基于 RSA 的防欺诈多秘密共享方案

郭现峰
GUO Xian-feng

西南民族大学 计算机科学与技术学院,成都 610041
College of Computer Science and Technology,Southwest University for Nationalities,Chengdu 610041,China
E-mail:guoxianf@126.com

GUO Xian-feng.cheat-proof multi-secret sharing scheme based on RSA.Computer Engineering and Applications,2009,45(17):9-10.

Abstract: Through investigating the secret sharing schemes,points out that YCH scheme is an efficient multi-secret sharing scheme,but it does not has the property of cheat-proof.To overcome this flaw,this paper presents a cheat-proof multi-secret sharing scheme based on RSA.Security analyses indicate that the proposed scheme can resist cheat efficiently.It is capabilities for many applications.

Key words: multi-secret sharing scheme;Rivest-Shamir-Adleman(RSA);cheat-proof;Shamir

摘 要:针对秘密共享方案进行了分析和研究,指出基于二元单向函数和 Shamir(t,n)门限方案的 YCH 多秘密共享方案无法有效防止欺诈,进而提出了一个基于 RSA 的防欺诈的多秘密共享方案。该方案在保留了 YCH 方案的优良特性同时,利用秘密片段和认证片段信息的模余关系来检测欺诈者,具有较强的实用性。

关键词:多秘密共享;RSA;防欺诈;Shamir
DOI:10.3778/j.issn.1002-8331.2009.17.003 **文章编号**:1002-8331(2009)17-0009-02 **文献标识码**:A **中图分类号**:TP309

1 引言

秘密共享方案是将共享的秘密在一组参与者之间进行分配,以达到多人掌管秘密的目的。它主要用于防止重要信息被丢失、破坏、篡改或落入坏人手里。最早由 Blakey[1]和 Shamir[2]各自分别提出了(t,n)门限秘密共享方案。在该方案中,一个秘密被分成 n 份,分别分发给 n 个参与者。n 个参与者中的任意 t 个合作能恢复共享秘密,少于 t 个则得不到秘密的相关信息。上述两个方案共享一个秘密并假定分发者与参与者都是诚实的,不存在欺诈。然而,在实际应用中,防止恶意分发者将伪秘密片段分发给特定参与者,或识别与防止非法参与者利用示伪片断阻止共享信息的恢复,或阻止非法参与者参与秘密共享而窃取共享信息等也是必不可少的部分。为此,方案[3-7]给出了几个较好的防欺诈单秘密共享方案。为了可以同时共享多个秘密,文献[8]提出了一个基于二元单向函数[9]和 Shamir(t,n)门限方案提出了一个多秘密共享方案(YCH 方案)。YCH 方案不仅可以共享多个秘密,还能重用秘密片段[10]。然而,YCH 方案既无法抵御分发者欺诈,也无法抵御参与者欺诈。文献[11]在 YCH 方案的基础上提出了一个可防止参与者欺诈的多秘密共享方案,但对恶意分发者给特定参与者分发伪秘密片段的情况仍无法有效抵御。

为了克服上述问题,在 YCH 方案和 RSA 密码算法的基础上提出了一个既能防止分发者欺诈又能防止参与者欺诈的多秘密共享方案。

2 YCH 方案回顾

2.1 初始化阶段

YCH 方案是一个(t,n)门限方案。其中,$f(r,s)$为二元单向函数,$P_1,P_2,\cdots,P_k$ 为 k 个要共享的秘密,秘密分发者 D 将随机选择的 n 个秘密片段 $s_1,s_2,\cdots,s_n$ 分发给每个参与者 M_i,并随机选择一个随机整数 r,计算 $f(r,s_i)$,其中,$i=1,2,\cdots,n$。

2.2 构造阶段

(1)$k\leqslant t$ 时

①随机选取一个大素数 Q 并构造 $t-1$ 次多项式 $h(x) \bmod Q$:

$$h(x)=P_1+P_2x+\cdots+P_kx^{k-1}+a_1x^k+a_2x^{k+1}+\cdots+a_{t-k}x^{t-1} \bmod Q$$

