Merged Talk:

Fixing and Mechanizing the Security Proof of Fiat-Shamir with Aborts and Dilithium

Manuel Barbosa Gilles Barthe Christian Doczkal Jelle Don
Serge Fehr Benjamin Grégoire Yu-Hsuan Huang Andreas
Hülsing Yi Lee Xiaodi Wu

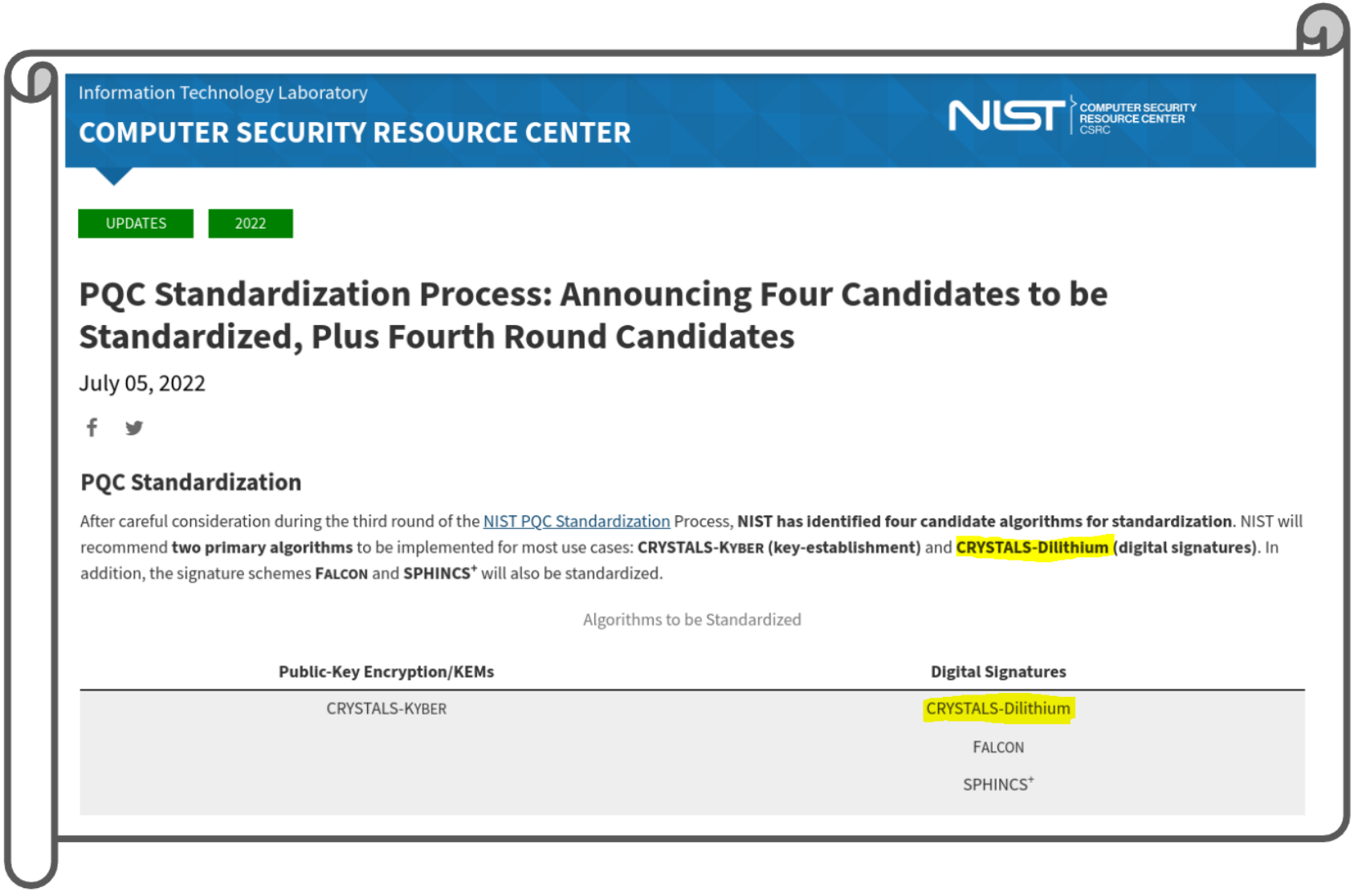
A Detailed Analysis of Fiat-Shamir with Aborts

Julien Devevey Pouria Fallahpour Alain Passelègue Damien Stehlè

Fixing and Mechanizing the Security Proof of Fiat-Shamir with Aborts and Dilithium

Manuel Barbosa Gilles Barthe Christian Doczkal
Jelle Don Serge Fehr Benjamin Grégoire
Yu-Hsuan Huang Andreas Hülsing **Yi Lee** Xiaodi Wu

Story Time: Dilithium



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

UPDATES 2022

PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

July 05, 2022

PQC Standardization

After careful consideration during the third round of the NIST PQC Standardization Process, **NIST has identified four candidate algorithms for standardization**. NIST will recommend **two primary algorithms** to be implemented for most use cases: **CRYSTALS-KYBER (key-establishment)** and **CRYSTALS-Dilithium (digital signatures)**. In addition, the signature schemes **FALCON** and **SPHINCS+** will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS+

Figure: Annoucement of NIST PQC Winners

Story Time: Fiat-Shamir with Aborts (FSwA)

Dilithium: a signature scheme based on FSwA

Story Time: Fiat-Shamir with Aborts (FSwA)

Dilithium: a signature scheme based on FSwA

History of FSwA:

- adapted from [FS86]

Amos Fiat (left) and Adi Shamir (right)

Story Time: Fiat-Shamir with Aborts (FSwA)

Dilithium: a signature scheme based on FSwA

History of FSwA:

- adapted from [FS86]
- origins: [Lyu09, Lyu12]

