The 23rd Annual International Conference on Information Security and Cryptology

# ICISC 2020

December 2 (Wed) ~ December 4 (Fri), 2020 | Virtual Conference

**Hosted by**
Korea Institute of Information Security and Cryptology (KIISC)
National Security Research Institute (NSR)

Korea Institute of Information Security & Cryptology

# Key Mismatch Attack on ThreeBears, Frodo and Round5


Jan Vacek, **Jan Václavek**

*Thales DIS, Prague*



# Outline

1. Targeted schemes
2. Key Mismatch Attack
3. State-of-the-art
4. Our attack
5. Results
6. Conclusion

# Targeted schemes

- **ThreeBears**
  - based on Integer Module Learning with Errors (I-MLWE)
  - NIST round 2 candidate
  - *C. Gu: "Integer Version of Ring-LWE and its Applications", 2017*
- **Frodo**
  - based on Learning with Errors (LWE)
  - NIST alternative round 3 candidate
  - *J. Bos et al.: "Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE", 2016*
- **Round5**
  - based on Learning with Rounding (LWR) and Ring Learning with Rounding (RLWR)
  - NIST round 2 candidate
  - *A. Banerjee et al.: "Pseudorandom Functions and Lattices", 2011*

# Key Mismatch Oracle Attack

- Consider some Public Key Encryption (PKE) with a fixed secret key $\boldsymbol{sk}$

- The goal of the attacker is to recover $\boldsymbol{sk}$ using the key mismatch oracle:

> - INPUT: - arbitrarily chosen ciphertext $\boldsymbol{ct}$ (not necessarily computed according to the specification)
>   - arbitrary plaintext $\boldsymbol{pt}$
> - OUTPUT: $\begin{cases} + & if\ decryption(\boldsymbol{sk}, \boldsymbol{ct}) = \boldsymbol{pt} \\ - & if\ decryption(\boldsymbol{sk}, \boldsymbol{ct}) \neq \boldsymbol{pt} \end{cases}$

# Practical relevance

- Access to the Key Mismatch Oracle even for actively secure (CCA) variants using e.g. side-channel attacks

- There is a risk of key reuse even though it is forbidden by the specification

- Significant state-of-the-art on the topic, e.g.:
    - S. Fluhrer: *"Cryptanalysis of ring-LWE based key exchange with key share reuse"*, 2016
    - S. Vaudenay et al.: *"Misuse Attacks on Post-Quantum Cryptosystems"*, EUROCRYPT 2019
    - S. Vaudenay et al.: *"Classical Misuse Attacks on NIST Round 2 PQC: The Power of Rank-Based Schemes"*, ACNS 2020
    - P. Ravi et al.: *"Generic Side-channel attacks on CCA-secure lattice-based PKE and KEM schemes"*, CHES 2020
    - S. Okada et al.: "*Improving Key Mismatch Attack on NewHope with Fewer Queries*", ACISP 2020

# Key mismatch oracle attack in the prior art

- Previous attacks target secret coefficients one by one

- Common technique – consider only queries such that:
  - the possible mismatch between the decrypted plaintext and the chosen plaintext can happen only on one position
  - the bit on this position depends only on the targeted secret coefficient

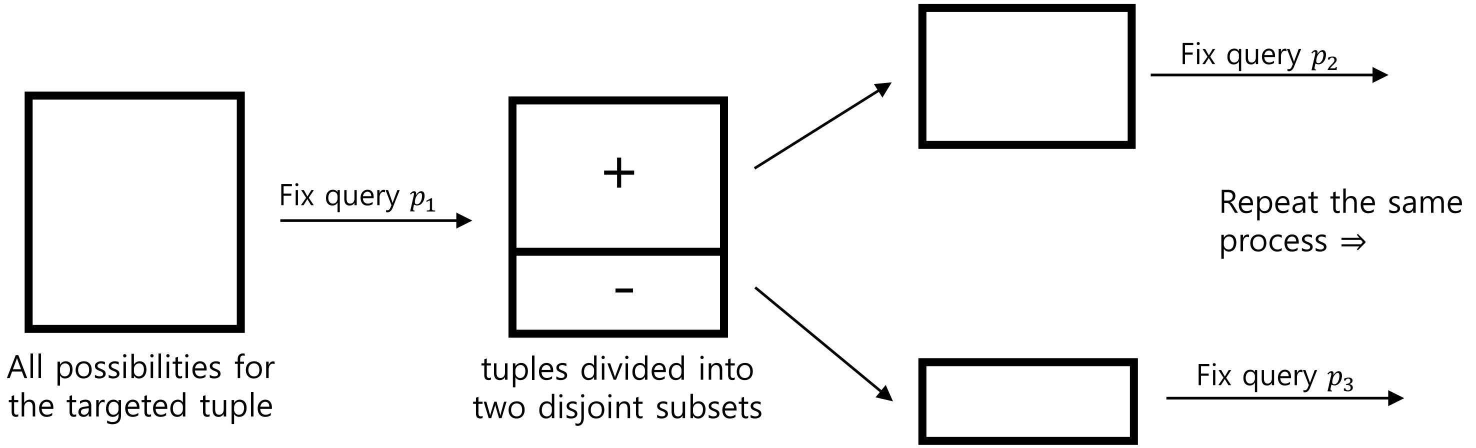
- Differences – how the output from the oracle is utilized:
  - “favorable cases” (ACISP 2020)
  - recover linear equations with the secret key as unknown (EUROCRYPT 2019)
  - oracle output tells if a coefficient is greater than a given threshold (ACNS 2020)
  - associate output sequences with targeted coefficients (CHES 2020)

