有效的无证书签名方案

明 洋，王育民

(西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)

【摘要】为了避免基于身份密码系统中的秘钥托管问题，同时不需要证书进行公钥的认证，出现了无证书密码系统。该文基于双线性对提出一个新的无证书签名方案。方案中签名算法简单的不需要任何对的计算，验证算法仅仅需要三个对的计算，并且不需要使用特殊的哈希函数。与已知所有的方案相比，所提的方案在计算代价上更加有效。

关 键 词 双线性对； 无证书签名； 哈希函数； 秘钥托管
中图分类号 TP918 文献标识码 A

Efficient Certificateless Signature Scheme Based on Bilinear Pairings

MING Yang and WANG Yu-min

(State Key Laboratory of Integrated Service Networks, Xidian University Xi'an 710071)

Abstract Due to eliminating the inherent key escrow in identity-based cryptosystem and yet not needing certificates to guarantee the authenticity of public keys, the concept of certificateless public key cryptosystem is introduced. In this paper, a new certificateless signature scheme based on bilinear pairings is present. The signing algorithm of the proposed scheme is very simple and does not require any pairing computation, and the verification algorithm only needs three pairings computation. Furthermore, the scheme does not need special hash function. Our proposed scheme is more efficient than all knowing schemes in terms of computation overhead.

Key words bilinear pairing; certificateless signature; hash function; key escrow

为了简化数字证书管理的过程，文献[1]提出基于身份密码系统的概念。但是，基于身份密码系统一个内在问题是密钥的托管，即密钥生成器(PKG)拥有所有用户的私钥，一个恶意的PKG就可以通过伪造用户的签名来陷害无辜的用户。文献[2]提出了无证书公钥密码系统(CL-PKC)的概念，解决了基于身份密码系统中密钥托管的问题，同时也不需要公钥证书来认证用户的公钥。因此减少了开支，更加适合低带宽和低功率的移动环境中的安全应用。自从文献[2]提出了无证书签名方案后，出现许多无证书的签名方案[3-5]。本文提出一个有效的基于双线性对的无证书签名方案，在签名阶段不需要对计算，在验证阶段仅仅需要三个对计算，同时不需要使用映射到点(MapToPoint)的特殊的哈希(Hash)函数。

1 基础知识

1.1 双线性对

设 G_1 是一个阶数为素数 p 的加法循环群，$P \in G_1$ 是群 G_1 的生成元，G_2 是一个阶数同样为素数 p 的乘法循环群。假设在群 G_1 和 G_2 中离散对数问题困难，一个双线性对是一个映射 $\hat{e}: G_1 \times G_1 \to G_2$，具有下面的三个性质：

(1) 双线性性。对所有的 R， $Q \in G_1$， $a,b \in Z_p$ 都有 $\hat{e}(aR,bQ) = \hat{e}(R,Q)^{ab}$。

(2) 非退化性。存在 R，$Q \in G_1$，满足 $\hat{e}(R,Q) \neq 1$。

(3) 可计算性。对所有的 R, $Q \in G_1$，存在有效的算法去计算 $\hat{e}(R,Q)$。

这样的对可以通过有限域上的超奇异椭圆曲线或超奇异椭圆曲线中的Weil对或Tate对来实现[6]。

1.2 安全假设

定义 1 q强Diffie-Hellman问题(q-SDHP)[7]：

在群 (G_1,G_2) 中，对于整数 q， $\alpha \in Z_p^*$， $P \in G_1$，给定 $q+1$ 元组 $(P,\alpha P,\alpha^2 P,\cdots,\alpha^q P)$ 作为输入，输出一个对 $\left(c,\frac{1}{c+\alpha}P\right)$，且 $c \in Z_p^*$。

定义算法 A 解q-SDHP成功概率为：

收稿日期：2006－08－30；修回日期：2007－01－28
基金项目：国家自然科学基金(60473027)
作者简介：明 洋(1979－)，男，博士生，主要从事数字签名和电子商务等方面的研究；王育民(1936－)，男，教授，博士生导师，主要从事密码、编码等方面的研究.

$$\Pr\left[A(P,\alpha P,\alpha^2 P,\cdots,\alpha^q P \mid \alpha\in Z_p^*, P\in G_1)=\left(c,\frac{1}{c+\alpha}P\right)\right]\geqslant\varepsilon$$

那么算法 A 以优势 ε 解群 (G_1,G_2) 中的 q 强Diffie-Hellman问题。

假设 1 q强Diffie-Hellman假设(q-SDHA)：

如果没有 t 时间的算法以优势 ε 解群 (G_1,G_2) 中 q强Diffie-Hellman问题，即在群 (G_1,G_2) 中 q-SDHP是 (t,ε) 困难的，则q强Diffie-Hellman假设成立。

