An Oblivious Transfer Protocol with Log-Squared Total Communication

*** Second public draft. April 26, 2004 ***

Helger Lipmaa

Laboratory for Theoretical CS, Department of CS&E
Helsinki University of Technology, P.O.Box 5400, FIN-02015 HUT, Espoo, Finland
{helger}@tcs.hut.fi

Abstract. We propose a $\binom{N}{1}$-computationally-private information retrieval protocol, based on the Damgård-Jurik public-key cryptosystem from PKC 2001, with total communication $\Theta(\log^2 N) \cdot k$. Based on this, we construct a four-round $\binom{N}{1}$-OT protocol with total communication $\Theta(\log^2 N)k$. These protocols are, respectively, the first $\binom{N}{1}$-CPIR and $\binom{N}{1}$-OT protocols with logarithmic sender-side and polylogarithmic client-side communication. We show that there is no straightforward methodology to improve the asymptotic communication of our protocols.
Keywords: computationally-private information retrieval, homomorphic public-key cryptosystem, oblivious transfer.

1 Introduction

During a (single-sender) $\binom{N}{1}$-computationally-private information retrieval ($\binom{N}{1}$-CPIR) protocol, Chooser retrieves an entry from Sender's database $\mu = (\mu[1], \ldots, \mu[N])$, so that a computationally bounded Sender will not obtain any information on which element was retrieved. In the case of the *(computationally chooser-private and information-theoretically sender-private) $\binom{N}{1}$-oblivious transfer protocol* ($\binom{N}{1}$-OT) it is additionally required that Chooser's retrieved information should be restricted to one entry from the database.

The first $\binom{N}{1}$-CPIR protocol with polylogarithmic (in N) communication was proposed by Cachin, Micali and Stadler in [CMS99]. The security of their protocol is based on a rather new Φ-Hiding Assumption, and both its sender-side and chooser-side communications is $\Omega(\log^4 N)k$, where k is the security parameter.

Slightly earlier, in 1998, Julien P. Stern [Ste98] proposed a family—that we call $\mathsf{HomCPIR}\,(\alpha)$—of $\binom{N}{1}$-CPIR protocols, based on an (almost) arbitrary semantically secure additively homomorphic public-key cryptosystem. In the asymptotically near-optimal case $\alpha = \sqrt{\log_\eta N}$, $\mathsf{HomCPIR}\,(\alpha)$ has super-logarithmic total communication $(1 + o(1))\eta\sqrt{\log_\eta N} \cdot \eta^{\sqrt{\log_\eta N}} \cdot k$, where η is the ciphertext expansion ratio of the underlying homomorphic cryptosystem. ($\eta = 2$ in the case of Paillier's cryptosystem.)

In this paper, we propose a modification of Stern's $\binom{N}{1}$-CPIR that takes full advantage of the length-flexible Damgård-Jurik semantically secure homomorphic cryptosystem from PKC 2001 [DJ01]. The resulting CPIR, that we call $\mathsf{DJCPIR}(\alpha)$, has total communication $\Theta(\log^2 N)k$ when $\alpha = \log N$ and is secure under the Decisional Composite Residuosity Assumption. This is the first CPIR with logarithmic sender-side and polylogarithmic chooser-side communication.

We then look at the possibilities to decrease the communication even further. We show that under two alternative additional assumptions on the used cryptosystem, there exist a CPIR with the asymptotically optimal total communication $\Theta(\log N)k$. The first assumption is that the encryption of a small constant in a smaller ciphertext-space can be transferred to the encryption of the same constant in a larger ciphertext-space even by somebody who does not know the private key. The second assumption is that the cryptosystem preserves homomorphic properties of a ring. The first assumption seems to be somewhat more plausible than the second assumption although results in a slightly larger constant in the Θ-expression. We conjecture that such cryptosystems exist, though we show that the Damgård-Jurik semantically secure homomorphic cryptosystem from PKC 2001 [DJ01] does not satisfy either of the requirements.

One of the direct corollaries from the construction of the $\mathsf{DJCPIR}(\alpha)$ is that one can construct a four-round (two-round, when we use the Fiat-Shamir heuristic [FS86] in the random-oracle model) $\binom{N}{1}$-OT protocol with total communication $\Theta(\log^2 N) \cdot k$.

Road-map. In Section 2, we introduce the reader to notation and preliminaries. In Section 3, we propose the new CPIR protocols. In Section 5, we compare different CPIR protocols from the efficiency viewpoint and discuss possible extensions. In Section 6, we describe the new $\binom{N}{1}$-OT protocol.

2 Preliminaries

Notation. For a natural number t, let $[t]$ denote the set $\{1, \ldots, t\}$. Let $\{i \stackrel{?}{=} j\} = 1$ if $i = j$ and 0, otherwise. All logarithms in this paper will be on base 2, unless explicitly mentioned. Let $x||y$ denote the concatenation of binary strings x and y. Let W be Lambert's W function, i.e., W satisfies the functional identity $W(x)e^{W(x)} = x$.

Semantically secure homomorphic cryptosystems. Public-key cryptosystem is a triple $\Pi = (G, E, D)$, where G is the key generation algorithm, E is the encryption algorithm and D is the decryption algorithm. Intuitively, Π is *semantically secure* when it is difficult for a polynomially bounded adversary to distinguish between random encryptions of two elements, chosen by herself. For fixed Π and private key x, let $C(x)$ be the ciphertext space, let $R(x)$ be the randomness space and let $P(x)$ be the plaintext space.

Π is an *(additively) homomorphic public-key cryptosystem* if for any key pair (K, x), any $m, m' \in P(x) = \mathbb{Z}_{|P(x)|}$ and any $r, r' \in R(x)$, $(E_K(m; r) \cdot E_K(m'; r') = E_K(m+m'; r \circ r')$, where $\circ$ is a groupoid operation, and $+$ is a group operation in $P(x)$. A few homomorphic cryptosystems [OU98,NS98,Pai99,DJ01,DJ03] are believed to be semantically secure under reasonable complexity assumptions.

Let $k := |P(x)|$ be the security parameter and let $\eta := \lceil |C(x)|/k \rceil$ be the *ciphertext expansion ratio* of Π; $\eta = 2$ for the Paillier cryptosystem [Pai99] and Damgård-Jurik cryptosystem from PKC 2001 [DJ01] and $\eta = 3$ for the Okamoto-Uchiyama cryptosystem [OU98] and $\eta \in \{2, 3\}$ for another cryptosystem by Damgård and Jurik [DJ03].

