无线网络信息公平可验证全同态安全加密方法

吴亚洁 [1]
WU Yajie

摘 要 无线网络信息验证过程中密文维数膨胀会影响算法对加密向量内积的准确计算，造成加密有界分布状态模糊，导致最终加密算法无法完全覆盖所有信息，完整性验证率不佳。为此，文章提出一种无线网络信息公平可验证全同态安全加密方法。考虑信息矩阵向量水平连接状态确定加密向量内积，在满足最大列向量的同时输入一个 BitDecomp 向量，生成固定加密矩阵，确定加密有界分布状态；考虑信息对接预设条件与加密覆盖节点关系构建的加密索引，按照概率多项关系随机均匀处理，生成多层级可验证全同态安全加密方案，覆盖全部信息完成加密。实验结果表明，所提方法应用后，在不同类型的无线网络信息下完整性验证率始终较高，未出现异常重叠问题，符合随机注入信息的加密密钥编解码要求，具有抗干扰鲁棒性。

关键词 无线网络；网络信息；信息公平；可验证；同态安全加密

doi：10.3969/j.issn.1672-9528.2026.01.027

0 引言

无线网络信息是通过 AP 接入点与 CAPWAP 等协议传输的数据信息，覆盖范围较广，组网模式包括 Infrastructure/Ad-hoc/Mesh 等多种模式。无线网络信息安全的影响因素较多 [1]，在技术层面，存在无线通信协议漏洞，加密技术或软硬件局限问题；在管理层面，存在网络配置错误、信道冲突、访问策略松散问题；在环境层面，存在物理攻击与信号干扰；在人为层面，包括内部人员恶意行为、第三方服务风险等，因此，进行无线网络信息公平可验证全同态安全加密是目前的必然选择。

为了确保信息安全，方晖提出考虑变拓扑结构的加密方法 [2]。该方法利用信道损耗模型规划最优动态传输路径并加密传感数据，保障了传输安全。但该方法依赖信道损耗模型规划路径加密数据，可能影响传输安全保障效果。黄磊等提出基于联邦学习和多方安全计算的加密方法 [3]。该方法采用结合同态加密技术的梯度提升决策树，作为模型训练的核心算法，三方对等协作训练出海铁联运潜在货源识别策略，运行中铁路可获路网潜在适运货源数量且各方数据隐私得以保护。但该方法易受决策树变化影响，导致完整性验证率较低。全斌提出基于 Docker 容器的加密方法 [4]。该方法主要收集网络负载数据量，进行 Docker 容器评估，联合目标防护信息确定传输调度状态，再定义混沌映射关系，结合离散变换生成安全性种子密钥，完成加密求解。但该方法易受静态污点影响，导致完整性验证率偏低。邓从香提出基于混沌序列的加密方法 [5]。该方法将风险转换为加密参考特征，利用三元联、五元联函数求解，确定风险变化特性，建立混沌序列密钥。但该方法易受加密顺序影响，导致完整性验证率过低。

为提升无线网络信息传输的安全性与可靠性，本文设计了一种有效的无线网络信息公平可验证全同态安全加密方法。

1 无线网络信息公平可验证全同态安全加密方法设计

1.1 生成无线网络信息公平可验证同态加密方案

加密向量内积作为信息加密过程中的关键参数，其准确性直接影响到后续的加密操作。而密文维数膨胀导致算法难以精准计算，进而使得加密有界分布状态变得模糊不清。因此，首先针对待加密的无线网络信息，利用自然数进行标记，生成有效的同态加密方案。

考虑信息矩阵向量的水平连接状态，可以确定加密向量内积，此时的范数 $\|x\|$ 为：

$$\|x\|=\sqrt{\sum_{i=1}^{n}x_i}\cdot l_{00} \tag{1}$$

式中：x_i 为功放谐波内积；l_{00} 为环境噪声，此时，可结合 SKK 算法开展浮点运算 [6-7]，在确保列向量达到最大化的同时，输入一个 BitDecomp 向量，进而生成一个固定加密矩阵。该矩阵的输入输出情景与逆函数相关，且具有特定的有界值 negl(λ) 为：

