一种无信任权威的基于身份的签密方案①

杨长兴，李克强

(中南大学 信息科学与工程学院，长沙 410000)

摘 要：签密是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，其计算量和通信成本都远远低于传统的先签名后加密。分析现有的基于身份的签密方案，利用双线性对提出了一种新的无需可信任中心的基于身份的签密方案，并对该方案的安全性及效率进行了分析。分析表明，该方案满足签密的安全性要求并具有更高的效率。

关键词：基于身份；签密；双线性对；安全；效率

Identity-Based Signcryption Scheme Without Trust Authority

YANG Chang-Xing, LI Ke-Qiang

(Institute of Information Science and Engineering, Central South University, Changsha 410000, China)

Abstract: Signcryption is a cryptographic primitive that combines both the functions of digital signature and public key encryption in a logical single step, at lower computational costs and communication overheads than the traditional signature-then-encryption approach. This thesis analyzes the present identity-based signcryption scheme, and puts forward a new identity-based signcryption scheme without trust authority by using bilinear pairings. In addition, it also analyzes the safety and efficiency of this scheme. Analysis shows that this proposal meets the safety and high efficiency requirement of Signcryption.

Keywords: identity-based; signcryption; bilinear pairings; safety; efficiency

1 引言

在传统的公钥密码学中，使用公钥基础设施(Public Key Infrastructure，PKI)中的证书机构(Certification Authority，CA)颁发证书的形式来建立用户身份与其所拥有的公钥之间的联系，而且 CA 的数字签名可保证证书的真实性。然而证书的管理过程需要很多的计算开销和存储开销。为了简化证书机构的管理负担，1984 年 Shamir 在美洲密码年会上提出了一种新颖的公钥密码系统[1]，在这个系统中，用户的公钥是由与用户身份相关的比特串构成，而私钥则由信任权威机构生成。这个密码体制便是基于身份的密码体制，显然，这种体制消除了对用户证书的依赖，简化了密钥的管理过程。2001 年，Dan Boneh 和 Matt Franklin 利用 weil 配对提出了第一个基于身份的加密系统[2]。

签密这一概念最早是由 Zheng 于 1997 年提出[3]，签密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，其计算量和通信成本都远远低于传统的先签名后加密。

目前，基于身份的签密体制已成为一个研究热点，出现了大量的基于双线性映射[4]的签密方案。Malone-Lee 提出了一种基于身份的签密方案[5]，但该方案被证明不是语义安全的，而且无法防止信任权威机构（Trust Authority，TA）或私钥产生中心（Private Key Generator，PKG）伪造签名。

如何防止 TA 或 PKG 任意伪造签名，成为了现今研究的一个难题。在扩展的 Boneh 与 Franklin 公钥加密体制中[6]，引入了两个 TA，在该体制中，只有两个 TA 合谋，才能伪造签名。依照这一方案的思维，李沛等人在文献[7]中引入了 n（n>=2）个 TA，极大的提高

① 收稿时间:2010-07-21;收到修改稿时间:2010-08-20

了签名的安全性。但是签名仍然有被伪造的可能，因为谁也无法保证所有的 TA 都是诚实的，并且加大了通信量和计算量。Chen 等人提出了一中无需可信任 PKG 的签名方案[8]，但是该方案需要四次对运算，效率太低。

本文在现有的研究基础上，提出了一种无可信任中心的基于身份的签密方案，该方案利用椭圆曲线上的双线性对，实现了机密性以及签名的不可伪造性、不可否认性，而且具有较高的效率。

2 预备知识

设 G_1 为一 q（q 为素数）阶加法循环群，G_2 为一 q 阶乘法循环群，双线性映射 e：$G_1\times G_1\rightarrow G_2$ 为满足下列性质的映射：

