FR-FPE：有限基保留格式加密算法

王小峰[1]，叶军[2]，刘文正[3]，孙兵[4]，吴华晖[5]，郭佳朴[1]
（1.国防科技大学计算机学院，湖南 长沙 410073；2.湖南安方信息技术有限公司，湖南 长沙 410221；
3.长沙理工大学计算机学院，湖南 长沙 410015；4.国防科技大学理学院，湖南 长沙 410073；
5.湖南省农村信用社联合社，湖南 长沙 410013）

摘　要：针对现有保留格式加密算法难以应对滑动关联及线性密码分析攻击且效率不高的问题，提出了有限基保留格式加密FR-FPE算法。通过设计基于CBC模式的参数向量加密机制和结构化调整参数全关联加密模型，有效抵御滑动关联及线性密码分析攻击。通过设计轻量化确定性加密结构，支持对不超过192 bit的明文和96 bit的调整参数进行加密，在保证算法与NIST FF1相同安全强度的同时，分组加密的调用次数比FF1减少45%（9次）。基于Game-Hopping博弈模型，给出了FR-FPE算法强伪随机置换（SPRP）安全性证明，并量化分析了算法抵御滑动关联及线性密码分析攻击的能力。实验结果表明，针对radix=36的数字字母混合数据集，FR-FPE的每秒加密次数比FF1平均高26.55%，加密数据吞吐率平均高21.25%。

关键词：保留格式加密；滑动关联攻击；线性密码分析攻击；强伪随机置换
中图分类号：TN918
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026080

FR-FPE: finite radix oriented format-preserving encryption algorithm

Wang Xiaofeng[1], Ye Jun[2], Liu Wenzheng[3], Sun Bing[4], Wu Huahui[5], Guo Jiapu[1]
1. College of Computer Technology, National University of Defense Technology, Changsha 410073, China
2. Hunan Secuber Information Technology Co., Ltd., Changsha 410221, China
3. School of Computer Science and Technology，Changsha University of Science and Technology, Changsha 410015, China
4. College of Science, National University of Defense Technology, Changsha 410073, China
5. Hunan Rural Credit Cooperative, Changsha 410013, China

Abstract: Existing format-preserving encryption algorithms were vulnerable to slide attack and linear cryptanalysis attack, and had low efficiency. A finite radix oriented format-preserving encryption (FR-FPE) algorithm was proposed. It designed a CBC mode based on initial vector encryption mechanism and a fully associated encryption model with structured tweak parameters, which could effectively defend against slide attack and linear cryptanalysis attack. A lightweight and deterministic encryption structure was designed to support plaintexts up to 192 bit and tweak parameters up to 96 bit. While ensuring the same security strength as NIST FF1, the number of block encryption calls was reduced by 45% (9 times) compared with FF1. Based on the Game-Hopping game model, the security proof of strong pseudorandom permutation (SPRP) for the FR-FPE algorithm was given, and the ability of the algorithm to resist sliding attacks and linear cryptanalytic attacks was quantitatively analyzed. Experimental results show that for a mixed alphanumeric dataset with radix=36, FR-FPE achieves an average increase of 26.55% in encryption times per second and 21.25% in encrypted data throughput compared to FF1.

Keywords: format-preserving encryption, slide attack, linear cryptanalysis attack, SPRP

收稿日期：2026–01–21；修回日期：2026–03–20
通信作者：王小峰，xf_wang@nudt.edu.cn

0　引言

随着信息技术的发展，各行业面临大量固定格式数据的加密保护需求，如信用卡号、身份证号等。传统分组加密算法（如SM4）一般需要扩充数据为无意义二进制串，不能保持明文数据的长度、格式和语义。这种格式的改变导致密文数据无法兼容现有系统或数据库，需要成本高昂且复杂的系统改造。为此，保留格式加密（format-preserving encryption, FPE）技术被提出，其能够保证密文长度、类型（如数字、字母、中文等）与明文一致。

FPE技术得到学术界和工业界的高度重视。美国国家标准局发布了FIPS74，提出了明密文格式相同的字符串加密方法[1]。Black 等[2]提出了Prefix、Cycle-Walking和Generalized-Feistel 3种FPE密码构造方法。美国国家标准与技术研究院（NIST）发布了NISTSP800-38G草案，提出了FF1和FF3两套保留格式加密算法标准[3]并持续更新。美国国家标准研究所发布ANSIX9.124-2-2018标准[4]，提出了基于计算器密钥流模式的保留格式加密算法。韩国也发布了保留格式加密算法标准FEA-1和FEA-2[5]。

尽管保留格式加密算法被诸多国际机构采纳并得到广泛应用[6-9]，但其安全性一直是研究的重点，其中滑动关联攻击和线性密码分析攻击对当前算法构成严重威胁。Amon 等[10]构造了3种滑动攻击方法，其中利用循环结构的滑动攻击使数据存储和时间复杂度达到最优，分别为$O\left(N^{\frac{11}{6}}\right)$和$O\left(N^{\frac{17}{6}}\right)$，其中$N$为集合大小。Beyne[11]利用轮次调整参数在两个值之间交替的特性，通过发起消息恢复攻击来概率性地推断出部分明文内容。该攻击将FF3-1消息还原攻击的数据复杂度降低为$O\left(N^{2.5}\right)$，并导致FF3-1在NIST的新标准中被移除，同时韩国的FEA-1和FEA-2标准也不再安全。

当前能够抵御线性密码分析攻击的FPE分组加密算法标准只有NIST FF1，但其向量与明文拼接的加密机制导致多次分组加密调用，效率较低。保留格式加密主要面向身份证号、手机号、银行卡号等有限长度（均小于192 bit）明文的加密需求，更长的明文可采用多次FPE分组加密的方式实现，因此需要面向定长加密，以实现更快的计算速度，如FF3-1为192 bit，FEA-2为64 bit。

为了使面向定长加密的FPE算法能够抵御线性密码分析攻击，中国密码行业标准化技术委员会GM/Y 5007-2024研究报告介绍了TE-FPE(SM4)算法，其在FF3算法基础上对调整参数进行加密截取，并作为轮函数的调整参数，从而能抵抗线性密码分析、滑动关联等攻击。但TE-FPE算法结构不固定，导致算法的软硬件实现复杂。其调整参数最长为56 bit，在小消息域场景下，算法的抗穷举攻击能力不强。TE-FPE算法未公开给出基本的伪随机置换（pseudorandom permutation, PRP）安全性证明，以及抵抗线性密码分析和滑动关联攻击的量化分析。

为此，本文提出了有限基保留格式加密（finite radix-oriented format-preserving encryption, FR-FPE）算法，支持对长度不超过192 bit的明文和不超过96 bit的调整参数进行加密，算法结构固定，在大大减少分组加密调用次数的情况下，能够抵抗滑动关联攻击和线性密码分析攻击。本文的主要贡献如下。

1) 基于CBC模式的参数向量关联加密机制，FR-FPE算法将明文参数、分组加密算法标识及调整参数的高位字节等构造为算法初始变量P，对其进行分组加密（如SM4）得到预加密值$F=\mathrm{CIPH}_K(P)$，并将预加密值F通过CBC模式参与所有Feistel轮次的明文加密操作，从而将关键参数强关联于整个加密过程，有效抵御滑动关联攻击。

2) 调整参数结构化全关联加密模型。不同于现有模型将调整参数或加密的调整参数分为左右两部分，再分别参与Feistel奇偶轮次加密，FR-FPE将调整参数的高位和低位字节同时参与Feistel所有轮次加密（高位字节以CBC模式参与，低位字节与轮数异或后再与明文拼接），保证了调整参数加密的伪随机置换性和对整体明文加密的关联性，有效抵御线性密码分析攻击。同时FR-FPE最高支持96 bit调整参数，显著增加小域加密穷举攻击难度[11]。

3) 轻量化确定性加密结构。基于CBC模式的参数向量加密机制，FR-FPE采用与FF1相同的固定10轮Feistel结构，但在明文长度不超过192 bit、调整参数不超过96 bit的情况下，FR-FPE分组加密的调用次数比FF1减少45%（9次），在保证与FF1相同安全强度的同时，大大提升了算法效率。