1. 贵阳职业技术学院信息科学系 贵州贵阳 550081

$$\mathrm{negl}(\lambda)=P_r\left[\|x\|\cdot B\right] \tag{2}$$

式中：P_r 为原向函数；B 为逆函数。

在满足式（2）所规定的加密有界分布条件的前提下，针对某一服从特定分布的随机变量，其对应的同态加密关系式为：

$$R_1=\begin{cases}m\times h-\xi_L-\xi_H-\xi_S-1, & \text{if } m=1\\ m\times h-\xi_L-\xi_H-1, & \text{if } m=0\end{cases} \tag{3}$$

式中：R_1 为无线网络信息验证空间；h 为加密信息的嵌入长度[8]；ξ_L 为密钥长度；ξ_H 为加密符号长度；ξ_S 为标记高斯参数；m 为条件判断变量。

针对有限域上分布的距离差异，生成均匀随机矩阵，并通过考量信息对接的预设条件与加密覆盖节点之间的关联，进而构建出相应的加密索引 D 为：

$$D=\left(e-\varphi\right)^2-e\times N \tag{4}$$

式中：e 为安全有界分布参数；φ 为传输均匀加密参数；N 为无线网络信息单元传输量。

对于加密索引 D 中的密文[9-10]，按照概率多项关系随机均匀处理，降低同态加密风险，此时的信息加密传输间距 R 为：

$$R=D\sum_{i=1}^{m}\sum_{j=1}^{h}\mathrm{isequal}\left(\xi_L(i,j),0\right) \tag{5}$$

式中：$\xi_L(i,j)$ 为加密节点嵌入信息。结合上述传输间距可以生成无线网络信息公平可验证全同态安全加密方案 DK 为：

$$\mathrm{DK}=R\left(\mathrm{ng},\mathrm{Enc},\mathrm{Evxl}\right) \tag{6}$$

式中：ng 为同态验证权重；Enc 为加密辅助参量；Evxl 为样本引入分布优势常量。由此调整加密指令执行公钥，为设计后续的多方计算协议做参考。

1.2 设计公平可验证全同态安全多方计算协议

在生成无线网络信息公平可验证同态加密方案后，部分关键数据可能因无法得到有效加密处理而处于暴露风险之中。因此，为有效提升无线网络信息处理的安全性、功能性和公平性，设计公平可验证全同态安全多方计算协议。

针对全同态安全加密方案受比特率变化影响，存在维数不佳问题，选取随机矩阵输出满足同态加密的计算随机关系的加密公钥 $x_n(\boldsymbol{i})$ 为：

$$x_n\left(\boldsymbol{i}\right)=\frac{\varepsilon}{2}\left[f(x_{n-1}(\boldsymbol{i}))+f(x_{n+1}(\boldsymbol{i}))\right] \tag{7}$$

式中：$\boldsymbol{i}$ 为加密离散权重；ε 为线性同态系数；n 为多阶联合区分常量。

按照解密性质恢复明文，避免泄露联合私钥信息，由此计算的加密混沌序列 $f'(\boldsymbol{i})$ 为：

$$f'(\boldsymbol{i})=\frac{k_i\left(\mathrm{DK}\right)}{\lambda(k_i-1)} \tag{8}$$

式中：k_i 为合作计算参与方概率；λ 为解密门限输入。

由于安全多方计算与加解密过程中的敌手状态紧密相关，因此，引入单值函数 δ 进一步保障相关操作的准确性与安全性。

$$\delta=\left[f'(\boldsymbol{i})\right]+\xi\cdot\pi-\mathrm{CRT} \tag{9}$$

式中：$[f'(\boldsymbol{i})]$ 为加密映射关系；ξ 为循环码；CRT 为敏感处理量。基于以上结果，按照参与方的数量与不同轮执行的操作状态调整同态运算随机解密密文，生成的公平可验证全同态安全多方计算协议如图 1 所示。

