# First-Order Masked Kyber on ARM Cortex-M4

## Work in Progress


Daniel Heinz[1, 5] Matthias J. Kannwischer[2] Georg Land[3, 4]
Thomas Pöppelmann[5] Peter Schwabe[2] Daan Sprenkels[6]

[1]Research Institute CODE, Universität der Bundeswehr München, Germany
[2]Max Planck Institute for Security and Privacy, Bochum, Germany
[3]Ruhr-Universität Bochum, Germany
[4]DFKI GmbH, Cyber-Physical Systems, Bremen, Germany
[5]Infineon Technologies AG, Germany
[6]Digital Security Group, Radboud University, Nijmegen, The Netherlands



3[rd] PQC Standardization Conference, June 8th, 2021

# Contents

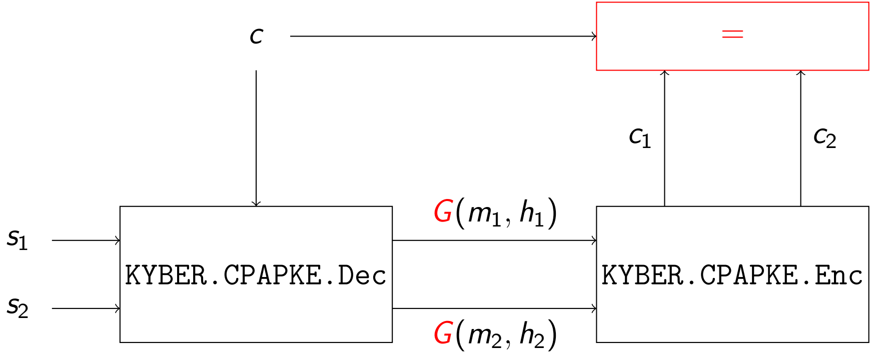
# Motivation

- KyberKEM is a finalist in NIST post-quantum standardization process
- Motivation
  - Comparability of masked implementations between different schemes
  - Gain more insights on side-channel security of proposed schemes
- Side-Channel security is an important research topic
  - [OSPG18] proposes first-order masked CCA2-secure Ring-Learning with errors (RLWE) scheme
  - [BDK+20] presents a first-order masked implementation of Saber (Cortex-M4)
  - [BGR+21] presents masked versions of Kyber on Cortex-M0
  - [FBR+21] presents masked hardware accelerators using RISC-V instruction set extensions
- Goal: An open-source fast first-order secure implementation on Cortex-M4

# CCA2-Security

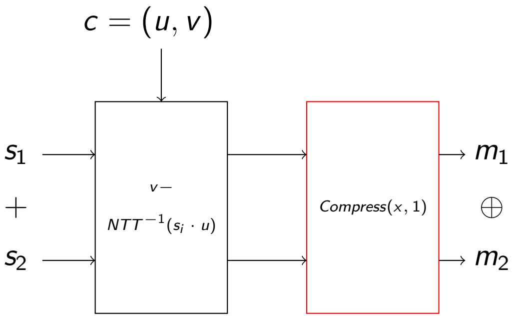
- Kyber is based on Module-Learning with errors (MLWE)
- RLWE and MLWE are only secure against Chosen-Plaintext Attacks
- Fujisaki-Okamoto Transform: Re-encryption during decryption (CCA)
- Re-encryption is dependent on the result of the decryption and therefore on the secret key
- Masking of re-encryption necessary

# KYBER.CCAKEM.Dec



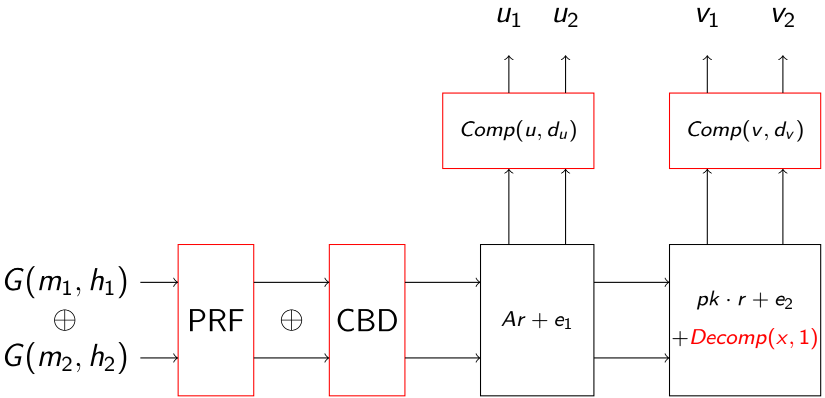

- Masked Comparison is non-trivial to mask
  - [BPO+20] shown to be flawed in [BDH+21]
  - [OSPG18] compares hash values ([BDH+21] shows leakage)
  - [BDK+20] adapts [OSPG18]

