Side-Channel and Fault Attacks in Modern Lattice-Based Cryptography

Mündliche Prüfung – Julius Hermelink

Gutachterin:	Prof. Dr. Gabi Dreo Rodosek	(UniBwM)
Gutachter:	Prof. Dr. Mark Manulis	(UniBwM)
Prüferin:	Prof. Dr. Eirini Ntoutsi	(UniBwM)
Prüfer:	Prof. Dr. Christof Paar	(MPI-SP)
Prüfer:	Prof. Dr. Arno Wacker	(UniBwM)

15.03.2024

The Quantum Threat

Quantum computers threaten currently used asymmetric cryptography.

We have to assume that:

- Large-scale quantum computer break commonly used asymmetric schemes.
- Adversaries: harvest now, decrypt later.

Therefore, we need:

- Post-quantum asymmetric cryptography.
- Most pressingly key exchanges.

The Quantum Threat

Quantum computers threaten currently used asymmetric cryptography.

We have to assume that:

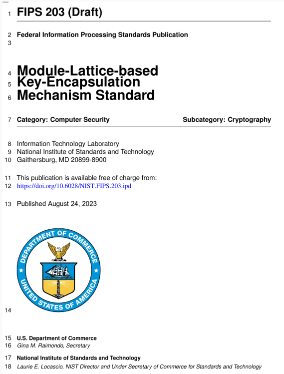
- Large-scale quantum computer break commonly used asymmetric schemes.
- Adversaries: harvest now, decrypt later.

Therefore, we need:

- Post-quantum asymmetric cryptography.
- Most pressingly key exchanges.

The NIST Standardization Process

NIST is in the process of standardizing post-quantum cryptography.



FIPS 203 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203.ipd

Published August 24, 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

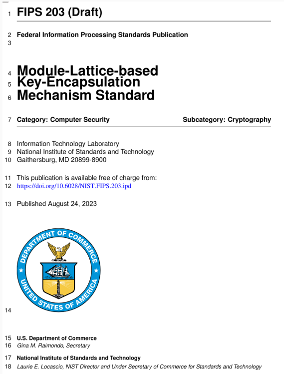
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST started a standardization process in 2016.

- Fourth round ongoing.
- Four candidates already selected.
- Three are lattice-based.
- Kyber selected as KEM (Kyber $\mapsto$ ML-KEM).

NIST draft standard, `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf`, accessed 16/02/2024.

NIST is in the process of standardizing post-quantum cryptography.


FIPS 203 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203.ipd

Published August 24, 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST started a standardization process in 2016.

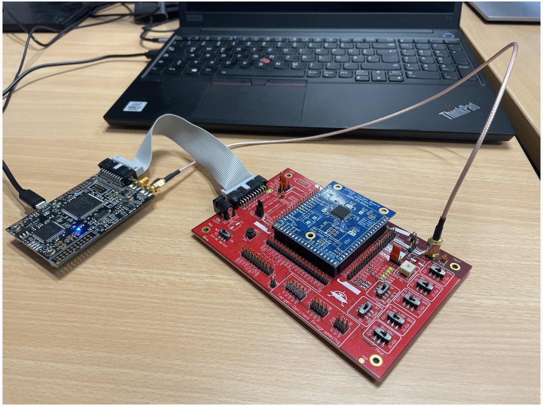
- Fourth round ongoing.
- Four candidates already selected.
- Three are lattice-based.
- Kyber selected as KEM (Kyber $\mapsto$ ML-KEM).

ML-KEM used in Signal, Chrome, iMessage, ...

NIST draft standard, `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf`, accessed 16/02/2024; applications: see [Aut23, Kre23, EA24].

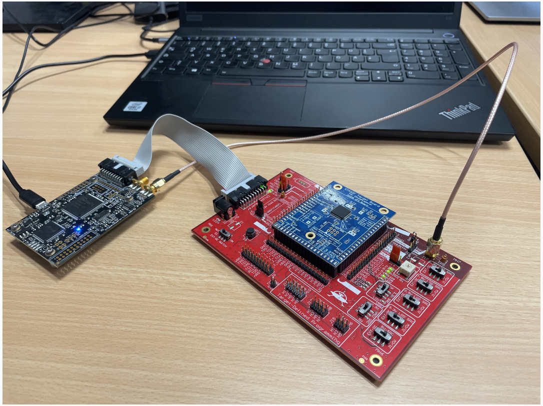
Attacks on Embedded Devices

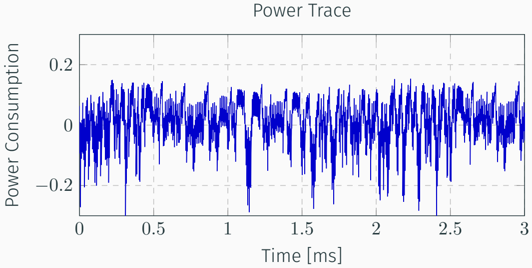
Embedded devices may be vulnerable to side-channel and fault attacks.



Attacks on Embedded Devices

Embedded devices may be vulnerable to side-channel and fault attacks.





Research Objective

Lattice-Based Cryptography uses different building blocks.

- Different underlying hard problems.
- Different multiplications (e.g., using number theoretic transforms).
- Error correction to recover message from noisy coefficients.
- Construction from PKE using FO-transforms to achieve IND-CCA security.
- ...

Which new vulnerabilities in regard to side-channel and fault attacks does this open up?

Research Objective

Lattice-Based Cryptography uses different building blocks.

- Different underlying hard problems.
- Different multiplications (e.g., using number theoretic transforms).
- Error correction to recover message from noisy coefficients.
- Construction from PKE using FO-transforms to achieve IND-CCA security.
- ...

