, \ldots, n\}$. *Let* $\mathcal{K} \stackrel{d}{=} \{s \subset [n] : |s| = k\}$ *be the set of all* k*-element subsets of* $[n]$.

Definition 2. *For* $s = \{\sigma_1, \ldots, \sigma_k\} \in \mathcal{K}$ *and* $\alpha \in \{0,1\}^n$, *define* $s(\alpha) \stackrel{d}{=} \bigoplus_{i=1}^{k} \alpha[\sigma_i]$, *where* $\oplus$ *denotes XOR, and* $\alpha[\sigma_i]$ *is the* σ_i*-th bit of* α.

Definition 3. *Let $H \subset \{0,1\}^n$. Let $s \in \mathcal{K}$. We say that s is* good *for H if*

$$\left| \frac{|\{\alpha \in H : s(\alpha) = 0\}|}{|H|} - \frac{|\{\alpha \in H : s(\alpha) = 1\}|}{|H|} \right| < 2^{-k/3}. \qquad (1)$$

Thus, if s is good for H, then $\{s(\alpha) : \alpha \in H\}$ is well balanced between 0's and 1's.

Definition 4. *Let $H \subset \{0,1\}^n$. We say that H is* fat *if $|H| \geq 2^{0.813n}$.*

The following Lemma 1 says that if H is *fat*, then *almost all* $s \in \mathcal{K}$ are *good* for H. The lemma follows directly from Main Lemma 1 of [24], by considering k-tuples in $[n]^k$ with *distinct* coordinates.

Lemma 1. *Let $H \subset \{0,1\}^n$. Denote*

$$B_H \stackrel{d}{=} \{s \in \mathcal{K} : s \textit{ is } \text{not } \textit{good for } H\}. \qquad (2)$$

If H is fat*, and $k < \sqrt{n}$* [1]*, then*

$$|B_H| < |\mathcal{K}| \cdot 2^{-k/3} = \binom{n}{k} \cdot 2^{-k/3}. \qquad (3)$$

In Appendix A we will give a proof lemma 1 from Main Lemma 1 of [24].

Notation: Let F be a finite set. The notation $x \stackrel{R}{\longleftarrow} F$ denotes choosing x uniformly from F.

Lemma 2. *Let $0 < \gamma, \nu < 1$ and $\nu < 1 - \gamma$. For any function $f : \{0,1\}^n \longrightarrow \{0,1\}^{\gamma n}$, for $\alpha \stackrel{R}{\longleftarrow} \{0,1\}^n$,*

$$\Pr\left[\left|f^{-1}(f(\alpha))\right| \geq 2^{(1-\gamma-\nu)n}\right] > 1 - 2^{-\nu n}.$$

Proof. Any function $f : \{0,1\}^n \longrightarrow \{0,1\}^{\gamma n}$ partitions $\{0,1\}^n$ into $2^{\gamma n}$ disjoint subsets $\Omega_1, \ldots, \Omega_{2^{\gamma n}}$, one for each $\eta \in \{0,1\}^{\gamma n}$, such that for each i, $\forall \alpha, \beta \in \Omega_i$, $f(\alpha) = f(\beta) = \eta_i \in \{0,1\}^{\gamma n}$. Let $\mu = 1 - \gamma - \nu$. We now bound the number of $\alpha \in \{0,1\}^n$ s.t. $\left|f^{-1}(f(\alpha))\right| < 2^{\mu n}$. Since there are at most $2^{\gamma n}$ j's such that $|\Omega_j| < 2^{\mu n}$, it follows that

$$\begin{aligned} \left|\left\{\alpha \in \{0,1\}^n : |f^{-1}(f(\alpha))| < 2^{\mu n}\right\}\right| &= \sum_{j:|\Omega_j|<2^{\mu n}} |\Omega_j| \\ &< 2^{\gamma n} \cdot 2^{\mu n} = 2^{(1-\nu)n}. \end{aligned}$$

[1] The condition $k < \sqrt{n}$ in Lemma 1 is valid, because k, the security parameter (e.g. $k = 1000$), is negligibly small compared to n (e.g. $n = 10^{15}$), which is larger than the adversary's storage capacity.

Therefore, for $\alpha \xleftarrow{R} \{0,1\}^n$,

$$\begin{aligned}\Pr\left[\left|f^{-1}(f(\alpha))\right| < 2^{\mu n}\right] &= \frac{\left|\left\{\alpha \in \{0,1\}^n : |f^{-1}(f(\alpha))| < 2^{\mu n}\right\}\right|}{2^n} \\ &< \frac{2^{(1-\nu)n}}{2^n} = 2^{-\nu n}.\end{aligned}$$

□

Corollary 1. *For any function $f : \{0,1\}^n \longrightarrow \{0,1\}^{n/6}$, for $\alpha \xleftarrow{R} \{0,1\}^n$,*

$$\Pr\left[f^{-1}(f(\alpha)) \text{ is fat}\right] > 1 - 2^{-0.02n}.$$

Proof. Let $\gamma = 1/6$ and $\nu = 0.02$ in Lemma 2. □

The rest of this section is devoted to the crucial tools employed by the CCM Protocol and our protocol.

2.1 Birthday Paradox

Lemma 3. *Let $\mathcal{A}, \mathcal{B} \subset [n]$ be two independent random subsets of $[n]$ with $|\mathcal{A}| = |\mathcal{B}| = u$. Then the expected size $E[|\mathcal{A} \cap \mathcal{B}|] = u^2/n$.*

Corollary 2. *Let $\mathcal{A}, \mathcal{B} \subset [n]$ be two independent random subsets of $[n]$ with $|\mathcal{A}| = |\mathcal{B}| = \sqrt{kn}$. Then the expected size $E[|\mathcal{A} \cap \mathcal{B}|] = k$.*

We now wish to bound the probability that $|\mathcal{A} \cap \mathcal{B}|$ deviates from the expectation. Note that standard Chernoff-Hoeffding bounds do not directly apply, since elements of the subsets $\mathcal{A}$ and $\mathcal{B}$ are chosen without replacement. We use the following version of Chernoff-Hoeffding from [4].

