doi:10.11959/j.issn.1000-436x.2015083

基于 Shamir 秘密共享的密钥分发与恢复算法

荣辉桂[1]，莫进侠[1]，常炳国[1]，孙光[2]，龙飞[3]
（1. 湖南大学 信息科学与工程学院，湖南 长沙 410082；
2. 湖南财政经济学院 信息管理系，湖南 长沙 410205；3. 长沙大学 经济管理系，湖南 长沙 410003）

摘 要：在经典的 Shamir 秘密共享方案中，秘密分发者把秘密 *s* 分为 *n* 个影子秘密并分发给持有者；其中任意不少于 *t* 个影子秘密均能恢复秘密 *s*，少于 *t* 个影子秘密则得不到秘密 *s* 的任何信息。现实的秘密恢复过程中可能存在超过 *t* 个参与者的情形。因此，在 Shamir 的秘密共享方案基础上讨论此种情形下秘密共享问题，通过引入影子秘密的线性组合——拉格朗日因子来恢复秘密，并进一步将其扩展为一个多秘密共享方案。理论分析与仿真实验表明：改进算法在同样复杂度条件下既保证影子秘密的安全，又能阻止欺骗者得到秘密，提高了整体安全性。

关键词：秘密共享；密钥分发；拉格朗日因子；密钥恢复
中图分类号：TP393 **文献标识码**：A

Key distribution and recovery algorithm based on Shamir's secret sharing

RONG Hui-gui[1], MO Jin-xia[1], CHANG Bing-guo[1], SUN Guang[2], LONG Fei[3]
(1. College of Computer Science and Engineering, Hunan University, Changsha 410082, China;
2. Department of Information Management, Hunan University of Finance and Economics, Changsha 410205, China;
3. Department of Economics and Management, Changsha University, Changsha 410003, China)

Abstract: In Shamir's secret sharing scheme, the dealer divided the secret *s* into *n* shadows and distributed it to shareholders in such a way that any *t* or more than *t* shadows can recover this secret, while fewer than *t* shadows cannot obtain any information about the secret *s*. During the actual secret recovery process, there exist other cases with more than *t* participants. The case of secret sharing problem was discussed based on Shamir's secret sharing scheme and reconstructs the secret by introducing a linear combination of shadows—Lagrange factor. Then, the improved algorithm of key distribution and recovery was proposed and extended to a multi-secret sharing scheme. Theoretical analysis and simulation show that the improved scheme improves its security under the same conditions of complexity.

Key words: secret sharing; key distribution; Lagrange factor; key recovery

1 引言

秘密共享技术是密码学和信息安全的一个重要研究内容，被广泛应用于密钥管理及数字签名领域。它最早由 Shamir[1]和 Blackly[2]在 1979 年分别基于 Lagrange 插值多项式和矢量方法提出。其基本思想是分发者通过秘密多项式将秘密 *s* 分为 *n* 个影子秘密并分发给持有者，其中任意不少于 *t* 个影子秘密均能恢复秘密，少于 *t* 个影子秘密则得不到主秘密的任何信息。它的出现解决了密钥安全保管的基本问题，既能保证秘密的安全性、完整性，又能防止秘密过于集中而带来的风险。由于秘密共享在数据保密及信息安全中扮演重要角色，对信息保存、传输及使用过程起着非常关键作用，在现实应

收稿日期：2014-09-14；**修回日期**：2015-02-10
基金项目：国家自然科学基金资助项目(61304184)；国家科技支撑计划基金资助项目(2013BAH45F02)；科技部创新基金资助项目(13C26214304053)；湖南重点建设学科基金资助项目；湖南大学“青年教师成长计划”基金资助项目(531107021115)
Foundation Items: The National Natural Science Foundation of China (61304184); The National Key Technology Support Program (2013BAH45F02); The Innovation Foundation of Science and Technology Ministry (13C26214304053); The Construct Program of the Key Discipline in Hunan; The Young Teachers Development Plan of Hunan University (531107021115)

用中应严格保证其安全性能。

早期的秘密共享是基于分发者和参与者的诚实性建立的，但在实际应用中经常会存在以下 2 类安全隐患[3]：外部攻击和内部欺骗。外部攻击是指授权子集外的人伪装成授权子集的成员去骗取他们的影子秘密，从而恢复出秘密。内部欺骗分为 2 种情况：授权子集中的某个参与者提供假的影子秘密，从而使秘密恢复失败；秘密分发者欺骗，即分发者在下发影子秘密时可能会给参与者无效的影子秘密。为了解决上述问题，已经有许多学者做了诸多探索与研究，主要可分为如下 2 种类型：可验证秘密共享和动态秘密共享。

Chor 于 1985 年首次提出可验证秘密共享的概念[4]，通过在秘密共享过程中添加一个认证过程，实现了秘密恢复过程中对子秘密的验证以防止欺骗。但是该方案需要秘密分发者与参与者进行多次交互，造成通信带宽的浪费；且在验证过程中参与者仅能验证或收到影子秘密的正确性，仅能检测秘密分发者诚实性而无法抵抗参与者欺骗。针对 Chor 等提出方案的欺骗问题，很多学者对其进行了深入研究并取得丰硕成果。其中，Kamer Kaya 等[5]以中国剩余定理为基础提出了一个可验证秘密共享方案，该方案能够阻止秘密分发者以及参与者之间相互欺骗的行为，但采用的范围证明技术导致其验证过程繁琐，运算量较大。文献[6]提出一个密钥分发存储方案，该方案以中国剩余定理、可验证秘密共享和可信计算为基础，解决可验证秘密共享方案中存在的欺骗问题及 Shamir 方案中的指数运算；基于中国剩余定理和可验证秘密共享提出分布式椭圆数字曲线签名标准认证方案，可以消除传统 DoS 攻击及故障攻击可能性，并证明了其安全性。Kaya K 等[7]分析已有可验证秘密共享方案中不能保证分发者欺骗情况，基于中国剩余定理提出一个新的可验证秘密共享方案，它能保证秘密分发过程中分发者和参与者欺骗；应用上述方案构建第一个联合随机秘密共享协议，协议可使一组参与者在无可信分发者时共同生成并共享一个秘密。在文献[8]中，Harn L 等基于中国剩余定理提出了无任何计算假设且无条件安全的 VSS 方案，它是 Azimuth- Bloom U_r 秘密共享方案的一个简单延伸，在验证阶段中使用秘密和验证秘密的一个线性组合来保护秘密及影子秘密的安全性。文献[9]基于 LUC 密码体制提出一个可验证的多秘密共享方案，在分发和恢复阶段均具有可验证性，可防止分发者和参与者欺骗；是一个理想的秘密共享方案，即信息率 $\rho=1$；方案不需要安全通道，降低通信开销；通过更新访问结构即可更新参与者或秘密。Hu C 等[10]提出 2 个安全有效的可验证秘密共享方案，方案 Ⅰ 使用拉格朗日插值多项式把秘密分成影子秘密并通过基于 LFSR 的公开密码系统验证数据的有效性；方案 Ⅱ 通过 LFSR 序列和基于 LFSR 的公开密码系统实现。这 2 个方案具有更好性能和更低的计算复杂度，能有效地检测出各类型欺骗行为，保证秘密恢复的安全性和可靠性，在实际应用中更易于实现，但它们不能动态地增加或者减少秘密个数。

