3ラウンドFeistel暗号に対するGroverのアルゴリズムを用いた効率的な鍵回復攻撃

台座 崇規[1,a)]　米山 一樹[2,b)]

概要：Feistel-KF 構造は Feistel 構造の特殊な形の一つであり，i 番目のラウンド関数は $\mathrm{F}_i(i$ 番目の鍵 $\oplus x)$ の形で表される．関数 F_i は入出力長が $n/2$ ビットの公開されたランダム関数である．3 ラウンドの Feistel-KF は古典攻撃に対し，online クエリ数 D+offline クエリ数 $T \ll 2^{n/4}$ において安全であることが Lampe と Seurin によって示されている．また，2012 年に Isobe と Shibutani が meet-in-the-middle attack により $(D,T) = (O(1), O(2^{n/2}))$ の古典攻撃を示した．しかし，彼らの攻撃では 2 個の段鍵を同時に導出しているため，Grover の量子アルゴリズムをそのまま当てはめ，2 個の段鍵の Grover 探索を行うことにより量子攻撃に拡張しようとすると，$O(2^{n/2})$ の計算量が必要となる．本稿では，量子モデルにおいて Grover のアルゴリズムを用い，段鍵を 1 個ずつ導出することにより $(D,T) = (O(1), O(2^{n/4}))$ の量子攻撃を示す．本攻撃は暗号化オラクルへの量子クエリを行わないため，Q1 model に相当する．

キーワード：共通鍵暗号，選択平文攻撃，Grover のアルゴリズム，Q1 model

Quantum Key Recovery Attack with Grover Search on 3-Round Feistel-KF Structure

Takanori Daiza[1,a)]　Kazuki Yoneyama[2,b)]

Abstract: Feistel-2 (Feistel-KF) structure is a variant of Feistel structure such that the i-th round function is given by $\mathrm{F}_i(k_i \oplus x)$, where F_i is a public random function and its input/output length is $n/2$ bits. Lampe and Seurin showed that 3-round Feistel-KF cipher is secure in the classical setting if $D + T \ll 2^{n/4}$. In 2012, Isobe and Shibutani showed a meet-in-the-middle attack which works for $(D,T) = (O(1), O(2^{n/2}))$ on 3-round Feistel-KF. In their attack, two round keys are recovered simulataneously. Hence, a naive application of Grover's algorithm needs the Grover search for two values in $T = O(2^{n/2})$. In this paper, in the quantum setting, we introduce a known plaintext attack and chosen plaintext attack on 3-round Feistel-KF using Grover's algorithm by recovering the round key one by one in $(D,T) = (O(1), O(2^{n/4}))$. Our attack does not need any quantum query to the encryption oracle and works in the Q1 model.

Keywords: symmetric cipher, chosen plaintext attack, Grover's Algorithm, Q1 model

1. はじめに

Feistel 構造はブロック暗号の代表的な構成法の一つであり，理論及び実用において重要な役割を持つ．基本的な r ラウンド Feistel 構造では，まず，平文 $P = (a_0, b_0)$ （但し，$a_0, b_0 \in \{0,1\}^{n/2}$）を全体の入力とし，各ラウンド $(i = 0, 1, \cdots, r-1)$ において以下の計算を行う．

$$(a_{i+1}, b_{i+1}) = (b_i \oplus \mathrm{R}_i(a_i), a_i)$$

ここで，$\mathrm{R}_i : \{0,1\}^{n/2} \mapsto \{0,1\}^{n/2}$ は鍵付きのランダム関数である．（**図 1** の左側を参照）最後のラウンドの計算結

[1] 茨城大学大学院理工学研究科
Graduate School of Science and Engineering, Ibaraki University
[2] 茨城大学
Ibaraki University
[a)] 20nm713t@vc.ibaraki.ac.jp
[b)] kazuki.yoneyama.sec@vc.ibaraki.ac.jp

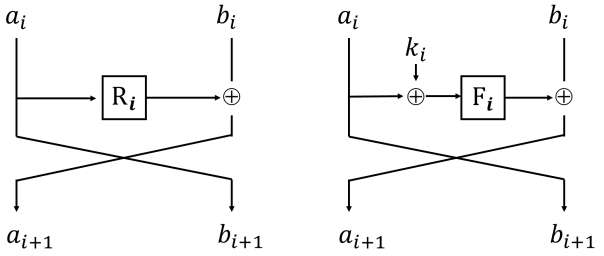

図 1 Feistel/Feistel-KF 構造
Fig. 1 Feistel/Feistel-KF structure

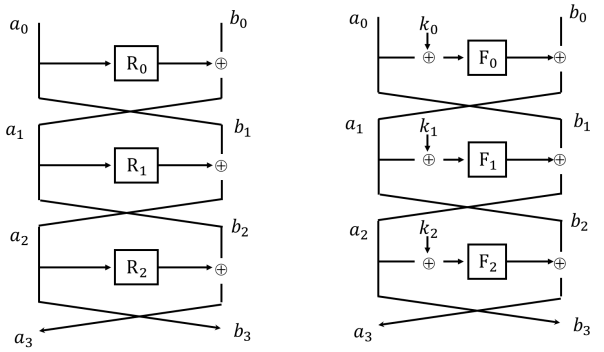

図 2 3 ラウンド Feistel/Feistel-KF 構造
Fig. 2 3-round Feistel/Feitel-KF structure

果 $C = (a_r, b_r)$ を全体の暗号文として出力する．

古典モデルにおいて，各ラウンド関数 R_i を独立なランダム関数であると考える．この仮定の下で，Luby と Rackoff [1] は，3 ラウンド Feistel 構造は $2^{n/4}$ 回までのクエリを行う選択平文攻撃 (CPA) に対して疑似ランダム置換となることを示した．また，彼らは 4 ラウンド Feistel 構造は $2^{n/4}$ 回までのクエリを行う選択暗号文攻撃 (CCA) に対して強疑似ランダム置換となることを示した．

