一种高安全的门限群签密方案*

冯 君，汪学明
（贵州大学 计算机科学与信息学院，贵阳 550025）

摘 要：为了满足群组通信的高安全性，将超椭圆曲线密码体制与 Schnorr 数字签名体制相结合，设计了一个高安全的同时具有(t,n)门限签密和(k,l)门限共享验证功能的门限群签密方案。该方案克服了彭等人和 Wang 等人方案的安全缺陷，利用 Desmedt 等人的密钥重新分配协议的思想实现了门限签密和门限解签密的密钥先应式秘密共享。与现有的面向群组通信的广义门限签密方案相比，该方案能避免恶意信息的攻击，能抵抗内部欺诈和外部攻击，具有更小的通信代价和更高的安全性，特别适用于解决带宽受限网络的安全问题。

关键词：门限群签密；门限验证；密钥重新分配；高安全；带宽受限；超椭圆曲线密码体制
中图分类号：TP393 **文献标志码**：A **文章编号**：1001-3695(2013)02-0503-04
doi:10.3969/j.issn.1001-3695.2013.02.051

Threshold group signcryption scheme with high security

FENG Jun, WANG Xue-ming
(*College of Computer Science & Information*, *Guizhou University*, *Guiyang* 550025, *China*)

Abstract: In order to meet the high security of group communication, by combining hyperelliptic curve cryptosystem with Schnorr's signature schemes, this paper proposed a high security group signcryption scheme with a (t,n) threshold signcryption and a (k,l) threshold verification. This scheme improved the security defects of Peng *et al.*, scheme and Wang *et al.*, scheme. It achieved proactive secret sharing of secrets of threshold signcryption and threshold unsigncryption by Desmedt *et al.*, secret redistribution protocol. The new scheme can avoid the attack of the evil information and provide the capability of detecting cheating and identifying the cheater besides the property which threshold group signcryption should have. It has lower communication cost and higher security which is especially suitable for solving security problems of the network with limited resource.

Key words: threshold group signcryption; threshold verification; secret redistribution; high security; limited resource; hyperelliptic curve cryptosystem(HECC)

0 引言

签密(signcryption)是 Zheng[1] 在 1997 年首次提出的认证加密方案，它是在一个合理的逻辑步骤中同时完成数字签名和信息加密，其计算代价和通信开销均比传统的“先签名后加密”方案低得多。在面向群体的网络通信中，群组 A 要发送消息给群组 B，要求仅当 A 中特定数目以上的人联合签密消息才能生效，而且仅当 B 中一定数目以上的人合作才能认证该消息并正确阅读。为了满足这种需要，一些学者提出了同时具有(t,n)签密和(k,l)解签密功能的门限群签密方案[2~9]。Wang 等人[2] 在文献中首次提出满足这种功能的方案，随后文献[3~6]指出此方案是不安全的。文献[6]给出了改进方案，但彭长根等人[7] 发现文献[6]需要密钥分配中心始终参与签密阶段和计算效率低，并提出了新的签密方案(简称 PLL 方案)。2010 年 Wang 等人[8] 指出当解签密群中有恶意成员时，文献[7]中方案是不安全的，并提出了新的方案(简称 WR 方案)。研究发现在签密群中有恶意成员时，PLL 和 WR 方案都是不安全的。而且上述方案都没有解决签密合成员可能有的欺诈行为，且解密密文后再验证签密，不能避免恶意信息的攻击。

超椭圆曲线密码体制(HECC)[10] 是近年来密码学研究的热点和难点问题，它是以超椭圆曲线的 Jacobian 群上离散对数问题的难解性为基础的，相对于其他密码体制而言，具有安全性高、操作数短等其他密码体制无法比拟的优点。近年来出现了一些基于 HECC 的签密或门限签名方案，如文献[11,12]，但是已公开文献中还没有基于 HECC 的群签密方案。

