无双线性对的可撤销的无证书加密

孙银霞[1],刘 静[2]

(1.南京师范大学计算机科学与技术学院,江苏 南京 210023)
(2.江苏联合职业技术学院,江苏 徐州 221008)

[摘要] 无证书公钥密码体制既克服了基于身份的公钥体制的密钥托管问题,又不需要像传统公钥体制那样管理公钥证书,是目前的研究热点.而对于任何公钥密码体制,如何撤销一个用户是必须解决的问题.然而,目前对无证书系统的撤销问题还缺乏理想的解决方案.本文基于无证书加密,提出了1种高效的无证书系统的撤销方法,构造了1个具体的可撤销的无证书加密方案.该方案不需要计算双线性对,密钥的更新在公共信道上就可以完成,所以我们的方案在效率方面远远优于现有方案.在安全性方面,本文的方案达到了CCA2安全.

[关键词] 撤销,无证书签名,无双线性对
[中图分类号]TP309 [文献标志码]A [文章编号]1001-4616(2015)04-0052-05

Revocable Certificateless Encryption Without Bilinear Pairing

Sun Yinxia[1],Liu Jing[2]

(1.School of Computer Science and Technology,Nanjing Normal University,Nanjing 210023,China)
(2.Jiangsu Union Technical Institute,Xuzhou 221008,China)

Abstract:Certificateless public key cryptosystem,without certificate and key escrow problem,has received wide attention. For a public key cryptosystem,how to revoke a user is a necessary problem to be addressed. However,there still lacks good method to solve the revocation problem in certificateless setting. Based on certificateless encryption,this paper presents a revocation method by constructing a revocable certificateless encryption scheme. Our scheme does not need any bilinear pairing,and the key-update is done via public channels. So,our scheme is more efficient than the existing solutions. The new scheme reaches CCA2 security.

Key words:revocable,certificateless encryption,without bilinear pairing

公钥密码学的发明是密码学史又一新的起点,它为解决日益突出的信息安全问题提供了新的思路和技术,使密钥分配变得十分简单.在公钥密码系统里,首先需要解决的是公钥的认证问题.传统的公钥系统通过公钥证书来实现认证,不足是公钥证书管理需要非常大的开销.1984年,著名的密码学家Shamir[1]提出了基于身份的公钥密码系统(identity based public key cryptography,IBPKC)的概念,该系统使用用户唯一的身份作为公钥,比如手机号、IP地址和Email地址,从而消除了管理公钥证书的任务.IBPKC的用户私钥是由系统的私钥生成器(PKG)来生成的,这导致PKG掌握了所有用户私钥,它可以解密任何用户的密文,以及代表任何用户进行签名.这种密钥托管问题在一些实际应用中是不被接受的.于是在2003年,Al-Riyami和Paterson[2]这两位学者综合了前两种公钥系统的优点,提出了无证书公钥密码系统(certificateless public key cryptography,CLPKC).CLPKC的用户私钥的生成采用的方法是,一部分由系统的密钥生成中心(KGC)生成,另一部分则由用户自己选取,从而巧妙地解决了证书管理问题和密钥托管问题,虽然在算法上略微增加了一些计算量,然而在一些实际应用环境中能取得比前两种公钥系统更好的效果.

任何公钥系统都必须解决用户的撤销问题.在传统公钥系统中,撤销技术较成熟,有撤销列表CRLs、

收稿日期:2015-02-16.
基金项目:江苏省自然科学基金青年基金(BK20130908)、江苏省高校自然科学基金(13KJD520006)、国家自然科学基金(61170298)、南京师范大学科研基金(2012119XGQ181).
通讯联系人:刘静,讲师,研究方向:网络与信息安全.E-mail:41477341@qq.com