Which new vulnerabilities in regard to side-channel and fault attacks does this open up?

Research Question 1

The number theoretic transform (NTT):

- Enables fast multiplication in several lattice-based schemes.
- Used at multiple points in all routines of ML-KEM.
- Inverse NTT processes data depending on the secret key during decryption.
- Previous work established (inverse) NTT as target for side-channel attacks.
- However, required noise levels limit attacks when targeting secret key.

RQ: To what extent is the number theoretic transform vulnerable to side-channel analysis.

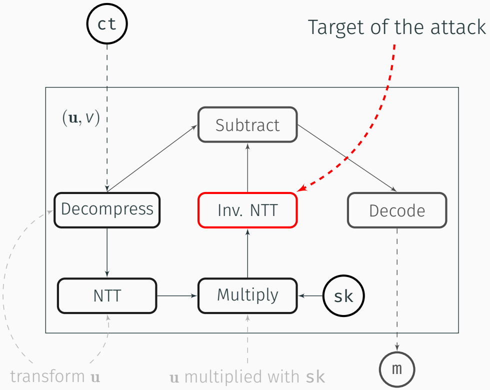
Research Question 1

The number theoretic transform (NTT):

- Enables fast multiplication in several lattice-based schemes.
- Used at multiple points in all routines of ML-KEM.
- Inverse NTT processes data depending on the secret key during decryption.
- Previous work established (inverse) NTT as target for side-channel attacks.
- However, required noise levels limit attacks when targeting secret key.

RQ: To what extent is the number theoretic transform vulnerable to side-channel analysis.

Chosen-Ciphertext k-Trace Attacks – Idea



Previous work [PPM17, PP19]:

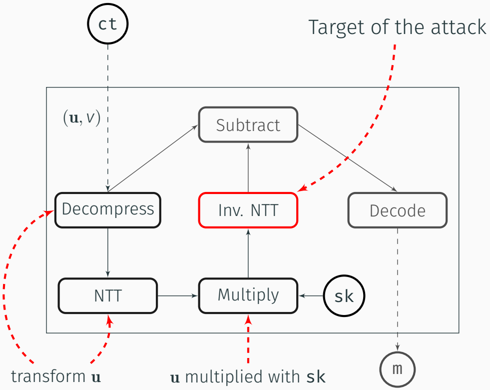
- Template attack on inv. NTT; then belief propagation.
- However, cannot target secret key with high noise tolerance.

Decryption as shown on the left:

- Ciphertext components are decompressed.
- Component is multiplied with secret.
- Results fed into the inv. number theoretic transform.

Attack strategy: Reduce entropy using compressible NTT-sparse chosen ciphertext.

Chosen-Ciphertext k-Trace Attacks – Idea



Previous work [PPM17, PP19]:

- Template attack on inv. NTT; then belief propagation.
- However, cannot target secret key with high noise tolerance.

Decryption as shown on the left:

- Ciphertext components are decompressed.
- Component is multiplied with secret.
- Results fed into the inv. number theoretic transform.

Attack strategy: Reduce entropy using compressible NTT-sparse chosen ciphertext.

Chosen-Ciphertext k-Trace Attacks

Our attack strategy for increased noise tolerance:

For targeted subkeys:

- Formulate as lattice problem.
- Run lattice reduction.
- Obtain compressible NTT-sparse `ct`.

For each `ct`:

- Record trace for `ct`.
- Obtain distributions for intermediates.
- Run belief propagation; obtain subkeys.

Using the subkeys:

- Formulate key recovery using subkeys as lattice problem.
- Run lattice reduction.
- Obtain full key.

Lattice reduction is computationally expensive and slow but done offline.

Mike Hamburg, **Julius Hermelink**, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. "Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.4 (2021), pp. 88–113

Chosen-Ciphertext k-Trace Attacks

Our attack strategy for increased noise tolerance:

For targeted subkeys:

- Formulate as lattice problem.
- Run lattice reduction.
- Obtain compressible NTT-sparse `ct`.

For each `ct`:

- Record trace for `ct`.
- Obtain distributions for intermediates.
- Run belief propagation; obtain subkeys.

Using the subkeys:

- Formulate key recovery using subkeys as lattice problem.
- Run lattice reduction.
- Obtain full key.

Lattice reduction is computationally expensive and slow but done offline.

Mike Hamburg, **Julius Hermelink**, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. “Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.4 (2021), pp. 88–113

Chosen-Ciphertext k-Trace Attacks

Our attack strategy for increased noise tolerance:

For targeted subkeys:

- Formulate as lattice problem.
- Run lattice reduction.
- Obtain compressible NTT-sparse `ct`.

For each `ct`:

- Record trace for `ct`.
- Obtain distributions for intermediates.
- Run belief propagation; obtain subkeys.

Using the subkeys:

- Formulate key recovery using subkeys as lattice problem.
- Run lattice reduction.
- Obtain full key.

Lattice reduction is computationally expensive and slow but done offline.

Mike Hamburg, **Julius Hermelink**, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. "Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.4 (2021), pp. 88–113

Adapting Belief Propagation to Counter Shuffling of NTTs

Real-world attacks have to take countermeasures into account.

Important classes of countermeasures:

- Masking circumvented.
- Hiding prevents these attacks.

Ravi et al. [RPBC20] (ascending security):

- Fine shuffling
- Coarse block shuffling
- Coarse full shuffling

We propose two techniques against hiding:

- Fine shuffling: Shuffle node adapts factor depending on processed information.
- Coarse shuffling: Extended attacker model and matching algorithm.

Adaptation to hiding countermeasures for belief-propagation-based attacks.

