NewHope

Original Submitters

Erdem Alkim, Roberto Avanzi (ARM), Joppe Bos (NXP), Léo Ducas (CWI Amsterdam), Antonio de la Piedra (Compumatica secure networks B.V.), Thomas Pöppelmann (Infineon Technologies), Peter Schwabe (Radboud University), Douglas Stebila (McMaster University),

Additional Round Two Contributors:

Martin R. Albrecht (Royal Holloway), Emmanuela Orsini (KU Leuven), Valery Osheter (Unbound Tech), Kenneth G. Paterson (ETH Zurich), Guy Peer (Unbound Tech), Nigel P. Smart (KU Leuven)

Presented by Thomas Pöppelmann on 24 August 2019 at the NIST Second PQC Standardization Conference

Recap 1

- NewHope is a suite of lattice-based key encapsulation mechanisms (KEM)
  - **NewHope-CPA-KEM**: Passively secure KEM (CPA = chosen plaintext attacks)
  - **NewHope-CCA-KEM**: Semantically secure KEM with respect to adaptive chosen ciphertext attacks (CCA)
- Security based on conjectured quantum hardness of Ring-Learning with Errors (RLWE)
- Uses threshold encoding to deal with decryption errors like NewHope-Simple (eprint 2016/1157)

Recap 2

- Three parameters (n,q,k): Fixed prime q=12289 and k=8 for binomial noise distribution
  - With n=512 (very conservative estimated) known quantum hardness of 101-bits (Level 1): ~1 Kbyte for pk/ciphertext
  - With n=1024 (very conservatively estimated) known quantum hardness of 233-bits (Level 5): ~2 Kbyte for pk/ciphertext
- Thus four instantiations ({CPA,CCA} x {512,1024})
  - NewHope512-CPA-KEM, NewHope1024-CPA-KEM, NewHope512-CCA-KEM, NewHope1024-CCA-KEM
- Implementations on ARM, Intel/AMD, MIPS64, FPGA are fast

Round 2 updates

- No change to parameters or implementation
  - Round 1 and 2 SW is compatible

- Some smaller fixes in specification
  - Fixed typos in definition of dRLWE and Theorem 4.4 identified by Bernstein
  - Updated variable naming and pari/gp script for NTT constant generation
  - Fixed typo in Algorithm 12 (return h instead of r)
  - NTT parameter γ does not match reference implementation in NewHope512. Update of document to not touch implementation. No security impact.

Performance

Scheme	Type	Gen	Enc	Dec
newhope1024cca	clean	1 460 167	2 264 773	2 410 906
kyber1024	clean	1 891 737	2 254 703	2 407 858
r5nd-5kemcca-5d	m4	1 228 319	1 782 156	2 332 469
firesaber	ref	3 815 672	4 745 405	5 402 295

- Results from eprint 2019/844 on Cortex-M4
  - NewHope implementation performs well in comparison to other schemes
  - Too many small differences to put them on one slide (security, sizes, trust, level of optimization)
- NewHope works well in (reconfigurable) hardware (e.g., FPGA) but also no major difference to other RLWE-based schemes
- NewHope is fast in SW (no major updates till round 1)

Review and next steps

- Review of tradeoffs made in Round 1/2
  - Other lattice-based schemes in round 2 do things differently (reconciliation, generation of secrets, parameters, security estimation, RLWR vs. RLWE)
  - We still see NewHope aiming at being “conservative” in terms of security and allowing a “simple” implementation
  - No major issues or attacks have been identified
  - Implementation and parameter sets are stable
- Next steps
  - Further optimizations of the implementation (help is always welcome) or exploration of tradeoffs
  - Protection of NewHope against fault and side-channel attacks
    - CCA transforms complicates things

Thank you for your attention!

Any questions?

NewHope

For more information visit

https://newhopecrypto.org/

The design of NewHope and its submission to the NIST process was supported by

- the European Commission through the ICT program under contract ICT-645622 (PQCRYPTO)
- a Veni Innovational Research Grant from NWO under project number 639.021.64
- TÜBITAK under 2214-A Doctoral Research Program Grant
- a grant from CWI from budget for public-private-partnerships and in part by a grant from NXP Semiconductor
- a Veni Innovational Research Grant from NWO under through Veni 2013 project 13114
- a Free Competition Grant
- the EPSRC grant “Bit Security of Learning with Errors for Post-Quantum Cryptography and Fully Homomorphic Encryption” (EP/P009417/1)
- the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701)
- European Union’s Horizon 2020 research and innovation programme under grant agreement No. 779391 (FutureTPM)
- the ERC StG 805031 (EPOQUE)
- the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery grant RGPIN-2016-05146
- the NSERC Discovery Accelerator Supplement grant RGPIN-2016-05146
- the ERC Advanced Grant ERC-2015-AdG-IMPaCT
- he EPSRC via grants EP/N021940/1, EP/M012824, EP/M013472/1,EP/L018543/1 and EP/P009417/1

Backup

Pros and Cons

- Advantages of NewHope
  - High performance: As shown by implementations
  - Simplicity and ease of implementation: Few changes between variants
  - Memory efficiency: In place computations due to NTT
  - Conservative design: Considerable security margin in our analysis (233-bit security does not mean we know a 233-bit complexity attack)
  - Implementation security: Some works already available as proof of concept (e.g., topics like constant time or side channels)
- Disadvantages of NewHope
  - Small noise distribution: For correctness we use k=8 which is not needed for ephemeral key exchange
  - Ring-LWE: More structure than LWE
  - Limited Parametrization: Either n=512 (level 1) or n=1024 (level 5) but no n=768
  - Restrictions due to usage of the NTT: NTT is part of the definition

Summary of Design Rationale

- Common to all NewHope variants
  - Use easy to sample centered binomial distribution instead of discrete Gaussian for error and secret of RLWE
  - No constants/against all authority/no all-for-the-price-of-one attacks – the polynomials **a** is freshly generated from a seed using a XOF
  - Conservative parameters that enable fast implementation of the Number Theoretic Transform (NTT)
  - Usage of the NTT in the definition of the scheme
- Our submission to the NIST process
  - We do not use reconciliation but modified threshold encoding
  - We move away from ephemeral key exchange (NewHope-Usenix) to a CPA-KEM and CCA-KEM approach using Targhi-Unruh transformation
  - We officially “support” the n=512 parameter set and set k=8 to achieve quasi error free decryption

Numbers

Parameter Set	NewHope512	NewHope1024
Dimension n	512	1024
Modulus q	12289	12289
Noise parameter k	8	8
NTT parameter γ	10968	7
Decryption error probability	2^{-213}	2^{-216}
Claimed post-quantum bit-security	101	233
NIST Security Strength Category	1	5

Parameter Set	$\|pk\|$	$\|sk\|$	$\|ciphertext\|$
NewHope512-CPA-KEM	928	869	1088
NewHope1024-CPA-KEM	1824	1792	2176
NewHope512-CCA-KEM	928	1888	1120
NewHope1024-CCA-KEM	1824	3680	2208