利用杂凑函数的在线秘密分享机制

吉文峰[1] ,吴秀贤[1] ,金晟柱[2] ,元东豪[1]
(1. 成均馆大学电子电气与计算机工学部,韩国;2. 韩国情报保护振兴院,韩国)

摘 要: 本文提出一种利用杂凑函数有效的在线秘密分享方式,此秘密分享方式通过一分享情报网可以生成多次秘密分享,使得秘密分享机制是多次性的. 既使接入结构(Access Structure)发生变化的情形下,成员的秘密分享值不需改变,只需变更公告牌(Notice board)公开的情报,就可任意次生成系统秘密,任何不诚实的成员不论多少都可以被事后检查出,因计算量小,可在群体协议或群体密码方式中有效的利用.

关键词: 杂凑函数; 秘密分享; 接入结构; 数字签名
中图分类号: TN911.2 **文献标识码**: A **文章编号**: 0372-2112 (2003) 01-0045-03

New On-Line Secret Sharing Scheme Using Hash Function

JI Wen-feng[1] ,Soohyun Oh[1] ,Seungjoo Kim[2] ,Dongho Won[1]
(1. *School of Electrical and Computer Engineering, Sungkyunkwan Univ, Korea*; 2. *KISA (Korea Information Security Agency, Korea)*)

Abstract: In this paper, we propose an efficient on-line secret sharing scheme using one-way hash function. The proposed scheme provides the property to share multiple secrets and allows participants to be added/deleted dynamically, without having to redistribute new shares. It is able to detect and identify cheaters even if majority of the participants are dishonest, and is more computationally efficient than previous schemes. Therefore, it can be applied to multi-party protocols, group-oriented cryptosystems and etc.

Key words: Hash function; secret sharing; access structure; digital signature

1 引言

秘密分享是把秘密情报 K 在一组参与者集 P 中进行分配,由他们共同分享,使 P 中的每个合格子集都能恢复秘密 K 的一种方式.

1979 年,Shamir 等首先提出了 n 名成员中 $t(t \leq n)$ 名以上成员参与合作就可以恢复秘密情报 K 的 (t, n)-门限秘密分享方案. 1988 年 Tompa, Woll 等指出了 Shamir 的秘密分享方法易受不诚实成员的攻击,并指出了解决方案[1].

Cachin 等首次引入公告牌(notice board)概念,提出了各成员利用与秘密情报大小相近的一个分享情报分享多个秘密情报的在线(on line)秘密分享方式[2]. 当一个秘密情报恢复以后,为了保证其他秘密情报的安全,各成员的分享情报不至于报露给其他成员,需增加一些必要的计算[3].

为此,Pinch 等提出了利用离散代数问题无需增加计算,在恢复秘密情报过程中成员的分享情报不泄露方案[4]. 但是此方案不能查出秘密情报恢复中分享情报不及时提供的不诚实成员.

为了解决此问题,Ghodosi 等提出了在恢复秘密情报之前,增加各成员是否正确提供自己的分享情报的验证过程[5]. 但是此方案对过半数不诚实成员合谋情况下是不安全的. 在 Ghodosi 方案中,为了防止过半数不诚实成员的合谋问题,Yeun 等提出了在 Pinch 的秘密分享方式中引入数字签名方法可随时检测不诚实成员的方案[6,7].

但是,这些秘密分享方案都是利用离散代数问题或 RSA 密码方式,所以在秘密情报恢复过程中需要很大的计算量.

本文提出了一种利用两种单向杂凑函数的在线秘密分享方案. 该方案代替了已有方案中的离散对数和 RSA 方式. 具有高效,安全(可以检测出不诚实的成员)等特点. 特别地,在本方案中,当接入结构发生变化时,各参与成员所拥有的分享情报可以重用,因此具有很高的实用价值.

2 Yeun 等的在线秘密分享方式

Yeun 等对 Pinch 的秘密分享方式进行了改进,提出了不诚实成员无论多少都可检测的方案. 此方案利用了离散代数问题和 RSA 密码方式[8],使秘密情报恢复过程中成员的分享情报不必泄露.

2.1 利用离散代数问题的秘密分享方式

系统设置

P:参与成员 $P_i (1 \leq i \leq n)$

D: dealer, $D \notin P$

Γ:接入结构 ($\Gamma \subseteq 2^{|P|}$)

Γ^*:最小合格子集(minimal authorized set)

K:要分享的秘密情报

h:单向杂凑函数

收稿日期:2001-11-12;修回日期:2002-04-25

S_{P_i}:成员 P_i 的数字签名(系统中有一个公开的数字签名算法,每个成员有秘密的签名密钥和公开的鉴别密钥).

