第 26 卷第 3 期 电子与信息学报 Vol.26No.3
2004 年 3 月 Journal of Electronics & Information Technology Mar. 2004

一个无条件匿名的签密算法 [1]

王继林 毛 剑 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要: 匿名技术在隐私保护中具有广泛应用，而签密可以在一个逻辑步骤内同时完成数字签名和公钥加密两项功能，其代价显著低于常规“先签名再加密”方法的代价．目前的签密算法中，签密人的具体身份是公开的．该文基于 Diffie-Hellman 密钥交换协议和匿名签名的思想，在不可分模型下提出了一个无法追踪签密人身份的无条件匿名签密算法，并证明了该算法的正确性和安全性．

关键词: 签密，无条件匿名性，群签名

中图分类号: TN918 **文献标识码**: A **文章编号**: 1009-5896(2004)03-0435-05

An Unconditional Anonymous Sign-Cryption Algorithm

Wang Ji-lin Mao Jian Wang Yu-min

(*National Key Lab. of ISN, Xidian Univ., Xian* 710071, *China*)

Abstract Techniques which can realize anonymity play an important role in the protection of partners' privacy. Sign-cryption can sign and encrypt message in one logic step and has lower cost than that of "firstly sign and then encrypt". Based on the thoughts of Diffie-Hellman decision problem and anonymous signature, an unconditionally anonymous sign-cryption algorithm is given in this paper.

Key words Sign-cryption, Unconditional anonymity, Group signature

1 引言

在电子拍卖、电子投票和电子现金等具体应用中，为了防止用户的个人信息被非法窃取和使用，需要进行匿名签名，即验证者仅能验证签名者是否属于某个特殊群体而不知道具体签名者的身份．

由 D. Chaum 和 E. van Heyst 等人提出的群签名 [1,2] 是一种重要的匿名签名技术．群签名允许一个群成员代表群进行匿名签名，但这种匿名性是可控制的，当发生争执时，群管理员可以揭露签名者的真实身份．在某些实际应用中，用户希望能够对群管理员的这种特权给以必要的约束，以防止其滥用职权．

$1/n$ 签名 [3,4] 和 Rivest 等人最近提出的环签名 [5] 可以实现签名者的无条件匿名性，即无法追踪签名人的身份．无条件匿名签名尽管引起了许多争议，大量的无条件匿名业务的开展必然会给违法犯罪分子提供有利条件，但在对信息需要长期保护的一些特殊环境中却非常有用．例如，即使 RSA 被攻破也必须保护匿名性的场合．最近无条件匿名签名问题特别是环签名引起了人们的普遍关注 [6,7] ．

签密作为一种新的密码学构件，能在一个逻辑步骤内同时完成数字签名和公钥加密，比先签名再加密的常规消息传递的代价小得多．当签密方案采用小的安全参数时 (公共模数为 512 位)，与常规方法比，签密的计算代价降低为 58%，消息扩展率为 70%；当采用长的安全参数

[1] 2002-12-09 收到，2003-05-06 改回
国家自然科学基金资助课题 (60073052)

时 (公共模数为 1536 位)，签密的计算代价降低为 50%，消息扩展率为 91%。签密的节省代价正比于安全参数的长度，当取较大安全参数时的安全性能更佳 [8,9]。

目前的签密算法中，都需要让解签密人知道具体签密人的公钥，以便解签密人来解签密文，这使得签密人的身份无法隐藏。利用匿名公钥技术可以实现匿名签密，群签密就是其典型代表，但这种匿名性是可以追踪的，签密人的真实身份可以被提供匿名公钥的管理员恢复。

本文基于 Diffie-Hellman 密钥交换协议和无条件匿名签名的思想，在不可分模型 (即参与者使用的系统参数是一样的) 下提出了一个无法追踪签密人身份的无条件匿名签密算法。可以证明所给算法是安全的、正确的。本文的组织结构如下：第 2 节介绍签密的基本算法和有关特点；第 3 节是我们的无条件匿名签密算法；第 4 节是正确性和安全性分析；最后是结束语。