Fiat-Shamir With Aborts: Applications to Lattice and Factoring-Based Signatures

Vadim Lyubashevsky *

Department of Computer Science
Tel-Aviv University
Tel Aviv 69978, Israel
vlyubash@cs.ucsd.edu

Story Time: Fiat-Shamir with Aborts (FSwA)

Dilithium: a signature scheme based on FSwA

History of FSwA:

- adapted from [FS86]
- origins: [Lyu09, Lyu12]
- quantum analysis: [KLS18]

A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model

Eike Kiltz [1] Vadim Lyubashevsky [2] Christian Schaffner [3]

February 20, 2018

[1] Ruhr Universität Bochum
eike.kiltz@rub.de
[2] IBM Research – Zurich
vad@zurich.ibm.com
[3] QuSoft and ILLC, University of Amsterdam
c.schaffner@uva.nl

Story Time: Fiat-Shamir with Aborts (FSwA)

Dilithium: a signature scheme based on FSwA

History of FSwA:

- adapted from [FS86]
- origins: [Lyu09, Lyu12]
- quantum analysis: [KLS18]

Plot-twist: gap in all previous security proofs of FSwA!

Story Time: Fiat-Shamir with Aborts (FSwA)

Dilithium: a signature scheme based on FSwA

History of FSwA:

- adapted from [FS86]
- origins: [Lyu09, Lyu12]
- quantum analysis: [KLS18]

Plot-twist: gap in all previous security proofs of FSwA!

Invalidates claimed proven security of:

- Dilithium
- all other FSwA schemes (e.g. SeaSign[DFG19])

Our Work: Three-fold Contributions

1. **Identify a gap** in the proof of FSwA:
   - found **via formal verification**
   - in the CMA-to-NMA reduction

Our Work: Three-fold Contributions

1. **Identify a gap** in the proof of FSwA:
   - found **via formal verification**
   - in the CMA-to-NMA reduction

2. **Fix FSwA** by a new proof:
   - covers **both quantum and classical** attacks
   - in the (quantum) random oracle model ((Q)ROM)
   - worse loss than [KLS18]
   - restore full security of Dilithium

Our Work: Three-fold Contributions

1. **Identify a gap** in the proof of FSwA:
   - found **via formal verification**
   - in the CMA-to-NMA reduction

2. **Fix FSwA** by a new proof:
   - covers **both quantum and classical** attacks
   - in the (quantum) random oracle model ((Q)ROM)
   - worse loss than [KLS18]
   - restore full security of Dilithium

3. **Formal verification** via Easycrypt, classically:
   - generic CMA-to-NMA reduction
   - full security proof of Dilithium

Our Work

Impact:

- We **fully restored** the security of Dilithium.
- works using FSwA [LNP22, DKL$^+$18, DFG19, BKP20, BDK$^+$22, ...] to be re-examined

Our Work

Impact:

- We **fully restored** the security of Dilithium.
- works using FSwA [LNP22, DKL$^+$18, DFG19, BKP20, BDK$^+$22, ...] to be re-examined

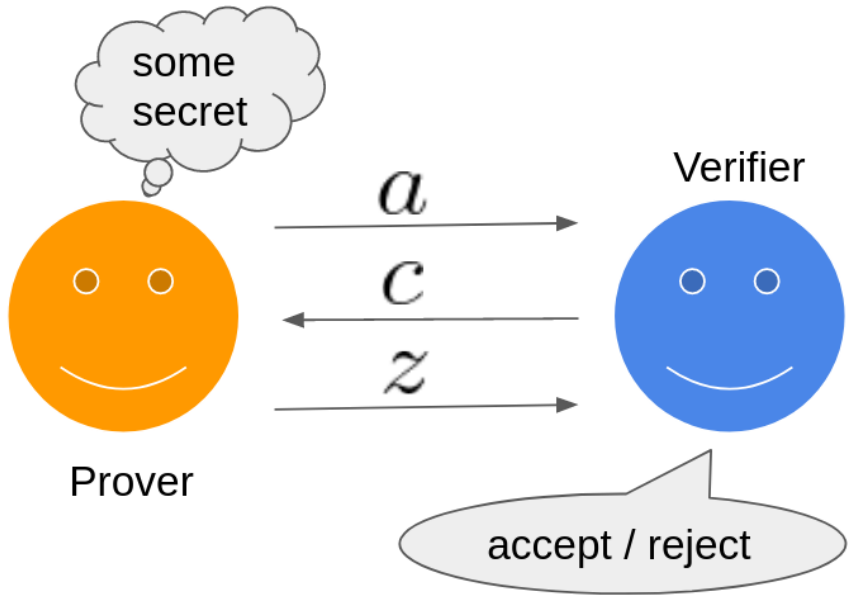
Concurrent work [Devevey, Fallahpour, Passelégue, Stehlé].

Outline

- Sigma Protocols
- Fiat-Shamir (with Aborts) Paradigm
- Fixing the Flaw
- Mechanizing Proofs

Sigma Protocol

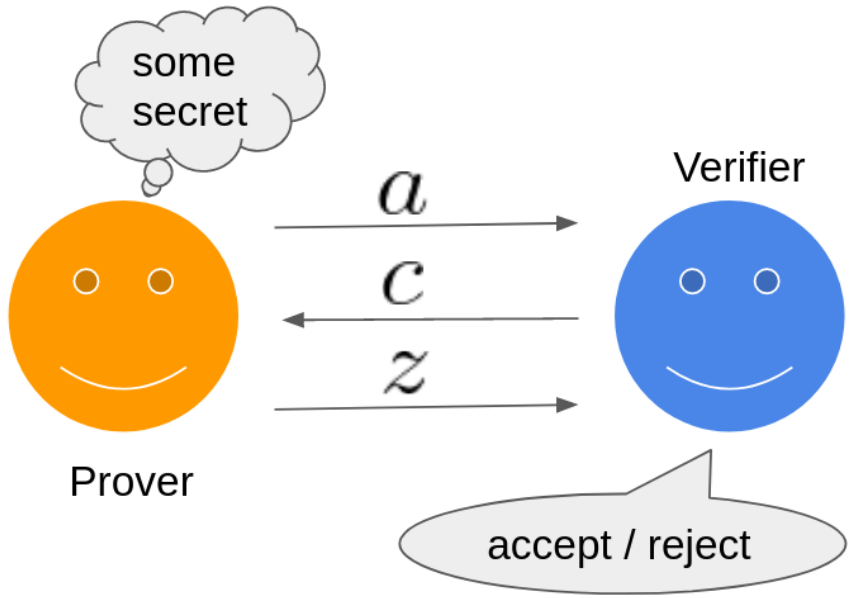
A 3-round protocol where:
Prover convinces Verifier that he knows some secret.