但し，Luby と Rackoff による基本的な Feistel 構造は，各ラウンド鍵 k_i に対して鍵を埋め込まれたラウンド関数 R_i を用意するという点で，実装が困難であった．Feistel-KF（Feistel-2）構造は，前述の Feistel 構造の特殊な形であり，各ラウンド関数 R_i を $\mathrm{F}_i(k_i \oplus x)$ の形で与えることで前述の問題を解決したものである．（図 1 の右側を参照）ここで，各 F_i は入出力長が $n/2$ ビットの公開されたランダム関数である．また，$k_i \in \{0,1\}^{n/2}$ はラウンドごとの段鍵であり，独立ランダムに選ばれる．

1.1 3 ラウンド Feistel 構造への識別攻撃の関連研究

古典モデルにおいて，平文/暗号文ペアを取得するための D 回の online クエリと内部の関数 F_i を計算するオラクルへの T 回の offline クエリを行う敵について考える．ここで，online クエリとは，敵が自力で計算を行えない処理（秘密鍵を用いた暗号化/復号計算など）の結果を受け取るようなクエリを表し，offline クエリとは敵が自力で計算できる処理（公開関数の演算など）であるようなクエリを表す．Lampe と Seurin [2] は，3 ラウンド Feistel-KF 構造（**図 2** の右側）は $D + T \ll 2^{n/4}$ の非適応的選択平文攻撃 (non-adaptive CPA) に対して疑似ランダム置換となることを示した．

一方，敵が量子コンピュータを用いた計算を行うことができる量子モデルについて考える．量子モデルは，敵の暗号化オラクル (鍵の情報が含まれる) への online クエリに関する条件により分類できる．敵が量子重ね合わせ状態によって暗号化オラクルへのクエリを行い，結果を同じく重ね合わせ状態で受け取ることが可能な攻撃モデルのことを Q2 model と呼ぶ．また，敵の暗号化オラクルへの量子アクセスを認めない攻撃モデルのことを Q1 model と呼ぶ．なお，Q1 model と Q2 model のどちらにおいても，offline での計算上で別のオラクル (鍵の情報を含まない) へ量子状態によってクエリを行うことは許容される．

Q2 model において，Kuwakado と Morii [15] は，各 R_i がランダム置換の場合に 3 ラウンド Feistel 構造は擬似ランダム置換とはならないことを示した．更に，Kaplan ら [16] は，各 R_i がランダム関数の場合でも 3 ラウンド Feistel 構造は擬似ランダム置換とはならないことを示した．これらの識別攻撃は Simon の量子アルゴリズム [14] に基づく．

1.2 Feistel-KF 構造への鍵回復攻撃の関連研究

古典モデル

Isobe と Shibutani [3] は 3 ラウンド Feistel-KF に対する既知平文攻撃 (KPA) を示した．彼らの攻撃は，$(D, T) = (O(1), O(2^{n/2}))$ の meet-in-the-middle attack であり，$M = O(2^{n/2})$ の古典メモリを要する．また，彼らは 4 ラウンド以上の Feistel-KF に対する攻撃への拡張 [4] も示している．Guo ら [6] は，Demirci と Selçuk [5] が提案した meet-in-the-middle attack を 6 ラウンド Feistel-KF に適用した攻撃を示した．Dinur ら [7] は，5 ラウンド以上の（鍵が埋め込まれた）Feistel 構造に対して，dissection attack による選択平文攻撃を示し，更にメモリの使用量がより効率的な攻撃 [8] も示した．Daiza と Kurosawa [9] は，3 ラウンド Feistel-KF に対して，$DT = O(2^{n/2})$ かつメモリの使用量が $M = O(1)$ である攻撃を示した．

Q1 model

Hosoyamada と Sasaki [12] は，6-round Feistel-KF に対し，Grover のアルゴリズム [10] や Brassard らの claw-finding アルゴリズム [11] に基づき Guo らの古典攻撃を Q1 model に適用した量子選択平文攻撃を示した．彼らの攻撃は $(D, T) = (O(2^{n/2}), O(2^{n/2}))$ であり，$Q = O(2^{n/2})$ の量子ビットと $M = O(2^{n/2})$ の古典メモリを要する．

Q2 model

Hosoyamada と Sasaki [12] は，Simon のアルゴリズ

ム [14] と Grover のアルゴリズム [10] を組み合わせる Leander と May による手法 [17] を利用し，r-round Feistel-KF 構造（$r \geq 4$）の段鍵を $O(2^{(r-3)n/4})$ の計算量で求める量子選択平文攻撃を示した．台座と黒澤 [18] は，$n/2$ ビットの Simon の問題を解くことにより，3 ラウンド Feistel-KF の段鍵を量子多項式時間で求める量子選択平文攻撃を示した．Cid ら [19] は，$n/2+1$ ビットの Simon の問題を解くことにより，d-branch $(2d-1)$ ラウンド contracting Feistel-KF 構造の段鍵を量子多項式時間で求める量子選択平文攻撃を示した．