其中,$0<P_1,P_2,\cdots,P_k,a_1,a_2,\cdots,a_{t-k}<Q$。

②计算 $y_i=h(f(r,s_i)) \bmod Q$,$i=1,2,\cdots,n$。

③公布$(r,y_1,y_2,\cdots,y_n)$。

(2)$k>t$ 时

①随机选取一个大素数 Q 并构造 $k-1$ 次多项式 $h(x) \bmod Q$:

$$h(x)=P_1+P_2x+\cdots+P_kx^{k-1} \bmod Q$$

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60572027);西南民族大学青年项目基金(No.07NQN007);博士基金资助课题(No.08NBS003)。

作者简介:郭现峰(1978-),男,博士生,讲师,CCF 会员,主要研究领域为密码协议及密码算法的构造和分析。

收稿日期:2009-02-11 **修回日期**:2009-03-16

其中,$0<P_1,P_2,\cdots,P_k<Q$。

②计算 $y_i=h(f(r,s_i)) \bmod Q, i=1,2,\cdots,n$。

③计算 $h(i) \bmod Q, i=1,2,\cdots,k-t$。

④公布$(r,y_1,y_2,\cdots,y_n,h(1),h(2),\cdots,h(k-t))$。

2.3 恢复阶段

假设参与者 $M=\{M_1,M_2,\cdots,M_t\}$ 将恢复共享秘密 $P_1,P_2,\cdots,P_k$,先分别计算各自的 $f(r,s_i)$,然后由 Lagrange 插值公式得到 $h(x) \bmod Q$ 如下:

(1)$k\leqslant t$ 时

$$h(x)=\sum_{i=1}^{t} y_i \prod_{j=1,j\neq i}^{t} \frac{x-f(r,s_j)}{f(r,s_i)-f(r,s_j)} \bmod Q=$$

$$P_1+P_2x+\cdots+P_kx^{k-1}+a_1x^k+a_2x^{k+1}+\cdots+a_{t-k}x^{t-1} \bmod Q$$

(2)$k>t$ 时

$$h(x)=\sum_{i=1}^{t} y_i \prod_{j=1,j\neq i}^{t} \frac{x-f(r,s_j)}{f(r,s_i)-f(r,s_j)} \bmod Q+$$

$$\sum_{i=1}^{k-t} h(i) \prod_{j=1,j\neq i}^{t} \frac{x-j}{i-j} \bmod Q=P_1+P_2x+\cdots+P_kx^{k-1} \bmod Q$$

3 本文方案

本文方案仍属于(t,n)门限秘密共享方案。$P_1,P_2,\cdots,P_k$ 为 k 个要共享的秘密,D 为秘密分发者,$M_1,M_2,\cdots,M_n$ 为 n 个参与者,r 为一随机数,$f(r,s)$为二元单向函数。

3.1 初始化阶段

(1)D 选择任意的互异的秘密大素数 p 和 q,计算 $m=pq$;

(2)选择任意 e_1,e_2,且 e_1,e_2 均与欧拉函数 $\phi(m)$ 互素,公开 e_1,e_2;

(3)计算 $d_1\equiv e_1^{-1} \bmod \phi(m), d_2\equiv e_2^{-1} \bmod \phi(m)$;

(4)对于秘密片段 $s_i(i=1,2,\cdots,n)$作如下处理:

①计算 $w_i\equiv s_i^{e_2d_1} \bmod m$。

②将 s_i 和 w_i 分别作为秘密片断和认证片断分配给参与者 M_i 来保管。

③计算 $N=f(r,w_i)$,并将其公布。

3.2 构造阶段

(1)$k\leqslant t$ 时

①随机选取一个素数 Q 并构造 $t-1$ 次多项式 $h(x) \bmod Q$:

$$h(x)=P_1+P_2x+\cdots+P_kx^{k-1}+a_1x^k+a_2x^{k+1}+\cdots+a_{t-k}x^{t-1} \bmod Q$$

其中,$0<P_1,P_2,\cdots,P_k,a_1,a_2,\cdots,a_{t-k}<Q$。

②计算 $y_i=h(f(r,s_i)) \bmod Q, i=1,2,\cdots,n$。

③公布$(r,y_1,y_2,\cdots,y_n)$。

(2)$k>t$ 时

①随机选取一个素数 Q 并构造 $k-1$ 次多项式 $h(x) \bmod Q$:

$$h(x)=P_1+P_2x+\cdots+P_kx^{k-1} \bmod Q$$

其中,$0<P_1,P_2,\cdots,P_k<Q$。

②计算 $y_i=h(f(r,s_i)) \bmod Q, i=1,2,\cdots,n$。

③计算 $h(i) \bmod Q, i=1,2,\cdots,k-t$。

④公布$(r,y_1,y_2,\cdots,y_n,h(1),h(2),\cdots,h(k-t))$。

3.3 验证阶段

根据参与者 M_i 的秘密片段 s_i 和认证片段 w_i,验证 $w_i^{e_1}\equiv s_i^{e_2} \bmod m$ 是否成立可以确定参与信息共享的秘密片段的合法性,验证 $f(r,w_i)=N$ 是否成立可以确定分发者分发的信息的合法性。