针对目前门限群签密方案安全性不高的问题，本文基于超椭圆曲线离散对数问题(HECDLP)和 Schnorr 数字签名体制，结合上述文献，设计了一个高安全的同时具有(t,n)门限签密和(k,l)门限共享验证功能的门限群签密方案。该方案完全克服了 PLL 方案签密组成员和解签密组成员欺诈的问题；克服了 WR 方案签密组成员内部欺诈；克服了现有门限群签密方案中签密合成员的欺诈问题；利用 Desmedt 等人[13] 的密钥重新分配协议的思想，实现了门限签密和门限验证群成员变化，群成员密钥不断更新，而签密组密钥和解签密组密钥保持不变；在解签密过程中，签密验证通过后再解密密文，避免已有门限群签密方案中可能存在的恶意信息的攻击问题；由于方案的安全性是建立在目前尚没有有效解决超椭圆曲线离散对数问题之上的，因而其安全性能够得到保证，具有操作数短、运算效率高的优势。

收稿日期：2012-07-04；**修回日期**：2012-08-31 **基金项目**：国家自然科学基金资助项目(61163049)；贵州大学研究生创新基金资助项目(理工 2012034)

作者简介：冯君(1986-)，男，河南南阳人，硕士研究生，主要研究方向为密码学及其应用(512675288@qq.com)；汪学明(1965-)，男，教授，博士，主要研究方向为密码学与信息安全、协议分析与模型检测.

1 高安全的面向群组通信的门限签密方案

本文提出的面向群组的门限签密方案共分为初始化、签密密钥重新分配、(t,n)门限签密生成、解签密密钥重新分配、(k,l)共享验证及消息恢复五个部分。文中用到的符号及参数如表 1 所示。

表 1 符号表

符号/参数	意义
$A_{G_s}^{(t,n)}$	由 n 个签密成员集合 G_s 和一个在一次签密中 t 个参与签密者 G_s 组成的访问结构
$\mathrm{ID}_i/\mathrm{ID}_j$	签密成员 U_i 验证成员 U_j 的身份特征
s_i/v_j	签密成员/验证成员的密钥
D_{si}/D_{vj}	签密成员/验证成员的公钥,$D_{si}=s_i\cdot D$,$D_{vj}=v_j\cdot D$
$[D]_e$	将 Jacobian 群元素映射到一个整数
H/KH	一个陷门哈希函数/带有密钥的哈希函数
E_k/D_k	关于密钥 k 的对称加/解密算法

1.1 初始化部分

本部分利用 Shamir 秘密共享方案和 Pedersen 可验证秘密分享方案思想实现签密密钥和共享验证密钥的分配。设有限域 F_q(q 是素数,且 $q>2^{80}$)上亏格为 g 的超椭圆曲线 $C:y^2+h(x)y=f(x)$;$J(C;F)$ 是超椭圆曲线 C 的 Jacobian 群;$\#J(C;F_q)=hn$,n 为大素数,h 是较小的余因子(可为 1);D 为 Jacobian 群上一个具有大素数阶 n 的约化除子,$n\geqslant 2^{80}$;$[D]_e$ 表示将 D 映射到一个正整数。

a)密钥分配中心 KDC 随机选择 $s,v\in Z_q$ 作为签密组和共享验证组私钥,计算签密组公钥 $D_s=s\cdot D\neq \mathrm{div}(1,0)$,共享验证组公钥 $D_v=v\cdot D\neq \mathrm{div}(1,0)$。

b)KDC 按 Shamir 的方案,随机选择 $t-1$ 和 $k-1$ 次多项式

$$f_s(x)=s+a_1x+\cdots+a_{t-1}x^{t-1}\in Z_q[x]$$

$$f_v(x)=v+b_1x+\cdots+b_{k-1}x^{k-1}\in Z_q[x]$$

计算 $s_i=f_s(\mathrm{ID}_i)$ 和 $v_j=f_v(\mathrm{ID}_j)$。其中:ID_i 为签密组成员的特征值,ID_j 为解签密组成员的特征值。分别将 s_i、v_j 秘密地发送给 U_i、U_j($i=1,2,\cdots,t-1$;$j=1,2,\cdots,k-1$)。

