From: Prasanna Ravi <prasanna.ravi@ntu.edu.sg> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results
Date: Tuesday, June 14, 2022 02:32:28 AM ET

Dear all,

We would like to share our recent work titled "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results" available at https://eprint.iacr.org/2022/737

Please find a short abstract of our work below:
In this work, we present a systematic study of Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA) on structured lattice-based schemes, with focus on Kyber Key Encapsulation Mechanism (KEM) and Dilithium signature scheme. We attempt to present a survey and classification of existing SCA/FIA on Kyber and Dilithium. Given the wide variety of reported attacks, simultaneous protection against all the attacks requires implementing customized protections/countermeasures for both Kyber and Dilithium. We therefore present a range of customized countermeasures, capable of providing defenses/mitigations against existing SCA/FIA. We implement the presented countermeasures within two well-known public software libraries for PQC - (1) **pqm4** library for the ARM Cortex-M4 based microcontroller and (2) **liboqs** library for the Raspberry Pi 3 Model B Plus based on the ARM Cortex-A53 processor. Our performance evaluation reveals that the presented custom countermeasures incur reasonable performance overheads, on both the evaluated embedded platforms. We therefore believe our work argues for usage of custom countermeasures within real-world implementations of lattice-based schemes, either in a standalone manner, or as reinforcements to generic countermeasures such as masking.
DETECTION-BASED COUNTERMEASURES (SANITY CHECK) AGAINST SCA/FIA ASSISTED CHOSEN-CIPHERTEXT ATTACKS:
We would like to particularly highlight two detection-based countermeasures against SCA/FIA assisted chosen-ciphertext attacks on LWE/LWR-based KEMs, that are discussed in this work. The core idea is to detect a malicious ciphertext and immediately refresh the long-term secret key to prevent further exposure. The first countermeasure is the ciphertext sanity check (Section 5.1.1) which filters low entropy ciphertexts (also proposed in [1]), and the second countermeasure is the message polynomial sanity check countermeasure which can detect malicious ciphertexts that work based on border-failure strategies. The recent talk titled "Surviving the FO-Calypse" by Azouaoui et al. [2] highlighted the difficulty of detecting

ciphertexts that work based on border-failure strategies. In this respect, we believe our proposed message polynomial sanity check countermeasure could be an interesting low-cost approach to thwart most if not all the proposed SCA/FIA assisted chosen-ciphertext attacks.

We appreciate any feedback/suggestions/discussions from the community in this topic.

With Thanks and Regards,
The Team.

References:

[1] Xu, Zhuang, Owen Michael Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers (2021).

[2] Surviving the FO-Calypse: Securing PQC Implementations in Practice, Melissa Azouaoui, Joppe W. Bos, Björn Fay, Marc Gourjon, Yulia Kuzovkova, Joost Renes, Tobias Schneider, Christine van Vredendaal in Collaboration with UCLouvain: Olivier Bronchain, Clément Hoffmann, François-Xavier Standaert, Real World Crypto Symposium, April 2022, Available athttps://iacr.org/submit/files/slides/2022/rwc/rwc2022/48/slides.pdf

---

CONFIDENTIALITY: This email is intended solely for the person(s) named and may be confidential and/or privileged. If you are not the intended recipient, please delete it, notify us and do not copy, use, or disclose its contents.

Towards a sustainable earth: Print only when necessary. Thank you.

From: Markku-Juhani O. Saarinen <mjos.crypto@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Prasanna Ravi <prasanna.ravi@ntu.edu.sg>
Subject: [pqc-forum] Re: Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results
Date: Tuesday, June 14, 2022 05:58:09 AM ET

On Tuesday, June 14, 2022 at 7:31:23 AM UTC+1 Prasanna Ravi wrote:

> Dear all,
>
> We would like to share our recent work titled "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results" available at https://eprint.iacr.org/2022/737

Dear Prasanna Ravi et al,

Thanks for this nice and useful survey! I especially liked the categorization of side-channel and fault attacks. However, I'd like to make some points about side-channel security metrics in the NIST context.

