基于大整数分解可公开验证的秘密共享方案①

曹 阳

(陕西理工学院 数学与计算机科学学院, 汉中 723000)

摘 要: 基于不定方程整数解的存在性及大整数分解的困难性, 以 Shamir(t,n)门限方案为基础, 提出了一种可公开验证的秘密共享方案. 方案利用大整数分解的困难性为共享者建立秘密份额, 通过不定方程整数解的存在性计算方程的特解组合, 共享秘密由共享者的秘密份额和特解组合元素共同计算恢复; 方案实现了对秘密份额、参与者之间及参与者对分发者的有效性验证. 安全分析表明, 该方案是安全的, 具有一定的实际应用价值.

关键词: 不定方程; 大整数分解; 秘密共享; 公开验证; 门限方案

Publicly Verifiable Secret Sharing Scheme Based on Large Numbers Factorization

CAO Yang

(School of Mathematics and Computer Science, Shaanxi University of Technology, Hanzhong 723000, China)

Abstract: Due to the existence of indeterminate equation integer solutions and the difficulty of large numbers factorization, a publicly verified secret sharing scheme was proposed based on Shamir(t, n) threshold scheme. With the difficulty of big integer factorization, the scheme established a secret share for the sharers and calculated special solution combination of equation through the existence of indeterminate equation integer solutions. Share secret was recovered common calculation of sharers' secret share and special solution combination elements. In addition, the scheme realized the effective validation of the secret share, between the participants, as well as participants and the distributors. Security analysis shows that the scheme is safe, and has certain practical value.

Key words: indeterminate equation; large numbers factorization; secret sharing; publicly verifiable; sharing scheme

密码学中, 密码体制的安全性取决于密钥的使用及管理, 但现实中却存在管理者不经意泄露主密钥、主密钥被他人窃取篡改毁坏、主密钥丢失等问题, 而无论那种问题都会导致系统处于不安全状态, 因此对密钥管理安全性研究便成为密码学研究中的一个极其重要的内容, 而秘密共享是密码学中的一个重要分支, 应用范围也由起初的密钥管理扩展到电子拍卖、数字签名、金融管理等多方面. 基于 Lagrange 插值多项式的 (t,n) 门限秘密共享方案最早由 Shamir[1]提出, 方案由一个秘密分发者 D 和 n 个共享者组成, 秘密分发者 D 将共享秘密数据拆分成 n 个子秘密数据分别交给 n 个共享者保管, 只有 t 个及 t 个以上的共享者共同合作才能恢复出共享秘密数据[1], 少于 t 个共享者合作无法得到共享秘密数据. 而这一秘密共享思想的提出为秘密安全存放提供了一个科学框架, 加之秘密数据的安全存放极其重要, 三十多年来, 大量的学者对此进行了大量的研究. 如文献[2, 3]对门限方案进行改进, 提出了多种门限方案的变体; 文献[4]基于大整数分解的困难问题, 提出了门限秘密共享方案; 文献[5]基于 RSA 算法和向量空间, 提出了一种向量空间上可公开验证的秘密共享方案; 文献[6]针对多个秘密由多个秘密持有者提供的情况, 提出了一个门限多重影子秘密共享方案; 文献[7, 8]基于向量空间, 提出了可验证、防欺诈秘密共享方案; 最终目的都是为了提高秘密共享的安全性. 本文针对秘密份额的有效性、共享者(包括分发者)之间欺诈行为, 以 Shamir(t,n)门限方案[1]为

① 基金项目:国家自然科学基金(21373132);陕西省教育厅资助项目(14JK1132);陕西理工学院科研计划资助项目(SLGKY14-09).
收稿时间:2015-06-26;收到修改稿时间:2015-09-06

基础, 基于不定方程整数解的存在性及大整数分解的困难性, 提出了一种可公开验证的秘密共享方案.

