Computer Security Symposium 2018
22 - 25 October 2018

Type-1 一般化 Feistel 暗号に対する量子識別攻撃の改良

伊藤 玄武[1]　岩田 哲[1]

概要：一般化 Feistel 暗号はブロック暗号の構成法の 1 つであり，様々な変形が存在する．n ビットのラウンド関数から dn ビット（$d \geq 2$）のブロック暗号を構成する，Type-1 及び Type-2 一般化 Feistel 暗号について，Dong，Li，Wang は量子識別攻撃と，それを用いた量子鍵回復攻撃を示した [eprint 2017/1249]．本稿では，ラウンド関数として置換を用いた Type-1 一般化 Feistel 暗号について，Dong らの $2d-1$ ラウンド量子識別攻撃を改良し，$3d-3$ ラウンド量子識別攻撃が可能であることを示す．

キーワード：一般化 Feistel 暗号，Simon のアルゴリズム，量子識別攻撃

Improved Quantum Distinguishing Attacks on Type-1 Generalized Feistel Ciphers

Gembu Ito[1]　Tetsu Iwata[1]

Abstract: A Generalized Feistel Cipher is one of the methods to construct a block cipher, and it has several variants. Dong, Li, and Wang showed quantum distinguishing attacks and quantum key-recovery attacks against Type-1 and Type-2 Generalized Feistel Ciphers, which are dn-bit ($d \geq 2$) block ciphers that use an n-bit round function [eprint 2017/1249]. In this paper, we consider Type-1 Generalized Feistel Ciphers that use a permutation as the round function. We improve the $(2d-1)$-round quantum distinguishing attacks by Dong et al. and we show that $(3d-3)$-round quantum distinguishing attacks are possible.

Keywords: Generalized Feistel Ciphers, Simon's algorithm, quantum distinguishing attacks

1. はじめに

Generalized Feistel 暗号はブロック暗号の構成法の 1 つであり，Zheng，Matsumoto，Imai は n ビットのラウンド関数から dn ビット（$d \geq 2$）のブロック暗号を構成する Type-1，Type-2，Type-3 一般化 Feistel 暗号を示した [8]．様々な暗号がこの構成法をもとにしており，例えば，CAST-256（Type-1），CLEFIA と RC6（Type-2），MARS（Type-3）がある．

現在使われている多くの公開鍵暗号は Shor の量子アルゴリズム [6] によって破られることが知られている．一方，共通鍵暗号に対しても，Simon の量子アルゴリズム [7] を用いた攻撃が報告されている．Kuwakado と Morii は 3 ラウンド Feistel 暗号のランダム置換との識別，および Even-Mansour 暗号に対する鍵回復攻撃を示した [4], [5]．Kaplan，Leurent，Leverrier，Naya-Plasencia は CBC-MAC などいくつかの認証方式に対する偽造や，繰り返し Even-Mansour 暗号に対するスライド攻撃を示している [3]．また，Dong，Li，Wang は，Type-1 及び Type-2 一般化 Feistel 暗号について，量子識別攻撃と，それに Grover のアルゴリズム [2] を組み合わせた量子鍵回復攻撃を示した [1]．このように，共通鍵暗号においても量子コンピュータが脅威となることが考えられる．

古典の選択平文攻撃に対し，Type-1 一般化 Feistel 暗号は $2d-1$ ラウンド，Type-2 および Type-3 一般化 Feistel 暗号については $d+1$ ラウンド以上で安全になることが証明されている [8]．これに対し，Dong らは，Type-1 一般化

[1] 名古屋大学大学院工学研究科，〒 464-8603 名古屋市千種区不老町．Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan. g_itou@echo.nuee.nagoya-u.ac.jp, tetsu.iwata@nagoya-u.jp

表 1　Type-1/2/3 一般化 Feistel 暗号の安全性と量子識別攻撃．古典の安全性は選択平文攻撃に対する安全性である．また，量子識別攻撃は記載のラウンドまで攻撃できることを示す．

	Type-1	Type-2	Type-3
古典の安全なラウンド数	$2d-1$ [8]	$d+1$ [8]	$d+1$ [8]
量子識別攻撃	$2d-1$ [1] $3d-3$ [本稿]	$d+1$ [1]	