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. "Adapting Belief Propagation to Counter Shuffling of NTTs". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.1 (2023), pp. 60–88

Adapting Belief Propagation to Counter Shuffling of NTTs

Real-world attacks have to take countermeasures into account.

Important classes of countermeasures:

- Masking circumvented.
- Hiding prevents these attacks.

Ravi et al. [RPBC20] (ascending security):

- Fine shuffling
- Coarse block shuffling
- Coarse full shuffling

We propose two techniques against hiding:

- Fine shuffling: Shuffle node adapts factor depending on processed information.
- Coarse shuffling: Extended attacker model and matching algorithm.

Adaptation to hiding countermeasures for belief-propagation-based attacks.

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. "Adapting Belief Propagation to Counter Shuffling of NTTs". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.1 (2023), pp. 60–88

Adapting Belief Propagation to Counter Shuffling of NTTs

Real-world attacks have to take countermeasures into account.

Important classes of countermeasures:

- Masking circumvented.
- Hiding prevents these attacks.

Ravi et al. [RPBC20] (ascending security):

- Fine shuffling
- Coarse block shuffling
- Coarse full shuffling

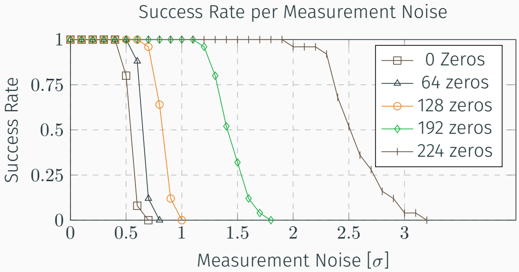
We propose two techniques against hiding:

- Fine shuffling: Shuffle node adapts factor depending on processed information.
- Coarse shuffling: Extended attacker model and matching algorithm.

Adaptation to hiding countermeasures for belief-propagation-based attacks.

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. "Adapting Belief Propagation to Counter Shuffling of NTTs". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.1 (2023), pp. 60–88

Evaluation in the leakage models provided by previous work [PPM17, PP19].



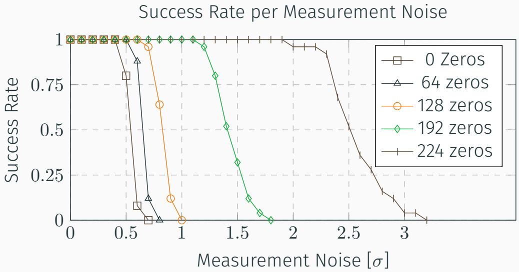
Attack	Secret Key	Noise Tolerance	Traces	Hiding considered
[PPM17]	Yes	$\sigma \leq 0.6$	1	No
[PP19]	No	$\sigma \leq 2.0$	1	No
This work	Yes	$\sigma \leq 1.7$ (3.1)	1-8	Yes

Noise tolerance increased from $\sigma \leq 0.6$ to $\sigma \leq 1.7$ ($\sigma \leq 3.1$).

Mike Hamburg, **Julius Hermelink**, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. “Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.4 (2021), pp. 88–113

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. “Adapting Belief Propagation to Counter Shuffling of NTTs”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.1 (2023), pp. 60–88

Evaluation in the leakage models provided by previous work [PPM17, PP19].



Attack	Secret Key	Noise Tolerance	Traces	Hiding considered
[PPM17]	Yes	$\sigma \leq 0.6$	1	No
[PP19]	No	$\sigma \leq 2.0$	1	No
This work	Yes	$\sigma \leq 1.7\ (3.1)$	1-8	Yes

Noise tolerance increased from $\sigma \leq 0.6$ to $\sigma \leq 1.7$ ($\sigma \leq 3.1$).

Mike Hamburg, **Julius Hermelink**, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. “Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.4 (2021), pp. 88–113

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. “Adapting Belief Propagation to Counter Shuffling of NTTs”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.1 (2023), pp. 60–88

Research Question 2

Learning with errors schemes recover the message from noisy coefficients:

- Observation whether introduced error causes failure: leaks information.
- Fujisaki-Okamoto (FO) transform achieves IND-CCA2 security.

Previous attacks:

- CCA to potentially cause failure; observe using SCA on comparison [GJN20, BDH+21].
- Or use fault against decoder to potentially cause failure and observe outcome [PP21].
- Require insufficiently protected comparison/decoder; reliable fault.

RQ: How can implementation attacks target the error correction and exploit decryption failure leakage in the presence of an FO-Transform?

Research Question 2

Learning with errors schemes recover the message from noisy coefficients:

- Observation whether introduced error causes failure: leaks information.
- Fujisaki-Okamoto (FO) transform achieves IND-CCA2 security.

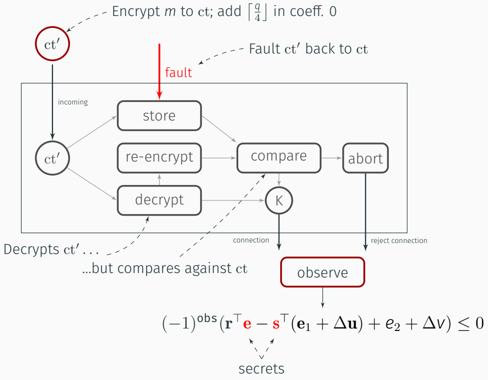
Previous attacks:

- CCA to potentially cause failure; observe using SCA on comparison [GJN20, BDH+21].
- Or use fault against decoder to potentially cause failure and observe outcome [PP21].
- Require insufficiently protected comparison/decoder; reliable fault.

RQ: How can implementation attacks target the error correction and exploit decryption failure leakage in the presence of an FO-Transform?

Fault-Enabled Chosen-Ciphertext Attacks

Introduce error through chosen ciphertext, then correct with fault.