When presenting new side-channel countermeasures (Section 5), it would be useful to include a quantitative evaluation of their effectiveness. For example, Table 3 makes simple yes/no claims, but I can't see details of the experimental set-up -- actual traces obtained with an oscilloscope or what the PASS/FAIL metric is. Hence the performance impact "overhead" percentages are less meaningful than they may first seem.

I realize that the countermeasures presented are intended to be incremental contributions to the research literature, and no definitive security claims are being made. However, I should point out that a maker of commercial NIST-compliant cryptography modules would not be able to proceed like this. We know that if we claim side-channel resistance, a third-party testing laboratory will eventually be obliged to test the entire module against such claims. Specifically, in NIST (FIPS 140-3) context -- in the long run -- this is likely to mean at least ISO 17825:202x type "non-invasive attack mitigation testing," as that standard is referenced in Annex F of 19790:2022 and also in Draft SP 800-140F Rev 1. This test should not be seen as a sufficient measure for security, but it is a piece of the required evidence for such a claim in the FIPS context. Many academics also use TVLA (similar to ISO 17825) as final sign-off evidence when presenting side-channel secure implementations.

Common Criteria evaluations commonly use a slightly different point-based "attack potential" approach, which can also indicate the complexity of key recovery and resistance to fault attacks.

Furthermore, all components that deal with CSPs must be protected, not just core decapsulation and signature functions -- but also key management operations. Hence it is unclear if libraries like pqm4 or liboqs -- that transfer, store, and even manipulate secret keys in plaintext -- can be made side-channel secure without very substantial changes. As far as I can see, the presented work (and related [47]) focuses on the protection of the NTT subcomponent; I can definitely say that protecting this component alone would not be sufficient to help a Dilithium or Kyber module (as a whole) pass a basic TVLA.

Finally, I'd note that one performs CSP analysis also to avoid false positives in such testing. For example, this work suggests that the "t0" in Dilithium is a CSP ("sensitive variable" -- Sect 7.4); however, I'd opine that the leakage of this half of "t" can be treated as a false positive in side-channel testing. The variable "t0" is an SSP, even though it is transmitted as a part of the secret key in order to minimize the public key size (Section 1.2 of the Dilithium 3.1 spec).
Cheers,

- markku

Dr. Markku-Juhani O. Saarinen

Senior Cryptography Architect

PQShield Ltd

E:mjos@pqshield.com

W:www.pqshield.com

> **Please find a short abstract of our work below:**
> In this work, we present a systematic study of Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA) on structured lattice-based schemes, with focus on Kyber Key Encapsulation Mechanism (KEM) and Dilithium signature scheme. We attempt to present a survey and classification of existing SCA/FIA on Kyber and Dilithium. Given the wide variety of reported attacks, simultaneous protection against all the attacks requires implementing customized protections/countermeasures for both Kyber and Dilithium. We therefore present a range of customized countermeasures, capable of providing defenses/

mitigations against existing SCA/FIA. We implement the presented countermeasures within two well-known public software libraries for PQC - (1) **pqm4** library for the ARM Cortex-M4 based microcontroller and (2) **liboqs** library for the Raspberry Pi 3 Model B Plus based on the ARM Cortex-A53 processor. Our performance evaluation reveals that the presented custom countermeasures incur reasonable performance overheads, on both the evaluated embedded platforms. We therefore believe our work argues for usage of custom countermeasures within real-world implementations of lattice-based schemes, either in a standalone manner, or as reinforcements to generic countermeasures such as masking.

