第 36 卷 第 20 期 计 算 机 工 程 2010 年 10 月
Vol.36 No.20 Computer Engineering October 2010
·安全技术· 文章编号：1000—3428(2010)20—0147—03 文献标识码：A 中图分类号：TP311.52

不含双线性对运算的无证书签密方案

葛爱军，陈少真
(信息工程大学信息工程学院，郑州 450002)

摘 要：当前无证书签密方案在具体应用时都要用到计算复杂的双线性对运算。针对该问题，提出一种安全的无需双线性对运算的无证书签密方案。该方案在随机预言模型下能够满足密文机密性和选择消息的不可伪造性，且安全性是基于离散对数难题和计算 Diffie- Hellman 难题的。实验结果表明，该方案具有明显的效率优势。

关键词：无证书密码；签密体制；随机预言模型；双线性对

Certificateless Signcryption Scheme Without Bilinear Pairings Calculation

GE Ai-jun, CHEN Shao-zhen
(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

【Abstract】 To solve the problem of all the certificateless signcryption schemes in the literature are built from bilinear mappings on elliptic curves which need costly operations, this paper presents the first concrete pairing-free certificateless signcryption. This scheme is provably secure in the random oracle model, relative to the hardness of the discrete logarithm problem and computational Diffie-Hellman problem. As there is no pairing operation in the new scheme, this scheme is more computationally efficient than others built from bilinear mappings.

【Key words】 certificateless cryptography; signcryption system; random oracle model; bilinear pairings

1 概述

为了解决基于身份密码体制的密钥托管问题，文献[1]把基于证书的密码体制与基于身份的密码体制相结合，给出了一种新的无证书公钥密码体制。在无证书密码体制中，用户的私钥是由两部分组成的，一部分私钥是由用户自己随机产生并秘密保存的，另一部分私钥是由 PKG 利用用户的身份信息给出的，这样 PKG 只能产生用户的一部分私钥，从而解决了基于身份密码体制固有的密钥托管问题。

使消息既保密又认证的传输是信息安全研究的主要目标之一，实现这一目标的传统方法是先签名后加密，但它所需的代价是签名和加密所需代价之和，因而效率极低。为了提高效率，文献[2]首次提出了签密的概念，并给出了一个具体的签密方案。文献[3]给出了第 1 个无证书签密方案，随后无证书签密体制得到了迅速发展，一系列无证书签密方案[4-5]相继被提出。

尽管人们在双线性映射的技术复杂性及如何提高其计算速度方面已做了大量工作，但是相比有限域上的模幂等运算，双线性对的运算花费仍然认为是比较高的。基于此，文献[6]首次给出了一种无证书加密方案，该方案不再依赖于双线性对运算，并且作者给出了随机预言模型下的安全性证明。本文在文献[6]无证书加密方案基础上给出一种不需双线性运算的无证书签密方案。因为没有复杂的双线性对运算，该方案具有极高的运算效率，并且在随机预言模型基于离散对数难题和计算 Diffie-Hellman 难题下是可证安全的。

2 预备知识

2.1 安全模型

在无证书密码体制中，因为没有证书来对用户的公钥进行认证，这样攻击者就可以把用户的公钥替换为自己任意选定的值，所以无证书密码体制存在 2 类攻击类型：第 1 类攻击者 A_I 不知道系统主密钥，但是他可以替换任意用户的公开密钥，而第 2 类攻击者 A_{II} 已经知道系统主密钥，所以他可以计算出每个用户的部分私钥，但是不可以替换用户的公钥。在实际应用中 A_I 模拟的是除 PKG 之外的攻击者，A_{II} 模拟的是恶意 PKG 的非法攻击。本文提出的无证书签密方案，同样要求体制在第一类攻击者 A_I 和第 2 类攻击者 A_{II} 下都满足机密性和不可伪造性。

2.2 复杂性假设

设 p, q 是 2 个素数且 $q \mid (p-1)$，设 G 是 $\mathbb{Z}_p^*$ 的一个阶为 q 的子群，g 是 G 的生成元，本文首先假设在 G 中的下列问题是难解的：

(1)离散对数问题(DLP)：给定元素 $\beta \in G$，寻找整数 $a \in \mathbb{Z}_q$，使得 $\beta = g^a \pmod p$。

(2)计算 Diffie-Hellman 问题(CDHP)：对 $a,b \in \mathbb{Z}_q^*$，已知 (g, g^a, g^b)，要计算 $g^{ab} \pmod p$。

