Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

# Information-theoretic secure rational secret sharing in asynchronous networks for untrusted cloud environments

Chingfang Hsu[1*], Lein Harn[2], Zhe Xia[3], Linyan Bai[1] and Ze Zhang[1]

**Abstract**

Today, cloud storage services increased the popular for data storage in the cloud and retrieve from any location without any time limitations. One of the most important demands required in cloud is secured data transmission in un-trusted cloud applications. Particularly, secure and efficient multiparty communications in Untrusted Cloud Environments (UCE) attract widespread attentions. The equipment used in UCE have the particularity of being heterogeneous and UCE communication environment are asynchronous networks in which multiple users cannot transmit their messages simultaneously. How to ensure secure communication between these heterogeneous intelligent devices is a major challenge for multiparty communication applied in UCE. In such an asynchronous environment, the asynchronous transmission can cause security problems in cryptographic functions. Therefore, how to implement rational secret sharing (RSS) in an asynchronous model of the UCE networks has become a burning research topic. The RSS refers to finding a solution composed of strategies to encourage players in the secret reconstruction to act honestly even players are rational to act for their own interest. If each player plays the game for the best response to the best response of other players, the game is in Nash equilibrium. The objective of an RSS is to achieve the Nash equilibrium state corresponding to the global optima. In this paper, we propose an information-theoretic secure RSS in asynchronous model for UCE. Our design uses Petersen's VSS to allow every player to divide his share into multiple pieces for other players. Then, shares can be revealed asynchronously. If any player acts maliciously, his share can be recovered by other players. This feature can encourage players to act honestly since any malicious action (i.e., either revealing a fake share or refusing to release one) is useless. Our scheme is practically valuable for secure group-oriented applications in UCE.

**Keywords:** Rational secret sharing, Verifiable secret sharing, Asynchronous model, Information-theoretic secure, UCE, Secure group-oriented applications

## Introduction

The rapid development of the Internet has brought people close together, and on this basis, it has been extended and expanded into the Internet of Things (IoT), that is, the Internet of all things connected [1–4]. As an emerging technology, the Internet of Things has effectively promoted the intelligent development of industry, agriculture, transportation and other aspects. Applications in smart home, pollution monitoring, medical health, and other fields closely related to life have greatly improved people's quality of life. Group-oriented technology shows its application potential in IoT. For example, the data collected jointly by using group-oriented technology can be used to analyze traffic conditions and realize multi-user interactive computing. As these group-oriented programs are applied on open and insecure networks, they face the need for security.

*Correspondence: cherryjingfang@gmail.com

[1] Computer School, Central China Normal University, Wuhan 430079, China
Full list of author information is available at the end of the article

At the same time, cloud computing services are more popular for data storage and retrieval in the cloud environment. Because of the user's data security, the encrypted data is persisted in the cloud to protect from permission denied users. The method considers cloud services provider (CSP) or trusted authority to take care the key management assurance like an "it confirmed that key cannot be compromised". However, some entities may interrupt communications between users and CSP. Hence, it compels the CSP to release user secrecy. In cloud surroundings, data holders, store data on the clouds which are transmitted through the deniable encryption scheme. Therefore, secure and efficient multiparty communications in Untrusted Cloud Environments (UCE) attract widespread attentions [5–9].

With the development of these technologies, more and more advanced companies are adopting the IoT and tend to transform to the intelligent systems (IS) to achieve high performance with less risk. IS refers to the application of smart devices with perception technology, data processing technology, and network communication technology to all links of intelligent transportation devices, which are connected through the network to achieve efficient utilization of resources, improve product quality and reduce resource consumption, thus realizing transportation intelligence. The devices in the IS have the particularity of heterogeneity, and the IS communication is carried out in an untrusted cloud environment, which is an asynchronous network, that is, multiple users cannot transmit their messages simultaneously. In such an Untrusted Cloud Environment (UCE), ensuring secure communication between these heterogeneous transportation devices is a major challenge for multiparty communication applied in IS, which is shown in Fig. 1. Furthermore, in such an asynchronous environment, the asynchronous transmission can cause security problems in cryptographic functions. How to make implementation of rational secret sharing (RSS) in an asynchronous model for UCE has become a burning research topic.

