计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(4):137−142 [doi: 10.15888/j.cnki.csa.008422]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

智能电网容错数据聚合方案①

李雅斌, 杨鹏飞

(长安大学 信息工程学院, 西安 710064)
通信作者: 李雅斌, E-mail: 963632227@qq.com

摘　要: 新一代智能电网的出现, 极大地提升了电网的安全性与可靠性, 这依赖于智能电表每 15 分钟发送一次数据, 但是这可能会暴露用户的隐私, 同时需要消耗很大的计算代价. 于是数据聚合技术被引入, 大多数现有聚合方案存在耗时大且当电表故障时系统无法正常运行等问题. 针对上述问题, 本文提出了一个智能电网中高效的支持错误容忍的数据聚合方案, 具体来说, 利用了改进的对称同态加密技术达到轻量级的效果, 在支持错误容忍的同时还能抵抗合谋攻击. 最后, 安全需求分析说明了该方案是安全的, 性能评价体现了本文的高效性, 这契合于资源有限的智能电表.

关键词: 智能电网; 隐私; 数据聚合; 错误容忍; 同态加密; 隐私保护; 无线传感器网络

引用格式: 李雅斌,杨鹏飞.智能电网容错数据聚合方案.计算机系统应用,2022,31(4):137–142. http://www.c-s-a.org.cn/1003-3254/8422.html

Data Aggregation Scheme with Fault Tolerant in Smart Grid

LI Ya-Bin, YANG Peng-Fei

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: The new generation of smart grids has greatly improved the security and reliability of power grids, which relies on smart meters to send data every 15 minutes. However, this may expose the privacy of users and also requires a huge computation cost. As a result, data aggregation technology is introduced. Most of the existing aggregation schemes are time-consuming and the system cannot run normally when its meter fails. In response to the above problems, this study proposes an efficient data aggregation scheme with fault tolerance in smart grids. Specifically, it uses the improved symmetric homomorphic encryption technology to be lightweight. It can resist collusion attacks while supporting fault tolerance. The security requirements analysis shows that the scheme is secure, and the performance evaluation reflects the efficiency of the scheme, which fits the smart meters with limited resources.

Key words: smart grid; privacy; data aggregation; fault tolerant; homomorphic encryption; privacy protection; wireless sensor network

随着传统电网的各种弊端不断显现, 智能电网以其双向通信, 多元化梯度电价, 状态分析预警等优势[1,2]逐渐被各个国家重视[3–5]起来.

在智能电网中, 部署了大量的传感器, 尤其是智能电表, 每隔 15 分钟发送电力数据给控制中心以供分析与调配[6]. 然而大量的实时传输数据不仅会损耗海量资源同时还存在隐私泄露的问题[7,8]. 因此为了克服以上问题, 数据聚合技术被引入, 它可以节省计算资源, 同时允许控制中心收集聚合数据而不是单个数据的思想很好的保护用户的隐私且不影响数据的分析和电力供应的调整.

但是, 现有大多数聚合方案存在以下两个问题: 很多方案设计时采用代价很高的公钥同态加密技术, 这对资源受限的智能电表很不友好; 许多方案没有

① 收稿时间: 2021-06-28; 修改时间: 2021-07-30; 采用时间: 2021-08-12; csa 在线出版时间: 2022-03-22

考虑错误容忍的问题, 但是智能电表是普通电子设备很有可能出现故障, 这样会导致整个系统无法正常运作.

基于上述问题, 本文提出了一个智能电网中高效的支持错误容忍的数据聚合方案, 该方案能抵抗由网关和控制中心发起的合谋攻击, 此外, 当智能电表故障时, 控制中心仍能正常恢复聚合数据.

1 背景知识

1.1 系统模型

本文的系统模型如图 1 所示, 其中有 4 个实体: 可信中心 TA, 控制中心 CC, 网关 GW 和智能电表 SM_i $(i=1,2,\cdots,n)$. GW 负责其下 n 个SM_i $(n>1)$.

