Journal of Computer and System Sciences 78 (2012) 1142–1157

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Communication-efficient distributed oblivious transfer

Amos Beimel[a,1], Yeow Meng Chee[b,2], Huaxiong Wang[b,2], Liang Feng Zhang[b,*]

[a] Department of Computer Science, Ben-Gurion University of the Negev, Beer Sheva, Israel
[b] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

ARTICLE INFO

Article history:
Received 1 December 2011
Received in revised form 4 February 2012
Accepted 21 February 2012
Available online 27 February 2012

Keywords:
Distributed oblivious transfer
Private information retrieval
Communication complexity

ABSTRACT

Distributed oblivious transfer (DOT) was introduced by Naor and Pinkas (2000) [31], and then generalized to (k,ℓ)-DOT-$\binom{n}{1}$ by Blundo et al. (2007) [8] and Nikov et al. (2002) [34]. In the generalized setting, a (k,ℓ)-DOT-$\binom{n}{1}$ allows a sender to communicate one of n secrets to a receiver with the help of ℓ servers. Specifically, the transfer task of the sender is distributed among ℓ servers and the receiver interacts with k out of the ℓ servers in order to retrieve the secret he is interested in. The DOT protocols we consider in this work are information-theoretically secure. The known (k,ℓ)-DOT-$\binom{n}{1}$ protocols require linear (in n) communication complexity between the receiver and servers. In this paper, we construct (k,ℓ)-DOT-$\binom{n}{1}$ protocols which only require sublinear (in n) communication complexity between the receiver and servers. Our constructions are based on information-theoretic *private information retrieval*. In particular, we obtain both a specific reduction from (k,ℓ)-DOT-$\binom{n}{1}$ to polynomial interpolation-based information-theoretic private information retrieval and a general reduction from (k,ℓ)-DOT-$\binom{n}{1}$ to any information-theoretic private information retrieval. The specific reduction yields (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocols of communication complexity $O(n^{1/\lfloor(k-\tau-1)/t\rfloor})$ between a semi-honest receiver and servers for any integers t and τ such that $1\leqslant t\leqslant k-1$ and $0\leqslant\tau\leqslant k-1-t$. The general reduction yields (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocols which are as communication-efficient as the underlying private information retrieval protocols for any integers t and τ such that $1\leqslant t\leqslant k-2$ and $0\leqslant\tau\leqslant k-1-t$.

1. Introduction

In an *oblivious transfer* protocol a sender sends information to a receiver such that the sender is oblivious to the information it sends. Specifically, in a one-out-of-n oblivious transfer, denoted by $\binom{n}{1}$-OT, the sender has n secrets $W_1,\ldots,W_n$, the receiver has an index $i\in[n]$, and the sender communicates W_i to the receiver such that the receiver learns no information about the remaining secrets and the sender knows nothing about i. The notion of oblivious transfer was introduced by Rabin [36] and then redefined in the form of $\binom{2}{1}$-OT by Even et al. [19] and $\binom{n}{1}$-OT by Brassard et al. [10], respectively. The $\binom{2}{1}$-OT, $\binom{n}{1}$-OT and Rabin's OT have been shown equivalent to each other [9,17]. As an important cryptographic primitive, oblivious transfer has found fundamental applications in cryptographic studies and protocol design [23,24,30,11,15,25].

[*] Corresponding author.
E-mail addresses: amos.beimel@gmail.com (A. Beimel), ymchee@ntu.edu.sg (Y.M. Chee), hxwang@ntu.edu.sg (H. Wang), liangfeng.zhang@ntu.edu.sg (L.F. Zhang).

[1] Partially supported by Israel Science Foundation grant 938/09.
[2] Partially supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

0022-0000/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcss.2012.02.002

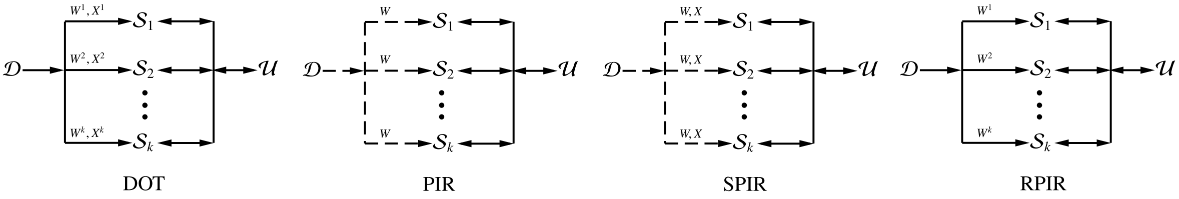

Fig. 1. DOT-related models.

Oblivious transfer has been implemented under a variety of assumptions [36,19,7,32,1,22,26,29]. However, these implementations are computationally secure and involve heavy public-key operations. Naor and Pinkas [31] introduced *distributed oblivious transfers* (DOT) which are information-theoretically secure and computationally efficient. Specifically, their (k,ℓ)-DOT-$\binom{2}{1}$ protocols [31] are based on polynomial interpolation and only involve arithmetic operations over finite fields. Subsequently, the (k,ℓ)-DOT-$\binom{2}{1}$ was generalized to (k,ℓ)-DOT-$\binom{n}{1}$ for any positive integer n by Blundo et al. [8] and Nikov et al. [34]. Informally, a (k,ℓ)-DOT-$\binom{n}{1}$ (see Fig. 1) involves a sender $\mathcal{D}$ who has n secrets $W_1,\ldots,W_n$, a receiver $\mathcal{U}$ who has an index $i \in [n]$, and ℓ servers $\mathcal{S}_1,\ldots,\mathcal{S}_\ell$. It consists of a *setup stage* when the sender $\mathcal{D}$ distributes the secrets among the ℓ servers by sending to each server $\mathcal{S}_h$ a message, and an *oblivious transfer stage* when the receiver $\mathcal{U}$ contacts k out of the ℓ servers to compute the secret W_i. It is required that $\mathcal{D}$ learns no information on i and $\mathcal{U}$ learns no more information except W_i. More precisely, a (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol should satisfy: (I) after the oblivious transfer stage, any coalition of up to t servers learns no information on i; (II) before the oblivious transfer stage, the receiver learns no information on the sender's secrets, even if it colludes with up to τ servers; (III) after the oblivious transfer stage, a malicious receiver is able to obtain at most one of the n secrets, even if it colludes with up to τ malicious servers.

Distributed oblivious transfers have important applications in the *privacy preserving architecture* of Naor et al. [33]. The architecture involves an *auction issuer*, several *auctioneers* and numerous *bidders*. Typically, in privacy preserving auctions, the auctioneers publish the details of the auctions they are organizing, receive both encrypted bids from the bidders and garbled programs from the auction issuer, and then compute and publish the auctions. The privacy of the bidders is preserved as long as the auction issuer and auctioneers do not collude. Let the auction issuer play the roles of sender and servers and the auctioneer play the role of receiver in the DOT model. Then any DOT protocol provides a solution for the privacy preserving auction problem. The known (k,ℓ)-DOT-$\binom{n}{1}$ protocols require the receiver to communicate $\Omega(n)$ bits with the contacted servers for retrieving one secret. The communication cost is unaffordable whenever n is large. Therefore, for a DOT-based privacy preserving auction, the auctioneers necessarily communicate a large number of bits with the auction issuer in order to compute and publish an auction. In the described scenario, communication-efficient DOT protocols, in which the receiver and servers exchange a much smaller number of bits, are preferred.

In this work, we construct communication-efficient DOT protocols. We propose both a specific reduction from communication-efficient (k,ℓ)-DOT-$\binom{n}{1}$ to polynomial interpolation-based information-theoretic *private information retrieval* (PIR) [14,5,38] and a general reduction from communication-efficient (k,ℓ)-DOT-$\binom{n}{1}$ to any information-theoretic PIR. The specific reduction yields DOT protocols of sublinear communication complexity between the receiver and servers. The general reduction yields extremely communication-efficient DOT protocols due to the recent progress in the research of PIR and *locally decodable codes* (LDCs) [39,18].

1.1. Related work

Private information retrieval (PIR). A t-private k-server information-theoretic private information retrieval protocol [14] allows a user $\mathcal{U}$ to retrieve a data item W_i from k servers $\mathcal{S}_1,\ldots,\mathcal{S}_k$, each of which has a copy of the database $W = W_1,\ldots,W_n$, such that any coalition of up to t servers learns no information on i. The efficiency of a PIR protocol is measured by its communication complexity, i.e., the total number of bits exchanged between the user and servers. Chor et al. [14] proved that in a single-server information-theoretic PIR protocol, the user has to exchange $\Omega(n)$ bits for retrieving one data item. On the other hand, if there are $k \geqslant 2$ non-communicating servers, then the communication complexity can be as small as $O(n^{1/k})$. There are numerous constructions [14,2,6,5,38,39,18,28,12] of PIR protocols. The most efficient 1-private 2-server and 3-server PIR protocols are of communication complexity $O(n^{1/3})$ [14] and $\exp(O(\sqrt{\log n \log\log n}))$ [18], respectively. For $k > t > 1$, the t-private PIR protocols [5,38] are of communication complexity $O(n^{1/\lfloor (2k-1)/t \rfloor})$. To compare with (k,ℓ)-DOT-$\binom{n}{1}$, one may think that there is a dummy sender $\mathcal{D}$ who distributes the database W to servers in any k-server PIR protocol (see Fig. 1). In this comparative PIR model, the secrets of $\mathcal{D}$ are completely disclosed to the servers and, furthermore, the user is not prevented from obtaining more information than what he is interested in (e.g., an execution of the 2-server PIR protocol of [14] reveals $O(n^{1/3})$ secrets to $\mathcal{U}$).

Symmetrically private information retrieval (SPIR). In a t-private k-server symmetrically private information retrieval [21], a user $\mathcal{U}$ is allowed to retrieve a data item W_i from k-servers $\mathcal{S}_1,\ldots,\mathcal{S}_k$, each of which has a copy of the database W, such that any coalition of up to t-servers learns no information on i and $\mathcal{U}$ learns no more information except W_i. Gertner et al. [21] proposed both general reductions and specific reductions from SPIR to PIR in the common random string model (i.e., all servers share a common random string X). In particular, their reductions preserve the asymptotic communication complexity of the underlying PIR protocols and require the use of a small number of additional auxiliary servers. One may think that there is a dummy sender $\mathcal{D}$ who distributes W and X to all servers in an SPIR protocol (see Fig. 1). In this comparative SPIR model, the secrets of $\mathcal{D}$ are completely disclosed to the servers. Therefore, SPIR does not provide solutions for DOT.

Random server model for private information retrieval (RPIR). In the PIR and SPIR models, the database W is replicated among multiple non-communicating servers. This data replication problem may be serious because each server could be broken into or sell the database behind the legitimate database owner's back. Gertner et al. [20] suggested that the database owner secret-shares W among random servers instead of simply replicating W among non-communicating servers. A PIR protocol in this random server model consists of a setup stage when the database owner $\mathcal{D}$ shares W among the random severs and an on-line stage when the user $\mathcal{U}$ retrieves a data item W_i by interacting with the random servers (see Fig. 1). Gertner et al. [20] proposed a general reduction from RPIR to PIR. Specifically, in order to preserve the asymptotic communication complexity of the underlying PIR protocols, their reduction requires a large number of random servers. As most PIR protocols, the RPIR protocols cannot prevent a user from obtaining more information than what he is interested in.

Locally random reduction (LRR). A (t,k)-locally random reduction [4] allows a user to evaluate a function f at a private input i with the help of k servers, each of which has a reduced form of the function f, such that any coalition of up to t servers learns no information on i. As PIR and RPIR, LRR cannot prevent the user from learning more information on f than $f(i)$.

Commodity-based private information retrieval (cbPIR). A commodity-based private information retrieval [16] involves a user who wants to retrieve W_i of a database W, a number of database servers which have W and commodity severs which send off-line messages (called commodities). A cbPIR consists of an off-line commodity stage when the commodity servers send commodities to the user and database servers and an on-line retrieval stage when the user retrieves W_i by interacting with the database servers. Although the commodity servers do not have any information on the database, the messages they send in the off-line commodity stage dramatically reduce the overall communication involving the user in the on-line retrieval stage. As PIR, RPIR and LRR, a cbPIR cannot prevent the user from obtaining more information on W than what he is interested in.