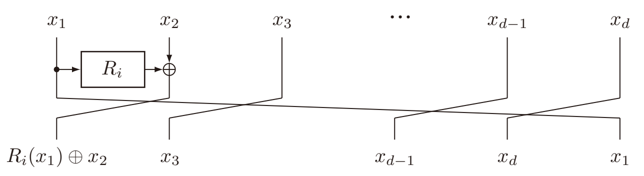

図 1　Type-1 一般化 Feistel 暗号

Feistel 暗号は $2d-1$ ラウンド，Type-2 一般化 Feistel 暗号については $d+1$ ラウンドの量子識別攻撃を示した [1]．本稿では，ラウンド関数として置換を用いた Type-1 一般化 Feistel 暗号について，Dong らの $2d-1$ ラウンド量子識別攻撃を改良し，$3d-3$ ラウンド量子識別攻撃が可能であることを示す．また，Dong らの論文では Simon のアルゴリズムを適用する条件を満たしていることが証明されていなかったが，それについても証明を行う．本稿の結果と従来結果を表 1 にまとめる．

2.　準備

2.1　記法

自然数 n に対し，$\{0,1\}^n$ ですべての n ビット列の集合を表す．$\mathrm{Perm}(n)$ で n ビット上のすべての置換の集合を，$\mathrm{Func}(n)$ で n ビット上のすべての関数の集合を表し，$\mathrm{Perm}(n)$ から一様ランダムに選ばれた置換をランダム置換と呼ぶ．$a \,\|\, b$ でビット列 a と b の連結を表す．また，おなじ次元のベクトル c と d に対し，$c \cdot d$ でベクトルの内積を表す．

2.2　Type-1 一般化 Feistel 暗号

Type-1 一般化 Feistel 暗号は 1 ラウンドにつきラウンド関数を 1 つ用いる構造である．d を 2 以上の整数として，dn ビットの平文 $M \in \{0,1\}^{dn}$ を入力にとり，dn ビットの暗号文 $C \in \{0,1\}^{dn}$ を出力する．r ラウンド Type-1 一般化 Feistel 暗号について，$1 \leq i \leq r$ として，$R_i \in \mathrm{Func}(n)$ を i ラウンド目のラウンド関数とすると，i ラウンド目は $x_j \in \{0,1\}^n (1 \leq j \leq d)$ を入力として

$$\mathrm{Round}_i(x_1, x_2, \ldots, x_d) = (R_i(x_1) \oplus x_2, x_3, \ldots, x_d, x_1)$$

と表される（図 1）．

2.3　Simon のアルゴリズム

この章では識別攻撃に用いる Simon の量子アルゴリズムを説明する．Simon の量子アルゴリズムは次の問題を効率的に解くことができるアルゴリズムである．

問題 1（[7]）．関数 $f : \{0,1\}^m \to \{0,1\}^n$ が，任意の $x, x' \in \{0,1\}^m$ に対し，$f(x) = f(x') \Leftrightarrow x' = x$ or $x \oplus s$（$s \neq 0$）を満たすとする．このとき周期 s を求めよ．

古典では $O(2^{m/2})$ の計算量が必要だが，Simon の量子アルゴリズムは $O(m)$ の量子計算量で s を求めることができる．関数 f を計算するユニタリ作用素 U_f（m 量子ビット $|x\rangle$ および n 量子ビット $|z\rangle$ に対し $U_f\,|x\rangle\,|z\rangle = |x\rangle\,|z \oplus f(x)\rangle$ と作用する）は与えられるものとする．また，アダマール変換 $H^{\otimes m}$ は m 量子ビット $|x\rangle$ に対し $H^{\otimes m}\,|x\rangle = \frac{1}{\sqrt{2^m}} \sum_{y \in \{0,1\}^m} (-1)^{x \cdot y}\,|y\rangle$ と作用する変換である．