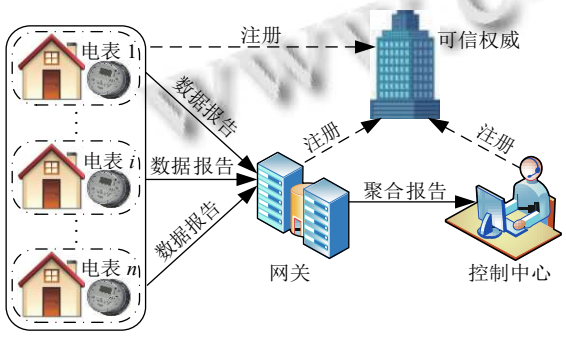

图 1 系统模型图

(1) TA: 表示完全可信的实体. TA 产生系统参数, 并负责SM_i, GW 和 CC 的注册. 如果SM_i产生故障, TA 生成虚拟密文.

(2) CC: 诚实且好奇的实体. 收到 GW 的聚合报告, CC 检查报告的完整性, 解密和分析电力测量数据.

(3) GW: 诚实且好奇的实体, 负责检验和聚合SM_i的电力报告并传输聚合报告给 CC.

(4) SM_i: 表示第 i 个智能电表, 是可信实体, SM_i主要收集和加密电力测量数据, 然后传输电力报告给 GW.

1.2 安全需求

(1) 机密性: 方案中使用的密文不能被敌手攻破, 即敌手不能获得真正的明文消息, 只能得到无意义的字符串.

(2) 可认证性: 敌手可能伪装成合法用户来破坏系统, 所以该方案应该对报告的来源进行身份认证.

(3) 完整性: 在公开信道中传输的报告可能被敌手拦截篡改再重新发送, 这会给正常报告注入错误数据. 因此该方案应该能检测报告是否被篡改.

(4) 错误容忍: 智能电表有可能发生故障, 当有故障发生时, 系统应该能继续正常运行.

(5) 抵抗合谋攻击: GW 和 CC 是半可信的实体, 他们联合起来好奇单个智能电表的电力数据. 在该方案中, 合谋攻击应该被抵抗.

(6) 抵抗重放攻击: 攻击者将以前在公开信道中传输的报告重新传输, 扰乱系统运行. 在该方案中, 重放攻击应该被抵抗.

1.3 设计目标

(1) 隐私保护: 除了 TA, 其他任何实体不允许知道单个SM_i的电力测量数据. 聚合的电力测量数据只允许 CC 获得, 用于分析和优化.

(2) 高效性: 由于智能电表和网关等实体的计算和通信资源都是有限的, 所以在满足上述隐私保护的前提下, 尽可能使方案的计算和通信代价最小.

1.4 椭圆曲线密码学

椭圆曲线 E 由方程$y^2=x^3+ax+b \bmod p$所定义[9], 该方程是基于有限域F_p上的, 这里$a,b\in F_p$且满足$4a^3+27b^2\neq 0$. 所有 E 上的点和无穷远点 O 共同组成了加法循环群$\mathbb{G}$, 阶数是 q, 生成元是 P. 标量点乘定义为 $kP=P+P+\cdots+P$ (k次), 这里$k\in\mathbb{Z}_q^*$.

椭圆曲线离散对数假设 (ECDLA): 给定任意 P, $aP\in\mathbb{G}$, $(a,b\in Z_q^*)$, 在多项式时间算法内很难算出 $a\in\mathbb{Z}_q^*$.

1.5 对称同态加密

文献 [10] 首次提出对称同态加密技术, 然而文献 [11] 将其攻破, 根据其弱点, 现在本文改进该技术, 具体描述如下:

$KeyGen(\tau)$: 输入安全参数τ, 密钥生成算法输出对称同态加密密钥$K=\{s,d,\hat{q},\hat{p}\}$, 其中两个大素数$\hat{p},\hat{q}$满足$\hat{p}\gg\hat{q}$, s是从$\mathbb{Z}_{\hat{p}}^*$随机选择的, 密文等级 d 是小的正整数. 计算公开参数$N=\hat{p}\hat{q}$.

