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

耐量子鍵カプセル化メカニズムに対する一般化サイドチャネル攻撃
A Generic Side-Channel Attack on Post-Quantum KEMs

上野 嶺 *†‡ Rei Ueno
草川 恵太 § Keita Xagawa
田中 裕太郎 *† Yutaro Tanaka
伊東 燦 *† Akira Ito
高橋 順子 § Junko Takahashi
本間 尚文 *† Naofumi Homma

キーワード 耐量子計算機暗号，鍵カプセル化メカニズム，公開鍵暗号，サイドチャネル攻撃，深層学習

あらまし

本論文では，耐量子鍵カプセル化メカニズム (KEM) に対して一般的に適用可能なサイドチャネル攻撃について述べる．多くの耐量子 KEM では，IND–CCA 安全性を達成するために鍵デカプセル化で再暗号化が実行される．提案攻撃では，再暗号化部の PRF/PRG のサイドチャネル情報を利用することで復号オラクルの一種である平文判定オラクルを実現し，KEM で利用されている CPA 安全な公開鍵暗号化スキームに対して選択暗号文攻撃を適用して秘密鍵を取得する．提案攻撃は，再暗号化やその亜種を用いている KEM に対して一般的に適用可能である．例として，表 1 に示すとおり，提案攻撃は NIST PQC 公募コンペティションの第三ラウンドの KEM 候補（最終候補五つと代替候補四つ）のうち八つの KEM の鍵回復が可能であり，再暗号化に着目した既存攻撃と比べて高い一般性を有する（Classic McEliece への適用可能性は同 KEM への鍵回復平文判定攻撃が知られていないため不明）．

さらに本論文では，平文判定オラクルをサイドチャネル波形から実現するために深層学習に基づく二値分類器を提案し，様々な再暗号化の実装（マスキング対策有り/無しのソフトウェアおよびハードウェア）に対して鍵回復に必要となる波形数を実験的に評価する．その結果，提案識別器は未対策ソフトウェアおよびハードウェアとマスキング対策ソフトウェアに対して数波形で高信頼な平文判定オラクルを実現して，様々な KEM に対して現実的に鍵回復攻撃が可能であることを確認するとともに，Threshold implementation に基づくマスキング対策ハードウェアが対策として有効であることも確認する．

表 1: 既存攻撃と提案攻撃の適用可能性と対策手法

		[1]	[2]	[3]	**This work**
	Attack type	Timing	Fault	Power/EM	
Lattice	Kyber	Yes	Yes	Yes	**Yes**
	Saber	Yes	Yes	Yes	**Yes**
	FrodoKEM	Yes	No	Yes	**Yes**
	NTRU	No	No	No	**Yes**
	NTRU Prime	Partially yes†	No	No	**Yes**
Code	HQC	Yes	No	No	**Yes**
	BIKE	Yes*	No	No	**Yes***
	Classic McEliece	Unknown	No	No	**Unknown**
Isogeny	SIKE	No	No	No	**Yes**
Countermeasure/mitigation		Constant-time	Redundancy	Masking	

† NTRU LPRime には適用できるが Streamlined NTRU Prime には適用不可.
* 部分鍵復元が可能（全鍵復元は困難）.

参考文献

[1] Guo, Q. et al.: A key-recovery timing attack on post-quantum primitives using the Fujisaki–Okamoto transformation and its application to FrodoKEM. In: CRYPTO '20, pp. 359–386 (2020)

[2] Pessl, P., Prokop, L.: Fault attacks on CCA-secure lattice KEMs. IACR Trans. Cryptogr. Hardw. Embedded Syst., **2021**(2), 37–60 (2021)

[3] Ravi, P. et al.: Generic side-channel attacks on CCA-secure lattice-based KEMs. IACR Trans. Cryptogr. Hardw. Embedded Syst., **2020**(3), 307–335 (2020)

* 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. E-mail: rei.ueno.a8@tohoku.ac.jp
† 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）
§ 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