Computer Science and Application 计算机科学与应用, 2019, 9(12), 2367-2374
Published Online December 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.912263

Hans汉斯

Universal Verifiability Design for the Combination of N Shamir Threshold Secret Sharing Schemes

Yonghao Guo, Hongru Wei

School of Mathematics and Physics, University of Science and Technology Beijing, Beijing
Email: yoho13070100495@163.com, weihr@ustb.edu.cn

Received: Dec. 2nd, 2019; accepted: Dec. 13th, 2019; published: Dec. 20th, 2019

Abstract

The verifiability of secret sharing scheme is an important research direction in secure multi-party computing protocols. The research in this field can be used as the basis for the fairness, security and correctness of security computing. This paper designed that a universal verifiability of a n-shamir threshold secret sharing scheme is different from the existing shamir threshold secret sharing scheme. This paper extends the secret number shared by each participant to *n*, *i.e.* the combination of n-shamir thresholds, rather than a single secret sharing, makes its application more extensive; at the same time, it makes up for the lack of verification of the existing general methods in the input phase and the computing phase. Finally, the continuity and transitivity of the verifiability of each stage and every step are achieved.

Keywords

Secret Sharing, Verifiability, Secure Multiparty Computing, Shamir Threshold

N个Shamir门限秘密共享方案组合的通用可验证性设计

郭涌浩，卫宏儒

北京科技大学数理学院，北京
Email: yoho13070100495@163.com, weihr@ustb.edu.cn

收稿日期：2019年12月2日；录用日期：2019年12月13日；发布日期：2019年12月20日

摘　要

秘密共享方案的可验证性是安全多方计算协议中重要的一个研究方向，该领域的研究可以作为安全计

文章引用: 郭涌浩, 卫宏儒. N 个 Shamir 门限秘密共享方案组合的通用可验证性设计[J]. 计算机科学与应用, 2019, 9(12): 2367-2374. DOI: 10.12677/csa.2019.912263

算的公平性、安全性、正确性研究基础。本文设计了一种n个Shamir门限秘密共享方案组合的通用可验证性，该方案与已有的Shamir门限秘密共享方案不同，本文将每个参与者分享的秘密数扩展到个，即个Shamir门限的组合，而不是单单的对于一个秘密的分享，使其应用的方面更加广泛；同时，弥补了现有通用方法在输入阶段和计算阶段的验证性的不足，最后实现了每个阶段、每个步骤可验证性的连续性、传递性。

关键词

秘密分享方案，可验证性，安全多方计算，Shamir门限

1. 引言

秘密共享是当今生活中广泛使用的技术，主要是对信息进行加密和保护，防止外泄。自 Shamir 和 Blakley [1] [2]引出秘密共享的问题并给出了非常简单的问题解决方案以来，关于这一主题的研究已经深入。Shamir 和 Blakley 的方案是在没有故障的模型中有效的解决方案。Tompa 和 Woll [3]以及 McEliece 和 Sarwate [4]的方案在存在故障的模型中给出了部分解决方案。近年来，许多学者已经开始研究秘密共享技术，并提出了各种秘密共享方案，其中有中国剩余定理、双线性对技术、签密与消息恢复算法、公钥密码体制等。蒋华等人基于公钥密码体制，对其进行改进，提出了一种双向认证的方案。只要是在申请人，身份验证者和服务器之间的相互身份验证加密[5]。2014 年张柄虹等人提出了一种方案，在该方案中，秘密分发的过程是独立的，并且与参与者的私钥计算分开[6]。2018 年，谷婷提出了一种秘密共享方案[7]。在该方案中，秘密份额由参与者产生，利用签密与消息恢复算法，参与的所有人都可以查验分发者的份额。