1.3 本研究の動機

Isobe と Shibutani [3] による前述の古典攻撃では，全探索によって 2 個の段鍵を同時に求めることを行っている．そのため，彼らの古典攻撃を単純に Q1 model における攻撃に拡張しようとすると，Grover の量子アルゴリズム [10] による $n/2 \times 2 = n$ ビットの値の Grover 探索になり，$T = O(2^{n/2})$ の計算量が必要となる．また，3 ラウンド Feistel-KF を 2 回繰り返し，6 ラウンドとみなすことで Hosoyamada と Sasaki [12] による前述の 6 ラウンド Feistel-KF への Q1 model における攻撃をそのまま利用することができるが，やはり $T = O(2^{n/2})$ の計算量が必要となる．我々の知る限りでは，古典攻撃の計算量より（漸近的に）効率の良い 3 ラウンド Feistel-KF への Q1 model における鍵回復攻撃は知られていない．

1.4 本研究の貢献

本稿では，古典攻撃より効率的な 3 ラウンド Feistel-KF への Q1 model における鍵回復攻撃を初めて提案する．我々の攻撃手法は，台座と黒澤 [9] の古典攻撃を拡張し，Grover の量子アルゴリズム [10] を用い，段鍵を 1 個ずつ導出する．まず，$(D, T) = (O(1), O(2^{n/4}))$ での量子既知平文攻撃を示す．次に，計算量は提案量子既知平文攻撃と漸近的に等しいが，ゲート数を改善した量子選択平文攻撃を示す．これらの攻撃では $Q = O(n)$ の量子ビットと $M = O(1)$ の古典メモリを用いる．また，本攻撃は暗号化オラクルへの量子クエリを行わないため，Q1 model となる．以上の関連研究との関係を**表 1** に示す．

2. 準備

ビット長が等しい 2 個の値 x, y に対し，$x \oplus y$ はビットごとの排他的論理和を表す．

2.1 量子オラクル

関数 $f : \{0,1\}^{l_1} \mapsto \{0,1\}^{l_2}$ の計算結果を量子オラクル O_f へのクエリによって得るとき，O_f はユニタリ演算子として一般的に次のような形で与えられる．

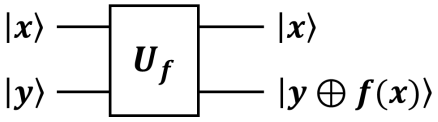

図 3 回路上の量子オラクル
Fig. 3 A given oracle on quantum circuit

$$O_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

ただし，$x \in \{0,1\}^{l_1}, y \in \{0,1\}^{l_2}$．また，$O_f$ のユニタリ演算子 U_f は量子回路上で**図 3** のように表される．

2.2 Grover の量子アルゴリズム

Grover の量子アルゴリズム [10] は，N 個の要素を持つデータベースから条件を満たす要素を $O(N^{1/2})$ の計算量で探索するアルゴリズムである．まず，以下の問題を考える．

[Grover の問題]
ある関数 $g : \{0,1\}^n \mapsto \{0,1\}$ は，特定の入力 $x = x_0$ に対してのみ $g(x_0) = 1$ を出力し，その他の入力 $x \neq x_0$ に対しては $g(x) = 0$ を出力するものとする．このとき，x_0 を求める．

上記の問題を解く Grover の量子アルゴリズムは，関数 g の計算に対応するユニタリ演算子 U_g を使用し，量子回路上で以下のような手順で行われる．(補助的な 1 量子ビットを使用せず，$g(x)$ の出力の値を格納せずに Grover 探索を行う方法もよく知られているが，簡単化のために本稿では補助ビットを使用するものとする．)
以降，$N = 2^n$ とする．

(1) 初期状態 $|0^n\rangle|0\rangle$ を用意する．
(2) 末尾 1 ビットに X ゲートを作用させ，$|0^n\rangle|1\rangle$ を得る．
(3) 先頭 n ビットに H ゲートを作用させ，

$$\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\right)|1\rangle$$

を得る．
(4) 全体に U_g を作用させ (g へのクエリを行うことに相当する)，

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|1 \oplus g(x)\rangle$$

を得る．
(5) 先頭 n ビットに拡散行列と呼ばれる $N \times N$ 行列

$$D_N = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{bmatrix}$$

を作用させる．
(6) 手順 (4)(5) の処理 (Grover iteration) を繰り返す．

表 1　Feistel-KF への鍵回復攻撃
Table 1　Related Key Recovery Attacks on Feistel-KF

文献	ラウンド数	モデル	攻撃	D	T	Q	M
[3]	3	古典	KPA	$O(1)$	$O(2^{n/2})$	-	$O(2^{n/2})$
[9]	3	古典	KPA	$O(1)$	$O(2^{n/2})$	-	$O(1)$
[9]	3	古典	CPA	$O(2^{n/4})$	$O(2^{n/4})$	-	$O(1)$
[4]	4	古典	CPA	$O(1)$	$O(2^{n/2})$	-	$O(2^{n/2})$
[6]	6	古典	CPA	$O(2^{3n/4})$	$O(2^{3n/4})$	-	$O(2^{n/2})$
[12]	$r \geq 4$	Q2	qCPA	$O(2^{(r-3)n/4})$	$O(n^3 2^{(r-3)n/4})$	$O(n^2)$	$O(n)$
[18]	3	Q2	qCPA	$O(n)$	$O(n^3)$	$O(n)$	$O(n)$
[19]	$2d-1$	Q2	qCPA	$O(Poly(n))$	$O(Poly(n))$	$O(Poly(n))$	$O(Poly(n))$
[12]	6	Q1	qCPA	$O(2^{n/2})$	$O(2^{n/2})$	$O(2^{n/2})$	$O(2^{n/2})$
提案攻撃 1（4.1 節）	3	Q1	qKPA	$O(1)$	$O(2^{n/4})$	$O(n)$	$O(1)$
提案攻撃 2（4.2 節）	3	Q1	qCPA	$O(1)$	$O(2^{n/4})$	$O(n)$	$O(1)$