Lemma 4. [4] *Let $Z_1, \ldots, Z_u$ be Bernoulli trials (not necessarily independent), and let $0 \le p_i \le 1$, $1 \le i \le u$. Assume that $\forall\, i$ and $\forall\,(e_1, \cdots, e_{i-1}) \in \{0,1\}^{i-1}$,*

$$\Pr\left[Z_i = 1 \mid Z_1 = e_1, \ldots, Z_{i-1} = e_{i-1}\right] \ge p_i.$$

Let $W = \sum_{i=1}^{u} p_i$. Then for $\delta < 1$,

$$\Pr\left[\sum_{i=1}^{u} Z_i < W \cdot (1-\delta)\right] < e^{-\delta^2 W/2}. \tag{4}$$

Corollary 3. *Let $\mathcal{A}, \mathcal{B} \subset [n]$ be two independent random subsets of $[n]$ with $|\mathcal{A}| = |\mathcal{B}| = 2\sqrt{kn}$. Then*

$$\Pr\left[|\mathcal{A} \cap \mathcal{B}| < k\right] < e^{-k/4}. \tag{5}$$

Proof. Let $u = 2\sqrt{kn}$. Consider any fixed u-subset $\mathcal{B} \subset [n]$, and a randomly chosen u-subset $\mathcal{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_u\} \subset [n]$. For $i = 1, \ldots, u$, let Z_i be the Bernoulli trial such that $Z_i = 1$ if and only if $\mathcal{A}_i \in \mathcal{B}$. Then clearly

$$\Pr\left[Z_i = 1 \mid Z_1 = e_1, \ldots, Z_{i-1} = e_{i-1}\right] \geq \frac{u - (i-1)}{n - (i-1)} > \frac{u - (i-1)}{n}. \quad (6)$$

Let $p_i = \frac{u - (i-1)}{n}$. Let $W = \sum_{i=1}^{u} p_i$. Then by (6),

$$W > \frac{1}{n} \cdot \sum_{i=1}^{u} i > \frac{u^2}{2n} = 2k. \quad (7)$$

Therefore, (5) follows from (4) and (7), with $\delta = 1/2$. □

2.2 Interactive Hashing

Interactive Hashing is a protocol introduced by M. Noar, Ostrovsky, Venkatesan, and Yung in the context of bit commitment and zero-knowledge proof [43]. Cachin, Crépeau, and Marcil [15] gave a new elegant analysis of interactive hashing. The protocol involves two parties, Alice and Bob. Bob has a secret t-bit string $\chi \in T \subset \{0,1\}^t$, where $|T| \leq 2^{t-k}$ and T is unknown to Alice. The protocol is defined to be correct and secure if

1. Bob sends χ in such a way that Alice receives two strings $\chi_0, \chi_1 \in \{0,1\}^t$, one of which is χ, but Alice does not know which one is χ.
2. Bob cannot force both χ_0 and χ_1 to be in T.

The following interactive hashing protocol is due to [43]. The same idea involving taking inner products over $GF(2)$, was first introduced by Valiant and V. Vazirani earlier in the complexity of UNIQUE SATISFIABILITY [51].

NOVY Protocol: Alice *randomly* chooses $t-1$ *linearly independent* vectors $a_1, \ldots, a_{t-1} \in \{0,1\}^t$. The protocol then proceeds in $t-1$ rounds. In Round i, for each $i = 1, \ldots, t-1$,

1. Alice sends a_i to Bob.
2. Bob computes $b_i = a_i \cdot \chi$, where $\cdot$ denotes inner product, and sends b_i to Alice.

After the $t-1$ rounds, both Alice and Bob have the same system of linear equations $a_i \cdot x = b_i$ over $GF(2)$. Since the vectors $a_1, \ldots, a_{t-1} \in \{0,1\}^t$ are linearly independent, the system of $t-1$ linear equations over $GF(2)$ with t unknowns has exactly two solutions, one of which is χ. Therefore, by solving the systems of equations $a_i \cdot x = b_i$, Alice receives two strings χ_0, χ_1, one of which is χ. It is clear that information-theoretically, Alice does not know which solution is χ. Thus Condition 1 of interactive hashing is satisfied.

The following important lemma, regarding Condition 2 of interactive hashing, was proved in [15]. The same result in a non-adversarial setting, more precisely in the case that the Bob is honest, was proved in [51].

Lemma 5. [15] *Suppose Alice and Bob engage in interactive hashing of a t-bit string, $\lg t \le k \le t$, by the NOVY protocol. Let $T \subset \{0,1\}^t$ be any subset with $|T| \le 2^{t-k}$. Then the probability that Bob can answer Alice's queries in such a way that T contains both strings χ_0, χ_1 received by Alice, is at most $2^{-O(k)}$.*

Corollary 4. *Let Alice and Bob engage in interactive hashing of a t-bit string as above. Let $T_0, T_1 \subset \{0,1\}^t$ be any two subsets with $|T_0|, |T_1| \le 2^{t-k}$. Then the probability that Bob can answer Alice's queries in such a way that either $\chi_0 \in T_0 \wedge \chi_1 \in T_1$, or $\chi_0 \in T_1 \wedge \chi_1 \in T_0$, is at most $2^{-O(k)}$.*

Proof. Let $T = T_0 \cup T_1$ in Lemma 5. □

3 Protocol for $\binom{2}{1}$-OT

Recall that in a $\binom{2}{1}$-OT, the sender Alice has two secret bits $M_0, M_1 \in \{0,1\}$, and the receiver Bob has a secret bit $\delta \in \{0,1\}$. By definition, a $\binom{2}{1}$-OT protocol is correct and secure if the following three conditions are all satisfied:

1. Bob receives M_δ.
2. Bob learns nothing about $M_{1\oplus\delta}$, except with a small probability $\nu(k)$, where k is a security parameter.
3. Alice learns nothing about δ.

