修士論文 要旨

Davies-Meyer 圧縮関数の原像計算に関する量子計算量下界の改善

数理情報学専攻 48-186226　安井 捷
指導教員　高木 剛 教授

1　はじめに

1.1　耐量子暗号の重要性

現在用いられている暗号技術の安全性の多くは，計算量的困難性に基づいている．例えば RSA 暗号 [7] の安全性は素因数分解問題の計算困難性仮定と関わりを持っており，ElGamal 暗号 [3] や楕円曲線暗号 [6] の安全性は離散対数問題の計算困難性仮定に基づいている．一方で量子計算の研究が発展するにしたがって，いくつかの計算量的困難性が量子計算を用いることで変化し，暗号の安全性に大きな影響を与えることが分かっている．最も有名な例としては，素因数分解問題や離散対数問題に対する多項式時間量子アルゴリズムである Shor のアルゴリズム [8] によって RSA 暗号や楕円曲線暗号などが破られることが挙げられる．これらの影響から量子計算機を用いても安全性が破られない，耐量子暗号の構成が重要視されている．

1.2　一方向ハッシュ関数

暗号学的ハッシュ関数とは，任意長のメッセージからハッシュ値と呼ばれる固定長の値を生成する関数であり，更に暗号学的な安全性要請を満たすようなものを指す．主に以下の 3 種類の安全性が考慮される．

- 原像計算困難性：与えられたハッシュ値から，元のメッセージを復元するのが困難
- 第二原像計算困難性：与えられたメッセージと，同じハッシュ値を持つような異なるメッセージを偽造するのが困難
- 強衝突耐性：同じハッシュ値を持つような異なるメッセージペアを求めるのが困難

本研究においては特に原像計算困難性を満たすハッシュ関数である，一方向ハッシュ関数を扱う．

耐量子性を持つ一方向ハッシュ関数は，耐量子暗号の構成において重要な応用を持っており，耐量子性を持つメッセージ認証符号 [1]，デジタル署名方式 [9] や擬似ランダム関数 [10] などの暗号技術が，一方向ハッシュ関数を用いて構成できることが知られている．

2　準備

2.1　Davies-Meyer 圧縮関数

n bit 整数全体の集合 $\{0,1,...,2^n-1\}$ のことを $\{0,1\}^n$ と記す．ブロックサイズ n bit，鍵サイズ m bit の Davies-Meyer 圧縮関数とは，ブロック関数 E によって決まる汎関数で

$$\mathrm{DM}^E(k,x) := E(k,x) \oplus x$$

と定義される．ここでブロック関数 E は，任意の m bit の鍵 $k \in \{0,1\}^m$ に対して $E_k := E(k,\cdot)$ が $\{0,1\}^n$ 上の全単射となるような関数であり，共通鍵暗号における暗号化関数と考えられる．

本稿で扱う Davies-Meyer 圧縮関数の原像とは，値 $y \in \{0,1\}^n$ に対して $(k,x) \in \{0,1\}^m \times \{0,1\}^n$ であって $\mathrm{DM}^E(k,x) = y$ を満たすものである．

2.2　量子クエリモデル

既存研究，本研究ともに量子クエリモデルと呼ばれる計算モデルを仮定して，Davies-Meyer 圧縮関数 DM^E の原像計算を考える．このモデルに於いて DM^E の原像計算を行う攻撃者は，ブロック関数 E に関する以下のユニタリ作用素オラクル $O_E^{\pm}$ にアクセスできる．

- $O_E^+ : \sum_{k,x} \alpha_{k,x} |k\rangle |x\rangle \mapsto \alpha_{k,x} |E(k,x)\rangle$
- $O_E^- : \sum_{k,y} \alpha_{k,y} |k\rangle |y\rangle \mapsto \alpha_{k,y} |E_k^{-1}(y)\rangle$

また攻撃にかかる計算量を，これらのオラクルの使用回数（クエリ数）で評価する．

アルゴリズム $\mathcal{A} : \{0,1\}^n \to \{0,1\}^m \times \{0,1\}^n$ に対して，$\mathcal{A}$ が DM^E の原像を正しく計算する確率を

$$\mathrm{Adv}^{inv}_{\mathrm{DM}^E}(\mathcal{A}) = \Pr_{E,y}\left[\mathcal{A}(y) = (k,x) \wedge \mathrm{DM}^E(k,x) = y\right]$$