c)KDC 计算 $D_{si}=s_i\cdot D$,$D_{vj}=v_j\cdot D$,$D_{ai}=a_i\cdot D$,$D_{bj}=b_j\cdot D$,$H_{ij}=H([s\cdot D_{vj}]_e)$,公开 $C(F_q)$,D,D_s,D_v,D_{si},D_{vj},D_{ai},D_{bj},H_{ij}($i=1,2,\cdots,t-1$;$j=1,2,\cdots,k-1$)。

d)按 Pedersen 可验证秘密分享方案的思想,所有签密组成员验证:

$$s_i\cdot D=D_s+\sum_{x=1}^{t-1}\mathrm{ID}_i^x\cdot D_{ax} \tag{1}$$

所有解签密组成员验证:

$$v_j\cdot D=D_v+\sum_{x=1}^{k-1}\mathrm{ID}_j^x\cdot D_{bx} \tag{2}$$

$$H_{ij}=H([v_j\cdot D_s]_e) \tag{3}$$

如果对所有签密组成员式(1)都成立,对所有解签密组成员式(2)(3)都成立,则密钥分配正确;否则 KDC 出现欺诈行为。

1.2 签密密钥重新分配部分

本部分主要利用 Desmedt 等人的密钥重新分配协议的思想,把签密密钥 s 从当前的 $A_{G_s}^{(t,n)}$ 重新分配到新的 $A_{G'_s}^{(t',n')}$ 中。

a)从当前的 $A_{G_s}^{(t,n)}$ 中随机选取一个参与签密集合 $GS=\{U_1,U_2,\cdots,U_t\}$,对于每个成员 U_i,随机选择 $t'-1$ 次多项式 $f'_{si}(x)=s_i+a_{i1}x+\cdots+a_{i(t'-1)}x^{t'-1}\in Zq[x]$,计算 s_i 的子密钥 $s_{ij}=f_{si}(\mathrm{ID}_j)$,其中 ID_j 是 G'_s 成员的特征值;然后通过安全信道发送给 G'_s 的成员,并公开 $D_{si}=s_i\cdot D$,$D_{aij}=a_{ij}\cdot D$($j\in\{1,2,\cdots,t'-1\}$)。

b)对于 G'_s 中的每个成员 U_j',验证:

$$s_{ij}\cdot D=D_{si}+\sum_{x=1}^{t'-1}\mathrm{ID}_j'^x\cdot(D_{aij})\quad i=1,\cdots,t \tag{4}$$

$$D_s=\sum_{i=1}^{t}L_i\cdot(D_{si}) \tag{5}$$

其中:$L_i=\prod_{j=1,j\neq i}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}$。

c)如果式(4)(5)都成立,则密钥分配正确,每个成员 U'_j 新的子密钥为 $s'_j=\sum_{i=1}^{t}(L_i\cdot s_{ij})$。

1.3 (t,n)门限签密生成部分

设 m 是被签密的消息,m 被加密后的密文为 ch,签密小组 $G_s=\{U_1,U_2,\cdots,U_t\}$。

a)每个 U_i 计算 $L_i=\prod_{j=1,j\neq i}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}$,$e_i=s_i\cdot L_i$,$D_{ei}=e_i\cdot D$,并在授权者中广播 ID_i、D_{ei}。

b)每个 U_i 随机选取一个整数 k_i、t_i,计算 $D_{i1}=k_i\cdot D$,$D_{i2}=k_i\cdot D_v$,$T_{i1}=t_i\cdot D$,$T_{i2}=t_i\cdot D_v$,$H_i=h([T_{i1}]_e\parallel[T_{i2}]_e)$,$T_i=t_i-k_i\cdot H_i$,并在授权者中广播。

c)对于每个成员 U_i,验证每一个 U_j($j\neq i$;$j=1,2,\cdots,t$)。

$$H_j=h([T_j\cdot D+H_j\cdot D_{j1}]_e\parallel[T_j\cdot D_v+H_j\cdot D_{j2}]_e) \tag{6}$$