2 本文的方案

基于文献[7]的身份签名方案，本文提出一个基于双线性对的有效的无证书签名方案，包含七个算法：系统建立、部分私钥提取、设置秘密值、设置私钥、设置公钥、签名生成和签名验证；涉及三个部分：密钥生成中心(KGC)、签名者和验证者。

2.1 系统建立算法

密钥生成中心(KGC)完成以下步骤：

(1) 选取 $<G_1,G_2,\hat{e}>$；

(2) 选取任意的生成元 $P\in G_1$ 以及计算 $g=\hat{e}(P,P)$；

(3) 随机选取主密钥 $s\in Z_p^*$，设整个系统的公钥为 $P_{\text{pub}}=sP$；

(4) 选取两个密码学的Hash函数：$H_1:\{0.1\}^*\to Z_p^*$ 和 $H_2:\{0,1\}^*\times G_2\to Z_p^*$，则系统参数为 $\text{param}=\{G_1,G_2,\hat{e},P,P_{\text{pub}},g,H_1,H_2\}$，主密钥 $s\in Z_p^*$。

2.2 部分私钥提取算法

部分私钥提取算法由密钥生成中心完成。首先验证签名者 i 的身份 ID_i；计算 $Q_i=H_1(\text{ID}_i)$；然后计算部分私钥 $D_i=\frac{1}{Q_i+s}P$，并在安全的信道下把 D_i 发送给签名者 i；签名者 i 通过检验 $e(D_i,Q_iP+P_{\text{pub}})=g$ 是否成立来验证 D_i 的正确性。

2.3 秘密值提取算法

给定参数 param 和签名者 i 的身份 ID_i，签名者 i 随机选取 $x_i\in Z_p^*$ 作为秘密值。

2.4 设置私钥算法

给定参数 param，签名者 i 的部分私钥 D_i 以及秘密值 $x_i\in Z_p^*$，签名者 i 计算 $\text{SK}_i=x_iD_i=\frac{x_i}{Q_i+s}P$ 作为自己的签名私钥。

2.5 设置公钥算法

给定参数 param，秘密值 $x_i\in Z_p^*$，签名者 i 计算自己的公钥 $\text{PK}_i=(X_i,Y_i)$，其中，$X_i=\frac{1}{x_i}P$，$Y_i=\frac{1}{x_i}P_{\text{pub}}=\frac{s}{x_i}P$。

2.6 签名生成算法

签名者 i 使用签名私钥 SK_i 对消息 $m\in\{0,1\}^*$ 进行签名：

(1) 随机选取 $r\in Z_p^*$，计算 $R=g^r\in G_2$；

(2) 计算 $h=H_2(m,R)\in Z_p^*$；

(3) 计算 $S=(r+h)\text{SK}_i$；

则消息 m 的签名为 (h,S)。

2.7 签名验证算法

当验证者从身份为 ID_i 的签名者 i 收到公钥 $\text{PK}_i=(X_i,Y_i)$、消息 m 及其签名 (h,S) 时，完成下面的步骤：

(1) 验证等式 $\hat{e}(X_i,P_{\text{pub}})=\hat{e}(Y_i,P)$ 是否成立，如果不成立，输出 $\perp$，并放弃；

(2) 计算 $R'=\hat{e}(S,Q_iX_i+Y_i)g^{-h}$；

(3) 验证 $h=H_2(m,R')$ 是否成立，如果成立，输出“接受”；否则输出“拒绝”。

3 本文方案的分析

3.1 正确性

如果在公钥 $\text{PK}_i=(X_i,Y_i)$ 下 (h,S) 是消息 m 的有效签名，则满足：

$$\hat{e}(X_i,P_{\text{pub}})=\hat{e}(x_iP,sP)=\hat{e}(x_isP,P)=\hat{e}(x_iP_{\text{pub}},P)=\hat{e}(Y_i,P)$$

$$R'=\hat{e}(S,Q_iX_i+Y_i)g^{-h}=\hat{e}\left((r+h)\frac{x_i}{Q_i+s}P,Q_i\frac{1}{x_i}P+\frac{1}{x_i}P_{\text{pub}}\right)g^{-h}=\hat{e}\left((r+h)\frac{x_i}{Q_i+s}P,\frac{Q_i}{x_i}P+\frac{s}{x_i}P\right)g^{-h}=\hat{e}((r+h)P,P)\ \hat{e}(P,P)^{-h}=\hat{e}(P,P)^{r+h}\ \hat{e}(P,P)^{-h}=\hat{e}(P,P)^r=g^r=R$$

