NTS-KEM — Round 2 Submission

M.R. Albrecht[1], C. Cid[1], K.G. Paterson[2], CJ Tjhai[3], M. Tomlinson[3]

[1]Information Security Group & Institute for Cyber Security Innovation,
Royal Holloway University of London,
Egham, Surrey, UK

[2]Department of Computer Science,
ETH Zurich
Zurich, Switzerland

[3]PQ Solutions Ltd,
50 Liverpool Street,
London, UK

Second NIST PQC Standardization Conference — August 2019

Introduction

- Code-based cryptography
  - Goppa codes
  - McEliece public-key encryption (PKE)
    - One-way (OW) secure
    - Difficult for an attacker to recover the underlying message **m** for some ciphertext **c**
- NTS-KEM is a key-encapsulation mechanism (KEM)
  - McEliece scheme combined with a transform akin to Fujisaki-Okamoto/Dent transform
  - Resistant to chosen ciphertext attacks (IND-CCA secure)
  - **New for round 2 – implicit rejection during decryption**

Algorithm Summary (unchanged from round 1)

- The key-generation, encapsulation and decapsulation algorithms are largely the same as those of McEliece's scheme
- The main difference: shortening of ciphertext
  - Property: the sum of two codewords is another codeword
  - $\mathbf{e} = (\mathbf{e}_a \mid \mathbf{e}_b \mid \mathbf{e}_c)$, where $\mathbf{e}_a \in \mathbb{F}_2^{k-\ell}$, $\mathbf{e}_b \in \mathbb{F}_2^{\ell}$ and $\mathbf{e}_c \in \mathbb{F}_2^{n-k}$
  - On encapsulation, set $\mathbf{m} = (\mathbf{e}_a \mid \mathbf{k}_e) \in \mathbb{F}_2^k$ where $\mathbf{k}_e = H_\ell(\mathbf{e}) \in \mathbb{F}_2^\ell$:

$$\begin{aligned}
\mathbf{c} &= (\mathbf{m} \mid \mathbf{m} \cdot \mathbf{Q}) + \mathbf{e} \\
&= (\mathbf{e}_a \mid \mathbf{k}_e \mid (\mathbf{e}_a \mid \mathbf{k}_e) \cdot \mathbf{Q}) + (\mathbf{e}_a \mid \mathbf{e}_b \mid \mathbf{e}_c) \\
&= (\mathbf{0}_a \mid \mathbf{k}_e + \mathbf{e}_b \mid (\mathbf{e}_a \mid \mathbf{k}_e) \cdot \mathbf{Q} + \mathbf{e}_c) \\
&= (\mathbf{0}_a \mid \mathbf{c}_b \mid \mathbf{c}_c)\,.
\end{aligned}$$

  - Discard the "*a*" section in the private-key and for syndrome computation in decapsulation

Implicit Rejection (new for round 2)

- The "Classic McEliece Comparison Task Force" suggested[1] using implicit rejection in case of decryption failure
- We modified our round 1 proposal to perform implicit rejection
- This is done in a way that is easy to implement in a constant-time manner
- Adds a 32-byte string to the private key, marginally increasing private key size; slightly changes running times
- Small tweaks to our existing IND-CCA proof were needed to accommodate the change
- Should ease production of QROM proofs

[1] https://classic.mceliece.org/nist/vsntskem-20180629.pdf

Parameter Sets (updated from round 1)

Scheme	NIST category	Security target†	n	k	d	pk (bytes)	sk (bytes)*	ct (bytes)
NTS-KEM (12,64)	1	128	4096	3328	129	$319,488$	$9,248$	128
NTS-KEM (13,80)	3	192	8192	7152	161	$929,760$	$17,556$	162
NTS-KEM (13,136)	5	256	8192	6424	273	$1,419,704$	$19,922$	253

†All classical security; *increased by 32 bytes from round 1 submission (no further changes)

NTS-KEM Security: IND-CCA Security (essentially unchanged from round 1)

Theorem

If there exists a (t, ε)-adversary $\mathcal{A}$ winning the $\mathrm{IND\text{-}CCA}$ game for NTS-KEM, then there exists a $\left(2\,t, \varepsilon - \frac{q_D}{2^\ell}\right)$-adversary $\mathcal{B}$ against the OW security of the McEliece PKE scheme with same code parameters. Here q_D is the number of queries made by $\mathcal{A}$ to its decapsulation oracle. The proof is in the Random Oracle Model.

