软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2024,35(10):4826−4836 [doi: 10.13328/j.cnki.jos.006957]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

FBC 模型的伪随机性和超伪随机性*

刘 楠[1], 金晨辉[1], 于俊伟[2], 崔 霆[1]

[1](战略支援部队信息工程大学, 河南 郑州 450001)

[2](河南工业大学 人工智能与大数据学院, 河南 郑州 450001)

通信作者: 刘楠, E-mail: liunan526@126.com

摘 要: FBC 分组密码算法是入选 2018 年全国密码算法设计大赛第 2 轮的 10 个分组密码算法之一. FBC 主要采用四分支两路 Feistel 结构设计, 是一个实现效率高的轻量级分组密码算法. 将 FBC 算法抽象为 FBC 模型, 并研究该模型的伪随机性和超伪随机性, 在 FBC 轮函数都是相互独立的随机函数的条件下, 给出能够与随机置换不可区分所需的最少轮数. 结论表明, 在选择明文攻击条件下, 4 轮 FBC 与随机置换不可区分, 因而具有伪随机性; 在自适应性选择明密文攻击条件下, 5 轮 FBC 与随机置换不可区分, 因而具有超伪随机性.

关键词: 分组密码; FBC 模型; 伪随机性; 超伪随机性

中图法分类号: TP309

中文引用格式: 刘楠, 金晨辉, 于俊伟, 崔霆. FBC模型的伪随机性和超伪随机性. 软件学报, 2024, 35(10): 4826–4836. http://www.jos.org.cn/1000-9825/6957.htm

英文引用格式: Liu N, Jin CH, Yu JW, Cui T. Pseudorandomness and Super-pseudorandomness of FBC Model. Ruan Jian Xue Bao/Journal of Software, 2024, 35(10): 4826–4836 (in Chinese). http://www.jos.org.cn/1000-9825/6957.htm

Pseudorandomness and Super-pseudorandomness of FBC Model

LIU Nan[1], JIN Chen-Hui[1], YU Jun-Wei[2], CUI Ting[1]

[1](PLA SSF Information Engineering University, Zhengzhou 450001, China)

[2](School of Artificial Intelligence and Big Data, Henan University of Technology, Zhengzhou 450001, China)

Abstract: As one of the ten block cipher algorithms selected for the second round of the 2018 National Cryptographic Algorithm Design Contest, Feistel-based block cipher (FBC) is an efficient and lightweight block cipher algorithm with a four-branch and two-fold Feistel structure. In this study, the FBC algorithm is abstracted as the FBC model, and the pseudorandomness and super-pseudorandomness of the model are studied. It is assumed that the FBC round functions are independent random functions, and a method to find the minimal number of FBC rounds is provided, which will keep FBC indistinguishable from a random permutation. Finally, the study comes to the conclusion that under the chosen-plaintext attack, four rounds of FBC are indistinguishable from random permutation, so the model has pseudorandomness; under the adaptive chosen-plaintext and ciphertext attack, five rounds of FBC are indistinguishable from random permutation, so the model has super-pseudorandomness.

Key words: block cipher; FBC model; pseudorandomness; super-pseudorandomness

1 引 言

无论是分组密码, 还是公钥密码, 其安全性是首先需要保证的. 公钥密码体制的安全性通常建立在难解数学问题的计算复杂性上, 而分组密码被认为是安全的, 通常是因为目前没有找到对它们的有效攻击. 但作为在各种安全系统中起着重要作用的分组密码算法, 这种情况显然不够可靠. 因此, 从可证明安全的角度探讨分组密码的安全性

* 基金项目: 河南省优秀青年科学基金 (222300420100); 国家自然科学基金 (61772547)
收稿时间: 2022-07-10; 修改时间: 2023-01-19, 2023-03-10; 采用时间: 2023-04-19; jos 在线出版时间: 2023-09-27
CNKI 网络首发时间: 2023-10-07

有着很重要的理论意义. 可证明安全理论在分组密码中的研究始于 Luby 等人的工作[1], 他们定义了伪随机置换和超伪随机置换的概念, 目前已成为衡量分组密码模型安全性的基本标准之一. 假设轮函数是随机函数的条件下, 分别在选择明文和自适应性选择明文密文攻击的条件下, 考察若干轮迭代形成的置换能否与随机置换不可区分, 即考察它们是否具有伪随机性和超伪随机性. Luby 等人在文献 [1] 中证明了 3 轮 Feistel 结构具有伪随机性、4 轮 Feistel 结构具有超伪随机性, 从而开启了从伪随机角度对分组密码可证明安全性的研究模式, 并引起人们的广泛关注. 文献 [2] 证明了 5 轮 Camellia 结构具有伪随机性和 8 轮 Camellia 结构具有超伪随机性. 文献 [3] 证明了 k 个并置 Feistel 模型叠加 $2k$ 个块的块移位一类广义 Feistel 结构的伪随机性和超伪随机性. 文献 [4] 证明了 4 轮 MISTRY 结构和 3 轮双重 MISTRY 结构的伪随机性. 文献 [5] 证明了双射 σ 为任意正形置换时, Lai-Massey 结构至少 3 轮具有伪随机特性, 双射 σ 为正形置换时 Lai-Massey 结构至少 4 轮才具有超伪随机性. 文献 [6] 给出当 S 盒是随机置换时, 3 轮 SPN 结构是超伪随机置换的结论. 文献 [7] 证明了 5 轮 P-SPN 的超伪随机性.

为推动密码学理论与应用、密码算法设计与实现的发展, 2018 年中国密码学会举办了全国密码算法设计大赛. 在经过第 1 轮评估之后, FBC 是入选第 2 轮的 10 个分组密码之一. FBC 是一族轻量级分组密码算法, 该算法主要基于两个并置的 Feistel 结构设计, 并以 Feistel-based block cipher 的首字母命名[8]. 主要包含 FBC128-128, FBC128-256 和 FBC256-256 这 3 个版本, 可支持 128 和 256 两种比特长度的明文分组以及 128 和 256 两种比特长度的密钥. FBC 算法采用 4 分支两路 Feistel 结构设计, 通过增加两个异或操作的微小代价提高了整体结构的扩散特性.

对一个密码模型整体结构的安全性分析通常包括两类: 一类是分析抵抗现有分析方法的能力, 尤其是抵抗差分分析和线性密码分析的能力; 另一类是分析密码模型的伪随机特性. 由于 FBC 算法整体结构具有较好的扩散特性, 目前尚未见到对该模型伪随机特性的研究. 本文将通过研究其伪随机性和超伪随机性的方法, 研究 FBC 模型的可证明安全性. 假设 FBC 模型的轮函数都是随机函数, 我们分别给出了在选择明文和自适应选择明文密文攻击条件下使该模型与随机置换不可区分所需的最少轮数. 结论表明, 在选择明文攻击条件下, 4 轮 FBC 模型和随机置换不可区分, 因而具有伪随机性; 在自适应性选择明文密文攻击条件下, 5 轮 FBC 模型和随机置换不可区分, 因而具有超伪随机性, 我们由此获得 FBC 模型的伪随机特性和超伪随机特性.

本文约定符号如下: (L_i,R_i,S_i,T_i) 为第 i 轮迭代的输出, $i=0,1,2,\ldots,r+1$, 特别地, (L_0,R_0,S_0,T_0) 为输入, $\oplus$表示异或运算, $\|$表示字符串连接符.

2 FBC 模型简介

FBC 模型的状态均由 4 个 n 比特的字组成, 明文总长度是分块长度的 4 倍. 设 i 为迭代轮数, FBC 轮函数的结构如图 1 所示.

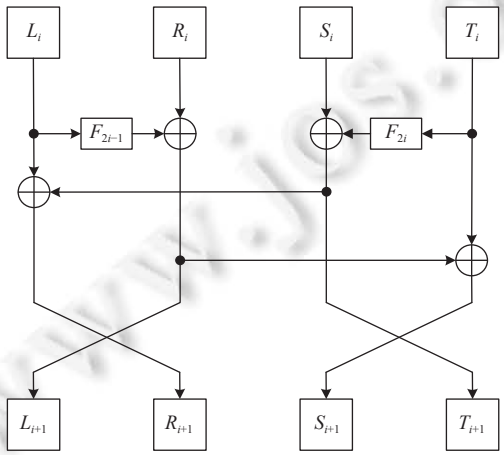

图 1 FBC 模型轮函数结构图

FBC 模型的加密过程如下: 首先将输入长度为 $4n$ 的明文分成 4 个子块, 即 $L_0||R_0||S_0||T_0$. 对 $i=1,2,\ldots,r$, 重复执行下列操作.

$$\begin{cases} L_i = R_{i-1} \oplus f_{2i-1}(L_{i-1}) \\ R_i = L_{i-1} \oplus T_i \\ S_i = L_i \oplus T_{i-1} \\ T_i = S_{i-1} \oplus f_{2i}(T_{i-1}) \end{cases}.$$

然后将 (R_r, L_r, T_r, S_r) 作为输出的密文. 为简单起见, 我们在分析时忽略最后一轮的交换, 将最后一轮的轮函数视为与前几轮相同的轮函数, 此时将 (L_r, R_r, S_r, T_r) 作为输出的密文.

