量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価

NTT セキュアプラットフォーム研究所
細山田　光倫

2020 年 1 月

エグゼクティブサマリー

量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価を行った．文献調査により，次のことを確認した．

- 量子コンピュータを用いた攻撃のモデル，特にハッシュ関数以外の（秘密鍵を用いる）共通鍵暗号系技術への攻撃のモデルには Q1 モデルと Q2 モデルの二種類のモデルが存在する．Q1 モデルにおいては鍵の埋め込まれたオラクルは古典的な攻撃モデルと同じ古典オラクルだが，Q2 モデルにおいては鍵の埋め込まれたオラクルが量子オラクルとなり，攻撃者はオラクルへの量子重ね合わせクエリを行える．Q2 モデルの攻撃を実行するには攻撃対象の暗号技術が（秘密鍵を埋め込んだうえで）量子回路上に実装されている必要がある．
- Q2 モデルにおいては，古典的に安全とされている共通鍵暗号系技術 (CBC-MAC や GCM など) に多項式時間の攻撃が存在する．多項式時間の攻撃には Simon の量子アルゴリズムが用いられる．
- Q1 モデルにおいては，古典的に安全とされている共通鍵暗号系技術に多項式時間の攻撃は現在の所存在しない．しかし従来より認識されていた Grover のアルゴリズムによる鍵全数探索の高速化のみならず，暗号技術の構造に依存した様々な攻撃が存在する．Even-Mansour 暗号および類似の構造を持つ暗号技術に対しては，Q1 モデルであっても Simon のアルゴリズムを活用して古典的攻撃より効率的な攻撃が実行できる．
- 既存研究において使用可能と想定されている量子計算のリソースは論文によって異なり，攻撃コストの評価方法も様々である．特にハッシュ関数への汎用攻撃 (衝突探索など) については，使用可能な量子計算のリソースに関する想定や攻撃コストの評価方法に応じて最良の攻撃が異なる．

また調査した文献の内容に考察を加えた結果，次のような結論を得た．

- ある関数を計算するための古典計算機向けのプログラムコードがあった場合その関数を量子回路上に実装することが可能になるため，Q2 モデルにおいて多項式時間の攻撃が可能な暗号技術については，例え難読化処理等を施しても，その関数 (例えば CBC-MAC でメッセー

ジからタグを計算する関数) を実装して秘密鍵を埋め込んだコードを，量子コンピュータを持った攻撃者に手渡すべきではない．しかし，攻撃対象となる暗号技術が量子回路上に実装されているような（あるいは量子回路上に移植可能となるような）非常に特殊な状況でない限り，既存の共通鍵暗号系技術，特に CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号系技術に，Q2 モデルの攻撃の影響が及ぶことは現状では無いと考えられる．

- 従来から指摘されていた通り，Grover のアルゴリズムによって k ビット鍵の全数探索が時間 $\tilde{O}(2^{k/2})$ で実行可能になるため，長期的に保護したいデータには秘密鍵の鍵長が 128 ビットの暗号技術でなく 192 ビットや 256 ビットの暗号技術を使用するのが賢明であると考えられる．
- 古典的に 128 ビット安全性のあるハッシュ関数の安全性に量子攻撃が現実的な脅威を直接及ぼすとは現状考えづらい．
- CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号系技術の安全性に量子コンピュータが直接与える影響は “Grover のアルゴリズムを用いると k ビット鍵の全数探索が時間 $\tilde{O}(2^{k/2})$ で実行できるため，長期的に保護したいデータには鍵長が 192 ビットや 256 ビットの暗号技術を使用した方が賢明である” という以上のものは現状では無いと考えられる．しかし Even-Mansour 暗号への Q1 モデルにおける攻撃のように安全性に現実的な影響を直接及ぼす可能性のある攻撃が今後も発見される可能性があるため，研究の動向には注意を払っておく必要がある．

目次

1　はじめに

Shor の量子アルゴリズム [Sho94] によって現在広く利用されている公開鍵暗号系技術が効率的に破れてしまうということが判明して以来，大規模な汎用量子コンピュータが実現してからも安全性を担保できる耐量子公開鍵暗号の研究が盛んに行われている．一方共通鍵暗号系技術の安全性については量子コンピュータが及ぼす影響は非常に限定的であると考えられていたが，従来は気づかれていなかった攻撃の存在を示す研究結果がここ数年で多数発表されている．本報告書では，量子コンピュータが共通鍵暗号系技術の安全性に及ぼす影響について，既存文献の調査と評価を報告する[*1]．

1.1　共通鍵暗号系技術に対する量子攻撃の研究の重要性

便利かつ安全な通信は公開鍵暗号系技術と共通鍵暗号系技術を組み合わせて初めて実現される．また複数の暗号技術を組み合わせて保護された通信やデータの安全性は使用されている暗号技術のうち最も弱いものによって決まる．ゆえに，量子コンピュータを持った攻撃者から通信やデータを保護するためには，公開鍵暗号系技術はもちろん，共通鍵暗号系技術も量子コンピュータを用いた攻撃から安全である必要がある．

ブロック暗号やハッシュ関数などの共通鍵暗号系プリミティブの耐量子性は，それらに対して有効な量子攻撃が存在するか否かのみによって評価され得る．ゆえに，量子コンピュータによる共通鍵暗号系技術の安全性へ及ぼす影響を把握するためには，具体的な共通鍵暗号系プリミティブへの量子攻撃を研究することが重要となる．

また公開鍵暗号系技術・共通鍵暗号系技術ともに，耐量子性の研究は大規模な汎用量子コンピュータが実現するよりもかなり早い段階で進めておく必要がある．これは主に次の二つの理由による：第一の理由は，現在量子コンピュータを保持していない攻撃者であっても，例えば数十年後に量子コンピュータを入手できた際に解読できるようになることを期待して，現在入手できる限りの暗号文を手に入れようとしている可能性が有る，と

[*1] 本報告書では「量子コンピュータ」あるいは「量子計算機」とは，ゲート型量子計算機のことを指すものとする．

いうものである．このような潜在的脅威を念頭に置くと，数十年単位で長期間安全に保護したいデータはなるべく早い段階から耐量子暗号技術で保護しておくことが望ましい．第二の理由は，基礎研究で知見が蓄えられてから耐量子暗号技術が広く使用されるようになるまでには１０年単位の時間がかかる，というものである．例えば以前米国の標準暗号であった DES への最初の理論攻撃 [BS92] が発表されてから次の世代の暗号である AES の標準化が公式に発表されるまで１０年近い時間がかかっている [NIS01]．よって大規模な汎用量子コンピュータが実現される前から，なるべく早く研究を進めておく必要がある．

1.2　本報告書の構成

本報告書の構成は以下のようになっている．2 章では，報告書全体を通して必要となる記法等について述べ，共通鍵暗号系技術への量子攻撃に欠かせない Grover のアルゴリズムと Simon のアルゴリズムの概要を記述する．3 章では，秘密鍵を使用する共通鍵暗号系技術への量子攻撃の 2 つのモデル（Q1 モデルと Q2 モデル）を紹介する．4 章では，攻撃アルゴリズムのコスト評価に関する議論を概観する．特に，使用可能な量子計算のリソースに関する想定に応じて最良の衝突探索アルゴリズムが変わるということを説明する．5 章では，暗号技術の内部構造によらず適用可能な汎用攻撃について，既存研究を概観する．6 章および 7 章ではそれぞれ，Q2 モデルと Q1 モデルにおける既存の量子攻撃の研究結果を紹介する．8 章において，本報告書全体についての考察とまとめを与える．

なお 3 章から 7 章までの内容は主に，共通鍵暗号系技術への（古典）攻撃の研究に明るい方が量子攻撃の既存研究を概観するために利用されることを意識して書かれている．本報告書の目的は理論の詳細を議論することでなく既存研究を広く調査し概観することであるため，理論的な厳密性より簡潔な説明を優先する．

2　準備

本報告書では量子計算のモデルとして量子回路モデル [NC10] を考えるものとし，量子回路は全て Clifford+T ゲートから構成されているものとする．量子回路が量子オラクルへのクエリを行うことが許される場合，オラ

クルクエリのための特別なゲートが用意され，回路に組み込まれているものとする（注意 2.1）．深さ D_C の量子回路 C が暗号技術 P への量子攻撃で用いられる際，ほかに断りの無い限り，C が入力を得てから最終的な出力を計算し終わるまでの時間は D_C/D_P であるとみなす．ここで D_P は攻撃対象の暗号技術 P を実装するのに必要な量子回路の深さであるとする[*2]．また他に断りの無い限り量子計算に関する全ての操作は誤り無しで実行されるものとし，量子誤り訂正は考慮に入れないものとする．量子状態の観測というと計算基底での観測を指すこととする．

$x, y \in \{0,1\}^n$ に対して $x \oplus y$ は x と y の排他的論理和を表すとする．また $x \in \{0,1\}^n$, $x' \in \{0,1\}^m$ に対して $x||x'$ は x と x' を結合した $(m+n)$ ビットのビット列を表すとする．集合 $\{0,1\}^n$ は演算 $\oplus$ について群を成すが，この群を $\mathbb{F}_2$ 上の n 次元ベクトル空間 $\mathbb{F}_2^n$ と同一視する．また $x = x_1||\cdots||x_n, y = y_1||\cdots||y_n \in \mathbb{F}_2^n$ $(x_i, y_i \in \{0,1\})$ に対して $x \cdot y$ は x と y のドット積 $x_1y_1 \oplus \cdots \oplus x_ny_n$ を表すとする．二つの n ビット列 x と y が直交するとは，$x \cdot y = 0$ が成り立つこととする．

注意 2.1. 一般に，関数 $f : \{0,1\}^m \to \{0,1\}^n$ の（古典）オラクルと言うと，任意の入力 $x \in \{0,1\}^m$ に対して値 $f(x)$ を返すブラックボックスのことを指すが，関数 f の量子オラクルは

$$U_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle \tag{1}$$

で定義されるユニタリ作用素としてモデル化される．

■量子ランダムアクセスメモリ（QRAM）　保存されたデータへの量子重ね合わせ状態でのランダムアクセスを可能にするメモリを量子ランダムアクセスメモリ（QRAM）と言う [GLM08]．これは古典的なランダムアクセスメモリ（RAM）の概念の拡張である．

古典的な RAM は N 個のデータ $D_1, \ldots, D_N$ が格納されているとき，アドレス i（$D_1 \leq i \leq D_N$）を渡すと対応するデータ D_i を効率的に返す．QRAM はこのデータ取得を量子重ね合わせで実行することを可能とする．即ち，アドレスの量子重ね合わせ状態 $\sum_i c_i |i\rangle$ を渡すと対応するデータの

[*2] 計算時間を D_C でなく D_C/D_P と見積もるのは，攻撃時間評価が攻撃対象の暗号技術をどう量子回路上に実装するかに依存せず決まるようにするためである．また共通鍵暗号の研究における古典的な攻撃時間評価の慣習と整合性を取るためでもある．

量子重ね合わせ状態 $\sum_i c_i |i\rangle |D_i\rangle$ を返す．

議論を簡単にするため，本稿では RAM・QRAM ともにアクセスに要する時間は定数時間であると仮定する．

2.1 Grover のアルゴリズム

問題 2.1 (データベース探索)**.** t を正の整数（$t \leq 2^n$）とする．関数 $f : \{0,1\}^n \to \{0,1\}$ について $|f^{-1}(1)| = t$ が成り立っているとする．f が（量子）オラクルとして与えられたとき，$f(x) = 1$ を充たす x を 1 つ見つけよ．

この問題を古典計算機のみを用いて定数確率で解くためには $\Omega(2^n/t)$ 回の古典クエリが必要であるが，量子計算機では Grover のアルゴリズム（あるいはその一般化）[Gro96, BBHT98] を使用すると $O\left(\sqrt{2^n/t}\right)$ 回の量子クエリで解けることが知られている．アルゴリズムに用いられる量子回路は幅 $O(n)$・深さ $O\left(2^{n/2}\right)$ となる（f へのクエリが時間 1 で実行されるとすると，アルゴリズムの実行に必要な時間も $O\left(\sqrt{2^n/t}\right)$ となる）．

また Grover のアルゴリズムの簡単な応用として，以下の問題を解くアルゴリズムを作ることができる [HSX17].