如果对所有 U_j 都成立,则 U_i 计算:

$$D_1=\sum_{i=1}^{t}D_{i1},D_2=\sum_{i=1}^{t}D_{i2},(k_1,k_2)=H([D_2]_e),\mathrm{ch}=E_{k1}(m)$$

$$R=KH_{k2}(\mathrm{ch}\parallel\mathrm{bind}_{\mathrm{info}})$$

然后计算部分签名 $S_i=(e_i\cdot R+k_i)\bmod q$,并发送给签密执行员。

d)签密合成员利用式(7)验证所有个体签名的有效性。

$$S_i\cdot D=R\cdot D_{ei}+D_{i1} \tag{7}$$

如果式(7)都成立,则计算签名 $S=\sum_{i=1}^{t}S_i$;否则拒绝 U_i 并停止。

e)对于每个签密成员验证:

$$S\cdot D=R\cdot D_s+D_1 \tag{8}$$

如果式(8)不成立,拒绝签密执行员计算的签名并返回到步骤 d)。

f)签密组将签密(R,S,ch)发送给共享验证组。

1.4 共享验证密钥重新分配部分

此部分主要功能是让共享验证的解签密组成员或参与解签密组改变(如成员数目增加、减少)或成员的子密钥更新,但是要求共享验证的密钥保持不变,原理同签密密钥重新分配部分,不同的是:在步骤 a)中当前选择的参与解签密的每个成员计算 $D_{vij}=v_{ij}\cdot D$,并公开 D_{vij};增加步骤 d)KDC 计算 $H_{vj}=H([s\cdot\sum_{i=1}^{t}(L_i\cdot D_{vij})]_e)$,并公开 H_{vj}($j=1,2,\cdots,k'-1$)。详细过程在此省略。

1.5 (k,l)共享验证及消息恢复部分

共享验证组在收到签密(R,S,ch)后,由 l 个成员中的 k 个来完成签密验证和消息恢复,k 个成员为 $G_v=\{U_1,U_2,\cdots,U_k\}$。

a)每个成员计算 $D_{j1}=v_j\cdot D_s$ 并公开。

b)每个成员验证:

$$h([D_{j1}]_e) = H_{vj} \tag{9}$$

如果式(9)成立,则解签密成员是诚实的。然后计算$D_{j2} = D_{vj} \cdot L_j \cdot S - L_j \cdot R \cdot D_{j1}$,$D_2 = \sum_{j=1}^{k} D_{j2}$,其中 $L_j = \prod_{i=1, i\neq j}^{k} \frac{-\mathrm{ID}_j}{\mathrm{ID}_j - \mathrm{ID}_i}$。计算$(k_1, k_2) = H([D_2]_e)$, 验证:

$$R = KH_{k2}(\mathrm{ch} \parallel \mathrm{bind}_{\mathrm{info}}) \tag{10}$$

如果式(10)成立,则接受签密,计算 $m = D_{k1}(\mathrm{ch})$;否则拒绝签密。

2　方案正确性和安全性分析

2.1　方案正确性分析

通过下面定理 1 ~5 分析方案的正确性。

定理 1　(t,n)门限签密生成部分,如果签密成员 U_j 是诚实的,则式(6)成立。

证明　如果签密成员 U_j 是诚实的,则有 $T_j \cdot D + H_j \cdot D_{j1} = T_j \cdot D + H_j \cdot k_j \cdot D = (T_j + k_j \cdot H_j) \cdot D = t_j \cdot D = T_{j1}$,$T_j \cdot D_V + H_j \cdot D_{j2} = T_j \cdot D_V + H_j \cdot k_j \cdot D_V = (T_j + k_j \cdot H_j) \cdot D_V = t_j \cdot D_V = T_{j2}$,$h([T_j \cdot D + H_j \cdot D_{j1}]_e) \parallel [T_j \cdot D_V + H_j \cdot D_{j2}]_e) = h(T_{j1} \parallel T_{j2}) = H_j$,即式(6)成立;反之,成员 U_j 有欺诈行为,则式(6)不成立,证毕。