即 $h=H_2(m,R')$。

3.2 效率

在表1中，本文比较所提方案和文献[3-5]中方案的计算代价。假设所有的方案在相同的 $<G_1,G_2,\hat{e}>$ 下实现。

很多文章已经讨论了对的复杂性和如何加速对的计算[8]，但是对的计算仍然很消耗时间。在本文的方案中，预计算 $g=\hat{e}(P,P)$ 并作为系统的参数发布，因此在签名的生成中不需要对的计算，在签名

的验证中仅仅需要三个对的计算；另一方面，本文的方案仅仅需要通常密码学上安全的Hash函数，而不需要映射到点(MapToPoint)特殊的Hash函数，通常该Hash函数是概率的、低效的[9]。因此本文的方案比已知所有的方案效率高。

表1　计算代价比较

方　案	对	G_1标量乘	G_1加法	G_1指数	Z_p^* 加法	MapTo Point 哈希函数
文献[3]	2	2	1	1	0	使用
签名验证	5	0	0	1	0	
文献[4]	0	2	1	0	1	使用
签名验证	3	1	1	0	0	
文献[5]	0	2	0	0	1	使用
签名验证	4	1	1	0	0	
本文方案	0	1	0	1	1	不使用
签名验证	3	1	1	1	0	

3.3　安全性

(1) 公钥替换攻击：在无证书签名方案中，由于公钥没有被明显的认证(因为没有使用公钥证书)，所以应该考虑公钥替换攻击。在公钥替换攻击中，任何主动攻击的敌手能够用自己选择的 P_i' 值来代替用户 i 公钥 P_i。这个的替换攻击是不能成功的，因为敌手不知道部分私钥 D_i 的知识，因此不能得到签名者的私钥 SK_i，所以不能伪造出签名。

(2) 伪造攻击：本文提出的无证书签名方案的安全性是基于解椭圆曲线上离散对数问题。由 $X_i=\frac{1}{x_i}P$ 计算 x_i，及由 $Y_i=\frac{1}{x_i}P_{\mathrm{pub}}$ 计算 x_i 的困难性等价于解椭圆曲线上离散对数的困难性。同时本文的方案是基于文献[7]提出的基于身份的签名方案，该方案被证明在随机预言机模型[10]中选择消息攻击和身份攻击下，成功伪造签名等价于解 q 强Diffie-Hellman问题，因此本文的方案在随机预言机模型下也是安全的。

4　结 束 语

无证书签名是一种新型的签名，它简化了公钥密码系统，保持文献[1]的基于身份签名的效率，同时不遭受密钥托管的问题。本文提出一个基于双线性对的无证书签名方案，对计算代价而言，所提的方案比已有的方案都高效，因此更加适合在低带宽和低功率的移动环境中的安全应用。

参 考 文 献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology-Crypto'84. Berlin: Springer-Verlag, 1985, LNCS 196: 7-53.

[2] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptography-Asiacrypt'03. Berlin: Springer-Verlag, 2003, LNCS 2894: 452-473.

[3] HUANG Xin-yi, SUSILO W, Mu Y, et al. On the security of certificateless signature schemes from Asiacrypt 2003[C] // International Conference on Cryptology and Network Security-CANS'05. Berlin: Springer-Verlag, 2005, LNCS 3810: 13-25.

[4] CHOUDARY G M, ASHUTOSH S. An efficient certificateless signature scheme[C]//Computational Intelligence and Security-CIS'05. Berlin: Springer-Verlag, 2005, LNAI 3802: 110-116.

[5] LI X, CHEN K. Certificateless signature and proxy signature schemes from bilinear pairings[J]. Lietuvos Matematikos Rinkinys, 2005, 45(1): 95-103.

[6] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM Journal of Computing, 2003, 32(3): 586-615.

[7] BARRETO P S L M, LIBERT B, McCullagh N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]//Advances in Cryptology-Asiacrypt'05. Berlin: Springer-Verlag, 2005, LNCS 3788: 515-532.

[8] BARRETO P S L M, KIM H Y, LYNN B, et al. Efficient algorithms for pairing-based cryptosystems[C]//Advances in Crptology-Crypto'02. Berlin: Springer-Verlag, 2002, LNCS 2442: 354-368.

[9] ZHANG F, SAFAVI-NAINI R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications[C]//Practice and Theory in Public Key Cryptography-PKC'04. Berlin: Springer-Verlag, 2004, LNCS 2947: 277-290.

[10] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[C]// ACM Conference on Computer and Communications Security- ACMCCS'93. [S.l.]: ACM Press, 1993: 62-67.

编　辑　税　红