問題 2.2 (ランダム関数の（多重）原像探索)**.** t を正の整数（$t \leq 2^n$）とする．$F : \{0,1\}^n \to \{0,1\}^n$ をランダム関数，L を $\{0,1\}^n$ の部分集合とし，$|L| = t$ とする．F が（量子）オラクルとして与えられるとき，$F(x) \in L$ となる x を一つ求めよ．

この問題を古典計算機のみを用いて定数確率で解くためには $\Omega(2^n/t)$ 回の F への古典クエリが必要であるが，F が量子オラクルとして与えられている場合，以下のような簡単な量子アルゴリズムを実行すると $O\left(\sqrt{2^n/t}\right)$ 回の F への量子クエリで問題 2.2 を解くことができる [HSX17] :

Grover のアルゴリズムを用いた自明な（多重）原像探索アルゴリズム

1. $f_L^F : \{0,1\}^n \to \{0,1\}$ を，$F(x) \in L$ であるときかつその時に限り $f_L^F(x) = 1$，と定義する．
2. f_L^F に Grover のアルゴリズムを適用する．

ステップ 1 の関数 f_L^F は幅 $\tilde{O}(|L|)$・深さ $\tilde{O}(1)$ の量子回路上に実装できる（あるいは，大きさ $\tilde{O}(|L|)$ の量子メモリ（QRAM）を用いて深さ $\tilde{O}(1)$ の量

子回路上に実装できる）．F がランダム関数であることから $f_L^F(x) = 1$ となる x はおおむね t 個存在し，よって上記アルゴリズムに必要な量子回路は幅 $\tilde{O}(|L|)$・深さ $O(\sqrt{2^n/t})$ となる．（F へのクエリが時間 1 で実行されるとすると，アルゴリズムの実行に必要な時間も $O(\sqrt{2^n/t})$ となる）．

注意 2.2. ランダム関数（ハッシュ関数）の原像探索問題やブロック暗号の鍵全数探索問題は自明に問題 2.2 の $t = 1$ の場合に帰着される．上記アルゴリズムにより，n ビット出力ハッシュ関数の原像探索は時間 $\tilde{O}(2^{n/2})$ で，また k ビット鍵ブロック暗号の鍵全数探索は時間 $\tilde{O}(2^{k/2})$ で，それぞれ実行可能となる．詳細は 5.1 節を参照されたい．

2.2 Simon のアルゴリズム

問題 2.3. 関数 $f : \{0,1\}^n \to \{0,1\}^n$ と $s \in \{0,1\}^n$ があって，以下の条件を満たすとする：

$$x = y \text{ または } x = y \oplus s \text{ であるとき，かつそのときに限り } f(x) = f(y)^{*3}. \quad (2)$$

f が（量子）オラクルとして与えられたとき，s を求めよ．

この問題を古典計算機で定数確率で解くには $\Omega(2^{n/2})$ 回の古典クエリが必要であるが，Simon の量子アルゴリズムを用いると $O(n)$ 回の量子クエリで解くことができる [Sim94]．以下にアルゴリズムの概要を示す：

Simon のアルゴリズム

1. 下記のサブルーチン **SSub** を cn 回繰り返して n 個の元 $y_1, \ldots, y_n \in \{0,1\}^n$ を得る（c は適当な定数，例えば $c = 2$）．
2. $\{0,1\}^n$ を $\mathbb{F}_2$ 上の n 次元ベクトル空間とみなしたときの $y_1, \ldots, y_n$ の張るベクトル空間の次元 d を計算する．
3. $d \neq n-1$ なら，アルゴリズムは失敗したとして終了する．
4. $d = n-1$ なら，$y_1, \ldots, y_n$ の全てに直交する $s' \in \{0,1\}^n$ を計算して出力する．

サブルーチン SSub

[*3] 条件 (2) は特に f が演算 $\oplus$ に関して周期 s を持つ周期関数であるということを示している．

1. $2n$ 量子ビットの量子状態
$$|0^n\rangle\,|0^n\rangle \tag{3}$$
を用意する．
2. 状態 (3) の左 n 量子ビットに Hadamard 変換 $H^{\otimes n}$ をかけ，
$$\sum_x \sqrt{1/2^n}\,|x\rangle\,|0^n\rangle \tag{4}$$
を得る．
3. f への量子クエリを行い（ユニタリ作用素 U_f ： $|x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle$ を状態 (4) に作用させ），
$$\sum_x \sqrt{1/2^n}\,|x\rangle\,|f(x)\rangle \tag{5}$$
を得る．
4. 状態 (5) の左 n 量子ビットに Hadamard 変換 $H^{\otimes n}$ をかけ，
$$\sum_{x,y} (-1)^{x\cdot y}/2^n\,|y\rangle\,|f(x)\rangle \tag{6}$$
を得る．
5. 状態 (6) の左 n 量子ビットを観測し，結果（n ビットのビット列 y）を出力する．

条件 (2) を使うと，サブルーチン **SSub** は（$\{0,1\}^n$ を $\mathbb{F}_2$ 上の n 次元ベクトル空間と見たとき）s に直交するベクトルを一様ランダムに出力することがわかる．ゆえに，Simon のアルゴリズムのステップ 2 において非常に高い確率で $d = n-1$ となり，$s' = s$ となることがわかる．サブルーチン **SSub** は幅 $2n$・深さ $O(1)$ の量子回路を用いて実行することができ，f へ 1 回だけクエリを行う．また Simon のアルゴリズムのステップ 2 と 4 はガウス消去法を用いて，時間 $O(n^3)$ で実行できる．よって Simon のアルゴリズム全体として，f へ行う量子クエリは $O(n)$ 回，使用する量子回路は幅 $O(n)$・深さ $O(1)$，また実行に必要な時間は f へのクエリが時間 1 で実行されるとした場合 $O(n^3)$ となる．

■条件 (2) の緩和　共通鍵暗号への攻撃に Simon のアルゴリズム適用する際，アルゴリズムを適用しようとする関数 f について
$$y = x \oplus s \text{ ならば } f(x) = f(y) \tag{7}$$

が成り立っていても，その逆

$$f(x) = f(y) \text{ ならば } y = x \oplus s \tag{8}$$

が成り立っているとは限らない．しかし Kaplan らは，条件 (8) が成り立たずとも f が s を周期に持つことを除いてほぼランダムな関数である場合，Simon のアルゴリズムを適用することにより多項式時間で s を計算できるということを示した [KLLN16a, Theorem 2].

3　攻撃のモデル：古典クエリと量子クエリ

本章では，量子計算機を用いた共通鍵暗号系技術への攻撃を考察する際の攻撃モデルについて述べる．

秘密鍵を使用する共通鍵暗号系技術（つまりハッシュ関数以外の共通鍵暗号系技術）への量子計算機を用いた攻撃には，攻撃者がアクセスできる鍵の埋め込まれたオラクルの種類に応じて二つのモデルがある．一つはオラクルが古典攻撃において与えられるオラクルと同じであるモデル（Q1 モデル），もう一方はオラクルへのクエリおよびオラクルの出力が量子重ね合わせ状態になることを許容する攻撃モデル（Q2 モデル）である [KLLN16b].

以下，まずは古典的な攻撃のモデルを振り返り，その後二つの量子攻撃モデルを説明する．

注意 3.1. ハッシュ関数は秘密鍵を使用しないため，攻撃のモデル化に際して鍵の埋め込まれたオラクルへのクエリという概念は存在しない．

3.1　古典的攻撃モデル

ハッシュ関数を除く共通鍵暗号系技術への攻撃の古典的なモデルは，攻撃者が計算機を持っており（あるいは，攻撃者自体がアルゴリズムであるとモデル化し），ランダムに生成された秘密鍵の埋め込まれたオラクル（暗号化オラクル・復号オラクルや認証タグ生成オラクル）へメッセージを自由にクエリしてその結果を得られる，というものである．

例えばブロック暗号 E_K（K は秘密鍵）に対する選択平文攻撃による鍵回復攻撃について考える際は，平文 M をクエリすると対応する暗号文 $E_K(M)$ を時間 1 で返してくれるオラクルの存在を前提とする．攻撃者は

オラクルへ様々な平文をクエリして対応する暗号文を取得しつつ，自らの所持する計算機上で秘密鍵を推測するための計算を行う（図 1 を参照）．

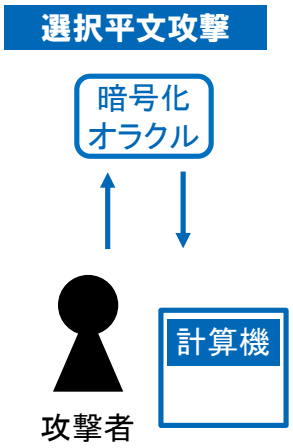

図 1　古典攻撃モデルの例（選択平文攻撃）

3.2　Q1 モデル（古典クエリ攻撃モデル）

このモデルにおいては，攻撃者の計算機が量子計算機になる（あるいは，攻撃者自体が量子アルゴリズムであるとモデル化する）が，それ以外の設定は基本的に古典的攻撃モデルと同じである．攻撃者はオラクルへ様々なデータをクエリしてその結果を取得しつつ，自らの所持する量子計算機上で攻撃に必要な計算を行う．

量子計算機は様々な問題を古典計算機より高速に解けるため，古典的攻撃モデルに比べて高速な攻撃が可能になる（図 2 を参照）．

3.3　Q2 モデル（量子クエリ攻撃モデル）

このモデルにおいては，攻撃者の計算機が量子計算機であることに加え，鍵の埋め込まれたオラクルの入出力も量子重ね合わせ状態になることを許容する．つまり攻撃者に与えられている鍵の埋め込まれたオラクルが量子オラクルであるという設定を考える（図 3 を参照）．

例えばブロック暗号 E_K に対する量子選択平文攻撃では，平文 M をクエリすると対応する暗号文 $E_K(M)$ が得られるのみでなく，二つの平文 M_1 と M_2 の量子重ね合わせ状態 $|\phi\rangle = \sqrt{1/2}\,|M_1\rangle\,|0^n\rangle + \sqrt{1/2}\,|M_2\rangle\,|0^n\rangle$ をクエ

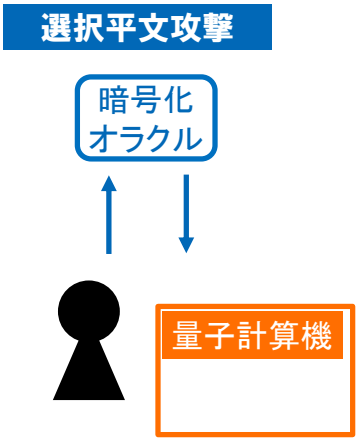

図 2　Q1 モデルの例（選択平文攻撃）

図 3　Q2 モデルの例（量子選択平文攻撃）

リすることが許される．$|\phi\rangle$ を E_K の量子オラクルへクエリすると，M_1 と M_2 が「同時」に暗号化され，量子重ね合わせ状態 $\sqrt{1/2}\,|M_1\rangle\,|E_K(M_1)\rangle + \sqrt{1/2}\,|M_2\rangle\,|E_K(M_2)\rangle$ が返される．

3.4　Q1 モデルと Q2 モデルの比較

Q2 モデルでは，攻撃者が鍵の埋め込まれたオラクルへ量子重ね合わせクエリを行える状況を想定している．例えばブロック暗号への量子選択平文攻撃であれば，秘密鍵の埋め込まれた暗号化関数が量子回路上に実装され

ており，攻撃者がその量子回路へ自由に入力を与えて出力を得ることが出来るという状況を想定している．（ただし攻撃者は回路がどのように実装されているか確認することはできない．あくまで自由に入力を選択し，対応する出力を得ることができるだけである．）

一般に，計算の過程で量子重ね合わせ状態を利用できる場面が増えれば増えるほど攻撃者の能力が強くなるため，Q2 モデルにおける攻撃者の能力は Q1 モデルにおける攻撃者の能力に比べて強い．実際，Q1 モデルでは多項式時間攻撃が発見されていないが Q2 では多項式時間攻撃が与えられているような暗号技術が存在する（Q2 モデルにおける攻撃についての詳細は 6 章を参照）．

Q1 モデルでは古典的攻撃モデルと同じく，鍵の埋め込まれたオラクルが古典計算機上に実装されている状況を想定しているため，Q1 モデルの方が Q2 モデルに比べてより現実的である．

しかし，Q2 モデルが「完全に非現実的なモデル」というわけではない [HS18a]．例えば以下のような状況では Q2 モデルが現実的なモデルになる：

a) 通信や情報処理の多くが量子状態で行われているような未来
b) 攻撃対象の暗号技術を実装し鍵の埋め込まれた（古典計算機用の）プログラムコードを攻撃者が入手可能な状況

a) の状況において Q2 モデルが現実的なモデルとなるのは明らかである．また原理上古典計算機用のプログラムは量子計算機上に移植可能であるため[*4]，b) の状況においても Q2 モデルが妥当なモデルとなる．ここで，b) の状況は，攻撃対象の暗号技術（何らかの鍵付きの暗号学的関数）F_K を実装したプログラムコードに何らかの方法で難読化処理が施されたものを攻撃者が保持している場合にも発生し得ることに注意されたい：難読化処理後のプログラムコードを $\mathcal{C}$ と置く．すると，例え古典攻撃で鍵 K などの秘密情報を抽出することが困難であっても，もし Q2 モデルにおいて F_K への効率的な鍵回復攻撃が存在するなら，攻撃者はプログラムコード $\mathcal{C}$ を量子計算機上に移植することで F_K の量子オラクルをシミュレートし，効率的に鍵を回復することが出来る．このような量子攻撃の可能性は Q1 モデ

