无证书的可验证签密方案

周 敏[1], 姚金涛[1], 万军洲[1], 巫莉莉[2]
(1 华南农业大学 信息学院,广东 广州 510642;2 华南农业大学 现代教育技术中心,广东 广州 510642)

摘要:签密是把加密和签名结合起来,能实现数据的机密性和认证性. 无证书密码体制实现无公钥证书且没有密钥托管的性质. 本文提出的方案是一种基于无证书的公钥可验证签密方案,该方案在 Al-Riyami 提出的安全证明模型中具有机密性和不可伪造性.

关键词:无证书签密; 不可伪造; 机密性; 可验证
中图分类号:TP309 **文献标志码**:A **文章编号**:1001-411X(2011)04-0110-03

The Certificateless Verifiable Signcryption Scheme

ZHOU Min[1], YAO Jin-tao[1], WAN Jun-zhou[1], WU Li-li[2]
(1 College of Informatics, South China Agricultural University, Guangzhou 510642, China;
2 Modern Education Technology Center, South China Agricultural University, Guangzhou 510642, China)

Abstract: Signcryption combines the signature and the encryption into one, and implements data confidentiality and authentication. Certificateless cryptosystem realizes the properties of the certificateless and the key-unescrow. So certificateless verifiable signcryption was proposed. The confidentiality and unforgeability of this scheme was proved under the secure model mentioned by Al-Riyam.

Key words: certificateless signcryption; unforgeability; confidentiality; verifiable

为了达到数据的机密性和认证性. 传统的方法是采用先签名后加密的方法,其运算代价是两者之和,效率比较低. 1997 年 Zheng[1] 首先提出了签密的概念(Signcryption),其主要思想是把加密系统和签名系统的功能结合起来,能在逻辑上同时实现数据的机密性和认证性,但是比传统的先签名后加密(Signature then encryption)的方法效率高.

签密的高效性使其得到了广泛的关注,近年来,有许多签密方案提出来. 但是,由于被签密的消息在签名的同时也被加密,不能像一般签名那样被公开验证. 1998 年 Feng 等[2] 以 Zheng 的签密方案为基础,提出了一种签名可公开验证的签密方案,即 BD 签密方案. 2000 年 Lee 等[3] 基于前人[4] 中的认证加密方案提出了一种可公开验证的签密方案,简称 Lee 方案. 张串绒等[5] 对 Lee 方案进行密码分析研究,发现了其中存在的安全问题,并给出了一个改进方案,简称 Zhang 方案. 2002 年 Malone-Lee[6] 定义了基于身份的签密方案的安全模型,利用双线性对构造了第一个基于身份的签密方案. 该模型能处理消息的机密性和签名的不可伪造性.

1978 年 Rivest 等[7] 第一次提出公钥加密方案. 1984 年 Shamir[8] 引进了基于身份的密码学 IDPKC 的概念. IDPKC 消除了对用户证书的依赖,极大地简化了密钥管理问题. 2003 年 Al-Riyami 等[9] 提出了基于无证书的公钥加密方案,系统参数由系统初始化,用户的部分私钥由一个可信密钥生成中心(KGC)生成,用户使用这个部分秘密钥和自己生成的秘密值独立地生成自己的公钥和秘密钥. 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.

收稿日期:2010-09-17
作者简介:周 敏(1973—),女,副教授,博士研究生,E-mail: zmfw@scau.edu.cn
基金项目:国家自然科学基金(60973134);广东省自然科学基金(9151064201000058,10351806001000000)

本文提出的方案是一种基于无证书的公钥签密方案,该方案在 Al-Riyami 提出的安全证明模型中具有机密性和不可伪造性.

1　基于无证书的可验证签密方案

1.1　系统参数建立

给定(G_1,G_2,q,e,P)随机参数$s\in\mathbb{Z}_q^*$并置$P_{pub}=sP$. 选择3个Hash函数$H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\times\mathbb{G}_2\rightarrow\mathbb{Z}_q$以及$H_3:\mathbb{G}_2\rightarrow\mathbb{Z}_q$. 系统公开的参数$(G_1,G_2,q,e,P,P_{pub},H_1,H_2,H_3)$. 系统的主密钥为$s$.

1.2　提取部分私钥

身份$ID_i\in\{0,1\}^*$作为输入,KGC计算$Q_i=H_1(ID_i)\in\mathbb{G}_1$,输出部分私钥$D_i$,$D_i=sQ_i\in\mathbb{G}_1$.