预防欺骗的另一种方法是 Laih 等[11]在 1990 年提出的动态秘密共享方案，该方案中参与者所拥有的影子秘密始终保持不变，而秘密可以任意更新。假如欺骗者获得有效个数影子秘密恢复出秘密，由于秘密是任意更新的，他得到的秘密不一定是有效的，这在一定程度上保证了秘密安全。但是该方案的安全性会因秘密更新次数的增加而降低。李大伟等[12]基于单向散列链特征构造更新多项式，从而避免计算开销；秘密共享过程基于 IBE 公钥体制，具有较好的安全性；在影子秘密的验证过程中基于有限域上离散对数难解问题有效避免了参与者欺骗。文献[13]基于单向散列函数及异或逻辑运算提出了一个动态多秘密共享方案，影子秘密能重复用于多个秘密恢复；使用动态更新秘密可防止欺骗者的攻击，并且有较好的复杂度。Qu J 等[14]在文献[13]的基础上通过增加离散对数难解性使每个参与者能自主选择影子秘密，这样可以杜绝分发者欺骗问题；方案可避免使用安全通道传送影子秘密，降低通信开销。但 MH Tadayon 等[15]证明了文献[13]方案需要安全通道及验证过程，并对其改进提出一个无需安全通道的秘密共享方案，方案基于椭圆曲线和双线性映射的离散对数难解性假设并比文献[11,13]更具实用性。贾秀芹等[16]针对圆性质的动态门限秘密共享方案中分发者和参与者欺骗、秘密传输需要安全通道等问题，基于 RSA 和离散对数密码体制、单向双变量函数和圆性质，提出一种抗欺诈的动态秘密共享方案，用于检测并识别秘密分发者对参与者的欺骗以及参与者之间的欺骗，并能减少重构步骤，提高重构秘密的成功率。由于在整个动态过程中，圆心和秘密份额始终不变，从而减小该方案的实施代价，使其具有更高的安全性和实用

性。文献[17]基于双线性映射提出一种无需安全通道的动态门限多秘密共享方案，该方案中秘密可以改变且门限值更具灵活性，通过双线性映射检测欺骗者。

除了上述动态秘密共享方案外，目前还存在一种与其相类似的方案——主动秘密共享方案[18]，通过在一个秘密共享方案周期内更新影子秘密而不改变原有秘密，欺骗者在一个周期内获得的信息在刷新之后变得毫无用处。Sun H 等在文献[19]中基于椭圆和双线性对的离散对数问题提出了一个有效的主动秘密共享方案，通过周期性地刷新影子秘密提高了其安全性，并能验证影子秘密的真实性，可应用于现实中秘密及数据库的长期保护。Wang X 等[20]基于离散对数难解性假设提出一种无可信方的可适应主动秘密共享方案，参与者数及门限值在 2 个相邻时间间隔内可变保证了方案安全性，但该方案的复杂度为 $O(n^3)$。文献[21]基于曲线密码体制提出一种主动秘密共享方案，每个成员既作分发者又作验证者，由秘密生命期的变化和成员间相互验证来实现动态性和不需第三可信方，并解决了秘密更新和影子密钥复用问题；方案在安全性上有所提高，具有较高实践工程价值。

此外，防止欺骗的秘密共享方案还可以依据解决方法分为以下 3 类：公钥体制加密方案、纠错编码方案、方案本身特点。对于第一类，分发者使用公钥体制将影子秘密进行加密后分发给参与者，参与者在收到影子秘密后可利用私钥进行验证或解密，可检测影子秘密的真实性，如文献[12,14,16,19,20]，影子秘密的验证基于离散对数的难解性，大整数分解的困难性假设。该类方法在验证欺骗时由于需要进行数字签名和信息交互，增加了通信量和公开参数。第二类是参与者收到分发者分发的一个编码后利用纠错码将其自动恢复，如文献[22]中方案，但若参与恢复过程中欺骗者过多时会增大通信量且验证方式有限制，一般适合于欺骗者较少的情况。另外还有一种就是使用方案本身特点防止欺骗，比如文献[23,24]中方案利用线性集合特点、散列函数、差集等数学工具来降低欺骗的概率。

显然，对于秘密共享过程中的欺诈问题，目前仍然缺乏保证高安全性、高扩展性、低复杂度的方案。本文在 Shamir 的秘密共享基础上，考虑多于 t 个参与者时所出现的安全问题，改进其影子秘密生成方案；在保证复杂度的前提下提高其安全性，为改善秘密共享过程的安全性提供新的方案。

2 Shamir 秘密共享机制

2.1 秘密共享同态

Benaloh[25]提出了秘密共享同态的概念，下面对其进行论述。S 为主秘密空间（secret domain），T 为对应主秘密的影子秘密空间，函数 $F_I: T \to S$ 是 (t,n) 秘密共享的诱导函数（induced function）。该函数把基于任意包含 t 个影子秘密 $\{s_{i_1}, s_{i_2}, \cdots, s_{i_t}\}$ 子集的秘密 s 定义为 $s = F_I(s_{i_1}, s_{i_2}, \cdots, s_{i_t})$，其中 $I = \{s_{i_1}, s_{i_2}, \cdots, s_{i_t}\}$。

定义 1 秘密共享同态[25]：假设 $\oplus$ 和 $\otimes$ 分别是在集合 S 和 T 元素上的 2 个函数，如果对于任意子集 I 和 $s = F_I(s_{i_1}, s_{i_2}, \cdots, s_{i_t})$，$s' = F_I(s'_{i_1}, s'_{i_2}, \cdots, s'_{i_t})$ 有 $s \oplus s' = F_I(s_{i_1} \otimes s'_{i_1}, s_{i_2} \otimes s'_{i_2}, \cdots, s_{i_t} \otimes s'_{i_t})$，就可认为一个 (t,n) 秘密共享方案具有 $(\oplus,\otimes)$ 同态性。

由定义 1 可知，Shamir 的 (t,n) 秘密共享方案满足同态 $(+,+)$ 性，即有 $s + s' = F_I(s_{i_1}, s_{i_2}, \cdots, s_{i_t}) + F_I(s'_{i_1}, s'_{i_2}, \cdots, s'_{i_t}) = F_I(s_{i_1} + s'_{i_1}, s_{i_2} + s'_{i_2}, \cdots, s_{i_t} + s'_{i_t})$ 成立。

