高效的基于 ID 的无可信中心签名方案 *

蔡光兴, 陈 华
(湖北工业大学 理学院, 武汉 430068)

摘 要: 针对现有的基于身份签名系统的密钥托管问题,提出了一种高效的基于身份的无可信中心签名方案。新方案通过将两个部分公钥绑定相同的一个身份,从而解决了密钥托管问题。在随机预言模型下,新方案被证明能够抵抗适应性选择消息和身份的存在性伪造攻击。与其他基于身份无可信中心签名方案相比,新方案具有更高的效率。

关键词: 基于身份的签名方案; 密钥托管问题; 无可信中心; 双线性对; 随机预言模型
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2009)07-2751-03
doi:10.3969/j.issn.1001-3695.2009.07.101

Efficient ID-based signature scheme without trusted party

CAI Guang-xing, CHEN Hua
(*School of Science*, *Hubei University of Technology*, *Wuhan* 430068, *China*)

Abstract: This paper proposed an efficient ID-based signature scheme without trusted party against the problem of key escrow of ID-based signature system. The new scheme could solve the key escrow problem through binding two partially public keys with a same identity and has been proved secure against existential forgery on adaptively chosen message and ID attack under random oracle model. The efficiency of the scheme is higher than the existing schemes.

Key words: ID-based signature; key escrow; non-trusted party; bilinear parings; random oracle model

1984 年 Shamir[1] 首先提出了基于身份的密码系统(ID based cryptosystem, IBC),其简化了基于证书公钥密码系统负担最重的密钥管理过程。在此之后,涌现了许多基于身份的密码方案,但是其中的大部分方案由于效率低而不实用。在 2000 年,Joux 在文献[2]做出了突破性的工作,第一次把本来用于密码攻击的双线性对(bilinear pairing)成功地用于密码系统的构造。它使得过去不知道的或不实用的方案现在密码学实现方面成为可能,更为幸运的是它们也是构造基于 ID 签名方案(ID based signature, IBS)的重要工具。近些年来,由双线性对构造的 IBS 方案不断涌现。在 2000 年的 SCIS'00 上,Sakai 等人在文献[3]中首次提出了由双线性对构造的 IBS 方案,然而他们并没有给出安全性分析。Paterson 在文献[4]中提出了一种基于双线性对的 IBS 方案,并且给出了大量的安全性假设,但是仍没有给出严格的安全性证明。2002 年,Hess 在文献[5]中提出了一种可证明安全的 IBS 方案,该方案能够抵抗适应性选择消息攻击和固定 ID 攻击下的存在性伪造。随之,Cha 等人在文献[6]中给出了一种针对 IBS 方案安全性的定义:抗适应性选择消息和 ID 攻击下的存在性伪造,并在此定义下,利用双线性对构造了第一个可证明安全的基于 GDH(gap Diffie-Hellman groups)群的 IBS 方案。Barreto 等人[7] 提出了一种基于 q-SDH(q-strong Diffie-Hellman)群的 IBS 方案,并在随机预言模型下证明了其方案能抵抗适应性选择消息和身份的存在性伪造攻击。但是这些方案都存在一个问题,即密钥托管问题:系统必须无条件信任私钥生成中心(private key generator, PKG),PKG 知道系统中所有用户的私钥,一旦 PKG 不诚实,就可以达到伪造合法用户有效签名的目的。目前,针对 IBS 密钥托管问题,提出了一些解决不需要可信中心的签名方案[8,9]。

1 数学背景及相关工作

1.1 双线性对

定义 设 G_1 与 G_2 是两个阶为 q 的循环群,q 为大素数。其中 G_1 是由 P 生成的加法循环群,G_2 是一个乘法循环群。假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题。双线性对是指具有下面性质的一个映射 $e: G_1 \times G_1 \rightarrow G_2$。

性质 1 双线性。对所有的 $P_1, P_2, Q \in G_1$,有

$$e(P_1 + P_2, Q) = e(P_1, Q) . e(P_2, Q)$$
$$e(Q, P_1 + P_2) = e(Q, P_1) . e(Q, P_2)$$

从而对于所有的 $P, Q \in G_1, a, b \in Z_q^*$,有

$$e(aP, bQ) = e(P, Q)^{ab}$$

性质 2 非退化性。存在 $P, Q \in G_1, P \neq O$,满足 $e(P, Q) \neq 1$。

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

注:可以利用椭圆曲线中的 Weil 和 Tate 配对来构造双线性对。

1.2 基于双线性对的困难问题

在这样的群 G_1 上,可以定义以下几个数学难题:

收稿日期: 2008-10-26; **修回日期**: 2008-12-28 **基金项目**: 湖北省科技厅自然科学基金资助项目(2008CDB011)

