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 2024 年度版

NTT 社会情報研究所 / NTT 理論量子情報研究センタ
細山田 光倫

2025 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．更に，古典的に $2k$ ビット以上の安全性があっても Q1 モデルでの安全性が k ビットを下回る例が示されている．
- 古典的な安全性証明は，ideal permutation model などプリミティブを理想化したモデルでなく反証可能な標準的仮定（ブロック暗号の PRP 安全性など）に依拠するものであれば，Q1 モデルでそのまま通用する．つまり，古典的な安全性証明がついていれば（ブロック暗号などのプリミティブに対する攻撃の影響を考慮する必要はあるが）データ量やクエリ回数などについて安全性が保障される範囲は古典的設定と Q1 モデルで変わらない．Ideal permutation model や ideal cipher model での安全性証明は Q1 モデルでも通用するとは限らず，方式ごとに安全性を再精査する必要がある．
- 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．
- 多くのハッシュ関数について，量子計算機が使えるようになれば衝突攻撃の攻撃可能段数が伸びることが示されている．攻撃可能段数が伸びるものには，CRYPTREC の電子政府推奨暗号リストにある SHA-256 と SHA-512 および SHA3-256 が含まれるが，破れているのはそれぞれ 64 段中 38 段，80 段中 39 段，および 24 段中 6 段で，まだ余裕がある．段数削減なしで衝突耐性が破れる心配は今の所無いと考えられるが，今後も研究の進展を注視する必要がある．

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技術や最近 NIST 標準として選ばれた Ascon 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 $O(2^{k/2})$ 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．またハッシュ関数の衝突攻撃可能段数が古典より伸びることが判明していることも考慮すると，重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えキャパシティ長）は BHT のアルゴリズムの計算量 $O(2^{n/3})$ を基準にして 384 ビットや 512 ビットのものを用いた方が無難であると考えられる．
- CRYPTREC の電子政府推奨暗号リストの共通鍵暗号技術および Ascon の安全性に量子コンピュータが直接与える影響は，Grover のアルゴリズムや BHT のアルゴリズム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り，また種々のハッシュ関数で古典より攻撃可能段数が伸びているため，研究の動向には今後も注意を払っておく必要がある．

2019 年度版のまとめとの差異

具体的な方式の実用面での安全性評価について，2019 年度版執筆時から今回までの間で一番大きな差異は，ハッシュ関数の衝突攻撃可能段数が古典計算機しか使えない場合に比べて伸びることが明らかになってきたということである．これを踏まえ，2019 年度版ではハッシュ関数について「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」と結論付けていたものを「重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えキャパシティ長）は BHT のアルゴリズムの計算量 $O(2^{n/3})$ を基準にして 384 ビットや 512 ビットのものを用いた方が無難であると考えられる」と変更した．まとめの他の部分については，2019 年度とこの 2024 年度版で大きな差異は無い．

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技術の研究が盛んに行われている．NIST では標準化プロセスが進み，既に電子署名と KEM のいくつかが FIPS 203-205 として標準化されている [NIS24b, NIS24a, NIS24c].

一方共通鍵暗号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の 10 年程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技術の安全性に及ぼす影響について，主に攻撃アルゴリズムの面から既存文献の調査と評価を報告する[*1].

1.1 共通鍵暗号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，公開鍵暗号技術と共通鍵暗号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，公開鍵暗号技術はもちろん，共通鍵暗号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．また古典的に安全性証明がついている方式も，量子計算機に対してどれだけ安全かはわからない．ゆえに，量子コンピュータが共通鍵暗号技術の安全性へ及ぼす影響を把握するためには，量子アルゴリズムを用いる攻撃を研究することが重要となる．

公開鍵暗号技術・共通鍵暗号技術ともに，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] 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．

1.2 本報告書の構成

本報告書の構成は以下の通りである．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，ハッシュ関数以外の（秘密鍵を利用する）共通鍵暗号技術への 2 つの攻撃モデル（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方法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 章ではそれぞれ主に，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 章では，特定のハッシュ関数の内部構造を利用した（汎用でない）攻撃について説明する．9 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．

1.3 2019 年度版との差異

この報告書は，2019 年度暗号技術関連の調査報告「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」[細 20] の改訂版である．特に大きく加筆・修正をした部分は，3.4 節，5.2 節，5.4 節，5.5 節，6.6 節，7.2 節，7.4 節，7.6 節，8 章，および 9 章である．他にも適宜，図表の追加・修正や表現の細かい見直しを行った．

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] を採用し，量子回路は全て Clifford+T ゲートで構成されているものとする．量子オラクルへのクエリが許される場合，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は，他に断りの無い限り，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/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 を実装するために必要な量子回路の深さである[*2]．また他に断りの無い限り，量子計算に関するすべての操作は誤り無しで実行されるものとし，量子誤り訂正に関連するコスト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．表記を簡潔にするため，計算量を示す際はパラメータの多項式程度の因子を省略することがある．

$x, y \in \{0,1\}^n$ 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 $x \in \{0,1\}^m$ と $x' \in \{0,1\}^n$ 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．古典ビット列を出力する（量子）アルゴリズム $\mathcal{A}$ に対して $x \leftarrow \mathcal{A}$ と書いたとき，これは $\mathcal{A}$ を実行した結果その出力が x になることを意味する．

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．一方，関数 f の量子オラクルは

$$U_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$$

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）　保存されたデータに量子重ね合わせ状態でランダムアクセスすることができるようなメモリを量子ランダムアクセスメモリ（QRAM）と言う [GLM08].

N 個のデータ $D_1, \ldots, D_N$ を格納している古典的な RAM にアドレス i を渡すと，対応するデータ D_i を効率的に取得できる．このデータ取得を量子重ね合わせで実行できるようにするのが QRAM である．即ち，アドレスの量子状態 $\sum_i c_i |i\rangle$ を QRAM に渡すと，対応するデータの量子重ね合わせ $\sum_i c_i |i\rangle |D_i\rangle$ を返す．

データの取得のみでなくデータの書き込みをも量子重ね合わせで行えるような QRAM を考えることもできる．前段落のようにデータの取得のみ量子重ね合わせを許容するものを QRACM，データの書き込みも量子重ね合わせを許容するものを QRAQM と呼んで区別することがある．攻撃アルゴリズムによっては QRAQM を必要とするものがあるが，本稿で QRAM といえば基本的に QRACM を指すとする。

[*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，また共通鍵暗号技術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ある．

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．

古典計算機でこの問題を解くには $\Omega(2^n/t)$ 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 $O(\sqrt{2^n/t})$ 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 $O(2^{n/2})$ 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)．

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で解くには F への古典クエリが $\Omega(2^n/t)$ 回必要である．しかし，F が量子オラクルとして与えられていれば，以下のような簡単な量子アルゴリズムを実行すると $O(\sqrt{2^n/t})$ 回の F への量子クエリで問題 2.2 を解くことができる：

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 $O(1)$ 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概ね時間 $2^{n/2}$ で，また k ビット鍵ブロック暗号の鍵全数探索は概ね時間 $2^{k/2}$ 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：

$$x = y \oplus s \text{ であるとき，かつそのときに限り } f(x) = f(y). \tag{1}$$

f が (量子) オラクルとして与えられたとき，s を求めよ．

条件 (1) は特に f が周期 s を持つ周期関数であるということを示しており，この問題は周期関数の周期を探索する問題である．

この問題を古典計算機で解くには $\Omega(2^{n/2})$ 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]．アルゴリズムの概要を以下に示す：

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，$y_1, \ldots, y_n$ に直交するベクトル s' を計算して出力する．

サブルーチン SSub

1. $2n$ 量子ビットの量子状態
$$|0^n\rangle |0^n\rangle \tag{2}$$
を用意する．
2. 状態 (2) の左 n 量子ビットに Hadamard 変換 $H^{\otimes n}$ をかけ，
$$\sum_x \sqrt{1/2^n} |x\rangle |0^n\rangle \tag{3}$$
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 (3) に作用させ)，
$$\sum_x \sqrt{1/2^n} |x\rangle |f(x)\rangle \tag{4}$$
を得る．
4. 状態 (4) の左 n 量子ビットに Hadamard 変換 $H^{\otimes n}$ をかけ，
$$\sum_{x,y} (-1)^{x \cdot y}/2^n |y\rangle |f(x)\rangle \tag{5}$$
を得る．

5. 状態 (5) 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 (1) 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 $O(n)$ かつ深さ $O(1)$，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 (1) の緩和　共通鍵暗号技術への攻撃に Simon のアルゴリズムを応用しようとする際，アルゴリズムを適用しようとする関数 f について

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

が成り立っていても，その逆

$$f(x) = f(y) \text{ ならば } y = x \oplus s \tag{6}$$

が成り立つとは限らない．しかし Kaplan らは，条件 (6) 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技術（つまりハッシュ関数以外の共通鍵暗号技術）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モデル（Q2 モデル）である [KLLN16b]．

本章の構成は次のとおりである．まず 3.1 節で古典的な攻撃のモデルを振り返り，3.2 節と 3.3 節で Q1 モデルと Q2 モデルを説明する．その後 3.4 節で二つのモデルを比較する．ハッシュ関数への攻撃のモデルについては 3.5 節で補足する．

3.1　古典的攻撃モデル

（ハッシュ関数を除く）共通鍵暗号技術への攻撃の典型的なモデルは，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について考える際は，平文 M をクエリすると $E_K(M)$ 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)．

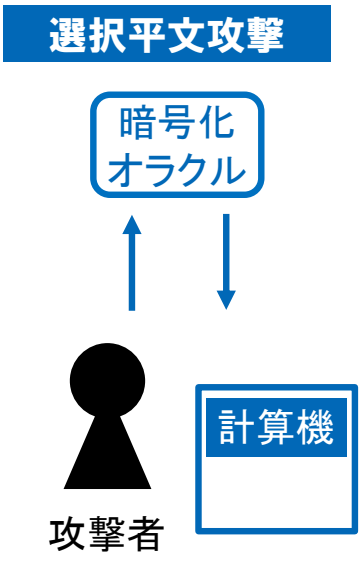

図 1　古典攻撃モデルの例（選択平文攻撃）

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).

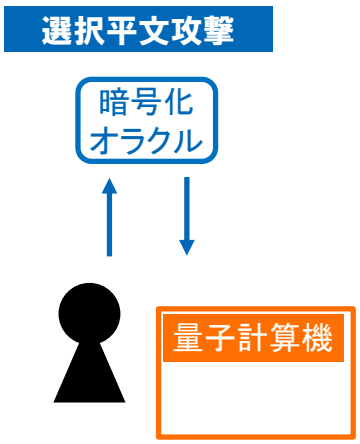

図 2　Q1 攻撃モデルの例（選択平文攻撃）

3.3　Q2 モデル（量子クエリ攻撃モデル）

このモデルでは，攻撃者の計算機が量子計算機であることに加え，鍵が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．つまり，攻撃者に量子オラクルが与えられる，という設定を考える（図 3 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 $|M\rangle$ 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 $\sqrt{1/2}\,|M_1\rangle\,|0^n\rangle + \sqrt{1/2}\,|M_2\rangle\,|0^n\rangle$ を E_K をクエリすることが許される．この状態をクエリすると，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，鍵の埋め込まれたオラクルへ量子重ね合わせクエリを攻撃者が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，その量子回路へ攻撃者が自由に入力を与えて出力を得られるという状況を想定している．

図 3　Q2 攻撃モデルの例（量子選択平文攻撃）

一般に，計算の過程で量子重ね合わせ状態を扱える場面が増えれば増えるほど攻撃者の能力が強くなる．よって攻撃者の能力は，Q1 モデルより Q2 モデルのほうが強い．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 モデルでは多項式時間攻撃が可能になる，というような暗号技術がいくつも存在する（Q2 モデルにおける攻撃についての詳細は 6 章を参照）．

また，Q1 モデルでは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実現可能性が高い．

しかし，Q2 モデルが「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．また古典計算機のプログラムは原理上量子計算機へ移植可能であるため，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 $\mathcal{C}$ とおく．すると，たとえ古典攻撃で鍵 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できる．このような量子攻撃の可能性は Q1 モデルのみでは捉えることができない．

加えて，いくつかの Q1 モデルにおける攻撃は，Q2 モデルにおける攻撃を元に考案されている（例えば 7.3 節で紹介する [BHN+19]）．より実現可能性が高い Q1 モデルでの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．

