基于 CRT 的快速 Paillier 同态加密算法研究

马培超[1],赵 德[2],白松林[3],李子臣[1]
(1. 北京印刷学院 信息工程学院,北京 102600;
2. 北京科技大学 计算机与通信工程学院,北京 100083;
3. 中新天津生态城智慧城市发展局,天津 300467)

摘 要:随着大数据时代的到来,数据安全和隐私保护问题日益凸显。隐私计算作为一种新兴技术,以其“可用不可见”的特性,为多方数据的安全协同计算提供了有效解决方案。在隐私计算的众多技术路线中,同态加密凭借其能够在密文状态下直接进行计算的独特优势,成为实现数据隐私保护的关键技术之一。然而,以 Paillier 算法为代表的传统同态加密方案在实际应用中面临着计算效率低下的瓶颈,严重制约了隐私计算的推广和落地。该文聚焦 Paillier 同态加密算法的效率优化问题,针对 Paillier 算法存在的效率瓶颈,提出了 CRT-Paillier 快速同态加密算法。该算法通过引入中国剩余定理对 Paillier 的加密结构进行优化,同时设计了预加密算法,有效降低了加密过程中的计算复杂度。为了验证 CRT-Paillier 算法的有效性和性能提升,进行了详细的仿真实验。实验结果表明,与原始 Paillier 算法相比,CRT-Paillier 算法在加密效率上提升了 76.4%,整体计算效率提升了 48.45%,进一步提升了同态加密算法在隐私计算领域的实用性。

关键词:隐私计算;同态加密;中国剩余定理;模数分解;Paillier
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2025)07-0079-05
doi:10.20165/j.cnki.ISSN1673-629X.2025.0071

Research on CRT-based Fast Paillier Homomorphic Encryption Algorithm

MA Pei-chao[1],ZHAO De[2],BAI Song-lin[3],LI Zi-chen[1]
(1. School of Information Engineering,Beijing Institute of Graphic Communication,Beijing 102600,China;
2. School of Computer and Communication Engineering,University of Science and Technology Beijing,
Beijing 100083,China;
3. China-Singapore Tianjin Eco-City Smart City Development Bureau,Tianjin 300467,China)

Abstract:With the advent of the big data era,issues of data security and privacy protection have gained significant prominence. As an emerging technology,privacy computation provides an effective solution for secure collaborative computation among multiple parties through its "computable but invisible" characteristic. Among various technical approaches in privacy computation,homomorphic encryption has become a key technology for achieving data privacy protection due to its unique advantage of enabling direct computations on ciphertext. However,traditional homomorphic encryption schemes,represented by the Paillier algorithm,face bottlenecks of low computational efficiency in practical applications,which severely hinders the widespread adoption of privacy computation. We focus on optimizing the efficiency of the Paillier homomorphic encryption algorithm. To address its efficiency limitations,we propose the fast CRT-Paillier homomorphic encryption algorithm. By introducing the Chinese remainder theorem to optimize the encryption structure of Paillier,and designing a pre-encryption algorithm,the proposed approach effectively reduces the computational complexity during encryption. To validate the effectiveness and performance improvements of CRT-Paillier,detailed simulation experiments were conducted. The results demonstrate that compared to the original Paillier algorithm,CRT-Paillier achieves a 76.4% improvement in encryption efficiency and a 48.45% enhancement in overall computational efficiency,significantly advancing the practicality of homomorphic encryption in privacy computation.

Key words:privacy computing;homomorphic encryption;Chinese remainder theorem;modulus factorization;Paillier

收稿日期:2024-10-26 **修回日期**:2025-02-28
基金项目:国家自然科学基金(62472040)
作者简介:马培超(2000-),男,在读硕士,研究方向为同态密码、隐私计算;通信作者:李子臣(1965-),男,教授,博士,研究方向为信息安全、密码学。

0 引 言

随着数字经济的增长,数据流通成为数据价值化的重要途径。隐私计算作为保障数据安全流通的有效方式,已广泛应用于金融、通信、互联网、政务、医疗、制造、能源等多个领域[1-4]。

同态加密(Homomorphic Encryption,HE)作为一种特殊的加密方式,允许数据以密文的方式参与运算,运算结果解密后与明文运算的结果保持一致。在保证数据安全性的同时,保留了密文的运算特性,为隐私计算中的数据加密和计算操作提供了核心支持,同样贯彻了隐私计算"可用不可见"的功能思想,使得在保持数据隐私的前提下进行数据处理和分析成为可能[5]。然而,同态加密的效率成为了限制隐私计算大规模落地应用的问题所在,即便是同态加密中效率较高的单同态加密算法(Partially Homomorphic Encryption,PHE)也时常无法满足隐私计算对于加密效率的需求。

