Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

**SCIS 2022** 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

# Google Adiantum に対する量子攻撃
# Quantum Attacks against Google Adiantum

栗原　昂汰 *　　岩田　哲 *
Kota Kuribara　　Tetsu Iwata

**キーワード** Google Adiantum，tweakable ブロック暗号，量子攻撃，Kuperberg のアルゴリズム

## あらまし

Adiantum は安価な端末のディスクセクタ暗号化のために Google が開発した暗号規格である [2]．Adiantum はハッシュ関数，ブロック暗号，ストリーム暗号を構成要素とする tweakable ブロック暗号であり，この構造は HBSH 構造と呼ばれる．Adiantum の内部ではブロック暗号として AES-256 を 1 回のみ実行し，ハッシュ関数の一部には Poly1305 を用いる．AES の呼び出し回数を減らしているため，安価な端末でも比較的高速にデータを処理できる．

古典モデルでは，設計者によってクエリ回数 $q$ が $2^{52}$ より十分小さい場合，ランダム置換と識別できないことが証明されている [2]．一方，HBSH 構造に対して $q$ が $2^{64}$ より大きい場合，tweakable ランダム置換と識別可能であることが示されている [4]．また識別攻撃を応用すると，Adiantum 内部で使用する Poly1305 の鍵の一部を求めることができる．この鍵を利用することで偽造攻撃，平文回復攻撃が可能であることが示されている [4]．

量子計算機の開発が活発に進められており，古典アルゴリズムよりも効率的に問題を解く量子アルゴリズムが開発されている．これらの量子アルゴリズムは現在使われている多くの暗号の安全性に大きく影響を与える．このうち，Kuperberg のアルゴリズムは Hidden Shift 問題と呼ばれる問題を効率的に解く量子アルゴリズムである [3]．Bonnetain と Naya-Plasencia はこのアルゴリズムを拡張し，ハッシュ関数 Poly1305 と，算術加算を用いた FX 構造への量子攻撃を示した [1]．

本稿では，Adiantum の量子攻撃に対する安全性を解析する．まず，Kuperberg のアルゴリズムを利用して，量子モデルにおいて Adiantum の構造である HBSH 構造に対し，量子クエリ回数がおおよそ $2^{20}$ 回でランダム置換と識別可能であることを示す．また Adiantum に対し，量子クエリ回数をおおよそ $2^{38}$ 回に増やすことで，偽造攻撃および平文回復攻撃が可能であることを示す．

表 1 に従来結果と本稿の結果をまとめる．

表 1: Adiantum の攻撃に必要な（量子）クエリ回数

| 計算モデル | 識別 | 偽造 | 平文回復 |
|---|---|---|---|
| 古典 [4] | $2^{64}$ | $2^{64}$ | $2^{64}$ |
| 量子 [本稿] | $2^{20}$ | $2^{38}$ | $2^{38}$ |

* 名古屋大学工学部 〒 464-8603 名古屋市千種区不老町．Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan. kuribara.kota@k.mbox.nagoya-u.ac.jp, tetsu.iwata@nagoya-u.jp

### 謝辞

本研究は JSPS 科研費 JP20K11675 の助成を受けたものです．

## 参考文献

[1] X. Bonnetain and M. Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. In *ASIACRYPT 2018, Proceedings, Part I.*

[2] P. Crowley and E. Biggers. Adiantum: length-preserving encryption for entry-level processors. *IACR Trans. Symmetric Cryptol.*, 2018(4):39–61, 2018.

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

[4] 土生 亮，岩田 哲．Google Adiantum に対する識別，偽造，平文回復攻撃．信学技報，ISEC 2020-2, pp. 7–14, 2020.