

基于智能电网的安全密钥共享算法

顾伟¹, 沈剑², 任勇军¹

(1. 南京信息工程大学计算机与软件学院, 江苏 南京 210044

2. 南京信息工程大学研究生院, 江苏 南京 210044)

摘要: 针对多数密钥建立协议存在中间参数泄露和私钥泄露问题, 提出新的公钥共享的对称加密(PKS-SE)算法, 进而维护智能电表与服务商间通信的安全。PKS-SE 算法以双线性映射、超奇异曲线为基础, 构建智能电表与服务商通信的通信密钥, 避免密钥托管问题。同时, PKS-SE 算法减少了认证过程中交互的消息数, 进而控制了 PKS-SE 算法的通信成本和运算成本。仿真结果表明, 所提 PKS-SE 算法有效地实现了公钥共享。

关键词: 智能电网安全; 密钥建立; 密钥托管; 通信成本; 运算成本

中图分类号: TP183

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021081

Secure key-sharing algorithm based on smart grid

GU Wei¹, SHEN Jian², REN Yongjun¹

1. School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

2. Graduate School, Nanjing University of Information Science and Technology, Nanjing 210044, China

Abstract: Most of establishment-key protocols suffer from both session-specific temporary information attack and private key leakage issue. Therefore, a novel public key sharing-based symmetric encryption algorithm (PKS-SE) was proposed, in order to maintain the security of communication between smart meter and service providers. Based on bilinear mapping and super-singular curve, PKS-SE algorithm constructed the communication key between intelligent electricity meter and service provider, in order to avoid the key escrow problem. At the same time, PKS-SE algorithm reduced the number of required messages during the mutual authentication to only two messages, thus controlling the communication cost and operation cost of PKS-SE algorithm. Simulation results show that the proposed PKS-SE algorithm can effectively realize public key-sharing

Keywords: smart grid security, key establishment, key escrow, communication cost, computation cost

收稿日期: 2021-02-24; 修回日期: 2021-06-10

通信作者: 顾伟, hbyu_89uh@yeah.net

基金项目: 国家自然科学基金优秀青年基金(61922045); 国家自然科学基金(62072249)

Foundation Items: The National Natural Science Foundation of China for Excellent Young Scholars (61922045), The National Natural Science Foundation of China (62072249)

论文引用格式: 顾伟, 沈剑, 任勇军. 基于智能电网的安全密钥共享算法[J]. 网络与信息安全学报, 2021, 7(4): 141-146.

GU W, SHEN J, REN Y J. Secure key-sharing algorithm based on smart grid[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 141-146.

1 引言

为了克服传统电网的不足,如单向通信、机电结构和集中管理^[1],智能电网(SG, smart grid)应运而生。SG 便捷了电力的控制和管理。在 SG 中,电力所与用户间存在信息和电力两项流量。例如,智能电表(SM, smart meter)收集用户的消费数据,并向服务商(SP, service provider)传输消息。反之,服务商也向 SM 传输消息。

借助于双向通信机制,通过优化电力管理和便捷消费数据的收集,SG 提高了电力资源的利用率^[2]。此外,需求响应或需求侧管理(DSM, demand-side management)是革新的 SG 的基本要求^[3-4]。而收集用户消费数据是 DSM 技术的基本作用^[5]。然而,用户向服务商发送消耗数据可能泄露用户的隐私^[6]。此外,众多网络攻击(如伪装攻击、重放攻击、中间人攻击)扰乱了消息的交互^[7]。为了防御网络攻击,SG 需采用有效的安全策略。

为了维护 SM 与服务商间数字通信链路的安全,通常采用对称密钥算法,然而,对称密钥算法需在两个通信实体间分享公密钥。为此,研究者针对对称密钥算法的密钥分布策略进行了大量研究。

