基于证书的抗连续泄露签名机制

周彦伟[1),2),3)] 马 岿[1),3)] 乔子芮[1)] 杨 波[1)] 顾纯祥[2)]

[1)](陕西师范大学计算机科学学院 西安 710062)

[2)](河南省网络密码技术重点实验室 郑州 450052)

[3)](广西密码学与信息安全重点实验室 广西 桂林 541004)

摘 要 为进一步提升密码原语的安全性,近年来抵抗泄露攻击的密码机制相继被研究者提出.基于证书的密码体制在解决传统公钥基础设施中证书复杂管理问题的同时,也避免了身份基密码机制的密钥托管不足,上述优势使得该体制在实际环境中具有广泛的应用前景,然而由于缺乏对该体制泄露容忍性的研究,制约了该机制在安全协议设计方面的应用推广.针对上述不足,为满足基于证书签名机制的抗泄露性需求,本文提出了基于证书的抗泄露签名机制的具体构造,并基于离散对数的困难性,在随机谕言机模型下使用分叉引理对本文方案的不可伪造性进行了形式化证明;由于未使用双线性映射运算,确保本文构造具有较高的计算效率.与现有相关机制的比较可知,在保持安全性可证明的基础上,本文构造为签名机制提供抵抗泄露攻击能力的同时,提升了相应的计算效率.此外,在上述基础方案之上,本文设计了基于证书的抗泄露聚合签名机制的具体构造,实现了同时完成多个签名的合法性验证目标,进一步提升了签名的合法性验证效率,上述优势确保本文构造能在实际应用中广泛使用,例如无线传感器网络等.

关键词 泄露容忍性;基于证书的密码学;基于证书的签名;分叉引理

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2022.02363

Certificate-Based Signature Scheme with Continuous Leakage Resilience

ZHOU Yan-Wei[1),2),3)] MA Kui[1),3)] QIAO Zi-Rui[1)] YANG Bo[1)] GU Chun-Xiang[2)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710062)

[2)](*Henan Key Laboratory of Network Cryptography Technology, Zhengzhou* 450052)

[3)](*Guangxi Key Laboratory of Cryptography and Information Security, Guilin, Guangxi* 541004)

Abstract To further improve the security of cryptographic primitives, the leakage resilience has become a necessary security, and leakage-resilient cryptography has been proposed in recent years. The certificate-based cryptography solved the certificate management problem of the traditional public key infrastructure and avoided the key escrow shortcoming of the identity-based cryptography, which was widely employed in the practical applications to design security protocol, and there is a lack of research for the leakage resilience of certificate-based cryptographic primitives, which restricts its application in the design of security protocol. In order to address the above problems, a leakage-resilient certificate-based signature (CBS) scheme will be created in this paper, and the security of our proposal is proved based on the hardness of discrete logarithm problem by using Forking lemma under the random oracle model. Also, our CBS scheme is created without using bilinear mapping, and provides the high computation efficiency. Compared with the

收稿日期:2021-09-15;在线发布日期:2022-07-21.本课题得到国家重点研发计划(2017YFB0802000)、国家自然科学基金(62272287,61802242,U2001205)、四川省科技计划项目(2020JDJQ0076)、广西密码学与信息安全重点实验室研究课题(GCIS202108)、河南省网络密码技术重点实验室研究课题(LNCT2021-A04)资助.**周彦伟**,博士,副教授,硕士生导师,主要研究兴趣为信息安全、密码学等. E-mail: zyw@snnu.edu.cn. **马 岿**,硕士研究生,主要研究方向为信息安全、密码学等. **乔子芮**(通信作者),博士研究生,主要研究方向为信息安全、密码学等. E-mail: qzr_snnu@163.com. **杨 波**(通信作者),博士,教授,博士生导师,主要研究领域为信息安全、密码学等. E-mail: byang@snnu.edu.cn. **顾纯祥**,博士,教授,博士生导师,主要研究领域为信息安全等.

previous constructions, our CLS scheme has provable security while the continuous leakage resilience is provided, and the corresponding computation efficiency is improved. Furthermore, a certificate-based aggregate signature scheme with leakage resilience is created from the above basic CBS scheme, which realizes the validity verification of multiple signatures at the same time and can further improve the validity verification efficiency of signatures. These advantages ensure that our proposal can be used in the actual applications, such as wireless sensor networks, etc.

Keywords leakage resilience; certificate-based cryptography; certificate-based signature; forking lemma

1 引 言

在现实环境中,边信道、电磁分析、冷启动等各种各样泄露攻击的普遍存在,使得攻击者能够通过泄露攻击获得密码机制内部秘密状态(如用户私钥、随机数等)的部分泄露信息,导致在传统理想安全模型下(该模型认为内部秘密信息对外界敌手是完全保密的)可证明安全的密码机制不再保持其所声称的安全性.为进一步增强密码机制的实用性,需研究能够抵抗泄露攻击的密码学原语[1-2],使其满足现实环境抵抗泄露攻击的实际应用需求.

各种各样泄露攻击的出现,使得抗泄露性已成为当前复杂网络环境下密码机制的一个必备安全属性.近年来,抗泄露密码机制的研究得到了密码学研究者的广泛关注,抗泄露的公钥加密机制[3-4]、抗泄露的基身份的加密机制[5-6]、抗泄露的属性基加密机制[7-8]等具备抗泄露属性的密码原语相继被提出.特别地,由于在实际应用中,敌手能够持续对密码机制发起泄露攻击,为缩小理论研究与实际应用需求间的差距,将要求密码原语需具备抵抗连续泄露攻击的能力,以达到进一步提升密码原语实用性的目的.

1984 年,为解决传统公钥基础设施中证书的颁发、撤销等复杂的管理问题,Shamir 在美密会上提出了身份基密码学(Identity-based Cryptography, IBC)的概念[9].在 IBC 中,用户的证件号码、电话号码、邮箱地址等唯一的身份信息将直接作为用户的公钥,其对应的用户秘密钥由可信第三方—密钥生成中心(Key Generation Center,KGC)为其生成,由于身份唯一信息与用户间具有自然的绑定关系,因此无需额外的证书来完成两者间的联系,所以简化了传统公钥基础设施中证书的复杂管理问题;然而,在 IBC 中由于 KGC 完全掌握任意用户的秘密钥,能够代替用户完成密文解密、签名合法性验证等操作,导致 IBC 中存在密钥托管的问题.在继承 IBC 中密钥管理优势的同时,为进一步解决 IBC 的密钥托管问题,Gentry 于 2003 年提出了基于证书的密码学(Certificate-Based Cryptography, CBC)的概念[10].在 CBC 中,用户自主完成公私钥的生成,KGC 负责为用户生成一个秘密的证书,该证书配合用户秘密钥完成相应的计算,由于 KGC 无法掌握用户的具体秘密钥,因此 KGC 无法代替任何用户执行密文解密、签名合法性验证等相关私有操作,上述优势使得 CBC 在现实应用中得到了广泛地关注.事实上,在 CBC 中,用户拥有秘密钥和证书两种不同的秘密信息.

作为保障消息完整性的重要基础工具,签名机制在各种应用协议(如身份认证、消息传输等)的构造中被广泛使用,因此需要具备抵抗泄露攻击的能力以增强上层应用协议的安全性.文献[11]提出了具有抗泄露攻击能力的群签名机制的形式化定义及安全模型,并在此基础上给出相应的实例化构造;针对环签名机制的抗泄露需求,文献[12]给出了具体构造,并对相应设计的安全性进行了形式化证明;文献[13]以对偶加密系统为底层核心工具,设计了对偶形式的抗泄露签名机制;文献[14]设计了抵抗泄露攻击的身份基签名机制;文献[15]提出具有轻量化验证性能的抗泄露加密数据聚合机制,该机制为智能电网提供将同一区域智能电表的数据加密聚合后在云服务器中长期存储;文献[16]设计了防泄露的密码输入机制,其主要思想是打破底层密码和敌手可观察到的交互间的相关性;针对认证密钥协商协议的抗泄露性需求,文献[17]提出无证书的抗泄露密钥协商协议的具体构造,并在支持泄露询问的 *e*CK(扩展的 Canetti Krawczyk)安全模型中证明了上述协议的安全性;文献[18]研究了基于证书的签名(Certificate-Based Signature, CBS)机制的抗泄露性,并提出了相应的构造方案,同时作者对该方案

的安全性进行了证明，然而该构造仅能抵抗有界的泄露攻击，由于实际应用中敌手能够通过持续的泄露攻击破坏密码原语的安全性，因此需要研究抗泄露性能更佳的 CBS 机制以满足现实环境的实际应用需求.

上述分析发现，近年来对 CBS 抗连续泄露性的研究并未引起密码学研究者的过多关注，鉴于基于证书密码体制的性能优势，针对 CBS 机制的抗连续泄露性需求，结合实际应用环境消息完整性的保护需要及合法性的验证目标，本文将开展 CBS 机制的高效构造方法和抗连续泄露性的相关研究工作，并取得了下述成果：

(1) 研究抗泄露的 CBS 机制，并基于离散对数(Discrete Logarithm，DL)问题的困难性在随机谕言机(Random Oracle，RO)模型下使用分叉引理(Forking Lemma)对本文 CBS 方案的不可伪造性进行形式化证明；此外，为提升 CBS 的计算效率，本文在不使用双线性映射的前提下构造了具体的实例化方案.

(2) 由于现实环境中，敌手能够通过连续执行泄露攻击的方式对密码机制的安全性进行持续破坏，因此抵抗连续泄露攻击的 CBS 机制更加接近现实环境的实际应用需求，针对上述需求本文在抗泄露 CBS 机制的研究基础上，通过对用户私钥提供定期更新的方式设计了抗连续泄露的 CBS 机制.

(3) 无线传感器的大面积部署和可穿戴设备的普及，改变了现有的生产生活方式；并且上述设施均具有低功耗的特征，因此迫切需要高传输效率和低计算消耗的密码机制为其提供必要的安全保护. 为提升消息签名的合法性验证效率，聚合签名这一新密码原语被研究者提出，它在提高消息签名传输效率的同时，能够提升签名合法性的验证效率. 鉴于聚合签名所具备的上述优势，本文在抗泄露 CBS 机制的基础之上，进一步研究了基于证书聚合签名(Certificate-Based Aggregate Signature，CBAS)机制的抗泄露性. 通过设计相应的聚合算法和聚合签名的合法性验证算法，提出 CBAS 机制的具体构造，并以智能电网为应用场景对上述机制的具体应用进行阐述.