Damgård-Jurik length-flexible cryptosystem. The Damgård-Jurik cryptosystem from PKC 2001 [DJ01] has flexible plaintext length parameterised by a constant $s \geq 1$. For fixed s, the plaintext space is $P_s(x) := \mathbb{Z}_{n^s}$, the randomness space is $R(x) = \mathbb{Z}_n^*$ and the ciphertext space is $C_s(x) := \mathbb{Z}_{n^{s+1}}^*$, thus $|C_s(x)|/|P_s(x)| \approx 1 + 1/s$. Encryption is defined as $E_K^s(m; r) := (1+n)^m \cdot r^{n^s} \mod n^{s+1}$. To decrypt $c = E_K^s(m; r)$, one first computes $c \mod n = r^{n^s} \mod n$, and then retrieves r and thus also $c' = (1+n)^m \mod n^{s+1}$. After that, a simple algorithm from [DJ01] is used to retrieve m from c'. The Damgård-Jurik cryptosystem is additively homomorphic since $E_K^s(m_1; r_1)E_K^s(m_2; r_2) = E_K^s(m_1 + m_2; r_1 r_2)$, and semantically secure assuming that the Decisional Composite Residuosity Problem is hard [DJ01].

Importantly, the same key K can be used to encrypt messages of different length, and $C_s(x) \subset P_{s+1}(x)$. A newer cryptosystem by Damgård and Jurik from ACISP 2003 [DJ03] has also flexible-length plaintexts, but is slightly less efficient with $|C_s(x)|/|P_s(x)| \approx 1 + 2/s$. Denote encryption and decryption with public key K and a fixed s by E_K^s and D_K^s.

Computationally-private information retrieval (CPIR). Private information retrieval protocol was first introduced in the information-theoretic setting [CGKS95]. During a (single-sender) $\binom{N}{1}$-computationally-private information retrieval ($\binom{N}{1}$-CPIR) protocol, Chooser fetches $\mu[\iota]$ from the database $\mu = \mu[1]|| \dots ||\mu[N]$, $\mu[i] \in \mathcal{D}$ for some fixed $\mathcal{D}$, so that a computationally bounded Sender does not know which entry Chooser is learning. This means, informally, that Sender's views when Chooser retrieves entries i and j, chosen by Sender from a database, chosen by Sender, are computationally indistinguishable. Unless mentioned explicitly, we will assume that $\mathcal{D} \subseteq P(x)$. Throughout this paper, N will denote Sender's database size. One requires from a CPIR protocol that $o(N)k$ bits should be transmitted.

The first CPIR with polylogarithmic total communication was proposed by Cachin, Micali and Stadler in [CMS99], but it has both chooser-side and sender-side complexity $\Omega(\log^4 N)$ and its security is based on the relatively little-studied Φ-Hiding assumption.

Stern's $\binom{N}{1}$-CPIR. The first $\binom{N}{1}$-CPIR with logarithmic sender-side communication was proposed by Stern [Ste98] (independently rediscovered by Chang [Cha04]). The Stern $\binom{N}{1}$-CPIR is based on an arbitrary semantically secure additively homomorphic cryptosystem with ciphertext expansion ratio $\eta \geq 2$. We next give a self-contained description of the Stern $\binom{N}{1}$-CPIR based on an arbitrary semantically secure homomorphic cryptosystem Π. For this, we recast Stern's $\binom{N}{1}$-CPIR in the contemporary language of homomorphic cryptosystems and using the hypercube approach from [Cha04].

Stern's $\binom{N}{1}$-CPIR is a family of CPIR-s with a parameter $\alpha \geq 1$. We call this family $\mathsf{HomCPIR}\,(\alpha)$. The main idea behind $\mathsf{HomCPIR}\,(\alpha)$ is as follows. Look at the database μ as at an α-dimensional hypercube with its elements $\mu(i_1, \dots, i_\alpha)$ addressed by coordinates $(i_1, \dots, i_\alpha)$; Chooser's query ι has thus also α coordinates, $\iota = (\iota_1, \dots, \iota_\alpha)$.

For every dimension i and every coordinate j along this dimension, Chooser sends an encryption $\kappa_{i,j}$ of $\{j \stackrel{?}{=} \iota_i\}$ to Sender. Fix a dimension, say 1. Sender constructs an $(\alpha-1)$-dimensional database as follows. For all dimensions $j \neq 1$ and for all coordinates i_j along those dimensions, set the $(i_2, \dots, i_j)$th element of the new database to be equal to the product $\prod_t \kappa_{1,t}^{\mu(t,i_2,\dots,i_\alpha)}$. Due to the homomorphicity of Π, this product is an encryption of $\mu(\iota_1, i_2, \dots, i_\alpha)$. Now, the same process is repeated with the $(\alpha-1)$-dimensional database of encrypted values $E_K(\mu(\iota_1, i_2, \dots, i_\alpha))$, then with the $(\alpha-2)$-dimensional database of doubly-encrypted values $E_K(E_K(\mu(\iota_1, \iota_2, i_3, \dots, i_\alpha)))$, until the final result, an α times encryption of $\mu(\iota_1, \dots, \iota_\alpha)$, results. Sender sends this result to the Chooser, who decrypts it α times.

Now, Stern's $\binom{N}{1}$-CPIR deviates from this basic idea due to the fact that Π has ciphertext expansion ratio $\eta \geq 2$. To account with this, there is η^j $(\alpha - j)$-dimensional databases, and the chooser transfers η^α ciphertexts to Chooser, who combines their decryptions to obtain $\mu(\iota_1, \dots, \iota_\alpha)$. Therefore, Stern's $\binom{N}{1}$-CPIR has chooser-side communication $\eta\alpha N^{1/\alpha}k$ bits and sender-side communication $\eta^\alpha k$ bits. One can minimise sender-side communication by minimising α. However, even in the close-to-optimal case when $\alpha = \sqrt{\log N}$, the total communication $\Theta\left(\sqrt{\log N} \cdot 2^{\sqrt{\log N}}\right) \cdot k$ will still be super-logarithmic. ([Ste98] erroneously claims that the total communication of $\mathsf{HomCPIR}\left(\sqrt{\log N}\right)$ is $\Theta\left(\eta^{\sqrt{\log N}}\right) \cdot k$.) Thus,

Proposition 1 ([Ste98,Cha04]). *Let Π be a semantically secure homomorphic cryptosystem. (a) Let $\alpha \geq 1$. W.l.o.g., assume that Sender's database $\mu = (\mu[1], \dots, \mu[N])$ contains $N = \ell^\alpha$ entries. There exists an $\binom{N}{1}$-CPIR protocol $\mathsf{HomCPIR}(\alpha)$ with chooser-side communication $\alpha N^{1/\alpha}\eta k$ and sender-side communication $\eta^\alpha k$ bits. (b) Fix $\alpha = \sqrt{\log_\eta N}$. There exists an $\binom{N}{1}$-CPIR protocol $\mathsf{HomCPIR}\left(\sqrt{\log_\eta N}\right)$ with total communication $(\eta\sqrt{\log_\eta N} + 1)\eta^{\sqrt{\log_\eta N}}k$ bits.*

Here, $\alpha = \sqrt{\log_\eta N}$ is the "on limit" solution of the equation $\alpha N^{1/\alpha} = \eta^\alpha$. For any $N \in \mathbb{Z}$ and $\alpha = \sqrt{\log_\eta N}$, the sender-side communication is smaller than the chooser-side communication.