Private information storage (PIS). A private information storage [35] allows users to privately read and write into a database W which is shared among a number of non-communicating servers such that each individual server learns absolutely no information on which location the users are reading or writing, and what the users are writing into the database. Ostrovsky et al. [35] built their PIS schemes on information-theoretic PIR. Specifically, they proposed a reduction from PIS to PIR which requires only one additional server and a polylogarithmic overhead in communication. As the previous models, PIS does not provide any privacy against malicious users.

Other models. Rivest [37] considered oblivious transfers in the trusted initializer model. A $\binom{n}{1}$-OT in this model involves a sender who has n secrets, a receiver who wants to learn one of the n secrets and a trusted initializer. It consists of a setup stage when the trusted initializer sends private information to the sender and receiver, and a request–reply stage when the receiver learns one secret by interacting with the sender. OT in this model is different from DOT because all secrets are completely disclosed to the sender (playing the role of servers in DOT model) who participates in the on-line request–reply stage and obliviously communicates one secret to the receiver.

1.2. Our results

In this work, we propose both a specific reduction from (k,ℓ)-DOT-$\binom{n}{1}$ to polynomial interpolation-based information-theoretic PIR and a general reduction from (k,ℓ)-DOT-$\binom{n}{1}$ to any information-theoretic PIR.

Specific reduction from (k,ℓ)-DOT-$\binom{n}{1}$ to polynomial interpolation-based PIR. We obtain a non-black-box construction of (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ from any polynomial interpolation-based t-private $(k-\tau)$-server PIR for semi-honest receivers. The DOT protocols we obtain have sublinear communication complexity between the receiver and servers. Specifically, we have that (due to Theorem 1):

– For any integers t, τ, k, ℓ such that $1 \leqslant t \leqslant k-1$, $0 \leqslant \tau \leqslant k-1-t$, and $t+\tau+1 \leqslant k \leqslant \ell$, there is a (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol of communication complexity $O(n^{1/\lfloor (k-1-\tau)/t \rfloor})$ between a semi-honest receiver and servers.

Our specific reduction yields (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ for a wide range of values of t, τ, k and ℓ. It shows a tradeoff between the receiver–server communication complexity and privacy.

General reduction from (k,ℓ)-DOT-$\binom{n}{1}$ to PIR. We obtain a black-box construction of (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ from any information-theoretic t-private $(k-t-\tau)$-server PIR. Specifically, we have that (due to Theorem 3):

- For any integers t, τ, k, ℓ such that $k \leqslant \ell$, $1 \leqslant t \leqslant k-2$, and $0 \leqslant \tau \leqslant k-1-t$, if there is a t-private $(k-t-\tau)$-server PIR protocol of communication complexity $\gamma(n)$, then there is a (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol of communication complexity $O(\gamma(n))$ between the receiver and servers.

Applying the general reduction to the polynomial interpolation-based PIR protocols of [5,38], we have that (due to Corollary 1):

- For any integers t, τ, k, ℓ such that $1 \leqslant t \leqslant k-2$, $0 \leqslant \tau \leqslant k-1-t$, and $\frac{3t+1}{2}+\tau \leqslant k \leqslant \ell$, there is a (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol of communication complexity $O(n^{1/\lfloor\frac{2(k-t-\tau)-1}{t}\rfloor})$ between the receiver and servers.

The general reduction allows us to obtain DOT protocols of extremely small receiver–server communication complexity due to the recent progress in the research of PIR and LDCs. Applying our general reduction to the t-private 3^t-server PIR protocols of communication complexity $\exp(O(\sqrt{\log n \log\log n}))$ (which are implied by [3,18]), we have that (due to Corollary 2):

- For any integers t, τ, ℓ such that $\ell \geqslant 3^t+t+\tau$, there is a (t,τ)-private $(3^t+t+\tau,\ell)$-DOT-$\binom{n}{1}$ protocol of communication complexity $\exp(O(\sqrt{\log n \log\log n}))$ between the receiver and servers.

For small values of t, τ, the above DOT protocols have extremely small communication complexity between the receiver and servers. For instance, for $t=\tau=1$ and $\ell \geqslant 5$, there is a $(1,1)$-private $(5,\ell)$-DOT-$\binom{n}{1}$ protocol of communication complexity $\exp(O(\sqrt{\log n \log\log n}))$ between the receiver and servers such that: (I) after the oblivious transfer stage, each individual server learns absolutely no information about which secret the receiver is interested in; (II) before the oblivious transfer stage, the receiver learns no information about the secrets, even if it colludes with any single server; (III) after the oblivious transfer stage, a malicious receiver is able to obtain at most one of the secrets, even if it colludes with one malicious server.

For some settings of the parameters ℓ and k, our reductions are inefficient in terms of *setup complexity*, i.e., each server may receive $O(\binom{\ell-1}{k-1}\binom{k-1}{t}n+\binom{\ell}{k}\binom{k}{t})$ field elements in the setup stage. However, this complexity becomes reasonable if $\ell=k$ and t is a constant less than k. Note that DOT protocols in a setting where $\ell=k$ have been considered by Cheong et al. [13]. Our reductions are efficient for that setting.

1.3. Organization

In Section 2, we provide both an informal and a formal definition of (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$, and develop several related information equalities; in Section 3, we present our specific reduction from DOT to polynomial interpolation-based information-theoretic private information retrieval; in Section 4, we present our general reduction from DOT to any information-theoretic private information retrieval; in Section 5 we give an evaluation of both reductions; finally, in Section 6, we conclude the paper.

2. Preliminaries

In this section, we define (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocols and develop related information equalities which effectively simplify our security proofs. Our definition follows the vein of [8] and has the strongest requirement for sender's privacy which is called *sender's privacy II* in our definition. The $(k-1,0)$-private (k,ℓ)-DOT-$\binom{n}{1}$ protocols achieving sender's privacy II have been called *strongly* private in [8] and are necessarily multi-round. However, our constructions in Sections 3 and 4 do yield one-round (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocols achieving sender's privacy II when $(t,\tau)\neq(k-1,0)$.

2.1. Informal description of (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$

Let t, τ, k, ℓ, and n be nonnegative integers. A *one-round (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol* $\mathcal{P}$ involves:

- a *sender* $\mathcal{D}$ who has n secrets $W=W_1,\ldots,W_n$, which are typically n elements of a finite field $\mathbb{F}$;
- a *receiver* $\mathcal{U}$ who has an index $i\in[n]$ and wants to retrieve W_i;
- additional ℓ *servers* $\mathcal{S}_1,\ldots,\mathcal{S}_\ell$;

and consists of two stages:

- a *setup stage* when $\mathcal{D}$ sends to each server $\mathcal{S}_h$ a message $D_h = \mathcal{D}(h, W, X)$ in a *secure* way, where $h \in [\ell]$ and X is the random input of $\mathcal{D}$;
- an *oblivious transfer stage* when $\mathcal{U}$ interacts with k out of the ℓ servers, say $\mathcal{S}_K = \{\mathcal{S}_h\colon h \in K\}$ where $K \subseteq [\ell]$ and $|K| = k$, sends to each server $\mathcal{S}_h$ a query $Q_h = \mathcal{Q}(n, i, K, Y)_h$ and receives the answer $A_h = \mathcal{S}_h(D_h, Q_h)$, where Y is the random input of $\mathcal{U}$,

such that the following requirements are satisfied:

- Correctness: The receiver $\mathcal{U}$ is able to correctly determine W_i after the oblivious transfer stage;
- Receiver's privacy: A coalition of up to t servers learns no information on i after the oblivious transfer stage;
- Sender's privacy I: A coalition of $\mathcal{U}$ and up to τ servers learns no information on W before the oblivious transfer stage;
- Sender's privacy II: Given the transcript of communication with k servers, a coalition of $\mathcal{U}$ and up to τ malicious servers learns at most one secret.

2.2. Formalization of correctness and privacy

Let $\bar{\mathcal{U}}$ and $\bar{\mathcal{S}}_h$ be the corrupted $\mathcal{U}$ and $\mathcal{S}_h$. We define the related random variables as follows:

- $\mathbf{W}$ and $\mathbf{I}$: the sequence of n secrets held by $\mathcal{D}$ and the index held by $\mathcal{U}$, respectively;
- $\mathbf{X}$ and $\mathbf{Y}$: the random inputs of $\mathcal{D}$ and $\mathcal{U}$ respectively;
- $\mathbf{D}_h$: the message sent to $\mathcal{S}_h$ by $\mathcal{D}$ during the setup stage;
- $\mathbf{Q}_h$: the query sent to server $\mathcal{S}_h$ by $\mathcal{U}$ during the oblivious transfer stage;
- $\mathbf{A}_h$: the answer sent to $\mathcal{U}$ by server $\mathcal{S}_h$ during the oblivious transfer stage;
- $\mathbf{C}_h$: the transcript of communication between $\mathcal{U}$ and $\mathcal{S}_h$ during the oblivious transfer stage, i.e., $\mathbf{C}_h = (\mathbf{Q}_h, \mathbf{A}_h)$;
- $\bar{\mathbf{Q}}_h$: the query sent to server $\mathcal{S}_h$ by $\bar{\mathcal{U}}$ during the oblivious transfer stage;
- $\bar{\mathbf{A}}_h$: the answer sent to $\mathcal{U}$ by $\bar{\mathcal{S}}_h$ or sent to $\bar{\mathcal{U}}$ by $\mathcal{S}_h$ during the oblivious transfer stage;
- $\bar{\mathbf{C}}_h$: the transcript of communication between $(\bar{\mathcal{S}}_h, \mathcal{U})$ or $(\mathcal{S}_h, \bar{\mathcal{U}})$ during the oblivious transfer stage, i.e., $\bar{\mathbf{C}}_h = (\bar{\mathbf{Q}}_h, \bar{\mathbf{A}}_h)$.

Let $\mathbf{U}_j$ be a random variable for every $j \in \mathbb{N}$. For any $J \subseteq \mathbb{N}$, we denote by $\mathbf{U}_J = (\mathbf{U}_j\colon\ j \in J)$ the sequence of random variables $\mathbf{U}_j$ indexed by $j \in J$. Let $H(\mathbf{U}) = -\sum_u \Pr[\mathbf{U} = u] \log \Pr[\mathbf{U} = u]$ be the *binary entropy* of $\mathbf{U}$. Let $\mathbf{U}'$ be a random variable. We denote by $\Pr[\mathbf{U} = u \mid u']$ the *conditional probability* that $\mathbf{U} = u$ given that $\mathbf{U}' = u'$.

Assumptions: As in [34,8], our formal definitions and security proofs are based on the following assumptions (1)–(8):

- The random input of $\mathcal{U}$ is truly random and independent of the inputs of $\mathcal{D}$, i.e., it holds that:
$$H(\mathbf{Y} \mid \mathbf{W}, \mathbf{X}) = H(\mathbf{Y}); \tag{1}$$
- The random input of $\mathcal{D}$ is truly random and independent of the inputs of $\mathcal{U}$, i.e., it holds that:
$$H(\mathbf{X} \mid \mathbf{I}, \mathbf{Y}) = H(\mathbf{X}); \tag{2}$$
- The private input of $\mathcal{U}$ is independent of any other data in the setup stage, i.e., it holds that:
$$H(\mathbf{I}) = H(\mathbf{I} \mid \mathbf{W}, \mathbf{X}, \mathbf{D}_{[\ell]}, \mathbf{Y}); \tag{3}$$
- Every index $i \in [n]$ will be the choice of $\mathcal{U}$ with positive probability, i.e., it holds that:
$$\Pr[\mathbf{I} = i] > 0 \quad \text{for every } i \in [n]; \tag{4}$$
- The secrets are all totally independent of each other, i.e., for every $K, K' \subseteq [n]$ such that $K \cap K' = \emptyset$:
$$H(\mathbf{W}_{K'} \mid \mathbf{W}_K) = H(\mathbf{W}_{K'})^3; \tag{5}$$
- For every $K \subseteq [\ell]$, the messages sent to $\mathcal{S}_K = \{\mathcal{S}_h\colon\ h \in K\}$ are determined by the inputs of $\mathcal{D}$:
$$H(\mathbf{D}_K \mid \mathbf{W}, \mathbf{X}) = 0; \tag{6}$$
- For every $K \subseteq [\ell]$, the queries sent to $\mathcal{S}_K$ are determined by the inputs of $\mathcal{U}$:
$$H(\mathbf{Q}_K \mid \mathbf{I}, \mathbf{Y}) = 0; \tag{7}$$

[3] The sender's n secrets are assumed to be *implication-free* in Section 4.1 of [8], i.e., $H(\mathbf{W}_i \mid \mathbf{W}_j) > 0$ whenever $i \neq j$. However, it is pointed out in Section 4.1 of [8] that the secrets are usually independent.