[1] Formalized by the existence of a simulator that can simulate the transcript.

Sigma Protocol

A 3-round protocol where:
Prover convinces Verifier that he knows some secret.



Knowledge soundness:

"Verifier can be convinced only if the Prover knows the secret."

Honest-Verifier Zero-Knowledge (HVZK)[1]:

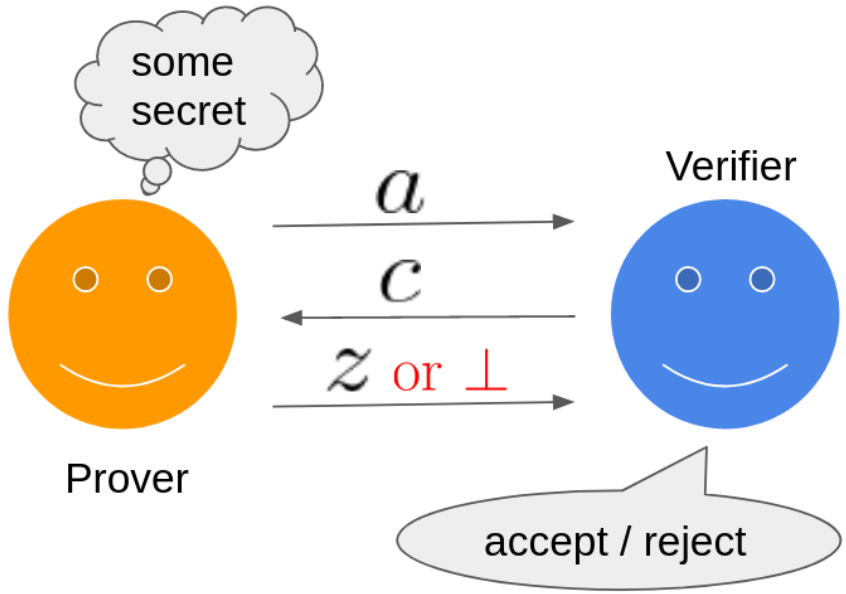
"Verifier learns nothing about the secret from the protocol."

[1] Formalized by the existence of a simulator that can simulate the transcript.

Aborting Sigma Protocol

In **aborting** Σ-protocols, Prover may abort with some probability.

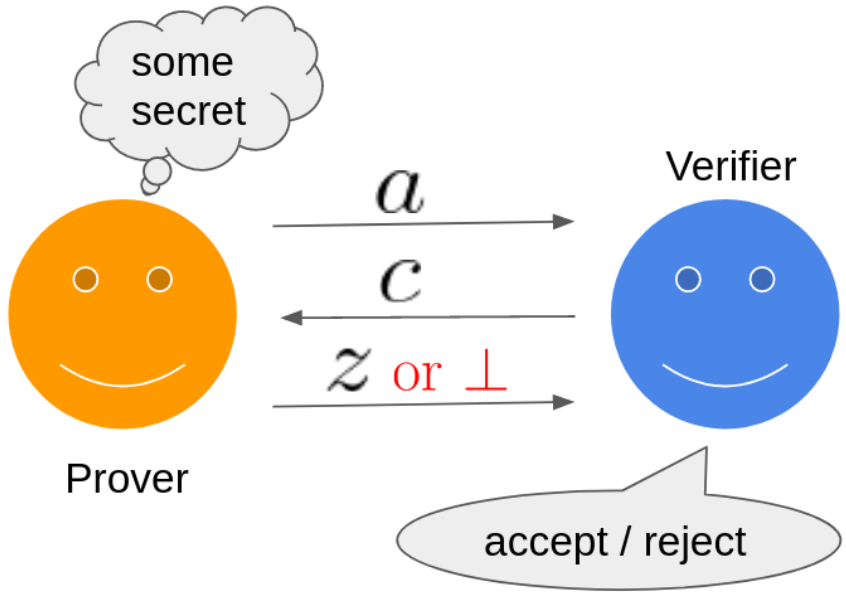
Relevant in the case of lattices or isogenies,



Aborting Sigma Protocol

In **aborting** Σ-protocols, Prover may abort with some probability.

Relevant in the case of lattices or isogenies,



- Protocol is **repeated until** $z \neq \perp$ to convince Verifier
- Typically satisfies weaker version of HVZK (acHVZK)