1 相关知识

设不定方程为:

$$b_{i_1}d_{\sigma(i_1)}+b_{i_2}d_{\sigma(i_2)}+...+b_{i_t}d_{\sigma(i_t)}=1+\delta\varphi(N) \quad (1)$$

其中, $b_{i_1},b_{i_2},...b_{i_t}$ 是两两互素的大整数且是从随机数序列 $b_i(1\le i\le n)$ 中任意选取的 t 个数, $\varphi(N)$ 是欧拉函数, δ 是随机大整数. 由于 $\gcd(b_1,b_2,...,b_n)=1$, 所以方程(1)必有一个正整数特解 $\{d_{\sigma(i_1)},d_{\sigma(i_2)},...,d_{\sigma(i_t)}\}$. 对于序列 b_i 能构成 C_n^t 个不定方程(1), 正整数特解共有 C_n^t 组, 称每一个方程的特解为特解组合. $A=\{A_1,A_2,...A_n\}$ 为合格子集, 其中 $A_i=\{d\sigma_{(i)}\}$ $(1\le i\le n)$, $\sigma_{(i)}$ 表示下标 $j_1j_2...j_t$, $j_1=i,j_2j_3...j_t$ 是 1 到 n 中除去 i 的 $n-1$ 个数中选取的 $t-1$ 个数递增排序, 显然 A_i 是各自所有特解组合中的一个元素.

2 秘密共享方案密钥协商协议

方案中, 共享者之间可相互验证有效性, 共享秘密恢复由共享者的秘密份额和不定方程特解组合元素共同计算恢复, 秘密份额的有效性验证过程中传递的是秘密份额的影子秘密. 方案由系统参数初始化、秘密份额分发、秘密份额的验证、秘密恢复四部分组成.

2.1 系统参数初始化

设 $U=\{U_1,U_2,...,U_n\}$ 是 n 个秘密共享者的集合, D 为分发者, $D\notin U$.

1) 随机选取两个大素数 p,q, 计算 $N=pq$, $\varphi(N)=(p-1)(q-1)$. 选取随机数 g, 满足 $g^{\varphi(N)}=1\bmod N$, 公开 N,g, $p,q,\varphi(N)$ 保密.

2) 分发者选取随机数 e, 满足 $(e,\varphi(N))=1$, 计算 d, $Q=g^e \bmod N$, 使得 $ed=1\bmod\varphi(N)$, 保密 e, 公开 Q,d.

2.2 秘密份额分发

1) 分发者 D 随机选取两两互素的大整数序列 $b_1,b_2,...b_n$, 使得 $s^{b_i}>N$ $(1\le i\le n)$, 其中 s 为共享秘密, $s<N$. 计算子秘密份额 $S_i=s^{b_i}\bmod N$, 并将 S_i 发送给共享者 U_i $(1\le i\le n)$.

2) 分发者 D 选取随机数 δ, 从两两互素的大整数序列 $b_1,b_2,...b_n$ 中任意取 t 个数 $b_{i_1},b_{i_2},...b_{i_t}$ 组建不定方程 $b_{i_1}d_{\sigma(i_1)}+b_{i_2}d_{\sigma(i_2)}+...+b_{i_t}d_{\sigma(i_t)}=1+\delta\varphi(N)$, 计算 $d\sigma_{(i)}$, 令 $A_i=\{d\sigma_{(i)}\}$, 并将 A_i 发送给共享者 U_i $(1\le i\le n)$.

3) 分发者 D 选取随机数 c_1,c_2, $c_1,c_2\in Z_{\varphi(N)}$, 计算 $c_0=c_1+c_2$, $x=c_0+S_1+S_2+...+S_t+A_1+A_2+...+A_t \bmod N$, $y=c_2-H(S_1)-H(S_2)-...-H(S_t)-H(A_1)-H(A_2)-...-H(A_t)\bmod N$, $k=(s+g^s)\bmod N$, $z=x+k$, $X_i=g^{S_i}\bmod N$, $Y_i=g^{S_i+H(S_i)}\bmod N$, $Y_0=g^{c_1}\bmod N$, 其中 $H()$ 是哈希函数, k 为共享秘密的影子秘密, 将 c_1 传送给 U_1, 公布 z,X_i,Y_i,Y_0,y.

2.3 秘密份额的验证

共享者 U_1 收到 c_1 后, 计算 $Y_0'=g^{c_1}\bmod N$, 判断 $Y_0'=Y_0$ 是否成立. 若成立, 则计算 $x_1=c_1+S_1+h(S_1)+A_1+h(A_1)\bmod N$, 同时传送 x_1 给 U_2, 否则说明分发者 D 有欺诈行为, 停止计算, 要求 D 重新传送.

