基于 *k*-分割 Feistel 网络的 FPE 方案

李经纬[1,2]，贾春福[1,2]，刘哲理[1,2]，李敏[1,2]

（1. 南开大学 信息技术科学学院，天津 300071；2. 福建师范大学 网络安全与密码技术重点实验室，福建 福州 350007）

摘 要：基于对保留格式加密(FPE, format-preserving encryption)方案中 Feistel 网络构造特点的分析，针对当前使用 2-分割 Feistel 网络构造的 FPE 密码分组长度范围较小的问题，提出基于 *k*-分割 type-2 Feistel 网络的 FPE 方案，以适应各种长度数据的加密需求。通过实验验证，type-2 Feistel 网络可以使用较小规模伪随机函数构造各种分组长度密码，具有广泛实用性。

关键词：保留格式加密；Feistel 网络；type-2 Feistel 网络

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2012)04-0062-07

FPE scheme based on *k*-splits Feistel network

LI Jing-wei[1,2], JIA Chun-fu[1,2], LIU Zhe-li[1,2], LI Min[1,2]

(1. College of Information Technical Science, Nankai University, Tianjin 300071, China;

2. Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

Abstract: The construction features and discipline of Feistel network-based FPE (format-preserving encryption) schemes were analyzed. Considering on the problem that 2-splits Feistel networks-based FPE cipher's block size was in narrow range, a type-2 Feistel network-based FPE scheme, which was suitable for constructing FPE cipher with scalable block size, was presented. Experiment show that type-2 Feistel network is able to use small-scaled pseudorandom function to construct cipher with scalable block size and that is practical.

Key words: format-preserving encryption; Feistel network; type-2 Feistel network

1 引言

保留格式加密(FPE, format-preserving encryption)[1]是一种新型加密技术，通过将某种特定格式的明文加密为与其具有相同格式的密文，使现有数据库中数据的加解密，既不需要改动应用系统，也不需要改动数据库结构。此外，FPE还可应用于数据遮蔽[2]、网络数据安全[3]和格式依赖加密[4]等领域。

国外已取得一些 FPE 相关理论研究成果[5~9]。其中，文献[5]关注整数集上的 FPE 问题，提出 generalized-Feistel 方法，该方法首次将 Feistel 网络引入到 FPE 方案构建。其后 FPE 方案 FFSEM[6]、FFX[7,8]、BPS[9]等都延续这一思想，采用各种类型

收稿日期：2011-06-22；**修回日期**：2011-12-05

基金项目：国家自然科学基金资助项目（60973141）；天津市自然科学基金资助项目（09JCYBJ00300）；高等学校博士学科点专项科研基金资助项目（20100031110030）；网络安全与密码技术福建省高校重点实验室开放课题基金资助项目（2011004）；中央高校基本科研业务费专项基金资助项目

Foundation Items: The National Natural Science Foundation of China (60973141); The Natural Science Foundation of Tianjin (09JCYBJ00300); The Specialized Research Fund for the Doctoral Program of Higher Education of China (20100031110030); Funds of Key Lab of Fujian Province University Network Security and Cryptology (2011004); The Fundamental Research Funds for the Central Universities

表 1　Feistel 网络在典型 FPE 方案中的应用情况

FPE 方案	处理的消息空间	采用的 Feistel 网络类型	伪随机函数构造方法	轮次数 r
Generalized-Feistel[5]	整数集 $\mathbb{Z}_n$	交互式 Feistel 网络的数值形式	假设 PRF 是随机函数	$r=3$
FFSEM[6]	整数集 $\mathbb{Z}_n$	平衡 Feistel 网络	基于 AES 的方案	未讨论
Integer FPE[3]	整数集 $\mathbb{Z}_n$	非平衡 Feistel 网络的数值形式 交互式 Feistel 网络的数值形式	基于 CBC-MAC 的方案	未讨论
FFX[7,8]	定长字符串集合 $chars^n$	非平衡 Feistel 网络 交互式 Feistel 网络	基于 CBC-MAC 的方案	1) 当 $n\geqslant 10$ 时，$r=12$； 2) 当 $n\in\{6,7,8,9\}$ 时，$r=18$； 3) 当 $n\in\{4,5\}$ 时，$r=24$
BPS[9]	定长字符串集合 $chars^n$	交互式 Feistel 网络	基于 HMAC 的方案	$r=8$