Pascal Paillier[6]于 1999 年基于符合剩余类困难问题(Composite Degree Residuosity Classes,CDRC)提出具有加法同态性的 Paillier 算法。因其效率高、安全性证明完备的特点,在隐私计算场景中被广泛使用。在之后的工作中,一些优化的方案被提出。2001 年,Damgard 等人[7]提出一种改进的 Paillier 加密算法,在保持原有同态运算性能和安全性的基础上,减小了扩展因子,使加密数据长度可根据需求自由选择,不受密文和密钥长度的限制。2003 年,Jurik[8]总结了 Paillier 同态加密算法的相关优化方案,并提出了一种具备更高加解密效率的算法变体。2015 年,Shafagh 等人[9]提出了一种明文打包方法,实现了同时对数据项进行同态加密,提升了 Paillier 算法的效率,但仅支持有限次数的同态运算。2020 年,Ogunseyi 等人[10]通过调整算法参数,减少模乘运算的频率,优化了算法的解密过程。2021 年,Ma 等人[11]提出了一种 Paillier 变体方案,在保证安全性和同态运算特性的同时,进一步提升了算法的加密效率。

近年来,Paillier 算法在隐私计算相关应用中表现活跃,广泛服务于区块链[3]、大数据[12]、云计算[13]、人工智能[14]等领域。但在隐私计算场景中对所使用的同态算法的加密效率提出了更高的要求。为解决上述隐私计算场景中所存在的同态算法效率问题,文中工作如下:

(1)通过结合中国剩余定理(Chinese Remainder Theorem,CRT)对 Paillier 的加密结构进行改进并设计预加密算法过程;

(2)以改进后的预加密和加密过程组建一个新的 CRT-Paillier 快速同态加密方案,保证具备正确性和明文信息安全;

(3)通过仿真实验分析得知,CRT-Paillier 相对于原版方案效率得到了较大提高。从而满足新形势下隐私计算对于加法同态算法的新效率要求,加速基于同态加密方案的隐私计算应用。

1 相关知识

1.1 Paillier 加密算法

Paillier 作为经典的公钥单同态加密算法,具有结构简单、适用性较强和计算效率较高的优点。尽管现如今已经出现了大量的全同态加密算法,Paillier 依然是被大量运用的同态加密算法。Paillier 加密算法分为四个部分:参数选取、加密、解密和同态运算。

算法:Paillier 同态加密。

输入:随机选择两个长度相等的质数 p 和 q,存在明文消息 $m \in \mathbb{Z}_n$;

(1)参数选取:首先随机选择两个长度相等的质数 p 和 q,同时需满足 pq 与 $(p-1)(q-1)$ 互质,即满足公式 $\gcd(pq,(p-1)(q-1))=1$;然后,计算 $n=pq$ 和最小公倍数 $\lambda = lcm(p-1,q-1)$,选择随机数 $g \in \mathbb{Z}_{n^2}^*$。定义 $L(x)=(x-1)/n$ 和 $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$,确保 $\gcd(L(g^\lambda \bmod n^2),n)=1$。获得 $PK_{Paillier}=(n,g)$ 和 $SK_{Paillier}=(\lambda,\mu)$。

(2)加密:选择随机数 $R \in \mathbb{Z}_{n^2}^*$,可得到密文 $c = g^m R^n \bmod n^2$。

(3)解密:得到密文 $c \in \mathbb{Z}_{n^2}^*$,计算明文为 $m = \mathrm{Decrypt}(c) = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$。

(4)同态运算:假设存在明文 m_1 和 m_2,其对应密文为 c_1 和 c_2。满足运算 $m_1 + m_2 = \mathrm{Decrypt}(c_1 * c_2)$。