– For every $K \subseteq [\ell]$, the answers of $\mathcal{S}_K$ are determined by the queries and messages it received:

$$H(\mathbf{A}_K \mid \mathbf{Q}_K, \mathbf{D}_K) = 0.^4 \tag{8}$$

Correctness: The protocol $\mathcal{P}$ is said to be *correct* if for every $i \in [n]$ and $K \subseteq [\ell]$ such that $|K| = k$,

$$H(\mathbf{W}_i \mid \mathbf{I} = i, \mathbf{Y}, \mathbf{C}_K) = 0. \tag{9}$$

Privacy: The protocol $\mathcal{P}$ is said to be (t, τ)-*private* if the following requirements are satisfied:

– Receiver's privacy: For every $T \subseteq [\ell]$ such that $|T| \leqslant t$ and corrupted servers $\bar{\mathcal{S}}_T$,

$$H(\mathbf{I} \mid \mathbf{D}_T, \mathbf{Q}_T) = H(\mathbf{I}); \tag{10}$$

– Sender's privacy I: For every $T \subseteq [\ell]$ such that $|T| \leqslant \tau$ and corrupted receiver $\bar{\mathcal{U}}$,

$$H(\mathbf{W} \mid \mathbf{I}, \mathbf{Y}, \mathbf{D}_T) = H(\mathbf{W}); \tag{11}$$

– Sender's privacy II: For every $K, T \subseteq [\ell]$ such that $|K| = k$, $|T| \leqslant \tau$, index i, random input Y and $\bar{\mathcal{U}}$,

$$H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \bar{\mathbf{C}}_K, \mathbf{D}_T, \mathbf{W}_i) = H(\mathbf{W} \mid \mathbf{W}_i).^5 \tag{12}$$

2.3. Related information equalities

In this section, we shall prove several information equalities on the random variables defined in Section 2.2. These equalities capture the essence of our definition of privacy and simplify the security proofs.

The first equality (see Lemma 1) shows that a set of corrupted servers can learn information on what the receiver is interested in only from the queries they may obtain from the receiver. Intuitively, this is true because the messages the corrupted servers may obtain are from either the sender or the receiver. However, the messages from the sender convey no information on what the receiver is interested in.

Lemma 1. *In a one-round (k, ℓ)-DOT-$\binom{n}{1}$ protocol, for every $T \subseteq [\ell]$, it holds that*

$$H(\mathbf{I} \mid \mathbf{D}_T, \mathbf{Q}_T) = H(\mathbf{I} \mid \mathbf{Q}_T). \tag{13}$$

Proof. Since $H(\mathbf{I} \mid \mathbf{Q}_T) - H(\mathbf{I} \mid \mathbf{D}_T, \mathbf{Q}_T) = H(\mathbf{D}_T \mid \mathbf{Q}_T) - H(\mathbf{D}_T \mid \mathbf{Q}_T, \mathbf{I})$, it is equivalent to show that $H(\mathbf{D}_T \mid \mathbf{Q}_T) = H(\mathbf{D}_T \mid \mathbf{Q}_T, \mathbf{I})$. Due to (7), we have $H(\mathbf{Q}_T \mid \mathbf{I}, \mathbf{Y}) = 0$ and therefore $H(\mathbf{D}_T) \geqslant H(\mathbf{D}_T \mid \mathbf{Q}_T) \geqslant H(\mathbf{D}_T \mid \mathbf{Q}_T, \mathbf{I}) \geqslant H(\mathbf{D}_T \mid \mathbf{Y}, \mathbf{I})$. Hence, it suffices to show that $H(\mathbf{D}_T) = H(\mathbf{D}_T \mid \mathbf{Y}, \mathbf{I})$. Due to (3), we have that $H(\mathbf{D}_T \mid \mathbf{Y}) - H(\mathbf{D}_T \mid \mathbf{Y}, \mathbf{I}) = H(\mathbf{I} \mid \mathbf{Y}) - H(\mathbf{I} \mid \mathbf{Y}, \mathbf{D}_T) = 0$ and therefore $H(\mathbf{D}_T \mid \mathbf{Y}, \mathbf{I}) = H(\mathbf{D}_T \mid \mathbf{Y})$. Hence, we turn to show that $H(\mathbf{D}_T) = H(\mathbf{D}_T \mid \mathbf{Y})$. Due to (6) and (1), we have that $H(\mathbf{Y}) \geqslant H(\mathbf{Y} \mid \mathbf{D}_T) \geqslant H(\mathbf{Y} \mid \mathbf{W}, \mathbf{X}) = H(\mathbf{Y})$, which implies $H(\mathbf{D}_T) - H(\mathbf{D}_T \mid \mathbf{Y}) = H(\mathbf{Y}) - H(\mathbf{Y} \mid \mathbf{D}_T) = 0$ and completes the proof. □

The second equality (see Lemma 2) shows that before the oblivious transfer stage any coalition of the receiver and a set of corrupted servers can learn information on the secrets of the sender only from what the corrupted servers may obtain from the sender during the setup stage. Intuitively, this is true because the input and random input of the receiver convey no information on the sender's secrets.

Lemma 2. *In a one-round (k, ℓ)-DOT-$\binom{n}{1}$ protocol, for every $T \subseteq [\ell]$, it holds that*

$$H(\mathbf{W} \mid \mathbf{I}, \mathbf{Y}, \mathbf{D}_T) = H(\mathbf{W} \mid \mathbf{D}_T). \tag{14}$$

Proof. Due to (3), we have $H(\mathbf{W} \mid \mathbf{Y}, \mathbf{D}_T) - H(\mathbf{W} \mid \mathbf{I}, \mathbf{Y}, \mathbf{D}_T) = H(\mathbf{I} \mid \mathbf{Y}, \mathbf{D}_T) - H(\mathbf{I} \mid \mathbf{W}, \mathbf{Y}, \mathbf{D}_T) = 0$. Therefore, $H(\mathbf{W} \mid \mathbf{I}, \mathbf{Y}, \mathbf{D}_T) = H(\mathbf{W} \mid \mathbf{Y}, \mathbf{D}_T)$. It suffices to show $H(\mathbf{W} \mid \mathbf{Y}, \mathbf{D}_T) = H(\mathbf{W} \mid \mathbf{D}_T)$. Since $H(\mathbf{W} \mid \mathbf{D}_T) - H(\mathbf{W} \mid \mathbf{Y}, \mathbf{D}_T) = H(\mathbf{Y} \mid \mathbf{D}_T) - H(\mathbf{Y} \mid \mathbf{D}_T, \mathbf{W})$, we

[4] Following Section 2.2 of [8], we suppose that for every $h \in [\ell]$ the message $\mathbf{D}_h$ contains the random bits needed by $\mathcal{S}_h$ in an execution of the protocol and, without loss of generality, the server $\mathcal{S}_h$ is deterministic.

[5] We are analyzing *unconditionally secure* protocols. Therefore, following Section 2.2 of [8], we can suppose that the corrupted receiver is deterministic. For simplicity, we suppose that i is the fixed input *actually contributed* by $\bar{\mathcal{U}}$ and Y is the fixed random input *used* by $\bar{\mathcal{U}}$, respectively. In case i is not in $\{1, 2, \ldots, n\}$, Eq. (12) should be interpreted as $H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \bar{\mathbf{C}}_K, \mathbf{D}_T) = H(\mathbf{W})$, i.e., the receiver $\bar{\mathcal{U}}$ learns nothing.

need to show $H(\mathbf{Y} \mid \mathbf{D}_T) = H(\mathbf{Y} \mid \mathbf{D}_T, \mathbf{W})$. Actually, due to (6) and (1), we have that $H(\mathbf{Y}) \geqslant H(\mathbf{Y} \mid \mathbf{D}_T) \geqslant H(\mathbf{Y} \mid \mathbf{D}_T, \mathbf{W}) \geqslant H(\mathbf{Y} \mid \mathbf{W}, \mathbf{X}) = H(\mathbf{Y})$, which implies the desired equality. □

The last equality (see Lemma 3) shows that given the transcript of the communication between the receiver and the servers labeled by a k-subset $K \subseteq [\ell]$, any coalition of the receiver and a set of corrupted servers labeled by $T \subseteq [\ell]$ can learn more information on the sender's secrets only from the messages that $\mathcal{S}_T$ may obtain from the sender and the answers that the receiver may obtain from the servers $\mathcal{S}_{K \setminus T}$. Intuitively, this is true because the servers are assumed to be deterministic and the answers of the servers $\mathcal{S}_{K \cap T}$ could have been computed by themselves using the messages from both the sender and the receiver.

Lemma 3. *In a one-round (k, ℓ)-DOT-$\binom{n}{1}$ protocol, for every $i \in [n]$, Y and $K, T \subseteq [\ell]$ such that $|K| = k$, it holds that*

$$\begin{aligned} &H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{C}_K, \mathbf{D}_T, \mathbf{W}_i) = H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K \setminus T}, \mathbf{D}_T), \\ &H(\mathbf{W}_i \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K \setminus T}, \mathbf{D}_T) = 0. \end{aligned} \tag{15}$$

Proof. Due to (9) and (8), we have that $H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{C}_K, \mathbf{D}_T, \mathbf{W}_i) = H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{C}_K, \mathbf{D}_T)$ and $H(\mathbf{A}_{K \cap T} \mid \mathbf{Q}_{K \cap T}, \mathbf{D}_{K \cap T}) = 0$. It follows that $H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{C}_K, \mathbf{D}_T) = H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{Q}_{K \setminus T}, \mathbf{Q}_{K \cap T}, \mathbf{A}_{K \setminus T}, \mathbf{A}_{K \cap T}, \mathbf{D}_{T \setminus K}, \mathbf{D}_{K \cap T}) = H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{Q}_K, \mathbf{A}_{K \setminus T}, \mathbf{D}_T)$. Due to (7), we have that $H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{Q}_K, \mathbf{A}_{K \setminus T}, \mathbf{D}_T) = H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K \setminus T}, \mathbf{D}_T)$, which implies the first equality of (15). Similarly, the second equality of (15) holds. □

3. Reducing (k, ℓ)-DOT-$\binom{n}{1}$ to polynomial interpolation-based PIR

In this section, we first develop a framework for polynomial interpolation-based information-theoretic PIR and then present a specific reduction from (k, ℓ)-DOT-$\binom{n}{1}$ to polynomial interpolation-based information-theoretic PIR in the presence of semi-honest receivers.

3.1. PIR based on polynomial interpolation

Let $\mathcal{S}_1, \ldots, \mathcal{S}_k$ be k servers, each of which has a copy of the database $W = W_1, \ldots, W_n$. Let $\mathcal{U}$ be a user who has an index $i \in [n]$ and wants to retrieve W_i from the servers without revealing i. A t-private k-server *polynomial interpolation-based* private information retrieval protocol (see Protocol 1) is an $(n+1)$-tuple $\mathcal{P} = (E; P_1, \ldots, P_n)$, where $E : [n] \to \mathbb{F}_q^m$ is an encoding of the indices and each function $P_j : \mathbb{F}_q^m \to \{0, 1\}$ is an m-variate polynomial of degree at most $d = \lfloor \frac{k-1}{t} \rfloor$ such that $P_j(E(a)) = \delta_{j,a}$ for all $j, a \in [n]$, where $\mathbb{F}_q$ is the finite field of order $q > k$ and $\delta_{j,a}$ is equal to 1 if $j = a$ and 0 otherwise. Each server $\mathcal{S}_h$ encodes W as an m-variate polynomial $P(Z_1, \ldots, Z_m) = \sum_{j=1}^{n} W_j \cdot P_j(Z_1, \ldots, Z_m)$ of degree at most d and is associated with a field element λ_h, where $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q \setminus \{0\}$ are distinct. To retrieve W_i, the user $\mathcal{U}$ picks t random vectors $V_1, \ldots, V_t \in \mathbb{F}_q^m$ and sends to each server $\mathcal{S}_h$ a query $Q_h = E(i) + \lambda_h V_1 + \cdots + (\lambda_h)^t V_t$. The server $\mathcal{S}_h$ replies with $A_h = P(Q_h)$. At last, $\mathcal{U}$ interpolates the univariate polynomial $G(\lambda) = P(E(i) + \lambda V_1 + \cdots + \lambda^t V_t)$ of degree at most $k - 1$ and outputs $G(0) = P(E(i)) = W_i$. The polynomial interpolation-based PIR protocols of [5,38] are summarized in Appendix A.