以下我们用 $\varphi(f_1,\ldots,f_{2r})$ 表示第 i 轮的 F 函数分别为 f_{2i-1} 和 f_{2i} 的 r 轮 FBC 模型.

3 准备工作

定义 1. 设 $v: N \to R$ 是自然数集至实数集的函数, 如果存在多项式函数 p, 使得对于充分大的 n, 都有 $v(n) > \frac{1}{p(n)}$, 则称 v 是不可忽略函数; 如果对任意常数 $c>0$, 都存在 $n_c>0$, 使得当 $n \geqslant n_c$ 时, 都有 $v(n) < \frac{1}{n^c}$, 则称 v 是可忽略函数[9].

设 $rand^{m\to n}$ 是 $\{0,1\}^m$ 到 $\{0,1\}^n$ 的所有映射构成的集合, $permu^n$ 是 $\{0,1\}^n$ 到自身的所有双射构成的集合.

引理 1. 设 f 是 $rand^{m\to n}$ 上的一个随机函数, $x_1, x_2, \ldots, x_k \in \{0,1\}^m$ 互不相同, 则:

(1) 随机变量 $(f(x_1), f(x_2), \ldots, f(x_k))$ 在 $\underbrace{\{0,1\}^n \times \ldots \times \{0,1\}^n}_{k\text{个}}$ 上服从均匀分布.

(2) 随机变量 $f(x_1), f(x_2), \ldots, f(x_k)$ 相互独立且都在 $\{0,1\}^n$ 上服从均匀分布.

引理 2. 设 $f_1, f_2, \ldots, f_t$ 是 $rand^{m\to n}$ 上相互独立的随机函数, $x_{i,j} \in \{0,1\}^m$, $1 \leqslant i \leqslant t$, $1 \leqslant j \leqslant k$ 则 t 个随机变量组 $(f_1(x_{1,1}), f_1(x_{1,2}), \ldots, f_1(x_{1,k})), \ldots, (f_t(x_{t,1}), f_t(x_{t,2}), \ldots, f_t(x_{t,k}))$ 相互独立.

引理 3. 设 ξ 和 $\eta_1, \ldots, \eta_k$ 都是有限群 Ω 上的随机变量, 如果 ξ 在 Ω 上服从均匀分布且 ξ 与 $(\eta_1, \ldots, \eta_k)$ 独立, 则 $\xi + \sum_{i=1}^{k} \eta_i$ 在 Ω 上服从均匀分布.

引理 4. 设 ξ 和 η 都是有限集 Ω 上相互独立的随机变量, f、g 是 Ω 上的两个实数值函数, 则 $f(\xi)$ 与 $g(\eta)$ 独立.

设 ψ_n 是 $\{0,1\}^n$ 到自身的一个特定的双射集合, 对于从 ψ_n 或 $permu^n$ 中等概选择的一个置换 π, 区分器 D 的目的是用来判断 π 是从 ψ_n 还是从 $permu^n$ 中选择的; 如果判定 $\pi \in permu^n$, 则输出 0; 如果判定 $\pi \in \psi_n$, 则输出 1.

定义 2. 设 D 是区分 ψ_n 与 $permu^n$ 的区分器, ψ_n 是一个特定的置换集合, 则 D 的区分优势 ρ_D 定义为:

$$\rho_D = \left| P\left(D \text{ output } 1 \middle| \pi \leftarrow permu^n\right) - P\left(D \text{ output } 1 \middle| \pi \leftarrow \psi_n\right) \right|.$$

定义 3. 设 ψ_n 是一个置换集合, 对于任意的区分器 D, 若选择的明文个数是 n 的多项式函数, 在选择明文攻击条件下, 如果 ρ_D 是可忽略的, 则称 ψ_n 是伪随机的; 在自适应性选择明文和密文攻击条件下, 如果 ρ_D 是可忽略的, 则称 ψ_n 是超伪随机的.

引理 5. 设 ξ_0, ξ_1, η 都是 $Z/(m)$ 上的随机变量, 如果在已知 n 个样本的条件下, ξ_0 与 η 的最大区分优势 $\leqslant h_0$, ξ_1 与 η 的最大区分优势 $\leqslant h_1$, 则在已知 n 个样本的条件下, ξ_0 与 ξ_1 的最大区分优势 $\leqslant h_0 + h_1$.

4 FBC 的可证明安全性分析

引理 6. 设 $p_{permu}(x,y)$ 为 $\{0,1\}^{4n}$ 上随机置换满足互不相同的 q 对输入输出时对应的概率, 则有 $2^{-4nq} \leqslant p_{permu}(x,y) < 3 \cdot 2^{-4qn}$.

引理 2 至引理 6 的证明过程详见附录 A.

引理 7. 设 3 轮 FBC 模型的 F 函数分别为 $f_1, f_2, f_3, f_4, f_5, f_6$, 其中 $f_1, \ldots, f_6$ 是从 $rand^{n\to n}$ 中独立、等概选取的随机函数. 再设 $(L_0^i, R_0^i, S_0^i, T_0^i)$ 是 q 个互不相同的输入, 对 $1 \leqslant i \leqslant q$, 令:

$$\varphi(f_1,\ldots,f_4)\left(L_0^i,R_0^i,S_0^i,T_0^i\right)=\left(L_2^i,R_2^i,S_2^i,T_2^i\right),\ \varphi(f_1,\ldots,f_6)\left(L_0^i,R_0^i,S_0^i,T_0^i\right)=\left(L_3^i,R_3^i,S_3^i,T_3^i\right),$$

并记 A_i,B_i 对于 $i=2,3$ 分别为 $L_i^1,L_i^2,\ldots,L_i^q$ 和 $T_i^1,T_i^2,\ldots,T_i^q$, 且互不相同, 有 $P\left(\bar{A}_i\right)\leqslant q(q-1)2^{-n}$ 和 $P\left(\bar{B}_i\right)\leqslant q(q-1)2^{-n}$.

证明: 用 $\bar{A}_i$ 表示 A_i 的非事件, 则有 $P\left(\bar{A}_2\right)\leqslant\sum_{1\leqslant i<j\leqslant q}P\left(L_2^i=L_2^j\right)$. 设 $1\leqslant i<j\leqslant q$, 下面计算 $P\left(L_2^i=L_2^j\right)$.

● 由 FBC 模型的定义知 $L_2^i=R_1^i\oplus f_3(L_1^i)=L_0^i\oplus T_1^i\oplus f_3(L_1^i)=L_0^i\oplus S_0^i\oplus f_2(T_0^i)\oplus f_3(L_1^i)$, 即 L_2^i 是随 L_0^i,S_0^i,T_0^i,L_1^i 变化而变化, 因此我们分以下 4 种情况进行讨论.

(1) 如果 $T_0^i\neq T_0^j$, 则由 f_2 是随机函数和引理 1 知 $f_2(T_0^i)$ 与 $f_2(T_0^j)$ $(1\leqslant i<j\leqslant q)$ 相互独立且都服从均匀分布, 因而 $L_0^i\oplus S_0^i\oplus f_2(T_0^i)$ 与 $L_0^j\oplus S_0^j\oplus f_2(T_0^j)$ 相互独立且都服从均匀分布, 又由 f_2,f_3 相互独立知 $f_3(L_1^i)$ 和 $f_3(L_1^j)$ 均与 $L_0^i\oplus S_0^i\oplus f_2(T_0^i)$ 和 $L_0^j\oplus S_0^j\oplus f_2(T_0^j)$ 独立, 故由 $L_0^i\oplus S_0^i\oplus f_2(T_0^i)$ 与 $L_0^j\oplus S_0^j\oplus f_2(T_0^j)$ 服从均匀分布和引理 3 知 L_2^i 与 L_2^j 均服从均匀分布, 且由引理 4 知 L_2^i 与 L_2^j 相互独立, 从而 $L_2^i\oplus L_2^j$ 服从均匀分布, 因而有 $P\left(L_2^i=L_2^j\right)=2^{-n}$.

(2) 如果 $L_1^i\neq L_1^j$, 则由 $L_2^i=L_0^i\oplus S_0^i\oplus f_2(T_0^i)\oplus f_3(L_1^i)$, 仿照 (1) 可证 $P\left(L_2^i=L_2^j\right)=2^{-n}$.

(3) 如果 $T_0^i=T_0^j$ 和 $L_0^i=L_0^j$. 若 $L_1^i=L_1^j$, 则由 $L_2^i=L_0^i\oplus S_0^i\oplus f_2(T_0^i)\oplus f_3(L_1^i)$ 知 $L_2^i=L_2^j$ 等价于 $S_0^i=S_0^j$, 再由 $L_1^i=R_0^i\oplus f_1(L_0^i)$ 和 $L_1^i=L_1^j$ 及 $L_0^i=L_0^j$ 知 $R_0^i=R_0^j$, 从而有 $(L_0^i,R_0^i,S_0^i,T_0^i)=\left(L_0^j,R_0^j,S_0^j,T_0^j\right)$, 这与假设矛盾. 该矛盾说明 $L_1^i\neq L_1^j$, 从而由 (2) 知 $P\left(L_2^i=L_2^j\right)=2^{-n}$.

