The Capacity of Symmetric Private Information Retrieval

Hua Sun and Syed A. Jafar
Center for Pervasive Communications and Computing (CPCC)
University of California Irvine, Irvine, CA 92697

Abstract—Private information retrieval (PIR) is the problem of retrieving as efficiently as possible, one out of $K$ messages from $N$ non-communicating replicated databases (each holds all $K$ messages) while keeping the identity of the desired message index a secret from each individual database. Symmetric PIR (SPIR) is a generalization of PIR to include the requirement that beyond the desired message, the user learns nothing about the other $K-1$ messages. The information theoretic capacity of SPIR (equivalently, the reciprocal of minimum download cost) is the maximum number of bits of desired information that can be privately retrieved per bit of downloaded information. We show that the capacity of SPIR is $1-1/N$ regardless of the number of messages $K$, if the databases have access to common randomness (not available to the user) that is independent of the messages, in the amount that is at least $1/(N-1)$ bits per desired message bit, and zero otherwise.

I. INTRODUCTION

The private information retrieval (PIR) problem \cite{A3, A4} seeks the most efficient way for a user to retrieve a desired message from a set of distributed databases, each of which stores all the messages, without revealing any information about which message is being retrieved to any individual database. This seemingly impossible mission has a trivial (expensive) solution, i.e., the user can request all the messages to hide its interest. The goal of the PIR problem is to find the most efficient solution. The capacity of PIR is defined as the maximum number of bits of desired message that can be privately downloaded per bit of downloaded information. In our recent work \cite{A3}, the capacity of PIR with $K$ messages and $N$ databases was shown to be $C_{PIR} = \left(1 + 1/N + \cdots + 1/(N^{K-1})\right)^{-1}$.

The original formulation of PIR only considers the privacy of the user. The privacy of the undesired messages is ignored. However, it is often desirable to restrict the user to retrieve nothing beyond his chosen message. This new constraint is called database privacy, and with this constraint, the problem is called symmetricPIR (SPIR) \cite{A4}. Symmetric PIR is especially challenging because the databases must individually learn nothing about the identity of the desired message, but must still collectively allow the user to retrieve his desired message in such a way that the user learns nothing about any other message besides his desired message. For example, the trivial solution of downloading everything, is no longer acceptable. The main contribution of this work is the characterization of the capacity of SPIR, i.e., the maximum number of bits of desired message that can be privately retrieved by a user per bit of downloaded information, without leaking any information about undesired messages to the user. For $K$ messages and $N$ databases, we show that the capacity is $1-1/N$.

Besides its direct applications, PIR is especially significant as a fundamental problem that lies at the intersection of several open problems in cryptography \cite{A5, A6}, coding theory \cite{A7, A8, A9} and complexity theory \cite{A10}. SPIR inherits many of these connections from PIR. For example, SPIR is essentially a (distributed) form of oblivious transfer \cite{A11, A12}, where the typical objective is that the transmitter(s) should not know which message is received by the receiver and the receiver should obtain nothing more than the desired message. Oblivious transfer is an important building block (primitive) in cryptography, whose feasibility leads to many other cryptographic protocols \cite{A13, A14}. Fundamental limits on the communication efficiency of various forms of oblivious transfer therefore represent an important class of open problems \cite{A15, A16}. The capacity characterization of SPIR is a promising step in this direction.

Notation: For $n_1, n_2 \in \mathbb{Z}, n_1 \leq n_2$, define the notation $[n_1 : n_2]$ as the set $(n_1, n_1+1, \cdots, n_2)$. For an index set $\mathcal{I} = \{i_1, i_2, \cdots, i_n\}$, with $i_1 < i_2 < \cdots < i_n$, the notation $\mathcal{A}_2$ represents the vector $(A_{i_1}, A_{i_2}, \cdots, A_{i_n})$. For an element $i_\theta$ in the set $\mathcal{I} = \{i_1, i_2, \cdots, i_n\}$, i.e., $i_\theta \in \mathcal{I}$, the notation $\mathcal{I}_{\theta}^c$ represents the complement of $\{i_\theta\}$, i.e., $\mathcal{I}_{\theta}^c = \{i_1, \cdots, i_{\theta-1}, i_{\theta+1}, \cdots, i_n\}$. For two sets $\mathcal{A}_1, \mathcal{A}_2$, $\mathcal{A}_1/\mathcal{A}_2$ represents the set of elements that are in $\mathcal{A}_1$ but not in $\mathcal{A}_2$.

