基于身份高安全性的签密方案①

陈 勤，朱春意，张 旻

(杭州电子科技大学 计算机学院，杭州 310017)

摘 要：前向安全性和公开验证性是签密算法的两个重要安全特性，如何设计同时满足这两个安全特性的签密算法一直以来都是签密研究的公开问题。根据张串绒等人在文献[1]中提出的签密方案的安全性缺陷，通过引入签密者秘密信息，提出了一个同时满足前向安全性、公开验证性以及 PKG 的不可诬陷性的新签密方案。同时，新方案在解签密过程中，签名验证通过后再进行解密密文，避免了恶意信息的攻击。

关键词：基于身份的签密；前向安全性；公开验证性；PKG 的不可诬陷性

ID-Based Signcryption with High Security

CHEN Qin, ZHU Chun-Yi, ZHANG Min

(College of Computer, Hangzhou Dianzi University, Hangzhou 310017, China)

Abstract: Forward security and public verifiability are two important security features of signcryption schemes. How to design schemes satisfying the two security features at the same time is a public problem in signcryption study. According to the security defect of the signcryption in the Reference [1] put forward by Zhang Chuanrong et al, a new signcryption scheme is proposed through the introduction of secret information of the signcryptioner in this paper, which satisfies with forward security, public verifiability and resistting the PKG to entrap at the same time. Simultaneously, the new scheme can avoid the attrack of the evil information throngh unsigncrying the ciphertext after the signature verification in the process of unsigncryption.

Keywords: identity-based signcryption; forward security; public verification; resistting the PKG to entrap

1 概述

签密[2]能够在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能，同时实现了消息传输的保密性和认证性，而其计算量和通信成本都远远低于传统的“先签名后加密算法[3]”因而是消息安全传输较为理想的方法。

签密虽然保证了消息传输的保密性和认证性，然而，如何设计同时满足前向安全性和公开验证性的签密方案一直以来都是签密研究的公开问题[4]。一方面，被签密消息在签名的同时也被加密，不能像一般签名那样被公开验证；另一方面，近年来，私钥的泄漏问题日益严重，一旦签密者私钥泄漏，任何得到签密者私钥的人都可以解签密签密者签密过的所有密文，从而获得消息明文。如何保证签密者私钥泄漏情况下签密密文的安全性即前向安全性是签密研究的难题。

文献[5]定义了一个新的安全模型，并在新模型下提出了一个满足前向安全性和公开验证性的签密方案，然而，该方案缺陷也很明显，如密文的无关联性和匿名性。文献[6]虽然也提出了同时满足前向安全性和公开验证性的签密方案，但是，该文所述方案需要两个私钥，一个用于签密，一个用于解签密。

文献[1]基于双线性对提出了一个适用于 AD-HOC 网络的签密方案，并在随机预言机模型下证明了所述方案的安全性。然而，经分析发现，该方案既不满足前向安全性，也不满足公开验证性，这就限制了该方案在实际中的应用。鉴于此，本文对该方案进行了改进，提出了一个安全性更高的签密方案。新方案不仅满足前向安全性和公开验证性，而且满足 PKG 的

① 收稿时间:2010-10-12;收到修改稿时间:2010-11-12

不可诬陷性。同时，新方案在解签密过程中，签名验证通过后再进行解密密文，避免了恶意信息的攻击。

2 预备知识

2.1 双线性映射

设 G_1 是一个阶为素数 q 的循环加法群，G_2 是一个阶为 q 的循环乘法群，P 是 G_1 的生成元。双线性映射[7]是指具有下列性质的映射 e：$G_1 \times G_1 \to G_2$ ：

(1)双线性。对所有的 P,Q$\in G_1$ 和 a,b$\in Z_q^*$，e(aP,bQ)=e(abP,Q)=e(P,Q)^{ab}

(2)非退化性。存在一个 P$\in G_1$，满足 e(P,P)$\neq 1$。

(3)可计算性。对 P,Q$\in G_1$，存在一个有效的算法计算 e(P,Q)。

在密码应用中，双线性映射可以从超奇异椭圆曲线中的 Weil 和 Tate 配对中得到,其计算可以用 Miller 算法[8]。

2.2 相关数学难题

G_1 是一个加法群，4 个相关困难问题如下：

(1) DLP(discrete logarithm problem)难题。P,Q$\in G_1$，求正整数 n$\in Z_q^*$，使之满足 Q=nP 是困难的。