Simon のアルゴリズムは次のステップを繰り返す：

(1) $(m+n)$ 量子ビット $|0^m\rangle\,|0^n\rangle$ の前半 m 量子ビットにアダマール変換 $H^{\otimes m}$ を適用する．

$$\frac{1}{\sqrt{2^m}} \sum_x |x\rangle\,|0^n\rangle$$

(2) ユニタリ作用素 U_f を適用する．

$$\frac{1}{\sqrt{2^m}} \sum_x |x\rangle\,|f(x)\rangle$$

(3) 再び前半 m 量子ビットにアダマール変換 $H^{\otimes m}$ を適用した後，測定を行い y を得る．

$$\frac{1}{2^m} \sum_{x,y} (-1)^{x \cdot y}\,|y\rangle\,|f(x)\rangle$$

$f(x) = f(x') \Leftrightarrow x' = x$ or $x \oplus s$ を満たすため，任意の x および y に対し $|y\rangle\,|f(x)\rangle = |y\rangle\,|f(x \oplus s)\rangle$ が成り立つ．よって最後の式は

$$\frac{1}{2^m} \sum_{x,y} ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y})\,|y\rangle\,|f(x)\rangle$$

と変形できる．$y \cdot s \equiv 1 \pmod 2$ を満たす y は，$(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y} = 0$ より消える．よって，測定によって得られる y は $y \cdot s \equiv 0 \pmod 2$ を満たすベクトルからランダムに得られる．このステップを $O(m)$ 回繰り返せば，高い確率で s を求めるのに十分な数の y が求まる．また，y による線形合同方程式を解くために必要な古典の計算量は $O(m^3)$ である．

3.　$2d-1$ ラウンド量子識別攻撃

この章では，Dong らによる $2d-1$ ラウンド量子識別攻撃 [1] を振り返る．識別攻撃の目標は，与えられたオラクル $\mathcal{O}$ が，Type-1 一般化 Feistel 暗号 T1FC か，ランダム置換 $\Pi \in \mathrm{Perm}(dn)$ かを識別することである．ここで，オラクル $\mathcal{O}$ は量子重ね合わせ状態の量子ビットを入出力できるものとする．つまり，任意の量子重ね合わせ状態の量子

ビット $\sum_{x,z}|x\rangle|z\rangle$ を入力として，$\sum_{x,z}|x\rangle|z\oplus\mathcal{O}(x)\rangle$ を出力する．

Dong らは，$\alpha_0,\alpha_1,x_2^0,\ldots,x_{d-1}^0\in\{0,1\}^n$ を任意の定数として（ただし $\alpha_0\neq\alpha_1$），次のような関数 $f:\{0,1\}^{n+1}\to\{0,1\}^n$ を定義した（図 2）．

$$\begin{aligned} f:\{0,1\}\times\{0,1\}^{n+1}&\to\{0,1\}^n\\ (b,x)&\mapsto\alpha_b\oplus y_2,\\ \text{where }(y_1,y_2,\ldots,y_d)&=\mathcal{O}(\alpha_b,x_2^0,\ldots,x_{d-1}^0,x). \end{aligned}$$

i ラウンド後の出力を $(x_1^i,x_2^i,\ldots,x_d^i)$ と表すと，$\mathcal{O}$ が T1FC のとき，関数 $f(b,x)$ は

$$\begin{aligned} &f(b,x)\\ &=\alpha_b\oplus x_2^{2d-1}\\ &=\alpha_b\oplus x_1^d\\ &=\alpha_b\oplus R_d(x_1^{d-1})\oplus\alpha_b\\ &=R_d(R_{d-1}(R_{d-2}(\cdots R_1(\alpha_b)\oplus x_2^0\cdots)\oplus x_{d-1}^0)\oplus x) \end{aligned}\tag{1}$$

と表される．2 つ目の等号では $x_1^i=x_d^{i+1}=x_{d-1}^{i+2}=\cdots=x_2^{i+d-1}$ を用いた．$h(\alpha_b)=R_{d-1}(R_{d-2}(\cdots R_1(\alpha_b)\oplus x_2\cdots)\oplus x_{d-1})$ とおくと，式 (1) は $f(b,x)=R_d(h(\alpha_b)\oplus x)$ と表せる．このとき

$$\begin{aligned} f(b,x)&=R_d(h(\alpha_b)\oplus x)\\ &=R_d(h(\alpha_{b\oplus1})\oplus h(\alpha_0)\oplus h(\alpha_1)\oplus x)\\ &=f(b\oplus1,x\oplus h(\alpha_0)\oplus h(\alpha_1)) \end{aligned}$$