本文基于Game-Hopping博弈模型，证明了

FR-FPE算法具有强伪随机置换（strong pseudorandom permutation, SPRP）安全性，量化分析了算法抵御滑动关联及线性密码分析攻击的能力。实验结果表明，相比FF1算法，FR-FPE的每秒加密次数平均高26.55%，加密数据吞吐率高21.25%；相比TE-FPE算法，FR-FPE加密速度在明文小于42 bit时平均快8.54%，在明文大于42 bit时平均慢17.7%（FR-FPE加密Feistel轮数多2轮，安全性更高）。

1　相关工作

保留格式加密的近期研究工作主要包括4个方面：安全模型、算法模型、攻击技术和标准化。

在安全模型方面，Black等[2]提出了保留格式加密基础模块是分组密码和伪随机函数，因此FPE的安全目标是PRP安全，如PRP-CPA1、PRP-CCA1等。

在算法模型方面，Black等[2]提出了3种FPE构建方法：Prefix方法基于预置换表建立消息空间内的置换；Cycle-Walking方法是通过反复应用加密操作，确保结果落在有效域内以符合格式要求；Generalized-Feistel方法通过Feistel网络迭代轮函数来处理数据的左右两半。Spies[12]以平衡Feistel网络为基础提出了FFSEM（Feistel finite set encryption mode）。Bellare等[13]在FFSEM模型的基础上提出了基于Feistel网络的FFX模型，加入调整因子[14]，并将消息空间的所有字符型数据与整数域的数据建立映射表。文献[15]提出了基于k-分割Feistel网络的FPE方案，以适应各种长度数据的加密需求。

在攻击技术和标准化方面，NIST于2013年发布SP800-38G草案，包括两种基于Feistel模式的FPE加密算法FF1和FF3，采用不同的加密轮数、调整参数及初始向量加密方式。Lee等[5]提出了基于Feistel结构的FPE方案FEA-1和FEA-2，并成为韩国的FPE标准（TTAK.KO-12.0275）。在标准算法提出之后，Bellare等[16]给出了基于Feistel结构的FPE方案消息恢复攻击，对于长度为8 bit的消息，采用8轮Generalized-Feistel结构的FF3方案，恢复消息的复杂度仅为2^{32}。Durak等[17]改进了FF1和FF3方案的攻击方法，指出在消息域规模较小时，FF1与FF3方案均无法提供128 bit的安全性。刘哲理等[18]基于调整参数构造和线性分析方法，将FF3-1消息恢复攻击的数据复杂性降低为$O(N^{2.5})$。为此，2025年NIST将FF3-1算法移除，仅保留FF1方案。但其向量与明文拼接的加密机制导致多次分组加密调用，效率较低。

2024年，中国密码行业标准化技术委员会介绍了TE-FPE(SM4)算法，针对不同长度的明文消息，算法的Feistel轮数不同（8、10、12轮等）、轮函数调整参数数据的长度不同（56、64 bit）、轮数字段的位数不同（4、8 bit），导致算法的软硬件实现复杂，理论安全性证明难度大。TE-FPE采用较短的56 bit调整参数，在小消息域场景下，算法的抗穷举攻击能力不强[11]。另外，算法未公开给出基本的PRP安全性证明，以及对线性密码分析和滑动关联攻击的量化分析。

综上所述，现有工作难以同时满足以下要求：轻量级确定性算法结构；支持96 bit调整参数和192 bit明文加密；严格的PRP安全性证明；能够抵御滑动关联和线性密码分析攻击，并给出量化分析。

2　预备知识与形式化定义

本节对有限基保留格式加密算法FR-FPE的语法和相关密码学概念进行定义。

2.1　算法语法

密钥空间$\mathcal{K}$：底层分组密码CIPH的有效密钥集合，$\mathcal{K}=\{0,1\}^{128}$。

格式空间$\mathcal{N}$：数据格式空间的集合，包括长度n、基数radix和分组加密算法标识符cid。$\mathcal{N}=(n,\text{radix},\text{cid})$。

调整参数空间$\mathcal{T}$：允许的调整参数集合。$\mathcal{T}=\{0,1\}^{96}$。

域$\mathcal{X}$：所有可能的明文/密文集合。$\mathcal{X}=\bigcup_{N=(n,\text{radix},\text{cid})\in\mathcal{N}}\Sigma_{\text{radix}}^{n}$。

FR-FPE加密函数$E:\mathcal{K}\times\mathcal{N}\times\mathcal{T}\times\mathcal{X}\to\mathcal{X}\cup\perp$：对于固定的密钥$K\in\mathcal{K}$、格式$N\in\mathcal{N}$和调整参数$T\in\mathcal{T}$，加密函数$E_{K,N,T}$是$\mathcal{X}_N$上的置换，$E_{K,N,T}(\cdot)\equiv E(K,N,T,\cdot)$将$\mathcal{X}_N$映射到$\mathcal{X}_N$。解密函数$D:\mathcal{K}\times\mathcal{N}\times\mathcal{T}\times\mathcal{X}\to\mathcal{X}\cup\perp$，其中$D_{K,N,T}$是$E_{K,N,T}$的逆函数。

2.2　安全性定义

保留格式加密的本质是在特定消息空间内的伪随机置换，其安全目标为PRP安全，下面分别给出非适应性选择明文攻击CPA1下的PRP安全[19]和非

适应性选择密文攻击 CCA1 下的 SPRP 安全的定义[20]。

定义 1　PRP 安全性。攻击者 A 针对 FPE 的 PRP 优势定义为

$$\mathrm{Adv}_{\varepsilon\mathrm{FPE}}^{\mathrm{PRP}}(A)=2\Pr[K\xleftarrow{\$}\mathcal{K};A^{O_1(N,T,X)}\Rightarrow\mathrm{true}]-1 \quad (1)$$

其中，$\mathcal{O}_1(N,T,X)=E_{K,N,T}(X)$ 为非适应性选择明文攻击下的查询预言机，要求攻击者在第一次查询预言机之前准备好所有问题，每次查询独立，且只允许查询加密预言机。

定义 2　SPRP 安全性。攻击者 A 针对 FPE 的 SPRP 优势定义为

$$\mathrm{Adv}_{\varepsilon\mathrm{FPE}}^{\mathrm{SPRP}}(A)=2\Pr[K\xleftarrow{\$}\mathcal{K};A^{O_1(N,T,X)};A^{\mathcal{O}_1^{-1}(N,T,X)}\Rightarrow\mathrm{true}]-1 \quad (2)$$

SPRP 优势 $\mathrm{Adv}_{\mathrm{FR\text{-}FPE}}^{\mathrm{SPRP}}(A)$ 的定义类似于 $\mathrm{Adv}_{\varepsilon\mathrm{FPE}}^{\mathrm{PRP}}(A)$，但攻击者 A 还可以访问解密预言机 $\mathcal{O}_1^{-1}(\cdot,\cdot,\cdot)$，$\mathcal{O}_1^{-1}(N,T,Y)=D_{K,N,T}(Y)$。但如果 Y 是之前查询 $\mathcal{O}_b(N,T,X)$ 的结果，则 A 不能查询 $\mathcal{O}_1^{-1}(N,T,Y)$。

2.3　攻击分析技术

保留格式加密技术安全性仍面临诸多挑战，当前主要的攻击分析技术如下。

1) 小域加密安全性。文献[13,17,21-22]研究表明，Feistel 网络在小域场景下更容易被穷举或统计分析。当加密域 $\mathrm{radix}^{\mathrm{minlen}}<10^6$ 时，Feistel 类 FPE 算法的实际安全强度显著弱化。这种安全性下降源于小域空间导致差分特征更易捕捉，且轮函数输出碰撞概率随域尺寸缩小呈指数级增长，导致算法的实际安全强度远低于底层分组加密算法（如 AES-128）提供的标称强度。攻击者可能通过收集少量密文或进行复杂度远低于穷举密钥的攻击来恢复明文。

2) 滑动关联攻击。Patarin[23]提出了滑动关联攻击，Amon 等[10]构造了对保留格式加密方案的 3 种滑动关联攻击方法，其中利用循环结构的滑动关联攻击使数据存储和时间复杂度达到最优，分别为 $O\left(N^{\frac{11}{6}}\right)$ 和 $O\left(N^{\frac{17}{6}}\right)$。攻击者试图寻找一对明文/密文 (X,C) 和 (X',C')，使 X' 是 X 经过少量轮数加密的结果，C' 是 C 经过相同少量轮数加密的结果，通过找到这样的“滑动对”，攻击者可以将完整 r 轮密码的攻击问题，转化为对 $r-s$ 轮密码的攻击问题（其中 s 是滑动的轮数）。这大大降低了攻击的复杂性。攻击者通过构造特殊 Tweak 序列 $(T_1,T_2,\cdots,T_n)$ 触发轮函数内部状态泄露，当 Tweak 序列重用次数超过 2^{32} 时，可建立明文–密文对应关系数据库，进而以 $O\left(\sqrt{N}\right)$ 复杂度恢复敏感数据。