[*4] ここでは，多項式時間で計算可能な関数を計算するための決定的アルゴリズムを実装したプログラム想定している

ルのみでは捉えることができない．

また最近では，Q2 モデルにおける攻撃を元に考案された Q1 モデルにおける攻撃も発表されている [BHN+19]（7.3 節を参照）．より現実的なモデルである Q1 モデルにおける攻撃を発見する前段階として，Q2 モデルにおける攻撃の研究は有用である．

ゆえに，Q2 モデルにおける攻撃の研究は共通鍵暗号系技術の耐量子性を評価する上で Q1 モデルにおける攻撃の研究と同様に重要である．

4　攻撃コスト評価方法に関する議論

本章では，攻撃アルゴリズムのコスト（或いは効率性）をどう評価すべきかということに関して，暗号研究者の間でなされている既存の議論をハッシュ関数に対する量子衝突探索アルゴリズムの研究の進展を軸に説明する．

量子計算機の研究開発自体がまだまだ発展途上であることから，攻撃コストの評価方法について暗号研究者の間で統一的な合意が取れているわけではない．既存研究において使用可能と想定されている量子計算のリソースは論文によって異なり，攻撃コストの評価方法も様々である．特にハッシュ関数への汎用攻撃（衝突探索など）については，使用可能な量子計算のリソースに関する想定や攻撃コストの評価方法に応じて最良の攻撃が異なる．

本章では，なるべく中立的な立場から既存の議論の概要を紹介することに努め，各々の議論が妥当であるか否かの判断には立ち入らないこととする．今後の研究の進展や技術の発展によって，着目すべきコスト評価方法が大きく変化する可能性があることに留意されたい．

注意 4.1. 本章で説明する攻撃は全てハッシュ関数の具体的な内部構造に依らず適用できる汎用攻撃（generic attack）である．

4.1　古典的衝突探索と誕生日のパラドクス

関数 $h : X \to Y$ の衝突とは，X の要素のペア (x, x') であって $x \neq x'$ かつ $h(x) = h(x')$ を充たすものである．h が安全な暗号学的ハッシュ関数（例えば SHA-2 や SHA-3）である場合 X のサイズは Y のサイズ以上で，また h は完全にランダムに振る舞うとみなして差し支えない．以下簡単の

ため，h はランダム関数，また $X = Y = \{0,1\}^n$ であるとする．

古典的には，有名な誕生日のパラドクスにより，以下の命題が成り立つことがわかる：

命題 4.1. $S \subset \{0,1\}^n$ をサイズ $\sqrt{2^n}$ の任意の部分集合とする．このとき $h|_S$ には確率 $\Theta(1)$ で衝突が存在する．[*5]

この命題を利用するとランダム関数 h の衝突を $\tilde{O}(2^{n/2})$ だけのメモリを使用して時間 $\tilde{O}(2^{n/2})$ で発見する自明なアルゴリズムが作成できる．更に，より洗練されたアルゴリズム（rho 法）を使用すれば，衝突探索にかかる時間 $\tilde{O}(2^{n/2})$ はそのままに，メモリ使用量を $\tilde{O}(1)$ に減らして衝突を発見できることが知られている [Pol75]．また任意の確率的アルゴリズムについて，ランダム関数 h の衝突を確率 $\Theta(1)$ で探索するには（並列計算を考慮に入れなければ）時間 $\Omega(2^{n/2})$ が必要であることが容易に証明される．より正確に言うと，関数 h の評価（h がオラクルとして与えられるときの h へのクエリの回数）が $\Omega(2^{n/2})$ 回必要であることが証明される．

4.2 最初の量子衝突探索アルゴリズム：BHT

Brassard らは 1997 年，Grover のアルゴリズムを応用し，出力長 n ビットのハッシュ関数の衝突を時間 $\tilde{O}(2^{n/3})$ で探索するアルゴリズムを発表した [BHT97][*6]．以下このアルゴリズムを，考案者らの頭文字をとって BHT のアルゴリズムと呼ぶ．前節で述べたように古典アルゴリズムは衝突探索に時間 $\Omega(2^{n/2})$ を要するため，BHT のアルゴリズムを用いると $\tilde{\Omega}(2^{n/6})$ ぶんの高速化が得られる．以下にアルゴリズムの概要を示す．

1. サイズ $2^{n/3}$ の部分集合 $S \subset \{0,1\}^n$ をとる．全ての $x \in S$ について $h(x)$ を計算し，ペア $(x, h(x))$ をリスト L に保存する．
2. $x' \in \{0,1\}^n \setminus S$ と $(x, h(x)) \in L$ の組であって $h(x') = h(x)$ であるようなものを，2.1 節で紹介した（Grover のアルゴリズムを自明に適用することによって得られる）多重原像探索アルゴリズムを用いて探索する．

[*5] ここでの確率は，関数 h を一様ランダムに選んだ際の確率である．

[*6] 正確に言うと原論文においてランダム（とみなせる）関数の衝突探索が議論されているわけではないが，ランダム関数の衝突探索にも適用できることが示される [HSTX19].

3. (x, x') を出力する．

なお，h の量子オラクルが攻撃者に与えられていると考え，h への 1 回のクエリは時間 1 で行えると仮定する．

リスト L のサイズが $2^{n/3}$ であるため，ステップ 1 に要する時間および h へのクエリ回数は $O(2^{n/3})$ である．またステップ 2 に要する時間および h へのクエリ回数は $\tilde{O}\left(\sqrt{2^n/|L|}\right) = \tilde{O}(2^{n/3})$ である（詳細は 2.1 節を参照）．ゆえにアルゴリズム全体で要する時間は $\tilde{O}(2^{n/3})$ となる．

ここで，ステップ 2 において 2.1 節の多重衝突探索アルゴリズムを用いる際，L を保存するためサイズ $\tilde{O}(2^{n/3})$ の量子メモリ（QRAM）が必要となることに留意されたい．

BHT のアルゴリズムは，サイズ $\tilde{O}(2^{n/3})$ の QRAM を使用し，時間 $\tilde{O}(2^{n/3})$ でランダム関数 h の衝突を見つけるアルゴリズムである．h の評価回数（h へのクエリ回数）は $O(2^{n/3})$ である．

なお，Zhandry によりランダム関数 h の衝突探索に必要な h の評価回数は $\Omega(2^{n/3})$ 以上であるということが証明されているため，h の評価回数という観点からは BHT のアルゴリズムは最良のアルゴリズムである [Zha15].

注意 4.2. 二つの関数 $h, g : \{0,1\}^n \to \{0,1\}^n$ に対して，ペア (x, x') であって $h(x) = g(x')$ を充たすものを関数 h と g の claw と呼ぶ．h と g がランダムであるとき，BHT のアルゴリズムを適用すると h と g の claw を時間 $\tilde{O}(2^{n/3})$ で見つけることができる（ステップ 1 とリスト L はそのままにして，ステップ 2 において多重原像探索アルゴリズムを L と g に適用すればよい）．ここで関数 h の評価は古典的に行えれば十分で，h を計算する量子回路（または h の量子オラクル）は必要が無いことに注意する．

4.3 BHT の効率性をめぐる議論

前節で述べたように BHT のアルゴリズムはランダム関数 h の衝突をサイズ $\tilde{O}(2^{n/3})$ の量子メモリ（QRAM）を用いて時間 $\tilde{O}(2^{n/3})$ で発見する．一見すると BHT のアルゴリズムが Grover のアルゴリズムを用いた自明な衝突探索アルゴリズム[*7]や古典アルゴリズムより効率的であることに議論

[*7] x をランダムに取って $h(x)$ を計算する．次に Grover のアルゴリズムを用いて $h(x') = h(x)$ を充たす $x' \neq x$ を探索する．すると時間 $O(2^{n/2})$ で h の衝突を発見できる．

の余地は無いように思われる．しかし，BHT のアルゴリズムが $\tilde{O}(2^{n/3})$ という非常に大きな量子メモリ（QRAM）を必要とすることから，Grover と Rudolph および Bernstein は BHT のアルゴリズムが Grover のアルゴリズムを用いた自明な衝突探索アルゴリズムや古典アルゴリズムより効率的とは言えないと主張した [Ber09, GR04].

まず Grover と Rudolph は，メモリ用の量子ビットと計算用の量子ビットは古典計算機におけるメモリと CPU のように明確に区別できるようなものではなく，よって大きさ $\tilde{O}(Q)$ の量子メモリを必要とする BHT の効率性を他の衝突探索アルゴリズムの効率性と比較する際は $\tilde{O}(Q)$ 個の量子ビットを全て演算に用いる（並列）量子アルゴリズムを比較対象に入れるのが妥当であると主張した [GR04]．特に，Grover のアルゴリズムを用いた自明な衝突探索アルゴリズムを $\tilde{O}(2^{n/3})$ 量子ビットを用いて並列化すれば BHT のアルゴリズムと同じく時間 $\tilde{O}(2^{n/3})$ で衝突を発見可能であり，よって BHT のアルゴリズムの効率性が並列化した自明な衝突探索アルゴリズムの効率性と変わらないと主張した[*8].

更に Bernstein は，そもそもサイズ $\tilde{O}(2^{n/3})$ の古典計算機がある（あるいは，$\tilde{O}(2^{n/3})$ 個の小さな計算機があって，それらが互いに通信し合い協調して計算を行える）場合は，古典アルゴリズム（並列 rho 法 [vOW94]）を用いて時間 $O(2^{n/6})$ で衝突を発見できることを示した [Ber09] [*9]．$\tilde{O}(2^{n/3})$ 個の量子ビットを使用可能な量子計算機はサイズ $\tilde{O}(2^{n/3})$ の古典計算機としても使えるため，実行時間と使用するハードウェアの大きさとのトレードオフの観点からは古典アルゴリズムの方が BHT の量子アルゴリズムより効率的であると主張した．

■通信コストに関する議論　Bernstein は [Ber09] において，攻撃アルゴリズムの効率を評価する際，通信コストを考慮に入れるべきだと主張している．ここでの通信コストとは，量子計算機を構成する量子ビットの間で情報をやり取りするのに必要なコスト，あるいは小さな（例えば定数サイズまたは多項式サイズの）量子計算機の集合が互いに量子通信を行い協調して計

[*8] なお，$\tilde{O}(2^{n/3})$ 個の量子ビットを用いて並列化した自明な衝突探索アルゴリズムは単位時間あたり $\tilde{O}(2^{n/3})$ 回の h の評価を独立して行うため，h の評価回数は合計で $\tilde{O}(2^{n/3}) \times O(2^{n/3}) = \tilde{O}(2^{2n/3})$ となって BHT のアルゴリズムが h を評価する回数 $O(2^{n/3})$ を大幅に上回る．

[*9] Bernstein の指摘した手法によっても h の評価回数は $\tilde{O}(2^{n/2})$ であり，h の評価回数という観点からは BHT のアルゴリズムの方が優れている．

算を行うことで大規模な（例えば指数的に大きなサイズの）量子計算機を実現しているような状況における通信のコストを指す．以下，大規模な量子計算機が小さな量子計算機の集合として実現されているとき，小さな量子計算機のことを量子プロセッサと呼ぶことにする．

量子回路モデルにおいては，任意の量子ビットのペアを 2 量子ビット入出力の量子ゲートの入力に取ることが可能である．これは大規模な量子計算機が小さな量子プロセッサの集合として実現されている状況において，任意の量子プロセッサ同士が時間 $O(1)$ で通信可能であることに対応する．

しかし現実世界で大規模な量子計算機を実現する際には，量子ビット（あるいは，小さな量子プロセッサたち）が二次元メッシュ状に並べられていて隣り合った量子ビット同士（隣り合ったプロセッサ同士）のみが直接通信できると想定するのが妥当である，と Bernstein は主張した [Ber09] [*10]．2^s 個のプロセッサが $\sqrt{2^s} \times \sqrt{2^s}$ の二次元格子状に配置されており隣り合った量子プロセッサ同士の通信にかかる時間が $O(1)$ のとき，最も離れたプロセッサ同士が通信をしようと思うと $O(\sqrt{2^s})$ だけの時間を要することになる．

Bernstein が [Ber09] において示した古典衝突探索アルゴリズム（並列 rho 法）は，量子ビット（あるいは小さな量子プロセッサ）を二次元格子状に配置した構造の量子計算機でも前述の計算量で衝突探索を実行できる．特に，サイズ 2^s の量子計算機を用いた際に衝突を発見するのに要する時間は $\tilde{O}(2^{n/2-s})$ である．

なお Grover と Rudolph が指摘した自明な衝突探索アルゴリズムの並列化は，多項式サイズの小さな量子プロセッサたちが互いに独立して計算を行うように並列化を行う．ゆえに，プロセッサ間の量子通信は発生しない．なお 2^s 個の多項式サイズの小さな量子プロセッサが利用可能なとき衝突探索に要する時間は $\tilde{O}(2^{(n-s)/2})$ となる．