2.2 Shamir 的(*t*,*n*)秘密共享方案

Shamir 提出的 (t,n) 秘密共享方案是基于 Lagrange 插值公式构造的，它可以描述如下[1]。

1) 初始化阶段：秘密分发者 D 随机地从有限域 $GF(p)$ 中选取 n 个不同的非零元素 $x_1, x_2, \cdots, x_n$ 标识每一个影子秘密持有者 $U_r = \{U_1, U_2, \cdots, U_n\}$ $(r = 1,2,\cdots,n)$，公开 x_r 及其对应的 U_r。

2) 秘密分发阶段：D 要分发的秘密为 $s \in Z_q$（q 为大素数），在 $GF(p)$ 内任意选择 $(t-1)$ 个元素 $a_i (i = 1,2,\cdots,t-1)$ 构成 $(t-1)$ 阶多项式

$$f(x) = \sum_{i=1}^{t-1} a_0 + a_i x^i \bmod p$$

其中，p 是一个大素数且 $p > s$，秘密 $s = f(0) = a_0$。D 为所有的 $U_r \in U$ 生成 n 个影子秘密

$$s_r = f(x_r) = \sum_{i=1}^{t-1} a_0 + a_i x_r^i \bmod p (r = 1,2,\cdots,n)$$

然后把 s_r 安全地发送给相应的 U_r。

3) 秘密恢复过程：任何 t 个影子秘密持有者 $\{U_1, U_2, \cdots, U_t\}$ 发送他们的影子秘密并使用拉格朗日插值公式

$$s = f(0) = \sum_{i=1}^{t} f(x_l) \prod_{v=1, v \neq l}^{t} \frac{-x_v}{x_l - x_v} \bmod p$$

便可以恢复出秘密 s。

Shamir 的方案满足秘密共享方案的安全需求，即：①任意不少于 t 个影子秘密能恢复出主秘密；②少于 t 个影子秘密不能得到主秘密的任何信息。

3　基于 Shamir 的秘密共享改进算法

在 Shamir 的秘密共享方案中，秘密分发者把秘密 s 分为 n 个影子秘密并分发给持有者，其中任意不少于 t 个影子秘密均能恢复秘密 s，少于 t 个影子秘密则得不到秘密 s 的任何信息。现实的秘密恢复过程中可能存在超过 t 个参与者的情形，在 Shamir 的秘密共享方案基础上，通过引入影子秘密的线性组合——拉格朗日因子（Lagrange factor）来恢复秘密，并进一步扩展为一个多秘密共享方案，增强其安全性及可靠性。

3.1　秘密共享模型

本节对秘密共享过程中包含欺骗者模型成员与过程进行描述。

3.1.1　秘密共享成员

1) 秘密分发者 D：把秘密 s 分为 n 个影子秘密，并分发给影子秘密持有者 U_r。

2) 影子秘密持有者 U_r：拥有分发者分发有效影子秘密的成员。

3) 敌手 A：秘密恢复过程中的敌手可以分为 2 类：内部敌手和外部敌手，外部敌手指秘密恢复时没有分发者分发有效影子秘密的攻击者，简称攻击者。内部敌手指参加秘密恢复时影子秘密持有者 U_r 中的共谋成员，简称欺骗者。

4) 参与者 P_j：参与秘密恢复过程成员，包括部分影子秘密持有者 U_r 和敌手 A。

3.1.2　模型描述

文中讨论在外部敌手参与秘密恢复过程并试图获取秘密的安全性。当有多于 t 个参与者参与秘密恢复过程时，外部敌手仍可获取秘密。下面提出一个安全秘密恢复方案的概念。

定义 2　安全秘密恢复方案。方案保证秘密仅能通过拥有有效影子秘密的参与者恢复，即外部敌手参与秘密恢复过程得不到秘密。

秘密恢复过程中超过 t 个参与者时，大部分论文仅讨论 t 个参与者情形。这可能存在一个安全问题：攻击者伪装成影子秘密持有者但提供无效影子秘密，得到 t 个影子秘密后即可恢复出秘密。换句话说，传统的用户身份认证方案或可验证秘密共享方案需要在秘密恢复之前确保所有参与者的影子秘密是有效的。由于 2 种方案一次分别仅能验证一个用户和一个影子秘密，增加了额外复杂度。此外，秘密恢复成功与否与仅与影子秘密有关。

在秘密恢复过程中，欺骗者通过提供无效影子欺骗诚实的 U_r。内部欺骗者能唯一地恢复秘密，而诚实的 U_r 得到无效秘密。

3.2　安全性需求

在 Shamir 的秘密共享方案基础上，为满足当前的实际安全要求，提出新的安全属性需求如下。

1) 对于秘密 s：每个秘密仅能通过任意不少于 t 个拥有有效影子秘密参与者恢复，而不能被攻击者恢复。

2) 对于影子秘密：多秘密共享方案中，U_r 的影子秘密能重复用于恢复多个秘密。因此，在秘密恢复过程中要保证其安全，否则不能重复使用。在进行安全分析时，应检测在攻击者能得到最多信息用于恢复秘密情形的安全性，即攻击者试图获取在恢复最后一个秘密过程的影子秘密，攻击者是最后一个发送拉格朗日因子给其他参与者的成员，并可获取所有另外的拉格朗日因子。因此假设秘密恢复阶段均有 n 个影子秘密参与。

3) 对于门限值：恢复的秘密不应该妥协任何未恢复秘密的隐秘性。因为每个恢复的秘密是影子秘密的一个函数，U_r 依据每个恢复的秘密建立影子秘密方程。这些方程不应该妥协影子秘密和未恢复秘密的隐秘性，否则未恢复秘密的门限值将减少。在门限安全分析阶段，将检测在敌手得到最多信息情形下门限值安全性，应假设有 $t-1$ 个欺骗者试图在其余秘密已恢复情形下去恢复最后一个秘密，即恢复最后一个秘密时欺骗者最后发送他们的拉格朗日因子。

3.3　改进算法流程

文中提出的改进算法主要分为初始化。秘密分发和秘密恢复 3 个阶段，每个阶段既有它独立的过程，又有相互联系的方面。流程图可以简要地表述整个秘密共享算法执行过程，如图 1 所示。

改进算法具体过程如下。

1) 初始化

秘密分发者 D 随机地从有限域 $GF(p)$ 中选择 $r(r=1,2,\cdots,n)$ 个非零常数 x_r 并对 U_r 进行标记，公开 x_r 及其对应的 U_r。

