

# 基于抗泄漏无证书的智能电网隐私保护协议

朱聪聪, 乔 治, 王志伟

(南京邮电大学 计算机学院、软件学院、网络空间安全学院, 江苏 南京 210046)

**摘 要:**作为下一代电力系统,智能电网显著提高了电力服务的可靠性、效率、安全性和可持续性。智能电网技术的进步使得智能电网中的用户可以实时收集用电数据,有助于高效调控当地电力,但也易导致用户信息泄露。如何平衡用户实时电量数据与保护用户隐私是一个至关重要的问题,其中数据聚合和隐私保护是一个可行的解决方案。但是大多数现有的数据聚合方案都依赖于可信第三方,存在密钥托管的风险。文中设计了一个基于抗泄漏无证书同态加密的用户电力数据聚合和隐私保护协议,该协议主要将弹性泄露密码体制与无证书同态加密技术相结合,既可以避免密钥托管问题又可以实现密钥抗泄露。安全性分析证明了该协议在若干攻击模型下的有效性,可以满足若干安全要求,在一定程度上保护了电网的安全。

**关键词:**智能电网;数据聚合;隐私保护;弹性泄露;加法同态;无证书加密

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2020)06-0087-07

doi:10.3969/j.issn.1673-629X.2020.06.017

## Data Aggregation and Privacy Protection Protocol Based on Anti-Leakage Certificateless Homomorphic Encryption for Smart Grid

ZHU Cong-cong, QIAO Zhi, WANG Zhi-wei

(School of Computer Science & Software & Cyberspace Security, Nanjing University of Posts and Telecommunications, Nanjing 210046, China)

**Abstract:** As the next generation of power systems, smart grids significantly improve the reliability, efficiency, security and sustainability of power service. With the development of smart grid technology, users can collect power usage data in real-time, which is conducive to the efficient regulation of local power, but it also leads to the leakage of user information. How to balance users' real-time power data and protect users' privacy is a crucial issue, where data aggregation and privacy protection could be a feasible solution. However, most of the existing data aggregation schemes rely on a trusted third party and are subject to the risk of key escrow. Therefore, we design a data aggregation and privacy protection protocol based on anti-leakage certificateless homomorphic encryption, which combines the resilient leakage cryptosystem with the certificateless homomorphic encryption technology to avoid the key escrow problem and realize the anti-leakage of keys. Security analysis shows that this protocol is effective under several attack models, which can meet some security requirements and protect the security of the grid to a certain extent.

**Key words:** smart grid; data aggregation; privacy protection; resilient leakage; addition homomorphism; certificateless encryption

### 0 引 言

智能电网<sup>[1]</sup>是一个计算机和电力相结合的基础设施网络,用于监控和管理能源使用情况。然而,随着智能电网技术的不断发展,也带来了一定的安全问题。一方面,实时的用电数据在一定程度上会泄露用户的行为隐私;而另一方面,电网网关的地理环境使得网关的安全性较低。因此,有效保护用户隐私并实现密钥抗泄露以及身份认证成为智能电网的研究热点。

在传统的公钥密码体制中,用户自己选择公钥,但

是需要由证书颁发机构的可信第三方进行验证,证书的管理过程复杂且代价较高。为了避免这种情况,Shamir<sup>[2]</sup>提出了基于身份的公钥密码体制(identity-based public key cryptography, ID-PKC),使用身份信息(如电子邮箱、姓名等)直接作为公钥,私钥由可信第三方密钥生成中心(key generation center, KGC)生成,存在恶意KGC的风险,导致密钥托管问题。随后,Al-Riyami等人<sup>[3]</sup>提出了无证书公钥密码体制(certificateless public key cryptography, CL-PKC),不

收稿日期:2019-07-25

修回日期:2019-11-26

基金项目:国家自然科学基金(61672016)

作者简介:朱聪聪(1995-),女,硕士研究生,研究方向为密码学;王志伟,教授,硕导,研究方向为应用密码学、密码协议、边缘/雾计算安全等。

仅避免了传统公钥密码体制的证书管理,也解决了基于身份的公钥密码体制中的密钥托管问题。在 CL-PKC 中, KGC 根据用户的身份为其生成部分私钥, 用户基于 KGC 为其计算的部分私钥和随机选取的秘密值生成最终的私钥, 公钥由用户的秘密值和部分私钥构成。也就是说, CL-PKC 中用户本身参与私钥和公钥的生成, KGC 不会知道用户的密钥, 也就不存在密钥托管的风险。

最近提出的一些方案建议聚合单个计量数据来保护用户隐私<sup>[4-7]</sup>。同态加密 (homomorphic encryption, HE) 是实现聚合的有效方法, 每个用户使用加法同态加密他的数据, 然后将密文发送给网关, 由于加法同态的性质, 网关进行解密可以获得计量数据的总和。Garcia 等人<sup>[4]</sup>提出一种多方计算协议, 它允许邻域中的多个智能电表计算其部分数据的聚合, 通过使用 Paillier 的加法同态性质, 使得单个的计量数据无法揭露。但是由于方案要求本地变电站完全聚合计量数据, 造成巨大的计算和通信开销, 而加法同态加密方案已满足大数据应用的要求。Li 等人<sup>[6-7]</sup>提出一种用于智能电网的分布式网内聚合方案, 该方案使用 Paillier 的同态加密将源智能电表到网关中所有智能电表的计量数据进行聚合, 从第一个电表开始, 路径上的每个智能电表将前一个智能电表发来的数据与自己的计量数据进行聚合, 然后再发送给下一个智能电表, 直到网关用其私钥解密聚合密文, 并且在不知道单独计量数据的情况下获得该路径上所有智能电表计量数据的总和。该方案虽然在计算和通信方面有效, 但是容易受到中间恶意电表和外部攻击者在发送途中伪造中间聚合数据。

