一种基于身份的环签密方案

黄欣沂, 张福泰, 伍 玮
(南京师范大学数学与计算机科学学院, 江苏南京 210097)

摘 要: 使用威尔配对, 本文提出了一种基于身份的环签密方案, 给出了具体的算法. 该方案能够使消息的发送者以一种完全匿名的方式发送消息, 并且同时实现保密性和认证性两种功能. 我们证明了在决策双线性 Diffie-Hellman问题难解的假设下, 新提出的方案对自适应选择密文攻击是安全的. 与传统的先签名后加密的方案相比, 本方案中密文长度有了明显的降低, 在低带宽的要求下更加可行.

关键词: 威尔配对; Diffie-Hellman问题; 身份; 环签密
中图分类号: TB11 文献标识码: A 文章编号: 0372-2112 (2006) 02-0263-04

An Identity-Based Ring Signcryption Scheme

HUANG Xin-yi, ZHANG Fu-tai, WU Wei
(School of Mathematics and Computer Science, Nanjing Normal University, Nanjing, Jiangsu 210097, China)

Abstract Using weil pairing an identity-based ring signcryption scheme is proposed. Its concrete algorithm is given. Using this scheme the message sender can anonymously send the message; the confidentiality and authenticity of message are realized at the same time. It is proved that the scheme is secure against adaptively chosen cipher text attack under the difficulty of the Decisional Bilinear Diffie-Hellman problem. Compared with the traditional "signature then encryption scheme", the cipher text of our scheme is rather short. So our scheme is more applicable to systems where cryptogram is sent over a low bandwidth channel.

Key words diffie-hellman problem; identity; ring signcryption

1 引言

保密和认证是当代密码系统最重要的两个方面. 在大多数情况下, 需要同时达到数据的保密性和认证性. 传统的方法是采用先签名后加密的方法来同时达到这两个目的, 其运算代价是两者之和, 效率比较低. 1997年 YuLiang Zheng[1] 首先提出了签密的概念 (signcryption), 其主要思想是把加密系统和签名系统的功能结合起来, 能在逻辑上同时实现数据的保密性和认证性, 但是比传统的先签名后加密 (signature then encryption)的方法效率高.

1984年, shamir[2] 首先提出了基于身份的公钥密码系统 (identity-based public key cryptosystem). 在这个密码系统中, 用户的公钥为该用户的身份信息, 用户的私钥是由一个可信的密钥生成中心 (TKGC)颁发的. 这样, 任何一对用户都可以安全地通讯, 而不需要交换他们的公钥证书, 不需要使用公钥字典, 也不需要使用第三方的在线服务. 但是直到 2001年才由 Boneh和 Franklin[3] 提出了一个实用的基于身份的密码系统.

环签名是由 Rivest, Shamir和 Tauman[7] 在 2001年正式提出的. 环签名可以让用户以一种完全匿名的方式对消息进行签名. 接收方只能确信签名来自于某个群体但是不知道是群体中的哪个成员对消息签名. 环签名可以看成是一种简化的群签名. 在环签名的方案中, 只有群体的用户而没有群体的管理者. 群签名和环签名的共同点是: 接收方都无法区别出是谁对消息进行签名. 但是在群签名当中, 群体的管理者可以在需要的时候指出谁是消息的签名者, 而在环签名中, 除了签名者以外没有人能够恢复出签名者的身份. 环签名开始是作为一种泄露秘密的技术被提出的, 它可以使泄密者无条件匿名. 既然泄露的是秘密, 泄露者一般并不想让任何人都能获得秘密, 而是希望把秘密泄露给一些特定的接收者. 因此, 对要泄露的秘密采取加密保护是非常必要的.

在本文中, 我们考虑在为泄密者提供无条件匿名性的同时, 如何用较小的代价来保护要泄露秘密的机密性. 我

收稿日期: 2004-05-08; 修回日期: 2005-08-24
基金项目: 江苏省高校自然科学研究重点项目 (No. 03KJA520066); "十五""211"工程重点学科项目 (No. 181070H901)

们首先提出了一种基于身份的环签密方案,该方案建立在基于身份的环签名方案的基础上[3],使得在达到数据的保密性和认证性要求的同时,消息的发送者可以完全匿名得发送消息,并且密文的长度比传统的"先签名后加密"方法有了明显的降低.