と定義し，さらに q クエリ以下を用いるアルゴリズム全体を考えて

$$\mathrm{Adv}^{inv}_{\mathrm{DM}^E}(q) = \max_{\mathcal{A}}\{\mathrm{Adv}^{inv}_{\mathrm{DM}^E}(\mathcal{A})\}$$

と定義する．

3 既存研究

Hosoyamada and Yasuda [5] によって，量子計算機上で一方向性を持つハッシュ関数が初めて構成された．彼らの構成したハッシュ関数は，Davies-Meyer 圧縮関数を繰り返し合成することによって定義されている．彼らは，構成したハッシュ関数が一方向ハッシュであることを持つことを証明したが，その証明は

1. Davies-Meyer 圧縮関数の原像計算困難性
2. Davies-Meyer 圧縮関数を合成して得られるハッシュ関数の一方向性

の順に行われている．これらの結果のうち，1 つ目の Davies-Meyer 圧縮関数の原像計算困難性に注目する．

彼らは DM^E に対する原像計算の成功確率について以下のオーダー評価を示した．

$$\mathrm{Adv}^{inv}_{\mathrm{DM}^E}(q) \leq \frac{q}{2^{n/2}}\mathrm{O}\left(\sqrt{n}\right) + 2^{m-n}\mathrm{O}\left(n^3\right)$$

但し Davies-Meyer 圧縮関数のブロックサイズを n bit，鍵サイズを m bit とする．この評価式から，Davies-Meyer 圧縮関数の逆像計算には少なくとも $q \in \Omega\left(\frac{2^{n/2}}{n^{1/2}}\right)$ のクエリ数が必要であることが示される．一方で Grover のアルゴリズム [4] [2] という量子アルゴリズムを用いることで，逆像計算は $q \in \mathrm{O}\left(2^{n/2}\right)$ で行えることが知られているため，この結果は $\sqrt{n}$ 倍を除いて計算量上界と一致する計算量下界を与えている．これが既存研究における Davies-Meyer 圧縮関数の原像計算困難性の根拠となっている．

4 本研究での結果

既存研究による成功確率評価をクエリ数 q の係数部分と定数部分に分けて観察すると，

- 原像計算の計算量下界：$q \in \Omega\left(2^{n/2}\sqrt{1/n}\right)$
- 原像計算困難性には $2^{m-n}n^3 \ll 1$ が必要

となっている．1 つ目の計算量評価は，Grover のアルゴリズムに必要なクエリ数 $q \in \mathrm{O}\left(2^{n/2}\right)$ と近く Davies-Meyer の原像計算困難性の根拠となっているが，理論的な観点ではギャップ部分の $n^{1/2}$ がどれだけ小さくできるのかは未解決である．さらに 2 つ目の条件は鍵サイズ m の制約を意味しており，この制約を緩くできるのかどうかはハッシュ構成などの応用において興味がある部分である．

本研究では，既存研究での成功確率の不等式評価をより厳密に行うことで，これらについてオーダー評価の意味で改善を行った．本研究では原像計算の成功確率について以下のオーダー評価を示した．

$$\mathrm{Adv}^{inv}_{\mathrm{DM}^E}(q) \leq \frac{q}{2^{n/2}}\mathrm{O}\left(\sqrt{\frac{n}{\log n}}\right) + 2^{m-n}\mathrm{O}\left(\frac{n}{\log n}\right)$$

計算量下界と鍵サイズ制約については以下のように，オーダーの意味で少し改善されている．

- 原像計算の計算量下界：$q \in \Omega\left(2^{n/2}\sqrt{\log n/n}\right)$
- 原像計算困難性には $2^{m-n}(n/\log n) \ll 1$ が必要

参考文献

[1] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 592–608. Springer, 2013.

[2] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, Vol. 46, No. 4-5, pp. 493–505, 1998.

[3] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, Vol. 31, No. 4, pp. 469–472, 1985.

[4] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pp. 212–219. ACM, 1996.

[5] Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-meyer and merkle-damgård constructions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 275–304. Springer, 2018.

[6] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pp. 417–426. Springer, 1985.

[7] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, Vol. 21, No. 2, pp. 120–126, 1978.

[8] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, Vol. 41, No. 2, pp. 303–332, 1999.

[9] Fang Song. A note on quantum security for post-quantum cryptography. In *International Workshop on Post-Quantum Cryptography*, pp. 246–265. Springer, 2014.

[10] Mark Zhandry. How to construct quantum random functions. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pp. 679–687. IEEE, 2012.