3 本文提出的不含双线性对的无证书签密方案

本文提出的不含双线性对运算的无证书签密方案具体如下：

(1)系统建立：输入安全参数 k，产生 2 个素数 $p, q > 2^k$ 且

基金项目：国家自然科学基金资助项目(60673081)；国家 863 ”计划基金资助项目(2006AA01Z417)

作者简介：葛爱军(1985－)，男，硕士研究生，主研方向：信息安全，数字签名；陈少真，教授

收稿日期：2010-02-20 **E-mail：**geaijun@163.com

$q|(p-1)$。随机选 $\mathbb{Z}_p^*$ 的一个阶为 q 的生成元 g，由 g 生成的子群记为 G。PKG 任意选主密钥 $x\in\mathbb{Z}_q^*$ 并计算 $y=g^x(\mathrm{mod}\,p)$。选择 3 个 Hash 函数：$H_1:\{0,1\}^*\times\mathbb{Z}_p^*\to\mathbb{Z}_q$，$H_2:\{0,1\}^l\times(\mathbb{Z}_p^*)^7\to\mathbb{Z}_q$，$H_3:\mathbb{Z}_p^*\times\mathbb{Z}_p^*\to\{0,1\}^l$，其中，$l$ 为消息的长度。

系统公开参数 $params=(p,q,g,G,y,H_1,H_2,H_3)$，主密钥 $msk=x$。

(2)密钥提取：给定一用户身份为 ID，PKG 随机选择 $s\in\mathbb{Z}_q^*$，计算该用户的部分公钥 $P_{ID}=w=g^s(\mathrm{mod}\,p)$，部分私钥 $D_{ID}=t=s+xH_1(ID,w)(\mathrm{mod}\,q)$，用户接收到 (P_{ID},D_{ID}) 后，首先验证 $g^{D_{ID}}\stackrel{?}{=}P_{ID}\cdot y^{H_1(ID,P_{ID})}$。若验证通过，用户再计算 $\mu_{ID}=g^{z_{ID}}(\mathrm{mod}\,p)$，其中，$z_{ID}\in\mathbb{Z}_q^*$ 是用户自己随机选的秘密值；否则，用户输出拒绝。最后算法输出用户的公钥 $PK_{ID}=(P_{ID},\mu_{ID})$，用户的私钥 $SK_{ID}=(D_{ID},z_{ID})$。

(3)签密算法: 输入消息 m (其长度为 l)，假设接收者 *Bob* 的公钥 $PK_B=(w_B,\mu_B)$，签密者 *Alice* 利用自己私钥 $SK_A=(t_A,z_A)$ 进行如下签密：

1)随机选择 $r_1,r_2\in_R\mathbb{Z}_q^*$，计算

$c_1=g^{r_1}(\mathrm{mod}\,p)$，$c_2=g^{r_2}(\mathrm{mod}\,p)$

2)令 $u=H_2(m,(w_By^{H_1(ID_B,w_B)})^{r_1},(\mu_B)^{r_1},c_2,PK_A,PK_B)$，计算

$v_1=r_1-uz_A(\mathrm{mod}\,q)$，$v_2=r_2-ut_A(\mathrm{mod}\,q)$

3)计算 $c=m\oplus H_3((\mu_B)^{r_1},(w_By^{H_1(ID_B,w_B)})^{r_1})$

最后 *Alice* 发送密文 $\sigma=(u,v_1,v_2,c)$ 给接收者 *Bob*。

(4)解签密算法：接收到签密文 $\sigma=(u,v_1,v_2,c)$ 之后，*Bob* 利用自己的私钥进行如下签密：

1)解密消息 $m=H_3((g^{v_1}\mu_A{}^u)^{z_B},(g^{v_1}\mu_A{}^u)^{t_B})\oplus c$；

2)验证 $u=H_2(m,(g^{v_1}\mu_A{}^u)^{t_B},(g^{v_1}\mu_A{}^u)^{z_B},(g^{v_2}w_Ay^{H_1(ID_A,w_A)})^u,PK_A,PK_B)$ 是否成立，如果等式成立，*Bob* 接受该消息，否则输出“拒绝”。