更に，鍵長が入力長より十分長いときは，量子オラクルをシミュレートすることにより Q2 モデ

ルの攻撃を Q1 モデルの攻撃へ変換できる．例えば，あるブロック暗号 E_K の入力長が n ビット，鍵長が k ビットで，$k > 2n$ であるとする（例：SKINNY [BJK+16]）．この E_K について，古典暗号化オラクルが与えられており（つまり Q1 モデル），また Q2 モデルにおいては Grover のアルゴリズムを用いた鍵全数探索より効率的な鍵回復攻撃が存在する，と仮定する．このときまず，E_K の full-codebook を得て QRAM に保存することを考える．即ち，ありうる全ての平文 x について，x を暗号化オラクルにクエリして $E_K(x)$ を得てペア $(x, E_K(x))$ を QRAM に保存しておく．するとこの QRAM を用いて $E_K(x)$ の量子オラクルを効率的にシミュレートでき，よって Q2 モデルの攻撃を実行できる．Full-codebook を QRAM に保存するにはクエリ・計算量ともに 2^n が必要であるが，$k > 2n$ であれば 2^n は Grover のアルゴリズムを用いた鍵全数探索（5.1 節を参照）の計算量 $2^{k/2}$ よりも小さい．ゆえに，鍵全数探索よりも効率的な Q1 モデルの攻撃が得られる．

以上の理由により，Q2 モデルにおける攻撃の研究は，共通鍵暗号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．

■Full-codebook を用いる攻撃についての注意　Full-codebook を用いる攻撃では全ての平文 x に対応する暗号文 $E_K(x)$ をクエリして保存する．これはかなりコストのかかる処理であり，かつ full-codebook を得てしまえば鍵を知らずとも任意の暗号文を復号できる．それでもなお，コストが（Grover のアルゴリズムを用いた）鍵全数探索を下回るような鍵回復攻撃が見つかった場合，暗号 E は理論上破られたと見做される．

なぜこのような考え方をするかという理由は幾つかあるが（そして研究者によって言うことが若干変わるのではないかと考えるが），まず挙げられる理由は「たとえ full-codebook を用いるものであったとしても，鍵全数探索より効率的な鍵回復攻撃が存在するということは，E が他の暗号に無い弱点を持つことを示す」というものである：入出力長や鍵長，そして処理効率が E と同じ別のブロック暗号 E' があったとする．鍵全数探索より効率的な鍵回復攻撃が E には見つかっていて E' には見つかっていないと仮定すると，E の内部構造は E' のそれと比べて暗号文に偏りを生み出しやすいと考えられる．E と E' の処理効率などが同じなのであれば，安全性の観点から E を使う理由は無く E' を用いるべきである．

3.5　ハッシュ関数への攻撃のモデル

SHA-2 や SHA-3 などのハッシュ関数は仕様が公開された決定的アルゴリズムであり，モードやプロトコルの構成部品として使われない限り秘密鍵を入力に取らない．ゆえにハッシュ関数への攻撃，特に衝突攻撃や原像攻撃などを考える際は，量子計算機の有無に関わらずオラクルが登場しない．攻撃者は，自分で用意した計算資源のみを用いて衝突や原像を探索する．

量子計算機が利用可能な場合，攻撃者はハッシュ関数を量子計算機上に実装して攻撃に利用できる．必要とあれば関数の量子オラクルを自分でシミュレートすることも可能である．その意味では，ハッシュ関数の攻撃は Q2 モデルに近いとも考えられる．（実際，量子ランダムオラクルモデル [BDF+11] においては，ハッシュ関数がランダム関数の量子オラクルであるとモデル化して様々な暗号技術の安全性証明が与えられる．）

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（あるいは効率性）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汎用衝突探索アルゴリズム[*3]の研究の進展を軸に説明する．汎用でない衝突攻撃，つまり具体的なハッシュ関数に対してその内部構造を活用するような衝突攻撃については，のちほど 8 章で詳述する．

量子計算機の研究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攻撃については，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．

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，各々の主張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．

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 以上で，また h は完全にランダムに振る舞うと見做して差し支えない．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[*4]．

この命題を利用するとランダム関数 h の衝突を $O(2^{n/2})$ のメモリを使用して時間 $O(2^{n/2})$ で発見する自明なアルゴリズムが得られる．更に，より洗練されたアルゴリズム (rho 法) を使用すると，時間は $O(2^{n/2})$ そのままに，メモリ使用量を $O(1)$ 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 $\Theta(2^{n/2})$ 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，h の評価 (h がオラクルとして与えられるときの，h へのクエリ回数) が $\Theta(2^{n/2})$ 回必要であることが証明される．

[*3] すなわち，ハッシュ関数の具体的な内部構造によらず適用できる衝突探索アルゴリズム．

[*4] 確率は関数 h を一様ランダムに選ぶ試行について定義される．

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，n ビットハッシュ関数の衝突探索を時間 $O(2^{n/3})$ で探索するアルゴリズムを発表した [BHT97][*5]．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，古典的な衝突探索アルゴリズムは時間 $\Omega(2^{n/2})$ を要するため，BHT のアルゴリズムを用いると $O(2^{n/6})$ の高速化が得られている．アルゴリズムの概要を以下に示す．

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（リスト L は QRAM に格納する）．
2. $x' \in \{0,1\}^n \setminus S$ と $(x, h(x)) \in L$ の組であって $h(x') = h(x)$ を満たすようなものを，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）多重衝突探索アルゴリズムを用いて見つける．
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．ゆえにアルゴリズム全体で要する時間は $O(2^{n/3})$ となる．

ここで，ステップ 2 において 2.1 節の重衝突探索アルゴリズムを用いる際，サイズ $2^{n/3}$ のリスト L へ量子重ね合わせアクセス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 $O(2^{n/3})$ の量子メモリ (QRAM) を使用し，時間 $O(2^{n/3})$ 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) もおよそ $2^{n/3}$ 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 4.1. 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 $2^{n/3}$ 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．

[*5] 正確に言うと現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容易に示せる [HSTX19].

4.3 BHT のアルゴリズム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 $O(2^{n/3})$ の量子メモリ（QRAM）を用いて時間 $O(2^{n/3})$ 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[*6]や古典アルゴリズムより効率的であることに議論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 $O(2^{n/3})$ 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 [GR04, Ber09].

まず Grover と Rudolph は，メモリ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ものではなく，よって大きさ $O(Q)$ 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 $O(Q)$ 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約 $2^{n/3}$ 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 $O(2^{n/3})$ 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[*7].

更に Bernstein は，そもそもサイズ $2^{n/3}$ の古典計算機がある（$2^{n/3}$ 個の CPU 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][*8]．$2^{n/3}$ 個の量子ビットを利用できる量子計算機はサイズおよそ $2^{n/3}$ の古典計算機として使用できるため，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

[*6] x をランダムに取って $h(x)$ を計算し，次に Grover のアルゴリズムで $h(x') \neq h(x)$ なる 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.

[*7] 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 $\tilde{O}(2^{n/3}) \times \tilde{O}(2^{n/3}) = \tilde{O}(2^{2n/3})$ となって BHT のアルゴリズムが h を評価する回数 $\tilde{O}(2^{n/3})$ を大幅に上回る.

[*8] Bernstein の指摘した手法によっても h の評価回数は $O(2^{n/2})$ 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.

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]．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 $O(2^{n/2-s})$ 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 $O(2^{(n-s)/2})$ となる．

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[*9]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もはや BHT のアルゴリズムはもちろんのこと Grover と Rudolph の並列原像探索や 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も，古典メモリ $O(2^{n/5})$ 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，ハッシュ関数の汎用衝突探索アルゴリズムに関する既存研究において，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

[*9] 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．

うに分類できる[*10]：

Case 0　小さいサイズの計算用の量子プロセッサと，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計算プロセッサが 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．また設定によっては古典計算機のサイズも宣言する．）

またそれぞれの設定において最良の汎用衝突探索アルゴリズムは異なる．Case 0 において最も速い汎用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 における現状で最良の汎用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汎用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．表 1 に，計算量のうち重要なものをまとめておく．

表 1　各ケースにおける衝突攻撃に必要な計算リソース．オーダー記号は省略している．Case 1a-1c については，のちに 8 章で紹介する特定のハッシュ関数に対する（汎用でない）衝突攻撃の議論において Case 1a が最も重要になるため，Case 1a のみ記載した．

設定	時間	計算用量子プロセッサの大きさ・数	古典メモリ	量子メモリ
Case 0	$2^{n/3}$	$\mathrm{poly}(n)$	$2^{n/3}$	$2^{n/3}$
Case 1a	$2^{n/2}/S$	S	S	S
Case 2	$2^{2n/5}$	$\mathrm{poly}(n)$	$2^{n/5}$	$\mathrm{poly}(n)$

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，また共通鍵暗号技術では実際のところ安全性パラメータ n は $n = 128$ などに固定されており，“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

[*10] 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．

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し安全性を評価しておくことが望ましい．

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図るべきである，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[*11]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．

原像探索問題はほぼ問題 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 $2^{n/2}$ で実行可能である．

以下，秘密鍵の全数探索について，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．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，$X = K$ のとき $f(X) = 1$，$X \neq K$ のとき $f(X) = 0$ となる．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．必要な量子ビットは $\tilde{O}(1)$ となる．計算量を表 2 にまとめる．

表 2　Grover のアルゴリズムを用いた鍵回復攻撃と原像探索に必要な計算量．k は秘密鍵の鍵長，n は関数の出力長である．原像探索のデータ・メモリで 1 と書いているのは，必要なデータは原像を求める値一つだけであり，またメモリはその値を蓄えるためのものだけであるという意味である．

攻撃の種類	適用先	時間	データ	（量子）メモリ
鍵回復	秘密鍵を用いる任意の暗号技術	$O(2^{k/2})$	$O(k)$ ビット	$O(k)$ ビット
原像探索	ハッシュ関数など	$O(2^{n/2})$	1	1

5.2　衝突探索および関連する問題

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 ビット出力の十分にランダムな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 $O(2^{n/3})$ 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）も $O(2^{n/3})$ であるが，大きさ $O(2^{n/3})$ の量子メモリを必要とする．

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

[*11] スポンジ関数のキャパシティ部分の衝突を見つける攻撃（5.2 節）やノストラダムス攻撃（5.5 節）はハッシュ関数の内部構造を若干利用していると見れなくもないが，便宜上汎用攻撃に含めるものとする．

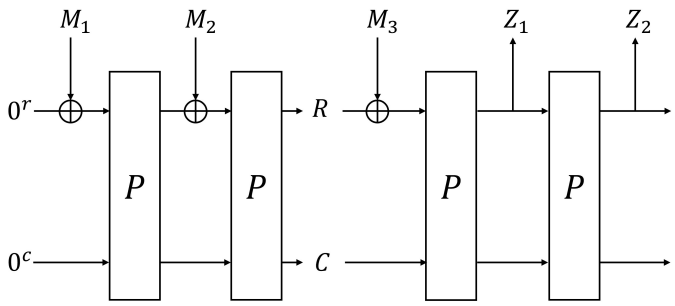

図 4　スポンジ構造．各 M_i と Z_i は r ビット．$Z_1||Z_2$ が出力であるとする．説明を簡単にするため，入力長は 3 ブロックで固定，パディングは無いものとする．

ながら並列計算を行える場合，時間 $O(2^{n/2-s})$ で衝突探索が可能であるが，関数を評価する回数は約 $O(2^{n/2})$ 回となる (4.3 節).

（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)．なお大きさ $\tilde{O}(2^{n/5})$ の古典メモリが必要である．

汎用衝突探索アルゴリズムの詳細は 4 章を参照されたい．

■スポンジ構造・XOF　SHA-3 などスポンジ構造を採用しているハッシュ関数は，内部状態のキャパシティの部分で衝突を見つけられれば出力の衝突を見つけることができる．例えば図 4 の関数において, C で示した部分の値が一致するような $M_1||M_2$ と $M_1'||M_2'$ を見つけられたとする．このとき対応するレート部分の値を R および R' とおくと，メッセージ $M = M_1||M_2||R$ と $M' = M_1'||M_2'||R'$ は関数の出力値が一致し，よってこのスポンジ関数の衝突となる．

キャパシティの部分で衝突を見つけるのに必要な古典計算量は $O(2^{c/2})$ である．よって，スポンジ構造の出力長を ℓ とすると，衝突を見つけるのに必要な古典計算量は $O(\min(2^{c/2}, 2^{\ell/2}))$ となる．これは特に出力長を自由に設定できる XOF において重要で，ℓ を非常に大きくしたとき衝突探索にかかる時間が $O(2^{\ell/2})$ ではなく $O(\min(2^{c/2}, 2^{\ell/2})) = O(2^{c/2})$ となる．

量子計算機を用いる場合も同様で，例えば BHT のアルゴリズムを用いる場合だと，スポンジ構造のハッシュ関数の衝突を探索するのに必要な計算時間と量子メモリは双方とも $O(\min(2^{c/3}, 2^{\ell/3}))$ になる．

5.2.1　大量の衝突を探索する問題

n ビット出力のランダム関数 f があってこの衝突を 2^k ペア探す，という問題を考える（定義域は十分大きく k はさほど多くないとする）．最も単純な探索の仕方は，単に衝突探索アルゴリズムを 2^k 回繰り返すというものであり，古典的には f の評価回数（クエリ回数）が $O(2^{n/2+k})$ 必要である．しかし，少し工夫を加えると f の評価回数を $O(2^{(n+k)/2})$ まで下げられる．これが量子計算機を用いると，f の評価回数を更に $O(2^{(n+2k)/3})$ まで下げられる [BCSS23].