# KYBER.CPAPKE.Dec




- Linear parts can be calculated on each share separately
- $Compress_q(x, 1)$ can be calculated analogously to Masked Decode in [OSPG18]

# KYBER.CPAPKE.Enc



# KYBER.CPAPKE.Enc

- Masked PRF:
  - PRF is instantiated as SHAKE256
  - Efficient first-order masking approach is taken from previous work (Bertoni et al. [BDPA10])
- Masked CBD:
  - Approach from Schneider et al. (PKC2019, [SPOG19])
- Masked Decomp(x,1):
  - Approach from Oder et al. (CHES2018, [OSPG18])
  - Usage of fixed A2B conversion ([BDV21])
- No masked compression:
  - Masked comparison as proposed recently in Bos et al. ([BGR$^+$21])

# Masked CBD Sampling

- Approach from [SPOG19]
- Input: masked buffer of pseudorandom bytes (output of masked PRF)
- Basic idea:
  1. Bitsliced computation of $HW(x) - HW(y) + \eta$
  2. $\text{B2A}_q$ from [SPOG19]
  3. Subtraction of $\eta$ from each masked coefficient
- Possible for higher-order masking

# Masked Comparison

- Approach from recent preprint [BGR+21]
- Basic idea:
  - No masked compression during re-encryption
  - Look up lower and upper bound for decompression of each coefficient in $\mathbf{u}, v$ from original ct
  - For each masked coefficient in $\mathbf{u}', v'$ from re-encryption: masked check if within possible boundaries
- A2B conversion needed to extract MSB from bound subtractions
- Alternative: use A2A conversion from [BDK+20] to extract MSB
- Possible for higher-order masking

# Performance Evaluation

- Randomness generation from internal RNG (not included in the cycle counts)
- Evaluation using ARM Cortex-M4 on STM32F303 MCU (7.37 MHz)
- Table shows average cycle counts (100 executions)
- t-test in Appendix

| Operation | Unmasked (PQM4) | Masked (1st order) |
|---|---|---|
| KYBER.CCAKEM.KeyGen | 751.487 | 2 520 913[1] |
| KYBER.CCAKEM.Dec | 847.584 | 3 596 193[1] |
| → KYBER.CPAPKE.Dec | 61 505 | 134 363 |
| → KYBER.CPAPKE.Enc | 683 813 | 3 122 497[1] |

[1]Not final: Masked binomial sampling still shows leakage in t-test

# Conclusion

- Comparison of first-order masked decapsulations (excluding randomness)

| Saber (Cortex-M4) | Kyber768 (Cortex-M0) | Kyber768 (Cortex-M4) |
|---|---|---|
| 2 833 348 | 12 208 000 | 3 596 193[1] |

- Relative overhead factor to unmasked Cortex-M4 decapsulation of 4.2 ([FBR+21] with masked accelerators and RISC-V IS extension reports 3.6)
- Recent work ([NDGJ21]) shows: First-order masking is not enough
- Possible future work:
  - Improve performance on Cortex-M4 (masked binomial sampling)
  - Extend masking to higher-order on Cortex-M4
  - Combine with other countermeasures (shuffling,...)

[1] Not final: Masked binomial sampling still shows leakage in t-test

[BDH+21] Shivam Bhasin, Jan-Pieter D'Anvers, Daniel Heinz, Thomas Pöppelmann, and Michiel Van Beirendonck. Attacking and defending masked polynomial comparison for lattice-based cryptography. *IACR Cryptol. ePrint Arch.*, 2021:104, 2021.

[BDK+20] Michiel Van Beirendonck, Jan-Pieter D'Anvers, Angshuman Karmakar, Josep Balasch, and Ingrid Verbauwhede. A side-channel resistant implementation of SABER. *IACR Cryptol. ePrint Arch.*, 2020:733, 2020.

[BDPA10] G. Bertoni, J. Daemen, Michaël Peeters, and G. V. Assche. Building power analysis resistant implementations of keccak. 2010.