The $(t,n)$ secret sharing scheme (SS) refers to dividing the secret into $n$ sub-secrets so that the secret can be recovered when any $t$ or more sub-secrets are known, but when the number of known sub-secrets is less than $t$, no information about the secret can be obtained. The SS has become a building block in many current cryptographic applications. There are multiple technologies that can be used to achieve secret sharing. For instance, Shamir [10] designed a $(k,n)$ threshold scheme using linear polynomial, Azimuth-Bloom [11] studied the secret sharing scheme based on the Chinese Remainder Theorem (CRT), and Blakely [12] introduced a secret sharing scheme using hyperplane geometry. Among them, Shamir's SS has been received most attention. This is because his SS is flexible and efficient, and it is information-theoretic secure.

If $t$ or more sub-secrets are known, Shamir's SS can reconstruct the secret using Lagrange Interpolation formula, and this process is very simple. However, in 2004, Halpern and Teague [13] have proposed the concept of *Rational SS (RSS)*. In an RSS, it assumes that the players in the game of secret reconstruction are rational. In other words, each player may be honest or malicious.

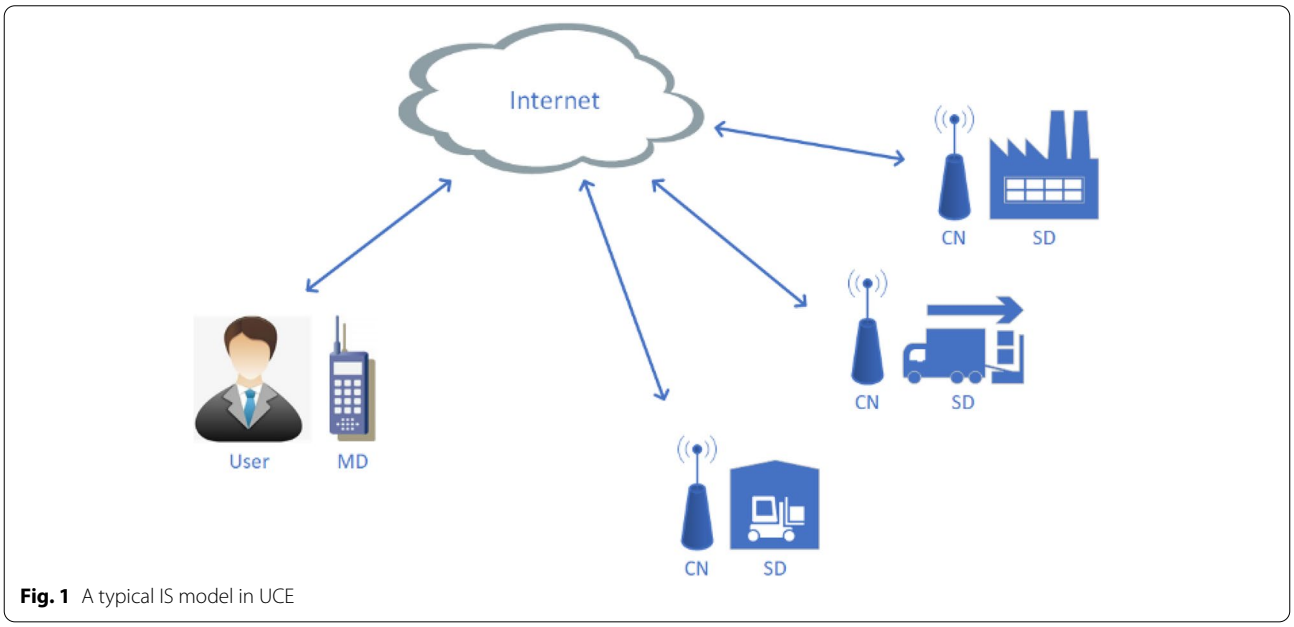


**Fig. 1** A typical IS model in UCE

The players in the secret reconstruction aim to maximize their own interests and take corresponding actions. The objective of an RSS is to find a solution that is composed of strategies to encourage players in the secret reconstruction to act honestly even players are rational to act for their own interest. If each player plays the game for the best response to the best response of other players, the game is in Nash equilibrium. Achieving the Nash equilibrium state corresponding to the global optima is the goal of an RSS. Halpern and Teague [13] have shown that Shamir's SS is not an RSS. This can be easily understood. Suppose there are $t$ players in the secret reconstruction, if one of them is malicious and he publishes a false sub-secret, at the same time, all other honest players publish valid sub-secrets, then only this malicious player can reconstruct the secret, while no other honest player has access to the secret. This is not an equilibrium state.