3.1 Outline of Basic Ideas

We first outline the basic ideas underling our protocol for $\binom{2}{1}$-OT. First, Alice chooses random $\mathcal{A} \subset [n]$, and Bob chooses random $\mathcal{B} \subset [n]$, with $|\mathcal{A}| = |\mathcal{B}| = u = 2\sqrt{kn}$. Public random string $\alpha \xleftarrow{R} \{0,1\}^n$ is broadcast. Alice retains $\alpha[i]$ $\forall\, i \in \mathcal{A}$, and Bob retains $\alpha[j]$ $\forall\, j \in \mathcal{B}$. Alice then sends her subset $\mathcal{A}$ to Bob, and Bob computes $\mathcal{A} \cap \mathcal{B}$. By the birthday paradox (Corollary 3), with very high probability, $|\mathcal{A} \cap \mathcal{B}| \ge k$.

Fact 1 (Encoding of Subsets) [15] *Each of the $\binom{u}{k}$ k-element subsets of $[u] = \{1, \ldots, u\}$ can be uniquely encoded as a $\lg \binom{u}{k}$-bit string. See* [15] *for an efficient method of encoding and decoding.*

Next, Bob encodes a random k-subset $s \subset \mathcal{A} \cap \mathcal{B}$ as a $\lg \binom{u}{k}$-bit string, and sends s to Alice via the NOVY interactive hashing protocol. By the end of interactive hashing, Alice and Bob will have created two "keys", a good key $S_G = s$, and a bad key S_B, each a k-subset of $\mathcal{A}$, such that: Bob knows $S_G(\alpha)$, but learns nothing about $S_B(\alpha)$, and Alice knows both $S_G(\alpha)$ and $S_B(\alpha)$, but does not know which key is good and which key is bad.

Once the keys S_G and S_B are created, the rest of the protocol is trivial. If Bob wants to read M_δ, then he simply asks Alice to encrypt M_δ with the good key S_G, and $M_{1\oplus\delta}$ with the good key S_B, i.e. Bob ask Alice to send $M_\delta \oplus S_G(\delta)$ and $M_{1\oplus\delta} \oplus S_B(\delta)$. The correctness and security of the protocol follow from the properties of S_B and S_G described above.

3.2 The Protocol, and Main Results

Notation: For a bit $Y \in \{0,1\}$, denote $\overline{Y} \stackrel{d}{=} 1 \oplus Y$.

Definition 5. *Let $\mathcal{X} = \{x_1, \ldots, x_u\}$ be an u-element set. For each subset $J \subset [u]$, define $\mathcal{X}_J \stackrel{d}{=} \{x_i : i \in J\}$.*

Notation: From now on, let $u = 2\sqrt{kn}$.

Our protocol for $\binom{2}{1}$-OT, Protocol A, is described below. Protocol A uses two public random strings $\alpha_0, \alpha_1 \stackrel{R}{\longleftarrow} \{0,1\}^n$. In each of Steps 2 and 3, Alice and Bob each store $u = 2\sqrt{kn}$ bits. In the interactive hashing of Step 4, Alice transmits and Bob stores t^2 bits, where $t = \lg \binom{u}{k} < k \cdot (\lg u - \lg k/e)$. Since $k << n$, the storage requirement is dominated by $O(u) = O(\sqrt{kn})$.

Protocol A:

1. Alice randomly chooses $\mathcal{A}^{(0)} = \left\{\mathcal{A}_1^{(0)}, \ldots, \mathcal{A}_u^{(0)}\right\}$, $\mathcal{A}^{(1)} = \left\{\mathcal{A}_1^{(1)}, \ldots, \mathcal{A}_u^{(1)}\right\} \subset [n]$, with $|\mathcal{A}^{(0)}| = |\mathcal{A}^{(1)}| = u$. Bob also chooses random $\mathcal{B}^{(0)} = \left\{\mathcal{B}_1^{(0)}, \ldots, \mathcal{B}_u^{(0)}\right\}$, $\mathcal{B}^{(1)} = \left\{\mathcal{B}_1^{(1)}, \ldots, \mathcal{B}_u^{(1)}\right\} \subset [n]$, with $|\mathcal{B}^{(0)}| = |\mathcal{B}^{(1)}| = u$.
2. The first public random string $\alpha_0 \stackrel{R}{\longleftarrow} \{0,1\}^n$ is broadcast. Alice stores the u bits $\alpha_0[\mathcal{A}_1^{(0)}], \ldots, \alpha_0[\mathcal{A}_u^{(0)}]$, and Bob stores $\alpha_0[\mathcal{B}_1^{(0)}], \ldots, \alpha_0[\mathcal{B}_u^{(0)}]$.
3. After a short pause, the second public random string $\alpha_1 \stackrel{R}{\longleftarrow} \{0,1\}^n$ is broadcast. Alice stores $\alpha_1[\mathcal{A}_1^{(1)}], \ldots, \alpha_1[\mathcal{A}_u^{(1)}]$, and Bob stores $\alpha_1[\mathcal{B}_1^{(1)}], \ldots, \alpha_1[\mathcal{B}_u^{(1)}]$.
4. Alice sends $\mathcal{A}^{(0)}, \mathcal{A}^{(1)}$ to Bob. Bob flips a coin $c \stackrel{R}{\longleftarrow} \{0,1\}$, and computes $\mathcal{A}^{(c)} \cap \mathcal{B}^{(c)}$. If $\left|\mathcal{A}^{(c)} \cap \mathcal{B}^{(c)}\right| < k$, then $\mathcal{R}$ aborts. Otherwise, Bob chooses a random k-subset $s = \left\{\mathcal{A}_{i_1}^{(c)}, \ldots, \mathcal{A}_{i_k}^{(c)}\right\} \subset \mathcal{A}^{(c)} \cap \mathcal{B}^{(c)}$, and sets $I = \{i_1, \ldots, i_k\}$. Thus by Definition 5, $s = \mathcal{A}_I^{(c)}$.
5. Bob encodes I as a t-bit string, where $t = \lg \binom{u}{k}$, and sends I to Alice via the NOVY interactive hashing protocol in $t-1$ rounds. Alice receives two k-subsets $I_0 < I_1 \subset [u]$. For some $b \in \{0,1\}$, $I = I_b$, but Alice does *not* know b. Bob also computes I_0, I_1 by solving the same system of linear equations, and knows b.
6. Bob sends $\varepsilon = b \oplus c$ and $\tau = \delta \oplus c$ to Alice, where c and b are defined in Steps 4 and 5 respectively.
7. Alice sets $s_0 = \mathcal{A}_{I_\varepsilon}^{(0)}$, $X_0 = s_0(\alpha_0)$, $s_1 = \mathcal{A}_{I_{\overline{\varepsilon}}}^{(1)}$, and $X_1 = s_1(\alpha_1)$. Alice then computes $C_0 = X_\tau \oplus M_0$, and $C_1 = X_{\overline{\tau}} \oplus M_1$, and sends C_0, C_1 to Bob.
8. Bob reads $M_\delta = C_\delta \oplus X_c = C_\delta \oplus \bigoplus_{j=1}^k \alpha_c[\mathcal{A}_{i_j}^{(c)}]$. (Note that an honest Bob following the protocol has stored $\alpha_c[\mathcal{A}_{i_j}^{(c)}]$ $\forall\, 1 \leq j \leq k$. Recall from Step 4 that $\forall\, 1 \leq j \leq k$, $\mathcal{A}_{i_j}^{(c)} \in s \subset \mathcal{B}^{(c)}$).

