NewHope

by 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)

Presented by Thomas Pöppelmann on 12 April 2018 at NIST First PQC Standardization Conference

Overview

- 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); no reconciliation as in NewHope paper@Usenix
- 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

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	49	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

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

Thank you for your attention!

Any questions?

NewHope

by 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)

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

Backup

History of the scheme (naturally biased)

- History of works related to NewHope
  - Hoffstein, Pipher, Silverman, 1996: NTRU cryptosystem
  - Regev, 2005: Introduce LWE-based encryption
  - Lyubashevsky, Peikert, Regev, 2010: Ring-LWE and Ring-LWE encryption
  - Ding, Xie, Lin, 2012: Transform to (R)LWE-based key exchange
  - Peikert, 2014: Peikert: remove key biases in Ding key exchange".
  - Bos, Costello, Naehrig, Stebila, 2015: Instantiate and implement Peikert's key exchange in TLS (BCNS)
  - Alkim, Ducas, Pöppelmann, Schwabe, Aug. 2016: NewHope – ephemeral key exchange (*NewHope-Usenix*)
  - Google, July 2016: Googles uses NewHope successfully in PQC experiment
  - Alkim, Ducas, Pöppelmann, Schwabe, Dec. 2016: NewHope-Simple removes reconciliation due to complexity (*NewHope-Simple*)
  - Erdem Alkim, Roberto Avanzi, Joppe Bos, Leo Ducas, Antonio de la Piedra, Thomas Pöppelmann, Peter Schwabe, Douglas Stebila, Nov. 2017, Submission of NewHope to NIST (*NewHope-CPA-KEM* and *NewHope-CCA-KEM*)

Performance

Cycle counts for reference implementation on Intel Haswell

Operation	NH-512-CPA-KEM	NH-512-CCA-KEM	NH-1024-CPA-KEM	NH-1024-CCA-KEM
NTT	21,772	21,772	49,920	49,772
NTT^{-1}	23,384	23,420	53,596	53,408
GenA	16,012	16,052	32,248	32,240
Gen	106,820	117,128	222,922	244,944
Encaps	155,840	180,648	330,828	377,092
Decaps	40,988	206,244	87,080	437,056

Cycle counts for AVX implementation on Intel Haswell

Operation	NH-512-CPA-KEM	NH-512-CCA-KEM	NH-1024-CPA-KEM	NH-1024-CCA-KEM
NTT	4888	4820	8416	8496
NTT^{-1}	6352	6344	11,708	11,680
GenA	10,804	10,808	21,308	21,480
Gen	56,236	68,080	107,032	129,670
Encaps	85,144	109,836	163,332	210,092
Decaps	19,472	114,176	35,716	220,864