4 本文方案分析

方案的正确性显然成立，以下讨论机密性和不可伪造性。

4.1 机密性

定理 1 在随机预言模型且计算 Diffie-Hellman 问题难解的情况下，本文提出的无证书签密方案在第一类攻击类型和第 2 类攻击类型均满足机密性。

证明：因为本签密方案的加密思想与文献[6]中无证书加密体制一致，这样签密文的机密性可以等同于文献[6]中无证书加密体制的密文不可区分性：如果敌手能够解密一个有效的签密文，那么就可以规约到该敌手可以有效地攻击文献[6]中的无证书加密方案，又因为文献[6]中无证书加密体制在第 1 类攻击类型和第 2 类攻击类型都被证明是安全的，所以我们的签密方案在第 1 类攻击类型和第 2 类攻击类型下都满足机密性。具体证明参见文献[6]。

4.2 不可伪造性

本文无证书签密方案满足不可伪造性，这由以下 2 个定理来保证。

定理 2 在随机预言模型且离散对数问题难解的情况下，本文的无证书签密方案在第 1 类攻击类型选择消息攻击下是存在性不可伪造的。

定理 3 在随机预言模型且离散对数问题是难解的情况下，本文无证书签密方案在第 2 类攻击类型选择消息攻击下仍然是存在不可伪造的。

其中，定理 3 的证明与定理 2 的思想大致相同，篇幅所限，这里仅给出定理 2 的完整证明如下：

证明：设 A_I 是一个第一类攻击者，给定算法 B 一个离散对数难题实例(g，$\beta=g^a$)，以下将演示算法 B 如何利用 A_I 来求解 a，进而解决离散对数难题。

算法 B 先运行 Setup 算法产生系统参数 $params=(p,q,g,G,y,H_1,H_2,H_3)$，其中，$y=g^x$，$B$ 返回 $params$ 给 A_I 并秘密保存主密钥 x。B 与 A_I 进行如下模拟算法：

(1)生成用户请求

假设 A_I 最多 q_{CU} 次用户生成请求，B 随机选择 $l\in[1,q_{CU}]$，记 $ID_l=ID^*$。对应 A_I 的第 i 次用户 ID_i 生成请求，如果 $ID_i\neq ID^*$，则 B 随机选择 $s_i,e_i,z_i\in\mathbb{Z}_q^*$，计算 $w_i=g^{s_i}(\mathrm{mod}\,p)$，$t_i=s_i+x\cdot e_i\,(\mathrm{mod}\,q)$，$\mu_i=g^{z_i}\,(\mathrm{mod}\,p)$。$B$ 添加 $<(ID_i,w_i),e_i>$ 到列表 L_1（L_1 用来追踪对预言机 H_1 的询问）；如果 $ID_i=ID^*$，则 B 随机选择 $z^*\in\mathbb{Z}_q^*$ 并计算 $\mu^*=g^{z^*}(\mathrm{mod}\,p)$，$w^*=\beta(=g^a)$，$t^*="\perp"$(即 B 不能计算对应 ID^* 的部分私钥)。B 添加对应 ID_i 的密钥信息 $(ID_i,D_{ID_i}=t_i,s_{ID_i}=z_i,PK_{ID_i}=(w_i,\mu_i))$ 到列表 L 中。

(2)部分私钥提取询问

A_I 询问对应 ID_i 的部分私钥，如果 $ID_i=ID^*$，则 B 输出“failure”，模拟失败；否则 B 查表 L 并返回 ID_i 的部分密钥 t_i 给 A_I。

(3)秘密值询问

对应 ID_i 的秘密值询问，B 查表 L 并返回 z_i 给 A_I。

(4)公钥替换请求

对 A_I 的公钥替换请求 $\{ID_i,PK'_{ID_i}=(w'_{ID_i},\mu'_{ID_i})\}$，$B$ 将密钥列表 L 中对应身份 ID_i 的公钥 PK_{ID_i} 替换为 PK'_{ID_i}，注意到对应的私钥未变化。

(5)预言机 H_i $(i=1,2,3)$ 询问

A_I 可以在任何时间访问随机预言机 H_i，首先 B 维持一张表 $L_i(i=1,2,3)$，当 A_I 访问预言机 H_i 时，B 在列表 L_i 中查找该值以前是否询问过，若是返回以前定义的值，否则 B 随机选择一个新的值返回给 A_I，并将其添加到相应列表 L_i 中。