5.2.2 多重衝突探索問題

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 $\Theta(2^{(\ell-1)n/\ell})$ 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].

5.2.3 k-XOR 問題

多重衝突探索問題に似た問題として k-XOR 問題(与えられた関数 f に対し, $f(x_1) \oplus \cdots \oplus f(x_k) = 0$ を満たす組 $(x_1, \ldots, x_k)$ を探す）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, NS20, Sch21].

5.3 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 $\sqrt{2^n/|L|}$, 時間 $\sqrt{2^n/|L|}$ 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 $O\left(\sqrt{\frac{2^n}{|L|\cdot 2^s}}\right)$ および $O\left(\sqrt{\frac{2^n}{|L|^{1/2}\cdot 2^s}}\right)$ 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 $\tilde{O}\left(2^{n/2-\ell/6}\right)$ 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 $\tilde{O}\left(2^{\ell/3}\right)$ 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 $\tilde{O}\left(2^{n/2-\ell/6-s/2}\right)$ 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 $\tilde{O}\left(2^{\ell/3}\right)$ の古典メモリを使用する．

5.4 Hellman の時間メモリトレードオフとレインボーテーブル

ランダムな関数 $H : \{0,1\}^n \to \{0,1\}^n$ の原像探索問題を解く，つまりランダムな y が与えられたときに $H(x) = y$ なる x を見つけるには，古典で時間 $\Omega(2^n)$ を要する．

しかし，これは攻撃者が事前に（y を与えられる前に）何も準備をしていなかった場合の話である．もしも攻撃者が y を与えられる前にペア $(x, H(x))$ を全ての x について計算しメモリに保存しておけば，原像探索問題は $O(1)$ で解ける．つまり，攻撃者が事前に何らかの計算をして H に依存する情報をメモリに保存しておけば，原像探索問題は時間 $O(2^n)$ よりもずっと早く解けるわけである．事前情報を蓄えるメモリサイズを S として，$S = 0$ が事前計算の無い通常の原像探索に対応し，$S = 2^n$ が全ての x に対して $(x, H(x))$ を計算し保存しておく状況に対応する．

攻撃に使えるメモリは少なくとも 0 ではないと想定するのが自然であるが，$S = 2^n$ ものメモリを使えるとも限らない．では使えるメモリのサイズ S が 0 と 2^n の間にある際，原像探索にかかる時間 T はどうなるだろうか？なお，メモリサイズ S の大小に限らず，事前計算に使える時間に制限は無いとする．

この問題を解くのに使える手法が，Hellman の時間メモリトレードオフ攻撃 [Hel80] と Oechslin のレインボーテーブル [Oec03] である．いずれも，時間とメモリのトレードオフ $T = O((2^n/S)^2)$ を与える．

Dunkelman らは，量子計算機を用いればトレードオフが上述の $T = O((2^n/S)^2)$ から $T = O((2^n/S)^{1.5})$ まで改善されることを示した [DKRS24]．以下，この高速化がどうやって得られるかについて説明を行う．高速化のアイデアの根っ子は，Hellman の攻撃とレインボーテーブルでほぼ同じである．レインボーテーブルの方が Hellman の攻撃より説明が簡潔に済むため，レインボーテーブルに焦点を当てる．

まずは古典的なレインボーテーブルを用いた手法の概要振り返ったのち，Dunkelman らのアイデアを説明する．最後に，時間とメモリだけでなくデータも含んだトレードオフについて紹介する．なお本節において量子計算リソースの設定は 4 章の Case 0，すなわち多項式サイズの小さい計算用量子プロセッサと指数的に大きなサイズの QRAM があると想定する．

5.4.1 レインボーテーブルによる時間メモリトレードオフ（古典）

まず，正の整数 t と m を適当に取る．$i = 1, \ldots, t$ に対して適当な可逆関数 $L_i : \{0,1\}^n \to \{0,1\}^n$ を取り（ビットの入れ替えなど），$f_i(x) := H(L_i(x))$ とおく．事前計算として，以下のプロセスを実行する．

■事前計算

1. $w_1, \ldots, w_m \in \{0,1\}^n$ をランダムに取る．
2. $i = 1, \ldots, m$ に対して $z_i = f_t(f_{t-1}(\cdots f_1(w_i)))$ を計算し，ペア (w_i, z_i) を保存する．

事前計算で，m 個のペアがメモリに蓄えられることになる．事前計算のあと，攻撃者は $y \in \{0,1\}^n$

を与えられる．メモリに蓄えたデータを以下のように利用し，以下の要領で $H(x) = y$ なる x を探索する．

■オンライン計算

1. $j = 1, \ldots, t$ に対して順に以下を実行：
   (a) $z' = f_t(f_{t-1}(\cdots f_j(y)))$ を計算する．
   (b) いずれかの i について $z' = z_i$ となる場合：高確率で $y = f_{j-1}(f_{j-2}(\cdots f_1(w_i)))$ が成り立ち，特に $x := L_{j-1}(f_{j-2}(\cdots f_1(w_i)))$ とおけば $H(x) = y$ を満たすはずである．そこで，この x を出力してアルゴリズムを終了する．
   (c) 全ての i について $z' \neq z_i$ の場合：何もせず次の j へ．

パラメータ m と t が $m \times t \approx 2^n$ を満たしていれば，上記の攻撃は高確率で成功する．メモリの大きさ S は m に等しく，またオンライン計算にかかる時間は $T \approx t^2$ である．ゆえに $m \times t \approx 2^n$ が満たされているとき，トレードオフ $T \approx (2^n/S)^2$ が成り立つ．例えば $t = 2^{n/3}$ かつ $m = 2^{2n/3}$ なら，$T = S = 2^{2n/3}$ となる．

5.4.2 Dunkelman らによる量子高速化 [DKRS24]

上述のアルゴリズムにおけるオンライン計算では，ステップ (a)-(c) を全ての $j = 1, \ldots, t$ について行っている．これは当然ながら，どの j が当たりか，つまり「ある i が存在して $z' = f_t(f_{t-1}(\cdots f_j(y))) = z_i$ が成り立つ」というような j が一体どれなのか，全通りチェックしないとわからないからである．

Dunkelman らのアイデアは，この j の探索に Grover のアルゴリズムを用いて，オンライン計算を高速化しようというものである（事前準備は古典のときと同じである）．より具体的には，Bool 関数 $F : \{1, \ldots, t\} \to \{0, 1\}$ を

$$F(j) := \begin{cases} 1 & (\text{ある } i \text{ が存在して } f_t(f_{t-1}(\cdots f_j(y))) = z_i \text{ が成り立つとき}) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

と定義し，この F に Grover のアルゴリズムを適用する．関数 F 自体の計算は

1. $z' = f_t(f_{t-1}(\cdots f_j(y)))$ を計算する．
2. 事前計算でメモリに蓄えられたデータを検索し，$z' = z_i$ となる i があるかチェックする

とすれば時間 $O(t)$ で可能である．Grover のアルゴリズムを F に適用すると，F の定義域サイズが t なので，Grover のアルゴリズムが F を呼び出す回数は $O(\sqrt{t})$ 回となる．よって，オンライン計算にかかる時間は $T = O(t) \times O(\sqrt{t}) = O(t^{3/2})$ となる．

攻撃成功に必要な条件が $m \times t \approx 2^n$ であったこと，$S = m$ であること，および $T \approx t^{3/2}$ より，トレードオフとしては

$$S \times T^{2/3} \approx 2^n$$

あるいはこれを整理して

$$T = O((2^n/S)^{3/2})$$

が得られる．例えば $S = 2^{3n/5}$ のとき $T = O(2^{3n/5})$ となる．

注意 5.1. 本節における説明は Dunkelman らのアイデアの要点を手短に説明することが目的であり，様々な部分で細かい説明を省略している．成功確率の評価，distinguished point に関する議論，Grover のアルゴリズムで呼び出す関数 F の量子回路としての実装（入力によらず計算時間が同じで，かつ計算が可逆である必要がある）等々，詳細は本節で紹介した原論文や関連研究を参照されたい．

5.4.3 時間・メモリ・データのトレードオフ

ここまでは，時間とメモリのトレードオフを与える古典アルゴリズムおよびその量子計算機を用いた高速化について説明した．しかし原像探索について述べたのみで，多重原像探索については触れていなかった．

多重原像探索問題では複数のターゲット $y_1, \ldots, y_D$ が与えられ，どれか一つの y_i について $H(x) = y_i$ となる i を見つけられれば良い．このようにターゲットが複数ある場合は，時間とメモリのみならずデータ量（つまりターゲットの個数 D）も含んだトレードオフ

$$T = O\left(\left(\frac{2^n}{S \cdot D}\right)^2\right)$$

が古典的に得られることが知られている（ただし $T \geq D^2$ のときのみ有効である）．例えば $D = 2^{n/4}$ かつ $S = 2^{n/2}$ のとき $T = 2^{n/2}$ となる．トレードオフは，前節で触れた Hellman の手法あるいはレインボーテーブルを用いた手法を改良することで得られる [BS00, BMS05, BBS06].

Dunkelman らの論文 [DKRS24] はこのデータを含むトレードオフについても量子計算による高速化を示している．具体的には

$$T = O\left(\left(\frac{2^n}{S \cdot D}\right)^{3/2}\right)$$

となる（$T \geq D^{1.5}$ のときのみ有効である）．例えば $D = 2^{2n/7}$ かつ $S = 2^{3n/7}$ のとき $T = 2^{3n/7}$ となる．高速化のアイデアは前節と同様で，オンライン計算の一部を上手く全探索とみなして Grover のアルゴリズムを適用するというものである．詳細は原論文 [DKRS24] を参照されたい．

5.5 ノストラダムス攻撃

Merkle-Damgård 構成のハッシュ関数に対するノストラダムス攻撃というものについて説明する．アリスとボブという二人の人がおり，アリスは予知能力を持っていて，来月当選発表がある宝くじの 1 等の番号 X が予測できるとする．アリスはこの能力があることを知人のボブに証明したいが，自分で宝くじを買って儲けるつもりはなく，またボブがアリスの能力を使って儲けるのも嫌だとする．このとき，安全な暗号学的ハッシュ関数 H を以下のように使えば，アリスは予知能力があるこ

とを証明できるのではないかと考えられる[*12].

1. アリスはランダム文字列 R を選んで $X||R$ をハッシュ関数 H にかけ，出力 $y = H(X||R)$ を計算して予言の証拠としてボブに渡す.
2. 一か月後, 宝くじの当選番号が発表される．アリスは値 R をボブに渡し，ボブは対応するハッシュ値 $z = H(X||R)$ を計算する．$y = z$ ならアリスの予言は正しかったことが確かめられる.

ここで，ハッシュ関数 H が安全であるということが重要である．もし H が安全でなければ,「アリスは実は予知能力が無く，y としてでたらめな値を選んでボブに渡し，当選番号 X の発表後に $y = H(X||R)$ を満たす R を求めてボブに渡していた」という可能性が排除できなくなってしまうからである.

裏を返せば，そのような R を見つけられるのであれば，予知能力がないのに予言者のふりができるかもしれない．これがノストラダムス攻撃である．より正確には，以下の状況を考える.

1. 攻撃者は何らかの値 y を事前に計算する.
2. X が選ばれ，攻撃者に与えられる.
3. 攻撃者は $H(X||R) = y$ を満たす R を求める.

古典的な結果として，Merkle-Damgård 構成によって作られた n ビット出力ハッシュ関数の場合，圧縮関数の評価 $O(2^{2n/3})$ 回でこの攻撃が成功することが知られている [KK06, BSU12] が，量子計算の場合はこの評価回数が $O(2^{3n/7})$ まで下げられることが示されている [BFH22].

5.6 汎用量子攻撃の具体的なコスト評価

AES や SHA-2・SHA-3 などの代表的な共通鍵暗号技術に対して 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, JNRV20, LPS20, AMG+16, LPZW23, LGQW23, ZWS+20, HS22, CLF+24, ZSWS24, Pre22, KHJ18, LKL+24, LLLC23]．例えば，深さ高々 2^{75}，幅高々 2^{13} 量子ビットの回路に，高々 2^{83} 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 [LPZW23].

[*12] これはいわゆるコミットメントをしようとしているわけであるが，この方式でコミットメント方式としての安全性証明がつくかどうかは考えない．あくまで攻撃を説明する都合上このような状況を例にとっているだけである.

