一个安全的无证书签密方案*

刘志远
(湖北理工学院 计算机学院, 湖北 黄石 435003)

摘 要: 无证书的密码体制不但消除了传统公钥密码体制中的证书管理问题,而且解决了基于身份密码体制中的密钥泄露问题。基于张磊等人的签名方案,构造了一个安全的无证书签密方案。方案的安全性分析表明,在 DL 和 CDH 问题困难性假设下,能够抵抗适应性选择消息攻击下的存在性伪造。

关键词: 无证书密码系统; 无证书签密; 双线性对; 离散对数问题; 计算 Diffie-Hellman 问题
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)05-1533-03
doi:10.3969/j.issn.1001-3695.2013.05.065

Secure certificateless signcryption scheme

LIU Zhi-yuan
(*College of Computer Science*, *Hubei Polytechnic University*, *Huangshi Hubei* 435003, *China*)

Abstract: Certificateless cryptography not only overcomes the certificate management problems in the traditional public key cryptosystems, but also solves the key escrow problems in identity-based cryptosystems. This paper presented a secure Certificateless signcryption scheme from pairings based on Zhang Lei et al.'s signature scheme. A security analysis proves that the proposed scheme is secure against existential forgery on an adaptively chosen message attack under the assumption of DL and CDH problems.

Key words: certificateless public key cryptography; certificateless signcryption; bilinear pairing; discrete logarithm problem (DLP); computational Diffie-Hellman problem

0 引言

1976 年,Diffie 等人[1]提出了公钥密码体制,用户公钥的认证方式通常有传统公钥体制、基于身份公钥体制和无证书公钥体制三种。传统公钥体制都离不开 PKI 的支持,用户公私钥可以由用户自己选取,用户在使用任何公钥前都需要先验证公钥证书的合法性,增加了用户的计算量;同时,在实际应用中证书的产生、管理、传输、验证等过程不仅复杂而且代价很高。基于身份公钥体制由 Shamir[2]于 1984 年首次提出。在基于身份的密码体制中,用户的公钥可以根据用户的身份信息(如姓名、身份证号码、电话号码、e-mail 地址等)直接计算出来,用户的私钥则是由一个称为私钥生成中心(PKG)的可信方生成。由于 PKG 知道所有用户的私钥,因此将不可避免地会引起密钥托管问题(即 PKG 可解密用户的密文或伪造用户的签名),并且不能被发现。为了解决基于身份的密码系统中的密钥托管问题,2003 年 Al-Riyami 等人[3]提出了无证书公钥密码学概念。在无证书密码体制中,由可信密钥生成中心生成用户的部分私钥和部分公钥;同时,用户选择一个秘密值和部分私钥相结合,生成自己独立的私钥和公钥。这样,它既消除了基于传统公钥基础设施中公钥证书的管理复杂性问题,同时也克服基于身份密码学中用户密钥托管问题。

签密的概念于 1997 年由 Zheng[4]提出。签密在计算量和通信成本上都要低于传统的先签名后加密方式,是信息安全中的一个重要工具,它提供了保密性、不可否认性、不可伪造性等安全服务。随着签密技术的发展,2008 年,第一个无证书签密方案由 Barbosa 等人[5]给出。该方案使用的是先加密后签名方式,但它并不能抗扩展不可伪造攻击。随后一些可证明安全的无证书签密方案[6~9]被学者们陆续提出,但是这些方案都存在着不同程度的安全弱点。例如文献[6]在签密时不能提供认证性和保密性,文献[7]在签密时不能提供保密性,具体的攻击方法在文献[8]中对文献[6,7]的不安全特性都给出了具体的证明。2009 年,Li 等人[9]提出了第一个在随机预言机模型下可证明安全的无证书签密方案,并在随机预言机模型下证明了其安全性。Li 等人的方案唯一不足的是对第 1 类攻击者并不能满足机密性。

2010 年,张磊等人[10]给出了一类无证书签名方案的构造方法。基于这种方法,本文构造了一个安全的基于双线性对的无证书签密方案。在 DL 和 CDH 问题困难性假设下,本文方案能够抵抗适应性选择消息攻击下的存在性伪造。