(4) 如果 $T_0^i=T_0^j$ 和 $L_0^i\neq L_0^j$, 则由 $L_1^i=R_0^i\oplus f_1(L_0^i)$ 及引理 1 知 L_1^i 与 L_1^j 相互独立且都服从均匀分布, 从而 $L_1^i\oplus L_1^j$ 服从均匀分布, 进而由 (2) 和全概率公式知:

$$\begin{aligned}P\left(L_2^i=L_2^j\right)&=P\left(L_2^i=L_2^j\middle|L_1^i\neq L_1^j\right)P\left(L_1^i\neq L_1^j\right)+P\left(L_2^i=L_2^j\middle|L_1^i=L_1^j\right)P\left(L_1^i=L_1^j\right)\\&\leqslant P\left(L_2^i=L_2^j\middle|L_1^i\neq L_1^j\right)+P\left(L_1^i=L_1^j\right)=2^{-n}+2^{-n}=2^{-n+1}.\end{aligned}$$

综合 (1) 至 (4) 知 $P\left(L_2^i=L_2^j\right)\leqslant 2^{-n+1}$, 故有 $P\left(\bar{A}_2\right)\leqslant\sum_{1\leqslant i<j\leqslant q}P\left(L_2^i=L_2^j\right)\leqslant C_q^2\cdot 2^{-n+1}=q(q-1)2^{-n}$.

同理可证 $P\left(\bar{B}_2\right)\leqslant q(q-1)2^{-n}$.

同样用 $\bar{A}_3$ 表示 A_3 的非事件, 则有 $P\left(\bar{A}_3\right)\leqslant\sum_{1\leqslant i<j\leqslant q}P\left(L_3^i=L_3^j\right)$. 设 $1\leqslant i<j\leqslant q$, 下面计算 $P\left(L_3^i=L_3^j\right)$.

● 由 FBC 模型的定义知 $L_3^i=R_2^i\oplus f_5(L_2^i)=T_0^i\oplus f_4(T_1^i)\oplus f_5(L_2^i)$, 我们分以下 3 种情况进行讨论.

(1) 如果 $L_2^i\neq L_2^j$, 仿照 (1) 可证 $P\left(L_3^i=L_3^j\right)=2^{-n}$.

(2) 如果 $T_1^i\neq T_1^j$, 仿照 (1) 可证 $P\left(L_3^i=L_3^j\right)=2^{-n}$.

(3) 如果 $T_0^i=T_0^j$, 若 $T_1^i=T_1^j$, 则由 $T_1^i=S_0^i\oplus f_2(T_0^i)$ 知 $S_0^i=S_0^j$, 由 $L_2^i=L_0^i\oplus S_0^i\oplus f_2(T_0^i)\oplus f_3(L_1^i)$ 知 $L_2^i=L_2^j$ 等价于 $L_0^i\oplus f_3(L_1^i)=L_0^j\oplus f_3(L_1^j)$, 故若 $L_1^i=L_1^j$, 则 $L_0^i=L_0^j$, 又由 $L_1^i=R_0^i\oplus f_1(L_0^i)$ 可知必有 $R_0^i=R_0^j$, 从而有 $(L_0^i,R_0^i,S_0^i,T_0^i)=\left(L_0^j,R_0^j,S_0^j,T_0^j\right)$, 这与假设矛盾. 该矛盾说明 $L_1^i\neq L_1^j$, 则由引理 1 可知 $f_3(L_1^i)$ 与 $f_3(L_1^j)$ 相互独立且服从均匀分布, 从而 $P\left(L_2^i=L_2^j\right)=P\left(L_0^i\oplus f_3(L_1^i)=L_0^j\oplus f_3(L_1^j)\right)=P\left(f_3(L_1^i)\oplus f_3(L_1^j)=L_0^i\oplus L_0^j\right)=2^{-n}$, 因此由 (1) 和全概率公式知:

$$\begin{aligned}P\left(L_3^i=L_3^j\right)&=P\left(L_3^i=L_3^j\middle|L_2^i\neq L_2^j\right)P\left(L_2^i\neq L_2^j\right)+P\left(L_3^i=L_3^j\middle|L_2^i=L_2^j\right)P\left(L_2^i=L_2^j\right)\\&\leqslant P\left(L_3^i=L_3^j\middle|L_2^i\neq L_2^j\right)+P\left(L_2^i=L_2^j\right)=2^{-n}+2^{-n}=2^{-n+1}.\end{aligned}$$

综合 (1) 至 (3) 知 $P\left(L_3^i=L_3^j\right)\leqslant 2^{-n+1}$, 故有 $P\left(\bar{A}_3\right)\leqslant\sum_{1\leqslant i<j\leqslant q}P\left(L_3^i=L_3^j\right)\leqslant C_q^2\cdot 2^{-n+1}=q(q-1)2^{-n}$.

同理可证 $P\left(\bar{B}_3\right)\leqslant q(q-1)2^{-n}$.

证毕.

定理 1. 设 4 轮 FBC 模型的 F 函数分别为 $f_1,\ldots,f_8$, 其中 $f_1,\ldots,f_8$ 是从 $rand^{n\to n}$ 中独立、等概选取的随机函数, 则在选择明文攻击下, $\varphi(f_1,\ldots,f_8)$ 与随机置换不可区分. 具体地说, 对于任意选择的 q 个明文, 在已知对应的密文时, 利用它们发起的对二者的区分攻击的区分优势小于 $q(q-1)2^{2-n}$.

证明: 设 $g\in\{\varphi(f_1,\ldots,f_8),rand^{4n\to 4n}\}$, 假设已知 g 的 q 个互不相同的输入 $\{(L_0^i,R_0^i,S_0^i,T_0^i),i=1,\ldots,q\}$ 且知道它们

对应的输出. 当 $g=\varphi$ 时, 对于 $\varphi(f_1,\ldots,f_8)$ 的输入 $(L_0^i,R_0^i,S_0^i,T_0^i)$, 有 $\varphi(f_1,\ldots,f_8)(L_0^i,R_0^i,S_0^i,T_0^i)=(L_4^i,R_4^i,S_4^i,T_4^i)$. 定义 $(L_0^i,R_0^i,S_0^i,T_0^i)$ 为第 i 次问询的明文, $\left(L_j^i,R_j^i,S^i{}_j,T_j^i\right)$ 为其第 j 轮的输出, 则由

$$\begin{cases}L_1^i=R_0^i\oplus f_1\left(L_0^i\right)\\R_1^i=L_0^i\oplus T_1^i\\S_1^i=L_1^i\oplus T_0^i\\T_1^i=S_0^i\oplus f_2\left(T_0^i\right)\end{cases},\quad\begin{cases}L_2^i=R_1^i\oplus f_3\left(L_1^i\right)\\R_2^i=L_1^i\oplus T_2^i\\S_2^i=L_2^i\oplus T_1^i\\T_2^i=S_1^i\oplus f_4\left(T_1^i\right)\end{cases},\quad\begin{cases}L_3^i=R_2^i\oplus f_5\left(L_2^i\right)\\R_3^i=L_2^i\oplus T_3^i\\S_3^i=L_3^i\oplus T_2^i\\T_3^i=S_2^i\oplus f_6\left(T_2^i\right)\end{cases},\quad\begin{cases}L_4^i=R_3^i\oplus f_7\left(L_3^i\right)\\R_4^i=L_3^i\oplus T_4^i\\S_4^i=L_4^i\oplus T_3^i\\T_4^i=S_3^i\oplus f_8\left(T_3^i\right)\end{cases},$$

知:

$$\begin{cases}L_4^i=R_3^i\oplus f_7\left(L_3^i\right)=S_0^i\oplus f_2\left(T_0^i\right)\oplus f_6\left(T_2^i\right)\oplus f_7\left(L_3^i\right)\\R_4^i=L_3^i\oplus T_4^i=T_0^i\oplus R_0^i\oplus f_1\left(L_0^i\right)\oplus f_4\left(T_1^i\right)\oplus f_8\left(T_3^i\right)\\S_4^i=L_4^i\oplus T_3^i=L_0^i\oplus S_0^i\oplus f_2\left(T_0^i\right)\oplus f_3\left(L_1^i\right)\oplus f_7\left(L_3^i\right)\\T_4^i=S_3^i\oplus f_6\left(T_3^i\right)=R_0^i\oplus f_1\left(L_0^i\right)\oplus f_5\left(L_2^i\right)\oplus f_8\left(T_3^i\right)\end{cases}\tag{1}$$

我们的证明思路是在限定 f_5,f_6,f_7,f_8 的输入互不相同时, 证明 $\varphi(f_1,\ldots,f_8)$ 的输出相互独立并且服从均匀分布, 再由该事件不发生的概率, 界定 φ 和随机置换的最大区分优势. 记 $E(L_0^i,R_0^i,S_0^i,T_0^i)=\varphi(f_1,\ldots,f_8)(L_0^i,R_0^i,S_0^i,T_0^i)$, 可知 $E(L_0^i,R_0^i,S_0^i,T_0^i)=(L_4^i,R_4^i,S_4^i,T_4^i)$ 成立蕴含公式 (1) 成立, 设 $E(L_0^i,R_0^i,S_0^i,T_0^i)=(L_4^i,R_4^i,S_4^i,T_4^i)$ 成立的概率为 P_{FBC}, 公式 (1) 成立的概率为 P_*, 则有 $P_{\mathrm{FBC}}\leqslant P_*$.