より，$f(b,x)$ は周期 $(1,h(\alpha_0)\oplus h(\alpha_1))$ を持つ．

Dong らの論文では，$f(x)=f(x')\Rightarrow x'=x$ or $x\oplus s$ の条件を満たすことが示されていないが，これはラウンド関数 R_i が置換の場合には以下のように示せる．任意の $b,b'\in\{0,1\}$ および $x,x'\in\{0,1\}^n$ に対して

$$\begin{aligned} &f(b,x)=f(b',x')\\ &\Leftrightarrow R_d(h(\alpha_b)\oplus x)=R_d(h(\alpha_{b'})\oplus x')\\ &\Leftrightarrow h(\alpha_b)\oplus x=h(\alpha_{b'})\oplus x'\\ &\Leftrightarrow x'=\begin{cases} x & (b'=b)\\ x\oplus h(\alpha_0)\oplus h(\alpha_1) & (b'\neq b)\end{cases} \end{aligned}$$

より，$f(b,x)=f(b',x')\Leftrightarrow(b',x')=(b,x)$ or $(b\oplus1,x\oplus h(\alpha_0)\oplus h(\alpha_1))$ が成り立つ．

$\mathcal{O}$ が Π の場合には f に周期が存在する確率は小さい．よって，s が求まるかどうかで $\mathcal{O}$ を識別することができる．

4. $3d-3$ ラウンド量子識別攻撃

この章では，ラウンド関数として置換を用いた Type-1 一般化 Feislet 暗号に対する，改良された $3d-3$ ラウンド量子識別攻撃を提案する．平文における α_b の位置を $(d-1)n$ ビット右にずらすことで，識別攻撃のラウンド数を $3d-3$ ラウンドに伸ばすことができる．

$R_i\in\mathrm{Perm}(n)$ とする．$\alpha_0,\alpha_1,x_1^0,\ldots,x_{d-2}^0\in\{0,1\}^n$ を任意の定数として（ただし $\alpha_0\neq\alpha_1$），関数 $f:\{0,1\}^{n+1}\to\{0,1\}^n$ を

$$\begin{aligned} f:\{0,1\}\times\{0,1\}^{n+1}&\to\{0,1\}^n\\ (b,x)&\mapsto\alpha_b\oplus y_2,\\ \text{where }(y_1,y_2,\ldots,y_d)&=\mathcal{O}(x_1^0,\ldots,x_{d-2}^0,\alpha_b,x) \end{aligned}$$

と定義する（図 3）．

$\mathcal{O}$ が T1FC のとき，関数 $f(b,x)$ は

$$\begin{aligned} f(b,x)&=\alpha_b\oplus x_2^{3d-3}\\ &=\alpha_b\oplus x_1^{2d-2} \end{aligned}\tag{2}$$

と表される．2 つ目の等号では $x_1^i=x_d^{i+1}=x_{d-1}^{i+2}=\cdots=x_2^{i+d-1}$ を用いた．この関数 f について，次の補題が成り立つ．

補題 1. 関数 f は，任意の $b,b'\in\{0,1\}$ および $x,x'\in\{0,1\}^n$ に対し

$$\begin{aligned} &f(b,x)=f(b',x')\\ &\Leftrightarrow(b',x')=(b,x)\\ &\quad\text{or }(b\oplus1,x\oplus R_{d-1}(C\oplus\alpha_0)\oplus R_{d-1}(C\oplus\alpha_1)) \end{aligned}$$

を満たす．つまり，関数 f は周期 $(1,R_{d-1}(C\oplus\alpha_0)\oplus R_{d-1}(C\oplus\alpha_1))$ をもつ．ただし

$$C=R_{d-2}(R_{d-3}(\cdots R_1(x_1^0)\oplus x_2^0\cdots)\oplus x_{d-2}^0)$$

である．

証明. まず，入力された α_b が一番左の n ビットに到達する，$d-2$ ラウンド後の出力は

$$\begin{aligned} &(x_1^{d-2},x_2^{d-2},\ldots,x_d^{d-2})\\ &=\mathrm{T1FC}_{d-2}(x_1^0,\ldots,x_{d-2}^0,\alpha_b,x)\\ &=(R_{d-2}(x_1^{d-3})\oplus\alpha_b,x,x_1^0,x_1^1,\ldots,x_1^{d-3}) \end{aligned}$$