1.3　密钥产生

1)设置秘密值:用户随机选取$x_i\in\mathbb{Z}_q^*$作为自己的秘密值;

2)设置秘密钥:用户计算自己的私钥,$S_i=x_iD_i=x_isQ_i$;

3)设置公开钥:用户计算自己的公钥$PK_i=(X_i,Y_i)=(x_iQ_i,x_iP)$.

1.4　签密

给定签密者私钥S_S,消息$m\in\{0,1\}^*$,执行以下步骤:

1)随机选取$k\in\mathbb{Z}_q^*$;

2)计算$a=x_SX_R$,$b=e(a,P_{pub})$,其中x_S是签密者的密值,X_R代表接收者的公开钥;

3)计算$r=e(P,P)^k$,$h=H_2(m,r)$,$h'=H_3(b)$;

4)计算$U=hS_S+kP$,$C=h'\oplus m$;

5)输出无证书的可验证签密(r,C,U).

1.5　解签密

给定身份ID_S的密值x_S的签名者对于消息m的无证书的可验证签密(C,r,U).

1)计算$b=e(S_R,Y_S)$,其中S_R代表接收者的秘密钥,Y_S代表签密者的公开钥;

2)$h'=H_3(b)$;

3)$m=C\oplus h'$;

4)计算$h=H_2(m,r)$,$Q_S=H_1(ID_S)$;

5)当且仅当$r=e(U,P)\cdot e(X_S,P_{pub})^{-h}$,接受,否则拒绝.

2　基于无证书的可验证签密方案的正确性和安全性证明

2.1　正确性

接收者接收签名,因为用双线性对的性质可以证明下列等式成立.

$b=e(S_R,Y_S)=e(x_RsQ_R,x_SP)=e(sX_R,x_SP)=e(x_SX_R,sP)=e(a,P_{pub})$.

$e(U,P)\cdot e(X_S,P_{pub})^{-h}=e(U,P)\cdot e(x_SQ_S,sP)^{-h}=e(U,P)\cdot e(x_SsQ_S,P)^{-h}=e(hS_S+kP,P)\cdot e(S_S,P)^{-h}=e(hS_S+kP,P)\cdot e(-hS_S,P)=e(kP,P)=e(P,P)^k=r$.

2.2　不可伪造性

定理1　无证书可验证签密方案在文献[9]定义的2种类型攻击下是适应性选择密文不可伪造的(Indistinguishability chosen ciphertext attacks, IND-CCA). 前提是CBDH和DBDH是困难的.

证明　因为本方案采用的无证书密码体制和文献[10]中的一致,所以不可伪造性等同于文献[10]中方案的不可伪造性. 具体证明参见文献[10].

2.3　不可否认性

因为在解签密阶段,恢复$b=e(S_R,Y_S)$要用到签密者的公钥,在签名验证阶段的$r=e(U,P)\cdot e(X_S,P_{pub})^{-h}$中也要用到签密者的公钥$X_S$,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.

2.4　机密性

定理2　本文的方案在无证书公钥密码体制下是IND-CCA安全的,前提是DBDH和CBDH是难解的.

证明　假设A是一个多项式有界IND-CCA的攻击者,B是多项式有界算法,S代表签密者,R代表接受者.

1)对于类型1,对未知的$k_1,k_2,k_3\in\mathbb{Z}_q^*$,令$P_{pub}=k_1P$(此处$k_1$相当于主密钥$s$). B随机选择$x_R\in\mathbb{Z}_q^*$,并$x_R=k_2$,则用户R公钥为$PK_R=(X_R,Y_R)=(x_RQ_R,x_RP)$并置$Q_R=k_3P$;随机选择$x_S\in\mathbb{Z}_q^*$,则用户S公钥为$PK_S=(X_S,Y_S)=(x_SQ_S,x_SP)$. B将这些参数发送给攻击者A. B随机选取$x\in\mathbb{Z}_q^*$,用新的公钥$PK_S=(X,Y)=(xQ_S,xP)$替换S的公钥$PK_S=(x_SQ_S,x_SP)$,攻击者A选择2个消息$m_1,m_2\in\{0,1\}^*$,攻击者A向B(多项式有界算法)发出签密请求. 然后B随机选择$i\in\{0,1\}$运行签密算法对m_i进行签密,并把签密发送给攻击者A,攻击者A根据签密猜测出i^*,若$i^*=i$,B就可以计算出$b=e(S_R,Y)=e(x_RsQ_R,xP)=e(k_2k_1k_3P,xP)=e(P,P)^{k_1k_2k_3x}$,因为B知道$x$,所以很容易计算出$e(P,P)^{k_1k_2k_3}$,B就可以利用$b$以及相应的密文求出相应的明文$m_i$,使攻击者A相信其对应的明文为$m_i$. 若$i^*\neq i$,B就认为$b\neq$

$e(P,P)^{k_1k_2k_3x}$,这样 B 就解决了 DBDH 问题,则 CBDH 问题也就相应解决了. 与假设矛盾.