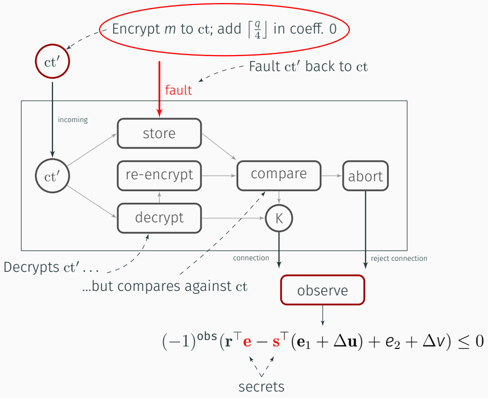
Our attack strategy:

- Ciphertext introduces error; fault corrects.
- Device decrypts `ct′`, but compares to `ct`.
- FO-comparison gives dec. failure oracle.
- Success can only occur if fault works.
- Allows for unreliable fault; attack surface over most of the execution time; may only target public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks

Introduce error through chosen ciphertext, then correct with fault.

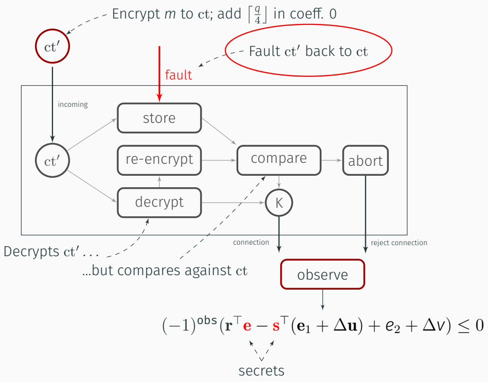


Our attack strategy:

- Ciphertext introduces error; fault corrects.
- Device decrypts `ct′`, but compares to `ct`.
- FO-comparison gives dec. failure oracle.
- Success can only occur if fault works.
- Allows for unreliable fault; attack surface over most of the execution time; may only target public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Introduce error through chosen ciphertext, then correct with fault.



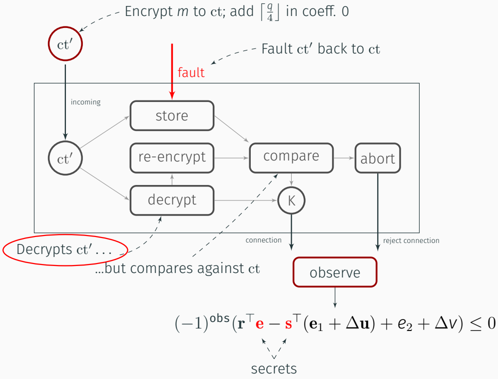
Our attack strategy:

- Ciphertext introduces error; fault corrects.
- Device decrypts `ct′`, but compares to `ct`.
- FO-comparison gives dec. failure oracle.
- Success can only occur if fault works.
- Allows for unreliable fault; attack surface over most of the execution time; may only target public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. “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.* Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks

Introduce error through chosen ciphertext, then correct with fault.



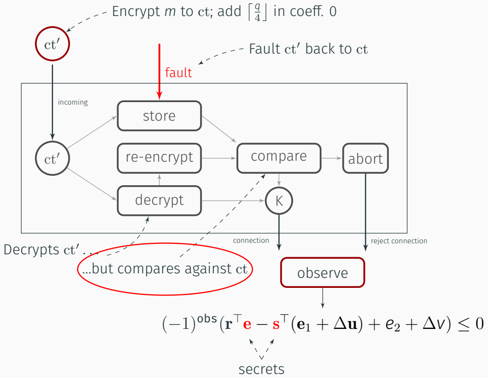
Our attack strategy:

- Ciphertext introduces error; fault corrects.
- Device decrypts `ct′`, but compares to `ct`.
- FO-comparison gives dec. failure oracle.
- Success can only occur if fault works.
- Allows for unreliable fault; attack surface over most of the execution time; may only target public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks

Introduce error through chosen ciphertext, then correct with fault.



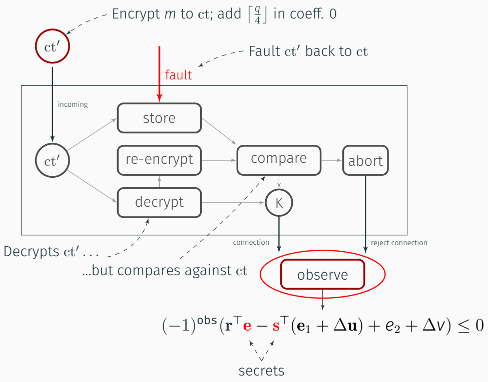
Our attack strategy:

- Ciphertext introduces error; fault corrects.
- Device decrypts `ct′`, but compares to `ct`.
- FO-comparison gives dec. failure oracle.
- Success can only occur if fault works.
- Allows for unreliable fault; attack surface over most of the execution time; may only target public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks

Introduce error through chosen ciphertext, then correct with fault.



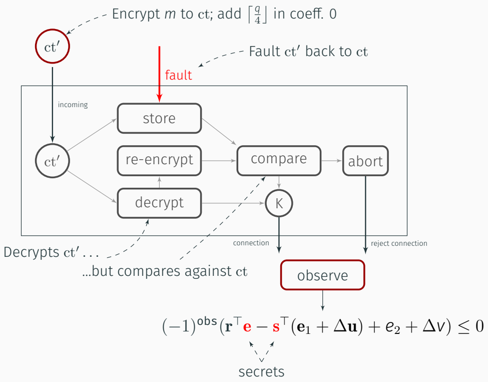
Our attack strategy:

- Ciphertext introduces error; fault corrects.
- Device decrypts `ct′`, but compares to `ct`.
- FO-comparison gives dec. failure oracle.
- Success can only occur if fault works.
- Allows for unreliable fault; attack surface over most of the execution time; may only target public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks

Introduce error through chosen ciphertext, then correct with fault.