II. PROBLEM STATEMENT

Consider $K$ independent messages $W_1, \cdots, W_K$ of size $L$ bits each.

$$H(W_1, \cdots, W_K) = H(W_1) + \cdots + H(W_K),$$

$$H(W_1) = \cdots = H(W_K) = L. \quad (1)$$

There are $N$ databases. Each database stores all the messages $W_1, \cdots, W_K$. A user wants to retrieve $W_{\theta}, \theta \in [1 : K]$ privately, i.e., without revealing anything about the message identity, $\theta$, to any individual database. The databases do not want to give out any information beyond the one message of the user’s choosing ($W_{\theta}$). In order to achieve database-privacy, we assume that the databases share a common random variable.
Fig. 1. The SPIR problem with $K$ messages and 2 databases.

Without loss of generality, assume that the user chooses a fixed index $\theta$ uniformly over $[1 : K]$. In order to retrieve message $W_{\theta}$, the user privately generates $N$ queries $Q_1^{[\theta]}, \ldots, Q_N^{[\theta]}$. Since the desired message index $\theta$ and the queries are determined by the user, who has no knowledge of the realizations of the messages and the common randomness, the queries and the desired message index must be independent of the messages and the common randomness,

$$I(W_1, \cdots, W_K, S; \theta, Q) = 0.$$  (3)

where $Q = [Q_n^{[\theta]}]_{k \in [1 : K], n \in [1 : N]}$.

The user sends query $Q_n^{[\theta]}$ to the $n$-th database, $\forall n \in [1 : N]$. Upon receiving $Q_n^{[\theta]}$, the $n$-th database generates an answering string $A_n^{[\theta]}$, which is a deterministic function of $Q_n^{[\theta]}$, all messages $W_1, \cdots, W_K$ and the common randomness $S$,

$$H(A_n^{[\theta]}|Q_n^{[\theta]}, W_1, \cdots, W_K, S) = 0.$$  (4)

Each database returns to the user its answer $A_n^{[\theta]}$. From all the information that is now available to the user, he must be able to correctly decode the desired message $W_{\theta}$, i.e., the following correctness criterion must be satisfied:

[Correctness] $H(W_{\theta}|A_1^{[\theta]}, \cdots, A_N^{[\theta]}, Q, \theta) = 0$.  (5)

To protect the user’s privacy, it must be true that any individual database learns nothing about the desired message index $\theta$. Information theoretically, $\theta$ must be independent of all the information available to any individual database. Thus, the following user-privacy constraint must be satisfied $\forall n \in [1 : N]$,

[User-Privacy] $I(\theta; Q_n^{[\theta]}, A_n^{[\theta]}, W_1, \cdots, W_K, S) = 0$.  (6)

Symmetric PIR also requires protecting the privacy of the database, i.e., it must be ensured that the user learns nothing more than the desired message $W_{\theta}$. So the vector $W_{\theta} = (W_1, \cdots, W_{\theta-1}, W_{\theta+1}, \cdots, W_K)$, must be independent of all the information available to the user. Thus, the following database-privacy constraint must be satisfied:

[DB-Privacy] $I(W_{\theta}; A_1^{[\theta]}, \cdots, A_N^{[\theta]}, Q, \theta) = 0$  (7)

The SPIR rate characterizes how many bits of desired information are retrieved per downloaded bit, and is defined as follows.

$$R \triangleq \frac{L}{\sum_{n=1}^{N} H(A_n^{[\theta]})}.$$  (8)

The capacity, $C$, is the supremum of $R$ over all SPIR schemes.

III. MAIN RESULT: CAPACITY OF SPIR

When there is only $K = 1$ message, note that the database-privacy constraint is satisfied trivially, so that SPIR reduces to the PIR setting and the capacity is 1. For $K \geq 2$, it is known that some common randomness $S$ is necessary for the feasibility of SPIR. Let us define $\rho$ as the amount of common randomness relative to the message size

$$\rho = \frac{H(S)}{H(W)} = \frac{H(S)}{L}.$$  (9)

The capacity should depend on $\rho$, and because availability of common randomness at the databases is a non-trivial requirement, this dependence is of some interest. The following theorem states our main result, the capacity of SPIR.