DETECTION-BASED COUNTERMEASURES (SANITY CHECK) AGAINST SCA/FIA ASSISTED CHOSEN-CIPHERTEXT ATTACKS:

We would like to particularly highlight two detection-based countermeasures against SCA/FIA assisted chosen-ciphertext attacks on LWE/LWR-based KEMs, that are discussed in this work. The core idea is to detect a malicious ciphertext and immediately refresh the long-term secret key to prevent further exposure. The first countermeasure is the ciphertext sanity check (Section 5.1.1) which filters low entropy ciphertexts (also proposed in [1]), and the second countermeasure is the message polynomial sanity check countermeasure which can detect malicious ciphertexts that work based on border-failure strategies. The recent talk titled "Surviving the FO-Calypse" by Azouaoui et al. [2] highlighted the difficulty of detecting ciphertexts that work based on border-failure strategies. In this respect, we believe our proposed message polynomial sanity check countermeasure could be an interesting low-cost approach to thwart most if not all the proposed SCA/FIA assisted chosen-ciphertext attacks.

We appreciate any feedback/suggestions/discussions from the community in this topic.

With Thanks and Regards,

The Team.

References:

[1] Xu, Zhuang, Owen Michael Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers (2021).

[2] Surviving the FO-Calypse: Securing PQC Implementations in Practice, Melissa Azouaoui, Joppe W. Bos, Björn Fay, Marc Gourjon, Yulia Kuzovkova, Joost Renes, Tobias Schneider, Christine van Vredendaal in Collaboration with UCLouvain: Olivier Bronchain, Clément Hoffmann, François-Xavier Standaert, Real World Crypto Symposium, April 2022, Available athttps://iacr.org/submit/files/slides/2022/rwc/rwc2022/48/slides.pdf

> contents.
> Towards a sustainable earth: Print only when necessary. Thank you.

--

From: Prasanna Ravi <prasanna.ravi@ntu.edu.sg> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results
Date: Friday, December 02, 2022 11:31:19 PM ET

Dear All,
We would like to share our recent work titled "Side-channelandFault-injectionattacksoverLattice-basedPost quantumSchemes(Kyber,Dilithium):SurveyandNewResults" available athttps://eprint.iacr.org/2022/737 (revised version).

We have focused on presenting a detailed survey of side-channel attacks and fault attacks on Kyber and Dilithium. Given the variety of attacks on Kyber and Dilithium, we have attempted to build a taxonomy for attacks on Kyber and Dilithium, classifying based on different characteristics such as profiled/non-profiled, number of traces, attack difficulty etc. To the best of our knowledge, we have tried to include all SCA and FIA reported on Kyber and Dilithium till date. Our hope is that this material will be useful, especially for anyone to navigate the landscape of SCA and FIA on lattice-based schemes.
As an added contribution, our work also collates ideas for several countermeasures proposed against different attacks by prior works, and we have also implemented some of these custom countermeasures against SCA and FIA on the reference implementation of Kyber and Dilithium. These custom countermeasures could be implemented as an additional protection on top of masked implementations as well. The software is available in the following link:
https://github.com/PRASANNA-RAVI/SCA_FIA_Protected_Kyber_Dilithium
Since the countermeasures are implemented in C, they can be ported to different libraries such as the pqm4 [1] and LibOQS [2]. We would like to encourage the community to evaluate our protected implementations and feedback on our work!
With Thanks and Regards,
Prasanna Ravi on behalf of the Team (Anupam Chattopadhyay, Jan Pieter D'Anvers, Anubhab Baksi).
References:
[1] https://github.com/mupq/pqm4
[2] https://github.com/open-quantum-safe/liboqs

From: Prasanna Ravi <prasanna.ravi@ntu.edu.sg>
Sent: Thursday, December 1, 2022 8:40 AM
To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>

Prasanna Ravi <prasanna.ravi@ntu.edu.sg>

Subject: Re: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results

Dear All,

We would like to share our recent work titled "Side-channelandFault-injectionattacksoverLattice-basedPost quantumSchemes(Kyber,Dilithium):SurveyandNewResults" available athttps://eprint.iacr.org/2022/737 (revised version).

