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の匿名性
Anonymity of NIST PQC Round-3 KEMs

草川恵太 *
Keita Xagawa

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，匿名性, 頑健性

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, Grubbs, Maram, Paterson [2] は匿名性および頑健性を調査した. 彼らは Kyber と Saber の変種および FrodoKEM の匿名性・頑健性を量子ランダムオラクルモデル (QROM) で示した. しかし他の方式の匿名性・頑健性については技術的な問題により未解決問題として残されていた.

本稿では, Grubbs らが未解決問題とした他の方式の匿名性を調査した. 結果をまとめると以下になる.

- NTRU: 基となる決定性公開鍵暗号方式 (DPKE) が強分離的模倣可能 (strongly disjoint-simulatable) であれば, NTRU は QROM で匿名である. また NTRU は QROM で衝突耐性を持つ. NTRU を KEM として適当な DEM と組み合わせたハイブリッド暗号は匿名かつ頑健である. 同様のことが BIKE, HQC (HQC-128 と HQC-196), NTRU LPRime, SIKE についても成立する.
- Classic McEliece: 基となる DPKE が強分離的模倣可能であれば, Classic McEliece は QROM で匿名である. Classic McEliece を KEM として適当な DEM と組み合わせたハイブリッド暗号は匿名である.

これらの結果をまとめると表 1 のようになる.

以上より, Grubbs ら [2] が未解決問題として残した 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 KEM の匿名性および頑健性についておおむね解決できた.

表1　調査結果の概要: IND= 識別不可能性, SPR= 強疑似ランダム性, ANO= 匿名性, CF= 衝突耐性, ROB= 頑健性である（それぞれ量子ランダムオラクルモデルで選択可能暗号文攻撃を許した場合の安全性を意味する）. また, Y = Yes, N = No, ? = Unknown を表す. 下線部が今回の調査で明らかになった点を表す.

		KEM					PKE	
Name	Trans.	IND	SPR	ANO	CF	ROB	ANO	ROB
Classic McEliece	$\mathrm{HU}^{\not\perp,\mathrm{prf}}$	Y	Y	Y	N	N	Y	N
Kyber	$\mathrm{FO}^{\not\perp\prime}$	?	?	?	?	N	?	?
NTRU	SXY	Y	Y	Y	Y	N	Y	Y
Saber	$\mathrm{FO}^{\not\perp\prime}$	?	?	?	?	N	?	?
BIKE	$\mathrm{FO}^{\not\perp}$	Y	Y	Y	Y	N	Y	Y
FrodoKEM	$\mathrm{FO}^{\not\perp\prime\prime}$	Y	Y	Y	Y	N	Y	Y
HQC-128/192	$\mathrm{HFO}^{\perp}$	Y	Y	Y	Y	Y	Y	Y
HQC-256	$\mathrm{HFO}^{\perp}$	Y	N	N	Y	Y	N	Y
Streamlined NTRU Prime	$\mathrm{HU}^{\not\perp,\mathrm{prf}}$	?	?	?	?	N	?	?
NTRU LPRime	$\mathrm{HFO}^{\not\perp,\mathrm{prf}}$	Y	Y	Y	Y	N	Y	Y
SIKE	$\mathrm{FO}^{\not\perp}$	Y	Y	Y	Y	N	Y	Y

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] Grubbs, P., Maram, V., and Paterson, K.G.: Anonymous, robust post-quantum public key encryption. Cryptology ePrint Archive: Report 2021/708. (2021) https://eprint.iacr.org/2021/708

* 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