作者简介:蔡光兴(1964-),男,教授,研究生导师,主要研究方向为代数、信息安全、信息编码(slxcai@mail.hbut.edu.cn);陈华(1981-),女,助教,博士研究生,主要研究方向为密码理论与技术、信息编码.

a)离散对数问题(DLP)。对给定的 $Q = xP \in G_1$,计算 $x \in Z_q^*$。

b)计算 Diffie-Hellman 问题(CDHP)。对 $a, b \in Z_q^*$,给定 $P, aP, bP \in G_1$,计算 abP。

c)判定 Diffie-Hellman 问题(DDHP)。给定 $P, aP, bP, cP \in G_1$。其中 $a, b, c \in Z_q^*$,判定 $c = ab \bmod q$ 是否成立。

d)间隙 Diffie-Hellman 问题(GDHP)。在 G_1 上,DDHP 易于解决而 CDHP 难以解决,则笔者称此群为间隙 Diffie-Hellman 群,简记 GDH 群。

2 一个新的基于 ID 的无可信中心签名方案

2.1 系统初始化(setup)

设 G_1 阶为大素数 q 的由 P 生成的加法循环群,通常取为有限域 Z_q 中的椭圆曲线上有理点群的一个加法子群;

G_2 阶为大素数 q 的乘法循环群,通常取为有限域 Z_q 中的椭圆曲线上有理点群的一个乘法子群;

$e: G_1 \times G_1 \rightarrow G_2$ 的双线性映射

H_1, H_2:无碰撞的哈希函数,

$$\{0,1\}^* \times G_1 \rightarrow Z_q^*$$

首先 PKG 随机选取主密钥 $S \in_R Z_q^*$,并计算它的公钥 $P_s = sP$;签名者同样随机选取一个整数 $s_1 \in_R Z_q^*$ 作为它的部分私钥,并计算 $Q_1 = s_1 P$ 作为自己的部分公钥。

2.2 密钥生成(extract)

签名人把 s_1 的使用期限 T 送给 PKG,并将其身份信息 ID 提交给 PKG,PKG 成功验证签名人身份后计算 $Q_2 = H_2(\mathrm{ID} \| T, Q_1)$,$s_2 = sQ_2$,通过安全信道传给签名人,$Q_2$、$s_2$ 分别作为签名人的部分公钥和私钥。最终签名人的公钥是$\{Q_1, Q_2\}$,私钥是$\{s_1, s_2\}$。

对于每一个身份来说,extract 设置一般只需要运行一次,而且每次都使用相同的系统参数(P_s, s)。

2.3 签名(sign)

假设签名人对消息 M 签名,签名人先随机选取一个整数 $k \in_R Z_q^*$,计算 $r = kQ_2$,$V = H_1(M, r)$,$U = ks_2 + Vs_1Q_2$。把(r, V, U)作为对消息 M 的签名。

2.4 签名验证(verify)

验证人首先计算 $Q_2 = H_2(\mathrm{ID} \| T, Q_1)$,$V = H_1(M, r)$,然后计算等式:

$$e(U, P) = e(r, P_s) . e(Q_2, Q_1)^V$$

是否成立,如果成立则接受签名人对消息 M 的签名,否则该签名无效。因为

$$e(U, P) = e(ks_2 + Vs_1Q_2, P) = e(ks_2, P)e(Vs_1Q_2, P) = e(skQ_2, p)e(Q_2, s_1P)^V = e(kQ_2, sP)e(Q_2, Q_1)^V = e(r, P_s) . e(Q_2, Q_1)^V$$

故新方案满足正确性。

3 方案安全性与性能分析

3.1 安全性分析

在这一部分,将给出在随机预言模型下[10]基于 ID 的无可信中心签名方案的安全性分析。

3.1.1 IBS 方案的攻击模型[6]

一个 IBS 签名方案包括 setup、extract、sign、verify 四个算法。称一个基于 ID 的数字签名方案在是安全的(能够抵抗适应性选择消息攻击和 ID 攻击下的存在性伪造),如果在下面的游戏中不存在多项式时间算法攻击者 A 通过借助挑战者 C 而能够以一个不可忽略的概率优势赢得游戏:

a)C 运行 setup 算法,把输出的系统参数发送给 A。

b)A 可以进行如下查询:(a)Hash 函数查询,C 计算请求输入的 hash 值,把结果返回给 A;(b)密钥生成查询,给定身份 ID,C 运行 extract 算法,将私钥返回给 A;(c)签名查询,给定身份 ID 和消息 M,C 运行 sign 算法,将对应签名返回给 A。

c)A 输出(ID, M, S),其中 S 是对消息 M 的签名。ID 和(ID, M)不能是之前进行的 extract 算法和 sign 算法的输入。笔者称如果 S 是 M 的有效签名,则 A 赢得该游戏。