(2) CDHP(computational Diffie-Hellman problem)难题。已知 P,aP,bP,计算 abP 是困难的，其中 a,b$\in Z_q^*$。

(3) DDHP(decision Diffie-Hellman problem)难题。已知 P,aP,bP,cP$\in G_1$，其中 a,b,c$\in Z_q^*$,要判定 c≡ab mod q 是否成立是困难的。

(4) 双线性配对求逆难题。即给出 P$\in$G 和 e(P,Q)$\in V$,找 Q$\in G$ 还不存在有效的算法。

3 文献[1]方案及其安全性分析

3.1 系统初始化

给定安全参数 k，PKG 首先选取椭圆曲线上的 2 个 q 阶的循环加法群G_1和循环乘法群G_2,P 为G_1的生成元，由G_1和G_2上的 Weil 对或 Tate 对的变形得到双线性变换记为 e：$G_1 \times G_1 \to G_2$ 。PKG 随机选取自己的私钥$\delta \in Z_q^*$，计算相应公钥$P_{pub}=\delta P$。PKG 再选取安全的对称密码算法(E,D)和 3 个散列函数 $H_1:\{0,1\}^{l_1} \to G_1$，$H_2:G_2 \to Z_q^*$，$H_3:\{0,1\}^{l_2} \times \{0,1\}^n \to Z_q^*$，其中$l_1$是身份$ID$的比特长度，$l_2$是$G_1$中元素的比特长度，$n$是明文比特长度。PKG 保密主密钥$\delta$，公布系统参数 $\{G_1,G_2,e,P,P_{pub},E,D,H_1,H_2,H_3\}$。

3.2 密钥生成

给定用户的身份ID_U，PKG 计算相应的公钥$Q_U=H_1(ID_U)$和私钥$S_U=\delta Q_U$;本算法中发送者 Alice 和接收者 Bob 的身份公私钥对分别记为(S_A,Q_A)和(S_B,Q_B)。

3.3 签密

假设 Alice 要将消息签密发送给 Bob，Alice 执行以下步骤：

(1) 随机选取 $x \in Z_q^*$，计算 $k_1=xQ_B$，$w=e(S_A,Q_B),k_2=H_2(w)$；

(2) 计算 $r=H_3(k_1,m),s=x/(r+S_A)$ 和 $t=E_{k_2}(s \| m) \in Z_q^*$。

Alice 生成的签密密文为$\sigma=(t,r)$，并通过安全通道发送给 Bob。

3.4 解签密

Bob 收到 Alice 的签密密文后，执行以下步骤：

(1) 计算$w=e(S_B,Q_A),k_2=H_2(w)$;

(2) 计算$s \| m=D_{k_2}(t)$;

(3) 计算$k_1=s(rQ_B+S_BQ_A)$，当且仅当等式$r=H_3(k_1,m)$成立时接受该密文σ。

关于该算法需要说明的是，S_A和S_B本来是G_1上的点，在计算签密中$s=x/(r+S_A)$和解签密中$k_1=s(rQ_B+S_BQ_A)$时需要先将它们转化成Z_q^*中的数。

3.5 安全性分析

对于原方案，在解签密过程中，有以下方程式成立：

$$e(S_B,Q_A)=e(S_A,Q_B)$$

Bob 可以用他的私钥S_B从方程左边计算出$w=e(S_B,Q_A)$。而当 Alice 的私钥S_A泄漏后，任何获得S_A的人都可以根据方程右边计算出$w=e(S_A,Q_B)$，进而计算出$k_2=H_2(w)$，解签密$s \| m=D_{k_2}(t)$获得明文m。不仅如此，知道签密者私钥的人还可以根据计算出来的 Alice 和 Bob 之间的长期会话私钥k_2，解签密他们之间以前通信的所有密文，获得明文消息。因此，该方案不具有前向安全性。