We have focused on presenting a detailed survey of side-channel attacks and fault attacks on Kyber and Dilithium. Given the variety of attacks on Kyber and Dilithium, we have attempted to build a taxonomy for attacks on Kyber and Dilithium, classifying based on different characteristics such as profiled/non-profiled, number of traces, attack difficulty etc. To the best of our knowledge, we have tried to include all SCA and FIA reported on Kyber and Dilithium till date. Our hope is that this material will be useful, especially for anyone to navigate the landscape of SCA and FIA on lattice-based schemes.

As an added contribution, our work also collates ideas for several countermeasures proposed against different attacks by prior works, and we have also implemented some of these custom countermeasures against SCA and FIA on the reference implementation of Kyber and Dilithium. These custom countermeasures could be implemented as an additional protection on top of masked implementations as well. The software is available in the following link:
https://github.com/PRASANNA-RAVI/SCA_FIA_Protected_Kyber_Dilithium
Since the countermeasures are implemented in C, they can be ported to different libraries such as the pqm4 [1] and LibOQS [2]. We would like to encourage the community to evaluate our protected implementations and feedback on our work!
With Thanks and Regards,

Prasanna Ravi on behalf of the Team (Anupam Chattopadhyay, Jan Pieter D'Anvers, Anubhab Baksi).

References:

[1] https://github.com/mupq/pqm4

[2] https://github.com/open-quantum-safe/liboqs

From: Markku-Juhani Olavi Saarinen <mjos@iki.fi>
Sent: Tuesday, June 14, 2022 5:24 PM
To: Prasanna Ravi <prasanna.ravi@ntu.edu.sg>
Cc: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results

Prasanna Ravi et al,

Thanks for this nice and useful review! I especially liked the categorization of side-channel and fault attacks. I'd like to make some points about side-channel security claims.

When presenting new side-channel countermeasures (Section 5), it would be prudent to include a quantitative evaluation of their effectiveness. For example, Table 3 makes simple yes/no claims, but I can't see details of the experimental set-up -- actual traces obtained with an oscilloscope or what the PASS/FAIL metric is. Hence the performance impact "overhead" percentages are less meaningful than they may first seem.

I realize that the countermeasures presented are intended to be incremental contributions to the research literature, and no definitive security claims are being made. However, I should point out that a maker of commercial NIST-compliant cryptography modules would not be able to proceed like this. We know that if we claim side-channel resistance, a third-party testing laboratory will be obliged to test the entire module against such claims. Specifically, in NIST (FIPS 140-3) context -- in the long run -- this is likely to mean at least ISO 17825:202x type "non-invasive attack mitigation testing," as that standard is referenced in Annex F of 19790:2022 and also in Draft SP 800-140F Rev 1. This test should not be seen as a sufficient measure for security, but it is a piece of the required evidence for such a claim in the FIPS context. Many academics also use TVLA (similar to ISO 17825) as final sign-off evidence when presenting side-channel secure implementations.

Common Criteria evaluations commonly use a slightly different point-based "attack potential" approach, which can also indicate the complexity of key recovery and resistance to fault attacks.

Furthermore, all components that deal with CSPs must be protected, not just core decapsulation and signature functions -- but also key management operations. Hence it is unclear if libraries like pqm4 or liboqs -- that transfer, store, and even manipulate secret keys in plaintext -- can be made side-channel secure without very substantial changes. As far as I can see the presented work only discusses SCA protection of the NTT subcomponent; I can definitely say this alone would not make a Dilithium module (as a whole) pass basic TVLA. Finally, I'd note that one performs CSP analysis also to avoid false positives. For example, this work suggests that the "t0" in Dilithium is a CSP ("sensitive variable" -- Sect 7.4); however, I'd opine that the leakage of this half of "t" can be treated as a false positive in side-channel testing. The variable "t0" is an SSP, even though it is transmitted as a part of the secret key in order to minimize the public key size (Section 1.2 of the Dilithium 3.1 spec).