(6)解签密询问

假设 A_I 作出解签密询问 (u,v_1,v_2,c,ID_S,ID_R)，其中，ID_S 为发送者的身份；ID_R 为接收者的身份。

1)若 $ID_R\neq ID^*$ 且对应 ID_R 的公钥未被替换时，B 首先查表 L 获得相应 ID_R 的私钥 $SK_{ID_R}=(t_R,z_R)$，然后计算 $k_1=(g^{v_1}\mu_s{}^u)^{t_R}(\mathrm{mod}\,p)$，$k_2=(g^{v_1}\mu_s{}^u)^{z_R}(\mathrm{mod}\,p)$，$B$ 再在对应预言机 H_3 的列表 L_3 中找到对应输入为 (k_1,k_2) 的输出 R，B 接着计算 $(m\,\|\,\sigma_3)=c\oplus R$ 并返回 m 给攻击者 A_I。如果在 L_3 列表中不存在 $<(k_1,k_2),R>$，B 返回“Reject”，意味着 (u,v_1,v_2,c,ID_S,ID_R) 不是一个有效的签密。

2)若 $ID_R=ID^*$ 或者对应 ID_R 的公钥被替换过，则 B 首先在列表 L_1 中找到对应 (ID_R,w_R) 的输出值 e_R，接着寻找 $<(m,\sigma_1),r_1>\in L_2$，$<(m,\sigma_2),r_2>\in L_2$，$<(k_1,k_2),R>\in L_3$，使得下列等式成立：

$c_1 = g^{r_1}$, $c_2 = g^{r_2}$, $c = R \oplus m$, $k_1 = (\mu_R)^{r_1}$, $k_2 = (w_R y^{e_R})^{r_1}$

如果存在相应的值满足上式，则输出 m 作为解密值，否则“Reject”。

(7)签密询问：对 A_I 的每个签密询问 (m, ID_S, ID_R)，其中 ID_S 为发送者的身份，ID_R 为接收者的身份，B 处理如下：

1)若 $ID_S \neq ID^*$ 且对应 ID_S 的公钥未被替换时，那么 B 通过查表 L 可以获得相应 ID_S 的私钥 $SK_{ID_S} = (t_S, z_S)$，然后利用该私钥及接收者 ID_R 的公钥即可完成签密算法。

2)否则，当 $ID_S = ID^*$ 或者对应 ID_S 的公钥被替换过时，B 随机选 $(u, v_1, v_2) \in_R \mathbb{Z}_q^*$，$c \in_R \{0,1\}^l$，并令 $u = H_2(m, (g^{v_1}(\mu_S{}^u))^{t_R}, (g^{v_1}(\mu_S{}^u))^{z_R}, g^{v_2}(w_S y^{H_1(ID_S, w_S)})^u, PK_S, PK_R)$，其中 $PK_{ID_S} = (w_S, \mu_S)$ 为用户 ID_S 在密钥列表 L 的当前公钥。注意到预言机 H_i 都是 B 控制的，所以上述签密询问的每个消息 m 的签密值 (u, v_1, v_2, c) 都能被解密并且能通过验证。

当上述多项式有界次模拟结束后，最终 A_I 以一个不可忽略的概率输出一发送者 ID_S 传送给接收者 ID_R 的有效签密 $\sigma = (u, v_1, v_2, c)$。如果 $ID_S \neq ID^*$，B 返回“Reject”。否则，通过充分利用 Forking 分叉引理[7]，B 可以解决离散对数难题。

B 通过将上述模拟过程重放 2 次，即可得到 2 个有效的签密 $\sigma = (u, v_1, v_2, c)$，$\sigma' = (u', v_1', v_2', c')$，其中，$u \neq u'$。并且满足以下的等式：

$$g^{v_2}(w^* y^{H_1(ID^*, w^*)})^u = g^{v_2'}(w^* y^{H_1(ID^*, w^*)})^{u'}$$

B 可以计算出 $a = \log_g \beta = \log_g(w^*) = ((v_2' - v_2)/(u - u')) - xH_1(ID, \beta)$，进而解决了离散对数难题。

接下来计算 B 解决离散对数难题的成功概率：

假设 A_I 在模拟仿真阶段至多进行了 q_{PPK} 次部分私钥提取询问，则 A_I 不询问对应 ID^* 的部分私钥的概率至少为 $(1-(1/q_{CU}))^{q_{PPK}}$。又 A_I 输出伪造签密 $(\sigma = (u, v_1, v_2, c), ID_S, ID_R)$ 中 $ID_S = ID^*$ 的概率至少为 $(1/q_{CU})$，故 B 解决离散对数的概率为 $Adv_B^{DL} \geq \frac{1}{q_{CU}}(1-\frac{1}{q_{CU}})^{q_{PPK}} Succ_{A_I}^{cma}$，其中，$Succ_{A_I}^{cma}$ 为 A_I 在第 1 类攻击模型下对本文的无证书签密方案选择消息攻击的成功概率。