本文第 2 节主要介绍相关基础知识；第 3 节将回顾无证书签名机制的形式化定义及抗泄露的安全模型；抗泄露 CBS 机制和抗连续泄露 CBS 机制的具体构造分别在第 4 节和第 5 节中提出；第 6 节给出抗泄露 CBAS 机制的具体设计，同时简要介绍该机制在智能电网的具体应用过程；最后是本文的结束语.

2　基础知识

本文中，用 κ 表示安全参数；$a \leftarrow_R A$ 表示从集合 A 中均匀随机的选取元素 a；$\mathrm{negl}(\kappa)$ 表示在 κ 上计算可忽略的值；$x \leftarrow \mathcal{A}(y)$ 表示算法 $\mathcal{A}$ 在输入 y 的作用下输出相应的计算结果 x.

2.1　统计距离和最小熵

令 $\mathrm{SD}(X,Y)=\frac{1}{2}\sum_{w\in\Omega}|\Pr[X=w]-\Pr[Y=w]|$ 表示有限域 Ω 上任意两个随机变量 X 与 Y 间的统计距离.

定义 1.　令 $H_\infty(X)=-\log(Max_x \Pr[X=x])$ 表示随机变量 X 的最小熵.

定义 2.　在变量 Y 已知时，随机变量 X 的平均最小熵为 $\widetilde{H}_\infty(X|Y)=-\log(E_{y\leftarrow Y}[2^{-H_\infty(X|Y=y)}])$，其中 E 是数学期望运算.

2.2　二源提取器

定义 3.　二源提取器[19]. 对于满足条件 $H_\infty(A)\geq l_n$ 和 $H_\infty(B)\geq l_m$ 的两个任意随机变量 $A\in\{0,1\}^{l_n}$ 和 $B\in\{0,1\}^{l_m}$，若 $\mathrm{SD}(2\text{-}\mathrm{Ext}(A,B),U_m)\leq\varepsilon$ 成立，则 $2\text{-}\mathrm{Ext}:\{0,1\}^{l_n}\times\{0,1\}^{l_m}\rightarrow\{0,1\}^{l_k}$ 是 (l_n,l_m,ε)-二源提取器，其中 ε 是安全参数上可忽略的值，$U_m\leftarrow_R\{0,1\}^{l_k}$ 是随机选取的变量.

2.3　困难性假设

定义 4.　DL 困难性假设. 令 G 是一个生成元为 P 的 q 阶加法循环群，已知 $aP\in G$ 且 $a\in Z_q^*$，DL 问题的目标是求解 a 的值.

对于给定的挑战元组 $(P,aP)\in G\times G$，任意的概率多项式时间算法 $\mathcal{A}$ 成功解决 DL 问题的优势

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DL}}(\kappa)=\Pr(\mathcal{A}(aP,P)=a)\leq\mathrm{negl}(\kappa)$$

是可忽略的.

2.4　单向函数

对于单向函数 $\mathrm{Fun}:\{0,1\}^{l_a}\rightarrow\{0,1\}^{l_b}$ 而言，当下述性质成立时，则称该函数具有抗泄露的单向性[20].

令 $\mathcal{A}$ 是攻击单向函数 $\mathrm{Fun}:\{0,1\}^{l_a}\rightarrow\{0,1\}^{l_b}$ 的敌手，那么它攻击成功的优势定义为

$$\mathrm{Adv}_{\mathcal{A}}(\kappa,\lambda)=\Pr\left[\begin{array}{l|l} x\neq x^* & x^*\leftarrow_R\{0,1\}^{l_a} \\ \mathrm{Fun}(x)=y^* & y^*=\mathrm{Fun}(x^*) \\ & x\leftarrow\mathcal{A}^{\mathcal{O}_{\mathrm{Leak}}(\cdot)}(y^*)\end{array}\right],$$

其中 $\mathcal{O}_{\mathrm{Leak}}(\cdot)$ 是泄露谕言机，输入高效可计算的泄露函数 $f:\{0,1\}^{l_a}\rightarrow\{0,1\}^*$，获得相应的泄露信息 f

(x^*)，敌手获得泄露信息的最大量为 λ 比特[20].

若敌手 $\mathcal{A}$ 的优势 $\mathrm{Adv}_{\mathcal{A}}(\kappa,\lambda)$ 是可忽略的，那么 $\mathrm{Fun}:\{0,1\}^{l_a}\rightarrow\{0,1\}^{l_b}$ 是 λ 泄露容忍的单向函数，其中 $\lambda\leq l_a-l_b-\omega(\log\kappa)$，$\omega(\log\kappa)$ 表示计算中的额外泄露量. 对于任意的单向函数 $\mathrm{Fun}:\{0,1\}^{l_a}\rightarrow\{0,1\}^{l_b}$ 而言，当条件 $\lambda\leq l_a-l_b-\omega(\log\kappa)$ 成立时，函数 Fun 具备抵抗泄露攻击的能力，其所能容忍的最大泄露量为 $l_a-l_b-\omega(\log\kappa)$[20].

特别地，单向函数的抗泄露性表明，对于任意的敌手，即使敌手获得单向函数输入的部分泄露信息，也无法伪造该单向函数的一个新输入，使其与原始输入具有相同的输出.

2.5 分叉引理

文献[21-22]对分叉引理及使用方法进行了详细介绍，由于篇幅所限且内容相似，本文不再赘述分叉引理，但由上述介绍可知，若存在一个多项式时间敌手能以明显的优势 ε 输出一个伪造签名，那么存在一个模拟器通过更改哈希谕言机输出的方式对该敌手进行重放，使其能以显而易见的优势 $\left(1-\frac{1}{e}\right)\frac{\varepsilon}{q_H}$ 输出两个有效伪造签名，其中 e 是自然对数底数，q_H 是敌手询问哈希谕言机的次数. 此时，模拟器通过借助上述两个伪造签名能以不可忽略的优势解决相应复杂假设的困难性.

3 基于证书的签名机制

在现有 CBS 相关工作[23-24]的基础上，本节将介绍 CBS 的形式化定义及相应的抗泄露安全模型.

3.1 形式化定义

CBS 方案由下述 5 个算法组成：

(1) 初始化. $\mathrm{Setup}(1^\kappa)$ 由 KGC 执行，通过输入安全参数 κ，输出相应的系统公开参数 $Params$ 和系统主密钥 msk，其中 $Params$ 还定义了用户身份空间 $\mathcal{ID}$ 和公私钥空间 $\mathcal{PK}\times\mathcal{SK}$，该算法可表示为 $(Params,msk)\leftarrow\mathrm{Setup}(1^\kappa)$. 特别地，$Params$ 是下述算法的公共输入，为了方便描述故将其省略.

(2) 密钥生成. $\mathrm{KeyGen}(id)$ 由用户自己执行，通过输入用户的身份 id，输出该用户的公私钥对 (pk_{id},sk_{id})，其中 pk_{id} 是公钥，sk_{id} 是私钥，该算法可表示为：$(pk_{id},sk_{id})\leftarrow\mathrm{KeyGen}(id)$.

(3) 证书生成. $\mathrm{CertGen}(msk,id,pk_{id})$ 由 KGC 负责执行，输入系统主密钥 msk，用户身份 id 和用户公钥 pk_{id}，输出该用户的证书 $Cert_{id}$，该算法可表示为：$Cert_{id}\leftarrow\mathrm{CertGen}(msk,id,pk_{id})$.

(4) 签名. $\mathrm{Sign}(\cdot)$ 由签名者执行，通过输入签名者的身份 id，私钥 sk_{id} 和证书 $Cert_{id}$，以及待签名消息信息 m，输出对应的签名 σ. 该算法可表示为 $\sigma\leftarrow\mathrm{Sign}(id,sk_{id},Cert_{id},m)$.

(5) 签名验证. 输入签名者的身份 id 和公钥 pk_{id}，以及相应的消息 m 和签名值 σ，若 σ 是有效签名，则签名验证算法 $\mathrm{Verify}(\cdot)$ 输出 1，否则输出 0，该算法可表示为 $1/0\leftarrow\mathrm{Verify}(id,\sigma,pk_{id},m)$.

CBS 的正确性要求：对于任意用户的身份 id，有等式 $\mathrm{Verify}(id,pk_{id},m,\mathrm{Sign}(id,sk_{id},Cert_{id},m))=1$ 成立，其中 $(pk_{id},sk_{id})\leftarrow\mathrm{KeyGen}(id)$ 和 $Cert_{id}\leftarrow\mathrm{CertGen}(msk,id,pk_{id})$.

特别地，基于证书的密码体制中，KGC 为用户生成秘密的证书，与用户的私钥一起使用. 在具体构造中 KGC 同时会为证书生成公开的合法性辅助验证信息，该信息是以公开参数的方式对外公布，但该辅助消息并不属于公钥的一部分，该信息由 KGC 负责公布.

3.2 安全模型

在 CBC 中，KGC 虽掌握了系统主密钥但其无法生成用户的完整公私钥对，因此在 CBC 中无需假设 KGC 是完全可信的第三方(这更加接近现实环境的实际情况，因为实际应用中构建完全可信的第三方是相对比较困难的)，那么对于 CBS 机制而言，签名者、签名验证者和 KGC 都有可能对方案的安全性进行攻击，其中恶意的用户能够通过替换其他用户公钥的方式对 CBS 方案进行攻击，基于替换公钥的方式使得外界相信攻击者所公布的公钥信息就是某个特定用户的公钥；而恶意的 KGC 能够利用掌握系统主密钥的这一优势进行攻击，即基于主密钥计算获得任意用户的证书. 特别地，KGC 并不对外泄露其所掌握的主私钥. 因此 CBS 将受到两类敌手的攻击，分别记为第一类敌手 $\mathcal{A}^1$ 和第二类敌手 $\mathcal{A}^2$.

(1) 第一类敌手 $\mathcal{A}^1$(即恶意用户)：此类敌手无法掌握系统的主密钥，但其具有替换合法用户公钥的能力. 此外，对 $\mathcal{A}^1$ 的限制是：① $\mathcal{A}^1$ 不能对挑战身份进行私钥生成询问和证书生成询问；② $\mathcal{A}^1$ 在挑战阶段之前不能替换挑战身份所对应的公钥.

(2) 第二类敌手 $\mathcal{A}^2$(即恶意 KGC)：此类敌手可掌握系统的主密钥，但其不具有替换合法用户公钥的能力. 此外，对 $\mathcal{A}^2$ 的限制是：① $\mathcal{A}^2$ 不能对挑战身份 id^* 进行私钥生成询问，此外 $\mathcal{A}^2$ 无需进行证书生成询问($\mathcal{A}^2$ 可自行计算任意用户的证书)；② $\mathcal{A}^2$ 不能替

换任何用户的公钥.