Remark: Each of $\mathcal{A}^{(0)}, \mathcal{A}^{(1)}, \mathcal{B}^{(0)}, \mathcal{B}^{(1)}$, as described in Protocol A, consists of u independently chosen elements of $[n]$, resulting in $u \lg n$ bits each. However, as noted in [15], we can reduce the number of bits for describing the sets to $O(k \log n)$, by choosing the elements with $O(k)$-wise independence, without significantly affecting the results.

Lemma 6. *The probability that an honest receiver Bob aborts in Step 4 of the protocol, is at most* $e^{-k/4}$.

Proof. By Corollary 3, $\Pr\left[\left|\mathcal{A}^{(c)} \cap \mathcal{B}^{(c)}\right| < k\right] \ < \ e^{-k/4}$. □

The following two lemmas about Protocol A are immediate.

Lemma 7. *The receiver Bob can read* M_δ *simply by following the protocol.*

Lemma 8. *The sender Alice learns nothing about* δ.

Proof. Because Alice does not learn c (defined in Step 4) and b (defined in Step 5) in Protocol A. □

Therefore, Conditions 1 and 2 for a correct and secure $\binom{2}{1}$-OT, are satisfied. We now come to the most challenging part, namely, Condition 3 regarding the security against a dishonest receiver Bob, who can store $B = n/6$ bits, and whose goal is to learn both M_0 and M_1. While α_0 is broadcast in Step 2, Bob computes an *arbitrary* function $\eta_0 = A_0(\alpha_0)$ using unlimited computing power, provided that $|\eta_0| = n/6$; and while α_1 is broadcast in Step 3, Bob computes an arbitrary function $\eta_1 = A_1(\eta_0, \alpha_1)$, $|\eta_1| = n/6$. In Steps 4 - 6, using η_1 and $\mathcal{A}^{(0)}, \mathcal{A}^{(1)}$, Bob employs an arbitrary strategy in interacting with Alice. At the end of the protocol, Bob attempts to learn both M_0 and M_1, using his information η_1 on (α_0, α_1), C_0, C_1 received from Alice in Step 7, and all information $\mathcal{I}$ he obtains in Steps 4 - 6. Thus in particular, $\mathcal{I}$ includes $\mathcal{A}^{(0)}, \mathcal{A}^{(1)}$ received from Alice in Step 4, and I_0, I_1 obtained in Step 5.

Theorem 1. *For any* $A_0 : \{0,1\}^n \longrightarrow \{0,1\}^{n/6}$ *and* $A_1 : \{0,1\}^{n/6} \times \{0,1\}^n \longrightarrow \{0,1\}^{n/6}$, *for any strategy Bob employs in Steps 4 - 6 of Protocol* A, *with probability at least* $1 - 2^{-O(k)} - 2^{-0.02n+1}$, $\exists\ \beta \in \{0,1\}$ *such that for any distinguisher* $\mathcal{D}$,

$$\left|\Pr\left[\mathcal{D}(\eta_1, \mathcal{I}, X_{\overline{\beta}}, X_\beta) = 1\right] - \Pr\left[\mathcal{D}(\eta_1, \mathcal{I}, X_{\overline{\beta}}, 1 \oplus X_\beta) = 1\right]\right| \ < \ 2^{-k/3}, \quad (8)$$

where $\eta_1 = A_1(\eta_0, \alpha_1)$, $\eta_0 = A_0^{(0)}(\alpha_0)$, $\mathcal{I}$ *denotes all the information Bob obtains in Steps 4 - 6, and* X_0, X_1 *are defined in Step 7 of Protocol* A.

Theorem 1 says that using all the information he has in his bounded storage, Bob is not able to distinguish between $(X_{\overline{\beta}}, X_\beta)$ and $(X_{\overline{\beta}}, 1 \oplus X_\beta)$, for some $\beta \in \{0,1\}$, where X_0, X_1 are defined in Step 7 of Protocol A. From Theorem 1, we obtain:

Theorem 2. *For any* $A_0 : \{0,1\}^n \longrightarrow \{0,1\}^{n/6}$ *and* $A_1 : \{0,1\}^{n/6} \times \{0,1\}^n \longrightarrow \{0,1\}^{n/6}$*, for any strategy Bob employs in Steps 4 - 6 of Protocol* A*, with probability at least* $1 - 2^{-O(k)} - 2^{-0.02n+1}$*,* $\exists\ \beta \in \{0,1\}$ *such that* $\forall\ M_0, M_1 \in \{0,1\}$*,* $\forall\ \delta \in \{0,1\}$*, for any distinguisher* $\mathcal{D}$*,*

$$\begin{aligned} &\Big| \Pr\left[\mathcal{D}(\eta_1, \mathcal{I}, X_{\overline{\beta}} \oplus M_\delta, X_\beta \oplus M_{\overline{\delta}}) = 1\right] \\ &- \Pr\left[\mathcal{D}(\eta_1, \mathcal{I}, X_{\overline{\beta}} \oplus M_\delta, X_\beta \oplus \overline{M}_{\overline{\delta}}) = 1\right] \Big| \quad < \quad 2^{-k/3}, \end{aligned} \tag{9}$$

where X_0, X_1*,* η_1 *and* $\mathcal{I}$ *are as above. Therefore, the VIEW of Bob is essentially the same if* $M_{\overline{\delta}}$ *is replaced by* $\overline{M}_{\overline{\delta}} = 1 \oplus M_{\overline{\delta}}$*. Hence, in Protocol* A*, Bob learns essentially nothing about any non-trivial function or relation involving* both M_0 *and* M_1*.*

Proof. It is clear that (9) follows from (8). Therefore, Theorem 2 follows from Theorem 1. □

4 Proof of Theorem 1

In this section, we consider a *dishonest* receiver Bob, and prove Theorem 1.