2 预备知识

在本节中,我们给出了与本方案相关的一些数学知识.

2.1 二次剩余(Quadratic Residue)

设 a, p, 是任意的整数, gcd (a, p) = 1, 如果同余式 $x^2 = a \pmod p$ 有解,那么 a 就称作模 p 的一个二次剩余.

欧拉准则: 设 p 是一个奇素数, gcd (a, p) = 1, 则 a 是模 p 的二次剩余当且仅当 $a^{(p-1)/2} = 1 \pmod p$.

如果 $p = 3 \pmod 4$, 且 a 是模 p 的二次剩余,则 a 模 p 的平方根是 $r_{\{1,2\}} = \pm a^{(p+1)/4} \pmod p$.

随机选取一个整数 a, a 是模 p 的二次剩余的概率大约是 1/2

2.2 Weil Pairing

设 p, q 是素数,且有 p = 12q - 1, E 是由 Weierstrass 方程 $y^2 = x^3 + 1$ 定义的在 F_p 上的超奇异(supersingular)椭圆曲线. E 在 F_p 上的点的集合 $E(F_p) = \{(x, y) \in F_p \times F_p : (x, y) \in E\}$ 形成了一个阶为 p + 1 的循环群. 而且,因为 p = 12q - 1, 所以 $E(F_p)$ 的阶为 q 的点和无穷远点 O 形成了一个循环子群,我们用 G_1 表示该子群,并设它的一个生成元为 g. G_2 是 $F_{p^2}^*$ 上的 q 阶子群. $x \in_R S$ 表示从集合 S 中按均匀分布随机选择一个元素,并且把它的值赋给 x. Weil Pairing 是满足以下的性质的映射 $e: G_1 \times G_1 \to G_2$:

①双线性(Bilinear): 对于任意 $a, b \in_R Z$, 有 $e(a \cdot g, b \cdot g) = e(g, g)^{ab} = e(a \cdot b \cdot g, g) = e(g, a \cdot b \cdot g)$.

②非退化性(Non-degenerate): $e(g, g) \in F_{p^2}^*$, 且 $e(g, g) \neq 1_{G_2}$, 1_{G_2} 为 G_2 的生成元.

③可计算性(Computable): 对于任意的 $a, b \in_R Z$, 有一个有效的算法来计算 $e(a \cdot g, b \cdot g) \in G_2$[4].

2.3 双线性 Diffie-Hellman 问题和决策双线性 Diffie-Hellman 问题

双线性 Diffie-Hellman(BDH)问题 设 G_1, G_2 是如上描述的循环群, e 也是如上描述的映射,给定 $(g, a \cdot g, b \cdot g, c \cdot g)$, $a, b, c \in_R Z_q$, 计算 $e(g, g)^{abc}$ 的值.

决策双线性 Diffie-Hellman(DBDH)问题 设 G_1, G_2 是如上描述的循环群, e 也是如上描述的映射,给定 $(g, a \cdot g, b \cdot g, c \cdot g, h)$, $a, b, c \in_R Z_q$, $h \in_R G_2$, 判断是否有 $h = e(g, g)^{abc}$.

显然,如果能够解决双线性 Diffie-Hellman(BDH)问题,那么决策双线性 Diffie-Hellman(DBDH)问题也就随之解决.

3 环签密算法的描述

我们利用 Weil Paring 构造的基于身份的环签密方案,简称为 IDRSC,由三个部分构成: 密钥的生成(key generation),签密(signcryption),解密和认证(unsigncryption).