Cheers,

- markku

Dr. Markku-Juhani O. Saarinen
Senior Cryptography Architect

PQShield Ltd

E:mjos@pqshield.com
W:www.pqshield.com

PQShield is a private limited company registered in England and Wales with registered number 11388567. PQShield's registered office is Prama House, 276 Banbury Rd., OX2 7HT Oxford, UK. This email and any attachment contain information that is private and confidential and is intended for the addressee only. If you are not an addressee, you are not authorised to read, copy or use the email or any attachment, If you have received this email in error, please notify the sender by return email and then destroy it. Any views expressed in this e-mail are not that of PQShield Ltd or its employees unless specifically stated. As e-mail communications are known to be unsecure, we accept no liability for any legal issues that may arise as a result of this e-mail. It is advised that you carry out a virus check with your own software before opening any attachments sent to you.

On Tue, Jun 14, 2022 at 7:31 AM 'Prasanna Ravi' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> Dear all,
>
> We would like to share our recent work titled "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results" available at https://eprint.iacr.org/2022/737
> **Please find a short abstract of our work below:**
> In this work, we present a systematic study of Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA) on structured lattice-based schemes, with focus on Kyber Key

Encapsulation Mechanism (KEM) and Dilithium signature scheme. We attempt to present a survey and classification of existing SCA/FIA on Kyber and Dilithium. Given the wide variety of reported attacks, simultaneous protection against all the attacks requires implementing customized protections/countermeasures for both Kyber and Dilithium. We therefore present a range of customized countermeasures, capable of providing defenses/ mitigations against existing SCA/FIA. We implement the presented countermeasures within two well-known public software libraries for PQC - (1) **pqm4** library for the ARM Cortex-M4 based microcontroller and (2) **liboqs** library for the Raspberry Pi 3 Model B Plus based on the ARM Cortex-A53 processor. Our performance evaluation reveals that the presented custom countermeasures incur reasonable performance overheads, on both the evaluated embedded platforms. We therefore believe our work argues for usage of custom countermeasures within real-world implementations of lattice-based schemes, either in a standalone manner, or as reinforcements to generic countermeasures such as masking.

DETECTION-BASED COUNTERMEASURES (SANITY CHECK) AGAINST SCA/FIA ASSISTED CHOSEN-CIPHERTEXT ATTACKS:

We would like to particularly highlight two detection-based countermeasures against SCA/ FIA assisted chosen-ciphertext attacks on LWE/LWR-based KEMs, that are discussed in this work. The core idea is to detect a malicious ciphertext and immediately refresh the long-term secret key to prevent further exposure. The first countermeasure is the ciphertext sanity check (Section 5.1.1) which filters low entropy ciphertexts (also proposed in [1]), and the second countermeasure is the message polynomial sanity check countermeasure which can detect malicious ciphertexts that work based on border-failure strategies. The recent talk titled "Surviving the FO-Calypse" by Azouaoui et al. [2] highlighted the difficulty of detecting ciphertexts that work based on border-failure strategies. In this respect, we believe our proposed message polynomial sanity check countermeasure could be an interesting low-cost approach to thwart most if not all the proposed SCA/FIA assisted chosen-ciphertext attacks.

We appreciate any feedback/suggestions/discussions from the community in this topic.

With Thanks and Regards,

The Team.

References:

[1] Xu, Zhuang, Owen Michael Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers (2021).