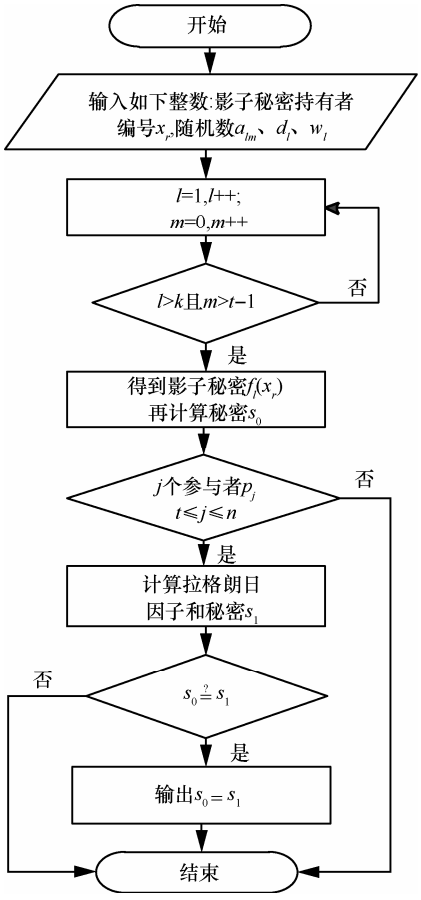


图 1 改进算法流程

2) 秘密分发

分发过程由可信的秘密分发者 D 执行，主要用于生成分发给每个 U_r 的影子秘密。秘密分发者执行影子秘密生成算法生成 n 个影子秘密并将其分发给对应的 U_r。

Step1 随机选择 $kt(kt>n-1)$ 个非零系数 $\{a_{lm}\mid a_{lm}\in GF(p);1\leqslant l\leqslant k,0\leqslant m\leqslant t-1;a_{lm}\neq 0\}$ 构造 k (k 为常数)个 $(t-1)$ 阶多项式

$$f_l(x)=\sum_{m=0}^{t-1}a_{lm}=a_{l0}+a_{l1}x+\cdots+a_{l(t-1)}x^{t-1} \quad (1)$$

Step2 计算 U_r 的影子秘密 $f_l(x_r)(l=1,2,\cdots,k)$。即有

$$f_l(x_r)=(\sum_{m=0}^{t-1}a_{1m}x_r^m,\sum_{m=0}^{t-1}a_{2m}x_r^m,\cdots,\sum_{m=0}^{t-1}a_{km}x_r^m) \quad (2)$$

Step3 对任意秘密 s， D 在有限域 $GF(p)$ 内总能找到整数 d_l 和 w_l (其中， $l=1,2,\cdots,k;w_i\neq w_j;w_i\notin\{x_1,x_2,\cdots,x_n\}$)满足

$$s=\sum_{l=1}^{k}d_lf_l(w_l)=d_1f_1(w_1)+\cdots+d_kf_k(w_k) \quad (3)$$

Step4 通过私有安全信道发送 $f_l(x_r)$ 给对应的 U_r，并广播整数 d_l 和 w_l。

3) 秘密恢复

需要恢复秘密 s 的参与者 P_r 向参与者成员 $\{P_1,P_2,\cdots,P_j\}(t\leqslant j\leqslant n)$ 发送恢复秘密请求，通过接收 $j-1$ 个参与者发送的拉格朗日因子 C_r^{ϕ} 来恢复秘密。拉格朗日因子 C_r^{ϕ} 为秘密 $s=\sum_{l=1}^{k}d_lf_l(w_l)$ 的一个线性组合，在秘密共享过程中的敌手得到其余参与者发送的拉格朗日因子也恢复不了真正有效的影子秘密，从而恢复出秘密 s，可提高影子秘密和秘密的安全性；此外，秘密恢复时拉格朗日因子可以直接防止欺骗问题，从而不需要对各参与者影子秘密进行逐个验证，提高了秘密恢复效率。设 U_r 中 j 个参与者组成的授权子集为 ϕ，其执行操作如下。

Step1 通过由 D 发送的影子秘密 $f_l(x_r)$，参与者 P_r 使用式(4)得到其唯一的拉格朗日因子 $C_r^{\phi}(1\leqslant r\leqslant j)$

$$C_r^{\phi}=\sum_{l=1}^{k}(d_lf_l(x_r)\prod_{v=1,v\neq r}^{j}\frac{w_l-w_v}{x_r-x_v} \quad (4)$$

其中， $\{\phi\in 1,2,\cdots,n\},|\phi|\geqslant t$。

Step2 参与者 P_r 在收到成员发送的秘密恢复申请后，将其拉格朗日因子 C_r^{ϕ} 通过秘密通道发送给其余 $j-1$ 个参与者。

Step3 P_r 通过收到的 $j-1$ 个拉格朗日因子 C_r^{ϕ} 使用式(5)计算出需恢复的秘密 s。

$$s=\sum_{r=1}^{j}C_r^{\phi} \quad (5)$$

3.4 多秘密共享扩展算法

在上述改进算法描述基础上，将其扩展为多秘密共享。需要满足如下 2 个安全要求：1)每个有效的影子秘密可重复用于恢复另外的秘密；2)为了保证门限值安全，每个恢复的秘密不能妥协未恢复秘密的隐秘性。下面就扩展为 h 个秘密的算法进行描述并在 4.2.2 节证明其安全性。

1) 秘密分发

D 选择 k (其中 k 为常数且) $\{kt>h(n+1)-2\}\cap\{k<(h-1)(n-t+2)\}$ $(t-1)$ 个 $(t-1)$ 阶随机多项式 $f_l(x)(l=1,2,\cdots,k)$，并对每个对应标记 x_r 的 U_r 生成影子秘密 $f_l(x_r)(l=1,2,\cdots,k)$。对任何一个秘密 $s_i(i=1,2,\cdots,h)$， D 在有限域 $GF(p)$ 内能找到满足 $s_i=\sum_{l=1}^{k}d_{i,l}f_l(w_l)(w_i\neq w_j,w_i\in\{x_1,x_2,\cdots,x_n\})$ 的整数 $d_{i,l}$、 $w_l(l=1,2,\cdots,k)$，且 $(d_{i,1},d_{i,2},\cdots,d_{i,k})(i=1,2,\ \cdots,h)$

是线性独立矢量。之后 D 公开整数 $d_{i,l}$、w_l 及 x_r。

2) 秘密恢复

在秘密恢复阶段有 $j(t \leqslant j \leqslant n)$ 个参与者 $\{P_1, P_2, \cdots, P_j\}$ 来恢复秘密 s_i，每个参与者使用他的影子秘密 $f_l(x_r)$ 计算并秘密发送一个拉格朗日因子

$$C_r^{\phi} = \sum_{l=1}^{k} d_{i,l} f_l(x_r) \prod_{v=1, v\neq r}^{j} \frac{w_l - x_v}{x_r - x_v}$$

$$r = 1,2,\cdots,j\ ;\ \ \phi \in \{1,2,\cdots,n\}\ ,\ \ |\phi| \geqslant t$$

给所有的参与者，每个参与者在知道另外 $j-1$ 个 C_r^{ϕ} 后均可使用 $s_i = \sum_{r=1}^{k} C_r^{\phi} (i = 1,2,\cdots,h)$ 来恢复秘密。