用 A_i,B_i $(i=2,3)$ 分别表示 $L_i^1,L_i^2,\ldots,L_i^q$ 和 $T_i^1,T_i^2,\ldots,T_i^q$ 的取值都互不相同的事件. 下面首先证明: 在事件 A_i,B_i $(i=2,3)$ 同时发生的条件下, 密文序列 $(L_4^1,\ldots,L_4^q,\ R_4^1,\ldots,R_4^q,\ S_4^1,\ldots,S_4^q,\ T_4^1,\ldots,T_4^q)$ 服从均匀分布.

(1) 由于 $T_2^1,T_2^2,\ldots,T_2^q$ 互不相同, 故由 f_6 是随机函数和引理 1 知 $(f_6(T_2^1),f_6(T_2^2),\ldots,f_6(T_2^q))$ 服从均匀分布, 再由 f_2,f_6,f_7 相互独立和引理 2 知:

$$(f_2(T_0^1),f_2(T_0^2),\ldots,f_2(T_0^q)),(f_7(L_3^1),f_7(L_3^2),\ldots,f_7(L_3^q)),(f_6(T_2^1),f_6(T_2^2),\ldots,f_6(T_2^q)),$$

相互独立, 故由 $(f_6(T_2^1),f_6(T_2^2),\ldots,f_6(T_2^q))$ 服从均匀分布和引理 3 知:

$$(f_7(L_3^1)\oplus f_2(T_0^1)\oplus f_6(T_2^1),f_7(L_3^2)\oplus f_2(T_0^2)\oplus f_6(T_2^2),\ldots,f_7(L_3^q)\oplus f_2(T_0^q)\oplus f_6(T_2^q)),$$

服从均匀分布, 再由 $S_0^1,S_0^2,\ldots,S_0^q$ 是常值知 $(L_4^1,L_4^2,\ldots,L_4^q)$ 服从均匀分布.

同理可证, $(R_4^1,R_4^2,\ldots,R_4^q)$, $(S_4^1,S_4^2,\ldots,S_4^q)$ 和 $(T_4^1,T_4^2,\ldots,T_4^q)$ 都服从均匀分布.

(2) 记 $\xi_5=(f_5(L_2^1),\ldots,f_5(L_2^q))$, $\xi_6=(f_6(T_2^1),\ldots,f_6(T_2^q))$, $\xi_7=(f_7(L_3^1),\ldots,f_7(L_3^q))$, $\xi_8=(f_8(T_3^1),\ldots,f_8(T_3^q))$, 则由 f_5,f_6,f_7,f_8 相互独立和各自的 q 个输入互不相同的假设知, $f_5(L_2^i),f_6(T_2^i),f_7(L_3^i),f_8(T_3^i)$ 相互独立且都服从均匀分布, 从而 $(\xi_5,\xi_6,\xi_7,\xi_8)$ 服从均匀分布, 进而 $(\xi_6\oplus\xi_7,\xi_8,\xi_7,\xi_5\oplus\xi_8)$ 服从均匀分布.

令:

$$\xi_1=(f_1(L_0^1),\ldots,f_1(L_0^q)),\quad \xi_2=(f_2(T_0^1),\ldots,f_2(T_0^q)),\quad \xi_3=(f_3(L_1^1),\ldots,f_3(L_1^q)),\quad \xi_4=(f_4(T_1^1),\ldots,f_4(T_1^q)),$$

则由 $f_1,f_2,\ldots,f_8$ 相互独立和引理 2 知 $\xi_1,\xi_2,\ldots,\xi_8$ 相互独立, 从而 $(\xi_1,\xi_2,\xi_3,\xi_4)$ 与 $(\xi_5,\xi_6,\xi_7,\xi_8)$ 独立. 由引理 4 知 $(\xi_2,\xi_1\oplus\xi_4,\xi_2\oplus\xi_3,\xi_1)$ 与 $(\xi_6\oplus\xi_7,\xi_8,\xi_7,\xi_5\oplus\xi_8)$ 相互独立, 再由 $(\xi_6\oplus\xi_7,\xi_8,\xi_7,\xi_5\oplus\xi_8)$ 服从均匀分布和引理 3 知 $(\xi_2\oplus\xi_6\oplus\xi_7,\xi_1\oplus\xi_4\oplus\xi_8,\xi_2\oplus\xi_3\oplus\xi_7,\xi_1\oplus\xi_5\oplus\xi_8)$ 服从均匀分布, 进而由 $L_0^{1\to q},R_0^{1\to q},S_0^{1\to q},T_0^{1\to q}$ 是常值即知 $(L_4^1,\ldots,L_4^q,\ R_4^1,\ldots,R_4^q,\ S_4^1,\ldots,S_4^q,\ T_4^1,\ldots,T_4^q)$ 服从均匀分布. 故:

$$p(L_4^{1\to q}=l_4^{1\to q},T_4^{1\to q}=t_4^{1\to q},R_4^{1\to q}=r_4^{1\to q},S_4^{1\to q}=s_4^{1\to q}|A_2,B_2,A_3,B_3)=2^{-4nq}.$$

即在事件 A_i,B_i $(i=2,3)$ 同时发生的条件下, 公式 (1) 成立的概率 $P_*=2^{-4nq}$, 此时密文序列 $(L_4^1,\ldots,L_4^q,\ R_4^1,\ldots,R_4^q,\ S_4^1,\ldots,S_4^q,\ T_4^1,\ldots,T_4^q)$ 的分布与均匀分布不可区分.

由引理 6 知, $P_*\leqslant P_{permu}$, 且 $P_{\mathrm{FBC}}\leqslant P_*$, 故 $P_{\mathrm{FBC}}\leqslant P_{permu}$. 记 $p_{permu}(x,y)$ 和 $p_{\mathrm{FBC}}(x,y)$ 分别是查询随机置换和查询 4 轮 FBC 模型时查询序列全部吻合的概率, 再记 $\Lambda=A_2\cap B_2\cap A_3\cap B_3$, 则利用 q 个选择明密文的查询结果进行区分攻击的区分优势为:

$$\rho = 2^{-4qn}\left|\sum_{(x,y)\in\Lambda}[p_{permu}(x,y)-p_{\mathrm{FBC}}(x,y)]+\sum_{(x,y)\in\bar{\Lambda}}[p_{permu}(x,y)-p_{\mathrm{FBC}}(x,y)]\right|$$

$$\leqslant 2^{-4qn}\left|\sum_{(x,y)\in\Lambda}[p_{permu}(x,y)-p_{\mathrm{FBC}}(x,y)]\right|+2^{-4qn}\left|\sum_{(x,y)\in\bar{\Lambda}}[p_{permu}(x,y)-p_{\mathrm{FBC}}(x,y)]\right|$$

$$\leqslant 2^{-4qn}\sum_{(x,y)\in\Lambda}p_{permu}(x,y)+2^{-4qn}\sum_{(x,y)\in\bar{\Lambda}}[1-0]\leqslant p_{permu}(x,y)+p(\bar{\Lambda})=p_{permu}(x,y)+p(\bar{A}_2\cup\bar{B}_2\cup\bar{A}_3\cup\bar{B}_3).$$

由引理 6 知 $p_{permu}(x,y)<3\times2^{-4qn}$, 由引理 7 知 $P(\bar{A}_i)\leqslant q(q-1)2^{-n}$ 和 $P(\bar{B}_i)\leqslant q(q-1)2^{-n}$, 因此, 区分优势 $\rho\leqslant p_{permu}(x,y)+p(\bar{A}_2\cup\bar{A}_3\cup\bar{B}_2\cup\bar{B}_3)<3\times2^{-4qn}+q(q-1)2^{-n+2}\approx q(q-1)2^{2-n}$.

这说明 4 轮 FBC 模型与随机置换在选择明文条件下的最大区分优势 $<q(q-1)2^{2-n}$, 故二者不可区分.

证毕.

定理 2. 在选择明密文条件下, 4 轮 FBC 模型与随机函数是可以区分的.