$Enc(K,m,r)$: 输入明文$m\in\mathbb{Z}_{\hat{q}}^*$和对称同态加密密钥 $K=\{s,d,\hat{q},\hat{p}\}$, 加密算法选择随机数$r\in\{0,1\}^\tau$满足$|r|+|\hat{q}|<|N|$, 然后加密明文:

$$c=s^d(r\hat{q}+m) \bmod N$$

$Dec(K,c)$: 输入密文 c 和对称同态加密密钥$K=\{s,d,\hat{q},\hat{p}\}$, 解密算法计算:

$$m=(s^{-d}c \bmod N) \bmod \hat{q}$$

2 本文方案

2.1 系统建立

(1) 基于非奇异椭圆曲线 E, TA 生成阶数为素数 q 的加法循环群$\mathbb{G}$和其生成元 P.

(2) TA 生成对称同态加密密钥 $K=\{s,d,\hat{q},\hat{p}\}$. TA 计算公开参数$N=\hat{p}\hat{q}$.

(3) TA 随机选取一组盲化因子$\xi_1,\xi_2,\cdots,\xi_n\in\mathbb{Z}_N^*$, 然后计算$\xi=\sum_{i=1}^{n}\xi_i$.

(4) TA 选择安全哈希函数$H_i:\{0,1\}^*\to\mathbb{Z}_q^*(i=1,2)$, 公布系统参数:$<\mathbb{G},q,P,N,H_1,H_2>$.

2.2 注册

所有$SM_i\ (i=1,2,\cdots,n)$, GW和CC都需要在可信中心 TA 处进行注册, 并获得相应的密钥和盲化因子.

(1) SM_i注册

① SM_i随机选择$s_i\in\mathbb{Z}_q^*$作为自己的签名私钥, 选择随机数$u_i\in\mathbb{Z}_q^*$, 计算对应公钥$S_i=s_iP$和知识签名$U_i=u_iP, v_i=s_iH_1(ID_i,S_i,U_i)+u_i$, 然后发送$<ID_i,S_i,U_i,v_i>$给 TA.

② TA 收到后, 检查$v_iP=S_iH_1(ID_i,S_i,U_i)+U_i$是否成立, 如果成立, 公布$<ID_i,S_i,U_i,v_i>$, 并秘密发送$<\xi_i,K>$给$SM_i$.

(2) GW 注册

① GW 随机选择$s_{GW}\in\mathbb{Z}_q^*$作为自己的签名私钥, 选择随机数$u_{GW}\in\mathbb{Z}_q^*$, 计算公钥$S_{GW}=s_{GW}P$和知识签名$U_{GW}=u_{GW}P, v_{GW}=s_{GW}H_1(ID_{GW},S_{GW},U_{GW})+u_{GW}$, 然后发送$<ID_{GW},S_{GW},U_{GW},v_{GW}>$给 TA.

② TA 收到消息后, 检查下列等式$v_{GW}P=S_{GW}H_1(ID_{GW},S_{GW},U_{GW})+U_{GW}$是否成立, 如果成立, 公布$<ID_{GW},S_{GW},U_{GW},v_{GW}>$.

(3) CC 注册

① CC 随机选择$s_{CC}\in\mathbb{Z}_q^*$作为自己的签名私钥, 选择随机数$u_{CC}\in\mathbb{Z}_q^*$, 计算对应公钥$S_{CC}=s_{CC}P$和知识签名$U_{CC}=u_{CC}P, v_{CC}=s_{CC}H_1(ID_{CC},S_{CC},U_{CC})+u_{CC}$, 然后发送$<ID_{CC},S_{CC},U_{CC},v_{CC}>$给 TA.

② TA 收到消息后, 检查下列等式$v_{CC}P=S_{CC}H_1(ID_{CC},S_{CC},U_{CC})+U_{CC}$是否成立, 如果成立, 公布$<ID_{CC},S_{CC},U_{CC},v_{CC}>$, 并秘密发送$<\xi,K>$给 CC.