Oblivious Transfer. An $\binom{N}{1}$-CPIR is an *(computationally chooser-private and information-theoretically sender-private) $\binom{N}{1}$-OT protocol* (with computational chooser-privacy) when also Sender's privacy is guaranteed: that is, when Chooser will receive no additional information—apart from $\mu[i]$—about sender's database. An $\binom{N}{1}$-oblivious transfer protocol with total communication $o(N)k$ is sometimes called a *symmetric computationally private information retrieval* protocol. Stern's $\binom{N}{1}$-OT protocol [OP98] requires four rounds but $\Theta\left(\eta\sqrt{\log_\eta N} \cdot \eta^{\sqrt{\log_\eta N}}\right) \cdot k$ communication, while some other $\binom{N}{1}$-OT protocols [NP01,AIR01,Lip03] require two rounds but $\Theta(N) \cdot k$ communication. Asymptotically, the most communication-efficient—with $\Omega(\log^4 N) \cdot k$ communication—previous $\binom{N}{1}$-OT protocol results when applying the Naor-Pinkas methodology from [NP99] to the $\binom{N}{1}$-CPIR from [CMS99]. However, Stern's $\binom{N}{1}$-OT protocol is more communication-efficient for all relevant database sizes.

3 New $\binom{N}{1}$-CPIR with Log-Squared Communication

Next, we use the length-flexibility property of the Damgård-Jurik cryptosystem from PKC 2001 to improve both the concrete and the asymptotic total communication of $\mathsf{HomCPIR}\,(\alpha)$, by presenting a family $\mathsf{DJCPIR}(\alpha)$ of $\binom{N}{1}$-CPIR protocols.

Assume that $\mathcal{D} \subseteq P_s(x)$ for some fixed s. Fix $\alpha \geq 1$. Consider the database $\mu = (\mu[1], \ldots, \mu[N])$ as an α-dimensional $\ell_1 \times \cdots \times \ell_\alpha$ hyper-rectangle. Thus, every element of μ is indexed by a tuple $(i_1, \ldots, i_\alpha)$. If $\alpha > 1$, Server computes an $(\alpha-1)$-dimensional database w_1 as follows: for every $(i_2, \ldots, i_\alpha)$, let $w_1(i_2, \ldots, i_\alpha) \leftarrow \prod_{t\in[\ell_1]} \kappa_{1,t}^{\mu(t,i_2,\ldots,i_\alpha)}$, where $D_K^s(\kappa_{1,t}) = \{t \stackrel{?}{=} \iota_1\}$ and $\kappa_{1,t}$ is obtained from Chooser. Thus, $D_K^s(w_1(i_2, \ldots, i_\alpha)) = \mu(\iota_1, i_2, \ldots, i_\alpha)$. If $\alpha > 2$, Sender repeats this process recursively on the database w_1 to obtain an $(\alpha-2)$-dimensional database w_2, so that $D_K^{s+1}(w_2(i_3, \ldots, i_\alpha)) = w_1(\iota_2, \ldots, i_\alpha)$, then an $(\alpha-3)$-dimensional database w_3, such that $D_K^{s+2}(w_3(i_4, \ldots, i_\alpha)) = w_2(\iota_3, \ldots, i_\alpha)$, etc.

Thus, the basic idea of the new protocol is similar to that of Stern's $\binom{N}{1}$-CPIR. After α steps, Sender has a single element w_α that is an α-time encrypted $\mu(\iota_1, \ldots, \iota_\alpha)$. He then returns w_α to Chooser, who decrypts it α times to obtain $\mu(\iota_1, \ldots, \iota_\alpha)$. Since the Damgård-Jurik cryptosystem has flexible-length plaintexts, instead of dividing every intermediate ciphertext into η chunks (as in the case of Stern's $\binom{N}{1}$-CPIR), we can just increase the length of the plaintexts. Therefore, it suffices for Sender to just send one value w_α, with length $|w_\alpha| = \alpha k$, to Chooser.

More precisely, for fixed α, define ℓ_i as

$$\ell_i = \left(\frac{(s+\alpha)!}{s!}\right)^{1/\alpha} \cdot \frac{1}{s+i} \cdot N^{1/\alpha} \enspace ;$$

this results in minimal $\sum_i i\ell_i$ under the constraint that $\prod \ell_i = N$. In practice, we must round ℓ_i-s to the nearest integers. For the simplicity of exposition, we will not explicitly mention such issues anymore. Thus, we assume that $N = \prod_{i=1}^{\alpha} \ell_i$ and define $\mu(i_1, \ldots, i_\alpha) := \mu[(i_1-1)\prod_{i=2}^{\alpha} \ell_i + (i_2-1)\prod_{i=3}^{\alpha} \ell_i + \cdots + (i_{\alpha-1}-1)\ell_\alpha + (i_\alpha - 1) + 1]$.

Protocol 1 depicts the new $\mathsf{DJCPIR}(\alpha)$ protocol.

Theorem 1. *Let Π be the Damgård-Jurik cryptosystem from PKC 2001. Assume that the Decisional Composite Residuosity Problem is hard. For every $\alpha \geq 1$, there exists a CPIR protocol $\mathsf{DJCPIR}(\alpha)$ with chooser-side and sender-side communication being respectively $((s+\alpha)!/s!)^{1/\alpha} \cdot \frac{\alpha}{s} \cdot N^{1/\alpha} k$ and $(1+\alpha/s) \cdot k$ bits.*

Proof. *Communication*: Chooser-side communication (the total length of ciphertexts κ_{jt}) is

$$\sum_{i=1}^{\alpha} \ell_i \frac{s+i}{s} k = \sum_{i=1}^{\alpha} \sqrt[\alpha]{\frac{(s+\alpha)!}{s!}} \cdot \frac{1}{s} N^{1/\alpha} k = \sqrt[\alpha]{\frac{(s+\alpha)!}{s!}} \cdot \frac{\alpha}{s} \cdot N^{1/\alpha} k \enspace .$$

PRIVATE INPUT: Chooser has $\iota = (\iota_1, \dots, \iota_\alpha)$, Sender has μ.
PRIVATE OUTPUT: Chooser has $\mu(\iota_1, \dots, \iota_\alpha)$.