6　量子クエリ攻撃 (Q2)

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] の暗号化関数は，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 5 を参照）．P がランダム置換であるという理想化された状況において，

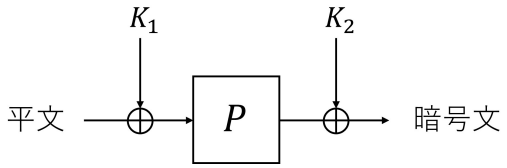

図 5　Even-Mansour 暗号

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評価することが出来る．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 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 も容易に計算できる．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．

[*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 Simon のアルゴリズムは K_1 を計算することができない．しかし P がランダムなら Simon のアルゴリズムは K_1 を返すということが示されている [KLLN16a].

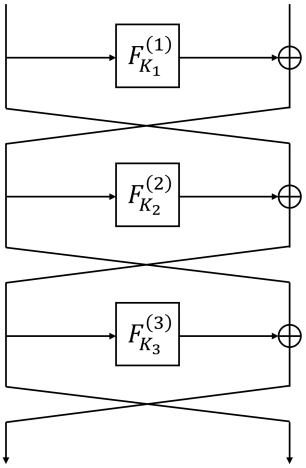

図 6　3 段 Feistel 暗号

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だが，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 3 段 Feistel 暗号（3 段 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 $i = 1, \cdots, r$ 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 $x_L||x_R \in \{0,1\}^n$（$x_L, x_R \in \{0,1\}^{n/2}$）に対し以下のようにして定められるブロック暗号である：

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

ただしここで

$$R_{K_i}^{(i)}(x_L, x_R) = \left(x_R \oplus F_{K_i}^{(i)}(x_L)\right)||x_L.$$

$r = 3$ の場合の暗号化関数 $\mathrm{Enc}_{K_1,K_2,K_3}$ を図 6 に示す．Feistel 暗号の構造は DES [Nat77] や 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 $F_{K_i}^{(i)}$ 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 $\mathrm{Enc}_{K1,K2,K3}$ 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 $\mathrm{Enc}_{K1,K2,K3}$ 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

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

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，

$$f^{\Pi}(b,x) := \mathrm{Enc}_{K1,K2,K3}(\alpha_b,x)_R \oplus \alpha_b = F^{(2)}_{K_2}\left(F^{(1)}_{K_1}(\alpha_b) \oplus x\right)$$

であるから

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

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，$\left(1, F^{(1)}_{K_1}(\alpha_0) \oplus F^{(1)}_{K_1}(\alpha_1)\right)$ を周期に持つ周期関数である．一方 $\Pi = \mathsf{PR}$ の場合，高確率で f^{Π} は周期的にならない．

よって，f^{Π} が周期をもつかを Simon のアルゴリズムを用いて調べることにより，Π が $\mathrm{Enc}_{K1,K2,K3}$ 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, CHLS20, HKK20]．また関連する後続研究として，ラウンド関数 $F^{(i)}_{K_i}$ 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].

また最近の関連する研究としては，この種の識別攻撃を切詰差分と関連させて段数を削減した LBlock[WZ11] や SIMON[BSS+13][*14]に対する識別攻撃を示している研究 [XWY+24]，5 段以上の Feistel 暗号に対する量子ウォークを用いた（指数時間）[CPT23, CCP24]，識別攻撃の発見を自動化する試み [CLS22] などがある．

6.3 CRYPTO 2016 における Kaplan らの結果

CRYPTO 2016 において Kaplan らは，Q2 モデルでは CBC-MAC（XCBC [BR00] や 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，

[*14] NSA が設計したブロック暗号である．Simon のアルゴリズムとは特に関係がない．

PMAC [BR02]，GMAC [MV04]，OCB [RBBK01, Rog04, KR11]，LRW 構成 [LRW02]，などがある．

攻撃のアイデアは Even-Mansour や Feistel への攻撃と同様，周期関数を作って Simon のアルゴリズムを適用するというものである．周期関数の作り方は攻撃対象によって異なるが，攻撃が直接操作できる値（平文，メッセージなど）に，秘密鍵に依存した値（Even-Mansour の場合は K_1，Feistel の場合は 1 段目のラウンド関数の出力）が XOR されていることを利用する．攻撃の詳細は原論文を参照されたい．

Kaplan らはまた同時に，古典的に指数時間を要するスライド攻撃 [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[*15]．

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，

$$E'(K_0, K_1, K_2, x) := E_{K_0}(x \oplus K_1) \oplus K_2 \tag{7}$$

により定義されるもののことである（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．

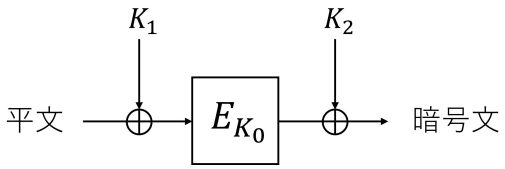

図 7　FX 構成

Q2 モデルにおいて FX 構成の鍵の回復を試みる際，まず自然な発想として思いつくのは，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，ということである．実際，秘密鍵のうち K_0 がわかっていれば，残りの鍵は Even-Mansour への攻撃と同様 Siomn のアルゴリズムを用いて多項式時間で回復できる[*16]．

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：

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

(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 $f_{K_0'}$ か否かで判定できる．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：

> 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 Simon 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] について説明する．

ブロック暗号などの共通鍵暗号技術に 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[*17]．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．$\mathbb{Z}/2^n\mathbb{Z}$ 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 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．

6.6 線形化攻撃

前節で説明した Kaplan らの攻撃は様々なモードに対する多項式時間攻撃を示したが，ISO 標準である LightMAC [LPTY16, ISO19] などへの多項式時間攻撃は見つかっていなかった．

LightMAC はブロック暗号モードであり，構造は図 8 の通りである（赤字・赤枠の部分は一旦無視していただきたい）．パラメータ s は n より小さい値で，i_s は整数 i の s ビット表現であり，また各メッセージブロック M_i は $(n-s)$ ビットのビット列である．メッセージブロック数 ℓ には $\ell \leq 2^s$ の制限がある．説明を簡単にするため，入力メッセージ M の長さが $(n-s)$ の倍数の時のみを考える．M はまず $M = M_0||M_1||\cdots||M_\ell$ とメッセージブロックに分割され，各 M_i は i_s と結合して n ビットのビット列 $i_s||M_i$ に変換される．最後の M_ℓ だけは $1\underbrace{0\cdots0}_{(s-1)\text{ 個}}$ を結合させる．その後ブロック

[*17] ここでは共通鍵暗号技術に対する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．

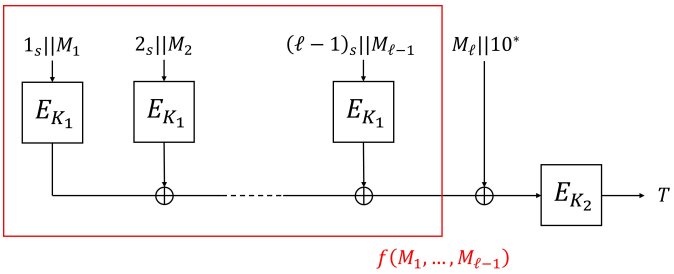

図 8　LigthtMAC.

暗号による暗号化や XOR 演算を図 8 の通りに行った出力が出力タグ T となる[*18].

図 8 を見ると，秘密鍵に依存する情報が最後のブロック M_ℓ へ XOR されているように見える．しかしこの M_ℓ を XOR するタイミングで 10^* の部分は攻撃者が値を操作できず，そのせいで Even-Mansour や Feistel 構造のときのような周期関数を構成できない．

Bonnetain らは，この問題を以下のようにして回避することができることを示した．まず図 8 の赤枠で囲った箇所（つまり $M_\ell||10^*$ を XOR する直前までの部分）を関数とみなして $f(M_1,\ldots,M_{\ell-1})$ とおく．次に任意の相異なる定数 $C_0, C_1 \in \{0,1\}^{n-s}$ を取り，$(\ell-1)$ ビットのビット列 x に対して

$$M_i(x) = \begin{cases} C_0 & x \text{ の } i \text{ ビット目が } 0 \text{ の場合} \\ C_1 & x \text{ の } i \text{ ビット目が } 1 \text{ の場合} \end{cases}$$

と置く．ここで $g : \{0,1\}^{\ell-1} \to \{0,1\}^n$ を

$$g(x) := f(M_1(x),\ldots,M_{\ell-1}(x))$$

で定めると，

$$g(x) = \left(\bigoplus_{1\le i\le \ell-1} (E_{K_1}(i_s||C_0) \oplus E_{K_1}(i_s||C_1)) \cdot x_i \right) \oplus g(0^{\ell-1})$$

が成り立ち，よって $g(x)$ はアフィン関数になることがわかる．特に，適当な行列 A と定数 c があって

$$g(x) = Ax \oplus c$$

と書ける．次に関数 $G : \{0,1\}^{\ell-1} \to \{0,1\}^t$ を

$$G(x) := \mathrm{LightMAC}(M_1(x),\ldots,M_{\ell-1}(x), C_0)$$

で定めると

$$G(x) = E_{K_2}(g(x) \oplus (C_0||10^*)) = E_{K_2}(Ax \oplus c')$$

となる（c' は何らかの定数）．ℓ を適当に大きくすれば（例えば $\ell = 2n$）線形写像 $x \mapsto Ax$ は必ず非自明なカーネルを持つ．カーネルの任意の元 $s \neq 0$ と任意の x に対して $A(x \oplus s) = Ax$ が成り立ち，ゆえに

$$G(x \oplus s) = E_{K_2}(A(x \oplus s) \oplus c') = E_{K_2}(Ax \oplus c') = G(x)$$

[*18] 本来であれば T のいくつかのビットを切り詰めたりするが，説明を簡単にするため省略する．

より，G は周期関数となる．ゆえに Simon のアルゴリズムを用いて LightMAC をランダム関数から識別できる．

Bonnetain らは線形化のアイデアを PMAC+ [IMPS17] や ZMAC [Yas11] などにも適用し，多項式時間攻撃を示している．また同じ論文で，Shor のアルゴリズム [Sho94] を応用した Poly1305 への攻撃なども示している．

6.7 関連鍵攻撃

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 $E^{-1}_{K\oplus x}(M)$ 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 $\mathcal{O}^{-1}_K$ 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，ゆえに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 による上記の攻撃は鍵 K 全体へ差分を自由に入れられるというものであるが，もう少し特殊な設定における関連鍵攻撃の研究も行われている [HA17, CHLS20].

6.8 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）で，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．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．

また最近の研究の流れとして，線形解読法や高速相関攻撃などの古典的な攻撃手法に現れる離散フーリエ変換をうまく量子フーリエ変換に対応づけようというものがある [Sch23, Hos23, Hos24].

7　古典クエリ攻撃 (Q1)

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[*19]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 $E_{K1,K2}(M) := P(M \oplus K_1) \oplus K_2$ と定義されるのであった．まず, 関数 $h : \{0,1\}^n \to \{0,1\}^n$ を $h(x) := E_{K_1,K_2}(x) \oplus E_{K_1,K_2}(\bar{x})$ で定義する．ここで $\bar{x}$ はビット列 x の各ビットを反転したもの，つまり $\bar{x} = x \oplus 1^n$ である．更に関数 $g : \{0,1\}^n \to \{0,1\}^n$ を $g(x) := P(x) \oplus P(\bar{x})$ 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 $h(x) = g(y)$ のとき高確率で $x = y \oplus K_1$ または $x = \bar{y} \oplus K_1$ 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 4.1 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．しかし P が公開置換なので，関数 g の評価は量子重ね合わせで行える．）一旦 K_1 を回復すれば，K_2 は容易に計算できる．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．

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 攻撃がオンライン計算とオフライン計算の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 章参照）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．

[*19] より正確には claw 探索アルゴリズム．

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[*20]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（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 $T = O(\sqrt{2^n/D})$ 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 $T^2 \cdot D = O(2^n)$ 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 節の他の 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（5.3 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 [HS18a] を参照されたい．

いくつかの共通鍵暗号技術は，（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

[*20] $f_s(x) = f_p(y)$ を充たす 9 ペア (x, y).