[*10] この主張が妥当か否かは今後の技術的発展・研究の進展に応じて決まっていくことに留意されたい．

4.4 使用量子ビット数の観点から効率的なアルゴリズム：CNS

量子計算機は古典計算機に比べて実現が非常に難しいという事実を鑑みると，攻撃者の使用可能なリソースとして大規模な古典計算機[*11]と多項式サイズ程度の小さな量子計算機がある，と想定することは妥当である．

このような設定では，BHT のアルゴリズムはもちろんのこと，Grover と Rudolph の指摘した自明な衝突探索アルゴリズムや Bernstein の指摘した並列 rho 法も衝突探索に時間 $O(2^{n/2})$ を要する．しかし Chailloux らはこのような設定において，古典メモリ $\tilde{O}(2^{n/5})$ とサイズ $O(\mathrm{poly}(n))$ の量子計算機を用いて時間 $\tilde{O}(2^{2n/5})$ で衝突を発見するアルゴリズムが存在することを示した [CNS17]．以下このアルゴリズムを，考案者らの頭文字を取って CNS のアルゴリズムと呼ぶことにする．

Chailloux らは [CNS17] において CNS のアルゴリズムを並列化した際の実行時間評価も与えている．CNS のアルゴリズムを 2^s 個の量子プロセッサを用いて並列化すると，時間 $\tilde{O}(2^{2n/5-3s/5})$ で衝突を発見する．なお使用する古典メモリのサイズは $\tilde{O}(2^{n/5+s/5})$ となる．またこの計算量は $s \leq n/4$ のときのみ有効であり，Grover と Rudolph らが指摘した並列アルゴリズムと同様，各量子プロセッサは独立して計算を行うためプロセッサ間の量子通信はしない．

4.5 ここまでのまとめ

本章でこれまでに説明したことを総合すると，ハッシュ関数の衝突探索についての既存研究において，使用可能とされる量子計算リソースの設定には様々なものがあり，以下のように分類できる[*12] ：

> Case 0　小さいサイズの計算用量子プロセッサと，指数的に大きなサイズの量子メモリ（QRAM）から成る量子計算機があるという想定
> Case 1a 小さいサイズの計算用量子プロセッサが大量に使用可能で

[*11] 古典攻撃の研究における典型的な設定に従い，CPU は一つしか持たず並列計算はできないが指数的に大きなメモリを持つと想定する．

[*12] この分類は Case 0 以外，CT-RSA 2018 における細山田と佐々木の分類 [HS18a] に従っている．細山田と佐々木らの分類は多重原像探索攻撃の効率性評価を念頭においたものであるが，衝突探索攻撃の効率性評価でも同じ分類を使うことができる．

あり，任意のプロセッサのペア同士が時間 $O(1)$ で通信できる．

Case 1b 小さいサイズの計算用量子プロセッサが大量に使用可能で２次元格子点状に配置されており，隣り合ったプロセッサ同士のみが（時間 $O(1)$ で）通信できる．

Case 1c 小さいサイズの計算用量子プロセッサが大量に使用可能であり，それらは互いに通信することなく独立して計算を行う．

Case 2　小さいサイズの計算用量子プロセッサが 1 つだけ使用可能である．

なお，小さいサイズというのは高々 n の多項式程度のサイズを指すものとする．また全てのケースにおいて，量子計算機とは別に，計算用プロセッサ（CPU）とメモリを備えた古典計算機が 1 つ追加で使用可能であると想定する（この古典計算機は並列計算を行わないものとし，メモリは指数的に大きなものが使用可能であるとする）．

またそれぞれの設定において最良の衝突探索アルゴリズムは異なる．Case 0 において最も速い衝突探索アルゴリズムは BHT のアルゴリズムである（4.2 節）．Case 2 における現状で最も速い衝突探索アルゴリズムは CNS のアルゴリズムである（4.4 節）．Case 1a-1c では，実行時間と使用する計算機のサイズのトレードオフによって効率性が評価される．利用可能な量子計算機および古典メモリのサイズが同一という条件下では，Case 1a および Case 1b における現状で最も速い衝突探索アルゴリズムは並列 rho 法である（4.3 節）．また Case 1c においては利用可能な量子計算機および古典メモリのサイズに応じて最良のアルゴリズムが変化する．

今後量子コンピュータの研究開発がどのように進展していくかはわからないということ，また共通鍵暗号系技術において安全性パラメータ n は比較的小さな値に固定されており（$n = 128$ など），“n について指数的に大きいサイズ” と “n について高々多項式的程度の小さいサイズ” の区別も曖昧である（例えば $n = 128$ なら $2^{n/3} \approx n^6$ である）ことから，できるだけ様々な状況を想定して攻撃の研究を行い安全性を評価しておくことが重要であると考えられる．

4.6　その他の議論

ここまで紹介した既存研究では簡単のため量子誤り訂正のコストや実際の物理的ハードウェアの実現法を無視し，量子回路の実行時間が回路の深さに比例するとみなして実行時間について論じられていた．しかし，量子誤り訂正のコストや実際の物理的ハードウェアの実現法を考慮に入れると暗号に対する量子アルゴリズムを用いた攻撃の実行コストは量子回路中で使用される量子ゲートの個数あるいは量子回路の幅と深さの積で評価すべきである，という議論も存在する．このような議論の詳細については，例えば Jaques と Schanck の論文 [JS19] を参照されたい．

5　汎用量子攻撃

本章では，暗号技術の内部構造に関わらず適用できるような汎用量子攻撃について，既存の主な研究結果を紹介する．

5.1　Grover のアルゴリズムを用いた鍵回復攻撃と原像探索

2 章の注意 2.2 で触れた，Grover のアルゴリズムを用いた鍵回復攻撃と原像探索の詳細について述べる．

原像探索問題は問題 2.2 の $t = 1$ の場合そのものであるため，n ビット出力ハッシュ関数の原像探索は時間 $O(2^{n/2})$ で実行可能である．

以下秘密鍵の回復について，ブロック暗号の場合を例に取って説明する．E を鍵長 k ビット，ブロック長 n ビットのブロック暗号とする（E は典型的なブロック暗号で k は高々 n の定数倍と仮定する）．まず，平文 P と対応する暗号文 $C = E_k(P)$ のペア (P, C) を $\ell := \lceil k/n \rceil$ 個集める．集めたペアを $(P_1, C_1), \ldots, (P_\ell, C_\ell)$ とする．次に関数 $f : \{0,1\}^k \to \{0,1\}$ を，$E_X(P_i) = C_i$ が全ての $1 \leq i \leq \ell$ について成り立つとき，またその時に限って $f(X) = 1$ となるように定義する．ブロック暗号 E が十分にランダムであれば，$f(K) = 1$ かつ $X \neq K$ なら $f(X) = 0$ が成り立つ．よって Grover のアルゴリズムを f に適用すれば，秘密鍵 K を時間 $O(2^{k/2})$ で発見できる．必要な量子ビットの個数は $\tilde{O}(1)$ となる．

5.2 衝突探索

4 章で述べたように，衝突探索問題については使用可能な量子計算のリソースに関する想定に応じて様々な量子アルゴリズムが存在する．

n ビット出力のランダム関数の衝突を探索するとき，BHT のアルゴリズム（4.2 節）は時間 $\tilde{O}(2^{n/3})$ で衝突を発見し，関数を評価する回数（関数へクエリする回数）は $O(2^{n/3})$ であるが，大きさ $\tilde{O}(2^{n/3})$ の量子メモリを必要とする（4.2 節）．

多項式サイズの小さな（古典または量子）計算用プロセッサが 2^s 個あって互いに通信を取り合いながら並列計算を行える場合，時間 $\tilde{O}(2^{n/2-s})$ で衝突探索が可能であるが，関数を評価する回数は $\tilde{O}(2^{n/2})$ 回となる（4.3 節）．なおこのアルゴリズムは古典アルゴリズム（並列 rho 法）である．

（通常の古典計算機に加えて）n の多項式サイズの小さい量子計算機のみが使える場合でも，CNS のアルゴリズムを用いると時間 $\tilde{O}(2^{2n/5})$ で衝突を探索することができる（4.4 節）．なお CNS のアルゴリズムは大きさ $\tilde{O}(2^{n/5})$ の古典メモリを使用する．

衝突探索アルゴリズムの詳細は 4 章を参照されたい．

5.3 多重衝突探索

関数 f の衝突というとペア (x_1, x_2) であって $x_1 \neq x_2$ かつ $f(x_1) = f(x_2)$ となるものを指すが，それを拡張した概念として関数 f の多重衝突がある．整数 $\ell \geq 2$ に対して関数 f の ℓ-多重衝突とは，組 $(x_1, \ldots, x_\ell)$ であって $i \neq j$ なる任意の i と j について $x_i \neq x_j$ が成り立ち，かつ $f(x_1) = \cdots = f(x_\ell)$ が成り立つものである．

古典計算においてランダム関数 $f : \{0,1\}^m \to \{0,1\}^n$ の ℓ-多重衝突を探索するのに必要な（f への）クエリ回数は $\Theta\left(2^{\frac{\ell-1}{\ell}n}\right)$ となることが知られている [STKT08]．これに対し，量子計算機を用いてランダム関数 f の ℓ-多重衝突を探索するのに必要な（量子）クエリの回数は $\Theta\left(2^{\frac{(2^{\ell-1}-1)}{2^{\ell}-1}n}\right)$ まで下がることが示されている [HSX17, HSTX19, LZ19]．

多重衝突探索問題に似た問題として k-XOR 問題があるが，これについても量子計算機を用いればある程度の高速化が得られることが示されている [CE05, GNS18, NS19]．

5.4 多重原像探索

2.1 節で紹介した多重原像探索問題（問題 2.2）を考える．つまり，ランダム関数 $F : \{0,1\}^n \to \{0,1\}^n$（量子オラクルとして与えられる）と $L \subset \{0,1\}^n$ が与えられたとき，$F(x) \in L$ となるような x を探索することを考える．

2.1 節で紹介した，Grover のアルゴリズムを自明に適用することによって得られる多重原像探索アルゴリズムは，F へのクエリ回数 $O(\sqrt{2^n/|L|})$，時間 $\tilde{O}(\sqrt{2^n/|L|})$ で原像 x を見つけるというものであった．このアルゴリズムは $O(|L|)$ の大きさの量子メモリ（QRAM）を必要とする（4.5 節の分類で言うところの Case 0 にあたる）．

Bernstein と Banegas は Case 1a と Case 1b において，サイズ 2^s の量子計算機を用いた場合にそれぞれ時間 $\tilde{O}\left(\sqrt{\frac{2^n}{|L|\cdot 2^s}}\right)$ および $\tilde{O}\left(\sqrt{\frac{2^n}{|L|^{1/2}\cdot 2^s}}\right)$ で原像を発見できることを示した [BB17]．なおこの計算量は $2^s \geq |L|$ のときのみ有効である．

Chailloux らは Case 2（サイズが高々 n の多項式の小さな量子計算機が一つ利用可能）において，時間 $\tilde{O}(2^{n/2-\ell/6})$ で原像を発見することが出来ることを示した [CNS17]．ここで $\ell := \log |L|$ である．またこの計算量評価は $\ell \leq 3n/7$ であるときに限り有効で，サイズ $\tilde{O}(2^{\ell/3})$ の古典メモリを使用する．

また Chailloux らは Case 1c において，サイズが高々 n の多項式の小さな独立した量子計算機がそれぞれ 2^s 個使用可能であるとき，時間 $\tilde{O}(2^{n/2-\ell/6-s/2})$ で原像を探索することが可能であることを示した [CNS17]．なおこの計算量評価は $\ell \leq (3n+3s)/7$ であるときに限り有効で，サイズ $\tilde{O}(2^{\ell/3})$ の古典メモリを使用する．

5.5 汎用量子攻撃の具体的なコスト評価

AES などの代表的な共通鍵暗号系技術に対して Grover のアルゴリズムを用いた鍵全数探索などの汎用攻撃を実行するのに必要なコストを，攻撃対象のプリミティブを量子回路上へ実装する際のコストも込みで具体的に見積もろうという研究もなされている [GLRS16, ASAM18, JNRV19, LPS20, AMG+16].