应用加法同态的一个重要问题就是防止数据在发送途中受到攻击。在实际中存在这样一类攻击者, 他们针对加密电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的侧信道信息泄露而对加密设备进行攻击, 此获得设备私钥的一部分, 这将导致重要信息的泄漏。为了抵御侧信道攻击, 许多研究人员引入并提出了泄露弹性 (leakage-resilient, LR) 密码<sup>[7-8]</sup>模型。现有的泄漏模型可分为三类: (1) 有界泄漏模型<sup>[9]</sup>。在系统生命周期内, 对手可以自适应地选择一个可计算的泄漏函数  $f$ , 它输入私钥并在有界泄漏模型中获得泄漏函数  $f(SK)$  的输出。由于整个过程中私钥的总泄漏量是有界的, 有效限制了泄漏函数  $f$  获得完整的私钥信息。(2) 连续泄漏模型<sup>[10]</sup>。在连续泄漏模型中, 私钥定期更新。两个连续私钥更新之间私钥泄漏的泄漏量是有界的, 但在整个过程中总泄漏量是无限的。构造连续泄露模型下安全的密码系统的主要问题在于如何更新私钥, 使得不同时间段的泄露无法

有意义地合并出整个私钥, 而导致密码系统崩溃。(3) 辅助输入模型<sup>[11]</sup>。在系统生命周期内, 无论信息泄露多少, 即使在理论上私钥全部泄露, 依然不存在概率多项式 (PPT) 攻击者可以用不可忽略的概率从  $f(SK)$  恢复  $SK$ 。也就是说, 即使这样的功能信息理论上揭示了整个私钥  $SK$ , 但是在计算上仍然是不可行的。

为了解决实际应用中的密钥泄露问题, 抗泄露加密方案<sup>[12]</sup>被陆续提出。Wang 等人<sup>[13]</sup>提出了基于身份的泄露弹性加法同态加密方案, 并在标准模型中证明了它的安全性, 但是这种方案存在密钥托管的风险。Xiong 等人<sup>[14]</sup>提出了第一个泄露弹性无证书公钥加密 (LR-CL-PKE) 方案, 该方案基于双线性对和非交互式零知识证明系统构造, 但并未给出非交互式零知识系统的具体构造方法, 导致方案的计算效率难以评估。Zhou 等人<sup>[15]</sup>提出一个不含双线性对的抗泄露无证书公钥加密方案, 并且证明了该方案在选择明文攻击 (chosen ciphertext attacks, CCA2) 下的安全性。

文中旨在为智能电网提出一种安全有效的数据聚合和隐私保护协议, 该协议不仅可以避免密钥托管, 还可用于实现网关抗泄露。通过修改 Wang 等人的方案<sup>[16]</sup>, 设计了一种基于抗泄漏无证书同态加密的智能电网数据聚合和隐私保护协议。为了有效解决加密系统中的密钥托管问题, 使用了无证书的加密方案, 解决了基于身份的加密系统中的可信第三方问题; 考虑到网关常年暴露在户外, 攻击者通过侧信道攻击很容易获得私钥的部分比特, 在协议中使用改进的 Goldreich-Levin 定理防止网关的密钥泄露; 同时, 智能电网需要实时收集用户数据并进行细粒度分析, 在协议中利用加法同态的性质, 使得网关在不知道单独计量数据的情况下获得该地区的总用电数据, 有效防止攻击者窃取单独用户的用电信息。

## 1 基础知识

### 1.1 数学概念

#### 1.1.1 双线性映射

设  $p$  是一个大素数,  $G$  和  $G_T$  是两个阶为  $p$  的循环加法群和循环乘法群。  $G$  到  $G_T$  的双线性映射  $e: G \times G \rightarrow G_T$  满足下面的性质:

(1) 双线性: 对于  $\forall P, Q \in G, a, b \in Z$ , 有  $e(aP, bQ) = e(P, Q)^{ab}$ 。

(2) 非退化性:  $\exists P, Q \in G$ , 使得  $e(P, Q) \neq 1$ 。

(3) 可计算性: 对于  $\forall P, Q \in G$ , 存在一个有效算法计算  $e(P, Q)$ 。

#### 1.1.2 计算 Diffie-Hellman (CDH) 假设

设  $G$  是阶为  $p$  的循环群,  $k$  为群生成算法  $\text{Gen}(1^k)$

的安全参数,  $g$  为  $G$  的生成元, 则计算 Diffie-Hellman (CDH) 假设定义为:

对于任意概率多项式时间 (PPT) 攻击者  $A$ , 随机选择  $a, b \in Z_p$ , 给定元组  $(g, g^a, g^b) \in G^3$ , 计算  $g^{ab}$  的优势  $\text{Adv}_A^{\text{CDH}}(k) = \Pr[A(q, G, g^a, g^b) = g^{ab}]$  可忽略不计。

### 1.1.3 判定型双线性 Diffie-Hellman (DBDH) 假设

设  $G$  和  $G_T$  是阶为素数  $p$  的两个循环群,  $\lambda$  为群生成算法  $\text{Gen}(1^\lambda)$  的安全参数,  $g$  为  $G$  的生成元,  $e: G \times G \rightarrow G_T$  为  $G$  到  $G_T$  的一个双线性映射。则  $\langle G, G_T, e \rangle$  上的判定型双线性 Diffie-Hellman (DBDH) 假设定义为:

对于任意概率多项式时间 (PPT) 攻击者  $A$ , 随机选择  $a, b, c, z \in Z_p$ ,  $A$  区分元组  $R = (g^a, g^b, g^c, e(g, g)^{abc})$  和元组  $D = (g^a, g^b, g^c, e(g, g)^z)$  的优势  $\text{Adv}_A^{\text{DBDH}}(\lambda) = |\Pr[A(R) = 1] - \Pr[A(D) = 1]|$  可忽略不计。