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．

■ストリーム暗号への時間・（メモリ）・トレードオフ攻撃の可能性？ [HS18a] では触れられていないが，この中間一致攻撃の設定は一部のストリーム暗号に対する古典的な時間・（メモリ）・データトレードオフ攻撃 [Bab95, Gol97, BS00, HS05] の設定に非常に近い．この攻撃はストリーム暗号の内部状態を回復するもので，内部状態のビット長を b としたときにトレードオフ $T \cdot D = O(2^b)$ が得られる．特に $D = 2^{b/2}$ とすれば攻撃時間は $T = 2^{b/2}$ となる．この攻撃が秘密鍵全探索より速くなってしまわないよう，一部のストリーム暗号は $b/2 \geq k$（k は秘密鍵の鍵長）が成り立つよう設計してある．

一方 Q1 モデル，例えば Case 0 で上記の量子アルゴリズムを適用すれば，$T = D = 2^{b/3}$ を満たすストリーム暗号への攻撃が得られる蓋然性が高い．ゆえに，上記のアルゴリズムを適用すれば鍵全数探索より速い攻撃が得られてしまうのではないかという懸念が生じる．

しかし，そもそも $b/2 \geq k$ ならば $2^{b/3} (\leq 2^{2k/3})$ は Grover のアルゴリズムによる鍵探索の計算量 $2^{k/2}$ を上回るため，上記の量子アルゴリズムが鍵全数探索より速くなることはない．（なお，ここで紹介したストリーム暗号への攻撃のトレードオフは 5.4.3 節で紹介したトレードオフに古典・量子ともに拡張されると考えられるが，同様の理由によって Grover のアルゴリズムを用いた鍵全探索より速くなることは無い．）

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報告されているが，それらの攻撃は全て鍵付き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用いて（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 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 $O(2^{n/3})$ 古典クエリ・時間 $\tilde{O}(2^{n/3})$ で実行可能である．他の攻撃との比較は表 3 を参照されたい．

表 3　Even-Mansour 暗号への Q1 モデルにおける攻撃の比較．多項式の因子およびオーダー記号は省略している．Bonnetain らの攻撃の計算量は最下段に赤字で示されている．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．

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]

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 $|\phi\rangle$ 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．

なお Q1 モデルにおける Even-Mansour 暗号への攻撃については，Bonnetain らの攻撃が最良で，それ以上効率的な攻撃は不可能であることが（quantum ideal permutation model で）証明されている [ABKM22].

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，これらの技術に本節の Q1 モデルにおける攻撃は適用できない．

7.4　古典的に $2k$ ビット安全なら k ビット耐量子安全か？

Grover のアルゴリズムを使うと，k ビット鍵の全数探索に必要な計算量が 2^k から $2^{k/2}$ まで落ちる．よく「量子計算機が出来た後も共通鍵暗号の安全性を今と同程度に保つには，鍵長を 2 倍以上にしないといけない」と言われるはこのためである．しかしその逆，つまり以下の主張は成り立つだろうか．

主張．鍵長が $2k$ 以上かつ，最も効率的な古典攻撃の計算量が 2^{2k} 以上ならば，量子計算機で

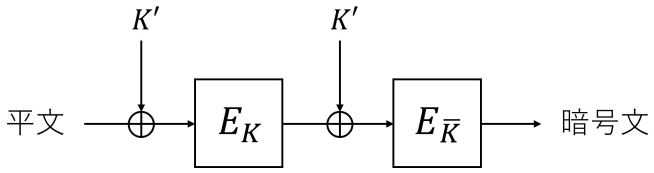

図 9　2XOR 構成．K' は K と独立した鍵で，$\bar{K}$ は K を適当な置換で変換したものである．

も破るのに時間 2^k がかかる．つまり，古典的に $2k$ ビット安全な共通鍵暗号技術は量子計算機に対して k ビット安全である．

Q2 モデルであれば，6.1 節などで挙げた多項式時間攻撃が可能になるため，上記の主張は明らかに成り立たない．更に Q1 モデル，つまりクエリが古典でもこの主張は成り立たないということが Eurocrypt 2022 において示された [BSS22].

ブロック暗号の鍵を伸ばすための構成としては，図 7 の FX 構成の他に 2XOR 構成 [GT12] というものがある（図 9）．この構成は，κ ビット鍵の n ビットブロック暗号 E から $(2n+\kappa)$ ビット鍵の n ビットブロック暗号を作るものである．E が理想的にランダムだというモデル（ideal cipher model）で，古典的に破るには時間 $O(2^{\kappa+n/2})$ が必要だということが証明されている [GT12]．例えば $\kappa = 2n$ なら，破るのに時間 $O(2^{5n/2})$ が必要である．

しかし $\kappa = 2n$ のとき，前節で紹介した Simon のアルゴリズムを用いる手法を応用すれば，Q1 モデルでも時間 $\tilde{O}(2^n)$ で破れてしまうことが示される [BSS22]．特に $k := 5n/4$ と置くと「2XOR 構成は古典的に $2k$ ビット安全だが，Q1 モデルでは k ビット安全ではない」ということになる．ゆえに先述の主張は Q1 モデルでも成り立たない．

7.5　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[*21]．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]，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．

また Q1 モデルにおいても，線形解読法や高速相関攻撃などの古典的な攻撃手法に現れる離散フーリエ変換をうまく量子フーリエ変換に対応づけようという研究が行われている [Sch23].

[*21] 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．

7.6 古典的安全性証明の結果が Q1 モデルへ持ち上がる場合

古典的安全性証明の結果は Q1 モデルにほぼそのまま持ち上がって有効になることがよくある．本節では，古典的な結果がいつ Q1 モデルに持ち上がるか，注意すべき点は何か，などについて説明する．なお古典的な議論との整合性を取るため，この節では量子計算機のリソースの想定として 4.5 節の Case 0（小さい多項式サイズの量子計算機が 1 つ使えて，QRAM は必要な分だけ大きなものを使える）を仮定する．

■CTR モードの古典的安全性証明　まず n ビットブロック暗号 E_K を用いる CTR モードを例に取って説明する．簡単のため高々定数個ブロック分の長さのメッセージしか暗号化しないと仮定する．（何か定数 c があって平文は常に $M = M_1||\cdots||M_c$ の形を取るとする．各 M_i は n ビット．）また CTR モードの定義にも流儀が色々あるが，各平文 M の暗号化が以下のように処理されるものを考える．

1. $IV \in \{0,1\}^n$ をランダムに取る．
2. $Z := E_K(IV)||E_K(IV+1)||\cdots||E_K(IV+c)$ を計算する．
3. $C := M \oplus Z$ を暗号文として出力する．

この暗号化処理の結果を $\mathrm{CTR}^{E_K}(M) = C$ と書くことにする．

任意のオラクルつきアルゴリズム（攻撃者）$\mathcal{A}$ に対し，共通鍵暗号（モード）$\mathcal{E}$ の IND$-CPA 安全性[*22]に関する識別利得 $\mathsf{Adv}^{\text{IND\$-CPA}}_{\mathcal{E}}(\mathcal{A})$ は

$$\mathsf{Adv}^{\text{IND\$-CPA}}_{\mathcal{E}}(\mathcal{A}) := \left|\Pr\left[1 \leftarrow \mathcal{A}^{\mathcal{E}_K(\cdot)}\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\$(\cdot)}\right]\right|$$

で定義される．ただし $\$(\cdot)$ は任意の入力に対してランダムな cn ビットの値を返すオラクルであり，秘密鍵 K は一様ランダムに取られるとする．また同様に，ブロック暗号 E の PRP 安全性に関する識別利得 $\mathsf{Adv}^{\text{PRP}}_{E}(\mathcal{A})$ は

$$\mathsf{Adv}^{\text{PRP}}_{E}(\mathcal{A}) := \left|\Pr\left[1 \leftarrow \mathcal{A}^{E_K}\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\mathsf{RP}}\right]\right|$$

で定義される．ここで RP は n ビット入出力のランダム置換であり，また秘密鍵 K は一様ランダムに取られるとする．このとき，CTR モードの安全性証明で示される結果は以下のようになる．

命題 7.1. $\mathcal{A}$ を CTR モードの IND$-CPA 安全性に関する任意の攻撃者として，その計算量が高々 t，クエリ回数が高々 q とする．このときブロック暗号 E の PRP 安全性に関する攻撃者 $\mathcal{B}$ であって計算量とクエリ回数がそれぞれ $O(t)$ と $O(q)$ であるようなものが存在し，

$$\mathsf{Adv}^{\text{IND\$-CPA}}_{\text{CTR}}(\mathcal{A}) \leq O(q^2/2^n) + \mathsf{Adv}^{\text{PRP}}_{E}(\mathcal{B})$$

が成り立つ．

[*22] 細かいことをいうとこの定義の流儀は本来 [Rog02] においてナンスベース暗号を念頭に導入されたものであるが，説明を簡単にするため今着目しているランダム IV のモード向けに改変して用いる．

この証明を示す上で重要になるのが以下の事実である（Game-playing proof technique [BR06] などを用いれば容易に証明できる）.

補題 7.1. RP を n ビットのランダム置換とし，CTR モードのうちブロック暗号の部分を RP に変えたものを $\mathrm{CTR}^{\mathsf{RP}}$ とおく．$\mathcal{A}$ を CTR モードの IND$-CPA 安全性に関する任意の攻撃者として，クエリ回数が高々 q とする．**なお $\mathcal{A}$ の計算時間には一切制限をつけないものとする．**このとき

$$\left|\Pr\left[1 \leftarrow \mathcal{A}^{\mathrm{CTR}^{\mathsf{RP}}(\cdot)}\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\$(\cdot)}\right]\right| \leq O(q^2/2^n)$$

が成り立つ.

この補題を用いると，命題 7.1 は以下のように証明される.

Proof. $\mathcal{B}$ を以下のようなアルゴリズムとする：$\mathcal{A}$ を走らせ，$\mathcal{A}$ がクエリしてきたときは，$\mathcal{B}$ に与えられたオラクル（E_K か RP）を用いて CTR モード（つまり CTR^{E_K} か $\mathrm{CTR}^{\mathsf{RP}}$）をシミュレートして返答する．$\mathcal{A}$ が最終的に出力したものを，$\mathcal{B}$ 自身の出力とする.

すると

$$\mathsf{Adv}_E^{\mathrm{PRP}}(\mathcal{B}) = \left|\Pr\left[1 \leftarrow \mathcal{A}^{\mathrm{CTR}^{E_K}(\cdot)}\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\mathrm{CTR}^{\mathsf{RP}}(\cdot)}\right]\right| \tag{8}$$

が成り立つ．この等式と補題 7.1 より，

$$\begin{aligned}
\mathsf{Adv}_{\mathcal{E}}^{\text{IND\$-CPA}}(\mathcal{A}) &= \left|\Pr\left[1 \leftarrow \mathcal{A}^{\mathcal{E}_K(\cdot)}\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\$(\cdot)}\right]\right| \\
&\leq \left|\Pr\left[1 \leftarrow \mathcal{A}^{\mathrm{CTR}^{E_K}(\cdot)}\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\mathrm{CTR}^{\mathsf{RP}}(\cdot)}\right]\right| \\
&\quad + \left|\Pr\left[1 \leftarrow \mathcal{A}^{\mathrm{CTR}^{\mathsf{RP}}(\cdot)}\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\$(\cdot)}\right]\right| \\
&\leq O(q^2/2^n) + \mathsf{Adv}_E^{\mathrm{PRP}}(\mathcal{B})
\end{aligned}$$

が成り立つ. □

■Q1 モデルへの持ち上げ　上述の議論をよく吟味すると，アルゴリズムが量子になっても Q1 モデルなら証明がそのまま通用することがわかる：そのまま通用するかどうか一見非自明なのは補題 7.1 の部分であるが，補題では $\mathcal{A}$ の計算時間に制限をつけていない．有名な事実として，任意の量子アルゴリズムの挙動は，時間に制限をつけず効率を度外視すれば古典アルゴリズムでシミュレートできる．ゆえに補題 7.1 は量子アルゴリズムに対しても（Q1 モデルで，クエリが古典である限り）適用できてしまう．よって命題 7.1 も Q1 モデルでそのまま成り立つことがわかる.

注意 7.2. Q2 モデルではこのようなことは成り立たない．補題 7.1 は古典クエリが前提になっており，Q2 モデルで量子重ね合わせクエリが発生すると有効ではなくなってしまうからである．ゆえに，6.2 節で紹介した 3 段 Feistel 暗号への量子選択平文攻撃のように，古典的に安全性証明があるにも関わらず Q2 モデルで破れてしまうという事態が発生する.