在秘密共享方案飞速发展的下，对于方案的正确性、有效性和安全性变得重要起来，即秘密共享方案的可验证有着十分深远的研究意义。Chor 等人[8]第一次定义了可验证秘密共享的完整概念，并给出了问题的解决方案。接下来的研究，在各种不同假设下，不同的学者给出了问题的解决方案。只是为了实现可验证性的目标，这些协议偏离了原始解决方案的简单性。它们需要繁重的计算和广泛的零知识证明。此外，为了重建秘密，还需要进行大量计算。大量的研究和实际操作表明，简单的协议是很重要的。Gennaro 的方案基于 Shamir 的秘密共享方案，并增加了额外的低成本结构。这种结构基本上是参与者对持有秘密的公开承诺。

2. 基本知识

本文设计的可验证性秘密共享方案涉及到以下三个知识：① shamir 门限秘密共享方案；② 零知识证明[9]；③ Pedersen 承诺协议[10]。

Shamir 的门限秘密共享方案通过构造多项式，利用多项式进行秘密的分享，本文秘密共享是基于 Shamir 门限秘密共享方案实现的；本文使用的零知识证明改编自 Cramer 和 Damgar 的方案，使其更具有证明的一般性，是本文计算阶段中的重要一环；Pedersen 承诺协议是一个满足无条件秘密性的同态承诺协议，作为本文可验证性设计的基本框架。

3. 秘密共享方案及可验证性设计设计

3.1. 秘密共享方案

本文将 Gennaro 的 VSS 方案和 Pedersen 同态承诺方案结合，实现了对份额正确性的验证。该 MPC 协议将待计算函数表示为加法和乘法组成的有向图，通过进行对应的加法协议和乘法协议来实现计算，其结构如图 1 所示。该协议可分为初试化阶段，输入阶段，计算阶段和输出阶段。

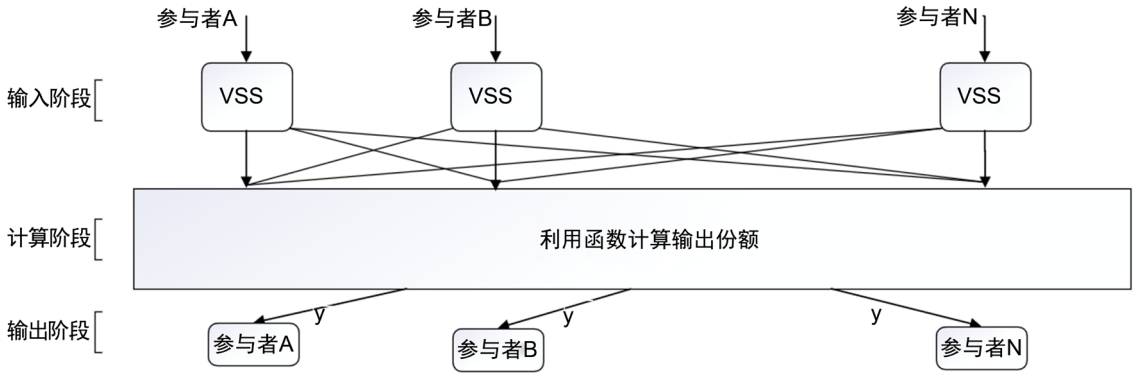

Figure 1. Structure of the secret sharing scheme
图 1. 秘密共享方案结构

初始化阶段：假设协议有 n 个参与者，分别记作 $P_1,P_2,\cdots,P_n$，每个参与者分别对应一个公开身份数 $x_i\in Z^*\left(i\neq j\Rightarrow x_i\neq x_j,x_0=0\right)$，以及一个秘密 $s_i\in Q^+,i=1,2,\cdots,n$。$n$ 个参与者协商一个大素数 p，该素数满足 $p=2q+1$，其中 q 也是素数，g 为 Z_p^* 的 q 阶元，h 为 g 生成的子群中的随机元素。上述的 p,g,h 是构造可验证性使用的承诺函数的参数。