2-分割 Feistel 网络。

目前，处理 $chars^n$ 上的 FPE 问题即意味着构造分组长度为 n 的 FPE 密码(尽管文献[9]提出 BPS 方案的 CBC 模式，但未给出相关安全性分析)。然而当前 2-分割 Feistel 网络，在 n 相当大时，使用的伪随机函数输入和输出宽度也相当大，设计和实现一个大规模伪随机函数通常是困难的[10]。

作者已在文献[11]中对已有 FPE 模型进行了分析，提出 FPE 方案设计框架，将任意问题域的 FPE 方案构造转移为编码方案设计和整数 FPE 算法设计。本文在此基础上，关注当前 FPE 方案中各种类型 Feistel 网络的适用性，针对使用 2-分割 Feistel 网络构造的 FPE 密码分组长度适应范围较小的问题，提出基于 *k*-分割 type-2 Feistel 网络的 FPE 方案，以满足各种长度数据的加密需求。该方案结合 cycle-walking[5]可以解决任意整数集上的 FPE 问题。最后通过实验发现和分析各种 Feistel 网络达到雪崩准则所需轮次数和时间开销，以验证 type-2 Feistel 网络可以使用较小规模伪随机函数构造各种分组长度密码。

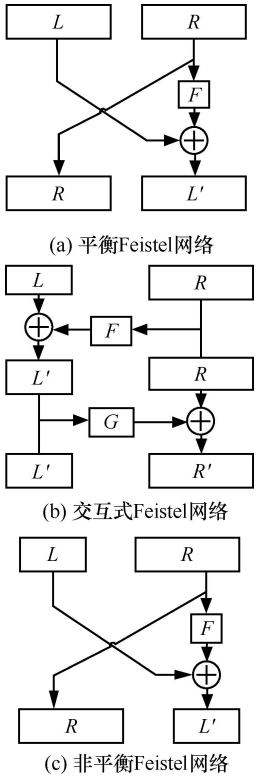

图 1　2-分割 Feistel 网络

2　Feistel 网络在 FPE 中的应用分析

目前已提出的 FPE 方案多数使用 Feistel 网络，表 1 总结了 Feistel 网络在典型 FPE 方案中应用情况，考虑的主要要素包括：Feistel 网络类型、伪随机函数构造方法和轮次数等。

由表 1 可知如下内容。

1) 当前 FPE 方案均采用 2-分割 Feistel 网络，包括平衡 Feistel 网络、非平衡 Feistel 网络、交互式 Feistel 网络以及它们的数值形式。2-分割 Feistel 网络都将输入等长或不等长地划分为 L 和 R 这 2 部分，然后使用伪随机函数分别执行如图 1 所示的轮运算，以形成下一轮输入。

2) Feistel 网络的效率主要取决于伪随机函数。当前使用 Feistel 网络的 FPE 方案中，伪随机函数构造方法包括基于伪随机置换的构造方案[6]和基于消息认证码的构造方案[3,7,9]，其本质都是填充原输入，通过伪随机置换或消息认证码作用，形成函数输出[12]。

3) 在采用安全伪随机函数的情况下，Feistel 网络安全性与轮次数相关。文献[13~15]证明至少 6 轮运算才能保证 Feistel 网络在各种攻击模型(已知明文攻击、自适应选择明文攻击和自适应选择明文密文攻击)下的安全性。文献[16]进一步分析一般 Feistel

网络(包括平衡、非平衡、交互式和 type-1, 2, 3 Feistel 网络)超越生日边界的安全性，证明执行足够多轮运算后，一般 Feistel 网络在选择密文攻击下，能够抵抗 $2^{m(1-\varepsilon)}$ 次恶意查询(这里 m 为一般 Feistel 网络使用的伪随机函数输入宽度，ε 为大于 0 的极小数)。

3　基于 *k*-分割 Feistel 网络的 FPE 方案

针对 2-分割 Feistel 网络构造的 FPE 密码分组长度适应范围较小的问题，构造基于 *k*-分割 Feistel 网络的整数 FPE 方案(这里以 4-分割为例，如果输入宽度很大，可考虑增加子分组数目)。该方案还可进一步扩展，结合文献[11]或 rank-then-encipher 方法[3]解决复杂问题域(如正则语言等)中的 FPE 问题。

