第 35 卷 第 5 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.5 Computer Engineering March 2009
·安全技术· 文章编号：1000—3428(2009)05—0147—03 文献标识码：A 中图分类号：TP309

高效的无证书可公开验证签密方案

王会歌，王彩芬，易 玮，俞惠芳
(西北师范大学数学与信息科学学院，兰州 730070)

摘 要：签密是将签名和加密相结合的一种方案，无证书密码体制实现无公钥证书且没有密钥托管的性质，该文在已有研究的基础上将签密和无证书公钥密码体制结合，实现一种改进的无证书可公开验证签密方案。在随机预言机模型下证明该方案可以抵抗文中定义的 2 种攻击。解签密中的对运算比 Malone-Lee J 的基于身份方案的对运算少 1 次，而且效率更高。

关键词：可公开验证；签密；不可区分选择密文攻击

High Efficiency Certificateless Publicly Verifiable Signcryption Scheme

WANG Hui-ge, WANG Cai-fen, YI Wei, YU Hui-fang
(College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070)

【Abstract】Signcryption is a scheme that combines the signature and the encryption into one. Certificateless cryptosystem realizes the properties of the certificateless, and the key-unescrow. This paper combines the signcryption and certificateless public key cryptosystem on the basis of the existing literature and realizes an improved certificateless publicly verifiable signcryption scheme. Under the random oracle model, it is provable secure against two attackers defined in the paper. The pairings in unsigncryption is less a time than that of Malone-Lee J's ID-based scheme and the efficiency is higher.

【Keywords】publicly verifiable; signcryption; Indistinguishability Chosen Ciphertext Attacks(IND-CCA)

1 概述

传统的加密签名体制通过先签名后加密的方式来保证通信双方的数据同时达到保密性和认证性，其计算量和通信量是两者之和，效率较低。为解决这一问题，文献[1]提出了签密方案，签密的实质是将签名和公钥密码合二为一，不仅可以实现认证性和保密性，而且效率远高于传统的先签名后加密方式。随着签密方案的发展，人们又提出了一些更有效的签密方案[2-3]。

在文献[4]提出的无证书公钥密码学概念中，系统参数由系统初始化，用户的部分私钥由一个可信第三方(KGC)生成，用户使用这个部分私钥和自己生成的秘密值独立地生成自己的公钥和私钥，克服了传统公钥密码学中的证书存在问题，而且消除了基于身份密码学中密钥托管的问题。

本文在文献[2]的基础上提出的一种无证书改进的可公开验证签密方案。文献[2]给出了方案的机密性和不可伪造模型，但文献[5]指出文献[2]的一个微小弱点，且在文献[6]的安全模型基础之上提出一种新的方案。尽管如此，文献[5]仍然是基于身份的密码体制，而本文提出的方案是一种基于无证书的改进的公钥签密方案，该方案在文献[4]提出的安全证明模型中具有机密性和不可伪造性，比文献[2]中的方案少了 1 次对运算，提高了系统的执行效率。

2 预备知识

2.1 双线性对

设 $(G_1,+)$ 和 $(G_2,.)$ 是阶数为 q 的循环群。其中，P 是 G_1 的生成元。$e:G_1\times G_1\to G_2$ 是一个映射，具有如下性质：(1)双线性：对 $a,b\in Z_q^*$，$R,Q\in G_1$ 满足 $e(aR,bQ)^{ab}=e(R,Q)^{ab}$；(2)非退化性：存在 $R,Q\in G_1$，满足 $e(R,Q)\neq 1$；(3)可计算性：对所有 $R,Q\in G_1$，存在有效算法计算 $e(R,Q)$。

满足上述性质的运算 e 称为双线性对。

2.2 复杂性假设

(1) CBDH(Computational Bilinear Diffie-Hellman)问题：对于任意的 $a,b,c\in Z_q^*$，给定 $<P,aP,bP,cP>$ 计算 $e(P,P)^{abc}$。