## 1.2 强提取器

定义 1 (单向散列函数族): 设  $H_{ow}(\varepsilon)$  是任意多项式时间可计算函数  $f: \{0, 1\}^n \rightarrow \{0, 1\}^*$  的类。给定随机数  $x$ , 计算  $y = f(x)$ , 如果满足对于任何 PPT 算法从  $y = f(x)$  中恢复  $x$  的概率都小于  $\varepsilon$ , 那么  $H_{ow}(\varepsilon)$  称为单向散列函数族。

定义 2 (带有辅助输入的  $(\varepsilon, \delta)$ -强提取器): 设  $\text{SE}: Z_p^m \times Z_p^m \rightarrow Z_p$ , 其中  $m = \text{poly}(\lambda)$ ,  $\lambda$  是安全参数,  $\text{SE}$  被称为带有辅助输入的  $(\varepsilon, \delta)$ -强提取器。对于任意的攻击者  $A$ , 给定  $f \in H_{ow}(\varepsilon)$  和  $x \in Z_p^m$ , 从  $Z_p^m$  随机选择  $s$ , 从  $Z_p$  随机选择  $\gamma$ , 使得

$$\begin{aligned} & \Pr[A(s, f(x), \text{SE}(s, x)) = 1] - \\ & \Pr[A(s, f(x), \gamma) = 1] < \delta \end{aligned}$$

定义 3 (改进的 Goldreich-Levin 定理): 设  $p$  是一个大素数,  $H$  为  $\text{GF}(p)$  的任意子集,  $H^n \rightarrow \{0, 1\}^*$  的映射  $f$  为任意多项式时间可计算函数, 然后从  $H^n$  中随机选择向量  $x$ , 计算  $y = f(x)$ 。从  $\text{GF}(p)^n$  中随机选择矢量  $s$ , 并从  $\text{GF}(p)$  中随机选择  $u$ 。如果存在一个运行时间为  $t$  的任意概率多项式时间 (PPT) 算法  $A$ , 使得

$$\begin{aligned} & \Pr[A(y, s, \langle s, x \rangle) = 1] - \\ & \Pr[A(y, s, u) = 1] < \varepsilon \end{aligned}$$

则存在一个运行时间为  $t' = t \cdot \text{poly}(n, p, 1/\varepsilon)$  的算法  $B$ , 它从  $y$  计算出  $x$  的概率为:

$$\Pr[B(y) = x] \geq \frac{\varepsilon^3}{512np^2}$$

然后, 根据改进的 Goldreich-Levin 定理从内积构造带有辅助输入的  $(\varepsilon, \delta)$ -强提取器。

## 2 协议设计

### 2.1 基于抗泄漏无证书同态加密和签名方案

#### 2.1.1 基本概念

基于抗泄漏无证书同态签密方案  $\Gamma$  由设置、部分私钥提取、设置秘密值、设置私钥、设置公钥、签密、解密 7 个算法组成。通常, 设置和部分私钥提取由 KGC 执行, 而其他算法由加密或解密用户执行。以下是各个算法的描述:

- $\text{Setup}(1^\lambda)$ : KGC 以安全参数  $\lambda$  作为输入, 生成双线性群参数  $(G, G_T, e: G \times G \rightarrow G_T)$ , 其中  $g$  是  $G$  的生成元,  $g_t$  是  $G_T$  的生成元。随机选择  $s \in Z_q$  作为主密钥, 即  $S_{\text{msk}} = s$ , 并设置主公钥为  $\text{mpk} = g^s$ 。选择加密散列函数  $H_1: \{0, 1\}^* \rightarrow G$ ,  $H_2: \{0, 1\}^* \rightarrow G$  和  $H_3 = \{0, 1\}^* \times G \times G \rightarrow Z_q$ 。公开系统参数  $\text{params} = \{q, G, G_T, g, g_t, e, H_1, H_2, H_3\}$ 。

- $\text{PartialPrivateKeyExtract}(\text{params}, \text{ID}, S_{\text{msk}})$ : KGC 随机选择  $r_1, \dots, r_m \in Z_q$ , 计算  $R_1 = g^{r_1}, \dots, R_m = g^{r_m}$ , 将  $y_1 = r_1 + S_{\text{msk}} H_3(\text{ID}, X_1, R_1), \dots, y_m = r_m + S_{\text{msk}} H_3(\text{ID}, X_m, R_m)$  作为部分私钥, 再计算  $Y_1 = g^{y_1}, \dots, Y_m = g^{y_m}$ , 输出部分私钥  $d_{\text{ID}} = (y_1, \dots, y_m)$ 。

- $\text{SetSecretValue}(\text{params}, \text{ID}, d_{\text{ID}})$ : 用户随机选择  $x_{\text{ID}} = (x_1, \dots, x_m)$  作为秘密值。

- $\text{SetPrivateKey}(\text{params}, \text{ID}, d_{\text{ID}}, x_{\text{ID}})$ : 输出用户的私钥为  $\text{sk}_{\text{ID}} = (x_1 + y_1, \dots, x_m + y_m)$ 。

- $\text{SetPublicKey}(\text{params}, \text{ID}, d_{\text{ID}}, x_{\text{ID}})$ : 输出该用户的公钥  $\text{pk}_{\text{ID}} = (X_1 Y_1, \dots, X_m Y_m)$ 。

