·安全技术· 文章编号：1000-3428(2018)12-0190-06 文献标志码：A 中图分类号：TP309

基于 WSN 的全同态数据加密聚合方案

王彩芬，成玉丹，刘 超

（西北师范大学 计算机科学与工程学院，兰州 730070）

摘 要： 传统无线传感器网络数据加密聚合方案在密文数据运算、抵御内/外部攻击、追查并修复错误等方面存在安全性和效率方面的不足。为此，提出一种全同态数据加密聚合方案。采用 DGHV 全同态算法对隐私数据进行加密，并将节点的身份信息嵌入到数字签名中，使方案具有追查并修复错误的能力。此外，该方案无需可信第三方，以簇为单位分配干扰因子，以抵御内部攻击并提高运行效率。实验结果表明，该方案是 IND-CPA 安全的，能抵御内/外部攻击且满足全同态性。

关键词： 无线传感器网络；全同态加密；簇；数据聚合；可信第三方

中文引用格式： 王彩芬，成玉丹，刘 超. 基于 WSN 的全同态数据加密聚合方案[J]. 计算机工程，2018，44(12)：190-195.

英文引用格式： WANG Caifen，CHENG Yudan，LIU Chao. Fully homomorphic data encryption aggregation scheme based on WSN[J]. Computer Engineering，2018，44(12)：190-195.

Fully Homomorphic Data Encryption Aggregation Scheme Based on WSN

WANG Caifen，CHENG Yudan，LIU Chao

（College of Computer Science and Engineering，Northwest Normal University，Lanzhou 730070，China）

【Abstract】 Traditional data encryption aggregation schemes in Wireless Sensor Network（WSN） have some shortcomings in security and efficiency，such as ciphertext data operation，resist internal/external attacks，tracking and repairing errors. To solve this problem，a fully homomorphic data encryption aggregation scheme is proposed. DGHV homomorphism algorithm is used to encrypt the privacy data，and the identity information of the node is embedded in the digital signature，so that the scheme has the ability to trace and repair errors. In addition，the scheme does not require a trusted third party，it allocates interference factors in clusters to defend against internal attacks and improve operational efficiency. Experimental results show that the scheme is IND-CPA secure，and it can resist internal/external attacks and satisfy the full homomorphism.

【Key words】 Wireless Sensor Network（WSN）；fully homomorphic encryption；cluster；data aggregation；trusted third party

DOI： 10.19678/j.issn.1000-3428.0049009

0 概述

无线传感器网络（Wireless Sensor Network，WSN）的基本结构有树形和簇形，均由若干个传感器节点和一个基站（Base Station，BS）组成，通信方式是无线链路通信，并且能够实时监测、感知和收集网络覆盖范围内的各种环境信息[1]。传感器能量受限，存储和计算能力较小，但基站有固定的能量来源，是整个网络的核心，存储空间大，计算能力强。

目前，国内外学者针对 WSN 中数据的安全传输问题进行了一定研究。早期采用基于对称加密机制的点到点数据聚合算法[2]，该算法的优点是容易实现且方便快捷，但其会造成密钥和明文的泄露。为得到较好的安全性能，文献[3]提出 2-DNF 非对称密码系统，通过同态的加乘运算实现数据的聚合，但其在数据验证和防止抵赖等方面仍存在局限性。此后，又出现了多个针对该方案的改进方法。文献[4]提出能够抵御内部攻击的数据聚合方案。文献[5]提出在 WSN 中基于同态原语的数据聚合方案。文献[6]在数据的机密性和完整性上进行改进，提出基于同态加密的 WSN 数据融合的机密性和完整性方案。文献[7]提出基于同态加密的可验证隐私数据聚合方案。文献[5-7]对 2-DNF 非对称密码系统的计算效率和安全性能均做了改进，但仍有不足之处：文献[5]需要一个额外的可信第三方来分发保密干扰因子，而且方案的构造方式复杂；文献[6]在抵御内部攻击上存在局限性；文献[7]通过聚合器本身对每一个传感器节点分配干扰因子，计算复杂度高，并