[2] Surviving the FO-Calypse: Securing PQC Implementations in Practice, Melissa Azouaoui, Joppe W. Bos, Björn Fay, Marc Gourjon, Yulia Kuzovkova, Joost Renes, Tobias Schneider, Christine van Vredendaal in Collaboration with UCLouvain: Olivier Bronchain, Clément

> Hoffmann, François-Xavier Standaert, Real World Crypto Symposium, April 2022, Available athttps://iacr.org/submit/files/slides/2022/rwc/rwc2022/48/slides.pdf
>
> ---
>
> CONFIDENTIALITY: This email is intended solely for the person(s) named and may be confidential and/or privileged. If you are not the intended recipient, please delete it, notify us and do not copy, use, or disclose its contents.
> Towards a sustainable earth: Print only when necessary. Thank you.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/HK0PR01MB22279EA0663248B5A486073AC7AA9%40HK0PR01MB2227.apcprd01.prod.exchangelabs.com.

From: Prasanna Ravi <prasanna.ravi@ntu.edu.sg> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results
Date: Saturday, December 03, 2022 06:40:22 AM ET

Dear All,

The link for protected implementations of Kyber and Dilithium is available in https://github.com/PRASANNA-RAVI/SCA_FIA_Protected_Kyber_Dilithium

The link was accidentally private, but now it should be accessible! Apologies for inconvenience caused.

With Thanks and Regards,

Prasanna Ravi.

From: 'Prasanna Ravi' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Saturday, December 3, 2022 12:30 PM
To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results

Dear All,
We would like to share our recent work titled "Side-channelandFault-injectionattacksoverLattice-basedPost quantumSchemes(Kyber,Dilithium):SurveyandNewResults" available athttps://eprint.iacr.org/2022/737 (revised version).
We have focused on presenting a detailed survey of side-channel attacks and fault attacks on Kyber and Dilithium. Given the variety of attacks on Kyber and Dilithium, we have attempted to build a taxonomy for attacks on Kyber and Dilithium, classifying based on different characteristics such as profiled/non-profiled, number of traces, attack difficulty etc. To the best of our knowledge, we have tried to include all SCA and FIA reported on Kyber and Dilithium till date. Our hope is that this material will be useful, especially for anyone to navigate the landscape of SCA and FIA on lattice-based schemes.
As an added contribution, our work also collates ideas for several countermeasures proposed against different attacks by prior works, and we have also implemented some of these

custom countermeasures against SCA and FIA on the reference implementation of Kyber and Dilithium. These custom countermeasures could be implemented as an additional protection on top of masked implementations as well. The software is available in the following link:
https://github.com/PRASANNA-RAVI/SCA_FIA_Protected_Kyber_Dilithium
Since the countermeasures are implemented in C, they can be ported to different libraries such as the pqm4 [1] and LibOQS [2]. We would like to encourage the community to evaluate our protected implementations and feedback on our work!
With Thanks and Regards,
Prasanna Ravi on behalf of the Team (Anupam Chattopadhyay, Jan Pieter D'Anvers, Anubhab Baksi).
References:
[1] https://github.com/mupq/pqm4
[2] https://github.com/open-quantum-safe/liboqs

From: Prasanna Ravi <prasanna.ravi@ntu.edu.sg>
Sent: Thursday, December 1, 2022 8:40 AM
To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results

Dear All,

We would like to share our recent work titled "Side-channelandFault-injectionattacksoverLattice-basedPost quantumSchemes(Kyber,Dilithium):SurveyandNewResults" available athttps://eprint.iacr.org/2022/737 (revised version).

We have focused on presenting a detailed survey of side-channel attacks and fault attacks on Kyber and Dilithium. Given the variety of attacks on Kyber and Dilithium, we have attempted to build a taxonomy for attacks on Kyber and Dilithium, classifying based on different characteristics such as profiled/non-profiled, number of traces, attack difficulty etc. To the best of our knowledge, we have tried to include all SCA and FIA reported on Kyber and Dilithium till date. Our hope is that this material will be useful, especially for anyone to navigate the landscape of SCA and FIA on lattice-based schemes.