- $\text{Signcrypt}(\text{params}, \text{ID}, M, \text{sk}_{\text{ID}}, \text{pk}_{\text{ID}})$ : 随机选择  $r_{i1}, \dots, r_{im} \in Z_q$ , 输出该用户对  $M$  加密的密文  $\text{CT} = (C_1, C_2) = (g^{r_{i1}}, \dots, g^{r_{im}}, g_t^M \cdot \prod_{j=1}^m e(\text{pk}_j, H_1(\text{ID})^{r_{ij}})$ , 计算签名  $V = H_2(C_2 || T_i)^{\text{sk}_{\text{ID}}}$ , 其中  $T_i$  为当前时间戳。

- $\text{Unsigncrypt}(\text{params}, \text{ID}, C, \text{sk}_{\text{ID}}, \text{pk}_{\text{ID}})$ : 验证  $e(g, V) = e(\text{pk}_{\text{ID}}, H_2(C_2 || T_i))$  是否成立, 输出该用户

对密文  $C$  解密的明文  $M_t = \frac{C_2}{\prod_{j=1}^m e(C_{ij}, H_1(\text{ID})^{\text{sk}_{\text{ID}}})}$ , 计算基于  $g_t$  的离散对数  $M = \log_{g_t} M_t$ 。

#### 2.1.2 安全证明

Wang 等人已经证明他们提出的基于身份的加密方案在 DBDH 和 CDH 假设下是 CPA 安全的, 由于基于身份的加密中本身存在恶意的 KGC 攻击, 所以文中提出的无证书方案对于 II 型攻击者也是 CPA 安全的。下面证明文中方案对于 I 型攻击者的安全性, 设  $F$  表示多项式时间可计算泄漏函数族,  $\Gamma$  表示基于抗泄漏无证书同态加密方案。

定理 1: 如果没有任何多项式时间的攻击者能够



以不可忽略的优势赢得下列游戏,那么文中方案对 I 型攻击者是 CPA 安全的。

证明: (Game<sub>0</sub>) 给定挑战者 C 一组输入  $(g, p, e, g^{\alpha_1}, g^{\alpha_2}, g^{\alpha_3}, h_i)$ , 其中  $h_0 = e(g, g)^x, x \in_R Z_p, h_1 = e(g, g)^{\alpha_1 \alpha \alpha_3}$ , 以进行下列询问应答。

· 设置: 挑战者 C 运行 Setup( $1^\lambda$ ), 将主公钥 mpk 发送给攻击者 A。C 还保持一个列表  $L_{ID}$ 。

·  $H_1$  查询: 当 A 对身份 ID 进行查询时, C 随机选择  $j \in \{0, 1\}$  和  $t \in Z_p$ , 当  $j = 0$  时, 令  $H_1(ID) = g^t$ , 当  $j = 1$  时, 令  $H_1(ID) = y^t$ , 然后将元组  $(ID, H_1, j)$  添加到表  $L_{ID}$  中。

· 部分私钥查询: C 首先检查  $L_{ID}$  中是否有元组  $(ID, d_{ID}, pk_{ID}, x_{ID}, j)$ , 如果有, C 将  $d_{ID}$  返回给 A。否则, 将  $j$  设为 1, 计算  $d_{id} = mpk^t$  和  $pk_{ID} = x_{ID}$ , 并将元组  $(ID, d_{ID}, pk_{ID}, x_{ID}, j)$  添加到表  $L_{ID}$  中。

· 公钥查询: C 首先检查  $L_{ID}$  中是否有元组  $(ID, pk_{ID}, x_{ID}, j)$ , 如果有, C 将  $pk_{ID}$  返回给 A。否则, 将  $j$  设为 1, C 随机选择  $w \in Z_p$ , 令  $pk_{ID} = g^{\alpha_1}$  和  $x_{ID} = \alpha_1$  并将  $pk_{ID}$  返回给 A, 将元组  $(ID, pk_{ID}, x_{ID}, j)$  添加到表  $L_{ID}$  中。

· 私钥查询: C 首先检查  $L_{ID}$  中是否有元组  $(ID, d_{ID}, pk_{ID}, sk_{ID}, j)$ , 如果有, C 将  $sk_{ID}$  返回给 A。否则, C 首先进行部分私钥查询得到  $d_{ID}$ , 然后进行公钥查询得到  $pk_{ID} = g^{\alpha_1}$  和  $x_{ID} = \alpha_1$ , 并将这些值添加到表  $L_{ID}$  中, 将  $sk_{ID} = (d_{ID}, \alpha_1)$  返回给 A。

· 公钥替换: A 可以用选择的公钥  $pk'_{ID}$  替换任意用户的公钥  $pk_{ID}$ 。

·  $H_2$  查询: 当 A 对元组  $(C, T)$  进行查询时, C 首先检查  $L_{ID}$  中是否有元组  $(C, T, l, j)$ , 如果有, 就将  $H_2$  的定义返回给 A, 否则, C 随机选择  $l \in Z_p$ , 令  $H_2(ID) = g^l$ , 然后将元组  $(C, T, l, j)$  添加到表  $L_{ID}$  中。

· 泄露查询: A 选择  $f \in F$  进行密钥泄露查询, C 用  $f(sk_{ID})$  进行响应。

· 签名查询: 当 A 对身份 ID 和 CT 进行查询时, C 首先恢复先前定义的  $H_1$ , 然后, 设置  $C_1 = g^{\alpha_1}$  并将其返回给 A。

· 挑战: A 向 C 发送两条关于身份 ID\* 的长度相同的消息  $m_0$  和  $m_1$ , C 首先设置  $H_1(ID^*) = g^{\alpha_2}$ , 然后随机选择一个比特位  $b$ , 并将密文  $CT^* = (C_1^*, C_2^*) = (g^{\alpha_3}, g_t^{m_i} \cdot h_i) (i = 0, 1)$  返回给 A。