2 签密的基本算法及其特点

2.1 签密的基本算法

数字签密由一对算法 (S, U) 构成，其中 S 为签密算法，U 为解签密算法；(S, U) 满足下列条件 [8,9]：

(1) *解签密惟一性* 给定任意长度的消息 m，算法 S 签密消息 m 输出已签密文 c。一旦输入 c，算法 U 解签密 c 并无二义地恢复消息。

(2) *安全性* (S, U) 同时实现加密方案的安全特性和签名方案的安全特性。这些性质主要包括消息内容的机密性、不可伪造性和不可否认性。

(3) *有效性* 在同样条件下，签密方案的计算和通信代价是小于常规的“先签名再签密”的方案。

表 1 是一个基于 ElGamal 数字签名的数字签密算法 [8]。

表 1 数字签密算法

由发送者 Alice 对 m 的签密		由接收者 Bob 对 (c,r,s) 解签密
$x \in_R [1,\cdots,q-1]$ $(k_1,k_2)=\text{hash}(y_b^x \bmod p)$ $c=E(k_1,m)$ $r=\text{KH}_{k_2}(m)$ $s=x/(r+x_a) \bmod q$	$\Rightarrow c,r,s \Rightarrow$	$(k_1,k_2)=\text{hash}((y_a\cdot g^r)^{sx_b} \bmod p)$ $m=E^{-1}(k_1,c)$ 仅当 $\text{KH}_{k_2}(m)=r$ 接受 m

参数注释如下：p 为大素数；q 为 $p-1$ 的大素因子；g 为从 $[1,\cdots,p-1]$ 随机选取的模 p 的 q 阶随机整数；hash 为单向杂凑函数；$E(k,m)$ 和 $E^{-1}(k,c)$ 为一对单钥加 / 解密算法 (如 DES 或 AES)，分别表示用密钥 k 加密消息 m 和解密密文 c。$\text{KH}_k(m)$ 为带密钥 k 的杂凑函数；$\in_R$ 表示随机均匀选取集合中的元素；x_a 为 Alice 从 $[1,\cdots,q-1]$ 选取的私钥，其相应的公钥 $y_a=g^{x_a} \bmod p$；类似地，Bob 的私钥为 x_b，相应的公钥为 $y_b=g^{x_b} \bmod p$。以上除对称加密的密钥和各人的私钥外，其余均是公开的。

2.2 签密算法的特点

效率 密码运算的代价可以通过信源和信宿加载于消息的计算时间和消息扩展率来测量，对于现有标准的“先加密再签名的”消息传递方式，用安全可信的方式交付消息的代价是数字签名和加密代价的总和。

签密与先签名再加密相比的显著优点在于计算量和通信管理量大大减少了，具体分析可参见文献 [9]。如果用 Cost 表示代价，从文献 [9] 的分析可以看出，下列不等式是成立的：Cost(signcryption) <<Cost(signature)+Cost(encryption)。

安全性 与任何其它密码系统相同，签密的安全性包括两个方面，(1) 签密的消息不希望泄露给除发送者 Alice 和接收者 Bob 以外的第三方，同时防止其它方 (包括 Bob) 伪装成 Alice；

(2) 抗击能接入 Alice 的签密算法和 Bob 的解签密算法的人们能想象的最强力攻击者的攻击。

具体地讲，签密算法如果满足不可伪造性、不可否认性和机密性，则该签密方案被认为是安全的。

可以证明，表 1 所给的签密算法是安全的 [8] 。

3 一个无条件匿名的签密算法

根据 Diffie-Hellman 密钥交换协议和匿名签名特别是文献 [4] 的思想，我们构造了一个不可分模型下无条件匿名的签密算法。有关参数的假定同 2.1 节中的描述，设第 i 个用户 B_i 的私钥为 x_i ，对应的公钥为 $y_i = g^{x_i} \bmod p$; $H : \{0,1\}^* \to Z_q$ 为一个公开的单向杂凑函数。