3.1 密钥的生成(key generation)

令 G_1 是一个阶为素数的 q 加法群,设其产生元是 g, G_2 是一个阶为素数 q 的乘法群,这里的 $q \geqslant 2^t$, k 是本算法的安全参数. 设 $e: G_1 \times G_2 \to G_2$ 是如上描述的 Weil pairing,设 $H_1: \{0, 1\}^* \to Z_q$, $H_2: G_2 \to \{0, 1\}^l$, $H_3: \{0, 1\}^l = \{0, 1\}^l$ 是三个安全哈希函数,其中 l 表示待加密的明文的长度. M, C 分别表示明文空间和密文空间. 密钥中心选择 $s \in_R Z_q^*$, 计算 $P_{pub} = s \cdot g$, 密钥中心公布 $\{G_1, G_2, g, p, q, k, e, P_{pub}, H_1, H_2, H_3\}$, 对 s 保密.

对于一个身份信息为 ID_i 的用户 u_i, TKGC 通过下面的算法把 ID_i 映射到 G_1 上. 我们用 Q_{ID_i}, Q_{ID_i} 分别表示用户 u_i 的公钥和私钥.

MapToCurve:

①设 j = 0, 且 $I = \lceil \log_2 (1/\delta) \rceil$, 其中 δ 是一个可以接受的失败概率.

②如果 j > I, 退出. 否则, $x_i = h(j, ID_i) \pmod p$, 且 $a = x_i^3 + 1 \pmod p$.

③如果 $a^{(p-1)/2} = 1 \pmod p$, 那么 $y_i = \min\{\pm a^{(p+1)/4} \pmod p\}$, 输出 $Q_{ID_i} = 12(x_i, y_i)$, 算法成功结束.

否则, j = j + 1, 转②.

注: 因为 $p = 3 \pmod 4$, p 上的二次剩余 a 的平方根可以由③确定. 因为 a 是模 p 上的二次剩余的概率是 1/2, 所以 MapToCurve 算法错误退出的概率小于 δ. 另外, $Q_{ID_i} \in G_1$ 是因为 $qQ_{ID_i} = 12q(x_i, y_i) = o$.

通过 Q_{ID_i}, TKGC 可以计算 u_i 的私钥 $D_{ID_i} = sQ_{ID_i}$, 并且通过安全的信道传递给 u_i.

3.2 签密(signcryption)

若一个用户 u_s 希望代表整个群体 $U = \{u_1, u_2, \cdots, u_n\}$ 对消息 m 进行签密,密文的接收方的身份为 ID_B, 接收方的公钥为 Q_{ID_B}, 私钥为 D_{ID_B}. u_s 进行如下的操作:

(1)利用上面的 MapToCurve 算法, u_s 得到自己的公钥 Q_{ID_s} 和私钥 D_{ID_s}.

(2)选择 $a_0 \in_R Z_q^*$, $m_r \in_R M$. 计算 $R_0 = a_0 \cdot g$, $R'_0 = e(a_0 \cdot P_{pub}, Q_{ID_B})$, $k = H_2(R'_0)$, $c_1 = m_r \oplus k$, $c_2 = m \oplus H_3(m_r)$.

(3)对 $\forall i \neq s$, 选择 $a_i \in_R Z_q^*$, 计算 $A_i = a_i \cdot g$, $R_i = e(A_i, g)$, $h_i = H_1(U, m, k, R_i)$

(4)选择 $a_s \in_R Z_q^*$ 计算 $A_s = a_s \cdot g$, $R_s = e(A_s, g) \cdot e(-P_{pub}, \sum_{i \neq s} h_i \cdot Q_{ID_i})$ 如果 $R_s = e(g, g)$ 或 $R_s = R_i (i \neq s)$, 重新选择 a_s.

(5)计算 $h_s = H_1(U, m, k, R_s)$, $\sigma = h_s \cdot D_{ID_s} + \sum_{i=1}^{n} A_i$.

(6)定义消息 M 对应的密文 C = (U, c_1, c_2, σ, R_0, R_1, …, R_n, h_1, h_2, …, h_n), 并且把 C 发送给接收方.

3.3 解密和验证(unsigncryption)

接收方在收到密文 C = (U, c_1, c_2, σ, R_0, R_1, …, R_n, h_1, h_2, …, h_n)后,用自己的私钥进 D_{ID_B}行解密和认证:

(1)计算 $k' = H_2(e(R_0, D_{ID_B}))$, 恢复明文 $m'_r = c_1 \oplus k'$, $m' = c_2 \oplus H_3(m'_r)$.