3) 线性密码分析攻击。通过构建形如 $aL_0\oplus bR_0\oplus aL_r\oplus bR_r=\Delta_T$ 的线性逼近方程，攻击者[11]可利用 Tweak 序列控制输入差分传播路径。轮函数输入输出比特数目受限，单轮线性近似的偏差较大，且轮数有限导致累积偏差无法迅速衰减至信息论不可区分水平，从而使攻击者可通过构造有意义的线性表达式，利用偏差累积原理对加密过程进行区分或猜测。

3　FR-FPE 算法设计

3.1　符号及定义

1) 密钥 K：一个对称密钥，密钥长度为 128 bit。密钥 K 用于底层的密码运算 CIPH_K，需要安全存储和保护。

2) 字符基数 radix：定义明文字符串 X 所使用的字符集的大小。例如，数字字符 radix = 10 代表数字字符共计 10 个，小写字母 radix = 26 代表小写字母字符共计 26 个。

3) 明文长度 n：需要加密的原始数据长度，范围是 $\log_{\mathrm{radix}}10^6\leqslant n\leqslant 2(\log_{\mathrm{radix}}2^{96})$。

4) 明文 X：需要加密的原始数据，表示为一个由 n 个字符组成的字符串 $X=X_1X_2\cdots X_n$。

5) 调整参数 T：一个公开的、用于调整明文加密的字符串参数，相同的密钥 K 及明文 X 通过不同的调整参数 T 得到不同的密文，FR-FPE 的调整参数长度 Tlen 不大于 96 bit。

6) 分组加密算法标识符 cid：标识底层分组加密算法的选择索引，通常为固定值，如 SM4 为 1，SM3-HMAC 为 2，AES 为 3。

7) 标准分组加密函数 $\mathrm{CIPH}_K(X)$：使用标准分组加密算法及密钥 K 对明文 X 进行加密，标准加密算法如 SM4、SM3-HMAC 和 AES 等。

8) 字符串到整数转换函数 $\mathrm{NUM}_{\mathrm{radix}}(S)$：将基数为 radix 的字符串 S 转换为一个非负整数。

9) 二进制比特串到整数转换函数 $\mathrm{NUM}(S)$：将二进制比特串 S 转换为一个非负整数。

10) 整数到字符串转换函数 $\mathrm{STR}_{\mathrm{radix}}^{m}(x)$：将非

负整数 x 转换为一个长度为 m、基数为 radix 的字符串。

11) 模加运算：在有限域上的加法运算。对于基数为 radix、长度为 m 的字符串所表示的整数 a 和 b，其模加运算定义为 $c=(a+b)\bmod \text{radix}^m$。

12) 模减运算：在有限域上的减法运算。对于基数为 radix、长度为 m 的字符串所表示的整数 a 和 b，其模减运算定义为 $c=(a-b)\bmod \text{radix}^m$（结果取非负最小剩余）。

3.2　算法结构

FR-FPE 算法的加密架构和解密架构分别如图 1 和图 2 所示。算法将数据分割为左右两部分，结合密码学安全的分组加密函数、初始变量 P 和调整参数 T，并经过多轮 Feistel 网络迭代处理，确保加密后的数据格式与明文完全相同。FR-FPE 采用与 FF1 算法相同的固定 10 轮 Feistel 结构，支持对长度不超过 192 bit 的明文和 96 bit 的调整参数进行加密。

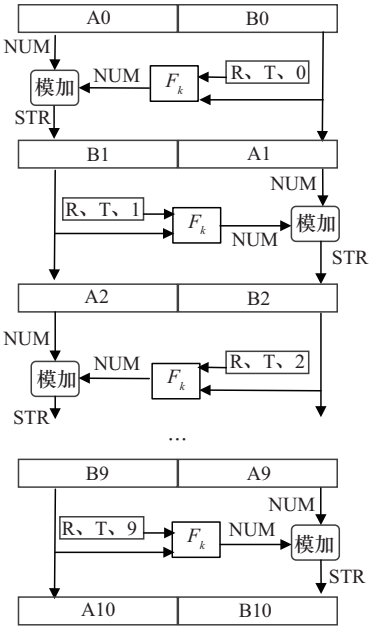


图 1　FR-FPE 算法的加密架构

FR-FPE 算法将明文参数、分组加密算法标识及调整参数的高位字节等构造为算法初始变量 P，对其进行分组加密（如 SM4）后，采用 CBC 模式参与所有 Feistel 轮次的加解密操作。同时，算法将调整参数的低位字节与轮数异或后与明文拼接，再与初始变量 P 进行 CBC 加密。通过 CBC 模式，算法保证了初始变量 P 和调整参数 T 能够参与所有 Feistel 轮次的加解密操作，确保了加密的伪随机置换性和对整体明文加密的关联性，能够有效抵御滑动关联攻击和线性密码分析攻击。

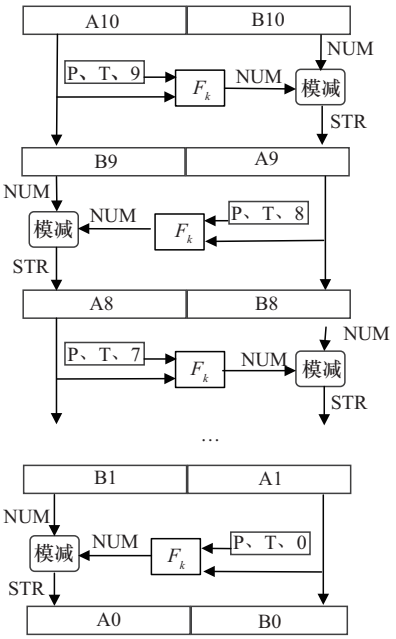


图 2　FR-FPE 算法的解密架构

3.3　加密算法

FR-FPE 加密算法流程如算法 1 所示。

算法 1　FR-FPE 加密算法流程

输入　密钥 K，长度为 n 的明文字符串 X，分组加密算法标识符 cid，调整参数 T，基数 radix

输出　长度为 n 的密文字符串 Y

1) $u \leftarrow \left\lfloor \frac{n}{2} \right\rfloor, v \leftarrow n-u$

2) $A \leftarrow X[1\cdots u]$，$B \leftarrow X[u+1\cdots n]$

3) $P=[1]^1 \| [\text{Tlen}]^1 \| [\text{radix}]^3 \| [u \bmod 256]^1 \| [n]^1 \| [\text{cid}]^1 \| [T_{\text{H}}]^8$

4) $F \leftarrow \text{CIPH}_K(P)$

5) for $i \leftarrow 0$ to 9 do

6)　$Q \leftarrow \left([T_{\text{L}}]^4 \oplus [i]^4\right) \| [\text{NUM}_{\text{radix}}(B)]^{12}$

7)　$R \leftarrow \text{CIPH}_K(F \oplus Q)$

8)　$y \leftarrow \text{NUM}(R)$

9)　if i is even then $m \leftarrow u$

10)　else $m \leftarrow v$

11)　end if

12)　$c \leftarrow \left(\text{NUM}_{\text{radix}}(A)+y\right) \bmod \text{radix}^m$

13)　$C \leftarrow \mathrm{STR}^{m}_{\mathrm{radix}}(c)$

14)　$A \leftarrow B$，$B \leftarrow C$

15) end for

16) return $A||B$

给定密钥K、明文X、调整参数T、算法标识符cid和基数radix，算法的主要过程如下。

1) 明文和调整参数分割

计算明文左右两半的长度分别为$u = \left\lfloor \frac{n}{2} \right\rfloor$和$v = n - u$，其中$n$为明文长度，$\left\lfloor \frac{n}{2} \right\rfloor$为$\frac{n}{2}$向下取整；将明文$X$分割为左部分$A = X[1\cdots u]$和右部分$B = X[u+1\cdots n]$；将调整参数$T$在高位字节用0补齐为96 bit，并分割为高64 bit字节$T_{\mathrm{H}} = T[1\cdots 64]$和低32 bit字节$T_{\mathrm{L}} = T[65\cdots 96]$。