命題そのものは Q1 モデルでも有効になるが，実際の安全性が保証される範囲については注意が必要である．命題 7.1 に現れるブロック暗号 E_K の識別利得 $\mathsf{Adv}_E^{\mathrm{PRP}}(\mathcal{B})$ は，E_K が十分安全かつア

ルゴリズムが全て古典なら，計算時間が 2^k に達するまで非常に小さいままである．しかしアルゴリズムが量子になると，$\mathsf{Adv}_E^{\mathrm{PRP}}(\mathcal{B})$ は時間 $2^{k/2}$ で（Grover の鍵全数探索により）ほぼ 1 になりうる．ゆえに，Q1 モデルで CTR モードの安全性が保証される範囲を具体的に述べると「クエリ数などは古典的に安全性が保証される範囲に収まり（つまり $q \ll 2^{n/2}$），かつ時間 $\leq 2^{k/2}$」となる．

■議論の一般化　ここまでの議論は CTR モードについてのものであったが，重要なのは

> （★）安全性証明がランダムオラクルモデル，ideal permutation model，ideal cipher model などプリミティブが理想化されたモデル下で与えられるのでなく，反証可能な標準的仮定（CTR モードなら E_K が PRP という仮定）のみに依存している

という点である．CTR モードで無くても，（★）が満たされている限り，古典的安全性証明の結果が Q1 モデルでもそのまま成り立つ．（ただし安全性が保証される範囲を具体的に述べようとすると，先述のように Grover のアルゴリズムで鍵全数探索等の影響を考慮する必要は発生する．）

一方，安全性が ideal permutation model などプリミティブが理想化されたモデル下で与えられている場合は，Q1 モデルであっても証明は有効にならない．これは理想化されたプリミティブへの量子クエリが発生してしまい，古典的な証明が通用しなくなるためである（例えば Even-Mansour の置換 P）．7.2 節（と 7.3 節）で触れた，Chaskey の古典的な安全性の見積もりが Q1 モデルで成り立たなくなるという結果は，本質的にこれが原因である（Chaskey の古典的安全性証明は ideal permutation model で与えられている）．

8　ハッシュ関数への（汎用でない）攻撃

本章では，ハッシュ関数への攻撃であって，（汎用攻撃とは違い）特定の圧縮関数や置換などの内部構造を利用するようなものについて紹介する．3 章で触れたように，ハッシュ関数は秘密鍵を用いないため鍵の埋め込まれたオラクルというものが存在しない．攻撃者はハッシュ関数あるいはその一部を量子計算機上に自由に実装することができる．

8.1　衝突攻撃

衝突攻撃は，量子計算機があれば攻撃可能段数が伸びることが多々あることがわかっている．これは細山田・佐々木の論文 [HS20] で初めて指摘されたもので，SHA-2 を初めとした様々なハッシュ関数（あるいはハッシュ関数の部品として使う圧縮関数）において衝突攻撃の攻撃可能段数が伸びることが判明している [HS21, DSS+20, CKS21, LH24, GLST22, FLN+20]．以下，なぜ攻撃可能段数が伸びるかということの概要を説明する．

8.1.1　古典的に「意味のある」衝突攻撃

攻撃のための古典アルゴリズムを見つけたとき，それが（少なくとも学術的に）意味があるとみなされるための条件は，対応する汎用攻撃よりも効率的なことである．出力長が n ビットのハッシュ関数に対する衝突攻撃であれば，対応する汎用攻撃は計算量 $2^{n/2}$ の誕生日攻撃（4.1 節）である．例えば出力長が 256 ビットである SHA-256 に衝突攻撃を思いついたとして，その計算量が 2^{120} などであれば，その攻撃は少なくとも学術的には意味があると見做される．

ここで例に挙げた 2^{120} というのは現実的には実行不可能な計算量である．しかし多くの攻撃の研究は，まず「少なくとも学術的には意味がある」と見做せるような攻撃が見つかって，その計算量がどんどん改善されていくという順序を辿る．例えば SHA-1 に対する衝突攻撃も，CRYPTO 2006 報告でされた最初の攻撃の計算量は 2^{69} 程度であったが [WYY05]，その後削減が進み CRYPTO 2017 で実際の衝突が報告されるに至った [SBK+17]．学術的に意味があると見做せる攻撃が見つかれば，アルゴリズムの移行を考え始めたほうが安全である．

■攻撃可能段数　ハッシュ関数やブロック暗号などの共通鍵プリミティブは同じような処理を何度も繰り返すような構造になっている．たとえば AES-128 が平文から暗号文を計算する際は，特定の変換をしてから秘密鍵（から計算された値）を足すという操作を 10 段繰り返す．SHA-256 の圧縮関数なら 64 段である．

ハッシュ関数にしろブロック暗号にしろ，急に破れるということはない．攻撃を研究する研究者はまず，その段数を削減したものを攻撃することを試みる．たとえば SHA-256 であれば「元の 64 段のものは破れないから段数を 20 段にまで削減したものを考えて，この 20 段の関数に対して汎用攻撃よりも効率的な衝突攻撃を試みよう」ということになる．実際に効率的な衝突攻撃が見つかれば「20 段まで破れた」と言い，次は 21 段を破る攻撃を探す，という具合に研究は進んでいく．元の段数のうち何段まで破れているかということも安全性指標の一つとみなせる．例えば元々 30 段ある

ハッシュ関数が 29 段まで破れてしまえば，元の（30 段の）関数もそろそろ危ないのではないかという気になってくる．

なお攻撃可能段数はセキュリティパラメータ（ハッシュ関数であれば出力長 n）と独立した指標であることに注意されたい．例えば，10 ビット出力のハッシュ関数があって，元々 40 段の段数のうち 5 段までしか破られていないとする．するとこのハッシュ関数は攻撃可能段数の面からは安心できるが，出力長がそもそも短すぎるので安全ではない．逆に 256 ビット出力・80 段のハッシュ関数があって，79 段まで衝突耐性が破れてしまっているなら，セキュリティパラメータは十分長いが攻撃可能段数という面では若干不安が出てくる．

8.1.2 意味のある量子衝突攻撃とは？

量子計算を用いた攻撃の話に戻る．量子計算機を用いた衝突攻撃でまず初めに見つかったのは BHT のアルゴリズム（4.2 節）である．しかしこのアルゴリズムは Shor のアルゴリズムと違って指数的な高速化が得られるわけではない．ゆえにハッシュ関数の出力長を少し長くしておけば特に何の影響も出ないだろう，というのが支配的な見方であった．

しかし，ハッシュ関数の安全性を考える上で重要になのは BHT などの汎用攻撃だけではない．古典的な安全性を評価する上で重要なことの一つは，先述のように，汎用攻撃よりも効率的な攻撃があるか，そして何段まで破れるかということであった．この考え方を量子計算を用いた衝突攻撃にも持ち込むとどうなるかということを考える．

まずは 4.5 節の Case 0，すなわち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 QRAM が利用可能であるという設定を考える．このとき（現在見つかっている中で）最も効率的な汎用衝突攻撃は BHT のアルゴリズムで，計算量は $2^{n/3}$ である．古典的な「衝突攻撃が意味を持つかどうかは汎用衝突攻撃（計算量 $2^{n/2}$）より効率的かどうかで決まる」という考え方と整合性を持たせようとすると，「Case 0 において衝突攻撃が意味を持つかどうかは BHT より効率的かどうかで決めるべきである」と言える．

ここで着目すべきは，意味があるかどうかの閾値が古典（誕生日攻撃の $2^{n/2}$）と量子（BHT の $2^{n/3}$）でそこまで大きく変わらないということである．秘密鍵の全数探索は Grover のアルゴリズムによって古典的計算量の平方根まで落ちるが，BHT を使っても計算量の下げ幅は平方根まで落ちない．

一方，特定のブロック暗号やハッシュ関数の内部構造を利用する攻撃は，量子計算機を使うと元の平方根まで落ちることがよくある．これはなぜかというと，差分解読法を初めとする古典攻撃の重要な部分の多くが全数探索と見做せて，そこに Grover のアルゴリズムを適用できるからである．

一旦状況を整理すると以下のとおりである：量子計算機がある世界では，衝突攻撃の意味があるかどうかの閾値が古典と比べて大きく変わらない．一方，特定のハッシュ関数の内部構造を利用した攻撃は，量子アルゴリズムを用いて比較的大きな高速化が得られる．

これは即ち，量子計算機のある世界では，特定のハッシュ関数に対する攻撃の威力が相対的に高まるということである．古典的な計算量が閾値を上回っていて意味がないとされるような攻撃も，Grover のアルゴリズムなどを使って高速化すれば，量子計算機がある世界では閾値を下回って意味

表 4　SHA-2 および SHA-3 に対する衝突攻撃のうち，古典攻撃よりも攻撃可能段数が大きいもの．いずれも Case 1a における攻撃で，計算機サイズ S は古典メモリも含めたものである．

攻撃対象	出力長	攻撃段数 / 全段数	時間	計算機サイズ（汎用攻撃より速くなる範囲）	出典
任意の関数	n	-	$2^{n/2}/S$	S	[Ber09]（汎用攻撃）
SHA-256	256	38 / 64	$2^{122}/\sqrt{S}$	$S(\leq 2^{12})$	[HS21]
SHA-512	512	39 / 80	$2^{252.7}/\sqrt{S}$	$S(\leq 2^{6.6})$	[HS21]
SHA3-224	224	6 / 24	$2^{97.75}/\sqrt{S}$	$S(\leq 2^{28.5})$	[GLST22]
SHA3-256	256	6 / 24	$2^{104.25}/\sqrt{S}$	$S(\leq 2^{47.5})$	[GLST22]

があると判定されるようになる可能性がある．

今までの議論は Case 0 におけるものであったが，他の設定でも同様である．例えば Case 2 における汎用衝突攻撃は CNS のアルゴリズム（4.4 節）で，計算量は $2^{2n/5}$ である．古典的な誕生日攻撃の計算量 $2^{n/2}$ からの下げ幅は BHT よりもさらに小さく，Case 2 においても攻撃が容易になると考えられる．

Case 1a に至っては，下げ幅がほぼ無いに等しくなる．使える計算機のサイズ（量子ビットの数のみでなく，古典的計算機のプロセッサの数やメモリの大きさをも全て含んだサイズ）を S とすると，Case 1a での汎用攻撃は parallel rho 法を用いたものであり [Ber09]，計算量は $2^{n/2}/S$ である．S が小さい場合は誕生日攻撃の計算量 $2^{n/2}$ とほぼ変わらない．よって，衝突攻撃が一層容易になる．

■具体例：SHA-2 と SHA-3　SHA-256（段数は全部で 64 段）と SHA-512（80 段）への衝突攻撃については，古典で破れているのは本原稿執筆時点で両方とも 31 段までである [LLW24]．一方量子計算機がある場合，Case 1a ではそれぞれ 38 段・39 段まで破れることが示されている [HS21]．また SHA-3 について，SHA3-224 と SHA3-256 は古典で 24 段中 5 段までしか破れていないが [GLL+20, SLG17]，量子計算の Case 1a だと 6 段まで破れることが示されている [GLST22]．計算量を表 4 にまとめる．

8.2　原像攻撃

ハッシュ関数について衝突攻撃と共に重要な攻撃は原像攻撃である．原像攻撃については，汎用攻撃の計算量は古典の 2^n に対し量子で $2^{n/2}$ であり（5.1 節），平方根程度の高速化が得られてしまう．よって衝突攻撃とは違い，量子計算機が使える設定になったからといって，特定のハッシュ関数に対する原像攻撃の攻撃可能段数が容易に伸びるとは言えない．実際，量子計算機を用いて特定のハッシュ関数に原像攻撃を行う研究は [SS22] 等で行われているが，攻撃可能段数は今のところ古典を上回るものではない．

9　考察とまとめ

量子コンピュータが共通鍵暗号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．それぞれのモデルにおけるハッシュ関数以外の暗号技術への攻撃と（モデルの区別がない）ハッシュ関数への攻撃について、汎用攻撃（暗号技術の内部構造を利用せず任意の方式に適用できる攻撃）と特定の方式の内部構造を利用する攻撃に分け、それぞれ既存研究を調査した．また主にハッシュ関数への汎用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．

以下，Q1 モデルの攻撃，Q2 モデルの攻撃，ハッシュ関数への攻撃に分けてそれぞれ簡潔にまとめを述べる．また種々の重要な方式の安全性への影響をまとめる．より具体的には，CRYPTREC の電子政府推奨暗号リストの方式，および CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版 [CRY23] で触れらているものの中で特に最近 NIST 標準に選ばれた Ascon に焦点を当てる．なお電子政府推奨暗号リストは本稿執筆時点で最新の令和 6 年 5 月 16 日版（CRYPTREC LS-0001-2022R1 [デ 24]）を参照する．また Ascon のアルゴリズムについては，NIST SP 800-232 の initial public draft [TMC+24] に定められているもの（Ascon-AEAD128, Ascon-Hash256, Ascon-(C)XOF128），および NIST 投稿版 [DEMS21] に含まれ耐量子性を考慮している Ascon-80pq を取り上げるものとする．

■Q2 モデルにおける攻撃　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（鍵長が長いときは Q2 攻撃を Q1 攻撃に変換できることがあるが，便宜上これは Q1 攻撃とみなすことにする）．

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．ゆえに，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．

特に，CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号技術や Ascon の安全性を評価する上で Q2 モデルの攻撃を考慮する必要性は低い．

■Q1 モデルにおける攻撃　Q1 モデルでの攻撃については，Q2 モデルと異なり，古典的に安全とされている共通鍵暗号技術に多項式時間の攻撃は存在しないことを確認した．

