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

NIST PQC Round3 候補の鍵カプセル化方式への故障注入攻撃
Fault-Injection Attacks against NIST's Post-Quantum Cryptography Round 3 KEM Candidates

草川恵太 * 伊東燦 †‡ 上野嶺 †‡ § 高橋順子 * 本間尚文 †‡
Keita Xagawa Akira Ito Rei Ueno Junko Takahashi Naofumi Homma

キーワード 耐量子計算機暗号，鍵カプセル化方式，公開鍵暗号，故障注入攻撃.

あらまし

NIST 耐量子計算機暗号標準化プロジェクトの第 3 ラウンドに選定された鍵カプセル化方式 (KEM) [1] に対して, 故障注入攻撃の観点から鍵回復攻撃について調査する. 全ての KEM が藤崎・岡本変換 [2] またはその亜種を用いている. 藤崎・岡本変換では, 復号アルゴリズムの内部で入力された暗号文と復号した平文を再暗号化した暗号文とを比較し, 等価であれば復号した平文から鍵を導出する. そのため, この等価判定は安全性の観点から非常に重要なものである.

本論文は, この等価判定を読み飛ばせる場合に鍵回復攻撃が可能かどうか調査した. Kyber, NTRU, Saber, FrodoKEM, HQC, NTRU Prime の Streamlined NTRU Prime, SIKE については既存の鍵回復攻撃が適用できることが分かった. NTRU Prime の NTRU LPRime については新しく鍵回復攻撃を提案する.

BIKE については鍵の情報を得る攻撃が存在することを報告する.

オープンソースソフトウェアである pqm4 ライブラリには, Classic McEliece と HQC 以外の鍵カプセル化方式が含まれている. Kyber, NTRU, Saber, BIKE, SIKE の pqm4 の実装に対しては, 各々ある 1 命令を読み飛ばすことで等価判定を無効化できることを示す. NTRU Prime の実装についてはもともと等価判定が無効化されていたことを報告する. また, FrodoKEM の実装については [3] が報告した時間差を利用したサイドチャネル攻撃ができる脆弱性が修正されていないことを報告する.

表1 調査結果の概要

Name	平文判定攻撃	攻撃対象領域	故障注入攻撃の影響
Classic McEliece	Unknown	N/A	N/A
Kyber	鍵回復	Skip	鍵回復
NTRU	鍵回復	Skip	鍵回復
Saber	鍵回復	Skip	鍵回復
BIKE	鍵漏洩 (New)	Skip	鍵漏洩
FrodoKEM	鍵回復	Timing bug	鍵回復
HQC	鍵回復	N/A	N/A
Streamlined NTRU Prime	鍵回復	CCA bug	鍵回復
NTRU LPRime	鍵回復 (New)	CCA bug	鍵回復
SIKE	鍵回復	Skip	鍵回復

参考文献

[1] Alagic, G. et al.: Status report on the second round of the NIST post-quantum cryptography standardization process. (2020) https://csrc.nist.gov/publications/detail/nistir/8309/final

[2] Fujisaki, E., Okamoto, T.: Secure Integration of Asymmetric and Symmetric Encryption Schemes. In: CRYPTO '99, pp. 537–554 (1999)

[3] Guo, Q., Johansson, T., Nilsson, A.: A key-recovery timing attack on post-quantum primitives using the Fujisaki–Okamoto transformation and its application to FrodoKEM. In: CRYPTO 2020, Part II, pp. 359–386 (2020)

* 日本電信電話株式会社 NTT 社会情報研究所, 〒 180–8585 東京都武蔵野市緑町 3–9–11. NTT Social Informatics Laboratories, Nippon Telegraph and Telephone Corporation, 3–9–11 Midori-cho, Musashino-shi, Tokyo, 180-8535, Japan. E-mail: keita.xagawa.zv@hco.ntt.co.jp
† 東北大学電気通信研究所〒 980–8577 宮城県仙台市青葉区片平 2–1–1. Research Institute of Electrical Communication, Tohoku University, 2–1–1 Katahira, Aoba-ku, Sendai-shi, Miyagi, 980–8577, Japan.
‡ JST CREST, 〒 332–0012 埼玉県川口市本町 4–1–8. CREST, JST, 4–1–8 Honcho, Kawaguchi, Saitama, 332-0012, Japan
§ JST さきがけ（住所は † に同じ）