软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(12):3196−3203 [doi: 10.13328/j.cnki.jos.004826]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

抗签名密钥泄露的可撤销无证书签名*

孙银霞[1,2], 张福泰[1,2], 沈丽敏[1,2,3]

[1](南京师范大学 计算机科学与技术学院,江苏 南京 210023)

[2](江苏省信息安全保密技术工程研究中心,江苏 南京 210023)

[3](西安电子科技大学,陕西 西安 710071)

通讯作者: 孙银霞, E-mail: bela_suno@163.com

摘 要: 当用户的私钥泄露或使用权限到期时,系统如何撤销该用户是亟待解决的问题.这一问题在传统公钥系统 TPKC 和基于身份的公钥系统 IBC 下已有解决方案,然而在无证书公钥系统中,这一问题至今没有得到很好的解决.我们知道,无证书公钥系统没有庞杂的证书库和密钥托管问题,只是算法的计算量稍有增加,是 TPKC 和 IBC 之外的一种较理想的公钥系统,所以对它的撤销机制的研究十分必要.设计了一种可撤销的无证书签名方案,基本原理是:系统定期地给每个未被撤销的用户生成新的时间密钥,并通过公共信道传输给用户.相比现有的 Al-Riyami 和 Paterson 的撤销机制而言,该方案更加高效.同时,新方案达到了抗签名密钥泄露的安全性,且签名密钥的长度非常短.在 CDH 困难性假设下,该方案是 UF-CMA 可证明安全的.

关键词: 无证书公钥系统;无证书签名;撤销;抗签名密钥泄露

中图法分类号: TP309

中文引用格式: 孙银霞,张福泰,沈丽敏.抗签名密钥泄露的可撤销无证书签名.软件学报,2015,26(12):3196−3203. http://www.jos.org.cn/1000-9825/4826.htm

英文引用格式: Sun YX, Zhang FT, Shen LM. Efficient revocable certificateless signature against signing key exposure. Ruan Jian Xue Bao/Journal of Software, 2015,26(12):3196−3203 (in Chinese). http://www.jos.org.cn/1000-9825/4826.htm

Efficient Revocable Certificateless Signature Against Signing Key Exposure

SUN Yin-Xia[1,2], ZHANG Fu-Tai[1,2], SHEN Li-Min[1,2,3]

[1](School of Computer Science and Technology, Nanjing Normal University, Nanjing 210023, China)

[2](Jiangsu Engineering Research Center of Information Security and Privacy Protection Technology, Nanjing 210023, China)

[3](Xidian University, Xi'an 710071, China)

Abstract: A necessary problem in public key cryptosystem is how to revoke a user when the user's private key is compromised or the permission is prohibited. There have been many effective solutions in both traditional public key cryptosystem (TPKC) and identity based cryptosystem (IBC). But, in certificateless public key cryptosystem the revocation problem still remains to be efficiently solved. As is known, certificateless cryptosystem is a good substitution for TPKC and IBC since it features no certificate and no key escrow with only a little more computation. So, it is very necessary to design efficient revocation solutions in the certificateless setting. This paper gives a revocable certificateless signature scheme in which the system periodically generates new time keys for all non-revoked users via public channels. Compared with the existing Al-Riyami and Paterson revocation mechanism, our scheme is much better in efficiency. Furthermore, the new scheme can resist signing key exposure with very short signing key. In the CDH assumption, our scheme is UF-CMA provably secure.

Key words: certificateless public key cryptosystem; certificateless signature; revoke; signing key exposure resilient

* 基金项目: 国家自然科学基金(61170298); 江苏省自然科学基金(BK20130908); 江苏省高校自然科学基金(13KJD520006)

Foundation item: National Natural Science Foundation of China (61170298); NSF of Jiangsu Province (BK20130908); Natural Science Foundation of the Higher Education Institutions of Jiangsu Province, China (13KJD520006)

收稿时间: 2013-11-01; 定稿时间: 2015-02-15

公钥密码技术在保障信息安全方面起着十分重要的作用,尤其是数字签名技术.传统的公钥系统通过颁发公钥证书认证用户公钥的真实性和有效性,不足是公钥证书的管理需要耗费较多的人力、物力和财力.1984年,Shamir 提出了基于身份的公钥密码系统[1],在该系统中,用户使用自己唯一的身份(比如手机号、IP 地址和Email 地址)作为公钥,从而摆脱了对公钥证书的依赖.但是,由于用户的私钥是由系统的私钥生成器(PKG)来生成的,所以 PKG 知道所有用户的私钥,就可以代表任何用户做签名.这种密钥托管问题的存在,在一些实际应用场合是不受欢迎的.为了克服这一不足,2003 年,Al-Riyami 和 Paterson 提出了无证书公钥密码系统[2],实际上,该系统可以看成是对前两种公钥系统的巧妙组合,这里的用户私钥由两部分构成:一部分是由系统的密钥生成中心(KGC)生成,另一部分则是由用户自己选取.无证书公钥系统既不用公钥证书也没有密钥托管问题的特点,使得它在一些应用环境下能取得比前两种公钥系统更好的效果.