D は平文/暗号文ペアの個数，T は計算時間，Q は量子メモリのサイズ，M は古典メモリのサイズをそれぞれ表す．

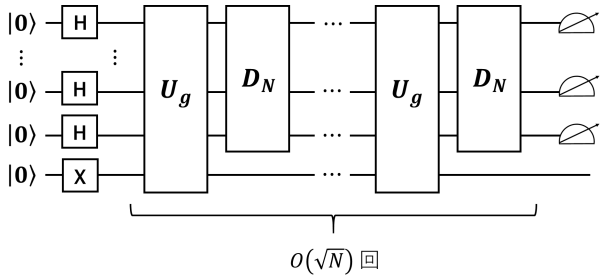

図 4　Grover のアルゴリズム

(7) 最後に先頭 n ビットを測定する．

なお，補助的な 1 量子ビットを利用しない方法では，手順 (4) において

$$U_g|x\rangle = \begin{cases} -|x\rangle & if\ x = x_0 \\ |x\rangle & if\ x \neq x_0 \end{cases}$$

の処理を行う．

手順 (4)(5) の処理 (Grover iteration) を $\left\lfloor \frac{\pi}{4}\sqrt{N} + \frac{1}{2} \right\rfloor$ 回繰り返すと，手順 (7) にて 1 に近い確率で $x = x_0$ を得る．このときの計算量は $O(2^{n/2})$ となる．

2.3　Hosoyamada と Sasaki の claw-finding

claw-finding アルゴリズムは, ハッシュ関数の衝突発見を行う量子アルゴリズムであり，Brassard ら [11] により提案された．その後，Hosoyamada と Sasaki [12] は次のような問題を考え，別の claw-finding アルゴリズムを提案した．

[claw-finding 問題]

関数 $f : \{0,1\}^u \times \{0,1\}^v \mapsto \{0,1\}^l$ と $g : \{0,1\}^v \mapsto \{0,1\}^l$ がブラックボックスで与えられており，ある 1 つのペア $(x, y) \in \{0,1\}^u \times \{0,1\}^v$ が $f(x, y) = g(y)$ を満たすとする．このとき，(x, y) を求める．但し，g のオラクルには古典クエリのみが可能であり，f のオラクルには量子クエリが可能でユニタリ演算子として量子回路上に実装されている．

Hosoyamada と Sasaki による claw-finding アルゴリズム [12] は $Q = O((u+v)2^p)$ $(p \leq v)$ の量子ビット，$M = O(2^v)$ の古典メモリを使用し，この問題を $O(T^c_{g,all} + 2^{\frac{u}{2}+v-p} \cdot T^q_f)$ の計算時間で解くことができる．ここで，$T^c_{g,all}$ は，古典クエリに基づき全ての y に対して $(y, g(y))$ を求めるまでの時間であり，T^q_f は f を実装した量子回路を 1 回実行する時間である．

3.　既存の攻撃

3.1　3 ラウンド Feistel-KF 構造

全体の平文を $P = (a_0, b_0)$ $(a_0, b_0 \in \{0,1\}^{n/2})$ とする．以下の計算を行い，$C = (a_3, b_3)$ を全体の暗号文として出力する．

$$(a_1, b_1) \leftarrow (b_0 \oplus \mathrm{F}_0(k_0 \oplus a_0), a_0)$$

$$(a_2, b_2) \leftarrow (b_1 \oplus \mathrm{F}_1(k_1 \oplus a_1), a_1)$$

$$(a_3, b_3) \leftarrow (b_2 \oplus \mathrm{F}_2(k_2 \oplus a_2), a_2)$$

a_3，b_3 の値は次の通りである．

$$\begin{aligned} b_3 &= a_2 \\ &= b_1 \oplus \mathrm{F}_1(k_1 \oplus a_1) \\ &= a_0 \oplus \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0 \oplus a_0) \oplus b_0) \end{aligned} \tag{1}$$

$$\begin{aligned} a_3 &= b_2 \oplus \mathrm{F}_2(k_2 \oplus a_2) \\ &= a_1 \oplus \mathrm{F}_2(k_2 \oplus b_1 \oplus \mathrm{F}_1(k_1 \oplus a_1)) \\ &= b_0 \oplus \mathrm{F}_0(k_0 \oplus a_0) \oplus \\ &\quad \mathrm{F}_2(k_2 \oplus \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0 \oplus a_0) \oplus b_0) \oplus a_0) \end{aligned} \tag{2}$$

以降において，関数 $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2$ は公開されたランダム関数（鍵の情報を含まない）であり，offline での計算上で $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2$ オラクルへの古典/量子クエリが可能であるとする．

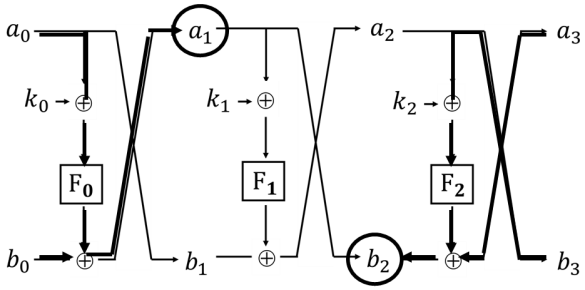

図 5 Isobe と Shibutani の MITM 攻撃 [3]
Fig. 5 MITM Attack on 3-round by Isobe and Shibutani[3]

3.2 3 ラウンド Feistel-KF への古典 MITM 攻撃 [3]