Round 1, Chooser: For all $j \in [\alpha]$ do, for all $t \in [\ell_j]$ do:
Generate $r_{jt} \leftarrow_r R(x)$.
Send $\kappa_{jt} \leftarrow E_K^{s+j-1}(\{t \stackrel{?}{=} \iota_j\}; r_{jt}) \in \mathbb{Z}_{n^{s+j}}$ to Sender.
Round 2, Sender:

For all $i_2 \in [\ell_2], \dots, i_\alpha \in [\ell_\alpha]$ do:
Set $w_1(i_2, \dots, i_\alpha) \leftarrow \prod_{t \in [\ell_1]} \kappa_{1,t}^{\mu(t, i_2, \dots, i_\alpha)} \mod n^{s+1}$.
For all $i_3 \in [\ell_3], \dots, i_\alpha \in [\ell_\alpha]$ do:
Set $w_2(i_3, \dots, i_\alpha) \leftarrow \prod_{t \in [\ell_2]} \kappa_{2,t}^{w_1(t, i_3, \dots, i_\alpha)} \mod n^{s+2}$.
$\vdots$
For all $i_{\alpha-1} \in [\ell_{\alpha-1}], i_\alpha \in [\ell_\alpha]$ do:
Set $w_{\alpha-2}(i_{\alpha-1}, i_\alpha) \leftarrow \prod_{t \in [\ell_{\alpha-2}]} \kappa_{\alpha-2,t}^{w_{\alpha-3}(t, i_{\alpha-1}, i_\alpha)} \mod n^{s+\alpha-2}$.
For all $i_\alpha \in [\ell_\alpha]$ do:
Set $w_{\alpha-1}(i_\alpha) \leftarrow \prod_{t \in [\ell_{\alpha-1}]} \kappa_{\alpha-1,t}^{w_{\alpha-2}(t, i_\alpha)} \mod n^{s+\alpha-1}$.
Set $w_\alpha \leftarrow \prod_{t \in [\ell_\alpha]} \kappa_{\alpha,t}^{w_{\alpha-1}(t)} \mod n^{s+\alpha}$.
Send $w_\alpha \in \mathbb{Z}_{n^{s+\alpha}}$ to Chooser.
Reconstruction, Chooser: Output $D_K^s(D_K^{s+1}(\dots(D_K^{s+\alpha-1}(w_\alpha))\dots))$.

Protocol 1: Protocol $\mathsf{DJCPIR}(\alpha)$, for fixed K and s.

Correctness: clear, since $D_K^{s+\alpha-1}(w_\alpha) = w_{\alpha-1}(\iota_\alpha)$, $D_K^{s+\alpha-2}(w_{\alpha-1}(\iota_\alpha)) = w_{\alpha-2}(\iota_{\alpha-1}, \iota_\alpha)$, $\dots$, $D_K^{s+i-1}(w_i(\iota_{i+1}, \dots, \iota_\alpha)) = w_{i-1}(\iota_i, \dots, \iota_\alpha)$, $\dots$, and $D_K^s(w_1(\iota_2, \dots, \iota_\alpha)) = \mu(\iota_1, \dots, \iota_\alpha)$.

Privacy of Chooser: Since the Decisional Composite Residuosity problem is hard, Π is semantically secure. Sender sees only random encryptions of 0-s and 1-s, and thus privacy of Chooser is guaranteed by the semantical security of Π. □

Asymptotically, total communication of $\mathsf{DJCPIR}(\alpha)$ is $(\alpha + O(\log \alpha)) \cdot \frac{\alpha}{s^2 e} N^{1/\alpha} \cdot k$. In the asymptotically optimal case $\alpha = \frac{\log N}{2}$ this is equal to $(1 + o(1)) \frac{\log^2 N}{s^2 e} \cdot k$.

In the case of the hypercube (i.e., when $\ell_i = N^{1/\alpha}$), chooser-side communication is $\sum_{i=1}^{\alpha} (1 + i/s) \cdot N^{1/\alpha} k = (\alpha s + \frac{\alpha(\alpha+1)}{2s}) N^{1/\alpha} k = \alpha(1 + \frac{\alpha+1}{2s}) N^{1/\alpha} k = (1 + o(1)) \frac{\alpha^2}{2s} \cdot N^{1/\alpha} k$. In the asymptotically optimal case $\alpha = \frac{\log N}{2}$, this will be equal to $(1 + o(1)) \frac{\log^2 N}{2s} \cdot k$. Thus, using the hyper-rectangle instead of the hypercube results in asymptotic win of $\frac{se}{2}$ times.

4 Two Hypothetical Logarithmic $\binom{N}{1}$-CPIR-s

The constructed $\binom{N}{1}$-CPIR $\mathsf{DJCPIR}(\alpha)$ has total communication $\Theta(\log^2 N) k$. However, the communication complexity of the non-private information retrieval is $\log N + \log |\mathcal{D}|$. A natural question arises: can one construct a $\binom{N}{1}$-CPIR with $\Theta(\log N) k$ total communication by just assuming that there exists a cryptosystem that satisfies some "reasonable" properties?

As we show next, $\mathsf{DJCPIR}(\alpha)$ can be modified to have logarithmic communication under some feasible additional conjectures on the used homomorphic cryptosystem. We do not know whether such cryptosystems exist. Both modifications are based on the next observation: $\mathsf{DJCPIR}(\alpha)$ has log-squared communication because the length of the values $\kappa_{j,t}$ depends on j. We propose two different modifications to the $\mathsf{DJCPIR}(\alpha)$ that overcome this obstacle.

In the first case, we assume that $\kappa_{j,t} = E_K^{s+j-1}(\{t \stackrel{?}{=} \iota_j\}; r_{j;t})$ can be securely communicated to Sender by using ηk bits. This involves an hypothesis of the existence of a certain "nice" cryptosystem. In the second solution, we assume that $\kappa_{j,t} = E_K^s(\{t \stackrel{?}{=} \iota_j\}; r_{j;t})$ is used as a multiplicand; this involves an alternative hypothesis of the existence of a ring-homomorphic cryptosystem. We conjecture so—although we also show that the Damgård-Jurik cryptosystem from PKC 2001 does not have the conjectured properties.

First case. We now make the next conjecture.

