Information Sciences 466 (2018) 44–54

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Secure rational numbers equivalence test based on threshold cryptosystem with rational numbers☆

Linming Gong[a], Bo Yang[b,*], Tao Xue[a], Jinguang Chen[a], Wei Wang[a]

[a] *The Shaanxi Key Laboratory of Clothing Intelligence, and the National and Local Joint Engineering Research Center for Advanced Networking & Intelligent Information Service, School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China*
[b] *School of Computer Science, Shaanxi Normal University, Xi'an 710062, China*

ARTICLE INFO

Article history:
Received 3 December 2017
Revised 16 July 2018
Accepted 24 July 2018
Available online 26 July 2018

Keywords:
Online collaboration
Secure equivalence test based on rational numbers
Standard (ideal/real) model
Threshold cryptosystem with rational numbers

ABSTRACT

In this study, we consider an equivalence test on rational numbers in a scenario with $K+2$ distributed parties, Alice, Bob, $P_1, P_2, \ldots, P_K$, where Alice has a private rational number x_a, Bob has a private rational number x_b, and party P_i has a secret s_i, where $i \in \{1, 2, \ldots, K\}$, $K \geq 2$. The parties want to cooperatively detect whether $x_a = x_b$ without revealing any information about their secrets. This problem has many applications in online collaboration, such as e-voting, which requires public verifiability. First, we develop a provably secure threshold cryptosystem for rational numbers. Next, based on the proposed threshold scheme, we construct a distributed plaintext equivalence test protocol in an honest majority environment. We prove that the proposed protocol is secure and robust in the standard (ideal/real) model.

1. Introduction

In this study, we consider the following scenario. $K+2$ parties, $\{P_i\}_{i=1,2,\ldots,K}$, Alice and Bob, with private inputs $\{s_i\}_{i=1,2,\ldots,K}$, x_a and x_b, respectively, want to cooperatively test whether $x_a = x_b$ (where s_i is a share of the private key of our threshold encryption scheme for rational numbers, and x_a and x_b are two rational numbers) under a limiting condition that none of them can learn anything about each other's private inputs. This scenario is known as the distributed plaintext equivalence test (PET), which is a special instance of secure multi-party computation [1,8,10–14,16,17,19,20,24,27,28,31]. The distributed PET is useful for applications such as e-voting [4], privacy preservation [2,29,33], private proximity testing [15], or verifying secrets [22,26].

The distributed PET was first proposed by Jakobsson and Juels [13] to test whether two plaintexts are equal based on the ElGamal encryptions but without disclosing the two plaintexts. The distributed PET can be defined briefly as follows.

(1) Each of the parties $\{P_i\}_{1,\,2,\ldots,\,K}$ first calculates $\hat{C}_i = (\frac{\hat{c}_1}{\hat{c}_2})^{r_i}$ and $\check{C}_i = (\frac{\check{c}_1}{\check{c}_2})^{r_i}$ using a random number $r_i \in Z_q^*$, where $c_1 = (\hat{c}_1, \check{c}_1)$ and $c_2 = (\hat{c}_2, \check{c}_2)$ are two ElGamal ciphertexts of x_a and x_b. They then publish $C_i = (\hat{C}_i, \check{C}_i)$.
(2) Each party computes $\tilde{C} = (\prod_{i=1}^{K} \hat{C}_i, \prod_{i=1}^{K} \check{C}_i)$. The K parties then jointly decrypt $\tilde{C}$. If $Dec(\tilde{C}) = 1$, then $x_a = x_b$.

☆ Supported by the National Natural Science Foundation of China (Grant Nos. 61572303 and 61601358), Nature Science Foundation of Shaanxi Province (Grant No. 2016Jm6030), Scientific Research Program funded by Shaanxi Provincial Education Department (Grant No. 2017JK0329), and the PhD Science Foundation of Xi'an Polytechnic University (Grant No. 107020331).

* Corresponding author.
E-mail address: byang@snnu.edu.cn (B. Yang).

https://doi.org/10.1016/j.ins.2018.07.046
0020-0255/© 2018 Elsevier Inc. All rights reserved.

This protocol is secure if less than t users are colluding. Several applications have been developed based on this method, such as those by [1,8,19]. In 2005, Li and Wu [16] proposed a three-party private equality test based on the Paillier cryptosystem. In 2008, Ting and Huang [27] extended the method of Li and Wu [16] to a multi-party distributed equivalence test protocol. In 2010, Yang et al. [32] presented an equivalence test protocol based on probabilistic public key encryption. Recently, this method was applied to some other interesting cases, such as those given by [18,31].

The protocols mentioned above can elegantly solve the PET problem, but they still have some limitations. First, they can only solve the PET with integers. Second, the Paillier encryption scheme was utilized incorrectly in some studies, such as that by [27], where the ciphertext $c_1 = g^{m_1} r_1^n \bmod n^2$ divided by the ciphertext $c_2 = g^{m_2} r_2^n \bmod n^2$ was incorrectly treated as a ciphertext of $m_1 - m_2$, i.e.,

$$\frac{c_1}{c_2} = \frac{g^{m_1} r_1^n \bmod n^2}{g^{m_2} r_2^n \bmod n^2} = g^{m_1 - m_2}(r_1 r_2^{-1})^n \bmod n^2.$$