在泄露环境下，CBS 适应性选择消息攻击下存在不可伪造性(Existential Unforgeability Against Adaptive Chosen Message，EUF-CMA)的安全实验如图 1 所示，其中 $\mathcal{O}^{\text{KeyGen}}(\cdot)$ 是密钥生成谕言机，敌手能够向 $\mathcal{O}^{\text{KeyGen}}(\cdot)$ 进行关于任意身份的密钥生成询问. $\mathcal{O}^{\text{CertGen}}(\cdot)$ 是证书生成谕言机，敌手能够向 $\mathcal{O}^{\text{CertGen}}(\cdot)$ 进行关于任意身份的证书生成询问；$\mathcal{O}^{\text{CertGen}}_{\neq id^*}(\cdot)$ 表示敌手能够对除 id^* 之外的任意身份进行证书生成询问. $\mathcal{O}^{\text{Sign}}(\cdot)$ 是签名谕言机，敌手能就任意的身份消息对 (id, M) 向 $\mathcal{O}^{\text{Sign}}(\cdot)$ 进行签名生成询问，并在对应的列表 L_{Sign} 中记录相应的询问信息 (id, M)，此处 L_{Sign} 的作用是用来跟踪敌手对 $\mathcal{O}^{\text{Sign}}(\cdot)$ 的询问，防止敌手使用 $\mathcal{O}^{\text{Sign}}(\cdot)$ 的应答信息进行挑战. $\mathcal{O}^{\text{Leakage}}_{sk}(\cdot)$ 和 $\mathcal{O}^{\text{Leakage}}_{Cert}(\cdot)$ 是泄露谕言机，敌手能够向 $\mathcal{O}^{\text{Leakage}}_{sk}(\cdot)$ 进行泄露询问并获得相关用户私钥的泄露信息，但同一私钥泄露信息的总量不超过系统设定的泄露啊参数 λ_1(称其为用户私钥泄露参数)；敌手能够向 $\mathcal{O}^{\text{Leakage}}_{Cert}(\cdot)$ 进行泄露询问并获得用户证书的泄露信息(证书的泄露信息实质上是主密钥的泄露)，但关于证书泄露信息的总量不超过系统设定的泄露参数 λ_2(称其为主密钥泄露参数). $\mathcal{O}^{\text{Re}}(\cdot)$ 是公钥替换谕言机，敌手 $\mathcal{A}^1$ 能将任意身份 id 的公钥 pk_{id} 替换为 pk'_{id}. 此外，由于 $\mathcal{A}^2$ 已掌握主密钥，能够自行计算任意用户的证书，因此 $\mathcal{A}^2$ 无需进行证书生成询问.

$\text{Ext}^{\text{EUF-CMA}}_{\mathcal{A}^1}(\kappa)$

$(Params, msk) \leftarrow \text{Setup}(1^\kappa)$;

$(\delta^*, id^*, m^*) \wedge (id^*, m^*) \notin L_{\text{Sign}} \leftarrow (\mathcal{A}^1)^{\mathcal{O}^{\text{KeyGen}}(\cdot), \mathcal{O}^{\text{CertGen}}_{\neq id^*}(\cdot), \mathcal{O}^{\text{Leakage}}_{sk}(\cdot), \mathcal{O}^{\text{Leakage}}_{Cert}(\cdot), \mathcal{O}^{\text{Re}}(\cdot), \mathcal{O}^{\text{Sign}}(\cdot)}(Params)$;

若 1=Verify(δ^*, id^*, m^*)，输出 1；否则，输出 0.

$\text{Ext}^{\text{EUF-CMA}}_{\mathcal{A}^2}(\kappa)$

$(Params, msk) \leftarrow \text{Setup}(1^\kappa)$;

$(\delta^*, id^*, m^*) \wedge (id^*, m^*) \notin L_{\text{Sign}} \leftarrow (\mathcal{A}^2)^{\mathcal{O}^{\text{KeyGen}}(\cdot), \mathcal{O}^{\text{Leakage}}_{sk}(\cdot), \mathcal{O}^{\text{Leakage}}_{Cert}(\cdot), \mathcal{O}^{\text{Sign}}(\cdot)}(Params, msk)$;

若 1=Verify(δ^*, id^*, m^*)，输出 1；否则，输出 0.

图 1　CBS 机制不可伪造性的安全模型

对于任意的概率多项式时间敌手 $\mathcal{A}^i (i=1,2)$，在上述相应的安全性实验中获胜的优势定义如下：

$$\text{Adv}^{\text{EUF-CMA}}_{\mathcal{A}^i}(\kappa) = \Pr(\text{Ext}^{\text{EUF-CMA}}_{\mathcal{A}^i}(\kappa) = 1).$$

定义 5.　适应性选择消息攻击下存在不可伪造性. 对于敌手 $\mathcal{A}^1$ 和 $\mathcal{A}^2$，若其在实验 $\text{Ext}^{\text{EUF-CMA}}_{\mathcal{A}^1}(\kappa)$ 和 $\text{Ext}^{\text{EUF-CMA}}_{\mathcal{A}^2}(\kappa)$ 中获胜的优势 $\text{Adv}^{\text{EUF-CMA}}_{\mathcal{A}^1}(\kappa)$ 和 $\text{Adv}^{\text{EUF-CMA}}_{\mathcal{A}^2}(\kappa)$ 分别是可忽略的，那么在泄露环境下相应的 CBS 机制在适应性选择消息攻击下是存在性不可伪造的.

4　基于证书的抗泄露签名机制

本节我们将提出抗泄露 CBS 机制的具体构造 $\Pi = (\text{Setup}, \text{KeyGen}, \text{CertGen}, \text{Sign}, \text{Verify})$，并基于 DL 困难问题在随机谕言机模型下借助分叉引理对方案的安全性进行形式化证明.

4.1　具体构造

(1) 初始化

算法 $(Params, msk) \leftarrow \text{Setup}(1^\kappa)$ 的主要操作包括：

设 G 是阶为 p 的加法循环群，P 是群 G 的生成元；选取安全单向哈希函数 $H_1: \mathcal{ID} \times G \times G \rightarrow Z_p^*$ 和 $H_2: \mathcal{ID} \times G \times G \times G \times \{0,1\}^* \rightarrow Z_p^*$.

令 2-Ext: $\{0,1\}^{l_n} \times \{0,1\}^{l_m} \rightarrow Z_p^*$ 是 $(l_n, l_m, \varepsilon_2)$ 二源提取器，ε_2 是 κ 上可忽略的值；Fun: $G \rightarrow \{0,1\}^{l_b}$ 是泄露参数为 λ 的抗泄露单向函数，其中有 $\lambda \leq \log p - l_b - \omega(\log\kappa)$.

随机选取 $m_1 \leftarrow_R \{0,1\}^{l_n}$ 和 $m_2 \leftarrow_R \{0,1\}^{l_m}$，并计算 $\alpha = 2\text{-Ext}(m_1, m_2)$ 和 $P_{pub} = \alpha P$.

秘密保存系统主密钥 $msk = \alpha$，并公开系统参数 $Params = \{p, G, P, P_{pub}, H_1, H_2, \text{Fun}, 2\text{-Ext}\}$.

特别地，主密钥 α 由二源提取器 2-Ext 基于两个随机字符串 m_1 和 m_2 生成. 对于任意敌手而言，由 2-Ext 的安全性可知当主密钥 α 的泄露信息不多于 $l_m + l_n - \log q - \omega(\log\kappa)$ 时，α 依然具有足够的随机性. 此外，KGC 基于主密钥 α 为所有用户生成相应的证书，系统建立后所有用户的证书都是基于相同的主密钥 α 生成.

(2) 密钥生成

算法 $(pk_{id}, sk_{id}) \leftarrow \text{KeyGen}(id)$ 的主要操作包括：

用户 U_{id}(令身份为 id)生成相应的公私钥 (sk_{id}, pk_{id}).

$$sk_{id} = s \text{ 和 } pk_{id} = sP,$$

其中 $s \leftarrow_R Z_p^*$.

(3) 证书生成

算法 $Cert_{id} \leftarrow \text{CertGen}(msk, id, pk_{id})$ 的主要操作包括：

KGC 基于用户 U_{id} 的身份 id 和公钥 pk_{id} 为其生成相应的证书 $Cert_{id} = (X_{id}, y_{id})$，其中 $x_{id} \leftarrow_R Z_p^*$，$X_{id} = x_{id} P$ 和 $y_{id} = x_{id} + \alpha H_1(id, X_{id}, pk_{id})$，其中 X_{id} 是用于证书合法性验证的辅助公开信息，并且 KGC 将 X_{id} 对外公布. 特别地，X_{id} 是由 KGC 负责公开的辅助信息，并不属于用户的公钥.

用户收到证书 $Cert_{id}$ 后，可由下述等式验证 $Cert_{id}$ 的合法性.

$$y_{id}P=X_{id}+P_{pub}H_1(id,X_{id},pk_{id}).$$

(4) 签名

签名算法 $\delta\leftarrow\text{Sign}(id,sk_{id},Cert_{id},m)$ 的主要操作包括：

① 随机选取 $n_1\leftarrow_R\{0,1\}^{l_n}$ 和 $n_2\leftarrow_R\{0,1\}^{l_m}$，并计算

$$t=2\text{-Ext}(n_1,n_2)\text{和 }T=tP.$$

② 计算

$$z=t+h_2(y_{id}+sk_{id}),$$

其中 $h_2=H_2(id,pk_{id},X_{id},T,m)$.

③ 输出对消息的签名 $\delta=\{T,z\}$.

特别地，在签名算法中基于二源提取器 2-Ext 实现了签名随机数 t 的抗泄露性处理. 对于任意敌手而言，由 2-Ext 的安全性可知当 t 的泄露信息不多于 $l_m+l_n-\log q-\omega(\log\kappa)$ 时，t 依然具有足够的随机性. 通过二源提取器实现了随机数的抗泄露性. 换句话讲，本文构造所能容忍的随机数的最大泄露量为 $l_m+l_n-\log q-\omega(\log\kappa)$，其中 $\omega(\log\kappa)$ 表示额外的计算消耗.

(5) 合法性验证

收到签名 $\delta=\{T,z\}$ 后，接收者执行验证算法 $1/0\leftarrow\text{Verify}(\delta,m,pk_{id})$，主要操作包括：

首先计算

$$V=T+h_2(X_{id}+P_{pub}H_1(id,X_{id},pk_{id})+pk_{id}),$$

其中 $h_2=H_2(id,pk_{id},X_{id},T,m)$.

然后验证等式

$$\text{Fun}(zP)=\text{Fun}(V).$$

是否成立，若该等式成立则输出 1；否则输出 0.