3.1　*k*-分割 Feistel 网络

k-分割 Feistel 网络包括 type-1、type-2 和 type-3，通过将输入比特串等分为 k 个子分组，能够有效避免大宽度伪随机函数设计和实现的困难，已被广泛应用于各种分组密码的构造，例如 CAST-256(type-1)、RC6(type-2)和 MARS(type-3)等。其每一轮工作原理如图 2 所示。

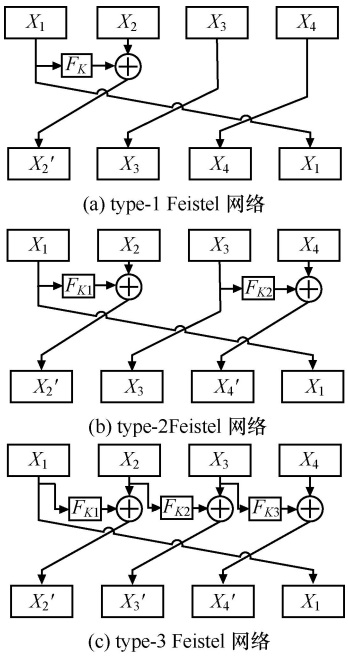

图 2　*k*-分割 Feistel 网络($k = 4$ 的情况)

1) Type-1 Feistel 网络执行 $X_2' = F_K(X_1) \oplus X_2$，连接 $X_2' \| X_3 \| X_4 \| X_1$ 作为下一轮迭代输入。

2) Type-2 Feistel 网络执行 $X_2' = F_{K1}(X_1) \oplus X_2$ 和 $X_4' = F_{K2}(X_3) \oplus X_4$，连接 $X_2' \| X_3 \| X_4' \| X_1$ 作为下一轮迭代输入。

3) Type-3 Feistel 网络执行 $X_2' = F_{K1}(X_1) \oplus X_2$，$X_3' = F_{K2}(X_2) \oplus X_3$ 和 $X_4' = F_{K3}(X_3) \oplus X_4$，连接 $X_2' \| X_3' \| X_4' \| X_1$ 作为下一轮迭代输入。

3.2　基于 type-2 Feistel 网络的整数 FPE 方案

在 *k*-分割 Feistel 网络中，type-2 具有安全和效率的最佳平衡：①扩散性方面，type-2 只需较少轮次即可达到与 type-1 相当的安全性，而 type-3 每一轮运算需调用更多次伪随机函数，计算复杂性较高[17]；②雪崩效应方面，虽然 type-2 满足雪崩准则所需 Feistel 轮次数略大于 type-3，但在调用伪随机函数次数上，type-2 大约只是 type-3 的一半[18]。

因此，试图设计基于 type-2 Feistel 网络的整数 FPE 方案，描述如下。

系统初始化 setup：初始化系统参数，包括：①基于 type-2 Feistel 网络的加密算法所需参数，如轮次数 r、伪随机函数 F 和子分组数目 k 等；②待解决问题域 $\mathbb{Z}_n = \{0,1,\cdots,n-1\}$；③密钥 $K = (K_1, K_2)$。

加密过程 encrypt：输入明文整数 M，执行 type-2 Feistel 网络加密过程。图 3 描述了 $k = 4$ 时使用 type-2 Feistel 网络加密的 Enc_Feistel 算法。

```
Algorithm Enc_Feistel
输入: 密钥: K = (K1, K2); 整数: X;
      Feistel 轮次数: r; 子分组数目 k;
输出: 整数: Y;
          X_bin ← CodeBin(X);
          (X_1^0, X_2^0, X_3^0, X_4^0) ← Split(X_bin, k);
          for i ← 0 to r − 1 do
X_1^{i+1} ← F_{K_1}(X_1^i, i) ⊕ X_2^i;
X_2^{i+1} ← X_3^i;
X_3^{i+1} ← F_{K_2}(X_3^i, i) ⊕ X_4^i;
X_4^{i+1} ← X_1^i;
          end
          Y ← CodeDec(X_1^r || X_2^r || X_3^r || X_4^r);
return Y
```