4　算法分析与仿真

4.1　改进算法复杂度

算法复杂度可分为度量算法执行时间长短的时间复杂度和度量算法所需存储空间大小的空间复杂度。由于近年存储技术快速发展，算法在执行过程中所需存储空间对算法影响逐渐减小。通过上述秘密共享算法分析，算法执行过程只需要存储公开信息和需要保密的秘密，存储空间较小；随着 U_r 和 P_j 增加，存储空间呈线性增加，在数量级上没有变化。此外，当前硬件的发展使得较小的代价即可获得较大的存储容量。因此，在该算法中时间复杂度成为衡量算法效率的主要因素，本文聚焦于秘密共享算法的时间复杂度分析。

文中算法时间开销主要集中在影子秘密生成 $s = \sum_{l=1}^{k} d_l f_l(w_l)$ 和秘密恢复 $s = \sum_{l=1}^{k} C_r^{\phi}$ 2 个过程，算法的时间复杂度由 2 部分的和构成。整个秘密共享过程中 n 表示分发者分发的影子秘密数量，k 表示秘密多项式的个数，t 表示门限值，j 表示参与恢复过程的参与者个数。具体分析如下。

//初始化

随机选择 $r(r = 1,2,\cdots,n)$ 个非零常数 x_r 并对 U_r 进行标记

//执行 $2n$ 次

//秘密分发

①选择 kt 个非零系数并构造 k 个 $t-1$ 阶多项式

//执行 $kt+k$ 次

②计算影子秘密 $f_l(x_r)$

```
for(i=1; i<k; i++){
    for(j=1; j<k;j++){
        计算影子秘密 f_l(x_r)；
    }
}                                   //执行 nk^2 次
```

③找到整数 d_l 和 w_l 计算秘密 s //执行 k 次

//秘密恢复

①计算拉格朗日因子

```
for(l=1; l<k; l++){
    while(i=1; i<n;i++){
        计算拉格朗日因子 C_r^φ；
    }
}                                   //执行 knlg^2 n 次
```

②通过因子累加计算得到秘密 s。//执行 j 次

算法总执行次数：$f(n) = kn\lg^2 n + nk^2 + kt + 2n + 2k + j$，忽略低次幂、高次幂系数、常数后可知该算法的计算复杂度为 $T(n) = O(n\lg^2 n)$。因此，在保证安全前提下，文中改进算法的时间复杂度和大多数基于 Lagrange 插值秘密共享算法均处于同一数量级，并未增加时间开销。

改进算法复杂度计算量的各组成部分如表 1 所示。

表 1　　改进算法计中算量构成

操作	秘密分发	秘密恢复
拉格朗日插值	0	$kn\lg^2 n$
构造插值多项式	nk^2+kt+k	0
累加运算	$2n+2k$	j

改进算法与已有研究中提出的方案在预防欺骗、复杂度与安全性等综合指标的比对分析如表 2 所示。

表 2　　与现有方案的指标比对

方案	预防欺骗	复杂度	安全性
文献[1](Shamir 秘密共享算法)	否	$O(n\lg^2 n)$	较低
文献[12](动态秘密共享算法)	能	$O(n\lg^2 n)$	条件安全
文献[20](主动秘密共享算法)	能	$O(n^3)$	条件安全
本文提出的 Shamir 改进算法	能	$O(n\lg^2 n)$	较高

表 1 可知，本文所提出的改进算法在保持同样时间的复杂度及稳定性同时提高了其安全性。

4.2　正确性与安全性

4.2.1　*改进算法*

1) 正确性

命题 1　在秘密恢复过程中，秘密 s 的计算方

法是正确的。

证明 要证明命题 1 只需证明式(3)和式(5)右边相等即可。由式(1)知，秘密共享过程中第 r 个参与为 x_r 的 k 个秘密多项式如下

$$\begin{cases} f_1(x)=\sum_{m=0}^{t-1}a_{1m}x^m=a_{10}+a_{11}x+\cdots+a_{1(t-1)}x^{t-1} \\ f_2(x)=\sum_{m=0}^{t-1}a_{2m}x^m=a_{20}+a_{21}x+\cdots+a_{2(t-1)}x^{t-1} \\ \quad\vdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \vdots \\ f_k(x)=\sum_{m=0}^{t-1}a_{km}x^m=a_{k0}+a_{k1}x+\cdots+a_{k(t-1)}x^{t-1} \end{cases} \tag{6}$$

则 D 发送给他的影子秘密为

$$f_l(x_r)=(\sum_{m=0}^{t-1}a_{1m}x_r^m,\sum_{m=0}^{t-1}a_{2m}x_r^m,\cdots,\sum_{m=0}^{t-1}a_{km}x_r^m)$$

将式(4)代入式(5)可得

$$\begin{aligned} s&=\sum_{r=1}^{k}C_r^{\phi}=\sum_{r=1}^{j}\sum_{l=1}^{k}d_lf_l(x_r)\prod_{v=1,v\neq r}^{j}\frac{w_l-x_v}{x_r-x_v} \\ &=\sum_{r=1}^{j}(d_1f_1(x_r)\prod_{v=1,v\neq r}^{j}\frac{w_l-x_v}{x_r-x_v}+d_2f_2(x_r) \\ &\prod_{v=1,v\neq r}^{j}\frac{w_2-x_v}{x_r-x_v}+\cdots+d_1f_1(x_r)\prod_{v=1,v\neq r}^{j}\frac{w_k-x_v}{x_r-x_v}) \end{aligned} \tag{7}$$

拉格朗日插值多项式

$$f_l(x)=\sum_{r=1}^{k}f_l(x_r)\prod_{v=1,v\neq r}^{j}\frac{x-x_v}{x_r-x_v} \tag{8}$$