(1) 双线性：令 P、Q、R 为 G_1 的生成元，a、b $\in Z_q^*$，则有：

$e(P+Q，R)=e(P，R)e(Q，R)$

$e(aP，bQ)=e(abP，Q)=e(P，abQ)=e(P，Q)^{ab}=e(aP，Q)^b=e(P，bQ)^a$

$e(P，Q+R)=e(P，Q)e(P，R)$

(2) 非退化性：存在 P、$Q\in G_1$ 使得 $e(P，Q)\neq 1$。

(3) 可计算性：存在一个高效的算法计算 e(P，Q)，P、$Q\in G_1$。

下面介绍本文用到的与双线性配对相关的数学问题：

离散对数问题(DLP)：设 P 和 Q 是群 G 中的两个元素，找到一个 $n\in Z_q^*$ 使 P=nQ 是困难的。

本文方案即是基于 DLP 问题求解的困难性。

3 一种基于身份的签密方案

本方案由三部分组成，公共参数生成器(Public Parameter Generator，PPG)、签密者 Alice、接收方 Bob。

其中，PPG 可以由 PC、路由器、防火墙或是安全网关设备担任。但是，为了防止不法分子伪装成 PPG，胡乱发布参数，干扰系统的正常运行，PPG 还需具有权威性，它的权威在于在某一信任域中，用户只认定其发布的公共参数，而拒绝按其它设备产生的参数生成密钥。

一般来说，公共参数生成器可以由 PKG 或是 TA 担任，只是它只负责参数的生成，而不生成主密钥，密钥的生成由用户自己完成。

3.1 系统初始化

PPG 选取以大素数 q 为阶的加法群 G_1 和乘法群 G_2，双线性映射 e：$G_1\times G_1\rightarrow G_2$，以及 G_1 的生成元 P，再选取三个哈希函数 H1：{0，1} $^*\times G_1\rightarrow G_1$，$H_2$：$G_2\rightarrow$ {0，1} n，H_3：{0，1} $n\times G_1\rightarrow Z_q^*$。公开参数$<G_1，G_2，P，e，q，H_1，H_2，H_3>$。

3.2 密钥对生成

设 ID 为信任域内某成员的唯一标识，用户随机选择 $r_{ID}\in Z_q^*$，计算其公钥 $Q_{ID}=H_1（ID，r_{ID}P）$，其私钥 $S_{ID}=r_{ID}Q_{ID}$，该用户在信任域内公布 $r_{ID}P$。本方案中，Alice 的密钥对为（Q_A，S_A），对应的 $r_{ID}P$ 为 r_AP；Bob 的密钥对为（Q_B，S_B），对应的 $r_{ID}P$ 为 r_BP。

3.3 签密方案

设 m 为待发送消息，Alice 获取 r_BP 并执行以下步骤：

1）选取随机数 $k\in Z_q^*$ ；

2）计算 $Q_B=H_1（ID_B，r_BP）$，$r=H_3（r_AP，m）$，$y=e（Q_B，k^{-1}r_BP）$，$K=H_2（y）$，$U=k^{-1}P$（k^{-1} 为 k 在 Z_q^*中的逆）；

3）计算密文 $C=K\oplus m$；

4）计算签名 $V=krS_A$；

5）Alice 将（U，C，V）作为密文发送给 Bob。

3.4 解密并验证签名

Bob 收到密文（U，C，V）后，获取 r_AP 并按以下步骤对该密文进行解密及验证签名：

1）解密：计算 $y=e（S_B，U）$，$K=H_2（y）$，$m=C\oplus K$，这是因为：

$e（S_B，U）=e（r_BQ_B，k^{-1}P）=e（Q_B，k^{-1}r_BP）$

2）验证签名：计算 $r=H_3（r_AP$ ，m），$Q_A=H_1（ID_A，r_AP）$，验证 $e（V，U）=e（Q_A，r_AP）r$ 是否成立，如果成立则可判断该消息是 A 发的；否则拒收，这是因为：

$e（V，U）=e（krS_A，k^{-1}P）=e（r_AQ_A，P）r=e（Q_A，r_AP）r$

4 安全性分析

(1) 该方案满足机密性。除接受者 Bob 外，任何人无法对 C 进行解密。要对 C 解密，需要计算 y，而除了 Bob 自己以外，任何人都不知道他的私钥 S_B，而要获得 Bob 的私钥，必须获得 r_B，由 DLP 求解的困难性可知，从 r_BP 中获得 r_B 是不可行的。