2011 年, Fouda 等^[8]提出基于 Diffie-Hellman 的密钥分布方案; Wu 等^[9]提出了基于椭圆曲线加密的密钥分布方案。然而,文献[9]的方案容易遭受中间人攻击。文献[10]针对智能电网短暂密钥泄露问题,提出了安全匿名密钥分发(SAKD, secure anonymous key distribution)方案。但 SAKD 方案存在密钥第三方托管问题,也存在短暂密钥泄露问题。文献[11]提出了可验证的安全认证密钥(PSAK, provably secure authenticated key)方案。尽管 PSAK 方案解决了短暂密钥泄露问题,但仍存在密钥第三方托管问题。相比 SAKD 方案、PSAK 方案,文献[12]提出的轻量级匿名密钥分发(LAKD, lightweight anonymous key distribution)方案的运算时间和通信成本较低,但 LAKD 方案也存在密钥泄露和密钥第三方托管问题。

为此,面向智能电表与服务商间通信问题,本文提出公钥共享的对称加密(PKS-SE, public key sharing-based symmetric encryption)算法。PKS-SE 算法利用双线性映射、非超奇异曲线以及基于身份加密算法实现通信实体间的密钥共享。性能分析表明,所提 PKS-SE 算法能够以较低的通信成本,解决密钥第三方托管和短暂密钥泄露问题。

2 系统模型及攻击实体

2.1 系统模型

系统模型是指(如图 1 所示)主要由 SM、SP 和第三方信任体(TA, trusted anchor)组成的安全系统。作为电力设备,SM 的计算能力和存储空间有限^[13],用于收集用户的用电数据^[10]。

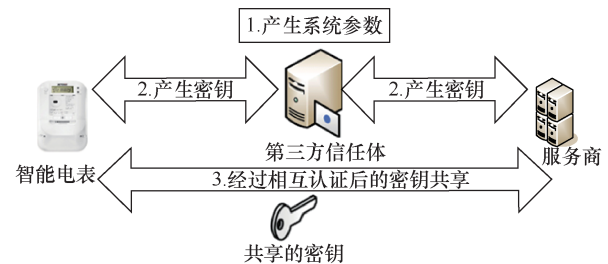


图 1 系统模型
Figure 1 System model

作为组织机构,SP 为电力消耗者提供服务^[14]。而 TA 是信任实体,其负责 SM 和 SP 的注册,产生 SM 和 SP 的私钥。

2.2 攻击实体

假定概率多项式时间攻击者 ρ 能够掌控交互的消息,即攻击者 ρ 能够窃听、篡改消息,且攻击者 ρ 通过具体攻击(EA, explicit attack)能够接入存储空间内的秘密信息^[15],对于任一实体 E ,攻击者 ρ 能够初始化实体 $E = \{E_0, E_1, \dots, E_\ell\}$ 。令 Υ_{ij}^s 表示实体 E_i 与实体 E_j 间的第 s 次通信,且 $i, j = 1, 2, \dots, \ell, i \neq j$ 。引用挑战者 κ 与攻击者 ρ 间的博弈游戏分析 PKS-SE 算法的安全性。

3 PKS-SE 算法

PKS-SE 算法主要由系统初始化、实体注册和密钥共享 3 个阶段构成。在系统初始化阶段,TA 产生系统参数;随后,进入实体注册阶段,SM

和服务商获取它们的私钥和公钥；最后，SM 和服务商建立公钥共享。

3.1 系统初始化

首先，TA 构建一个双线性映射 e ：

$$e: G_1 \times G_1 \rightarrow G_2 \quad (1)$$

其中， G_1 为加性循环群； G_2 是以 q 为阶数的乘法循环群。令 $P \in G_1$ 和 $g = e(P, P) \in G_2$ 为生成元。

在超奇异曲线 $E_1: y^2 = x^3 + x \bmod p_1$ 定义双线性映射 e ，其中 p_1 为 512 bit 的素数。 G_1 的阶数 q_1 为 160 bit 的素数。此外，TA 选择非超奇异曲线 E ，其定义如式(2)所示。

$$E(a, b): y^2 = x^3 + ax + b \bmod p \quad (2)$$

式中， $a, b \in Z_p^*$ 。 p 为 160 bit 的素数。

然后，TA 选择 4 个安全 Hash 函数 $\{h_1, h_2, h_3, h_4\}$ ，其定义如式(3)所示。

$$\begin{cases} h_i: \{0, 1\}^* \rightarrow Z_q^*, & i=1, 2, 3 \\ h_4: G_2 \times \{0, 1\}^* \rightarrow \{0, 1\}^m \end{cases} \quad (3)$$