任何公钥系统都会面临用户的撤销问题,比如:当用户的使用权限到期了,或用户的私钥泄露了,或用户做了违规操作,那么这时系统需要撤销这类用户.在传统公钥系统中,撤销技术较成熟,有撤销列表 CRLs、在线证书状态协议 OCSP[3]和 Novomodo[4]等.在没有证书的公钥系统中,用户的撤销需要寻找新的途径.根据基于身份的和无证书的公钥系统的构建特点,主流的撤销技术是系统为用户定期更新密钥,这也是最初 Boneh-Franklin[5]和 AlRiyami-Paterson[2]在他们的论文中提到的方法,但是显而易见,每次更新的密钥都必须通过秘密信道传输给用户,而秘密信道的建立需要系统和用户做很多计算,极大地增加了通信开销.所以,如何少用秘密信道而改用公共信道是一个要解决的问题.在基于身份的公钥系统中,这一问题已有不少解决方案[6,7].Boldyreva 等人[6]设计了一个具有可扩展性的可撤销基于身份的加密方案,随后,Libert 和 Vergnaud[8]对该方案作了改进,提高了安全性.Tseng-Tsai[9,10]在随机预言模型下给出了高效的可撤销的基于身份加密和签名方案.

然而,对无证书公钥系统的用户撤销问题的研究却较少,文献[2,11]提到了定期为用户更新部分私钥的方法,但是同样存在秘密信道开销过大的缺点.尽管 Shen 等人[12]提出了新的方案,可以通过公共信道来更新密钥,但是他们的方案存在安全漏洞.所以,如何设计高效的无证书系统的用户撤销方案,仍然是亟待解决的问题.

本文将通过构造一个具体的无证书签名方案来给出一种撤销的方法.用户的部分私钥采用 BLS 短签名算法,密钥生成中心(KGC)定期给所有用户更新时间密钥,这些时间密钥是公开的.当系统撤销某个用户时,KGC停止为该用户生成新的时间密钥.并且,我们的方案能够抵抗解密密钥泄露(后面将使用“签名密钥泄露”),即,任意一个时间段的签名密钥的泄露不会影响到其他时间段的签名密钥的安全性.最早在撤销机制中引入这一安全概念的是在 2013 年的 PKC 会议上[13],作者在基于身份的公钥系统下提出了一种抗解密密钥泄露的高效的可撤销加密方案,核心技术是:在构造用户某个时间段的解密密钥时,引用了新的随机数.当然,在无证书公钥系统下,我们可以采用同样的方法来计算用户的解密密钥(签名密钥).但是新随机数的加入,显然将增加系统的计算代价和存储开销.有意思的是,我们研究发现在无证书系统下,可以充分利用用户选取的密秘值来构造签名密钥,而没有必要增加新的随机数.总之,本文的可撤销的无证书签名方案具有 3 方面的特点:(1) 密钥的更新是在公共信道上完成的;(2) 可以抵抗签名密钥泄露攻击;(3) 签名密钥的生成没有新的随机数的参与,长度很短.与现有方案相比,新方案具有明显的优势.

1 预备知识

本节介绍几个预备知识,主要包括可撤销的无证书签名方案的定义、安全模型和相关数学知识,其中,前两个是我们首次给出的.

1.1 可撤销的无证书签名方案的定义

考虑到签名密钥泄露的威胁,用户用于签名的密钥不能是原有私钥和时间密钥的简单组合,所以我们在通常的框架下增加了生成签名密钥的算法,具体而言,一个可撤销的无证书签名方案由以下 8 个算法构成:

(1) 建立系统:输入安全参数,该算法生成一组系统公开参数和一个系统主密钥;

(2) 生成部分私钥:该算法由 KGC 执行,输入一个用户的身份 ID,输出该用户的部分私钥 D_{ID}.该部分私钥由用户保存不变;

(3) 更新时间密钥:KGC 在每个时间段 T,为每个用户生成一个时间密钥 $D_{ID,T}$;

(4) 生成秘密值:用户选取一个秘密值 s_{ID};

(5) 生成签名密钥:输入部分私钥、时间密钥和秘密值,用户计算出签名密钥 $SK_{ID,T}$;

(6) 生成公钥:输入系统公开参数和秘密值 s_{ID},输出用户 ID 的公钥 PK_{ID};

(7) 签名:输入用户身份 ID,时间 T,消息 M,签名密钥以及系统公开参数,输出签名 σ;

(8) 验证:验证者用签名人的公钥验证签名的有效性.

1.2 安全模型

本节讨论可撤销的无证书签名的安全模型.针对一般的无证书公钥系统,需要考虑两类攻击者:第 1 类攻击者和第 2 类攻击者.其中,第 1 类攻击者模拟外部攻击者,能够替换任何用户的公钥;第 2 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签名,需要再考虑一类攻击者(后面称为第 3 类攻击者):恶意的被撤销的用户,并且允许他替换其他用户的公钥.

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

游戏:

(1) $(params,msk)\leftarrow \boldsymbol{C}^{Setup}(1^k)$;

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

(3) $(ID^*,PK_{ID^*},m^*,\sigma^*)\leftarrow \boldsymbol{A}$,$\boldsymbol{A}$ 获胜当且仅当签名有效.