acHVZK: the transcript **conditioned on** $z \neq \perp$, can be simulated

Outline

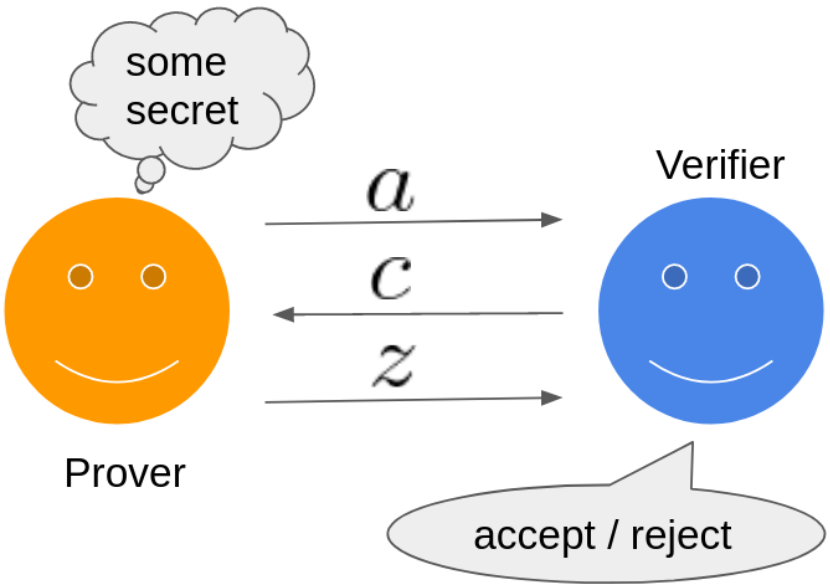
Sigma Protocol

- Fiat-Shamir (with Aborts) Paradigm
- Fixing the Flaw
- Mechanizing Proofs

Fiat-Shamir Paradigm

a "recipe" for designing signature schemes / NIZK

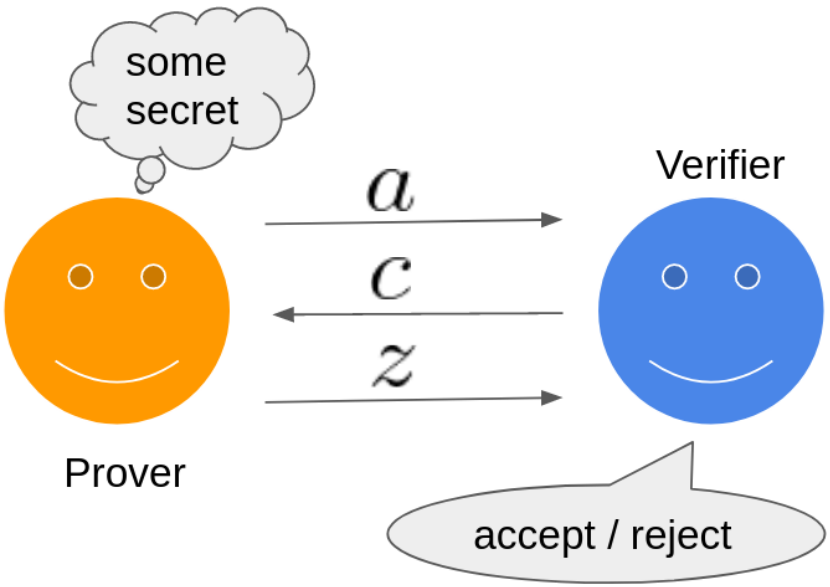
Ingredient: a Sigma protocol Σ



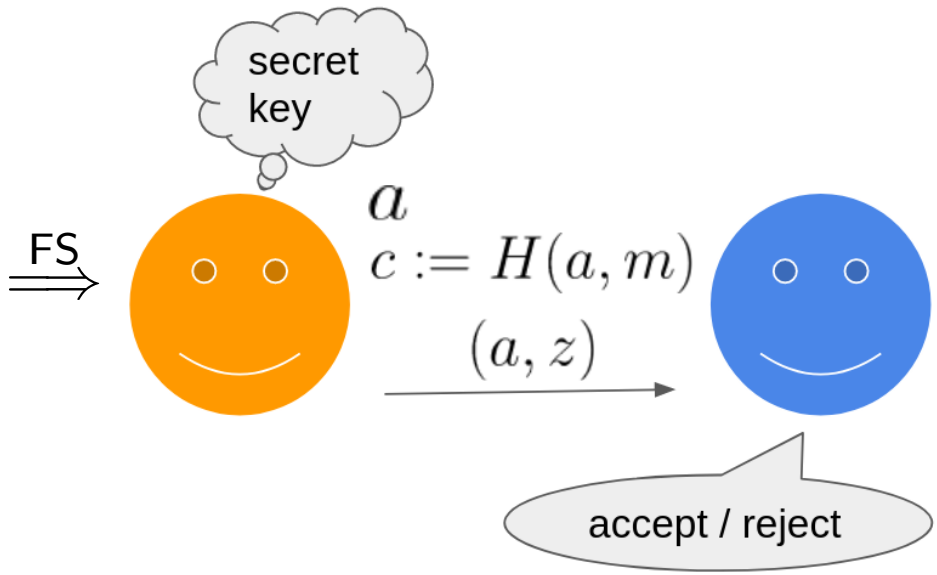
Fiat-Shamir Paradigm

a "recipe" for designing signature schemes / NIZK

Ingredient: a Sigma protocol Σ



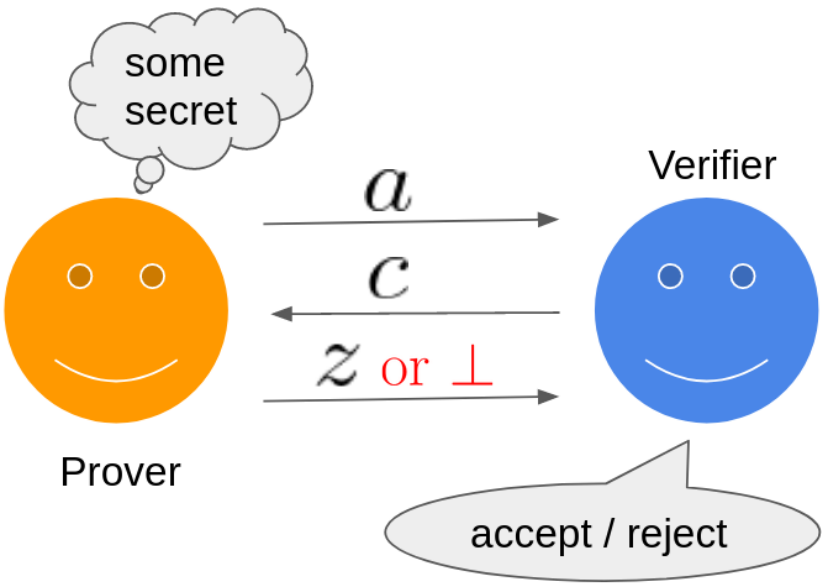
Result: a signature FS[Σ]