基金项目： 国家自然科学基金(61562077，61662069，61662071)。

作者简介： 王彩芬(1963—)，女，教授，主研方向为密码协议、网络编码；成玉丹、刘 超，硕士研究生。

收稿日期： 2017-10-19 **修回日期：** 2017-12-14 **E-mail：** 2289887757@qq.com

且其采用 ElGamal 方案加密隐私数据,仅满足了乘法同态性,并不满足全同态性。

针对上述方法的不足,本文在文献[7]的基础上,基于簇的网络结构提出 WSN 中全同态的数据加密聚合方案。采用具有全同态性的 DGHV[8] 方案加密隐私数据,同时将包含节点身份信息的签名嵌入到密文中,通过签名验证其正确性,使方案具有抵抗数据被篡改、追查并纠正错误数据的能力。本文方案以簇为单位,通过聚合器为簇内的传感器节点分发保密干扰因子,以避免由第三方带来的安全问题。

1　预备知识

1.1　符号和参数定义

若 G 是一个循环群,则 $H:\{0,1\}^{*}\rightarrow G$ 表示一个哈希函数。用 $\mathbb{Z}_q^{*}$ 表示整数模 q 剩余类环 $\mathbb{Z}_q$ 中所有对模乘可逆的元素组成的集合,其中,$\mathbb{Z}_q^{*}=\mathbb{Z}_q\backslash\{0\}$,且 q 是素数。$(a\parallel b)$ 表示将 2 个对象 a、b 按顺序连成一个整体。$x\xleftarrow{R}B$ 表示从集合 B 中随机取值并将该值赋予变量 x。

给定安全参数 λ,参数的设置为:ρ 表示噪音长度,η 表示私钥长度,γ 表示公钥长度,τ 表示公钥中整数的个数。为满足该方案的安全性,上述参数需满足如下条件:

1)$\rho=\omega(\mathrm{lb}\ \lambda)$,使方案能够抵抗噪音的蛮力攻击。

2)$\eta\geqslant\rho\Theta(\lambda\ \mathrm{lb}^2\lambda)$,使方案能够支持足够深的电路同态评估。

3)$\gamma=\omega(\eta^2\mathrm{lb}\ \lambda)$,使方案能阻止各种基于格的攻击,比如近似的最大公因子(Greatest Common Divisor, GCD)问题。

4)$\tau\geqslant\gamma+(\omega\ \mathrm{lb}\ \lambda)$,使方案能够在 GCD 中使用剩余的哈希引理。

1.2　双线性映射

定义 1(双线性映射)[9]　设 G_1、G_2 是阶为素数 q 的乘法循环群,$a,b\in\mathbb{Z}_q^{*}$,一个双线性映射 $e:G_1\times G_1\rightarrow G_2$ 具有如下性质:

1)双线性:对任意的 $u,v\in G_1$,满足 $e(u^a,v^b)=e(u,v)^{ab}$。

2)非退化性:$e(u,v)\neq 1_{G_2}$,其中,1_{G_2} 为 G_2 中的单位元。

3)可计算性:对任意 $u,v\in G_1$,存在有效算法能够计算 $e(u,v)$。

1.3　困难问题假设

定义 2(计算性 Co-Diffie-Hellman 问题)　设 q 是一个大素数,G 是阶为 q 的循环群,g 是 G 的生成元,已知 $(g,g^a,g^b)\in G^3$,其中,$a,b\in\mathbb{Z}_q^{*}$,求 $g^{ab}\in G$ 即为计算性 Co-Diffie-Hellman 问题。

定义 3(GCD 问题)[8]　参数为 ρ、η、γ、p 为一个随机的 η bit 的素数,$x_0=pq_0$,$q_0\in Z\cap[0,2^{\gamma}/p)$。

$$D_{\gamma,\rho}(p)=\left\{\begin{matrix}q\leftarrow[0,q_0),r\leftarrow Z\cap(-2^{\rho},2^{\rho}):\\x=pq+r\end{matrix}\right\}$$

求 p 的过程就是 GCD 问题。

1.4　全同态加密

定义 4(全同态加密)[10]　同态加密指在不解密密文的情况下,通过对密文执行操作来实现对明文的加密,且其结果一致,这里的全同态是指同时满足加法同态和乘法同态。全同态加密方案中包含 4 个函数:$KeyGen(\lambda)$,$Encrypt(pk,m)$,$Decrypt(sk,\boldsymbol{c})$ 和 $Evaluate(pk,C,\boldsymbol{c})$。其具体操作如下:

1)$KeyGen(\lambda)$:根据安全参数 λ 产生公私钥对 (pk,sk)。

2)$Encrypt(pk,m)$:在公钥 pk 下把明文 m 加密成密文 $\boldsymbol{c}$。

3)$Decrypt(sk,\boldsymbol{c})$:用私钥 sk 解密密文 $\boldsymbol{c}$,得到明文 m。

4)$Evaluate(pk,C,\boldsymbol{c})$:输入一个公钥 pk、电路 C 和一个密文元组 $\boldsymbol{c}=\langle c_1,c_2,\cdots,c_t\rangle$,输出另一个密文元组 $\boldsymbol{c}$。