Protocol 1. Polynomial interpolation-based PIR

Input of $\mathcal{S}_h$: the database $W = W_1, \ldots, W_n \in \mathbb{F}_q^n$.
Input of $\mathcal{U}$: the index $i \in [n]$.
$\mathcal{U}$: choose $V_1, \ldots, V_t \in \mathbb{F}_q^m$ uniformly and send $Q_h = E(i) + \lambda_h V_1 + \cdots + (\lambda_h)^t V_t$ to $\mathcal{S}_h$ for every $h \in [k]$;
$\mathcal{S}_h$: send $P(Q_h)$ to $\mathcal{U}$, where $P(Z_1, \ldots, Z_m) = \sum_{j=1}^{n} W_j \cdot P_j(Z_1, \ldots, Z_m)$;
$\mathcal{U}$: interpolate $G(\lambda) = P(E(i) + \lambda V_1 + \cdots + \lambda^t V_t)$ and output $G(0)$.

3.2. Reduction in the presence of semi-honest receivers

Let $\mathcal{P} = (E; P_1, \ldots, P_n)$ be a t-private $(k - \tau)$-server polynomial interpolation-based PIR protocol. Protocol 2, described below, converts $\mathcal{P}$ to a (t, τ)-private (k, ℓ)-DOT-$\binom{n}{1}$ protocol. During the setup stage, the sender $\mathcal{D}$ shares the secrets using *Shamir's τ-private threshold sharing scheme* (TSSS) with every k-subset of the ℓ servers. During the oblivious transfer stage, the receiver $\mathcal{U}$ invokes $\mathcal{P}$ with k out of the ℓ servers.

Protocol 2. (k,ℓ)-DOT-$\binom{n}{1}$ BASED ON POLYNOMIAL INTERPOLATION-BASED PIR

INPUT of $\mathcal{D}$: n secrets $W = W_1, \ldots, W_n \in \mathbb{F}_q^n$.
INPUT of $\mathcal{U}$: an index $i \in [n]$.
SETUP STAGE
$\mathcal{D}$: choose polynomials $B_0(\lambda) = \sum_{a=0}^{k-1} B_{0,a}\lambda^a \in \mathbb{F}_q[\lambda]$ and $B_j(\lambda) = \sum_{a=0}^{\tau} B_{j,a}\lambda^a \in \mathbb{F}_q[\lambda]$ uniformly such that $B_0(0) + B_j(0) = W_j$ for every $j \in [n]$;
$\mathcal{D}$: define $F(\lambda, Z_1, \ldots, Z_m) = B_0(\lambda) + \sum_{j=1}^{n} B_j(\lambda) \cdot P_j(Z_1, \ldots, Z_m)$;
$\mathcal{D}$: for any k-subset $K \subseteq [\ell]$, choose $(X_{K,h}\colon h \in K) \in \mathbb{F}_q^k$ uniformly such that $\sum_{h\in K} X_{K,h} = 0$;
$\mathcal{D}$: send $\{\{X_{K,h}\colon h \in K \subseteq [\ell] \text{ and } |K| = k\}, F(\lambda_h, Z_1, \ldots, Z_m)\}$ to $\mathcal{S}_h$ for every $h \in [\ell]$.
OBLIVIOUS TRANSFER STAGE
$\mathcal{U}$: choose k servers, say $\mathcal{S}_K = \{\mathcal{S}_h\colon h \in K\}$, where $K \subseteq [\ell]$ and $|K| = k$;
$\mathcal{U}$: choose $V_1, \ldots, V_t \in \mathbb{F}_q^m$ uniformly and send K, $Q_h = E(i) + \sum_{a=1}^{t} (\lambda_h)^a V_a$ to $\mathcal{S}_h$ for every $h \in K$;
$\mathcal{S}_h$: send $A_h = F(\lambda_h, Q_h) \prod_{j\in K\setminus\{h\}} \frac{-\lambda_j}{\lambda_h - \lambda_j} + X_{K,h}$ to $\mathcal{U}$, where $h \in K$;
$\mathcal{U}$: output $\sum_{h\in K} A_h$.

Lemma 4. *Protocol* 2 *satisfies the correctness requirement.*

Proof. The univariate polynomial $G(\lambda) = F(\lambda, E(i) + \lambda V_1 + \cdots + \lambda^t V_t)$ is of degree at most $\max\{k-1, \tau + dt\} \leqslant k-1$. Due to Lagrange polynomial interpolation, we have that

$$\sum_{h\in K} A_h = \sum_{h\in K} \left[F\big(\lambda_h, E(i) + \lambda_h V_1 + \cdots + (\lambda_h)^t V_t\big) \prod_{j\in K\setminus\{h\}} \frac{-\lambda_j}{\lambda_h - \lambda_j} \right] = G(0) = W_i.$$

Hence, the receiver is able to determine the value of W_i by interacting with k servers. □

Referring to Protocol 2, let $\mathcal{K}$ be the collection of all k-subsets of $[\ell]$. For every $K \in \mathcal{K}$ and $h \in K$, we denote by $\mathbf{X}_{K,h}$ the random variable representing $X_{K,h}$. For every $h \in [\ell]$ and $j \in \{0, 1, \ldots, n\}$, we denote by $\mathbf{B}_j(\lambda_h)$ the random variable representing $B_j(\lambda_h)$. Let

$$\mathbf{X}_{k,h} = (\mathbf{X}_{K,h}\colon h \in K \in \mathcal{K}), \qquad \mathbf{X}_{B,h} = \big(\mathbf{B}_0(\lambda_h), \ldots, \mathbf{B}_n(\lambda_h)\big), \qquad \mathbf{F}_h = \mathbf{B}_0(\lambda_h) + \sum_{j=1}^{n} \mathbf{B}_j(\lambda_h) P_j(Z_1, \ldots, Z_m). \tag{16}$$

Then the random variable representing the messages sent to $\mathcal{S}_h$ by $\mathcal{D}$ is

$$\mathbf{D}_h = (\mathbf{X}_{k,h}, \mathbf{F}_h). \tag{17}$$

For every $h \in [\ell]$, let $\mathbf{Q}_h$ be the random variable representing the query Q_h sent to $\mathcal{S}_h$ by $\mathcal{U}$. Then we have that

$$\mathbf{A}_h = \prod_{j\in K\setminus\{h\}} \frac{-\lambda_j}{\lambda_h - \lambda_j} \left[\mathbf{B}_0(\lambda_h) + \sum_{j=1}^{n} \mathbf{B}_j(\lambda_h) P_j(\mathbf{Q}_h) \right] + \mathbf{X}_{K,h} \tag{18}$$

is the random variable representing the answer of $\mathcal{S}_h$ on receiver's query $\mathbf{Q}_h$ and sender's message $\mathbf{D}_h$. For every $h \in [\ell]$, we define

$$\mathbf{D}_h^* = (\mathbf{X}_{k,h}, \mathbf{X}_{B,h}). \tag{19}$$

Let $\mathcal{T}$ be the collection of all τ-subsets of $[\ell]$. Following the notations in Section 2.2, for any $T \in \mathcal{T}$, the definitions of the random variables $\mathbf{X}_{k,T}$, $\mathbf{X}_{B,T}$, $\mathbf{F}_T$, $\mathbf{D}_T$, $\mathbf{A}_T$ and $\mathbf{D}_T^*$ are straightforward. It is not hard to see that $\mathbf{D}_T$ is a function of $\mathbf{D}_T^*$ and therefore $H(\mathbf{D}_T \mid \mathbf{D}_T^*) = 0$.

Let $\mathbf{B} = (\mathbf{B}_{0,0}, \ldots, \mathbf{B}_{n,\tau})$ be a random vector describing the coefficient vector $B = (B_{0,0}, \ldots, B_{n,\tau})$ of the random polynomials $B_0(\lambda), \ldots, B_n(\lambda)$. For a specific τ-subset $T = \{1, 2, \ldots, \tau\} \in \mathcal{T}$, we define

$$\Lambda' = \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{k-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{k-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda_\tau & \cdots & \lambda_\tau^{k-1} \end{bmatrix}, \qquad \Lambda'' = \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{\tau} \\ 1 & \lambda_2 & \cdots & \lambda_2^{\tau} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda_\tau & \cdots & \lambda_\tau^{\tau} \end{bmatrix}$$

and $\Lambda = \operatorname{diag}(\Lambda', \Lambda'', \ldots, \Lambda'')$, where Λ'' occurs exactly n times.

Lemma 5. *Protocol* 2 *satisfies the receiver's privacy requirement.*

Proof. Let $\mathcal{S}_T = \{\mathcal{S}_h\colon h \in T\}$ be any coalition of t servers, where T is a t-subset of $[\ell]$. We show that the receiver's index is protected, that is a coalition of t servers do not learn any information about the index. We need to show that $H(\mathbf{I} \mid \mathbf{D}_T, \mathbf{Q}_T) = H(\mathbf{I})$. Due to Lemma 1, it suffices to show that $H(\mathbf{I} \mid \mathbf{Q}_T) = H(\mathbf{I})$. For every $i \in [n]$ and $Q_T = (Q_h\colon h \in T) \in (\mathbb{F}_q^m)^t$, we have that $\Pr[\mathbf{Q}_T = Q_T \mid \mathbf{I} = i] = 1/q^{mt}$ due to the privacy of Shamir's t-private TSSS. It follows that $\mathbf{I}$ and $\mathbf{Q}_T$ are independent. Hence, $H(\mathbf{I} \mid \mathbf{Q}_T) = H(\mathbf{I})$. □

The following lemma shows any coalition of τ servers and the user has no information about the secrets after the setup stage.

Lemma 6. *Protocol* 2 *satisfies the sender's privacy I requirement.*

Proof. Let $\mathcal{S}_T$ be a set of servers colluding with $\mathcal{U}$, where $T \in \mathcal{T}$ is arbitrary. For simplicity, we suppose that $T = \{1, 2, \ldots, \tau\}$. Due to Lemma 2, it suffices to show $H(\mathbf{W} \mid \mathbf{D}_T) = H(\mathbf{W})$. It is obvious that

$$H\bigl(\mathbf{W} \bigm| \mathbf{D}_T^*\bigr) = H\bigl(\mathbf{W} \bigm| \mathbf{D}_T, \mathbf{D}_T^*\bigr) \leqslant H(\mathbf{W} \mid \mathbf{D}_T) \leqslant H(\mathbf{W}).$$

On the other hand, we have that $H(\mathbf{W} \mid \mathbf{X}_{B,T}) - H(\mathbf{W} \mid \mathbf{D}_T^*) = H(\mathbf{X}_{k,T} \mid \mathbf{X}_{B,T}) - H(\mathbf{X}_{k,T} \mid \mathbf{X}_{B,T}, \mathbf{W}) = 0$ in Protocol 2. Hence, $H(\mathbf{W} \mid \mathbf{X}_{B,T}) = H(\mathbf{W} \mid \mathbf{D}_T^*)$. We turn to show that $H(\mathbf{W} \mid \mathbf{X}_{B,T}) = H(\mathbf{W})$.

Let $W \in \mathbb{F}_q^n$ and $X_{B,T} = (B_0(\lambda_1), \ldots, B_n(\lambda_\tau)) \in \mathbb{F}_q^{(n+1)\tau}$ be arbitrary. For every $j \in [n]$, let $\rho^j = (1, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{F}_q^{k+n(\tau+1)}$ be a vector with nonzero entries $\rho_1^j = 1$ and $\rho_{k+(j-1)\tau+1}^j = 1$. We calculate the number of coefficient vectors B of the random polynomials $B_0(\lambda), \ldots, B_n(\lambda)$, which are chosen randomly by $\mathcal{D}$ in Protocol 2 and satisfy the following two linear equation systems

$$\text{(I)}\quad \Lambda \cdot B = \begin{bmatrix} B_0(\lambda_1) \\ \vdots \\ B_n(\lambda_\tau) \end{bmatrix} \quad \text{and} \quad \text{(II)}\quad \boldsymbol{\rho} \cdot B = \begin{bmatrix} \rho^1 \\ \vdots \\ \rho^n \end{bmatrix} \cdot B = \begin{bmatrix} W_1 \\ \vdots \\ W_n \end{bmatrix} \tag{20}$$

simultaneously. Clearly, the linear equations given by (I) and (II) ensure that $\mathbf{X}_{B,T} = X_{B,T}$ and $\mathbf{W} = W$, respectively. It is clear that the matrix $\left[\begin{smallmatrix} \Lambda \\ \boldsymbol{\rho} \end{smallmatrix}\right]$ is of full rank $(n+1)\tau + n$ and therefore (20) has exactly $q^{k-\tau}$ solutions. On the other hand, $\boldsymbol{\rho}$ is of full rank n and (II) have exactly $q^{k+n\tau}$ solutions. It follows that

$$\Pr[\mathbf{X}_{B,T} = X_{B,T} \mid \mathbf{W} = W] = \frac{\text{the number of solutions of (20)}}{\text{the number of solutions of (II)}} = \frac{1}{q^{(n+1)\tau}},$$

i.e., $\mathbf{X}_{B,T} \mid W$ is uniformly distributed in its domain $\mathbb{F}_q^{(n+1)\tau}$, which implies that $\mathbf{W}$ and $\mathbf{X}_{B,T}$ are independent. Hence, $H(\mathbf{W} \mid \mathbf{X}_{B,T}) = H(\mathbf{W})$. □

Finally, we prove privacy after the oblivious transfer stage.