证明: 对于 $\varphi(f_1,f_2,f_3,f_4,f_5,f_6)$ 的输入 (L_0,R_0,S_0,T_0), 有:

$$\begin{cases}L_1^i=R_0^i\oplus f_1(L_0^i)\\R_1^i=L_0^i\oplus T_1^i\\S_1^i=L_1^i\oplus T_0^i\\T_1^i=S_0^i\oplus f_2(T_0^i)\end{cases},\ \begin{cases}L_2^i=R_1^i\oplus f_3(L_1^i)\\R_2^i=L_1^i\oplus T_2^i\\S_2^i=L_2^i\oplus T_1^i\\T_2^i=S_1^i\oplus f_4(T_1^i)\end{cases},\ \begin{cases}L_3^i=R_2^i\oplus f_5(L_2^i)\\R_3^i=L_2^i\oplus T_3^i\\S_3^i=L_3^i\oplus T_2^i\\T_3^i=S_2^i\oplus f_6(T_2^i)\end{cases},\ \begin{cases}L_4^i=R_3^i\oplus f_7(L_3^i)\\R_4^i=L_3^i\oplus T_4^i\\S_4^i=L_4^i\oplus T_3^i\\T_4^i=S_3^i\oplus f_8(T_3^i)\end{cases}.$$

取 $(L_0,R_0,S_0,T_0)=(0,0,0,0)$, 则有:

$$\begin{cases}L_4^1=f_2(0)\oplus f_6(f_1(0)\oplus f_4f_2(0))\oplus f_7(f_4f_2(0)\oplus f_5(f_2(0)\oplus f_3f_1(0)))\\R_4^1=f_1(0)\oplus f_4f_2(0)\oplus f_8(f_3f_1(0)\oplus f_6(f_1(0)\oplus f_4f_2(0)))\\S_4^1=f_2(0)\oplus f_3f_1(0)\oplus f_7(f_4f_2(0)\oplus f_5(f_2(0)\oplus f_3f_1(0)))\\T_4^1=f_1(0)\oplus f_5(f_2(0)\oplus f_3f_1(0))\oplus f_8(f_3f_1(0)\oplus f_6(f_1(0)\oplus f_4f_2(0)))\end{cases}.$$

再取 $(L_0,R_0,S_0,T_0)=(0,X,0,0)$, 则有:

$$\begin{cases}L_4^2=f_2(0)\oplus f_6(X\oplus f_1(0)\oplus f_4f_2(0))\oplus f_7(f_4f_2(0)\oplus f_5(f_2(0)\oplus f_3(X\oplus f_1(0))))\\R_4^2=X\oplus f_1(0)\oplus f_4f_2(0)\oplus f_8(f_3(X\oplus f_1(0))\oplus f_6(X\oplus f_1(0)\oplus f_4f_2(0)))\\S_4^2=f_2(0)\oplus f_3(X\oplus f_1(0))\oplus f_7(f_4f_2(0)\oplus f_5(f_2(0)\oplus f_3(X\oplus f_1(0))))\\T_4^2=X\oplus f_1(0)\oplus f_5(f_2(0)\oplus f_3(X\oplus f_1(0)))\oplus f_8(f_3(X\oplus f_1(0))\oplus f_6(X\oplus f_1(0)\oplus f_4f_2(0)))\end{cases}.$$

由于 4 轮 FBC 模型求逆变换对 (L,R,S,T) 的脱密结果为:

$$\begin{cases}LL_4=T\oplus f_8(S\oplus L)\oplus f_5(S\oplus f_7(R\oplus T))\oplus f_1(LR_4)\\LR_4=S\oplus L\oplus f_6(R\oplus f_8(L\oplus S))\oplus f_3(T\oplus f_8(L\oplus S)\oplus f_5(S\oplus f_7(R\oplus T)))\\LS_4=T\oplus R\oplus f_5(S\oplus f_7(R\oplus T))\oplus f_4(L\oplus f_7(R\oplus T)\oplus f_6(R\oplus f_8(L\oplus S)))\\LT_4=L\oplus f_7(R\oplus T)\oplus f_6(R\oplus f_8(L\oplus S))\oplus f_2(LS_4)\end{cases}.$$

下面根据对 $(0,0,0,0)$ 和 $(0,X,0,0)$ 的加密结果, 选择待脱密的密文.

取 $L=L_4^1, R=R_4^1\oplus X, S=S_4^1, T=T_4^1\oplus X$, 解密可得:

$$\begin{aligned}LR_4&=f_3f_1(0)\oplus f_3(X\oplus f_1(0))\oplus f_6(f_1(0)\oplus f_4f_2(0))\oplus f_6(X\oplus f_1(0)\oplus f_4f_2(0))\\&=L_4^1\oplus S_4^1\oplus L_4^2\oplus S_4^2,\end{aligned}$$

即 $LR_4=L_4^1\oplus S_4^1\oplus L_4^2\oplus S_4^2$ 总成立.

当 ξ 是随机函数时, 如果 $X\neq0$, 则 $(0,0,0,0)\neq(0,X,0,0)$, 故由引理 1 知, $(L_4^1,R_4^1,S_4^1,T_4^1)$ 与 $(L_4^2,R_4^2,S_4^2,T_4^2)$ 相互独立且都服从均匀分布, 因而 $L_4^1\oplus S_4^1\oplus L_4^2\oplus S_4^2$ 服从均匀分布, 从而对于任意 LR_4, $LR_4=L_4^1\oplus S_4^1\oplus L_4^2\oplus S_4^2$ 成立的概率为 2^{-n}, 据此可设计区分攻击算法如下.

Step 1. 选择明文 $(0,0,0,0)$ 和明文 $(0,X,0,0)$ 且 $X\neq0$, 并得到对应的密文 $(L_4^1,R_4^1,S_4^1,T_4^1)$ 和 $(L_4^2,R_4^2,S_4^2,T_4^2)$.

Step 2. 选择密文 $(L_4^1,R_4^1\oplus X,S_4^1,T_4^1\oplus X)$, 并得到对应的明文 (LL_4,LR_4,LS_4,LT_4).

Step 3. 如果 $LR_4 = L_4^1 \oplus S_4^1 \oplus L_4^2 \oplus S_4^2$, 则判定是 4 轮 FBC 模型, 否则判定为随机置换.

4 轮 FBC 在上述攻击下, 与随机函数的区分优势为 $1-2^{-n}$, 又因为随机置换与随机函数在自适应选择明文密文攻击下[1], 最大区分优势 $< 2^{-16n}$, 因而由引理 5 知, 该攻击与随机置换的区分优势 $\geqslant 1-2^{-n}-2^{-16n}$. 这说明 4 轮 FBC 在自适应选择明文密文攻击下与随机置换可以区分.

证毕.

定理 3. 设 5 轮 FBC 模型的 F 函数都是从 $rand^{n\to n}$ 中独立等概选择的, 则 $\varphi(f_1,\dots,f_{10})$ 是超伪随机置换, 即对于任意选定的 q 个选择明密对, $\varphi(f_1,\dots,f_{10})$ 与随机置换的最大区分优势小于 $q(q-1)2^{2-n}$.

证明: 设 A 是一个区分攻击算法, 对于自适应性选择明密文攻击, 设:

$$H=\left\{\left((l_0^i,r_0^i,s_0^i,t_0^i)_{i=1}^q,(l_5^i,r_5^i,s_5^i,t_5^i)_{i=1}^q\right):\varphi(f_1,\dots,f_{10})(l_0^i,r_0^i,s_0^i,t_0^i)=(l_5^i,r_5^i,s_5^i,t_5^i),1\leqslant i\leqslant q\right\},$$

其中, $\left((l_0^i,r_0^i,s_0^i,t_0^i),(l_5^i,r_5^i,s_5^i,t_5^i)\right)$ 是 q 次选择明文密文攻击的查询结果, 且 $(l_0^i,r_0^i,s_0^i,t_0^i)$ 是互不相同的明文.

由 FBC 模型的定义知:

$$\begin{cases} l_1^i=r_0^i\oplus f_1\left(l_0^i\right)\\ r_1^i=l_0^i\oplus t_1^i\\ s_1^i=l_1^i\oplus t_0^i\\ t_1^i=s_0^i\oplus f_2\left(t_0^i\right)\end{cases},\begin{cases} l_2^i=r_1^i\oplus f_3\left(l_1^i\right)\\ r_2^i=l_1^i\oplus t_2^i\\ s_2^i=l_2^i\oplus t_1^i\\ t_2^i=s_1^i\oplus f_4\left(t_1^i\right)\end{cases},\begin{cases} l_3^i=r_2^i\oplus f_5\left(l_2^i\right)\\ r_3^i=l_2^i\oplus t_3^i\\ s_3^i=l_3^i\oplus t_2^i\\ t_3^i=s_2^i\oplus f_6\left(t_2^i\right)\end{cases},\begin{cases} l_4^i=r_3^i\oplus f_7\left(l_3^i\right)\\ r_4^i=l_3^i\oplus t_4^i\\ s_4^i=l_4^i\oplus t_3^i\\ t_4^i=s_3^i\oplus f_8\left(t_3^i\right)\end{cases},\begin{cases} l_5^i=r_4^i\oplus f_9\left(l_4^i\right)\\ r_5^i=l_4^i\oplus t_5^i\\ s_5^i=l_5^i\oplus t_4^i\\ t_5^i=s_4^i\oplus f_{10}\left(t_4^i\right)\end{cases}.$$

