* 1

基于身份的前向安全和可公开验证签密方案

张串绒[1,2]，　张玉清[2]
(1. 空军工程大学　电讯工程学院，陕西　西安　710077；2 中科院　研究生院，北京　100049)

摘　要：针对具有前向安全性和可公开验证的签密方案进行研究，基于 Liber 和 Quisquater 的签密方案，给出了一个新的签密方案，并对所提出方案的安全性和效率进行了分析。结果表明：文章给出的签密方案实现了同时提供前向安全性和可公开验证性；而基于身份公钥密码和双线性对技术，使该方案又具有密钥长度短和密钥管理简单的特点，使其具有与 LQ 签密方案相当的效率。这种高效性和高安全性签密方案的提出，不仅对相关公开问题的解决具有一定理论意义，同时文中签密方案能更好的满足电子商务等实际应用的高安全需求，因此也具有一定应用价值。

关键词：签密；前向安全性；可公开验证性；基于身份的公钥密码；双线性对
DOI：10. 3969/j. issn. 1009 - 3516. 2009. 03. 017
中图分类号：TN918. 1　　**文献标识码**：A　**文章编号**：1009 - 3516(2009)03 - 0078 - 04

可公开验证性和前向安全性作为 2 个重要的密码性质，在许多实际应用中是需要满足的。一直以来，设计具有这 2 个密码性质的签密方案是签密研究的一个公开问题，受到广泛的关注。文献[1 - 4]针对该问题进行了研究，但其中的实现方案都是基于传统公钥密码体制的。2002 年 Malone - Lee 提出基于身份的签密，签密的这一公开问题的研究在身份密码领域取得了重大进展，一个重要成果是 2003 年 Liber 和 Quisquate 提出 2 个高效语意安全的基于身份的签密方案[5]，简称 LQ 签密方案，其中一个是可以公开验证的，简称 P - LQ 签密方案，另一个是具有前向安全性的，简称 F - LQ 签密方案。这 2 个方案在研究具有可公开验证和前向安全性的签密中作出了重要贡献，但问题是所提出的这 2 个方案，要么只提供前向安全性，要么只提供可公开验证性，不能同时提供这 2 种安全性，因此不能满足实际中同时需要这 2 个性质的应用环境。为此，基于 LQ 的签密方案，本文给出了同时具备可公开验证和前向安全性的签密方案，简称 P - F IDSC，并对其安全性和效率分别进行了分析和证明。

1　相关基础

1.1　基于身份的公钥密码和双线性对

基于身份的公钥密码(ID - based Public Key Cryptosystem)是 Shamir 于 1984 年提出来的[6]，它的最大特点是可以用任意比特串的用户身份信息作为用户的公钥。利用基于身份的公钥密码进行通信，不需要交换公钥证书，不必保存公钥证书列表，也不必使用在线的第 3 方，避免了用证书对公钥进行认证的管理模式。Shamir 在提出基于身份密码系统概念的同时就给出了一种基于身份的签名方案，随后有许多基于身份的签名方案被提出来，2001 年 Boneh 和 Franklin 基于椭圆曲线上双线性对给出了第一个基于身份的加密方案。

所谓双线性对是一种变换，定义如下：

* **收稿日期**：2008 - 11 - 12
基金项目：国家自然科学基金资助项目(60873233)；中国博士后科学基金资助项目(20080440550)；陕西省科技攻关基金资助项目(2008 - k04 - 21)；西安市产学研合作基金资助项目(CXY08016)；国家“863”高科技计划资助项目(2007AA01Z427)
作者简介：张串绒(1965 -)，女，陕西眉县人，副教授，博士(后)，主要从事密码学与网络安全研究；
E - mail：crzhang369@163. com
张玉清(1966 -)，男，陕西宝鸡人，教授，主要从事密码学与网络攻防研究.