Theorem 1: For SPIR with $K \geq 2$ messages and $N$ databases, the capacity is

$$C_{SPIR} = \begin{cases} 1 - \frac{1}{N} & \text{if } \rho \geq \frac{1}{N-1} \\ 0 & \text{otherwise} \end{cases}.$$  (10)

The achievability proof appears in Section IV. The converse proof appears in Section V.

We notice a surprising threshold phenomenon in the dependence of SPIR capacity, $C_{SPIR}$, on the amount of common randomness $\rho$. When $\rho < \frac{1}{N-1}$, SPIR is not feasible and $C_{SPIR} = 0$. However, when $\rho \geq \frac{1}{N-1}$, SPIR is not only possible, but the rate can immediately be increased to the maximum possible, i.e., the capacity. Therefore, the minimum common randomness required to achieve any positive rate is already sufficient to achieve the capacity of SPIR. A pictorial illustration of the SPIR capacity and its dependency on the amount of common randomness appears in Figure 2.

Another surprising observation is that the capacity of SPIR is independent of the number of messages, $K$. When the capacity is non-zero, the capacity is strictly increasing in the number of databases, $N$, and when $N$ approaches infinity, the capacity approaches 1. It is interesting to compare the capacity of SPIR and the capacity of PIR [3].

$$C_{PIR} = \left(1 + 1/N + 1/N^2 + \cdots + 1/N^{K-1}\right)^{-1}.$$  (11)

We see that the capacity of SPIR is strictly smaller than the capacity of PIR (the additional requirement of preserving
database-privacy strictly hurts) and the capacity of PIR approaches the capacity of SPIR when the number of messages, $K$, approaches infinity (in the large number of messages regime, the penalty vanishes), i.e., $C_{PIR} > C_{SPIR}$ for any finite $K$ and $C_{SPIR} \to C_{SPIR}$ when $K \to \infty$.

IV. PROOF OF THEOREM I: ACHIEVABILITY

In this section, we present the scheme that achieves rate $1 - 1/N$, when $\rho = 1/(N - 1)$. To this end, we assume each message consists of $N - 1$ bits and each answering string is 1 bit. Specifically, we assume $W_k = (x_{k,1}, \ldots, x_{k,N-1}), \forall k \in [1 : K]$ where each $x_{k,i}, i \in [1 : N - 1]$ is one bit. We further assume the entropy of the common random variable $S$ is 1 bit, i.e., $S$ is uniformly distributed over $\{0, 1\}$. Note that $S$ is independent of the messages.

Next we specify the queries functions. To retrieve $W_\theta$ privately, the user first generates a random vector of length $(N - 1)K$, $[h_{1,1}, \ldots, h_{1,N-1}, \ldots, h_{\theta,1}, \ldots, h_{K,N-1}]$, where each element is uniformly distributed over $\{0, 1\}$. Then the answers are set as follows.

$$Q_1^{[\theta]} = [h_{1,1}, \ldots, h_{\theta,1}, \ldots, h_{\theta,N-1}, \ldots, h_{K,N-1}]$$

$$Q_2^{[\theta]} = [h_{1,1}, \ldots, h_{\theta,1} + 1, \ldots, h_{\theta,N-1}, \ldots, h_{K,N-1}]$$

$$\ldots$$

$$Q_K^{[\theta]} = [h_{1,1}, \ldots, h_{\theta,1}, \ldots, h_{\theta,N-1} + 1, \ldots, h_{K,N-1}]$$

The answering strings are generated by using the query vector as the combining coefficients and producing the corresponding linear combination of message bits. We further add the common random variable to each answer.

$$A_1^{[\theta]} = \sum_{k=1}^{K} \sum_{i=1}^{N-1} h_{k,i}x_{k,i} + S$$

$$A_2^{[\theta]} = \sum_{k=1}^{K} \sum_{i=1}^{N-1} h_{k,i}x_{k,i} + x_{\theta,1} + S$$

$$\ldots$$

$$A_K^{[\theta]} = \sum_{k=1}^{K} \sum_{i=1}^{N-1} h_{k,i}x_{k,i} + x_{\theta,N-1} + S$$

The user obtains $x_{\theta,i}, i \in [1 : N - 1]$ by subtracting $A_1^{[\theta]}$ from $A_{\theta+1}^{[\theta]}$. Therefore, the correctness condition is satisfied.