1.5　DGHV 方案

文献[8]在 Gentry 方案的基础上提出基于整数的全同态加密方案 DGHV。其中各函数具体操作如下:

1)$KeyGen(\lambda)$:选取一个 η 位的奇整数 $p\xleftarrow{\$}[2^{\eta_i-1},2^{\eta_i})\cap(2Z+1)$ 作为私钥 sk,选择 $q_i\xleftarrow{\$}Z\cap[0,2^{\gamma}/p)$,$r_i\xleftarrow{\$}Z\cap(-2^{\rho},2^{\rho})$,其中,$q_0$ 最大且为奇数,令 $x_0=pq_0+r_0$,$x_i=[pq_i+r_i]_{x_0}$,$0\leqslant i\leqslant\tau$。公钥 $pk=\langle x_0,x_1,\cdots,x_{\tau}\rangle$。

2)$Encrypt(pk,m)$:随机选取一个集合 $S\subseteq\{1,2,\cdots,\tau\}$ 和一个随机整数 $r\leftarrow(-2^{\rho},2^{\rho})$,明文 $m\in\{0,1\}$,输出密文 $c\leftarrow\left[m+2r+\sum_{i\in S}x_i\right]_{x_0}$。

3)$Decrypt(sk,\boldsymbol{c})$:输出明文 $m\leftarrow[[\boldsymbol{c}]_p]_2$。在解密过程中,首先通过密文模私钥 p,再模 2 即可得到 1 bit 的明文。

4)$Evaluate(pk,C,c_1,c_2,\cdots,c_t)$:输入公钥 pk、电路 C 和 t 个密文 $c_1,c_2,\cdots,c_t$,其中,$c_i=Encrypt(pk,m_i)$,$i=1,2,\cdots,t$。输出 $c^{*}=Evaluate(pk,C,c_1,c_2,\cdots,c_t)$ 且满足 $Decrypt(sk,c^{*})=C(m_1,m_2,\cdots,m_t)$。该算法集中体现了全同态加密的技术优势,其通过门电路或者函数对密文进行任意操作后再解密,结果和操作明文的结果一致。

2　WSN 中全同态数据加密方案

WSN 的构建方式有多种,同时也产生了很多标准协议,如文献[11]提出的标准聚合协议和文献[12]中的网络构建方式。假定本文方案中的聚合器拥有足够的计算能力且是诚实但好奇的,即其可

能会自主地做出一些错误的举动,但不会与其他实体实施共谋攻击[13]。同时,它能够有效地完成方案中涉及的签名验证和解密操作。

目前提出的基于 WSN 的同态加密聚合方案仅仅实现了加法同态或乘法同态,文献[7]以簇为单位分发干扰因子,但是每一个传感器拥有独立的干扰因子在很大程度上增加了方案的计算复杂度。由干扰因子的作用可知,它不涉及隐私信息,所以对它的改进主要是提高运算效率,降低计算复杂度。因此,本文在文献[7]的基础上,以簇为网络结构,提出基于 WSN 的全同态数据加密聚合算法,实现隐私数据的加法和乘法同态。在干扰因子的分发过程中,每一个簇内的传感器节点拥有相同的干扰因子,这样既保证了方案能够抵抗内部攻击,又在很大程度上降低了计算复杂度。

2.1 网络模型

本文采用的网络模型是基于簇的网络结构[14],如图 1 所示。该结构的优点是将簇内节点的信息收集起来,统一向上一级节点传送,能够节省通信开销,增强扩展性。网络模型结构包含 3 类角色:基站 BS,聚合器 Agg 和传感器节点。整个网络由多个非重叠的簇组成,每个簇中包含一个聚合器(簇头)和 n 个传感器节点。簇头的功能是给簇内的每一个传感器节点分发干扰因子 π 和身份标识 ID,π 只分发一次,即每一个传感器节点具有相同的干扰因子,同时从传感器节点接收加密的数据,将其聚合验证后传给 BS;每一个传感器节点将接收到的数据采用带有干扰因子的 DGHV 方案加密,用自己的身份标识签名,然后将密文发送给聚合器。