输入阶段：每个参与者 $P_i\left(i=1,2,\cdots,n\right)$ 独立随机地选择 $2t+1$ 个 t 次多项式，使用上述多项式分别在有理数域上共享 $s_i,s_i^2,\cdots,s_i^{2t},s_i^{2t+1}$，即 $f_{i_1}\left(0\right)=s_i,f_{i_2}\left(0\right)=s_i^2,\cdots,f_{i_{2t+1}}\left(0\right)=s_i^{2t+1}$

$$\begin{aligned}
f_{i_1}\left(x\right)&=s_i+a_{i_1 1}x+\cdots+a_{i_1 t}x^t\\
f_{i_2}\left(x\right)&=s_i^2+a_{i_2 1}x+\cdots+a_{i_2 t}x^t\\
&\vdots\\
f_{i_{2t+1}}\left(x\right)&=s_i^{2t+1}+a_{i_{2t+1}1}x+\cdots+a_{i_{2t+1}t}x^t
\end{aligned}\tag{3-1}$$

其中 s_i 为参与者 P_i 的秘密。

同样的，P_i 生成随机数 $r_i,c_i\in Q^+$，并独立地随机选择两个 t 次多项式 $r_i\left(x\right),c_i\left(x\right)$，分别在有理数域上分享 r_i,c_i，即 $r_i\left(0\right)=r_i,c_i\left(0\right)=c_i$

$$\begin{aligned}
r_i\left(x\right)&=r_i+a_{i1}x+a_{i2}x^2+\cdots+a_{it}x^t\\
c_i\left(x\right)&=c_i+b_{i1}x+b_{i2}x^2+\cdots+b_{it}x^t
\end{aligned}\text{。}\tag{3-2}$$

分别使用式(3-1) (3-2)计算 $f_{i_1}\left(x_j\right),f_{i_2}\left(x_j\right),\cdots,f_{i_{2t+1}}\left(x_j\right),r_i\left(x_j\right),c_i\left(x_j\right)$，并将 $\left(f_{i_1}\left(x_j\right),f_{i_2}\left(x_j\right),\cdots,f_{i_{2t+1}}\left(x_j\right),r_i\left(x_j\right),c_i\left(x_j\right)\right)$ 发送给 P_j，其中 $j=1,2,\cdots,n$。同时，P_i 将承诺集合 $\left(A_{i_1 j},A_{i_2 j},\cdots,A_{i_{2t+1}j},A_{ij}\right),i\neq j,j=1,2,\cdots,n$，进行广播，

$$\begin{aligned} A_{i_1 j} &= g^{f_{i_1}(x_j)} h^{c_i(x_j)} \bmod p \\ A_{i_2 j} &= g^{f_{i_2}(x_j)} h^{c_i(x_j)} \bmod p \\ &\vdots \\ A_{i_{2t+1} j} &= g^{f_{i_{2t+1}}(x_j)} h^{c_i(x_j)} \bmod p \\ A_{ij} &= g^{r_i(x_j)} h^{c_i(x_j)} \bmod p \end{aligned} \quad 。 \tag{3-3}$$

计算阶段：步骤(1)：n 个参与者约定在式(3-2)中的 $r_1(x), r_2(x), \cdots, r_n(x)$ 取定 $2t+1$ 个随机多项式，不妨就将这 $2t+1$ 个多项式记为 $r_1(x), r_2(x), \cdots, r_{2t+1}(x)$，其对应的 $2t+1$ 参与者分别是 $P_1, P_2, \cdots, P_{2t+1}$。每个参与者 P_j 计算

$$g_i(x_j) = r_1(x_j) f_{i_1}(x_j) + r_2(x_j) f_{i_2}(x_j) + \cdots + r_{2t+1}(x_j) f_{i_{2t+1}}(x_j) \tag{3-4}$$

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{2t} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{2t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{2t+1} & x_{2t+1}^2 & \cdots & x_{2t+1}^{2t} \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \cdots & \lambda_{2t+1} \\ * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{pmatrix}$$