接着，TA 选择两个随机数 $s_1 \in Z_{q_1}^*$ 和 $s \in Z_q^*$ ，并将 s_1 和 s 作为系统的私钥。计算系统公钥 $P_{\text{pub}}^1 = s_1 P_1$ 和 $P_{\text{pub}} = sP$ ，其中， $P_1 \in G_1$ ，但 $P_1 \neq P$ 。

最后，TA 在网络内分发系统的公共参数为 $(G_1, G_2, e, p, q, p_1, q_1, g, P_1, P, P_{\text{pub}}^1, P_{\text{pub}}, h_1, h_2, h_3, h_4)$ (4)

3.2 实体注册

3.2.1 SP 注册

令 SP_j 表示第 j 个服务商。以 SP_j 为例，阐述 SP 的注册过程，如图 2(a)所示。

步骤 1 SP_j 选择一个随机数 $r_j \in Z_q^*$ ，并计算 $R_j = r_j P$ ，再将 $\{ID_j, R_j\}$ 通过安全信道传输 TA，其中 ID_j 表示 SP_j 的 ID 号。

步骤 2 一旦收到 $\{ID_j, R_j\}$ 消息，TA 选择一个随机数 $r_t \in Z_q^*$ ，并计算见证令牌 (WT, witness token) WT_j 。

$$WT_j = R_j + r_t P_{\text{pub}} \quad (5)$$

再依据式(6)计算 s_j 。

$$s_j = (h_1(ID_j \parallel WT_j) + r_t) s \bmod q \quad (6)$$

式中， $\parallel$ 表示连接符号。

随后，TA 产生基于身份的解密密钥 K_j 。

$$K_j = \frac{1}{s_1 + h_1(ID_j)} P_1 \quad (7)$$

通过安全信道，TA 向 SP_j 传输参数 $\{WT_j, s_j, K_j\}$ 。

步骤 3 SP_j 依据式(8)计算私钥 k_j 和公钥 Q_j 。

$$\begin{cases} k_j = (r_j + s_j) \bmod q \\ Q_j = k_j P \end{cases} \quad (8)$$

任一实体通过验证等式 $Q_j = WT_j + h_1(ID_j \parallel WT_j) P_{\text{pub}}$ ，证实 SP_j 的公钥 Q_j 的真实性。

理论 1 当满足 $Q_j = WT_j + h_1(ID_j \parallel WT_j) P_{\text{pub}}$ 时，通过 s_j 能够推导出公钥 Q_j 。

证明过程如下。

$$\begin{aligned} Q_j &= k_j P = (r_j + s_j) P = r_j P + s_j P = \\ &= ((h_1(ID_j \parallel WT_j) + r_t) s) P = \\ &= R_j + h_1(ID_j \parallel WT_j) P_{\text{pub}} + r_t P_{\text{pub}} = \\ &= WT_j + h_1(ID_j \parallel WT_j) P_{\text{pub}} \end{aligned}$$

步骤 4 SP_j 将 $\{K_j, k_j, Q_j, WT_j\}$ 存储于防干扰 (tamper-proof) 单元。

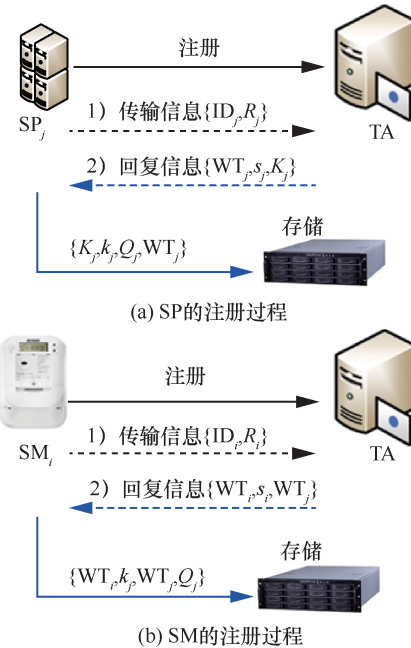


图2 SP 和 SM 向 TA 的注册过程
Figure 2 The registration process of SP and SM with TA

3.2.2 SM 注册

令 SM_i 表示第 i 个智能电表，以 SM_i 为例，阐述 SP 的注册过程，如图 2(b)所示。

步骤 1 SM_i 选择一个随机数 $r_i \in Z_q^*$ ，并计算 $R_i = r_i P$ ，再将 $\{ID_i, R_i\}$ 通过安全信道传输 TA，其中 ID_j 表示 SM_i 的 ID 号。