We first note that it suffices to prove the theorem in the case that Bob's recording functions A_0, A_1 are deterministic. This does not detract from the generality of our results for the following reason. By definition, a randomized algorithm is an algorithm that uses a random help-string r for computing its output. A randomized algorithm A with each fixed help-string r gives rise to a *deterministic* algorithm A^r. Therefore, that Theorem 1 holds for any deterministic recording algorithm implies that for any randomized recording algorithm A, *for each fixed* help-string r, A using r cannot succeed. Hence, by an averaging argument, A using a randomly chosen r does not help. The reader might notice that the help-string r could be arbitrarily long since Bob has unlimited computing power. In particular, it could be that $|r| > B$, thereby giving rise to a deterministic recording algorithm with length $|A^r| = |A| + |r| > B$. But our model imposes *no restriction* on the *program size* of the recording algorithm. The only restriction is that the length of the output $|A^r(\alpha)| = B$ for each r. In the formal model, A is an unbounded non-uniform Turing Machine whose output tape is bounded by B bits.

We prove a slightly stronger result, namely, Theorem 1 holds even if Bob stores not only η_1, but also η_0, where $\eta_0 = A_0(\alpha_0)$ and $\eta_1 = A_1(\eta_0, \alpha_1)$, A_0, A_1 are Bob's recording functions, and α_0, α_1 are the public random strings used in Steps 2 and 3 of Protocol A. Let

$$\begin{aligned} H_0 &\stackrel{d}{=} A_0^{-1}(\eta_0) \ = \ \{\alpha \in \{0,1\}^n : A_0(\alpha) = \eta_0\}\,; \\ H_1 &\stackrel{d}{=} \{\alpha \in \{0,1\}^n : A_1(\eta_0, \alpha) = \eta_1\}\,. \end{aligned}$$

After η_0 and η_1 are computed in Steps 2 and 3 of Protocol A, the receiver Bob can compute H_0 and H_1, using unlimited computing power and space. But given

η_0 and η_1, all Bob knows about (α_0, α_1) is that it is *uniformly random* in $H_0 \times H_1$, i.e. each element of $H_0 \times H_1$ is equally likely to be (α_0, α_1) .

Recall from Definition 4 that $H \subset \{0,1\}^n$ is *fat* if $|H| > 2^{0.813n}$. By Corollary 1 and a union bound, for $\alpha_0, \alpha_1 \xleftarrow{R} \{0,1\}^n$, for any recording functions A_0, A_1,

$$\Pr\left[\textit{Both } H_0 \text{ and } H_1 \text{ are } \textit{fat}\right] \quad > \quad 1 \;-\; 2^{-0.02n+1}. \tag{10}$$

Thus, consider the case that both H_0 and H_1 are fat. By Lemma 1, for any fat $H \subset \{0,1\}^n$,

$$|B_H| \;<\; |\mathcal{K}| \cdot 2^{-k/3} \;=\; \binom{n}{k} \cdot 2^{-k/3}, \tag{11}$$

where B_H is defined in (2), i.e. almost all k-subsets of $[n]$ are *good* for H (See Definition 3 for the definition of goodness). Next, we show that if H is fat, then for a uniformly random $\mathcal{A} \subset [n]$ s.t. $|\mathcal{A}| = u$, with overwhelming probability, almost all k-subsets of $\mathcal{A}$ are *good* for H.

Definition 6. *For $\mathcal{A} \subset [n]$, define $\mathcal{K}_\mathcal{A} \stackrel{d}{=} \{s \subset \mathcal{A} : |s| = k\}$, i.e. $\mathcal{K}_\mathcal{A}$ is the set of all k-subsets of $\mathcal{A}$.*

Definition 7. *For $\mathcal{A} \subset [n]$ and $H \subset \{0,1\}^n$, define*

$$B_H^\mathcal{A} \;\stackrel{d}{=}\; \{s \in \mathcal{K}_\mathcal{A} : s \textit{ is } \text{not } \textit{good for } H\}\,.$$

Lemma 9. *Let $H \subset \{0,1\}^n$ be fat. For a uniformly random $\mathcal{A} \subset [n]$ with $|\mathcal{A}| = u$,*

$$\Pr\left[\left|B_H^\mathcal{A}\right| \;<\; |\mathcal{K}_\mathcal{A}| \cdot 2^{-k/6} \;=\; \binom{u}{k} \cdot 2^{-k/6}\right] \quad > \quad 1 \;-\; 2^{-k/6}.$$

In other words, for almost all $\mathcal{A} \subset [n]$ with $|\mathcal{A}| = u$, almost all k-subsets of $\mathcal{A}$ are good for any fat H.