Conjecture 1. There exists a length-flexible semantically secure homomorphic cryptosystem $\Pi = (G, E, D)$, such that (a) $C_s(x) \subseteq P_{s+1}(x)$, (b) $|C_s(x)| \approx (s+1)k$ and (c) for every s, z there exist efficient functions $g_s : P_s(x) \times R(x) \to Z_s(x)$ and $f_{s,z} : Z_s(x) \to C_{s+z}(x)$, such that $f_{s,z}(g_s(m;r)) = E_K^{s+z}(m;r')$, for $m \in \{0,1\}$ and for any $r \in R(x)$. Moreover, $|Z_s(x)|$ does not depend on z (or at least it is sub-linear in z). When $|Z_s(x)| = |C_s(x)| = s \log n$ for some n then we call such a cryptosystem *"nice"*.

Based on a "nice" cryptosystem Π, we can construct a new $\binom{N}{1}$-CPIR protocol, that looks almost exactly the same as Protocol 1, except that (a) $\kappa_{j,t}$ is defined as $\kappa_{j,t} \leftarrow g_s(\{t \stackrel{?}{=} \iota_j\}; r_{jt})$, and (b) when using $\kappa_{j,t}$ in the i-th sub-round of round 2, Sender first applies the function f_i on it. For example, he sets

$$w_\alpha \leftarrow \prod_{t \in [\ell_\alpha]} f_\alpha(\kappa_{\alpha,t})^{w_{\alpha-1}(t)} \mod n^{s+\alpha} \enspace .$$

Thus, Chooser communicates every $\kappa_{j,t}$ to Sender by just using ηk bits.

Theorem 2. *Let Π be a (hypothetical) "nice" cryptosystem. (a) For every $\alpha \geq 1$, there exists a CPIR protocol $\mathsf{HypoCPIR}^1(\alpha)$ with chooser-side and sender-side communication being respectively $\alpha N^{1/\alpha}(1 + 1/s)k$ and $(1 + \alpha/s)k$ bits. (a) Let $a = (W(\frac{1}{e(s+1)}) + 1) \cdot \log e$. There exists a CPIR protocol $\mathsf{HypoCPIR}^1(\frac{\log 2}{a} \log N)$ with chooser-side and sender-side communication being respectively $\frac{2^{a+1}}{a} \log N \cdot k$ and $(1 + \frac{1}{a} \cdot \log N) \cdot k$ bits.*

Proof. Correctness: By Conjecture 1, $f_j(\kappa_{jt}) \mod n^{s+j} = E_K^{s+j-1}(\{t \stackrel{?}{=} \iota_j\}; r_{jt})$. Communication: Chooser-side communication (the total length of ciphertexts κ_{jt}) is $\alpha \cdot N^{1/\alpha}(1 + 1/s) \cdot k$. Privacy of Chooser: Sender sees only random encryptions of 0-s and 1-s, and thus Chooser's privacy is guaranteed by the semantical security of Π. □

The constant a has been chosen to optimise the total communication. Note that for $s = 1$, chooser-side communication is approximately $3.81076 \cdot \log N \cdot k$ and sender-side communication is approximately $(1 + 0.59899 \log N)k$.

On the (im)possibility of "nice" cryptosystems. Since Π is a semantically secure homomorphic cryptosystem, it must be the case that $E^s_K(m_1; r_1) \cdot E^s_K(m_2; r_2) = E^s_K(m_1 + m_2; r_1 \circ r_2)$. For all well-known semantically secure homomorphic cryptosystems, $\cdot$ corresponds to the modular multiplication in $C_s(x) = \mathbb{Z}^*_{n_s}$ for some n_s. Thus, in such a case $E^s_K(m; r) = g^m_s f(r, s) \mod n_s$ for some element $g_s \in \mathbb{Z}^*_{n_s}$ and for some function f.

Moreover, when Π is length-flexible then it holds—at least for the currently known length-flexible cryptosystems Π—that $\ell = |C_{s+1}(x)|/|C_s(x)|$ is an integer. Also, $E^{s+1}_K(m; r) = g^m_{s+1} f(r, s + 1) \mod n_{s+1}$ where $n_{s+1} = \overline{n} n_s$ for some integer $\overline{n}$.

Assume now that $E^s_K(m; r) = a \mod n_s$ (e.g., $a = g^m_s f(r, s)$ without modular reduction), that is, $a = E^s_K(m; r) + bn_s$ for some b. We want to establish for which functions h, $h(a) \mod n_{s+1}$ can be computed from $a \mod n_s$—that is, for which functions h, $h(a) \mod n_{s+1}$ does not depend on b.

When we assume that h does not involve modular reductions, we can easily find that h must be one of the next basic operations or their composite. First, $h_1(a) = a\overline{n}$. Then $h_1(a) \equiv a\overline{n} \equiv E^s_K(m; r)\overline{n} \mod n_{s+1}$, thus $h_1(a) \mod n_{s+1}$ can be computed from $a \mod n_s$. Second, $h_2(a) = a^{\overline{n}}$, since $h_2(a) \equiv E^s_K(m; r)^{\overline{n}} \mod n_{s+1}$. Assuming $E^{s+1}_K(m; r) = g^m_s f(r, s+1) \mod n_{s+1}$, we get $a^{\overline{n}} \equiv g^{\overline{n}m}_s f(m, s+1)^{\overline{n}} \mod n_{s+1}$.

No other function on $a \mod n_s$, a is an arbitrary integer, except the two cases above (h_1 and h_2) and their compositions with each other and with functions in $\mathbb{Z}_{n_{s+1}}$, can return a meaningful function $h(a) \mod n_{s+1}$: e.g., for $\overline{n} \nmid j$, $a^j \equiv (E^s_K(m; r) + bn_s)^j \equiv (E^s_K(m; r)^j + \binom{j}{2} E^s_K(m; r)^{j-1} b + \dots) \mod n_{s+1}$ depends also on b—a value that is unknown to the potential Sender.

Thus, $\mathsf{HypoCPIR}^1(\alpha)$ exists either when some composition of h_1 and h_2 can transform a valid ciphertext from $C_s(x)$ to a valid ciphertext of the same element but from $C_{s+1}(x)$. Let us look at the case of the Damgård-Jurik cryptosystem from PKC 2001.