Many researchers have proposed RSS schemes [14–16]. In these schemes, players can only exchange information in a synchronized channel. Since the synchronous channel is difficult to be implemented in practice, the existing communication networks are asynchronous networks in which multiple users cannot transmit their messages simultaneously. The asynchronous transmission can cause security problems. Therefore, it is imminent to implement RSS in the asynchronous model. Up to now, there are very few RSS solutions designed for asynchronous channels, including those designed by Maleka et al. [17], designed by Fuchsbauer et al. [14], designed by Ong et al. [15], and designed by Moses et al. [18]. In [17], the game needs to be repeated and an interactive dealer is required [14]. requires the use of cryptographic primitives. In [15, 18], multiple rounds of the game are played and a certain number of players are assumed to be honest.

In 1995, Lin et al. [19] presented a fair secret reconstruction scheme suitable for asynchronous models. In this scheme, the secret $s$ is hidden in the sequence, $\{d_1, d_2, \ldots, d_{j-1}, d_j, d_{j+1}, \ldots, d_k\}$, and it can be reconstructed as a whole in the asynchronous network, where $d_j = s$, $d_{j+1} = D$, $D$ is public, and $d_i$, $i \neq j$, $j+1, \forall i$, is random integer. Furthermore, Maleka et al. [20] first proposed the concept of repeated games in the RSS problem and proved that limited repeated games are impossible when the player knows the number of repetitions of the game. In [19], instead of requiring all players to release their sub-secrets at the same time, the secret reconstruction process restores one element at a time in the order of the sequence until the secret is derived. If the certificate and sub-secret submitted by the player pass the verification, the rebuild process continues down the line, otherwise it is forced to stop. Until $D$ is restored, the players can be sure that the previous restoration is the secret. In addition, it should be noted that if the player correctly guesses the location of the secret, he can get exclusive access to the secret. Then the probability that this malicious player has exclusive access to the secret and other honest players cannot obtain the secret is $\frac{1}{k}$. In a recent paper [17], the scheme has been improved to include some other features.

In this paper, we propose an RSS protocol which uses VSS for secure group communications in UCE, one of the most popular cryptographic primitives, as a strategy to enforce all players in the secret reconstruction to act honestly to reach the Nash equilibrium state. Our proposed RSS is information-theoretic secure. And it has two phases. In the first phase, each player acts as the dealer in Peterson's VSS [21] to divide his/her share into sub-shares for other players. In addition, the player needs to make Peterson's commitments publicly known. Using these commitments, these sub-shares can be verified. After all sub-shares of players being verified successfully, the scheme is advanced into the second phase. In the second phase, players take turn to reveal their shares asynchronously. Each revealed share can be verified separately. If any share has been verified unsuccessfully, other players can work together to recover the share. Since each share has been shared by other players in the first phase, this feature encourages players to reveal their shares honestly in the second phase. In other words, if players release fake shares in the second phase, their "real" shares can still be recovered by other honest players. The main contributions of this paper are as follows.

- An information-theoretic secure RSS in asynchronous model is proposed.
- The RSS uses Peterson's VSS as building block. It allows every player to divide his share into multiple pieces for other players. Then, shares can be revealed asynchronously. If any player acts maliciously, his share can be recovered by other players.
- The RSS is deterministic and simple. This unique feature can encourage players to act honestly since any malicious action (i.e., either revealing a fake share or refusing to release one) is useless.

The rest of paper is organized as follows. Petersen's VSS is reviewed in Review of Petersen's VSS section. Model section introduces the model of the presented protocol, including protocol description, type of attacks. In Proposed scheme section, our RSS scheme is proposed. Analysis section analyzes the security of RSS. We conclude this paper in Conclusion section.

## Review of Petersen's VSS

Our proposed RSS is designed on the basis of Pedersen's VSS [21]. We review this protocol in this section.

The notion of VSS was proposed by Chor et al. [22], which means that participants can verify whether the received sub-secret is valid without revealing their own secrets. We give a definition of VSS below.

### Definition 1. T-out-of-n Verifiable Secret Sharing Scheme (VSS)

A t-out-of-n verifiable secret sharing scheme $\pi = (G, R, V)$ consists of a sharing algorithm G, a reconstruction algorithm R, and a verification algorithm V. The sharing algorithm G ensures that no adversary can reconstruct the secret from less than t shares. The reconstruction algorithm G guarantees that participants can reconstruct the secret based on any t or more known shares. The verification algorithm V enables participants to verify that their shares are generated consistently while ensuring the security of their shares and secrets.

