一种基于IBE的(t,n)门限调整方案

俞昌国,杨 庚,李大伟
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:Baek提出了一个基于身份的门限秘密共享方案IdThdBm,该方案门限值作为参数在系统初始化时确定,无法灵活改变,难以适应网络环境动态变化的安全需求。针对这个问题,提出了一个基于IBE的(t,n)门限秘密共享方案及其门限调整算法。方案通过IBE公钥算法进行秘密分发,影子秘密通过RSA算法进行验证,可有效避免参与者欺骗,当门限值改变时,只需在原有影子秘密基础上增加相应信息,其安全性基于CDH问题难解性。形式化分析和证明显示,新方案能在保证安全性的基础上灵活调整门限值,与已有方案对比分析,新方案具有计算复杂度和影子秘密复用率等方面优势。

关键词:门限秘密共享;IBE;RSA;拉格朗日插值
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2009)11-0128-04

A (t,n) Threshold Adjustment Scheme Based on IBE

YU Chang-guo, YANG Geng, LI Da-wei
(College of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Baek proposed a threshold secret sharing scheme based on IBE named IdThdBm, however, the value of threshold is fixed in system's initialization, it is not flexible enough to abapt the security requiement of the communication scope dynamic changing. To solve this problem, proposed a (t,n) threshold secret sharing scheme based on IBE and the threshold adjustment algorithm. This scheme distributed the secret based on IBE public key algorithm, the shadow secret was demonstrated via RSA algorithm to avoid the cheating between participants. When the value of the threshold changed, the corresponding information should be added to the former shadow secret, the security is based on the CDH problem. The analysis and proof showed that the new scheme not only can adjust the value neatly, but also can insure the security. Compared with the existing scheme, new scheme has some advantages such as the complexity and the rate of reusing the shadow secret and so on.

Key words: threshold secret sharing; IBE; RSA; Lagrange interpolation

0 引 言

秘密共享是信息安全方向的一个重要分支,是安全协议的设计基础。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,秘密共享最早由Shamir和Blakley分别独立提出。所谓(t,n)门限秘密共享方案,就是将共享的秘密信息分成 n 个片段分别分配给 n 个合法的参与者,即一个秘密被 n 个参与者所共享,当且仅当 t 或 t 个以上的参与者联合才可以恢复秘密;而 $(t-1)$ 个或者更少的参与者不能得到该秘密的任何信息。该类方案将安全权限分布于服务节点中,具有很好的鲁棒性。同时很好的适应分布式网络自组织,无中心节点的特性,引起了研究者的广泛关注[1~3]。

在(t,n)门限方案中,门限值 t 很多都是固定不变的,而门限值 t 的选择对方案的性能有很大的影响,若 t 值过大,请求节点短时间内找不到足够多的服务节点,造成时延增大甚至认证失败;若 t 值过小,则容易受到合谋攻击,系统安全性难以保证。而在分布式网络环境下群组通信具有很大的动态性。通信过程中,随着组成员的不断加入和退出,通信规模动态发生变化。初始化时门限值被固定难以满足组通信规模动态变化时可用性和安全性的需求。因此需要设计一种更加灵活的门限秘密共享机制。

目前已有学者在可变门限方面进行了一些探索,Chen等人提出了一种基于双线性映射的动态门限秘密共享方案[4]。该方案中每个参与者持有一个永久私

收稿日期:2009-03-11;**修回日期**:2009-06-18
基金项目:国家自然科学基金项目(60873231);江苏省高校自然科学基金项目(08KJB520006);江苏省"六大人才高峰"基金项目(06-E-044)
作者简介:俞昌国(1984-),男,硕士研究生,研究方向为计算机通信与网间互联、密钥管理;杨 庚,博士后,教授,博士生导师,研究方向为计算机通信与网间互联、网络安全、分布式与并行计算。

钥,秘密分发者选择共享秘密,利用范德蒙德矩阵和参与者的公钥构造线性方程组,通过求解线性方程组可以重构共享秘密,该方案通过调整线性方程组的个数来调整门限值,复杂度为 $O(n\log n)$,但是该方案在秘密重构前未对影子秘密进行验证,容易受到合谋攻击。文献[5]提出的动态门限多秘密共享方案基于 RSA 和 Shamir 门限方案为基础,由参与者自己选择密钥,秘密分发者不知道每个参与者所持有的份额,无需安全信道,且密钥更新、参与者加入退出时均无需更新秘密份额,但其中的插值多项式和模指数计算量较大。黄东平等人[6]基于有限域上离散对数难解性问题提出的方案子秘密由参与者自己保存,子秘密可以复用,且能动态添加或者删除参与者。算法复杂度为 $O(n^2)$。文献[7]提出的 IdThdBm 方案将门限思想跟 IBE 结合,提出了基于身份的门限秘密共享方案。该方案将特定 ID 对应的私钥 D_{id} 作为共享秘密,PKG 可以在生成私钥后进入离线状态。该方案基于 BDH 问题难解性可以抵抗选择密文攻击。