2) 构造初始向量

选取调整参数长度Tlen、明文基数radix、明文左部分长度u、明文长度n、分组加密算法标识符cid、调整参数的高64 bit T_{H}以及常数项，编码成定长字符并串联组合成一个128 bit的组合变量P。

$$P = [1]^1||[\mathrm{Tlen}]^1||[\mathrm{radix}]^3||[u \bmod 256]^1||[n]^1||[\mathrm{cid}]^1||[T_{\mathrm{H}}]^8 \tag{3}$$

其中，$[1]^1$表示将常数1编码成1字节字符，$[\mathrm{Tlen}]^1$是调整参数T的1字节表示，$[\mathrm{radix}]^3$是基数radix的3字节表示，$[u \bmod 256]^1$是u对256取模的1字节表示，$[n]^1$是长度n的1字节表示，$[\mathrm{cid}]^1$是分组加密算法标识的1字节表示，$[T_{\mathrm{H}}]^8$是调整参数的高8 B。

3) 对初始向量进行对称加密

对初始向量进行对称加密，得到初始向量密文$F = \mathrm{CIPH}_K(P)$，$\mathrm{CIPH}_K(P)$表示使用CIPH对称加密算法和密钥K对初始向量P进行加密，CIPH对称加密算法由分组加密算法标识符cid确定。

4) 执行10轮Feistel迭代

① 构造轮加密明文Q，先将调整参数低4 B $[T_{\mathrm{L}}]^4$与轮数i的4 B编码$[i]^4$进行按位异或，再与右部分明文B转化为整数后的12 B编码进行拼接，计算式为$Q = \left([T_{\mathrm{L}}]^4 \oplus [i]^4\right)||[\mathrm{NUM}_{\mathrm{radix}}(B)]^{12}$。

② CBC轮加密密文R：将初始向量密文F与轮加密明文Q按位异或，再使用CIPH对称加密算法和密钥K对异或结果进行加密，计算式为$R = \mathrm{CIPH}_K(F \oplus Q)$。

③ 将R转换为整数$y = \mathrm{NUM}(R)$。

④ 确定左部分输入A字符串长度m：若i为偶数，则$m = u$，否则$m = v$。

⑤ 对左部分输入A计算轮更新数据C：将基数radix的字符串A转换为整数$\mathrm{NUM}_{\mathrm{radix}}(A)$，并计算整数$c = \left(\mathrm{NUM}_{\mathrm{radix}}(A) + y\right) \bmod \mathrm{radix}^m$，然后使用字节转换函数$\mathrm{STR}^{m}_{\mathrm{radix}}$将整数$c$转换为radix基数字符串$C$。

⑥ 更新轮输出左右部分：$A = B$，$B = C$。

5) 输出密文

10轮Feistel迭代后，将最终的A和B拼接，得到输出密文$Y = A||B$。

3.4　解密算法

FR-FPE解密算法流程如算法2所示。

算法2　FR-FPE解密算法流程

输入　密钥K，长度为n的密文字符串X，分组加密算法标识符cid，调整参数T，基数radix

输出　明文字符串Y

1) $u \leftarrow \left\lfloor \frac{n}{2} \right\rfloor, v \leftarrow n - u$

2) $A \leftarrow X[1\cdots u]$，$B \leftarrow X[u+1\cdots n]$

3) $P = [1]^1||[\mathrm{Tlen}]^1||[\mathrm{radix}]^3||[u \bmod 256]^1||[n]^1||[\mathrm{cid}]^1||[T_{\mathrm{H}}]^8$

4) $F \leftarrow \mathrm{CIPH}_K(P)$

5) for $i \leftarrow 9$ to 0 do

6)　$Q \leftarrow \left([T_{\mathrm{L}}]^4 \oplus [i]^4\right)||[\mathrm{NUM}_{\mathrm{radix}}(A)]^{12}$

7)　$R \leftarrow \mathrm{CIPH}_K(F \oplus Q)$

8)　$y \leftarrow \mathrm{NUM}(R)$

9)　if i is even then $m \leftarrow u$

10)　else $m \leftarrow v$

11)　end if

12)　$c \leftarrow \left(\mathrm{NUM}_{\mathrm{radix}}(B) - y\right) \bmod \mathrm{radix}^m$

13)　$C \leftarrow \mathrm{STR}^{m}_{\mathrm{radix}}(c)$

14)　$B \leftarrow A, A \leftarrow C$

15) end for

16) return $A||B$

给定密钥K、密文X、调整参数T、分组加密

算法标识符cid和基数radix，算法的主要过程如下。

1) 密文和调整参数分割

计算密文左右两半的长度分别为$u=\left\lfloor\frac{n}{2}\right\rfloor$和$v=n-u$，其中$n$为明文长度，$\left\lfloor\frac{n}{2}\right\rfloor$为$\frac{n}{2}$向下取整；将密文$X$分割为左部分$A=X[1\cdots u]$和右部分$B=X[u+1\cdots n]$；将调整参数$T$在高位字节用0补齐为96 bit，并分割为高64 bit字节$T_{\mathrm{H}}=T[1\cdots 64]$和低32 bit字节$T_{\mathrm{L}}=T[65\cdots 96]$。

2) 构造初始向量

选取调整参数长度Tlen、明文基数radix、明文左部分长度u、明文长度n、加密算法标识符cid、调整参数的高64 bit T_{H}以及常数项，编码成定长字符并串联组合成一个128 bit的组合向量P。

$$P=[1]^1\|[\mathrm{Tlen}]^1\|[\mathrm{radix}]^3\|[u \bmod 256]^1\|[n]^1\|[\mathrm{cid}]^1\|\left[T_{\mathrm{H}}\right]^8 \tag{4}$$

各字段编码方式与加密算法一致。

3) 对初始向量进行对称加密

与加密算法一致，计算初始向量密文$F=\mathrm{CIPH}_K(P)$。

4) 逆序执行10轮Feistel迭代

① 构造轮加密明文Q，先将调整参数低4 B $\left[T_{\mathrm{L}}\right]^4$与轮数$i$的4 B编码$[i]^4$进行按位异或，再与左部分输入$A$转化为整数后的12 B编码进行拼接，计算式为$Q=\left(\left[T_{\mathrm{L}}\right]^4\oplus[i]^4\right)\|[\mathrm{NUM}_{\mathrm{radix}}(A)]^{12}$。

② 计算轮加密密文R：将初始向量密文F与轮加密明文Q按位异或，再使用CIPH对称加密算法和密钥K对异或结果进行加密，计算式为$R=\mathrm{CIPH}_K(F\oplus Q)$。

③ 将R转换为整数$y=\mathrm{NUM}(R)$。

④ 确定右部分输入B字符串长度m：若i为偶数，则$m=u$；否则$m=v$。

⑤ 对右部分输入B计算轮更新数据C：将基数radix的字符串A转换为整数$\mathrm{NUM}_{\mathrm{radix}}(B)$，并计算整数$c=\left(\mathrm{NUM}_{\mathrm{radix}}(B)-y\right)\bmod \mathrm{radix}^m$，然后使用字节转换函数$\mathrm{STR}^m_{\mathrm{radix}}$将整数$c$转换为radix基数字符串$C$。