3.1.2 安全性分析与证明

1)敌手伪造签名

定理 1[6] 在 IBS 方案中,如果存在一个算法 F_0 在时间 t_0 内经过 n_{H_2} 次 H_2 查询,以 ε_0 的概率成功地对本方案进行适应性选择消息和身份攻击,那么就存在一个算法 F_1 在 $t_1 \leqslant t_0$ 的时间范围内进行与 F_0 相同次数的密钥生成查询、签名查询和 hash 函数查询,以 $\varepsilon_1 \leqslant \varepsilon_0 \quad 1 - 1/q \quad 1/n_{H_2}$ 的概率成功地对本方案进行适应性选择消息和固定身份攻击。

定理 1 假设存在一个算法 F_1 进行 n_{H_1} 次 H_1 查询、n_{H_2} 次 H_2 查询、n_s 次签名查询,在时间 t 内以 $\varepsilon_1 \leqslant 10(n_s + 1)(n_s + n_{H_1})1/q$ 的概率对本方案进行固定身份的适应性选择消息攻击,那么就存在多项式时间算法 F_2 解决 CDHP 困难问题。

证明 设给定的身份是 ID,根据文献[11,12]的分叉引理(forking lemma),如果方案存在一个固定身份 ID 的适应性选择消息攻击的多项式时间算法 F_1,那么就存在一个有效的算法 F_3,该算法能对某个消息 M 产生两个有效签名(r, V, U)和(r, V', U')。其中 $V \neq V'$,那么就能够得到以下等式:

$$e(U, P) = e(r, P_s) . e(Q_2, Q_1)^V$$

$$e(U', P) = e(r, P_s) . e(Q_2, Q_1)^{V'}$$

推得

$$e((U' - U) - s_1Q_2(V' - V), P) = 1$$

因为双线性对是非退化的,所以

$$(U' - U) - s_1Q_2(V' - V) = O$$

即

$$s_1Q_2 = (V' - V)^{-1}(U' - U)$$

注意到由 $Q_1 = s_1P = aP$,$Q_2 = bP$ 计算 $s_1Q_2 = s_1bP = abP$ 是一个 CDHP 困难问题,所以算法 F_3 有效地解决了 CDHP 困难问题。

综合定理 1 和 2,本方案满足如下定理:

定理 3 本方案基于 CDHP 困难问题能抵抗随机预言模型下的适应性选择消息和身份的存在性伪造攻击。

2)PKG 伪造签名

第一种情况,PKG 想伪造对消息 M 的签名,使得该签名与签名人对消息 M 的签名相同。由签名方程 $U = ks_2 + Vs_1Q_2$ 知,PKG 必须知道 k 和 s_1 才能伪造,显然 PKG 得到 s_1 是不可能的,得到 k 又与 DLP 困难问题相矛盾。

第二种情况,PKG 想伪造对消息 M 的签名,该签名与签名

人对消息 M 的签名不同。PKG 可以伪造签名人的公钥对 $\{Q'_1, Q'_2\}$,私钥对 $\{s'_1, s'_2\}$,然后生成一个可验证的有效签名 (r', V', U')。但是,合法的签名人可以向仲裁者提供一个证据,证明 PKG 伪造了他的签名。按照下述协议就可以证明签名人确实知道 s_2:仲裁者随机选取 $a \in_R Z_q^*$,把 $aH_2(\mathrm{ID} \| T, Q_1)P$ 通过安全通道交给签名人,签名人计算:$e(s_2, aH_2(\mathrm{ID} \| T, Q_1)P)$,然后传给仲裁者,如果

$$e(s_2, aH_2(\mathrm{ID} \| T, Q_1)P) = e(Q_2, Q_2)^{ap_s}$$

成立,就说明签名人确实知道 s_2,这时仲裁者就可以判断 PKG 伪造了签名人的签名。这是因为 1)中证明可知除 PKG 外的任何人都无法得到 s,进而无法伪造签名人的签名。

由此可见,PKG 不能伪造签名,即使伪造,也会被发现,从而解决了 IBS 系统中固有的密钥托管问题。

3.2　效率分析与比较

本文所提出的签名方案与文献[8]所提出的方案都是基于 GDH 群的基于 ID 的无可信中心签名方案,具有相同的安全性,并且在系统初始化和密钥生成过程中运算相同,因此笔者只比较两种方案在签名和验证过程中的运算,假设"e"为对运算,"M"为点乘运算,"h"为 hash 函数运算,"E"为指数运算,比"A"为加法运算。比较结果如表 1 所示。