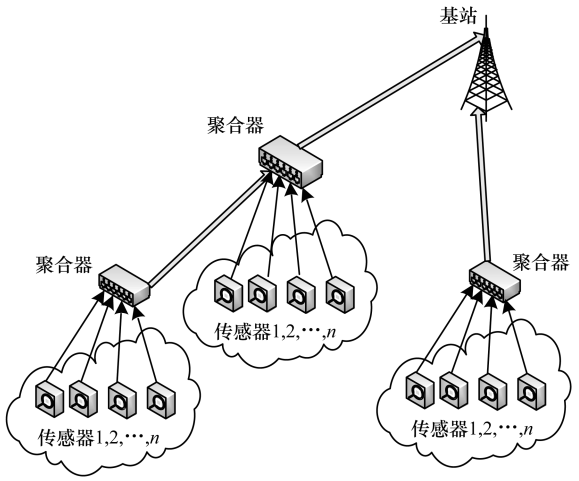

图 1 基于簇的网络拓扑

2.2 方案设计

在基于簇的 WSN 构建完成后,加密聚合方案主要包括 3 个基本过程:系统建立阶段,加密签名阶段和验证聚合阶段。在系统建立阶段,聚合器作为整个簇的核心,为每一个传感器节点分配身份标识 ID、公私钥和干扰因子 π;在加密签名阶段,传感器节点收集信息,利用公私钥和 π 对消息加密,用 ID 对消息签名;在验证聚合阶段,聚合器发出消息聚合的命令,每一个传感器节点将加密的消息发送给聚合器,聚合器完成数据的聚合并进行验证,若验证成功,则进行相应操作得到消息,若验证失败,则检测每一个节点的数据,并要求数据传输错误的节点重新传输数据。

2.2.1 系统建立阶段

设在每一个簇内由一个聚合器控制着 n 个传感器节点 $U_i(i=0,1,\cdots,n-1)$。聚合器作为密钥生成中心,通过 DGHV[8] 方案和 DF[15] 方案为簇内的每一个节点分配公私钥和干扰因子。该阶段的 2 个基本操作如下:

1)密钥生成阶段:

(1)聚合器对控制的每一个传感器节点分配身份标识 $ID_i(i=0,1,\cdots,n-1)$。

(2)设置安全参数 λ。

(3)随机选取 η 位的大素数 p 和整数 $q_i,r_i,q_i \xleftarrow{\$} Z\cap[0,2^{\gamma}/p)$,$r_i \xleftarrow{\$} Z\cap(-2^{\rho},2^{\rho})$,其中,$0\leqslant i\leqslant n-1$ 且 q_i 是远大于 p 的整数,r_i 是一个较小的整数且 $2r_i<p/2$,计算 $x_i=pq_i+2r_i$ 得到 $pk=\langle x_0,x_1,\cdots,x_{n-1}\rangle$,其中假设 x_0 为最大值且 $N=x_0$。

(4)生成 N 阶乘法循环群 G。

(5)在 G 中取生成元 g。

(6)发布公钥 $PK=\{pk,g\}$,私钥 $SK=p$。

2)分配保密干扰因子 $\pi_k(k=0,1,\cdots,n-1$,表示聚合器的个数)。

保密干扰因子的生成和分发过程是保密的,由于它不涉及核心消息 m_i,因此对它的保密要求比较低,而对其效率的要求较高。本文采用与 DF[15] 方案相同的分配方式,若聚合器为每一个传感器都分配保密干扰因子,会增加计算复杂度。为降低计算复杂度,本文采用基于簇的传感器网络。假设以 n 个传感器节点为一个簇,每一个簇分配一个保密干扰因子,即 n 个节点具有相同的干扰因子。聚合器(簇头)的具体分配过程如下:

1)随机选择一个整数 $r\in\mathbb{Z}_N$ 和 r 模 N 的逆 $r^{-1}\in\mathbb{Z}_N$。

2)选择一个随机整数 $\pi_k\in\mathbb{Z}_N$。

3)计算 $\pi_k^*=\pi_k\cdot r^k \bmod N$。

4)为计算方便,令 $\pi_0=-\pi_k^* r^{-k}$。

2.2.2 加密签名阶段

当传感器节点 $U_i(i=0,1,\cdots,n-1)$ 收到聚合器发布的数据聚合的命令时,进行数据加密签名的操作,在此过程中,传感器节点可以对多次加密的数据

实现全同态操作,再用身份标识 ID_i 签名,然后上传给聚合器。具体过程如下:

1)读取需加密的数据 $m_i \in \{0,1\}$,任取一个私钥 $p \in \mathbb{Z}_p$,生成相应的公钥 $pk = \langle x_0, x_1, \cdots, x_{n-1} \rangle$。