と表される．$1\leq i\leq d-3$ においては

$$x_1^i=R_i(R_{i-1}(\cdots R_1(x_1^0)\oplus x_2^0\cdots)\oplus x_i^0)\oplus x_{i+1}^0$$

と表せる．$x_1^0,\ldots,x_{d-2}^0$ が定数なので，x_1^i は定数である．ここで，定数 $C\coloneqq R_{d-2}(x_1^{d-3})$ とおくと，この 1 ラウンド後，つまり $d-1$ ラウンド後の出力は

$$\begin{aligned} &(x_1^{d-1},x_2^{d-1},\ldots,x_d^{d-1})\\ &=\mathrm{Round}_{d-1}(C\oplus\alpha_b,x,x_1^0,x_1^1,\ldots,x_1^{d-3})\\ &=(R_{d-1}(C\oplus\alpha_b)\oplus x,x_1^0,x_1^1,\ldots,x_1^{d-3},C\oplus\alpha_b) \end{aligned}$$

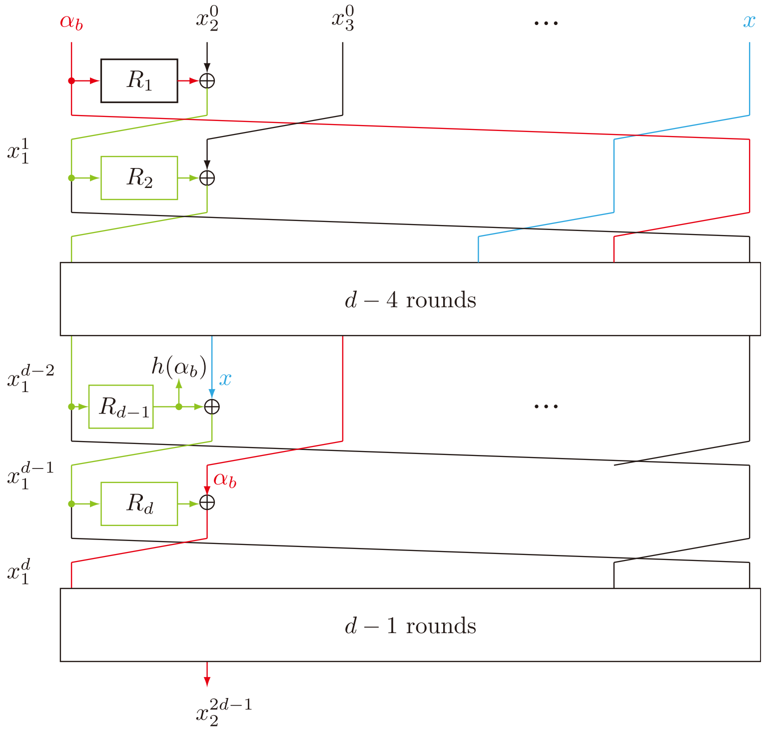

図 2 $2d-1$ ラウンド量子識別攻撃

と表される．ここから，再び $C \oplus \alpha_b$ が一番左の n ビットに到達する，$2d-2$ ラウンド後の出力を考えると，$R'(z) = R_{2d-2}(R_{2d-3}(\cdots R_{d+1}(R_d(z) \oplus x_1^0) \oplus x_1^1 \cdots) \oplus x_1^{d-3})$ として

$$\begin{aligned}&(x_1^{2d-2}, x_2^{2d-2}, \ldots, x_d^{2d-2})\\&= \mathrm{T1FC}_{2d-2}(x_1^0, \ldots, x_{d-2}^0, \alpha_b, x)\\&= (R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus \alpha_b \oplus C, x_2^{2d-2}, \ldots, x_d^{2d-2})\end{aligned} \tag{3}$$

と表される．先に述べたように，$x_1^0, x_1^1, \ldots, x_1^{d-3}$ は定数なので，$R'(z)$ は b, x と無関係である．式 (2) および式 (3) より，関数 $f(b, x)$ は

$$\begin{aligned}f(b, x) &= \alpha_b \oplus R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus \alpha_b \oplus C\\&= R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus C\end{aligned}$$

と表せる．このとき

$$\begin{aligned}&f(b, x)\\&= R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus C\\&= R'(R_{d-1}(C \oplus \alpha_{b \oplus 1}) \oplus R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1)\\&\qquad \oplus x) \oplus C\\&= f(b \oplus 1, x \oplus R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1))\end{aligned}$$