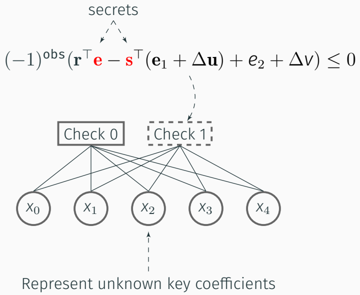
Our attack strategy:

- Ciphertext introduces error; fault corrects.
- Device decrypts `ct′`, but compares to `ct`.
- FO-comparison gives dec. failure oracle.
- Success can only occur if fault works.
- Allows for unreliable fault; attack surface over most of the execution time; may only target public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks – BP

We propose solving decryption failure inequalities using belief propagation.



Belief propagation inspired by [PP21]:

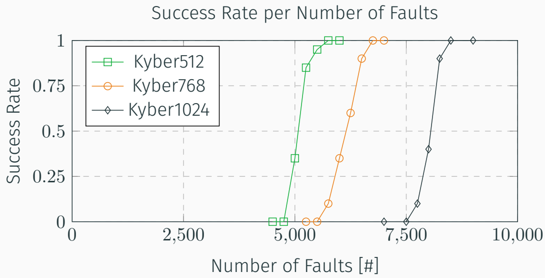
- Check nodes represent inequalities.
- Variable nodes represent unknown coefficients.
- Priors are binomial distributions of secrets.

Requires fewer inequalities while being more computationally efficient.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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.* Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks – Results

Gives a more general class of attacks resulting from our method.



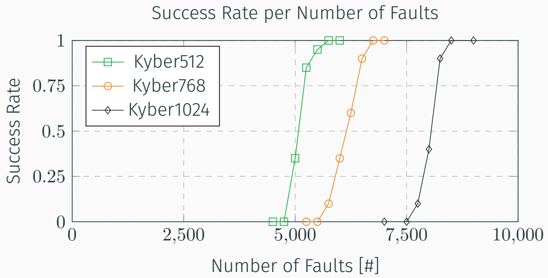
Attack	Type	Point of Attack	Requirement/Robustness
[GJN20]	Timing	Comparison	Non-constant time
[BDH+21]	SCA	Comparison	Leaking comparison
[PP21]	Fault	Decoding	Unprotected decoding
[DHP+22]	SCA	Comparison	Max. first order protection
[Del22]	Fault	Multiple	Unreliable/Imprecise fault
[Wei22]	SCA/ML	Multiple	Defeats 1th order masking
[FKK+22]	Rowhammer	Key Generation	KeyGen Failure Boosting
This work [HPP21]	Fault	Multiple	Unreliable fault

Allows for very unreliable fault, enlarges attack surface, only targets public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Fault-Enabled Chosen-Ciphertext Attacks – Results

Gives a more general class of attacks resulting from our method.



Attack	Type	Point of Attack	Requirement/Robustness
[GJN20]	**Timing**	**Comparison**	**Non-constant time**
[BDH+21]	**SCA**	**Comparison**	**Leaking comparison**
[PP21]	**Fault**	**Decoding**	**Unprotected decoding**
[DHP+22]	SCA	Comparison	Max. first order protection
[Del22]	Fault	Multiple	Unreliable/Imprecise fault
[Wei22]	SCA/ML	Multiple	Defeats 1th order masking
[FKK+22]	Rowhammer	Key Generation	KeyGen Failure Boosting
This work [HPP21]	Fault	Multiple	Unreliable fault

Allows for very unreliable fault, enlarges attack surface, only targets public data.

Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334

Research Question 3

Decryption failures leak information in form of inequalities:

- Exploited in wide variety of attacks including ours.
- Particularly hard to mitigate.
- Our attack strategy improved by [Del22], further enlarged attack surface.

Attacks require recovery method to solve for secret key:

- Partial information not considered; no security estimates.
- Error resistance increases #inequalities.
- General problem: combine belief propagation and algebraic methods?

RQ: Which techniques allow for key recovery from partially leaked decryption failure information?

Research Question 3

Decryption failures leak information in form of inequalities:

- Exploited in wide variety of attacks including ours.
- Particularly hard to mitigate.
- Our attack strategy improved by [Del22], further enlarged attack surface.

Attacks require recovery method to solve for secret key:

- Partial information not considered; no security estimates.
- Error resistance increases #inequalities.
- General problem: combine belief propagation and algebraic methods?

RQ: Which techniques allow for key recovery from partially leaked decryption failure information?

Research Question 3

Decryption failures leak information in form of inequalities:

- Exploited in wide variety of attacks including ours.
- Particularly hard to mitigate.
- Our attack strategy improved by [Del22], further enlarged attack surface.

Attacks require recovery method to solve for secret key:

- Partial information not considered; no security estimates.
- Error resistance increases #inequalities.
- General problem: combine belief propagation and algebraic methods?

RQ: Which techniques allow for key recovery from partially leaked decryption failure information?

Security Estimates for Error-Tolerant Key Recovery

Decryption failures in LWE leak information in form of inequalities.

Several methods to obtain secret from inequalities exist:

Method	Inequalities	Error Resistant	Estimates
Pessl and Prokop [PP21]	8000	No	No
Hermelink et al. [HPP21]	5750	No	No
Delvaux [Del22]	9000	Yes	No
Dachman-Soled et al. [DDGR20, DGHK22]	≥ 10000	No	Yes

How can we combine the advantages of previous methods?

[1] Used for key recovery from such decryption failure information on widely available hardware in a concrete attack.

