NTS-KEM

M. Albrecht[1], C. Cid[1], K. Paterson[1], **CJ Tjhai**[2], M. Tomlinson[2]

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

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

NIST First PQC Standardization Conference

13th April 2018

Introduction

- Code-based cryptography
  - Goppa codes
  - McEliece public-key encryption (PKE)
    - One-wayness (OW) secure
    - Difficult for an attacker to recover the underlying message $\mathbf{m}$ for some ciphertext $\mathbf{c}$
- NTS-KEM is a key-encapsulation mechanism (KEM)
  - Mixture of McEliece and Niederreiter schemes combined with a transform akin to Fujisaki-Okamoto or Dent transforms.
  - Resistant against chosen ciphertext attacks (CCA)

Algorithm Summary

- The key-generation, encapsulation and decapsulation algorithms are the same as those of McEliece's scheme (in general)
- The main difference: the 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 *a* section in the private-key and for syndrome computation in decapsulation

Parameter Sets

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	9,216	128
NTS-KEM (13,80)	3	192	8192	7152	161	929,760	17,524	162
NTS-KEM (13,136)	5	256	8192	6424	273	1,419,704	19,890	253

†All classical security

Performance Analysis

- CPU cycle counts on AVX2.0 platform (MacBook with Intel® Core™ m3-6Y30 1.1GHz processor, 8GB of RAM)

Parameter set	Key-gen (kilocycles)	Encap (kilocycles)	Decap (kilocycles)
NTS-KEM(12, 64)	18,691	52	177
NTS-KEM(13, 80)	51,275	178	332
NTS-KEM(13, 136)	108,501	266	644

- Approximate memory requirements

Parameter set	Key-gen (KB)	Encap (KB)	Decap (KB)
NTS-KEM(12, 64)	750	320	23
NTS-KEM(13, 80)	2,070	931	48
NTS-KEM(13, 136)	3,310	1,421	53

NTS-KEM Security: IND-CCA Secure

Theorem

If there exists a (t, ε)-adversary $\mathcal{A}$ winning the IND-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:

- in the Random Oracle Model; and,
- when the decapsulation algorithm succeeds with probability 1 for all public keys $(\mathbf{Q}, \tau, \ell)$ and all well-formed ciphertexts;

with q_D being the number of queries made by $\mathcal{A}$ to its decapsulation oracle.

- **Tight security reduction**
  - Standard Fujisaki-Okamoto conversion is not tight
  - HHK17[1] tight conversion may result in larger ciphertext

[1] 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

- 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[2], the minimum m and τ pairs are:
  - Work-factor 2^{128}: $m = 12$ and $\tau = 64$, time-complexity[3]: $2^{158.4}$
  - 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

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

[3] 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

- Best quantum attack: application of Grover's algorithm and quantum random walks to speed up ISD algorithms
- Bernstein[4] 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[5] considered how to speed up some of the more advanced ISD algorithms on quantum computers
  - Small improvement over Bernstein's

---

[4] 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.

[5] 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

Advantages

- Strong security guarantee
  - Conservative proposal of McEliece and Niederreiter 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

Advantages (cont'd)

- 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

Disadvantage

- The size of the public-key
  - May not be an issue for optical networks[6]

[6] Joo Yeon Cho, Implementation of Hybrid Mode Quantum-safe Key Exchange over Optical Communication Systems, The Sixth Code-Based Cryptography Workshop, Florida Atlantic University, Florida, April 5-6, 2018, slides

Thank You

https://nts-kem.io