1 预备知识

1.1 双线性对

设 G_1 是由 P 生成的加法循环群,阶为素数 q。G_2 是一个乘法循环群,阶也是 q。双线性映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 的性质为:

a)双线性性。如果对所有的 $P, Q \in G_1$, $a, b \in Z_q^*$,都有 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$。

收稿日期: 2012-08-17; **修回日期**: 2012-09-29 **基金项目**: 湖北省自然科学基金资助项目(2011CDC063);湖北省教育厅重点项目(D20114401)

作者简介:刘志远(1972-),男,湖北鄂州人,副教授,博士,主要研究方向为无线网络安全(shengdiwl@163.com).

b)非退化性。存在 $P,Q\in G_1$. 使得$\hat{e}(P,Q)\neq 1$。

(3)可计算性。有一个多项式时间算法来计算$\hat{e}(P,Q)$。

1.2 困难性假设

a)离散对数问题(DLP)。给定两个元素 $P\in G_1$ 和 $Q\in G_1$,计算 $a\in Z_q^*$,使 $Q=aP$ 成立。

b)计算 Diffie-Hellman 问题(computational diffie-hellman problem,CDH 问题)。已知 $P,aP,bP,a,b\in Z_q^*$,计算 abP。

1.3 签密体制的安全特性

a)保密性(confidentiality)。攻击者从一个密文中获取任何明文信息在计算上是不可行的。

b)不可伪造性(unforgeability)。攻击者产生一个合法的签密密文在计算上是不可行的。

c)不可否认性(non-repudiation)。发送者不能否认他已经签密过的消息。也就是说,消息的接收者可以向第三方证明发送者的确发送过此消息。

1.4 无证书签密方案

一个无证书签密方案由 KGC、签密用户和接收用户三个合法的参与人以及系统参数生成、部分密钥生成、设置秘密值、设置私钥、设置公钥、签密以及验证 7 个算法组成[11]。通常,前两个算法由 KGC 执行,而其他算法由签名或验证用户执行。

a)系统建立算法。给定一个安全参数 k,PKG 利用该算法生成系统公开参数和主密钥 s。PKG 公开参数并保留 s。

b)部分私钥生成算法。给定一个用户身份 ID,KGC 为用户生成部分私钥 D_{ID}。

c)用户秘密值生成算法。输入用户身份 ID,用户 ID 输出秘密值 $x\in Z_q^*$,作为其长期密钥。

d)用户私钥生成算法。输入给定用户身份 ID,用户的部分私钥 D_{ID}及其长期私钥 x,返回用户的私钥 $Sk=(x,D_{\mathrm{ID}})$。

e)用户公钥生成算法。输入给定用户身份 ID、用户的部分私钥 D_{ID}对应的公钥 P 及其长期私钥 x,返回用户 ID 的公钥 Pk。

f)签密算法(signcrypt)。输入消息 m、签密者身份 ID 及其私钥 Sk、接收者的身份 ID 及其公钥 Pk,返回密文。

g)解签密验证算法(unsigncrypt)。输入 σ、签密者身份 ID 及其私钥 Pk、接收者的身份 ID 及其公钥 Sk,如果通过验证,则用户输出明文 m;否则拒绝接收消息 m。

2 一个安全的无证书签密方案

基于文献[10]的签名方案,本文构造了一个安全的无证书的签密方案。方案的具体执行过程描述如下:

a)系统建立。设 G_1 为由 P 生成的循环加法群,阶为 q,G_2 为具有相同阶 q 的循环乘法群,$\hat{e}:G_1\times G_1\rightarrow G_2$ 为一个双线性映射。定义安全的哈希函数 $H_1,H_2:\{0,1\}^*\rightarrow G_1$,$H_3:\{0,1\}^*\rightarrow Z_q^*$,$H_4:G_2\rightarrow\{0,1\}^n$。PKG 随机选择一个主密钥 $s\in Z_q^*$,计算 $P_{\mathrm{pub}}=sP$。PKG 公开系统参数$\{G_1,G_2,q,\hat{e},P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4\}$,保密主密钥 s。