· 输出: A 输出  $b$  的猜测位  $b'$ 。

假设攻击者 A 能够以概率  $\varepsilon$  攻破基于抗泄漏无证书同态加密方案, 由于  $m_b$  隐藏在  $C_2^*$  中, 要想赢得游戏, 必须算出当  $i = 1$  时,  $CT^*$  是  $m_b$  的有效密文, 此时他区分出  $i$  的概率为

$|\Pr[b' = b | h_0] - \Pr[b' = b | h_1]| = \frac{1}{2} + \varepsilon$ , 这是不可忽略的, 与 DBDH 假设相矛盾, 因此文中方案是 CPA 安全的。

定理 2: 如果 SE 是带有辅助输入的  $(\varepsilon, \delta)$ -强提取器, 那么文中方案  $\Gamma$  相对于族  $H_{ow}(\varepsilon)$  是 AI-CPA 安全的。

证明: (Game<sub>1</sub>) 设  $s = \gcd(sk_1, \dots, sk_m)$ ,  $\vec{s} = (sk_1/s, \dots, sk_m/s)$ ,  $\vec{x} = (x_1, \dots, x_m)$ 。SE:  $Z_p^m \times Z_p^m \rightarrow Z_p$  是一个带有辅助输入的  $(\varepsilon, \delta)$ -强提取器。挑战者 C 已知  $(\vec{s}, f_1(x), \dots, f_q(x), h_i)$ , 其中  $h_2 = \langle \vec{s}, \vec{x} \rangle$ 。令  $\text{Adv}_A^{\text{Game}_i}(\prod)$  表示攻击者 A 使用协议  $\Gamma$  赢得 Game<sub>i</sub> 的优势。现在, 假设  $|\text{Adv}_A^{\text{Game}_0}(\prod) - \text{Adv}_A^{\text{Game}_1}(\prod)| \geq \varepsilon$ , 其中  $\varepsilon$  不可忽视。只是当加密挑战密文时, 用随机数  $\gamma \in Z_p$  代替 SE( $s, x$ )。

· 设置: 挑战者 C 运行 Setup( $1^\lambda$ ), 并将主公钥 mpk 发送给攻击者 A。挑战者 C 保密 msk。

· 查询: 查询部分与 Game<sub>0</sub> 相同。

· 挑战: A 向 C 发送两条关于身份 ID\* 的长度相同的消息  $m_0$  和  $m_1$ , C 选择一个随机位  $b$ , 然后对  $m_b$  进行加密, 并将密文  $CT = (C_1, C_2) = (g^3, g_t^{m_i} \cdot e(g, g)^{h_2}) (i = 0, 1)$  返回给 A。

· 输出: 攻击者 A 输出  $b$  的猜测位  $b'$ 。

如果  $b' = b$ , 则 A 赢得上述游戏。

由于假设  $|\text{Adv}_A^{\text{Game}_0}(\prod) - \text{Adv}_A^{\text{Game}_1}(\prod)| \geq \varepsilon$ , 可以很容易得到  $|\Pr[b' = b | h_0] - \Pr[b' = b | h_2]| \geq \varepsilon$ 。然而, 它与强提取器 SE( $s, x$ ) 的性质相矛盾。因此, 没有 PPT 攻击者能够以不可忽略的概率区分 Game<sub>0</sub> 和 Game<sub>1</sub>。所以文中协议可以抵抗密钥泄漏引起的攻击。

该方案的加法同态特性如下:

$$C \cdot C' = (g^{r_a+r'_a}, \dots, g^{r_m+r'_m}, g_t^{M+M'})$$

$$\prod_{j=1}^m e(pk_j, H_1(ID))^{r_j} \cdot g_t^M$$

$$\prod_{j=1}^m e(pk_j, H_1(ID))^{r'_j} = (g^{r_a+r'_a}, \dots, g^{r_m+r'_m}, g_t^{M+M'})$$

$$\prod_{j=1}^m e(pk_j, H_1(ID))^{r_j+r'_j} =$$

$$\text{Encrypt}(\text{params}, ID, M + M', pk)$$

## 2.2 基于抗泄漏无证书同态加密的智能电网数据聚合和隐私保护协议

### 2.2.1 系统模型

系统模型由四个部分组成, 如图 1 所示。第一个

部分是密钥生成中心(KGC),SM、AGW和ESP分别需要与KGC进行交互,用无证书方式生成私钥。首先,实体选择秘密值并生成公共元素发送给KGC,然后,KGC生成部分私钥再发送给实体,最后,实体根据接收到的部分私钥结合秘密值生成最终私钥和公钥。第二个部分是智能电表(SM),SM计量各自的用电数据并用自己的私钥加密然后进行签名,然后再将密文和签名发送给AGW。第三个部分是区域网关(AGW),

AGW首先验证SM发来的签名是否正确,如果正确,则接收密文,然后对电表传来的密文进行聚合,并进行签名。第四个部分是电力服务提供商(ESP),ESP首先验证网关身份,如果通过,则解密聚合电量。由于聚合密文使用的是加法同态加密,所以ESP在解密完密文之后可以获得该地区各个用户的用电数据,方便灵活分析并对该区域的电力实施高效调控。