しかし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．ブロック暗号の攻撃可能段数が古典より伸びるという例は今のところ見つかっていないが，古典的に $2k$ ビット以上の安全性があっても Q1 モデルでの安全性が k ビットを下回る例が示されている（7.4 節）．Q1 モデルであっても，鍵を 2 倍にしたら古典と同じ安全性が保障されるとは限らないため，暗号技術ごとに確認が必要である．また Even-Mansour 暗号および類似の構造を持つ暗号技術（Chaskey など）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（7.2 節および 7.3 節），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必要がある．

主にモードについて，ideal permutation model などプリミティブを理想化したモデルでなく反証可能な標準的仮定（ブロック暗号の PRP 安全性など）に依拠する古典的安全性証明は Q1 モデルにそのまま持ち上がる．つまり，古典的な安全性証明がついていれば，（ブロック暗号などのプリミティブに対する攻撃の影響を考慮する必要はあるが）データ量やクエリ回数などについて安全性が保障される範囲は古典的設定と Q1 モデルで変わらない．Ideal permutation model や ideal cipher model で証明された安全性は Q1 モデルに持ち上がるとは限らないので，方式ごとに安全性を再精査する必要がある．

幸い Q1 モデルにおいて，CRYPTREC の電子政府推奨暗号リストにある（ハッシュ関数以外の）共通鍵暗号技術や Ascon-AEAD128 と Ascon-80pq の安全性に量子コンピュータが与える影響は“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 $O(2^{k/2})$ 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へ現実的な影響を直接及ぼしうる攻撃が今後発見される可能性もあるため，研究の動向には今後も注意を払っておく必要がある．

電子政府推奨暗号リストにあるハッシュ関数以外の方式と Ascon-AEAD および Ascon-80pq について，Q1 モデルで安全性が現状期待できる範囲を表 5 に示す．

■ハッシュ関数への攻撃　多くのハッシュ関数について，量子計算機が使えるようになれば衝突攻撃の攻撃可能段数が伸びることが示されている（8.1 節）．攻撃可能段数が伸びるものには，CRYPTREC の電子政府推奨暗号リストにある SHA-256 と SHA-512 および SHA3-256 が含まれるが，破れているのはそれぞれ 64 段中 38 段，80 段中 39 段，および 24 段中 6 段で，まだ余裕がある．段数削減なしで衝突耐性が破れる心配は今の所無いと考えられるが，今後も研究の進展を注視する必要がある．特に，CRYPTREC の電子政府推奨暗号リストにあるハッシュ関数や Ascon（Ascon-Hash256, Ascon-(C)XOF128）の安全性に量子計算機が及ぼす影響については，汎用的な攻撃の影響のみ考慮すれば今のところは充分である．

汎用的な攻撃のうち主に考慮に入れるべきものは，（量子計算の有無に関わらず）原像探索と衝突探索である．原像探索については，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を発見するの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（5.1 節）．また衝突探索については，BHT のアルゴリズムを用いれば衝突を発見するのに要する時間が古典の $O(2^{n/2})$ から量子の $O(2^{n/3})$ まで高速化される（4.2 節）．なおスポンジ構造，特に XOF について

表 5　電子政府推奨暗号リストにあるハッシュ関数以外の共通鍵暗号技術と Ascon-AEAD および Ascon-80pq について，Q1 モデルで安全性が期待できる範囲．古典計算機のみが使える典型的な安全性評価と整合性を取るため，単一鍵の安全性に焦点を当て，量子計算機のリソースの想定としては 4.5 節の Case 0（小さい多項式サイズの量子計算機が 1 つ使えて，QRAM は必要な分だけ大きなものを使える）を仮定する．この表にある暗号技術については，Q1 モデルにおいて（古典的に考慮すべき事項から追加して）現状考慮すべきと思われる事柄は Grover のアルゴリズムによる鍵回復のみである．

技術分類	暗号技術名	鍵長（ビット）	Q1 モデルで安全性が期待できる範囲
ブロック暗号	AES, Camellia	128	時間 $\leq 2^{64}$
		192	時間 $\leq 2^{96}$
		256	時間 $\leq 2^{128}$
ストリーム暗号	KCipher-2	128	時間 $\leq 2^{64}$
秘匿モード	CBC, CFB, CTR, OFB, XTS	k	時間 $\leq 2^{k/2}$ かつ古典的に安全性が保障される範囲
認証付き秘匿モード	CCM, GCM	k	時間 $\leq 2^{k/2}$ かつ古典的に安全性が保障される範囲
メッセージ認証コード	CMAC, HMAC	k	時間 $\leq 2^{k/2}$ かつ古典的に安全性が保障される範囲
認証暗号	ChaCha20-Poly1305	256	時間 $\leq 2^{128}$ かつ古典的に安全性が保障される範囲
認証暗号	Ascon-AEAD128	128	時間 $\leq 2^{64}$ かつ古典的に安全性が保障される範囲
認証暗号	Ascon-80pq	160	時間 $\leq 2^{80}$ かつ古典的に安全性が保障される範囲

は，内部状態のキャパシティ部分で衝突を見つけられれば出力の衝突を見つけられる．よって，出力長とキャパシティがそれぞれ ℓ ビットおよび c ビットのとき，$O\left(\min(2^{\ell/3}, 2^{c/3})\right)$ の計算時間と量子メモリで衝突を見つけられる．

BHT のアルゴリズムは非常に大きな量子メモリを必要とし，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る（4 章）．しかし，SHA-256 や SHA-512，SHA3-256 を含むハッシュ関数の攻撃可能段数が古典より伸びることがここ数年で判明していることも考慮すると，重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えキャパシティ長）は BHT のアルゴリズムの計算量を基準にして 384 ビッ

表 6　電子政府推奨暗号リストのハッシュ関数と Ascon-Hash256 および Ascon-(C)XOF128 に対して BHT のアルゴリズム（4.2 節）を適用する際に必要な計算時間と量子メモリの概算値．計算時間の値はそのまま，安全性が期待できる時間の範囲の上限に対応する．なお出力長とキャパシティの単位はいずれもビットである．スポンジ構造のハッシュ関数，特に XOF（SHAKE128，SHAKE256，Ascon-(C)XOF128）については，内部状態のキャパシティ部分で衝突を見つける攻撃も考慮に入っていることに注意されたい．

暗号技術名	キャパシティ	出力長	計算時間	量子メモリ
SHA-256	-	256	$2^{85.3}$	$2^{85.3}$
SHA-512/256	-			
SHA3-256	512			
SHA-384	-	384	2^{128}	2^{128}
SHA3-384	768			
SHA-512	-	512	$2^{170.7}$	$2^{170.7}$
SHA3-512	1024			
SHAKE128	256	ℓ (≥ 256)	$\min(2^{85.3}, 2^{\ell/3})$	$\min(2^{85.3}, 2^{\ell/3})$
SHAKE256	512	ℓ (≥ 256)	$\min(2^{170.7}, 2^{\ell/3})$	$\min(2^{170.7}, 2^{\ell/3})$
Ascon-Hash256	256	256	$2^{85.3}$	$2^{85.3}$
Ascon-(C)XOF128	256	ℓ (> 0)	$\min(2^{85.3}, 2^{\ell/3})$	$\min(2^{85.3}, 2^{\ell/3})$

トや 512 ビットのものを用いた方が無難であると考えられる．

電子政府推奨暗号リストと Ascon-Hash256 および Ascon-(C)XOF128 について，BHT のアルゴリズムに必要な計算時間および量子メモリの概算値を表 6 にまとめる．

参考文献

[ABKM22] Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz. Post-quantum security of the Even-Mansour cipher. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 458–487. Springer, 2022.

[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 E. Tavares, editors, *SAC 2000, Proceedings*, volume 2012 of *Lecture Notes in Computer Science*, 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 M. Heys, editors, *Selected Areas in Cryptography - SAC 2016 - 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers*, volume 10532 of *Lecture Notes in Computer Science*, 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, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 65–93, 2017.

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

[Bab95] S.H. Babbage. Improved "exhaustive search" attacks on stream ciphers. In *European Convention on Security and Detection, 1995.*, pages 161–166, 1995.

[BB17] Gustavo Banegas and Daniel J. Bernstein. Low-communication parallel quantum multi-target preimage search. In Carlisle Adams and Jan Camenisch, editors, *Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, volume 10719 of *Lecture Notes in Computer Science*, 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.

[BBS06] Elad Barkan, Eli Biham, and Adi Shamir. Rigorous bounds on cryptanalytic time/memory tradeoffs. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 1–21. Springer, 2006.

[BCSS23] Xavier Bonnetain, André Chailloux, André Schrottenloher, and Yixin Shen. Finding many collisions via reusable quantum walks - application to lattice sieving. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 221–251. Springer, 2023.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[Ber05] Daniel J. Bernstein. The Poly1305-AES message-authentication code. In Henri Gilbert and Helena Handschuh, editors, *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*, volume 3557 of *Lecture Notes in Computer Science*, pages 32–49. Springer, 2005.

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

[BFH22] Barbara Jiabao Benedikt, Marc Fischlin, and Moritz Huppert. Nostradamus goes quantum. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III*, volume 13793 of *Lecture Notes in Computer Science*, pages 583–613. Springer, 2022.

[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 *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, 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.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BMS05] Alex Biryukov, Sourav Mukhopadhyay, and Palash Sarkar. Improved time-memory trade-offs with multiple data. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, volume 3897 of *Lecture Notes in Computer Science*, pages 110–127. Springer, 2005.

[BN18] Xavier Bonnetain and María Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, pages 560–592, 2018.

[BNS19a] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. On quantum slide attacks. In Kenneth G. Paterson and Douglas Stebila, editors, *Selected Areas in Cryptography - SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12-16, 2019, Revised Selected Papers*, volume 11959 of *Lecture Notes in Computer Science*, 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, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, 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, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 384–397. Springer, 2002.

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 409–426. Springer, 2006.

[BS92] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round DES. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 487–496. Springer, 1992.

[BS00] Alex Biryukov and Adi Shamir. Cryptanalytic time/memory/data tradeoffs for stream ciphers. In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings*, volume 1976 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2000.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. IACR Cryptology ePrint Archive 2013/404, 2013.

[BSS22] Xavier Bonnetain, André Schrottenloher, and Ferdinand Sibleyras. Beyond quadratic speedups in quantum attacks on symmetric schemes. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 315–344. Springer, 2022.

[BSU12] Simon R. Blackburn, Douglas R. Stinson, and Jalaj Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. *Des. Codes Cryptogr.*, 64(1-2):171–193, 2012.

[BW99] Alex Biryukov and David A. Wagner. Slide attacks. In Lars R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 245–259. Springer, 1999.

[BW00] Alex Biryukov and David A. Wagner. Advanced slide attacks. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May*

14-18, 2000, Proceeding, volume 1807 of *Lecture Notes in Computer Science*, pages 589–606. Springer, 2000.

[CCP24] Maya Chartouny, Benoit Cogliati, and Jacquess Patarin. Classical and quantum generic attacks on 6-round Feistel schemes. IACR Cryptology ePrint Archive 2024/458, 2024.

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

[CHLS20] Carlos Cid, Akinori Hosoyamada, Yunwen Liu, and Siang Meng Sim. Quantum cryptanalysis on contracting Feistel structures and observation on related-key settings. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 373–394. Springer, 2020.

[CKS21] Amit Kumar Chauhan, Abhishek Kumar, and Somitra Kumar Sanadhya. Quantum free-start collision attacks on double block length hashing with round-reduced AES-256. *IACR Trans. Symmetric Cryptol.*, 2021(1):316–336, 2021.

[CLF+24] Jingwen Chen, Qun Liu, Yanhong Fan, Lixuan Wu, Boyun Li, and Meiqin Wang. New SAT-based model for quantum circuit decision problem: Searching for low-cost quantum implementation. *IACR Commun. Cryptol.*, 1(1):31, 2024.

[CLS22] Federico Canale, Gregor Leander, and Lukas Stennes. Simon's algorithm and symmetric crypto: Generalizations and automatized applications. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 779–808. Springer, 2022.

[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, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 211–240. Springer, 2017.

[CPT23] Maya Chartouny, Jacques Patarin, and Ambre Toulemonde. Quantum cryptanalysis of 5 rounds Feistel schemes and Benes schemes. In Said El Hajji, Sihem Mesnager, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security - 4th International Conference, C2SI 2023, Rabat, Morocco, May 29-31, 2023, Proceedings*, volume 13874 of *Lecture Notes in Computer Science*, pages 196–203. Springer,

2023.

[CRY23] CRYPTREC 暗号技術評価委員会. Cryptrec 暗号技術ガイドライン（軽量暗号）2023年度版, 2023. 文書番号 CRYPTREC GL-2006-2023.

[DEMS21] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2 Submission to NIST, 2021.

[DKRS24] Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Quantum time/memory/data tradeoff attacks. *Des. Codes Cryptogr.*, 92(1):159–177, 2024.

[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.