2)任取一个集合 $S \subseteq \{1,2,\cdots,\tau\}$,随机整数 $r \xleftarrow{\$} (-2^\rho, 2^\rho)$,计算密文 $c_1 = g^{\pi_k}[m_1 + 2r + \sum_{i \in S} x_i]_{x_0}$。

3)重复上述 2 个步骤,得到 $c_2 = g^{\pi_k}[m_2 + 2r + \sum_{i \in S} x_i]_{x_0}$,对 c_1、c_2 进行全同态运算,得到密文 $c_i = c_1 \oplus c_2$($\oplus$表示某种同态运算)。

4)计算签名 $\sigma_i = H(c_i \parallel ID_i)^p$ 及 $y_i = g^p$。

5)将 $\{c_i, y_i, \sigma_i\}$ $(i = 0,1,\cdots,n-1)$ 发送至聚合器。

2.2.3　验证聚合阶段

在验证聚合阶段,聚合器首先对上传的数据进行聚合,然后利用双线性映射验证其正确性,若验证正确,则可以计算得到聚合的消息,具体操作如下:

1)聚合器接收所有传感器节点 U_i 传来的数据 $\{c_i, y_i, \sigma_i\}$ $(i = 0,1,\cdots,n-1)$。

2)任取 $\delta_i \xleftarrow{R} \mathbb{Z}_p$,选取一个非退化可计算的双线性映射 $e: G \times G \to G$,验证聚合等式 $e(\prod_{i=1}^{n} \sigma_i^{\delta_i}, g) = \prod_{i=1}^{n} e(H(c_i \parallel ID_i)^{\delta_i}, y_i)$ 是否成立。若成立,则此次聚合的数据全部通过;若不成立,则需对每一个传感器节点的数据进行检测,对数据传输错误的节点,要求其重新传输数据给聚合器。

3)若以上验证通过,则计算 $V = g^{\pi_0} \cdot \prod_{i=1}^{n} c_i = g^{\pi_0} \cdot \prod_{i=1}^{n} g^{\pi_k}[m_i + 2r + \sum_{i \in S} x_i]_{x_0}$。

4)计算 $V \bmod 2 = \{\prod_{i=1}^{n}[m_i + 2r + \sum_{i \in S} x_i]_{x_0}\} \bmod 2 = \prod_{i=1}^{n} m_i + \sum_{i \in S} pq_i$,记作 V'。

5)计算 $V' \bmod p$,得到最终的聚合结果 $\prod_{i=1}^{n} m_i$。

2.3　方案的正确性分析

本文方案的正确性分析具体如下:

1)签名验证的正确性:

$$\prod_{i=1}^{n} e(H(c_i \parallel ID_i)^{\delta_i}, y_i) = \prod_{i=1}^{n} e(H(c_i \parallel ID_i)^{\delta_i}, g^p) = \prod_{i=1}^{n} e(H(c_i \parallel ID_i)^{p\delta_i}, g) = \prod_{i=1}^{n} e(\sigma_i^{\delta_i}, g) = e(\prod_{i=1}^{n} \sigma_i^{\delta_i}, g)。$$

2)聚合解密的正确性:

将 $c_i = g^{\pi_k}[m_i + 2r + \sum_{i \in S} x_i]$ 代入 $V = g^{\pi_0} \cdot \prod_{i=1}^{n} c_i$ 可得 $V = g^{\pi_0} \cdot \prod_{i=1}^{n} g^{\pi_k}[m_i + 2r + \sum_{i \in S} x_i]$,化简得 $V = \prod_{i=1}^{n}[m_i + 2r + \sum_{i \in S} x_i]$,因为 $x_i = pq_i + 2r_i$,将其代入上式可得 $V = \prod_{i=1}^{n} m_i + 2(\sum_{i \in S} r_i + r) + \sum_{i \in S} pq_i$,将 $V \bmod 2$ 可得 $V' = \prod_{i=1}^{n} m_i + \sum_{i \in S} pq_i$,注意到 p 是私钥,对 $V' \bmod p$ 可得 $V'' = \prod_{i=1}^{n} m_i$。通过以上过程可得聚合结果,即 $V'' = \prod_{i=1}^{n} m_i$。