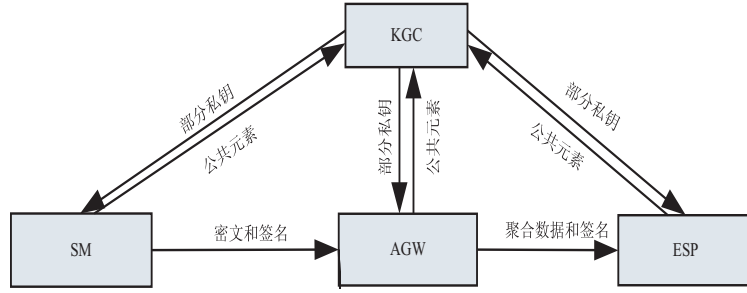


图1 智能电网的系统模型

### 2.2.2 协议构建

#### (1) 系统初始化。

步骤1:KGC以安全参数 $\lambda$ 作为输入,生成双线性群参数 $(G, G_T, e: G \times G \rightarrow G_T)$ ,其中, $G$ 和 $G_T$ 具有素数阶 $q > 2^\lambda$ ,设 $g$ 是 $G$ 的生成元, $g_t$ 是 $G_T$ 的生成元。

步骤2:随机选择 $s \in Z_q$ 作为主密钥,即 $S_{msk} = s$ ,并设置主公钥为 $P_{pub} = g^s$ 。

步骤3:选择加密散列函数 $H_1: \{0,1\}^* \rightarrow G$ , $H_2: \{0,1\}^* \rightarrow G$ 和 $H_3: \{0,1\}^* \times G \times G \rightarrow Z_q$ 。

步骤4:KGC公开系统参数 $params = \{q, G, G_T, g, g_t, e, P_{pub}, H_1, H_2, H_3\}$ 。

#### (2) 实体注册。

步骤1 智能电表注册:一个区域内有 $n$ 个智能电表,每个智能电表通过无证书方式与KGC交互生成私钥,其中第 $i$ 个智能电表的私钥为 $sk_{ID_i}$ 。

步骤1.1 设置秘密值:智能电表随机选择秘密值 $x_{ID_i} \in Z_q$ ,计算公共元素 $X_{ID_i} = g^{x_{ID_i}}$ ,将身份 $ID_i$ 和公共元素 $X_{ID_i}$ 发送给KGC。

步骤1.2 部分私钥提取:KGC随机选择秘密值 $r_{ID_i} \in Z_q$ ,计算 $R_{ID_i} = g^{r_{ID_i}}$ , $y_{ID_i} = r_{ID_i} + S_{msk} H_3(ID_i, X_{ID_i}, R_{ID_i})$ ,然后计算 $Y_{ID_i} = g^{y_{ID_i}}$ ,并发送 $R_{ID_i}$ ,部分私钥 $y_{ID_i}$ 和 $Y_{ID_i}$ 给智能电表。

步骤1.3 设置私钥:智能电表设置 $sk_{ID_i} = x_{ID_i} + y_{ID_i}$ 作为私钥。

步骤1.4 设置公钥:智能电表计算 $pk_{ID_i} = X_{ID_i} Y_{ID_i}$ 作为公钥。

步骤2 网关注册:网关使用无证书方式与KGC交互生成私钥。

步骤2.1 设置秘密值:网关随机选择秘密值 $x_{ID_g}$ ,

$\in Z_q$ ,用于将部分私钥转换为私钥,网关保密 $x_{ID_g}$ ,计算公共元素 $X_{ID_g} = g^{x_{ID_g}}$ ,将身份 $ID_g$ 和公共元素 $X_{ID_g}$ 发送给KGC。

步骤2.2 部分私钥提取:KGC随机选择秘密值 $r \in Z_q$ ,设置 $R = g^r$ ,然后计算 $y_{ID_g} = r + S_{msk} H_3(ID_g, X_{ID_g}, R)$ 作为部分私钥,再计算 $Y_{ID_g} = g^{y_{ID_g}}$ ,并将 $R$ , $Y_{ID_g}$ 和部分私钥 $y_{ID_g}$ 发送给网关。

步骤2.3 设置密钥:网关设置 $sk_{ID_g} = x_{ID_g} + y_{ID_g}$ 作为最终私钥,计算 $pk_{ID_g} = X_{ID_g} Y_{ID_g}$ 作为公钥。

步骤3 ESP注册:KGC和ESP执行交互协议,用无证书方式生成私钥:

步骤3.1 设置秘密值:ESP随机选择秘密值 $x_1, \dots, x_m \in Z_q$ ,计算公共元素 $X_1 = g^{x_1}, \dots, X_m = g^{x_m}$ ,将身份 $ID_{esp}$ 和公共元素 $X_1, \dots, X_m$ 发送给KGC。

步骤3.2 部分私钥提取:KGC随机选择秘密值 $r_1, \dots, r_m \in Z_q$ ,计算 $R_1 = g^{r_1}, \dots, R_m = g^{r_m}$ ,将 $y_1 = r_1 + S_{msk} H_3(ID_{esp}, X_1, R_1), \dots, y_m = r_m + S_{msk} H_3(ID_{esp}, X_m, R_m)$ 作为部分私钥,再计算 $Y_1 = g^{y_1}, \dots, Y_m = g^{y_m}$ ,并发送 $R_1, \dots, R_m$ ,部分私钥 $y_1, \dots, y_m$ 和 $Y_1, \dots, Y_m$ 给ESP。

步骤3.3 设置私钥:输入系统参数 $params$ ,ESP身份 $ID_{esp}$ ,部分私钥 $y_1, \dots, y_m$ 和秘密值 $x_1, \dots, x_m$ ,ESP私钥为 $sk = (x_1 + y_1, \dots, x_m + y_m)$ 。

步骤3.4 设置公钥:ESP计算 $pk = (X_1 Y_1, \dots, X_m Y_m)$ 作为公钥。

步骤4 计算 $W = (W_1, \dots, W_m) = (e(X_1 Y_1, H_1(ID_{esp})), \dots, e(X_m Y_m, H_1(ID_{esp})))$ 的值,KGC将其发送到所有智能电网设备。