文中基于 IdThdBm 方案提出可变门限秘密方案,新方案基于 RSA 公钥算法对影子秘密进行验证,并能根据实际需要灵活调整门限值的大小。

1　笔者的方案

1.1　预备知识

首先给出一些定义和基本假设[8,9]。记 $Z_q = \{0, \cdots, q-1\}$ 为素数阶 q 的加法群,Z 为正整数,G 为加法群,F 为乘法群。

定义 1(双线性映射)

对所有的 $x, y, z \in G; a, b \in Z$,映射 $\hat{e}: G \times G \to F$ 称为双线性映射,当且仅当满足:

(1) 双线性性:$\hat{e}(ax, by) = \hat{e}(x, y)^{ab}$;

(2) 非退化性:若 x 是 G 的生成元,则 $\hat{e}(x, x)$ 也是 F 的生成元;

(3) 可计算性:给定 $x, y \in G$,存在有效的算法计算 $\hat{e}(x, y)$。

定义 2(Computable Diffie - Hellman 问题)

给定 $< G, q, P, aP, bP >$,随机选择 $a, b \in Z_p^*$,计算 $abP \in G$,称为群 G 上的 CDH 问题。

IBE 公钥加密算法:

IBE 公钥加密算法包括 Setup,Extract,Encrypt,Decrypt 四个函数,分别实现系统参数初始化,私钥提取,加解密过程。

(1)Setup:PKG 生成 q 阶群 G 和生成元 P,以及双线性映射 $\hat{e}: G \times G \to F$。

PKG 随机选取 $s \in Z_q^*$ 计算 $P_{pub} = sP$,选择散列函数:

$H_1: \{0,1\}^* \to G^*$,$H_2: F \to \{0,1\}^l$,明文 $M = \{0,1\}^*$,主密钥 $s \in Z_q^*$。

(2)Extract:对给定的 ID 计算 $Q_{id} = H_1(ID)$,$D_{ID} = sQ_{ID}$,$k_{ID} = Q_{ID}^s$。

(3)Encrypt:计算 $Q_{id} = H_2(ID)$,随机选取 $r \in Z_q^*$,密文 $C = (U, V)$,$U = rP$,$V = H_2(g_{ID}^r) \oplus M$,$g_{ID}^r = \hat{e}(Q_{id}, P_{pub})^r$。

(4)Decrypt:$C = (U, V)$ 为密文,明文 $M = H_2(\hat{e}(k_{ID}, U)) \oplus V$。

RSA 公钥加密算法:

(1) 选择两个大素数 p 和 q,令 $n = pq$,$\phi(n)$ 为欧拉函数。

(2) 选取一个与 $\phi(n)$ 互素的整数 $e < n$,计算整数 d 满足 $ed \bmod \phi(n) = 1$,则公钥为 (e, n),私钥为 d。

(3) 设 M 为明文,则密文为 $c = M^e \bmod n$ 且 $M = c^d \bmod n$。

1.2　方案描述

该方案需要一个系统公告牌用来公布系统参数,参与者可以阅读和下载。PKG 运行密钥生成算法 GK,根据系统安全参数 k 生成系统参数 para 和系统公钥 P_{pub},当收到私钥请求时,运行算法 EX 根据相应 ID 产生公钥 Q_{ID} 私钥 D_{ID},秘密分发者运行算法 DK 将 D_{ID} 转换成影子密钥 S_i 分发给 n 个解密服务器,解密服务器计算认证密钥 R_i。给定一个 ID,加密者运行算法 E 将明文 M 转化为密文 C,解密时,解密服务器运行密钥份额生成算法 D 生成解密份额,解密者运行 SV 验证收到的解密份额,运行算法 SC 重构秘密,运行算法 TC 可调整系统门限值。

1.2.1　*系统初始化*

给定一个安全参数 k,算法 $G(1^k)$ 生成两个 $m(m > 2^k)$ 阶的加法群 G 和乘法群 F,确定双线性映射 $\hat{e}: G \times G \to F$ 和 hash 函数 H_1, H_2, H_3:

$H_1: \{0,1\}^* \to G^*$;

$H_2: F \to \{0,1\}^l$;

$H_3: G^* \times \{0,1\}^l \to G^*$;($l$ 为明文长度)

选择主密钥 $s \in Z_m^*$,计算系统公钥 $P_{pub} = sP$,同时为实现验证秘密份额的有效性,首先 PKG 随机选取两个安全素数 p 和 q,令 $N = pq$。从 $[N^{1/2}, N]$ 中随机选取一个整数 g,使得 $g \neq p$ 且 $g \neq q$,并将 p 和 q 保密,再从 $[2, N]$ 中随机选取一个整数 S_0,满足 S_0 与 $p-1$ 和 $q-1$ 互素,并计算 $R_0 = g^{s_0} \bmod N$,求取一个满足 $S_0 h = 1 \bmod \phi(n)$ 的整数 h,在公告牌上返回系统参数:para $= (G, m, P, \hat{e}, H_1, H_2, H_3, P_{pub}, p, q, N,$

S_0, R_0)。

1.2.2 秘密生成和分发

私钥分配算法:

系统将用于解密的私钥 D_{ID} 分成 n 份子秘密,相比于将主密钥 s 共享的优势在于可以解决PKG一直在线的问题,设解密服务器节点数为 n,解密门限值为 t,$1 \leqslant t \leqslant n < q$,随机选择 $a_1, a_2, \cdots, a_{t-1} \in G^*$,构造 $t-1$ 阶多项式:

$F(x) = D_{ID} + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$,其中,$x \in \{0\} \cup IN, a_{t-1} \neq 0$。

计算每个解密服务器节点 T_i 的影子秘密:$S_i = F(i)$,验证密钥 $R_i = g^{s_i} \bmod N, 1 \leqslant t \leqslant n$。然后分发 (i, S_i) 和 R_i,T_i 将 S_i 保密,将 R_i 在公告牌上公布。

解密份额生成算法(D):

设解密服务器的密钥份额为 S_i,密文 $C = (U, V, W)$,计算 $\overline{H}_3 = H_3(U, V)$。

验证:$\hat{e}(P, W) = \hat{e}(U, \overline{H}_3)$ 是否成立,如果通过验证,计算 $k_i = \hat{e}(S_i, U), R_i = g^{s_i}$;在公告牌上公布 $< i, k_i, R_i >$。

1.2.3 秘密重构

子秘密验证算法(SV):

给定密文 $C = (U, V, W)$,认证密钥集合 $\{y_1, y_2, \cdots, y_n\}$ 和 D 的输出,计算 $\overline{H}_3 = H_3(U, V)$,验证:$\hat{e}(P, W) = \hat{e}(U, \overline{H}_3)$,若通过验证,验证 $\hat{e}(P, W) = \hat{e}(U, \overline{H}_3)$ 是否成立。

若通过验证,进行秘密重构,否则退出协议。

秘密重构算法(SC):

给定密文 C 和任意不少于 t 个密钥份额,计算 $\overline{H}_3 = H_3(U, V)$,验证 $\hat{e}(P, W) = \hat{e}(U, \overline{H}_3)$

若通过验证,计算 $k = \prod_{j \in \phi} k_j^{c_{0j}^{\phi}}$。

根据拉格朗日插值定理,c_{ij}^{ϕ} 定义为:

$$c_{kj}^{\phi} = \prod_{l \neq j}^{l \in \phi} x - l/j - l \in Z_q$$

集合 $\phi \subset \{1, 2, \cdots, n\}$ 且 $|\phi| \geqslant t$

于是得到明文:$M = H_2(k) \oplus V$

1.2.4 门限值调整

门限 t 调整算法(TC):

(1) 门限值增大调整算法($t_{new} > t$)。

重新运行密钥分配算法,随机选择 $a_t, a_{t+1}, \cdots, a_{t_{new}-1} \in G$,构造 $t_{new} - t$ 阶多项式:

$$G(x) = a_t x^t + \cdots + a_{t_{new}-1} x^{t_{new}-1}, a_{t_{new}-1} \neq 0$$

计算:$\Delta S_i = G(i), 1 \leqslant i \leqslant n$,将 ΔS_i 发送给解密服务器节点 T_i。此时解密服务器 T_i 的密钥份额为 $S'_i = S_i + \Delta S_i$,