[BDV21] Michiel Van Beirendonck, Jan-Pieter D'Anvers, and Ingrid Verbauwhede. Analysis and comparison of table-based arithmetic to boolean masking. *IACR Cryptol. ePrint Arch.*, 2021:67, 2021.

[BGR+21] Joppe W. Bos, Marc Gourjon, Joost Renes, Tobias Schneider, and Christine van Vredendaal. Masking kyber: First- and higher-order implementations. *IACR Cryptol. ePrint Arch.*, 2021:483, 2021.

[BPO+20] Florian Bache, Clara Paglialonga, Tobias Oder, Tobias Schneider, and Tim Güneysu. High-speed masking for polynomial comparison in lattice-based kems. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(3):483–507, 2020.

[FBR+21] Tim Fritzmann, Michiel Van Beirendonck, Debapriya Basu Roy, Patrick Karl, Thomas Schamberger, Ingrid Verbauwhede, and Georg Sigl. Masked accelerators and instruction set extensions for post-quantum cryptography. *IACR Cryptol. ePrint Arch.*, 2021:479, 2021.

[NDGJ21] Kalle Ngo, Elena Dubrova, Qian Guo, and Thomas Johansson. A side-channel attack on a masked IND-CCA secure saber KEM. *IACR Cryptol. ePrint Arch.*, 2021:79, 2021.

[OSPG18] Tobias Oder, Tobias Schneider, Thomas Pöppelmann, and Tim Güneysu. Practical CCA2-secure and masked ring-lwe implementation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(1):142–174, 2018.

[SPOG19] Tobias Schneider, Clara Paglialonga, Tobias Oder, and Tim Güneysu. Efficiently masking binomial sampling at arbitrary orders for lattice-based crypto. In Dongdai Lin and Kazue Sako, editors, *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part II*, volume 11443 of *Lecture Notes in Computer Science*, pages 534–564. Springer, 2019.

# Appendix: t-test Evaluation

- Evaluation on ChipWhisperer with STM32F303 target
- 100 000 traces captured
- Randomness was generated in advance (constant-time)

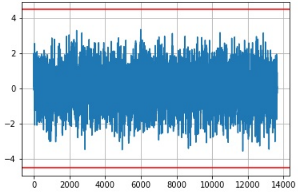



Figure: `polyinvntt_masked()`

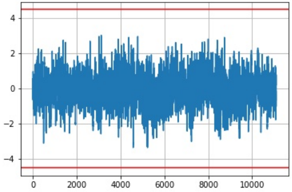



Figure: `polysub_masked()`

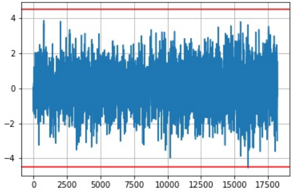



Figure: `polybasemul_masked()`

# Appendix: t-test Evaluation

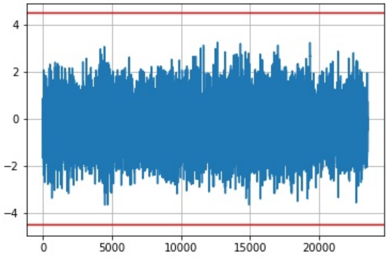



Figure: `polytomsg_masked()`

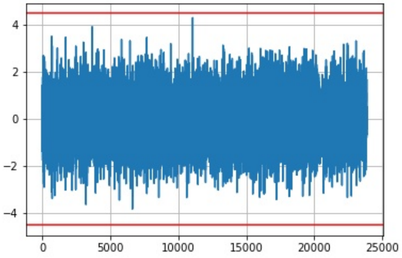



Figure: `polyfrommsg_masked()`

# Appendix: t-test Evaluation

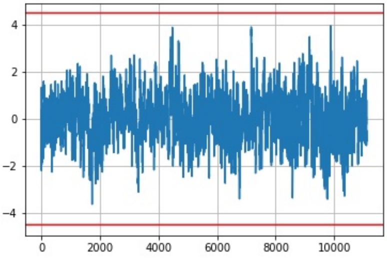



Figure: `polyreduce_masked()`

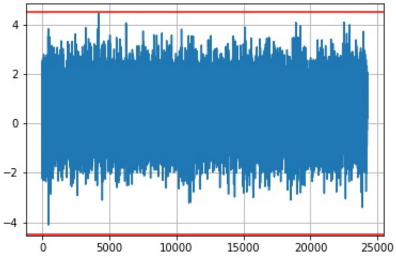



Figure: `polycompare_masked()`