Decryption Errors and Implementation Attacks on Kyber

Julius Hermelink

Universität der Bundeswehr München

27.04.2023

Short CV:

- PhD Student at UniBw M (supervisors: Gabi Dreo, Mark Manulis at UniBw, Thomas Pöppelmann, Peter Pessl at Infineon).
- Until 03/2023 in cooperation with Infineon.
- Master's in Mathematics from LMU.
- Working student at Infineon since 2014.

Research interests:

- Implementation attacks on lattice-based schemes.
- Adapting attacks to/circumventing countermeasures.
- Key recovery methods using statistical and algebraic approaches.
- In the future: Improve SASCA using neural networks.

The Quantum Threat

Quantum computers threaten current cryptography.

- RSA
- Diffie-Hellman
- ECDSA
- ...

- Keccak/SHA-3
- SHA-2
- AES
- ...

The Quantum Threat

NIST selected algorithms for standardization in 2022.

- Several selected schemes are based on *learning with errors* (lattice-based).
- Main candidate for key exchanges, Kyber, is (module) learning with errors based.
- Kyber is comparably performant with small key sizes.
- Thus, especially suited for embedded devices.

Decryption Errors

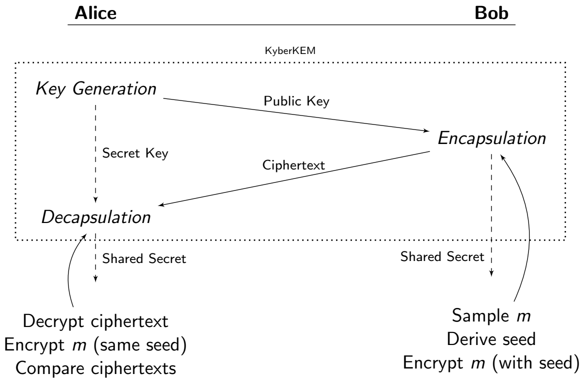
In LWE schemes, decryption errors leak information about the secret key.

- Encryption: Message bits are mapped to coefficients in $\mathbb{F}_q$.
- Decryption: Retrieves noisy version of message coefficients.
- If noise too large, decryption fails.
- Attacker can add to noise using chosen-ciphertext or fault.
- If they can observe decryption errors: Learns if noise term positive.

Probability for decryption errors without manipulation very low.

Key Encapsulation - CCA Security

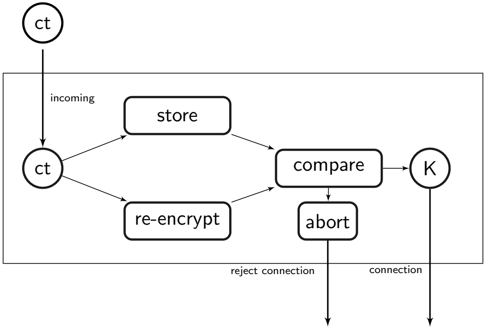
KyberKEM is build from KyberPKE using an FO-Transform.



- Re-encrypt and compare: Chosen-ciphertext causes decapsulation error.
- No information leaked when using chosen-ciphertext.

FO-Transform

An incoming ciphertext is re-encrypted and compared against the re-encrypted result:



An manipulated ciphertext leads to a decapsultation error without revealing potential decryption errors.

Decryption Errors and Decapsulation Errors

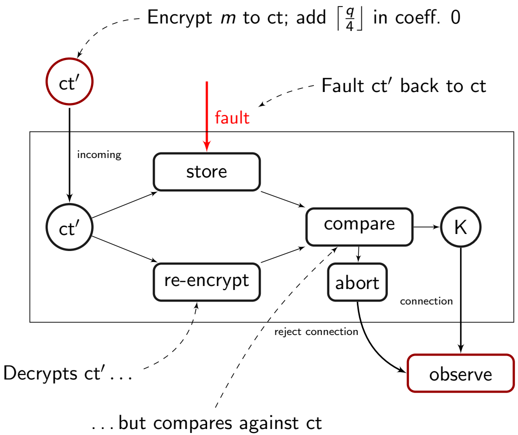
Decryption errors:

- Observing if added noise causes decryption errors leaks information on noise term.
- Error term contains information about secret.
- Attacker can derive inequality involving secret key.

Decapsulation errors:

- Decapsulation errors always occur when ciphertext manipulated.
- Decapsulation thereby hides decryption errors when using chosen-ciphertext.

Fault-Enabled Chosen-Ciphertext Attacks



- m is encrypted to ct; ct′ has $\lceil \frac{q}{4} \rfloor$ error.
- Fault changes ct′ to ct.
- Device decrypts ct′ but compares against ct.
- Depending on error term, $\lceil \frac{q}{4} \rfloor$ causes decryption error.