对给定密文 $C = (U, V, W)$,计算 $\overline{H}_3 = H_3(U, V)$,验证 $\hat{e}(P, W) = \hat{e}(U, \overline{H}_3)$ 是否成立,

若通过验证,计算:$R'_i = g^{s_i}$。

密钥份额验证阶段,对于给定的密文 $C = (U, V, W)$ 和认证密钥集合 $\{R_1, R_2, \cdots, R_n\}$,计算 $\overline{H}_3 = H_3(U, V)$。

验证 $\hat{e}(P, W) = \hat{e}(U, \overline{H}_3), (R_0^{S_i'})^h = R_i' \bmod N$ 是否成立,若验证失败,终止协议。

给定密文 C 和任意 t_{new} 个密钥份额,

计算 $\overline{H}_3 = H_3(U, V)$,验证 $\hat{e}(P, W) = \hat{e}(U, \overline{H}_3)$ 是否成立,若通过验证,计算 $k' = \prod_{j \in \phi} k_j^{c_{0j}^{\phi}}$

其中 c_{0j}^{ϕ} 为拉格朗日系数,且 $|\phi| \geqslant t_{new}$ 明文:$M = H_2(k') \oplus V$。

(2) 门限值减小调整算法 $t_{new} < t$。

计算并分发解密服务器的影子秘密:$S_i = F(i), 1 \leqslant i \leqslant n$。

解密请求者得到 t_{new} 个合法的秘密份额时(验证方法不变),计算:$\xi = \prod_{i=1}^{t_{new}} k_i$,将 ϕ 和 ξ 发送给秘密分发者。秘密分发者验证 $|\phi| = t_{new}, \xi = \hat{e}(\sum_{i \in \phi} S_i, U)$。

验证通过后,从 IN 中随机选择 $t - t_{new}$ 个不同于 ϕ 中元素的最小整数 d_i,计算 $Z_{d_i} = F(d_i), l_i = \hat{e}(Z_i, U), \delta = g^{\hat{e}(\sum_{i=1}^{t-t_{new}} l_i, R_0)}$,将得到的 $< d_i, l_i >$ 发送给解密请求者,将 δ 在公告牌上公布,解密请求者验证 $\lg\delta = \sum_{i=1}^{t-t_{new}} \hat{e}(l_i, R_0) \lg g$,通过验证后,令集合 $\phi' = \phi \cup \{d_i \mid i = t_{new} + 1, \cdots, t\}$,计算 $k' = \prod_{j=1}^{t_{new}} K_j^{c_{0j}^{\phi}} \cdot \prod_{j=t_{new}+1}^{t} l_j^{c_{0j}^{\phi'}}$,其中 $c_{0j}^{\phi'}$ 为拉格朗日系数,且 $|\phi'| \geqslant t_{new}$ 明文:$M = H_2(k') \oplus V$。

2 性能分析与对比

安全性方面,该方案的安全性基于 Baek 等人的方案 IdThdBm,文献[8]基于 BDH 问题难解性在随机预言模型下形式化证明了方案安全性。在分发影子秘密时,分发者发送的是插值多项式的值 S_i, R_i 的计算方法为 $R_i = g^{S_i} \bmod N$。根据离散对数的性质,由 R_i 推算 S_i 是 NP 难度问题,因此攻击者截取 R_i 无法得到插值多项式的任何信息,也就无法得到共享秘密的信息。

在加密者过程中,加密者通过散列函数 H_1, H_2, H_3 和双线性映射 $\hat{e}$ 以及指数异或运算将明文 M 加密得到 C;在解密过程中,解密者收集并验证解密服务器 T_i 的秘密份额然后重构秘密,解密过程主要使用散列

函数 H_2, H_3,双线性映射 $\hat{e}$,指数异或运算和拉格朗日插值运算。

方案计算量具体见表 1。

表 1　方案计算量

运算	加解密	秘密重构	门限值调整	
			增大	减小
$\hat{e}$	4	4	7	$2(\Delta t+1)$
Hash	4	3	5	0
XOR	1	1	1	1
指数	1	2	2	0
插值	0	1	1	1