Lemma 7. *Protocol* 2 *satisfies the sender's privacy II requirement.*

Proof. Let $i \in [n]$, $K \in \mathcal{K}$ and $T \in \mathcal{T}$ be arbitrary. For simplicity, we suppose $T = \{1, 2, \ldots, \tau\}$. Let $Y = (V_a\colon a \in [t]) \in (\mathbb{F}_q^m)^t$ be the random vectors chosen by $\mathcal{U}$. Due to Lemma 3, it suffices to show that

$$H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T) = H(\mathbf{W} \mid \mathbf{W}_i).$$

Let $\Gamma = [n] \setminus \{i\}$. We have that $H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T) = H(\mathbf{W}_\Gamma \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T)$ due to Eq. (15) and $H(\mathbf{W} \mid \mathbf{W}_i) = H(\mathbf{W}_\Gamma)$ due to Eq. (5). Thus, it is sufficient to show that

$$H(\mathbf{W}_\Gamma \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T) = H(\mathbf{W}_\Gamma).$$

Since $H(\mathbf{D}_T \mid \mathbf{D}_T^*) = 0$, we have that $H(\mathbf{W}_\Gamma) \geqslant H(\mathbf{W}_\Gamma \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T) \geqslant H(\mathbf{W}_\Gamma \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T^*)$. Hence, it is enough to show that

$$H\bigl(\mathbf{W}_\Gamma \bigm| \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T^*\bigr) = H(\mathbf{W}_\Gamma).$$

Let $W_\Gamma \in \mathbb{F}_q^{n-1}$ and $(A_{K\setminus T}, D_T^*)$ be such that $\Pr[\mathbf{W}_\Gamma = W_\Gamma] > 0$ and $\Pr[\mathbf{A}_{K\setminus T} = A_{K\setminus T}, \mathbf{D}_T^* = D_T^* \mid \mathbf{W}_\Gamma = W_\Gamma, \mathbf{I} = i, \mathbf{Y} = Y] > 0$. We want to compute the conditional probability of $(A_{K\setminus T}, D_T^*)$ when $\mathcal{D}$'s secrets indexed by Γ are W_Γ and $\mathcal{U}$'s index and random input are i and Y, respectively. In other words, we want to compute

$$p_1 = \Pr\bigl[\mathbf{A}_{K\setminus T} = A_{K\setminus T}, \mathbf{D}_T^* = D_T^* \bigm| \mathbf{W}_\Gamma = W_\Gamma, \mathbf{I} = i, \mathbf{Y} = Y\bigr]. \tag{21}$$

Note that $D_T^* = (X_{k,T}, X_{B,T})$, where $X_{k,T}$ and $X_{B,T}$ are in the domains of $\mathbf{X}_{k,T}$ and $\mathbf{X}_{B,T}$, respectively. Clearly, $\mathbf{X}_{k,T}$ is independent of $\mathbf{W}_\Gamma$ for fixed i and Y in Protocol 2. For every $h \in T$ and $K \in \mathcal{K}$ such that $h \in K$, the server $\mathcal{S}_h$ receives a random field element $X_{K,h}$. It follows that $\mathcal{S}_h$ receives exactly $\binom{\ell-1}{k-1}$ random field elements in an execution of Protocol 2, i.e., the message $X_{k,h}$ received by $\mathcal{S}_h$ contains exactly $\binom{\ell-1}{k-1}$ random field elements. Therefore, the messages $X_{k,T}$ received by servers $\mathcal{S}_T$ contain exactly $\tau\binom{\ell-1}{k-1}$ random field elements. Hence, we have that

$$\Pr[\mathbf{X}_{k,T} = X_{k,T} \mid W_\Gamma, i, Y] = \frac{1}{q^{\tau\binom{\ell-1}{k-1}}}. \tag{22}$$

Due to Eq. (15), we have that $H(\mathbf{W}_i \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T^*) \leqslant H(\mathbf{W}_i \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T) = 0$. Therefore, the data $(A_{K\setminus T}, D_T^*)$ uniquely determines a secret $W_i \in \mathbb{F}_q$ for fixed i and Y. Due to Eq. (5) and the choice of $X_{k,T}$ in Protocol 2, we have that $\mathbf{W}_i$ is independent of $(\mathbf{X}_{k,T}, \mathbf{W}_\Gamma)$ for fixed i and Y. Hence,

$$\Pr[\mathbf{W}_i = W_i \mid X_{k,T}, W_\Gamma, i, Y] = \Pr[\mathbf{W}_i = W_i]. \tag{23}$$

The choice of $X_{B,T}$ in Protocol 2 should be consistent with the value of W and independent of any other data. Therefore, as in the proof of Lemma 6, we have that

$$\Pr[\mathbf{X}_{B,T} = X_{B,T} \mid W_i, X_{k,T}, W_\Gamma, i, Y] = \Pr[\mathbf{X}_{B,T} = X_{B,T} \mid W_i, W_\Gamma] = \frac{1}{q^{(n+1)\tau}}. \tag{24}$$

Due to Eqs. (7), (16) and (18), the tuple $(X_{B,T}, W_i, X_{k,T}, W_\Gamma, i, Y)$ uniquely determines A_T. Clearly, any valid answers $A_{K\setminus T}$ replied by servers $\mathcal{S}_{K\setminus T}$ should satisfy $\sum_{h\in K\setminus T} A_h + \sum_{h\in T} A_h = W_i$. Therefore, the domain of $\mathbf{A}_{K\setminus T}$ is equal to $\mathbb{A}_{K\setminus T} = \{(a_1, \ldots, a_{|K\setminus T|})\colon \sum_{h=1}^{|K\setminus T|} a_h = W_i - \sum_{h\in T} A_h\}$. Furthermore, it is clear that $\mathbf{A}_{K\setminus T}$ is uniformly distributed on $\mathbb{A}_{K\setminus T}$ (see step 3 in the oblivious transfer stage of Protocol 2). Hence,

$$\Pr[\mathbf{A}_{K\setminus T} = A_{K\setminus T} \mid X_{B,T}, W_i, X_{k,T}, W_\Gamma, i, Y] = \frac{1}{|\mathbb{A}_{K\setminus T}|} = \frac{1}{q^{|K\setminus T|-1}}. \tag{25}$$

Due to Eq. (21), p_1 is equal to the product of the left-hand sides of Eqs. (22), (23), (24) and (25). Hence, we have that

$$p_1 = \frac{1}{q^{\tau\binom{\ell-1}{k-1}}} \cdot \Pr[\mathbf{W}_i = W_i] \cdot \frac{1}{q^{(n+1)\tau}} \cdot \frac{1}{q^{|K\setminus T|-1}},$$

which implies that $(\mathbf{A}_{K\setminus T}, \mathbf{D}_T^*)$ and $\mathbf{W}_\Gamma$ are independent as long as i and Y are fixed. It follows that $H(\mathbf{W}_\Gamma \mid \mathbf{I} = i, \mathbf{Y} = Y, \mathbf{A}_{K\setminus T}, \mathbf{D}_T^*) = H(\mathbf{W}_\Gamma)$. □

Communication complexity. The receiver sends to each server $\mathcal{S}_h$ a vector $Q_h \in \mathbb{F}_q^m$ and a subset $K \in \mathcal{K}$ as its query and receives an answer $A_h \in \mathbb{F}_q$ in return. Therefore, the communication complexity between the receiver and servers is $\gamma(n) = k(m+1)\log q + \log\binom{\ell}{k}$. The polynomial interpolation-based PIR protocols enumerated in Appendix A require $m = O(n^{1/\lfloor\frac{k-\tau-1}{t}\rfloor})$. Hence, we have that:

Theorem 1. *Let t, τ, k, ℓ be positive integers such that $\ell \geqslant k \geqslant t + \tau + 1$. Protocol 2 is a (t, τ)-private (k, ℓ)-DOT-$\binom{n}{1}$ protocol of communication complexity $O(n^{1/\lfloor\frac{k-\tau-1}{t}\rfloor})$ between a semi-honest receiver and servers.*

4. Reducing (k, ℓ)-DOT-$\binom{n}{1}$ to any PIR

In this section, we build communication-efficient DOT from any PIR. The privacy of any 1-private PIR protocols can be boosted without increasing the asymptotic communication complexity due to the transformation of [3]. On the other hand, [21] provides a method of converting any PIR to SPIR without increasing the asymptotic communication complexity. Eventually, the reduction from DOT to SPIR (see Protocol 3) enables us to build DOT from any PIR.

Replication-based threshold secret sharing scheme. A τ-private k-participant replication-based threshold secret sharing scheme $\mathrm{CNF}_{\tau,k}$ (based on [27]) involves a dealer $\mathcal{D}$ who has a secret $g \in \mathbb{G}$ and k participants $\mathcal{S}_1, \ldots, \mathcal{S}_k$, where $\mathbb{G}$ is an abelian group. The scheme proceeds as follows: (I) The dealer $\mathcal{D}$ chooses $\binom{k}{\tau}$ random group elements, each of which is indexed by a τ-subset of $[k]$, say $\{g_T\colon T \subseteq [k],\ |T| = \tau\}$, such that $\sum_T g_T = g$; (II) The dealer $\mathcal{D}$ sends $\{g_T\colon h \notin T\}$ to $\mathcal{S}_h$ for every $h \in [k]$. The τ-privacy of $\mathrm{CNF}_{\tau,k}$ follows from the fact that any τ participants $\mathcal{S}_T$ do not know the share g_T.

Reduction from (k,ℓ)*-DOT-*$\binom{n}{1}$ *to SPIR.* Let t, τ, k, ℓ be positive integers such that $t+\tau<k\leqslant\ell$. We reduce (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ to any t-private $(k-\tau)$-server SPIR by the following Protocol 3. During the setup stage, the sender $\mathcal{D}$ distributes the secrets W among each k-subset of servers $\mathcal{S}_K$ using $\mathrm{CNF}_{\tau,k}$. During the oblivious transfer stage, the receiver $\mathcal{U}$ interacts with k out of the ℓ servers. Specifically, $\mathcal{U}$ invokes an instance of the SPIR with each subset of $k-\tau$ servers $\mathcal{S}_{K\setminus T}$, where $T\subseteq K$ and $|T|=\tau$. The receiver $\mathcal{U}$ receives $k-\tau$ answers from $\mathcal{S}_{K\setminus T}$ which reveal $[W_{K,T}]_i$, the i-th data item of $W_{K,T}$.

