Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Efficient k-out-of-n oblivious transfer scheme with the ideal communication cost

Jianchang Lai [a,*], Yi Mu [a], Fuchun Guo [a,*], Rongmao Chen [b], Sha Ma [c]

[a] *Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, Australia*
[b] *College of Computer, National University of Defense Technology, Changsha, China*
[c] *College of Mathematics and Informatics, South China Agricultural University, Guangzhou, Guangdong, China*

ARTICLE INFO

Article history:
Received 22 April 2016
Received in revised form 14 December 2017
Accepted 18 December 2017
Available online xxxx
Communicated by G. Persiano

Keywords:
Oblivious transfer
Privacy
Minimum communication cost
Encryption

ABSTRACT

In this paper, we propose a two-round k-out-of-n oblivious transfer scheme with the minimum communication cost. In our proposed scheme, the messages sent by the receiver R to the sender S consist of only *three* elements, which is independent of n and k, while the messages from S to R are $(n+1)$ elements when the sender holds n secrets. Our scheme features a nice property of universal parameter, where the system parameter can be used by all senders and receivers. The proposed k-out-of-n oblivious transfer scheme is the most efficient two-round scheme in terms of the number of messages transferred between two communicating parties in known constructions. The scheme preserves the privacy of receiver's choice and sender's security.

1. Introduction

Oblivious transfer (OT) is one of the most important building blocks to construct secure and privacy-preserving protocols in cryptography, such as contract signing [11], private information retrieval [6] and secure function evaluation [12]. An oblivious transfer scheme is a two-party protocol between a *sender* S and a *receiver* R. The sender holds several secrets and the receiver wants to obtain some of them in the way that the receiver gets the secrets of his/her choice only, without revealing anything about his choice to the sender. The sender should not know which secrets are obtained by the receiver. The first OT scheme was proposed by Rabin [32], where the sender sends a secret to the receiver, and the receiver obtains the secret with probability 1/2. Even, Goldreich and Lempel [11] gave a more general OT scheme called 1-out-of-2 OT (OT_2^1) where the sender has two one-bit secrets (m_0, m_1). Brassard, Crépeau and Robert [4] extended the OT_2^1 to 1-out-of-n OT (OT_n^1) where the sender holds n secrets and the receiver wants to obtain one of them of its choice.

In OT schemes, one of the most general types is k-out-of-n oblivious transfer (OT_n^k), where the sender holds n different secrets and the receiver wants to obtain k $(k < n)$ secrets simultaneously.[1] As the large bandwidth resource is not always available and usually expensive, it is desired to reduce the total communication cost as much as possible during the communication. Many OT_n^k schemes [28,8,7,15,14,27,34] have been studied. In these schemes, the ideal communication rounds

* Corresponding authors.
E-mail addresses: jl967@uowmail.edu.au (J. Lai), ymu@uow.edu.au (Y. Mu), fuchun@uow.edu.au (F. Guo), rc517@uowmail.edu.au (R. Chen), sma@uow.edu.au (S. Ma).

[1] The OT_n^k scheme with such features is called *non-adaptive* OT_n^k.

https://doi.org/10.1016/j.tcs.2017.12.019
0304-3975/© 2017 Elsevier B.V. All rights reserved.

Table 1
Comparison of two-round OT_n^k schemes in terms of communication cost.

	System Parameter	Messages $(R \to S)$	Messages $(S \to R)$
Mu et al. [27]	$2n\|\mathbb{Z}_p\|$	$2n$	$2n$
Zhang and Wang [34]	$\|\mathbb{G}\|$	$k+3$	$2n$
Chu and Tzeng [8]	$\|\mathbb{G}\|$	k	$n+k+1$
Chu and Tzeng [7]	$\|\mathbb{G}\|$	k	$n+k$
Guo et al. [14]	$(n^2+3n+3)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	4	$3n$
Guo et al. [15]	$(n+1)\|\mathbb{G}\|$	3	$2n$
Ours	$(2n+2)\|\mathbb{G}\|$	3	$n+1$

can be two only. Supposing the indices of secrets and system parameters are known by the sender and the receiver, the receiver sends her/his choice as a request to the sender in the first round, then the sender should respond the request in the second round.[2]