⑥ 更新轮输出左右部分：$B=A$，$A=C$。

5) 输出明文

10轮Feistel迭代后，将最终的A和B拼接，得到输出明文$Y=A\|B$。

3.5 算法能力比较分析

FR-FPE算法与NIST标准FF1、FF3-1算法、国密标准研究报告SM4-TE-FPE算法的对比如表1所示。

表1 FR-FPE与经典保留格式加密算法对比

算法	明文及调整参数长度	安全性	调整参数加密方式	分组加密算法调用次数/次（明文长度n≤192 bit，调整参数长度Tlen≤96 bit）	分组加密算法调用次数/次（明文长度n>192 bit，调整参数长度为96 bit）	Feistel轮数/轮
FR-FPE	明文长度不超过192 bit，调整参数长度不超过96 bit	强伪随机置换安全性证明、抗滑动关联攻击定性定量分析、抗线性密码分析攻击定性定量分析	T_{H}全局关联加密，T_{L}异或轮数，再全局关联加密	11	$11\left\lfloor\frac{n}{192}\right\rfloor$	10
FF1	明文长度不超过2^{32} bit，调整参数长度不限	伪随机置换安全性证明、抵御参数滑动关联攻击、抵御线性密码分析攻击	整体全局关联加密	至少20	$10\left\lfloor\left\lfloor\frac{n}{2}-24}{128}\right\rfloor+\left\lceil\frac{n+64}{256}\right\rceil\right\rfloor$	10
FF3-1	明文长度不超过192 bit 调整参数长度不超过56 bit	无法抵御参数滑动关联攻击、无法抵御线性密码分析攻击	T_{L}异或轮数，参与奇数轮加密，T_{R}异或轮数，参与偶数轮加密	8	$8\left\lfloor\frac{n}{192}\right\rfloor$	8
TE-FPE	明文长度不超过192 bit，调整参数长度不超过56 bit	无伪随机置换安全性公开证明、抗滑动关联攻击定性分析、抗线性密码分析攻击定性分析	加密后截取重组为$\frac{T_{\mathrm{L}}}{T_{\mathrm{R}}}$，截取后信息熵降低，$T_{\mathrm{L}}$异或轮数，参与奇数轮加密，$T_{\mathrm{R}}$异或轮数，参与偶数轮加密	动态9、11、17和23	$9\left\lfloor\frac{n}{192}\right\rfloor$	动态8、10、16和22

在明文及调整参数长度方面，FR-FPE 明文长度上限为 192 bit，与 FF3-1 和 TE-FPE 相同，主要面向身份证号、手机号、银行卡号等有限长度明文(均小于 192 bit)，较长的明文可采用多次 FPE 分组加密的方式实现。FR-FPE 调整参数长度上限为 96 bit，显著高于 FF3-1 和 TE-FPE 的 56 bit，当明文域规模较小时，安全性更高。

在安全性上，FF3-1 无法抵御参数滑动关联攻击和线性密码分析攻击，已被移出标准。FR-FPE 和 FF1 给出了算法伪随机置换安全性证明，TE-FPE 未给出公开的 PRP 证明。FR-FPE、FF1 和 TE-FPE 算法都能抵御线性密码分析和滑动关联攻击，其中 FR-FPE 给出了抵御线性密码分析和滑动关联攻击的定性、定量分析。

在调整参数加密方式上，FR-FPE 支持最长 96 bit 调整参数，并将其高位和低位字节同时参与 Feistel 所有轮次加密（高位字节以 CBC 模式，低位字节与轮数异或后再与明文拼接），保证了调整参数加密的伪随机置换性和对整体明文全局加密的关联性，安全性与 FF1 调整参数整体全局加密相当。TE-FPE 调整参数最长 56 bit，通过对其加密后截取为 $\frac{T_{\mathrm{L}}}{T_{\mathrm{R}}}$，分别参与 Feistel 奇偶轮的加密。

在分组加密算法调用次数和 Feistel 轮数方面，在明文长度不超过 192 bit 的范围内，与 FF1 相比，FR-FPE 的 Feistel 轮数同为固定的 10 轮，但分组加密调用次数仅为 11 次，少于 FF1 的至少 20 次，分组加密调用次数减少 45%（9 次）。在明文长度 n>192，调整参数长度为 96 bit 时，FR-FPE 分组加密次数为 $11\left\lceil\frac{n}{192}\right\rceil$ 次，FF1 为 $10\left(\left\lceil\frac{\frac{n}{2}-24}{128}\right\rceil+\left\lceil\frac{n+64}{256}\right\rceil\right)$，约等于 $10\left\lceil\frac{n+8}{128}\right\rceil$ 次。在不限明文长度时，FR-FPE 分组加密调用次数小于 FF1 的分组加密调用次数，FR-FPE 分组加密调用次数平均减少 27%。因此，在明文长度不超过 192 bit 和大于 192 bit 的情况下，FR-FPE 分组加密调用次数都低于 FF1，明文长度越小，优势越大，在保证与 FF1 相同安全强度的同时，大大提升了算法效率。TE-FPE 的 Feistel 轮数为动态 8、10、16 和 22 轮，分组加密调用次数为动态 9、11、17 和 23 次，结构复杂且不固定。

4　安全性分析

密码方案的安全性论证通常有两种模型：一是假设底层逻辑是理想的，在此基础上建立安全证明；二是在已知攻击条件下，论证算法的安全性。为此，本节首先假设 CIPH 函数是一个安全的 PRF，给出 FR-FPE 算法 SPRP 安全性证明；然后结合最新的 FPE 算法攻击技术，理论分析 FR-FPE 算法如何抵抗特定攻击。

4.1　算法伪随机置换安全性

分组密码函数 CIPH:$\mathcal{K}\times\{0,1\}^{128}\to\{0,1\}^{128}$ 使用标准的分组加密算法，因此函数 CIPH_K 是一个安全的 PRF。FR-FPE 算法轮数为 $r=10$，设 q 是攻击者 A 对其预言机的总查询次数，$m_{\min}$ 是在所有查询的格式 $N=(n,\cdots)$ 中，$\min(u,v)$ 的最小值（其中 $u=\left\lfloor\frac{n}{2}\right\rfloor, v=n-u$），$\mathrm{radix}_{\min}$ 是查询的最小基数。

定理 1　FR-FPE 的 SPRP 安全性。对于任何攻击者，对其预言机进行最多 q 次总查询的 SPRP 攻击者 A，存在攻击者 B_0,B_1 使

$$\mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{FR-FPE}}(\mathrm{A})\leqslant q\mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{CIPH}_K}(B_0)+10q\mathrm{Adv}^{\mathrm{PRF}}_{\mathrm{CIPH}_K}(B_1)+\frac{q^2}{2^{129}}+\epsilon\left(q,10,\mathrm{radix}^{m_{\min}}_{\min}\right)\quad(5)$$

其中，B_0 的运行时间与 A 相似，对 CIPH 及其逆函数进行最多 q 次查询；B_1 的运行时间与 A 相似，对 CIPH_K 进行最多 $10q$ 次查询。

证明　设 A 是针对 E=FR-FPE 的 SPRP 攻击者。证明过程通过定义一系列博弈来进行，从现实世界（博弈 G0）开始，到预言机是一个随机置换的理想世界（博弈 G4）结束，计算连续博弈之间攻击者成功概率的差值。

博弈 G0：这是真实的 SPRP 实验，选择一个密钥 $K\xleftarrow{\$}\mathcal{K}$，攻击者 A 与预言机 $\mathcal{O}_1(N,T,X)=E_{K,N,T}(\mathrm{X})$ 和 $\mathcal{O}_1^{-1}(N,T,Y)=D_{K,N,T}(Y)$ 交互。

$$\Pr\left[A^{\mathrm{G0}}\Rightarrow 1\right]=\Pr\left[\mathrm{SPRP}^1_{\mathrm{FR-FPE}}(A)\right]\quad(6)$$

博弈 G1：此博弈与博弈 G0 相同，只是计算 $F=\mathrm{CIPH}_K(P)$ 被替换为 $F=f(P)$，其中 f: $\{0,1\}^{128}\to\{0,1\}^{128}$ 是一个在博弈开始时选择的真正的随机函数。内部计算 $\mathrm{CIPH}_K(F\oplus Q)$ 仍然使用原始密钥 K 和分组密码算法 CIPH。

为了计算差值$\left|\Pr\left[A^{\mathrm{G0}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G1}}\Rightarrow 1\right]\right|$，本文构造一个对抗CIPH的SPRP攻击者$B_0$。$B_0$接收一个预言机$\mathcal{O}_{\mathrm{CIPH}}$的响应，$\mathcal{O}_{\mathrm{CIPH}}$是$\mathrm{CIPH}_K$及其逆函数（$B_0$的现实世界）或随机置换$\rho$及其逆函数（$B_0$的理想世界）二者中的一种。