U_2 收到 x_1 后, 计算判断 $g^{x_1}=Y_0Y_1\bmod N$ 是否成立. 若成立, 则计算 $x_2=x_1+S_2+H(S_2)+A_2+H(A_2)\bmod N$, 同时传送 x_2 给 U_3, 否则说明 U_1 有欺诈行为, 要求重新传送.

依此类推, U_t 收到 x_{t-1} 后, 计算判断 $g^{x_{t-1}}=Y_0Y_1...Y_{t-1}\bmod N$ 是否成立. 若成立, 则计算 $x_t=x_{t-1}+S_t+H(S_t)+A_t+H(A_t)\bmod N$, $x'=x_t+y$, $k=z-x'$, 从而恢复出影子秘密 k, 再将 k 传送给其他秘密共享者.

$$\begin{aligned}x'&=x_t+y\\&=.....\\&=x_{t-1}+S_t+H(S_t)+A_t+H(A_t)+c_2-H(S_1)-H(S_2)-...-H(S_t)-H(A_1)-H(A_2)-...-H(A_t)\\&=x_{t-2}+S_{t-1}+H(S_{t-1})+A_{t-1}+H(A_{t-1})+S_t+H(S_t)+A_t+H(A_t)+c_2-H(S_1)-H(S_2)...-H(S_t)-H(A_1)-H(A_2)...-H(A_t)\\&=c_1+c_2+S_1+S_2+...+S_t+A_1+A_2+...+A_t\\&=c_0+S_1+S_2+...+S_t+A_1+A_2+...+A_t\\&=x\end{aligned}$$

2.4 秘密恢复

合格子集 A 中的共享者收到 k 后, 计算公开 $R_i=Q^{s_i}\bmod N$. 任何共享者都可通过等式 $R_i^{d}\bmod N=U_i$ 来判断 U_i 的有效性. 若等式成立, 说明共享者 U_i 提供的秘密份额有效, 否则说明 U_i 提供的秘密份额存在欺诈行为, 验证者可向全体成员发出报怨, 要求 U_i 提供真实的秘密份额. 如果 U_i 不提供真实的秘密份额, 则终止协议.

A 中全体成员的秘密份额通过验证后, 任意 t 个成员 $U_{i_1},U_{i_2},...,U_{i_t}$ 要计算共享秘密 s, 则他们必须拿出

自己的秘密份额 $S_{i_1},S_{i_2},...,S_{i_t}$ 和 $A_{i_1},A_{i_2},...,A_{i_t}$ 中对应选出的特解组合 $\{d_{\sigma(i_1)},d_{\sigma(i_2)},...,d_{\sigma(i_t)}\}$，计算 $g^{S_{i_1}d_{\sigma(i_1)}S_{i_2}d_{\sigma(i_2)}\cdots S_{i_t}d_{\sigma(i_t)}} \bmod N$

$$\begin{aligned} & g^{S_{i_1}d_{\sigma(i_1)}S_{i_2}d_{\sigma(i_2)}\cdots S_{i_t}d_{\sigma(i_t)}} \bmod N \\ =\ & g^{s^{b_{i_1}d_{\sigma(i_1)}}s^{b_{i_2}d_{\sigma(i_2)}}\cdots s^{b_{i_t}d_{\sigma(i_t)}}} \bmod N \\ =\ & g^{s^{[b_{i_1}d_{\sigma(i_1)}+b_{i_2}d_{\sigma(i_2)}+\ldots+b_{i_t}d_{\sigma(i_t)}]\bmod\varphi(N)}} \bmod N \\ =\ & g^{s^{[1+\delta\varphi(N)]\bmod\varphi(N)}} \bmod N \\ =\ & g^{s} \end{aligned}$$