From the state-of-art two-round OT_n^k schemes in the literature, the most efficient one with the minimum number of messages from R to S was proposed by Guo, Mu and Susilo in [15]. The authors first presented an efficient subset membership encryption scheme (SME) and applied the SME scheme to construct an efficient OT_n^k scheme. In their scheme, the receiver sends only three messages to the sender, which is independent of k and n. While the tradeoff is that the messages from S to R are $2n$, which is larger than the other OT_n^k schemes. Chu and Tzeng [7] proposed an efficient OT_n^k scheme based on [29]. Their scheme achieves the minimum number of messages from S to R, namely $n+k$, in the known constructions. But the messages from R to S in [7] are linear in the receiver's choice k.

1.1. Ideal communication cost

In the OT_n^k schemes with ideal communication rounds, as the sender holds n secrets and does not know the receiver's choice, S has to send the messages including n encrypted secrets to R. To decrypt the ciphertext successfully, the messages from S to R should be $O(n)$. For example, to encrypt a secret using ElGamal encryption, the ciphertext consists of two elements. One of them is used to recover the encryption key. Thus, in a secure OT_n^k scheme, the ideal communication cost is that the messages from R to S are constant which is independent of n and k, and the messages from S to R is $(n+1)$ in public key cryptosystems. The additional one element is used to recover the decryption keys. From the above, we note that both schemes in [15] and [7] cannot achieve ideal communication cost. The scheme in [15] achieves ideal communication cost from R to S, but cannot achieve that from S to R. While the scheme in [7] does not possess this property in any round. There are no existing known constructions of secure OT_n^k in the literature can achieve the ideal communication cost.

1.2. Our contributions

In this paper we propose the first two-round OT_n^k scheme with ideal communication cost; precisely, the messages from R to S are constant, with only *three* elements which are independent of n and k, and the messages from S to R contain $n+1$ elements. Compared with the two-round OT_n^k schemes in the literature, our proposed OT_n^k scheme is the most efficient one in terms of each round. The system parameter in our scheme is universal, which can be used by any users. We give an overview of the comparing results in Table 1.

In the first round, the receiver sends a token which contains the receiver's choice, and a proof information which is used to prove that its choice is not larger than k to the sender. In the second round, the sender responds with encrypted secrets after checking the validity of the received token. Finally, the receiver uses its choice set and secret key to decrypt the ciphertext and only retrieves the secrets whose indexes are in its choice set. To analyze the security of our proposed scheme, we propose two new assumptions and prove that our proposed assumptions are hard in the generic group model. Based on these two assumptions, we derive the security of our proposed scheme under three non-adaptive games and show that our scheme is unconditionally secure for receiver's choice and preserves the sender's security. Any choice larger than k can be detected easily by the sender. The tradeoff of our scheme is that the system parameter consists of $2n+2$ elements in the group $\mathbb{G}$.

1.3. Other related work

The notion of oblivious transfer was put forth by Rabin [32] to achieve secure two-party communication, and the author proposed a bit-OT protocol based on quadratic roots modulo a composite. Even et al. [11] extended this notion to OT_2^1, where the sender holds two one-bit secrets and the receiver would like to receive one of them of his choice. Brassard et

[2] We refer one communication (a flow of information transmission) between two parties as *one round* in this paper. Thus the ideal communication rounds OT schemes under this definition is "two-round" OT schemes.

Please cite this article in press as: J. Lai et al., Efficient k-out-of-n oblivious transfer scheme with the ideal communication cost, Theoret. Comput. Sci. (2018), https://doi.org/10.1016/j.tcs.2017.12.019