3　方案性能分析

3.1　全同态性分析

由于本文方案的加密算法运用了基于整数的全同态加密方案 DGHV,因此其全同态性的详细证明过程可参考文献[8]。

3.2　保密干扰因子的安全性分析

在本文方案中,保密干扰因子 π_k $(k = 0,1,\cdots,n-1$表示聚合器的个数)是以簇为单位分配的,作用是在保证安全的基础上提高方案的效率,其分配方式根据 DF[15] 方案构造,故本文方案中保密干扰因子安全性的详细证明过程可参考文献[15]。

3.3　基于 AGCD 问题的安全性证明

本文方案的安全性基于近似公因子(AGCD)难题和计算版本的 Co-Diffie-Hellman 问题。Co-Diffie-Hellman问题作为一些密码系统困难问题的基础,已经得到了证明和广泛应用。本文对基于 AGCD 问题的安全性进行证明,主要证明思路是使用攻击算法 A 来构造求解困难问题的算法 B,该过程包括4 个步骤:1)利用困难问题产生方案的公钥;2)利用 A 构造求解 p 的商的最小比特位;3)执行 Binary-GCD 算法;4)恢复 p。

定理 1　在第 2.1 节的方案中,固定参数$(\rho, \eta, \gamma, \tau)$与安全系数 λ。任意的攻击者 A 以优势 ε 攻击加密方案,都可以转化成求解器 B 以至少 $\varepsilon/2$ 优势求解参数为(ρ, η, γ)的近似 AGCD 问题。B 的运行时间是 t_A、λ 和 $1/\varepsilon$ 的多项式,其中,t_A 是 A 的运行时间。

证明　攻击者 A 以 ε 的优势攻击本文方案,即 A 以 ε 的优势输入公钥和密文(由本文方案的算法获得公钥和密文),正确输出明文的概率至少是 $1/2 + \varepsilon$。

在参数为 ρ、η、γ 时,构造求解近似 AGCD 困难问题的求解器 B,对于随机选取的 η bit 的奇整数 p,求解器 B 需要从 $D_{r,\rho}(p)$ 分布中获得多个样本来求解目标 p。步骤如下:

步骤 1　创建公钥。首先,求解器 B 为方案创建一个公钥 $pk = \langle x_0, x_1, \cdots, x_\tau \rangle$。

步骤 2　利用最低有效位(Least Significant Bit, LSB)子程序求解 p 的近似倍数的最小比特位。B 调用以下子程序:

子程序 *Learn-LSB*(z,pk)

输入 $z\in[0,2^{\gamma})$,$|r_p(z)|<2^{\rho}$,公钥 $pk=\langle x_0,x_1,\cdots,x_\tau\rangle$

输出 $q_p(z)$的最低有效位

1. For i=1 to poly(λ)/ε do://ε 是 A 的整体优势;

2. 随机选择比特 $t_i\xleftarrow{\$}(-2^{\rho'},2^{\rho'})$,$m_i\xleftarrow{\$}\{0,1\}$,$S_i\subseteq\{0,1,\cdots,\tau\}$;

3. 计算 $c_i\leftarrow[z+m_i+2t_i+\sum_{i\in S}x_i]_{x_0}$;

4. 调用 A 访问随机预言机得到 $a_i\leftarrow A(pk,c_i)$;

5. 设置 $b_i\leftarrow a_i\oplus\text{parity}(z)\oplus m_i$;

6. 输出主要向量 $b_i's$.

步骤 3 运用 Binary-GCD 算法[8]计算 p。给定任意的 2 个整数 $z_1=q_p(z_1)\cdot p+r_p(z_1)$ 和 $z_2=q_p(z_2)\cdot p+r_p(z_2)(r_p(z_i)<<p)$。

步骤 4 恢复 p。求解器 B 执行 Binary-GCD 算法,其中,$GCD(q_p(z_1^*),q_p(z_2^*))$互质的概率至少是 $\pi^2/6\approx0.6$。输出元素 $\tilde{z}=1+p\times0.1+r$,其中,$|r|<2^{\rho}$。一旦得到 $\tilde{z}$,则可以通过 $GCD(z_1^*,z_2^*)$找到 $q_p(z_1)$,然后 B 恢复 $p=[z_1^*/q_p(z_1^*)]$。