初始化过程

(1) Dealer 选取一个大素数 P 和有限域 Z_P 上位数为素数 $q(q|P-1)$ 的元素 g_X. 为每一个成员随机地选择 $S_1, S_2, \cdots, S_n \in_R Z_q$,通过安全渠道秘密地将 S_i 传给成员 P_i,并将成员的 ID 和分享情报安全的保管.

(2) Dealer 计算对应 $X(X \in \Gamma^*)$ 的 $T_X = K - h(g_X^{\prod_{x \in X} S_x}) \bmod p$ 的值. 在公告牌上公开 g_X, T_X, $h(X)$.

恢复过程

(1) 设成员集 $X = \{P_1, P_2, \cdots, P_t\}$ 成员 P_1 从公告牌中读取对应 X 的 g_X, T_X 和 $h(K)$. 计算 $V_1 \equiv g_X^{S_1} \bmod p$, $S_{P_1} = Sig_{p1}(g_X^{S_1} \bmod p \,\|\, X \,\|\, g_X)$,然后传给成员 P_2.

(2) 成员 P_2 从成员 P_1 中得到 V_1 和 S_{p1}后验证成员 P_1 的数字签名 S_{P1}. 计算 $V_2 \equiv g_X^{S_1 S_2} \bmod p$ 和对此的数字签名 S_{P2}. 然后传给成员 P_3. 以此类推.

(3) 成员 P_t 验证成员 P_{t-1}的数字签名 $S_{P_{t-1}}$,并计算 $V_t = (V_{t-1})^{S_t} \bmod p \equiv g_X^{S_1 S_2 \cdots S_{t-1} S_t} \bmod p$. 然后恢复系统秘密 $K' \equiv T_X + h(V_t) \bmod p$.

(4) 最后,为验证系统秘密恢复的正确性,比较公告牌公开的情报 $h(K)$,如 $h(K) = h(K')$,可知系统秘密正确的恢复.

2.2 利用 RSA 密码方式的秘密分享机制

初始化过程

(1) Dealer 选择大的素数 p 和 q,计算 $n = p * q$,选取使 $gcd(e, \phi(n)) = 1$ 的 e 值. Dealer 选择分享情报 $S_1, S_2, \cdots, S_n \in_R Z_n$ 并通过安全渠道秘密地传送给成员 $P_1, P_2, \cdots, P_n$. 并将各成员的 ID 与秘密分享情报安全的保管.

(2) Dealer 计算对应 $X(X \in \Gamma^*)$ 的 $T_X = K \oplus h(\prod_{x \in X} S_x^e \bmod n)$. 在公告牌上公开情报 X, e, nT_X 和 $h(K)$.

恢复过程

(1) 成员 P_1 计算 $V_1 \equiv S_1^e \bmod n$ 和数字签名 $S_{P_1} = Sig_{P_1}(S_1^e \bmod n \,\|\, X \,\|\, e \,\|\, n)$ 并传送给成员 P_2.

(2) 成员 P_2 从成员 P_1 中得到 V_1 和 S_{P_1},利用数字签名 S_{P_1}验证 V_1 的正确性. 然后计算 $V_2 \equiv S_1^e S_2^e \bmod n$ 和对此的数字签名 $S_{P_2} = Sig_{P_2}(S_1^e S_2^e \bmod n \,\|\, X \,\|\, e \,\|\, n)$.

(3) 成员 P_t 验证成员 P_{t-1}对 V_{t-1}数字签名 $S_{P_{t-1}}$,计算 $V_t \equiv S_1^e S_2^e \cdots S_t^e \bmod n$. 然后恢复系统秘密 $K' = T_X \oplus h(V_t)$.

(4) 最后,为验证系统秘密恢复的正确性,比较公告牌公开的情报 $h(K)$,如 $h(K) = h(K')$,可知系统秘密正确的恢复.

3 本文提出的在线秘密分享机制

如上所述,Yeun 等的秘密分享机制是利用离散代数问题和 RSA 密码方式. 在不泄漏各成员的分享情报下可恢复系统秘密,但可看出此方式需很多乘方运算,计算量大大增加. 本文提出一种利用单向杂凑函数代替离散代数问题和 RSA 密码方式的在线的秘密分享机制. 本文提出的秘密分享与恢复协议如下.