如果 $\boldsymbol{A}$ 为第 1 类攻击者,那么 $inf=\varnothing$(空集);如果 $\boldsymbol{A}$ 为第 2 类攻击者,那么 $inf=msk$;如果 $\boldsymbol{A}$ 为恶意的被撤销的用户,那么 $inf=\{D_{ID},s_{ID}\}$.攻击者在阶段(2)可访问如下预言器(oracles):

- 部分私钥询问(第 1 类、第 3 类攻击者):攻击者提供一个用户身份 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(第 1 类、第 3 类攻击者):攻击者询问(ID_i,T_j)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,但是不允许询问一个被替换的公钥对应的秘密值;
- 签名密钥询问:攻击者询问 ID_i 在时间段 T_j 的签名密钥,挑战者运行签名密钥生成算法,输出 SK_{ID_i,T_j}.攻击者不允许询问一个被替换的公钥对应的签名密钥;
- 公钥询问:攻击者可以向挑战者询问每个用户的公钥 PK_{ID_i};
- 公钥替换(第 1 类、第 3 类攻击者):攻击者可以替换任何公钥;
- 签名询问:攻击者询问 ID_i 在时间段 T_j 对消息 M 的签名,挑战者运行签名算法,把签名返回给攻击者.

定义攻击者 $\boldsymbol{A}$ 在以上游戏中的优势为:伪造的签名是一个有效的签名的概率.

定义 1. 如果没有任何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,那么称一个可撤销的无证书签名方案在选择消息攻击下是不可伪造的(UF-CMA 安全).其中,不可忽略的定义如下:

定义 2. 如果对所有的多项式 h,总是存在一个整数 N,使得当 $x\geqslant N$,有$|f(x)|\leqslant 1/|h(x)|$,则称函数 f 是可忽略的.

1.3 数学知识

1.3.1 双线性对

设 G_1 和 G_2 分别表示阶为素数 q 的加法循环群和乘法循环群,P 是 G_1 的一个生成元.

若映射 $\hat{e}:G_1\times G_1\rightarrow G_2$ 满足下列性质,则被称为双线性对:

(1) 双线性性:对任意 $a,b\in Z_q^*$,$\hat{e}(aP,bP)=\hat{e}(P,P)^{ab}$;

(2) 非退化性:$\hat{e}(P,P)\neq 1_{G_2}$;

(3) 可计算性:对所有 $P,Q\in G_1$,都能有效计算出 $\hat{e}(P,Q)$ 的值.

双线性对 $\hat{e}$ 可以通过有限域上的超椭圆曲线上的 Tate 对或 Weil 对来构造.以下介绍本文所依赖的数学困难问题,设这些困难问题都定义在(G_1,G_2,q,P)上.

1.3.2 Diffie-Hellman 问题

定义 3(计算 Diffie-Hellman(CDH)问题). 给定$\langle aP,bP\rangle$,其中,a,b 是群 Z_q^* 里的两个随机数,计算 abP 的值.

设 $\boldsymbol{B}$ 是一个 CDH 问题解决者,定义 $\boldsymbol{B}$ 的优势为 $\Pr[\boldsymbol{B}(aP,bP)=abP]$.CDH 困难性假设指,任何攻击者不能以不可忽略的优势解决 CDH 问题.

2 具体方案的构造

本节给出详细方案,该方案的构造方法巧妙地利用了 Al-Riyami 和 Paterson 的无证书加密技术,具体如下:

(1) 建立系统:输入安全参数 l.设 G_1 和 G_2 是阶为素数 q 的双线性群,P 是 G_1 的一个生成元,$\hat{e}:G_1\times G_1\to G_2$ 是双线性对.随机选取 $s\in Z_q^*$,计算 $P_0=sP$.选取 3 个 hash 函数 $H_1:\{0,1\}^*\to G_1$,$H_2:\{0,1\}^*\to G_1$ 和 $H_3:\{0,1\}^*\to G_1$.输出公开参数 $(G_1,G_2,q,P,\hat{e},P_0,H_1,H_2,H_3)$ 和系统主密钥 s;

(2) 生成部分私钥:输入用户身份 ID,计算部分私钥 $D_{ID}=sH_1(ID)$;

(3) 更新时间密钥:输入时间 T 和用户身份 ID,计算时间密钥 $D_{ID,T}=sH_2(ID,T)$;

(4) 生成秘密值:随机选取 $x\in Z_q^*$,计算 $PK_{ID,1}=xP$ 和 $PK_{ID,2}=xP_0$;

(5) 生成签名密钥:用户计算签名密钥 $SK_{ID,T}=x(D_{ID}+D_{ID,T})$;

(6) 生成公钥:用户 ID 的公钥为 $PK_{ID}=(PK_{ID,1},PK_{ID,2})$;

(7) 签名:用户 ID 对消息 M 签名,随机选取 $r\in Z_q^*$,计算 $U=rP,V=SK_{ID,T}+rH_3(ID,T,M,PK_{ID,2},U)$,输出签名 $\sigma=(U,V)$;

(8) 验证:首先验证 $e(V,P)=e(H_1(ID)+H_2(ID,T),PK_{ID,2})e(H_3(ID,T,M,PK_{ID,2},U),U)$和 $e(P_0,PK_{ID,1})=e(P,PK_{ID,2})$ 是否同时成立:若是,则签名有效;否则,签名无效.