定义　设 G_1,G_2 是 2 个 q 阶的循环群,如果变换 e 满足条件:

1) 双线性:对任意 $P_1,P_2,Q\in G_1$ 有 $e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$;

对任意 $P,Q_1,Q_2\in G_1$ 有 $e(P,Q_1+Q_2,)=e(P,Q_1)e(P,Q_2)$;

2) 非退化性:存在 $P\in G_1$,使 $e(P,P)\neq 1$;

3) 可计算性:对所有的 $P_1,P_2\in G_1$,存在有效的算法计算 $e(P_1,P_2)$,则称 e 是双线性对,又称双线性变换。

双线性对具有双线性性,即 $e(P,aQ)=e(aP,Q)=e(P,Q)^a$,使得 a 可以在双线性对作用的 2 个变量之间自由转换,给构造各类密码体制带来了很大的方便。双线性对目前能通过对椭圆曲线或超椭圆曲线中的 Weil 对或 Tate 对的变形得到,具体方法见文献[7]。目前,椭圆曲线上双线性 Weil 对和 Tate 对已经成为设计基于身份密码体制的重要工具。

1.2　基于身份和双线性对的签密

第一个提出基于身份签密的是 Malone - Lee,他给出了一种基于身份的签密方案[8],随后,有许多基于身份的签密方案被提出来。

基于身份签密方案包括以下过程,其中 ID_a 和 ID_b 分别是消息发送者 Alice 和接收者 Bob 的身份信息,(Q_a,d_a)和(Q_b,d_b)分别是他们的公钥对。

1)系统建立:给定系统安全参数 k,由密钥生成中心 PKG 生成系统参数;

2)密钥提取:对给出的用户身份 ID,由 PKG 生成与之相应的用户公私钥对(Q_a,d_a)和(Q_b,d_b);

3)签密算法:输入 d_a,ID_b 和消息 m,生成密文 σ;

4)解签密算法:输入 d_b,ID_a 和 σ,输出 m 或 $\perp$,$\perp$ 表示 σ 为无效签密密文;

目前,已有基于身份的签密方案都是利用椭圆曲线上的双线性对,即 Weil 对或改进的 Tate 对实现的,这种基于椭圆曲线密码上双线性对的签密方案,具有更小的密钥长度、更小的带宽要求和更快的实现速度。

2　LQ 签密方案

2.1　可公开验证的 LQ 签密方案 P - LQ

系统建立和密钥生成:给定安全参数, PKG 首先选取 2 个 q 阶的循环群$(G_1,+)$和$(G_2,\cdot)$, G_1 的生成元为 P,G_1 和 G_2 上的双线性变换为 $e:G_1\times G_1\rightarrow G_2$。PKG 随机选取自己的私钥 $\delta\in Z_q^*$,计算相应公钥 $P_{pub}=\delta P\in G_1$。PKG 再选取安全的对称密码算法(E,D)和 Hash 函数 $H_1:\{0,1\}^*\rightarrow G_1$,$H_2:G_2\rightarrow\{0,1\}^n$ 和 $H_3:\{0,1\}^*\times G_2\rightarrow Z_q$,其中 n 是明文长度。这样,该方案的系统参数是$(G_1,G_2,n,e,P,P_{pub},E,D,H_1,H_2,H_3)$。关于密钥生成,给出用户的身份 ID_u,PKG 计算相应的公钥 $Q_u=H_0(ID_u)$和私钥 $d_u=\delta Q_u$;本方案中发送者 Alice 和接收者 Bob 的基于身份的密钥对分别记为(Q_a,d_a)和(Q_b,d_b)。

假定 Alice 要将通过签密的消息 m 发送给 Bob,下面是签密和解签密过程。

Alice 签密:

1)计算 $Q_b=H_1(ID_b)$;

2)随机选取 $x\in_R Z_q^*$,计算 $k_1=e(P,P_{pub})^x$,　$k_2=H(e(P_{pub},Q_b)^x)$;

3)计算 $c=E_{k_2}(m)$,$r=H_3(c,k_1)$,$s=xP_{pub}-rd_a$。

Alice 发送密文 $\sigma=(c,r,s)$给 Bob,Bob 收到密文 σ 后执行下面的解签密:

Bob 解签密:

1)计算 $Q_a=H_1(ID_a)$;

$k_1=e(P,s)e(P_{pub},Q_b)^r$,$t=e(s,Q_b)e(Q_b,d_b)^r$,$k_2=H_2(t)$;

2)计算 $m=D_{k_2}(c)$;

3)验证 $r=H_3(c,k_1)$是否成立,成立则输出 m,否则输出 $\perp$。

P - LQ 方案是可公开验证的签密方案,当需要验证时,Bob 将(c,r,k_1)给出,任何第 3 方都可通过 $r=H_3(c,k_1)$对签密的有效性进行验证。

2.2　前向安全的 LQ 签密方案 F - LQ

系统参数和收发方的密钥对与 P - LQ 方案相同,以下是 F - LQ 方案的签密和解签密过程。

Alice 签密:

1)计算 $Q_b = H_1(\mathrm{ID}_b)$;

2)随机选取 $x \in_R Z_q^*$,计算$(k_1, k_2) = H_2(e(P_{\mathrm{pub}}, Q_b)^x)$;

3)计算 $c = E_{k_2}(m)$,$r = H_3(c, k_1)$,$s = xP_{\mathrm{pub}} - rd_a$,$R = rQ_a$。

Alice 发送密文 $\sigma = (c, R, s)$给 Bob,Bob 收到密文 σ 后执行下面的解签密;

Bob 解签密:

1)计算 $Q_a = H_1(\mathrm{ID}_a)$;

$(k_1, k_2) = H_2(e(s, Q_b)e(R, d_b))$

2)计算 $m = D_{k_2}(c)$,$r = H_3(c, k_1)$;

3)验证 $R = rQ_a$ 是否成立,成立则输出 m,否则,输出 $\perp$。

F-LQ 签密方案是具有前向安全性的,因为除了 Bob 以外,其它任何人即使知道 Alice 的私钥 d_a,由于不知道 r,都不能解密出消息 m。

3 基于身份的签密方案 P-FIDSC

该方案的系统建立和密钥生成与 LQ 签密方案的基本相同,不同之处是,P-FIDSC 方案的系统参数是 $(G_1, G_2, n, e, P, P_{\mathrm{pub}}, E, D, H_1, H_2, H_3, H_4)$,其中 Hash 函数 $H_1: \{0,1\}^* \to G_1$,$H_2: G_2 \to \{0,1\}^n$,$H_3: G_2 \to \{0,1\}^n$ 和 $H_4: \{0,1\}^* \times G_2 \to Z_q$。

Alice 签密:

1)计算 $Q_b = H_1(\mathrm{ID}_b)$;

2)随机选取 $x \in_R Z_q^*$,计算 $k = e(P_{\mathrm{pub}}, Q_b)^x$,$k_1 = H_2(k)$,$k_2 = H_3(k)$;

3)计算 $c = E_{k_1}(m)$,$r = H_4(c, k_2)$,$s = xP_{\mathrm{pub}} - rd_a$,$R = rQ_a$。

Alice 发送密文 $\sigma = (c, R, s)$给 Bob,Bob 收到密文 σ 后执行下面的解签密过程。

Bob 解签密:

1)计算 $Q_a = H_1(\mathrm{ID}_a)$,$k = e(s, Q_b)e(R, d_b)$,$k_1 = H_2(k)$,$k_2 = H_3(k)$;

2)验证 $R = H_4(c, k_2)Q_a$ 是否成立,不成立输出 $\perp$,成立则执行下一步;

3)计算 $m = D_{k_1}(c)$,并输出 m。

P-FIDSC 方案的正确性证明如下:

$e(s, Q_b)e(R, d_b) = e(s, Q_b)e(rQ_a, \delta Q_b) = e(s, Q_b)e(r\delta Q_a, Q_b) = e(s, Q_b)e(rd_a, Q_b) = e(s + rd_a, Q_b) = e(xP_{\mathrm{pub}}, Q_b) = e(P_{\mathrm{pub}}, Q_b)^x = k$

4 P-FIDSC 方案的安全性和效率分析

4.1 P-FIDSC 方案的安全性

P-FIDSC 方案的机密性和不可伪造性的证明与 LQ 签密方案的类似,限于篇幅,证明过程不再叙述。下面着重分析其可公开验证和前向安全性。

在 P-FIDSC 方案中,当需要对签密进行公开验证时,Bob 将(c, R, k_2)给出,任何第 3 方都可通过 $R = H_4(c, k_2)Q_a$对签密的有效性进行验证,而这种验证不泄露消息 m,也不需要 Bob 的私钥等秘密信息,从而实现了签密的公开验证. 这里特别要说明的是,这里的公开验证不像文献[1]等那样是对签名的公开验证,而是真正的对签密的公开验证,因为它不需要提供秘密消息 m 及任何机密信息。

在 P-FIDSC 方案中,下面的等式成立:$e(s + rd_a, Q_b) = e(s, Q_b)e(R, d_b)$。

Alice 利用等式左边计算出 k,Bob 由等式右边计算出 k。任何得知 Alice 的私钥 d_a 的人,由于不知道 r,所以不能从等式左边计算出 k,也就不能解密出消息 m,因此,该方案关于发送者的私钥具有前向安全性。