承诺 $\left(B_{ji_1}, B_{ji_2}, \cdots, B_{ji_{2t+1}}\right), i \neq j, i = 1,2,\cdots,n$ 进行广播。

$$\begin{aligned} B_{ji_1} &= g^{\lambda_j r_1(x_j) f_{i_1}(x_j)} h^{u_j(x_j)} \bmod p \\ B_{ji_2} &= g^{\lambda_j r_2(x_j) f_{i_2}(x_j)} h^{u_j(x_j)} \bmod p \\ &\vdots \\ B_{ji_{2t+1}} &= g^{\lambda_j r_{2t+1}(x_j) f_{i_{2t+1}}(x_j)} h^{u_j(x_j)} \bmod p \end{aligned} \tag{3-5}$$

其中 $u_j(x)$ 为 P_j 随机选择与承诺相关的 t 次多项式。

步骤(2)：$P_1, P_2, \cdots, P_{2t+1}$ 中的每个 P_j 随机选择 n 个 t 次多项式 $h_{j_1}(x_k), h_{j_2}(x_k), \cdots, h_{j_n}(x_k)$ 分别用来共享 $\lambda_j g_1(x_j), \lambda_j g_2(x_j), \cdots, \lambda_j g_n(x_j)$，其中 $h_{j_i}(0) = \lambda_j g_i(x_j), 1 \le i \le n$，接着随机选择 1 个 t 次多项式 $v_j(x)$ 用来共享 $(2t+1)u_j(x_j)$，即 $v_j(0) = (2t+1)u_j(x_j)$。然后 P_j 计算 $h_{j_1}(x_k), h_{j_2}(x_k), \cdots, h_{j_n}(x_k), v_j(x_k)$，并将 $\left(h_{j_1}(x_k), h_{j_2}(x_k), \cdots, h_{j_n}(x_k), v_j(x_k)\right)$ 发送给 $P_k, 1 \le k \le n$。承诺集合 $\left(C_{j_1 k}, C_{j_2 k}, \cdots, C_{j_n k}\right), k \neq j, k = 0,1,2,\cdots,n$。其中，当 $k = 0$ 时，有 $x_k = x_0 = 0$。将承诺集合进行广播，

$$\begin{aligned} C_{j_1 k} &= g^{h_{j_1}(x_k)} h^{v_j(x_k)} \bmod p \\ C_{j_2 k} &= g^{h_{j_2}(x_k)} h^{v_j(x_k)} \bmod p \\ &\vdots \\ C_{j_n k} &= g^{h_{j_n}(x_k)} h^{v_j(x_k)} \bmod p \end{aligned} \quad 。 \tag{3-6}$$

输出阶段：对于每个 P_j，计算输出

$$y_j=\left(y_{j_1},y_{j_2},\cdots,y_{j_n}\right)=\left(\sum_{i=1}^{2t+1}h_{i_1}\left(x_j\right),\sum_{i=1}^{2t+1}h_{i_2}\left(x_j\right),\cdots,\sum_{i=1}^{2t+1}h_{i_n}\left(x_j\right)\right) \tag{3-7}$$

其中， $j=1,2,\cdots,n$，广播承诺集合

$$\begin{aligned}D_{j_1}&=g^{y_{j1}}h^{w_j}\bmod p\\D_{j_2}&=g^{y_{j2}}h^{w_j}\bmod p\\&\vdots\\D_{j_n}&=g^{y_{jn}}h^{w_j}\bmod p\end{aligned} \tag{3-8}$$

其中， $w_j=\sum_{i=1}^{2t+1}v_i\left(x_j\right)$。

重构阶段：每个 P_j 具有输出 $y_j\left(1\le j\le n\right)$。使用拉格朗日插值公式，任意的 $t+1$ 个参与者都可以恢复 $s_i'=r_1s_i+r_2s_i^2+\cdots+r_{2t+1}s_i^{2t+1}$。