- **Tight security reduction**
  - Standard Fujisaki-Okamoto conversion is not tight
  - HHK17[2] tight conversion may result in larger ciphertext
  - Some tweaks were needed to the proof of our round 1 scheme to handle implicit rejection

[2] D. Hofheinz, K. Hövelmanns, and E. Kiltz, A modular analysis of the Fujisaki-Okamoto transformation, TCC 2017, Part I (pp. 341–371), Springer, Heidelberg, 2017

NTS-KEM Security: Parameter Estimates (unchanged from round 1)

- Simplistic Information Set Decoding (ISD) analysis to derive minimum m and τ value pair to reach a target work-factor $N(m,\tau) \approx \binom{n}{k} / \binom{n-\tau}{k}$
  - $m \geq 12$, $\tau \geq 42$, $N(m,\tau) \geq 2^{128}$
  - $m \geq 13$, $\tau \geq 53$, $N(m,\tau) \geq 2^{192}$
  - $m \geq 13$, $\tau \geq 90$, $N(m,\tau) \geq 2^{256}$
- Using more recent results of BJMM algorithm[3], the minimum m and τ pairs are:
  - Work-factor 2^{128}: $m = 12$ and $\tau = 64$, time-complexity[4]: $2^{158.4}$
  - Work-factor 2^{192}: $m = 13$ and $\tau = 80$, time-complexity: $2^{239.9}$
  - Work-factor 2^{256}: $m = 13$ and $\tau = 136$, time-complexity: $2^{305.1}$
- The above estimates are conservative

[3] L. Both and A. May. Optimizing BJMM with Nearest Neighbors: Full Decoding in $2^{\mathbf{21}n/\mathbf{2}}$ and McEliece Security. The Tenth International Workshop on Coding and Cryptography 2017

[4] D. J. Bernstein, T. Lange, and C. Peters. Smaller decoding exponents: Ball-collision decoding. Advances in Cryptology CRYPTO 2011, pages 743–760, Santa Barbara, CA, USA

NTS-KEM Security: Quantum Attacks (unchanged from round 1)

- Best quantum attack: application of Grover's algorithm and quantum random walks to speed up ISD algorithms
- Bernstein[5] showed that Prange's ISD can be done in about

$$c^{(1/2)n/\log n} \text{ iterations}, \quad c = 1/\left(1 - \frac{k}{n}\right)^{1-\frac{k}{n}}$$

  where each iteration requires $O(n^3)$ qubit operations
- Kachigar and Tillich[6] considered how to speed up some of the more advanced ISD algorithms on quantum computers
  - Small improvement over Bernstein

[5] D. J. Bernstein. Grover vs. McEliece. In Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings, pages 73–80, 2010.

[6] G. Kachigar and J. Tillich. Quantum Information Set Decoding Algorithms. In Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings, pages 69–89, 2017

NTS-KEM Advantages (unchanged from round 1)

- Strong security guarantee
  - Conservative proposal of McEliece variant, nearly 40 years of attention from cryptographic community
  - Tight relationship between IND-CCA security of NTS-KEM and the problem of inverting McEliece PKE scheme
- Simple and well-understood mathematical problem
- Conservative parameter set, likely to offer a reasonable security margin within the aimed security categories
- Long-term post-quantum security
  - Best-case quantum attack offers at best a quadratic speed-up on classical ISD

NTS-KEM Advantages (ctd) (unchanged from round 1)

- High-degree of flexibility in the parameter set
  - Easy to consider potential trade-off between performance and security
  - Parameters may be set deliberately low to test any new proposed cryptanalytic technique
- Good long-term keys
  - Deterministic decoding in decapsulation algorithm
- Compact ciphertext size
- Efficient operations

NTS-KEM Disadvantages (updated from round 1)

- Relatively large public-key
- NTS-KEM does not (yet) have a QROM security proof
- NTS-KEM does not (yet) have a constant-time implementation

We look forward to further comments and open collaboration to help develop NTS-KEM

https://nts-kem.io