Isobe と Shibutani は，3 ラウンド Feistel-KF への meet-in-the-middle attack による既知選択平文攻撃 (KPA) を示した．以下にその手順を示す．

$D = 2$ 個の平文/暗号文ペア (P_1, C_1)，(P_2, C_2) が与えられているとし，$P_1 = (a_0, b_0)$，$C_1 = (a_3, b_3)$ とする．

(1) 全ての $i \in \{0,1\}^{n/2}$ に対し，$i \oplus a_0$ を入力とした F_0 オラクルへの古典クエリを行い，

$$a_{1,i} = \mathrm{F}_0(i \oplus a_0) \oplus b_0$$

を計算する．テーブル A_1 に各 $(i, a_{1,i})$ を記録する．

(2) 全ての $j \in \{0,1\}^{n/2}$ に対し，$j \oplus b_3$ を入力とした F_2 オラクルへの古典クエリを行い，

$$b_{2,j} = \mathrm{F}_2(j \oplus b_3) \oplus a_3$$

を計算する．テーブル A_2 に各 $(j, b_{2,j})$ を記録する．

(3) A_1, A_2 を用いて $a_{1,i} = b_{2,j}$ を満たすような (i, j) を探す．(**図 5** を参照)

(4) 別の平文/暗号文ペア P_2, C_2 においても等式が成立するかを確める．成り立てば，$(k_0, k_2) = (i, j)$ とする．

(5) 全ての $\kappa \in \{0,1\}^{n/2}$ に対し，

$$\mathrm{F}_1(\kappa \oplus a_{1,i}) \oplus a_0 = b_3$$

が成り立つかどうかを確かめる．等式を満たす κ を k_1 とし，(k_0, k_1, k_2) を出力する．

この攻撃では $D = 2$ 個の平文/暗号文ペアを受け取り，$D = O(1)$ である．また，offline での計算上で $T = O(2^{n/2})$ 回の $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2$ オラクルへのクエリを行い，この際に $M = O(2^{n/2})$ の古典メモリを必要とする．

3.3 6 ラウンド Feistel-KF への量子 DS-MITM 攻撃 [12]

Demirci と Selçuk が提案した DS-MITM 攻撃 [5] では，与えられた暗号化/復号オラクルに対して鍵回復処理を行う部分と識別処理を行う部分に分けて考える．(**図 6** を参照) 攻撃の手順の概要を以下に示す．

(1) ある 1 つの鍵の推定を行う．

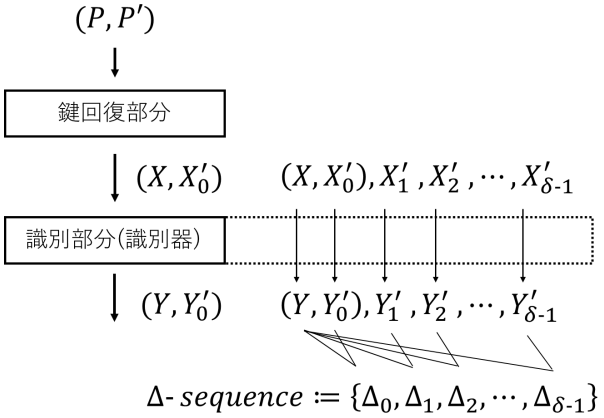

図 6 鍵回復部分と識別部分
Fig. 6 Key-recovery part and distinguisher

(2) 推定値に従い，様々な平文のペア (P, P') に対して手順 (3) から (5) を古典計算で行う．

(3) 識別部分の入力差分 $\Delta X = (X, X_0')$，出力差分 $\Delta Y = (Y, Y_0')$ を用意する．

(4) X_0' の値をずらし，$X_1', X_2', \cdots, X_{\delta-1}'$ を計算する．また，それぞれについて識別部分の出力 $Y_1', Y_2', \cdots, Y_{\delta-1}'$ を得る．

(5) Y_i' $(i = 0, 1, \cdots, \delta - 1)$ に対して，Y との差分を Δ_i とし，

$$\Delta\text{-}sequence := (\Delta_0, \Delta_1, \cdots, \Delta_{\delta-1})$$

をリスト L へ記録する．

(6) 量子回路上で Δ-*sequence* の値を求める処理を行い，L の要素との衝突判定を行う．衝突が見つかれば，鍵の推定は正しいとする．

Hosoyamada と Sasaki [12] は，拡張した claw-finding アルゴリズムを用いて Guo らの 6-round Feistel-KF への古典 DS-meet-in-the-middle attack の適用を Q1 model へ拡張した選択平文攻撃を示した．以下にその方法を簡潔に述べる．

まず，c, X を定数とする．$2 \times 2^{n/2}$ 個の平文 $\{(c, 0\cdots00), (c, 0\cdots01), \cdots, (c, 1\cdots11)\}$，$\{(c \oplus X, 0\cdots00), (c \oplus X, 0\cdots01), \cdots, (c \oplus X, 1\cdots11)\}$ を用意する．そして，暗号化オラクルへの古典クエリを行い，平文の差分 $\Delta P = (X||*)$ かつ暗号文の差分 $\Delta C = (*||0)$ を満たすような $2^{n/2}$ 個の平文のペアを記録する．この段階では，$D = O(2^{n/2})$ 回の古典クエリ，$O(2^{n/2})$ の古典メモリを必要とする．

続いて，暗号文の差分 ΔC の左半分を Y とし，次のような古典計算の関数 $g : \{0,1\}^{n/2} \mapsto \{0,1\}^{\delta n/2}$ (∴2.3 節の $v = n/2$) を考える．g は，Y を入力とし，暗号文の差分が Y となるような平文のペアを選び，Δ-*sequence* を出力する．Y を動かして g を繰り返し，リスト L に $O(2^{n/2})$ 個の