b)密钥提取。给定一个用户的身份 ID,KGC 计算该用户的部分私钥 $D_{\mathrm{ID}}=sQ$,其中 $Q=H_1(\mathrm{ID})$。用户选取 $x\in Z_q^*$,计算部分公钥 $P_{\mathrm{ID}_{\mathrm{part}}}=xP$,用户的完整私钥为 $S_{\mathrm{ID}}=xU+D_{\mathrm{ID}}$,其中 $U=H_2(\mathrm{ID},P_{\mathrm{ID}_{\mathrm{part}}})$公钥为 $P_{\mathrm{ID}}=(P_{\mathrm{ID}_{\mathrm{part}}},H_1(\mathrm{ID}))$。因此,用户 Alice(签密者)的私钥 $S_A=x_AU+D_A$,$P_A=(P_{A_{\mathrm{part}}},H_1(\mathrm{ID}_A))$;用户 Bob(解签密者)的私钥 $S_B=x_BU+D_B$,$P_B=(P_{B_{\mathrm{part}}},H_1(\mathrm{ID}_B))$。KGC 计算 $\hat{e}(P,H_1(\mathrm{ID}_A))$,$\hat{e}(P,H_1(\mathrm{ID}_B))$,$\hat{e}(P_{\mathrm{pub}},H_1(\mathrm{ID}_A))$,$\hat{e}(P_{\mathrm{pub}},H_1(\mathrm{ID}_B))$。

c)签密。为了发送一个消息 m 给 Bob,Alice 执行以下步骤:

(a)随机选取 $r\in Z_q^*$,计算 $R=\hat{e}(P,H_1(\mathrm{ID}_A))$,$W=rP$。

(b)计算 $h=H_3(m,\mathrm{ID}_A,R,P_{A_{\mathrm{part}}})$,$V=rH_1(\mathrm{ID}_A)+hS_A$。

(c)计算 $z=\hat{e}(P_{\mathrm{pub}},H_1(\mathrm{ID}_B))^r\hat{e}(U,P_{B_{\mathrm{part}}})^r$ 和 $c=m\oplus H_4(z)$。

(d)发送密文 $\sigma=(c,W,h,V)$给 Bob。

d)解签密。当收到密文 σ 时,Bob 执行以下步骤:

(a)计算 $z=\hat{e}(W,S_B)$,恢复消息 $m=c\oplus H_4(z)$。

(b)计算 $U=H_2(\mathrm{ID}_A,P_{A_{\mathrm{part}}})$,$H_1(\mathrm{ID}_A)$,$R=\hat{e}(P,V)(\hat{e}(U,P_{A_{\mathrm{part}}},H_1(\mathrm{ID}_A)))^{-h}$,检查等式 $h=H_3(m,\mathrm{ID}_A,R,P_{A_{\mathrm{part}}})$是否成立,如果上述等式成立,Bob 接收这个消息,否则认为密文 σ 不合法。

3 安全性分析

3.1 有效性分析

a)敌手从密文 $\sigma=(c,W,h,V)$中获取任何明文信息等同于求解 DL 问题和哈希碰撞问题,故在在计算上是不可行的。

b)若密文 $\sigma=(c,W,h,V)$是合法的,则一定可以通过等式 $h=H_3(m,\mathrm{ID}_A,R,P_{A_{\mathrm{part}}})$的验证。因为:

$$\begin{aligned}R&=\hat{e}(P,V)(\hat{e}(U,P_{A_{\mathrm{part}}})\hat{e}(P_{\mathrm{pub}},H_1(\mathrm{ID}_A)))^{-h}=\\&\hat{e}(P,rH_1(\mathrm{ID}_A)+hS_A)\hat{e}(U,hP_{A_{\mathrm{part}}})\hat{e}(P_{\mathrm{pub}},hH_1(\mathrm{ID}_A))=\\&\hat{e}(P,rH_1(\mathrm{ID}_A)+hS_A-hx_AU-hsH_1(\mathrm{ID}_A))=\\&\hat{e}(P,rH_1(\mathrm{ID}_A))=\hat{e}(P,H_1(\mathrm{ID}_A))^r\end{aligned}$$