Benaloh [23] proposed an interactive VSS. Cryptographic commitment schemes have been used in Feldman [24] and Pedersen [21] VSSs. The scheme in [24] is proven to be bitwise safe, using the difficulty of discrete logarithms. And the scheme in [21] ensures unconditionally the security of the secret, in which the correctness of the sub-secret depends on the calculation assumptions. However, in addition to verifying the validity of the participant's own sub-secret, these VSS schemes cannot verify the sub-secrets of other participants. Stadler [25] first presented a publicly verifiable secret sharing (PVSS) scheme, which ensures that the validity of a participant's sub-secret can be verified by other participants. Subsequently, Schoenmaker [26] made improvements on the basis of the PVSS scheme proposed by Stadler, using the standard Diffie-Hellman difficult hypothesis. Peng and Wang [27] applied the model designed by Schoenmaker to construct a PVSS solution based on linear code. A PVSS protocol based on Pailler's encryption [28] was proposed by Ruiz and Villar [29]. In addition, non-interactive PVSS scheme using bilinear mapping have been presented [30, 31].

Pedersen's VSS is information-theoretic secure. There are public parameters, $g$, $h \in Z_p$, and assumes that no one knows $log_g h$. Pedersen's VSS uses the following commitment scheme.

#### Pedersen's commitment scheme

To commit the secret $s$, the dealer computes and publishes a commitment $E(s,k) = g^s h^k = E_0 \, mod \, p$, where $k \in Z_p$ and $k$ is randomly selected. Such a commitment can later be opened by releasing $s$ and $k$.

The Pedersen's VSS is shown in Fig. 2.

## Model

### Description of our proposed RSS

Our proposed RSS has two phases. In the first phase, each player is regarded as a dealer in Peterson's VSS [21] to divide his/her share into sub-shares for other players. The sub-shares can be verified by other players. In this phase, all sub-shares of players need to be verified successfully. In the second phase, players take turn to reveal their shares asynchronously. Each revealed share can be verified separately. If any share has been verified unsuccessfully, other players can work together to use their sub-shares obtained in the first phase to recover

***Share generation***

To commit the secret $s$, the dealer computes and publishes a commitment $E(s,k) = g^s h^k = E_0 \, mod \, p$, where $k$ is a random integer with $k \in Z_p$. Then, the dealer randomly selects two polynomials, $f(x) = s + a_1 x + \cdots + a_{t-1} x^{t-1} \, mod \, p$ and $g(x) = k + b_1 x + \cdots + b_{t-1} x^{t-1} \, mod \, p$, with degree $t-1$ and $f(0) = s$ and $g(0) = k$. Dealer generates shares, $\left(f(x_j), g(x_j)\right), j = 1,2,\cdots,n$, of users. The dealer computes and publishes commitments of the above two polynomial coefficients, and this commitment is recorded as $E(a_i, b_i) = g^{a_i} h^{b_i} \, mod \, p = E_i, i = 1,2,\cdots,t-1$, where $E(a_i, b_i)$ is Petersen's commitment.

***Share verification***

User $U_i$ can verify each pair of shares $\left(f(x_i), g(x_i)\right)$ by checking whether $E\left(f(x_i), g(x_i)\right) \stackrel{?}{=} \prod_{j=0}^{t-1} E_j^{x_i^j} \, mod \, p$. If it passes the test, the user is convinced that the pair of shares is generated consistently.

***Secret reconstruction***

When the shares $\left\{f(x_{i_1}), f(x_{i_2}), \cdots, f\left(x_{i_j}\right)\right\}$ owned by $j$ (i.e., $t \le j \le n$) shareholders are known, the secret can be recovered by calculating $s = f(0) = \sum_{r=1}^{j} f(x_{i_r}) \prod_{v=1, v \ne r}^{j} \frac{-x_{i_v}}{x_{i_r} - x_{i_v}} \, mod \, p$.

**Fig. 2** Pedersen's VSS

the share. This feature encourages players to reveal their shares honestly in the second phase.

#### Entities and possible attacks

In a VSS, the owner of the secret is the *prover* and all other users are the *verifiers*. In the case of ensuring the security of the secret, the verifiers want to verify that the shares they get are generated consistently. In Pedersen's VSS, verification is based on the commitments computed by the owner of the secret. Each verifier can verify the share individually without interaction. Inconsistent shares may be generated due to the following two reasons: (a) in shares generation/distribution, nature noise, such as transmission noise or computational error, may cause the inconsistency; (b) inconsistent shares may be generated by a user who tries to cheat other honest users.