Lemma 1. *Let $\Pi = (G, E, D)$ be the Damgård-Jurik cryptosystem from PKC 2001. Let $\alpha = E^s_K(m; r)$ for some $m \in \mathbb{Z}_{n^s}$ and $r \in \mathbb{Z}^*_n$. Then $E^{s+1}_K(mn; r) = \alpha^n \mod n^{s+2}$ and thus $E^{s+\alpha}_K(mn^\alpha; r) = \alpha^{n^\alpha} \mod n^{s+\alpha+1}$ for any $\alpha > 0$.*

Proof. First, $\alpha = (1 + n)^m r^{n^s} \mod n^{s+1}$. Thus, $\alpha^n \equiv ((1 + n)^m r^{n^s} \mod n^{s+1})^n \mod n^{s+2}$. But

$$((1 + n)^m \mod n^{s+1})^n \equiv \left(1 + mn + \dots + \binom{m}{s} n^s\right)^n \equiv (1 + n)^{mn} \mod n^{s+2}$$

and $(r^{n^s} \mod n^{s+1})^n \equiv r^{n^{s+1}} \mod n^{s+2}$. Therefore, $\alpha^n \equiv (1 + n)^{mn} r^{n^{s+1}} \mod n^{s+2}$. □

In this case, $\overline{n} = n$. Then, $E^s_K(m; r) \cdot n \mod n^{s+2}$ is not a valid ciphertext and $E^s_K(m; r)^n \equiv E^{s+1}_K(mn; r) \mod n^{s+2}$. The latter value cannot be used to compute $E^{s+1}_K(m; r)$ by anybody who does not know the factorisation of n, since n is not an invertible element of $P_{s+1}(x)$. Thus, the Damgård-Jurik cryptosystem from PKC 2001 is not "nice".

An hypothetical CPIR based on a ring-homomorphic cryptosystem. Assume that Π is a ring-homomorphic cryptosystem, that is, $D_K^s(E_K^s(m_1; r_1) \otimes E_K^s(m_2; r_2)) = m_1 \cdot m_2$ and $D_K^s(E_K^s(m_1; r_1) \oplus E_K^s(m_2; r_2)) = m_1 + m_2$ where $C_s(x)$ is a finite ring with operations $(\otimes, \oplus)$ and $P_s(x)$ is a finite ring with operations $(\cdot, +)$. In this case, we again modify Protocol 1 just be changing the definitions of $\kappa_{j,t}$ and w_i. First, set $\kappa_{j,t} \leftarrow E_K^s(\{t \stackrel{?}{=} \iota_j\}; r_{j,t})$. Then, set

$$w_1(i_2, \dots, i_\alpha) \leftarrow \bigoplus_t \left(E_K^s(\mu(t, i_2, \dots, i_\alpha); r'_{i_2,\dots,i_\alpha}) \otimes \kappa_{1,t}\right) \quad ,$$

thus $D_K^s(w_1(i_2, \dots, i_\alpha)) = \mu(\iota_1, i_2, \dots, i_\alpha)$. Computation of w_i for $i > 1$ is analogous.

The resulting hypothetical $\binom{N}{1}$-CPIR $\mathsf{HypoCPIR}^2(\alpha)$ is slightly more efficient than $\mathsf{HypoCPIR}^1(\alpha)$ since the sender would only return one ciphertext from $C_s(x)$ and not from $C_{s+\alpha}(x)$, as in the case of $\mathsf{HypoCPIR}^1(\alpha)$.

Theorem 3. *Let Π be a (hypothetical) ring-homomorphic cryptosystem. (a) For every $\alpha \geq 1$, there exists a CPIR protocol $\mathsf{HypoCPIR}^2(\alpha)$ with chooser-side and sender-side communication being respectively $\alpha N^{1/\alpha}(1 + 1/s)k$ and $(1 + 1/s)k$ bits. (a) Let $\alpha = \log N$. There exists a CPIR protocol $\mathsf{HypoCPIR}^2(\log N)$ with chooser-side and sender-side communication being respectively $2(1 + 1/s) \log N \cdot k$ and $(1 + 1/s) \cdot k$ bits.*

For $s = 1$, the chooser-side communication of $\mathsf{HypoCPIR}^2(\log N)$ is $4 \cdot \log N \cdot k$ and the sender-side communication is $2 \cdot k$. However, the Damgård-Jurik cryptosystem is not ring-homomorphic and moreover, no such cryptosystems are currently known. Our intuition is that it is "easier" to construct "nice" cryptosystems.

5 Comparisons and Discussion

Communication complexity. Fix $s = 1$. Table 1 summaries the next discussion. The difference between the communications of $\mathsf{HomCPIR}\left(\sqrt{\log N}\right)$, $\mathsf{DJCPIR}(\frac{\log N}{2})$ and the hypothetical $\mathsf{HypoCPIR}^1(\ln N/a)$ (where a is as defined in Thm. 2) is depicted by the Figure 1. Note that $\mathsf{DJCPIR}(\frac{\log N}{2})$ is more communication-efficient than $\mathsf{HomCPIR}\left(\sqrt{\log N}\right)$ for all N-s.

Chooser-side versus sender-side communication. One of the nice properties of $\mathsf{HomCPIR}\,(\alpha)$ is that by varying α, one can minimise the sender-side communication to be ηk (although then chooser-side communication will be linear) or the chooser-side communication to $\Theta(\log N)k$ (although then sender-side communication will be linear). In the $\mathsf{DJCPIR}(\alpha)$, the minimal chooser-side communication is $\Theta(\log^2 N)k$

Protocol	Chooser-side	Sender-side
Without privacy	$\log N$	$\log \lvert\mathcal{D}\rvert \leq s \log n = k$
$\mathsf{HomCPIR}\,(\alpha)$	$\eta\alpha N^{1/\alpha} \cdot k$	$\eta^{\alpha} \cdot k$
$\mathsf{HomCPIR}\,(\log_\eta N)$	$\eta^2 \log_\eta N \cdot k$	$N \cdot k$
$\mathsf{HomCPIR}\,(\sqrt{\log_\eta N})$	$\eta\sqrt{\log_\eta N}\eta^{\sqrt{\log_\eta N}} \cdot k$	$\eta^{\sqrt{\log_\eta N}} \cdot k$
$\mathsf{HomCPIR}\,(1)$	$\eta N \cdot k$	ηk
$\mathsf{DJCPIR}(\alpha)$	$\left(\frac{(s+\alpha)!}{s!}\right)^{1/\alpha} \cdot \frac{\alpha}{s} N^{1/\alpha} k$	$(\alpha+1) \cdot k$
$\mathsf{DJCPIR}(\frac{\log N}{2})$	$\frac{1+o(1)}{se} \log^2 N \cdot k$	$(\frac{\log N}{2}+1) \cdot k$
$\mathsf{DJCPIR}(1)$	$(1+1/s)Nk$	$2k$
$\mathsf{HypoCPIR}^1(\alpha)$	$\frac{s+1}{s} \cdot \alpha N^{1/\alpha} \cdot k$	$(1+\alpha/s)k$
$\mathsf{HypoCPIR}^1(\frac{\ln N}{a})$	$\frac{2^{a+1}}{a} \cdot \log N \cdot k$	$(1+\log N/a)k$
$\mathsf{HypoCPIR}^2(\alpha)$	$\frac{s+1}{s} \cdot \alpha N^{1/\alpha} \cdot k$	$(1+1/s)k$
$\mathsf{HypoCPIR}^2(\log N)$	$2^{\frac{s+1}{s}} \cdot \log N \cdot k$	$(1+1/s)k$