As an added contribution, our work also collates ideas for several countermeasures proposed against different attacks by prior works, and we have also implemented some of these custom countermeasures against SCA and FIA on the reference implementation of Kyber and

Dilithium. These custom countermeasures could be implemented as an additional protection on top of masked implementations as well. The software is available in the following link:
https://github.com/PRASANNA-RAVI/SCA_FIA_Protected_Kyber_Dilithium
Since the countermeasures are implemented in C, they can be ported to different libraries such as the pqm4 [1] and LibOQS [2]. We would like to encourage the community to evaluate our protected implementations and feedback on our work!
With Thanks and Regards,

Prasanna Ravi on behalf of the Team (Anupam Chattopadhyay, Jan Pieter D'Anvers, Anubhab Baksi).

References:

[1] https://github.com/mupq/pqm4

[2] https://github.com/open-quantum-safe/liboqs

From: Markku-Juhani Olavi Saarinen <mjos@iki.fi>
Sent: Tuesday, June 14, 2022 5:24 PM
To: Prasanna Ravi <prasanna.ravi@ntu.edu.sg>
Cc: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Study of Side-Channel and Fault Injection Attacks over Lattice-based Schemes: Survey and New Results

Prasanna Ravi et al,

Thanks for this nice and useful review! I especially liked the categorization of side-channel and fault attacks. I'd like to make some points about side-channel security claims.

When presenting new side-channel countermeasures (Section 5), it would be prudent to include a quantitative evaluation of their effectiveness. For example, Table 3 makes simple yes/no claims, but I can't see details of the experimental set-up -- actual traces obtained with an oscilloscope or what the PASS/FAIL metric is. Hence the performance impact "overhead" percentages are less meaningful than they may first seem.

I realize that the countermeasures presented are intended to be incremental contributions to the research literature, and no definitive security claims are being made. However, I should point out that a maker of commercial NIST-compliant cryptography modules would not be able to proceed like this. We know that if we claim side-channel resistance, a third-party testing laboratory will be obliged to test the entire module against such claims. Specifically, in NIST (FIPS 140-3) context -- in the long run -- this is likely to mean at least ISO 17825:202x type "non-invasive attack mitigation testing," as that standard is referenced in Annex F of 19790:2022 and also in Draft SP 800-140F Rev 1. This test should not be seen as a sufficient measure for security, but it is a piece of the required evidence for such a claim in the FIPS context. Many academics also use TVLA (similar to ISO 17825) as final sign-off evidence when presenting side-channel secure implementations.

Common Criteria evaluations commonly use a slightly different point-based "attack potential" approach, which can also indicate the complexity of key recovery and resistance to fault attacks.

Furthermore, all components that deal with CSPs must be protected, not just core decapsulation and signature functions -- but also key management operations. Hence it is unclear if libraries like pqm4 or liboqs -- that transfer, store, and even manipulate secret keys in plaintext -- can be made side-channel secure without very substantial changes. As far as I can see the presented work only discusses SCA protection of the NTT subcomponent; I can definitely say this alone would not make a Dilithium module (as a whole) pass basic TVLA. Finally, I'd note that one performs CSP analysis also to avoid false positives. For example, this work suggests that the "t0" in Dilithium is a CSP ("sensitive variable" -- Sect 7.4); however, I'd opine that the leakage of this half of "t" can be treated as a false positive in side-channel testing. The variable "t0" is an SSP, even though it is transmitted as a part of the secret key in order to minimize the public key size (Section 1.2 of the Dilithium 3.1 spec).

Cheers,

- markku

Dr. Markku-Juhani O. Saarinen
Senior Cryptography Architect

PQShield Ltd

E:mjos@pqshield.com
W:www.pqshield.com

PQShield is a private limited company registered in England and Wales with registered number 11388567. PQShield's registered office is Prama House, 276 Banbury Rd., OX2 7HT Oxford, UK. This email and any attachment contain information that is private and confidential and is intended for the addressee only. If you are not an addressee, you are not authorised to read, copy or use the email or any attachment, If you have received this email in error, please notify the sender by return email and then destroy it. Any views expressed in this e-mail are not that of PQShield Ltd or its employees unless specifically stated. As e-mail communications are known to be unsecure, we accept no liability for any legal issues that may arise as a result of this e-mail. It is advised that you carry out a virus check with your own software before opening any attachments sent to you.