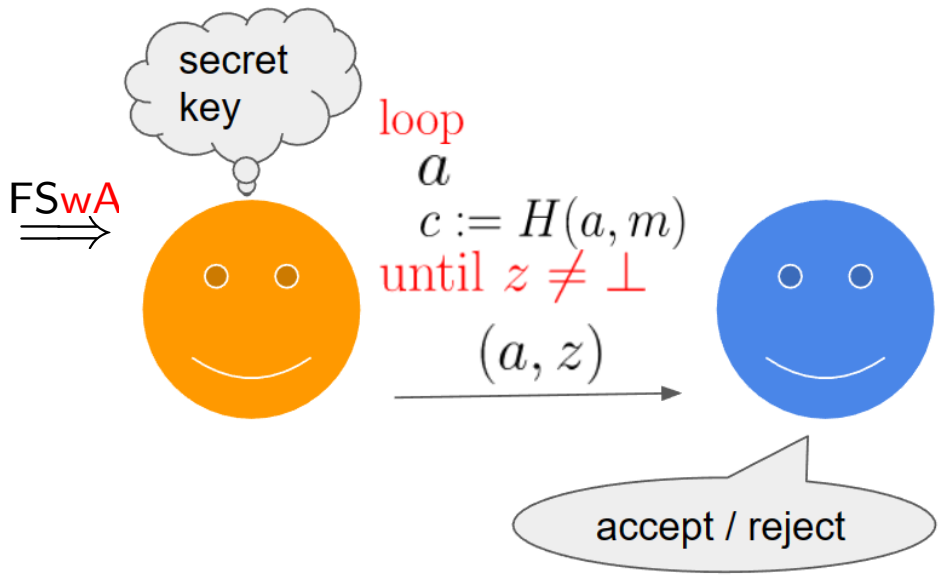
Fiat-Shamir with Aborts Paradigm

a "recipe" for designing signature schemes / NIZK

an aborting Sigma protocol Σ



Result: a signature FSwA[Σ]



Security of Fiat-Shamir (with Aborts)

- knowledge soundness $\Rightarrow$ hard to forge a signature (UF-NMA)

Security of Fiat-Shamir (with Aborts)

- knowledge soundness $\Rightarrow$ hard to forge a signature (UF-NMA)
- (weak) HVZK $\overset{!}{\Rightarrow}$ CMA-to-NMA reduction, i.e. seeing valid signatures does not help forging

Security of Fiat-Shamir (with Aborts)

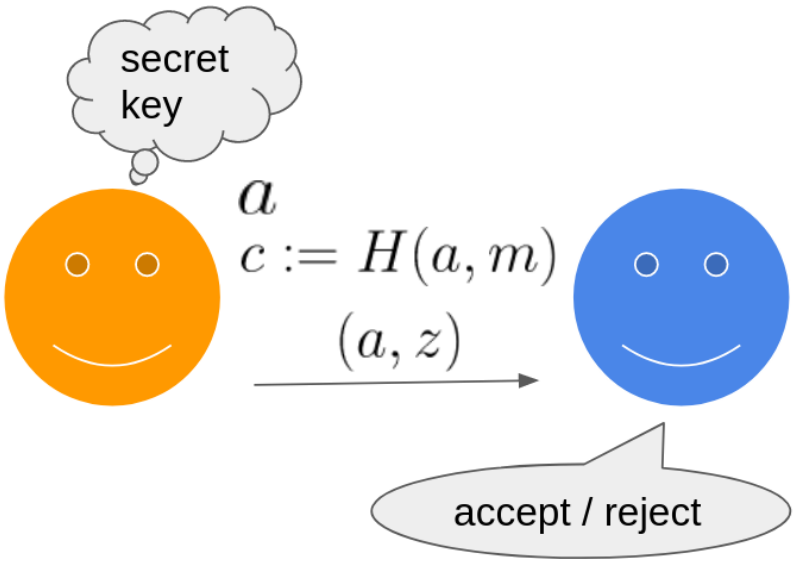
- knowledge soundness $\Rightarrow$ hard to forge a signature (UF-NMA)
- (weak) HVZK $\overset{!}{\Rightarrow}$ CMA-to-NMA reduction, i.e. seeing valid signatures does not help forging

"$\overset{!}{\Rightarrow}$" holds for Fiat-Shamir,
but here lies the catch for FSwA

Security of Fiat-Shamir (with Aborts)

Reduction: a forger could've simulated signatures by himself

FS[Σ]



simulated by $\Longrightarrow$

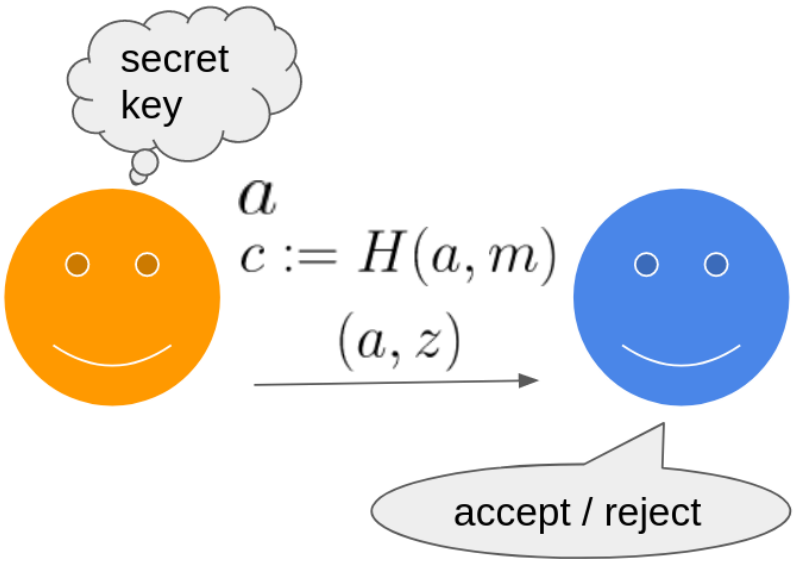
$(a, c, z) \leftarrow$ HVZK-Sim

$H(a, m) := c$

Security of Fiat-Shamir (with Aborts)