Attackers may try to obtain secrets from commitments. Pedersen's commitment can prevent this attack. Moreover, it is necessary to prevent malicious players from attacking in the process of rebuilding the secret. In our RSS, all information exchanged among players is transmitted through an asynchronous channel. To prevent players from revealing their shares last in the process and knowing the secret by themselves only, there are two phases in our presented RSS. In the first phase, every player needs to follow Petersen's VSS and act as a dealer to divide his own share (the secret) for other players. The generated shares of his own share are called the *sub-shares*. Each sub-share is sent to individual player secretly. Some public commitments of the secret need to make publicly known. Each sub-share also needs to be verified successfully by each player. Only after all sub-shares being successfully verified, the scheme advances in the second phase.

The shares of players are released asynchronously in the second phase. Since each revealed share can be verified based on the VSS commitments generated in the first phase and any fake share can also be recovered by other players based on their sub-shares, this feature encourages players to act honest.

#### Properties

Our proposed RSS has the following properties:

*Secrecy.* From the commitment of the secret and shares, it is impossible for the secret to be restored by the attackers.

*Fairness.* The RSS needs to have strategies to encourage players in the secret reconstruction to act honestly. If players act dishonestly then all players either get no secret or get the secret.

*Efficiency.* In our proposed RSS, we use Pedersen's VSS [21] based on polynomials. In the first phase, each user needs to act as a dealer to compute sub-shares for other players and compute some public commitments. There has no interaction among users to verify shares in Petersen's VSS.

*Un-deniability.* In the process to reveal shares in Phase 2, no player can deny to release his share since share can be recovered by other players based on sub-shares distributed in the first phase.

## Proposed scheme

### RSS scheme

Suppose there are $n$ players, $U=\{U_1, U_2, ..., U_n\}$, participated in the RSS. The scheme is introduced in detail in Fig. 3.

#### Discussion

The proposed RSS scheme is composed of three algorithms, namely share generation, share verification and secret reconstruction.

##### *Share generation and share verification*

The first two algorithms are identical to the Petersen's VSS except that for each shares, $(f(x_i), g(x_i))$, of player, $U_i$, the dealer computes $E\left(f(x_i), g(x_i)\right) = g^{f(x_i)}h^{g(x_i)} = E_0^i \bmod p, i = 1, 2, \ldots, n$. It is worth noting that in the first stage, each player needs to allocate his shares to other players The reason why these public commitment values of player's shares are published by the dealer is to prevent players from cheating by generating sub-shares of fake shares.

##### *Secret reconstruction*

It consists two phases, generating sub-shares and commitments phase, and revealing shares.

##### *Phase 1: generating sub-shares and commitments phase*

In this phase, each player needs to act as the dealer to follow Petersen's VSS to divide his own shares. Players' own shares are treated as secrets and sub-shares are allocated to other players. From commitments published by the dealer and the owner of shares, sub-shares can be verified to be generated consistently.

##### *Phase 2: revealing shares phase*

In this phase, shares of players are revealed asynchronously. Each revealed share can be verified based on the commitments published by the dealer in *share generation.* If any revealed share cannot be verified successfully or any player refuses to reveal his share, share can still be recovered by sub-shares of other players. Note that each revealed sub-shares can also be verified by other players since the shares are generated following Petersen's VSS in

***Share generation***

The dealer follows Petersen's VSS to generate shares and commitments of the secret $s$. To commit $s$, the dealer computes and publishes a commitment $E(s,k) = g^s h^k = E_0 \, mod \, p$, where $k \in Z_p$ and $k$ is randomly selected. At the end of this phase, each player $U_i$ receives shares, $\big(f(x_i), g(x_i)\big)$, from the dealer. The dealer calculates and publishes commitments of the above two polynomial coefficients, and this commitment is recorded as $E(a_i, b_i) = g^{a_i} h^{b_i} \, mod \, p = E_i$, $i = 1,2,\cdots, t-1$. Furthermore, the for each share, $\big(f(x_i), g(x_i)\big)$, of player $U_i$, the dealer computes and publishes $E\big(f(x_i), g(x_i)\big) = g^{f(x_i)} h^{g(x_i)} = E_0^i \, mod \, p$, $i = 1,2,\cdots, n$.

***Share verification***

User $U_i$ can verify each pair of shares $\big(f(x_i), g(x_i)\big)$ by checking whether $E\big(f(x_i), g(x_i)\big) \stackrel{?}{=} \prod_{j=0}^{t-1} E_j^{x_i^j} \, mod \, p$. If it passes the test, the player is convinced that the pair of shares is generated consistently; otherwise, player, $U_i$ requests the dealer to re-generate shares.