1.2 中国剩余定理

中国剩余定理最早可见于中国南北朝时期数学著作《孙子算经》中"物不知数"问题:"今有物不知其数,三三数之剩二;五五数之剩三;七七数之剩二。问物几何?"。CRT 可以解决一元同余方程式组问题,求解出其整数解。设 $p_1,p_2,\cdots,p_k$ 为两两互质的正整数,c 和 $r_i(i=1,2,\cdots,k)$ 为正整数。便可构建一元同余方程组 $c \equiv r_i(\bmod p_i)(i=1,2,\cdots,k)$。在文中可以表示为 $c = \mathrm{CRT}_{(p_1,p_2,\cdots,p_k)}(r_1,r_2,\cdots,r_k)$,通过计算 $P=\prod_{i=1}^{k} p_i$ 和 $P_i = P/p_i$ 可以得到 P 和 $P_i(i=1,2,\cdots,k)$。除此之外,依次计算 P_i 在模 p_i 上的乘法逆元 $I_i \equiv P_i^{-1} \bmod p_i(i=1,2,\cdots,k)$。最终通过公式 $c \equiv \sum_{i=1}^{k} P_i I_i r_i (\bmod P)$ 计算得出 c。

2 基于 CRT 的快速 Paillier 加密算法

通过对 Paillier 算法研究可以发现加密过程后的

运算均处于 $\mathbb{Z}_{n^2}^*$ 中,也就是在加密的每个过程中任意运算均需要通过 $\mathrm{mod}n^2$。CRT 的计算特性便是将分散在各个子模环 $\mathbb{Z}_{p_i}^*(i=1,2,\cdots,k)$ 上的子解 $r_i(i=1,2,\cdots,k)$ 恢复模环 $\mathbb{Z}_p^*$ 上的解 c,以此类比到 Paillier 算法加密后的运算过程中。由于 $n=pq$,因此可以将 $\mathbb{Z}_{n^2}^*$ 上的运算分解至 $\mathbb{Z}_{p^2}^*$ 和 $\mathbb{Z}_{q^2}^*$ 上,然后预计算模 p^2 和模 q^2 中的逆元,最后通过构建 $k=2$ 情况下的 CRT 公式恢复出 $\mathbb{Z}_{n^2}^*$ 上运算的结果。

下面,将 CRT 与 Paillier 算法进行结合,可以将 Paillier 算法中在 $\mathbb{Z}_{n^2}^*$ 上进行运算分解到 $\mathbb{Z}_{p^2}^*$ 和 $\mathbb{Z}_{q^2}^*$ 上进行运算。将原本的加密结构进行改造,增设了一个预加密环节,从而提高效率。

2.1　CRT-Paillier 算法设计

CRT-Paillier 算法结构分为 5 个部分:参数计算 $\mathrm{getPara}()\rightarrow\mathrm{para}$、预加密 $\mathrm{preEnc}(\mathrm{PK},m)\rightarrow(c_1,c_2)$、加密 $\mathrm{Enc}(c_1,c_2)\rightarrow c$、解密 $\mathrm{Dec}(\mathrm{SK},c)\rightarrow m$ 和同态计算 $\mathrm{Eval}(\{c_i\})\rightarrow c^*$。

(1)参数计算 $\mathrm{getPara}()\rightarrow\mathrm{para}$。

如 1.1 部分中 Paillier 参数生成过程计算得出 $\mathrm{para}=\{p,q,n,\lambda,\mu,g\}$,生成 $\mathrm{Key}=(n,p,q,g)$。

(2)预加密 $\mathrm{preEnc}(\mathrm{Key},m)\rightarrow(c_1,c_2)$。

$$\begin{cases}c_1=(l_p\cdot q^2\cdot I_1+l_q\cdot p^2\cdot I_2)\mathrm{mod}n^2\\ c_2=(R_p\cdot q^2\cdot I_1+R_q\cdot p^2\cdot I_2)\mathrm{mod}n^2\end{cases}\tag{1}$$

其中假设明文消息 m 和随机数 $R\in\mathbb{Z}_{n^2}^*$,设 $R_p=R^n\mathrm{mod}p^2$ 和 $R_q=R^n\mathrm{mod}q^2$,同理假定 $l_p=g^m\mathrm{mod}p^2$ 和 $l_q=g^m\mathrm{mod}q^2$。其他变量通过如下计算可得:首先计算 $P=p_1\cdot p_2=p^2\cdot q^2=n^2$、$P_1=P/p_1$ 和 $P_2=P/p_2$,然后计算 P_1 在模 p^2 上的逆元 $I_1\equiv(P_1)^{-1}\mathrm{mod}p^2$,同理,计算得出 P_2 在模 q^2 上的逆元 $I_2\equiv(P_2)^{-1}\mathrm{mod}q^2$。

(3)加密 $\mathrm{Enc}(c_1,c_2)\rightarrow c$。

$$c=(c_1\cdot c_2)\mathrm{mod}n^2\tag{2}$$

(4)解密 $\mathrm{Dec}(\mathrm{Key},c)\rightarrow m$。

$$m=(L(c^\lambda\mathrm{mod}n^2)/L(g^\lambda\mathrm{mod}n^2))\mathrm{mod}n\tag{3}$$