系统设置

Γ:接入结构($\Gamma \in 2^{|P|}$) $X \in \Gamma$ 时,属于 X 的各成员可利用分享的秘密情报恢复出原来的秘密情报 K(系统秘密). $X \notin \Gamma$ 时,无法恢复出原来的秘密情报 K.

K:需要秘密分享的秘密情报(系统秘密)

f, h:无碰撞的单向杂凑函数

秘密分享协议

(1) Dealer 随机选取数 r 和各成员的分享情报 $S_1, S_2, \cdots, S_n \in_R Z_P$,将各成员的分享情报通过安全渠道传秘密送给成员 $P_1, P_2, \cdots, P_n$,并将各成员的 ID 和分享情报安全的保管.

(2) Dealer 对 $X \in \Gamma$ 的 $X = \{P_1, P_2, \cdots, P_t\}$,计算 T_X. 在公告牌上公开情报 X, r, T_X 和 $h(K)$. 其中 $T_X = K \oplus f(h(S_1 \,\|\, r) \oplus h(S_2 \,\|\, r) \oplus \cdots \oplus h(S_t \,\|\, r))$.

图 1 为秘密分享协议图.

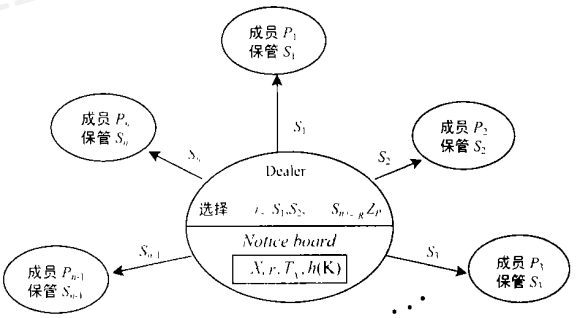

图 1 秘密分享与公告牌

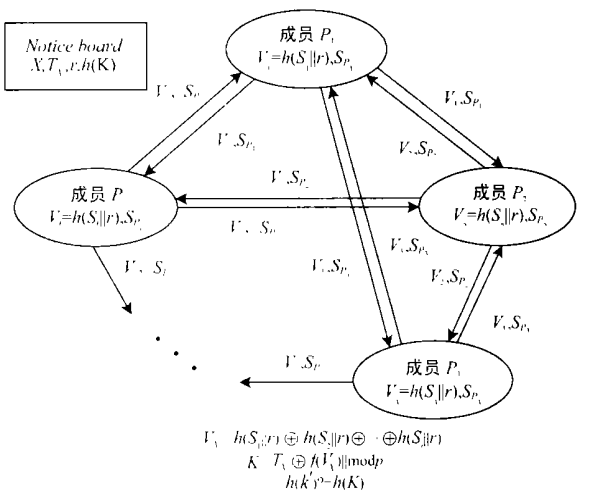

图 2 系统秘密恢复协议

秘密恢复协议

(1) 设成员集为 $X = \{P_1, P_2, \cdots, P_t\}$. 各成员 $P_i(P_i \in X)$ 从公告牌上读取对应于 X 的随数 r,利用自己的分享情报 S_i 计算 $V_i = h(S_i \,\|\, r)$ 和数字签名 $S_{P_i} = Sig_{P_i}(h(S_i \,\|\, r) \,\|\, X \,\|\, r)$.

(2) 成员 P_i 将 V_i, S_{P_i}传送给成员 $P_j(P_j \in X, P_i \neq P_j)$. 成员 P_j 验证从成员 P_i 中得到的数字签名. 然后计算 $V_X = h(S_1 \,\|\, r) \oplus h(S_2 \,\|\, r) \oplus \cdots \oplus h((S_t \,\|\, r)$.

(3)最后,各成员 P_i 恢复系统秘密 K', $K' = T_x \oplus f(V_X)$. 为验证恢复的系统秘密的正确性,计算 $h(K')$ 于公告牌公开的 $h(K)$ 相比较.

图 2 为系统秘密恢复协议图.

4　本文提议的在线秘密分享方式的特征

本文提出的利用杂凑函数的秘密分享方式,具有高效,安全等特点. 本提案是一种动态的秘密分享机制. 可以增加新的成员参与,可以删除已参与的成员. 在接入结构变化时,Dealer 构造新的接入结构,生成相应的 X, r, T_X 并公布在公告牌上. 合理成员的分享情报无需改变即可再用.