Proof. Let $\mathcal{U}$ be the set of all the $\binom{n}{u}$ u-subsets of $[n]$. For each $\mathcal{A} \in \mathcal{U}$, let $W_\mathcal{A} \stackrel{d}{=} \left|B_H^\mathcal{A}\right|$, i.e. $W_\mathcal{A}$ is the number of k-subsets of $\mathcal{A}$ that are *bad* for H. Let $W \stackrel{d}{=} \sum_{\mathcal{A} \in \mathcal{U}} W_\mathcal{A}$. Since each k-subset of $[n]$ is contained in exactly $\binom{n-k}{u-k}$ u-subsets, in the sum W each bad k-subset of $[n]$ for H, i.e. every element of B_H (defined in (2)), is counted exactly $\binom{n-k}{u-k}$ times. Together with (11), we have

$$W \;=\; \sum_{\mathcal{A} \in \mathcal{U}} W_\mathcal{A} \;=\; |B_H| \cdot \binom{n-k}{u-k} \;<\; \binom{n-k}{u-k}\binom{n}{k} \cdot 2^{-k/3}. \tag{12}$$

Fact 2 *For $k \le u \le n$,*

$$\binom{n}{k}\binom{n-k}{u-k} \;=\; \binom{n}{u}\binom{u}{k}. \tag{13}$$

Therefore, by (12) and (13),

$$W \;=\; \sum_{\mathcal{A}\in\mathcal{U}} W_{\mathcal{A}} \;<\; \binom{n}{u}\binom{u}{k}\cdot 2^{-k/3}. \qquad (14)$$

It follows that there can be at most a $2^{-k/6}$ fraction of u-subsets $\mathcal{A}$ such that $\left|B_H^{\mathcal{A}}\right| \ge \binom{u}{k}\cdot 2^{-k/6}$, for otherwise we would have $W \;\ge\; \binom{u}{k}\cdot 2^{-k/6}\cdot\binom{n}{u}\cdot 2^{-k/6} \;=\; \binom{n}{u}\binom{u}{k}\cdot 2^{-k/3}$, contradicting (14). The lemma thus follows. □

Again let $\mathcal{A}^{(0)}, \mathcal{A}^{(1)}$ be the random u-subsets of $[n]$ Alice chooses in Step 1 of Protocol A. By (10), Lemma 9 and a union bound, for $\alpha_0, \alpha_1 \xleftarrow{R} \{0,1\}^n$, and uniformly random $\mathcal{A}^{(0)}, \mathcal{A}^{(1)} \subset [n]$ with $|\mathcal{A}^{(0)}| = |\mathcal{A}^{(1)}| = u$, with probability at least $1 - 2^{-k/6+1} - 2^{-0.02n+1}$,

$$\left|B_{H_0}^{\mathcal{A}^{(0)}}\right|, \left|B_{H_1}^{\mathcal{A}^{(1)}}\right| \;<\; \binom{u}{k}\cdot 2^{-k/6}. \qquad (15)$$

Thus consider the case that both $B_{H_0}^{\mathcal{A}^{(0)}}, B_{H_1}^{\mathcal{A}^{(1)}}$ satisfy (15).

For each $c \in \{0,1\}$, denote $\mathcal{A}^{(c)} = \left\{\mathcal{A}_1^{(c)}, \ldots, \mathcal{A}_u^{(c)}\right\}$. Recall from Definition 5 that for $J = \{j_1, \ldots, j_k\} \subset [u]$, $\mathcal{A}_J^{(c)} \stackrel{d}{=} \left\{\mathcal{A}_{j_1}^{(c)}, \ldots, \mathcal{A}_{j_k}^{(c)}\right\}$. By Definition 6, $\mathcal{A}_J^{(c)} \in \mathcal{K}_{\mathcal{A}^{(c)}}$. Define

$$T_0 \;\stackrel{d}{=}\; \left\{J \subset [u] : |J| = k \;\wedge\; \mathcal{A}_J^{(0)} \in B_{H_0}^{\mathcal{A}^{(0)}}\right\},$$
$$T_1 \;\stackrel{d}{=}\; \left\{J \subset [u] : |J| = k \;\wedge\; \mathcal{A}_J^{(1)} \in B_{H_1}^{\mathcal{A}^{(1)}}\right\}.$$

Clearly $|T_0| = \left|B_{H_0}^{\mathcal{A}^{(0)}}\right|$, and $|T_1| = \left|B_{H_1}^{\mathcal{A}^{(1)}}\right|$. Thus by (15), we have

$$|T_0|, |T_1| \;<\; \binom{u}{k}\cdot 2^{-k/6}. \qquad (16)$$

Consider I_0, I_1 defined in Step 5 of Protocol A. Let ε be the first bit Bob sends Alice in Step 6 of Protocol A. Then by (10), (15), (16), and Corollary 4 of Lemma 5 on interactive hashing, for any strategy Bob uses in Steps 4 - 6, with probability at least $1 - 2^{-O(k)} - 2^{-0.02n+1}$, $I_\varepsilon \notin T_0 \;\vee\; I_{\overline{\varepsilon}} \notin T_1$, where $\overline{\varepsilon} = 1 \oplus \varepsilon$. WLOG, say $I_{\overline{\varepsilon}} \notin T_1$. Let $s_0 = \mathcal{A}_{I_\varepsilon}^{(0)}$, $X_0 = s_0(\alpha_0)$, $s_1 = \mathcal{A}_{I_{\overline{\varepsilon}}}^{(1)}$, and $X_1 = s_1(\alpha_1)$, as defined in Step 7 of Protocol A. Since $I_{\overline{\varepsilon}} \notin T_1$, by definition $s_1 \notin B_{H_1}^{\mathcal{A}^{(1)}}$, i.e. s_1 is *good* for H_1. Note again that given η_0 and η_1, and thus H_0 and H_1, all Bob knows about (α_0, α_1) is that (α_0, α_1) is *uniformly random* in $H_0 \times H_1$. Since s_1 is good for H_1, by (1) for the definition of goodness, for $\alpha_1 \xleftarrow{R} H_1$,

$$\left|\Pr[X_1 = 0] \;-\; \Pr[X_1 = 1]\right| \;<\; 2^{-k/3}. \qquad (17)$$

For $(\alpha_0, \alpha_1) \xleftarrow{R} H_0 \times H_1$, X_0 and X_1 are *independent*. Thus together with (17), for $(\alpha_0, \alpha_1) \xleftarrow{R} H_0 \times H_1$, for any $b_0 \in \{0,1\}$,

$$\left|\Pr[X_1 = 0 \mid X_0 = b_0] \;-\; \Pr[X_1 = 1 \mid X_0 = b_0]\right| \;<\; 2^{-k/3}. \qquad (18)$$

Thus, from (18) and all the above, Theorem 1 follows (with $\beta = 1$).

5 Discussion

Building on the work of Cachin, Crépeau, and Marcil [15], we have given a similar but more efficient protocol for $\binom{2}{1}$-OT in the bounded storage model, and provided a stronger security analysis.