3.2. 可验证性分析

3.2.1. 输入阶段的可验证性

以 A_{i_1j} 为例，根据式(3-3)所示，有承诺 $A_{i_1j}=g^{f_{i_1}\left(x_j\right)}h^{c_i\left(x_j\right)}\bmod p$，则根据(3-1)式，可将多项式组写成矩阵乘积的形式

$$\begin{pmatrix}1&0&\cdots&0\\1&1&\cdots&1\\\vdots&\vdots&\ddots&\vdots\\1&t&\cdots&t^t\end{pmatrix}\begin{pmatrix}s_i\\a_{i_1}1\\\vdots\\a_{i_1t}\end{pmatrix}=\begin{pmatrix}f_{i_1}\left(x_0\right)\\f_{i_1}\left(x_1\right)\\\vdots\\f_{i_1}\left(x_t\right)\end{pmatrix}$$

不妨记为：

$$V\begin{pmatrix}s_i\\a_{i_1}1\\\vdots\\a_{i_1t}\end{pmatrix}=\begin{pmatrix}f_{i_1}\left(x_0\right)\\f_{i_1}\left(x_1\right)\\\vdots\\f_{i_1}\left(x_t\right)\end{pmatrix}$$

根据上述多项式，容易得到矩阵 V 是可逆的，所以可将上式写成：

$$\begin{pmatrix}s_i\\a_{i_1}1\\\vdots\\a_{i_1t}\end{pmatrix}=V^{-1}\begin{pmatrix}f_{i_1}\left(x_0\right)\\f_{i_1}\left(x_1\right)\\\vdots\\f_{i_1}\left(x_t\right)\end{pmatrix}$$

对于任意的 δ，有

$$\begin{aligned}A_{i_1\delta}'&=g^{f_{i_1}\left(x_\delta\right)}h^{c_i\left(x_\delta\right)}\bmod p\\&=g^{s_i+\sum_{m=1}^{t}a_{i_1m}x_\delta^m}h^{c_i+\sum_{m=1}^{t}b_{im}x_\delta^m}\bmod p\end{aligned}$$

为了方便起见，记 $a_{i_10}=s_i,b_{i0}=c_i$，则上式记作

$$A_{i_1j}'=g^{\sum_{m=0}^{t}a_{i_1m}x_\delta^m}h^{\sum_{m=0}^{t}b_{im}x_\delta^m}\bmod p \tag{3-9}$$

记 α_{mk} 为 V^{-1} 的第 m 行第 k 列的值，所以可得 $a_{i_1 m}=\sum_{k=0}^{t}\alpha_{mk}f_{i_1}(x_k)$，并代入到式(3-9)中，可得

$$\begin{aligned}A'_{i_1\delta}&=g^{\sum_{m=0}^{t}\sum_{k=0}^{t}\alpha_{mk}f_{i_1}(x_k)x_\delta^m}h^{\sum_{m=0}^{t}\sum_{k=0}^{t}\alpha_{mk}c_i(x_k)x_\delta^m}\bmod p\\&=\prod_{k=0}^{t}\left(g^{f_{i_1}(x_k)}h^{c_i(x_k)}\right)^{\Delta_k}\bmod p=\prod_{k=0}^{t}\left(A_{i_1k}\right)^{\Delta_k}\end{aligned}$$

其中 $\Delta_k=\sum_{m=0}^{t}\alpha_{mk}x_\delta^m$，以上所述，将 $A'_{i_1\delta}$ 与 $A_{i_1\delta}$ 作比较，即可验证自己收到的份额是否和其他参与者收到份额出自同一组多项式(这里不妨记作 VSPS 性质)，从而来判断自己收到的份额是否有效，即正确性得到检验。

3.2.2. 计算阶段的可验证性

第一步：经过了输入阶段的验证，每个参与方 P_j 已经收到经过输入阶段 VSPS 验证的正确份额 $\left(f_{i_1}(x_j),f_{i_2}(x_j),\cdots,f_{i_{2t+1}}(x_j),r_i(x_j),c_i(x_j)\right)$，以此承诺函数 $\left(A_{i_1 j},A_{i_2 j},\cdots,A_{i_{2t+1}j},A_{ij}\right)$ 也是经过 VSPS 验证被证实正确的。利用正确承诺函数 $\left(A_{i_1 j},A_{i_2 j},\cdots,A_{i_{2t+1}j},A_{ij}\right)$ 和 $\left(\lambda_1,\lambda_2,\cdots,\lambda_{2t+1}\right)$ 并使用前文提到的零知识证明方法，每一个参与者 P_i 对 P_j 广播的承诺 $\left(B_{ji_1},B_{ji_2},\cdots,B_{ji_{2t+1}}\right)$ 进行比较，来保证正确的秘密份额被使用。