(5)同态计算 $\mathrm{Eval}(\{c_i\})\rightarrow c^*$。

$$c^*=\prod_{i=1}c_i\tag{4}$$

2.2　正确性证明

定理:1.2 提出的方案架构具有加解密正确性。

证明:假设存在明文 m、密文 c、参数 para 和随机数 $R\in\mathbb{Z}_{n^2}^*$,则可以获得密文:

$$c=(l_pq^2I_1+l_qp^2I_2)(R_pq^2I_1+R_qp^2I_2)\mathrm{mod}n^2\tag{5}$$

对上述公式使用 CRT 公式进行转化后可以得到:

$$c=g^mR^n\mathrm{mod}n^2\tag{6}$$

带入解密公式可以得到:

$$c=(L(c^\lambda\mathrm{mod}n^2)/L(g^\lambda\mathrm{mod}n^2))\mathrm{mod}n=[L((g^mR^n)^\lambda)\mathrm{mod}n^2]\cdot\mu\tag{7}$$

引理(卡米歇尔定理):若 a 与 n 互素,$a^{\lambda(n)}\equiv1\mathrm{mod}n$ 中对于所有满足 $\gcd(a,n)=1$ 的所有 a,得 $a^m\equiv1\mathrm{mod}n$ 成立的最小正整数 m 称为 n 的卡米歇尔函数,为 $\lambda(n)$。

根据引理知 $R^{\lambda n}\mathrm{mod}n^2=1$。入解密过程公式可以得到:

$$\mathrm{Dec}(\mathrm{SK},c)=[L(g^{\lambda m})\mathrm{mod}n^2]\cdot\mu\tag{8}$$

因为 $g\in\mathbb{Z}_{n^2}^*$ 且 $n+1\in\mathbb{Z}_{n^2}^*$,存在唯一一对 (a,b) 满足:

$$g^\lambda\mathrm{mod}n^2=[(1+n^{a\lambda})\cdot b^{n\lambda}]\mathrm{mod}n^2=(1+a\cdot\lambda\cdot n)\mathrm{mod}n^2\tag{9}$$

同理,转化表示 μ 可以得到 $\mu=L(1+a\cdot\lambda\cdot n\mathrm{mod}n^2)^{-1}\mathrm{mod}n$。上述公式代入解密过程可以得到公式 10,定理得证。

$$\mathrm{Dec}(\mathrm{SK},c)=(a\cdot m\cdot\lambda)\cdot(a\cdot m\cdot\lambda)^{-1}\mathrm{mod}n=m\tag{10}$$

3　实验设计与实验分析

3.1　实验设计

CRT-Paillier 相对于 Paillier 算法的改进是在加密环节,本部分将对 CRT-Paillier 和 Paillier 的加密环节的效率进行对比。硬件环境:CPU 为 Intel(R) Core(TM) i5-9400 CPU @ 2.90 GHz,机带 RAM 为 16 GB 和操作系统为 Windows 10 22H2。软件环境:算法采用 Python 编程实现,版本为 3.12.8,使用依赖库 gmpy2,版本为 2.0.8。

实验的目标在于探究 CRT-Paillier 相对于 Paillier 方案在效率上的提高。包含加密环节效率提升、算法整体运行效率提升和同态应用场景下的效率提升。

3.2　实验分析

首先,相较于同类方案,CRT-Paillier 有着较大的效率优势。固定明文长度为 256 bits,系统参数 p、q 选取长度为 1 024 bits 的质数。以程序连续运行 1 000 次加密算法作为一组,计算单次加密平均时长,作为本组的测试结果。循环测试 40 轮次,统计测试结果中出现的最大值、最小值并计算平均值,以测算算法在实际应用中的性能。以 Paillier 原方案加密时间为基准,计算时间效率提升百分比,形成表 1 所示的数据。该仿真实验表明,CRT-Paillier 相对于 Paillier 算法及相关同类衍生算法具备效率优势。

随后,固定系统参数 p、q 保持不变,不断调整明文大小,对比 Paillier 与 CRT-Paillier 在不同明文长度下的加密效率,结果如图 1 所示。在明文长度大于 256 bits 后,CRT-Paillier 的效率优势更加明显。将某一消息进行 1 次加密过程和解密过程的总和称为方案