3.4 秘密信息恢复阶段

假设参与者 $M=\{M_1,M_2,\cdots,M_t\}$中的成员将恢复秘密 $P_1,P_2,\cdots,P_k$,先分别计算各自的 $f(r,s_i)$,然后由 Lagrange 插值公式得到 $h(x) \bmod Q$ 如下:

(1)$k\leqslant t$ 时

$$h(x)=\sum_{i=1}^{t} y_i \prod_{j=1,j\neq i}^{t} \frac{x-f(r,s_j)}{f(r,s_i)-f(r,s_j)} \bmod Q=$$

$$P_1+P_2x+\cdots+P_kx^{k-1}+a_1x^k+a_2x^{k+1}+\cdots+a_{t-k}x^{t-1} \bmod Q$$

(2)$k>t$ 时

$$h(x)=\sum_{i=1}^{t} y_i \prod_{j=1,j\neq i}^{t} \frac{x-f(r,s_j)}{f(r,s_i)-f(r,s_j)} \bmod Q+$$

$$\sum_{i=1}^{k-t} h(i) \prod_{j=1,j\neq i}^{t} \frac{x-j}{i-j} \bmod Q=P_1+P_2x+\cdots+P_kx^{k-1} \bmod Q$$

4 本文方案的分析

4.1 正确性分析

由 $d_1\equiv e_1^{-1} \bmod \phi(m), d_2\equiv e_2^{-1} \bmod \phi(m)$和 $w_i\equiv s_i^{e_2d_1} \bmod m$ 知 $w_i^{e_1}\equiv (s_i^{e_2d_1})^{e_1} \bmod m=s_i^{e_2(d_1e_1)} \bmod m=s_i^{e_2} \bmod m$,即 $w_i^{e_1}\equiv s_i^{e_2} \bmod m$,因此,其防欺诈验证是正确的。

4.2 安全性分析

(1)如果外部欺诈者 E 欲从公布的 $N=f(r,w_i)$中获得 M_i 的秘密片段 s_i,则必须首先攻破二元单向函数 $N=f(r,w_i)$得到 w_i,再攻破 RSA 加密算法从 w_i 求出 s_i 使得 $w_i^{e_1}\equiv s_i^{e_2} \bmod m$ 成立。

(2)如果恶意分发者 D 欲分发伪秘密信息和认证信息给特定参与者 M_i,则其只有攻破二元单向函数 $N=f(r,w_i)$找到 w_i'使得 $f(r,w_i')=N$ 成立,并利用 e_1,d_2 计算出 $s_i'=w_i'^{e_1d_2} \bmod m$,将$(s_i',w_i')$分发给参与者 M_i。

(3)恶意参与者 M_i 找到同时满足 $w_i^{e_1}\equiv s_i^{e_2} \bmod m$ 和 $N=f(r,w_i)$ 的伪信息(s_i',w_i')的困难性等同于攻破二元单向函数 $N=f(r,w_i)$ 和 RSA 加密算法。

从上面的分析得出,提出的方案不仅可以有效防止恶意参与者阻止信息的恢复,还可以防止恶意分发者给特定参与者分发伪信息,具有很高的安全性。

5 结论

本文在 YCH 方案的基础上提出了一个防止欺诈的多秘密共享方案,在保留了原有方案各种优良特性的同时,利用 RSA 加密算法实现了秘密分发者和秘密恢复参与者之间的相互认证。安全性分析证明,该方案的抗欺诈能力至少等同于 RSA 加密算法的安全性,是一个较为实用的多秘密共享方案。

参考文献:

[1] Blakley G R.Safeguarding cryptographic keys[C]//Proc AFIPS 1979, National Computer Conference.New York,USA:AFIPS Press,1979.

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

(下转 79 页)