Protocol 3. (k,ℓ)-DOT-$\binom{n}{1}$ BASED ON SPIR

```
INPUT of $\mathcal{D}$: $n$ secrets $W = W_1,\dots,W_n \in \mathbb{F}_q^n$.
INPUT of $\mathcal{U}$: an index $i \in [n]$.
PROCEDURE: $\mathcal{P} = (\mathcal{Q},\mathcal{A},\mathcal{R})$, a $t$-private $(k-\tau)$-server SPIR protocol.
SETUP STAGE
$\mathcal{D}$: for every $K \in \mathcal{K}$, $T \in \mathcal{T}$ such that $T \subseteq K$, choose $W_{K,T} \in \mathbb{F}_q^n$ uniformly such that $\sum_T W_{K,T} = W$;
$\mathcal{D}$: send $D_h = \{W_{K,T}\colon\ K \in \mathcal{K},\ T \in \mathcal{T},\ T \subseteq K,\ h \in K \setminus T\}$ to each server $\mathcal{S}_h$;
$\mathcal{D}$: generate a random string $X = \{X_{K,T}\colon\ K \in \mathcal{K},\ T \in \mathcal{T},\ T \subseteq K\}$ and send $X$ to each $\mathcal{S}_h$.
OBLIVIOUS TRANSFER STAGE
$\mathcal{U}$: choose a $K \in \mathcal{K}$ and a random input $Y_K = \{Y_{K,T}\colon\ T \in \mathcal{T},\ T \subseteq K\}$;
$\mathcal{U}$: for every $T \in \mathcal{T}$, $T \subseteq K$ and $h \in K \setminus T$, send $Q_{K,T,h} = \mathcal{Q}(n,i,Y_{K,T})_h$ to $\mathcal{S}_h$;
$\mathcal{S}_h$: send $A_{K,T,h} = \mathcal{A}(n,W_{K,T},Q_{K,T,h},X_{K,T})$ to $\mathcal{U}$ for every $T \in \mathcal{T}$ such that $T \subseteq K$, $h \in K \setminus T$;
$\mathcal{U}$: for every $T \in \mathcal{T}$, $T \subseteq K$, compute $\Phi_{K,T} = \mathcal{R}(i,Y_{K,T},\{Q_{K,T,h},A_{K,T,h}\colon\ h \in K \setminus T\})$;
$\mathcal{U}$: output $\sum_{T\colon\ T \in \mathcal{T}, T \subseteq K} \Phi_{K,T}$.
```

Let $K\in\mathcal{K}$, $T\in\mathcal{T}$ be such that $T\subseteq K$. For every $h\in K\setminus T$, we denote by $\mathbf{Q}_{K,T,h}$ the random variable representing the query sent to $\mathcal{S}_h$ by $\mathcal{U}$ when the $\mathcal{P}$ instance between $\mathcal{U}$ and $\mathcal{S}_{K\setminus T}$ is invoked. For any $T'\subseteq[\ell]$, we denote by $\mathbf{Q}_{K,\star,T'}=(\mathbf{Q}_{K,T,T'\cap(K\setminus T)}\colon\ T\in\mathcal{T},\ T\subseteq K)=(\mathbf{Q}_{K,T,h}\colon\ T\in\mathcal{T},\ T\subseteq K,\ h\in T'\cap(K\setminus T))$ the queries received by $\mathcal{S}_{T'}$ during the oblivious transfer stage. For every $h\in K$, let $\mathbf{D}_{K,\star,h}=(\mathbf{W}_{K,T}\colon\ T\in\mathcal{T},\ T\subseteq K,\ h\in K\setminus T)$ be the messages received by $\mathcal{S}_h$ in the $\mathrm{CNF}_{\tau,k}$ instances between $\mathcal{D}$ and $\mathcal{S}_K$. For every $T'\subseteq[\ell]$, let $\mathbf{D}_{K,\star,T'}=(\mathbf{D}_{K,\star,h}\colon\ h\in T'\cap K)$ and $\mathbf{D}_{T'}=(\mathbf{D}_{K,\star,T'}\colon\ K\in\mathcal{K})$.

Lemma 8. *Protocol* 3 *satisfies the correctness requirement.*

Proof. Due to the correctness of $\mathcal{P}$, for every $T\in\mathcal{T}$ such that $T\subseteq K$, it holds that $\Phi_{K,T}=[W_{K,T}]_i$ and therefore

$$\sum_{T\colon\ T\in\mathcal{T},\ T\subseteq K}\Phi_{K,T}=\sum_{T\colon\ T\in\mathcal{T},\ T\subseteq K}[W_{K,T}]_i=\left[\sum_{T\colon\ T\in\mathcal{T},\ T\subseteq K}W_{K,T}\right]_i=W_i.\qquad\square$$

Lemma 9. *Protocol* 3 *satisfies the receiver's privacy requirement.*

Proof. Let $\mathcal{S}_K$ be the set of servers interacted by $\mathcal{U}$ and $T\in\mathcal{T}$ be a subset of K. Due to the user privacy of $\mathcal{P}$, for every t-subset $T'\subseteq[\ell]$, it holds that $H(\mathbf{I}\mid\mathbf{Q}_{K,T,T'\cap(K\setminus T)})=H(\mathbf{I})$. Let $\mathcal{S}_{T'}\subseteq\mathcal{S}_K$ be any coalition of t servers. Due to Lemma 1, it suffices to show that $H(\mathbf{I}\mid\mathbf{Q}_{K,\star,T'})=H(\mathbf{I})$.

Let $i\in[n]$ and $Q_{K,\star,T'}=(Q_{K,T,T'\cap(K\setminus T)}\colon\ T\in\mathcal{T},\ T\subseteq K)$ be arbitrary. Since the instances of $\mathcal{P}$ are totally independent of each other, it holds that

$$\Pr[\mathbf{Q}_{K,\star,T'}=Q_{K,\star,T'}\mid\mathbf{I}=i]=\prod_{T\colon\ T\in\mathcal{T},\ T\subseteq K}\Pr[\mathbf{Q}_{K,T,T'\cap(K\setminus T)}=Q_{K,T,T'\cap(K\setminus T)}\mid\mathbf{I}=i].$$

However, we have that $\Pr[\mathbf{Q}_{K,T,T'\cap(K\setminus T)}=Q_{K,T,T'\cap(K\setminus T)}\mid\mathbf{I}=j]=\Pr[\mathbf{Q}_{K,T,T'\cap(K\setminus T)}=Q_{K,T,T'\cap(K\setminus T)}\mid\mathbf{I}=i]$ for every $j\in[n]$ since $H(\mathbf{I}\mid\mathbf{Q}_{K,T,T'\cap(K\setminus T)})=H(\mathbf{I})$. It follows that $\Pr[\mathbf{Q}_{K,\star,T'}=Q_{K,\star,T'}\mid\mathbf{I}=i]=\Pr[\mathbf{Q}_{K,\star,T'}=Q_{K,\star,T'}\mid\mathbf{I}=j]$, i.e., $\mathbf{Q}_{K,\star,T'}$ and $\mathbf{I}$ are independent. Hence, we have that $H(\mathbf{I}\mid\mathbf{Q}_{K,\star,T'})=H(\mathbf{I})$. $\square$

Lemma 10. *Protocol* 3 *satisfies the sender's privacy I requirement.*

Proof. Let $\mathcal{S}_{T'}$ be τ servers colluding with $\mathcal{U}$, where $T'\in\mathcal{T}$. Due to Lemma 2, it suffices to show that $H(\mathbf{W}\mid\mathbf{D}_{T'})=H(\mathbf{W})$. The sender $\mathcal{D}$ invokes $\binom{\ell}{k}$ instances of $\mathrm{CNF}_{\tau,k}$ which are totally independent of each other. Let $K\in\mathcal{K}$ be arbitrary. If $T'\subseteq K$, then the servers in $\mathcal{S}_{T'}$ do not learn $\mathbf{W}_{K,T'}$. Hence, $H(\mathbf{W}\mid\mathbf{D}_{K,\star,T'})=H(\mathbf{W})$. If $T'\setminus K\neq\emptyset$, then $\mathcal{S}_h$ learns no information on $\{\mathbf{W}_{K,T}\colon\ T\in\mathcal{T},\ T\subseteq K\}$ if $h\in T'\setminus K$ or no information on $\{\mathbf{W}_{K,T}\colon\ T\in\mathcal{T},\ K\cap T'\subseteq T\subseteq K\}$ if $h\in K\cap T'$. Hence, we have that $H(\mathbf{W}\mid\mathbf{D}_{K,\star,T'})=H(\mathbf{W})$.

Let $W \in \mathbb{F}_q^n$ be arbitrary and $D_{T'} = (D_{K,\star,T'}\colon\ K \in \mathcal{K})$ be any message tuple sent to $\mathcal{S}_{T'}$ by $\mathcal{D}$. Since the $\mathrm{CNF}_{\tau,k}$ instance are totally independent of each other, we have that $\Pr[\mathbf{D}_{T'} = D_{T'} \mid \mathbf{W} = W] = \prod_{K \in \mathcal{K}} \Pr[\mathbf{D}_{K,\star,T'} = D_{K,\star,T'} \mid \mathbf{W} = W]$. For every $W' \in \mathbb{F}_q^n$, we have that $\Pr[\mathbf{D}_{K,\star,T'} = D_{K,\star,T'} \mid \mathbf{W} = W] = \Pr[\mathbf{D}_{K,\star,T'} = D_{K,\star,T'} \mid \mathbf{W} = W']$ since $H(\mathbf{W} \mid \mathbf{D}_{K,\star,T'}) = H(\mathbf{W})$. It follows that $\Pr[\mathbf{D}_{T'} = D_{T'} \mid \mathbf{W} = W] = \Pr[\mathbf{D}_{T'} = D_{T'} \mid \mathbf{W} = W']$, i.e., $\mathbf{D}_{T'}$ and $\mathbf{W}$ are independent. Hence, $H(\mathbf{W} \mid \mathbf{D}_{T'}) = H(\mathbf{W})$. □

Lemma 11. *Protocol* 3 *satisfies the sender's privacy II requirement.*

Proof. Let $\mathcal{S}_K$ and $\mathcal{S}_{T'}$ be the servers interacted by $\mathcal{U}$ and colluding with $\mathcal{U}$ respectively, where $K \in \mathcal{K}$ and $T' \in \mathcal{T}$. Let $\mathcal{T}^*$ be the set of all τ-subsets of K, $\mathcal{T}_1^* = \{T \in \mathcal{T}^*\colon\ (T' \cap K) \subseteq T\}$ and $\mathcal{T}_2^* = \{T \in \mathcal{T}^*\colon\ (T' \cap K) \setminus T \neq \emptyset\}$. That is, $\mathcal{T}_2^* = \mathcal{T}^* \setminus \mathcal{T}_1^*$. Furthermore, $\tau' = |T' \cap K| \leqslant \tau$ and $\delta = |\mathcal{T}_1^*| = \binom{k-\tau'}{\tau-\tau'}$. Let $i \in [n]$, $Y_K = (Y_{K,T}\colon\ T \in \mathcal{T}^*)$ and $Q_K = (Q_{K,T,K\setminus T}\colon\ T \in \mathcal{T}^*)$ be the fixed index, random input and query of $\mathcal{U}$, respectively. For every $T \in \mathcal{T}^*$, an instance of $\mathcal{P}$ is invoked between $\mathcal{U}$ and $\mathcal{S}_{K\setminus T}$ with $\mathbf{W}_{K,T}$ as the database. We denote

$$\mathbf{A}_K = \bigl(\mathbf{A}_{K,T,K\setminus T}\colon\ T \in \mathcal{T}^*\bigr); \qquad \mathbf{A}_{K,\mathcal{T}_1^*} = \bigl(\mathbf{A}_{K,T,K\setminus T}\colon\ T \in \mathcal{T}_1^*\bigr); \qquad \mathbf{A}_{K,\mathcal{T}_2^*} = \bigl(\mathbf{A}_{K,T,K\setminus T}\colon\ T \in \mathcal{T}_2^*\bigr).$$

Semi-honest case. For every $T \in \mathcal{T}^*$, consider the instance $\mathcal{P}$ between a semi-honest $\mathcal{U}$ and $\mathcal{S}_{K\setminus T}$. Due to the data privacy of $\mathcal{P}$, it holds that

$$H(\mathbf{W}_{K,T} \mid \mathbf{I} = i, \mathbf{Y}_{K,T} = Y_{K,T}, \mathbf{A}_{K,T,K\setminus T}) = H\bigl(\mathbf{W}_{K,T} \bigm| [\mathbf{W}_{K,T}]_i\bigr). \tag{26}$$

Therefore, for every $W_{K,T}, W'_{K,T} \in \mathbb{F}_q^n$ such that $[W'_{K,T}]_i = [W_{K,T}]_i$ and $A_{K,T} \in \mathbb{F}_q^{k-\tau}$, it holds that

$$\Pr[\mathbf{A}_{K,T} = A_{K,T} \mid W_{K,T}, i, Y_{K,T}] = \Pr\bigl[\mathbf{A}_{K,T} = A_{K,T} \bigm| W'_{K,T}, i, Y_{K,T}\bigr]. \tag{27}$$