1. Decryption error: ct′ decrypts to $m' \neq m$, comparison fails $\rightarrow$ decapsulation error.
2. Decryption success: ct′ decrypts to $m' = m$, comparison succeeds $\rightarrow$ decapsulation success.

$\rightarrow$ We can observe decryption errors as decapsulation errors.

[HPP21] **Hermelink, J.**, Pessl, P. and Pöppelmann, T., 2021. Fault-enabled chosen-ciphertext attacks on Kyber. In Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22 (pp. 311-334). Springer International Publishing.

Decryption Errors and Implementation Attacks

Several other attacks exploit decryption errors:

- Pessl and Prokop [PP21] use a fault applied to the decoding method,
- Bhasin et al. [BDH+21] and D'Anvers et al. [DHP+22] exploited EM-leakage,
- Hermelink et al. [HPP21] and Delvaux [Del22] used a fault to turn FO into a decryption error oracle,
- and Fahr et al. [FKK+22] present a failure boosting attack on FrodoKEM.

Whenever side-channel allows observing comparison, attack as in [BDH+21, DHP+22] possible.

Recovering the Secret Key

Inequalities contain information about the secret key, but how to recover?

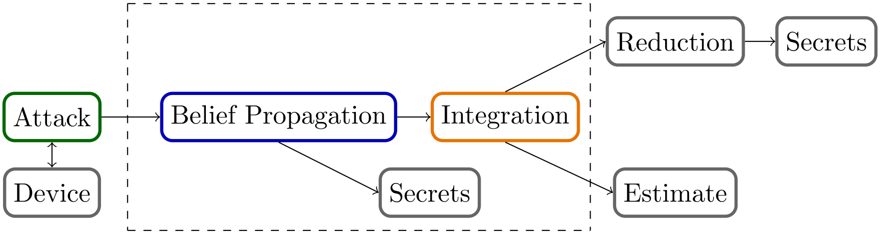
Several methods to obtain secret from inequalities exist:

Method	Inequalities	Error Resistant	Practical[1]	Estimates
Pessl and Prokop [PP21]	8000	No	Yes	No
Hermelink et al. [HPP21]	5750	No	Yes	No
Delvaux [Del22]	9000	Yes	Yes	No
Dachman-Soled et al. [DDHG20]	≥ 10000	No	No	Yes
Dachman-Soled et al. [DGH+22]	n.a.	No	No	Yes

[1] Successfully used in a practical attack for full key recovery from this kind of inequalities.

Combining BP and lattice reduction

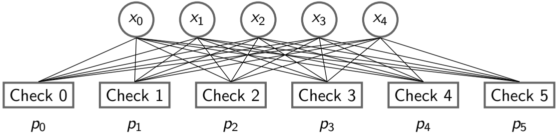
General problem: How to combine statistical method with lattice reduction?



Belief propagation output can be integrated into a lattice problem.

Error Tolerant BP

Belief Propagation (BP) can solve inequalities which are incorrect with probability p_i:



- BP is message passing algorithm.

- Variable nodes: Unknowns coefficients.

- Factor nodes: Inequalities.

- Messages represent belief.

- Initial: Sampling distribution.

- Factors update according to inequality.

- Variables combine incoming information.

- Incorrectness probability: Integrated in Bayesian update process in factors.

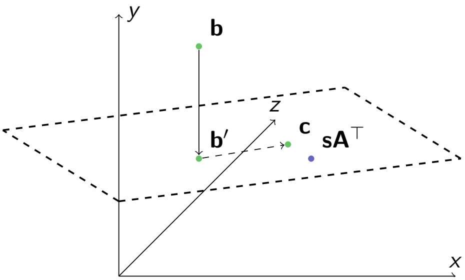
Integrate Statistical Information

Integration of belief propagation works in two steps:

Two steps of integrating information:

1. Reduce dimension with recovered coefficients.
2. Find closer vector with remaining information.

First step works directly on LWE equation, $\mathbf{s}\mathbf{A}^\top + \mathbf{e} \equiv \mathbf{b} \mod q$ instead of CVP/SVP; this enables the second step.



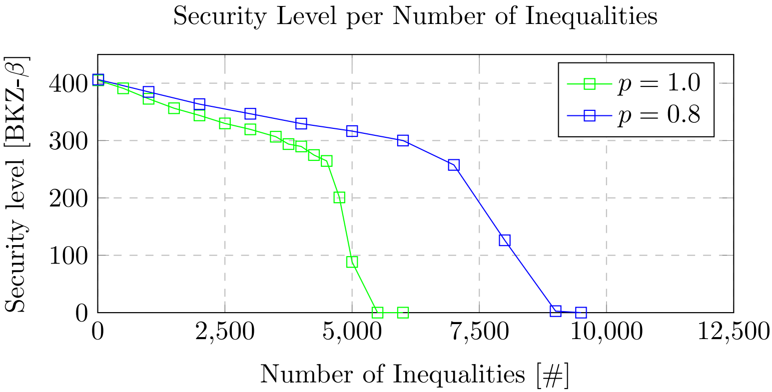
Our Method

We modified the belief propagation to be error resistant and explained how to integrate into lattice problem.