Having proved a stronger result than that of [15], we note that the model of [15] is slightly stronger than ours in the following sense. In [15], the dishonest receiver Bob computes an arbitrary function on *all* public random bits, and stores B bits of output. In our model, α_0 is first broadcast, Bob computes and stores $\eta_0 = A_0(\alpha_0)$, which is a function of α_0. Then α_0 disappears. After a short pause, α_1 is broadcast, and Bob computes and stores $\eta_1 = A_1(\eta_0, \alpha_1)$, which is a function of η_0 and α_1. However, we claim that our model is reasonable, as with limited storage, in practice it is impossible for Bob to compute a function on all of α_0 and α_1, with $|\alpha_0| = |\alpha_1| > B$, that are broadcast one after another, with a pause in between. Furthermore, we believe that by a more detailed analysis, it is possible to show that our results hold even in the stronger model, where Bob computes an arbitrary function $A(\alpha_0, \alpha_1)$ on all bits of α_0 and α_1.

As the CCM Protocol, our protocol employs interactive hashing, resulting in an inordinate number of interactions. Further, the communication complexity of the NOVY protocol is quadratic in the size of the string to be transmitted. It thus remains a most important open problem to make this part of the protocol non-interactive and more communication efficient.

Can the storage requirement of our protocol be further improved? For very large n, $\Omega(\sqrt{kn})$ may not be small enough to be practical. It becomes another important open problem to investigate the feasibility of reducing the storage requirement for OT in the bounded storage model, and establish lower bounds.

We also note that the constant hidden by $O(\cdot)$ in our results is not optimized. We believe that this can be improved by refining the analysis of Lemma 9, as well as the analysis of interactive hashing in [15].

References

1. Y. Aumann and M. O. Rabin. Information Theoretically Secure Communication in the Limited Storage Space Model. In *Advances in Cryptology - CRYPTO '99*, pages 65-79, 1999.
2. Y. Aumann, Y. Z. Ding, and M. O. Rabin. Everlasting Security in the Bounded Storage Model. Accepted to *IEEE Transactions on Information Theory*, 2001.
3. Y. Aumann and U. Feige. One message proof systems with known space verifier. In *Advances in Cryptology - CRYPTO '93*, pages 85-99, 1993.
4. Y. Aumann and M. O. Rabin. Clock Construction in Fully Asynchronous Parallel Systems and PRAM Simulation. *TCS*, 128(1):3-30, 1994.
5. D. Beaver. Commoditiy-Based Cryptography. In *Proc. 29th ACM Symposium on Theory of Computing*, pages 446-455, 1997.
6. M. Bellare and S. Micali. Non-interactive oblivious transfer and applications. In *Advances in Cryptology - CRYPTO '89*, pages 200-215, 1989.
7. C. H. Bennett, G. Brassard, C. Crépeau, and M.H. Skubiszewska. Practical quantum oblivious transfer protocols. In *Advances in Cryptology - CRYPTO '91*, pages 351-366, 1991.

8. M. Blum. How to exchange (secret) keys. *ACM Transactions of Computer Systems*, 1(20): 175-193, 1983.
9. G. Brassard and C. Crépeau. Oblivious transfers and privacy amplification. In *Advances in Cryptology - EUROCRYPT '97*, pages 334-347, 1997.
10. G. Brassard, C. Crépeau, and J-M. Roberts. Information theoretic reductions among disclosure problems. In *Proc. 27th IEEE Symposium on the Foundations of Computer Science*, pages 168-173, 1986.
11. G. Brassard, C. Crépeau, and J-M. Roberts. All-or-nothing disclosure of secrets. In *Advances in Cryptology - CRYPTO '86*, pages 234-238, 1986.
12. G. Brassard, C. Crépeau, and M. Sántha. Oblivious transfers and intersecting codes. *IEEE Transactions on Information Theory*, 42(6): 1769-80, 1996.
13. C. Cachin. *Entropy Measures and Unconditional Security in Cryptography*, volume 1 of *ETH Series in Information Security and Cryptography.* Hartun-Gorre Verlag, Konstanz, Germany, 1997.
14. C. Cachin. On the foundations of oblivious transfer. In *Advances in Cryptology - EUROCRYPT '98*, pages 361-374, 1998.
15. C. Cachin, C. Crépeau, and J. Marcil. Oblivious transfer with a memory-bounded receiver. In *Proc. 39th IEEE Symposium on Foundations of Computer Science*, pages 493-502, 1998.
16. C. Cachin and U. Maurer. Unconditional security against memory bounded adversaries. In *Advances in Cryptology - CRYPTO '97*, pages 292-306, 1997.
17. A. Condon. Bounded Space Probabilistic Games. *JACM*, 38(2):472-494, 1991.
18. A. Condon, and R. Ladner. Probabilistic Game Automata. *JCSS*, 36(3):452-489, 1987.
19. C. Crépeau. Equivalence between two flavours of oblivious transfer. In *Advances in Cryptology - CRYPTO '87*, pages 351-368, 1987.
20. C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *Proc. 29th IEEE Symposium on the Foundations of Computer Science*, 42-52, 1988.
21. C. Crépeau and M. Sántha. On the reversibility of oblivious transfer. In *Advances in Cryptology - EUROCRYPT '91*, pages 106-113, 1991.
22. C. Crépeau, J. van de Graff, and A. Tapp. Committed oblivious transfer and private multi-party computations. In *Advances in Cryptology - CRYPTO '95*, pages 110-123, 1995.
23. A. De-Santis, G. Persiano, and M. Yung. One-message statistical zero-knowledge proofs with space-bounded verifier. In *Proc. 19th ICALP*, pages 28-40, 1992.
24. Y. Z. Ding and M. O. Rabin. Provably Secure and Non-Malleable Encryption. To appear, 2001.
25. Y. Dodis and S. Micali. Lower bounds for oblivious transfer reductions. In *Advances in Cryptology - EUROCRYPT '99*, pages 42-55, 1999.
26. C. Dwork and L. J. Stockmeyer. Finite State Verifiers I: The Power of Interaction. *JACM* 39(4): 800-828, 1992
27. C. Dwork and L. J. Stockmeyer. Finite State Verifiers II: Zero Knowledge. *JACM* 39(4): 829-858, 1992.
28. S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology - CRYPTO '82*, pages 205-210, 1982.
29. J. A. Garay and P. Mackenzie. Concurrent Oblivious Transfer. In *Proc. 41th IEEE Symposium on the Foundations of Computer Science*, pages 314-324, 2000.
30. O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proc. 19th ACM Symposium on Theory of Computing*, pages 218-229, 1987.