从上可见,P-FIDSC 方案同时具有和 F-LQ 签密方案一样的前向安全性,及与 P-LQ 签密方案一样的可公开验证性。另外,该方案在解签密中,还采取了先验证,验证通过后再解密消息的方法,这样能更好的保护接收者免遭恶意信息的攻击。

4.2 关于 P-F IDSC 方案的效率

首先, P－FIDSC 方案是基于身份和椭圆曲线上双线性对的签密方案,与已有文献[1－4]中的基于传统公钥密码的具有前向安全性或可公开验证的签密方案相比,基于身份和双线性对的签密方案,使得用户系统的管理开销和计算复杂度得到降低,并且具密钥长度短、带宽要求低和实现速度快的特点,从而提高了方案的效率。其次,将 P－FIDSC 方案与 LQ 签密方案进行比较,从计算量上看,与 P－LQ 签密方案相比,P－FIDSC 方案少了一个双线性对的运算,与 F－LQ 签密方案相比,它是用一个 Hash 运算代替了 F－LQ 签密方案一个密钥的分拆过程;而其传输量与 F－LQ 签密方案的相等。可见,本文给出的 P－FIDSC 方案有着与 LQ 签密方案相当的效率优势。

5　结束语

本文在文献[5]中签密方案的基础上给出了一个新的签密方案,该方案在满足签密一般安全性的前提下能同时提供前向安全性和可公开验证性这 2 个密码性质;从效率方面看,算法本身计算和传输代价是与文献[5]的签密方案相当的,而与基于传统公钥的相关结果相比,基于身份和双线性对,使其又具有短的密钥和管理简单的特点。因此,本文给出的方案是一个高效的具有良好密码性质的签密方案。

参考文献:

[1] Bao F, Deng R H. A Signcryption Scheme with Signature Directly Verifiable by Public key[C]//Proc of PKC'98, LNCS 1431. Berlin:Springer, 1998: 55－59.

[2] Jung H Y, Chang K S, Lee D H. Signcryption Schemes with Forward Secrecy[C]//Proceeding of WISA. Korea:[s. n.]2001: 403－475.

[3] Jung H Y, Lee D H, Lim J I, et al. Chang, Signcryption Schemes with Forward Secrecy. [C/OL] Proc. of WISA'01, (2001－04－02)[2005－12－08]http://cist. korea. ac. kr/Tr/TR016.

[4] Shin Jun－Bum, Lee Kwangsu, Shim Kyungah. New DSA－verifiable Signcryption Schemes[C]//Information Security and Cryptology－ICISC 2002, 5th International Conference. Berlin:Springer Verlag,2002: 28－29.

[5] Libert B, Quisquater J J. New Identity－based Signcryption Schemes from Pairings [C]//IEEE Information Theory Workshop. Berlin:Springer Verlag,2003:155－158.

[6] Shamir A. Identity Based Cryptosystems and Signature Schemes[C]//Cryptology－Crypto' 84, LNCS 0196. Berlin:Springer Verlag,1984:47－53.

[7] Menezes A J. Elliptic Curve Public Key Cryptosystems[M]. Kluwer Academic Publishers, 1993.

[8] J Malone－Lee. Identity Based Signcryption[Eb/OL]. [2004－05－12]http://eprint. iacr. org/2002/098/.

(编辑:徐楠楠)

Identity Based Signcryptin Scheme with Forward Security and Public Verifiability

ZHANG Chuan－rong[1,2], ZHANG Yu－qing[2]

(1. Telecommunication Engineering Institute, Air force Engineering University, Xi'an 710077, China; 2. Graduate University of Chinese Academy of Science, Beijing 100049, China)

Abstract: In this paper, by conducting an investigation in signcryption schemes with forward security and public verifiability and based on Liber and Quisquaters signcryption schemes, a new signcryption scheme is proposed, and its security and efficiency are analyzed at the same time. The result shows that the new signcryption scheme proposed can provide forward security and public verifiability simultaneously; moreover, it has the property of shorter length of parameter key and simple management is simple compared with the traditional PKI owing to the use of Id－based PKC and bilinear pairing technique in the scheme; therefore, it has the same efficiency with the LQ signcryption scheme. This work of giving such an efficient and secure signcryption scheme is not only significant in theory in solving the related public problem but also has practical value for the high level requirement of practical application such as the electronic business.

Key words: signcryption; forward security; public verifiability; ID－based PKC; bilinear pairing