因此，如果一个第 1 类攻击者 A_I 能以不可忽视的概率 $Succ_{A_I}^{cma}$ 攻击该体制，那么就存在一个算法 B 可以以不可忽视的概率解决离散对数难题，所以基于离散对数困难假设下，本文的无证书签密体制在第一类攻击下是安全的。

5 结束语

本文提出一个不需双线性对运算的无证书签密方案，并且在随机预言模型基于离散对数难题和计算 Diffie-Hellman 难题给出了安全性证明。本文方案在模幂运算增加不是很多的情况下，通过减少双线性对运算数目(与文献[3]相比减少了 6 次对运算，与文献[4]相比减少了 4 次对运算)，从而极大地提高了运算效率。此方案构造简单，在实现上更加接近于传统的 PKI，具有广泛的应用前景。

参考文献

[1] Riyami A S, Paterson K G. Certificateless Public Key Cryptography[C]//Proc. of CRYPT'03. [S. l.]: IEEE Press, 2003.

[2] Zheng Yuliang. Digital Signcryption or How to Achieve Cost[C]// Proc. of CRYPT'97. [S. l.]: IEEE Press, 1997.

[3] Barbosa M, Farshim P. Certificateless Signcryption[C]//Proc. of 2008 ACM Symposium on Information, Computer and Communications Security. [S. l.]: ACM Press, 2008.

[4] Wu Chenhuang, Chen Zhixiong. A New Efficient Certificateless Signcryption Scheme[C]//Proc. of the International Symposium on Information Science and Engineering. [S. l.]: IEEE Press, 2008.

[5] Li Fagen, Masaaki S, Tsuyoshi T. Certificateless Hybrid Signcryption[C]//Proc. of ISPEC'09. [S. l.]: IEEE Press, 2009.

[6] Baek J, Safavi N R, Susilo W. Certificateless Public Key Encryption Without Pairing[C]//Proc. of ISC'05. Wollongong, Australia: [s. n.], 2005.

[7] Pointcheval D, Stern J. Security Arguments for Digital Signature and Blind Signature[J]. Journal of Cryptology, 2000, 13(3): 361-396.

编辑 陈 文

(上接第 146 页)

本算法加密的数据处在 slice 层。加密时该层以下的数据是不需要解码的。文献[3]算法针对的是 DC、AC、MV 等的 VLC 编码，这些数据处在视频的 block 层内，因此，加密必须完全解码视频，而解码是十分耗时的。

本算法加密数据只需要产生伪随机排列，加密过程较快，而文献[3]算法采用传统的 AES 和 DES 等方法加密数据，加密过程较慢。

综上所述，本算法在加密速度上明显优于文献[3]算法。

5.4 对数据压缩率的影响

由于是一一映射加密，因此加密宏块条层起始符后 8 位得到的数值仍然用 8 位表示。加密前后的数据量一样，对数据压缩率没有影响。在对数据压缩率的影响方面，本算法与文献[3]算法是一样的。

6 结束语

本文结合 MPEG 视频标准和保持格式兼容的思想，提出了一种通过加密宏块条竖直位置值的视频加密算法。与文献[3]的算法相比，本文算法是一个简单易行、安全性高、加密数据量少、加密速度快、对数据压缩率无影响的格式兼容的算法。

参考文献

[1] Tang Lei. Methods for Encrypting and Decrypting MPEG Video Data Efficiently[C]//Proceedings of the 4th ACM International Multimedia Conferences. Boston, USA: [s. n.], 1996: 219-230.

[2] Shi Changgui, Wang Sheng-yih. MPEG Video Encryption in Real-time Using Secret Key Cryptography[C]//Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications. Las Vegas, Nevada, USA: [s. n.], 1999: 2822-2828.

[3] Wen Jiangtao, Severa M. A Format-compliant Configurable Encryption Framework for Access Control of Video[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2002, 12(6): 545-557.

[4] ISO. ISO/IEC 13818-2-1995 Information Technology Generic Coding of Moving Pictures and Associated Audio Information: Video[S]. 1995.

[5] Durstenfeld R. Algorithm 235: Random Permutation[J]. Communications of the ACM, 1964, 7(7): 420.

编辑 张 帆