3 安全证明和效率评估

3.1 安全证明

本节证明上述方案的 UF-CMA 安全性.分别通过定理 1~定理 3 来证明方案对于 3 类攻击者是安全的.

定理 1. 如果存在第 1 类攻击者 $\boldsymbol{A}_{\mathrm{I}}$,他能在时间 t 内以优势 ε 伪造有效的消息/签名对,那么就存在算法 $\boldsymbol{B}$,能在时间 t' 内以概率 ε' 解决 CDH 问题.其中,q_{ppk} 表示询问部分私钥的次数,q_{tk} 表示询问时间密钥的次数,q_{sv} 表示询问秘密值的次数,q_{pk} 表示询问公钥的次数,q_s 表示询问签名的次数,q_i 表示询问随机预言器 H_i 的次数.

证明:现有算法 $\boldsymbol{B}$,其目标是解决 CDH 问题,即:任意给定$(aP,bP\in G_1)$,计算 abP.$\boldsymbol{B}$ 将利用第 1 类攻击者 $\boldsymbol{A}_{\mathrm{I}}$ 伪造有效签名的能力来求解 CDH 问题.

首先,$\boldsymbol{B}$ 建立系统,设置系统公共参数$(p,G_1,G_2,P,P_0,e,H_1,H_2,H_3)$,其中,取 $P_0=aP$.

然后 $\boldsymbol{A}_{\mathrm{I}}$ 开始攻击,他将作一系列询问.所有的询问-回答都将被保留在相应的列表中.设允许 $\boldsymbol{A}_{\mathrm{I}}$ 询问 H_1 的次数为 q_1,$\boldsymbol{B}$ 选择 $I\in[1,q_1]\cap Z$.

具体询问描述如下:

- Hash 询问:对 H_1,H_2 和 H_3 的询问,挑战者从相关的域中随机选取一个值作为回答.除了当 $\boldsymbol{A}_{\mathrm{I}}$ 对 H_1 作第 I 次询问 ID^* 时,$\boldsymbol{B}$ 计算 $H_1(ID^*)=bP$;
- 部分私钥询问:当 $\boldsymbol{A}_{\mathrm{I}}$ 询问 ID_i 的部分私钥时,若 $i\neq I$,则 $\boldsymbol{B}$ 搜索 H_1 列表,得到 $H_1(ID_i)=h_iP$,然后计算 ID_i 的部分私钥 $D_{ID_i}=h_iaP$;否则,游戏结束;
- 时间密钥询问:当 $\boldsymbol{A}_{\mathrm{I}}$ 询问(ID_i,T_j)的时间密钥时,$\boldsymbol{B}$ 搜索 H_2 列表,得到 $H_2(ID_i,T_j)=h_{ij}P$,然后计算 ID_i 的时间密钥 $D_{ID_i,T_j}=h_{ij}aP$;
- 秘密值询问:对于每个秘密值询问,$\boldsymbol{B}$ 从 Z_p 中随机选取元素 x_i 作为对该询问的回答,但是 $\boldsymbol{A}_{\mathrm{I}}$ 不允许询问一个被替换的公钥对应的秘密值;

- 签名密钥询问:当 $\boldsymbol{A}_{\mathrm{I}}$ 询问 ID_i 在时间段 T_j 的签名密钥时,$\boldsymbol{B}$ 计算 $SK_{ID_i,T_j}=x_i(D_{ID_i}+D_{ID_i,T_j})$.当$(ID_i,T_j)=(ID^*,T^*)$时,游戏结束.但是,$\boldsymbol{A}_{\mathrm{I}}$不允许询问一个被替换的公钥对应的签名密钥;
- 公钥询问:对于每个公钥询问,$\boldsymbol{B}$ 首先从秘密值列表中找出对应的秘密值 x_i,然后计算公钥:

$$PK_{ID_i}=(PK_{ID_i,1},PK_{ID_i,2})=(x_iP,x_iP_0);$$

- 公钥替换:$\boldsymbol{A}_{\mathrm{I}}$可以替换任何公钥;
- 签名询问:当 $\boldsymbol{A}_{\mathrm{I}}$ 询问 ID_i 在时间段 T_j 对一个消息 M 的签名时:
  - 如果$(ID_i,T_j)\neq(ID^*,T^*)$且公钥未被替换,则 $\boldsymbol{B}$ 用 ID_i 在时间段 T_j 的签名密钥对消息进行签名,并输出结果;
  - 否则,$\boldsymbol{B}$ 随机选取 $u\in Z_p$,计算 $U=uPK_{ID,2}, V=x_{ID_i}uh_3P_0+h_iP_0+h_{ij}P_0$,输出$\sigma=(U,V)$作为对该询问的签名回答.这里,设 $H_1(ID_i)=h_iP, H_2(ID_i,T_j)=h_{ij}P, H_3(ID_i,T_j,M,PK_{ID_i,2},U)=h_3P.x_{ID_i}$ 为用户 ID_i 的原始秘密值(即使 ID_i 的公钥被替换,签名人仍将用自己正确的签名密钥作签名);