在线证书状态协议OCSP和Novomodo[3]等.但是在没有证书的公钥系统中,用户的撤销却变得更为复杂.根据基于身份的和无证书的公钥系统的特点,目前的撤销技术主要是通过系统为用户更新密钥来实现,这也是最初Boneh-Franklin[5]和AlRiyami-Paterson[2]在他们的论文中提到的撤销技术.这种方法原理简单,但实际操作消耗的计算资源较多,因为每次更新的密钥都必须通过秘密信道传递,而秘密信道的建立意味着大的计算和通信开销.目前对基于身份的公钥系统,这一问题已有不少解决方案[5-6],Boldyreva等人[5]设计的可撤销的基于身份的加密方案具有可扩展性,减轻了PKG的负担,随后Libert和Vergnaud[8]对该方案作了改进,提高了安全性.其它的相关方案有比如参考文献[8-10]的方案.在PKC2013上,Seo等人[11]又进一步探讨了应对解密密钥泄露威胁的措施.

然而,对无证书公钥系统下的撤销问题的研究却相对较少,所以研究高效的可撤销的无证书密码方案具有重要的理论和实际意义.Al-Riyami在参考文献[2,12]中提到的撤销方法是定期为用户更新部分私钥.这依赖于秘密信道,并不具备很好的实用性.尽管最近Limin Shen等人[13]提出了新的无证书撤销方案,但是他们的方案存在安全漏洞.近期,我们也设计了1个标准模型下的可撤销的无证书加密方案[14].

本论文构造1个无双线性对的可撤销的无证书加密方案.用户的部分私钥和时间密钥采用Schnnor签名算法,KGC定期给所有未被撤销的用户更新密钥,这些更新的时间密钥通过公开信道传输.当系统需要撤销某个用户时,它就停止为该用户生成新的时间密钥.与普通的无证书加密方案相比,本文的方案在获得撤销功能的同时,加密和解密算法在效率方面几乎没有受到影响,KGC增加的计算量是计算时间密钥,这对于计算能力越来越强大的服务器而言是完全具有现实意义的.而对于计算终节点来说,不需要计算复杂的双线性对是一件好事.本文的方案在选择密文攻击下是可证明安全的.

1 预备知识

在给出具体构造之前,先介绍预备知识,包括可撤销的无证书加密的定义、安全模型和基于的数学困难问题.

1.1 可撤销的无证书加密的定义

一个可撤销的无证书加密方案由以下8个算法构成:

(1)建立系统:输入安全参数k,生成1组系统公开参数和1个系统主密钥.

(2)生成部分私钥:该算法由KGC执行,输入1个用户的身份ID,输出该用户的部分私钥D_{ID}.该部分私钥通过秘密信道传输给用户,由用户保存.

(3)生成时间密钥:KGC在每个时间段T,为每个用户生成1个时间密钥$D_{ID,T}$.该时间密钥通过公开信道传输给用户.

(4)生成秘密值:用户选取1个秘密值SV_{ID}.

(5)生成私钥:用户的完整私钥SK_{ID}由用户的部分私钥D_{ID}和秘密值组SV_{ID}成.

(6)生成公钥:输入系统参数和秘密值S_{ID},计算用户ID的公钥为PK_{ID}.

(7)加密:发送者在时间T加密消息M发送给用户ID,输入公钥、时间参数和系统参数,计算并输出密文C.

(8)解密:接收者用私钥、时间密钥解密密文.

1.2 安全模型

本小节讨论可撤销的无证书加密的安全模型.无证书公钥系统存在两类攻击者:第一类攻击者和第二类攻击者.其中,第一类攻击者模拟外部攻击者,能够替换任何用户的公钥;第二类攻击者模拟诚实但好奇的KGC.本论文所讨论的可撤销的无证书加密,还需要考虑恶意的被撤销的用户.

首先给出后面将要用到的"不可忽略"的概念.

定义2.1 如果对于所有的正多项式$h(x)$,总是存在1个整数$N>0$使得当$x>N$,有$f(x)\leqslant 1/h(x)$,则称函数$f(x)$是可忽略的.

下面我们通过攻击者A与挑战者$\mathcal{C}$之间的游戏来定义可撤销的无证书加密的安全性.