#### (3) 收集阶段。

步骤1 智能电表计算密文:第 $i$ 个智能电表的计

量数据为  $m_i$ , 智能电表随机选择  $r_{i1}, \dots, r_{im} \in Z_q$  并计算密文  $CT_i = (C_{1i}, C_{2i}) = (g^{r_{i1}}, \dots, g^{r_{im}}, g_i^{m_i} \cdot \prod_{j=1}^m W_j^{r_{ij}})$ , 存在  $\sum_{i=1}^n m_i$  不应该是大数的限制。

步骤 2 智能电表进行数字签名: 设  $T_i$  为当前时间戳, 智能电表计算签名  $V_i = H_2(C_{2i} || T_i)^{sk_{i0}}$ , 并将  $(CT_i, V_i, T_i)$  发送到网关。

步骤 3 网关验证电表身份: 网关首先验证  $e(g, V_i) = e(pk_{i0}, H_2(C_{2i} || T_i))$  是否成立来检查电表发送的密文, 如果成立, 则网关接收电表上传的数据, 否则拒绝。

#### (4) 聚合阶段。

步骤 1 网关聚合总电量: 计算聚合的密文为  $CT = (C_1, C_2) = (g^{r_{a1}}, \dots, g^{r_{am}}, g_i^{m_i} \cdot \prod_{j=1}^m W_j^{r_{ij}})$ , 并将密文发送到 ESP。

步骤 2 网关进行数字签名: 设  $T_c$  为网关当前时间戳, 计算签名  $V = H_2(C_2 || T_c)^{sk_{c0}}$ 。

#### (5) 解密阶段。

步骤 1 ESP 验证网关身份: ESP 首先计算  $e(g, V) = e(pk_{c0}, H_2(C_2 || T_c))$  是否成立, 如果成立, 则 ESP 接收网关上传的数据, 否则拒绝。

步骤 2 ESP 解密聚合电量: ESP 首先计算  $M_i = \frac{C_2}{\prod_{j=1}^m e(g^{r_{ij}}, H_1(ID_{esp})^{sk_{ij}})}$ , 然后计算基于  $g_i$  的  $M_i$  的离散对数  $M = \log_{g_i} M_i$  来获得该地区总的用电数据。

### 3 安全性分析

文中设计的安全有效的基于抗泄漏无证书同态加密的智能电网数据聚合和隐私保护协议旨在防止网关暴露在开放环境中的密钥泄露问题, 并防止未经授权对象读取电表数据并进行细粒度分析。在本节中, 针对协议的一系列攻击进行正式安全和隐私分析。

#### 3.1 抵御侧信道攻击

攻击者可以通过收听侧道信息获得加密设备密钥的部分比特来对设备进行攻击。在该协议中, 使用改进的 Goldreich-Levin 定理构造了一个带有辅助输入的  $(\epsilon, \delta)$ -强提取器, 定理 2 的证明表明在私钥泄露的情况下即使攻击者截获密文  $CT_i = (C_{1i}, C_{2i}) = (g^{r_{i1}}, \dots, g^{r_{im}}, g_i^{m_i} \cdot \prod_{j=1}^m W_j^{r_{ij}})$ , 也无法从密文中恢复出相对应的明文, 从而改变智能电表的计量数据, 因为攻击者伪造的签名  $V_i = H_2(C_{2i} || T_i)^{sk_{i0}}$  无法通过身份验证。因此, 该协议可以抵御侧信道攻击。

#### 3.2 抵御中间人攻击

中间人攻击是模仿合法的角色, 通过读取发送方的信息向接收方发送虚假的消息。在智能电网系统中

存在两个中间人攻击。一种是智能电表与网关之间的攻击, 假的智能电表向网关发送错误的计量数据。在该协议中, 电表在发送数据之前需要先和网关验证身份, 定理 2 证明了基于抗泄漏无证书同态签密方案是安全的, 所以攻击者无法获得智能电表的私钥, 以此通过身份验证。另一种是网关和 ESP 之间的攻击, 攻击者通过模仿网关向 ESP 发送聚合电量。在该协议中, 网关通过将聚合数据添加在签名中, 攻击者即使获得了网关的私钥, 也不可能伪造出正确的签名, 通过身份验证, 因此该协议可以抵御中间人攻击。

#### 3.3 抵御内部攻击

在智能电网系统中存在两种内部攻击。一种是网关攻击, 攻击者可以在未授权的情况下与智能电表交互获得电表的用电信息。在收集阶段, 网关只能获得由电表加密过的计量数据  $CT_i = (C_{1i}, C_{2i}) = (g^{r_{i1}}, \dots, g^{r_{im}}, g_i^{m_i} \cdot \prod_{j=1}^m W_j^{r_{ij}})$ , 定理 2 的证明表明攻击者从密文中恢复  $m_i$  的概率可忽略不计; 在聚合阶段, 攻击者也无法从  $CT = \prod_{i=1}^n CT_i$  中恢复总用电数据, 因此可以抵抗网关攻击。另一种是 ESP 攻击, 攻击者可以在未授权的情况下与网关交互获得该地区用电数据的聚合密文。在该协议中, 由于  $r_{i1}, \dots, r_{im} \in Z_q$  是由每个电表随机选择, 攻击者并不知道每个密文相对应的随机数, 所以攻击者智能解密出聚合数据该地区的总用电数据, 却无法获得每个电表的单独的计量数据, 并不能够达到对数据进行细粒度分析的目的。因此该协议可以抵抗 ESP 攻击。