3.2 不可伪造性分析

在无证书系统中有两类攻击者[8]。第一类攻击者,即攻击者不能拥有系统主密钥,但可以替换任何用户的公钥,这是一类普通的攻击者;第二类攻击者,即攻击者拥有系统主密钥,可以自己产生部分私钥,但是他们不能替换任何用户的公钥,这属于恶意的 PKG 攻击。本文的方案在随机预言机下的不可伪造性证明过程可参考文献[10]。下面给出方案不可伪造性的一个更为直观的证明。

定理 1 基于 DL 和 CDH 问题困难性假设,本文的签密方案对于第一类攻击者是安全的。

证明 敌手能够替换用户的公钥,但是不知道系统的主密钥 s,所以无法获得用户 A 的部分私钥 D_{ID}。假定敌手截获了密文 σ 和获取了用户的公钥 P_A,为了伪造用户 A 的密文 σ,敌手必须伪造一个随机数 $x_w\in Z_q^*$,计算部分公钥 $P_{\mathrm{ID}_{\mathrm{part}}}=x_wP$,同时伪造主密钥 s_w,计算该用户 A 的部分私钥 $D_{\mathrm{ID}}=s_wH_1(\mathrm{ID})$,则伪造的公钥为 $P_A=(P_{A_{\mathrm{part}}},H_1(\mathrm{ID}_A),)$。故其伪造的密文为 $\sigma_w=(c,W,h,V)$。但是在 Bob 进行验证时,由于 x_w 和 s_w 都是伪造的,故等式 $h=H_3(m,\mathrm{ID}_A,R,P_{A_{\mathrm{part}}})$在验证时是不相等的,因此本文的方案在 DL 和 CDH 问题困难性假设下,敌手是不

能伪造的。

定理 2　基于 DL 问题困难性假设,本文的签密方案对于第二类攻击者是安全的。

证明　假定敌手拥有系统的主私钥 s,但是没有替换用户公钥的能力。由于敌手拥有系统的主私钥 s,所以他可以很容易地计算用户 A 的部分私钥 D_{ID}。但是要伪造密文 σ,敌手必须使用户的部分公钥 $P_{\mathrm{ID}_{\mathrm{part}}}=xP$,这相当于在群 G_1 求解离散对数问题。而敌手伪造 x_w,计算 $V=rH_1(\mathrm{ID}_A)+hS_A$ 得到的密文 $\sigma_w=(c,W,h,V)$ 是不能通过 Bob 的检验的。因此本文的方案是能够抵御第二类攻击的。

3.3　效率分析

本文将运算(p)、点乘运算(mul)和指数运算(exp)三个方面的计算量与文献[12]进行了比较。比较结果如表 1 所示。

表 1　方案的计算开销比较

方案	Signcrypt			Unsigncrypt		
	exp	p	mul	exp	p	mul
文献[12]	0	1	3	0	3	3
本文方案	2	1	2	1	3	0

在有预计算的情况下,从表 1 可以看出,本文的方案在指数运算方面虽然有三次运算,但文献[12]在点乘运算方面总共比本文的方案多 4 次,并且本文的方案是基于文献[10]构造而成的,其签密长度比文献[12]更短,因此本文方案能更好地适应计算量受限的环境。

4　结束语

无证书密码体制很好地克服了基于身份密码体制中固有的密钥托管问题和消除了基于传统公钥基础设施中公钥证书的复杂性管理问题,近年来得到了广泛的应用。本文提出了一个安全的无证书签密方案,在较强的安全模型下对用该方法所构造的方案的安全性进行了证明。结果表明,本文方案是能够抵御保密性、不可伪造性和可否认性等攻击的。进一步提高无证书签密方案的安全性能以及设计能很好地适应对计算量受限的环境(如 Ad hoc 网络环境)的无证书签密方案,将是笔者需要重点研究的课题。

参考文献:

[1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Trans on Information Theory,1976,22(6):644-654.