例えば，深さ高々 2^{76}，幅高々 2^{11} 量子ビットの回路に，高々 2^{86} 個の Clifford+T ゲートを使用することで Grover のアルゴリズムを用いた AES-128 への鍵回復攻撃を実装できることが示されている [LPS20]．同様に SHA-2 や SHA-3 への原像探索攻撃にかかるコスト評価の研究も行われている [AMG+16]（原像探索のコスト評価の詳細については，原論文を参照されたい）．

6 Q2 モデルにおける攻撃

本章では Q2 モデルにおける攻撃，すなわち攻撃者が量子計算機を所有していることに加え秘密鍵の埋め込まれたオラクルへ量子クエリを行えるという状況下での攻撃について，これまでに発表されている主な結果を紹介する．

6.1 Even-Mansour 暗号への鍵回復攻撃

P を n ビットの公開置換とする．Even-Mansour 暗号 [EM91] は，その暗号化関数が P および 2 つの n ビット鍵 K_1, K_2 を用いて $E_{K_1,K_2}(M) = P(M \oplus K_1) \oplus K_2$ と定義されるブロック暗号である（図 4 を参照）．P が

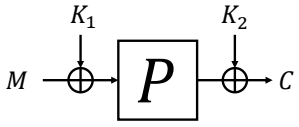

図 4　Even-Mansour 暗号

ランダム置換であるという理想化された状況において，Even-Mansour 暗号は多項式時間の古典攻撃に対し安全な強擬似ランダム置換（SPRP）であることが証明されている．しかし桑門と森井は，Q2 モデルにおいては Even-Mansour 暗号の鍵を多項式時間で回復できるということを示した [KM12]．以下攻撃の概要を述べる．

まず関数 $f : \{0,1\}^n \to \{0,1\}^n$ を $f(x) := E_{K_1,K_2}(x) \oplus P(x)$ と定義す

る．すると，

$$\begin{aligned} f(x \oplus K_1) &= E_{K_1,K_2}(x \oplus K_1) \oplus P(x \oplus K_1) \\ &= P(x \oplus K_1 \oplus K_1) \oplus K_2 \oplus P(x \oplus K_1) \\ &= P(x) \oplus K_2 \oplus P(x \oplus K_1) \\ &= f(x) \end{aligned}$$

が成り立ち，f は秘密鍵 K_1 を周期に持つ周期関数である．Q2 モデルでは，攻撃者に暗号化関数 E_{K_1,K_2} の量子オラクルが与えられている．また P は公開置換であるので，攻撃者は置換 P の値を量子重ね合わせで計算することが出来る．よって攻撃者は関数 f の値も量子重ね合わせで評価することが出来る（f の量子オラクルをシミュレートすることが出来る）．P が十分にランダムであれば，攻撃者は f へ Simon のアルゴリズムを適用することにより多項式時間で K_1 を回復することが出来る[*13]．一旦 K_1 を回復することができれば，$K_2 = E_{K_1,K_2}(x) \oplus P(x \oplus K_1)$ が全ての x について成り立つため，K_2 も容易に計算することが出来る．以上が桑門と森井による Even-Mansour 暗号への鍵回復攻撃の概要である．

Even-Mansour の構造を持つ暗号技術として，Chaskey [MMH+14] が挙げられる．Chaskey 自体はブロック暗号ではなくメッセージ認証コードであるが，メッセージ長が短いときの構造は本質的に Even-Mansour 暗号であり，上記の攻撃を適用することができる．

6.2 Feistel 暗号（Luby-Rackoff 構成）への識別攻撃

本節では桑門と森井による Feistel 暗号（Luby-Rackoff 構成） [LR85] への識別攻撃 [KM10] の概要を述べる．

r を正整数とする．鍵付き関数 $F_{K_i}^{(i)} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ が $i = 1, \ldots, r$ について与えられているとき，r 段 Feistel 暗号（あるいは r 段 Luby-Rackoff 構成）は暗号化関数 $\mathrm{Enc}_{K_1,\ldots,K_r}$ が平文 $x_L||x_R \in \{0,1\}^n$（ここで $x_L, x_R \in \{0,1\}^{n/2}$）に対し以下のようにして定められるブロック暗号

[*13] P が十分にランダムでないと Simon のアルゴリズムを適用しても K_1 を回復することはできない．たとえば P が恒等置換である場合，$f(x) = K_1 \oplus K_2$ が全ての x について成り立ってしまう．このとき Siomon のアルゴリズムを用いても K_1 を計算することができない．しかし P が十分にランダムであれば Simon のアルゴリズムが K_1 を返すということが示される [KLLN16a].

である:

$$\mathrm{Enc}_{K_1,\ldots,K_r}(x_L, x_R) := \left(R^{(r)}_{K_r} \circ \cdots \circ R^{(1)}_{K_1}\right)(x_L, x_R), \tag{9}$$

ただしここで

$$R^{(i)}_{K_i}(x_L, x_R) = \left(x_R \oplus F^{(i)}_{K_i}(x_L)\right) || x_L. \tag{10}$$

$R^{(i)}$ については図 5 を，$r = 3$ の場合の暗号化関数 $\mathrm{Enc}_{K_1,K_2,K_3}$ については図 6 を，それぞれ参照されたい． Feistel 暗号の構造は DES [Nat77] や

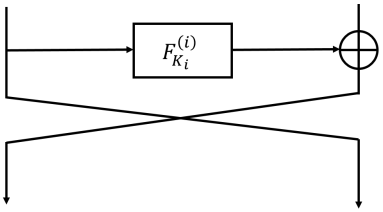

図 5　Feistel 暗号の第 i ラウンド

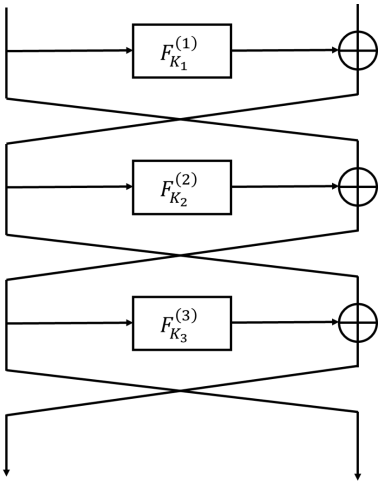

図 6　3 ラウンド Feistel 暗号

Camellia [AIK+00] を初めとした様々なブロック暗号に採用されている．以下，簡単のため鍵付き関数の鍵長は全て同じであるとする．

各 $F^{(i)}_{K_i}$ が多項式時間の古典攻撃に対して安全な擬似ランダム関数（PRF）のとき，3 段 Feistel 暗号は多項式時間の古典選択平文攻撃に対して安全な擬似ランダム置換（PRP）になり，また 4 段 Feistel 暗号は多項式時間の古

典選択暗号文攻撃に対して安全な強擬似ランダム置換（SPRP）になることが証明されている [LR85]．一方桑門と森井は，たとえ各 $F_{K_i}^{(i)}$ が多項式時間の量子クエリ攻撃に対して安全な擬似ランダム関数であったとしても，3 段 Feistel 暗号を多項式時間の量子選択平文攻撃によって n ビットランダム置換から識別する攻撃アルゴリズムが存在する（つまり 3 段 Feistel 暗号は量子擬似ランダム置換（qPRP）ではない）ことを示した．以下，桑門と森井による量子識別攻撃の概要を述べる．

まず識別攻撃の設定を説明する．攻撃者には n ビット置換 Π の量子オラクルが与えられている．Π は 3 段 Feistel 暗号の暗号化関数 $\mathrm{Enc}_{K_1,K_2,K_3}$ あるいは n ビットランダム置換 RP のいずれかである．攻撃者の目的は Π が $\mathrm{Enc}_{K_1,K_2,K_3}$ と RP のいずれであるかを識別することである．

桑門と森井による攻撃では，まず $\alpha_0, \alpha_1 \in \{0,1\}^{n/2}$ であって $\alpha_0 \neq \alpha_1$ となるものを任意に取って固定し，関数 $f^{\Pi} : \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ を

$$f^{\Pi}(b,x) := \Pi(\alpha_b, x)_R \oplus \alpha_b \tag{11}$$

と定義する．ただしここで $\Pi(\alpha_b, x)_R$ は $\Pi(\alpha_b, x)$ の下位 $n/2$ ビットである．

$\Pi = \mathrm{Enc}_{K_1,K_2,K_3}$ ならば，

$$f^{\Pi}(b,x) = \mathrm{Enc}_{K_1,K_2,K_3}(\alpha_b, x)_R \oplus \alpha_b = F_{K_2}^{(2)}\left(F_{K_1}^{(1)}(\alpha_b) \oplus x\right) \tag{12}$$

であるから

$$f^{\Pi}\left((b,x) \oplus \left(1, F_{K_1}^{(1)}(\alpha_0) \oplus F_{K_1}^{(1)}(\alpha_1)\right)\right) = f(b,x)$$

が任意の $(b,x) \in \{0,1\} \times \{0,1\}^n$ に対して成り立つことがわかる．特に f^{Π} は $\left(1, F_{K_1}^{(1)}(\alpha_0) \oplus F_{K_1}^{(1)}(\alpha_1)\right)$ を周期とする周期関数である．一方 $\Pi = \mathsf{RP}$ の場合，高確率で f^{Π} は周期的にならない．

よって f^{Π} が周期をもつか否か Simon のアルゴリズムを用いて調べることにより，Π が $\mathrm{Enc}_{K_1,K_2,K_3}$ と RP のどちらであるか多項式時間で識別することができる．以上が桑門と森井による識別攻撃の概要である．

この攻撃は 4 段 Feistel 暗号への量子選択暗号文攻撃による識別攻撃 [IHM+19] や一般化 Feistel 暗号への攻撃にも拡張されている [DLW19, NIDI19]．また関連する後続研究として，ラウンド関数 $F_{K_i}^{(i)}$ が特定の構造

を持つ状況下での攻撃の研究や，識別攻撃を鍵回復攻撃へ拡張する研究などがある [BNS19a, DW18, HS18b].

6.3 種々の暗号利用モードに対する多項式時間攻撃

CRYPTO 2016 において Kaplan らは，Q2 モデルにおいて Simon のアルゴリズムを適用すると，CBC-MAC（XCBC [BR00]，OMAC [IK03]，CMAC [NIS05] などの変種を含む）や GCM [MV04] など現在幅広く使用されている様々な共通鍵暗号系技術，特にブロック暗号利用モードが多項式時間で破られることを示した [KLLN16a]．多項式時間で破られることが示された暗号技術は CBC-MAC や GCM の他に，PMAC [BR02]，GMAC [MV04]，OCB [RBBK01, Rog04, KR11]，LRW 構成 [LRW02]，などがある．Kaplan らはまた同時に，古典的に指数時間を要する slide attack [BW99] が Q2 モデルにおいて多項式時間まで高速化可能であることも示した[*14]．攻撃の詳細は原論文を参照されたい．

6.4 Grover のアルゴリズムと Simon のアルゴリズムの組み合わせ

本節では，Leander と May による FX 構成への Q2 モデルにおける攻撃 [LM17] の概要を紹介する．攻撃は，Grover のアルゴリズムと Simon のアルゴリズムの組み合わせにより実現される．

まず鍵長 k ビットの n ビットブロック暗号 $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ から作られる FX 構成 [KR96] とは，鍵長 $(k+2n)$ ビットの n ビットブロック暗号 $E' : \{0,1\}^{k+2n} \times \{0,1\}^n \to \{0,1\}^n$ であって，

$$E'(K_0, K_1, K_2, x) := E_{K_0}(x \oplus K_1) \oplus K_2 \tag{13}$$

により定義されるものことである．（ここで，$K_0 \in \{0,1\}^k$ かつ $K_1, K_2, x \in \{0,1\}^n$ である．図 7 参照.）古典的には，E が理想的にランダムなブロック暗号であれば，FX 構成 E' をランダム置換と識別するためには暗号化オラクルおよび復号オラクルへおよそ $2^{(m+n)/2}$ 回のクエリを行わねばならないことが証明される．

Q2 モデルにおいて FX 構成の鍵を回復を試みる際，まず自然な発想とし

[*14] この結果はのちに advanced slide attack [BW00] の指数的高速化に拡張されている [BNS19a].