特别地，在签名验证阶段，基于抗泄露单向函数 $\text{Fun}:G\rightarrow\{0,1\}^{l_b}$ 实现抵抗泄露攻击的目的，当泄露信息的长度满足条件 $\lambda\leq\log p-l_b-\omega(\log\kappa)$ 时，确保其输出依然是随机的分布，敌手无法伪造出该函数的合法输出. 也就是说，敌手在已知私钥泄露信息的前提下，无法伪造一个值 z(签名 $\delta=\{T,z\}$ 的核心元素，同时也是单向函数的输入)使得 $\text{Fun}(zP)=\text{Fun}(V)$ 成立，抗泄露单向函数的使用保证了在用户私钥泄露的前提下签名是不可伪造的. 综上所述，抗泄露密码机制的设计核心是确保秘密信息在存在泄露的情况下对任意的攻击者而言是随机的.

4.2 正确性

本文构造的正确性将由下述等式获知.

$$\begin{aligned}zP&=(t+h_2(y_{id}+sk_{id}))P\\&=(t+h_2(x_{id}+\alpha H_1(id,X_{id},pk_{id})+sk_{id}))P\\&=T+h_2(X_{id}+P_{pub}H_1(id,X_{id},pk_{id})+pk_{id})\\&=V;\end{aligned}$$

其中 $h_2=H_2(id,pk_{id},X_{id},T,m)$.

4.3 安全性证明

本节在适应性选择消息攻击下，基于 DL 困难性假设，对本文 CBS 机制的不可伪造性进行形式化证明. 特别地，对于 CBS 而言，有两类秘密状态需要进行保护，其中一类是主密钥，另外一类是用户私钥；任意敌手能够通过证书所参与的相关运算得到主密钥的部分泄露信息. 在 CBS 机制中，主密钥是由 KGC 持有，用户保存私钥和相应的证书，因为主密钥用于生成用户的证书，同样需提供抗泄露性的保护，因此本文对主密钥和用户私钥分别进行了抗泄露性处理.

在本文 CBS 的安全性证明中，我们将通过两个泄露参数 λ_1 和 λ_2 分别刻画主密钥和用户私钥的抗泄露能力，其中 λ_1 是主密钥的泄露参数，λ_2 是用户私钥的泄露参数. 此外，由于 CBS 机制将面临两类敌手 $\mathcal{A}^1$ 和 $\mathcal{A}^2$ 的攻击，下面将分别证明在上述两类敌手选择消息攻击下本文 CBS 机制的不可伪造性. 特别地，在定理 2 的证明中，挑战者需向敌手 $\mathcal{A}^2$ 提供主私钥，因此困难性问题不能嵌入到主公钥中.

定理 1. 第一类敌手 $\mathcal{A}^1$ 选择消息攻击下的不可伪造性. 在随机谕言机模型下，对于主密钥的泄露参数 $\lambda_1\leq l_m+l_n-\log p-\omega(\log\kappa)$ 和用户私钥的泄露参数 $\lambda_2\leq\log p-l_b-\omega(\log\kappa)$，若 $\mathcal{A}^1$ 能在多项式时间内以不可忽略的优势 $\varepsilon_1(\kappa)$ 攻破本文 CBS 机制的不可伪造性，那么存在一个算法 $\mathcal{C}$ 在多项式时间内能以明显的优势

$$\left(1-\frac{1}{\text{e}}\right)\frac{\varepsilon_1(\kappa)}{\text{e}(q_1+q_2+1)q_{H_1}}$$

成功解决 DL 问题的困难性，其中 q_1 为 $\mathcal{A}^1$ 提交的证书生成询问的次数，q_2 为 $\mathcal{A}^1$ 提交的密钥生成询问的次数，q_{H_1} 为 $\mathcal{A}^1$ 进行谕言机 H_1 询问的次数，e 是自然对数底数.

特别地，定理 1 证明过程中 H_2 不是谕言机，仅是正常的单向哈希函数，因此证明过程未涉及对上述函数的询问应答介绍.

证明. 假设挑战者 $\mathcal{C}$ 是解决 DL 问题的一个敌手，其输入是 DL 困难问题的挑战元组 (P,aP)，目标是求解未知的随机数 a. $\mathcal{C}$ 与敌手 $\mathcal{A}^1$ 间的消息交互过程如下所述.

初始化. 挑战者$\mathcal{C}$令 $P_{pub}=aP$(隐含设定主密钥 $msk=a$,但是$\mathcal{C}$不掌握主密钥),并随机选取单向哈希函数 $H_2:\mathcal{ID}\times G\times G\times G\times\{0,1\}^*\rightarrow Z_p^*$,输出公开参数 $Params=\{p,G,P,P_{pub},H_1,H_2,\text{Fun},\text{2-Ext}\}$ 给$\mathcal{A}^1$,其中 H_1是谕言机,同时维持初始为空的列表 L_k,L_c和L_{H_1}分别用于跟踪$\mathcal{A}^1$对用户密钥生成,证书生成和谕言机 H_1的询问应答信息,其中 L_{H_1},L_k和 L_c的元组格式分别为$(id_i,pk_{id_i},h_{id_i}^1)$,$(id_i,pk_{id_i},sk_{id_i})$和$(id_i,cert_{id_i})$. 此外,$\mathcal{C}$基于列表 L_{Sign}完成对敌手$\mathcal{A}^1$所提交的签名询问的跟踪.

询问阶段. 该阶段,$\mathcal{A}^1$能够适应性地进行多项式时间次的下述询问. 在伪造阶段之前,挑战者$\mathcal{C}$无法确定$\mathcal{A}^1$的挑战身份,$\mathcal{C}$只能在$\mathcal{A}^1$的询问过程中适应性地猜测一个挑战身份id',由于$\mathcal{A}^1$共提交了 q_1+q_2+1 个不同的身份,则$\mathcal{C}$能以概率$\dfrac{1}{q_1+q_2+1}$猜中$\mathcal{A}^1$所选择的挑战身份.

(1)密钥生成询问. 当$\mathcal{C}$收到$\mathcal{A}^1$对用户 id_i的密钥生成询问时,若$(id_i,pk_{id_i},sk_{id_i})\in L_k$,则返回相应的$(pk_{id_i},sk_{id_i})$给$\mathcal{A}^1$;否则,随机选取 $s\in Z_q^*$,并计算 $pk_{id_i}=sP$ 和 $sk_{id_i}=s$,在 L_k中添加$(id_i,pk_{id_i},sk_{id_i})$,然后查找 L_k中 id_i所对应的元组$(id_i,pk_{id_i},sk_{id_i})$,返回相应的$(pk_{id_i},sk_{id_i})$给$\mathcal{A}^1$. 特别地,当 $id_i=id'$时,$\mathcal{C}$返回$(pk_{id_i},\perp)$给$\mathcal{A}^1$.

(2)证书生成询问. 当$\mathcal{C}$收到$\mathcal{A}^1$对用户 id_i的证书生成询问(id_i,pk_{id_i})时,若 $id_i=id'$,则游戏终止;否则,执行下述操作:

若$(id_i,Cert_{id_i})\in L_c$,则返回相应的 $Cert_{id_i}$给$\mathcal{A}^1$;否则选取随机值 $y_{id_i}\in Z_q^*$ 和 $h_{id_i}^1\in Z_q^*$,并计算 $X_{id_i}=y_{id_i}P-P_{pub}h_{id_i}^1$,返回 $Cert_{id_i}=(X_{id_i},y_{id_i})$给$\mathcal{A}^1$,添加元组$(id_i,Cert_{id_i})$到 L_c;此外,添加相应的元组$(id_i,pk_{id_i},X_{id_i},h_{id_i}^1)$到 L_{H_1}.

(3)谕言机 H_1询问. 当$\mathcal{C}$收到$\mathcal{A}^1$对 id_i的谕言机 H_1询问时,若$(id_i,pk_{id_i},h_{id_i}^1)\in L_{H_1}$,则返回相应的 $h_{ID_i}^1$给$\mathcal{A}^1$;否则,则$\mathcal{C}$对 id_i先执行密钥生成询问,获得相应的应答$(pk_{id_i},\perp/sk_{id_i})$后,对$(id_i,pk_{id_i})$进行证书生成询问(在该询问中相应的元组$(id_i,pk_{id_i},X_{id_i},h_{id_i}^1)$被添加到列表 L_{H_1}中),然后搜索 L_{H_1}并返回相应的 $h_{ID_i}^1$给$\mathcal{A}^1$.

(4)公钥替换询问. 由于$\mathcal{C}$收到$\mathcal{A}^1$对 id_i的公钥替换询问时,若 $id_i=id'$,则$\mathcal{C}$忽略本次询问;否则,$\mathcal{C}$将 id_i的公钥 pk_{id_i}替换为$\mathcal{A}^1$所提交的 pk'_{id_i}.

(5)用户私钥泄露询问. 由于$\mathcal{C}$能够运行密钥生成算法生成任意用户 id_i的公私钥对(pk_{id_i},sk_{id_i}),因此$\mathcal{C}$返回相应的泄露信息 $f_1(sk_{id_i})$给$\mathcal{A}^1$,其中 $f_1:\{0,1\}^*\rightarrow\{0,1\}^{\lambda_2}$是由$\mathcal{A}^1$提交的高效可计算的泄露函数. 假设$\mathcal{A}^1$提交一次用户私钥泄露询问,并获得不超过 λ_2比特的泄露信息;也就是说,对于同一用户 id_i的私钥 sk_{id_i},$\mathcal{A}^1$获得的最大泄露量为 λ_2比特,即$\sum_{j=1}^{i}f_1(sk_{id_j})\leq\lambda_2$.

(6)证书泄露询问. 由于$\mathcal{C}$能够运行证书生成询问生成任意用户 id_i的证书 $Cert_{id}$,因此$\mathcal{C}$返回相应的泄露信息 $f_2(Cert_{id})$给$\mathcal{A}^1$,其中 $f_2:\{0,1\}^*\rightarrow\{0,1\}^{\lambda_1^i}$是由$\mathcal{A}^1$提交的高效可计算的泄露函数,并且对于所有的证书泄露询问满足条件$\sum_{j=1}^{i}\lambda_1^j\leq\lambda_1$. 也就是说,所有证书泄露询问应答的最大尺寸为 λ_1比特.

(7)签名生成询问. 当$\mathcal{C}$收到$\mathcal{A}^1$关于身份 id_i和消息m_i的签名询问时,$\mathcal{C}$首先生成身份 id_i的相应私钥 sk_{id_i}和证书 $Cert_{id_i}$后,然后运行签名算法 $\sigma_i=\text{Sign}(id_i,m_i,Cert_{id_i},sk_{id_i})$并将相应的结果 σ_i返回给$\mathcal{A}^1$,同时将(id_i,m_i)记录到列表 L_{Sign}中. 特别地,若身份 id_i所对应的公钥 pk_{id_i}被替换,由于$\mathcal{C}$拥有相应的私钥 sk_{id_i},因此直接运行签名生成算法即可输出相应的签名,因此公钥替换询问并不影响$\mathcal{C}$对相应签名询问的应答.