2.3 报告产生

(1) SM_i收集电力测量数据m_i, 随机选择r_i满足$|r_i|+|\hat{q}|<|N|$, 计算:

$$C_i=s^d(r_i\hat{q}+m_i+\xi_i)\bmod N$$

(2) SM_i随机选择$e_i\in\mathbb{Z}_q^*$, 计算:

$$E_i=e_iP,\sigma_i=s_iH_2(C_i,S_i,ID_i,E_i,T_i)+e_i$$

其中, T_i是当前时间戳. SM_i发送$<C_i,ID_i,E_i,\sigma_i,T_i>$给 GW.

2.4 报告聚合

(1) 当收到所有SM_i的报告$<C_i,ID_i,E_i,\sigma_i,T_i>$后, GW 首先检查时间戳T_i的有效性, 然后为了加速验证[12], GW 随机选取一组小数$\theta_1,\theta_2,\cdots,\theta_n\in[1,2^n]$, 检查等式:

$$\left(\sum_{i=1}^{n}\theta_i\sigma_i\right)P=\sum_{i=1}^{n}\theta_iS_iH_2(C_i,S_i,ID_i,E_i,T_i)+\sum_{i=1}^{n}\theta_iE_i$$

是否成立, 如果成立, 计算:

$$C=\sum_{i=1}^{n}C_i\bmod N$$

(2) GW 随机选择$e_{GW}\in\mathbb{Z}_q^*$, 计算$E_{GW}=e_{GW}P,\sigma_{GW}=s_{GW}H_2(C,S_{GW},ID_{GW},E_{GW},T_{GW})+e_{GW}$其中$T_{GW}$是当前时间戳. 最后, GW 发送报告$<C,ID_{GW},E_{GW},\sigma_{GW},T_{GW}>$给 CC.

2.5 报告阅读

(1) 当收到 GW 的报告$<C,ID_{GW},E_{GW},\sigma_{GW},T_{GW}>$后, CC 首先检查时间戳T_{GW}的有效性, 然后验证等式:

$$\sigma_{GW}P=S_{GW}H_2(C,S_{GW},ID_{GW},E_{GW},T_{GW})+E_{GW}$$

(2) 如果等式成立, CC 解密聚合的电力报告:

$$\sum_{i=1}^{n}m_i=[(s^{-d}C-\xi)\bmod N]\bmod\hat{q}$$

(3) CC 分析该 GW 所管辖区域的电力数据并优化电力分配策略.

正确性:

$$\begin{aligned}&\left[\left(s^{-d}C-\xi\right)\bmod N\right]\bmod\hat{q}\\&=\left[\left(s^{-d}\sum_{i=1}^{n}C_i-\xi\right)\bmod N\right]\bmod\hat{q}\\&=\left[\left(s^{-d}\sum_{i=1}^{n}(s^d(r_i\hat{q}+m_i+\xi_i))-\xi\right)\bmod N\right]\bmod\hat{q}\\&=\left[\left(\hat{q}\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}m_i+\sum_{i=1}^{n}\xi_i-\xi\right)\bmod N\right]\bmod\hat{q}\\&=\left(\hat{q}\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}m_i\right)\bmod\hat{q}\\&=\sum_{i=1}^{n}m_i\end{aligned}$$

本方案的具体流程如图 2 所示.

2.6 错误容忍

假如第 1 个到第$t\ (t<n)$个SM_i是正常工作的, 第$t+1$个到第 n 个SM_i发生了故障, 无法发送电力报告给 GW.

(1) *GW* 像第 2.4 节一样先进行时间戳的检查和完整性的验证, 然后计算 $\hat{C}=\sum_{i=1}^{t}C_i \bmod N$ 并发送给 *CC*, 同时告知 *TA* 故障的智能电表有哪些.

(2) *TA* 收到后, 替所有故障的电表计算聚合虚拟密文 $C_{TA}=s^d\left(r_i\hat{q}+0+\sum_{i=t+1}^{n}\xi_i\right) \bmod N$, 发送它给 *CC*.