当A发起查询时，B_0计算初始向量P并向预言机$\mathcal{O}_{\mathrm{CIPH}}$查询获得$F^*$，然后使用$F^*$为$A$模拟FR-FPE操作的其余部分。如果$\mathcal{O}_{\mathrm{CIPH}}$是$\mathrm{CIPH}_K$，则$A$处于博弈G0的环境中。如果$\mathcal{O}_{\mathrm{CIPH}}$是$\rho$，则$A$处于博弈G1的环境中。$B_0$在区分预言机方面的优势是$\left|\Pr\left[A^{\mathrm{G0}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G1}}\Rightarrow 1\right]\right|$，故

$$\left|\Pr\left[A^{\mathrm{G0}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G1}}\Rightarrow 1\right]\right|\leqslant \mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{CIPH}_K}\left(B_0\right) \tag{7}$$

此外，假设F^*值中没有发生碰撞，q_F是查询的不同输入P的数量（$q_F\leqslant q$），则$\mathcal{O}_{\mathrm{CIPH}}$输出中发生碰撞的概率$\Pr\left[\mathrm{Coll}_F\right]\leqslant\dfrac{q_F^2}{\left(2\cdot 2^{128}\right)}\leqslant\dfrac{q^2}{2^{129}}$。本文将此碰撞概率加入总界限中。

$$\left|\Pr\left[A^{\mathrm{G0}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G1}}\Rightarrow 1\right]\right|\leqslant q\mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{CIPH}_K}\left(B_0\right)+\frac{q^2}{2^{129}} \tag{8}$$

博弈G2：此博弈与博弈G1相同，只是计算$R=\mathrm{CIPH}_K\left(F\oplus Q\right)$时，$F=f(P)$被替换为$R=g\left(F\oplus Q\right)$，其中$g\colon\{0,1\}^{128}\rightarrow\{0,1\}^{128}$是独立的真正的随机函数。

为了计算差值$\left|\Pr\left[A^{\mathrm{G1}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G2}}\Rightarrow 1\right]\right|$，本文构造一个对抗CIPH的PRF攻击者$B_1$。$B_1$接收一个预言机$\mathcal{O}_{\mathrm{PRF}}$的响应，它要么是$\mathrm{CIPH}_K$，要么是一个真正的随机函数$g$。$B_1$为$A$模拟博弈G1或G2。当$A$发起查询时，$B_1$使用其自身的随机函数$f$计算$F=f(P)$，然后计算$F\oplus Q$发送给预言机$\mathcal{O}_{\mathrm{PRF}}$查询获得$R^*$。它使用$R^*$为$A$完成10轮Feistel模拟。如果$\mathcal{O}_{\mathrm{PRF}}$是$\mathrm{CIPH}_K$，则$A$处于博弈G1的环境中。如果$\mathcal{O}_{\mathrm{PRF}}$是$g$，则$A$处于博弈G2的环境中。$B_1$对其预言机总共进行了$10q$次查询。$B_1$在区分预言机方面的优势是$\left|\Pr\left[A^{\mathrm{G1}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G2}}\Rightarrow 1\right]\right|$，故

$$\left|\Pr\left[A^{\mathrm{G1}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G2}}\Rightarrow 1\right]\right|\leqslant(10q)\mathrm{Adv}^{\mathrm{PRF}}_{\mathrm{CIPH}_K}\left(B_1\right) \tag{9}$$

博弈G3：此博弈运行一个$r=10$轮非平衡Feistel网络，使用独立的随机函数f替代CIPH_K，预言机是$\mathcal{O}(N,T,X)=E^{\mathrm{ideal}}_{f,g,N,T}(X)$及其逆函数。此博弈在功能上与博弈G2相同。

$$\Pr\left[A^{\mathrm{G3}}\Rightarrow 1\right]=\Pr\left[A^{\mathrm{G2}}\Rightarrow 1\right] \tag{10}$$

博弈G4：此博弈将博弈G3中的理想Feistel置换$E^{\mathrm{ideal}}_{\mathrm{f},g,N,T}$及其逆函数替换为对于每个$(N,T)$独立的真正的随机置换$\pi_{N,T}$及其逆函数$\pi^{-1}_{N,T}$，定义为

$$\Pr\left[A^{\mathrm{G4}}\Rightarrow 1\right]=\Pr\left[\mathrm{SPRP}^0_{\mathrm{FR-FPE}}(A)\right] \tag{11}$$

$\left|\Pr\left[A^{\mathrm{G3}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G4}}\Rightarrow 1\right]\right|$为SPRP攻击者在区分一个理想Feistel密码（使用随机函数f和g）与一个真正的随机置换方面的最大优势差值。设此信息论优势为$\epsilon\left(q,10,N_{\mathrm{domain}}\right)$，其中$N_{\mathrm{domain}}\approx\mathrm{radix}^{m_{\min}}_{\min}$。Patarin[23]的研究结果表明，对于任意区分器发出的q次明密文查询，其与理想随机可调分组密码之间的区分优势可以被上界为$\epsilon\left(q,10,N\right)\leqslant O\left(\dfrac{q^2}{N^{10-2}}\right)$，在$\mathrm{radix}^{m_{\min}}_{\min}\geqslant 10^6$的情况下，$\epsilon$可忽略不计，故

$$\left|\Pr\left[A^{\mathrm{G3}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G4}}\Rightarrow 1\right]\right|\leqslant\epsilon\left(q,10,\mathrm{radix}^{m_{\min}}_{\min}\right)=\mathrm{negl}(k) \tag{12}$$

结论　使用三角不等式结合界限有

$$\begin{aligned}\mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{FR-FPE}}(A)&=\left|\Pr\left[A^{\mathrm{G0}}\Rightarrow 1\right]-\Pr\left[A^{\mathrm{G4}}\Rightarrow 1\right]\right|\leqslant\\&\left(q\mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{CIPH}_K}\left(B_0\right)+\frac{q^2}{2^{129}}\right)+\\&\left((10q)\mathrm{Adv}^{\mathrm{PRF}}_{\mathrm{CIPH}_K}\left(B_1\right)\right)+\mathrm{negl}(k)\leqslant\\&q\mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{CIPH}_K}\left(B_0\right)+10q\mathrm{Adv}^{\mathrm{PRF}}_{\mathrm{CIPH}_K}\left(B_1\right)+\frac{q^2}{2^{129}}\end{aligned} \tag{13}$$

若CIPH_K是一个安全的伪随机函数，对于任何进行q次查询的PPT敌手A，其PRF-CCA1优势$\mathrm{Adv}^{\mathrm{SPRP}}_{\mathrm{FR-FPE}}(A)$是可忽略的。故FR-FPE算法是安全的，其行为在计算上不可区分于一个真正的随机置换。证毕。

上述证明表明，只要底层分组密码算法CIPH_K是一个安全的SPRF，且操作的明文域大小$\mathrm{radix}^{m_{\min}}_{\min}\geqslant 10^6$，那么任何多项式时间的敌手区分FR-FPE与一个随机置换的优势是可忽略的。这为FR-FPE提供了一个基于计算复杂性理论的一般性安全保证。

4.2　抵抗攻击能力

本节分析FR-FPE对小域攻击、滑动关联攻击和线性密码分析攻击的抵抗能力。

1) 小域攻击抵抗能力

Feistel网络在小域下更容易被穷举或统计分析。此类攻击的必要条件是加密域$\text{radix}^{m_{\min}} < 10^6$。小域空间导致差分特征更易捕捉，且轮函数输出碰撞概率随域尺寸缩小呈指数级增长。攻击者可能通过收集少量密文或进行复杂度远低于穷举密钥的攻击来恢复明文。

FR-FPE通过10轮Feistel网络以及约定$\text{radix}^{m_{\min}} > 10^6$来抵抗小域攻击，条件$\text{radix}^{m_{\min}} > 10^6$（其中$m_{\min} = \min(u,v)$）确保了操作域足够大。对于10轮Feistel网络，依据文献[23]的Coefficients H技术分析结果，此域大小（大于100万）在10轮Feistel结构下区分该构造与真随机置换的优势非常小。由于$\text{radix}^{m_{\min}} > 10^6$的约束，针对小域的经典攻击，如穷举或完整置换表构建等攻击是不可行的。

2) 滑动关联攻击抵抗能力

滑动关联攻击试图寻找一对明文/密文(X,C)和(X',C')，使X'是X经过少量轮数加密的结果，C'是C经过相同少量轮数加密的结果，通过找到这样的“滑动对”，攻击者可以将对完整r轮密码的攻击问题转化为对$r-s$轮密码的攻击问题，其中s是滑动的轮数。滑动关联攻击的成功需要依赖两个条件：一是轮函数的输入具有对称性或周期性，允许攻击者通过调整输入（如Tweak）控制滑动偏移；二是存在可检测的滑动对，通常利用差分或线性特征进行统计识别。

