文章编号:2095－0411(2015)02-0068-04

一种门限可追踪的匿名签密方案*

殷凤梅[1],濮光宁[2],侯整风[3]

(1.合肥师范学院 公共计算机教学部,安徽 合肥 230601;2.安徽财贸职业学院 雪岩贸易学院,安徽 合肥 230601;3.合肥工业大学 计算机与信息学院,安徽 合肥 230009)

摘要:为解决匿名签密算法中签密者身份的追踪问题,提出了一种门限可追踪的匿名签密方案。该方案借助范德蒙行列式生成成员的公钥和私钥,通过在匿名签密过程中附加一些与签密者身份相关的额外信息,实现签密者身份的门限追踪。在不可分模型下,证明了该方案满足匿名性、门限可追踪性、不可伪造性和不相关性。

关键词:签密;追踪性;门限性;1/n 签名;范德蒙行列式

中图分类号:TP 309.7 **文献标识码**:A **doi**:10.3969/j.issn.2095－0411.2015.02.015

AThreshold Traceable Anonymous Signcryption Scheme

YIN Feng-mei[1], PU Guang-ning[2], HOU Zheng-feng[3]

(1.Department of Public Computer Teaching, Hefei Normal University, Hefei 230601, China; 2.Xueyan Trade Faculty, Anhui Finance & Trade Vocational College, Hefei 230601, China; 3.School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: A new threshold traceable anonymous signcryption scheme was presented to solve the problem of tracking the signcrypter's identity in the anonymous signcryption scheme. The member's private key and public key could be obtained with the help of the theory of vandermonde determinant, some additional information related to the identity of the signcrypter was attached in the anonymous signcryption process, which could achieve threshold trace. The scheme proved to satisfy anonymity, threshold traceability, unforgeability and irrelevance in the non-separable model.

Key words: sign-cryption; traceability; threshold; 1 out of n signatures; vandermonde determinant

信息在不安全的信道中传输需要保证其机密性和认证性,可分别通过加密和数字签名来实现。1997 年,Zheng[1]首次提出了签密的概念,即在数字签名的同时完成公钥加密。与传统的"先签名再加密(EtS)"或"先加密再签名(StE)"方案相比,签密方案的计算代价和通信代价大大降低[2]。2002 年,Baek 等[3]在文献[1]基础上给出了签密方案的标准模式。

早期的签密算法为了让解签密者能解签密文,需要将签密者的公钥事先透漏给解签密者,这使得签密者的身份无法隐藏,于是出现了匿名签密技术。匿名签密技术主要采用群签名[4-5]、环签名[6]或1/n 签名[7]技术实现。其中,王继林等[8]基于 1/n 签名思想提出了一个无条件匿名签密算法。由于 1/n

* **收稿日期**:2014-12-24。

基金项目:安徽省高等学校省级优秀青年人才基金重点项目(2013SQRL063ZD);安徽省高等学校省级质量工程教学研究项目(2013jyxm174)。

作者简介:殷凤梅(1981－),女,安徽肥东人,硕士,讲师,主要从事网络与信息安全研究。

签名的特性,该方案只能验证签密者身份的真实性,而无法追踪签密者的真实身份,即实现了签密者的无条件匿名性,可这种特性会给恶意签密者提供了违法犯罪后又无法追踪身份的机会。为了防止签密者的不诚实行为,孙庆英等[9]基于环签名提出了一种可追踪签名者的环签密方案。由于环签名中不存在管理者,签名者身份被追踪时需要环中所有成员协作,若存在某个成员因为有事不能参加追踪,可能导致追踪不成功。

本文在文献[8]的无条件匿名签密过程中附加一些与签密者身份相关的额外信息,需要追踪签密者身份时,任意 t 个成员联合可实现门限追踪,实现签密者身份的门限追踪。

1 文献[8]的无条件匿名签密方案

x_i 是用户 B_i 随机选取的私钥,$y_i=g^{x_i} \bmod p$ 是其对应的公钥,H 是单向哈希函数。无条件匿名签密算法包括签密和解签密 2 个算法。

1.1 匿名用户 B_k 的签密算法

1) 选随机数 $c_i(1\leqslant i\leqslant n, i\neq k)$ 和 α,计算 $z=g^{\alpha}\prod_{i=1,i\neq k}^{n} y_i^{c_i} \bmod p$。

2) 计算 $c=H(L\|m\|z)$,$c_k=c-\sum_{i=1,i\neq k}^{n} c_i \bmod q$,$s=\alpha-x_k c_k \bmod q$,$w=E(y_b^s, m\|s)$(符号"‖"表示串联)。