Remark on the incorrect utilization of the Paillier encryption scheme: According to **Lemma 3** in the Paillier scheme [21] ($\mathbb{B}_\alpha \in Z_{n^2}$ is denoted by the set of elements of order $n\alpha$ and by $\mathbb{B}$ their disjoint union for $\alpha = 1, 2, \ldots, \lambda$), if $x \in Z_n$, $y \in Z_n^*$ and $g \in \mathbb{B}$, then Paillier's encryption function $z = g^x y^n \bmod n^2$ is bijective. Thus, for $g \in \mathbb{B}$ and $z \in Z_{n^2}$, the n-th residuosity class of z with respect to g is the unique integer $x \in Z_n$ for which $y \in Z_n^*$ exists such that $z = g^x y^n \bmod n^2$. $c_1 = g^{m_1} r_1^n \bmod n^2$ and $c_2 = g^{m_2} r_2^n \bmod n^2$ are two integers in $Z_{n^2}^*$, so obviously, $\frac{c_1}{c_2} = \frac{g^{m_1} r_1^n \bmod n^2}{g^{m_2} r_2^n \bmod n^2}$ is not an integer, except when $c_1 = \gamma c_2$, where $\gamma c_2 < n^2$. Hence, for $\frac{c_1}{c_2}$, no pair $(\tilde{x}, \tilde{y})$ may exist with a high probability such that $\frac{c_1}{c_2} = g^{\tilde{x}} \tilde{y}^n \bmod n^2$.

Therefore, it is not correct to evaluate the ciphertext of $m_1 - m_2$ by employing the method given above ($\frac{c_1}{c_2} = g^{m_1 - m_2}(r_1 r_2^{-1})^n \bmod n^2$).

In the present study, in order to avoid the incorrect utilization of the Paillier encryption scheme and to test whether two rational numbers are equal, we first construct a threshold encryption scheme for rational numbers. Based on this threshold encryption, we develop a distributed private equivalence test protocol, where $K+2$ parties jointly test whether $x_a = x_b$ (where x_a, x_b are rational numbers that belong to Alice and Bob, respectively) given that $\{P_i\}_{i=1,2,\ldots,K}$, and Alice and Bob cannot learn anything about other's private inputs. This protocol is efficient and secure with an honest majority assumption, and we prove its security in a formal secure multi-party computation framework [[9], Chap. 7].

2. Building blocks and primitives

2.1. Adversary model and security definition for secure multiparty computation

Adversary model. We prove the security of the distributed PET protocol in the secure multiparty computation model according to [5,9,25]. Thus, the privacy of the participants in the protocol is defined in terms of the different views of the participants with respect to the real-life model and the ideal model.

In the real model, all of the participants jointly conduct the real protocol under attacks from the adversary $\mathcal{A}$ who fully controls $t-1$ participants $\{P_i\}_{i=1,2,\ldots,t-1}$ as he wishes. At the end of the protocol, all of the participants should output exactly what the protocol specifies, and $\mathcal{A}$ outputs arbitrary functions (denoted by $V_{\mathcal{A}}$) of their joint views.

In the ideal model, all of the participants first deliver their private inputs to a fully trusted party $\mathbf{P}_{Trust}$. Next, $\mathbf{P}_{Trust}$ privately evaluates the functional values that should be exported by each participant in the specified protocol, and then sends the evaluated functional values to each participant. The adversary $\mathcal{A}$ fully controls $t-1$ participants $\{P_i\}_{i=1,2,\ldots,t-1}$ with the same index used in the real model. All of the participants output their received values, and the adversary $\mathcal{A}$ outputs arbitrary functions (denoted by $V_{\mathcal{A}}$) of their joint views.

Definition 1. A PET protocol with $K+2$ participants is secure with an honest majority if for any probabilistic polynomial-time adversary $\mathcal{A}$ who fully controls $t-1$ ($t = \frac{K}{2}$) participants such that for $2K+2$ private inputs $x_a, x_b, x_1, x_2, \ldots, x_K, x_1', x_2', \ldots, x_K'$, the distribution $(X_a(x_a)$, $X_b(x_b)$, $X_1(x_1)$, $X_2(x_2)$, $\ldots, X_K(x_K), V_{\mathcal{A}})_{real}$ and the distribution $(X_a(x_a), X_b(x_b), X_1(x_1'), X_2(x_2'), \ldots,$ $X_K(x_K'), V_{\mathcal{A}})_{ideal}$ are computationally indistinguishable. $X_a(x_a)$, $X_b(x_b)$ are the outputs of Alice and Bob, respectively, and $X_i(x_i), X_i(x_i')$ are the outputs of P_i from the real and ideal models.

2.2. Paillier encryption scheme

The Paillier encryption scheme $\mathcal{E}_P(\mathcal{G}, \mathtt{Enc}, \mathtt{Dec})$ [21] has the additive homomorphism (for all m_1, $m_2 \in Z_n$ and $k \in \mathbb{N}$):

$$E_{pk}(m_1) E_{pk}(m_2) \bmod n^2 = E_{pk}(m_1 + m_2), \tag{1}$$

$$\begin{aligned} E_{pk}(k \cdot m \bmod n) &= E_{pk}^k(m \bmod n) \bmod n^2 \\ &= E_{pk}^m(k \bmod n) \bmod n^2, \end{aligned} \tag{2}$$

which is essential for the design of the homomorphic tallying process for many multiparty secure computing protocols. We briefly summarize this scheme in Fig. 1, where p and q are two big prime numbers with equal length, $n = pq$, $\lambda = \mathrm{lcm}(p-1, q-1)$, $g = 1 + kn$ ($k \in Z_n^*$), $L(\cdot) = \frac{U-1}{n} (0 < U < n^2)$, and m, r are integers.