游戏:

(1)$(params,msk)\leftarrow\mathcal{C}^{\text{Setup}}(1^k)$

(2)$A^{oracles}(params,inf)$

(3)$(M_0,M_1,ID^*,T^*)\leftarrow A, C^*\leftarrow \mathscr{C}$

(4)$A^{oracles}$

(5)$\beta'\in\{0,1\}\leftarrow A$

如果A为第一类攻击者,那么$inf=\phi$(空集);如果A为第二类攻击者,那么$inf=msk$;如果A为恶意的被撤销的用户,那么$inf=\{D_{ID^*},SV_{ID^*}\}$. 攻击者在阶段(2)和阶段(4)可访问如下预言器(oracles):

部分私钥询问(第一、三类攻击者):攻击者提供1个用户身份ID,挑战者运行"生成部分私钥"算法得到该用户的部分私钥D_{ID},并把D_{ID}返回给攻击者.

时间密钥询问:攻击者询问(ID,T)的时间密钥,挑战者运行"生成时间密钥"算法得到$D_{ID,T}$,并把$D_{ID,T}$返回给攻击者.

秘密值询问:攻击者可以询问任何用户的秘密值,但是不允许询问1个被替换的公钥对应的秘密值.

私钥询问:攻击者可以询问用户的私钥,除了挑战身份对应的私钥.

公钥询问:攻击者可以向挑战者询问每个用户的公钥.

公钥替换:第一类和第三类攻击者可以替换任何用户公钥.

解密询问:攻击者可以询问任何密文的明文. 在阶段(4)不能询问挑战密文的明文.

定义攻击者A在以上游戏中的优势为$2(\Pr[A]-1/2)$. $\Pr[A]$表示A在游戏中获胜的概率.

定义2.2　如果不存在多项式时间的攻击者在以上游戏中以不可忽略的优势获胜,那么称1个可撤销的无证书加密方案在选择密文攻击下是密文不可区分的(IND-CCA2安全).

1.3　计算Diffie-Hellman问题

定义2.3　计算Diffie-Hellman问题(CDH问题):给定$g^a,g^b\in Z_p^*$,其中p是素数,g是群Z_p^*的1个q阶生成元,计算g^{ab}的值.

2　方案的具体构造

本节构造1个无双线性对的可撤销的无证书加密方案,该方案很好地解决了用户撤销问题,同时由于没有双线性对的计算,因此所需计算资源较少,是1种实用的无证书加密方案. 具体由以下8个算法组成:

(1)建立系统:选择两个素数p,q,使得$p=2q+1$,g是Z_p^*的1个q阶元素,随机选取$x\in Z_p^*$,计算$y=g^x\cdot H_1:\{0,1\}^*\rightarrow Z_q^*$.

(2)生成部分私钥:随机选取$r\in Z_p^*$,计算$w_{ID}=g^r, d_{ID}=r+xH_1(ID,w_{ID})$. 输出部分私钥$(w_{ID},d_{ID})$.

(3)生成时间密钥:在时间段T,KGC为用户ID计算时间密钥. 随机选取$r'\in Z_p^*$,计算$w_{ID,T}=g^{r'}$,$d_{ID,T}=r'+xH_2(ID,T,w_{ID,T})$. 输出时间密钥$(w_{ID,T},d_{ID,T})$. 其中$w_{ID,T}$以某种方式公开发布.

(4)生成秘密值:随机选取$v_{ID}\in Z_p^*$作为秘密值.

(5)生成私钥:用户的完整私钥为$SK_{ID}=(d_{ID},v_{ID})$.

(6)生成公钥:用户ID的公钥为$PK_{ID}=(PK_{ID,0},PK_{ID,1})=(g^{v_{ID}},w_{ID})$.

(7)加密:输入用户ID的时间参数T、$w_{ID,T}$、公钥和消息M. 随机选取$\sigma\in\{0,1\}^l$,计算$r=H_3(\sigma,M), U=g^r$以及$V=(\sigma\|M)\oplus H_4(PK_{ID,O}{}^r, w_{ID}{}^r y^{H_1(ID,w_{ID})r}, w_{ID,T}{}^r y^{H_2(ID,w_{ID,T},T)r})$. 输出密文$C=(U,V)$.