(2) DBDH(Decisional Bilinear Diffie-Hellman)问题：对于任意的 $a,b,c\in Z_q^*$，给定 $<P,aP,bP,cP>$ 和 $h\in G_2$，判定 $h=e(P,P)^{abc}$ 是否相等。

2.3 无证书签密模型

无证书签密方案的合法参与者包含：私钥生成中心 *KGC*，签密者 *S*，解签密者 *R*。此签密模型由如下 7 个多项式时间算法组成：

(1)系统参数建立算法：由 KGC 完成的概率性多项式时间算法。输入参数 k，输出主密钥 s。计算 $P_{pub}=sP$ 并输出系统参数 *params*。

(2)部分私钥提取算法：由 *KGC* 完成的确定性多项式时间算法。输入 *params*、主密钥 s 和用户的身份 $ID_i\in\{0,1\}^*$。输出用户的部分私钥 D_i。

基金项目：2008 年教育部科学技术研究基金资助重点项目“电子商务协议若干问题研究”(208148)；甘肃省自然科学基金资助项目(3ZS051-A25-042)；甘肃省科技攻关计划基金资助项目(2GS064-A52-035-03)

作者简介：王会歌(1981－)，女，硕士研究生，主研方向：计算机信息安全，密码学；王彩芬，教授、博士生导师；易 玮、俞惠芳，硕士研究生

收稿日期：2008-07-24 **E-mail：**whgexf@163.com

(3)设置秘密值算法：由用户完成的概率性多项式时间算法。输入 *params* 和用户的身份 ID_i，输出用户的秘密值 x_i。

(4)私钥提取算法：一个由用户完成的概率多项式时间算法，输入 *params*、用户的部分私钥 ID_i 和用户的秘密值 x_i，输出用户的私钥 S_i。

(5)公钥提取算法：由用户完成的确定性多项式时间算法。输入 *params*、用户的身份 ID_i 以及用户的秘密值 x_i，输出用户的公钥 PK_i。

(6)签密算法:由签密者 S 完成的概率性多项式时间算法。输入 *params*、消息 m、签密者的私钥 S_S、解签密者的身份 ID_R, PK_R，输出公开可验证签密 SC。

(7)解签密算法：由解签密者完成的确定性多项式时间算法，输入 *params*、签密者的公钥 PK_S、解签密者的私钥 S_R，输出明文 m。如果签密验证通过，输出“接受”，否则输出“拒绝”。

2.4 安全模型

在无证书签密方案中需要同时考虑签密的机密性和不可伪造性。文献[4]中定义了 2 种类型的攻击：(1)攻击者 A_I 能替换用户的公钥，但不能获得主密钥 s，同时 A_I 能够多项式次适应性进行 hash 询问。如果最后 A_I 输出一个在自己选取的新的公钥下有效的消息签密对，且该消息没有进行过签密询问，则敌手 A_{II} 获得成功。(2)攻击者 A_{II} 可以获取主密钥，但不能替换公钥，和 A_I 一样也能多项式次适应性进行 hash 询问。最后 A_{II} 输出一个有效的消息签密对，且该消息没有进行过签密询问，则敌手 A_{II} 获得成功。

3 本文提出的改进方案

(1)系统参数建立(Setup)：KGC 选择 2 个阶数为素数 $q \geqslant 2^k$ 的循环群 G_1, G_2，P 为 G_1 的生成元，双线性对 $e: G_1 \times G_1 \to G_2$，3 个 hash 函数 $H_1: \{0.1\}^* \to G_1^*$，$H_2: \{0,1\}^* \to Z_q^*$，$H_3: Z_q^* \to \{0,1\}^*$。*KGC* 随机选取主密钥 s，并计算 $P_{pub} = sP$，则 $params = < G_1, G_2, e, P, q, H_1, H_2, H_3, P_{pub} >$，主密钥为 s。

(2)部分私钥提取：输入身份 ID_i，其中，$i \in \{S, R\}$。*KGC* 计算 $Q_i = H_1(ID_i)$，输出部分私钥 $D_i = sQ_i$。