[2] SHAMIR A. Identity-based cryptosystems and signatures schemes [C]//Proc of CRYPTO on Advances in Cryptology. Berlin:Springer-Verlag,1985:47-53.

[3] AL-RIYAMI S S,PATERSON K G. Certificateless public key cryptography[C]//Proc of the 9th International Conference on the Theory and Application of Cryptology and Information Seaurity. Berlin:Springer-Verlag,2003:452-473.

[4] ZHENG Yu-liang. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost(encryption)[C]// Proc of the 17th Annual International Cryptology Conference. Berlin: Springer-Verlag,1997:165-179.

[5] BARBOSA M, FARSHIM P. Certificateless signcryption[C]//Proc of ACM Symposium on Infomation,Computer and Communications Security. New York:ACM Press,2008: 369-372.

[6] ARANHA D, CASTRO R. Efficient certificateless signcryption[EB/OL]. (2008). http://sbseg2008. inf. ufrgs. br/proceedings/data/pdf/st03_Ol_resumo. pdf.

[7] WU C H, CHEN Z X. A new efficient cenificateless signcryption scheme[C]//Proc of ISISE. 2008:661-664.

[8] SHARMILA D S, VIVEK S S, PANDU R C. On the security of certificateless signcryption schemes,Report 2009/298[R]. [S. l.]:Cryptology ePrint Archive,2009.

[9] LI Fa-gen, SHIRASE M,TAKAGI T. Certificateless hybrid signcryption[C]//Proc of the 5th International Conference on Information Security Practice and Experience. Berlin: Springer-Verlag, 2009: 112-123.

[10] 张磊,张福泰. 一类无证书签名方案的构造方法[J]. 计算机学报,2009,32(5):940-945.

[11] 刘文浩,许春香. 无双线性配对的无证书签密方案[J]. 软件学报,2011,22(8):1918-1926.

[12] 陈明,吴开贵,何盼. 一种新的无证书签密方案[J]. 计算机应用研究,2011,28(10):3799-3802,3822.

(上接第 1532 页)

参考文献:

[1] YAO A C. Protocols for secure computations[C]//Proc of the 23rd Annual Symposium on Foundations of Computer Science. Washington DC:IEEE Computer Society,1982:160-164.

[2] GOLDREICH O,MICALI S,WIGDERSON A. How to play any mental game[C]//Proc of the 19th Annual ACM Conference on Theory of Computing. New York:ACM Press,1987:218-229.

[3] ATALLAH M J, DU Wen-liang. Secure multi-party computational geometry[C]//Proc of the 7th International Workshop on Algorithms and Data Structures. Berlin:Springer-Verlag,2001:165-179.

[4] 罗永龙,黄刘生,荆巍巍,等. 保护私有信息的叉积协议及其应用[J]. 计算机学报,2007,30(2):248-254.

[5] LI Shun-dong, DAI Yi-qi. Secure two-party computational geometry [J]. Journal of Computer Science and Technology, 2005, 20 (2):258-263.

[6] 刘文,王永滨. 安全多方信息比较相等协议及其应用[J]. 电子学报,2012,40(5):871-876.

[7] 程文娟,董莹莹,汪庆,等. 有关保护私有信息的三角不等式判定问题研究[J]. 合肥工业大学学报:自然科学版,2012,35(5):625-628.

[8] 徐滨,彭长根. 恶意模型下公平的安全两方计算协议[J]. 贵州大学学报:自然科学版,2012,29(1):75-78,87.

[9] DU Wen-liang,ATALLAH M J. Secure multi-party computation problems and their applications:a review and open problems[C]//Proc of Workshop on New Security Paradigms. New York:ACM Press,2001: 11-20.

[10] 杨锦钜. 用一般方程表示的空间两平行直线间的距离公式[J]. 佛山大学佛山师专学报:理工版,1990,8(4):81-87.

[11] BRASSARD G, CREPEAU C, ROBERT J M, All-or-nothing disclosure of secrets[C]//Proc of CRYPTO on Advances in Cryptology. Berlin:Springer-Verlag,1986:234-238.

[12] 王萼芳,石生明. 高等代数[M]. 3 版. 北京:高等教育出版社,2003.