关于公开验证性，方案的验证式是$r=H_3(k_1,m)$，只有解密出明文消息m后才能验证，而m是私密信息，不能泄漏。因此，只有 Bob 才

能验证，原方案不具有公开验证性。

4 改进方案及其安全性分析

4.1 系统初始化

系统参数与原方案完全相同。

4.2 密钥生成

密钥生成过程如下：

(1) 用户 U 随机选择 $k_U \in Z_q^*$，计算并发送 $K_U = k_U P$ 给 PKG。

(2) PKG 计算用户公钥 $Q_U = H_1(ID_U, K_U)$，私钥 $S_U = \delta Q_U$，并通过安全通道发送给用户。

4.3 签密

假设 Alice 要将消息签密并发送给 Bob，Alice 执行以下步骤：

随机选取 $x \in Z_q^*$，并计算

$$k_1 = xk_A Q_B$$

$$k_2 = x^{-1} Q_A$$

$$w = e(S_A, Q_B)^{x^{-1}}$$

$$k_3 = H_2(w)$$

$$t_1 = E_{k_1}(m)$$

$$r = H_3(k_1, t_1)$$

$$s = xk_A/(r + S_A)$$

$$t = E_{k_3}(s \| t_1)$$

Alice 生成的签密密文为 $\sigma = (k_2, r, t)$，并通过安全通道发送给 Bob。

4.4 解签密

Bob 收到 Alice 的签密密文 σ 后，依次计算：

$$w = e(S_B, k_2)$$

$$k_3 = H_2(w)$$

$$s \| t_1 = D_{k_3}(t)$$

$$k_1 = s(rQ_B + S_B Q_A)$$

$$m = D_{k_1}(t_1)$$

当且仅当 $r = H_3(k_1, t_1)$ 时接受该密文。

关于签密中 $s = xk_A/(r + S_A)$ 和解签密中 $k_1 = s(rQ_B + S_B Q_A)$ 的计算方法见原方案的算法说明，如需深入了解，可参考文献[9]。

5 改进方案的安全性及效率分析

5.1 正确性

可以通过以下等式证明：

$$w = e(S_A, Q_B)^{x^{-1}} = e(\delta Q_A, Q_B)^{x^{-1}}$$

$$= e(Q_A, \delta Q_B)^{x^{-1}} = e(S_B, Q_A)^{x^{-1}}$$

$$= e(S_B, x^{-1} Q_A) = e(S_B, k_2)$$

$$k_1 = xk_A Q_B = s(r + S_A) Q_B$$

$$= srQ_B + s\delta Q_A Q_B$$

$$= s(rQ_B + S_B Q_A)$$

5.2 安全性

在随机预言机模型下，新方案的机密性与不可伪造性证明方法与原方案类似，详见文献[1]。下面着重证明下前向安全性、公开验证性和 PKG 的不可诬陷性。

5.2.1 前向安全性

新方案中，即使发送者的私钥意外泄漏，得到私钥的人由于不知道 x 的值无法求出 w 和 k_3，也就无法解签密密文。如果得到发送者私钥的人想要通过 $k_2 = x^{-1} Q_A$ 求出 x，必然遇到 DLP 难题。

5.2.2 公开验证性

新方案中，当遇到纠纷时，接收者只需将 k_1, t, r 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，新方案满足公开验证性。