(3)设置秘密值：用户随机选择 $x_i \in Z_q^*$，$i \in \{S, R\}$ 作为自己的秘密值。

(4)设置私钥：用户运行此算法，计算自己的私钥 $S_i = x_i D_i = x_i s Q_i$，$i \in \{S, R\}$。

(5)设置公钥：用户运行设置公钥算法，计算自己的公钥为 $PK_i = (X_i, Y_i) = (x_i P, x_i Q_i)$。

(6)签密生成：对于给定的消息 m，签密者 S 运行签密生成算法，计算签密过程如下：

1)随机选取 $a \in Z_q^*$；

2)计算 $U = aP_{pub}$；

3) $r = H_2(U \| m)$；

4) $w = x_S Y_R$；

5) $V = arS_S$；

6) $y = e(w, P_{pub})$；

7) $K = H_3(y)$；

8) $C = K \oplus m$； $SC = (C, U, V)$。

(7)解签密：对于给定的签密 $SC = (C, U, V)$，解签密者 R 运行解签密算法，解签密过程如下：

1)解签密者首先计算 $y = e(S_R, X_S)$；

2) $K = H_3(y)$；

3) $m = K \oplus C$；

4) $r = H_2(U \| m)$；

5)计算 $e(V, P)$ 与 $e(Y_S, U)^r$ 是否相等。如果相等，输出“接受”，否则输出“拒绝”。

4 方案分析

4.1 正确性验证

正确性验证如下：

$$y = e(w, P_{pub}) = e(x_s Y_R, P_{pub}) = e(x_s x_R Q_R, sP) = e(x_R s Q_R, x_s P) = e(S_R, X_S)$$

$$e(V, P) = e(arS_S, P) = e(arx_s sQ_S, P) = e(x_s Q_S, asP)^r = e(Y_S, aP_{pub})^r = e(Y_S, U)^r$$

4.2 可公开验证性

在解签密阶段，当解签密者解出了明文 m 后就可通过计算 $r = H_2(U \| m)$ 来获取 r，在明文已解的情况下签名的公开验证是可行的，这是因为在双线性对等式 $e(V, P) = e(Y_S, U)^r$ 中的参数在此阶段都已经公开，所以可以供任何第三方验证。

4.3 不可伪造性

定理 1 无证书可公开验证签密方案在 2.4 节中定义的 2 种类型的攻击者下是适应性选择密文(INDistinguishability Chosen Ciphertext Attacks, IND-CCA)不可伪造的，前提是 CBDH 问题在 G_1 上是困难的，而且 DBDH 问题在 $G1$ 和 $G2$ 上是困难的。

证明：因为本方案采用的无证书密码体制和文献[7]中的一致，所以签密中签密文的不可伪造性等同于文献[7]中方案密文的不可为造性。具体证明参见文献[7]。

4.4 不可否认性

因为在解签密阶段，恢复用户的加密密钥 $y = e(S_R, X_S)$ 要用到签密者的公钥 X_S，在签名验证阶段的 $e(V, P) = e(Y_S, U)^r$ 中也要用到签密者的公钥(否则无法恢复签密)，且上述已证明了本文的方案是不可伪造的，所以签密者无法否认自己的签密。因此，该方案满足不可否认性。

4.5 机密性

定理 2 设 H_1, H_2, H_3 是随机预言机，并设本文的方案是选择密文不可伪造的，那么如果在 DBDH 和 CBDH 是难解的前提下，本文的方案在无证书公钥密码体制下是 IND-CCA 安全的。假设 A 是一个多项式有界的 IND-CCA 攻击者，他在时间 t 内以优势 ε 并且做至多 q_{sc} 次签密询问，q_{usc} 次解签密询问，并分别对随机预言机 H_1, H_2, H_3 做至多 $q_{H_1}, q_{H_2}, q_{H_3}$ 次询问，则存在一个多项式有界算法 B 能在时间 $t' \leqslant 120\,686 q_{H_1} q_{H_2} q_{H_3} t / \varepsilon$ 内以优势 $\varepsilon > 10 q_{H_1}(q_S + 1)(q_S + q_{H_2})(q_S + q_{H_3}) / q$ (数据详见文献[8])解决 DBDH 和 CBDH 问题。