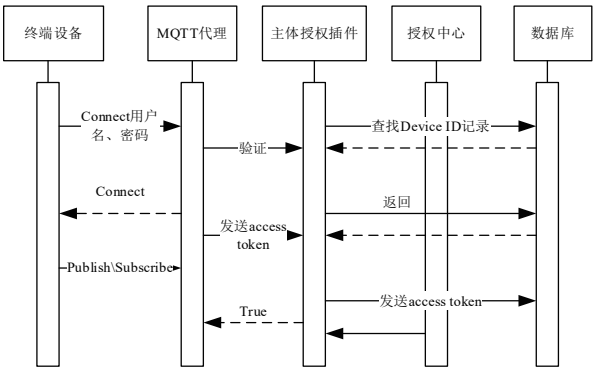

图 1 公平可验证全同态安全多方计算协议

由图 1 可知，该协议满足的调度私钥关系 $C(r)$ 为：

$$C(r)=\sum_{i=1}^{m}\sum_{j=1}^{h}H(r-\delta|a_i-a_j|) \tag{10}$$

式中：H 为混沌加密层；r 为比特分解量；a_i 为加密序列最大长度；a_j 为加密模拟替代值。

使用上述协议可以从证据磁带中获取理想集，通过模拟部分代替真实解密发布，避免受恶意对手影响，有效提高完整性验证率。

2 实验分析

2.1 参数与准备

基于无线网络信息传输要求与加密变量状态，本文设计了有效的同态加密场景，如图 2 所示。

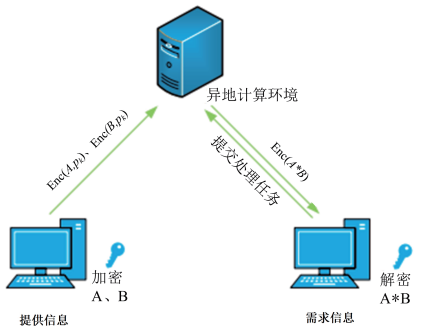

图 2 同态加密场景

在图 2 同态加密场景中选取 Interface 功放谐波传感器作为动态密钥生成装置，其参数如表 1 所示。通过设置自适应密钥加密门限阈值，超表面阵列发射器分发物理层多维度密钥，在保证基础数据状态的同时调整计算开销，获取有效的同态安全加密结果。

表 1 Interface 功放谐波传感器参数

类别	参数项	技术规格
射频性能	频率范围	1.5~6 GHz
	谐波检测阶数	2~5 及以上
	谐波幅度精度	±0.2 dB
	动态范围	70 dB
电气特性	供电电压	3.3 V±5%（DC）
	功耗	≤120 mW
	接口协议	SPI/I²C（可配置）
环境适应性	工作温度	-40 ℃~85 ℃
	谐波温漂系数	≤0.005 dB/℃
	抗震等级	20 GRMS
安全与认证	谐波指纹唯一性	相关系数≤ 0.03
	侧信道攻击防护	内置随机时延屏蔽电路
	安全认证	FIPS 140-2 Level 3
信号处理	ADC 分辨率	14 bit
	谐波抑制比	>40 dBc
	输出数据格式	32 位定点数

实验过程中，相关参数设定如下：信息矩阵为 50×50 的方阵，其元素取值范围在 0~100 之间，以此确定信息矩阵向量水平连接状态；最大列向量设定为 50 维，同时输入的 BitDecomp 向量维度为 100 维，用于生成固定加密矩阵；在确定加密索引时，预设信息对接数量为 200 条，加密覆盖节点选取 50 个，按照概率多项关系中二次多项式的形式进行随机均匀处理；信号强度阈值设定为大于等于 -75 dBm，规划信道选用 5 GHz CH144，以此构建多层级可验证全同态安全加密方案并生成同态安全加密协议开展实验。

2.2 可视化结果

将 EMP-Tool/Microsoft SEAL/HElib 作为算法库，通过 Zcash zk-SNARKs 构建同态加密框架，生成 Grafana 可视化引擎，此时通过终端采集物理层参数，构建数据加密索引，输入 Result 验证参数，得到的网络信息公平可验证全同态安全加密可视化结果如图 3 所示。所提方法能有效完成加密过程，未出现严重的加解密错误，这表明该方法在加密算法的设计与实现上具有高度的准确性，能够精准地对网络信息进行加密处理，确保数据在传输和存储过程中的保密性。同时，可视化结果中各项参数的稳定呈现，也反映出该方法在处理不同数据特征时的适应性较强，不会因数据的复杂性和多样性而出现明显的性能波动，进一步证明了其参数匹配效果较好，具有较高的可行性。