Security Estimates for Error-Tolerant Key Recovery

Decryption failures in LWE leak information in form of inequalities.

Several methods to obtain secret from inequalities exist:

Method	Inequalities	Error Resistant	Estimates
Pessl and Prokop [PP21]	8000	No	No
Hermelink et al. [HPP21]	5750	No	No
Delvaux [Del22]	9000	Yes	No
Dachman-Soled et al. [DDGR20, DGHK22]	≥ 10000	No	Yes

How can we combine the advantages of previous methods?

[1] Used for key recovery from such decryption failure information on widely available hardware in a concrete attack.

Security Estimates for Error-Tolerant Key Recovery

Decryption failures in LWE leak information in form of inequalities.

Several methods to obtain secret from inequalities exist:

Method	Inequalities	Error Resistant	Estimates
Pessl and Prokop [PP21]	8000	No	No
Hermelink et al. [HPP21]	5750	No	No
Delvaux [Del22]	9000	Yes	No
Dachman-Soled et al. [DDGR20, DGHK22]	≥ 10000	No	Yes

How can we combine the advantages of previous methods?

[1] Used for key recovery from such decryption failure information on widely available hardware in a concrete attack.

Security Estimates for Error-Tolerant Key Recovery

Decryption failures in LWE leak information in form of inequalities.

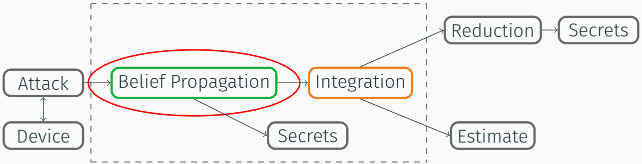
Several methods to obtain secret from inequalities exist:

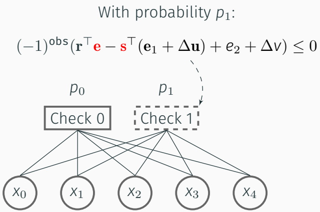
Method	Inequalities	Error Resistant	Estimates
Pessl and Prokop [PP21]	8000	No	No
Hermelink et al. [HPP21]	5750	No	No
Delvaux [Del22]	9000	Yes	No
Dachman-Soled et al. [DDGR20, DGHK22]	≥ 10000	No	Yes

How can we combine the advantages of previous methods?

[1] Used for key recovery from such decryption failure information on widely available hardware in a concrete attack.

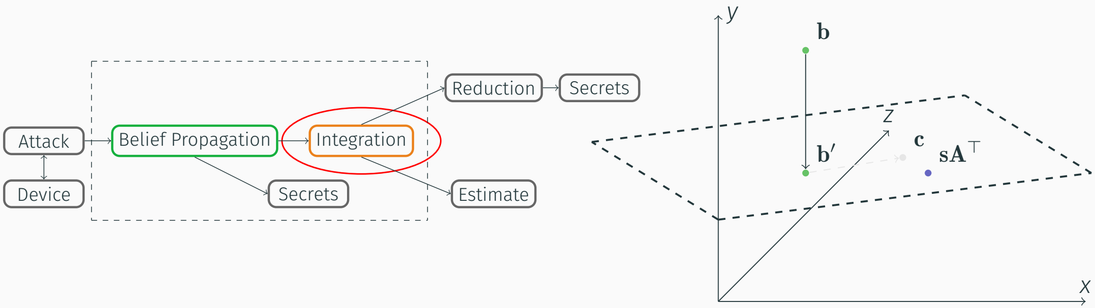
New error-tolerant belief propagation with two-step lattice integration:





Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. "Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023), pp. 287–317

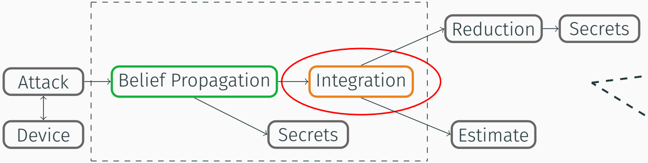
New error-tolerant belief propagation with two-step lattice integration:

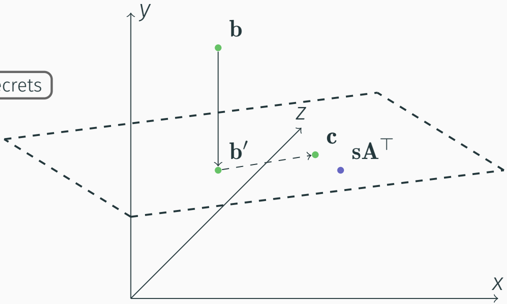


Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. “Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023), pp. 287–317

Security Estimates for Error-Tolerant Key Recovery

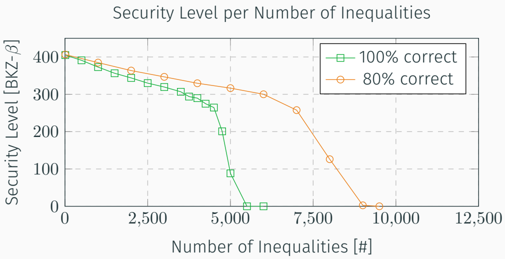
New error-tolerant belief propagation with two-step lattice integration:





Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. "Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023), pp. 287–317

Security Estimates for Error-Tolerant Key Recovery

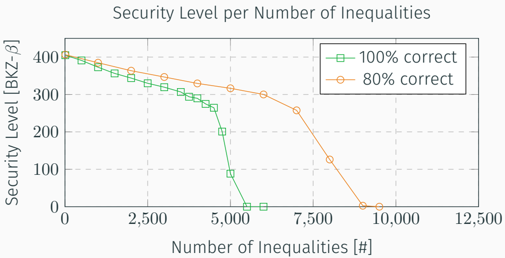


Method	Inequalities	Error resistant	Security Estimates
[PP21]	8000	No	No
[HPP21]	5750	No	No
[Del22]	9000	Yes	No
[DDGR20, DGHK22]	≥ 10000	No	Yes
This work [HMS+23b]	5500	Yes	Yes

Hybrid approach: fewer inequalities, error-tolerant, and provides security estimates.

Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. "Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023), pp. 287–317

Security Estimates for Error-Tolerant Key Recovery



Method	Inequalities	Error resistant	Security Estimates
[PP21]	8000	No	No
[HPP21]	5750	No	No
[Del22]	9000	Yes	No
[DDGR20, DGHK22]	≥ 10000	No	Yes
This work [HMS+23b]	5500	Yes	Yes

Hybrid approach: fewer inequalities, error-tolerant, and provides security estimates.

Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. "Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023), pp. 287–317

Contributions

NIST is standardizing ML-KEM – a lattice-based scheme.

Our work provides:

- Improvement on the state of the art in side-channel and fault attacks on lattice-based schemes.
- Attack strategies against lattice-based schemes enabling future attacks (e.g., [Del22]).
- Statistical and algebraic tools relevant to a variety of attacks (used, e.g., in [DHP+22]).
- Extended assessment on vulnerabilities of major building blocks of modern lattice-based key encapsulation mechanisms.

Contributions

NIST is standardizing ML-KEM – a lattice-based scheme.

Our work provides:

- Improvement on the state of the art in side-channel and fault attacks on lattice-based schemes.
- Attack strategies against lattice-based schemes enabling future attacks (e.g., [Del22]).
- Statistical and algebraic tools relevant to a variety of attacks (used, e.g., in [DHP+22]).
- Extended assessment on vulnerabilities of major building blocks of modern lattice-based key encapsulation mechanisms.

NIST is standardizing ML-KEM – a lattice-based scheme.

Our work provides:

- Improvement on the state of the art in side-channel and fault attacks on lattice-based schemes.
- Attack strategies against lattice-based schemes enabling future attacks (e.g., [Del22]).
- Statistical and algebraic tools relevant to a variety of attacks (used, e.g., in [DHP+22]).
- Extended assessment on vulnerabilities of major building blocks of modern lattice-based key encapsulation mechanisms.

Contributions

NIST is standardizing ML-KEM – a lattice-based scheme.

Our work provides:

- Improvement on the state of the art in side-channel and fault attacks on lattice-based schemes.
- Attack strategies against lattice-based schemes enabling future attacks (e.g., [Del22]).
- Statistical and algebraic tools relevant to a variety of attacks (used, e.g., in [DHP+22]).
- Extended assessment on vulnerabilities of major building blocks of modern lattice-based key encapsulation mechanisms.

Contributions

NIST is standardizing ML-KEM – a lattice-based scheme.

Our work provides:

- Improvement on the state of the art in side-channel and fault attacks on lattice-based schemes.
- Attack strategies against lattice-based schemes enabling future attacks (e.g., [Del22]).
- Statistical and algebraic tools relevant to a variety of attacks (used, e.g., in [DHP+22]).
- Extended assessment on vulnerabilities of major building blocks of modern lattice-based key encapsulation mechanisms.

Publications

[HHP+21] Mike Hamburg, **Julius Hermelink**, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. “Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.4 (2021), pp. 88–113. URL: `https://doi.org/10.46586/tches.v2021.i4.88-113`

[HSST23] **Julius Hermelink**, Silvan Streit, Emanuele Strieder, and Katharina Thieme. “Adapting Belief Propagation to Counter Shuffling of NTTs”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.1 (2023), pp. 60–88. URL: `https://doi.org/10.46586/tches.v2023.i1.60-88`

[HMS+23b] **Julius Hermelink**, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. “Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.4 (2023), pp. 287–317. URL: `https://doi.org/10.46586/tches.v2023.i4.287-317`

[HPS+20] **Julius Hermelink**, Thomas Pöppelmann, Marc Stöttinger, Yi Wang, and Yong Wan. “Quantum safe authenticated key exchange protocol for automotive application”. In: *18-th escar Europe : The World’s Leading Automotive Cyber Security Conference (Konferenzveröffentlichung)*. 2020

[HPP21] **Julius Hermelink**, Peter Pessl, and Thomas Pöppelmann. “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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334. URL: `https://doi.org/10.1007/978-3-030-92518-5_15`

References (1)

[Aut23] Chromium Blog Authors. *Protecting Chrome Traffic with Hybrid Kyber KEM*. 2023. URL: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.

[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". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.3 (2021), pp. 334–359. URL: https://doi.org/10.46586/tches.v2021.i3.334-359.

[DDGR20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. "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*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 329–358. URL: https://doi.org/10.1007/978-3-030-56880-1_12.

[Del22] Jeroen Delvaux. "Roulette: A Diverse Family of Feasible Fault Attacks on Masked Kyber". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.4 (2022), pp. 637–660. URL: https://doi.org/10.46586/tches.v2022.i4.637-660.

[DGHK22] Dana Dachman-Soled, Huijing Gong, Tom Hanson, and Hunter Kippen. "Revisiting Security Estimation for LWE with Hints from a Geometric Perspective". In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14085. Lecture Notes in Computer Science. Springer, 2022, pp. 748–781. URL: https://doi.org/10.1007/978-3-031-38554-4_24.

References (2)

[DHP+22] Jan-Pieter D'Anvers, Daniel Heinz, Peter Pessl, Michiel Van Beirendonck, and Ingrid Verbauwhede. "Higher-Order Masked Ciphertext Comparison for Lattice-Based Cryptography". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.2 (2022), pp. 115–139. URL: `https://doi.org/10.46586/tches.v2022.i2.115-139`.