2)对于类型 2,攻击者 A 可以拥有主密钥 s. 对于未知的 $k_1, k_2, k_3 \in \mathbb{Z}_q$, B 设置 $Q_R = k_3P$, $X_R = k_2Q_R$, $Y_S = k_1P$,然后 B 运行 Setup,并随机选择 $s \in \mathbb{Z}_q^*$,计算 $P_{pub} = sP$. B 将这些参数发送给攻击者 A,并随机选择 $i \in \{0,1\}$,运行签密算法对 m_i 签密,并把签密发送给攻击者 A,攻击者 A 根据签密文猜测出 i^*,若 $i^* = i$,B 就可以计算出 $b = e(S_R, Y_S) = e(x_R sQ_R, Y_S) = e(sX_R, k_1P) = e(sk_2Q_R, k_1P) = e(sk_2k_3P, k_1P) = e(P,P)^{k_1k_2k_3s}$,并结合给定的密文就可以解出 m_i,因为攻击者 A 知道主密钥 s,所以 B 就可很容易地计算出 $e(P,P)^{k_1k_2k_3}$. B 就可利用 b 以及相应的密文求出相应的明文 m_i,使攻击者相信其对应的明文为 m_i,若 $i^* \neq i$,B 就认为 $b \neq e(P,P)^{k_1k_2k_3s}$,这样 B 就解决了 DBDH 问题,则 CBDH 问题也就相应解决. 与假设矛盾.

综合 1)和 2),本方案在无证书公钥密码体制下是 IND-CCA 安全的.

2.5 可公开验证

在解签密阶段,当接收者解出了 $b = e(S_R, Y_S)$,就可通过计算 $h' = H_3(b)$来获取明文 m. 在解出明文的情况下签名是可公开验证的,这是因为在等式 $r = e(U,P) \cdot e(X_S, P_{pub})^{-h}$中的参数都已经公开,所以可以供任何第三方验证.

2.6 效率分析

本方案和文献[6]方案的效率比较如表 1 所示. 本方案最大的特点就是消除了基于身份密码学中密钥托管的问题.

表 1 方案效率比较

Tab.1 Comparison of Scheme's Efficiency 次

操作	本文方案		文献[6]的方案	
	签密	解签密	签密	解签密
对运算	2	3	1	4
乘运算	3	0	3	0
指数运算	1	1	0	1
有无密钥托管	无	无	有	有

3 小结

本文在无公钥证书的基础上提出一种可公开验证的签密方案,给出该方案的正确性证明,并在 DBDH 和 CBDH 问题难解的前提下证明了该方案的不可伪造性和机密性. 该方案还具有可公开验证性.

参考文献:

[1] ZHENG Yu-liang. Digital signcryption or how to achieve cost(signature & encryption) ≤ cost (signature) + cost (encryption)[J]. LNCS, 1997(1294):165-179.

[2] FENG Bao, ROBERT H D. A signcryption scheme with signature directly verifiable by public key[J]. LNCS, 1998(1431):55-59.

[3] LEE M K, KIM D K, PARK K. An authenticated encryption scheme with public verifiability[M] // Anon. 5th Japan Korea Joint Workshop on Algorithms and Computation. Tokyo:IEEE,2000: 49-56.

[4] HORSTER P, MICHELS M, PETERSEN H. Authenticated encryption schemes with low communication costs[J]. Electronics Letters,1994,30(15):1212-1213.

[5] 张串绒,肖国镇. 一个可公开验证签密方案的密码分析和改进[J]. 电子学报,2006,34(1): 177-179.

[6] MALONE-LEE J. Identity based signcryption[EB/OL]. [2010-08-20]. http://eprint.iacr.org/2002/098.pdf.

[7] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2):120-126.

[8] SHAMIR A. Identity based cryptosystems and signature schemes[J]. LNCS,1985(196):47-53.

[9] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[J]. LNCS,2003(2894):452-473.

[10] LEE Y R, LEE H S. An authenticated certificateless public key encryption scheme[J]. Information Center for Mathematical Sciences,2005,8(1):177-187.

【责任编辑 周志红】