***Secret reconstruction***

**Phase 1: Generating sub-shares and commitments phase**

Each player $U_i$, follows Petersen's VSS to generate sub-shares and commitments of the share $\big(f(x_j), g(x_j)\big)$. Furthermore, all sub-shares need to be verified successfully. If there is any sub-share cannot be verified successfully, new sub-shares need to be re-generated by the owner of the share.

Step 1. Each player $U_i$, randomly selects two polynomials, $f^i(x) = f(x_i) + a_1^i x + \cdots + a_{k-1}^i x^{k-1} mod \, p$ and $g^i(x) = g(x_i) + b_1^i x + \cdots + b_{k-1}^i x^{k-1} mod \, p$, with degree $k-1$ and $f^i(0) = f(x_i)$, $g^i(0) = g(x_i)$. $U_i$ allocates sub-shares $\big(f^i(x_j), g^i(x_j)\big)$, $j = 1,2,\cdots, n$, to other players. And then, $U_i$ computes and publishes commitments to the coefficients of $f^i(x)$ and $g^i(x)$, which are recorded as $E\big(a_j^i, b_j^i\big) = g^{a_j^i} h^{b_j^i} \, mod \, p = E_i$, $j = 1,2,\cdots, k-1$.

Step 2. $U_i$ verifies the legality of sub-shares $\big(f^j(x_i), g^j(x_i)\big)$, received from other player $U_j$ by checking $E\big(f^j(x_i), g^j(x_i)\big) \stackrel{?}{=} E_0^j \prod_{l=1}^{k-1} E_l^{x_i^l} \, mod \, p$, for $j = 1,2,\cdots, n$, $j \neq i$. If the verification fails, $U_i$ requests $U_j$ to re-generate new sub-shares.

**Phase 2: Revealing shares phase**

***Only after all sub-shares being verified successfully, the scheme is advanced into this phase.***

Step 1. Each player $U_i$ reveals its share, $\big(f(x_i), g(x_i)\big)$, to other players in a broadcast channel.

Step 2. After receiving $\big(f(x_i), g(x_i)\big)$ from $U_i$, every other player $U_j$, $j \neq i$, follows same procedure as described in ***Share verification*** to verify the pair of shares. If this verification is unsuccessful or any player refuses to reveal his share, then all other players work together to recover this pair of shares by revealing their sub-shares, $\big(f^i(x_j), g^i(x_j)\big)$, $j = 1,2,\cdots, n$, in the first phase. Note that each revealed sub-shares can also be verified by other players since the shares are generated following Petersen's VSS in the first phase.

Step 3. After recovering the complete set of valid shares, $f(x_i)$, $i = 1,2,\cdots, n$, the secret can be easily obtained by calculating $\sum_{i=1}^{n} f(x_i) \prod_{v=1, v\neq i}^{n} \frac{-x_v}{x_i - x_v} \, mod \, p = f(0) = s$.

**Fig. 3** Proposed RSS

the first phase. At last, the secret can be recovered successfully based on all shares.

## Analysis

### Security analysis

This section will first prove that our scheme is information-theoretically secure, and then analyze the security properties of the proposed RSS protocol, which have been defined in Properties section.

There are two types of security in most cryptographic schemes, either information-theoretic secure or computationally secure. If a scheme is computationally secure, the security of the scheme is based on some mathematical assumptions. If a scheme is information-theoretic

secure, there is no mathematical assumption made to achieve its security. Since information-theoretic security (also called unconditionally security) does not depend on any computational assumption, schemes with information-theoretic security are more attractive than most schemes with computational security. In the following theorem, we prove that our proposed RSS scheme is information-theoretic secure.

#### *Theorem 1*

The proposed RSS scheme is unconditionally secure.

#### *Proof*

Information-theoretic security implies that no assumptions are made about the computing power and resources available to an adversary. We can see that there is not any computational assumption in our scheme. The proposed RSS scheme uses Peterson's VSS as building block. Pedersen's VSS is information-theoretic secure. Hence, our RSS scheme is information-theoretic secure.

#### *Secrecy*

It is obvious that Petersen's VSS prevents players to get the secret/shares from public commitments. In the first phase, each share of player is divided into multiple sub-shares using a polynomial with degree $k-1$. Assuming that the majority of players are always honest (i.e., at least $k = \lceil \frac{n}{2} \rceil$ players are honest in the process of secret reconstruction), this ensures that colluded dishonest players (i.e., there are at most $n-k<k$ colluded players) cannot recover any share/secret from any subset of sub-shares generated in this phase. Thus, shares and the secret are protected. In other words, if multiple players decide to act maliciously, no one can get the secret. On the other hand, since we assume that there exist at least $k = \lceil \frac{n}{2} \rceil$ players who are honest, this ensures that each share can be recovered successfully by sub-shares of honest players.