(2)对于 $\forall i \in \{1, 2, \cdots, n\}$, 验证是否有 $h_i = H_1(U, m', k', R_i)$

(3)验证是否有 $e(\sigma, g) = R_1 \cdot R_2, \cdots, R_n \cdot e(P_{pub}, \sum_{i=1}^{n} h_i \cdot Q_{ID_i})$.

如果(2), (3)都成立, 则接收方认为密文 C 是有效的,否则认为C 在传输过程中遭到窜改.

4 算法的分析

4.1 算法的正确性和匿名性分析

如果密文 C 是按照上面的步骤产生的,并且在传播的过程中没有改变,那么有 $e(R_0, D_{ID_B}) = e(s \cdot a_0 \cdot g, Q_{D_B}) = e(a_0 \cdot P_{pub}, Q_{ID_B}) = R'_0$, 所以 $k' = H_2(e(R_0, D_{ID_B})) = k$, 显然 $m' = m$, $h_i = h'_i$. 那么 $R_1 \cdot R_2 \cdot \cdots \cdot R_n \cdot e(P_{pub}, \sum_{i=1}^{n} h_i \cdot Q_{ID_i}) = e(A_1, g) \cdot e(A_2, g) \cdot \cdots \cdot e(A_n, g) \cdot e(-P_{pub}, \sum_{i \neq s} h_i \cdot Q_{ID_i}) \cdot e(P_{pub}, \sum_{i=1}^{n} h_i \cdot Q_{ID_i}) = e(\sum_{i=1}^{n} A_i, g) \cdot e(P_{pub}, h_s \cdot Q_{ID_s}) = e(\sigma, g)$, 所以该算法的验证算法是有效的.另外, 该算法的匿名性是显然的, 由于该算法是完全对称的, 那么仅从密文来看, 任何一个用户是消息签密者的可能性是相等的均为 1/n.

4.2 密文的安全性

下面我们证明, 如果上的决策双线性 Diffie-Hellman 问题是难解的,那么我们的签密算法对文献[8]中所提出的自适应选择密文攻击是安全的.

定理 1 如果 A 是一个针对上述环签密方案(IDRSC)的自适应选择密文攻击者,并且攻击成功的概率为 ε, 那么存在算法 B 可以利用 A 来解决决策双线性 Diffie-Hellman问题 (DBDH)的一个实例.

证明: 设(g, ag, bg, cg, h)是 DBDH 问题的一个随机的实例,其中 a, b, $c \in_R Z_q$, $h \in_R G_2$. 我们证明如果 A 可以成功的攻击上述的环签密方案(IDRSC), 那么存在一个算法 B 可以利用 A 成功的判断出是否有 $h = e(g, g)^{abc}$.

我们用 B 模拟加密器, B 令 $P_{pub} = cg$, A 选择两个消息 m_0, m_1, 一个用户群体 U, 和一个身份为 ID 的消息接收方, A 向 B 发出签密请求, B 令 $Q_{ID} = bg$, $R_0 = ag$, $R'_0 = h$, 由于(g, ag, bg, cg, h)是随机选取的, 所以 A 不可能觉察这些变化. 随后 B 在{m_0, m_1}中随机选择一个 m_i, $i \in \{0, 1\}$, 按照 3.2中描述的步骤对消息 m_i 进行签密, 并且把密文 C 发送给 A. A 根据密文, 猜测出 i'. 若 $i' = i$(其概率为 ε), B 就认为 $h = e(g, g)^{abc}$, 因为利用 h, B 计算出的密文 C 使 A 相信其对应的明文为 m_i. 若 $i' \neq i$, B 就认为 $h \neq e(g, g)^{abc}$. 这样 B 就解决了 DBDH 问题的一个实例.