[DSS+20] Xiaoyang Dong, Siwei Sun, Danping Shi, Fei Gao, Xiaoyun Wang, and Lei Hu. Quantum collision attacks on AES-like hashing with low quantum random access memories. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 727–757. Springer, 2020.

[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, *Advances in Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Fujiyoshida, Japan, November 11-14, 1991, Proceedings*, volume 739 of *Lecture Notes in Computer Science*, pages 210–224. Springer, 1991.

[FLN+20] Antonio Flórez-Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, and Ferdinand Sibleyras. New results on Gimli: Full-permutation distinguishers and improved collisions. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 33–63. Springer, 2020.

[GLL+20] Jian Guo, Guohong Liao, Guozhen Liu, Meicheng Liu, Kexin Qiao, and Ling Song. Practical collision attacks against round-reduced SHA-3. *J. Cryptol.*, 33(1):228–270, 2020.

[GLM08] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum random access memory. *Phys. Rev. Lett.*, 100:160501, Apr 2008.

[GLRS16] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. Applying Grover's algorithm to AES: quantum resource estimates. In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*, pages 29–43. Springer, 2016.

[GLST22] Jian Guo, Guozhen Liu, Ling Song, and Yi Tu. Exploring SAT for cryptanalysis: (Quantum) collision attacks against 6-round SHA-3. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III*, volume 13793 of *Lecture Notes in Computer Science*, pages 645–674. Springer, 2022.

[GNS18] Lorenzo Grassi, María Naya-Plasencia, and André Schrottenloher. Quantum algorithms for the k -xor problem. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 527–559. Springer, 2018.

[Gol97] Jovan Dj. Golic. Cryptanalysis of alleged A5 stream cipher. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 239–255. Springer, 1997.

[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, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.

[GT12] Peter Gazi and Stefano Tessaro. Efficient and optimally secure key-length extension for block ciphers via randomized cascading. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 63–80. Springer, 2012.

[HA17] Akinori Hosoyamada and Kazumaro Aoki. On quantum related-key attacks on iterated Even-Mansour ciphers. In Satoshi Obana and Koji Chida, editors, *Advances*

in Information and Computer Security - 12th International Workshop on Security, IWSEC 2017, Hiroshima, Japan, August 30 - September 1, 2017, Proceedings, volume 10418 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2017.

[Hel80] Martin Hellman. A cryptanalytic time-memory trade-off. *IEEE transactions on Information Theory*, 26(4):401–406, 1980.

[HKK20] Samir Hodzic, Lars Ramkilde Knudsen, and Andreas Brasen Kidmose. On quantum distinguishers for type-3 generalized Feistel network based on separability. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*, volume 12100 of *Lecture Notes in Computer Science*, pages 461–480. Springer, 2020.

[Hos23] Akinori Hosoyamada. Quantum speed-up for multidimensional (zero correlation) linear distinguishers. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part III*, volume 14440 of *Lecture Notes in Computer Science*, pages 311–345. Springer, 2023.

[Hos24] Akinori Hosoyamada. Quantum algorithms for fast correlation attacks on lfsr-based stream ciphers. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part VIII*, volume 15491 of *Lecture Notes in Computer Science*, pages 396–430. Springer, 2024.

[HS05] Jin Hong and Palash Sarkar. Rediscovery of time memory tradeoffs. *IACR Cryptology ePrint Archive*, page 90, 2005.

[HS18a] Akinori Hosoyamada and Yu Sasaki. Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations. In Nigel P. Smart, editor, *Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*, volume 10808 of *Lecture Notes in Computer Science*, 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, *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, volume 11035 of *Lecture Notes in Computer Science*, pages 386–403. Springer, 2018.

[HS20] Akinori Hosoyamada and Yu Sasaki. Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT*

2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II, volume 12106 of *Lecture Notes in Computer Science*, pages 249–279. Springer, 2020.

[HS21] Akinori Hosoyamada and Yu Sasaki. Quantum collision attacks on reduced SHA-256 and SHA-512. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 616–646. Springer, 2021.

[HS22] Zhenyu Huang and Siwei Sun. Synthesizing quantum circuits of AES with lower t-depth and less qubits. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III*, volume 13793 of *Lecture Notes in Computer Science*, pages 614–644. Springer, 2022.

[HSTX19] Akinori Hosoyamada, Yu Sasaki, Seiichiro Tani, and Keita Xagawa. Improved quantum multicollision-finding algorithm. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 350–367. Springer, 2019.

[HSX17] Akinori Hosoyamada, Yu Sasaki, and Keita Xagawa. Quantum multicollision-finding algorithm. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 179–210. Springer, 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, *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, volume 11405 of *Lecture Notes in Computer Science*, pages 391–411. Springer, 2019.

[IK03] Tetsu Iwata and Kaoru Kurosawa. OMAC: One-Key CBC MAC. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 129–153. Springer, 2003.

[IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO*

2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III, volume 10403 of *Lecture Notes in Computer Science*, pages 34–65. Springer, 2017.

[ISO19] ISO/IEC. ISO/IEC 29192-6:2019 Information technology — Lightweight cryptography Part 6: Message authentication codes (MACs), 2019.

[JNRV20] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. Implementing grover oracles for quantum key search on AES and LowMC. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 280–310. Springer, 2020.

[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, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 32–61. Springer, 2019.

[Kap16] Marc Kaplan. Quantum attacks against iterated block ciphers. *Mat. Vopr. Kriptogr.*, 7:71–90, 2016.

[KHJ18] Panjin Kim, Daewan Han, and Kyung Chul Jeong. Time–space complexity of quantum search algorithms in symmetric cryptanalysis: Applying to AES and SHA-2. *Quantum Information Processing*, 17(12):339, 2018.

[KK06] John Kelsey and Tadayoshi Kohno. Herding hash functions and the Nostradamus attack. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 183–200. Springer, 2006.

[KLLN16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, 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 *IEEE International Sympo-*

sium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings, pages 2682–2685. IEEE, 2010.

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316. IEEE, 2012.

[KR96] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 252–267. Springer, 1996.

[KR11] Ted Krovetz and Phillip Rogaway. The software performance of authenticated-encryption modes. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, 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.

[LGQW23] Zhenqiang Li, Fei Gao, Sujuan Qin, and Qiaoyan Wen. New record in the number of qubits for a quantum implementation of AES. *Frontiers in Physics*, 11:1171753, 2023.

[LH24] Dongjae Lee and Seokhie Hong. Improved quantum rebound attacks on double block length hashing with round-reduced AES-256 and ARIA-256. *IACR Trans. Symmetric Cryptol.*, 2024(3):238–265, 2024.

[LKL+24] Jongheon Lee, Yousung Kang, You-Seok Lee, Boheung Chung, and Dooho Choi. Toffoli-depth reduction method preserving in-place quantum circuits and its application to SHA3-256. *Quantum Information Processing*, 23(4):153, 2024.

[LLLC23] Jongheon Lee, Sokjoon Lee, You-Seok Lee, and Dooho Choi. T-depth reduction method for efficient SHA-256 quantum circuit construction. *IET Information Security*, 17(1):46–65, 2023.

[LLW24] Yingxin Li, Fukang Liu, and Gaoli Wang. New records in collision attacks on SHA-2. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I*, volume 14651 of *Lecture Notes in Computer Science*, pages 158–186. Springer, 2024.

[LM17] Gregor Leander and Alexander May. Grover meets Simon - quantumly attacking

the FX-construction. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 161–178. Springer, 2017.

[LPS20] Brandon Langenberg, Hai Pham, and Rainer Steinwandt. Reducing the cost of implementing the advanced encryption standard as a quantum circuit. *IEEE Transactions on Quantum Engineering*, 1:1–12, 2020.

[LPTY16] Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. A MAC mode for lightweight block ciphers. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 43–59. Springer, 2016.

[LPZW23] Qun Liu, Bart Preneel, Zheng Zhao, and Meiqin Wang. Improved quantum circuits for AES: Reducing the depth and the number of qubits. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part III*, volume 14440 of *Lecture Notes in Computer Science*, pages 67–98. Springer, 2023.

[LR85] Michael Luby and Charles Rackoff. How to construct pseudo-random permutations from pseudo-random functions (abstract). In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, page 447. Springer, 1985.

[LRW02] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.

[LZ19] Qipeng Liu and Mark Zhandry. On finding quantum multi-collisions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, 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 M. Youssef, editors, *Selected Areas in*

Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers, volume 8781 of *Lecture Notes in Computer Science*, 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 Kapalee Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, volume 3348 of *Lecture Notes in Computer Science*, 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*. 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, *Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings*, volume 11898 of *Lecture Notes in Computer Science*, pages 433–455. Springer, 2019.

[NIS01] NIST. Advanced Encryption Standard (AES). NIST FIPS PUB 197, 2001.

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

[NIS24a] NIST. Module-lattice-based digital signature standard. NIST FIPS PUB 204, 2024.

[NIS24b] NIST. Module-lattice-based key-encapsulation mechanism standard. NIST FIPS PUB 203, 2024.

[NIS24c] NIST. Stateless hash-based digital signature standard. NIST FIPS PUB 205, 2024.

[NS20] María Naya-Plasencia and André Schrottenloher. Optimal merging in quantum k-xor and k-xor-sum algorithms. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 311–340. Springer, 2020.

[Oec03] Philippe Oechslin. Making a faster cryptanalytic time-memory trade-off. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 617–630. Springer, 2003.

[Pol75] JM Pollard. A Monte Carlo method for factorization. *BIT Numerical Mathematics*,

15(3):331–334, 1975.

[Pre22] Richard H Preston. Applying Grover's algorithm to hash functions: a software perspective. *IEEE Transactions on Quantum Engineering*, 3:1–10, 2022.

[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 of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001*, pages 196–205. ACM, 2001.

[Rog02] Phillip Rogaway. Authenticated-encryption with associated-data. In Vijayalakshmi Atluri, editor, *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002*, pages 98–107. ACM, 2002.

[Rog04] Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, 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.

[SBK+17] Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov. The first collision for full SHA-1. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 570–596. Springer, 2017.

[Sch21] André Schrottenloher. Improved quantum algorithms for the k-xor problem. In Riham AlTawy and Andreas Hülsing, editors, *Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers*, volume 13203 of *Lecture Notes in Computer Science*, pages 311–331. Springer, 2021.

[Sch23] André Schrottenloher. Quantum linear key-recovery attacks using the QFT. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Proceedings, Part V*, volume 14085 of *Lecture Notes in Computer Science*, pages 258–291. Springer, 2023.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134. IEEE Computer Society,

1994.

[Sim94] Daniel R. Simon. On the power of quantum computation. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 116–123. IEEE Computer Society, 1994.

[SLG17] Ling Song, Guohong Liao, and Jian Guo. Non-full sbox linearization: Applications to collision attacks on round-reduced keccak. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 428–451. Springer, 2017.

[SS22] André Schrottenloher and Marc Stevens. Simplified MITM modeling for permutations: New (quantum) attacks. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 717–747. Springer, 2022.

[STKT08] Kazuhiro Suzuki, Dongvu Tonien, Kaoru Kurosawa, and Koji Toyota. Birthday paradox for multi-collisions. *IEICE Transactions*, 91-A(1):39–45, 2008.

[TMC+24] Meltem Sönmez Turan, Kerry McKay, Donghoon Chang, Jinkeon Kang, and John Kelsey. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions. NIST SP 800-232 (Initial Public Draft), 2024.

[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 '94, Proceedings of the 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 2-4, 1994*, 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.

[WYY05] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36. Springer, 2005.

[WZ11] Wenling Wu and Lei Zhang. LBlock: A lightweight block cipher. In Javier López and Gene Tsudik, editors, *Applied Cryptography and Network Security - 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings*,

volume 6715 of *Lecture Notes in Computer Science*, pages 327–344, 2011.

[XWY+24] Zejun Xiang, Xiaoyu Wang, Bo Yu, Bing Sun, Shasha Zhang, Xiangyong Zeng, Xuan Shen, and Nian Li. Links between quantum distinguishers based on Simon's algorithm and truncated differentials. *IACR Trans. Symmetric Cryptol.*, 2024(2):296–321, 2024.

[Yas11] Kan Yasuda. A new variant of PMAC: Beyond the birthday bound. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 596–609. Springer, 2011.

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

[ZSWS24] Mengyuan Zhang, Tairong Shi, Wenling Wu, and Han Sui. Optimized quantum circuit of AES with interlacing-uncompute structure. *IEEE Transactions on Computers*, 73(11):2563–2575, 2024.

[ZWS+20] Jian Zou, Zihao Wei, Siwei Sun, Ximeng Liu, and Wenling Wu. Quantum circuit implementations of AES with fewer qubits. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 697–726. Springer, 2020.

[デ 24] デジタル庁，総務省，経済産業省. 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）, 2024. 文書番号 CRYPTREC LS-0001-2022R1.

[細 20] 細山田光倫. 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, 2020. 報告書文書番号 CRYPTREC EX-2901-2019.