图 3　Enc_Feistel 算法

Enc_Feistel 算法将输入整数 X 表示为二进制形式 X_{bin}，并均匀分割为 X_1^0、X_2^0、X_3^0 和 X_4^0，如果 $|X_{\text{bin}}|$ 位数不足，则以 0 填充，然后执行 r 轮运算，以加密二进制串 $X_1^0 \| X_2^0 \| X_3^0 \| X_4^0$，最后返回 $X_1^r \| X_2^r \| X_3^r \| X_4^r$ 的十进制形式作为算法输出。

单纯 Feistel 网络只适用于加密二进制符号串，可通过结合 cycle-walking 方法确保二进制输出最终

落在指定整数集内，以解决任意整数集上的 FPE 问题。结合 cycle-walking 的整个加密过程如图 4 所示。

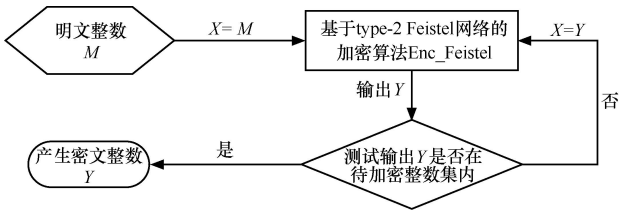

图 4　基于 type-2 Feistel 网络的整数 FPE 方案

解密过程 decrypt：类似于 encrypt，将整数密文 Y 编码为二进制数后，进行基于 type-2 Feistel 网络的解密，并结合 cycle-walking，直到有合法明文输出为止。

3.3　伪随机函数构造

Type-2 Feistel 网络的效率主要取决于采用的伪随机函数，设计安全高效的伪随机函数是构造基于 type-2 Feistel 网络 FPE 密码的关键。上节提出的 FPE 方案将采用截断伪随机置换输出的方式构造伪随机函数。

如图 5 所示，在采用截断伪随机置换的构造方式中，首先将输入串 X 和调整因子 t 填充为适应伪随机置换分组长度的二进制向量 *Vector*，不足分组长度时以 0 填充，然后基于密钥 K 使用伪随机置换加密 *Vector*（这里 i=1 或 2），最后根据所需位数截断加密结果。

Algorithm F

输入: 密钥: K; 二进制串: X;

　　调整因子: t; 所采用伪随机置换的分组长度: l

输出: 二进制串: Y

　　$t_{\text{bin}} \leftarrow \text{CodeBin}(t)$;

　　$Vector_{\text{bin}}[0\cdots|X|-1] \leftarrow X$;

　　$Vector_{\text{bin}}[|X|\cdots|X|+|t_{\text{bin}}|-1] \leftarrow t_{\text{bin}}$;

　　$Vector_{\text{bin}}[|X|+|t_{\text{bin}}|\cdots l-1] \leftarrow 0$;

　　return $Y = \text{PRP}_K(Vector_{\text{bin}})$ & $2^{|X|}-1$

图 5　伪随机函数构造算法

需要指出的是：①在伪随机函数构造中引入调整因子，以保证每一轮使用的伪随机函数不同(如图 5 所示，可将当前轮次数作为伪随机函数调整因子输入)；②采用的伪随机置换 PRP 可以是任意安全的对称分组密码(例如 DES、AES 等)，但 PRP 分组长度必须不小于伪随机函数输入输出规模，如果待构造的伪随机函数输入输出规模超过一个 PRP 分组长度，只能通过增加 type-2 Feistel 网络子分组个数，将大规模伪随机函数的构造分散为构造多个小规模伪随机函数。

3.4　安全性分析

2002 年，Black 和 Rogaway[5]首次提出保留格式加密标准安全目标，即伪随机置换安全。FPE 本质是特定消息空间内的伪随机置换。

2011 年，文献[19]总结保留格式加密的相关攻击模型和安全目标，指出 FPE 是一种特殊的对称密码，其安全性归约为采用基础模块的安全性。

本文提出的 FPE 方案基础模块包括：①type-2 Feistel 网络，用于构造分组长度略大于 log$n$ 的分组密码(这里 n 为待加密消息空间大小)；②cycle-walking，用于保证分组密码最终输出在可接受范围内。鉴于文献[16]对 type-2 Feistel 网络超越生日边界安全性的结论以及文献[5]和文献[3]关于 cycle-walking 不会降低密码安全性的分析，因此，基于 type-2 Feistel 网络构建的整数 FPE 方案是安全的。