3.1 匿名用户 B_k 的签密算法

设每个人的公钥是公开的，签密者 B_k 首先任选一些公钥 (包括他自己的公钥) ，构成本次的匿名集 L ，为了方便叙述，不妨假定 $L = \{y_1 \| y_2 \| \cdots \| y_n\}$ ，然后对消息 m 计算其签密 $S(B_k, m)$ 如下：

$S(B_k, m)$

(1) $\alpha \in_R Z_q$, for $i = 1, 2, \cdots, k-1, k+1, \cdots, n$, $c_i \in_R Z_q$; $z = g^{\alpha} \prod_{i=1, i \neq k}^{n} y_i^{c_i} \bmod p$;

(2) $c = H(L \| m \| z)$;

(3) $c_k = c - (c_1 + \cdots + c_{k-1} + c_{k+1} + \cdots + c_n) \bmod q$;

(4) $s = \alpha - x_k c_k \bmod q$;

(5) $w = E(y_b^s, m \| s)$;

(6) Return $\sigma = (L, w, g^s, c_1, c_2, \cdots, c_n)$ 。

3.2 接收者 Bob 的解签密算法

$U(\sigma)$

$m' \| s' = E^{-1}((g^s)^{x_b}, w)$;

$c' = (c_1 + \cdots + c_{k-1} + c_k + c_{k+1} + \cdots + c_n) \bmod q$;

If $c' = H(L \| m' \| g^{s'} \prod_{i=1}^{n} y_i^{c_i} \bmod q)$;

then Accept m';

else Reject 。

4 算法分析

4.1 特点

在该算法中，签密和解密的计算量主要花费在 n 个 $y_i^{c_i}$ 的计算上，签密文 σ 的长度也线性依赖于 n 。值得注意的是，算法中的匿名群体的成员个数 n 是由签密人自由选取的。n 越大，匿名范围越广，但计算量和提交数据的长度也就越大。签密人可以根据自己对匿名强度的需要进行灵活地选取。

4.2 安全性

为了实现签密人的无条件匿名性，需要在这里对前述的普通签密算法的安全性要求做一些调整。

定义 1　一个签密算法是无条件匿名的，就是指攻击者即便非法获取了所有可能的签密者的私钥，他能确定出真正的签密者的概率不超过 $1/n$ ，这里 n 为匿名集合中元素 (可能的签密者) 个数。

定义 2　一个无条件匿名的签密算法是安全的，如果它满足机密性、不可伪造性和不相关性。

这里的机密性同普通签密算法一样，是指签密的消息不会泄露给除发送者和接收者以外的第三方；这里的不可伪造性是指被指定的匿名集合外的人在不知道匿名集合中任何成员的私钥的情况下，无法伪造任何一个消息 m 的签密被接收方接收；不相关性是指无法判定两次不同的签密是否来自同一个签密人。

定理 1(正确性) 上述签密算法满足解签密的唯一性。

证明 这一结论是显然的，因为 c' 是同一个，如果解签密不唯一，则存在 m' 和 m'' 满足 $H(L\|m'\|g^{s'}\prod_{i=1}^{n}y_i^{c_i}\bmod q)=H(L\|m''\|g^{s'}\prod_{i=1}^{n}y_i^{c_i}\bmod q)$ 。

定理 2(正确性) 上述签密算法满足签密人的无条件匿名性。

证明 算法中除了签密人 B_k 的 c_k 外，其余的 c_i 都是在 Z_q 上随机选取的。由于 α 也是在 Z_q 上均匀选取的，故 c_k 在 Z_q 上的分布是均匀的。对于固定的 m, $(c_1,c_2,\cdots,c_n)$ 有 q^n 种等可能的取值，而 s 完全由 m, $(c_1,c_2,\cdots,c_n)$ 和 α 唯一确定。因此，从 $(g^s,c_1,c_2,\cdots,c_n)$ 判断出具体为哪个签密人的签密是不可能的。由于匿名集合中任何成员的地位是一样的，即便所有人的私钥泄露也无法确定具体签密人。因而上述算法满足签密人的无条件匿名性。

广义 Diffie-Hellman Problem(DHP)：已知循环群 G, g 为 G 的生成元，且已知 g^a, g^b 为 G 中元素，求 g^{ab} 的问题为广义 Diffie-Hellman 问题。