Due to (8) and (7), we have that $H(\mathbf{A}_{K,\mathcal{T}_2^*} \mid \mathbf{I} = i, \mathbf{Y}_K = Y_K, \mathbf{D}_{T'}) = 0$. Due to (15), it suffices to show that

$$H(\mathbf{W} \mid \mathbf{I} = i, \mathbf{Y}_K = Y_K, \mathbf{A}_{K,\mathcal{T}_1^*}, \mathbf{D}_{T'}) = H(\mathbf{W} \mid \mathbf{W}_i). \tag{28}$$

Let $A_{K,\mathcal{T}_1^*}$ and $D_{T'}$ be in the domains of $\mathbf{A}_{K,\mathcal{T}_1^*}$ and $\mathbf{D}_{T'}$, where $D_{T'} = (W^\star_{K,T}\colon\ K \in \mathcal{K},\ T \in \mathcal{T}^*,\ T' \cap (K \setminus T) \neq \emptyset)$. The secret $W_i = b \in \mathbb{F}_q$ is uniquely determined by $A_{K,\mathcal{T}_1^*}$ and $D_{T'}$ since i, Y_K are fixed. For every $W \in \mathbb{F}_q^n$ such that $W_i = b$, denote

$$p_W = \Pr[\mathbf{A}_{K,\mathcal{T}_1^*} = A_{K,\mathcal{T}_1^*}, \mathbf{D}_{T'} = D_{T'} \mid W, i, Y_K]. \tag{29}$$

Let $W' \in \mathbb{F}_q^n$ be such that $W'_i = b$. Due to the τ-privacy of $\mathrm{CNF}_{\tau,k}$, we have that

$$\Pr[\mathbf{D}_{T'} = D_{T'} \mid W, i, Y_K] = \Pr\bigl[\mathbf{D}_{T'} = D_{T'} \bigm| W', i, Y_K\bigr]. \tag{30}$$

For $S = W$ or W', we define $\Omega_S = \{w = (w_1, \ldots, w_\delta) \in \mathbb{F}_q^{\delta \times n}\colon\ \sum_{h=1}^{\delta} w_h = S - \sum_{T \in \mathcal{T}_2^*} W^\star_{K,T}\}$. For every $(b_1, \ldots, b_\delta) \in \mathbb{F}_q^\delta$ such that $\sum_{h=1}^{\delta} b_h = b - \sum_{T \in \mathcal{T}_2^*} [W^\star_{K,T}]_i$ and $w \in \Omega_W$ and $w' \in \Omega_{W'}$ such that $w_i = w'_i = (b_1, \ldots, b_\delta)$, it is not hard to see that

$$\Pr[\mathbf{W}_{K,\mathcal{T}_1^*} = w \mid D_{T'}, W, i, Y_K] = \Pr\bigl[\mathbf{W}_{K,\mathcal{T}_1^*} = w' \bigm| D_{T'}, W', i, Y_K\bigr]. \tag{31}$$

On the other hand, due to (8), we have that

$$\Pr[\mathbf{A}_{K,\mathcal{T}_1^*} = A_{K,\mathcal{T}_1^*} \mid \mathbf{W}_{K,\mathcal{T}_1^*} = w, D_{T'}, W, i, Y_K] = \Pr\bigl[\mathbf{A}_{K,\mathcal{T}_1^*} = A_{K,\mathcal{T}_1^*} \bigm| \mathbf{W}_{K,\mathcal{T}_1^*} = w', D_{T'}, W', i, Y_K\bigr]. \tag{32}$$

Eqs. (27) and (28) imply that

$$\Pr[\mathbf{A}_{K,\mathcal{T}_1^*} = A_{K,\mathcal{T}_1^*} \mid D_{T'}, W, i, Y_K] = \Pr\bigl[\mathbf{A}_{K,\mathcal{T}_1^*} = A_{K,\mathcal{T}_1^*} \bigm| D_{T'}, W', i, Y_K\bigr]. \tag{33}$$

It follows that $p_W = p_{W'}$ due to Eqs. (26) and (29). Hence, $(\mathbf{A}_{K,\mathcal{T}_1^*}, \mathbf{D}_{T'})$ and $\mathbf{W}$ are independent as long as i, Y_K and $\mathbf{W}_i$ are fixed, i.e., (28) holds and sender's privacy II is satisfied if $\mathcal{U}$ is semi-honest.

Malicious case. Let $\mathcal{S}_K$ and $\mathcal{S}_{T'}$ be the servers interacted by $\mathcal{U}$ and colluding with $\mathcal{U}$ respectively, where $K \in \mathcal{K}$ and $T' \in \mathcal{T}$. In order to learn as much information as possible, it is not hard to see that T' should be a subset of K, i.e., $T \in \mathcal{T}^*$. Due to the τ-privacy of the $\mathrm{CNF}_{\tau,k}$ TSSS, the coalition of $\bar{\mathcal{U}}$ and server $\mathcal{S}_{T'}$ is able to learn W as long as the share $W_{K,T'}$ is known. Consider the instance $\mathcal{P}$ between $\bar{\mathcal{U}}$ and $\mathcal{S}_{K\setminus T'}$. If $\bar{\mathcal{U}}$ contributes no valid index, then the coalition learns no information on $W_{K,T'}$ and therefore it learns no information on W. If $\bar{\mathcal{U}}$ contributes an index $j \in [n]$, then the coalition learns at most the secret W_j due to the data privacy of the instance $\mathcal{P}$ between $\bar{\mathcal{U}}$ and $\mathcal{S}_{K\setminus T'}$ and the privacy of $\mathrm{CNF}_{\tau,k}$. □

Communication complexity. For an invocation of Protocol 3, the receiver invokes $\binom{k}{\tau}$ instances of $\mathcal{P}$ with the interacted servers. Let $\gamma(n)$ be the communication complexity of $\mathcal{P}$. Then the communication complexity between the receiver and servers is $\binom{k}{\tau}\gamma(n)$.

Theorem 2. *If there is a t-private $(k-\tau)$-server SPIR protocol of communication complexity $\gamma(n)$, then for every integer $\ell \geqslant k$, there is a (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol of communication complexity $O(\gamma(n))$ between the receiver and servers.*

Gertner et al. [21] proposed a general transformation from any one-round t-private k-server PIR protocol of communication complexity $\gamma(n)$ to a one-round t-private $(k+t)$-server SPIR protocol of communication complexity $O(\gamma(n))$. Due to this transformation and Theorem 2, we have

Theorem 3. *If there is a t-private $(k-t-\tau)$-server PIR protocol of communication complexity $\gamma(n)$, then for every integer $\ell \geqslant k$, there is a (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol of communication complexity $O(\gamma(n))$ between the receiver and servers.*

Applying Theorem 3 to the polynomial interpolation-based t-private k-server PIR of [5,38] gives:

Corollary 1. *For any integers t, τ, k, ℓ such that $1 \leqslant t \leqslant k-2$, $0 \leqslant \tau \leqslant k-1-t$ and $\frac{3t+1}{2}+\tau \leqslant k \leqslant \ell$, there is a (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ protocol of communication complexity $O(n^{1/\lfloor\frac{2(k-t-\tau)-1}{t}\rfloor})$ between the receiver and servers.*

Note that it is required that $k \geqslant \frac{3t+1}{2}+\tau$ for obtaining sublinear communication complexity between the receiver and servers in the above corollary.

The recent progress [39,18,28,12] in the research of LDCs yields the most efficient 1-private PIR protocols to date. Specifically, 1-private 3-server PIR protocols of communication complexity $\exp(O(\sqrt{\log n \log\log n}))$ have been obtained. Barkol et al. [3] proposed a transformation from any 1-private k-server PIR of communication complexity $\gamma(n)$ to t-private k^t-server PIR of communication complexity $O(\gamma(n))$. Due to these results and Theorem 3, we have

Corollary 2. *For any positive integers t, τ, ℓ such that $\ell \geqslant 3^t+t+\tau$, there is a (t,τ)-private $(3^t+t+\tau,\ell)$-DOT-$\binom{n}{1}$ protocol of communication complexity $\exp(O(\sqrt{\log n \log\log n}))$ between the receiver and servers.*

As an example, for $t=\tau=1$ and any $\ell \geqslant 5$, there is a $(1,1)$-private $(5,\ell)$-DOT-$\binom{n}{1}$ protocol of communication complexity $\exp(O(\sqrt{\log n \log\log n}))$ between the receiver and servers.

5. Evaluation of the reductions

In this section, we evaluate our reductions. Specifically, we compare them with known constructions of DOT and with each other.

Privacy. The one-round (k,ℓ)-DOT-$\binom{n}{1}$ protocols of [8] do not satisfy sender's privacy II. In terms of our definition, their (k,ℓ)-DOT-$\binom{n}{1}$ protocols achieve $(k-1)$-receiver privacy, $(k-1)$-sender's privacy I and 0-sender's privacy II. For semi-honest receivers, if we take $t=k-1$ and $\tau=0$ in Protocol 2 and apply the encoding E of indices of [38] for $m=n$, then the one-round (k,ℓ)-DOT-$\binom{n}{1}$ of [8] can be obtained. The (k,ℓ)-DOT-$\binom{n}{1}$ of [34] achieves t-receiver privacy, $(k-1-t)$-sender's privacy I and $(k-1-t)$-sender's privacy II for any positive integer $t<k-1$. Our specific reduction yields (k,ℓ)-DOT-$\binom{n}{1}$ which achieves the same privacy whenever $t+\tau=k-1$. Hence, the specific reduction shows a tradeoff between receiver–server communication complexity and privacy. The specific reduction is secure for semi-honest receivers. It is left open to modify the specific reduction such that the sender's privacy I and II can be achieved for malicious receivers. On the other hand, our general reduction is fully secure.

Receiver–server communication complexity. Let t, τ be positive integers. It has been proved by [34] that $k \geqslant t+\tau+1$ in any (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$. If $t+\tau+1 \leqslant k \leqslant 2t+\tau$, then the (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ obtained by the general reduction require linear communication complexity between the receiver and servers due to Corollary 1. Hence, we prefer the specific reduction. If $k>2t+\tau$, then $\lfloor\frac{2(k-t-\tau)-1}{t}\rfloor > \lfloor\frac{k-\tau-1}{t}\rfloor$ and therefore the (t,τ)-private (k,ℓ)-DOT-$\binom{n}{1}$ obtained by the general reduction is more efficient due to Theorem 1 and Corollary 1. Hence, we prefer the general reduction. Furthermore, for small values of t and τ, the reduction given by Corollary 2 is much better than those given by Theorem 1 and Corollary 1 since it is based on the 3-server PIR protocols of extremely small communication complexity $\exp(O(\sqrt{\log n \log\log n}))$.

Number of interacted servers. For availability, the receiver should interact with a small number of servers. The specific reduction of Theorem 1 achieves the lower bound given by [34] and therefore is optimal in terms of the number of interacted servers. In contrast, the general reductions of Corollaries 1 and 2 require $k \geqslant \frac{3t+1}{2}+\tau$ and $k=3^t+t+\tau$, respectively. Hence, they are not optimal in terms of the number of interacted servers.

Setup complexity. The setup complexity of our reductions may be large for some settings of the parameters ℓ and k. For example, in the setup stage of our specific reduction, each server receives $\binom{\ell-1}{k-1}$ random masks (field elements) and an m-variate polynomial of small constant degree; in the setup stage of our general reduction from DOT to SPIR, each server receives $\binom{\ell-1}{k-1}\binom{k-1}{t}$ shares (vectors of n field elements) of the database and $\binom{\ell}{k}\binom{k}{t}$ random masks (field elements). However, the setup complexity becomes reasonable if $\ell = k$ and t is a constant less than k. We note that the DOT protocols in a setting where $\ell = k$ have been considered by Cheong et al. [13]. Our reductions are efficient for that setting.

Independence of secrets. We assume that the sender's secrets are *totally independent* in Section 2.2, i.e., Eq. (5) holds. However, our security proofs for the general reduction from DOT to SPIR in Section 4 do not depend on this assumption. On the other hand, the assumption is necessary for our specific reduction.

6. Conclusion

In this paper, we study DOT of sublinear communication complexity between the receiver and servers. We present both a specific reduction from DOT to polynomial interpolation-based PIR and a general reduction from DOT to any PIR. The specific reduction yields DOT protocols which are optimal in terms of the number of interacted servers and are secure for semi-honest receivers. The general reduction yields DOT protocols of extremely small communication complexity between the receiver and servers and are secure for malicious receivers. The setup complexity of our reductions could be large for some settings of the parameters. It is an open problem to reduce the setup complexity of our reductions.