#### *Fairness*

In the second phase, shares are revealed asynchronously. If any player decides to reveal a fake share, Petersen's VSS can detect this fake shares. Assuming that most players are always honest. The shares are divided into sub-shares using polynomials having degree $k-1$ in the first phase. Thus, any share can be recovered by the subset of sub-shares of honest players. Note that whether a player is honest or dishonest in revealing his share/sub-share can be determined by other players using Petersen's commitments generated by the dealer and the owner of the share previously. Moreover, if any player decides not to reveal any share, same procedure can be applied to recover the share and the secret. In summary, players acting maliciously in this phase will not affect all other honest players to restore the secret.

#### *Un-deniability*

The un-deniable feature is provided in the first phase by employing Petersen's VSS to share each share of player. After completing the first phase, no player can deny to reveal the real share in the second phase since any malicious action is useless. The share can always be recovered by the majority of players. This feature of un-deniability encourages players in the secret reconstruction to act honestly in revealing their shares in the second phase.

### Efficiency analysis

This section will analyze the efficiency property of the proposed RSS protocol, which have been defined in Properties section.

#### *Efficiency*

At the beginning of each phase, each player needs to compute and release values to others. But there has no interaction among players to verify sub-shares. In the first phase, each player needs to execute $2(k-1)$ modular exponentiations to compute his commitments and $2(k+1)$ modular exponentiations to verify each pair of sub-shares. Overall, each player needs $2(k-1)+2(n-1)(k+1)$ modular exponentiations. In the second phase, each player needs $t+1$ modular exponentiations to verify each share of other player. Overall, each player needs $(n-1)(t+1)$ modular exponentiations to verify all shares from other players.

## Conclusion

The existing communication networks in UCE are asynchronous networks in which multiple users cannot transmit their messages simultaneously. The asynchronous transmission can cause security problems. An information-theoretic RSS is proposed in this paper for secure group communications in UCE. This RSS can be deployed in an asynchronous network. Our design uses Petersen's VSS to allow each player to divide his share obtained from the dealer originally and shared with all other players before revealing it to the public. This feature encourages all players to reveal their shares honestly since any malicious behavior (i.e., either revealing a fake share or refusing to release one) is useless. The proposed scheme is practically valuable for secure group-oriented application in UCE.

**Acknowledgements**

I would like to express my very great appreciation to all researchers for their valuable and constructive suggestions during the planning and development of this research work.

**Authors' contributions**
The authors confirm contribution to the paper as follows: study conception and design: Chingfang Hsu, Lein Harn; data collection: Zhe Xia; analysis and interpretation of results: Chingfang Hsu, Zhe Xia; draft manuscript preparation: Chingfang Hsu. Lein Harn, Zhe Xia. All authors reviewed the results and approved the final version of the manuscript.

**Funding**
This work was partially supported by the National Natural Science Foundation of China (Grants Nos. 62172181, 62072133) and the key projects of Guangxi Natural Science Foundation (no. 2018GXNSFDA281040).

**Availability of data and materials**
The data used to support the findings of this study are included within the article.

## Declarations

**Ethics approval and consent to participate**
Not applicable.

**Consent for publication**
Not applicable.

**Competing interests**
The authors declared that they have no conflicts of interest to this work.

**Author details**
[1]Computer School, Central China Normal University, Wuhan 430079, China. [2]Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO 64110, USA. [3]Department of Computer Science, Wuhan University of Technology, Wuhan 430071, China.

Received: 16 February 2022 Accepted: 12 November 2022
Published online: 08 December 2022