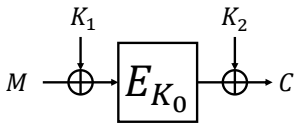

図 7　FX 構成

て思い付くのは，FX 構成が Even-Mansour 暗号に似ているから Simon のアルゴリズムで攻撃できないだろうか，というアイデアである．実際，秘密鍵のうち K_0 が判っていれば，残りの鍵 K_1 および K_2 は Even-Mansour への攻撃と同様 Simon のアルゴリズムを用いて多項式時間で回復できる[*15]．

このアイデアを用いると，以下のようにして全ての秘密鍵を回復することができる．なお FX 構成 $E'_{K_0,K_1,K_2}(x) = E_{K_0}(x \oplus K_1) \oplus K_2$ の暗号化関数の量子オラクルが与えられているものとする．

1. 全ての $K'_0 \in \{0,1\}^k$ に対して以下のステップ a と b を実行する：
   （a）関数 $f_{K'_0}$ を $f_{K'_0}(x) := E'_{K_0,K_1,K_2}(x) \oplus E_{K_0}(x)$ で定義する．（$K'_0 = K_0$ であれば $f_{K'_0}$ は周期関数になり，また E が理想的にランダムなブロック暗号であれば $K_0 \neq K'_0$ のとき $f_{K'_0}$ は周期関数にならないため，$K'_0 = K_0$ かどうかを $f_{K'_0}$ が周期関数かどうかで判定できる．なお f_{K_0} の周期は K_1 である．）
   （b）Simon のアルゴリズムを $f_{K'_0}$ へ適用し，$f_{K'_0}$ が周期関数か否か，すなわち $K'_0 = K_0$ であるか調べる．$K'_0 = K_0$ であればステップ 2 へ移る．
2. f_{K_0} に Simon のアルゴリズムを適用して K_1 を回復する．また $K_2 = E'_{K_0,K_1,K_2}(0^n) \oplus E_{K_0}(K_1)$ であることを用いて K_2 を回復する．

ステップ 1 では 2^k 個の鍵候補を全数探索しており，また Simon のアルゴリズムは多項式時間で実行できることから，この攻撃の実行時間は $\tilde{O}(2^k)$ となる．

ここで，次のアイデアが自然な発想として浮かんでくる：

[*15] E_{K_0} を 6.1 節における置換 P とみなせばよい．

2^k 個の鍵の全数探索を Grover のアルゴリズムで行えば攻撃時間を $\tilde{O}(2^{k/2})$ まで下げられるのではないか？

K_0 を Grover のアルゴリズムで探索するためには関数 $F : \{0,1\}^k \to \{0,1\}$ であって $F^{-1}(1) = \{K_0\}$ となるものを量子重ね合わせで評価できる量子回路を実装する必要がある．関数 F の実装として自然なものは先述したアルゴリズムのステップ 1a-1b，すなわち “$f_{K_0'}$ に Simon のアルゴリズムを適用し，$f_{K_0'}$ が周期関数のとき，またその時に限って $F(K_0') = 1$ と計算する” というものである．

しかしここで Simon のアルゴリズムが量子状態の観測を複数回行うことが問題になる：Grover のアルゴリズムを F に適用する際，F を実装する量子回路は途中での観測を行ってはならない．ところが Siomon のアルゴリズムは複数回の量子状態の観測を含むため，F の量子回路をどう構築すれば良いかは自明ではない．

Leander と May は Asiacrypt 2017 において，Simon のアルゴリズムのサブルーチン **SSub**（2.2 節を参照）から最後の観測を除いたものを並列して走らせることで途中の観測なしで F を実装する量子回路を示し，また詳細な誤差解析を行って実際に FX 構成の秘密鍵を時間 $\tilde{O}(2^{k/2})$ で回復できることを証明した [LM17]．攻撃に必要な量子ビットの個数は高々 k と n の多項式で抑えられる．

Leander と May の論文は FX 構成への攻撃しか取り扱っていないが，Grover と Simon の二つのアルゴリズムを組み合わせて攻撃に用いたいという場面では基本的に Leander と May の手法が適用可能である．

6.5 隠れシフト問題と Kuperberg のアルゴリズム

本節では共通鍵暗号系技術に対する量子攻撃と隠れシフト問題および Kuperberg のアルゴリズム [Kup05] との関わりについて概観する．

ブロック暗号などの共通鍵系暗号系技術に Simon のアルゴリズムを用いた量子攻撃を行う際は，秘密鍵に依存するようなある秘密情報 $s \in \{0,1\}^m$ と全ての $x \in \{0,1\}^m$ に対して $f_0(x) = f_1(x \oplus s)$ が成り立つような 2 つの関数 $f_0, f_1 : \{0,1\}^m \to \{0,1\}^n$ を，鍵の埋め込まれたオラクルから構成することが多い．なぜなら，このような関数 f_0, f_1 を構成できたとすると，関数 $F : \{0,1\} \times \{0,1\}^m \to \{0,1\}^n$ を $F(b,x) = f_b(x)$ と定義すれば F は

$(1, s)$ を周期に持つ周期関数になり，Simon のアルゴリズムを F へ適用することで秘密情報 s を得られることが多いからである．

上記の関数 f_1 は関数 f_0 から隠れた（秘密の）情報 s だけ入力がシフトされた関数であると見ることができる．一般に G を有限群，X を集合とし，二つの関数 $f_0, f_1 : G \to X$ が次の条件を満たすとする：或る $g \in G$ があって任意の $x \in G$ に対して $f_0(g) = f_1(g \cdot s)$ が成り立つ[*16]．f_0 と f_1 のオラクルが与えられたときに s を求める問題を隠れシフト問題と呼ぶ．

隠れシフト問題は $G = (\mathbb{Z}/\mathbb{Z}_2)^n$ のときは上述のように Simon のアルゴリズムを用いて効率的に解くことができるが，G が巡回群 $\mathbb{Z}/2^n\mathbb{Z}$ の場合は多項式時間で解けるアルゴリズムが知られていない．$G = \mathbb{Z}/2^n\mathbb{Z}$ の場合，現時点での最良のアルゴリズムは Kuperberg のアルゴリズム [Kup05] であり，問題を解くのに要する計算量は $\tilde{O}\left(2^{\sqrt{2\log_2(3)n}}\right)$ である．

Alagic と Russell はこの事実に着目し，（ある条件下での）隠れシフト問題を多項式時間で解くことが困難であると仮定して，共通鍵暗号系技術で使用される群演算を $(\mathbb{Z}/\mathbb{Z}_2)^n$ の演算（XOR 演算）から $\mathbb{Z}/2^n\mathbb{Z}$ の演算（Modular Addition）に変更すれば，本章でここまでに紹介したような多項式時間攻撃が効かなくなるということを示した [AR17]．

しかしのちに Bonnetain と Naya-Plasencia は，共通鍵暗号系技術で実際に使用されるパラメータ n が小さい（ブロック暗号のブロック長としてよく用いられるのは $n = 128$）を考慮すると，Kuperberg のアルゴリズムの計算量 $\tilde{O}\left(2^{\sqrt{2\log_2(3)n}}\right)$ はさほど大きくなく，このような演算の変更は Q2 モデルにおける量子攻撃への対策として必ずしも効果的とは言えないということを指摘した [BN18]．

例えば n ビットブロックの Even-Mansour 暗号について，Simon のアルゴリズムを用いた攻撃（6.1 節参照）を防ぐために XOR 演算を Modular Addition に変更したとしても，Kuperberg のアルゴリズムを用いれば n が 5000 程度であれば時間 2^{128} を下回るような攻撃が可能であると示されている．Bonnetain らと Naya-Plasenia は同時に，Kuperberg のアルゴリズムを応用するとメッセージ認証コード Poly1305 [Ber05] を攻撃できるということも示している．

[*16] ここでは共通鍵暗号系技術への攻撃への応用を考えるため，f_0 と f_1 および s はランダムに選ばれる状況を考える．

6.6 関連鍵攻撃

本節では関連鍵攻撃の量子版に関する既存研究について概観する．

古典的な関連鍵攻撃の設定として，E_K を k ビット鍵の n ビットブロック暗号としたとき（$K \in \{0,1\}^k$ は秘密鍵），入力 $(x, M) \in \{0,1\}^k \times \{0,1\}^n$ に対して $E_{K\oplus x}(M)$ を返すオラクル $\mathcal{O}_K$ と，入力 $(x, C) \in \{0,1\}^k \times \{0,1\}^n$ に対して $E^{-1}_{K\oplus x}(C)$ を返すオラクル $\mathcal{O}_K^{-1}$ が攻撃者に与えられる，というものがある [WH87]．E が理想的にランダムなブロック暗号であれば，古典的にはこの設定で秘密鍵 K を回復するのに指数時間を必要とする．

一方 Rötteler と Steinwandt は，$\mathcal{O}_K$ の量子オラクルが与えられていれば以下のようにして秘密鍵 K を多項式時間で回復できることを示した [RS15]：$M \in \{0,1\}^n$ を任意に固定し，関数 f を $f(x) := \mathcal{O}_K(x, M) \oplus E_x(M) = E_{x\oplus K}(M) \oplus E_x(M)$ と定義する．すると f は明らかに秘密鍵 K を周期に持つ周期関数であり，Simon のアルゴリズムを適用することによって K を多項式時間で回復することが出来る．

この攻撃はほぼ全ての（古典的に安全な）ブロック暗号に適用可能なものであり理論上興味深いものではあるが，$\mathcal{O}_K$ の量子オラクルが攻撃者に与えられるような状況が現実的に起こることは想定しづらい．Rötteler と Steinwandt による上記の攻撃の外にも，スライド攻撃を拡張した関連鍵攻撃が可能であることが示されている [HA]．

6.7 その他の古典攻撃の高速化

量子計算機を用いると様々なアルゴリズムが高速化され得るため，代表的な古典攻撃が量子計算機を用いた際どれだけ高速化できるかということは，たとえ指数的高速化が得られずとも重要な研究の対象となる．量子クエリが行える状況下（Q2 モデル）における古典攻撃の高速化に関する前節までに挙げたもの以外の主な研究結果としては，差分解読法・線型解読法の高速化 [KLLN16b] などが挙げられる[*17]．なお [KLLN16b] で論じられている差分解読法・線型解読法の量子版は，対応する古典攻撃でかかる時間を T としたとき，大雑把に言って $\sqrt{T}$ あるいはそれ以上の時間を要する．

[*17] Q1 モデルにおける攻撃は Q2 モデルにおける攻撃としても成立するが，本節では Q1 モデルの攻撃は紹介しない．Q1 モデルにおける同様の研究結果については 7.4 節を参照されたい．

7　Q1 モデルにおける攻撃

本章では Q1 モデルにおける攻撃，すなわち攻撃者が量子計算機を所有しているが攻撃者に与えられる鍵の埋め込まれたオラクルは古典オラクルであるという状況下での攻撃について，これまでに発表されている主な研究結果を紹介する．

7.1　桑門・森井による Even-Mansour 暗号への鍵回復攻撃

6.1 節で紹介した Q2 モデルにおける Even-Mansour 暗号への多項式時間攻撃は秘密鍵の埋め込まれたオラクルへの量子クエリを必要とするため，Q1 モデルでは実行できない．しかし桑門と森井は，Q1 モデルにおいても量子衝突探索アルゴリズム[*18]を用いれば時間 $\tilde{O}(2^{n/3})$ で鍵を回復できることを示した [KM12]．以下その概要を述べる．

Even-Mansour 暗号の暗号化関数は，公開置換 P と秘密鍵 K_1, K_2 を用いて $E_{K_1,K_2}(M) := P(M \oplus K_1) \oplus K_2$ と定義されるのであった．まず，関数 $h : \{0,1\}^n \to \{0,1\}^n$ を $h(x) := E_{K_1,K_2}(x) \oplus E_{K_1,K_2}(\overline{x})$ で定義する．ここで $\overline{x}$ はビット列 x の各ビットを反転したもの，つまり $\overline{x} = x \oplus 1^n$ である．更に関数 $g : \{0,1\}^n \to \{0,1\}^n$ を $g(x) := P(x) \oplus P(\overline{x})$ で定義する．すると $h(x \oplus K_1) = g(x)$ が全ての x について成り立つ．更に，P が十分にランダムであれば $h(x) = g(y)$ であるとき高確率で $x = y \oplus K_1$ または $x = \overline{y} \oplus K_1$ となることが期待できる．よって，$h(x) = g(y)$ となるペア (x, y) を見つければ（つまり関数 h と g の claw を見つければ）K_1 を回復することができる．そのようなペアは BHT のアルゴリズムにより，時間 $\tilde{O}(2^{n/3})$ で探索することができる．（注意 4.2 を参照．今は Q1 モデルにおける攻撃を考えているため暗号化オラクルは古典オラクルであり関数 h の評価は古典的にしか行えないが，P が公開置換であるため関数 g の評価は量子重ね合わせで行うことが出来る．）一旦 K_1 を回復することができれば，K_2 は容易に計算することができる．なおこの攻撃は BHT のアルゴリズムを用いるため大きさ $\tilde{O}(2^{n/3})$ の量子メモリを必要とする．

[*18] より正確には claw 探索アルゴリズム．

7.2　オンライン-オフライン中間一致攻撃

細山田と佐々木は，前節で紹介した桑門と森井の Q1 モデルにおける攻撃が中間一致攻撃の一種（オンライン-オフライン中間一致攻撃）とみなせることに着目し，使用可能な量子計算のリソースに関する想定（4.5 節参照）に応じてトレードオフが変化すること，また Even-Mansour 暗号以外にも FX 構成などに同種のオンライン-オフライン中間一致攻撃を適用できることを示した [HS18a]．以下，オンライン-オフライン中間一致攻撃およびその量子版の概要を述べる．

まず，攻撃対象の暗号技術の暗号化関数等から，次のような性質を充たす関数 $f_s, f_p : \{0,1\}^n \to \{0,1\}^n$ を構成できるという状況を考える：

1. f_s は秘密鍵に依存する関数であり，鍵の埋め込まれたオラクルへのクエリをしないと値を計算できない．
2. f_p は秘密鍵に依存しない関数であり，鍵の埋め込まれたオラクルへのクエリなしで，オフラインで計算できる関数である．
3. f_s と f_p の間の claw[*19]を発見すれば何らかの秘密情報（秘密鍵等）を抽出できる．