伪造. $\mathcal{A}^1$输出关于挑战身份 id^*和挑战消息 m^*的伪造签名 $\sigma^*=(T^*,z^*)$(其中 $T^*=t^*P$ 和 $z^*=t^*+(x_{id^*}+ah_{id^*}^1+sk_{id^*})h_{id^*}^2$),若 $id^*\neq id'$或$(id^*,m^*)\in L_{\text{Sign}}$,则$\mathcal{C}$终止;否则,由于$\mathcal{C}$无法利用敌手$\mathcal{A}^1$的一次成功伪造解决困难问题,则将要求$\mathcal{A}^1$提供更多的有效伪造签名. 根据分叉引理[21-22]可知,$\mathcal{C}$欲通过更改谕言机 H_1的输出 $\tilde{h}_{id^*}^1$,使得敌手$\mathcal{A}^1$基于相同的随机数 t^*和不同的谕言机应答 $\tilde{h}_{id^*}^1$生成一个新的关于挑战身份 id^*和挑战消息 m^*的有效伪造签名 $\sigma'=(T^*,z')$(其中 $T^*=t^*P$ 和 $z'=t^*+(x_{id^*}+a\tilde{h}_{id^*}^1+sk_{id^*})h_{id^*}^2$),由于上述签名 σ'和 σ^*都是有效的,那么有下述关系成立:

$$\begin{cases}z^*=t^*+(x_{id^*}+ah_{id^*}^1+sk_{id^*})h_{id^*}^2,\\ z'=t^*+(x_{id^*}+a\tilde{h}_{id^*}^1+sk_{id^*})h_{id^*}^2,\end{cases}$$

其中 $h_{id^*}^2=H_2(id^*,pk_{id^*},X_{id^*},T^*,m^*)$.

由上述方程式,$\mathcal{C}$能求得 DL 困难问题的解:

$$a=\frac{z^*-z'}{h_{id^*}^2(h_{id^*}^1-\tilde{h}_{id^*}^1)},$$

那么$\mathcal{C}$利用$\mathcal{A}^1$作为子程序成功地解决了 DL 问题的

困难性.特别地,$\mathcal{C}$通过下述方式更改谕言机 H_1 的输出:首先查找列表 L_{H_1} 中 id^* 所对应的元组$(id^*, pk_{id^*}, X_{id^*}, h^1_{id^*})$,然后随机选取满足条件 $\tilde{h}^1_{id^*} \neq h^1_{id^*}$ 的 $\tilde{h}^1_{id^*} \in Z_q^*$ 返回给敌手$\mathcal{A}^1$,并且$\mathcal{C}$更新 L_{H_1} 中的相关元组$(id^*, pk_{id^*}, X_{id^*}, \tilde{h}^1_{id^*})$.

令$\mathcal{E}_1$表示$\mathcal{A}^1$在询问阶段不终止,$\mathcal{E}_2$表示$\mathcal{A}^1$在伪造阶段不终止,则$\mathcal{A}^1$在询问训练阶段和伪造阶段未终止的概率分别为

$$\Pr(\mathcal{E}_1) \geq \left(1-\frac{1}{q_1+q_2+1}\right)^{q_1} \text{ 和 } \Pr(\mathcal{E}_2) = \frac{1}{q_1+q_2+1}.$$

令$\mathcal{E}_3$表示$\mathcal{A}^1$成功输出两个有效伪造签名 $\sigma^* = (T^*, z^*)$ 和 $\sigma' = (T^*, z')$.由分叉引理[21-22]可知,若$\mathcal{A}^1$输出一个有效伪造签名的概率为 $\varepsilon_1(\kappa)$,那么,$\mathcal{A}^1$成功输出两个有效签名$\sigma^* = (T^*, z^*)$和$\sigma' = (T^*, z')$的概率为

$$\Pr(\mathcal{E}_3) \geq \left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_1(\kappa)}{q_{H_1}}.$$

因此,有

$$\begin{aligned}&\Pr(\mathcal{E}_1 \wedge \mathcal{E}_2 \wedge \mathcal{E}_3)\\ &\geq \left(1-\frac{1}{q_1+q_2+1}\right)^{q_1}\frac{1}{q_1+q_2+1}\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_1(\kappa)}{q_{H_1}}\\ &\geq \left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_1(\kappa)}{\mathrm{e}(q_1+q_2+1)q_{H_1}}.\end{aligned}$$

特别地,主密钥的抗泄露性是由二源提取器实现,由 2-Ext:$\{0,1\}^{l_n} \times \{0,1\}^{l_m} \to Z_p^*$ 的安全性可知:

$$\lambda_1 \leq l_m + l_n - \log p - \omega(\log\kappa);$$

此外,用户私钥的抗泄露性由抗泄露单向函数实现,由 Fun:$G \to \{0,1\}^{l_b}$ 的安全性可知:

$$\lambda_2 \leq \log p - l_b - \omega(\log\kappa).$$

综上所述,对于 $\lambda_1 \leq l_m + l_n - \log p - \omega(\log\kappa)$ 和 $\lambda_2 \leq \log p - l_b - \omega(\log\kappa)$,若 $\varepsilon_1(\kappa)$ 是不可忽略的,那么$\mathcal{C}$至少能以明显的优势

$$\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_1(\kappa)}{\mathrm{e}(q_1+q_2+1)q_{H_1}}$$

成功解决 DL 问题的困难性.特别地,$\omega(\log\kappa)$表示签名机制运行过程中的额外泄露量. 证毕.

定理 2. 第二类敌手$\mathcal{A}^2$选择消息攻击下的不可伪造性.在随机谕言机模型下,对于主密钥泄露参数 $\lambda_1 \leq l_m + l_n - \log p - \omega(\log\kappa)$ 和用户私钥泄露参数 $\lambda_2 \leq \log p - l_b - \omega(\log\kappa)$,若$\mathcal{A}^2$能在多项式时间内以不可忽略的优势 $\varepsilon_2(\kappa)$攻破本文 CBS 机制的不可伪造性,那么存在一个算法$\mathcal{C}$在多项式时间内能以明显的优势

$$\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_2(\kappa)}{2^{\lambda_2}(q_2+1)q_{H_2}}$$

成功解决 DL 问题,其中 q_2 为$\mathcal{A}^2$提交的密钥生成询问的次数,q_{H_2} 为$\mathcal{A}^2$对谕言机 H_2 的询问次数.

特别地,定理 2 证明过程中 H_1 不是谕言机,仅是正常的密码学哈希函数,因此证明过程未涉及对上述函数的询问应答介绍.

证明. 假设挑战者$\mathcal{C}$是解决 DL 问题的一个敌手,其输入是 DL 问题的挑战元组(P, aP),目标是求解未知的随机数 a.$\mathcal{C}$与敌手$\mathcal{A}^2$间的消息交互过程如下所述.

初始化. 挑战者$\mathcal{C}$运行系统初始化算法$(Params, msk) \leftarrow \mathrm{Setup}(1^\kappa)$,并发送系统公开参数 $Params = \{p, G, P, P_{pub}, H_1, H_2, \mathrm{Fun}, \text{2-Ext}\}$和主密钥 msk 给敌手$\mathcal{A}^2$,其中 H_1是谕言机.同时,$\mathcal{C}$维持初始为空的列表 L_k和 L_{H_2} 分别用于跟踪$\mathcal{A}^2$对用户密钥生成和谕言机 H_2的询问应答信息,其中 L_{H_2} 和 L_k的元组格式分别为$(id_i, pk_{id_i}, X_{id_i}, m_i, T_{id_i}, h^2_{id_i})$和$(id_i, pk_{id_i}, sk_{id_i})$.此外,$\mathcal{C}$基于列表 L_{Sign} 完成对敌手$\mathcal{A}^2$签名询问的跟踪.

询问阶段. 该阶段敌手$\mathcal{A}^2$能够适应性的对下述询问进行多项式时间次的询问.在伪造阶段之前,挑战者$\mathcal{C}$无法确定敌手$\mathcal{A}^2$的挑战身份,$\mathcal{C}$在$\mathcal{A}^2$的询问过程中适应性地猜测一个挑战身份 id',由于$\mathcal{A}^2$共提交了 q_2+1 个不同的身份,则$\mathcal{C}$能以概率$\frac{1}{q_2+1}$猜中敌手$\mathcal{A}^2$的挑战身份.

(1)密钥生成询问.当$\mathcal{C}$收到$\mathcal{A}^2$对 id_i的公钥生成询问时,若$(id_i, pk_{id_i}, sk_{id_i}) \in L_k$,则返回$(pk_{id_i}, sk_{id_i})$给$\mathcal{A}^2$,否则执行下述步骤:

① 若 $id_i \neq id'$,随机选择 $s \in Z_q^*$,并计算

$$sk_{id_i} = s \text{ 和 } pk_{id_i} = sP,$$

并在 L_k中添加相应的元组$(id_i, pk_{id_i}, sk_{id_i})$,然后返回$(pk_{id_i}, sk_{id_i})$给$\mathcal{A}^2$;

② 若 $id_i = id'$,令 $pk_{id_i} = aP$(隐含设定 $sk_{id_i} = a$),并在列表 L_k中添加元组$(id_i, pk_{id_i}, \perp)$,然后返回 pk_{id_i}给$\mathcal{A}^2$,其中,$\perp$表示$\mathcal{A}^2$不知道相应的值.

(2) H_2询问.当$\mathcal{C}$收到$\mathcal{A}^2$关于 id_i的谕言机 H_2询问时,查看列表 L_{H_2} 中是否存在 id_i所对应元组$(id_i, pk_{id_i}, X_{id_i}, m_i, T_{id_i}, h^2_{id_i})$,若存在,返回相应的 $h^2_{id_i}$给$\mathcal{A}^2$;若不存在,则$\mathcal{C}$随机选择 $h^2_{id_i} \in Z_q^*$,在 L_{H_2} 中添加相应的元组$(id_i, pk_{id_i}, X_{id_i}, m_i, T_{id_i}, h^2_{id_i})$,并返回相应的 $h^2_{id_i}$给$\mathcal{A}^2$.