Reduction: a forger could've simulated signatures by himself

FS[Σ]



simulated by $\Longrightarrow$

$(a, c, z) \leftarrow$ HVZK-Sim

$H(a, m) := c$

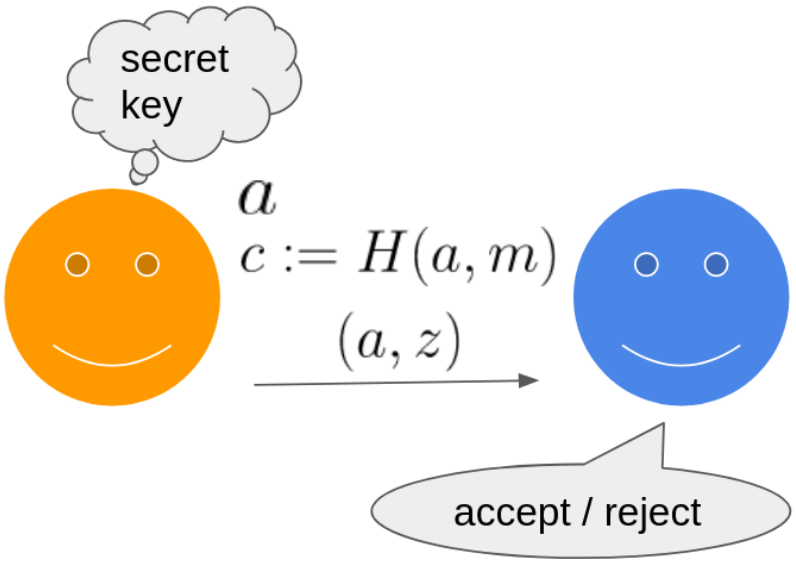
c is random and independent of a

distribution of H unaffected (basically)

Security of Fiat-Shamir (with Aborts)

Reduction: a forger could've simulated signatures by himself

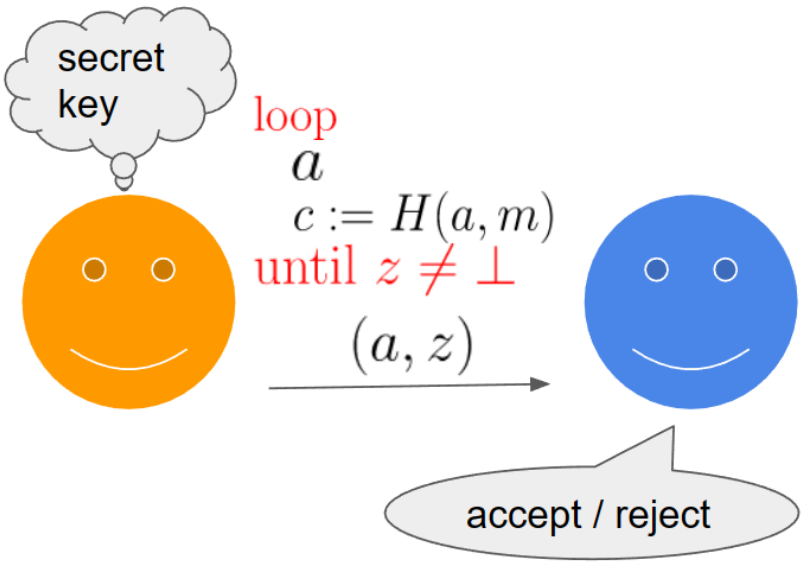
FS[Σ]



simulated by $\Longrightarrow$ $(a, c, z) \leftarrow$ HVZK-Sim, $H(a, m) := c$

c is random and independent of a
distribution of H unaffected (basically)

FSwA[Σ]

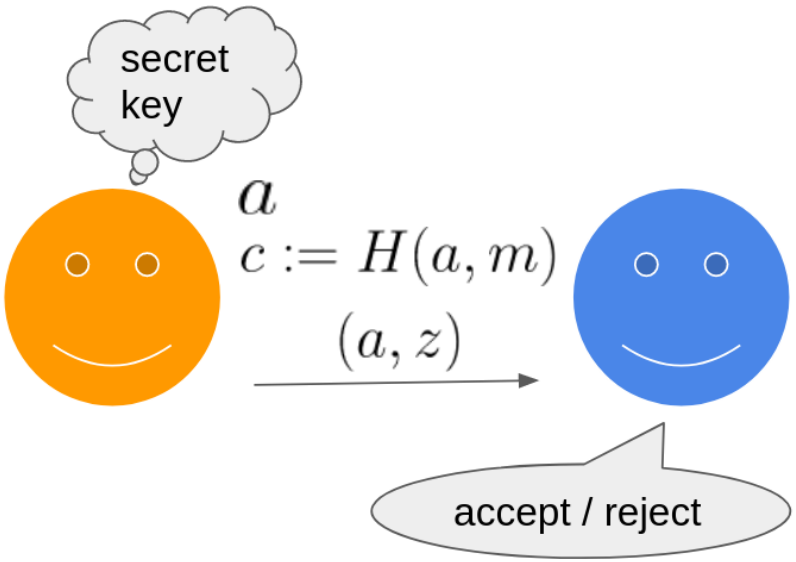


simulated by $\Longrightarrow$ $(a, c, z) \leftarrow$ acHVZK-Sim, $H(a, m) := c$

Security of Fiat-Shamir (with Aborts)

