基于 RSA 和单向函数防欺诈的秘密共享体制*

费如纯[1,3], 王丽娜[2,4+]

[1](东北大学 信息科学与工程学院,辽宁 沈阳 110004)
[2](武汉大学 软件工程国家重点实验室,湖北 武汉 430071)
[3](本溪冶金高等专科学校 信息工程系,辽宁 本溪 117022)
[4](中国科学院 软件研究所 计算机科学重点实验室,北京 100080)

Cheat-Proof Secret Share Schemes Based on RSA and One-Way Function

FEI Ru-Chun[1,3], WANG Li-Na[2,4+]

[1](School of Information Science and Engineering, Northeastern University, Shenyang 110004, China)
[2](State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430071, China)
[3](Department of Information Engineering, Benxi College of Metallurgy, Benxi 117022, China)
[4](Key Laboratory of Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)
+ Corresponding author: Phn: 86-27-87653733, E-mail: lnawang@163.com
http://www.whu.edu.cn
Received 2002-04-08; Accepted 2002-07-02

Fei RC, Wang LN. Cheat-Proof secret share schemes based on RSA and one-way function. *Journal of Software*, 2003,14(1):146~150.

Abstract: The cheat-proof method in threshold secret sharing scheme is researched. The threshold secret sharing scheme is integrated with RSA and one-way function. And the RSA and one-way function are fully utilized to verify the validity of data. A threshold secret sharing scheme based on RSA is proposed, at which the cheating is equal to attacking RSA scheme. A threshold secret sharing scheme based on RSA and one-way function is also presented, at which the cheating is equal to attacking RSA scheme or one-way function. These two schemes have so strong power to identify cheaters that they can restrict the probability of successful cheating to a very small value no matter how skilled cheaters are, so they are unconditionally secure. In addition, the schemes proposed in this paper have very high information rate.

Key words: secret sharing; threshold scheme; cheating; RSA; one-way function; information rate

摘 要: 对门限秘密共享体制中的防欺诈措施进行了研究,将门限秘密共享体制与 RSA 与单向函数相结合,充分利用 RSA 和单向函数进行数据合法性的验证.提出了基于 RSA 防欺诈的门限秘密共享体制,对该体制的欺诈等价于攻击 RSA 体制;又提出了基于 RSA 和单向函数防欺诈的门限秘密共享体制,对该体制的欺诈等价于攻击 RSA 体制或单向函数.这两个体制具有很强的防止欺诈能力,使欺诈成功的概率限定于一个很小的值,而不论欺

* Supported by the National Natural Science Foundation of China under Grant Nos.90104005, 66973034, 60173051 (国家自然科学基金)

第一作者简介: 费如纯(1969－),男,河北昌黎人,讲师,主要研究领域为计算机安全,密码学.

诈者具有多么高的技术,因而是无条件安全的.另外,所提出的防欺诈的门限秘密共享体制具有很高的信息率.

关键词: 秘密共享;门限体制;欺诈;RSA;单向函数;信息率

中图法分类号: TP309 **文献标识码**: A

秘密共享是密码技术研究的一个很重要的方向.无论在理论上还是在实践上,对于计算机及网络的安全保密均具有重要的意义.

自从 Blakley[1]和 Shamir[2]在 1979 年分别提出了秘密共享体制以来,有关秘密共享体制的研究受到了人们的广泛关注.Asmuth 和 Bloom[3]等人对基于中国剩余定理的门限秘密共享体制进行了研究.He[4]、刘焕平、杨义先和杨放春[5]利用单向 Hash 函数给出了多级秘密共享体制.Karnin 和 Greene[6]等人将信息论方法引入秘密共享体制的研究,更为清晰地刻画了秘密共享体制的实质.(t,n)门限秘密共享体制,就是将共享的秘密信息分为 n 个片段分配给 n 个合法参与者,必要时可以利用任意 t 个片段恢复原秘密信息,而利用任意少于 t 个片段则不能完成恢复过程.

在实际应用中,仅仅考虑如何对秘密信息进行共享是不够的,还应考虑在秘密共享体制中如何抵抗欺诈行为,即如何识别非法参与者以及如何识别出示伪片段,以阻止秘密信息恢复的合法参与者.许多学者设计了可防止欺诈的(t,n)门限秘密共享体制.McEliece 和 Sarwate[7]利用纠错码构造了一个(t,n)门限秘密共享体制,当 $t+2e$ 个参与者中有少于 e 个欺诈者时也能恢复原秘密,但当欺诈者超过 e 个时就不能发现欺诈行为.Okada 和 Kurosawa[8]也利用纠错码防欺诈进行了研究.Rabin 和 Ben-Or[9]构造的(t,n)门限秘密共享体制能使诚实的参与者以一定概率发现欺诈者,但该体制的信息率较低,为 $1/(3n-2)$.张建中和肖国镇[10]基于 Shamir 体制构造了一个(t,n)门限秘密共享体制,使信息率有了很大的提高,信息率为 $1/(t+2n-2)$.