Privacy of the user is guaranteed because each query is independent of the desired message index $\theta$. This is because regardless of the desired message index $\theta$, each of the query vectors $Q_n^{[\theta]}, \forall n$ is individually comprised of elements that are i.i.d. uniform over $\{0, 1\}$. Thus, each database learns nothing about which message is requested.

We now show that database-privacy is preserved as well.

$$I(W_\theta ; A_1^{[\theta]}, A_2^{[\theta]}, \ldots, A_K^{[\theta]}, Q, \theta) \leq I(W_\theta ; A_1^{[\theta]}, A_2^{[\theta]}, \ldots, A_K^{[\theta]}, Q, \theta)$$

(12)

(13)

(14)

(15)

(16)

(17)

where in each step, the transformation on the variables is invertible such that mutual information remains the same. The last step follows from the independence of the messages and the common randomness.

Note that because each answering string is 1 bit and the message is $L = N - 1$ bits, the rate achieved is $(N - 1)/N = 1 - 1/N$ which matches the capacity. Also note that only the minimum threshold amount of common randomness is utilized, i.e., $\rho = 1/(N - 1)$.

V. PROOF OF THEOREM I: CONVERSE

For the converse we allow any feasible SPIR scheme, and prove that its rate cannot be larger than $C_{SPIR}$. Let us start with two lemmas that will be used later in the proof.

**Lemma 1:**

$$H(A_n^{[K]} | W_k, Q_n^{[K]}) = H(A_n^{[K']} | W_k, Q_n^{[K']})$$

$$H(A_n^{[K]} | Q_n^{[K]}) = H(A_n^{[K']} | Q_n^{[K']})$$

(18)

(19)

**Proof:** Since the proofs of (18) and (19) follow from the same arguments, here we will present only the proof of (18).

From the User-Privacy constraint we know that $\forall k \in [1 : K]$, $I(\theta; A_n^{[\theta]} | W_k, Q_n^{[\theta]}) = 0$. Therefore, we must have $\forall k' \in [1 : K]$,

$$H(A_n^{[K]} | W_k, Q_n^{[K]}) - H(A_n^{[K']} | W_k, Q_n^{[K']}) = 0$$

(20)

But we also know that $\forall k \in [1 : K]$, $I(W_k, Q_n^{[\theta]} | \theta) = 0$, so we must also have

$$H(W_k, Q_n^{[K]}) = H(W_k, Q_n^{[K']})$$

(21)

Combining (20) and (21), we obtain $H(A_n^{[K]} | W_k, Q_n^{[K]}) = H(A_n^{[K']} | W_k, Q_n^{[K']})$.

**Lemma 2:**

$$H(A_n^{[K]} | W_k, Q, Q_n^{[K]}) = H(A_n^{[K]} | W_k, Q_n^{[K]})$$

(22)

**Proof:** Since

$$H(A_n^{[K]} | W_k, Q_n^{[K]}) - H(A_n^{[K]} | W_k, Q, Q_n^{[K]}) = I(A_n^{[K]}; Q | W_k, Q_n^{[K]}) \geq 0,$$

(23)

(24)
we only need to prove $I(A_{[k]}^{[k]}; Q|W_k, Q_{[n]}^{[k]}) \leq 0$.

$$I(A_{[k]}^{[k]}; Q|W_k, Q_{[n]}^{[k]})$$

$$\leq I(A_{[k]}^{[k]}, W_1, \ldots, W_K, S; Q|W_k, Q_{[n]}^{[k]})$$

$$= I(W_1, \ldots, W_K, S; Q|W_k, Q_{[n]}^{[k]})$$

$$+ I(A_{[k]}^{[k]}, Q|W_1, \ldots, W_K, S, W_k, Q_{[n]}^{[k]})$$

$$= 0$$

(27)

(28)

(29)

where the second term in (27) is zero because of (44) and (29) follows from (43).