5.2.3 PKG 的不可诬陷性

假设 PKG 按以下步骤伪造一个密文 σ'：

随机选取 $k_A' \in Z_q^*$ 代替 k_A，依次计算：

$$k_1' = xk_A' Q_B$$

$$k_2' = x^{-1} Q_A$$

$$w' = e(S_A, Q_B)^{x^{-1}}$$

$$k_3' = H_2(w')$$

$$t_1' = E_{k_1'}(m)$$

$$r' = H_3(k_1', t_1')$$

$$s' = xk_A'/(r' + S_A)$$

$$t' = E_{k_3}(s \| t_1')$$

至此，PKG 伪造的签密密文为 $\sigma' = (k_2', r', t')$。

下文将证明 PKG 伪造的签密密文跟真正的密文是可区分的。

对于真正的密文，有

$$e(k_1,k_2)=e(xk_AQ_B,x^{-1}Q_A)$$
$$=e(k_AQ_B,Q_A)=e(Q_B,Q_A)^{k_A}$$

而对于 PKG 伪造的密文，有

$$e(k_1',k_2')=e(xk_A'Q_B,x^{-1}Q_A)$$
$$=e(k_A'Q_B,Q_A)=e(Q_B,Q_A)^{k_A'}$$

因此，当 PKG 伪造了签密者的密文时，签密者可以通过出示其秘密信息来证明该密文是 PKG 伪造的。

6 结束语

新方案克服了原方案的安全缺陷，同时实现了前向安全性、公开验证性和 PKG 的不可诬陷性；并且，新方案在解签密过程中，签名验证通过后再进行解密，避免了恶意信息的攻击，安全性得到了显著的提高，实用性更强。

参考文献

1 张申绒,张玉清,李发根,肖鸿.适于 ad hoc 网络安全通信的新签密算法.通信学报,2010,31(3):19–24.

2 Zheng Y. Digital signcryption or how to achieve cost (Signature&Encryption)<<Cost(Signature)+Cost(Encryption) .In:Crypto'971 Berlin:Springer,1997.165–179.

3 Zheng Y. Signcryption and its applications in efficient public key solution.ISW'97, LNCS 1397, Springer-Verlag, 1998.

4 Shamir A. Identity-based cryptosystems and signature schemes.Advances in Cryptology-Crypto'84, LNCS 196, New York: Springer-Verlag, 1984.47–53.

5 Ibert LB, Isquater QJJ. A new identity based signcryption schemes from pairings. Proc of IEEE Information Theory Workshop. Springer-Verlag, 2003. 155–158.

6 Boyen X. Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography. Advances in Cryptology-CRYPT0 2003. Berlin: Springer-Verlag, 2003: 383–399.

7 Chow SSM, Yiu SM, Hui LCK, et al. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity Information Security and Cryptology-ICISC'03. Berlin: Springer-Verlag, 2004:352–369.

8 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. Advances in Cryptology-Crypro'2001, Berlin: Springer-Verlag,2001.213–229.

9 Miller V. Short Programs for Functions on Curves. [2009-02-23]. http://crypto.Stanford.edu/miller/miller.pdf

10 Zheng Y, Imai H. How to construct effcient signcryption schemes on elliptic curves. Information Processing Letters, 1998,68:227–233.

(上接第 81 页)

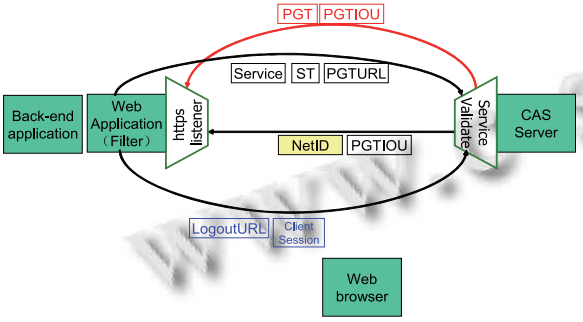

图 6 对 CAS 简单代理协议的修改

参考文献

1 Nakano H, Sugitani K, Nagai T, Kubota S, Migita, M, Musashi Y, Iriguchi N, Usagawa T, Kita T, Matsuba R. Web-based time schedule system for multiple LMSs on the SSO/portal environment. In: Education Engineering (EDUCON), 2010 IEEE. 153–158.

2 The Open Group. Single Sign-On. 1995-2010. http://www.opengroup.org/security/sso

3 JA-SIG Central Authentication Service. 2009. http://www.ja-sig.org/products/cas/

4 谭立球,费耀平,李建华.企业信息门户单点登录系统的实现.计算机工程,2005,31(17):102–104.

5 Petro A. CAS and JSR-168. 2007-02. http://www.ja-sig.org/wiki/display/CASC/CAS+and+JSR-168

6 Petro A. Proxy CAS Walkthrough. 2009-2. http://www.ja-sig.org/wiki/display/CAS/Proxy+CAS+Walkthrough

7 Turing D. 剖析 CAS Proxy 的设计原理. 2006-04. http://www.blogjava.net/security/archive/2006/04/26/sso_cas proxy.html