**References**

1. Hu R, Yan Z, Ding W et al (2020) A survey on data provenance in IoT. World Wide Web 23:1441–1463. https://doi.org/10.1007/s11280-019-00746-1
2. Huang Z, Wang Q (2020) A PUF-based unified identity verification framework for secure IoT hardware via device authentication. World Wide Web 23:1057–1088. https://doi.org/10.1007/s11280-019-00677-x
3. He J, Rong J, Sun L et al (2020) A framework for cardiac arrhythmia detection from IoT-based ECGs. World Wide Web. https://doi.org/10.1007/s11280-019-00776-9
4. Hong H, Sun Z (2018) Sharing your privileges securely: a key-insulated attribute based proxy re-encryption scheme for IoT. World Wide Web 21:595–607. https://doi.org/10.1007/s11280-017-0475-8
5. Peng C, Luo M, Li L, Choo K-KR, He D (2021) Efficient certificateless online/offline signature scheme for wireless body area networks. IEEE Internet Things J 18(8):14287–14298
6. Shen J, Yang H, Vijayakumar P, Kummar N (2021) A privacy-preserving and untraceable group data sharing scheme. IEEE Trans Depend Secure Comput. https://doi.org/10.1109/TDSC.2021.3050517
7. Qiu S, Wang D, Xu G, Kumari S (2022) Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for Mobile lightweight devices. IEEE Trans Dependable Secure Comput 19(2):1338–1351
8. Han J, Chen L, Schneider S, Treharne H, Wesemeyer S (2021) Privacy-preserving electronic ticket scheme with attribute-based credentials. IEEE Trans Dependable Secure Comput 18(4):1836–1849
9. Jiang Q, Zhang X, Zhang N, Tian Y, Ma X, Ma J (2021) Three-factor authentication protocol using physical Unclonable function for IoV. Comput Commun 173:45–55. https://doi.org/10.1016/j.comcom.2021.03.022
10. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
11. Asmuth C, Bloom J (1983) A modular approach to key safeguarding. IEEE Trans Inf Theory IT-29(2):208–210
12. Blakley GR (1979) Safeguarding cryptographic keys. In: *Managing Requirements Knowledge, International Workshop on*. IEEE Computer Society, pp 313–313
13. Halpern J, Teague V (2004) Rational secret sharing and multiparty computation: extended abstract. In: *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing - STOC '04*, pp 623–632
14. Fuchsbauer G, Katz J, Naccache D (2010) Efficient rational secret sharing in standard communication networks. In: *Theory of Cryptography Conference*. Springer, Berlin, Heidelberg, pp 419–436
15. Ong SJ, Parkes DC, Rosen A et al (2009) Fairness with an honest minority and a rational majority. In: *Theory of Cryptography Conference*. Springer, Berlin, Heidelberg, pp 36–53
16. Tartary C, Wang H, Zhang Y (2011) An efficient and information theoretically secure rational secret sharing scheme based on symmetric bivariate polynomials. Int J Found Comput Sci 22(6):1395–1416
17. Harn L, Iin CL, Li Y (2015) Fair secret reconstruction in (*t*, *n*) secret sharing. J Inform Secur Appl 23:1–7
18. Moses WK Jr, Rangan CP (2011) Rational secret sharing over an asynchronous broadcast channel with information theoretic security. Int J Netw Secur Appl 3(6):1–18
19. Lin HY, Harn L (1995) Fair reconstruction of a secret. Inf Process Lett 55(1):45–47
20. Maleka S, Shareef A, Rangan C P (2008) Rational secret sharing with repeated games. In: *International Conference on Information Security Practice and Experience*. Springer, Berlin, Heidelberg, pp 334–346
21. Pedersen TP (1991) Non-interactive and information-theoretic secure verifiable secret sharing. In: *Annual international cryptology conference*. Springer, Berlin, Heidelberg, pp 129–140
22. Chor B, Goldwasser S, Micali S, Awerbuch B (1985) Verifiable secret sharing and achieving si multaneity in the presence of faults. In: *Proc. 26th FOCS*. IEEE, Piscataway, pp 383–395
23. Benaloh JC (1986) Secret sharing homomorphisms: Keeping shares of a secret secret. In: *Conference on the theory and application of cryptographic techniques*. Springer, Berlin, Heidelberg, pp 251–260
24. Feldman P (1987) A practical scheme for verifiable secret sharing. In: *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, New York, pp 427–438
25. Stadler M (1996) Publicly verifiable secret sharing. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, pp 190–199
26. Schoenmakers B (1999) A simple publicly verifiable secret sharing scheme and its application to electronic voting. In: *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, pp 148–164
27. Peng A, Wang L (2010) One publicly verifiable secret sharing scheme based on linear code. In: *Proceeding of 2nd Conference on Environmental Science and Information Application Technology*, pp 260–262
28. Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: *International conference on the theory and applications of cryptographic techniques*. Springer, Berlin, Heidelberg, pp 223–238
29. Ruiz A, Villar JL (2005) Publicly verifiable secret sharing from Paillier's cryptosystem. In: *Proceedings of WEWoRC '05*, LNI P-74, pp 98–108
30. Tian Y, Peng C, Ma J (2012) Publicly verifiable secret sharing schemes using bilinear pairings. Int J Netw Secur 14(3):142–148
31. Wu T, Tsenga Y (2011) A pairing-based publicly verifiable secret sharing scheme. J Syst Sci Complex 24(1):186–194

## Publisher's Note