FR-FPE算法结构破坏了滑动关联攻击的两个实施条件：一是FR-FPE采用基于CBC模式，将初始向量P分组加密后参与所有Feistel轮次的运算，使每轮的输入与全局参数强关联，破坏了轮函数输入的对称性与滑动偏移的可控性；二是FR-FPE将调整参数的高位和低位字节同时引入Feistel所有轮次（高位字节以CBC模式参与，低位字节与轮数异或后拼接明文）加密，从而将调整参数强关联至整个加密过程，增加滑动对构造和检测难度。

在FR-FPE中，第i轮轮函数等价于

$$F_i(x) = E_K(x \oplus E_K(P) \oplus g(T,i)) \tag{14}$$

其中，$E_K(P)$是固定但不可预测的全局随机量，$g(T,i)$是调整参数与轮数的混合编码，显式依赖轮数i。

对于任意两个轮次$i \neq j$，其轮函数输入满足

$$x \oplus E_K(P) \oplus g(T,i) \neq x' \oplus E_K(P) \oplus g(T,j) \tag{15}$$

由于FR-FPE中$g(T,i)$包含轮数与调整参数的混合编码，其在攻击者视角下等价于独立均匀分布的随机变量，因此滑动对不可构造的概率上界为

$$\Pr[\, g(T,i) = g(T,j) \,] \leqslant 2^{-32} \tag{16}$$

在10轮Feistel结构下，攻击者同时构造任意一组有效滑动对的成功概率至多为多项式的2^{-32}，在实际攻击模型下可忽略。

因此，FR-FPE的轮函数在代数层面上不存在轮间等价或周期性结构，滑动关联攻击所需的“轮函数同构性”条件被系统性破坏，FR-FPE能够抵御滑动关联攻击。

3) 线性密码分析攻击抵抗能力

线性密码分析攻击通过寻找明文、密文、密钥比特间的概率性线性关系来攻击密码算法。Beyne[11]对FF3-1的线性分析能够成功，核心在于其调整参数的分治使用方式，其调整参数左右两边分别独立地仅影响奇数和偶数轮。这使攻击者能够相对容易地构建跨越若干轮的、涉及特定Tweak比特的线性逼近路径。因此，FF3-1、FEA等FPE类算法的线性密码分析攻击依赖于两个条件：一是调整参数以明文固定模式参与轮函数，攻击者可利用其规律构建线性路径，如FF3-1和FEA中轮次间调整参数交替出现；二是加密明文域规模较小，单轮加密线性近似的偏差难以通过有限的轮数衰减。

FR-FPE算法结构破坏了线性密码分析攻击的两个实施条件：一是FR-FPE算法将调整参数高位字节以CBC模式全程关联所有轮加密，低位字节则与轮数异或后拼接明文再加密，打破了调整参数交替或固定参与轮函数的可预测条件，显著增加了构建线性路径的复杂度；二是FR-FPE算法约束最小明文域满足$\text{radix}^{m_{\min}} > 10^6$，并采用10轮Feistel结构，确保线性偏差在多轮迭代中充分衰减，无法形成有效的统计区分。在标准线性分析模型下，其概率性线性逼近关系为

$$\Pr[\, \langle \alpha, X \rangle \oplus \langle \beta, F(X) \rangle = 0 \,] = \frac{1}{2} + \varepsilon \tag{17}$$

其中，X为明文，α为明文侧线性掩码，$F(X)$为第10轮加密后的密文，β为密文侧线性掩码，ε为线性逼近偏差。

在FR-FPE中，每轮轮函数等价为

$$F_i(x)=E_K\left(x\oplus E_K(P)\oplus g(T,i)\right)=E_K(x\oplus R_i) \tag{18}$$

其中，$R_i=E_K(P)\oplus g(T,i)$，在攻击者视角下，R_i为未知常量，因此F_i等价于一个独立PRF。

基于Piling-up原理[24]，总体线性偏差衰减为$\varepsilon_{\text{total}}\leqslant(2\varepsilon)^r$，在FR-FPE算法中，单轮最大偏差$\varepsilon\leqslant 2^{-32}$，在轮数$r=10$的情况下，总体线性偏差$\varepsilon_{\text{total}}\leqslant 2^{-310}$，远低于可利用阈值。因此，FR-FPE能够有效抵御线性密码分析攻击。

5　实验及性能分析

本文选取NIST标准FF1算法以及中国密码行业标准化技术委员会GM_Y 5007-2024研究报告中的TE-FPE算法与FR-FPE算法进行性能对比分析，底层分组加密算法均采用国密SM4算法。测试数据集为radix=36的数字及英文字母混合数据集，明文长度≤192 bit。一个简单的保留格式加密示例如表2所示，对36字符（比特长度为36lb radix≈187 bit）的明文（数字及英文字母混合）加密，得到相同格式相同长度的密文。

表2　保留格式加密示例

参数项	取值	说明
调整参数	aabbccddeeff001122334455	96 bit调整参数
明文长度	36字符（约187 bit）	187 bit
明文	6B17FR23BN1901UY00 13PT238F3DF9F8H5R8	36字符明文
密文	7T9S2K8F4D1G0H3J6L5Z 7X2C9V8B4N60Q2W5	36字符密文

实验的硬件平台如下：Intel Core i5-1135G7处理器@ 2.40 GHz，16 GB DDR4内存。算法软件使用C语言实现，通过GCC9.4.0编译并启用-O2优化等级，底层分组密码函数SM4国密算法库GMSSL。运行环境为Ubuntu 20.04 LTS系统。测试方法：加密操作每次测试运行100 000次，取90 000次的平均耗时（排除冷启动影响），最终结果取10轮测试的平均数。实验结果如图3所示。

在radix=36的数字及字母混合数据集下，3种算法的每秒加密次数对比如表3所示，加密数据吞吐率对比如表4所示。FR-FPE的每秒加密次数比FF1平均高26.55%，加密数据吞吐率平均高21.25%。

```
====================== 实验环境配置 ========================
硬件平台: Intel Core i5-1135G7 (2.40GHz/4核) | 内存: 16GB DDR4 3200MHz
软件环境: Ubuntu 20.04 LTS | GCC 9.4.0 |  国密GMSSL开源库
测试规则: 每轮执行90000次加密操作，共测试10轮
======================== FR-FPE算法性能测试=========================
--------------------------------------------------------------------------
明文长度 | 10轮测试耗时 (秒)              | 平均耗时(秒) | 平均每秒加密(次)
--------------------------------------------------------------------------
4字符    | 1.184 1.160 1.172 1.172 1.184
         | 1.184 1.160 1.184 1.196 1.243  | 1.184        | 76033
8字符    | 1.768 1.841 1.823 1.768 1.786
         | 1.841 1.841 1.841 1.841 1.696  | 1.804        | 49876
16字符   | 3.350 3.383 3.317 3.284 3.350
         | 3.383 3.284 3.350 3.317 3.151  | 3.317        | 27132
36字符   | 7.865 7.631 7.865 7.787 7.709
         | 7.631 7.631 7.631 7.709 8.410  | 7.787        | 11558
======================== FF1算法性能测试=========================
--------------------------------------------------------------------------
明文长度 | 10轮测试耗时 (秒)              | 平均耗时(秒) | 平均每秒加密(次)
--------------------------------------------------------------------------
4字符    | 1.592 1.592 1.530 1.530 1.530
         | 1.545 1.545 1.576 1.561 1.608  | 1.561        | 57662
8字符    | 1.485 1.455 1.470 1.455 1.500
         | 1.500 1.515 1.470 1.500 1.500  | 1.485        | 60605
16字符   | 2.583 2.635 2.635 2.558 2.532
         | 2.532 2.583 2.609 2.532 2.635  | 2.583        | 34837
36字符   | 6.278 6.278 6.278 6.215 6.278
         | 6.278 6.405 6.278 6.215 6.912  | 6.342        | 14192
======================== TE-FPE算法性能测试=========================
--------------------------------------------------------------------------
明文长度 | 10轮测试耗时 (秒)              | 平均耗时(秒) | 平均每秒加密(次)
--------------------------------------------------------------------------
4字符    | 1.729 1.678 1.695 1.712 1.695
         | 1.678 1.695 1.661 1.712 1.695  | 1.695        | 53105
8字符    | 2.210 2.233 2.188 2.210 2.188
         | 2.277 2.233 2.233 2.188 2.367  | 2.233        | 40311
16字符   | 3.549 3.443 3.478 3.549 3.478
         | 3.478 3.513 3.549 3.443 3.654  | 3.513        | 25616
36字符   | 8.077 8.158 7.995 8.077 7.995
         | 8.321 8.158 8.158 7.995 8.648  | 8.158        | 11032
```