算法的计算量表明该方案的算法复杂性的主要部分由计算双线性映射运算 $\hat{e}$ 和 hash 函数 H 构成,目前求解双线性映射的可行算法是 Boneh 和 Franklin 提出的基于超奇异椭圆曲线的算法[9]。借助有限域内超椭圆曲线上的 Weil Pairing,双线性映射 $\hat{e}$ 可以表示为:$\hat{e}(P,Q)=f_P(A_Q)f_Q(A_P)^{-1}$。其中 $f_P(A_Q)$ 和 $f_Q(A_P)$ 为具有相同复杂度 $O(\log_2 q)$,因此求解 $\hat{e}$ 的复杂度为 $O(\log_2 q)$,求解 hash 函数使用 SHA1 算法,其计算复杂度为 $O(n)$。

通过拉格朗日插值法实现的秘密共享方案,其性能受插值算法的影响较大,目前有效的拉格朗日插值算法复杂度为 $O(n\log_2^2 n)$,于是不难得到该方案的计算复杂度为 $O(n\log_2^2 n)$。

下面就计算复杂度,插值次数等方面将该方案与已有方案进行对比(见表 2)。

通过对比不难看出:

(1) 在插值次数和复杂度方面,文献[4]中秘密重构由线性方程组实现,故插值次数为 0,由于需要重新生成方程组,当门限值需要调整时已有影子秘密无法重用,因此在空间复杂度方面不占优势。文献[5]使用了公告牌的方式进行门限值更新,需要 C_n^t 次插值运算,其计算代价大大高于文中所提方案。文献[6]在秘密分发过程中对 $n+1$ 个点插值,其时间复杂度为 $O(n\lg^2 n)$;而在秘密恢复时需预先在 k 个点对多项式 $x^k\sum_{i=k}^{n}a_i x^{i-k}$ 求值,在最坏的情况下这个过程要进行 $n\lg^2 n$ 次。该算法在 n 较大,且 $k\approx n/2$ 时具有良好的性能,然而在一般接入结构下满足这种条件的概率很小。当 n,k 值不满足以上条件时,此方案复杂度提高为 $O(n^2)$。

(2) 在秘密份额复用方面,本方案与文献[4 ~ 6]一样,每个参与者的秘密份额可以勇于多次秘密共享过程而无需更新,而文献[7]在每次秘密共享过程前都需要重新分发秘密份额,通信量比较大。

表 2　与现有方案的对比分析

	影子复用	安全信道	插值次数	时间复杂度
IdthdBm	否	需　要	1	$O(n\log_2^2 n)$
文献[4]	是	需　要	0	$O(n\log n)$
文献[5]	是	不需要	C_n^t	$O(nC_n^t\log_2^2 n)$
文献[6]	部分重用	不需要	2	$O(n\lg^2 n)$
该方案	是	不需要	1	$O(n\log_2^2 n)$

3　结束语

文中基于 IdthdBm 门限秘密共享方案和 RSA 密码体制,提出了门限值可变的动态秘密共享方案,并进行了分析和证明,新方案提高了门限固定方案的灵活性,能更好地适应分布式计算环境,方案同时具有影子秘密可重用、可验证、保密性能好等优点。同已有方案对比,该方案具有明显的优越性。

参考文献:

[1] Chen H, Ling S, Xing C. Access structures of elliptic secret sharing schemes[J]. IEEE Transactions on Information Theory, 2008, 54(2): 850 - 852.

[2] Chen W, Li H. Modelling threshold secret sharing schemes in ad hoc networks[J]. IEEE Computer Society, 2008, 43(13): 207 - 214.

[3] Zhang X, Zhang L, Zhang Q, et al. A secret sharing shuffling scheme based on polynomial[J]. Proceedings of the IEEE, 2008, 14(3): 1746 - 1750.

[4] Chen W, Long I, Bai Y. A new dynamic threshold secret sharing scheme from bilinear maps[J]. IEEE Computer Society, 2007, 28(5): 19 - 20.

[5] 庞辽军,李慧贤,王育民. 动态门限多重秘密共享方案[J]. 计算机工程, 2008, 34(15): 164 - 165.

[6] 黄东平,王华勇,黄连生. 动态门限秘密共享方案[J]. 清华大学学报:自然科学版, 2006, 46(1): 102 - 105.

[7] Baek J, Zheng Y. Identity - based threshold decryption, Public Key Cryptography [C]//Proceedings of PKC' 04, LNCS 2947. Berlin: Springer - Verlag, 2004: 262 - 276.

[8] 杨　庚,王江涛,程宏兵,等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报, 2007, 35(1): 180 - 184.

[9] Boneh D, Franklin M. Identity - based encryption from the weil pairing[C]//Advances in Cryptology - CRYPTO2001. [s.l.]: Springer - Verlag, 2001: 213 - 229.