定理 2　在(t,n)门限签密生成部分,如果签密合成员是诚实的,则式(8)成立。

证明　因为 $S_i = (e_i \cdot R + k_i) \bmod q$,$e_i = s_i \cdot L_i$,如果签密合成员是诚实的,则有 $S_i = (s_i \cdot L_i \cdot R + k_i) \bmod q$,$S_i \cdot D = (s_i \cdot L_i \cdot R + k_i) \cdot D$,$\sum_{i=1}^{t} S_i \cdot D = \sum_{i=1}^{t} (s_i \cdot L_i \cdot R + k_i) \cdot D$,$S \cdot D = \sum_{i=1}^{t} s_i \cdot L_i \cdot R \cdot D + \sum_{i=1}^{t} k_i \cdot D$。由 Lagrange 插值多项式有$\sum_{i=0}^{t} s_i \cdot L_i (\bmod q) = \sum_{i=0}^{t} f_s(\mathrm{ID}_i) \cdot \prod_{j\neq i, j=1}^{t} \frac{-\mathrm{ID}_j}{\mathrm{ID}_j - \mathrm{ID}_i} (\bmod q) = f_s(0) = s$。所以 $S \cdot D = s \cdot D \cdot R + D_1$,$S \cdot D = D_s \cdot R + D_1$,即式(8)成立;反之,签密合成员有欺诈行为,则式(8)不成立,证毕。

定理 3　在(k,l)共享验证及消息恢复部分,如果解签密成员是诚实的,则式(9)成立。

证明　在初始化部分 KDC 计算 $H_{vj} = H([s \cdot D_{vj}]_e)$,并公开 $H_{vj}(j = 1, 2, \cdots, k-1)$,而 $H([s \cdot D_{vj}]_e) = H([s \cdot v_j \cdot D]_e) = H(v_j \cdot D_s)$;在共享验证密钥重新分配部分,KDC 计算 $H_{vj} = H([s \cdot \sum_{i=1}^{t} (L_i \cdot D_{vij})]_e)$,并公开 $H_{vj}(j = 1, 2, \cdots, k'-1)$,而 $H([s \cdot \sum_{i=1}^{t} (L_i \cdot D_{vij})]_e) = H([s \cdot \sum_{i=1}^{t} (L_i \cdot v_{ij} \cdot D)]_e) = H([s \cdot D_{vj}]_e) = H([s \cdot v_j \cdot D]_e) = H(v_j \cdot D_s)$。解签密群中每个成员用自己的子密钥计算 $D_{j1} = v_j \cdot D_s$,并公开 D_{j1}。如果解签密成员是诚实的,则 $H(D_{j1}) = H_{vj}$,即式(9)成立,证毕。

定理 4　本文提出的门限群签密方案实现了门限签密密钥和门限验证密钥的先应式秘密共享。

证明　密钥 s 从当前的 $A_{G_s}^{(t,n)}$ 重新分配到新的 $A_{G'_s}^{(t',n')}$。

$s' = \sum_{j=1}^{t'} (s'_j \cdot L'_j) = \sum_{j=1}^{t'} \{[\sum_{i=1}^{t} (L_i \cdot s_{ij})] \cdot L'_j\} = \sum_{j=1}^{t'} [\sum_{i=1}^{t} (L_i \cdot s_{ij} \cdot L'_j)] = \sum_{i=1}^{t} [L_i \cdot \sum_{j=1}^{t'} (s_{ij} \cdot L'_j)] = \sum_{i=1}^{t} [L_i \cdot \sum_{j=1}^{t'} (s_{ij} \cdot L_{ij})] = \sum_{i=1}^{t} (s_i \cdot L_i) = s$,密钥 s 保持不变,在此过程中可以增加或减少成员,即改变 t 或 n,通过重新分配密钥改变成员子密钥,从而实现了门限签密密钥和门限验证密钥的先应式秘密共享,证毕。