步骤 2 一旦接收 $\{ID_i, R_i\}$ 消息，TA 选择新的随机数 $r_i \in Z_q^*$ ，计算 $WT_i = R_i + r_i P_{pub}$ ，并将 WT_i 作为 WT。再计算 $s_i = (h_1(ID_i \parallel WT_i) + r_i) s \bmod q$ 。随后，TA 通过安全信道，向 SM_i 传输 $\{WT_i, s_i, WT_j\}$ 信息。

步骤 3 SM_i 收到 $\{WT_i, s_i, WT_j\}$ 信息后， SM_i 依据式(10)计算私钥和公钥。

$$\begin{cases} k_i = (r_i + s_i) \bmod q \\ Q_i = k_i P \end{cases} \quad (9)$$

步骤 4 SM_i 将 $\{WT_i, k_i, WT_j, Q_i\}$ 存储于防干扰单元。

3.3 公钥共享

步骤 1 SM_i 选择一个随机数 $a_i \in Z_q^*$ ，并计算 $A_i = a_i Q_i$ ；再选择一个随机数 $z_i \in Z_{q_1}^*$ ，并计算 $T_i = z_i (h_1(ID_j) P_1 + P_{pub}^1)$ ，根据式(10)计算参数 C_i ：

$$C_i = h_4(g^{z_i}, ID_j) \oplus (ID_i, WT_i) \quad (10)$$

式中， $\oplus$ 表示异或操作。

根据式(11)计算参数 B_i 。

$$B_i = k_i (WT_j + h_1(ID_j \parallel WT_j) P_{pub}) \quad (11)$$

随后，由 SM_i 验证 $V_i = h_2(ID_i \parallel A_i \parallel B_i \parallel WT_i \parallel CT_i)$ 。 SM_i 向 SP_j 传输信息 $\{C_i, T_i, A_i, V_i, CT_i\}$ 。其中， CT_i 为发送消息的时间戳。

步骤 2 一旦收到消息， SP_j 验证 $|CT_j - CT_i| < \Delta T$ ，保证消息的新鲜度。其中 CT_j 为接收消息的时间戳， ΔT 是最大的传输时延。

SP_j 计算 $g^{z_i} = e(T_i, K_j)$ 和 $(ID_i, WT_i) = C_i \oplus h_4(g^{z_i}, ID_j)$ ，获取 SM_i 的身份和 WT。随后， SP_j 根据式(12)计算 B_j 。

$$B_j = k_j (WT_i + h_1(ID_i \parallel WT_i) P_{pub}) \quad (12)$$

验证等式 $h_2(ID_i \parallel A_i \parallel B_i \parallel WT_i \parallel CT_i) \stackrel{?}{=} V_i$ 。如果验证通过，则说明所接收的消息未被篡改，发送消息的发送者 (SM_i) 身份合法。

SP_j 选择随机数 $a_j \in Z_q^*$ ，并计算 $A_j = a_j Q_j$ 和 $K_{ji} = a_j k_j A_i$ 。然后， SP_j 验证 $V_j = h_2(ID_j \parallel A_j \parallel B_j \parallel WT_j \parallel K_{ji} \parallel CT_j)$ ，再向 SM_i 传输 $\{A_j, V_j, CT_j\}$ ，进而使 SP_j 获取 $Trans = (A_i \parallel A_j \parallel V_i \parallel V_j)$ 。最后， SP_j 根据式(13)计算共享的密钥 SK_{ij} 。

$$SK_{ij} = h_3(ID_i \parallel ID_j \parallel Trans \parallel K_{ji}) \quad (13)$$