图3　3种算法加密速度测试数据

这得益于FR-FPE的分组加密调用次数比FF1减少45%。与TE-FPE相比，在明文小于8字符（约42 bit）时，FR-FPE的每秒加密次数平均高8.54%，加密数据吞吐率平均高6.44%。在明文大于8字符（约42 bit）时，FR-FPE的每秒加密次数平均低17.7%，加密数据吞吐率平均低15.3%。在长明文（8个数字以上）情况下，FR-FPE的Feistel结构比TE-FPE多两轮，因此性能降低，但安全性更高。FR-FPE采用与美国NIST FF1相同的固定10轮Feistel结构设计，在支持算法轻量确定性结构高效实现的前提下，能够保证算法同时满足短明文加密的安全性和长明文加密的高性能。

表3　　3种算法每秒加密次数对比

算法	每秒加密次数/次			
	4字符（约21 bit）	8字符（约42 bit）	16字符（约83 bit）	36字符（约187 bit）
FR-FPE	76 033	49 876	27 132	11 558
TE-FPE	57 662	60 605	34 837	14 192
FF1	53 105	40 311	25 616	11 032

表4　　3种算法加密数据吞吐率对比

算法	加密数据吞吐率/(Mbit·s^{-1})			
	4字符（约21 bit）	8字符（约42 bit）	16字符（约83 bit）	36字符（约187 bit）
FR-FPE	3.09	4.18	4.61	5.12
TE-FPE	2.08	4.75	5.51	5.98
FF1	2.08	3.23	4.06	4.65

6　结束语

针对现有保留格式加密算法标准难以应对滑动关联及线性密码分析攻击、算法效率不高的问题，本文提出了FR-FPE算法，支持对不超过192 bit的明文和不超过96 bit的调整参数进行加密。算法通过基于CBC模式的参数向量加密机制和结构化调整参数全关联加密模型，有效抵御滑动关联及线性密码分析攻击。通过轻量化确定性加密结构，有效减少算法底层分组加密的次数。基于Game-Hopping博弈模型，本文证明了FR-FPE算法具有SPRP安全性。实验结果表明，针对radix=36的数字字母混合数据集，FR-FPE的每秒加密次数比FF1平均高26.55%，加密数据吞吐率平均高21.25%。

参考文献：

[1] National Bureau of Standards. FIPS PUB 74, guidelines for implementing and using the DES data encryption standard[S]. 1981.

[2] Black J, Rogaway P. Ciphers with arbitrary finite domains[C]//Topics in Cryptology-CT-RSA 2002. Berlin: Springer, 2002: 114-130.

[3] Dworkin M. NIST SP 800-38G, recommendation for block cipher modes of operation: methods for format-preserving encryption[S]. 2013.

[4] ANSI X9.124-1-2023. Symmetric key cryptography for the financial services industry format preserving encryption - Part 1: definitions and mode[S]. 2023.

[5] Lee J K, Koo B, Roh D, et al. Format-preserving encryption algorithms using families of tweakable blockciphers[C]//Information Security and Cryptology - ICISC 2014. Berlin: Springer, 2015: 132-159.

[6] Jang W, Lee S Y. Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment[J]. International Journal of Distributed Sensor Networks, 2020, 16(3): 155014772091477.

[7] Kim D, Kim H, Jang K, et al. Deep-learning-based neural distinguisher for format-preserving encryption schemes FF1 and FF3[J]. Electronics, 2024, 13(7): 1196.

[8] Majeed M A, Sulaiman R, Shukur Z. New text steganography technique based on part-of-speech tagging and format-preserving encryption[J]. KSII Transactions on Internet and Information Systems, 2024, 18: 170-191.

[9] Vidhya S. Enhancing cloud security for structured data: an AES-GCM based format-preserving encryption approach[C]//Artificial Intelligence Based Smart and Secured Applications. Berlin: Springer, 2025: 196-205.

[10] Amon O, Dunkelman O, Keller N, et al. Three third generation attacks on the format preserving encryption scheme FF3[C]//Advances in Cryptology - EUROCRYPT 2021. Berlin: Springer, 2021: 127-154.

[11] Beyne T. Linear cryptanalysis of FF3-1 and FEA[C]//Advances in Cryptology - CRYPTO 2021. Berlin: Springer, 2021: 41-69.

[12] Spies T. Format preserving encryption[R]. 2008.

[13] Bellare M, Rogaway P, Spies T. The FFX mode of operation for format-preserving encryption [R]. Unpublished NIST Proposal, 2010.

[14] Liskov M, Rivest R L, Wagner D. Tweakable block ciphers[C]//Advances in Cryptology - CRYPTO 2002. Berlin: Springer, 2002: 31-46.

[15] 李经纬, 贾春福, 刘哲理, 等. 基于k-分割Feistel网络的FPE方案[J]. 通信学报, 2012, 33(4): 62-68.
Li J W, Jia C F, Liu Z L, et al. FPE scheme based on k-splits Feistel network[J]. Journal on Communications, 2012, 33(4): 62-68.

[16] Bellare M, Hoang V T, Tessaro S. Message-recovery attacks on feistel-based format preserving encryption[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 444-455.

[17] Durak F B, Vaudenay S. Breaking the FF3 format-preserving encryption standard over small domains[C]//Advances in Cryptology-CRYPTO 2017. Berlin: Springer, 2017: 679-707.

[18] 刘哲理, 贾春福, 李经纬. 保留格式加密技术研究[J]. 软件学报, 2012, 23(1): 152-170.
Liu Z L, Jia C F, Li J W. Research on the format-preserving encryption techniques[J]. Journal of Software, 2012, 23(1): 152-170.

[19] Bellare M, Ristenpart T, Rogaway P, et al. Format-preserving encryption[C]//Selected Areas in Cryptography. Berlin: Springer, 2009:

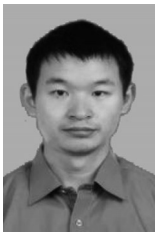
295-312.
[20] Hoang V T, Miller D, Trieu N. Attacks only get better: how to break FF3 on large domains[C]//Advances in Cryptology - EUROCRYPT 2019. Berlin: Springer, 2019: 85-116.
[21] Hoang V T, Tessaro S, Trieu N. The curse of small domains: new attacks on format-preserving encryption[C]//Advances in Cryptology-CRYPTO 2018. Berlin: Springer, 2018: 221-251.
[22] Biryukov A, Wagner D. Slide attacks[C]//Fast Software Encryption: 6th International Workshop, FSE'99. Berlin: Springer, 1999: 245-259.
[23] Patarin J. Security of random feistel schemes with 5 or more rounds[C]//Advances in Cryptology-CRYPTO 2004. Berlin: Springer, 2004: 106-122.
[24] Matsui M. Linear cryptanalysis method for DES cipher[C]//Advances in Cryptology - EUROCRYPT'93. Berlin: Springer, 1994: 386-397.

[作者简介]

王小峰（1982– ），男，江苏南通人，博士，国防科技大学研究员，主要研究方向为密码学、网络信任安全、智能数据安全。

叶军（1985– ），男，湖南长沙人，湖南安方信息技术有限公司高级工程师，主要研究方向为无线网络安全和数据安全。

刘文正（1991– ），男，湖南浏阳人，博士，长沙理工大学副教授、硕士生导师，主要研究方向为人工智能和大数据安全。



孙兵（1981– ），男，江苏如皋人，博士，国防科技大学教授、博士生导师，主要研究方向为对称密码算法设计、密码安全分析。

吴华晖（1979– ），男，湖南邵阳人，湖南省农村信用社联合社工程师，主要研究方向为金融数字化转型、数据治理体系建设、数据安全应用。

郭佳朴（1993– ），男，河南许昌人，国防科技大学工程师，主要研究方向为网络安全、公钥密码和网络身份认证。