Reduction: a forger could've simulated signatures by himself

FS[Σ]

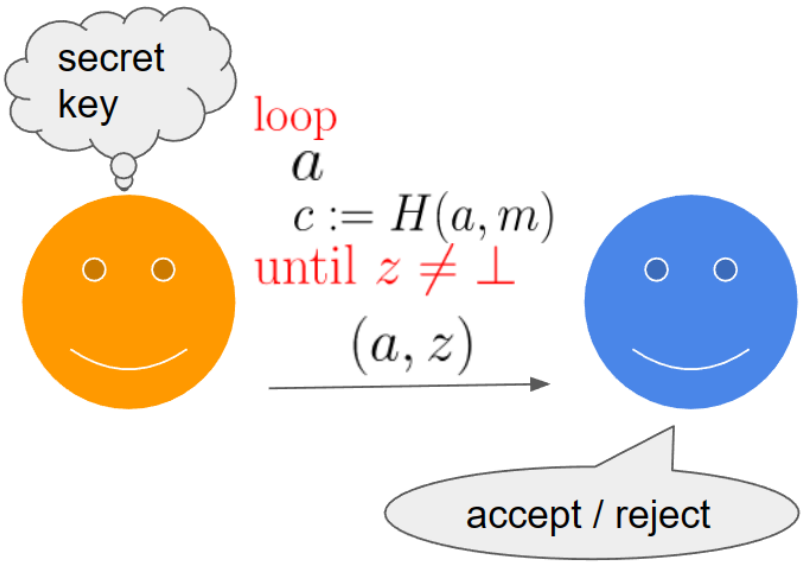


simulated by $\Longrightarrow$ $(a, c, z) \leftarrow$ HVZK-Sim, $H(a, m) := c$

c is random and independent of a

distribution of H unaffected (basically)

FSwA[Σ]



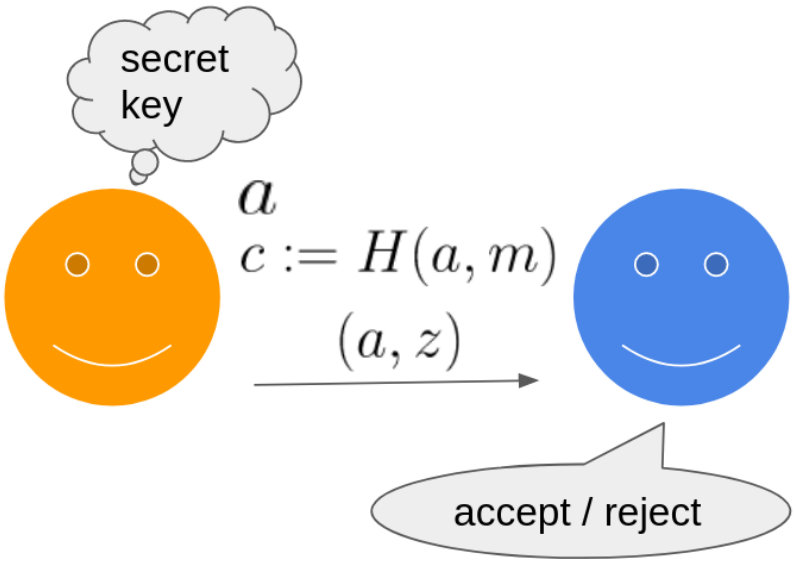
simulated by $\Longrightarrow$ $(a, c, z) \leftarrow$ acHVZK-Sim, $H(a, m) := c$

c is not random and independent of a

Security of Fiat-Shamir (with Aborts)

Reduction: a forger could've simulated signatures by himself

FS[Σ]

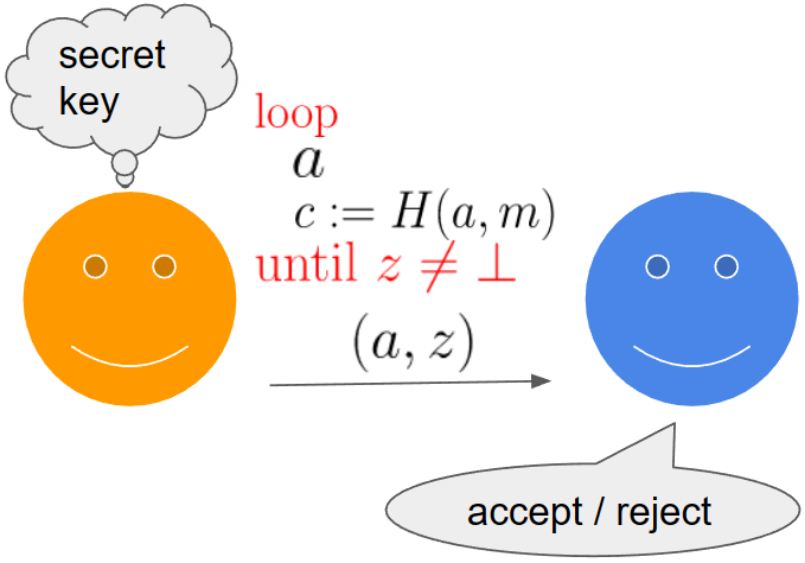


simulated by $\Longrightarrow$ $(a, c, z) \leftarrow$ HVZK-Sim, $H(a, m) := c$

c is random and independent of a

distribution of H unaffected (basically)

FSwA[Σ]



simulated by $\Longrightarrow$ $(a, c, z) \leftarrow$ acHVZK-Sim, $H(a, m) := c$

c is not random and independent of a

H is biased, ruining previous proofs!

Outline

Sigma Protocol

Fiat-Shamir (with Aborts) Paradigm

- Fixing the Flaw
- Mechanizing Proofs

Fixing the Flaw

No easy patch. Had to redo the proof from scratch!