Method	Inequalities	Error Resistant	Practical[1]	Estimates
Pessl and Prokop [PP21]	8000	No	Yes	No
Hermelink et al. [HPP21]	5750	No	Yes	No
Delvaux [Del22]	9000	Yes	Yes	No
Dachman-Soled et al. [DDHG20]	≥ 10000	No	No	Yes
Dachman-Soled et al. [DGH+22]	n.a.	No	No	Yes
Hermelink et al. [HMS+23]	5500	Yes	Yes	Yes

[1] Successfully used in a practical attack for full key recovery from this kind of inequalities.

Results



Optimal code with optimal decoding would require $\sim$ 2,500 inequalities.

Conclusion

The occurance of decryption errors can be exploited for implementation attacks:

- Decryption errors allow for powerful implementation attacks.
- Large attack surface and securing comparison not sufficient.
- Recovering the secret by combining belief propagation and lattice reduction.
- Combination of belief propagation and lattice reduction likely useful in other attacks (e.g. [PP19, HHP21+, HSST23]).

Open Question and Future Work

Several questions open:

- How to (optimally) solve inequalities where coefficients correlated (occuring in [FKK+22], solved in [DGHK22])?
- Compare to/unify with/improve using the method of [DGHK22]?
- How to better model belief propagation with regards to coding theory?
- Threat of neural networks learning decryption failure from traces (as e.g. in [Weik22])?
- Generally applicable countermeasures apart from shutting device down after n decryption errors?

References

[PP19] Pessl, P. and Primas, R., 2019. More practical single-trace attacks on the number theoretic transform. In Progress in Cryptology–LATINCRYPT 2019: 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2–4, 2019, Proceedings 6 (pp. 130-149). Springer International Publishing.

[DDGR20] Dachman-Soled, D., Ducas, L., Gong, H. and Rossi, M., 2020, August. LWE with side information: attacks and concrete security estimation. In Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II (pp. 329-358). Cham: Springer International Publishing.

[HHP+21] Hamburg, M., **Hermelink, J.**, Primas, R., Samardjiska, S., Schamberger, T., Streit, S., Strieder, E. and van Vredendaal, C., 2021. Chosen ciphertext k-trace attacks on masked CCA2 secure kyber. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.88-113.

[PP21] Pessl, P. and Prokop, L., 2021. Fault attacks on CCA-secure lattice KEMs. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.37-60.

[BDH+21] Bhasin, S., D'Anvers, J.P., Heinz, D., Pöppelmann, T. and Van Beirendonck, M., 2021. Attacking and defending masked polynomial comparison for lattice-based cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.334-359.

[DHP+21] D'Anvers, J.P., Heinz, D., Pessl, P., Van Beirendonck, M. and Verbauwhede, I., 2021. Higher-order masked ciphertext comparison for lattice-based cryptography.

[HPP21] **Hermelink, J.**, Pessl, P. and Pöppelmann, T., 2021. Fault-enabled chosen-ciphertext attacks on Kyber. In Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22 (pp. 311-334). Springer International Publishing.

References

[Del22] Delvaux, J. (2022) “Roulette: A Diverse Family of Feasible Fault Attacks on Masked Kyber”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(4), pp. 637–660.

[FKK+22] Fahr Jr, M., Kippen, H., Kwong, A., Dang, T., Lichtinger, J., Dachman-Soled, D., Genkin, D., Nelson, A., Perlner, R., Yerukhimovich, A. and Apon, D., 2022, November. When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 979-993).

[DGHK22] Dachman-Soled, D., Gong, H., Hanson, T. and Kippen, H., 2022. Refined Security Estimation for LWE with Hints via a Geometric Approach. Cryptology ePrint Archive.

[Weik22] Weik, A. Machine-Learning-based Side-Channel Attacks on Lattice-based Key Encapsulation Mechanisms, 2022. Master’s Thesis. Technical University of Munich.

[HSST23] **Hermelink, J.**, Streit, S., Strieder, E. and Thieme, K., 2023. Adapting Belief Propagation to Counter Shuffling of NTTs. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.60-88.

[HMS+23] **Hermelink, J.**, Mårtensson, E., Samardjiska, S., Pessl, P. and Rodosek, G.D., 2023. Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors. Cryptology ePrint Archive.