Several Oblivious Transfer Variants in Cut-and-Choose Scenario

Chuan Zhao, School of Computer Science and Technology, Shandong University, Jinan, China
Han Jiang, School of Computer Science and Technology, Shandong University, Jinan, China
Qiuliang Xu, School of Computer Science and Technology, Shandong University, Jinan, China
Xiaochao Wei, School of Computer Science and Technology, Shandong University, Jinan, China
Hao Wang, School of Computer Science and Technology, Shandong University, Jinan, China

ABSTRACT

Oblivious transfer is a fundamental tool in modern cryptography. In the past few years, many studies concentrate on oblivious transfer variants with more powerful functions. In this paper, the authors propose several variants of oblivious transfer in cut-and-choose scenario, providing multiple ways of transferring data in an oblivious manner. In addition, based on homomorphic encryption, the authors construct instantiations of these primitives, which can be proven secure in malicious model under ideal/real simulation paradigm and achieve the highest security level in the real world.

Keywords: Cut-and-Choose, Homomorphic Encryption, Ideal/Real Simulation Paradigm, Malicious Model, Oblivious Transfer, Oblivious Transfer Variant, Secure Two-Party Computation, Security Protocol

INTRODUCTION

The era of Big Data has arrived, and a plenty of new technologies, such as cloud computing and Internet of things, provide powerful instrument for data collection and processing. But at the same time, the privacy-preserving issue has caused extensive attention and anxiety. Ensuring data security and designing security protocols become an urgent task. As a fundamental tool of many typical security protocols, oblivious transfer plays a significant role in both theoretical research and practical applications.

DOI: 10.4018/IJISP.2015040101
Oblivious transfer is a two-party transfer task, where one party known as the sender provides several values, and the other party known as the receiver chooses some of them to receive. As a result, the receiver obtains the input values corresponding to its choice, without learning anything about the other values; while the sender learns nothing throughout. Oblivious transfer has received considerable attention from cryptographic research community since it is firstly introduced by Rabin (1981). In the follow-up studies, some works focus on designing more secure or efficient oblivious transfer protocols (Even, Goldreich, & Lempel, 1985; Crépeau, 1988; Camenisch & Neven, 2007; Peikert, Vaikuntanathan, & Waters, 2008); while many other works explore the possibility of variants with more powerful functions, such as committed oblivious transfer (Garay, MacKenzie, & Yang, 2004; Kiraz, Schoenmakers, & Villegas, 2007), committing oblivious transfer (Bellare & Micali 1990; Naor & Pinkas, 2001) and oblivious transfer extensions (Ishai, Kilian, Nissim, & Petran, 2003; Nielsen, Nordholt, Orlandi, & Burra, 2012; Asharov, Lindell, Schneider, & Zohner, 2013; Asharov, Lindell, Schneider, & Zohner, 2015) etc. These variants aim at improving the security or efficiency of the outer protocols that invoke them, or being applicable for different kinds of transfer tasks.

Among various of oblivious transfer variants, cut-and-choose oblivious transfer proposed by Lindell and Pinkas (2011) is a novel one. On the basis of 1-out-of-2 oblivious transfer, cut-and-choose oblivious transfer introduces for the receiver a cut-and-choose index bit, which indicates whether the receiver chooses to obtain both input values or just one of them. With this variant applied in secure two-party computation protocols based on cut-and-choose paradigm, oblivious transfer and circuit checks are intertwined and the problem of selective failure attack pointed out by Kiraz and Schoenmakers (2006) is solved. However, cut-and-choose oblivious transfer can only be used to transfer the garbled keys associated with one party’s circuit input wires. It still needs many rounds of interactions between the two parties to transfer the corresponding garbled keys of the other party. Apparently the round complexity of secure computation protocols based on this primitive is high.

Inspired by the work of Lindell and Pinkas (2011), we propose two additional variants in cut-and-choose scenario. One is an “inverted” version of cut-and-choose oblivious transfer, which we call “cut-and-choose inverted oblivious transfer”. The word “inverted” means that it is the sender, rather than the receiver, has the choice bit. It is an interesting new primitive and can be applied to many cut-and-choose scenarios. The other one is a “bilateral” version, and we call it “cut-and-choose bilateral oblivious transfer”. In this primitive, both parties have a choice bit and the sender accordingly has two pairs of input values. Compared with cut-and-choose oblivious transfer, cut-and-choose bilateral oblivious transfer is much more powerful. When applied in secure computation protocols, this new primitive can transfer all necessary data in only one phase. As a result, the round complexity is significantly decreased.

The major contributions of this paper consist of the following:

1. Several variants of oblivious transfer in cut-and-choose scenario are proposed, which provide multiple means of transferring data in an oblivious manner, enabling the participants to accomplish different kinds of transfer tasks on the Internet. Furthermore, when invoked in security protocols based on cut-and-choose paradigm, cut-and-choose bilateral oblivious transfer helps to simplify the protocol framework and reduce the round complexity of the outer protocols;
2. Based on homomorphic encryption, the instantiations of the proposed variants as well as cut-and-choose oblivious transfer are constructed. These protocols can be proven secure in malicious model under ideal/real simulation paradigm, which implies the highest security level in the real world.
10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

[www.igi-global.com/article/several-oblivious-transfer-variants-in-cut-and-choose-scenario/148063?camid=4v1](www.igi-global.com/article/several-oblivious-transfer-variants-in-cut-and_choose-scenario/148063?camid=4v1)


[www.igi-global.com/e-resources/library_recommendation/?id=2](www.igi-global.com/e-resources/library_recommendation/?id=2)

Related Content

A Projection of the Future Effects of Quantum Computation on Information Privacy
[w](www.igi-global.com/article/projection-future-effects-quantum_computation/2463?camid=4v1a)

Social and Health Risks of Female Genital Mutilation for Medication and Braveness
[w](www.igi-global.com/article/social-and-health-risks-of-female-genital-mutilation-for-medication-and-braveness/191217?camid=4v1a)
Ensuring Privacy and Confidentiality in Digital Video Surveillance Systems
www.igi-global.com/chapter/ensuring-privacy-confidentiality-digital-video/61503?camid=4v1a

Addressing Covert Channel Attacks in RFID-Enabled Supply Chains
www.igi-global.com/chapter/addressing-covert-channel-attacks-rfid/75518?camid=4v1a