4.3 签名的安全性

本文提出的基于身份的环签密方案是建立在基于身份的环签名方案的基础上的文[3], 不难看出如果攻击者能够伪造出一个有效的密文, 那么他也能伪造出文献[3]中的签名算法对应的有效签名. 在文献[3]中已经证明如果群 G_1 上的 D-H 问题是难解的, 那么文献[3]中的签名算法是安全的. 所以如果群 G_1 上的 D-H 问题是难解的, 那么本算法中对应的签名也是安全的.

4.4 算法的分析

我们把该算法和其它的先签名后加密的算法进行比较, 这里签名的算法是文献[3]中提出的, 我们用 IDRS 表示. 加密算法是文献[6]中提出的, 我们用 BF 表示. 用 IDRSC 表示本文中提出的算法. 用 l 表示待加密的明文的长度, 用 $|G_1|$表示 G_1 一个点的长度, $|G_2|$表示 G_2 中一个点的长度, n 表示群体中用户的个数, |U |表示群体信息的长度. 通过下表列出的密文长度, 我们发现 IDRSC 的密文长度有了明显的降低, 大约降低了一半左右, 尤其适合在低带宽条件下更加可行.

表 1

算法	密文长度
IDRSC	$\|U\| + 2\|+ 2\|G_1\| + n\|G_2\| + nq$
IDRS and BF	$2 \cdot (\|U\| + \|G_1\| + n\|G_2\| + nq + l) + \|G_1\|$

5 结束语

本文首先提出了一种基于身份的环签密方案(IDRSC), 使消息的发送者能够以一种匿名的方式发送消息, 并且同时达到消息的保密性和认证性. 这样的环签密方案用于泄露秘密时, 不仅能为泄密者提供无条件匿名性, 而且还可以有效地保护所泄露的秘密的机密性, 使得非法的接受者无法获得秘密. 我们从理论上证明了新提出的环签密方案的安全性建立在决策双线性 Diffie-Hellman问题的难解性基础上. 和传统的先签名后加密的方法相比, 本方案的密文长度有了明显的降低, 在低带宽的条件下更加适用. 在实际应用中, 如果一个群体(组织, 公司, 军队等)中的某个人希望把秘密信息透露给其他人, 他可以采用本文中的 IDRSC 方案, 以一种匿名的方式发送秘密信息, 接收方可以恢复出秘密信息, 验证信息的完整性并且知道信息确实是由这个群体发出的, 但他却无法知道到底是谁发出的.

参考文献:

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption)[A]. Advances in Cryptology-Crypto'97,

LNCS 1294[C]. Berlin: Springer-Verlag, 1997. 165-179.
[2] Shamir A. Identity based cryptosystems and signature schemes[A]. Advances in Cryptology-Crypto′84, LNCS 196[C]. Berlin: Springer-Verlag, 1984. 47-53.
[3] Herranz Javier, Sáez Germán. A provable secure ID-based ring signature scheme[DB/OL]. Available at http://eprint.iacr.org/2003/261.
[4] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing[A]. Asiacrypt′01, LNCS 2248[C]. Berlin: Springer-Verlag, 2001. 514-532.
[5] Baek Joonsang, Zheng Yuliang. Identity-based threshold decryption[A]. PKC′04, LNCS 2947[C]. Berlin: Springer-Verlag, 2004. 262-276.
[6] Boneh D, Franklin M. Identity-based encryption from the weil pairing[A]. Crypto′01, LNCS 2139[C]. Berlin: Springer-Verlag, 2001. 213-229.
[7] Rivest R L, Shamir A, Tauman Y. How to leak a secret[A]. Asiacrypt′01, LNCS 2248[C]. Berlin: Springer-Verlag, 2001. 552-565.
[8] Baek Joonsang, Ron Steinfeld, Yuliang Zheng. Formal proofs for the security of signcryption[A]. PKC′02, LNCS 2274[C]. Berlin: Springer-Verlag, 2002. 80-98.

作者简介:

黄欣沂 男, 1981年出生于江苏仪征, 助教, 研究方向: 网络安全. E-mail: xinyinjnu@126.com.

张福泰 男, 1965生于陕西陇县, 教授, 博士, 主要研究方向: 信息安全及电子商务. E-mail: zhangfutai@njnu.edu.cn.