3.5　效率分析

Type-2 Feistel 网络每一轮加密的时间消耗包括：①将输入划分成 k 个长度为 m 位子分组的时间 t_{split}(不失一般性，这里始终假设 $k=4$)；②伪随机函数作用子分组的时间 t_{compute}；③连接各子分组形成下一轮输入或最终密文的时间 t_{joint}。如果采用的轮次数为 r，则 type-2 Feistel 网络加密总耗时 $T_{\text{Feistel}} = t_{\text{split}} + 2rt_{\text{compute}} + t_{\text{joint}}$。

为确保 type-2 Feistel 网络加密结果最终输出在可接受范围内，需结合 cycle-walking 方法。其中，每次迭代结果属于指定整数集的概率与该整数集大小和基于 type-2 Feistel 网络的密码分组长度相关。

如果待加密消息空间为 $\mathbb{Z}_n$，所采用密码分组长度为 N。假设 type-2 Feistel 网络构造的密码为理想分组密码(即对任意明文加密，其密文为消息空间任意点的概率都相同)，那么每一次迭代输出结果落入 $\mathbb{Z}_n$ 的概率约为 $p = \dfrac{n}{2^N}$。

通常情况下，为使概率值 p 尽可能大，可根据待加密消息空间大小构造合适宽度的 Feistel 网络。此时 type-2 Feistel 网络的宽度应为不小于 $\log n$ 且能被 k 整除的整数，因此各子分组宽度为 $\dfrac{\log n}{k}$，整个 type-2 Feistel 网络宽度 $N = k\dfrac{\log n}{k}$ (这里 x

表示不小于 x 的最小整数)。

需要指出的是，虽然能够通过构造合适宽度的 Feistel 网络，在一定程度上降低迭代次数，但是，由于每一次迭代输出结果落入 $\mathbb{Z}_n$ 的概率为 $p=\frac{n}{2^N}=\frac{n}{2^{k\frac{\log n}{k}}}$，因此，应在伪随机函数构造许可的情况下，尽可能使用较少子分组数目；$n=2^{sk}+1(s=1,2,\cdots)$ 是方案最坏情况，此时每次迭代输出属于 $\mathbb{Z}_n$ 的近似概率为 $p_{\text{worst}}=\frac{2^{sk}+1}{2^{k\frac{sk+1}{k}}}=\frac{2^{sk}+1}{2^{k(s+1)}}\approx\frac{1}{2^k}$。

根据以上分析，应用所提方案处理 $\mathbb{Z}_n$ 上的 FPE 问题，在 n 略大于 2^{sk} 时，效率较低。事实上，目前基于 Feistel 网络的整数 FPE 方案均存在上述缺陷，在任意整数集上探索无需结合 cycle-walking 的高效 FPE 方案仍为开放性问题。

4 实验

以雪崩准则作为加密算法实际安全性指标，对比分析各种分组长度下，type-2 Feistel 网络与当前 FPE 方案中其他 Feistel 网络达到雪崩准则所需 Feistel 轮次数和时间开销。

4.1 雪崩准则

分组密码设计目的在于通过提供足够混淆和扩散特性，以抵抗对手针对密码体制的统计分析。混淆和扩散对密文的影响可用雪崩准则衡量：如果一种密码满足雪崩准则，那么在任何时候，改变其输入比特串中某一位，将会致使至少一半输出比特发生改变[20]，其数学定义如下。

定义 1 E 为分组长度为 N 的分组密码，如果对于任意密钥 K 和明文 $X_1\neq X_2$ 但 $|X_1|=|X_2|$，都有

$$\text{Exp}(\text{dist}(E_K(X_1),E_K(X_2))\,|\,\text{dist}(X_1,X_2)=1)\geqslant\frac{N}{2}$$