より，$f(b, x)$ は周期 $(1, R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1))$ を持つ．

また，$R'(z)$ は置換と定数の排他的論理和を繰り返すのみであり，置換である．このとき，任意の $b, b' \in \{0, 1\}$ および $x, x' \in \{0, 1\}^n$ に対して

$$\begin{aligned}&f(b, x) = f(b', x')\\&\Leftrightarrow R'(R_{d-1}(C \oplus \alpha_b) \oplus x) = R'(R_{d-1}(C \oplus \alpha_{b'}) \oplus x')\\&\Leftrightarrow R_{d-1}(C \oplus \alpha_b) \oplus x = R_{d-1}(C \oplus \alpha_{b'}) \oplus x'\\&\Leftrightarrow x' = \begin{cases} x & (b' = b)\\ x \oplus R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1) & (b' \neq b)\end{cases}\end{aligned}$$

より

$$\begin{aligned}&f(b, x) = f(b', x')\\&\Leftrightarrow (b', x') = (b, x)\\&\qquad \text{or } (b \oplus 1, x \oplus R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1))\end{aligned}$$

が成り立つ． □

よって，$\mathcal{O}$ が T1FC のときは Simon のアルゴリズムを用いることで周期が求まる．識別アルゴリズムは次のように動作する．

(1) 空の集合 $\mathcal{Y}$ を用意する．
(2) Simon のアルゴリズムの各ステップを行い，得た y を $\mathcal{Y}$ に加える．
(3) ステップ (2) を $O(n)$ 回繰り返す．
(4) すべての $y \in \mathcal{Y}$ と直交するベクトル $1 \| s' \in \{0, 1\}^{n+1}$ を求める．ランダムに $b \in \{0, 1\}$ および $z \in \{0, 1\}^n$ を選び，$f(b, z)$ および $f(b \oplus 1, z \oplus s')$ をオラクルを用いて計算する．$f(b, z) = f(b \oplus 1, z \oplus s')$ ならば $\mathcal{O}$ は T1FC，それ以外なら Π と出力する．

$\mathcal{O}$ が Π の場合には，周期 s が存在する確率は小さく，s'