[EA24] Apple Security Engineering and Architecture. *iMessage with PQ3: The new state of the art in quantum-secure messaging at scale*. 2024. URL: `https://security.apple.com/blog/imessage-pq3/`.

[FKK+22] Michael Fahr, Hunter Kippen, Andrew Kwong, Thinh Dang, Jacob Lichtinger, Dana Dachman-Soled, Daniel Genkin, Alexander Nelson, Ray A. Perlner, Arkady Yerukhimovich, and Daniel Apon. "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, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi. ACM, 2022, pp. 979–993. URL: `https://doi.org/10.1145/3548606.3560673`.

[GJN20] Qian Guo, Thomas Johansson, and Alexander Nilsson. "A Key-Recovery Timing Attack on Post-quantum Primitives Using the Fujisaki-Okamoto Transformation and Its Application on FrodoKEM". In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 359–386. URL: `https://doi.org/10.1007/978-3-030-56880-1_13`.

[HHP+21] Mike Hamburg, Julius Hermelink, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. "Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.4 (2021), pp. 88–113. URL: `https://doi.org/10.46586/tches.v2021.i4.88-113`.

References (3)

[HMS+23b] Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. "Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.4 (2023), pp. 287–317. URL: https://doi.org/10.46586/tches.v2023.i4.287-317.

[HPP21] Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "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*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, 2021, pp. 311–334. URL: https://doi.org/10.1007/978-3-030-92518-5_15.

[HPS+20] Julius Hermelink, Thomas Pöppelmann, Marc Stöttinger, Yi Wang, and Yong Wan. "Quantum safe authenticated key exchange protocol for automotive application". In: *18-th escar Europe : The World's Leading Automotive Cyber Security Conference (Konferenzveröffentlichung)*. 2020.

[HSST23] Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. "Adapting Belief Propagation to Counter Shuffling of NTTs". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.1 (2023), pp. 60–88. URL: https://doi.org/10.46586/tches.v2023.i1.60-88.

[Kre23] Ehren Kret. *Quantum Resistance and the Signal Protocol*. 2023. URL: https://signal.org/blog/pqxdh/.

References (4)

[PP19] Peter Pessl and Robert Primas. “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*. Ed. by Peter Schwabe and Nicolas Thériault. Vol. 11774. Lecture Notes in Computer Science. Springer, 2019, pp. 130–149. URL: `https://doi.org/10.1007/978-3-030-30530-7_7`.

[PP21] Peter Pessl and Lukas Prokop. “Fault Attacks on CCA-secure Lattice KEMs”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.2 (2021), pp. 37–60. URL: `https://doi.org/10.46586/tches.v2021.i2.37-60`.

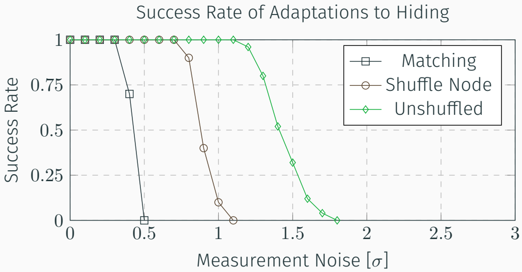
[PPM17] Robert Primas, Peter Pessl, and Stefan Mangard. “Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption”. In: *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. Lecture Notes in Computer Science. Springer, 2017, pp. 513–533. URL: `https://doi.org/10.1007/978-3-319-66787-4_25`.

[RPBC20] Prasanna Ravi, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay. “On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT - A Performance Evaluation Study over Kyber and Dilithium on the ARM Cortex-M4”. In: *Security, Privacy, and Applied Cryptography Engineering - 10th International Conference, SPACE 2020, Kolkata, India, December 17-21, 2020, Proceedings*. Ed. by Lejla Batina, Stjepan Picek, and Mainack Mondal. Vol. 12586. Lecture Notes in Computer Science. Springer, 2020, pp. 123–146. URL: `https://doi.org/10.1007/978-3-030-66626-2_7`.

[Wei22] Andreas Weik. “Machine-Learning-based Side-Channel Attacks on Lattice-based Key Encapsulation Mechanisms”. Master’s Thesis at the Technical University of Munich 2022. Oct. 2022.

Adapting Belief Propagation – Results

Real-world attacks have to take countermeasures into account.



Our results show that

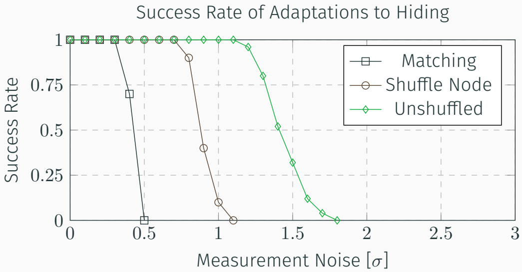
- Attacks not fully prevented by hiding countermeasures.
- However, noise tolerance reduced.
- Strongest from of shuffling protects requires vast computational resources.
- Large-scale adversaries might even circumvent coarse full shuffling.

Several hiding countermeasures can be circumvented; protected NTT still vulnerable.

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. “Adapting Belief Propagation to Counter Shuffling of NTTs”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.1 (2023), pp. 60–88

Adapting Belief Propagation – Results

Real-world attacks have to take countermeasures into account.



Our results show that

- Attacks not fully prevented by hiding countermeasures.
- However, noise tolerance reduced.
- Strongest from of shuffling protects requires vast computational resources.
- Large-scale adversaries might even circumvent coarse full shuffling.

Several hiding countermeasures can be circumvented; protected NTT still vulnerable.

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme. "Adapting Belief Propagation to Counter Shuffling of NTTs". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.1 (2023), pp. 60–88