成立，那么 E 满足雪崩准则。这里，dist(·,·) 为汉明距离，Exp(·) 为期望。

4.2 达到雪崩准则的 Feistel 网络轮次数分析

实验环境为：CPU 为 Intel(R) Core 2 Quad，主频 2.66GHz，内存 3GB。测试的分组长度为 128~512bit，并规定：①对于每种分组长度，随机产生密钥及该分组长度下的明文 A、B，这里 A、B 仅有一个比特不同；②采用 AES 作为基础分组密码构造伪随机函数。当伪随机函数规模要求小于 128bit 时，直接截断密文作为函数输出；当伪随机函数规模要求大于 128bit 时，这种构造是困难的，这里通过截断 AES-CBC 的密文来近似伪随机函数；③分别使用 FFSEM(对应平衡 Feistel 网络)、FFX-1(对应非平衡 Feistel 网络)、FFX-2(对应交互式 Feistel 网络)和 type-2 Feistel 网络对 A 和 B 进行加密，若存在 100 轮以内运算使该类型 Feistel 网络达到雪崩准则，表明成功，否则认为失败。

针对每种分组长度和 Feistel 网络类型，进行了 100 次测试，并对成功达到雪崩准则所需的平均轮次数以及成功次数进行统计，实验数据如表 2 所示。

表 2 Feistel 网络成功达到雪崩准则时平均轮次数

分组长度/bit	FFSEM	FFX-1(3:2)	FFX-2(3:2)	type-2
128	3.91 / 100	3.80 / 100	4.05 / 100	6.30 / 100
160	4.02 / 100	4.03 / 100	4.27 / 100	6.32 / 100
192	3.97 / 99	3.99 / 99	4.13 / 99	6.83 / 99
224	4.05 / 98	93.35 / 51	— / 0	6.31 / 100
256	3.73 / 100	50.06 / 100	— / 0	6.39 / 100
288	4.22 / 9	23.64 / 100	— / 0	6.17 / 100
320	4.11 / 18	7.83 / 100	— / 0	6.29 / 100
352	4.77 / 26	5.75 / 100	4.31 / 26	6.23 / 100
384	3.71 / 38	5.86 / 100	3.88 / 42	6.21 / 100
416	4.68 / 37	5.66 / 99	3.89 / 37	5.94 / 99
448	3.51 / 49	6.02 / 100	— / 0	6.05 / 100
480	3.88 / 50	6.65 / 100	— / 0	6.35 / 100
512	3.94 / 49	6.13 / 100	— / 0	5.99 / 100

注：表中 x/y 表示 100 组测试样例中，有 y 组在 100 轮内达到雪崩准则，其平均所需轮次为 x。

由表 2 可知如下内容。

1) FFSEM 的平衡 Feistel 网络在 128~256bit 分组长度范围内，只需较少轮次数，然而分组长度超过 256bit 时，需构造 128bit 以上的伪随机函数，此时采用的截断 AES-CBC 密文方式，达成的效果明显不如基于 AES 的截断方法，因此造成失败次数增加。但随分组长度继续增加，成功次数略有回升，说明采用 AES-CBC 密文截断方式构造的近似伪随机函数，随着单个分组长度范围内构造的函数规模的增加，随机性也会缓慢提升，但仍达不到要求。

2) FFX-1 的非平衡 Feistel 网络(这里采用 3:2 非

平衡划分)在 128~192bit 分组长度范围内，采用直接截断 AES 的方式构造伪随机函数，较少轮次即可达到雪崩准则。然而，当分组长度为 224bit 时，需通过 AES-CBC 密文截断构造具有 90bit 输入和 134bit 输出的伪随机函数，近似构造方式导致的较低随机性严重影响 Feistel 网络效率。其后，Feistel 网络成功率和轮次效率逐渐提升是因为FFX-1采用扩张的伪随机函数(输入宽度小于输出宽度)，随分组长度增加，扩张效果愈发明显，一定程度降低了不良伪随机函数的影响。

3) FFX-2 的交互式 Feistel 网络(这里采用 3:2 非平衡划分)在 128~192bit 范围内具有较高轮次效率。由于与 FFX-1 相同的原因，并且 FFX-2 在偶数轮次采用压缩的伪随机函数(输入宽度大于输出宽度)，在 224~320bit 范围内，轮次效率降至最低。其后，随伪随机函数规模的增加，效率和成功率缓慢提升。但分组长度为 448bit 时，偶数轮次需构造具有 268bit 输入和 180bit 输出的伪随机函数，采用 AES-CBC 密文截断方式，可能造成碰撞(不同输入被映射为相同输出)，效率极低。