The 23rd Annual International Conference on Information Security and Cryptology
ICISC 2020
December 2 (Wed) – December 4 (Fri), 2020 | Virtual Conference

Korea Institute of Information Security & Cryptology

# Idea of our attack

- Secret coefficients targeted in tuples, not necessary one by one
- Gradually reduce the possibilities for the targeted tuple



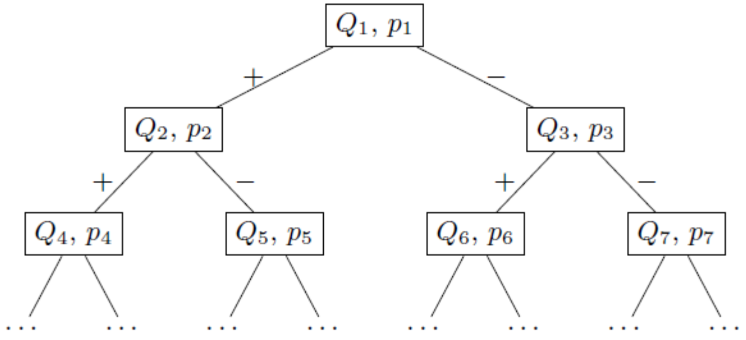




**Fig. 2.** Tree structure.

❖ We want $|Q_i| = 1$ for the leaves

# The attack

- The attacker follows a path from the root to some leaf according to the outputs from the oracle
- The attacker does not perform any computation, all the queries are stored within the tree
- The number of queries to recover some tuple equals the depth of the leaf corresponding to this tuples

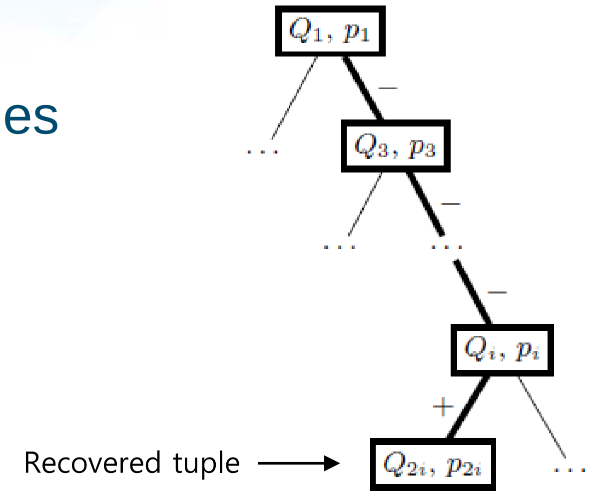



**Fig. 3.** Path in the tree.

# Construction of trees

- Tree is constructed recursively: looking for the tree which minimizes the expected number of queries to the oracle

- The expected number of queries: weighted average of the probabilities of the tuples and of the depths of the leaves corresponding to these tuples

- Not possible to try each tree ⇒ the following heuristic is used: split a set of possible tuples such that the two disjoint subsets have similar probabilities

# Results for ThreeBears

- We provide the first attack on ThreeBears
- Coefficients targeted only one by one

| Error-correcting code | NIST security level | Expected number of queries | Success probability |
|---|---|---|---|
| Yes | 1 | 1 414 | 100% |
| Yes | 3 | 1 638 | 100% |
| Yes | 5 | 2 223 | 100% |
| No | 1 | 1 443 | 100% |
| No | 3 | 2 150 | 100% |
| No | 5 | 2 847 | 100% |

# Results for Frodo

- Coefficients targeted one by one and by pairs (called dimension of the attack)
- Existing attack by Vaudenay et al. from EUROCRYPT 2019

| | NIST security level | Dimension of the attack | Expected number of queries | Success probability |
|---|---|---|---|---|
| EUROCRYPT 2019 | 1 | - | 65 536 | not clear |
| | 1 | 1 | 18 359 | 100% |
| | 1 | 2 | 18 239 | 100% |
| | 3 | 1 | 25 934 | 100% |
| | 3 | 2 | 25 672 | 100% |
| | 5 | 1 | 29 377 | 100% |
| | 5 | 2 | 28 008 | 100% |

# Results for Round5

- Coefficients targeted one by one, by pairs, triplets and quadruplets
- Existing attack by Ravi et al. from CHES 2020

| | variant | NIST security level | Dimension of the attack | Expected number of queries | Success probability |
|---|---|---|---|---|---|
| CHES 2020 | RLWR+ECC | 1 | - | 978 | 100% |
| | RLWR+ECC | 1 | 4 | 656 | 100% |
| | RLWR+ECC | 3 | 4 | 1277 | 100% |
| | RLWR | 1 | 3 | 687 | 100% |
| | RLWR | 3 | 2 | 1221 | 100% |
| | LWR | 1 | 4 | 5 790 | 100% |
| | LWR | 3 | 4 | 8 436 | 100% |

# Conclusion

- The first key mismatch attack on ThreeBears and variants of Round5
- Improved key mismatch attack on Frodo and variant of Round5
- The method is applicable against other LWE-based candidates, e.g. against Kyber, Saber, NewHope
- Targeting bigger tuples (if possible) gives better results, but it is not possible to target arbitrary tuples

# Thank you for your attention!

# Questions?