综上,若随机预言机能计算出$[q_p(z)]_2$(z 的噪声远小于 p),则 B 就可以恢复 p。接下来分析在随机预言机模型下 B 成功的概率。

由步骤 1 可得,求解器 B 产生公钥的分布与本文方案产生的正确分布相同,如文献[8]所述:如果 A 猜测成功的可能性为 ε,则敌方猜测成功的可能性至少为 $\varepsilon/2$。如果固定 p,在对应的公钥 pk 下 A 猜测成功的可能性至少是 $\varepsilon/4$,敌方猜测成功的可能性至少为 $\varepsilon/4$。在子程序 *Learn-LSB*(z,pk)的步骤 4 中,A 猜测成功的可能性至少是 $\varepsilon/4-negl$,对于该子程序而言,返回正确值的可能性很大,B 有很大概率恢复出 p。对于这样的 p,公钥 pk 下的概率 $\varepsilon/4-negl$ 也成立,则求解器 B 在运行中恢复 p 的概率至少是 $1/2(\varepsilon/4-negl)$,B 重复调用算法$(8/\varepsilon)\omega(\text{lb}\,\lambda)$次,此时 B 的时间复杂度是 $poly(\lambda,1/\varepsilon)$,因此,求解器 B 成功恢复 p 的概率至少是$\varepsilon/2$。至此,定理 1 证明完毕,本文方案是 IND-CPA 安全的。

3.4 网络内部攻击分析

网络内部的攻击者可以在数据聚合前后的 2 个阶段获得数据。从这 2 个方面进行如下分析:

1)在聚合前,内部攻击者要获得明文消息 m_i,在得到传感器的加密私钥 p 的同时,也要得到干扰因子 π_k。由于本文方案以簇为单位分配干扰因子,因此簇内每一个节点的干扰因子都相同。为获知内部攻击者是否会进行重复性攻击,作如下证明:在一个簇内随机选取一个节点的 2 个消息 m_1、m_2,加密之后的密文为 c_1、c_2。

$$c_1=g^{\pi_k}[m_1+2r+\sum_{i\in S}x_i] \tag{1}$$

$$c_2=g^{\pi_k}[m_2+2r+\sum_{i\in S}x_i] \tag{2}$$

式(1)、式(2)相减并化简可得:

$$g^{\pi_k}=\frac{c_1-c_2}{m_1-m_2} \tag{3}$$

对于式(3),分 2 种情况讨论:

(1)m_1-m_2 的值未知,则不能得到干扰因子 π_k。

(2)假设 m_1-m_2 的值已知,在 N 阶乘法循环群内求解 π_k 属于离散对数困难问题,故也不能得到干扰因子 π_k。因此,π_k 的获取是困难的。

2)在聚合后,若内部攻击者想从聚合结果 $V=g^{\pi_0}\cdot\prod_{i=1}^{n}c_i$ 中获取明文 m_i,则需要解决 GCD 问题和计算性 Co-Diffie-Hellman 问题,这显然更困难。

由以上分析可得,本文方案可有效抵御来自网络内部的攻击。

4 不同方案性能对比

表 1 所示为文献[4,7,14]中的经典方案和本文方案的主要性能对比。其中,同态性指方案是否能实现全同态性。

表 1 4 种方案性能比较

方案	抵御外部攻击	抵御内部攻击	可信第三方	数据验证	形式化证明	加密时间复杂度	同态性
文献[4]方案	能	能	需要	有	有	$O(1)$	无同态
文献[7]方案	能	能	不需要	有	有	$O(n)$	半同态
文献[14]方案	能	不能	不需要	有	无	$O(n)$	半同态
本文方案	能	能	不需要	有	有	$O(1)$	全同态

由表 1 可以看出,与文献[4]方案相比,本文方案无需可信第三方并且满足全同态性;与文献[7]方案相比,本文方案时间复杂度更低且能够进行全同态运算;与文献[14]方案相比,本文方案能够抵御内部网络攻击。因此,与已有方案相比,本文方案在无需可信第三方的情况下,时间复杂度较低且满足全同态性。

5 结束语

为改善 WSN 中的数据聚合效果,本文提出一种基于全同态加密的数据聚合方案,该方案具有如下优点:1)采用全同态加密方案,聚合器无需对密文解密就可以进行全同态运算;2)聚合器没有解密密钥,每个簇内的传感器都有保密因子,并且不需要可信第三方来分配,因此,该方案既可以抵御内部攻击也能节约存储空间;3)以簇为单位分配保密干扰因子,将计算复杂度降低到 $O(1)$。实验结果验证了该方案的性能优越性。下一步考虑改进公钥产生算法并缩短公钥的长度,以减少本文算法的运行时间,提高运算效率。

参考文献

[1] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine,2002,40(8):102-114.

[2] DOMINGO-FERRER J. A provably secure additive and multiplicative privacy homomorphism[C]//Proceedings of the 5th International Conference on Information Security. Berlin, Germany: Springer,2002:471-483.