A. The proof for $R \leq C_{SPIR}$

For every feasible SPIR scheme, we must satisfy the database-privacy constraint,

$$0 = I(W_P; A_{[k]}^{[k]}, \ldots, A_N^{[k]}, Q, \theta)$$

(30)

So we must have $\forall k' \in [1 : K]$

$$0 = I(W_P; A_{[k]}^{[k]}, \ldots, A_N^{[k]}, Q)$$

(31)

and $\forall n \in [1 : N], \forall k \in [1 : K], k \neq k'$

$$0 = I(W_k; A_{[k]}^{[k]}, Q_{[n]}^{[k]})$$

(32)

$$= I(W_k; A_{[k]}^{[k]}, Q^{[k]})$$

(33)

$$= H(A_{[k]}^{[k]}|Q^{[k]}) - H(A_{[k]}^{[k]}|W_k, Q_{[n]}^{[k]})$$

(34)

$$= H(A_{[k]}^{[k]}|Q^{[k]}) - H(A_{[k]}^{[k]}|Q_{[n]}^{[k]})$$

(35)

In the last step we used (18) in Lemma 1. Now, consider the answering strings $A_{[k]}^{[k]}, \ldots, A_N^{[k]}$, from which we can decode $W_k$.

$$L = H(W_k) = H(W_k|Q)$$

(36)

$$\leq I(W_k; A_{[k]}^{[k]}, \ldots, A_N^{[k]}|Q)$$

(37)

$$= H(A_{[k]}^{[k]}|\ldots, A_N^{[k]}|Q)$$

$$- H(A_{[k]}^{[k]}, \ldots, A_N^{[k]}|W_k, Q)$$

(38)

$$\leq H(A_{[k]}^{[k]}|\ldots, A_N^{[k]}|Q) - H(A_{[k]}^{[k]}|W_k, Q, Q_{[n]}^{[k]})$$

(39)

(using Lemma 2)

$$= H(A_{[k]}^{[k]}, \ldots, A_N^{[k]}|Q) - H(A_{[k]}^{[k]}|W_k, Q_{[n]}^{[k]})$$

(40)

(41)

(42)

(43)

(44)

(45)

(46)

(47)

Adding (42) for $n = [1 : N]$, we have

$$NL \leq N H(A_{[k]}^{[k]}, \ldots, A_N^{[k]}|Q) - \sum_{n=1}^{N} H(A_{[n]}^{[k]}|Q)$$

$$\leq (N - 1) H(A_{[k]}^{[k]}, \ldots, A_N^{[k]}|Q)$$

$$\leq (N - 1) \sum_{n=1}^{N} H(A_{[n]}^{[k]})$$

$$\leq (N - 1) \sum_{n=1}^{N} H(A_{[n]}^{[k]})$$

$$\Rightarrow R = \frac{L}{\sum_{n=1}^{N} H(A_{[n]}^{[k]})} \leq \frac{N - 1}{N} = 1 - \frac{1}{N}$$

(48)

(49)

(50)

(51)

(52)

(53)

(54)

(55)

(56)

(57)

(58)

(59)

(60)

where (46) follows from the condition $I(A_{[n]}^{[k]}; \theta) = 0$ so that $H(A_{[n]}^{[k]}) = H(A_{[n]}^{[k]}), \forall k \in [1 : K]$. Thus, the rate of any feasible SPIR scheme cannot be more than $C_{SPIR}$.

B. The proof for $\rho \geq 1/(1 - N)$

Suppose a feasible SPIR scheme exists that achieves a non-zero SPIR rate. Then we will show in this section that it must have $\rho \geq 1/(1 - N)$. Consider the answering strings $A_{[k]}^{[k]}, \ldots, A_N^{[k]}$, from which we can decode $W_k$.

From the database-privacy constraint, we have

$$0 = I(W_P; A_{[k]}^{[k]}, \ldots, A_N^{[k]}, Q)$$

(48)

$$= I(W_P; A_{[k]}^{[k]}, \ldots, A_N^{[k]}|Q)$$

(49)

$$\geq I(W_P; A_{[k]}^{[k]}, \ldots, A_N^{[k]}, W_k|Q)$$

(50)

$$= I(W_P; A_{[k]}^{[k]}, \ldots, A_N^{[k]}|W_k, Q)$$

(51)

$$\geq I(W_P; A_{[k]}^{[k]}, \ldots, A_N^{[k]}|W_k, Q)$$

(52)

$$= H(A_{[k]}^{[k]}|W_k, Q) - H(A_{[k]}^{[k]}|W_k, Q|W_k, Q)$$

(53)

(54)

(55)

(56)

(57)

(58)

(59)

where (50) follows from the fact that from $A_{[k]}^{[k]}, \ldots, A_N^{[k]}$, we can decode $W_k$. (51) is due to the independence of the messages, and (52) follows from the fact that the answers are deterministic functions of the queries, all messages and the common random variable. (57) follows from Lemma 2. (58) is obtained because of (55). (59) follows from (19) in Lemma 1.