Fixing the Flaw

No easy patch. Had to redo the proof from scratch!

Technical hurdles:

- FSwA runs aborting Sigma protocol for **unbounded** times.
- de-tour hybrid steps to handle biased H

Fixing the Flaw

No easy patch. Had to redo the proof from scratch!

Technical hurdles:

- FSwA runs aborting Sigma protocol for **unbounded** times.
- de-tour hybrid steps to handle biased H

Generically, obtain worse security loss.

Fixing the Flaw

Assuming perfect (weak) HVZK, for CMA-to-NMA reduction:

- [KLS18]: quantum and classical loss $\leq \epsilon := \max_{a^\circ} \Pr[a = a^\circ]$
- Ours:

$$\text{quantum loss} \leq O\left(\sqrt{q_H^2 q_S \epsilon} + \sqrt{q_S^3 \epsilon}\right)$$

$$\text{classical loss} \leq O\left(q_H q_S \epsilon + q_S^2 \epsilon\right)$$

Fixing the Flaw

Assuming perfect (weak) HVZK, for CMA-to-NMA reduction:

- [KLS18]: quantum and classical loss $\leq \epsilon := \max_{a^\circ} \Pr[a = a^\circ]$
- Ours:

$$\text{quantum loss} \leq O\left(\sqrt{q_H^2 q_S \epsilon} + \sqrt{q_S^3 \epsilon}\right)$$

$$\text{classical loss} \leq O\left(q_H q_S \epsilon + q_S^2 \epsilon\right)$$

For Dilithium, full security restored!

Fixing the Flaw

Assuming perfect (weak) HVZK, for CMA-to-NMA reduction:

- [KLS18]: quantum and classical loss $\leq \epsilon := \max_{a^\circ} \Pr[a = a^\circ]$
- Ours:

$$\text{quantum loss} \leq O\left(\sqrt{q_H^2 q_S \epsilon} + \sqrt{q_S^3 \epsilon}\right)$$

$$\text{classical loss} \leq O\left(q_H q_S \epsilon + q_S^2 \epsilon\right)$$

For Dilithium, full security restored!

Restored via better control over ϵ, partially computer-aided

- [KLS18]: $\epsilon \lesssim 2^{-255}$
- Ours, for NIST3 parameters: $\epsilon \lesssim 2^{-844}$

Outline

- Sigma Protocol
- Fiat-Shamir (with Aborts) Paradigm
- Fixing the Flaw
- Mechanizing Proofs

Role of Formal Verification Efforts

- Machine-checked proofs using EasyCrypt
- Discovery of the [KLS18] flaw

Our Mechanized Proof

- Main proofs: $\sim$ 6000 lines
  - CMA-to-NMA reduction in the ROM
  - Properties of Dilithium

Our Mechanized Proof

- Main proofs: $\sim$ 6000 lines
  - CMA-to-NMA reduction in the ROM
  - Properties of Dilithium
    - Underlying aborting sigma-protocol is acHVZK
    - NMA to lattice assumptions
    - Commitment-recovery optimization

Our Mechanized Proof

- Main proofs: $\sim$ 6000 lines
  - CMA-to-NMA reduction in the ROM
  - Properties of Dilithium
    - Underlying aborting sigma-protocol is acHVZK
    - NMA to lattice assumptions
    - Commitment-recovery optimization
- $+$ several thousand lines of library extensions
- Novelty: Expected number of iterations, infinite hybrids

Our Mechanized Proof: Future Directions

- Extend results to optimized implementation
- Incorporate side-channel resistance

Summary

1. **Identify a gap** in the proof of FSwA:
   - found **via formal verification**
   - in the CMA-to-NMA reduction

Summary

1. **Identify a gap** in the proof of FSwA:
   - found **via formal verification**
   - in the CMA-to-NMA reduction

2. **Fix FSwA** by a new proof:
   - covers **both quantum and classical** attacks
   - in the (quantum) random oracle model ((Q)ROM)
   - worse loss than [KLS18]
   - restore full security of Dilithium

Summary

1. **Identify a gap** in the proof of FSwA:
   - found **via formal verification**
   - in the CMA-to-NMA reduction

2. **Fix FSwA** by a new proof:
   - covers **both quantum and classical** attacks
   - in the (quantum) random oracle model ((Q)ROM)
   - worse loss than [KLS18]
   - restore full security of Dilithium

3. **Formal verification** via EasyCrypt, classically:
   - generic CMA-to-NMA reduction
   - full security proof of Dilithium

Summary

1. **Identify a gap** in the proof of FSwA:
   - found **via formal verification**
   - in the CMA-to-NMA reduction

2. **Fix FSwA** by a new proof:
   - covers **both quantum and classical** attacks
   - in the (quantum) random oracle model ((Q)ROM)
   - worse loss than [KLS18]
   - restore full security of Dilithium

3. **Formal verification** via EasyCrypt, classically:
   - generic CMA-to-NMA reduction
   - full security proof of Dilithium

Call for action: Re-examine your own FSwA signatures!

Thank you for listening!

Eprint: ia.cr/2023/246

References I

[BDK+22] Ward Beullens, Samuel Dobson, Shuichi Katsumata, Yi-Fu Lai, and Federico Pintore. Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 95–126. Springer, 2022.

[BKP20] Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and Falafl: logarithmic (linkable) ring signatures from isogenies and lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 464–492. Springer, 2020.

References II

[DFG19] Luca De Feo and Steven D Galbraith. SeaSign: compact isogeny signatures from class group actions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 759–789. Springer, 2019.

[DKL+18] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268, 2018.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Crypto*, volume 86, pages 186–194. Springer, 1986.

References III

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 552–586, Cham, 2018. Springer International Publishing.

[LNP22] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plancon. Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. *Cryptology ePrint Archive*, 2022.

[Lyu09] Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 598–616. Springer, 2009.

References IV

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 738–755. Springer, 2012.