On Tue, Jun 14, 2022 at 7:31 AM 'Prasanna Ravi' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> Dear all,
>
> We would like to share our recent work titled "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results" available at https://eprint.iacr.org/2022/737
> **Please find a short abstract of our work below:**
> In this work, we present a systematic study of Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA) on structured lattice-based schemes, with focus on Kyber Key Encapsulation Mechanism (KEM) and Dilithium signature scheme. We attempt to present a survey and classification of existing SCA/FIA on Kyber and Dilithium. Given the wide variety of reported attacks, simultaneous protection against all the attacks requires implementing customized protections/countermeasures for both Kyber and Dilithium. We therefore present a range of customized countermeasures, capable of providing defenses/ mitigations against existing SCA/FIA. We implement the presented countermeasures within two well-known public software libraries for PQC - (1) **pqm4** library for the ARM Cortex-M4 based microcontroller and (2) **liboqs** library for the Raspberry Pi 3 Model B Plus based on the ARM Cortex-A53 processor. Our performance evaluation reveals that the presented custom countermeasures incur reasonable performance overheads, on both the evaluated embedded platforms. We therefore believe our work argues for usage of custom countermeasures within real-world implementations of lattice-based schemes, either in a standalone manner, or as reinforcements to generic countermeasures such as masking.
> **DETECTION-BASED COUNTERMEASURES (SANITY CHECK) AGAINST SCA/FIA ASSISTED CHOSEN-CIPHERTEXT ATTACKS:**
> We would like to particularly highlight two detection-based countermeasures against SCA/ FIA assisted chosen-ciphertext attacks on LWE/LWR-based KEMs, that are discussed in this work. The core idea is to detect a malicious ciphertext and immediately refresh the long-term secret key to prevent further exposure. The first countermeasure is the ciphertext sanity check (Section 5.1.1) which filters low entropy ciphertexts (also proposed in [1]), and

> the second countermeasure is the message polynomial sanity check countermeasure which can detect malicious ciphertexts that work based on border-failure strategies. The recent talk titled "Surviving the FO-Calypse" by Azouaoui et al. [2] highlighted the difficulty of detecting ciphertexts that work based on border-failure strategies. In this respect, we believe our proposed message polynomial sanity check countermeasure could be an interesting low-cost approach to thwart most if not all the proposed SCA/FIA assisted chosen-ciphertext attacks.
>
> We appreciate any feedback/suggestions/discussions from the community in this topic.
>
> With Thanks and Regards,
> The Team.
>
> **References:**
>
> [1] Xu, Zhuang, Owen Michael Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers (2021).
>
> [2] Surviving the FO-Calypse: Securing PQC Implementations in Practice, Melissa Azouaoui, Joppe W. Bos, Björn Fay, Marc Gourjon, Yulia Kuzovkova, Joost Renes, Tobias Schneider, Christine van Vredendaal in Collaboration with UCLouvain: Olivier Bronchain, Clément Hoffmann, François-Xavier Standaert, Real World Crypto Symposium, April 2022, Available athttps://iacr.org/submit/files/slides/2022/rwc/rwc2022/48/slides.pdf
>
> ---
>
> CONFIDENTIALITY: This email is intended solely for the person(s) named and may be confidential and/or privileged. If you are not the intended recipient, please delete it, notify us and do not copy, use, or disclose its contents.
> Towards a sustainable earth: Print only when necessary. Thank you.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/HK0PR01MB22279EA0663248B5A486073AC7AA9%40HK0PR01MB2227.apcprd01.prod.exchangelabs.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/TYZPR01MB4115C9EC502409182B35E89DC7169%40TYZPR01MB4115.apcprd01.prod.exchangelabs.com.