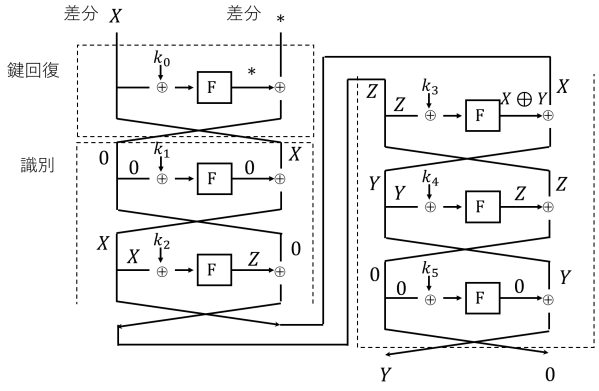

図 7 識別部分に関する入力/出力差分
Fig. 7 Input/Output difference in 5-round distinguisher

Δ-*sequence* を記録する．この段階では，$T^c_{g,all} = O(2^{n/2})$ の計算時間，$O(2^{n/2})$ の古典メモリを必要とする．

鍵 k_0 を求めるにあたり，6 ラウンドの内の鍵回復部分と識別部分（識別器）を**図 7** のように構成する．ここで，識別器の 2 ラウンド目のラウンド関数 F の出力差分の値を Z とおくと，3 ラウンド目の入力差分及び 4 ラウンド目の出力差分も Z となる．

続いて，次のような量子計算の関数 $f : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \mapsto \{0,1\}^{\delta n/2}$ ($\because$2.3 節の $u = v = n/2$) を考える．f は，量子状態 Y, Z を入力とし，Grover のアルゴリズムを用いて識別器の $2, 3, 4$ 番目のラウンド関数 F の入力/出力差分を，それぞれ $O(2^{n/4})$ の計算量と $O(n)$ の量子ビットによって求める．その後，(Y, Z) に対応する Δ-*sequence* を計算し f の出力とする．Δ-*sequence* を計算する処理は Grover 探索に比べて充分小さいため，この段階では $T^q_f = O(2^{n/4})$ の計算時間となり，$O(n)$ の量子ビットを必要とする．

claw-finding アルゴリズムでは，量子回路上で f を繰り返し呼び出し，f の出力である Δ-*sequence* と L 内に格納されている Δ-*sequence* の衝突を探す．つまり，量子状態 Y, Z から $f(Z, Y) = g(Y)$ の衝突を満たすような Z の値を決定する．このアルゴリズムでは $Q = O((u+v)2^p)$ $(p \leq v)$ の量子ビットを使用する．$p = 2^{n/2}$ としたとき，$Q = O(n2^{n/2})$ となり，計算時間は

$$\begin{aligned} T &= O(T^c_{g,all} + 2^{\frac{u}{2}+v-p} \cdot T^q_f) \\ &= O(2^{n/2} + 2^{\frac{n}{4}+\frac{n}{2}-\frac{n}{2}} \cdot 2^{n/4}) = O(2^{n/2}) \end{aligned}$$

となる．

以上の識別処理によって Z が発見できれば，鍵回復部分における鍵 k_0 の推定は正しいとする．他の段鍵についても同様の手順を行い，段鍵を全て求める．結局，6 ラウンド Feistel-KF に対するこの攻撃では $(D, T, Q, M) = (O(n2^{n/2}), O(n2^{n/2}), O(n2^{n/2}), O(n2^{n/2}))$ となる．また，3 ラウンド Feistel-KF の鍵回復攻撃にも，暗号化オラクルを 2 回連続で使用することでこの攻撃が直接適用できる．

4. 提案攻撃手法

3.2 節に示した Isobe と Shibutani の攻撃では，$n/4$ ビットの段鍵を 2 個同時に全探索する．そのため，彼らの古典攻撃を Grover の量子アルゴリズム [10] を直接適用して Q1 model に拡張しようとすると $n/2 \times 2 = n$ ビットの値の Grover 探索になり，計算量は $T = O(2^{n/2})$ となる．我々は，$T = O(2^{n/4})$ の計算量の攻撃を示す．

我々のアイディアは，式 (1)

$$b_3 = \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0 \oplus a_0) \oplus b_0) \oplus a_0$$

に含まれる k_1 と $\mathrm{F}_0(k_0 \oplus a_0)$ を分離し，Grover のアルゴリズムによって関数 F_0 の逆計算を行うことで段鍵 k_0 を鍵回復するというものである．本攻撃は暗号化オラクルへの量子クエリを行わないため Q1 model に相当する．

4.1 攻撃 1(qKPA)

関数 $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2$ は公開されたランダム関数であるとする．$\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2$ オラクルには offline 計算において量子クエリが可能で，ユニタリ演算子として量子回路上に実装されているとする．

提案量子既知平文攻撃 (qKPA) では，式 (1) における F_1 への入力 $k_1 \oplus \mathrm{F}_0(k_0 \oplus a_0) \oplus b_0$ を 2 つ求めることを行い，それらを足し合わせることにより k_1 を除去する．以下にその手順を示す．$D = 3$ 個の平文/暗号文ペア (P_1, C_1)，(P_2, C_2)，(P_3, C_3) が与えられており，$P_i = (a_{i,0}, b_{i,0})$，$C_i = (a_{i,3}, b_{i,3})$ $(i = 1, 2, 3)$ とする．