由式(7)和(8)可知，式(3)与式(7)相等。因此等式(3)和(5)右边相等，即命题 1 正确。

2) 安全性

本方案在秘密发送的过程中采用安全的信道进行，以避免内外部敌手。

① 有攻击者的安全性

秘密恢复过程中，如果参与者中包含持有无效影子秘密人员，导致最后恢复的秘密无效。为了验证该方案安全性，假设攻击者在参与秘密恢复过程中能获得最多信息，即恢复阶段中有 n 个参与者 $\{P_1,P_2,\cdots,P_n\}$ 且攻击者是最后一个发送其拉格朗日因子的人，只需验证攻击者在获取了 $n-1$ 个 C_r^{ϕ} 后能否恢复出秘密即可。由式(6)可知，k 个 $t-1$ 阶多项式 $f_l(x)(l=1,2,\cdots,k)$ 包含 kt 个系数，它的系数构成一个 $k\times t$ 矩阵 $\boldsymbol{A}=[a_{lm}](l=1,2,\cdots,k;m=0,1,\cdots,t-1)$，且每个 C_r^{ϕ} 是 $f_l(x)$ 的线性函数，攻击者得到 $n-1$ 个 C_r^{ϕ} 后可构建 $n-1$ 个方程。因为 $kt>n-1$，由线性方程组解的条件可知，攻击者通过解这 $n-1$ 个方程得不到唯一解，他只能得到秘密 s 的一个线性关系或者完全得不到 s 的任何信息，即得不到秘密多项式 $f_l(x)$，恢复秘密失败。因此，即使攻击者在获得 $n-1$ 个 C_r^{ϕ} 也恢复不了秘密，算法安全。

② 有欺骗者的安全性

接下来分析有任意 $t-1$ 个欺骗者时该算法的安全性。欺骗者试图从他们自己的影子秘密 $f_l(x_r)=(\sum_{m=0}^{t-1}a_{1m}x_r^m,\sum_{m=0}^{t-1}a_{2m}x_r^m,\cdots,\sum_{m=0}^{t-1}a_{km}x_r^m)$ 恢复秘密。由于在 k 个 $t-1$ 阶多项式 $f_l(x)(l=1,2,\cdots,k)$ 上秘密 $s=\sum_{l=1}^{k}d_lf_l(w_l)$ 是一个线性组合。欺骗者使用他们持有的 $k(t-1)$ 个影子秘密可构造 $k(t-1)$ 个方程。因为 $kt>n-1$（kt 是每个 $(t-1)$ 阶多项式 $f_l(x)(l=1,2,\cdots,k)$ 未知系数个数），欺骗者解不出秘密多项式 $f_l(x)$，秘密恢复失败。因此内部欺骗者不能通过 $t-1$ 个影子秘密恢复出秘密。

此外，对于任意秘密 s，针对每对 i 和 j，秘密 $s=\sum_{l=1}^{k}d_lf_l(w_l)$ 时 D 需要选择 $w_i\neq w_j$。如果 $w=w_i=w_j$，对于每对 i 和 j，敌手在知道 t 个 C_r^{ϕ} 后仍能恢复出秘密。这是因为秘密 s 是一个由 $t-1$ 阶多项式 $\sum_{l=1}^{k}d_lf_l(x)$ 叠加而成的，每个参与者 P_r 需要使用他自己的影子秘密计算并发送拉格朗日因子 C_r^{ϕ} 给每个参与者。敌手可通过每个发送的拉格朗日因子 C_r^{ϕ} 中恢复出影子秘密叠加 $\sum_{l=1}^{k}d_lf_l(x_r)$。因而，在知道 t 个影子秘密的叠加后，敌手就能恢复出多项式的叠加 $\sum_{l=1}^{k}d_lf_l(x)$，从而得到秘密。相反，当 $w_i\neq w_j$ 时，敌手得不到秘密 s。

4.2.2 扩展算法

1) 正确性

由命题 1 知，改进算法中秘密 s 的计算方法是正确的，即可通过 $s=\sum_{l=1}^{k}C_r^{\phi}$ 得到秘密。而在扩展算法中共有 h 个秘密，每个秘密均采用相同的方法计算，则可以恢复出 h 个秘密。

2) 安全性

① 影子秘密安全性

因为每个 U_r 发送的拉格朗日因子 $C_r^{\phi}=\sum_{l=1}^{k}(d_lf_l(x_r)\prod_{v=1,v\neq r}^{j}\frac{w_l-x_v}{x_r-x_v})$ 是 k 个影子秘密 $f_l(x_r)(l=1,2,\cdots,k)$ 的一个线性组合，因此每个参与者发送的拉格朗日因子可以保证影子秘密的安全性。下面考虑给予外部攻击者最多的信息来恢复影

子秘密的情形。首先假设在秘密恢复阶段中敌手是 j 个参与者中最后一个发送 C_r^{ϕ} 的人并试图得到恢复最后一个秘密 s_h 的影子秘密（前面 $h-1$ 个秘密 $s_i(i=1,2,\cdots,h-1)$ 已经恢复了）。假设用 n 个拉格朗日因子恢复每个秘密（包括当前正在恢复的秘密 s_h）。由于每个发送的拉格朗日因子和每个秘密是 kt 个系数的 $t-1$ 阶多项式 $f_l(x)$ 的线性函数，敌手从拉格朗日因子和已恢复秘密的 $n-1$ 个方程中最多能构建 $(h-1)n+(n-1)$ 个方程。总地来说，敌手最多可以得到 $(h-1)n+(n-1)+(h-1)$ 个方程。由于 $kt>(h-1)n+(n-1)+(h-1)\rightarrow kt>h(n+1)-2$，不能得出秘密多项式 $f_l(x)(l=1,2,\cdots,k)$ 唯一解。因此，敌手不能恢复影子秘密。

② 门限值安全性

接下来分析多个欺骗者获取最多信息时门限值的安全性。假设有 $t-1$ 个欺骗者，他们在 $h-1$ 个秘密 $s_i(i=1,2,\cdots,h-1)$ 已经恢复前提下试图恢复最后一个秘密 s_h。首先，分析是否可以从预先恢复的秘密 s_i 的一个线性组合恢复出 s_h。对于每对 i 和 j，每个秘密为 $s_i=\sum_{l=1}^{k}d_{i,l}f_l(w_l)(w_i\neq w_j)$，由于 $(d_{i,1},d_{i,2},\cdots,d_{i,k})(i=1,2,\cdots,h)$ 是独立线性矢量，他们不可能从预先恢复秘密的线性组合中得到 s_k。其次，再检验是否能从欺骗者自己影子秘密的组合内容、预先恢复的 $h-1$ 个秘密 $s_i(i=1,2,\cdots,h-1)$ 及另外 $n-t+1$ 个 U_r 发送的拉格朗日因子中恢复 s_h。假设有 s 个拉格朗日因子用于恢复每个秘密 s_i。因为每个发送的拉格朗日因子和每个秘密是 $t-1$ 阶，且含有 kt 个系数多项式 $f_l(x)(l=1,2,\cdots,k)$ 的线性函数，欺骗者能构建 $(h-1)(n-(t-1)+(h-1))$ 个方程（其中 $(h-1)(n-(t-1))$ 个方程来自于另外 U_r 发送的拉格朗日因子，$h-1$ 个方程来自于已恢复的秘密）。此外，这些欺骗者可以使用他们自己拥有的 $h(t-1)$ 个影子秘密构建 $k(t-1)$ 个方程。总地来说，他们能构造 $(h-1)(n-(t-1)+(h-1))+(h-1)+k(t-1)$ 个方程。$kt>(h-1)(n-(t-1)+(h-1))+(h-1)+k(t-1)\rightarrow k>(h-1)(n-t+2)$，这能防止欺骗者解出秘密多项式 $f_l(x)(l=1,2,\cdots,k)$ 而得到最后的秘密 s_h。因此，未恢复秘密的门限值依然与原有值相同。