(8)解密:对于密文(U,V),输入用户ID的私钥,时间密钥$d_{ID,T}$. 首先计算$\sigma\|M=V\oplus H_4(U^{v_{ID}},U^{d_{ID}},U^{d_{ID,T}})$,计算$r=H_3(\sigma,M)$并验证等式$g^r=U$是否成立:若是,则输出明文$M$;否则输出$\perp$表示解密失败.

3　安全证明和效率分析

3.1　安全性证明

本小节讨论以上方案的安全性,通过定理1,定理2和定理3不难得出结论:本文的方案满足IND-CCA2安全性. 其中我们只详细证明定理2.

定理1 如果存在一个第一类攻击者 A_I,他能以优势 ε 区分两个等长明文的密文,那么就存在一个算法B,能以概率 $\varepsilon' \geq \frac{\varepsilon}{q_4}$ 解决CDH问题.其中, q_4 表示询问随机预言器 H_4 的次数.

定理2 如果存在1个第二类攻击者 A_{II},他能以优势 ε 区分两个等长明文的密文,那么就存在1个算法B,能以概率 $\varepsilon' \geq \frac{\varepsilon}{q_4}$ 解决CDH问题.其中, q_4 表示询问随机预言器 H_4 的次数.

证明 现有算法B,其目的是解决CDH问题,即任意给定 g^a, $g^b \in Z_p$,计算 g^{ab}.B将利用第二类攻击者来解决CDH问题.

首先,B建立系统,随机选取 $x \in Z_p$ 作为系统主密钥,计算 $y=g^x$,系统公共参数为(p,q,y,H_1,H_2,H_3),并把 x 发送给攻击者 A_{II}.

然后 A_{II} 开始攻击,他将作一系列如下询问,并把每个询问—回答记录到相应的列表中. A_{II} 首先选取将要攻击的用户 ID^*.

Hash询问:对 H_1、H_2、H_3 和 H_4 的询问,挑战者从相关的域中随机选取1个值作为回答.

秘密值询问:当 A_{II} 询问某个用户 ID 的秘密值时,若 $ID \neq ID^*$,则B从 Z_q 中随机选取1个元素 v_{ID} 作为对该询问的回答;否则,游戏结束.

公钥询问:对于每个公钥询问 (ID),若 $ID=ID^*$,则B输出公钥 $PK_{ID,0}=g^a$;否则,B先从秘密值列表中找出对应的秘密值 v_{ID},然后计算公钥 $PK_{ID,0}=g^{v_{ID}}$.

解密询问:当 A_{II} 询问 $(C=(U,V),ID,T)$ 的明文时,

(1)如果 $ID \neq ID^*$,则B运行解密算法,并输出结果;

(2)否则,B随机选取一个 $M \in \{0,1\}^n$ 作为回答.

挑战: A_{II} 输出两个等长的明文消息 (M_0,M_1),时间 T^*.B设定 $U^*=g^b$,然后随机选取 $V^* \in \{0,1\}^{n+l}$,输出挑战密文 $C^*=(U^*,V^*)$.

A_{II} 继续如前一阶段作一系列询问,除了 ID^* 的秘密值以及挑战密文的明文.

猜测: A_{II} 输出 $\beta' \in \{0,1\}$.B从 H_4 列表中随机选取1个记录 (u_0,u_1,u_2,h_4),输出其中的第一项 u_0 作为对CDH问题的回答.

分析:由于 H_4 是模拟成随机预言器的,所以假如 A_{II} 能以1个不可忽略的优势 ε 猜测成功,那么其必然会以不小于 ε 的优势向 H_4 询问 $(dh(g^a,\ g^b),u_1,u_2)$ 的hash值.因此,B解决CDH问题的概率为 $\varepsilon' \geq \frac{\varepsilon}{q_4}$.