知:

$$\begin{cases} f_1(l_0^i)\oplus f_8(t_3^i)\oplus f_5(l_2^i)=r_0^i\oplus s_5^i\oplus l_5^i\\ f_2(t_0^i)\oplus f_7(l_3^i)\oplus f_6(t_2^i)=s_0^i\oplus r_5^i\oplus t_5^i\\ f_2(t_0^i)\oplus f_3(l_1^i)\oplus f_7(l_3^i)\oplus f_{10}(s_5^i\oplus l_5^i)=l_0^i\oplus s_0^i\oplus t_5^i\\ f_1(l_0^i)\oplus f_4(t_1^i)\oplus f_8(t_3^i)\oplus f_9(r_5^i\oplus t_5^i)=r_0^i\oplus s_0^i\oplus l_5^i\end{cases}\tag{2}$$

记 $F(l_0^i,r_0^i,s_0^i,t_0^i)=\varphi(f_1,\dots,f_{10})(l_0^i,r_0^i,s_0^i,t_0^i)$, 可知 $F(l_0^i,r_0^i,s_0^i,t_0^i)=(l_5^i,r_5^i,s_5^i,t_5^i)$成立蕴含公式 (2) 成立, 设 $F(l_0^i,r_0^i,s_0^i,t_0^i)=(l_5^i,r_5^i,s_5^i,t_5^i)$成立的概率为 P'_{FBC}, 公式 (2) 成立的概率为 P'_*, 则有 $P'_{\mathrm{FBC}}\leqslant P'_*$.

定义查询序列构成的集合如下:

$Bad(H)=\left\{\left((l_0^i,r_0^i,s_0^i,t_0^i)_{i=1}^q,(l_5^i,r_5^i,s_5^i,t_5^i)_{i=1}^q\right):\exists 1\leqslant i<j\leqslant q,\text{使}l_2^i=l_2^j,t_2^i=t_2^j,l_3^i=l_3^j,t_3^i=t_3^j\text{中至少一种情况发生}\right\}$ 现设查询的序列 $\left\{\left((l_0^i,r_0^i,s_0^i,t_0^i)_{i=1}^q,(l_5^i,r_5^i,s_5^i,t_5^i)_{i=1}^q\right)\right\}\notin Bad(H)$.

(1) 由于 $l_2^1,l_2^2,\dots,l_2^q$ 互不相同, 故由 f_5 是随机函数知 $(f_5(l_2^1),f_5(l_2^2),\dots,f_5(l_2^q))$ 服从均匀分布, 再由 f_1,f_5,f_8 相互独立和引理 2 知:

$$\left(f_1(l_0^1),f_1(l_0^2),\dots,f_1(l_0^q)),(f_5(l_2^1),f_5(l_2^2),\dots,f_5(l_2^q)),(f_8(t_3^1),f_8(t_3^2),\dots,f_8(t_3^q)\right),$$

相互独立, 故由 $(f_5(l_2^1),f_5(l_2^2),\dots,f_5(l_2^q))$ 服从均匀分布和引理 3 知

$$\left(f_1(l_0^1)\oplus f_8(t_3^1)\oplus f_5(l_2^1),f_1(l_0^2)\oplus f_8(t_3^2)\oplus f_5(l_2^2),\dots,f_1(l_0^q)\oplus f_8(t_3^q)\oplus f_5(l_2^q)\right),$$

服从均匀分布.

同理可证, $(f_2(t_0^1)\oplus f_7(l_3^1)\oplus f_6(t_2^1),\dots,f_2(t_0^q)\oplus f_7(l_3^q)\oplus f_6(t_2^q))$, $(f_2(t_0^1)\oplus f_3(l_1^1)\oplus f_7(l_3^1)\oplus f_{10}(s_5^1\oplus l_5^1),\dots,$ $f_2(t_0^q)\oplus f_3(l_1^q)\oplus f_7(l_3^q)\oplus f_{10}(s_5^q\oplus l_5^q)\right)$ 和$\left(f_1(l_0^1)\oplus f_4(t_1^1)\oplus f_8(t_3^1)\oplus f_9(r_5^1\oplus t_5^1),\dots,f_1(l_0^q)\oplus f_4(t_1^q)\oplus f_8(t_3^q)\oplus f_9(r_5^q\oplus t_5^q)\right)$ 都服从均匀分布.

(2) 记 $\xi_5=(f_5(l_2^1),\dots,f_5(l_2^q))$, $\xi_6=(f_6(t_2^1),\dots,f_6(t_2^q))$, $\xi_7=(f_7(l_3^1),\dots,f_7(l_3^q))$, $\xi_8=(f_8(t_3^1),\dots,f_8(t_3^q))$, 则由 f_5,f_6,f_7,f_8 相互独立和各自的 q 个输入互不相同的假设知, $f_5(l_2^i),f_6(t_2^i),f_7(l_3^i),f_8(t_3^i)$ 相互独立, 从而 $(\xi_5,\xi_6,\xi_7,\xi_8)$ 服从均匀分布, 进而 $(\xi_8\oplus\xi_5,\xi_7\oplus\xi_6,\xi_7,\xi_8)$ 服从均匀分布.

令:

$$\begin{cases}\xi_1=(f_1(l_0^1),\dots,f_1(l_0^q)),\ \xi_2=(f_2(t_0^1),\dots,f_2(t_0^q)),\ \xi_3=(f_3(l_1^1),\dots,f_3(l_1^q)),\ \xi_4=(f_4(t_1^1),\dots,f_4(t_1^q))\\ \xi_9=(f_9(r_5^1\oplus t_5^1),\dots,f_9(r_5^q\oplus t_5^q)),\ \xi_{10}=(f_{10}(s_5^1\oplus l_5^1),\dots,f_{10}(s_5^q\oplus l_5^q))\end{cases},$$

则由 $f_1,f_2,\dots,f_{10}$ 相互独立和引理 2 知 $\xi_1,\xi_2,\dots,\xi_{10}$ 相互独立, 从而 $(\xi_1,\xi_2,\xi_3,\xi_4,\xi_9,\xi_{10})$ 与 $(\xi_6,\xi_8,\xi_7,\xi_5)$ 独立. 由引理 4

知 $(\xi_1,\xi_2,\xi_2\oplus\xi_3\oplus\xi_{10},\xi_1\oplus\xi_4\oplus\xi_9)$ 与 $(\xi_8\oplus\xi_5,\xi_7\oplus\xi_6,\xi_7,\xi_8)$ 相互独立, 再由 $(\xi_8\oplus\xi_5,\xi_7\oplus\xi_6,\xi_7,\xi_8)$ 服从均匀分布和引理 3 知 $(\xi_1\oplus\xi_8\oplus\xi_5,\xi_2\oplus\xi_7\oplus\xi_6,\xi_2\oplus\xi_3\oplus\xi_7\oplus\xi_{10},\xi_1\oplus\xi_4\oplus\xi_8\oplus\xi_9)$ 服从均匀分布.

由此可知, 在查询的序列 $\left\{\left((l_0^i,r_0^i,s_0^i,t_0^i)_{i=1}^q,(l_5^i,r_5^i,s_5^i,t_5^i)_{i=1}^q\right)\right\}\notin Bad(H)$ 时, 公式 (2) 成立的概率: $P'_*=2^{-4qn}$.

考虑同样的查询序列, 对于随机置换 ξ, 由引理 6 知 $P_{permu}\geqslant 2^{-4qn}$, 从而由 $P'_*=2^{-4qn}\geqslant P'_{\mathrm{FBC}}$ 知, $P_{permu}\geqslant P'_{\mathrm{FBC}}$, 再记 $P_{permu}(x,y)$ 和 $P'_{\mathrm{FBC}}(x,y)$ 分别是查询随机置换和查询 5 轮 FBC 模型时查询序列全部吻合的概率, 则利用 q 个选择明密文的查询结果进行区分攻击的区分优势为:

$$\begin{aligned}\rho&=\frac{1}{2^{4qn}}\left|\sum_{(x,y)\in\overline{Bad(H)}}[P_{permu}(x,y)-P'_{\mathrm{FBC}}(x,y)]+\sum_{(x,y)\in Bad(H)}[P_{permu}(x,y)-P'_{\mathrm{FBC}}(x,y)]\right|\\&\leqslant\frac{1}{2^{4qn}}\left|\sum_{(x,y)\in\overline{Bad(H)}}[P_{permu}(x,y)-P'_{\mathrm{FBC}}(x,y)]\right|+\frac{1}{2^{4qn}}\left|\sum_{(x,y)\in Bad(H)}[P_{permu}(x,y)-P'_{\mathrm{FBC}}(x,y)]\right|\\&\leqslant 2^{-4qn}\sum_{(x,y)\in\overline{Bad(H)}}P_{permu}(x,y)+2^{-4qn}\sum_{(x,y)\in Bad(H)}[1-0]\\&\leqslant P_{permu}(x,y)+2^{-4qn}\cdot|Bad(H)|.\end{aligned}$$

下面计算 $|Bad(H)|$ 的上界.