4) Type-2 Feistel 网络在整个分组长度范围内，均可采用 AES 直接截断的方式构造伪随机函数，所需轮次数和成功率都具有稳定性。

由以上分析可知，目前较大规模伪随机函数很难构造，AES-CBC 无法达到真正伪随机性，导致 FFSEM 和 FFX-2 效果不佳；FFX-1 采用扩张的伪随机函数，一定程度上降低了不良伪随机函数的影响，但在 224~288bit 范围内，所需伪随机函数规模刚好超过一个 AES 分组长度，轮次效率和成功率仍然较低；type-2 能够使用较小规模伪随机函数应对较大分组长度范围内数据加密的情况，具有广泛实用性。

4.3　达到雪崩准则的 Feistel 网络效率分析

由于 FFSEM 和 FFX-2 在分组长度较大时失败几率较高，其轮次数无法真正说明问题，因此这里将仅对 FFX-1 和 type-2 完成不同分组长度下数据加密的时间开销进行对比分析。

实验规定如 4.2 节，这里只测试 FFX-1 和 type-2 成功达到雪崩准则时，消耗的平均时间。需要指出的是，这里的时间消耗包括 2 部分：①对随机产生的样例 A 和 B 进行 Feistel 轮运算加密消耗的时间；②每一轮加密结束后，比较输出结果与原始明文间比特位差异消耗的时间。

图 6 对比了 FFX-1 和 type-2 成功达到雪崩准则的时间效率（当分组长度为 224bit 时，使用 FFX-1 的 100 组样例，在 100 轮运算内均不能满足雪崩准则），其变化趋势由 4.2 节讨论的轮次数决定，这里不再详述。需要指出的是，分组长度在 128~208bit 范围内，FFX-1 和 type-2 都采用直接 AES 截断方式构造，但 FFX-1 每一轮只需调用一次伪随机函数，而 type-2 需调用 2 次，因此，FFX-1 在较短分组长度情况下，效率优于 type-2。

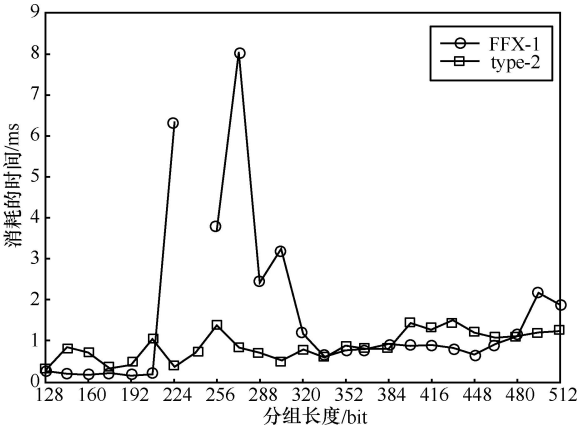

图 6　Feistel 网络成功达到雪崩准则时的时间消耗

由以上分析可知，FFX-1 存在 224~304bit 的低效范围，而且效率具有严重的不稳定性。type-2 Feistel 网络在整个分组长度范围内都能稳定地在 2ms 内达到雪崩准则，具有较高效率。

5　结束语

本文关注当前 FPE 方案中 Feistel 网络的适用性，从 Feistel 网络类型、伪随机函数构造方式以及轮次数与安全性的关系，分析了 Feistel 网络在 FPE 中应用现状。

目前 FPE 中 Feistel 网络都为 2-分割，对伪随机函数要求较高，不能适应于构造灵活分组长度的 FPE 密码。针对此问题，提出基于 *k*-分割的 type-2 Feistel 网络的 FPE 方案，该方案结合 cycle-walking 能够解决任意整数集上的 FPE 问题。但是，也指出在结合 cycle-walking 时，最坏情况下每一次迭代输出落入 $\mathbb{Z}_n$ 的概率大约只有 $\frac{1}{2^k}$ (这里 k 为 type-2 Feistel 网络划分的子分组个数)，效率较低。

基于 Feistel 网络的 FPE 方案，核心在于 Feistel 网络，由于 Feistel 网络的不同，使其具有不同适用性。通过实验对比各种 Feistel 网络达到雪崩准则所

需轮次数和时间开销，发现 type-2 Feistel 网络在 128~512bit 分组长度范围内均可采用 AES 直接截断的方式构造伪随机函数，具有较高成功率和稳定的效率，从而验证了基于 type-2 Feistel 网络构造的 FPE 方案具有广泛的实用性。

参考文献：

[1] SPIES T. Format preserving encryption. unpublished white paper[EB/OL]. http://www.voltage.com, 2008.