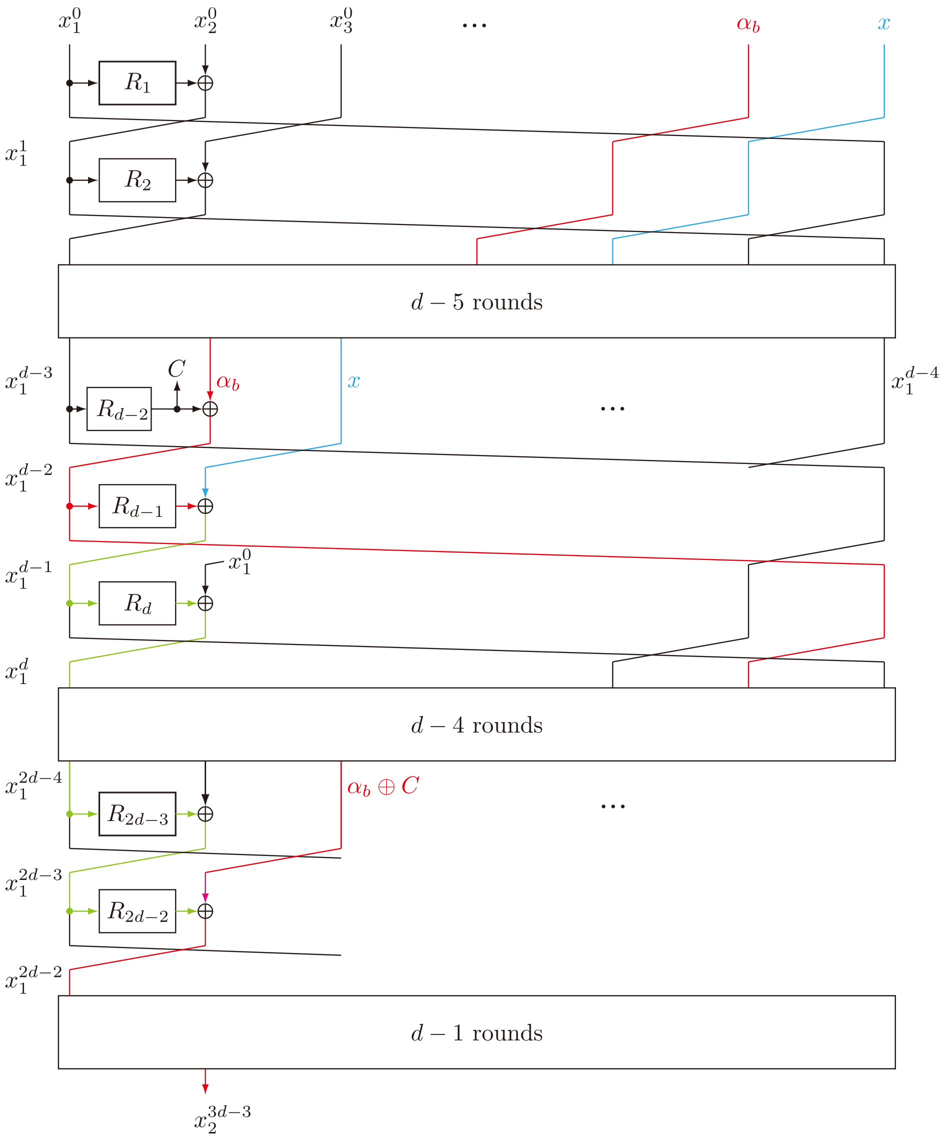

図 3　$3d-3$ ラウンド量子識別攻撃

が得られたとして $f(b,z) = f(b \oplus 1, z \oplus s')$ となる確率は小さい．よって，$O(n)$ の量子時間で $\mathcal{O}$ を識別することができる．

5.　まとめ

本稿では，ラウンド関数として置換を用いた Type-1 一般化 Feistel 暗号について，Dong らの $2d-1$ ラウンド量子識別攻撃を改良し，$3d-3$ ラウンド量子識別攻撃が可能であることを示した．また，量子識別攻撃において，Simon のアルゴリズムを適用する条件を満たしていることについても証明を行った．より多いラウンド数に対する識別攻撃が存在するかは今後の課題である．また，ラウンド関数が置換でない場合でも識別できるかを明らかにすることも課題である．

参考文献

[1] Dong, X., Li, Z. and Wang, X.: Quantum cryptanalysis on some Generalized Feistel Schemes, Cryptology ePrint Archive, Report 2017/1249 (2017). `https://eprint.iacr.org/2017/1249`.

[2] Grover, L. K.: A Fast Quantum Mechanical Algorithm for Database Search, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996* (Miller, G. L., ed.), ACM, pp. 212–219 (online), DOI: 10.1145/237814.237866 (1996).

[3] Kaplan, M., Leurent, G., Leverrier, A. and Naya-Plasencia, M.: Breaking Symmetric Cryptosystems Using Quantum Period Finding, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II* (Robshaw, M. and Katz, J., eds.), Lecture Notes in Computer Science, Vol. 9815, Springer, pp. 207–237 (online), DOI: 10.1007/978-3-662-53008-5_8 (2016).

[4] Kuwakado, H. and Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permu-

tation, *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, IEEE, pp. 2682–2685 (online), DOI: 10.1109/ISIT.2010.5513654 (2010).

[5] Kuwakado, H. and Morii, M.: Security on the quantum-type Even-Mansour cipher, *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, IEEE, pp. 312–316 (online), available from ⟨http://ieeexplore.ieee.org/document/6400943/⟩ (2012).

[6] Shor, P. W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM J. Comput.*, Vol. 26, No. 5, pp. 1484–1509 (online), DOI: 10.1137/S0097539795293172 (1997).

[7] Simon, D. R.: On the Power of Quantum Computation, *SIAM J. Comput.*, Vol. 26, No. 5, pp. 1474–1483 (online), DOI: 10.1137/S0097539796298637 (1997).

[8] Zheng, Y., Matsumoto, T. and Imai, H.: On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings* (Brassard, G., ed.), Lecture Notes in Computer Science, Vol. 435, Springer, pp. 461–480 (online), DOI: 10.1007/0-387-34805-0_42 (1989).