定理 5　上述新的门限群签密方案生成的签密(R, S, ch)如果满足 $R = \mathrm{KH}_{k2}(\mathrm{ch} \parallel \mathrm{bind}_{\mathrm{info}})$则签密有效;否则签密无效。其中:$(k_1, k_2) = H([D_2]_e)$,$D_2 = \sum_{j=1}^{k} D_{j2}$,$D_{j2} = D_{vj} \cdot L_j \cdot S - L_j \cdot R \cdot D_{j1}$,$L_j = \prod_{i=1, i\neq j}^{k} \frac{-\mathrm{ID}_j}{\mathrm{ID}_j - \mathrm{ID}_i}$,$D_{j1} = v_j \cdot D_s$。

证明　$D_2 = \sum_{j=1}^{k} D_{j2} = \sum_{j=1}^{k} (D_{vj} \cdot L_j \cdot S - L_j \cdot R \cdot D_{j1}) = \sum_{j=1}^{k} (v_j \cdot D \cdot L_j \cdot S - L_j \cdot R \cdot v_j \cdot D_s) = (S \cdot D - D_s \cdot R) \cdot \sum_{j=1}^{k} v_j \cdot L_j (\bmod q)$,由 Lagrange 插值多项式性质有$\sum_{j=1}^{k} v_j \cdot L_j (\bmod q) = \sum_{j=0}^{k} f_v(\mathrm{ID}_j) \cdot \prod_{i\neq j, i=1}^{k} \frac{-\mathrm{ID}_i}{\mathrm{ID}_i - \mathrm{ID}_j} (\bmod q) = f_v(0) = v$,又由于 $S \cdot D - D_s \cdot R = D_1$,所以 $D_2 = v \cdot D_1$,又由于$(k_1, k_2) = H([D_2]_e)$,所以 $\mathrm{KH}_{k2}(\mathrm{ch} \parallel \mathrm{bind}_{\mathrm{info}}) = R$,证毕。

2.2　方案安全性分析

本文方案的安全性是基于有限域超椭圆曲线的 Jacobian 上的离散对数问题的难解性,除了具有一般门限群签密方案的特点外,还具有以下特点:

a)克服了 PLL 和 WR 方案的安全缺陷

在 PLL 方案(t,n)门限签密阶段的步骤 a)中,如果签密组中有恶意成员计算 $Y_{i1} = k_i \cdot P$ 和 $y_{i2} = k_i \cdot Q_v$ 使用不同的 k_i,或签密成员发送任意的 Y_{i1}、y_{i2},而签密组中的其他成员却无法辨别,即使签密组中的其他成员严格遵循签密步骤,生成的签密也无法通过接收组的认证。因为恶意成员计算 Y_{i1} 和 y_{i2} 使用不同值的 k_i,$Y_{i1} \neq v \cdot y_{i2}$,$Y_1 \neq v \cdot Y_2$,而在接收组却利用 $Y_1 = v \cdot Y_2$,所以签密在接收组不能通过验证。

同样,在 WR 方案门限签密阶段过程步骤 a)中,签密组中若有欺诈成员计算 k_{si}、r_{si}使用不同值的 t_{si},或使用欺诈的私钥,或发送给另外 $t-1$ 个成员的 Y_{i1}、y_{i2}是任意的,而 WR 方案却无法发现此成员有欺诈行为。

在 PLL 方案(k,l)共享验证及消息恢复阶段的步骤 a)中,如果在接收组成员中有欺诈成员,发送任意的 Y_{j2},而 PLL 方案不能发现此欺诈成员,即使签密组发送的是合法签密也不能通过验证。