Table 1. Total communication of $\mathsf{HomCPIR}\,(\alpha)$, $\mathsf{DJCPIR}(\alpha)$, $\mathsf{HypoCPIR}^1(\alpha)$ and $\mathsf{HypoCPIR}^2(\alpha)$ protocols when retrieving $< k$ bits with a single query. (For simplicity, we omit the ceiling signs, but it must be remembered that α and α are integers.) Here, a is as defined in Thm. 2

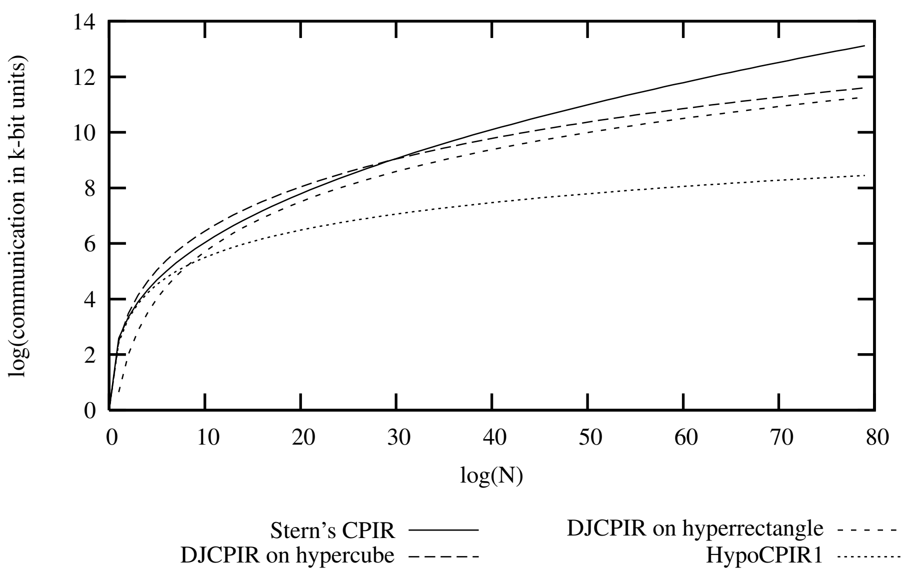

Fig. 1. Communication of $\mathsf{HomCPIR}\,(\sqrt{\log N})$, $\mathsf{DJCPIR}(\frac{1}{2}\log N)$ (on hypercube) and $\mathsf{DJCPIR}(\frac{\ln N}{2})$ (on hyper-rectangle) in logarithm of k-bit units on logarithmic scale in N, assuming that $\eta = 2$ and $s = 1$. Comparison is also given with the hypothetical $\mathsf{HypoCPIR}^1(\frac{\ln N}{a})$

(although in this case the sender-side communication is logarithmic) and the minimal sender-side communication is $2k$ (and then the chooser-side communication is linear).

On the other hand, the $\binom{N}{1}$-OT protocols of [NP01,AIR01,Lip03] have constant chooser-side communication and linear sender-side communication. It is an interesting open question to construct a (non-hypothetical) $\binom{N}{1}$-CPIR with logarithmic chooser-side communication and polylogarithmic sender-side communication.

Computational complexity. The time to encrypt and decrypt by using the Damgård-Jurik cryptosystem depends polynomially on s; let us conservatively assume that the dependence is quadric. Therefore, computing $E_K^{s+\alpha}$ is $\alpha^{O(4)} = \log^{O(4)} N$ times slower than computing E_K^s. On the other hand, in $\mathsf{HomCPIR}\left(\sqrt{\log N}\right)$, Sender must do $\Theta(2^{\sqrt{\log N}})$ exponentiations modulo n. Therefore, asymptotically $\mathsf{DJCPIR}(\log N)$ is also faster than $\mathsf{HomCPIR}\left(\sqrt{\log N}\right)$ since $\log^{1+O(4)} N$ grows slower than $2^{\sqrt{\log N}}$.

Retrieval of big blocks. Let $m = |\mathcal{D}|$. Assume that $n^{s-1} \leq m < n^s$ for $s \geq 1$, thus $k = s \log n$. Then one can execute $\mathsf{DJCPIR}(\frac{\ln N}{2})$ to transmit a single entry with total communication $\Theta(\log^2 N) \cdot k$.

6 Oblivious Transfer with Log-Squared Communication

The $\mathsf{DJCPIR}(\alpha)$ protocol can be modified to an oblivious transfer protocol by letting Chooser to accompany the first round of the $\mathsf{DJCPIR}(\alpha)$ protocol with a standard witness-indistinguishable proof of knowledge (WIPOK) that he chose the inputs correctly. This means (in the case of hypercube) $\alpha N^{1/\alpha}$ WIPOK-s that an encrypted value is either 0 or 1, and $N^{1/\alpha}$ WIPOK-s that the product of α ciphertexts decrypts to 1. Again, some of these WIPOK-s are done with a larger s, so that the total overhead of the WIPOK-s is $\Theta(\log^2 N)k$. This does not increase the asymptotic communication complexity of the protocol. Therefore, we can construct a four-round $\binom{N}{1}$-OT protocol with total communication $\Theta(\log^2 N)k$ that can be made two-round in the random-oracle model by using the Fiat-Shamir heuristic.

We will now give a detailed description of the WIPOK that $D_K^s(c) \in \{0, 1\}$. For this, one first computes $c_1 = c/E_K(0; 0)$ and $c_2/E_K(1; 0)$ and then proves that either $D_K(c_1) = 0$ or $D_K(c_2) = 0$, as follows. Let Π be a semantically secure additively homomorphic cryptosystem. Assume that $c_1 = E_K(0; r)$. Let c_2 be another ciphertext. The next protocol for proving that either $D_K(c_1) = 0$ or $D_K(c_2) = 0$ was proposed in [DJ01]:

1. Chooser chooses a random $r_1 \leftarrow R(x)$ and sets $a_1 \leftarrow E_K^s(0; r_1)$. He generates a view (a_2, e_2, z_2) by setting $e_2 \leftarrow \{0,1\}^t$, $z_2 \leftarrow \mathbb{Z}_n$ and $a_2 \leftarrow E_K^s(0; z_2) \cdot c_2^{-e_2} \mod n^{s+1}$. He sends (a_1, a_2) to Sender.
2. Sender chooses a random t-bit number d, and sends d to Chooser.
3. Chooser computes $e_1 \leftarrow d - e_2 \mod 2^t$ and $z_1 \leftarrow r_1 r^{e_1} \mod n$. He sends (e_1, z_1, e_2, z_2) to Sender.