(1) (P_1, C_1)，(P_2, C_2) のそれぞれに対して

$$a_{1,0} \oplus b_{1,3} = \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0 \oplus a_{1,0}) \oplus b_{1,0})$$

$$a_{2,0} \oplus b_{2,3} = \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0 \oplus a_{2,0}) \oplus b_{2,0})$$

を計算する．(**図 8** を参照) また，上 2 式における関数 F_1 の入力の値に関して，β_1, β_2 を

$$\beta_1 = k_1 \oplus \mathrm{F}_0(k_0 \oplus a_{1,0})$$

$$\beta_2 = k_1 \oplus \mathrm{F}_0(k_0 \oplus a_{2,0})$$

とする．

(2) Grover のアルゴリズムによって

$$\mathrm{F}_1(\beta_1 \oplus b_{1,0}) = a_{1,0} \oplus b_{1,3}$$

を満たすような関数 F_1 への入力 $\beta_1 \oplus b_{1,0}$ を探索し，β_1 の値を計算する．

(3) 同様に，Grover のアルゴリズムによって

$$\mathrm{F}_1(\beta_2 \oplus b_{2,0}) = a_{2,0} \oplus b_{2,3}$$

を満たすような関数 F_1 への入力 $\beta_1 \oplus b_{2,0}$ を探索し，

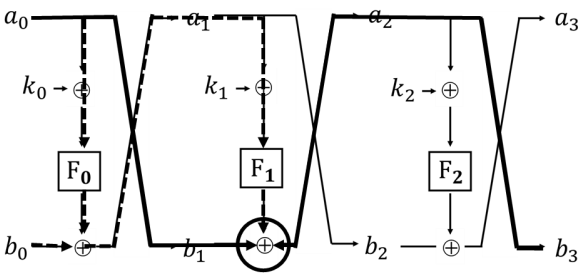

図 8 提案方法の手順 (1)
Fig. 8 Step (1) of our attack in 4.1

β_2 の値を計算する．

(4) Grover のアルゴリズムによって

$$\mathrm{F}_0(k'_0 \oplus a_{1,0}) \oplus \mathrm{F}_0(k'_0 \oplus a_{2,0}) = \beta_1 \oplus \beta_2$$

を満たすような $k'_0 \in \{0,1\}^{n/2}$ の値を探索する．

(5) k'_1 を，$k'_1 := \beta_1 \oplus \mathrm{F}_0(k'_0 \oplus a_{1,0})$ とする．

(6) (P_1, C_1) に対して，t_1, t_2 を

$$t_1 = \mathrm{F}_1(k'_1 \oplus \mathrm{F}_0(k'_0 \oplus a_{1,0}) \oplus b_{1,0}) \oplus a_{1,0}$$
$$t_2 = \mathrm{F}_0(k'_0 \oplus a_{1,0}) \oplus b_{1,0}$$

とする．

(7) Grover のアルゴリズムによって

$$\mathrm{F}_2(k'_2 \oplus t_1) \oplus t_2 = a_{1,3}$$

を満たすような $k'_2 \in \{0,1\}^{n/2}$ の値を探索する．

(8) (k'_0, k'_1, k'_2) が (P_3, C_3) に対しても式 (1)(2) の等号をみたすかどうかを確かめ，成り立てば，

$$(k_0, k_1, k_2) = (k'_0, k'_1, k'_2)$$

として出力する．

この攻撃では $D = 3$ 個の平文/暗号文ペアを受け取り，$D = O(1)$ である．手順 (2),(3),(4),(7) では $n/2$ ビットの値の Grover 探索を行っており，それぞれ計算量は $O(2^{n/4})$ である．$\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2$ オラクルへの古典クエリは高々 $O(1)$ 回である．よって，本攻撃における計算量は $T = O(2^{n/4})$ となる．また，使用する量子ビット数は $Q = O(n)$，使用する古典メモリは $M = O(1)$ である．

4.2 攻撃 2(qCPA)

提案量子選択平文攻撃 (qCPA) では，1 回目の暗号化クエリを元に $k_1 \oplus \mathrm{F}_0(k_0)$ を求め，これを 2 回目の暗号化オラクルへの入力としてクエリを行うことにより k_1 を除去する．以下にその手順を示す．

(1) 平文を $(a_0, b_0) = (0^{n/2}, 0^{n/2})$ として暗号化オラクルへの古典クエリを行い，暗号文 (a_3, b_3) を得る．このとき，$b_3 = \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0))$ である．

(2) Grover のアルゴリズムによって

$$\mathrm{F}_1(\beta_1) = b_3$$

を満たすような $\beta_1 \in \{0,1\}^{n/2}$ の値を探索する．

(3) 平文を $(a_0, b_0) = (0 \cdots 01, \beta_1)$ として暗号化オラクルへの古典クエリを行い，暗号文 (a_3, b_3) を得る．このとき，

$$b_3 \oplus a_0 = \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0 \oplus 0 \cdots 01) \oplus \beta_1)$$

である．ここで，$\beta_1 = k_1 \oplus \mathrm{F}_0(k_0)$ の場合に

$$b_3 \oplus a_0 = \mathrm{F}_1(\mathrm{F}_0(k_0 \oplus 0 \cdots 01) \oplus \mathrm{F}_0(k_0))$$