步骤 3 当接收 $\{A_j, V_j, CT_j\}$ 后， SM_i 确认 $|CT_i - CT_j| < \Delta T$ ，并计算 $K_{ij} = a_i k_i A_j$ ，再验证 $h_2(ID_j \parallel A_j \parallel B_i \parallel WT_j \parallel K_{ij} \parallel CT_j) \stackrel{?}{=} V_j$ 。若通过验证， SM_i 继续计算 $Trans = (A_i \parallel A_j \parallel V_i \parallel V_j)$ ，进而共享密钥 $SK_{ij} = h_3(ID_i \parallel ID_j \parallel Trans \parallel K_{ij})$ 。图 3 描述了密钥共享流程。

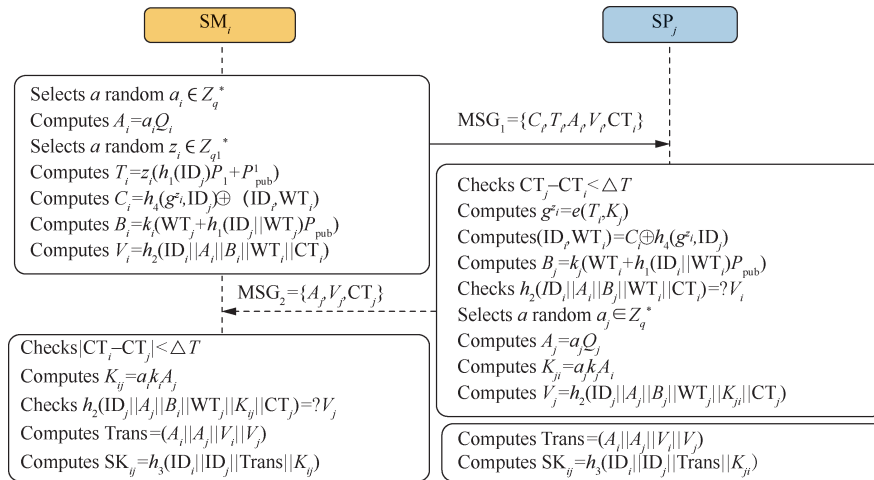


图 3 密钥共享流程

Figure 3 Key sharing process

4 性能分析

4.1 安全性能分析

(1) 抵御中间参数泄露的攻击

PKS-SE 算法利用 $h_3(\text{ID}_i \parallel \text{ID}_j \parallel \text{Trans} \parallel K_{ji})$ 或 $h_3(\text{ID}_i \parallel \text{ID}_j \parallel \text{Trans} \parallel K_{ij})$ 计算密钥 SK_{ij} 。其中 $K_{ij} = a_i k_i A_j$ 、 $K_{ji} = a_j k_j A_i$ 。因此, 即使中间秘密参数 a_i 和 a_j 被泄露于攻击者 φ , 攻击者 φ 也无法推算 K_{ij} 或 K_{ji} 。

(2) 防御私钥泄露攻击

即使攻击者 φ 窃取了中间参数 a_i 和 a_j , 并拥有公共参数 $\{C_i, T_i, A_i, V_i, \text{CT}_i\}$ 和 $\{A_j, V_j, \text{CT}_j\}$, 攻击者 φ 也无法推算 SM 的私钥 k_i 。PKS-SE 算法用式(14)计算 SM 的私钥。

$$\begin{cases} B_i = k_i (\text{WT}_j + h_1(\text{ID}_j \parallel \text{WT}_j) P_{\text{pub}}) \\ K_{ij} = a_i k_i A_j \end{cases} \quad (14)$$

因此, 即使攻击者 φ 窃取了 a_i 和 A_j , 甚至攻击者 φ 窃取了 K_{ij} , 由于攻破椭圆曲线离散对数问题(ECDLP, elliptical curve discrete logarithm problem)的难度, 攻击者 φ 也无法推算私钥 k_i 。

4.2 通信成本和运算成本分析

为了更好地分析 PKS-SE 算法的通信成本和运算成本, 选择 SKAD 算法、PSAK 算法和 LAKD 算法作为参照, 并对比分析它们的性能。

(1) 通信成本

假定 p_1 、 p 、 q_1 和 q 的尺寸分别为 512 bit、160 bit、160 bit 和 160 bit, 而 G_1 、 G_2 的尺寸均为 1024 bit^[12]。此外, 考虑身份的尺寸和 Hash 输出序列均为 160 bit。时间戳尺寸为 32 bit, 随机数为 126 bit。