第二步：根据上述第一步，参与者 P_j 有经过前面检验的 $\left(B_{ji_1},B_{ji_2},\cdots,B_{ji_{2t+1}}\right)$，根据式(3-6)，可验证性如下：

以 $C_{j_1k}=g^{h_{j_1}(x_k)}h^{v_j(x_k)}\bmod p$ 为例，

1) 当 $k=0$ 时，即 $x_k=x_0=0$ 时，即：

$$C_{j_1k}=g^{h_{j_1}(x_k)}h^{v_j(x_k)}\bmod p=g^{h_{j_1}(0)}h^{v_j(0)}\bmod p$$

所以有 $C_{j_1k}=g^{h_{j_1}(0)}h^{v_j(0)}\bmod p$，根据 $h_{j_1}(x),v_j(x)$ 的定义，原式可以写成：

$$\begin{aligned}C_{j_1k}&=g^{\lambda_j g_1(x_j)}h^{(2t+1)u_j(x_j)}\bmod p\\&=g^{\lambda_j\left(r_1(x_j)f_{i_1}(x_j)+r_2(x_j)f_{i_2}(x_j)+\cdots+r_{2t+1}(x_j)f_{i_{2t+1}}(x_j)\right)}h^{(2t+1)u_j(x_j)}\bmod p\end{aligned}$$

所以，根据模的运算性质，和承诺函数集合 $\left(B_{ji_1},B_{ji_2},\cdots,B_{ji_{2t+1}}\right)$ 的形式，上式可以写成

$$\begin{aligned}C_{j_1k}&=g^{\lambda_j r_1(x_j)f_{i_1}(x_j)}h^{u_j(x_j)}g^{\lambda_j r_2(x_j)f_{i_2}(x_j)}h^{u_j(x_j)}\cdots g^{\lambda_j r_{2t+1}(x_j)f_{i_{2t+1}}(x_j)}h^{u_j(x_j)}\bmod p\\&=B_{ji_1}B_{ji_2}\cdots B_{ji_{2t+1}}\end{aligned}$$

所以，在步骤(1)中，验证正确的承诺函数集合 $\left(B_{ji_1},B_{ji_2},\cdots,B_{ji_{2t+1}}\right)$，就可以将 C_{j_1k} 与 $B_{ji_1}B_{ji_2}\cdots B_{ji_{2t+1}}$ 的乘积作比较，可以判断函数 $h_{j_1}(x_k),h_{j_2}(x_k),\cdots,h_{j_n}(x_k)$ 是否分别用来共享 $\lambda_j g_1(x_j),\lambda_j g_2(x_j),\cdots,\lambda_j g_n(x_j)$。

2) 当 $k\neq 0$ 时，同理如输入阶段，使用 VSPS 验证来验证自己收到的份额是否有效。

3.2.3. 输出阶段的可验证性

经过了计算阶段的验证，每个参与方 P_j 已经收到了经过验证的正确的份额 $\left(h_{i_1}(x_j),h_{i_2}(x_j),\cdots,h_{i_n}(x_j),v_i(x_j)\right)$，和验证正确的承诺 $\left(C_{i_1 j},C_{i_2 j},\cdots,C_{i_n j}\right)$