7.1 節の攻撃で言うと，f_s と f_p が h と g にそれぞれ対応する．以下簡単のため f_s と f_p はランダム関数であるとみなす．また，各 x に対する値 $f_s(x)$ の計算は，鍵の埋め込まれたオラクルへのクエリを $O(1)$ 回行えば時間 $O(1)$ で可能だと仮定し，また各 x に対する値 $f_p(x)$ の計算は時間 $O(1)$ で可能であるとする．

古典的な設定（攻撃者が古典計算機のみを所持している設定）では，以下のようにして f_s と f_p の claw (x, y) を発見し，何らかの秘密情報を抽出することができる：

1. 鍵の埋め込まれたオラクルへのクエリ（オンラインクエリ）を行い $(x, f_s(x))$ の形のペアを異なる D 個の x について計算してリスト L に保存する．
2. L（の各要素の第二成分たち）を原像探索の標的として f_p について

[*19] ペア (x, y) であって $f_s(x) = f_p(y)$ を充たすもの

（古典）多重原像探索を行う．

ステップ 2 に要する計算時間（関数 f_p の評価回数）を T とすると，$T = \tilde{O}(2^n/D)$ が成り立つ．換言すれば，オンラインクエリの回数 D とオフラインの計算時間 T について $T \cdot D = \tilde{O}(2^n)$ のトレードオフが得られる．

この攻撃は鍵の埋め込まれたオラクルへのオンラインクエリを行うことによってのみ計算できる関数 f_s とオフラインで計算できる関数 f_s の値が一致しているペア (x, y) を探索する攻撃であることから，オンライン-オフライン中間一致攻撃と呼ばれる．

次に Q1 モデルにおける攻撃を考える．関数 $f_s(x)$ の値を計算をするためには古典的攻撃と同様各 x に対して $O(1)$ 回ずつ鍵の埋め込まれたオラクルへ古典クエリを行わざるを得ないが，f_p は鍵に依存しないため攻撃者が量子計算機を用いてオフラインで計算できる．特に，先述した古典攻撃のうち，ステップ 2 における f_p についての多重原像探索を量子計算機を用いて高速化することができる．

例えば 4.5 節でいうところの Case 0 の設定（QRAM が使用可能な状況）では，2.1 節で紹介した Grover のアルゴリズムを直接応用した多重原像探索アルゴリズムを用いることにより，時間 $T = \tilde{O}(\sqrt{2^n/D})$ のオフライン量子計算によって f_s と f_p の claw を発見できる．換言すれば，T と D について $T^2 \cdot D = \tilde{O}(2^n)$ のトレードオフを得られる．7.1 節の攻撃は，この例で $f_s = h$，$f_p = g$，$D = 2^{n/3}$ と設定した場合とみなすことができる．

細山田と佐々木は 4.5 節における他の Case についても，それぞれの設定で最良の多重原像探索アルゴリズム（5.4 節参照）を用いた場合に得られる T と D のトレードオフを示している．詳細は原論文を [HS18a] を参照されたい．

いくつかの共通鍵暗号系技術は，（古典）オンライン-オフライン中間一致攻撃が最良の攻撃であるという前提で安全性を見積もっている．例えば Chaskey（$n = 128$）の設計者たちは，$D \leq 2^{48}$ である限り実行時間が $2^{80}(= 2^n/2^{48})$ を下回るような攻撃は存在しない，と主張している [MMH+14]．しかし Q1 モデルにおいて上述のように量子多重原像探索アルゴリズムを用いると，その主張は 4.5 節のいずれのケースにおいても成り立たないことになる．たとえば Case 2（通常の古典計算リソースに加えて量子ビットが高々 n の多項式個の小さい量子計算機を 1 つ使用可能）の

場合であっても，およそ 2^{48} 回程度の古典クエリをしておけば，時間およそ 2^{56} のオフライン計算により秘密鍵を回復可能であることが示される．

7.3 量子クエリ無しでの Simon のアルゴリズムの応用

6 章で述べたように，古典的に安全とされる共通鍵暗号系技術であっても Simon のアルゴリズムを用いると多項式時間で破れてしまう場合があるという研究結果が近年複数発表されているが，それらの攻撃は全て鍵の埋め込まれたオラクルへの量子クエリを前提とする攻撃（Q2 モデルにおける攻撃）である．

Q2 モデルにおいては Simon のアルゴリズムにより各種攻撃の指数的高速化が可能となる一方で，鍵の埋め込まれたオラクルが古典オラクルである Q1 モデルにおいて Simon のアルゴリズムの恩恵を受けることができるかどうかは不明であった．しかし Bonnetain らは Asiacrypt 2019 において，Q1 モデルでの攻撃でも Simon のアルゴリズムを応用した攻撃が可能なことを示した [BHN+19]．

Bonnetain らの攻撃は，大雑把に言って

1. Q2 モデルにおいて Simon のアルゴリズム（または Simon のアルゴリズムと別の量子アルゴリズムの組み合わせ）を用いた攻撃が可能
2. 7.2 節のオンライン-オフライン中間一致攻撃が適用可能

という二つの条件が満たされるような共通鍵暗号系技術に対し，高々多項式個の量子ビットを使うような小さい量子計算機のみをもちいて（4.5 節での Case 2 に対応），既存の攻撃より高速な攻撃を実現するものである．

攻撃を適用可能な共通鍵暗号系技術としては Even-Mansour 暗号や FX 構成が挙げられる．例えば Bonnetain らの攻撃を Even-Mansour 暗号へ適用すると，鍵回復攻撃を多項式サイズの量子メモリおよび古典メモリのみを用いて $\tilde{O}(2^{n/3})$ 古典クエリ・時間 $\tilde{O}(2^{n/3})$ で実行可能となる．他の攻撃との比較は表 1 を参照されたい．

Bonnetain らの攻撃ではまず，指数回の古典クエリを鍵の埋め込まれたオラクルへ行い，クエリを一回行うごとにクエリの結果に応じて（多項式サイズの）量子メモリに保存されている量子状態を少しずつ変化させていく．必要な古典クエリが終ったのち，量子メモリに保存された量子状態 $|\phi\rangle$

4.5 節の Case	時間	クエリ	量子ビット (量子メモリ)	古典メモリ	出典
Case 0	$2^{n/3}$	$2^{n/3}$	$2^{n/3}$	$2^{n/3}$	[KM12]
Case 1a	$2^{n/4}$	$2^{n/4}$	$2^{n/4}$	$2^{n/4}$	[HS18a]
Case 1b	$2^{2n/7}$	$2^{2n/7}$	$2^{2n/7}$	$2^{2n/7}$	[HS18a]
Case 1c	$2^{3n/10}$	$2^{3n/10}$	$2^{3n/10}$	$2^{3n/10}$	[HS18a]
Case 2	$2^{3n/7}$	$2^{3n/7}$	$\mathrm{poly}(n)$	$2^{n/7}$	[HS18a]
Case 2	$2^{n/3}$	$2^{n/3}$	$\mathrm{poly}(n)$	$\mathrm{poly}(n)$	[BHN+19]

表 1　Even-Mansour 暗号への Q1 モデルにおける攻撃の比較．Bonnetain らの攻撃の計算量は最下段に赤字で示されている．なおオーダー記号は省略している．また計算量はクエリ回数と時間が（Case 1a-1c については更にメモリも）バランスする点のみを示している．

を用いて，Simon のアルゴリズムと Grover のアルゴリズムを組み合わせたオフライン計算により秘密情報を回復する．量子メモリに保存する $|\phi\rangle$ をうまく取ることによって Simon のアルゴリズムを活用することが可能となる．攻撃の技術的詳細は原論文 [BHN+19] を参照されたい．

注意 7.1. 6.3 節で Q2 モデルにおいては CBC-MAC，GCM，PMAC，GMAC，OCB，LRW 構成等が多項式時間で破られるという結果を紹介したが，これらの暗号技術に本節で紹介した攻撃は適用できない．

7.4　その他の古典攻撃の高速化

Q2 モデルと同様 Q1 モデルにおいても，量子計算機を用いると様々なアルゴリズムが高速化され得るため，代表的な古典攻撃が量子計算機を用いた際どれだけ高速化できるかということは重要な研究の対象となる[*20]．Q1 モデルにおける古典攻撃の高速化に関する前節までに挙げたもの以外の主な研究結果としては，繰り返し構造を持つブロック暗号への中間一致攻撃の高速化 [Kap16] や差分解読法・線型解読法の高速化 [KLLN16b]，積分攻撃の高速化 [BNS19b]，Demiric-Selçuk 中間一致攻撃の高速化 [HS18b, BNS19b]，

[*20] Q1 モデルにおける攻撃はそのまま Q2 モデルにおける攻撃として成立するため，ここで挙げた攻撃は全て Q2 モデルにおける攻撃とみなすこともできる．Q2 モデルにおける同様の研究結果については 6.7 節を参照されたい．

などが挙げられる．なおいずれの攻撃も，対応する古典攻撃でかかる時間を T としたとき，大雑把に言って $\sqrt{T}$ あるいはそれ以上の時間を要する．

8 考察とまとめ

量子コンピュータが共通鍵暗号系技術の安全性に及ぼす影響の調査および評価を報告した．既存文献について調査を行い，量子コンピュータを用いた攻撃のモデル，特にハッシュ関数以外の（秘密鍵を用いる）共通鍵暗号系技術への攻撃のモデルには Q1 モデルと Q2 モデルの二種類のモデルが存在することを確認した．Q1 モデルにおいては鍵の埋め込まれたオラクルは古典的な攻撃モデルと同じ古典オラクルだが，Q2 モデルにおいては鍵の埋め込まれたオラクルが量子オラクルとなる．それぞれのモデルでの攻撃，およびそれらモデルに依存せず利用できる汎用攻撃について既存文献を調査した．また主にハッシュ関数への衝突探索攻撃について，攻撃コストの評価に関する既存の議論の調査を行った．

Q2 モデルにおいては，古典的に安全とされているいくつかの共通鍵暗号系技術（CBC-MAC や GCM など）に多項式時間の攻撃が存在するが，このモデルでの攻撃を実行するためには攻撃対象の暗号技術が量子回路上に実装されている必要がある．ある関数を計算するための古典計算機向けのプログラムコードがあった場合その関数を量子回路上に実装することが可能になるため，Q2 モデルにおいて多項式時間の攻撃が可能な暗号技術については，例え難読化処理等を施しても，その関数（例えば CBC-MAC でメッセージからタグを計算する関数）を実装して秘密鍵を埋め込んだコードを，量子コンピュータを持った攻撃者に手渡すべきではない．しかし，攻撃対象となる暗号技術が量子回路上に実装されているような（あるいは量子回路上に移植可能となるような）非常に特殊な状況でない限り，既存の共通鍵暗号系技術，特に CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号系技術に，Q2 モデルの攻撃の影響が及ぶことは現状では無いと考えられる．

Q1 モデルでの攻撃およびハッシュ関数への攻撃については，Q2 モデルでの攻撃と異なり，古典的に安全とされている共通鍵暗号系技術に対する多項式時間の攻撃は存在しないことを確認した．従来から言われていた通り，Grover のアルゴリズムによって k ビット鍵の全数探索が時間 $O(2^{k/2})$

で実行可能になるため，長期的に保護したいデータには秘密鍵の鍵長が 128 ビットの暗号技術でなく 192 ビットや 256 ビットの暗号技術を使用するのが賢明であると考えられる．

ハッシュ関数については，Grover のアルゴリズムを用いれば n ビット出力ハッシュ関数の原像探索に要する時間が古典の $O(2^n)$ から $O(2^{n/2})$ にまで高速化される．また BHT の衝突探索アルゴリズムを用いれば衝突探索に要する時間が古典の $O(2^{n/2})$ から $\tilde{O}(2^{n/3})$ にまで高速化される．しかし BHT のアルゴリズムはサイズ $\tilde{O}(2^{n/3})$ の非常に大きい量子メモリを必要とするため，BHT のアルゴリズムが古典衝突探索アルゴリズムや他の単純な衝突探索アルゴリズムと比べて真に効率的か否かについては様々な議論があり，BHT のアルゴリズムが実際のハッシュ関数の安全性に現実的な影響を直接及ぼすか否かは明らかでない．現状で最も現実的に影響を及ぼすと思われる量子衝突探索アルゴリズムは CNS のアルゴリズムで，時間 $\tilde{O}(2^{2n/5})$ で衝突を発見する．しかし $n \geq 256$（古典的に 128 ビット安全性のあるハッシュ関数）であれば $2^{2n/5} > 2^{100}$ となるため，古典的に 128 ビット安全性のあるハッシュ関数の安全性に CNS のアルゴリズムが現実的な脅威を直接及ぼすとは考えづらい．

ハッシュ関数以外の（秘密鍵を利用するような）共通鍵暗号系技術については，近年の攻撃研究の進展により，暗号技術の内部構造に依存した攻撃が Q1 モデルにおいても多数報告されている．特に Even-Mansour 暗号および類似の構造を持つ暗号技術については，使用される置換が n ビット置換であるとき，n の多項式個程度の量子ビットを計算に使用できる量子コンピュータがあれば時間 $\tilde{O}(2^{n/3})$ で鍵回復が可能になるため，量子コンピュータに対して k ビット安全性を達成したい場合は $3k$ ビット以上の大きさの置換を使用するのが賢明である．

CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号系技術の安全性に量子コンピュータが直接与える影響は “Grover のアルゴリズムを用いると k ビット鍵の全数探索が時間 $\tilde{O}(2^{k/2})$ で実行できるため，長期的に保護したいデータには鍵長が 192 ビットや 256 ビットの暗号技術を使用した方が賢明である” という以上のものは現状では無いと考えられる．しかし Even-Mansour 暗号への Q1 モデルにおける攻撃のように安全性に現実的な影響を直接及ぼす可能性のある攻撃が今後発見される可能性もあるため，研究の動向には注意を払っておく必要がある．

参考文献

[AIK+00] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis. In Douglas R. Stinson and Stafford Tavares, editors, *SAC 2000, Proceedings*, volume 2012 of *LNCS*, pages 39–56. Springer, 2000.