(3) *CC* 收到 $<\hat{C},C_{TA}>$ 后, 解密计算:

$$\sum_{i=1}^{t}m_i=[(s^{-d}(\hat{C}+C_{TA})-\xi) \bmod N] \bmod \hat{q}$$

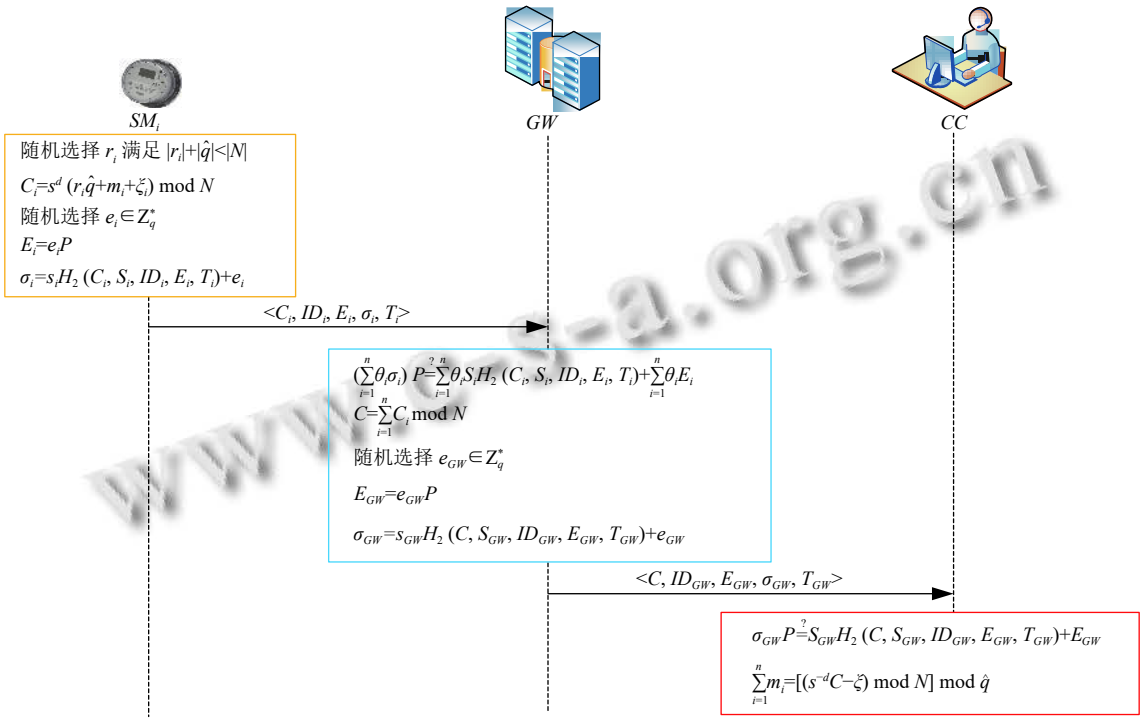

图 2　方案流程图

3　安全分析与性能评价

3.1　安全需求分析

本小节将逐个分析第 1.2 节中所提出的安全需求.

(1) 机密性: 方案中, 假如外部敌手获得了一个明文密文对 (m_i,C_i), 还存在 5 个未知数; 即使敌手获得 λ 对 (m_i,C_i), 仍然存在 $2\lambda+3$ 个未知数, 由于欠定非线性系统的求解是 NP 困难的[10], 这样无法在多项式时间内破解该方程. 因此, 该方案能保证机密性.

(2) 可认证性: SM_i 提前用自己的身份进行了注册, 后面发送报告时, *GW* 在对签名验证的同时也对身份合法性进行认证. 因此, 该方案可以实现用户的认证.

(3) 完整性: 利用 Schnorr 签名[13], 密文报告被签名为 (σ_i,E_i), 基于 ECDL 假设, 没有密钥 s_i 的敌手无法产生合法签名, 篡改的报告在检测时就会被拒绝. 所以, 方案可以保证报告的完整性.

(4) 错误容忍: 在方案中, 如果某些智能电表 SM_i 发生故障无法发送报告, *TA* 会替故障电表产生聚合的虚拟密文 C_{TA} 来保证 *CC* 可以顺利解密密文. 因此, 本方案可以支持错误容忍.