的整体时间,绘制了整体效率对比曲线,如图 2 所示。CRT-Paillier 的效率在明文大小超过 1 024 bits 后相对于 Paillier 有着较大的提高。为了更加直观地显示出 CRT-Paillier 的效率提升,图 3 分析了在不同明文大小的情况下 CRT-Paillier 在加密和加解密全过程中的效率提升情况,在加密过程和整体过程中分别提高了 76.4% 和 48.45% 。

表 1 加密环节时间效率提升百分比 %

方案	最大值	最小值	平均值
同类方案[15]	35.49	26.00	28.69
CRT-Paillier	42.29	42.46	42.44

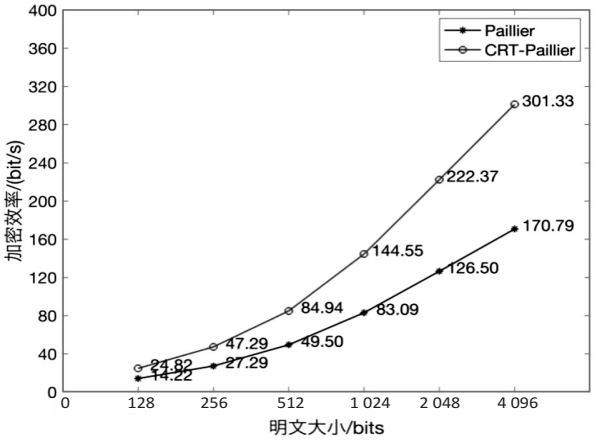

图 1 CRT-Paillier 与 Paillier 加密效率对比

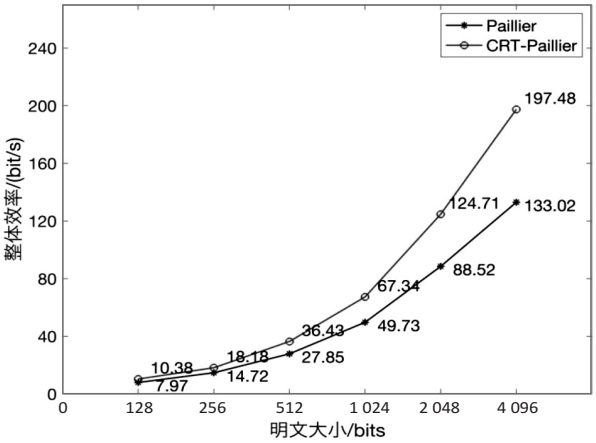

图 2 CRT-Paillier 与 Paillier 整体效率对比

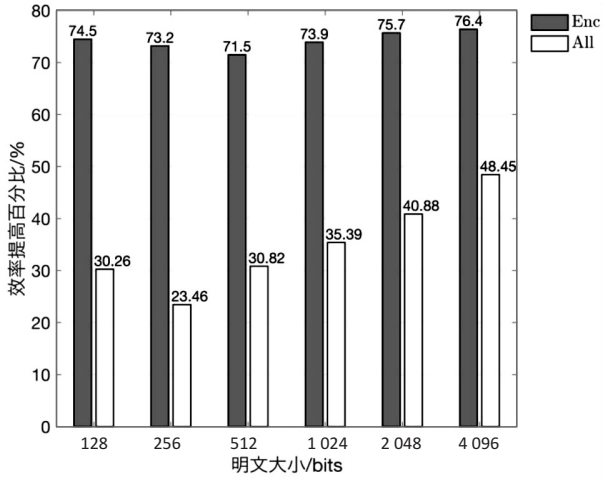

图 3 CRT-Paillier 相对于 Paillier 的效率提升

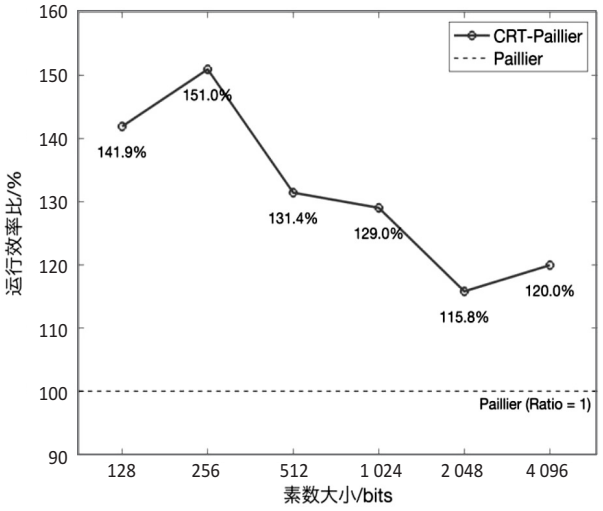

图 4 同态场景运行效率比率

最后,模拟了同态场景下 CRT-Paillier 和 Paillier 算法的不同效率表现。分别测算不同系统参数 p 、q 下 CRT-Paillier 和 Paillier 算法明文经历 1 次加密,100 次同态加法,1 次解密的时间,并以 Paillier 运行时间为基准绘制了相对运行时间比率,如图 4 所示。在以上同态场景下,算法运行效率提升比率在 115.8% 到 151% 之间。因此,CRT-Paillier 算法可以在同态场景中提供有效的效率提升。

通过以上仿真实验可以得知,CRT-Paillier 相对于 Paillier 有着较大的效率提升。

4 结束语

该文将中国剩余定理和传统的 Paillier 同态加密算法相结合,构建了 CRT-Paillier 同态加密算法,解决了 Paillier 算法效率过低的问题。首先,通过对 Paillier 算法进行细致的拆解和分析,明细算法效率瓶颈;其次,通过结合中国剩余定理将大模环上的运算进行分解,构建 CRT-Paillier 的算法结构;最后,通过理论验证和仿真实验证明了 CRT-Paillier 的正确性和加密过程效率的提高。

下一步工作的重点是基于中国剩余定理加速多种同态加密算法或全同态算法,进一步提升同态加密算法的实用性和效率。

参考文献:

[1] 郜金锋,王兴芬. 一种大宗商品交易数据共享的同态加密方法[J]. 信息技术与信息化,2024(7):146-150.

[2] 杨敏艺,宋秀兰,杨燕玲,等. Paillier 同态加密下车辆协同自适应预测巡航控制[J]. 计算机测量与控制,2024,32(8):153-160.

[3] 李　洋,王萌萌,朱建明,等. 一种基于 Paillier 和 FO 承诺的新型区块链隐私保护方案[J]. 信息安全研究,2023,9(4):306-312.

[4] 朱　嵩,王化群. 基于 Paillier 算法的智能电网数据聚合与激励方案[J]. 计算机工程,2021,47(11):166-174.

[5] MARCOLLA C,SUCASAS V,MANZANO M,et al. Survey on fully homomorphic encryption, theory, and applications [J]. Proceedings of the IEEE,2022,110(10):1572-1609.

[6] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//International conference on the theory and applications of cryptographic techniques. Berlin:Springer,1999:223-238.