在本方案中,在(t,n)门限签密生成部分,每个签密成员利用式(6)验证其他成员是否有欺诈行为,证明见定理 1。在(k,l)共享验证及消息恢复部分,解签密成员用式(9)验证其他成员是否有欺诈行为,证明见定理 3。

b)具有签密合成员合成的签密的可验证性

现已公开发表的门限群签密方案中都没有对签密合成员合成的签密进行验证。如果签密合成员有欺诈行为,那么签密组的签密是无效的,签密在传输过程中也可能受到外部攻击,接收组拒绝签密,但以往方案却无法检测出无效签密是合成员欺诈造成的还是外部攻击造成的。本方案利用式(8)验证可得,证明见定理 2。如果式(8)成立,则无效的签密是外部攻击造成的。

c)防恶意信息的攻击

现已公开发表的门限群签密方案中都是先解密信息后再进行验证签密,如果外部攻击者发送的是恶意信息,接收组就可能受到验证严重的攻击。在本方案中,签密(R, S, ch)在经过 $R = \mathrm{KH}_{k2}(\mathrm{ch} \parallel \mathrm{bind}_{\mathrm{info}})$验证合法后,再用 $m = D_{k1}(\mathrm{ch})$解密信息,避免了恶意信息的攻击。

d)公开验证性

当遇到纠纷时,接收组只需将(R,S,ch)提交给仲裁方,即可验证密文的真伪。整个验证过程不需要明文和接收者的私钥,方案满足公开验证性。

e)具有密钥短和安全性高优势

该方案充分发挥了 HECC 密钥短、安全性高的优点。如果所选超椭圆曲线亏格为 3,所基于的有限域为 60 bit,方案的安全性与 180 bit 的 ECC 等同,远远大于 1 024 bit 的 RSA。因此该方案特别适用于解决带宽受限网络的安全问题。

3 结束语

新方案同时具有(t,n)门限签密和(k,l)门限共享验证功能,在保留已有门限群签名方案优点的基础上,克服了 PLL 和 WR 方案的安全缺陷,对签密合成员合成的签密进行验证,在门限解签名阶段用先验证签密后解密的方式避免了恶意信息的攻击,满足可公开验证性。利用 Desmedt 等人的密钥重新分配协议的思想,密钥保存不变,成员或子密钥不断更新,建立在超椭圆曲线密码体制上,具有更高的安全性,其运算效率、操作数相对于其他公钥密码体制有较大的优势,具有很好的实用性。

参考文献:

[1] ZHENG Yu-liang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption)[C]// Proc of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin:Springer-Verlag,1997:165-179.

[2] WANG C T,CHANG C C,LIN C H. Generalization of threshold signature and authenticated encryption for group communications[J]. IEICE Trans on Fundamentals,2000,E83-A(6): 1228-1237.

[3] TSENG Y M,JAN J K,CHIEN H Y. On the security of generalization of threshold signature and authenticated encryption for group communication[J]. IEICE Trans on Fundamentals,2001,E84-A(10): 2606-2609.

[4] LEE N Y. The security of the improvement on the generalization of threshold signature and authenticated encryption[J]. IEICE Trans on Fundamentals of Electronics,Communications and Computer Sciences,2002,E85-A(10):2364-2367.

[5] WANG Shu-hong,WANG Gui-lin,BAO Feng,*et al*. Security notes on generalization of threshold signature and authenticated encryption for group communication[J]. IEICE Trans on Fundamentals,2004, E87-A(12):3443-3446.

[6] HSU C L,WU T S,WU T C. Improvements of generalization of threshold signature and authenticated encryption for group communications [J]. Information Processing Letters,2002,81(1):41-45.

[7] 彭长根,李祥,罗文俊. 一种面向群组通信的通用门限签密方案[J]. 电子学报,2007,35(1):64-67.