依据上述条件, 表 1 给出 PKS-SE 算法、SKAD 算法、PSAK 算法和 LAKD 算法的通信成本。从表 1 可知, 相比 SKAD 算法和 LAKD 算法, PKS-SE 算法有效地控制了通信成本。然而, 相比 LAKD 算法, PKS-SE 算法的通信成本仍存在较大的压缩空间。

(2) 运算成本

依据文献[12]的研究, 表 2 列出加密算法中各个运算所需的时间。在 Windows 7 操作系统、8 GB 内存、core i7 CPU 的 PC 上运行算法。

表 1 各算法的通信成本

Table 1 Communication cost of each algorithm

算法	消息	通信成本/bit
SKAD	$\{C_1, C_2\}, \{R_1, R_2\}, \{C_3\}$	3 520
PSAK	$\{T_1, C_1, A_1\}, \{g_1, A_2\}, \{A_3\}$	3 840
LAKD	$\{A\}, \{B, R_{sp}, \beta_{sp}\}, \{\varphi_{SM}\}$	1 760
PKS-SE	$\{C_1, T_i, A_i, \text{CT}_i\}, \{A_j, V_j, \text{CT}_j\}$	2 528

表 2 加密算法中各个运算所需的运算时间

Table 2 The computation time required for each operation in encryption algorithm

操作	运算时间/s
双线性对	0.032 713
Hash函数	0.000 006
在 G_1 的点乘	0.013 405
在 G_1 的加法	0.000 056
在 G_2 的乘法	0.000 008
在 G_2 的指数运算	0.002 249
一个ECC 点乘	0.003 350
一个ECC 点加	0.000 014

依据表 2 的各个运算所需的运算时间, 表 3 列出 SKAD 算法、PSAK 算法、LAKD 算法及 PKS-SE 算法的执行时间。

表 3 各个算法的执行时间

Table 3 Execution time of each algorithm

算法	执行时间/s	总执行时间/s
SKAD	SM: 0.056 SP: 0.108	0.164
PSAK	SM: 0.043 SP: 0.095	0.138
LAKD	SM: 0.013 SP: 0.020	0.033
PKS-SE	SM: 0.043 SP: 0.046	0.089

从表 3 可知, PKS-SE 算法的执行时间优于 SKAD 算法和 PSAK 算法。PKS-SE 算法的执行时间为 0.089 s, 而 SKAD 算法和 PSAK 算法的执行时间分别为 0.164 s 和 0.138 s。相比于 LAKD 算法, PKS-SE 算法的执行时间较长。

4.3 安全性能的对比分析

表 4 给出 PKS-SE 算法、SKAD 算法、PSAK 算法和 LAKD 算法在安全方面的性能。其中, F1 表示抵御中间攻击; F2 表示抵御伪装攻击; F3 表示抵御重放攻击; F4 表示无须 TA 的帮助下具有相互认证的能力; F5 表示具有强的 SM 匿名性; F16 表示无密钥托管问题; F7 表示抵御短暂的密钥泄露攻击。

表4 PKS-SE 算法的安全性能
Table 4 Safety performance of PKS-SE algorithm

算法	F1	F2	F3	F4	F5	F6	F7
SKAD	√	√	√	√	√	×	×
PSAK	√	√	√	√	√	×	√
LAKD	√	√	√	√	√	×	×
PKS-SE	√	√	√	√	√	√	√

注: √ 表示满足; × 表示不满足。

从表4可知,相比SKAD算法、PSAK算法和LAKD算法,PKS-SE算法在安全性能上具有优势。

5 结束语

智能电网中的数据传输是智能电表与服务商间通信链路的基本功能。然而,数据传输容量易遭受网络攻击。对称加密算法是维护通信安全的常用算法。为此,本文提出了PKS-SE算法,该算法采用对称加密算法,使智能电表与服务商安全地共享密钥。性能分析表明,PKS-SE算法有效地解决了密钥托管问题,并控制了通信成本和计算成本。