[2] RADHAKRISHNAN R, KHARRAZI M, MEMON N. Data masking: a new approach for steganography[J]. Journal of VLSI Signal Processing, 2005, 41(3):293-303.

[3] BELLARE M, RISTENPART T, ROGAWAY P, *et al*. Format-preserving encryption[A]. Selected Areas in Cryptography 16th Annual International Workshop, SAC 2009[C]. Springer, Lecture Notes in Computer Science, 2009. 295-312.

[4] STUTZ T, UHL A. Efficient format-compliant encryption of regular languages: block-based cycle-walking[A]. 11th IFIP TC 6/TC 11 International Conference[C]. Springer, Lecture Notes in Computer Science, 2010. 81-92.

[5] BLACK P, ROGAWAY P. Ciphers with arbitrary finite domains[A]. Topics in Cryptology-CT-RSA'02[C]. 2002. 114-130.

[6] SPIES T. Feistel finite set encryption mode[EB/OL]. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffsem/ffsem-spec.pdf.

[7] BELLARE M, ROGAWAY P, SPIES T. The FFX mode of operation for format-preserving encryption[EB/OL]. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf.

[8] BELLARE M, ROGAWAY P, SPIES T. Addendum to the FFX mode of operation for format-preserving encryption[EB/OL]. http://csrc.ncsl.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ ffx-spec2.pdf.

[9] BRIER E, PEYRIN T, STERN J. BPS: a format-preserving encryption proposal[EB/OL]. http://brutus.ncsl.nist.gov/groups/ST/ tookit/BCM/documents/proposedmodes/bps/bps-spec.pdf.

[10] CANDA V, TRUNG T. Scalable block ciphers based on Feistel-like structure[J]. Tara Mt Math Publ, 2002, 25: 39-66.

[11] 刘哲理, 贾春福, 李经纬. 保留格式加密模型研究[J]. 通信学报, 2011, 32(6): 184-190.
LIU Z L, JIA C F, LI J W. Research on format-preserving encryption modes[J]. Journal on Communications, 2011, 32(6): 184-190.

[12] HALL C, WAGNER D, KELSEY J, *et al*. Building PRFs from PRPs[A]. LNCS 1462: Fast Software Encryption[C]. Berlin: Springer, 1998. 370-389.

[13] LUBY M, RACKOFF C. How to construct pseudorandom permutations from pseudorandom functions[J]. SIAM Journal on Computing, 1988, 17(2): 373-386.

[14] PATARIN J. Pseudorandom permutations based on the DES scheme[A]. LNCS 514: Eurocode'90[C]. Berlin: Springer, 1990. 193- 204.

[15] PATARIN J. Security of random Feistel schemes with 5 or more rounds[A]. LNCS 3152: 24th Annual International Cryptology Conference[C]. Berlin: Springer, 2004. 135-158.

[16] HOANG T, ROGAWAY P. On generalized Feistel networks[A]. LNCS 6223: 30th Annual International Cryptology Conference[C]. Berlin: Springer, 2010. 613-630.

[17] IBRAHIM S, MAAROF M, IDRIS N. Avalanche analysis of extended Feistel network[EB/OL]. http://eprints.utm.my/3258/1/Subariah_PARS05.pdf.

[18] IBRAHIM S, MAAROF M. Diffusion analysis of a scalable Feistel network[A]. Proceeding of 3rd World Enformatika Conference, Istanbul[C]. 2005.98-101.

[19] 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 format-preserving encryption techniques[J]. Journal of Software, 2012,23(1):152-170.

[20] HEYS H, TAVARES S. Avalanche characteristics of substitution permutation encryption networks[J]. IEEE Transactions on Computer, 44(9): 1131-1139.

作者简介：

李经纬（1987-），男，四川成都人，南开大学博士生，主要研究方向为应用密码学。

贾春福（1967-），男，河北文安人，博士，南开大学教授、博士生导师，主要研究方向为信息安全与可信计算、恶意代码发现与分析。

刘哲理（1978-），男，山东潍坊人，南开大学讲师，主要研究方向为密码学及应用、智能卡操作系统。

李敏（1975-），女，天津静海人，南开大学博士生，主要研究方向为应用密码学。