记 $x^i=(l_0^i,r_0^i,s_0^i,t_0^i)$, $y^i=(l_5^i,r_5^i,s_5^i,t_5^i)$, 设 $Bad(H_1)=\{(x^i,y^i)_{i=1}^q:\exists 1\leqslant i<j\leqslant q,\text{使}t_2^i=l_2^j\}$, $Bad(H_2)=\{(x^i,y^i)_{i=1}^q:\exists 1\leqslant i<j\leqslant q,\text{使}t_2^i=t_2^j\}$, $Bad(H_3)=\{(x^i,y^i)_{i=1}^q:\exists 1\leqslant i<j\leqslant q,\text{使}l_3^i=l_3^j\}$ 和 $Bad(H_4)=\left\{(x^i,y^i)_{i=1}^q:\exists 1\leqslant i<j\leqslant q,\text{使}t_3^i=t_3^j\right\}$, 则有 $|Bad(H)|\leqslant|Bad(H_1)|+|Bad(H_2)|+|Bad(H_3)|+|Bad(H_4)|$, 由引理 7 知 $|Bad(H_i)|\leqslant 2^{(4q-1)n}\cdot q(q-1),i=1,2,3,4$, 所以 $|Bad(H)|\leqslant q(q-1)2^{(4q-1)n+2}$.

由引理 6 知 $p_{permu}(x,y)<3\cdot 2^{-4qn}$, 故区分优势 $\rho<3\cdot 2^{-4qn}+q(q-1)2^{-n+2}\approx q(q-1)2^{2-n}$, 这说明在自适应性选择明文密文攻击条件下, 5 轮 FBC 和随机置换不可区分.

证毕.

5 结束语

本文采用判断伪随机性和超伪随机性的方法, 分析了 FBC 模型的可证明安全性. 结论表明在选择明文攻击条件下, 4 轮 FBC 和随机置换不可区分, 因而满足伪随机性; 在自适应性选择明密文条件下, 5 轮 FBC 和随机置换不可区分, 因而满足超伪随机性, 这个结果比 Feistel 结构的超伪随机性少了一轮, 这应该是其轮函数的主干是两路 Feistel 结构并置的原因.

References:

[1] Luby M, Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing, 1988, 17(2): 373–386. [doi: 10.1137/0217022]

[2] Wu WL. Pseudorandomness of Camellia-like scheme. Journal of Computer Science and Technology, 2006, 21(1): 82–88. [doi: 10.1007/s11390-006-0082-0]

[3] Suzaki T, Minematsu K. Improving the generalized Feistel. In: Proc. of the 17th Int'l Workshop on Fast Software Encryption. Seoul: Springer, 2010. 19–39. [doi: 10.1007/978-3-642-13858-4_2]

[4] Kang JS, Yi O, Hong D, Cho H. Pseudorandomness of MISTY-type transformations and the block cipher KASUMI. In: Proc. of the 6th Australasian Conf. on Information Security and Privacy. Sydney: Springer, 2001. 60–73. [doi: 10.1007/3-540-47719-5_7]

[5] Guo R, Jin CH. On the pseudorandomness of the Lai-Massey scheme. Journal of Electronics & Information Technology, 2014, 36(4): 828–833 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2013.00870]

[6] Dodis Y, Katz J, Steinberger J, *et al.* Provable security of substitution-permutation networks. 2017. https://eprint.iacr.org/2017/016

[7] Guo C, Standaert FX, Wang WJ, Wang X, Yu Y. Provable security of SP networks with partial non-linear layers. IACR Trans. on Symmetric Cryptology, 2021, 2021(2): 353–388. [doi: 10.46586/tosc.v2021.i2.353-388]

[8] Feng XT, Zeng XY, Zhang F, Zeng G, Tang D, Gan GH, Wang YX. On the lightweight block cipher FBC. Journal of Cryptologic

Research, 2019, 6(6): 768–785 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000340]

[9] Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997. [doi: 10.1201/9780429466335]

附中文参考文献:

[5] 郭瑞, 金晨辉. Lai-Massey结构伪随机特性研究. 电子与信息学报, 2014, 36(4): 828–833. [doi: 10.3724/SP.J.1146.2013.00870]

[8] 冯秀涛, 曾祥勇, 张凡, 曾光, 唐灯, 甘国华, 王永兴. 轻量级分组密码算法FBC. 密码学报, 2019, 6(6): 768–785. [doi: 10.13868/j.cnki.jcr.000340]

附录 A. 引理证明

引理 2. 设 $f_1,f_2,\ldots,f_t$ 是 $rand^{m\to n}$ 上相互独立的随机函数, $x_{i,j}\in\{0,1\}^m, 1\leqslant i\leqslant t, 1\leqslant j\leqslant k$, 则 t 个随机变量组 $(f_1(x_{1,1}),f_1(x_{1,2}),\ldots,f_1(x_{1,k})),\ldots,(f_t(x_{t,1}),f_t(x_{t,2}),\ldots,f_t(x_{t,k}))$ 相互独立.

证明: 设 $y_{i,j}\in\{0,1\}^n, 1\leqslant i\leqslant t, 1\leqslant j\leqslant k$, 现考察使得 $f_i(x_{i,j})=y_{i,j}$ 对 $1\leqslant i\leqslant t, 1\leqslant j\leqslant k$ 成立的函数 $(f_1,f_2,\ldots,f_t)$ 的个数.

如果存在 $1\leqslant i\leqslant t$ 和 $1\leqslant j_1,j_2\leqslant k$ 使得 $x_{i,j_1}=x_{i,j_2}$ 但 $y_{i,j_1}\neq y_{i,j_2}$, 则有 $p(f_i(x_{i,j})=y_{i,j}, 1\leqslant j\leqslant k)=0$ 和 $p(f_i(x_{i,j})=y_{i,j}, 1\leqslant i\leqslant t, 1\leqslant j\leqslant k)=0$.

此时有:

$$p(f_i(x_{i,j})=y_{i,j}, 1\leqslant i\leqslant t, 1\leqslant j\leqslant k)=\prod_{i=1}^{t}p(f_i(x_{i,j})=y_{i,j}, 1\leqslant j\leqslant k).$$

下设对于 $1\leqslant i\leqslant t$, $1\leqslant j\leqslant k$, 当 $x_{i,j_1}=x_{i,j_2}$ 都有 $y_{i,j_1}=y_{i,j_2}$. 不妨设对于 $1\leqslant i\leqslant t$, $x_{i,1},x_{i,2},\ldots,x_{i,k}$ 中共有 w_i 个不同元且 $x_{i,1},x_{i,2},\ldots,x_{i,w_i}$ 互不相同.

由于 f_1 是随机函数, 故在 $f_1(x_{1,j})=y_{1,j}$ 对 $1\leqslant j\leqslant w_1$ 成立时, 对 $\forall x\in\{0,1\}^m\backslash\{x_{1,1},x_{1,2},\ldots,x_{1,w_1}\}$, $f_1(x)$ 都有 2^n 种不同的取法, 故此时 f_1 共有 $(2^n)^{2^m-w_1}$ 种不同的取法. 又因 f_2 与 f_1 独立, 因而 f_1 的取定不影响 f_2 的取值, 故在 f_1 取定时, 对 $\forall x\in\{0,1\}^m\backslash\{x_{2,1},x_{2,2},\ldots,x_{2,w_2}\}$, $f_2(x)$ 都有 2^n 种不同的取法, 故此时 f_2 共有 $(2^n)^{2^m-w_2}$ 种不同的取法. 同理, 在 $f_1,f_2,\ldots,f_{t-1}$ 取定时, f_t 共有 $(2^n)^{2^m-w_t}$ 种不同的取法, 这说明使得 $f_i(x_{i,j})=y_{i,j}$ 对 $1\leqslant i\leqslant t, 1\leqslant j\leqslant w_i$ 成立的函数 $(f_1,f_2,\ldots,f_t)$ 的个数为 $\prod_{i=1}^{t}(2^n)^{(2^m-w_i)}$. 又因不加任何限制时 $(f_1,f_2,\ldots,f_t)$ 的个数为 $\prod_{i=1}^{t}(2^n)^{2^m}$, 因而:

$$\begin{aligned}p(f_i(x_{i,j})=&y_{i,j}, 1\leqslant i\leqslant t, 1\leqslant j\leqslant k)=p(f_i(x_{i,j})=y_{i,j}, 1\leqslant i\leqslant t, 1\leqslant j\leqslant w_i)\\&=\frac{\prod_{i=1}^{t}(2^n)^{(2^m-w_i)}}{\prod_{i=1}^{t}(2^n)^{2^m}}=\frac{1}{\prod_{i=1}^{t}(2^n)^{w_i}}=\prod_{i=1}^{t}\prod_{j=1}^{w_i}p(f_i(x_{i,j})=y_{i,j})\\&=\prod_{i=1}^{t}p(f_i(x_{i,j})=y_{i,j}, 1\leqslant j\leqslant w_i)=\prod_{i=1}^{t}p(f_i(x_{i,j})=y_{i,j}, 1\leqslant j\leqslant k).\end{aligned}$$

这说明此时有 $p(f_i(x_{i,j})=y_{i,j}, 1\leqslant i\leqslant t, 1\leqslant j\leqslant k)=\prod_{i=1}^{t}p(f_i(x_{i,j})=y_{i,j}, 1\leqslant j\leqslant k)$, 故总有:

$$p(f_i(x_{i,j})=y_{i,j}, 1\leqslant i\leqslant t, 1\leqslant j\leqslant k)=\prod_{i=1}^{t}p(f_i(x_{i,j})=y_{i,j}, 1\leqslant j\leqslant k).$$

这说明 $(f_1(x_{1,1}),f_1(x_{1,2}),\ldots,f_1(x_{1,k})),\ldots,(f_t(x_{t,1}),f_t(x_{t,2}),\ldots,f_t(x_{t,k}))$ 相互独立.