Appendix A. Polynomial interpolation-based PIR protocols

We enumerate four polynomial interpolation-based PIR protocols in this appendix. Originally, the first two do not follow the framework depicted by Protocol 1. However, from our point of view, they fall into the framework of polynomial interpolation-based PIR protocols.

A.1. Beimel–Ishai–Kushilevitz PIR Protocol I [5]

- Let $\Omega = \{v \in \{0,1\}^m \mid \mathrm{wt}(v) \leqslant d\} \subseteq \mathbb{F}_q^m$, where $\mathrm{wt}(v)$ is the number of nonzero components of v. The encoding $E : [n] \to \Omega$ is a one-to-one mapping satisfying $\mathrm{wt}(E(i)) \geqslant \mathrm{wt}(E(j))$ for every $i < j$.
- Let $S_j = \{a \in [m]\colon E(j)_a = 1\}$ for every $j \in [n]$. The polynomials P_j are defined inductively as follows

$$P_j(Z_1,\ldots,Z_m) = \prod_{a\in S_j} Z_a - \sum_{i\colon S_j \subset S_i} P_i(Z_1,\ldots,Z_m).$$

A.2. Beimel–Ishai–Kushilevitz PIR Protocol II [5]

- Let $\Omega = \{v = v_1 \circ \cdots \circ v_d \mid \forall a \in [d],\ v_a \in \{0,1\}^b \text{ and } \mathrm{wt}(v_a) = 1\} \subseteq \mathbb{F}_q^m$, where $m = bd$. For $i \in [n]$,

$$E(i) = e_{i_1+1} \circ \cdots \circ e_{i_d+1} \in \Omega,$$

  where i has base-b expansion $\sum_{a\in[d]} i_a \cdot b^{a-1}$ and e_{i_a+1} is the (i_a+1)st unit vector for every $a \in [d]$.
- Identify $(Z_1,\ldots,Z_m) = (Z_{1,1},\ldots,Z_{1,b};\ldots;Z_{d,1},\ldots,Z_{d,b})$. For every $j = \sum_{a\in[d]} j_a \cdot b^{a-1} \in [n]$,

$$P_j(Z_{1,1},\ldots,Z_{1,b};\ldots;Z_{d,1},\ldots,Z_{d,b}) = Z_{1,j_1+1} \ldots Z_{d,j_d+1}.$$

A.3. Beimel–Ishai–Kushilevitz PIR Protocol III [5]

- Let $\Omega = \{\omega_0,\ldots,\omega_d\}^m \subseteq \mathbb{F}_q^m$, where $\omega_0,\ldots,\omega_d \in \mathbb{F}_q \setminus \{0\}$ are distinct. The encoding $E : [n] \to \Omega$ is one-to-one and for every $i \in [n]$,

$$E(i) = (w_{i_1},\ldots,w_{i_m}) \in \Omega,$$

  where $\sum_{a\in[m]} i_a \leqslant d$. For any $i < j$ and $E(j) = (\omega_{j_1},\ldots,\omega_{j_m}) \in \Omega$, it is required that $\sum_a i_a \geqslant \sum_a j_a$.
- The polynomials $P_j(Z_1,\ldots,Z_m)$ are defined inductively as follows

$$r_j(Z_1,\ldots,Z_m) = \prod_{a=1}^{m} \prod_{h=0}^{j_a-1} \frac{Z_a - w_h}{w_{j_a} - w_h},$$

$$P_j(Z_1,\ldots,Z_m) = r_j(Z_1,\ldots,Z_m) - \delta_j \cdot \sum_{i=1}^{j-1} r_j\bigl(E(i)\bigr) P_i(Z_1,\ldots,Z_m),$$

  where $\delta_j = 1$ if $\sum_a j_a = d$ and 0 otherwise.

A.4. Woodruff–Yekhanin PIR Protocol [38]

- Let $\Omega = \{v \in \{0,1\}^m \mid \mathrm{wt}(v) = d\} \subseteq \mathbb{F}_q^m$. The encoding $E : [n] \to \Omega$ is any one-to-one mapping.
- Let $S_j = \{a \in [m]\colon\ E(j)_a = 1\}$ for every $j \in [n]$. The polynomials P_j are defined as follows

$$P_j(Z_1, \ldots, Z_m) = \prod_{a \in S_j} Z_a.$$

References

[1] W. Aiello, Y. Ishai, O. Reingold, Priced oblivious transfer: How to sell digital goods, in: Advances in Cryptology – EUROCRYPT 2001, in: Lecture Notes in Comput. Sci., vol. 2045, Springer-Verlag, 2001, pp. 119–135.

[2] A. Ambainis, Upper bound on the communication complexity of private information retrieval, in: Proceedings of the 24th International Colloquium on Automata, Languages and Programming, in: Lecture Notes in Comput. Sci., vol. 1256, Springer-Verlag, 1997, pp. 401–407.

[3] O. Barkol, Y. Ishai, E. Weinreb, On locally decodable codes, self-correctable codes, and t-private PIR, in: Proceedings of APPROX and RANDOM 2007, in: Lecture Notes in Comput. Sci., vol. 4627, Springer-Verlag, 2007, pp. 311–325.

[4] D. Beaver, J. Feigenbaum, J. Kilian, P. Rogaway, Locally random reductions: improvements and applications, J. Cryptology 10 (1) (1997) 17–36.

[5] A. Beimel, Y. Ishai, E. Kushilevitz, General constructions for information-theoretic private information retrieval, J. Comput. System Sci. 71 (2) (2005) 213–247.

[6] A. Beimel, Y. Ishai, E. Kushilevitz, J.F. Raymond, Breaking the $O(n^{1/(2k-1)})$ barrier for information-theoretic private information retrieval, in: Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science, 2002, pp. 261–270.

[7] M. Bellare, S. Micali, Non-interactive oblivious transfer and applications, in: Advances in Cryptology – CRYPTO 1989, in: Lecture Notes in Comput. Sci., vol. 435, Springer-Verlag, 1990, pp. 547–557.

[8] C. Blundo, P. D'Arco, A. De Santis, D.R. Stinson, On unconditionally secure distributed oblivious transfer, J. Cryptology 20 (3) (2007) 323–373.

[9] G. Brassard, C. Crépeau, J.M. Robert, Information theoretic reductions among disclosure problems, in: Proceedings of the 27th IEEE Symposium on Foundations of Computer Science, 1986, pp. 168–173.

[10] G. Brassard, C. Crépeau, J.M. Robert, All-or-nothing disclosure of secrets, in: Advances in Cryptology – CRYPTO 1986, in: Lecture Notes in Comput. Sci., vol. 263, Springer-Verlag, 1987, pp. 234–238.

[11] D. Chaum, I. Damgård, J. van de Graaf, Multiparty computations ensuring privacy of each party's input and correctness of the result, in: Advances in Cryptology – CRYPTO 1987, in: Lecture Notes in Comput. Sci., vol. 293, Springer-Verlag, 1988, pp. 87–119.

[12] Y.M. Chee, T. Feng, S. Ling, H. Wang, L.F. Zhang, Query-efficient locally decodable codes of subexponential length, arXiv:1008.1617v1 [cs.CC], 2010.

[13] K.Y. Cheong, T. Koshiba, S. Nishiyama, Strengthening the security of distributed oblivious transfer, in: Proceedings of the 14th Australasian Conference on Information Security and Privacy, in: Lecture Notes in Comput. Sci., vol. 5594, Springer-Verlag, 2009, pp. 377–388.

[14] B. Chor, O. Goldreich, E. Kushilevitz, M. Sudan, Private information retrieval, in: Proceedings of the 36th IEEE Symposium on Foundations of Computer Science, 1995, pp. 41–50.

[15] C. Crépeau, Verifiable disclosure of secrets and applications, in: Advances in Cryptology – CRYPTO 1989, in: Lecture Notes in Comput. Sci., vol. 434, Springer-Verlag, 1990, pp. 181–191.

[16] G. Di Crescenzo, Y. Ishai, R. Ostrovsky, Universal service-providers for database private information retrieval, in: Proceedings of the 17th ACM Symposium on Principles of Distributed Computing, 1998, pp. 91–100.

[17] C. Crépeau, Equivalence between two flavors of oblivious transfers, in: Advances in Cryptology – CRYPTO 1987, in: Lecture Notes in Comput. Sci., vol. 293, Springer-Verlag, 1988, pp. 350–354.

[18] K. Efremenko, 3-query locally decodable codes of subexponential length, in: Proceedings of the 41st ACM Symposium on Theory of Computing, 2009, pp. 39–44.

[19] S. Even, O. Goldreich, A. Lempel, A randomized protocol for signing contracts, Commun. ACM 28 (6) (1985) 637–647.

[20] Y. Gertner, S. Goldwasser, T. Malkin, A random server model for private information retrieval, in: Proceedings of RANDOM 1998, in: Lecture Notes in Comput. Sci., vol. 1518, Springer-Verlag, 1998, pp. 200–217.

[21] Y. Gertner, Y. Ishai, E. Kushilevitz, T. Malkin, Protecting data privacy in private information retrieval protocols, in: Proceedings of the 30th ACM Symposium on the Theory of Computing, 1998, pp. 151–160.

[22] O. Goldreich, Foundations of Cryptography, vol. II: Basic Applications, Cambridge University Press, 2004.

[23] O. Goldreich, S. Micali, A. Wigderson, How to play any mental game or a completeness theorem for protocols with honest majority, in: Proceedings of the 19th ACM Symposium on the Theory of Computing, 1987, pp. 218–229.

[24] O. Goldreich, R. Vainish, How to solve any protocol problem – an efficiency improvement, in: Advances in Cryptology – CRYPTO 1987, in: Lecture Notes in Comput. Sci., vol. 293, Springer-Verlag, 1988, pp. 73–86.

[25] S. Goldwasser, L.A. Levin, Fair computation of general functions in presence of immoral majority, in: Advances in Cryptology – CRYPTO 1990, in: Lecture Notes in Comput. Sci., vol. 537, Springer-Verlag, 1991, pp. 77–93.

[26] I. Haitner, Implementing oblivious transfer using collection of dense trapdoor permutations, in: Proceedings of the 1st Theory of Cryptography Conference, in: Lecture Notes in Comput. Sci., vol. 2591, Springer-Verlag, 2004, pp. 394–409.

[27] M. Ito, A. Satio, T. Nishizeki, Secret sharing scheme realizing general access structure, Electron. Commun. Japan 72 (9) (1989) 56–64.

[28] T. Itoh, Y. Suzuki, New constructions for query-efficient locally decodable codes of subexponential length, IEICE Trans. Inf. Syst. E93-D (2) (2010) 263–270.

[29] Y.T. Kalai, Smooth projective hashing and two-message oblivious transfer, in: Advances in Cryptology – EUROCRYPT 2005, in: Lecture Notes in Comput. Sci., vol. 3494, Springer-Verlag, 2005, pp. 78–95.

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

[31] M. Naor, B. Pinkas, Distributed oblivious transfer, in: Advances in Cryptology – ASIACRYPT 2000, in: Lecture Notes in Comput. Sci., vol. 1976, Springer-Verlag, 2000, pp. 205–219.

[32] M. Naor, B. Pinkas, Efficient oblivious transfer protocols, in: Proceedings of the 12th SIAM Symposium on Discrete Algorithms, 2001, pp. 448–457.

[33] M. Naor, B. Pinkas, R. Sumner, Privacy preserving auctions and mechanism design, in: Proceedings of the 1st ACM conference on Electronic Commerce, 1999, pp. 129–139.

[34] V. Nikov, S. Nikova, B. Preneel, J. Vandewalle, On unconditionally secure distributed oblivious transfer, in: Progress in Cryptology – INDOCRYPT 2002, in: Lecture Notes in Comput. Sci., vol. 2551, 2002, pp. 395–408.

[35] R. Ostrovsky, V. Shoup, Private information storage, in: Proceedings of the 29th ACM Symposium on the Theory of Computing, 1997, pp. 294–303.

[36] M.O. Rabin, How to exchange secrets by oblivious transfer, Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[37] R. Rivest, Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer, unpublished manuscript, http://theory.lcs.mit.edu/~rivest/publications.html, 1999.

[38] D.P. Woodruff, S. Yekhanin, A geometric approach to information-theoretic private information retrieval, in: Proceedings of the 20th IEEE Conference on Computational Complexity, 2005, pp. 275–284.

[39] S. Yekhanin, Towards 3-query locally decodable codes of subexponential length, in: Proceedings of the 39th ACM Symposium on Theory of Computing, 2007, pp. 266–274.