(5) 抵抗合谋攻击: 如果 *GW* 和 *CC* 合谋想获得某一个 SM_i 的电力数据, 通过密钥 *K* 的解密, *CC* 只能获得 $m_i+\xi_i$, 电力数据 m_i 被盲化因子 ξ_i 所保护. 因此, 本方案可以抵抗合谋攻击.

(6) 抵抗重放攻击: SM_i 和 *GW* 发送的报告中都包含时间戳 T_i 或 T_{GW}, *GW* 和 *CC* 可以检查报告的新鲜度. 因此, 本方案可以抵抗重放攻击.

3.2　功能比较

本小节将所提方案与文献 [14–16] 进行功能对比. 如表 1, 其中 F1 表示机密性; F2 表示可认证性; F3 表示完整性; F4 表示错误容忍; F5 表示抵抗合谋攻击; F6 表示抵抗重放攻击. 从表 1 中可以看出, 文献 [14] 无法支持错误容忍功能, 文献 [15] 不能抵抗重放攻击, 文献 [16] 不能抵抗合谋攻击. 而我们所提出的方案可以满足所有在第 1.2 节中描述的安全需求.

表 1 功能对比

功能	文献[14]	文献[15]	文献[16]	本文方案
F1	√	√	√	√
F2	√	√	√	√
F3	√	√	√	√
F4	×	√	√	√
F5	√	√	×	√
F6	√	×	√	√

注: “√”表示满足, “×”表示不满足

3.3 计算代价比较

文献 [14,16] 基于双线性对, 它定义为$e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_T$, 这里$\mathbb{G}_1$是加法循环群; ECC 中循环群记作$\mathbb{G}$. 本文使用 MIRACL Crypto SDK[17] 得到密码学操作的执行时间并列举在表 2 中, 其硬件设备为 2.53 GHz i5CPU 和 4 GB 内存的笔记本电脑, 操作系统是 64 位 Windows 10.

表 2 密码学操作执行时间 (ms)

符号	描述	执行时间
T_{BP}	双线性对操作	10.31
T_{mtp}	映射到点的哈希	3.58
$T_{e\text{-}T}$	$\mathbb{G}_T$下的指数运算	0.52
$T_{e\text{-}n}$	$\mathbb{Z}_n$下的指数运算	0.58
$T_{\log}$	解决离散对数操作	0.64
$T_{e\text{-}G}$	$\mathbb{G}_1$下的指数运算	1.42
$T_{e\text{-}p}$	$\mathbb{Z}_p^*$下的指数运算	0.13
$T_{e\text{-}N}$	模N下的指数运算	0.22
$T_{e\text{-}n^2}$	$\mathbb{Z}_{n^2}$下的指数运算	2.02
$T_{E\text{-}P}$	Paillier公钥加密	11.82
$T_{D\text{-}P}$	Paillier公钥解密	9.89
$T_{m\text{-}E}$	*ECC*下的标量乘法运算	0.38

注: 加法和一般哈希的执行时间已经被忽略

对于文献 [14] 来说, 报告产生阶段的计算时间是$T_{E\text{-}P}+2T_{e\text{-}p}+T_{m\text{-}E}+T_{mtp}=16.04$ ms, 聚合阶段的时间是$(n+2)T_{BP}+(n+1)T_{mtp}+T_{m\text{-}E}=(13.89n+24.58)$ ms, 阅读阶段的时间是$2T_{BP}+T_{mtp}+T_{D\text{-}P}+2T_{e\text{-}p}=34.35$ ms. 总的计算开销是$(29.93n+58.93)$ ms.

对于文献 [15] 来说, 报告产生阶段的计算时间是$T_{e\text{-}n^2}+T_{E\text{-}P}+T_{e\text{-}G}+T_{e\text{-}n}=15.84$ ms, 聚合阶段的时间是$(n+2)T_{e\text{-}n}+nT_{e\text{-}G}=(2n+1.16)$ ms, 阅读阶段的时间是$T_{e\text{-}n}+T_{D\text{-}P}=10.47$ ms. 总的开销是$(17.84n+11.63)$ ms.