#### 3.4 抵御网关和 $N-1$ 个智能电表合谋攻击

当网关和  $N-1$  个智能电表展开合谋攻击, 除了一个智能电表以外的所有电表都是不诚实的。在这种情况下, 网关和  $N-1$  个智能电表试图获得唯一诚实的智能电表的明文。假设智能电表  $SM_i$  和 ESP 是诚实的, 由于基于抗泄漏无证书同态签密方案是 CPA 安全的, 所以攻击者无法从密文  $CT_i = (C_{1i}, C_{2i}) = (g^{r_{i1}}, \dots, g^{r_{im}}, g_i^{m_i} \cdot \prod_{j=1}^m W_j^{r_{ij}})$  解密出明文, 同时, 攻击者无法获得 ESP 的私钥, 以此模仿 ESP 解密聚合电量, 从而通过减去其他电表的计量数据获得  $SM_i$  的明文。因此该协议可以抵抗网关和  $N-1$  个智能电表合谋攻击。

#### 3.5 抵御 ESP 和 $N-2$ 个智能电表合谋攻击

当网关和  $N-2$  个智能电表展开合谋攻击, 除了两个智能电表  $SM_i$  和  $SM_j$  以外的所有电表都是不诚实的。在这种情况下, ESP 和  $N-2$  个智能电表试图区分两个诚实的智能电表的明文。假设网关也是诚实的, 定理 1 的证明表示在基于抗泄漏无证书同态签密方案中, 攻击者区分两条长度相同的挑战密文的概率可忽

略不计,也就是说即使攻击者得到了电表  $SM_i$  和  $SM_j$  的密文,也无法区分出每个电表相对应的明文,因此该协议可以抵抗 ESP 和  $N-2$  个智能电表合谋攻击。

### 3.6 抵御重放攻击

如果攻击者获得双方发送过的信息,他拦截通信并恶意重放信息来达到欺骗系统的目的,这称为重放攻击。在该协议中,使用当前时间戳来抵御重放攻击。如果攻击者想要模仿签名中的时间戳来重放签名,必须先获得设备的密钥,但是攻击者获得私钥的概率忽略不计,因此攻击者不可能进行重放攻击。

## 4 结束语

随着大规模物联网的发展,用户的隐私受到了越来越多的威胁,在智能电网中,攻击者可以通过窃取用户的用电数据,以此分析该用户的行为模式。文中设计了一个基于抗泄漏无证书同态加密的用户电力数据聚合和隐私保护协议,该协议主要将弹性泄露密码体制与无证书同态加密技术相结合,在用户隐私保护与实时电量数据之间实现一个良好的平衡,并且通过在智能电网的典型攻击下的安全属性分析,体现了协议实现的安全性能。

但现在只是实现协议安全性的理论证明,下一步工作可以使用密码学协议的自动形式化验证分析来验证协议的安全性,更进一步可以搭建智能电网系统的模拟实验环境,使用设计的认证协议来进行安全性分析,从而进一步完善协议。

### 参考文献:

- [1] MENG W, MA R, CHEN H H. Smart grid neighborhood area networks: a survey[J]. IEEE Network, 2014, 28(1): 24-32.
- [2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceedings of CRYPTO 1984 LNCS196. [s. l.]: Springer-Verlag, 1985: 47-53.
- [3] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Cryptology - Asiacrypt 2003, LNCS 2894. [s. l.]: Springer-Verlag, 2003: 452-473.
- [4] GARCIA F D, JACOBS B. Privacy-friendly energy-metering via homomorphic encryption[C]//Proceedings of privacy-friendly energy-metering via homomorphic encryption. [s. l.]: Springer-Verlag, 2010: 226-238.
- [5] LI J, TENG M, ZHANG Y, et al. A leakage-resilient CCA-secure identity-based encryption scheme[J]. Comput J, 2016, 59(7): 1066-1075.
- [6] LI Fengjun, LUO Bo, LIU Peng. Secure and privacy-preserving information aggregation for smart grids[J]. International Journal of Security and Networks, 2011, 6: 28-39.
- [7] LI S, ZHANG F, SUN Y, et al. Efficient leakage-resilient public key encryption from DDH assumption[J]. Cluster Computing, 2013, 16(4): 797-806.
- [8] NAOR M, SEGEV G. Public-key cryptosystems resilient to key leakage[J]. SIAM J Comput, 2012, 41(4): 772-814.
- [9] QIN B, LIU S, CHEN K. Efficient chosen-ciphertext secure public-key encryption scheme with high leakage-resilience[J]. IET Information Security, 2015, 9(1): 32-42.
- [10] ALWEN J, DODIS Y, NAOR M, et al. Public-key encryption in the bounded-retrieval model[C]//Advances in cryptology - CRYPTO 2009, LNCS 6110. [s. l.]: Springer-Verlag, 2010: 36-54.
- [11] DODIS Y, HARALAMBIEV K, LOPEZ-ALT A, et al. Cryptography against continuous memory attacks[C]//IEEE 54th annual symposium on foundations of computer science. Las Vegas, Nevada, USA: IEEE, 2010: 511-520.
- [12] XIONG H, YUEN T, ZHANG C, et al. Leakage-resilient certificateless public key encryption[C]//Proc 1st ACM workshop on Asia public-key cryptography. Hangzhou: ACM, 2013: 13-22.
- [13] WANG Z, YOU S. Attribute-based encryption resilient to auxiliary input[C]//Prov Sec 2015, LNCS 9451. [s. l.]: Springer-Verlag, 2015: 371-390.
- [14] GOLDWASSER A A, VAIKUNTANATHAN G S. Simultaneous hardcore bits and cryptography against memory attacks[C]//Proc. of CRYPTO. [s. l.]: Springer-Verlag, 2009: 36-54.
- [15] LI S, XUE K, YANG Q, et al. PPMA: privacy-preserving multi-subset aggregation in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(2): 462-471.
- [16] WANG Z. Leakage resilient additively homomorphic IBE for big data security[C]//Prov Sec LNCS 11442. [s. l.]: Springer-Verlag, 2017: 331-352.