根据式(4-7)，并以式(4-8)中的 D_{j_1} 为例，

$$\begin{aligned} D_{j_1} &= g^{y_{j_1}} h^{w_j} \bmod p \\ &= g^{\sum_{i=1}^{2t+1} h_{i_1}(x_j)} h^{\sum_{i=1}^{2t+1} v_i(x_j)} \bmod p \\ &= \left(\prod_{i=1}^{2t+1} g^{h_{i_1}(x_j)}\right)\left(\prod_{i=1}^{2t+1} h^{v_i(x_j)}\right) \bmod p \\ &= \prod_{i=1}^{2t+1} g^{h_{i_1}(x_j)} h^{v_i(x_j)} \bmod p = \prod_{i=1}^{2t+1} C_{i_1 j} \end{aligned}$$

将参与者 P_j 的承诺 D_{j_1} 与计算阶段经过验证的承诺 $\prod_{i=1}^{2t+1} C_{i_1 j}$ 作比较，就可以判断对于输出的 y_j 是否是正确的。

4. 结束语

关于安全多方计算协议的构造一直是密码学领域中的一个难解的问题。本文针对个 Shamir 门限的组合的秘密共享方案的可验证性进行设计，完成了 Shamir 门限组合的秘密共享方案的通用可验证性。该项研究有着很重要的意义。现实中攻击者都是理性的，已有很多学者[11]采取惩罚措施，约束恶意攻击者来实现安全多方计算中最难实现的公平性。这些利用惩戒措施实现公平性的研究，都是建立在可验证秘密共享方案的基础上，只有尽可能完全的实现可验证性，对不诚实的恶意参与者进行有效的识别，才能使惩戒措施有效的发挥作用。其次，本文的方案追求的是尽可能完整的可验证性，所以在计算上会有些复杂，这也为下一步的研究指明了方向。

基金项目

国家自然科学基金(No.U1603116、No.61672509)。

参考文献

[1] Blakley, G.R. (1979) Safeguarding Cryptographic Keys. *Proceedings of AFIPS National Computer Conference*, Washington DC, 4-7 June 1979, 313-317. https://doi.org/10.1109/MARK.1979.8817296

[2] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613. https://doi.org/10.1145/359168.359176

[3] Tompa, M. and Woll, H. (1988) How to Share a Secret with Cheaters. *Journal of Cryptology*, **1**, 133-138. https://doi.org/10.1007/BF02252871

[4] McEliece, R.J. and Sarwate, D.V. (1981) On Sharing Secrets and Reed-Solomon Codes. *Communications of the ACM*, **24**, 583-584. https://doi.org/10.1145/358746.358762

[5] 蒋华, 张乐乾, 阮玲玲. 基于公钥密码体质的 802.1x 双向认证研究[J]. 计算机应用于软件, 2016, 33(2): 290-293.

[6] 张柄虹, 张串绒, 焦和平, 张欣威, 高胜国. 一种基于双线性对的公平可验证多秘密共享方案[J]. 空军工程大学学报(自然科学版), 2014, 15(4): 83-87.

[7] 谷婷. 无可信中心可验证可更新的向量空间秘密共享[J]. 科技与创新, 2018, 99(3): 35-39.

[8] Chor, B., Goldwasser, S., Micali, S. and Awerbuch, B. (1985) Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. *Proceeding 26th Annual Symposium on the Foundations of Computer Science*, Portland, 21-23 October 1985, 383-395. https://doi.org/10.1109/SFCS.1985.64

[9] Gennaro, R. and Rabin, M.O. (1998) Simplified VSS and Fast-Track Multiparty Computations with Applications to Threshold Cryptography. *Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing*, Puerto Vallarta, 28 June-2 July 1998, 101-111. https://doi.org/10.1145/277697.277716

[10] Qiu, G., Wang, H., Wei S.M. and Xiao, G.Z. (2006) Information-Theoretic Secure Verifiable Secret Sharing over RSA

Modulus. *Wuhan University Journal of Natural Sciences*, **11**, 1849-1852. https://doi.org/10.1007/BF02831890

[11] Andrychowicz, M., Dziembowski, S., Malinowski, D., *et al*. (2014) Secure Multiparty Computations on Bitcoin. *Proc of IEEE Symposium on Security and Privacy*, San Jose, 18-21 May 2014, 76-84. https://doi.org/10.1109/SP.2014.35