• 伪造:$\boldsymbol{A}_{\mathrm{I}}$输出伪造的消息签名对$(M^*,\sigma^*)$、用户身份 ID^*和时间段 T^*.由于 Hash 函数 H_3 是随机预言器,所以 $\boldsymbol{A}_{\mathrm{I}}$一定会以某种概率(与 $\boldsymbol{A}_{\mathrm{I}}$的优势密切相关)询问 $H_3(ID^*,T^*,M^*,\tilde{P}K_{ID,2},U^*)$,这里的公钥 $\tilde{P}K_{ID,2}$ 是 ID^*的当前公钥.$\boldsymbol{B}$ 从 H_3 列表中随机取出一个回答 h_3^*P,若伪造的签名有效,则应满足验证等式 $e(V^*,P)=e(H_1(ID^*)+H_2(ID^*,T^*),\tilde{P}K_{ID^*,2})e(H_3(ID^*,T^*,M^*,\tilde{P}K_{ID^*,2},U^*),U^*)$,从而,$\boldsymbol{B}$ 可以计算出:

$$abP=\tilde{x}_{ID^*}^{-1}(V^*-h_3^*U^*-h_{ij}^*\tilde{P}K_{ID^*,2}).$$

分析:$\boldsymbol{A}_{\mathrm{I}}$ 询问 $H_3(ID^*,T^*,M^*,\tilde{P}K_{ID^*,2},U^*)$ 的概率等于其攻击优势,所以 $\boldsymbol{B}$ 解决 CDH 问题的概率为 $\frac{\varepsilon}{q_1q_3}$. □

定理 2. 如果存在第 2 类攻击者 $\boldsymbol{A}_{\mathrm{II}}$,他能在时间 t 内以优势ε伪造有效的消息/签名对,那么就存在算法 $\boldsymbol{B}$,能在时间 t'内以概率ε'解决 CDH 问题.其中,q_{sv} 表示询问秘密值的次数,q_{pk} 表示询问公钥的次数,q_s 表示询问签名的次数,q_i 表示询问随机预言器 H_i 的次数.

证明:现有算法 $\boldsymbol{B}$,其目的是解决 CDH 问题,即:任意给定$(aP,bP\in G_1)$,计算 abP.$\boldsymbol{B}$ 将利用第 1 类攻击者 $\boldsymbol{A}_{\mathrm{II}}$ 伪造有效签名的能力来求解 CDH 问题.

首先,$\boldsymbol{B}$ 建立系统,随机选取 $s\in Z_p$ 作为系统主密钥,计算 $P_0=sP$,系统公共参数为$(p,G_1,G_2,P,P_0,e,H_1,H_2,H_3)$,并把 s 发送给攻击者 $\boldsymbol{A}_{\mathrm{II}}$.

然后 $\boldsymbol{A}_{\mathrm{II}}$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.设允许 $\boldsymbol{A}_{\mathrm{II}}$ 询问 H_2 的次数为 q_2,$\boldsymbol{B}$ 选择一个 $I\in[1,q_2]\cap Z$:

- Hash 询问:对 H_1,H_2 和 H_3 的询问,挑战者从相关的域中随机选取一个值作为回答.除了:当 $\boldsymbol{A}_{\mathrm{I}}$对 H_2 作第 I 次询问(ID^*,T^*)时,$\boldsymbol{B}$ 随机选择 $h\in Z_p$,计算$(ID^*,T^*)=bP-hP$;当 $\boldsymbol{A}_{\mathrm{I}}$对 H_1 询问 ID^*时,$\boldsymbol{B}$ 输出 $H_1(ID^*)=hP$;
- 秘密值询问:当 $\boldsymbol{A}_{\mathrm{II}}$ 询问 ID_i 的秘密值时,若 $ID_i\neq ID^*$,则 $\boldsymbol{B}$ 从 Z_p 中随机选取一个元素 x_i 作为对该询问的回答;否则,游戏结束;
- 签名密钥询问:当 $\boldsymbol{A}_{\mathrm{II}}$ 询问 ID_i 在时间段 T_j 的签名密钥时,$\boldsymbol{B}$ 计算 $SK_{ID_i,Tj}=x_i(D_{ID_i}+D_{ID_i,T_j})$.当 $ID_i=ID^*$ 时, $SK_{ID_i,T_j}=a(hP+h_{ij}P)=haP+h_{ij}P$.这里,$H_1(ID_i)=hP$,$H_2(ID^*,T)=h_{ij}P$.当$(ID_i,T_j)=(ID^*,T^*)$时,游戏结束;
- 公钥询问:对于每个公钥询问(ID_i),若 $ID_i=ID^*$,则 $\boldsymbol{B}$ 输出公钥 $PK_{ID}=(PK_{ID,1},PK_{ID,2})=(aP,asP)$;否则,$\boldsymbol{B}$ 先从秘密值列表中找出对应的秘密值 x_i,然后计算公钥 $PK_{ID_i}=(PK_{ID_i,1},PK_{ID_i,2})=(x_iP,x_iP_0)$;
- 签名询问:当 $\boldsymbol{A}_{\mathrm{II}}$ 询问 ID_i 在时间段 T_j 对一个消息 M 的签名时:
  - 如果$(ID_i,T_j)\neq(ID^*,T^*)$,则 $\boldsymbol{B}$ 用 ID_i 在时间段 T_j 的签名密钥对消息进行签名,并输出结果;
  - 否则,$\boldsymbol{B}$ 随机选取 $u\in Z_p$,计算 $U=uPK_{ID,2}, V=x_{ID_i}s(hP+uh_3P)$ (若 $ID_i=ID^*$,即 $x_{ID_i}=a$,则计算 $V=s(haP+uh_3aP)$),输出$\sigma=(U,V)$作为对该询问的签名回答.这里,设 $H_1(ID_i)+H_2(ID_i,T_j)=hP$ 以及 $H_3(ID_i,T_j,M,PK_{ID_i,2},U)=h_3P$;
- 伪造:$\boldsymbol{A}_{\mathrm{II}}$输出伪造的消息签名对$(M^*,\sigma^*)$、用户身份 ID^*和时间段 T^*.由于 Hash 函数 H_3 是随机预言器,