(3)用户私钥泄露询问.由于$\mathcal{C}$已掌握除挑战身份之外的其他任何身份 id_i的私钥 sk_{id_i},因此$\mathcal{C}$能够返回相应的泄露信息 $f_1(sk_{id_i})$给敌手$\mathcal{A}^2$;然而,对

于挑战身份 id^* 所对应私钥 sk_{id^*} 的泄露询问，$\mathcal{C}$ 只能通过猜测完成相应的泄露应答，敌手 $\mathcal{A}^2$ 猜测正确的概率为 $\frac{1}{2^{\lambda_2}}$.

签名生成询问与定理 1 相类似，此处不再进行赘述；此外，由于敌手 $\mathcal{A}^2$ 已掌握系统主密钥，能够自主完成任意身份对应证书的计算，因此无需进行证书生成和证书泄露询问.

伪造. $\mathcal{A}^2$ 输出一个关于身份 id^* 和消息 m^* 伪造签名 $\sigma^*=(T^*,z^*)$，若 $id^*\neq id'$ 或 $(id^*,m^*)\in L_{\mathrm{Sign}}$，则 $\mathcal{C}$ 终止；否则，由于 $\mathcal{C}$ 无法利用敌手 $\mathcal{A}^2$ 的一次成功伪造解决困难问题，根据分叉引理[21-22]可知，$\mathcal{C}$ 通过更改谕言机 H_2 的输出 $\tilde{h}^2_{id^*}$（更改方法与定理 1 相类似），使得敌手 $\mathcal{A}^2$ 基于相同的随机数 t^* 生成了一个新的伪造签名 $\sigma'=(T^*,z')$，以进一步解决困难问题. 由于上述签名 σ' 和 σ^* 都是有效的，有下述关系成立：

$$\begin{cases} z^*=t^*+(x_{id^*}+\alpha h^1_{id^*}+a)h^2_{id^*}, \\ z'=t^*+(x_{id^*}+\alpha h^1_{id^*}+a)\tilde{h}^2_{id^*}, \end{cases}$$

基于上述方程式，$\mathcal{C}$ 能求得 DL 困难问题的解

$$a=\frac{z^*-z'}{h^2_{id^*}-\tilde{h}^2_{id^*}}-x_{id^*}-\alpha h^1_{id^*},$$

那么 $\mathcal{C}$ 利用敌手 $\mathcal{A}^2$ 作为子程序成功地解决了离散对数问题的困难性.

令 $\mathcal{F}_1$ 表示 $\mathcal{A}^2$ 在伪造阶段不终止，则 $\mathcal{A}^2$ 在伪造阶段不终止的概率为 $\Pr(\mathcal{F}_1)=\frac{1}{q_2+1}$. 令 $\mathcal{F}_2$ 表示 $\mathcal{A}^2$ 在询问阶段获得了关于用户私钥的正确泄露应答，则 $\Pr(\mathcal{F}_2)=\frac{1}{2^{\lambda_2}}$.

令 $\mathcal{F}_3$ 表示 $\mathcal{A}^2$ 成功输出两个有效伪造签名 $\sigma^*=(T^*,z^*)$ 和 $\sigma'=(T^*,z')$. 由于 $\mathcal{A}^2$ 输出一个有效签名的概率为 $\varepsilon_2(\kappa)$，由分叉引理[21-22]可知，$\mathcal{A}^2$ 成功输出两个有效伪造签名 $\sigma^*=(T^*,z^*)$ 和 $\sigma'=(T^*,z')$ 的概率为

$$\Pr(\mathcal{F}_3)\geq\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_2(\kappa)}{q_{H_2}}.$$

因此，有

$$\begin{aligned}\Pr(\mathcal{F}_1\wedge\mathcal{F}_2\wedge\mathcal{F}_3)&\geq\frac{1}{2^{\lambda_2}}\frac{1}{q_2+1}\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_2(\kappa)}{q_{H_2}}\\&=\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_2(\kappa)}{2^{\lambda_2}(q_2+1)q_{H_2}}.\end{aligned}$$

综上所述，对于 $\lambda_1\leq l_m+l_n-\log p-\omega(\log\kappa)$ 和 $\lambda_2\leq\log p-l_b-\omega(\log\kappa)$，若 $\varepsilon_2(\kappa)$ 是不可忽略的，那么 $\mathcal{C}$ 至少能以明显的优势

$$\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon_2(\kappa)}{2^{\lambda_2}(q_1+1)q_{H_2}}$$

成功解决 DL 问题的困难性，其中泄露参数 λ_1 和 λ_2 的分析过程与定理 1 相类似，此处不再赘述. 证毕.

由定理 1 和定理 2 可知，对于任意的概率多项式时间敌手 $\mathcal{A}^1$ 和 $\mathcal{A}^2$，本文 CBS 机制在适应性选择消息攻击下是存在性不可伪造的. 特别地，本文对主密钥和用户私钥分别进行了抗泄露性处理，其中二源提取器为主密钥提供抗泄露性，单向哈希函数为用户私钥提供抗泄露性.

本文构造能够通过改变相关参数的大小达到适应性调节方案泄露能力的目的，其中通过改变初始化字符串 m_1,m_2 的大小 l_m 和 l_n，实现增加泄露参数 $\lambda_1\leq l_m+l_n-\log p-\omega(\log\kappa)$ 的目的；通过减少抗泄露单向函数 $\mathrm{Fun}:G\rightarrow\{0,1\}^{l_b}$ 的输出长度 l_b，实现增加泄露参数 $\lambda_2\leq\log p-l_b-\omega(\log\kappa)$ 的目的；并且上述调节过程中，本文构造的公私钥是保持不变的，确保在不影响存储和计算效率的前提下实现了 CBS 机制抗泄露能力的调节.

由上述安全性证明过程可知，分叉引理主要协助挑战者通过重放的途径获得两个（或更多）有效的伪造签名，方便挑战者消除用于构造签名的未知随机数，但不能消除困难性问题的相应解，因此分叉引理将作用在困难问题相关解上的哈希函数视为是与其配合使用的随机谕言机，通过谕言机的不同应答将未知的随机数消除，达到求解困难问题解的目的.

5　基于证书的抗连续泄露签名机制

由于抵抗连续泄露攻击的 CBS 机制更接近现实应用环境的实际应用需求，因此本节将在第 4 节 CBS 机制的抗泄露性研究基础上，对抗连续泄露的 CBS 机制展开研究. 文献[25]指出当满足下述两个条件时，相应的抵抗有界泄露攻击的密码机制具备抵抗连续泄露攻击的能力：(1) 用户私钥能够周期性更新，并且更新后的用户私钥与原始私钥是不可区分的，此外无论密钥更新算法被执行多少次相应私钥所对应的公钥始终保持不变；(2) 用户私钥更新前后，相应的密码机制依然保持其原有的性能和安全性，并且在用户私钥更新算法的两次执行间隔内，任意的敌手只能获得有界的泄露信息. 由上述结论可知，虽然连续泄露容忍性较复杂，但它的最大优

点是能够将其通过密钥更新的方式转变为有界泄露容忍性,因此本节将在上述有界泄露容忍的 CBS 机制的基础上设计用户私钥的更新算法.

5.1 具体构造

抗连续泄露 CBS 机制的密钥生成、密钥更新和签名等算法的具体构造如下所述,其他算法如初始化和签名验证等算法与第 4 节的基础 CBS 机制保持一致,此处不再赘述.

(1)密钥生成

算法$(pk_{id},sk_{id})\leftarrow$KeyGen$(id)$的主要操作有:

用户 U_{id}(身份为 id)选取两个随机值 $s_1,s_2\leftarrow_R Z_p^*$,然后计算公私钥对$(sk_{id},pk_{id})$,其中

$$sk_{id}=(s_1,s_2)\text{和 }pk_{id}=(s_1+s_2)P.$$

在保持相应公钥不变的前提下,为方便用户私钥的更新,对用户私钥 sk_{id} 进行秘密分割,使其包含多个分量.

(2)用户私钥更新

用户私钥更新算法 $sk'_{id}\leftarrow$Update(sk_{id})的主要操作包括:

对于原始私钥 $sk_{id}=(s_1,s_2)$,用户 U_{id} 随机选取 $\eta\leftarrow_R Z_p^*$,设置

$$sk'_{id}=(s'_1,s'_2)=(s_1+\eta,s_2-\eta).$$

由公钥 $pk_{id}=(s_1+s_2)P$ 可知,其对应的核心秘密是 s_1+s_2,为保证签名机制的正确性,密钥更新算法在更新用户私钥的同时,不能改变其底层的核心秘密.本文更新后的私钥 $sk'_{id}=(s'_1,s'_2)$ 满足等式 $s'_1+s'_2=s_1+s_2$,因此 $sk'_{id}\leftarrow$Update(sk_{id}) 是正确的.事实上,抗连续泄露性的实质是在密码原语的私钥与公钥间建立多对一的映射,密钥更新操作实现用户私钥空间中各元素间的转换.特别地,公钥事实上确定了方案的底层核心秘密(它们间是一一对应的),实现连续泄露容忍性的本质是需要构建私钥与底层核心秘密的多对一映射,这样就能够实现在私钥更新的同时确保了公钥的不变性.

(3)签名

签名算法$\delta\leftarrow$Sign$(id,sk_{id},Cert_{id},m)$(其中$sk_{id}=(s_1,s_2)$)的主要操作包括:

① 随机选取 $n_1\leftarrow_R\{0,1\}^{l_n}$ 和 $n_2\leftarrow_R\{0,1\}^{l_m}$,然后计算

$$t=2\text{-Ext}(n_1,n_2)\text{和 }T=tP.$$

② 计算

$$z=t+(y_{id}+s_1+s_2)h_2,$$

其中 $h_2=H_2(id,pk_{id},X_{id},T,m)$.

③ 输出对消息的签名 $\delta=\{T,z\}$.

5.2 安全性

密钥更新算法 Update 选取了随机的参数 $\eta\in Z_p^*$ 完成了对原始用户私钥 sk_{id} 的更新,并输出更新后的用户私钥 sk'_{id}.在保证相应公钥 pk_{id} 不变的前提下,通过使用随机数确保 sk'_{id} 和 sk_{id} 对于任意敌手而言是不可区分的,因此算法 Update 满足文献[25]中的条件一.

两次密钥更新算法 Update 执行间隔内任意敌手只能获得关于用户私钥的有界泄露信息,泄露界为 $\lambda_2\leq\log p-l_b-\omega(\log\kappa)$;此外,由底层基础 CBS 机制的抗泄露性可知,上述构造在用户私钥更新前后依然保持其原有的性能和安全性,因此算法 Update 满足文献[25]中的条件二.

综上所述,由底层基础 CBS 机制的抗泄露性和密钥更新算法 Update 的性能可知,上述构造是抗连续泄露的 CBS 机制.