4. Sender checks that $d = e_1 + e_2 \mod 2^t$, $E^s_K(0; z_1) = a_1 c_1^{e_1} \mod n^{s+1}$, $E^s_K(0; z_2) = a_2 c_2^{e_2} \mod n^{s+1}$, and that $u_1, u_2, a_1, a_2, z_1, z_2$ are relatively prime to n. He accepts iff all verifications succeed.

Total communication of this WIPOK is $2|C_s(x)|+3t+2\lceil\log(n+1)\rceil = 2(1+1/s)k+3t+\frac{2}{s}k = 3t+2(1+2/s)\cdot k$.

In total, the WIPOK-s of this type add $\sum_{i=1}^{\alpha} \ell_i(3t+2(1+(i+1)/s)\cdot k)$ bits of communication to the $\sum_{i=1}^{\alpha} \ell_i((1+i/s)\cdot k)$ bits of communication of the CPIR. Let us assume for simplicity that $\ell_i = N^{1/\alpha}$ for all i. Then the communication overhead of the $\binom{N}{1}$-OT protocol is

$$N^{1/\alpha}\sum_{i=1}^{\alpha}(3t+2(1+(i+2)/s)\cdot k) = N^{1/\alpha}(3t\alpha+\frac{1}{s}\cdot(2\alpha(s+2)+\alpha^2+\alpha)k)$$
$$= (1+o(1))N^{1/\alpha}\cdot\frac{\alpha^2}{s}\cdot k \ .$$

In the near-optimal case $\alpha = \frac{\log N}{2}$, this is $(1/s+o(1))\log^2 N\cdot k$ bits. Recall that in the case of the hypercube-$\mathsf{DJCPIR}(\frac{\log N}{2})$, the total communication is $(1+o(1))\frac{\log^2 N}{2s}k$, thus the communication only asymptotically triples after adding the WIPOK-s. (The $N^{1/\alpha}$ proofs that some product of ciphertexts decrypts to 1 does not add a significant amount of communication.)

Theorem 4. *Let Π be the Damgård-Jurik cryptosystem from PKC 2001. Assume that the Decisional Composite Residuosity Problem is hard. For every $\alpha \geq 1$, there exists an $\binom{N}{1}$-oblivious transfer protocol $\mathsf{DJOT}(\alpha)$ with total communication $\frac{3}{2s}(1+o(1))\alpha^2 N^{1/\alpha}k$ bits. In particular, there exists an $\binom{N}{1}$-OT protocol $\mathsf{DJOT}(\frac{\log N}{2})$ with total communication $\frac{3}{2s}(1+o(1))\log^2 N\cdot k$ bits.*

Alternative constructions. Alternative $\binom{N}{1}$-OT protocol constructions are possible (e.g., based on the methodology of [NP99]) and will be analysed in the final version of this paper.

Acknowledgements

We would like to thank Yan-Cheng Chang for comments. This work was partially supported by the Finnish Defence Forces Institute for Technological Research and by the Finnish Academy of Sciences.

References

[AIR01] William Aiello, Yuval Ishai, and Omer Reingold. Priced Oblivious Transfer: How to Sell Digital Goods. In Birgit Pfitzmann, editor, *Advances in Cryptology — EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 119–135, Innsbruck, Austria, 6–10 May 2001. Springer-Verlag.

[CGKS95] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private Information Retrieval. In *36th Annual Symposium on Foundations of Computer Science*, pages 41–50, Milwaukee, Wisconsin, October 23–25 1995. IEEE.

[Cha04] Yan-Cheng Chang. Single Database Private Information Retrieval with Logarithmic Communication. In Josef Pieprzyk and Huaxiong Wang, editors, *The 9th Australasian Conference on Information Security and Privacy (ACISP 2004)*, volume ? of *Lecture Notes in Computer Science*, pages ?–?, Sydney, Australia, 13–15 July 2004. Springer-Verlag. Accepted.

[CMS99] Christian Cachin, Silvio Micali, and Markus Stadler. Computational Private Information Retrieval with Polylogarithmic Communication. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 402–414, Prague, Czech Republic, 2–6 May 1999. Springer-Verlag.

[DJ01] Ivan Damgård and Mads Jurik. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. In Kwangjo Kim, editor, *Public Key Cryptography 2001*, volume 1992 of *Lecture Notes in Computer Science*, pages 119–136, Cheju Island, Korea, 13–15 February 2001. Springer-Verlag.

[DJ03] Ivan Damgård and Mads Jurik. A Length-Flexible Threshold Cryptosystem with Applications. In Rei Safavi-Naini, editor, *The 8th Australasian Conference on Information Security and Privacy*, volume 2727 of *Lecture Notes in Computer Science*, pages 350–364, Wollongong, Australia, July 9-11 2003. Springer-Verlag.

[FS86] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology—CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194, Santa Barbara, California, USA, 11–15 August 1986. Springer-Verlag, 1987.

[Lip03] Helger Lipmaa. Verifiable Homomorphic Oblivious Transfer and Private Equality Test. In Chi Sung Laih, editor, *Advances on Cryptology — ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 416–433, Taipei, Taiwan, 30 November–4 December 2003. Springer-Verlag.

[NP99] Moni Naor and Benny Pinkas. Oblivious Transfer and Polynomial Evaluation. In *Proceedings of the Thirty-First Annual ACM Symposium on the Theory of Computing*, pages 245–254, Atlanta, Georgia, USA, 1–4 May 1999. ACM Press.

[NP01] Moni Naor and Benny Pinkas. Efficient Oblivious Transfer Protocols. In *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 448–457, Washington, DC, USA, January 7–9 2001. ACM Press.

[NS98] David Naccache and Jacques Stern. A New Public Key Cryptosystem Based on Higher Residues. In *5th ACM Conference on Computer and Communications Security*, pages 59–66, San Francisco, CA, USA, 3–5 November 1998. ACM Press.

[OP98] Kazuo Ohta and Dingyi Pei, editors. *Advances on Cryptology — ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, Beijing, China, October 1998. Springer-Verlag.

[OU98] Tatsuaki Okamoto and Shigenori Uchiyama. A New Public-Key Cryptosystem as Secure as Factoring. In Kaisa Nyberg, editor, *Advances in Cryptology — EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 308–318, Helsinki, Finland, May 31 – June 4 1998. Springer-Verlag.

[Pai99] Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238, Prague, Czech Republic, 2–6 May 1999. Springer-Verlag.

[Ste98] Julien P. Stern. A New and Efficient All or Nothing Disclosure of Secrets Protocol. In Ohta and Pei [OP98], pages 357–371.