对于文献 [16] 来说, 报告产生阶段的计算时间是$2T_{e\text{-}T}+T_{e\text{-}G}=2.46$ ms, 报告聚合阶段的计算时间是$(n+3)T_{e\text{-}G}=(1.42n+4.26)$ ms, 报告阅读阶段的计算时间是$3T_{e\text{-}G}+T_{BP}+T_{\log}=15.21$ ms. 总的计算开销是$(3.88n+19.47)$ ms.

对于本方案来说, 报告产生阶段的计算时间是$T_{m\text{-}E}+T_{e\text{-}N}=0.6$ ms, 报告聚合阶段的计算时间是$(n+2)T_{m\text{-}E}=(0.38n+0.76)$ ms, 报告阅读阶段的时间是$2T_{m\text{-}E}+T_{e\text{-}N}=0.98$ ms. 总的开销是$(0.98n+1.74)$ ms.

图 3 展示了总体计算代价与智能电表数量之间的关系比较图, 从图中可以看出: 相比于文献 [14–16], 所提方案的总体计算代价的增长是最缓慢的. 这很适合于计算资源有限的智能电表和网关.

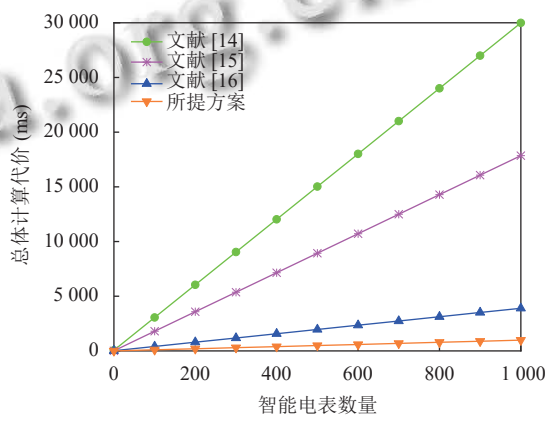

图 3 总体计算代价比较

3.4 通信代价比较

为了更清晰地比较通信代价, 本文做了如下设定: $|\mathbb{G}|=160$ bits; $|\mathbb{G}_1|=512$ bits; $|\mathbb{G}_T|=1024$ bits; $|\mathbb{Z}_q^*|=160$ bits; $|\mathbb{Z}_n|=1024$ bits; $|\mathbb{Z}_{n^2}|=2048$ bits; $|N|=768$ bits; 身份和时间戳的长度均为32 bits. 表 3 比较了文献 [14–16] 与所提方案的通信代价.

表 3 通信代价比较 (bits)

方案	*SM*到*GW*的通信代价	*GW*到*CC*的通信代价
文献[14]	3264	3264
文献[15]	3648	3104
文献[16]	2272	2784
本文方案	1152	1152

图 4 形象地展示了通信代价比较图. 从图中可以看出: 相比于文献 [14–16], 所提方案的 *SM* 到 *GW* 之间的和 *GW* 到 *CC* 之间的通信代价是最低的, 十分契合通信资源有限的 *SM* 和 *GW*.

4 结论

为了克服现有数据聚合方案的问题, 本文提出了

一个智能电网中高效的支持错误容忍的数据聚合方案, 其利用改进的对称同态加密技术实现高效性, 同时利用椭圆曲线密码学技术满足了报告的完整性和可认证性. 另外该方案可以抵抗合谋攻击和重放攻击, 保护了用户的隐私信息. 当有智能电表发生故障无法发送报告时, 权威中心会帮忙产生聚合的虚拟密文以确保控制中心正常解密聚合数据. 最后, 本文满足所提的安全需求, 并且轻量级的计算代价和通信代价适用于资源有限的智能电表.