Adding (58) for $n \in [1 : N]$, we have

$$0 \geq \sum_{n=1}^{N} H(A_{[n]}^{[k]}|Q_{[n]}^{[k]}) - NH(S)$$

(60)
\begin{align}
\geq & \quad H(A_1^{[k]}, \ldots, A_N^{[k]} | Q) - NH(S) \tag{61} \\
\geq & \quad \frac{N}{N-1} L - NH(S) \tag{62} \\
\Rightarrow H(S) & \geq \frac{1}{N-1} L \tag{63} \\
\Rightarrow & \quad \rho = \frac{H(S)}{L} \geq \frac{1}{N-1} \tag{64}
\end{align}

where (62) follows from (44). Thus, the amount of common randomness relative to the message size of any feasible SPIR scheme cannot be less than \(1/(N-1)\).

VI. CONCLUSION

For \(K\) messages and \(N\) databases, the capacity of SPIR was shown to be \(C = 1 - 1/N\). In order to achieve any positive rate for SPIR, the minimum amount of common randomness needed among the databases was shown to be \(1/(N-1)\) bits per message bit. Remarkably, this is also sufficient to achieve the capacity of SPIR.

REFERENCES

[1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private information retrieval,” in Proceedings of the 36th Annual Symposium on Foundations of Computer Science, 1995, pp. 41–50.
[2] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private Information Retrieval,” Journal of the ACM (JACM), vol. 45, no. 6, pp. 965–981, 1998.
[3] H. Sun and S. A. Jafar, “The Capacity of Private Information Retrieval,” arXiv preprint arXiv:1602.09134, 2016.
[4] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, “Protecting data privacy in private information retrieval schemes,” in Proceedings of the thirtieth annual ACM symposium on Theory of computing. ACM, 1998, pp. 151–160.
[5] W. Gasarch, “A Survey on Private Information Retrieval,” in Bulletin of the EATCS. Citeseer, 2004.
[6] S. Yekhanin, “Private Information Retrieval,” Communications of the ACM, vol. 53, no. 4, pp. 68–73, 2010.
[7] J. Katz and L. Trevisan, “On the efficiency of local decoding procedures for error-correcting codes,” in Proceedings of the thirty-second annual ACM symposium on Theory of computing. ACM, 2000, pp. 80–86.
[8] S. Yekhanin, “Locally Decodable Codes and Private Information Retrieval Schemes,” Ph.D. dissertation, Massachusetts Institute of Technology, 2007.
[9] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, “Batch codes and their applications,” in Proceedings of the thirty-sixth annual ACM symposium on Theory of computing. ACM, 2004, pp. 262–271.
[10] Y. Ishai and E. Kushilevitz, “On the hardness of information-theoretic multiparty computation,” in Advances in Cryptology-EUROCRYPT 2004. Springer, 2004, pp. 439–455.
[11] M. O. Rabin, “How to exchange secrets with oblivious transfer.” 1981.
[12] S. Even, O. Goldreich, and A. Lempel, “A randomized protocol for signing contracts,” Communications of the ACM, vol. 28, no. 6, pp. 637–647, 1985.
[13] J. Kilian, “Founding crytpography on oblivious transfer,” in Proceedings of the twentieth annual ACM symposium on Theory of computing. ACM, 1988, pp. 20–31.
[14] Y. Ishai, M. Prabhakaran, and A. Sahai, “Founding cryptography on oblivious transfer–efficiently,” in Annual International Cryptology Conference. Springer, 2008, pp. 572–591.
[15] R. Ahlswede and I. Csiszár, “On oblivious transfer capacity,” in Information Theory, Combinatorics, and Search Theory. Springer, 2013, pp. 145–166.
[16] A. C. Nascimento and A. Winter, “On the oblivious-transfer capacity of noisy resources,” IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2572–2581, 2008.