31. O. Goldreich and R. Vainish. How to solve any protocol problem - an efficiency improvement. In *Advances in Cryptology - CRYPTO '87*, pages 73-86, 1987.
32. S. Goldwasser and L. Levin. Fair Computation of General Functions in Presence of Immoral Majority. In *Advances in Cryptology - CRYPTO '90*, pages 77-93, 1990.
33. J. Kilian. Founding cryptography on oblivious transfer. In *Proc. 20th ACM Symposium on Theory of Computing*, pages 20-31, 1988.
34. J. Kilian. Zero-knowledge with Log-Space Verifiers. In *Proc. 29th IEEE Symposium on the Foundations of Computer Science*, pages 25-35, 1988.
35. J. Kilian. A general completeness theorem for two-party games. In *Proc. 23th ACM Symposium on Theory of Computing*, pages 553-560, 1991.
36. J. Kilian, E. Kushilevitz, S. Micali, and R. Ostrovsky. Reducibility and completeness in private computations. *SIAM Journal on Computing*, 29(4): 1189-1208, 2000.
37. U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53-66, 1992.
38. U. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733-742, 1993.
39. U. Maurer and S. Wolf. Toward characterizing when information-theoretic secret key agreement is possible. In *Advances in Cryptology - ASIACRYPT'96*, pages 196-209, 1996.
40. U. Maurer. Information-theoretically secure secret-key agreement by NOT authenticated public discussion. *Advances in Cryptology - EUROCRYPT '97*, pages 209-225, 1997.
41. U. Maurer and S. Wolf. Unconditional secure key agreement and the intrinsic conditional information. *IEEE Transaction on Information Theory*, 45(2): 499-514, 1999.
42. U. Maurer and S. Wolf. Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free. In *Advances in Cryptology - EUROCRYPT '00*, pages 351-368, 2000.
43. M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung. Perfect zero-knowledge arguments for NP using any one-way function. *Journal of Cryptology*, 11(2): 87-108, 1998.
44. M. Naor and B. Pinkas. Distributed Oblivious Transfer. In *Advances in Cryptology - ASIACRYPT '00*, pages 205-219, 2000.
45. N. Nisan. Pseudorandom generators for space-bounded computation. In *Proc. 22rd ACM Symposium on Theory of Computing*, pages 204-212, 1990.
46. N. Nisan and D. Zuckerman. Randomness is linear in space. *JCSS* 52(1): 43-52, 1996.
47. M. O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard University, 1981.
48. M. O. Rabin. Transaction Protection by Beacons. *JCSS* 27(2): 256-267, 1983.
49. R. Rivest. Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer. Manuscript, 1999.
50. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Computing*, 26(5): 1484-1509, 1997.
51. L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. In *Proc. ACM Symposium on Theory of Computing*, pages 458-463, 1985.
52. A. C. Yao. How to generate and exchange secrets. In *Proc. 27th IEEE Symposium on the Foundations of Computer Science*, pages 162-167, 1986.

Appendix A: Proof of Lemma 1

Definition 8. *Let* $s = (\sigma_1, \ldots, \sigma_k) \in [n]^k$*. For* $\alpha \in \{0,1\}^n$*, define* $s(\alpha)$ *as in Definition 2, i.e.* $s(\alpha) \stackrel{d}{=} \bigoplus_{i=1}^k \alpha[\sigma_i]$*.*

Definition 9. *Let* $s \in [n]^k$*. Let* $H \subset [n]$*. Define the goodness of* s *for* H *as in Definition 3, i.e.* s *is good for* H *if (1) holds.*

The following main lemma is proved in [24].

Main Lemma 1 [24] *Let* $H \subset \{0,1\}^n$*. Denote*

$$\hat{B}_H \stackrel{d}{=} \left\{ s \in [n]^k : s \text{ is not good for } H \right\}. \tag{19}$$

If H *is* fat*, then*

$$|\hat{B}_H| < n^k \cdot 2^{-k/3-1}. \tag{20}$$

We now prove Lemma 1 from Main Lemma 1. Let $\tilde{B}_H \subset \hat{B}_H$ be the subset of bad k-tuples with k *distinct* coordinates, i.e.

$$\tilde{B}_H \stackrel{d}{=} \left\{ s = (\sigma_1, \ldots, \sigma_k) \in \hat{B}_H : \ \sigma_i \neq \sigma_j \ \forall \ i \neq j \right\}. \tag{21}$$

Then clearly

$$|\tilde{B}_H| = |B_H| \cdot k!, \tag{22}$$

where B_H is defined in (2). By way of contradiction, suppose that Lemma 1 does not hold, i.e.

$$|B_H| \geq \binom{n}{k} \cdot 2^{-k/3}. \tag{23}$$

Then by (22) and (23), and the fact that $\tilde{B}_H \subset \hat{B}_H$, we have

$$|\hat{B}_H| \geq |\tilde{B}_H| = |B_H| \cdot k! \geq \binom{n}{k} \cdot k! \cdot 2^{-k/3}. \tag{24}$$

Observe that

$$\binom{n}{k} \cdot k! = n^k \cdot \left(1 - \frac{1}{n}\right) \cdots \left(1 - \frac{k-1}{n}\right) > n^k \cdot \left(1 - \frac{\sum_{i=1}^{k-1} i}{n}\right)$$
$$> n^k \cdot \left(1 - \frac{k^2}{2n}\right) > \frac{n^k}{2} \qquad \text{for } k < \sqrt{n}. \tag{25}$$

Therefore, if Lemma 1 does not hold, i.e. if (23) holds, then by (24) and (25),

$$|\hat{B}_H| > n^k \cdot 2^{-k/3-1}, \tag{26}$$

contradicting (20). Thus, Lemma 1 must hold.