表 1　方案比较

方案	签名	验证
文献[8]方案	$4M+2A+2H$	$4e+1M+2A+3H$
新方案	$4M+1A+1H$	$3e+1E+2H$

显然,新方案具有更高的执行效率。

4　结束语

本文针对现有的基于身份签名系统的密钥托管问题,提出了一种高效的基于身份的无可信中心签名方案。在新方案中,用户签名密钥由 PKG 和用户共同产生,从而 PKG 不能够伪造合法者的签名,即使能够伪造,也会被发现,从而解决了 IBS 系统中固有的密钥托管问题。在随机预言模型下,新方案被证明能够抵抗适应性选择消息和身份的存在性伪造攻击,假设 CDHP 是困难的。新方案不仅解决了密钥托管问题,而且与其他基于身份无可信中心签名方案相比具有更高的效率。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of Advances in Cryptology-Crypto'84. New York :Springer-Verlag,1985:47-53.

[2] JOUX A. A one round protocol for tripartite Diffie-Hellman[J]. Journal of Ctyptology, 2004, 17(4): 263-276.

[3] SAKAI R, OHGISHI K, KASAHARA M. Cryptosystems based on paring[C]//Proc of Symposium on Cryptography and Information Security-SCIS'00. Okinawa: [s. n.], 2000:26-28.

[4] PATERSON K G. Id-based signatures from parings on elliptic curves [J]. Electronics Letters, 2002, 38(18):1025-1026

[5] HESS F. Efficient identity based signature schemes based on parings [C]//Proc of Selected Areas in Crypto-graphy-SAC'02. Berlin: Springer, 2003: 310-324.

[6] CHA J C, CHEON J H. An identity-based signature from gap Diffie-Hellman groups[C]//Proc of Public Key CryptoGraphy-PKC 2003. Berlin:Springer,2003:18-30.

[7] BARRETO P, LIBERT B, MCCULLAGH N, *et al*. Efficient and provably secure identity-based signature and signcryption from bilinear maps[C]//Proc of Asiacrypt, Advance in Cryptology-ASIACRYPT 2005. Berlin:Springer-Verlag,2005:515-532.

[8] CHEN X, ZHANG F, KIM K. A new ID-based group signature scheme from bilinear pairings[EB/OL]. (2003). http://eprint.iacr.org/2003/116. pdf.

[9] GORANTLA M C, SAXENA A. An efficient certificate-less signature scheme[C]//Proc of Cmputational Intelligence and Security. Berlin: Springer, 2006: 110-116.

[10] BELLARE M, ROGAWAY P. Random oracles are practical; a paradigm for designing efficient protocols[C]//Proc of the 1st CCCS. 1993:62-73.

[11] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3):361-396.

[12] GU Chun-xiang, ZHU Yue-fei. Forking lemma and the security proofs for a class of ID-based signatures[J]. Journal of Software, 2007, 18(4):1007-1014.

(上接第 2731 页)作进行了简化。对于过往用户再次访问站点情形,会话密钥协商过程仅需一次对称加解密运算(与一次乘法运算量相当)即可完成。相对于 SSL、SSH 等协议,同样情形下会话密钥协商需一次非对称加解密运算加一次对称加解密运算。基于非对称加解密运算的巨大运算量(指数级),本方法对于服务端密钥交换运算负荷的降低是显而易见的。

此外,本方案中,客户端本地存储与服务器交换所得主密钥,服务端在客户端发出再次连接请求后,可由自身密钥与客户端发送的客户端标志信息快速计算出通信主密钥。该方法大大减少了服务端密钥存储量,同时加密强度依赖于所选密码算法强度,等同于 SSL 等协议安全性。

本方案在相当的安全性下,可极大降低服务端提供通信加密的运算和存储复杂度,易于推广实现,有效防止第三方监控,进而保护用户隐私,确保 Web 通信中敏感数据的安全传递。

参考文献:

[1] KRAWCZYK H, BELLARE M, CANETTI R. RFC 2104, HMAC: keyed-hashing for message authentication[S]. 1997.

[2] NISTFIPS PUB 180-1, Secure hash standard[S]. National Institute of Standards and Technology, U. S. Department of Commerce, Work in Progress, 1994.

[3] HOUSLEY R, FORD W, POLK W, *et al*. RFC 2459, Internet public key infrastructure: part I: X.509 certificate and CRL profile[S]. 1999.

[4] RSA Laboratories, PKCS #1: RSA extended certificate syntax standard, version 1.5[S]. 1993.

[5] RSA Laboratories, PKCS #6: RSA extended certificate syntax standard, version 1.5[S]. 1993.

[6] RSA Laboratories, PKCS #7: RSA extended certificate syntax standard, version 1.5[S]. 1993.