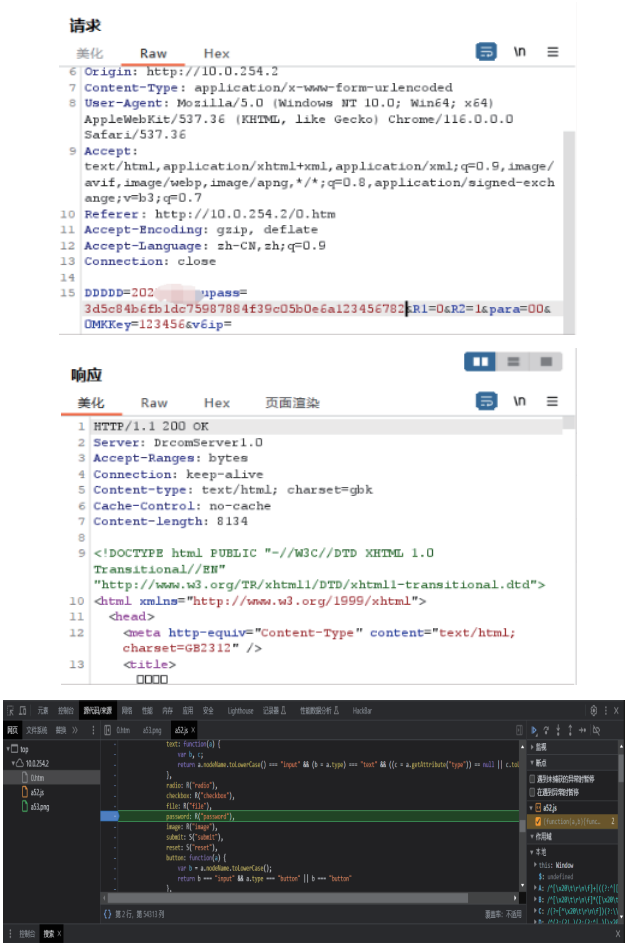

图 3 加密可视化结果

2.3 加密响应结果

在不同类型攻击下，得到的无线网络信息公平可验证全同态安全加密响应结果如图 4 所示。

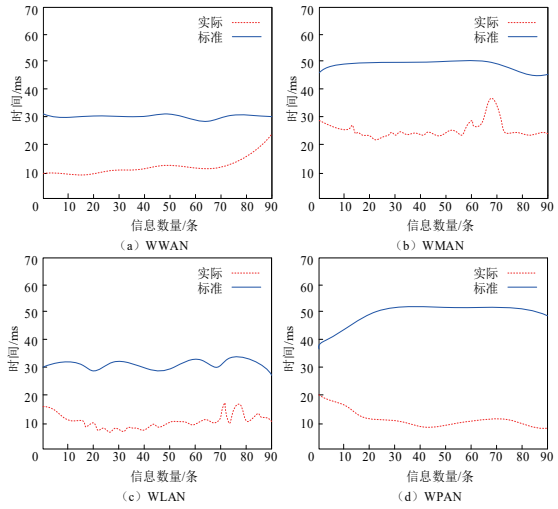

图 4 加密响应结果

由图 4 可知，在不同类型攻击下，所提方法的加密响应时间较短，满足预设的响应时间要求，具有响应高效性。所提方法能够在面对各种攻击时快速做出响应，得益于其动态密钥参数的确定机制，能够根据功放谐波频谱与环境噪声能量的变化实时调整密钥，增强了加密系统的灵活性和适应性。同时，多网络切换连续性的调整以及对频率、偏振态、空间距离等多维度的信息获取和处理，使得加密系统能够全面感知网络环境的变化，提前做好应对攻击的准备，从而在攻击发生时能够迅速启动加密和验证流程，确保数据的安全性和实时性，体现了该方法在复杂网络环境下的高效性和可靠性。

2.4 完整性验证率性能结果

选取 WAPI 2.0 作为协议栈，在 a1~a6（身份认证信息、访问控制信息、数据共享信息、升级信息、物联网设备指令信息、跨域信息）下得到的完整性验证率性能结果如表 2 所示。