由 g^s 和 k 即可计算出共享秘密 $s=(k-g^s)\bmod N$

3 安全性分析

从秘密恢复 $g^{S_{i_1}d_{\sigma(i_1)}S_{i_2}d_{\sigma(i_2)}\cdots S_{i_t}d_{\sigma(i_t)}} \bmod N$ 来看. 一方面, 方案需要 t 个共享者合作才能恢复出共享秘密, 少于 t 个共享者是不能计算出共享秘密 s, 也不能得到秘密 s 的任何信息; 另一方面, 由 $S_i=s^{b_i} \bmod N$ 知, 要得到正确的 S_i 必须知道 s、b_i, b_i 是随机大素数, 通过 $k=(s+g^s)\bmod N$ 推导出共享秘密 s 是不可能的. 而 $d_{\sigma(i_1)},d_{\sigma(i_2)},...,d_{\sigma(i_t)}$ 是用户 U_i 从 A_i 中选出的特解组合, 由 2.2 秘密份额分发(2)知, 攻击要想得到正确的 $d_{\sigma(i_1)},d_{\sigma(i_2)},...,d_{\sigma(i_t)}$ 必须知道 $b_{i_1},b_{i_2},...,b_{i_t}$, δ, $\varphi(N)$, 其中 $b_{i_1},b_{i_2},...,b_{i_t}$ 是两两互素的大素数, δ 为随机数, $\varphi(N)=(p-1)(q-1)$, p,q 为随机大素数, 由公开的 N 求 p,q 也是不可能的. 方案的安全性基于大整数分解的困难性及离散对数的困难问题[9].

秘密份额验证时, 用户 U_i 将 x_i 传送给用户 U_{i+1}, 由 $x_i=x_{i-1}+S_i+H(S_i)+A_i+H(A_i)\bmod N$ 知, x_{i-1}, S_i, $H(S_i)$, A_i, $H(A_i)$ 未知, U_{i+1} 也无法求得 S_i, 即使知道 x_{i-1} 仍计算不出 S_i. 由离散对数的困难性和哈希函数的不可逆性, 攻击要想从公开的信息 Y_i 获得 S_i 是不可能的.

秘密恢复时, 共享秘密 $s=(k-g^s)\bmod N$. 一方面, 任何共享者通过等式 $R_i^d \bmod N=U_i$ 判断共享者 U_i 的有效性, 若 U_i 提供了虚假份额, 由离散对数和的安全性知, U_i 通不过 U_{i+1} 的验证, 也就不可能计算出 g^s, 即不能恢复出共享秘密 s; 另一方面, k 为共享秘密的影子秘密, 秘密验证时共享者如果不能恢复出正确的 k, 秘密恢复时也不能恢复出共享秘密 s. 所以方案具有防欺诈性.

4 结语

本文提出的基于大整数分解可公开验证的秘密共享方案安全性基于大整数分解、离散对数问题的难解性及哈希函数的不可逆性. 方案中对秘密份额进行验证, 任何共享者都可相互验证有效性, 包括对分发者有效性的验证. 该方案与现在的秘密共享方案相比, 秘密信息量少, 计算复杂度小, 安全性较高, 具有一定的实际应用价值.

参考文献

1 Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612–613.

2 Nojourmian M, Stinson DH, Grainger M. Unconditionally secure social secret sharing scheme. IET Information Security, 2010, 4(2): 202–211.

3 Nojoumian M, Stinson DR. On dealer-free dynamic threshold schemes. advances in Mathematics of Communications 2013, 7(1): 39–56.

4 李滨.基于大数分解的门限秘密共享方案.湖北大学学报(自然科学版),2014,36(6):543–547.

5 高冬梅,刘锋,刘绍武,等.基于向量空间上的秘密共享方案.兰州大学学报(自然科学版),2008,44(3):74–76.

6 杨捷.门限多重影子秘密共享方案及应用.南京工业职业技术学院学报,2014,14(2):51–53.

7 杨刚,李慧.向量空间上可公开验证的秘密共享.北京理工大学学报,2004,24(4):715–718.

8 雷娟,李志慧,张倩倩.基于向量空间的防欺诈秘密共享方案.计算机工程,2011,37(24):100–104.

9 曹阳,郝玉洁,洪歧.一种基于 ECDLP 有身份认证的 ECDH 密钥协商方案.重庆邮电大学学报,2012,24(1):118–120.