任何不诚实的成员无论多少事后可以查出. 秘密情报恢复过程中,任意一成员提供不诚实的情报. 那么恢复的秘密情报 K 的 $h(K')$ 值与公告牌公开的 $h(K)$ 值不一致. 这时,各成员向 dealer 提出在秘密情报恢复过程中向其他成员传送的数字签名 $S_{P_i}(1 \leq i \leq t)$,Dealer 利用自己保管的 $S_i(1 \leq i \leq t)$ 和 r 计算 $h(S_i \| r)(1 \leq i \leq t)$,验证各成员的数字签名,找出不诚实的成员.

5　结论

本论文提出了利用一个分享情报可任意恢复不同的系统秘密 K 的基于单向杂凑函数的在线秘密分享机制. 此方案比利用离散代数问题和 RSA 密码方式恢复秘密情报过程中需要的计算量减少,是更有效的秘密分享机制.

特别地,此方案在参与结构改变时,公告牌公开的情报相应地变更. 参与成员的分享情报无需改变而继续使用. 系统秘密恢复过程中不诚实成员无论多少都可以查出.

参考文献:

[1] M Tompa, H Woll. How to share a secret with cheater [J]. Journal of Cryptology 1, 1988: 133 - 138.

[2] C Cachin. On-line secret sharing [A]. In C. Boyd, editor, Proceeding of the 5th IMA conference on Cryptography and Coding [C]. Berlin: Springer-Verlag, 199: 90 - 198.

[3] O Goldreich, S Micali, A Wigderson. How to play any mental game or a completeness theorem for protocol with honest majority [A]. in Proc. 19th ACM Symposium on Theory of Computing (STOC) [C]. 1987.

[4] R G E Pinch. On-line multiple secret sharing [J]. Electronic Letters, 1996: 1087 - 1088.

[5] H Ghodosi, J Pieprzyk G R Chaudhry, J Seberry. How to prevent cheating in pinch's scheme [J]. Electronic Letters, 1997, 33(17): 1453 - 1454.

[6] Chan Yeob Yeun, Chris J Mitchell. How to identify all cheater in pinch's scheme [A]. JWIS'98 [C]. Singapore: Japan-Singapore Joint Workshop on Information Security, 1998.

[7] Chan Yeob Yeun, Chris J Mitchell, Mike Burmester. An online secret sharing which identifies all cheater [A]. Proceeding of NORDSEC'98 [C]. Norway: The Third Nordic workshop on Secure IT Systems, 1998.

[8] R Rivest, A Shamir, L Adleman. A method for Obtaining Digital signature and Public key Cryptosystems [J]. Communication of the ACM, 1978: 120 - 128.

作者简介:

吉文峰　男,1964 年 12 月 5 日出生于吉林省吉林市,1985 年延边大学数学系毕业获理学学士学位,1985 年～1995 年黑龙江省汤原县朝鲜族高级中学任教,2000 年留学韩国成均馆大学电子电气与计算机工学科攻读硕士学位,主要研究领域:现代密码学,发表论文"移动通信环境下适用于电子商务的 Proxy-Signcryption 方式". e-mail: wtji@dosan.skku.ac.kr

吴秀贤　1998 年获成均馆大学情报工学系工学学士学位,2000 年获成均馆大学情报工学系工学硕士学位(主攻密码学),现今成均馆大学情报工学系攻读博士学位(主攻密码学). e-mail: skim@kisa.or.kr

金晟柱　1994 年获成均馆大学情报工学系工学学士学位,1996 年获成均馆大学情报工学系工学硕士学位(主攻密码学),1999 年获成均馆大学情报工学系工学博士学位(主攻密码学),1999 年至今韩国情报保护振兴院(密码技术组课题负责人),2000 年至今韩国情报通信技术协会(情报保护技术委员会,密码技术研究班),e-mail: skim@kisa.or.kr

元东豪(Dongho Won)　1949 年 9 月 23 日生. 成均馆大学电子工学系(学士,硕士,博士)1978 年～1980 年韩国电子通信研究所专任研究员 1985 年～1986 年日本东京工大客座研究员. 1992 年～1994 年成均馆大学电算所所长 1995 年～1997 年成均馆大学教学处长 1996 年～1998 年国务总理室情报化促进委员会质询委员. 1998 年～1999 年成均馆大学情报通信技术研究所所长. 1990 年～1999 年韩国情报保护学会理事. 1999 年～2001 年成均馆大学电子电气与计算机工学部学部长. 1999 年～2001 年成均馆大学情报通信大学院院长. 1982 年～至今成均馆大学电子电气与计算机工学部教授. 1999 年～至今韩国情报保护学会会长. 2000 年～至今情报通信部指定情报保护认证技术研究中心中心长. e-mail: dhwon@dosan.skku,ac,kr