4.3 仿真实验

4.3.1 实验环境设置及指标获取

实验采用和文献[12]相似环境，使用 MyEclipse 8.6 实现并部署文中算法，在局域网下计算机配置 4 GB 内存及 Win7 操作系统；因局域网下计算机使用不同主频 CPU，因此仿真过程中以 CPU 时间作为衡量指标。实验整体环境贴近真实随机的秘密共享过程，以反映算法在真实环境中的有效性。

文中提出的改进算法在时间复杂度上与传统经典算法相比较处于同一个数量级上，可假定它们的执行效率基本一致。

4.3.2 实验结果及分析

在实验中，可依据秘密恢复过程中影子秘密数量 n、秘密多项式的个数 k、门限 t 这 3 个值来验证算法有效性。

图 2 给出秘密分发执行时间随影子秘密数量 n 变化情况，随着影子秘密数目增加，执行时间呈线性增长。

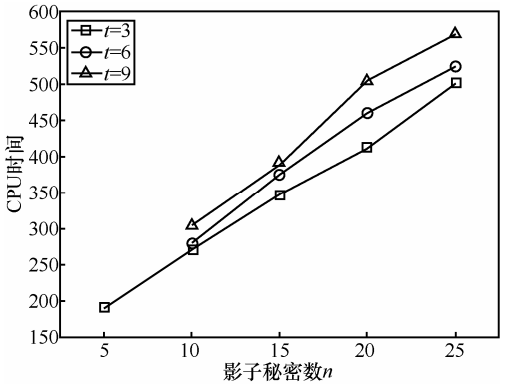


图 2　秘密分发计算量随影子秘密 n 变化曲线

图 3 给出不同的门限值 t 对计算性能影响情况，结果表明门限值对计算性能影响较小。

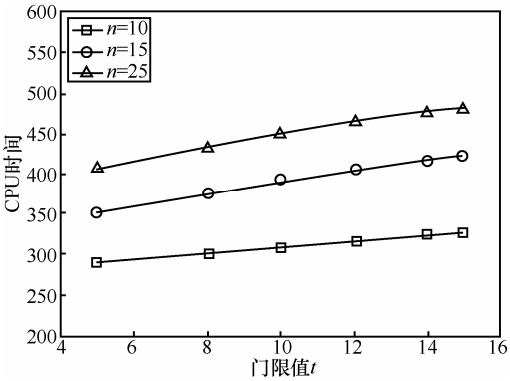


图 3　秘密分发计算量随 t 值变化曲线

图 4 给出秘密分发阶段计算量随影子秘密数量变化情况。当秘密多项式个数一定时，其计算性能

改变不明显；当其增大到一定程度时计算性能会随着影子秘密数有激增。

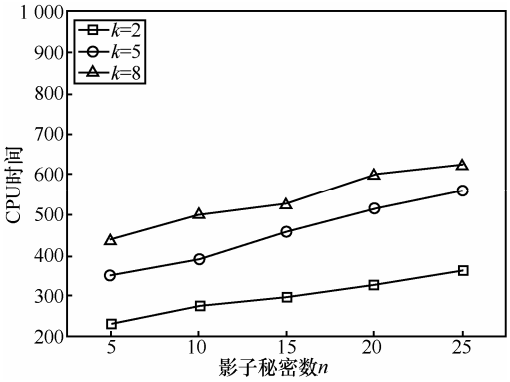


图 4 秘密分发计算量影子秘密 n 变化曲线

图 5 给出秘密恢复过程计算量随 k 值变化，不同网络规模对其计算性能影响不大，但随着秘密多项式增加其复杂度明显增大。因为恢复过程中有拉格朗日插值计算，多项式个数过多会影响其性能。

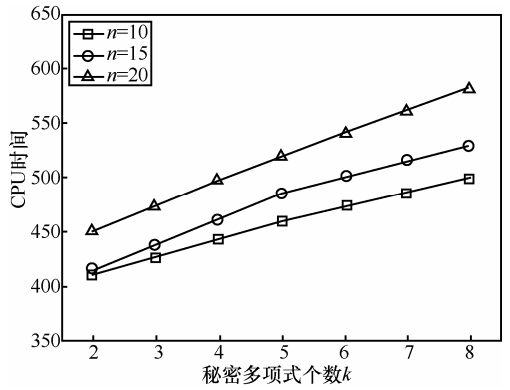


图 5 秘密恢复过程计算量随 k 值变化曲线

图 6 和图 7 验证了执行时间与门限值及秘密多项式个数的关系。结果显示相较于门限值，秘密多项式个数对算法执行影响更大。

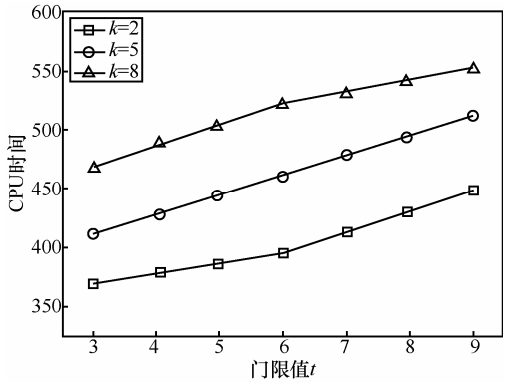


图 6 秘密恢复过程计算量随门限值 t 变化曲线

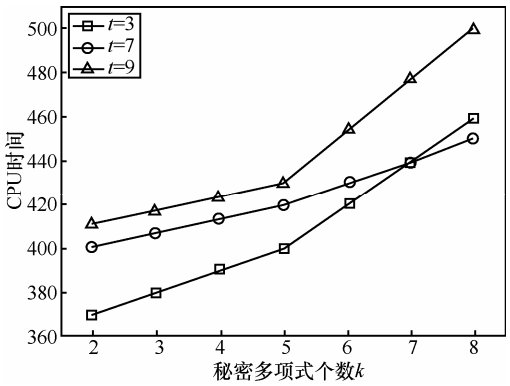


图 7 秘密恢复过程计算量随秘密多项式 k 变化曲线

5 结束语

本文在 Shamir 的秘密共享方案基础上讨论此种情形下秘密共享问题，提出了一个秘密共享过程中包含欺骗者模型；分析了 Shamir 的秘密恢复方案并说明在 Shamir 的秘密恢复过程中有多于 t 个参与者时，通过改进 Shamir (t,n) 秘密共享方案可防止欺骗者获取秘密，本文进一步将其扩展为一个多秘密共享方案。与现有秘密共享方案相比，该方案在同样复杂度条件下改善了安全性。

参考文献：

[1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[2] BLAKLEY G R. Safeguarding cryptographic keys[A]. Managing Requirements Knowledge, International Workshop[C]. IEEE Computer Society, 1979.313-313.