[8] WANG Xue-ming,REN Rui-fang. Design of generalization of threshold signcryption scheme based on ECC[C]//Proc of IEEE International Conference on Information Theory and Information Security. 2010:46-49.

[9] 刘丹妮,王兴伟,郭磊,等. 一种高效的(t,n)门限群签名方案[J]. 计算机科学,2011,38(1):110-112.

[10] MENEZES A J, WU Yi-hong, ZUCCHEZALO R J. An elementary introduction to hyperelliptic curve [EB/OL]. (1996). http://www.math. uwaterloo. ca/ ~ ajmeneze/publications/hyperelliptic. pdf.

[11] NIZAMUDDIN,CHAUDHZY S A,NASAZ W,*et al*. Efficient signcryption schemes based on hyperelliptic curve cryptosystem[C]//Proc of the 7th International Conference on Emerging Technologies. 2011: 1-4.

[12] 陈逢林,胡万宝,孙广人. 基于超椭圆曲线的顺序多重盲签名[J]. 计算机工程,2011,37(9):160-162.

[13] DESMEDT Y,JAJODIA S. Redistributing secret shares to new access structures and its applications,TR-97-01[R]. Virginia:George Mason University,1997.

(上接第 502 页)其中,P 的计算开销约为 Pm 的 9.6 倍,MtP 的计算开销同 Pm 相当。由表 1 可以看出,本算法的计算开销为 7 Pm 加上四次公钥签名和两次公钥加/解密,微大于文献[6],小于文献[3],但是本方案的安全性都高于文献[3,6];而且本方案的计算开销对于航空自组网是完全可以接受的。因此本方案的整体性能优于文献[3,6]。另外,本方案中当用户节点在有效期内再次进行认证时,整个过程 M 与节点 V 之间消息交互次数为一次,只需两次点乘运算。综合以上分析,本方案具有更高的执行效率,更加适合在资源受限的航空自组网中应用。

表 1 各方案效率比较

比较项	文献[3]	文献[6]	本方案
双线性对(M/FA/HA)	4/4/4	0/0/1	0/0/0
公钥签名与验证(M/FA/HA)	0/1/1	0/2/2	0/2/2
公钥加/解密(M/FA/HA)	0/0/0	0/0/0	0/1/1
点乘(M/FA/HA)	7/6/4	5/1/2	3/2/2
消息交互数(M-FA/FA-HA)	3/2	2/2	2/2

4 结束语

在航空自组织网络环境下,对于漫游接入认证具有特殊的要求。本文提出的方案满足双向身份认证、安全的会话密钥建立以及用户身份匿名性等安全性要求。而且与现有的同类方案相比,本方案在满足安全性要求的基础上,用户节点的计算开销和总计算开销明显减少。因此该方案相比于其他漫游接入认证方案更适用于航空自组织网络环境。

参考文献:

[1] YAO Yao, WEI Wang-xing. A cross-domain authentication protocol based on hypercube[C]//Proc of Control and Decision Conference. 2011:3528-3532.

[2] SHIM K A. An ID-based aggregate signature scheme with constant pairing computations[J]. Journal of Systems and Software,2010, 83(10):1873-1880.

[3] 朱辉,李晖,苏万力. 基于身份的匿名无线认证方案[J]. 通信学报, 2009,30(4):130-136.

[4] WANG Yan-jiong, WEN Qiao-yan, ZHANG Hua. A single sign-on scheme for cross domain Web applications using identity-based cryptography[C]//Proc of the 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing. Washington DC:IEEE Computer Society,2010:483-485.

[5] 刘小琼,潘进,李国朋. 基于无证书的两方跨域认证密钥协商协议[J]. 计算机应用研究,2012,29(2):646-649.

[6] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006,29(8):1271-1281.

[7] BELLARE M,NAMPREMPRE C,NEVEN G. Security proofs for identity-based identification and signature schemes[J]. Journal of Cryptology,2008,22(1):1-61.