表 2 完整性验证率性能结果

信息类型	本文方法 /%	文献 [2] 方法 /%	文献 [3] 方法 /%
a1（身份认证）	99	62	48
a2（访问控制）	99	62	48
a3（数据共享）	100	63	47
a4（升级信息）	99	62	49
a5（物联网指令）	100	63	48
a6（跨域信息）	99	62	47

由表 2 可知，本文方法在不同类型的无线网络信息下完整性验证率始终较高，未出现异常重叠问题，这一结果充分体现了该方法在密码学设计上的严谨性和科学性。通过合理的密码学假设和公私钥生成机制，确保了加密过程的不可逆性和安全性，使得攻击者难以破解加密数据。同时，对加密节点分布状态的准确确定，结合 WPA3 等协议增强传输安全性，进一步保障了数据在传输过程中的完整性和保密性。计算任务分配状态的合理规划以及加密结果聚合与解密反馈的高效完成，也体现了该方法在系统架构和算法实现上的优化，能够有效地应对不同类型的无线网络信息，确保数据的完整性和准确性，符合随机注入信息的加密密钥编解码要求，具有抗干扰鲁棒性。

3 结语

通过第三方服务器进行执行计算指令，无需暴露原始位置即可完成传输，提高结果的可信性，抵御异常攻击。同时，将 CRS 模型与可验证全同态加密方法融合，可以有效处理多轮变种问题，剔除恶意攻击者的攻击指令，还可以完成容错学习与非交互调整，生成同态协议，保证加密的安全性与容错性。实验结果表明，该方法能有效完成加密过程，未出现严重加解密错误，参数匹配效果良好，可行性高；在不同类型攻击下加密响应时间短，满足预设要求，具有高效性和可靠性；在不同类型无线网络信息下完整性验证率始终较高，符合加密密钥编解码要求，具备抗干扰鲁棒性。此次研究为无线网络信息安全加密提供了新思路和方法，为推动无线网络信息化进步作出了一定的贡献。

参考文献：

[1] 冼德锟 . 基于无监督学习的通信网络异常数据流智能识别方法 [J]. 长江信息通信 ,2025,38(6)216-218.

[2] 方晖 . 变拓扑结构下无线网络节点数据同态加密传输算法设计 [J]. 工业控制计算机 ,2024,37(6):105-107.

[3] 黄磊 , 易文姣 , 王英 , 等 . 基于联邦学习和多方安全计算的海铁联运数据安全共享方法研究 [J]. 铁道运输与经济 , 2024, 46(4): 58-67.

[4] 全斌 . 基于 Docker 容器的航天网络隐私数据安全防护控制研究 [J]. 计算机测量与控制 ,2024,32(5):201-207.

[5] 邓从香 . 基于混沌序列的供应链隐私网络信息加密算法 [J]. 吉林大学学报 (信息科学版),2025,43(2):303-308.

[6] 陆春阳 , 王潇炜 , 范凯迪 , 等 . 基于加密节点与单元区块子标签的综合能源信息安全共享算法 [J]. 电工技术 , 2025(7): 80-83.

[7] 单杰 , 崔敏 , 胡玉星 , 等 . 基于超混沌加密算法的 35kV 预制舱无人值守消防系统信息技术安全性研究 [J]. 自动化与仪器仪表 ,2024(12):62-66.

[8] 杨海龙 , 靳新华 . 基于 ECC 复合加密的医院网络隐私信息安全保护方法 [J]. 自动化技术与应用 ,2024,43(8):140-143.

[9] 张利胜 , 刘睿淋 , 王雪妍 . 基于光催化反应拉曼光谱信息加密纠错研究 [J]. 首都师范大学学报 (自然科学版), 2024, 45(2): 124-130.

[10] 田如意 , 顾风军 , 彭坤 , 等 . 基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密 [J]. 计算机测量与控制 , 2023,31(6):280-286.

【作者简介】

吴亚洁（1983—），女，天津蓟州人，硕士，讲师，研究方向：电子信息。

（收稿日期：2025-07-21 修回日期：2026-01-15）