[3] 肖清华. 秘密共享及相关应用研究[D]. 杭州：浙江大学, 2005.
XIAO Q H. Research on Secret Sharing and Its Related Applications [D]. Hangzhou: Zhejiang University, 2005.

[4] CHOR B, GOLDWASSER S, MICALI S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults[A]. 2013 IEEE 54th Annual Symposium on Foundations of Computer Science[C]. 1985. 383-395.

[5] KAYA K, SELÇUK A A. A verifiable secret sharing scheme based on the Chinese remainder theorem[A]. Progress in Cryptology- INDOCRYPT 2008[C]. Springer Berlin Heidelberg, 2008. 414-425.

[6] LU Q, XIONG Y, HUANG W, *et al*. A distributed ECC-DSS authentication scheme based on CRT-VSS and trusted computing in MANET[A]. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference[C]. 2012.656-665.

[7] KAYA K, SELÇUK A A. A verifiable secret sharing scheme based on the chinese remainder theorem[A]. Progress in Cryptology-INDOCRYPT 2008[C]. Springer Berlin Heidelberg, 2008.414-425.

[8] HARN L, FUYOU M, CHANG C C. Verifiable secret sharing based on the Chinese remainder theorem[J]. Security and Communication Networks, 2014, 7(6): 950-957.

[9] ZHANG L, GUO F, LIU S, *et al*. A verifiable multi-secret sharing scheme based on LUC cryptosystem[A]. Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on IEEE[C]. 2011.2905-2908.

[10] HU C, LIAO X, CHENG X. Verifiable multi-secret sharing based on LFSR sequences[J]. Theoretical Computer Science, 2012, 445: 52-62.

[11] LAIH C S, HARN L, LEE J Y, *et al*. Dynamic threshold scheme based on the definition of cross-product in an n-dimensional linear space[A]. Advances in Cryptology—CRYPTO'89 Proceedings[C]. Springer New York, 1990.286-298.

[12] 李大伟, 杨庚. 基于单向散列链的可更新(*t*,*n*)门限秘密共享方案[J]. 通信学报, 2010,31(7):128-135.
LI D W, YANG G. Renewable (*t*, *n*) threshold secret sharing scheme based on one-way hash chain[J].Journal on Communications, 2010, 31(7): 128-135.

[13] LIN H Y, YEH Y S. Dynamic multi-secret sharing scheme[J]. International Journal of Contemporary Mathematical Sciences, 2008, 3(1): 37-42.

[14] QU J, ZOU L, ZHANG J. A practical dynamic multi-secret sharing scheme[A]. Information Theory and Information Security (ICITIS), 2010 IEEE International Conference[C]. 2010. 629-631.

[15] TADAYON M H, KHANMOHAMMADI H, ARABI S. An attack on a dynamic multi-secret sharing scheme and enhancing its security[A]. Electrical Engineering (ICEE), 2013 21st Iranian Conference[C]. 2013.1-5.

[16] 贾秀芹, 赖红. 抗欺诈的动态(*t*, *n*)门限秘密共享方案[J]. 计算机工程, 2011, 37(4):152-154.
JIA X Q, LAI H. Anti-cheat and dynamic (*t*, *n*) threshold secret sharing scheme[J]. Computer Engineering, 2011, 37(4):152-154.

[17] ESLAMI Z, RAD S K. A new verifiable multi-secret sharing scheme based on bilinear maps[J]. Wireless Personal Communications, 2012, 63(2): 459-467.

[18] HERZBERG A, JARECKI S, KRAWCZYK H, *et al*. Proactive secret sharing or: How to cope with perpetual leakage[A]. Advances in Cryptology—CRYPT0'95[C]. Springer Berlin Heidelberg, 1995. 339-352.

[19] SUN H, ZHENG X, YU Y. A proactive secret sharing scheme based on elliptic curve cryptography Education Technology and Computer Science[A]. First International Workshop on IEEE[C]. 2009.666-669.

[20] WANG X. A novel adaptive proactive secret sharing without a trusted party[J]. IACR Cryptology ePrint Archive, 2011,241.

[21] 范畅, 茹鹏. 一种基于 ECC 的动态秘密共享方案[J]. 计算机仿真, 2012, 29(12): 131-134.
FAN C, RU P. Proactive secret sharing scheme based on ECC[J]. Computer Simulation, 2012, 29(12): 131-134.

[22] NIKOV V, NIKOVA S. On a relation between verifiable secret sharing schemes and a class of error-correcting codes[A]. Coding and Cryptography[C]. Springer Berlin Heidelberg, 2006.275-290.

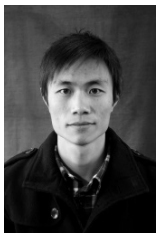
[23] OGATA W, KUROSAWA K, STINSON D R. Optimum secret sharing scheme secure against cheating[J]. SIAM Journal on Discrete Mathematics, 2006, 20(1): 79-95.

[24] JHANWAR M P, SAFAVI-NAINI R. On the share efficiency of robust secret sharing and secret sharing with cheating detection[A]. Progress in Cryptology–INDOCRYPT 2013[C]. Springer International Publishing, 2013.179-196.

[25] BENALOH J C. Secret sharing homomorphisms: Keeping shares of a secret secret[A]. Advances in Cryptology—CRYPTO'86[C]. Springer Berlin Heidelberg, 1987.251-260.

作者简介：

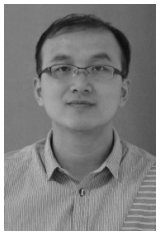
荣辉桂（1975-），男，湖南株州人，博士，湖南大学副教授、硕士生导师，主要研究方向为大数据、云计算、电子商务等。



莫进侠（1987-），男，湖南邵阳人，湖南大学硕士生，主要研究方向为数据分类、云计算、移动互联网等。

常炳国（1965-），男，陕西榆林人，博士，湖南大学副教授，主要研究方向为数据集成、云存储管理、电子政务理论及应用等。

孙光（1972-），男，山东金乡人，博士，湖南财政经济学院副教授，主要研究方向为云安全、大数据应用、云隐蔽软件等。



龙飞（1983-），男，湖南岳阳人，博士，长沙大学讲师，主要研究方向为云计算、电子商务、信息系统等。