本文基于 RSA[11]加、解密算法和单向函数提出了两个可以防止欺诈的(t,n)门限秘密共享体制.这两个体制的突出优点是具有很强的防止欺诈的能力并具有很高的信息率.

1 基于 RSA 防欺诈的门限秘密共享体制的构造

设(t,n)门限秘密共享体制的公开信息包括:一个大素数 $r>n$,β是有限域 $GF(r)$的本原元素,$m=pq$,这里 p 和 q 为互异的素数且保密.

1.1 秘密片段及认证片段的分配

设 n 个参与者依次为 $P_1,P_2,...,P_n$,共享的秘密信息为 $k\in GF(r)$,则秘密片段和认证片段的分配者进行分配的算法如下:

(1) 秘密选择一个 $t-1$ 次多项式 $f(x)=b_{t-1}x^{t-1}+...+b_1x+k \bmod r$,这里,$b_1,b_2,...,b_{t-1}$ 及 $f(x)$均属于 $GF(r)$;

(2) 任意选择 e_1,e_2,且 e_1 和 e_2 均与 $\phi(m)$ 互素,公开 e_1 和 e_2,这里,$\phi(m)$ 是欧拉函数;

(3) 计算 $d_1=e_1^{-1} \bmod \phi(m)$,$d_2=e_2^{-1} \bmod \phi(m)$,这里,形如 $x=b^{-1} \bmod c$ 的式子表示 b 关于模 c 的乘法逆元素为 x;

(4) 对于 $i=1,2,...,n$,作如下处理:

(a) 计算 $S_i=f(\beta^i)$;

(b) 计算 $W_i=S_i^{e_2d_1} \bmod m$,这里,形如 $x=b \bmod c$ 的式子的含义是 b 除以 c 的余数为 x;

(c) 将 S_i 和 W_i 分别作为秘密片段和认证片段分配给参与者 P_i 来保管.

1.2 秘密信息的恢复

当需要使用共享的秘密信息时,只要 n 个参与者中任意 t 个合作即可恢复秘密信息 k.不失一般性,假设 $P_1,P_2,...,P_t$ 合作,则利用他们所保管的 t 个秘密片段可以得到 t 个插值点$(\beta^1,S_1),(\beta^2,S_2),...,(\beta^t,S_t)$,进而使用 Lagrange 插值可以重构 $t-1$ 次多项式 $f(x)$,使得 $S_i=f(\beta^i)$,最终可以计算出 $k=f(0)$.秘密信息 k 的具体计算公式如下:

$$k=\sum_{i=1}^{t}S_i\prod_{j=1,j\neq i}^{t}\frac{-\beta^j}{\beta^i-\beta^j} \mod r.$$

1.3 欺诈者的检测

当需要恢复共享的秘密信息 k 时,t 个参与者中有可能存在内部欺诈者或外部欺诈者,其中内部欺诈者出示假的片段以阻止共享的秘密信息 k 的正确恢复,外部欺诈者则设法参与共享的秘密信息的恢复以获得 k.该体制可以利用认证片段有效地检测出内部欺诈者和外部欺诈者,以保证体制的安全性.

假设参与恢复共享的秘密信息 k 的参与者为 $P_1,P_2,...,P_t$,对于参与者 $P_i(1\leq i\leq t)$,如果 $W_i^{e_1}\equiv S_i^{e_2} \bmod m$,则 P_i 为出示了真正片段的合法参与者,否则 P_i 为内部欺诈者或外部欺诈者,这里,形如 $x\equiv y \pmod m$的式子的含义是 x 和 y 关于模 m 同余.

1.4 正确性、安全性及信息率

在本文所提出的基于 RSA 防欺诈的(t,n)门限秘密共享体制中,秘密片段分配和共享的秘密信息的恢复采用了基于 Lagrange 插值的 Shamir 体制.从 Shamir[2]秘密共享体制可知,本体制中秘密片段的分配以及利用秘密片段恢复原秘密信息的算法是正确无疑的.下面讨论认证片段的分配以及利用认证片段检测欺诈者的算法的正确性.