[3] DAN B, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]//Proceedings of International Conference on Theory of Cryptography. Berlin, Germany: Springer,2005:325-341.

[4] FAN C I, HUANG S Y, LAI Y L. Privacy-enhanced data aggregation scheme against internal attackers in smart grid[J]. IEEE Transactions on Industrial Informatics,2013,10(1):666-675.

[5] ZHOU Q, YANG G, HE L. An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks[J]. International Journal of Distributed Sensor Networks,2014(7):11-15.

[6] OTHMAN S B, BAHATTAB A A, TRAD A, et al. Confidentiality and integrity for data aggregation in WSN using homomorphic encryption[J]. Wireless Personal Communications,2015,80(2):867-889.

[7] 王会勇,冯　勇.基于同态加密的可验证隐私数据聚合方案[J].四川大学学报(工程科学版),2016,48(4):144-149.

[8] DIJK M, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[C]//Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer,2010:24-43.

[9] 马米米,何德彪,陈建华,等.大数据环境下支持多关键字的可搜索公钥加密方案[J].南京信息工程大学学报,2017,9(5):462-471.

[10] GENTRY C. Fully homomorphic encryption using ideal lattices[EB/OL].[2017-10-05]. http://web.cse.ohio-state.edu/~lai.1/5359-aut13/02.Gentry-FHE-bootstrapping.pdf.

[11] MADDEN S, FRANKLIN M J, HELLERSTEIN J M, et al. TAG: a tiny aggregation service for ad-hoc sensor networks[J]. ACM SIGOPS Operating Systems Review,2002,36(S):131-146.

[12] 万本庭,全小凤.基于遗传算法的移动传感节点路径规划策略研究[J].计算机工程,2017,43(8):144-150.

[13] ODED G. Foundations of cryptography: volume 2, basic applications[M]. Cambridge, UK: Cambridge University Press,2004.

[14] 刘雪艳,李战明.无线传感器网中基于隐私同态的数据聚合方案[J].计算机工程,2014,40(8):101-105.

[15] 宁多彪,张　兵.基于连通支撑集的无线传感网数据聚合调度算法[J].计算机工程,2016,42(9):58-62,70.

编辑　吴云芳

(上接第 189 页)

[11] KOO T M, CHANG H C, CHUANG C C. Detecting and analyzing fast-flux service networks[J]. Advances in Information Sciences and Service Sciences, 2012, 4(10):183-190.

[12] KOO T M, CHANG H C, SU W H. Building a P2P Botnet based on a new key management scheme[J]. Advances in Information Sciences and Service Sciences, 2012,4(5):199-207.

[13] HOLE T, GORECKI C, RIECK K, et al. Measuring and detecting fast-flux service networks[C]//Proceedings of Network and Distributed System Security Symposium. San Diego, USA: [s.n.],2008:487-492.

[14] ALMOMANI A, GUPTA B B, ATAWNEH S, et al. A survey of phishing email filtering techniques[J]. IEEE Communications Surveys and Tutorials, 2013, 15(4): 2070-2090.

[15] KONTE M, FEAMSTER N, JUNG J. Dynamics of online scam hosting infrastructure[C]//Proceedings of International Conference on Passive and Active Network Measurement. Berlin, Germany: Springer,2009:219-228.

[16] HSU C H, HUANG C Y, CHEN K T. Fast-flux bot detection in real time[C]//Proceedings of International Conference on Recent Advances in Intrusion Detection. Berlin, Germany: Springer,2010:464-483.

[17] PERDISCI R, CORONA I, DAGON D, et al. Detecting malicious flux service networks through passive analysis of recursive DNS traces[C]//Proceedings of Computer Security Applications Conference. [S.1.]: IEEE Computer Society,2009:311-320.

[18] ALDUWAIRI B N, ALHAMMOURI A T. Fast flux watch: a mechanism for online detection of fast flux networks[J]. Journal of Advanced Research, 2014, 5(4):473-479.

[19] MARTINEZ-BEA S, CASTILLO-PEREZ S. Real-time malicious fast-flux detection using DNS and bot related features[C]//Proceedings of the 11th International Conference on Privacy, Security and Trust. Washington D. C., USA: IEEE Press,2013:369-372.

[20] CAGLIYAN A, TOOTHAKER M, DAN D, et al. Real-time detection of fast flux service networks[C]//Proceedings of Cybersecurity Applications and Technology Conference on Homeland Security. [S.1.]: IEEE Computer Society,2009:285-292.

编辑　索书志