5.3 性能比较

由于目前对抗泄露 CBS 机制的相关研究较少,本节将本文方案与相关抗泄露签名机制的计算效率和性能进行比较,其中计算效率主要统计签名和验证算法对相关密码操作的执行次数;通信效率由签名和公钥的长度衡量;性能分析主要以方案的抗泄露性、密钥托管等安全属性为分析标准.文献[26]提出了抗泄露的无证书签名机制,文献[18]提出了抗泄露的基于证书签名机制,文献[14,27-28]分别提出了三个抗泄露的身份基签名机制,下面将本文方案与上述机制分别进行对比,结果如表 1 和表 2 所示.

表 1 本文构造与相关机制的计算效率比较结果

机制	签名算法	验证算法
文献[14]	$5\mathcal{O}_E+5\mathcal{O}_M$	$2\mathcal{O}_E+2\mathcal{O}_M+3\mathcal{O}_B$
文献[18]	$7\mathcal{O}_E+9\mathcal{O}_M$	$2\mathcal{O}_E+4\mathcal{O}_M+3\mathcal{O}_B$
文献[26]	$6\mathcal{O}_E+6\mathcal{O}_M$	$2\mathcal{O}_E+3\mathcal{O}_M+3\mathcal{O}_B$
文献[27]	$3\mathcal{O}_E+2\mathcal{O}_M$	$1\mathcal{O}_E+2\mathcal{O}_M+2\mathcal{O}_B$
文献[28]	$4\mathcal{O}_E+6\mathcal{O}_M$	$3\mathcal{O}_E+5\mathcal{O}_M+4\mathcal{O}_B$
本文构造	$1\mathcal{O}_N+1\mathcal{O}_{\text{Ext}}$	$2\mathcal{O}_N+2\mathcal{O}_A$

表 2 本文构造与相关机制的通信效率比较结果

机制	签名长度	公钥(或公开参数)长度
文献[14]	$3\mathcal{L}_E$	$6\mathcal{L}_E$
文献[18]	$2\mathcal{L}_E$	$2\mathcal{L}_E$
文献[26]	$2\mathcal{L}_E$	$2\mathcal{L}_E$
文献[27]	$2\mathcal{L}_E$	$3\mathcal{L}_E$
文献[28]	$4\mathcal{L}_E$	$6\mathcal{L}_E$
本文构造	$1\mathcal{L}_E+1\mathcal{L}_A$	$1\mathcal{L}_E+1\mathcal{L}_A$

(1)效率比较

在表 1 中用 $\mathcal{O}_E$ 表示乘法群上的指数运算,$\mathcal{O}_M$

表示乘法群上的元素乘运算，$\mathcal{O}_N$表示加法群上的数乘运算，$\mathcal{O}_A$表示加法群上的加法运算，$\mathcal{O}_B$表示双线性映射运算，$\mathcal{O}_{\text{Ext}}$表示二源提取运算. 各符号前的系数表示相应操作的执行次数.

由表 1 可知，本文构造未使用双线性映射运算，而其他方案[14,18,26-28]均基于双线性映射构造，因此本文构造具有较高的计算效率.

基于 PBC 算法库，在台式电脑(机器配置为 Intel(R) Core i3-2310，CPU@2.10 GHz，4 GB 内存和 Ubuntu 14.04 操作系统)上对上述基本操作的耗时进行测算，通过对基本操作求解 10 次的平均值得到$\mathcal{O}_B \approx 2.483$，$\mathcal{O}_A \approx 0.001$，$\mathcal{O}_N \approx 0.326$，$\mathcal{O}_M \approx 0.059$和$\mathcal{O}_E \approx 0.316$，上述数值的单位为毫秒(ms). 因此本文构造与相关机制[14,18,26-28]的计算耗时比较结果如图 2 所示.

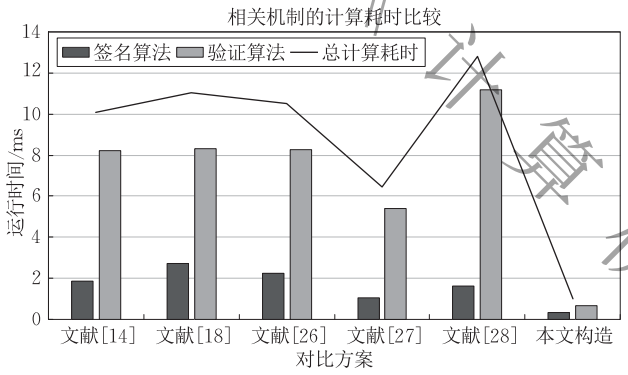

图 2　本文构造与相关机制的计算耗时比较结果

特别地，二源提取操作主要用于生成签名算法所使用的随机数，因此在算法执行前可执行该操作，提前准备好算法所使用的具备抗泄露性能的随机数，因此图 2 中我们并未统计二源提取操作的运行时间.

在表 2 中用$\mathcal{L}_E$表示乘法(或加法)循环群中元素的长度，$\mathcal{L}_A$表示整数的长度. 由表 2 可知，本文构造在获得高计算效率的同时，保持了现有相关构造[26]高通信效率的优势. 相较于本文和文献[26]中的方案，其他构造[14,18,27-28]的通信数据量较大.

(2) 性能分析

由表 3 可知文献[14,18,27]中的方案仅具有抵抗有界泄露攻击的能力，而本文构造和文献[26,28]的方案具备抵抗连续泄露攻击的能力；此外，本文构造和文献[18,26]的方案不仅避免了传统公钥基础设施中的证书管理问题，而且能够解决身份基密码机制[14,26]的密钥托管不足. 与文献[27-28]的方案相比，本文构造具备更佳的计算效率和通信效率.

表 3　本文构造与相关机制的性能比较结果

机制	连续泄露攻击	有界泄露攻击	密钥托管不足
文献[14]	不抵抗	抵抗	存在
文献[18]	不抵抗	抵抗	不存在
文献[26]	抵抗	抵抗	不存在
文献[27]	不抵抗	抵抗	存在
文献[28]	抵抗	抵抗	存在
本文构造	抵抗	抵抗	不存在

6　基于证书的抗泄露聚合签名机制

随着工业物联网的兴起，大量数据需要由底层传感器传输到指定服务器，为保证传输数据的安全性，通常使用签名机制确保消息的不可伪造性. 然而大量数据的签名合法性验证将浪费服务器的计算资源，为进一步提升服务器对数据签名的计算效率，聚合签名机制被提出，能够通过验证聚合签名的合法性完成多个签名的有效性验证. 本节将在第 4 节抗泄露 CBS 机制的基础上，设计抗泄露的 CBAS 机制.

6.1　具体构造

(1) 聚合签名算法

聚合签名算法 $\delta \leftarrow \text{AggSign}(\delta_1, \cdots, \delta_n)$的主要操作包括：

① 聚合者收到 n 个签名 $\delta_i = \{T_i, z_i\}_{i=1,2,\cdots,n}$后，通过计算对单个签名 δ_i中的核心元素 z_i进行聚合.

$$z = \sum_{i=1}^{n} z_i.$$

② 令 $\boldsymbol{T} = \{T_1, T_2, \cdots, T_n\}$.

③ 输出相应的聚合签名 $\delta = \{\boldsymbol{T}, z\}$. 聚合签名将原始 n 个签名的总元素个数由 $2n$ 降低到 $n+1$，长度缩短到原始的二分之一，有效提升了签名的传输效率.

(2) 合法性验证

收到聚合签名 $\delta = \{\boldsymbol{T}, z\}$后，接收者执行聚合验证算法 $1/0 \leftarrow \text{AggVerify}(\delta, \boldsymbol{M}, \boldsymbol{pk}, \boldsymbol{X}_{id})$(其中 $\boldsymbol{M} = \{m_1, \cdots, m_n\}$、$\boldsymbol{pk} = \{pk_{id}^1, \cdots, pk_{id}^n\}$和 $\boldsymbol{X}_{id} = \{X_{id}^1, \cdots, X_{id}^n\}$)，主要操作包括：

首先计算

$$V = \sum_{i=1}^{n} T_i + \sum_{i=1}^{n} h_2^i (X_{id}^i + h_1^i P_{pub} + pk_{id}^i),$$

其中，$h_1^i = H_1(id_i, X_{id}^i, pk_{id}^i)$和 $h_2^i = H_2(id_i, pk_{id}^i, X_{id}^i, T_i, m_i)$.

然后验证等式

$$\text{Fun}(zP) = \text{Fun}(V)$$

是否成立，若该等式成立则输出 1，表示聚合签名对

应的 n 个签名$\{\delta_1,\cdots,\delta_n\}$都是合法的;否则输出 0,表示 n 个签名$\{\delta_1,\cdots,\delta_n\}$中存在非法的签名.

聚合签名验证算法通过执行一次签名验证算法就能完成对 n 个签名的合法性验证,将签名验证算法的执行次数由原始的 n 次,缩减到 1 次,降低了签名机制的计算负载,提升了签名的计算效率.

6.2 正确性

聚合签名 $\delta=\{\boldsymbol{T},z\}$的正确性由下述等式获得:

$$\begin{aligned}zP&=\Big(\sum_{i=1}^{n}z_i\Big)P\\&=\Big(\sum_{i=1}^{n}(t_i+(y_{id}^i+sk_{id}^i)h_2^i)\Big)P\\&=\sum_{i=1}^{n}t_iP+\sum_{i=1}^{n}h_2^i(y_{id}^i+sk_{id}^i)P\\&=\sum_{i=1}^{n}T_i+\sum_{i=1}^{n}h_2^i(x_{id}^i+\alpha h_1^i+sk_{id}^i)P\\&=\sum_{i=1}^{n}T_i+\sum_{i=1}^{n}h_2^i(X_{id}^i+h_1^iP_{pub}+pk_{id}^i)\\&=V,\end{aligned}$$

其中,$h_1^i=H_1(id_i,X_{id}^i,pk_{id}^i)$和 $h_2^i=H_2(id_i,pk_{id}^i,X_{id}^i,T_i,m_i)$.

6.3 抗泄露 CBAS 机制在智能电网中的应用

智能电网建立了双向互动的服务模式,用户可以实时了解供电能力、电能质量、电价状况和停电信息,合理安排电器使用;电力企业可以获取用户的详细用电信息,为其提供更多的增值服务.智能电网建立在集成的、高速双向通信网络基础之上,实现电网可靠、安全、经济、高效地运行,基于双向通信网络实现数据的互通互联,使得数据通信及其合法性验证是智能电网的重要安全性需求,并且数据合法性的验证效率也是衡量智能电网性能的重要指标之一.