定理3 如果存在1个被撤销用户攻击者 A_{re},他能以优势 ε 区分两个等长明文的密文,那么就存在一个算法B,能以概率 $\varepsilon' \geq \frac{\varepsilon}{q_4}$ 解决CDH问题.其中, q_4 表示询问随机预言器 H_4 的次数.

3.2 性能评价

本文给出的方案是无证书公钥系统下的1个加密方案,该方案以较小的代价解决了用户撤销问题,同时方案不需要进行双线性对计算.现有的无证书系统的撤销技术主要有两种:一种是周期更新用户的部分私钥并通过秘密信道传输给用户,另一种是设置1个可信中介SEM来协助用户完成解密操作.与第一种比较,本文的方案节省了建立秘密信道的开销;与第二种方法比较,采用本文的方案,用户之间可以独立通信,而无需可信第三方的协助.

4 结语

无证书公钥系统没有复杂的证书管理,也没有用户私钥托管,虽然计算量有所增加,但与其优点相比,无证书系统仍然不失为一种较理想的公钥密码体制.撤销问题是公钥密码系统必须解决的问题,然而,目前无证书公钥系统的撤销问题依然缺乏高效实用的解决方法.

在现有的无证书撤销技术中,主要的方法是KGC周期性地为每个用户更新部分私钥,然后通过秘密信道传输给用户.但秘密信道的建立需要KGC和用户消耗更多的计算资源.本文针对无证书系统的撤销问题,设计了1个不使用双线性对的可撤销的无证书加密方案,密钥的更新通过公开信道传输,且没有复

杂的双线性对运算,从而大大节约了计算和通信开销.在计算Diffie-Hellman问题的困难性假设下,我们的方案是IND-CCA2可证明安全的.

[参考文献]

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//LNCS 196, Crypto 1984, Berlin: Springer-Verlag, 1984:47-53.

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

[3] MICALI S. Novomodo: scalable certificate validation and simplified PKI management[C]//Proceedings of 1st annual PKI research workshop 2002, Gaithersburg: NIST, 2002: 15-25.

[4] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//LNCS 2139, CRYPTO 2001, Berlin: Springer-Verlag, 2001:213-229.

[5] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]//Proceeding of CCS 2008, New York: ACM Press, 2008:417-426.

[6] LIBERT B, QUISQUATER J J. Efficient revocation and threshold pairing based cryptosystems[C]//Proceeding of PODC 2003, New York: ACM Press, 2003:163-171.

[7] LIBERT B, VERGNAUD D. Adaptive-ID secure revocable identity-based encryption[C]//LNCS 5473, CT-RSA 2009, Berlin: Springer-Verlag, 2009:1-15.

[8] TSENG Y M, TASI T T. Efficient revocable ID-based encryption with a public channel[J]. The computer journal, 2012, 55(4): 475-486.

[9] TSAI T T, TSENG Y M, WU T Y. Revocable ID-based signature scheme with batch verifications[C]//Proceeding of IIHMS 2012, Piraeus: IEEE, 2012:49-54.

[10] TSAI T T, TSENG Y M, WU T Y. Provably secure revocable ID-based signature in the standard model[J]. Security and communication networks, 2013, 6(10): 1 250-1 260.

[11] SEO J H, EMURA K. Revocable identity-based encryption revisited: security model and construction[C]//LNCS 7778, PKC 2013, Berlin: Springer-Verlag, 2013:216-234.

[12] AL-RIYAMI S S. Cryptographic schemes based on elliptic curve pairings[D]. London: University of London, 2004.

[13] SHEN L, ZHANG F, SUN Y. Efficient revocable certificateless encryption secure in the standard model[J]. The computer journal, 2014, 57(4): 592-601.

[14] SUN Y, ZHANG F, SHEN L. Efficient revocable certificateless encryption secure against decryption key exposure[J]. IET information security, 2015, 9(3): 158-166.

[责任编辑:顾晓天]