证明：一旦 B 接收到了 BDH 问题的一个随机实例 $< P, aP, bP, cP >$，就必须计算形如 $e(P, P)^{abc}$ 的值。对于某些未知的 $a, b, c \in Z_q^*$，首先 B 令 $P_{pub} = cP$ (暗含 $s = c$)，类型 1 攻击者 A_I 选择 2 个消息 m_0, m_1，并分别选取 2 个用户 S 和 R，A_I 向 B 发出签密请求。B 随机选择 $x_R \in Z_q^*$，并设置 $x_R = b$，$Q_R = aP$，则用户 R 的公钥为 $PK_R = (x_R P, x_R Q_R) = (bP, bQ_R)$，且 B 随机选择 $x_S \in Z_q^*$，令 $PK_S = (x_S P, x_S Q_S)$，B 将这些参数

发送给 A_I，然后 B 随机选择 $i \in \{0,1\}$ 和 $x \in Z_q^*$，用新的公钥 $PK_S = (X,Y) = (xP, xQ_S)$ 替换 S 的公钥 $PK_S = (X_S, Y_S)$，然后运行签密算法对 m_i 进行签密，并把签密文 SC^* 发送给 A_I，A_I 根据签密文猜测出 i^*，若 $i^* = i$ (概率为 ε)，B 就可以计算出 $y = e(S_R, X_S) = e(x_R sQ_R, x_S P) = e(bcQ_R, xP) = e(P,P)^{abcx}$，因为 B 知道 x，所以很容易计算出 $e(P,P)^{abc}$，B 就可以利用 y 以及相应的密文求出相应的明文 m_i，使 A_I 相信其对应的明文为 m_i，若 $i^* \neq i$，B 就认为 $y \neq e(P,P)^{abcx}$，这样 B 就解决了 DBDH 问题，则 CBDH 问题也就相应解决了。

对于类型 2 攻击者 A_{II} 同样可以解 DBDH 问题。一旦 B 接收到了 BDH 问题的一个随机实例 $< P, aP, bP, cP >$ 就必须计算形如 $e(P,P)^{abc}$ 的值。因为攻击者 A_{II} 可以拥有主密钥 s，所以这里的证明过程和上述的证明过程不完全相同。

证明：对于某些未知的 $a,b,c \in Z_q^*$，B 设置 $Q_R = aP$，$Y_R = bQ_R$，$X_S = cP$，然后 B 运行 Setup，并随机选择 $s \in Z_q^*$，计算 $P_{pub} = sP$。B 将这些参数发送给 A_{II} 并选择 $i \in \{0,1\}$，运行签密算法对 m_i 签密，并把签密文 SC^* 发送给 A_{II}，A_{II} 根据签密文猜测出 i^*，若 $i^* = i$ (概率为 ε)，B 就可以计算出 $y = e(S_R, X_S) = e(sY_R, X_S) = e(sabP, cP) = e(P,P)^{abcs}$，并结合给定的密文就可以解出 m_i，对于此实例中的指数 s，因为 A_{II} 知道主密钥 s，所以 B 就可很容易地计算出 $e(P,P)^{abc}$。B 就可利用 y 以及相应的密文求出相应的明文 m_i，使 A_{II} 相信其对应的明文为 m_i，若 $i^* \neq i$ (概率为 ε)，B 就认为 $y \neq e(P,P)^{abcs}$，这样 B 就解决了 DBDH 问题，则 CBDH 问题也就相应解决。