となる．

(4) Grover のアルゴリズムによって

$$\mathrm{F}_1(\beta_2) = b_3 \oplus a_0$$

を満たすような $\beta_2 \in \{0,1\}^{n/2}$ の値を探索する．

(5) Grover のアルゴリズムによって

$$\mathrm{F}_0(k'_0 \oplus 0 \cdots 01) \oplus \mathrm{F}_0(k'_0) = \beta_2$$

を満たすような $k'_0 \in \{0,1\}^{n/2}$ の値を探索する．

(6) k'_1 を，$k'_1 := \beta_1 \oplus \mathrm{F}_0(k'_0)$ とする．

(7) 平文を $(a_0, b_0) = (\mathrm{F}_1(k'_1), \mathrm{F}_0(k'_0 \oplus \mathrm{F}_1(k'_1)))$ として暗号化オラクルへの古典問い合わせを行い，暗号文 (a_3, b_3) を得る．このとき，

$$\begin{aligned} a_3 = {} & \mathrm{F}_0(k_0 \oplus \mathrm{F}_1(k'_1)) \oplus \mathrm{F}_0(k'_0 \oplus \mathrm{F}_1(k'_1)) \\ & \oplus \mathrm{F}_2(k_2 \oplus \mathrm{F}_1(k'_1) \oplus \mathrm{F}_1(k_1 \oplus \mathrm{F}_0(k_0 \oplus \mathrm{F}_1(k'_1)) \\ & \oplus \mathrm{F}_0(k'_0 \oplus \mathrm{F}_1(k'_1)))) \end{aligned}$$

である．ここで，$(k'_0, k'_1) = (k_0, k_1)$ の場合に

$$a_3 = \mathrm{F}_2(k_2)$$

となる．

(8) Grover のアルゴリズムによって

$$\mathrm{F}_2(k'_2) = a_3$$

を満たすような $k'_2 \in \{0,1\}^{n/2}$ の値を探索する．

(9) ランダムに $(a_0, b_0) \in (\{0,1\}^{n/2})^2$ を選び，平文暗号化オラクルへの古典クエリを行い，暗号文 (a_3, b_3) を得る．そして，この平文/暗号文ペアに対しても (k'_0, k'_1, k'_2) が式 (1)(2) の等号をみたすかどうかを確かめ，成り立てば，

$$(k_0, k_1, k_2) = (k'_0, k'_1, k'_2)$$

として出力する．

この攻撃は提案量子既知平文攻撃（4.1 節）と漸近的には

同等の (D, T, Q, M) を要する．しかし，手順 (2),(4),(5),(8) での Grover 探索において，$\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2$ オラクルへの入力の際に XOR の処理をほとんど行わないため，指数関数的に繰り返される Grover iteration のゲート数が少ないという利点がある．

参考文献

[1] Michael Luby, Charles Rackoff: How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM J. Comput. 17(2): 373-386 (1988)

[2] Rodolphe Lampe, Yannick Seurin: Security Analysis of Key-Alternating Feistel Ciphers. FSE 2014: 243-264

[3] Takanori Isobe, Kyoji Shibutani: All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach. Selected Areas in Cryptography 2012: 202-221

[4] Takanori Isobe, Kyoji Shibutani: Generic Key Recovery Attack on Feistel Scheme. ASIACRYPT (1) 2013: 464-485

[5] Hüseyin Demirci and Ali Aydin Selçuk, A meet-in-the-middle attack on 8-round AES. In Kaisa Nyberg, editor, Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers, volume 5086 of Lecture Notes in Computer Science, pages 116-126. Springer, 2008.

[6] Jian Guo, Jeŕrémy Jean, Ivica Nikolic, and Yu Sasaki. Meet-in-the-middle attacks on generic Feistel constructions. In Palash Sarkar and Tetsu Iwata, editors, Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I, volume 8873 of Lecture Notes in Computer Science, pages 458-477. Springer, 2014

[7] Itai Dinur, Orr Dunkelman, Nathan Keller, Adi Shamir: New Attacks on Feistel Structures with Improved Memory Complexities. CRYPTO (1) 2015: 433-454

[8] Itai Dinur, Orr Dunkelman, Nathan Keller, Adi Shamir: Efficient Dissection of Bicomposite Problems with Cryptanalytic Applications. J. Cryptol. 32(4): 1448-1490 (2019)

[9] Takanori Daiza, Kaoru Kurosawa, "Optimum Attack on 3-Round Feistel-2 Structure", IWSEC 2021

[10] Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Miller, G.L. (ed.) Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, pp. 212-219. ACM (1996)

[11] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions", LATIN'98: Theoretical Informatics, Lecture Notes in Computer Science, vol. 1380, pp. 163-169, 1998

[12] Akinori Hosoyamada and Yu Sasaki, "Quantum Demiric-Sel, cuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions", Security and Cryptgraphy for Networks, LNS, volume.11035, pp.12-14, 2018

[13] Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki and André Schrottenloher, "Quantum Attacks without Superposition Queries: the Offline Simon's Algorithm", ASIACRYPT 2020

[14] D. R. Simon. "On the power of quantum computation", SIAM J. Comput., 26(5):1474–1483, 1997.

[15] Hidenori Kuwakado, Masakatu Morii: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. ISIT 2010: 2682-2685

[16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia: Breaking Symmetric Cryptosystems Using Quantum Period Finding. CRYPTO (2) 2016: 207-237

[17] Gregor Leander, Alexander May: Grover Meets Simon - Quantumly Attacking the FX-construction. ASIACRYPT (2) 2017: 161-178

[18] 台座 崇規, 黒澤 馨, 3 ラウンド Feistel-KF 構造に対する量子鍵回復攻撃, SCIS 2021

[19] Carlos Cid, Akinori Hosoyamada, Yunwen Liu, Siang Meng Sim: Quantum Cryptanalysis on Contracting Feistel Structures and Observation on Related-Key Settings. INDOCRYPT 2020: 373-394