对于欺诈者的检测方法,如果 P_i 是出示真正片段的合法参与者,则必定满足

$$W_i^{e_1}\equiv S_i^{e_1e_2d_1}\equiv S_i^{e_2} \pmod m.$$

因此,该体制是正确的.

定理 1. 本文提出的基于 RSA 防欺诈的(t,n)门限秘密共享体制是完善的.

证明:该体制的基础是完善的 Shamir 秘密共享体制,因而该体制是完善的(t,n)门限秘密共享体制,已知任意少于 t 个片段得不到有关共享的秘密的任意部分信息. □

定理 2. 在均匀分布和等长编码情况下,基于 RSA 防欺诈的(t,n)门限秘密共享体制的信息率为

$$\frac{\log_2 r}{\log_2 r+\log_2 m}.$$

证明:设共享秘密信息的空间为 K、分配给参与者的秘密片段的空间为 S、认证片段的空间为 W,可知 $|K|=|S|=r,|W|=m$.根据文献[12],考虑均匀分布和等长编码情况,信息熵 $H(K)=H(S)=\log_2 r$,$H(W)=\log_2 m$.当需要对共享秘密 $k\in K$ 进行共享时,分配给参与者 $P_i(1\leq i\leq n)$的片段为(S_i,W_i),其中 $S_i\in S,W_i\in W$.因此,在均匀分布情况下,该体制的信息率为

$$\frac{H(K)}{H(S)+H(W)}=\frac{\log_2 r}{\log_2 r+\log_2 m}.$$ □

由定理 2 可知,当 m 与 r 为相同量级时,对于(3,5)门限秘密共享体制,Rabin-Ben-Or 体制的信息率为 1/12,张建中-肖国镇体制的信息率为 1/11,而该体制的信息率约为 1/2;对于(6,10)门限秘密共享体制,Rabin-Ben-Or 体制的信息率为 1/28,张建中-肖国镇体制的信息率为 1/24,而该体制的信息率依然不变.可见,本文提出的秘密共享体制的信息率是很高的,并且它与体制中的 t 和 n 的值无关.

定理 3. 对于基于 RSA 防欺诈的(t,n)门限秘密共享体制,欺诈者欺诈成功等价于攻破 RSA 加解密算法.

证明:从本文提出的体制防止欺诈的措施可知,如果欺诈者 P_i 改 S_i 为 S_i^*,则他必须计算 W_i^*,使得

$$W_i^{*e_1}\equiv S_i^{*e_2} \pmod m,$$

才能通过验证,但是他不知道满足

$$e_1d_1\equiv 1 \pmod{\phi(m)}$$

的 d_1,所以他能够计算出 W_i^*等价于攻破 RSA 加解密体制;如果欺诈者 P_i 改 W_i 为 W_i^*,则他必须计算 S_i^*,使得

$$S_i^{*e_2}\equiv W_i^{*e_1} \pmod m,$$

才能通过验证,同理,这等价于攻破 RSA 加解密体制. □

为了保证安全性,在本文提出的体制中,要求不定方程 $x^{e_2} \equiv y^{e_1} \pmod{m}$的非平凡解($x$ 或 y 的取值不是 0,1,$m-1$)是难解的.如果能够求解出非平凡解 $x=a$ 和 $y=b$ 满足 $x^{e_2} \equiv y^{e_1} \pmod{m}$,则参与者 $P_i(1\le i\le n)$可以用 (aS_i,bW_i)代替(S_i,W_i),这样,P_i 就可以在不被检测为欺诈者的情况下达到阻止共享秘密正确恢复的目的.

由定理 3 可知,欺诈者欺诈成功具有与攻破 RSA 体制相同的难度,欺诈成功的概率被限定在一个很小的值,而不论他有多大的计算能力.因此,本文提出的体制是无条件安全的.

2 基于 RSA 和单向函数防欺诈的门限秘密共享体制

设 n 个参与者依次为 $P_1,P_2,...,P_n$,共享的秘密信息为 $k\in GF(r)$,H 是一个单向函数,则秘密片段和认证片段的分配者进行分配的算法如下:

(1) 秘密选择一个 $t-1$ 次多项式 $f(x)=b_{t-1}x^{t-1}+...+b_1x+k \bmod r$,这里,$b_1,b_2,...,b_{t-1}$ 及 $f(x)$均属于 $GF(r)$;

(2) 任意选择 e,且 e 与 $\phi(m)$ 互素,公开 e,这里,$\phi(m)$ 是欧拉函数;

(3) 计算 $d=e^{-1} \mod \phi(m)$;

(4) 对于 $i=1,2,...,n$,作如下处理:

(a) 计算 $S_i=f(\beta^i)$;

(b) 计算 $W_i=H(S_i)^d \bmod m$;

(c) 将 S_i 和 W_i 分别作为秘密片段和认证片段分配给参与者 P_i 来保管.