4.6 效率分析

本文方案和文献[2]方案的效率比较如表 1 所示。

表 1 效率比较

操作类型	本文方案		文献[2]的方案	
	签密	解签密	签密	解签密
对估计	1	3	1	4
乘运算	3	0	3	0
指数运算	0	1	0	1
有无密钥托管	无	无	有	有

可以看出，与文献[2]的方案相比，本文方案减少了 1 次对运算，而且本文方案是无证书的，解决了基于身份中的密钥托管问题，便于实际应用。

5 结束语

本文在无公钥证书的基础上提出一种高效的可公开验证的签密方案，给出该方案的正确性证明，并在随机预言机下证明了该方案的不可伪造性，在 DBDH 和 CBDH 问题难解的前提下证明了该方案的机密性。分析表明，本文的方案与文献[2]的方案相比效率更高，且克服了文献[2]中的密钥托管问题，是一种高效的无证书签密方案。

参考文献

[1] Zheng Yuliang. Digital Signcryption or How to Achieve Cost (Signature & Encryption)≤Cost(Signature)+Cost(Encryption)[C]// Proc. of CRYPTO'97. New York, USA: Springer-Verlag, 1997.

[2] Malone-Lee J. Identity-based Signcryption[Z]. (2002-01-01). http://eprint.iacr.org/2002/098.

[3] Chen Liqun, Malone-Lee J. Improved Identity-based Signcryption[C]//Proc. of PKC'05. [S. l.]: Springer-Verlag, 2005.

[4] Al-Riyami S S, Paterson K. Certificateless Public Key Cryptography[C]//Proc. of Asiacrypt'03. [S. l.]: Springer-Verlag, 2003.

[5] Libertand B, Quisquater J. New Identity-based Signcryption Schemes from Pairings[C]//Proc. of IEEE Information Theory Workshop. Paris, France: [s. n.], 2003.

[6] Boyen X. Multipurpose Identity-based Signcryption: A Swiss Army Knife for Identity-based Cryptography[C]//Proc. of CRYPTO'03. Berlin, Germany: Springer-Verlag, 2003.

[7] Lee R Y, Lee H S. An Authenticated Certificateless Public Key Encryption Scheme[Z]. [2008-04-14]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.58.3580.

[8] Pointcheval D, Stern J. Security Proofs for Signature Schemes[C]// Proceedings of Eurocrypt'96. Saragossa, Spain: [s. n.], 1996.

编辑 顾姣健

（上接第 138 页）

参考文献

[1] 金康双, 王泽兵, 冯 雁, 等. SIP 协议的认证机制及其性能分析[J]. 计算机应用研究, 2004, 21(8): 110-112.

[2] 万晓榆, 樊自甫, 宗晓飞. 下一代网络安全技术[M]. 北京: 人民邮电出版社, 2007.

[3] Potlapally N, Raghunathan A. A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols[J]. IEEE Transactions on Mobile Computing, 2006, 5(2): 128-143.

[4] 闵 涵, 陈莘萌, 张琦辉. 基于 SIP 协议的网络安全性分析[J]. 计算机工程与设计, 2004, 25(3): 386-389.

编辑 顾姣健

（上接第 146 页）

参考文献

[1] Ker A D. Steganalysis of LSB Matching in Grayscale Images[J]. IEEE Signal Processing Letters, 2005, 12(6): 441-444.

[2] 张 涛, 平西建. 针对一类信息伪装算法的隐藏信息检测[J]. 通信学报, 2002, 23(5): 123-129.

[3] 施智平, 胡 宏, 李清勇, 等. 到基于纹理谱描述的图像检索[J]. 软件学报, 2005, 16(6): 1039-1045.

[4] Wong Ping, Chen Hong, Tang Zhongjue. On Steganalysis of Plus-Minus One Embedding of Continuous Tone Images[C]//Proc. of Conf. on SPIE-IS&T Electronic Imaging. [S. l.]: IEEE Press, 2005.

[5] Groundtruth Imagedatabase[Z]. [2008-02-25]. http://www.cs.washington.edu/research/imagedatabase/groundtruth/.

编辑 张 帆