3) 产生签密 $\sigma=(L, w, g^s, c_1, c_2, \cdots, c_n)$ 并发送给接受者。

1.2 接受者 Bob 的解签密算法

1) 计算 $m'\|s'=E^{-1}((g^s)^{x_b}, w)$,$c'=\sum_{i=1}^{n} c_i \bmod q$。

2) 如果 $c'=H(L\|m'\|g^{s'}\prod_{i=1}^{n} y_i^{c_i} \bmod q)$ 接受 m',否则拒绝 m'。

2 门限可追踪的匿名签密方案

本文在文献[8]的基础上,在不可分模型下(即参与者使用的系统参数都是一样的),利用范德蒙行列式[10]生成成员的公钥和私钥,并在签密中附加一些额外信息,实现门限可追踪的匿名签密方案。本方案主要包含 4 个部分:系统初始化、匿名签密、解签密验证、签密身份追踪。

2.1 系统初始化

本方案中含有 n 个成员 $B_i(1\leqslant i\leqslant n)$,$H:\{0,1\}^* \rightarrow Z_q$ 公开的单向哈希函数,$E(k,m)$ 和 $E^{-1}(k,u)$ 表示用秘钥 k 加密消息 m 和解密密文 u 的对称加/解密算法。可信中心 SC 选取参数 p, q, g(p 是大素数,q 是 $p-1$ 的大素因子,g 是 Z_q 上的 q 阶元素)并公开。SC 选取 t 个随机数 $w_1, w_2, \cdots, w_t$ 并公开,要求每个 w_i 都不相同,且 $((w_i-w_j), p)=1$ $(1\leqslant j<i\leqslant n)$,生成 $n\times t$ 矩阵 $\boldsymbol{W}$。

$$\boldsymbol{W}=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ w_1 & w_2 & w_3 & \cdots & w_t \\ w_1^2 & w_2^2 & w_3^2 & \cdots & w_t^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ w_1^t & w_2^t & w_3^t & \cdots & w_t^t \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ w_1^n & w_2^n & w_3^n & \cdots & w_t^n \end{pmatrix} \tag{1}$$

SC 选取 t 个随机数 $a_1, a_2, \cdots, a_t$ 并保密,按照式(2)计算每个 $x_i(0\leqslant i\leqslant n)$。

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \cdots \\ x_t \\ \cdots \\ x_n \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ w_1 & w_2 & w_3 & \cdots & w_t \\ w_1^2 & w_2^2 & w_3^2 & \cdots & w_t^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ w_1^t & w_2^t & w_3^t & \cdots & w_t^t \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ w_1^n & w_2^n & w_3^n & \cdots & w_t^n \end{pmatrix}\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \cdots \\ a_t \end{pmatrix} \bmod p \tag{2}$$

从式(2)可知,每个 $x_i(0\leqslant i\leqslant n)$ 可用式(3)表示,其中 $x_0=(a_1+a_2+\cdots+a_t) \bmod p$,与 t 个随机数 a_i 直接相关,因此将 x_0 作为门限追踪中的陷门信息保密存储,而将 $x_i(1\leqslant i\leqslant n)$ 作为私钥发送给对应的成员 B_i。

$$x_i=(a_1 w_1^i+a_2 w_2^i+a_3 w_3^i+\cdots+a_t w_t^i) \bmod p \tag{3}$$

SC 计算群公钥 y_0 和每个成员的公钥 $y_i(1\leqslant i\leqslant n)$ 并公开。

$$y_i=g^{x_i} \bmod p \tag{4}$$

反过来,任意 t 个成员的私钥 x_j 由式(2)中相应的 t 个线性方程,构成一个非齐次线性方程组。由于系数行列式为范德蒙行列式,$((w_i-w_j), p)=1$,$|\boldsymbol{W}|\neq 0$,可求出一组唯一解 $(a_1, a_2, \cdots, a_t)$,继而求出 x_0,即 x_0 可用 t 个 x_j 表示。

$$x_0=\sum_{j=1}^{t} b_j x_j \bmod p \tag{5}$$

其中 $b_j(1\leqslant j\leqslant t)$可以由矩阵 $\boldsymbol{W}$ 变化得到。

2.2 匿名签密过程

签密成员 B_k 任选一些公开的成员公钥,构成匿名集 $L=\{y_1\parallel\cdots\parallel y_k\parallel\cdots\parallel y_d\}$,为消息 m 生成签密 σ,并发送给接收方 B_v 解签密。