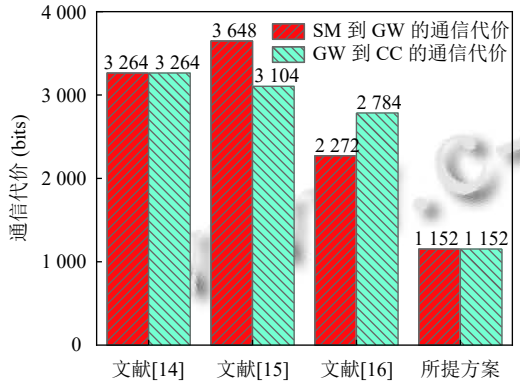

图 4 通信代价比较

参考文献

1 刘文, 杨慧霞, 祝斌. 智能电网技术标准体系研究综述. 电力系统保护与控制, 2012, 40(10): 120–126. [doi: 10.3969/j.issn.1674-3415.2012.10.022]

2 Li FX, Qiao W, Sun HB, *et al*. Smart transmission grid: Vision and framework. IEEE Transactions on Smart Grid, 2010, 1(2): 168–177. [doi: 10.1109/TSG.2010.2053726]

3 Rahimi F, Ipakchi A. Demand response as a market resource under the smart grid paradigm. IEEE Transactions on Smart Grid, 2010, 1(1): 82–88. [doi: 10.1109/TSG.2010.2045906]

4 Deng RL, Yang ZY, Chow MY, *et al*. A survey on demand response in smart grids: Mathematical models and approaches. IEEE Transactions on Industrial Informatics, 2015, 11(3): 570–582. [doi: 10.1109/TII.2015.2414719]

5 张瑶, 王傲寒, 张宏. 中国智能电网发展综述. 电力系统保护与控制, 2021, 49(5): 180–187.

6 Yan Y, Qian Y, Sharif H, *et al*. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE Communications Surveys & Tutorials, 2013, 15(1): 5–20.

7 Anzalchi A, Sarwat A. A survey on security assessment of metering infrastructure in smart grid systems. Proceedings of Southeast Con 2015. Fort Lauderdale: IEEE, 2015. 1–4.

8 陈思光, 杨熠, 黄黎明, 等. 基于雾计算的智能电网安全与隐私保护数据聚合研究. 南京邮电大学学报 (自然科学版), 2019, 39(6): 62–72.

9 Miller VS. Use of elliptic curves in cryptography. In: Williams HC, ed. Advances in Cryptology —CRYPTO '85 Proceedings. Berlin, Heidelberg: Springer, 1985. 417–426.

10 Li LC, Lu RX, Choo KKR, *et al*. Privacy-preserving-outsourced association rule mining on vertically partitioned databases. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1847–1861. [doi: 10.1109/TIFS.2016.2561241]

11 Wang BC, Zhan Y, Zhang ZL. Cryptanalysis of a symmetric fully homomorphic encryption scheme. IEEE Transactions on Information Forensics and Security, 2018, 13(6): 1460–1467. [doi: 10.1109/TIFS.2018.2790916]

12 Liu JK, Yuen TH, Au MH, *et al*. Improvements on an authentication scheme for vehicular sensor networks. Expert Systems with Applications, 2014, 41(5): 2559–2564. [doi: 10.1016/j.eswa.2013.10.003]

13 Schnorr CP. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4(3): 161–174. [doi: 10.1007/BF00196725]

14 Shen H, Liu YJ, Xia Z, *et al*. An efficient aggregation scheme resisting on malicious data mining attacks for smart grid. Information Sciences, 2020, 526: 289–300. [doi: 10.1016/j.ins.2020.03.107]

15 Guan ZT, Zhang Y, Zhu LH, *et al*. EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. Science China Information Sciences, 2019, 62(3): 32103. [doi: 10.1007/s11432-018-9451-y]

16 Ding Y, Wang BY, Wang YJ, *et al*. Secure metering data aggregation with batch verification in industrial smart grid. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6607–6616. [doi: 10.1109/TII.2020.2965578]

17 Shamus Software. Multi precision integer and rational arithmetic cryptographic library (MIRACL). http://www.certivox.com/miracl/. [2021-01-10].