在本文提出的体制中,对于参与者 P_i,如果 $W_i^e \equiv H(S_i) \pmod{m}$,则 P_i 为出示了真正片段的合法参与者,否则 P_i 为内部欺诈者或外部欺诈者.如果欺诈者 P_i 改 S_i 为 S_i^*,则他必须计算 W_i^*,使得

$$W_i^{*e} \equiv H(S_i^*) (\bmod m),$$

才能通过验证,但是他不知道 d_1,所以他能够计算出 W_i^*等价于攻破 RSA 加解密体制;如果欺诈者 P_i 改 W_i 为 W_i^*,则他必须计算 S_i^*使得

$$H(S_i^*) \equiv W_i^{*e} (\bmod m).$$

在单向函数具有足够的安全性时,这也是难以实现的.

在本文提出的体制中,共享秘密的恢复算法与第 1 种体制共享秘密的恢复算法一致.

对于本体制,欺诈成功等价于攻破 RSA 加解密体制或单向函数,因而具有很强的安全性.同理,本文提出的体制也是完善的,并且其信息率为

$$\frac{\log_2 r}{\log_2 r+\log_2 m}.$$

3 结 论

本文以 Shamir 秘密共享体制为基础,结合 RSA 加密、解密体制和单向函数构造了两个可防止欺诈的(t,n)门限秘密共享体制,这两个体制均是完善的,并且欺诈成功等价于攻破 RSA 加密、解密体制或攻破单向 Hash 函数.只要相应的 RSA 体制和单向函数具有足够的安全性,本文提出的体制就具有很强的防止欺诈性能,也就能够以很大的概率发现欺诈者.另外,Rabin-Ben-Or 体制、张建中-肖国镇体制等可防止欺诈的(t,n)门限秘密共享体制的信息率随着 t 或 n 取值的增大而减小,而本文所提出的两个可防止欺诈的(t,n)门限秘密共享体制的信息率为

$$\frac{\log_2 r}{\log_2 r+\log_2 m}.$$

该值与 t 和 n 的取值无关,因而具有非常高的信息率.

References:

[1] Blakley GR. Safeguarding cryptographic keys. In: Merwin RE, Zanca JT, Smith M, eds. Proceedings of the National Computer Conference. Montvale, NJ: AFIPS Press, 1979. 313~317.

[2] Shamir A. How to share a secret. Communications of the ACM, 1979,24(11):612~613.

[3] Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Transactions on Information Theory, 1983,29(2):208~210.

[4] He J, Dawson E. Multistage secret sharing based on one-way function. electronics letters, 1994,30(19):1591~1592.

[5] Liu HP, Yang YX, Yang, FC. Multistage secret sharing based on one-way function. Journal of Electronics, 1999,21(4):561~564 (in Chinese with English).

[6] Karnin ED, Greene JW, Hellman ME. On secret sharing systems. IEEE Transactions on Information Theory, 1983,29(1):231~241.

[7] McEliece RJ, Sarwate DV. On sharing secrets and Reed-Solomon codes. Communications of the ACM, 1981,24(8):583~584.

[8] Okada K, Kurosawa K. MDS secret sharing scheme secure against cheaters. IEEE Transactions on Information Theory, 2000,46(3): 1078~1081.

[9] Rabin T, Ben-Or M. Verifiable secrets sharing and multiparty protocols with honest majority. In: Johnson DS, ed. Proceedings of the 21st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1989. 73~85.

[10] Zhang JZ, Xiao GZ. A secret sharing scheme to identify cheaters. Journal of Electronics, 1999,21(4):516~521 (in Chinese with English Abstract).

[11] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 1978,21(2):120~126.

[12] Blundo C, Santis AD, Simone RD, Vaccaro U. Tight bounds on the information rate of secret sharing schemes. Designs, Codes and Cryptography, 1997,11(2):102~122.

附中文参考文献:

[5] 刘焕平,杨义先,杨放春.基于单向函数的多级秘密共享方案.电子科学学刊,1999,21(4):561~564.

[10] 张建中,肖国镇.一个可防止欺诈的秘密分享方案.电子科学学刊,1999,21(4):516~521.