1) B_k 选择随机数 λ_k,计算 A_k 和 D_k 并公开。

$$A_k=g^{\lambda_k}\bmod p \tag{6}$$

$$D_k=y_0^{\lambda_k}y_k\bmod p \tag{7}$$

2) B_k 选随机数 $c_i(1\leqslant i\leqslant d,i\neq k)$ 和 α,按照顺序计算 Z、c、c_k、s 和 r。

$$Z=g^{\alpha}\prod_{i=1,i\neq k}^{d}y_i^{c_i}\bmod p \tag{8}$$

$$c=H(L\parallel m\parallel Z) \tag{9}$$

$$c_k=c-\sum_{i=1,i\neq k}^{d}c_i\bmod q \tag{10}$$

$$s=\alpha-x_kc_k\bmod q \tag{11}$$

$$r=E(y_v^{s},m) \tag{12}$$

3) B_k 产生消息 m 的签密 $\sigma=(L,r,g^s,c_1,c_2,\cdots,c_d)$,并发送给验证者 B_v。

2.3 解签密验证过程

接收方 B_v 收到签密 σ 后,首先解签密 σ 获得消息原文 m',然后验证签密是否合法。

1) B_v 计算获得 m' 和 c'。

$$m'=E^{-1}((g^s)^{x_v},r) \tag{13}$$

$$c'=\sum_{i=1}^{d}c_i\bmod q \tag{14}$$

2) B_v 验证等式(15)是否成立。

$$H(L\parallel m'\parallel g^s\prod_{i=1}^{d}y_i^{c_i}\bmod q)=c' \tag{15}$$

若等式(15)成立,B_v 接受消息 m';否则拒绝消息 m',并丢弃签密 σ。

2.4 签密身份追踪过程

如果签密成员有不诚实或破坏行为时,任意 t 个成员可联合追踪签密成员的身份,即实现门限匿名追踪。

1) 每个成员 B_i 使用各自的私钥 x_i 计算 e_i,然后联合计算 E_k。

$$e_i=A_k{}^{b_ix_i}\bmod p \tag{16}$$

$$E_k=\prod_{i=1}^{t}e_i\bmod p \tag{17}$$

2)输出示证者公钥身份信息 $y_{k'}$。

$$\frac{D_k}{E_k}\bmod p=y_{k'} \tag{18}$$

3 方案分析与比较

3.1 方案分析

安全的匿名签密算法需要满足匿名性、不可伪造性和不相关性。下面从 5 个方面分析本文方案满足匿名签密算法的安全需求。

定理 1 签密算法满足解签密的唯一性。

解签密中的 c' 与签密中的 c 是同一个,接收方可通过等式(15)来判定签密是否是伪造的。等式(15)的正确性证明如下:

$$\begin{aligned}&H(L\parallel m'\parallel g^s\prod_{i=1}^{d}y_i^{c_i}\bmod q)\\&=H(L\parallel m'\parallel g^{\alpha-x_kc_k}\prod_{i=1}^{d}y_i^{c_i}\bmod q)\\&=H(L\parallel m'\parallel g^{\alpha-x_kc_k}g^{x_kc_k}\prod_{i=1,i\neq k}^{d}y_i{}^{c_i}\bmod q)\\&=H(L\parallel m'\parallel g^{\alpha}\prod_{i=1,i\neq k}^{d}y_i{}^{c_i}\bmod q)\\&=H(L\parallel m'\parallel Z)=c'\end{aligned}$$

从等式(15)的证明过程可知,不可能存在 m' 和 m'' 同时满足等式(15)。因此,本签密算法满足解签密的唯一性。

定理 2 签密者身份具备匿名性。

每个 $c_i(1\leqslant i\leqslant d,i\neq k)$ 都是在 Z_q 上随机选取的,因此由等式(10)计算得到的 c_k 在 Z_q 上分布均匀,由等式(11)计算得到的 s 在 Z_q 上也分布均匀,从 $(g^s,c_1,c_2,\cdots,c_d)$ 判断出是哪一个成员签密几乎不可能,即匿名签密过程可以保证签密者的匿名身份。

定理 3 签密者身份具备门限可追踪性。

任意 t 个合法成员联合计算 E_k,通过等式(18)可追踪到签密者 B_k 的公钥身份 $y_{k'}$。

等式(18)的正确性证明如下:

$$\begin{aligned}&E_k=\prod_{i=1}^{t}e_i\bmod p=\prod_{i=1}^{t}A_k{}^{b_ix_i}\bmod p\\&=g^{\lambda_k\sum_{i=1}^{t}b_ix_i}\bmod p=g^{\lambda_kx_0}\bmod p\\&=y_0{}^{\lambda_k}\bmod p\end{aligned}$$