如图 3 所示,智能电网在不同位置、区域部署了大量传感器用于收集设备运行情况、用户的用电量等相关信息,每个区域分别部署一个数据聚合者(该聚合者可由区域网络的出口网关充当)完成本区域数据的聚合发送,具体步骤如下:

(1)每个底层的用户数据传感器基于签名算法 Sign 生成相应电力数据 m_j^i 的签名 δ_j^i,并将数据 m_j^i 连同签名 δ_j^i 一起发送给本地网关.

(2)区域网关收到本区域的所有签名$\{\delta_j^1,\cdots,\delta_j^n\}$后,通过聚合算法 AggSign 生成相应的聚合签名 δ_j,并将其发送给管理中心.

(3)管理中心运行聚合验证算法 AggVerify,通过验证聚合签名 δ_j 的合法性,完成对相应区域中所有签名$\{\delta_j^1,\cdots,\delta_j^n\}$的合法性判断.

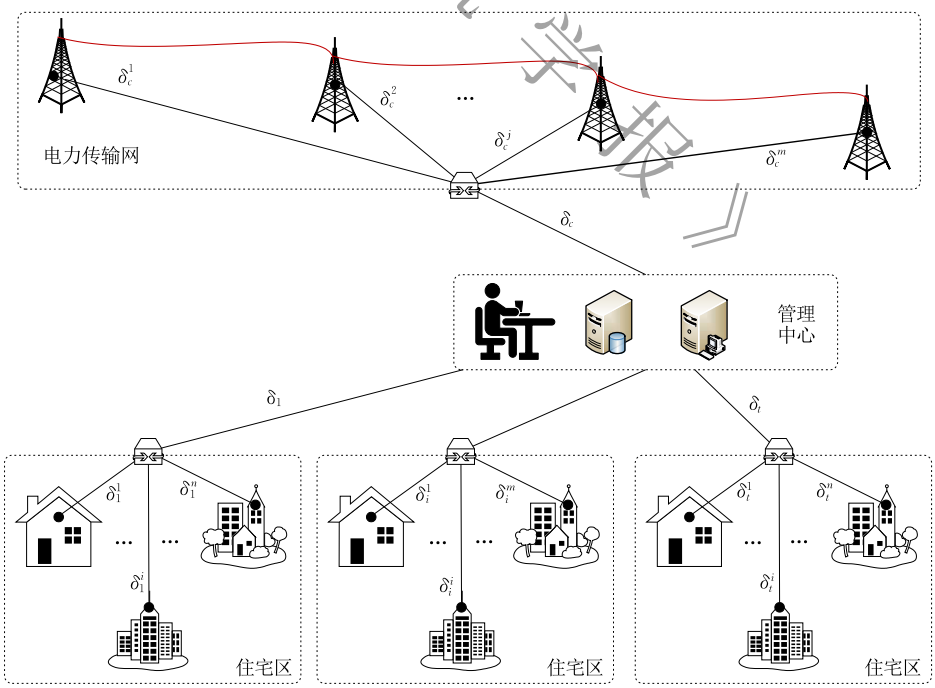

图 3 智能电网中的数据聚合传输

7 结束语

为满足签名机制的抗泄露性需求,本文设计了性能更优的基于证书的抗泄露签名机制,并在随机谕言机模型下基于离散对数问题使用分叉引理对本文实例的不可伪造性进行了形式化证明;同时,由于本文构造并未使用计算量较大的双线性映射运算,

使得本文构造具有更高的计算效率.

由于标准模型下的安全性证明过程更加接近实际应用环境,因此下一阶段将在本文工作的基础上,研究标准模型下抗泄露 CBS 机制的构造.

参 考 文 献

[1] Zhou Yanwei, Yang Bo, Xia Zhe, et al. Novel generic construction of leakage-resilient PKE scheme with CCA security. Designs, Codes and Cryptography, 2021, 89(7): 1575-1614

[2] Zhou Yanwei, Yang Bo, Xia Zhe, et al. Identity-based encryption with leakage-amplified chosen-ciphertext attacks security. Theoretical Computer Science, 2020, 809: 277-295

[3] Lyu Lin, Liu Shengli, Gu Dawu. Structure-preserving public-key encryption with leakage-resilient CCA security. Theoretical Computer Science, 2019, 795: 57-80

[4] Chakraborty S, Rangan C P. Public key encryption resilient to post-challenge leakage and tampering attacks//Proceedings of the Cryptographers' Track at the RSA Conference 2019. San Francisco, USA, 2019: 23-43

[5] Nishimaki R, Yamakawa T. Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio//Proceedings of the 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography. Beijing, China, 2019: 466-495

[6] Zhou Yanwei, Yang Bo. Practical continuous leakage-resilient CCA secure identity-based encryption. Frontiers of Computer Science, 2020, 14(4): 144804

[7] Zhang Leyou, Shang Yujie. Leakage-resilient attribute-based encryption with CCA2 security. International Journal of Network Security, 2019, 21(5): 819-827

[8] Zhang Leyou, Zhang Jingxia, Mu Yi. Novel leakage-resilient attribute-based encryption from hash proof system. The Computer Journal, 2017, 60(4): 541-554

[9] Shamir A. Identity-based cryptosystems and signature schemes //Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 1984: 47-53

[10] Gentry C. Certificate-based encryption and the certificate revocation problem//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Warsaw, Poland, 2003: 272-293

[11] Huang Jianye, Huang Qiong, Susilo W. Leakage-resilient group signature: Definitions and constructions. Information Sciences, 2020, 509: 119-132

[12] Huang Jianye, Huang Qiong, Susilo W. Leakage-resilient ring signature schemes. Theoretical Computer Science, 2019, 759: 1-13

[13] Huang Jianye, Huang Qiong, Susilo W. Leakage-resilient dual-form signatures. The Computer Journal, 2018, 61(8): 1216-1227

[14] Wu Jui-Di, Tseng Yuh-Min, Huang Sen-Shan. Leakage-resilient ID-based signature scheme in the generic bilinear group model. Security and Communication Networks, 2016, 9(17): 3987-4001

[15] Zhang Xiaojun, Huang Chao, Xu Chunxiang, et al. Key-leakage resilient encrypted data aggregation with lightweight verification in fog-assisted smart grids. IEEE Internet of Things Journal, 2021, 8(10): 8234-8245

[16] Li Yan, Cheng Yao, Meng Weizhi, et al. Designing leakage-resilient password entry on head-mounted smart wearable glass devices. IEEE Transactions on Information Forensics and Security, 2021, 16: 307-321

[17] Hsieh Tsung-Che, Tseng Yuh-Min, Huang Sen-Shan. A leakage-resilient certificateless authenticated key exchange protocol withstanding side-channel attacks. IEEE Access, 2020, 8: 121795-121810

[18] Wu Jui-Di, Tseng Yuh-Min, Huang Sen-Shan, Tsai Tung-Tso. Leakage-resilient certificate-based signature resistant to side-channel attacks. IEEE Access, 2019, 7: 19041-19053

[19] Halevi S, Lin Huijia. After-the-fact leakage in public-key encryption//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Warsaw, Poland, 2011: 107-124

[20] Boyle E, Segev G, Wichs D. Fully leakage-resilient signatures. Journal of Cryptology, 2013, 26(3): 513-558

[21] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000, 13(3): 361-396

[22] Yang Bo. Modern Cryptography. 3rd Edition. Beijing: Tsinghua University Press, 2015: 65-69(in Chinese)
(杨波. 现代密码学. 第 3 版. 北京: 清华大学出版社, 2015: 65-69)

[23] Zhou Yanwei, Yang Bo, Wang Tao, et al. Continuous leakage-resilient certificate-based encryption scheme without bilinear pairings. The Computer Journal, 2020, 63(4): 508-524

[24] Li Jiguo, Huang Xinyi, Zhang Yichen, Xu Lizhong. An efficient short certificate-based signature scheme. Journal of Systems and Software, 2012, 85(2): 314-322

[25] Dodis Y, Haralambiev K, López-Alt A, Wichs D. Cryptography against Continuous Memory Attacks//Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010). Las Vegas, USA, 2010: 511-520

[26] Wu Jui-Di, Tseng Yuh-Min, Huang Sen-Shan. Leakage-resilient certificateless signature under continual leakage model. Information Technology and Control, 2018, 47(2): 363-386

[27] Galindo D, Vivek S. A practical leakage-resilient signature scheme in the generic group model//Proceedings of the International Conference Selected Areas in Cryptography. Windsor, Canada, 2012: 50-65

[28] Wu Jui-Di, Tseng Yuh-Min, Huang Sen-Shan, Tsai Tung-Tso. Leakage-resilient revocable identity-based signature with cloud revocation authority. Informatica, 2020, 31(3): 597-620

ZHOU Yan-Wei, Ph. D., associate professor, M. S. supervisor. His current research interests include information security and cryptography.

MA Kui, M. S. candidate. His research interests include information security and cryptography.

QIAO Zi-Rui, Ph. D. candidate. Her research interests include information security and cryptography.

YANG Bo, Ph. D., professor, Ph. D. supervisor. His current research interests include information security and cryptography.

GU Chun-Xiang, Ph. D., professor, Ph. D. supervisor. His current research interest is information security.

Background

The certificate-based cryptography can solve the certificates management problem of the traditional public key infrastructure and avoided the key escrow shortcoming of the identity-based cryptography, which was widely employed in the actual application to create security protocol. Furthermore, the traditional cryptographic primitives cannot obtain their claimed security, because the additional information of the secret states can be captured by the adversary through performing various leakage attacks, such as side channel attacks, cold boot attacks, etc. Therefore, leakage resilience has become a necessary security property of cryptographic primitives.

In this paper, to provide the leakage resilience for the certificate-based signature(CBS) scheme, a concrete construction of leakage-resilient CBS scheme is created without using bilinear mapping operations, and the security of our proposal is proved based on the hardness of discrete logarithm problem by using Forking lemma under the random oracle. Compared with the previous constructions, we have that our construction has provable security while the leakage resilience is provided, and the corresponding computation efficiency is improved. Furthermore, a certificate-based aggregate signature scheme with continuous leakage resilience is created from the above basic CBS scheme, which realizes the validity verification of multiple signatures at the same time and further improves the computation efficiency. Furthermore, compared with the existing CBS schemes, our proposal has certain advantages in security, computation efficiency and communication efficiency.

This work was supported by the National Key R&D Program of China (2017YFB0802000), the National Natural Science Foundation of China(62272287, 61802242, U2001205), the Sichuan Science and Technology Program (2020JDJQ0076), the Research Funds of Guangxi Key Laboratory of Cryptography and Information Security (GCIS202108), and the Research Funds of Henan Key Laboratory of Network Cryptography Technology (LNCT2021-A04).