证毕.

引理 3: 设 ξ 和 $\eta_1,\ldots,\eta_k$ 都是有限群 Ω 上的随机变量, 如果 ξ 在 Ω 上服从均匀分布且 ξ 与 $(\eta_1,\ldots,\eta_k)$ 独立, 则

$\xi+\sum_{i=1}^{k}\eta_i$ 在 Ω 上服从均匀分布.

证明: 设 $a\in\Omega$, $\eta=(\eta_1,\ldots,\eta_k)$, 则由全概率公式和 ξ 与 η 独立及 ξ 在 Ω 上服从均匀分布知:

$$p(\xi+\sum_{i=1}^{k}\eta_i=a)=\sum_{b\in\Omega^k}p(\xi+\sum_{i=1}^{k}\eta_i=a,\eta=b)=\sum_{b\in\Omega^k}p(\xi=a-\sum_{i=1}^{k}b_i,\eta=b)$$

$$=\sum_{b\in\Omega^k}p(\xi=a-\sum_{i=1}^{k}b_i)p(\eta=b)=\sum_{b\in\Omega^k}\frac{1}{|\Omega|}p(\eta=b)=\frac{1}{|\Omega|}\sum_{b\in\Omega^k}p(\eta=b)=\frac{1}{|\Omega|}.$$

证毕.

引理 4. 设 ξ 和 η 都是有限集 Ω 上相互独立的随机变量, f,g 是 Ω 上的两个实数值函数, 则 $f(\xi)$ 与 $g(\eta)$ 独立.

证明: 设 R 是实数集, $a,b\in R$, 则有:

$$p(f(\xi)=a,g(\eta)=b)=\sum_{x\in\Omega,f(x)=a}\sum_{y\in\Omega,g(y)=b}p(\xi=x,\eta=y)$$

$$=\sum_{x\in\Omega,f(x)=a}\sum_{y\in\Omega,g(y)=b}p(\xi=x)p(\eta=y)=\left[\sum_{x\in\Omega,f(x)=a}p(\xi=x)\right]\left[\sum_{y\in\Omega,g(y)=b}p(\eta=y)\right]$$

$$=p(f(\xi)=a)p(g(\eta)=b).$$

因而 $f(\xi)$ 与 $g(\eta)$ 独立.

证毕.

引理 5. 设 ξ_0,ξ_1,η 都是 $Z/(m)$ 上的随机变量, 如果在已知 n 个样本的条件下, ξ_0 与 η 的最大区分优势 $\leqslant h_0$, ξ_1 与 η 的最大区分优势 $\leqslant h_1$, 则在已知 n 个样本的条件下, ξ_0 与 ξ_1 的最大区分优势 $\leqslant h_0+h_1$.

证明: 设 $\xi\in\{\xi_0,\xi_1\}$, $\Omega=\{a\in[Z(m)]^n:D(a)=1\}$ 是利用 ξ 的 n 个样本的判决 D 的判决域, 记 $a=(a_1,a_2,\ldots,a_n)\in[Z/(m)]^n$, 则 ξ_1 与 ξ_0 的最大区分优势为:

$$\frac{1}{m^n}\left|\sum_{a\in\Omega}\left[p\left(\xi_1^{(n)}=a\right)-p\left(\xi_0^{(n)}=a\right)\right]\right|=\left|\frac{1}{m^n}\sum_{a\in\Omega}\left[p\left(\xi_1^{(n)}=a\right)-p\left(\eta^{(n)}=a\right)\right]+\frac{1}{m^n}\sum_{a\in\Omega}\left[p\left(\eta^{(n)}=a\right)-p\left(\xi_0^{(n)}=a\right)\right]\right|$$

$$\leqslant\frac{1}{m^n}\left|\sum_{a\in\Omega}\left[p\left(\xi_1^{(n)}=a\right)-p\left(\eta^{(n)}=a\right)\right]\right|+\frac{1}{m^n}\left|\sum_{a\in\Omega}\left[p\left(\eta^{(n)}=a\right)-p\left(\xi_0^{(n)}=a\right)\right]\right|$$

$$\leqslant h_1+h_0.$$

证毕.

引理 6. 设 $p_{permu}(x,y)$ 为 $\{0,1\}^{4n}$ 上随机置换满足互不相同的 q 对输入输出时对应的概率, 则有 $2^{-4nq}\leqslant p_{permu}(x,y)<3\cdot2^{-4qn}$, 其中 $C_{q+1}^2\leqslant2^{4n}$.

证明: 首先, 由于 $p_{permu}(x,y)$ 为 $\{0,1\}^{4n}$ 上随机置换满足互不相同的 q 对输入输出的概率, 故:

$$p_{permu}(x,y)=\frac{\prod_{i=q}^{2^{4n}-1}(2^{4n}-i)}{2^{4n}!}=\left[\prod_{i=0}^{q-1}(2^{4n}-i)\right]^{-1}\geqslant2^{-4qn}.$$

又由 $p_{permu}(x,y)=\left[\prod_{i=0}^{q-1}(2^{4n}-i)\right]^{-1}=\frac{1}{2^{4qn}}\times\prod_{i=0}^{q-1}\frac{2^{4n}}{2^{4n}-i}=\frac{1}{2^{4qn}}\times\prod_{i=1}^{q-1}\frac{2^{4n}}{2^{4n}-i}$, 其中 $\ln\prod_{i=1}^{q-1}\frac{2^{4n}}{2^{4n}-i}=-\sum_{i=1}^{q-1}\ln\left(1-\frac{i}{2^{4n}}\right)$, 下面分析 $\ln\left(1-\frac{i}{2^{4n}}\right)$. 对于 $0<x\leqslant\frac{q}{2^{4n}}$, 这里 $q\neq2^{4n}$, 令 $f'(x)=\frac{1}{x-1}+a=\frac{1+ax-a}{x-1}$, 则有 $f'(x)=\frac{1}{x-1}+a=\frac{1+ax-a}{x-1}$, 故由 $x-1<0$ 知 $f'(x)>0$ 等价于 $1+ax-a<0$, 即 $a>\frac{1}{1-x}$, 由于 $\max\left\{\frac{1}{1-x}:0<x\leqslant\frac{q}{2^{4n}}\right\}=\frac{2^{4n}}{2^{4n}-q}$, 因而只要取 $a>\frac{2^{4n}}{2^{4n}-q}$, 就有 $f'(x)>0$, 从而对于 $0<x\leqslant\frac{q}{2^{4n}}$, 都有 $f(x)=\ln(1-x)+ax\geqslant f(0)=0$, 即 $\ln(1-x)\geqslant-ax$.

因而 $\ln\prod_{i=1}^{q-1}\frac{2^{4n}}{2^{4n}-i}=-\sum_{i=1}^{q-1}\ln\left(1-\frac{i}{2^{4n}}\right)\leqslant\frac{2^{4n}}{2^{4n}-q}\sum_{i=1}^{q-1}\frac{i}{2^{4n}}=\frac{2^{4n}}{2^{4n}-q}\times\frac{1}{2^{4n}}\times\frac{q(q-1)}{2}=\frac{C_q^2}{2^{4n}-q}$.

进而有:

$$p_{permu}(x,y)=\frac{1}{2^{4qn}}\times\prod_{i=1}^{q-1}\frac{2^{4n}}{2^{4n}-i}=\frac{1}{2^{4qn}}\mathrm{e}^{\ln\prod_{i=1}^{q-1}\frac{2^{4n}}{2^{4n}-i}}\leqslant\frac{1}{2^{4qn}}\mathrm{e}^{\frac{C_q^2}{2^{4n}-q}}.$$

故当 $C_{q+1}^2\leqslant 2^{4n}$ 时, 有 $\mathrm{e}^{\frac{C_q^2}{2^{4n}-q}}\leqslant\mathrm{e}<3$, 从而有 $p_{permu}(x,y)<3\cdot 2^{-4qn}$.

证毕.

刘楠(1977－), 女, 博士生, 副教授, 主要研究领域为密码算法的设计与分析.

于俊伟(1980－), 男, 博士, 副教授, CCF 专业会员, 主要研究领域为智能信息处理.

金晨辉(1965－), 男, 博士, 教授, 博士生导师, 主要研究领域为密码学, 信息安全.

崔霆(1985－), 男, 博士, 教授, 博士生导师, 主要研究领域为密码算法的设计与分析.