则:$\dfrac{D_k}{E_k}\bmod p=y_k{}'$

定理 4 签密过程满足不可伪造性

如果攻击者试图伪装成某个成员 B_i 通过解签密认证,需要提供正确的签密 $\sigma=(L,r,g^s,c_1,c_2,\cdots,c_d)$ 给验证者。从 2.2 节可知,签密的生成需要用到成员 B_i 的私钥 x_i,因而攻击者需要获得 x_i,而 x_i 是保密的,攻击者只能从公开的公钥 y_i 中试图获得,这就需要攻破离散对数求解问题,而在现阶段这几乎是不可能的。因此,攻击者无法伪装成合法的签密成员。

定理5 签密过程满足不相关性

每次匿名签密,签密者选择的 α 和 c_k 的都是随机的,生成的签密 σ 也将不同,因而不能判定两次签密是否是来自同一个签密人。

3.2 方案比较

为了实现签密者身份的可追踪性,在文献[8]的基础上,本文方案只是在签密过程中附加了与签密者身份相关的额外信息,在保证匿名签密算法安全需求的前提下,实现了签密者身份的可追踪性。

文献[9]在 MIBAS 通信方案基础上实现环签密的可追踪性,基于椭圆曲线离散对数难解问题,实现匿名签密的不可伪造性,随机选择随机数 x_i 和 t_i,使得签密过程满足不相关性。由于文献[9]基于环签名实现签密,追踪环节需要环全体成员的参与,追踪自由度不高。本文方案在门限秘密共享思想的基础上,实现了匿名签密的门限可追踪性,在保证匿名安全性的同时,提高了追踪的灵活度。

3种匿名签密方案的性质比较如表1所示。

表1 匿名签密方案性质比较

Table 1 Comparison of anonymous signcryption

方案	匿名性	可追踪性	是否门限可追踪	不可伪造性	不相关性
文献[8]方案	√	×	×	√	√
文献[9]方案	√	√	×	√	√
本文方案	√	√	√	√	√

4 结 论

本文利用范德蒙行列式生成成员的公钥和私钥,通过在文献[8]的无条件匿名签密过程中附加一些额外信息,实现了签密者身份的门限可追踪性。通过分析证明,本方案满足匿名签密算法的安全性。与文献[8]相比,本方案可有效地御防签密人的不诚实行为。与文献[9]相比,本方案可实现签密者身份的门限追踪。下一步我们将对动态门限追踪的签密方案进行深入研究,并设计出切实可行的实际应用方案。

参考文献:

[1]Zheng Y.Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption)[M]//Advances in Cryptology - CRYPTO'97. Berlin: Springer - Verlag, 1997:165-179.

[2] Zheng Y.Signcryption and its applications in efficient public key solutions[M]//Information Security. Berlin: Springer - Verlag, 1998:291-312.

[3] Baek J, Steinfeld R, Zheng Y. Formal proofs for the security of signcryption[C]//PKC 2002. Berlin: Springer-Verlag, 2002: 80-98.

[4] Chaum D, Heyst V E. Group Signatures[C]//Proceedings of Eurcrypt'91. Berlin: Springer-Verlag, 1991: 257-265.

[5] Camenisch J, Stadler M. Efficient group signature schemes for large groups[M]//Advances in Cryptology - Crypto'97. Berlin: Springer-Verlag, 1997: 410-424.

[6] Rivest R L, Shamir A, Tauman Y. How to leak a secret [A]. Proc of Asiacrypt'01[C]. Berlin: Springer- Verlag, 2001: 552-565.

[7] Abe M, Ohkubo M, Suzuki K. 1-out-of-n signatures from a variety of keys[A]. Proc of Asiacrypt'02 [C]. Berlin: Springer- Verlag, 2002: 415 - 423.

[8] 王继林,毛剑,王育民.一个无条件匿名的签密算法[J].电子与信息学报,2004,26(4):435-439.

[9] 孙庆英,吴克力,徐会艳.一种可追踪签名者的环签密方案[J].计算机工程,2011,37(16):129-131.

[10] 吴春英,李顺东.高效的强(n,t,n)可验证秘密共享方案[J].计算机科学,2013,40(9):130-132.

(责任编辑:李艳)