参考文献:

- [1] COLAK I, SAGIROGLU S, FULLI G. A survey on the critical issues in smart grid technologies[J]. Renewable Sustain Energy Rev, 2016, 54(8): 396-405.
- [2] 葛少云, 张有为, 刘洪. 考虑网架动态重构的主动配电网双层扩展规划[J]. 电网技术, 2018, 42(5): 36-42.
GE S Y, ZHANG Y W, LIU H. Bi-layer expansion programming method for active distribution network considering dynamic grid reconfiguration[J]. Power System Technology, 2018, 42(5): 36-42.
- [3] MOGHADDAM M H, LEON-GARCIA Y A, MOGHADDASIAN M. On the performance of distributed and cloud-based demand response in smart grid[J]. IEEE Trans Smart Grid, 2018, 9(5): 5403-5417.
- [4] YAGHMAEE M H, MOGHADDASIAN M. Autonomous two-tier cloud-based demand side management approach with microgrid[J]. IEEE Trans Ind Inform, 2017, 13(3): 1109-1120.
- [5] KEMENT C E, GULTEKIN H, TAVLI B, et al. Comparative analysis of load-shaping-based privacy preservation strategies in a smartgrid[J]. IEEE Trans Ind Inform, 2017, 13(6): 3226-3235.
- [6] FAN C I, HUANG S Y, LAI Y L. Privacy-enhanced data aggregation scheme against internal attackers in smart grid[J]. IEEE Transactions Ind Inform, 2014, 10(1): 666-675.
- [7] SAXENA N, GRIJALVA S. Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication[J]. IEEE Trans Ind Inform, 2017, 13(3): 1482-1491.
- [8] FOUDA M M, FADLULLAH Z M, KATO N. A lightweight message authentication scheme for smart grid communications[J]. IEEE Trans Smart Grid, 2011, 2(4): 675-685.

- [9] WU D, ZHOU C. Fault-tolerant and scalable key management for smart grid[J]. IEEE Trans Smart Grid, 2011, 2(2): 375-381.
- [10] TSAI J L, LO N W. Secure anonymous key distribution scheme for smart grid[J]. IEEE Trans Smart Grid, 2016, 7(2): 906-914.
- [11] ODELU V, DAS A K, WAZID M. Provably secure authenticated key agreement scheme for smart grid[J]. IEEE Trans Smart Grid, 2018, 9(3): 1900-1910.
- [12] HE D, WANG H, KHAN M K, et al. Light weight anonymous key distribution scheme for smart grid using elliptic curve cryptography[J]. IET Communication, 2016, 10(14): 1795-1802.
- [13] 彭楚宁, 罗冉冉, 王晓东. 新一代智能电表支撑泛在电力物联网技术研究[J]. 电测与仪表, 2019, (15): 34-43.
PENG C N, LUO R R, WANG X D. Research on a new generation of smart meter-technology supports ubiquitous power internet of things[J]. Electrical Measurement & Instrumentation, 2019, (15): 34-43.
- [14] 李德峰, 陈述. 配电网雷电防护措施总结分析及其应用[J]. 电网与清洁能源, 2014, (12): 45-52.
LI D F, CHEN S. The Summary of lightning protection measures and its applications for the distribution network[J]. Power System and Clean Energy, 2014, (12): 45-52.
- [15] CANETTI R, KRAWCZY H. Analysis of key-exchange protocols and their use for building secure channels[C]//Proc Int Conf Theory Appl Cryptographic Techn. 2001: 453-474.

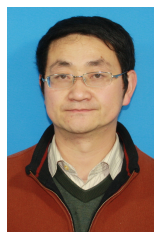
[作者简介]



顾伟(1983—),男,江苏靖江人,南京信息工程大学高级实验师,主要研究方向为模式识别、人工智能、数据挖掘、信息安全。



沈剑(1985—),男,江苏南京人,博士,南京信息工程大学教授、博士生导师,主要研究方向为密码学、公钥密码学、数据安全。



任勇军(1974—),男,河北承德人,博士,南京信息工程大学副教授,主要研究方向为信息安全和区块链。