[AMG+16] Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, and John M. Schanck. Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. In Roberto Avanzi and Howard Heys, editors, *SAC 2016, Proceedings*, volume 10532 of *LNCS*, pages 317–337. Springer, 2016.

[AR17] Gorjan Alagic and Alexander Russell. Quantum-secure symmetric-key cryptography based on hidden shifts. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Proceedings, Part III*, volume 10212 of *LNCS*, pages 65–93. Springer, 2017.

[ASAM18] Mishal Almazrooie, Azman Samsudin, Rosni Abdullah, and Kussay N. Mutter. Quantum reversible circuit of AES-128. *Quantum Information Processing*, 17(5), 2018. Article number: 112.

[BB17] Gustavo Banegas and Daniel J. Bernstein. Low-communication parallel quantum multi-target preimage search. In Carlisle Adams and Jan Camenisch, editors, *SAC 2017, Proceedings*, volume 10719 of *LNCS*, pages 325–335. Springer, 2017.

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4-5):493–505, 1998.

[Ber05] Daniel J. Bernstein. The Poly1305-AES message-

authentication code. In Henri Gilbert and Helena Handschuh, editors, *FSE 2005, Proceedings*, volume 3557 of *LNCS*, pages 32–49, 2005.

[Ber09] Daniel J Bernstein. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? In *SHARCS*, 2009.

[BHN+19] Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: The offline Simon's algorithm. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Proceedings, Part I*, volume 11921 of *LNCS*, pages 552–583, 2019.

[BHT97] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. *SIGACT News*, 28(2):14–19, 1997.

[BN18] Xavier Bonnetain and María Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Proceedings, Part I*, volume 11272 of *LNCS*, pages 560–592. Springer, 2018.

[BNS19a] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. On quantum slide attacks. In Kenneth G. Paterson and Douglas Stebila, editors, *SAC 2019, Proceedings*, volume 11959 of *LNCS*, pages 492–519. Springer, 2019.

[BNS19b] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of AES. *IACR Trans. Symmetric Cryptol.*, 2019(2):55–93, 2019.

[BR00] John Black and Phillip Rogaway. CBC MACs for arbitrary-length messages: The three-key constructions. In Mihir Bellare, editor, *CRYPTO 2000, Proceedings*, volume 1880 of *LNCS*, pages 197–215. Springer, 2000.

[BR02] John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In Lars R.

Knudsen, editor, *EUROCRYPT 2002, Proceedings*, volume 2332 of *LNCS*, pages 384–397. Springer, 2002.

[BS92] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round DES. In Ernest F. Brickell, editor, *CRYPTO 1992, Proceedings*, volume 740 of *LNCS*, pages 487–496. Springer, 1992.

[BW99] Alex Biryukov and David A. Wagner. Slide attacks. In Lars Knudsen, editor, *FSE 1999, Proceedings*, volume 1636 of *LNCS*, pages 245–259. Springer, 1999.

[BW00] Alex Biryukov and David A. Wagner. Advanced slide attacks. In Bart Preneel, editor, *EUROCRYPT 2000, Proceedings*, volume 1807 of *LNCS*, pages 589–606. Springer, 2000.

[CE05] Andrew M. Childs and Jason M. Eisenberg. Quantum algorithms for subset finding. *Quantum Information & Computation*, 5(7):593–604, 2005.

[CNS17] André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Proceedings, Part II*, volume 10625 of *LNCS*, pages 211–240. Springer, 2017.

[DLW19] Xiaoyang Dong, Zheng Li, and Xiaoyun Wang. Quantum cryptanalysis on some generalized Feistel schemes. *SCIENCE CHINA Information Sciences*, 62(2):22501:1–22501:12, 2019.

[DW18] Xiaoyang Dong and Xiaoyun Wang. Quantum key-recovery attack on Feistel structures. *SCIENCE CHINA Information Sciences*, 61(10):102501:1–102501:7, 2018.

[EM91] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *ASIACRYPT 1991, Proceedings*, volume 739 of *LNCS*, pages

210–224. Springer, 1991.

[GLM08] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum random access memory. *Physical review letters*, 100(16):160501, 2008.

[GLRS16] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. Applying Grover's algorithm to AES: quantum resource estimates. In Tsuyoshi Takagi, editor, *PQCrypto 2016, Proceedings*, volume 9606 of *LNCS*, pages 29–43. Springer, 2016.

[GNS18] Lorenzo Grassi, María Naya-Plasencia, and André Schrottenloher. Quantum algorithms for the k-xor problem. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Proceedings, Part I*, volume 11272 of *LNCS*, pages 527–559. Springer, 2018.

[GR04] Lov K. Grover and Terry Rudolph. How significant are the known collision and element distinctness quantum algorithms? *Quantum Information & Computation*, 4(3):201–206, 2004.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *STOC 1996, Proceedings*, pages 212–219. ACM, 1996.

[HA] Akinori Hosoyamada and Kazumaro Aoki. On quantum related-key attacks on iterated Even-Mansour ciphers. In Satoshi Obana and Koji Chida, editors, *IWSEC 2017, Proceedings*, volume 10418 of *LNCS*. Springer.

[HS18a] Akinori Hosoyamada and Yu Sasaki. Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations. In Nigel P. Smart, editor, *CT-RSA 2018, Proceedings*, volume 10808 of *LNCS*, pages 198–218. Springer, 2018.

[HS18b] Akinori Hosoyamada and Yu Sasaki. Quantum Demiric-Selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In Dario Catalano and

Roberto De Prisco, editors, *SCN 2018, Proceedings*, volume 11035 of *LNCS*, pages 386–403. Springer, 2018.

[HSTX19] Akinori Hosoyamada, Yu Sasaki, Seiichiro Tani, and Keita Xagawa. Improved quantum multicollision-finding algorithm. In Jintai Ding and Rainer Steinwandt, editors, *PQCrypto 2019, Proceedings*, volume 11505 of *LNCS*, pages 350–367, 2019.

[HSX17] Akinori Hosoyamada, Yu Sasaki, and Keita Xagawa. Quantum multicollision-finding algorithm. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Proceedings, Part II*, volume 10625 of *LNCS*, pages 179–210, 2017.

[IHM+19] Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata. Quantum chosen-ciphertext attacks against Feistel ciphers. In Mitsuru Matsui, editor, *CT-RSA 2019, Proceedings*, volume 11405 of *LNCS*, pages 391–411, 2019.

[IK03] Tetsu Iwata and Kaoru Kurosawa. OMAC: one-key CBC MAC. In Thomas Johansson, editor, *FSE 2003, Proceedings*, volume 2887 of *LNCS*, pages 129–153. Springer, 2003.

[JNRV19] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. Implementing Grover oracles for quantum key search on AES and LowMC. *IACR Cryptology ePrint Archive 2019/1146*, 2019.

[JS19] Samuel Jaques and John M. Schanck. Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Proceedings, Part I*, volume 11692 of *LNCS*, pages 32–61. Springer, 2019.

[Kap16] Marc Kaplan. Quantum attacks against iterated block ciphers. *Mathematical Aspects of Cryptography*, 7(2):71–90, 2016.

[KLLN16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosys-

tems using quantum period finding. In Matthew RobshawJonathan Katz, editor, *CRYPTO 2016, Proceedings, Part II*, volume 9815 of *LNCS*, pages 207–237. Springer, 2016.

[KLLN16b] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(1):71–94, 2016.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In *ISIT 2010, Proceedings*, pages 2682–2685. IEEE, 2010.

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *ISITA 2012, Proceedings*, pages 312–316. IEEE, 2012.

[KR96] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In Neal Koblitz, editor, *CRYPTO 1996, Proceedings*, volume 1109 of *LNCS*, pages 252–267. Springer, 1996.

[KR11] Ted Krovetz and Phillip Rogaway. The software performance of authenticated-encryption modes. In Antoine Joux, editor, *FSE 2011, Proceedings*, volume 6733 of *LNCS*, pages 306–327. Springer, 2011.

[Kup05] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.

[LM17] Gregor Leander and Alexander May. Grover meets Simon - quantumly attacking the FX-construction. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Proceedings, Part II*, volume 10625 of *LNCS*, pages 161–178. Springer, 2017.

[LPS20] Brandon Langenberg, Hai Pham, and Rainer Steinwandt. Reducing the cost of implementing AES as a quantum cir-

cuit. *IEEE Transactions on Quantum Engineering*, 1:1–12, 2020.

[LR85] Michael Luby and Charles Rackoff. How to construct pseudo-random permutations from pseudo-random functions (abstract). In Hugh C. Williams, editor, *CRYPTO 1985, Proceedings*, volume 218 of *LNCS*, page 447. Springer, 1985.

[LRW02] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. In Moti Yung, editor, *CRYPTO 2002, Proceedings*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

[LZ19] Qipeng Liu and Mark Zhandry. On finding quantum multi-collisions. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Proceedings, Part III*, volume 11478 of *LNCS*, pages 189–218. Springer, 2019.

[MMH+14] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In Antoine Joux and Amr Youssef, editors, *SAC 2014, Proceedings*, volume 8781 of *LNCS*, pages 306–323. Springer, 2014.

[MV04] David A. McGrew and John Viega. The security and performance of the Galois/counter mode (GCM) of operation. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *INDOCRYPT 2004, Proceedings*, volume 3348 of *LNCS*, pages 343–355. Springer, 2004.

[Nat77] National Bureau of Standards. Data encryption standard. *FIPS 46*, January 1977.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[NIDI19] Boyu Ni, Gembu Ito, Xiaoyang Dong, and Tetsu Iwata. Quantum attacks against type-1 generalized Feistel ciphers

and applications to CAST-256. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *INDOCRYPT 2019, Proceedings*, volume 11898 of *LNCS*, pages 433–455. Springer, 2019.

[NIS01] NIST. Advanced Encryption Standard (AES). NIST FIPS PUB 197, National Institute of Standards and Technology, November 2001.

[NIS05] NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. NIST SP 800-38B, National Institute of Standards and Technology, May 2005.

[NS19] María Naya-Plasencia and André Schrottenloher. Optimal merging in quantum k-xor and k-sum algorithms. *IACR Cryptology ePrint Archive*, 2019:501, 2019.

[Pol75] JM Pollard. A Monte Carlo method for factorization. *BIT Numerical Mathematics*, 15(3):331–334, 1975.

[RBBK01] Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryption. In Michael K. Reiter and Pierangela Samarati, editors, *CCS 2001, Proceedings*, pages 196–205. ACM, 2001.

[Rog04] Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *ASIACRYPT 2004, Proceedings*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.

[RS15] Martin Rötteler and Rainer Steinwandt. A note on quantum related-key attacks. *Inf. Process. Lett.*, 115(1):40–44, 2015.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS 1994, Proceedings*, pages 124–134. IEEE, 1994.

[Sim94] Daniel R. Simon. On the power of quantum computation. In *FOCS 1994, Proceedings*, pages 116–123. IEEE, 1994.

[STKT08] Kazuhiro Suzuki, Dongvu Tonien, Kaoru Kurosawa, and

Koji Toyota. Birthday paradox for multi-collisions. *IEICE Transactions*, 91-A(1):39–45, 2008.

[vOW94] Paul C. van Oorschot and Michael J. Wiener. Parallel collision search with application to hash functions and discrete logarithms. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, and Ravi S. Sandhu, editors, *CCS 1994, Proceedings*, pages 210–218. ACM, 1994.

[WH87] Robert S. Winternitz and Martin E. Hellman. Chosen-key attacks on a block cipher. *Cryptologia*, 11(1):16–20, 1987.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Information & Computation*, 15(7&8):557–567, 2015.