(2) 该方案满足公开验证性。若对 Alice 的签名产生了纠纷，只需将<U，V，r>发送给第三方仲裁者，验证者即可验证 e（V，U）=e（Q_A，r_AP）r 是否成立。由于 Q_A 可由 rAP 计算得到，而 r_AP 是公开的，r 为已知，因此可实现机密性基础上的公开验证。

(3) 该方案满足不可伪造性。本方案中，只有 Alice 本人知道自己的私钥，攻击者无法对其签名进行伪造。若攻击者要伪造 Alice 的签名，必须伪造 r_A'，计算 $S_A' = r_A' Q_A$，再伪造 k'，计算 $V' = k' rS_A'$，$U' = k'^{-1}P$，伪造签名即为<V'，U'>。接受者接到改签名进行验证 e（V'，U'）=e（Q_A，r_AP）r 是否成立，由于 S_A' 中的 r_A' 是伪造的，故 $r_A' P \neq r_AP$，因此该验证不会被通过，攻击者伪造签名无效。

(4) 该方案具有不可否认性。由于该方案具有不可伪造性，B 只需验证 e（V，U）=e（Q_A，r_AP）^{r}成立，A 无法否认曾经发送过这个消息，因为 e（V，U）=e（krS_A，k-1P）=e（r_AQ_A，P）^{r}= e（Q_A，r_AP）^{r}。

(5) 该方案满足前向安全性。假如 Alice 的密钥不小心泄漏，攻击者仍然不能恢复 Alice 过去所签密的消息。因为攻击者不知道 S_B，无法计算 y=e（S_B，U），因此，该方案满足前向安全性。

5 效率分析

一般认为，签名方案中最耗时的运算为对运算（记为 pair），指数运算（记为 exp），点乘运算（记为 mul），pair 运算次数 x+(y)表示 x 次对运算，y 次对预运算。将本文方案与几种典型的签密方案进行比较，比较结果如表 1 所示。由表 1 可知，本方案的密文长度与文献[5]及文献[9]方案的密文长度一致，但是拥有更高的效率。

表 1 本文方案与其他方案的比较结果

方案	签密			验证			密文长度
	mul	exp	pair	mul	exp	pair	
文献[5]	3	0	0+(1)	0	1	3+(1)	$\|2G_1\|+\|m\|$
文献[8]	3	0	0	1	0	4	$\|6G_1\|$
文献[9]	4	1	0+(1)	2	0	2+(2)	$\|2G_1\|+\|m\|$
本文方案	4	0	0+(1)	0	1	2+(1)	$\|2G_1\|+\|m\|$

5 结束语

本文提出了一种无可信任中心的基于身份的签密方案，由于本文方案无可信任中心，因此不存在 PKG 伪造签名的问题。本文对该方案进行了安全性及效率分析，在 DLP 问题求解困难性的假设下，该方案被证明是安全的并且具有更高的效率。

参考文献

1 Shamir A. Identity-based cryptosystems and signatures chemes. Advances in Cryptology-Crypto'84, LNCS 196, NewYork:Springer-Verlag, 1984: 47−53.

2 Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing.Kilian J.Advances in Cryptology-Crypto 2001. Berlin, Heidelberg: Springer-Verlag, 2001: 213−229.

3 Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). Proceedings of the CRYPTO 1997, California, USA, 1997: 165−179.

4 Mambo M, Usuda K, Okamoto E. Proxy signatures: delegation of the power to sign messages. IEICE Transaction Fundament,1996,E79-A (9):1338−1354.

5 Malone-Lee J. Identity Based Signcryption. http://eprint.iacr.org/2002/098.

6 徐茂智,游林.信息安全与密码学.北京:清华大学出版社,2007.178−197.

7 李沛,王天芹,潘美姬.基于身份的签名方案.计算机工程与应用,2008,44(14):103−106.

8 Chen X, Zhang F, Kim K. A new ID-based group signatrue scheme from bilinear pairings. Proc. of WISA'03, LNCS 2908. Berlin: Springer-Verlag, 2003: 585−592.

9 李发根,胡予濮,李刚.一个高效的基于身份的签密方案.计算机学报,2006,29(9):1641−1647.