所以 $\boldsymbol{A}_{\mathrm{II}}$ 一定会以某种概率(与 $\boldsymbol{A}_{\mathrm{II}}$ 的优势密切相关)询问 $H_3(ID^*,T^*,M^*,PK_{ID,2},U^*)$.$\boldsymbol{B}$ 从 H_3 列表中随机取出一个回答 h_3^*P,若伪造的签名有效,则应满足验证等式:

$$e(V^*,P)=e(H_1(ID^*)+H_2(ID^*,T^*),PK_{ID^*,2})e(H_3(ID^*,T^*,M^*,PK_{ID^*,2},U^*),U^*),$$

即 $e(V,P)=e(sabP,P)e(h_3^*U,P)$,从而,$\boldsymbol{B}$ 可以计算出 $abP=s^{-1}(V^*-h_3^*U^*)$.

分析:$\boldsymbol{A}_{\mathrm{II}}$ 询问 $H_3(ID^*,T^*,M^*,PK_{ID,2},U^*)$的概率等于其攻击优势,所以,$\boldsymbol{B}$ 解决 CDH 问题的概率为 $\frac{\varepsilon}{q_2q_3}$. □

定理 3. 如果存在被撤销用户攻击者 $\boldsymbol{A}_{\mathrm{re}}$,他能在时间 t 内以优势ε伪造有效的消息/签名对,那么就存在算法 $\boldsymbol{B}$,能在时间 t'内以概率ε'解决 CDH 问题.其中,q_{ppk}表示询问部分私钥的次数,q_{tk}表示询问时间密钥的次数,q_{sv}表示询问秘密值的次数,q_{pk}表示询问公钥的次数,q_s表示询问签名的次数, q_i表示询问随机预言器 H_i的次数.

证明:CDH 问题解决者 $\boldsymbol{B}$:对于任意给定$(aP,bP\in G_1)$,计算 abP.$\boldsymbol{B}$ 将利用被撤销的用户攻击者 $\boldsymbol{A}_{\mathrm{re}}$ 伪造有效签名的能力来求解 CDH 问题.

首先,$\boldsymbol{B}$ 建立系统,设置系统公共参数$(p,G_1,G_2,P,P_0,e,H_1,H_2,H_3)$,其中,取 $P_0=aP$.

然后 $\boldsymbol{A}_{\mathrm{re}}$ 开始攻击,他将作一系列询问,所有的询问-回答都将被保留在相应的列表中.设允许 $\boldsymbol{A}_{\mathrm{re}}$ 询问 H_2 的次数为 q_2,$\boldsymbol{B}$ 选择一个 $I\in[1,q_2]\cap Z$.

具体询问描述如下:

- Hash 询问:对 H_1,H_2 和 H_3 的询问,挑战者从相关的域中随机选取一个值作为回答.除了:当 $\boldsymbol{A}_{\mathrm{re}}$ 对 H_2 作第 I 次询问(ID^*,T^*)时,$\boldsymbol{B}$ 随机选择 $h\in Z_p$,计算 $H_2(ID^*,T^*)=bP-hP$;当 $\boldsymbol{A}_{\mathrm{re}}$ 对 H_1 询问 ID^*时,$\boldsymbol{B}$ 输出 $H_1(ID^*)=hP$;
- 部分私钥询问:当 $\boldsymbol{A}_{\mathrm{re}}$ 询问 ID_i 的部分私钥时,$\boldsymbol{B}$ 搜索 H_1 列表,得到 $H_1(ID_i)=h_iP$,然后计算 ID_i 的部分私钥 $D_{ID_i}=h_iaP$;
- 时间密钥询问:当 $\boldsymbol{A}_{\mathrm{re}}$ 询问 ID_i 在时间段 T_j 的时间密钥时,$\boldsymbol{B}$ 搜索 H_1 列表,得到 $H_2(ID_i,T_j)=h_{ij}P$,然后计算 ID_i 的部分私钥 $D_{ID_i,T_j}=h_{ij}aP$.当$(ID_i,T_j)=(ID^*,T^*)$时,游戏结束;
- 秘密值询问:对于每个秘密值询问,$\boldsymbol{B}$ 从 Z_q 中随机选取元素 x_i 作为对该询问的回答;
- 签名密钥询问:当 $\boldsymbol{A}_{\mathrm{re}}$ 询问 ID_i 在时间段 T_j 的签名密钥时,$\boldsymbol{B}$ 计算 $SK_{ID_i,T_j}=x_i(D_{ID_i}+D_{ID_i,T_j})$.当$(ID_i,T_j)=(ID^*,T^*)$时,游戏结束;
- 公钥询问:对于每个公钥询问,$\boldsymbol{B}$ 首先从秘密值列表中找出对应的秘密值 x_i,然后计算公钥:

$$PK_{ID_i}=(PK_{ID_i,1},PK_{ID_i,2})=(x_iP,x_iP_0);$$

- 签名询问:当 $\boldsymbol{A}_{\mathrm{re}}$ 询问 ID_i 在时间段 T_j 对消息 M 的签名时:
  - 如果$(ID_i,T_j)\neq(ID^*,T^*)$,则 $\boldsymbol{B}$ 用 ID_i 在时间段 T_j 的签名密钥对消息进行签名,并输出结果;
  - 否则,$\boldsymbol{B}$随机选取 $u\in Z_p$,计算 $U=uPK_{ID,2}$, $V=x_{ID_i}uh_3P_0+h_iP_0+h_{ij}P_0$,输出$\sigma=(U,V)$作为对该询问的签名回答.这里,设 $H_1(ID_i)=h_iP$,$H_2(ID_i,T_j)=h_{ij}P$, $H_3(ID_i,T_j,M,PK_{ID_i,2},U)=h_3P$.$x_{ID_i}$ 为用户 ID_i 的秘密值;

• 伪造:$\boldsymbol{A}_{\mathrm{re}}$输出伪造的消息签名对$(M^*,\sigma^*)$、用户身份 ID^*和时间段 T^*.由于 Hash 函数 H_3 是随机预言器,所以 $\boldsymbol{A}_{\mathrm{re}}$一定会以某种概率(与 $\boldsymbol{A}_{\mathrm{re}}$的优势密切相关)询问 $H_3(ID^*,T^*,M^*,\tilde{P}K_{ID,2},U^*)$,这里的公钥 $\tilde{P}K_{ID,2}$ 是 ID^*的当前公钥.$\boldsymbol{B}$ 从 H_3 列表中随机取出一个回答 h_3^*P,若伪造的签名有效,则应满足验证等式:

$$e(V^*,P)=e(H_1(ID^*)+H_2(ID^*,T^*),PK_{ID^*,2})e(H_3(ID^*,T^*,M^*,PK_{ID^*,2},U^*),U^*),$$

即 $e(V^*,P)=e(x_{ID^*}abP,P)e(h_3^*U^*,P)$,从而,$\boldsymbol{B}$ 可以计算出 $abP=x_{ID^*}^{-1}(V^*-h_3^*U^*)$.

分析:$\boldsymbol{A}_{\mathrm{re}}$ 询问 $H_3(ID^*,T^*,M^*,PK_{ID^*,2},U^*)$ 的概率等于其攻击优势;另外,游戏不退出的概率为 $\frac{1}{q_2}$.所以,$\boldsymbol{B}$ 解

决 CDH 问题的概率为 $\frac{\varepsilon}{q_2 q_3}$. □

3.2 效率评估

本文给出的方案是无证书公钥系统下的一个签名方案,该方案以较小的代价解决了用户撤销问题,同时实现了前向和后向安全.即使某个时间段的签名密钥泄露了,也不会影响到其他时间段的签名密钥的安全性.该方案共包含 8 种算法,KGC 执行生成部分私钥和更新时间密钥算法,每次执行算法只需进行一次点乘运算,时间密钥只需通过公共信道传输给用户.用户生成签名密钥和公钥只需计算 3 个点乘,并且用户需要秘密存储的签名密钥长度较短.我们通过表 1 把本文的方案与文献[13]、AP 式方案(周期更新用户的部分私钥,并通过秘密信道传输给用户,不妨设采用本文的签名技术)进行了详细的比较.

Table 1

表 1

方案	签名密钥长度	签名计算	验证计算	密钥更新信道
文献[13]	⩾480bit	–	–	公共
AP 方案	160bit	2s	5p	秘密
本文方案	160bit	2s	5p	公共

被比较的方案是目前能抵抗签名(或解密)密钥泄露的 3 类可撤销方案,我们分别从签名密钥长度、签名和验证的计算量以及更新密钥所需的信道类别进行对比,其中,签名密钥的长度涉及到占用终端用户的存储空间多少;签名和验证的计算量涉及到占用用户多少计算资源;传输更新的密钥的信道意味着 KGC 和用户是否要做更多额外的计算,它包括两种——公共信道和秘密信道:公共信道表示信息以明文的形式在上面传输,对任何人都是可见的;而秘密信道意味着在上面传输的信息,除了通信双方,其他人是不可见的.公共信道是现成的;而秘密信道的建立需要通信双方的协商认证,比如,一般可以采用 DES 加密和 MAC 技术来实现.