定理 3(安全性) 设 G 上，广义 Diffie-Hellman Problem 困难，则上述签密算法满足机密性。

证明 对消息 m 的签密算法中，对称加密密钥为 g^{sx_b} ，在 Diffie-Hellman Problem 困难假设下，除发方和接收方外，其它用户是不可能解出密钥 g^{sx_b} 的，因而也就不可能解密出消息 m 。

定理 4(安全性) 上述签密算法满足不可伪造性。

证明 外部攻击者要假冒 L 中某个用户进行签密，他可以构造出 σ 中的 L, g^s, c_1, c_2, $\cdots$, c_n ，但为了构造出能被收方接受的 w ，他需要从 g^s 中提取出对应的 s 。在不知道匿名集 L 中任何成员的私钥的情况下，求解 s 等价于求解离散对数问题。

定理 5(安全性) 上述签密算法满足不相关性。

证明 因为签密人每次签密时选用的 α 和 c_i 是随机的，其用到的 s 和 g^s 也是随机的。故不能判定两次签密是否来自同一个签密人。

5 结束语

签密可以在一个逻辑步骤内同时完成数字签名和公钥加密两项功能，其代价显著低于常规“先签名再加密”方法的代价。目前的签密算法中都需要让解签密人知道具体签密人的公钥，以便解签密人解签密，即便像群签密那样采用匿名公钥技术，也是能够追踪出签密人的具体身份的。但在电子选举、电子投标等隐私保护较强的一些应用中，需要无条件地保护参与者的匿名性。本文基于 Diffie-Hellman 密钥交换协议和匿名签名的思想，在不可分模型下提出了一个无法追踪签密人身份的无条件匿名签密算法，并证明了算法是正确的、安全的。

参 考 文 献

[1] Chaum D, Van Heyst E. Group signatures. In D. W. Davies, editor, Proc. of Eurocrypt'91, LNCS, Springer-Verlag, 1992, vol.547: 257–265.

[2] Camenisch J, Stadler M. Efficient group signature schemes for large groups. In Advances in Cryptology-CRYPTO'97, LNCS, Springer-Verlag, 1997, vol.1296: 410–424.

[3] Cramer R, Damgard I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. In Y. G. Desmedt, editor, CRYPTO'94, LNCS, Springer-Verlag, 1994, vol.839: 174–187.

[4] Abe M, Ohkubo M, Suzuki K. 1-out-of-n signatures from a variety of keys. Asiacrypt'2002, LNCS, Berlin, Heidelberg, Springer-Verlag, 2002, vol.2501: 415–423.

[5] Rivest R L, Shamir A, Tauman Y. How to leak a secret. In C. Boyd, editor, in Proc. of Asiacrypt'01, LNCS, Springer-Verlag, 2001, vol.2248: 552–565.

[6] Bresson, Stern, Szydlo. Threshold ring signatures for ad-hoc groups. Cryptology'2002, LNCS, Berlin Heidelberg, Springer-Verlag, 2002, vol.2442: 465–480.

[7] Fangguo Zhang, Kwangjo Kim. ID-Based blind signature and ring signature from pairings. Asiacrypt'2002, LNCS, Berlin Heidelberg Springer-Verla, 2002, vol.2501: 533–547.

[8] Zheng Y. Digital signcryption or how to achieve cost(signature and encryption) << cost(signature)+cost(encryption). B. Kaliski(Ed), Advances in Cryptology, in Proceedings Crypto'97, LNCS, Springer-Verlag, 1997, vol.1294: 165–179.

[9] Zheng Y. Signcryption and its application in efficient public key solutions. in Proc. of Information Security Workshop(ISW'97), LNCS, Springer-Verlag, 1998, vol.1396: 291–312.

王继林：　男，1965 年生，副教授，博士生，研究方向为电子商务的安全技术.

毛　剑：　女，1978 年生，博士生，研究方向为通信网的安全.

王育民：　男，1936 年生，教授，博士生导师，研究方向为密码学.