[7] DAMGÅRD I,JURIK M. A generalisation, a simplification and some applications of Paillier´s probabilistic public-key system [C]//Public key cryptography: 4th international workshop on practice and theory in public key cryptosystems,PKC 2001. Cheju IslandSpringer,2001:119-136.

[8] JURIK M J. Extensions to the paillier cryptosystem with applications to cryptological protocols[M]. Shanghai:BRICS, 2003.

[9] SHAFAGH H,HITHNAWI A,DRÖSCHER A,et al. Talos: encrypted query processing for the internet of things[C]// Proceedings of the 13th ACM conference on embedded networked sensor systems. New York:Association for Computing Machinery,2015:197-210.

[10] OGUNSEYI T B,BO T. Fast decryption algorithm for paillier homomorphic cryptosystem [C]//2020 IEEE international conference on power, intelligent computing and systems (ICPICS). Shenyang:IEEE,2020:803-806.

[11] MA H,HAN S,LEI H. Optimized Paillier's cryptosystem with fast encryption and decryption[C]//Proceedings of the 37th annual computer security applications conference. New York: Association for Computing Machinery, 2021: 106-118.

[12] 田　静,杜云明,李　帅,等. Paillier 加密的隐私保护群智感知任务发布算法[J]. 计算机科学与探索,2022,16(6):1327-1333.

[13] EL MAKKAOUI K,EZZATI A,BENI-HSSANE A,et al. Fast Cloud - Paillier homomorphic schemes for protecting confidentiality of sensitive data in cloud computing[J]. Journal of Ambient Intelligence and Humanized Computing, 2020,11(6):2205-2214.

[14] WANG J,JIN C,MEFTAH S,et al. Popcorn:Paillier meets compression for efficient oblivious neural network inference [J]. arXiv:2107.01786,2021.

[15] 尚家秀,吴宗航,史腾飞. 基于中国剩余定理的 Paillier 加密改进方法[J]. 信息技术与信息化,2023(3):133-136.