上述比较以 RSA 的 1024bit 安全级别为基准,s 表示点乘运算,p 表示 pairing 运算.文献[13]是在基于身份的公钥系统下研究的,所以在此对签名和验证不作比较.对于签名密钥(也就是解密密钥)长度的考虑,主要是基于技术层面的(用新的随机数来构造).

通过比较容易得出:新方案在具备抵抗签名密钥泄露的优势前提下,还拥有签名密钥长度短和密钥更新信道公开的两大优点.因此,本文方案具有综合优势,更加适合实际应用.

4 总 结

当用户的私钥泄露或使用权限到期,系统如何撤销该用户是一个必须要解决的问题.这一问题在传统的使用证书的公钥系统 TPKC 已有较成熟的解决方案,在基于身份的公钥系统 IBC 也有不少撤销技术被相继提出.无证书公钥系统没有庞杂的证书库,也不存在密钥托管问题,只是算法的计算量稍有增加,所以是 TPKC 和 IBC 之外的一种较理想的公钥系统.然而,目前对无证书公钥系统的用户撤销问题却研究甚少,主要难点在于用户公私钥结构的特殊性.

Al-Riyami 和 Paterson 最早在 2003 年提到的撤销方法是 KGC 周期性地为每个用户更新部分私钥,这些部分私钥必须通过秘密信道传输给用户,使得 KGC 和用户双方都需要消耗更多的计算资源.本文考虑在确保抗签名密钥泄露的前提下,通过定期给用户更新密钥来建立撤销机制,不同的是:更新的密钥仅需在公共信道上传输,极大地节约了成本.当然,公开传输密钥可能存在一定风险,比如更容易引起敌人的好奇心,导致密钥被篡改.但我们知道,即使这样,敌人仍然不能对传输的真实消息构成任何威胁.在随机预言模型和 CDH 困难性假设下,我们的方案是 UF-CMA 安全的.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Proc. of the Crypto'84. LNCS 196, Springer-Verlag, 1984. 47−53. [doi: 10.1007/3-540-39568-7_5]

[2] Al-Riyami SS, Paterson K. Certificateless public key cryptography. In: Proc. of the Asiacrypt 2003. LNCS 2894, Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[3] Myers M, Ankney R, alpani A, Galperin S, Adams C. X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol (OCSP). RFC, 2560.

[4] Micali S. Novomodo: Scalable certificate validation and simplified PKI management. In: Proc. of the 1st Annual PKI Research Workshop. 2002. 15−25.

[5] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Proc. of the CRYPTO 2001. LNCS 2139, Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[6] Boldyreva A, Goyal V, Kumar V. Identity-Based encryption with efficient revocation. In: Proc. of the CCS 2008. ACM Press, 2008. 417−426. [doi: 10.1145/1455770.1455823]

[7] Libert B, Quisquater JJ. Efficient revocation and threshold pairing based cryptosystems. In: Proc. of the Symp. on Principles of Distributed Computing (PODC 2003). 2003. [doi: 10.1145/872035.872059]

[8] Libert B, Vergnaud D. Adaptive-ID secure revocable identity-based encryption. In: Proc. of the CT-RSA 2009. LNCS 5473, Springer-Verlag, 2009. 1−15. [doi: 10.1007/978-3-642-00862-7_1]

[9] Tseng YM, Tasi TT. Efficient revocable ID-based encryption with a public channel. The Computer Journal, 2012,55(4):475−486. [doi: 10.1093/comjnl/bxr098]

[10] Tsai TT, Tseng YM, Wu TY. Revocable ID-based signature scheme with batch verifications. In: Proc. of the 2012 8th Int'l Conf. on Intelligent Information Hiding and Multimedia Signal. 2012. 49−54. [doi: 10.1109/IIH-MSP.2012.18]

[11] Al-Riyami SS. Cryptographic schemes based on elliptic curve pairings [Ph.D. Thesis]. Royal Holloway, University of London, 2004.

[12] Shen L, Zhang F, Sun Y. Efficient revocable certificateless encryption secure in the standard model. The Computer Journal, 2014, 57(4):592−601. [doi: 10.1093/comjnl/bxt040]

[13] Seo JH, Emura K. Revocable identity-based encryption revisited: Security model and construction. In: Proc. of the PKC 2013. LNCS 7778, 2003. 216−234. [doi: 10.1007/978-3-642-36362-7_14]

孙银霞(1979－),女,江苏常州人,博士,讲师,主要研究领域为密码学,网络安全.

沈丽敏(1978－),女,讲师,主要研究领域为密码学,信息论与编码.

张福泰(1965－),男,博士,教授,博士生导师,主要研究领域为密码学理论与技术及其应用.