Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives

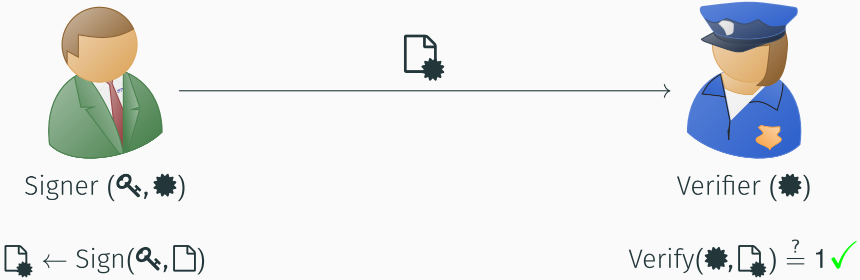
Melissa Chase, David Derler, **Steven Goldfeder**, Claudio Orlandi, **Sebastian Ramacher**, Christian Rechberger, Daniel Slamanig, Greg Zaverucha

CCS 2017, November 2, 2017

Princeton University and Graz University of Technology

Digital Signatures

Digital Signatures



Overview

Digital Signatures in a post-quantum world

- RSA and DLOG based schemes insecure

New schemes

- Based on structured hardness assumptions (lattices, codes, isogenies, etc.)
- Based on symmetric primitives: hash-based signatures

Other alternatives only relying on symmetric primitives?

High-level View

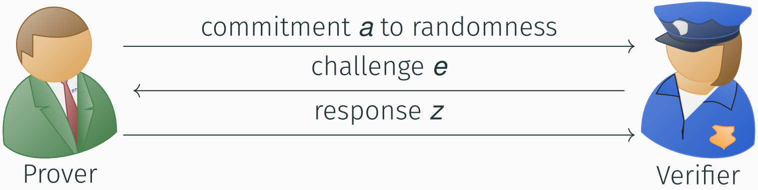
Recent years progress in two areas

- Symmetric-key primitives with few multiplications
- Practical ZK-Proof systems over general circuits

New signature schemes based on these advances

Σ-Protocols

Three move protocol:



- aka (Interactive) Honest-Verifier Zero-Knowledge Proofs

Non-interactive variant via Fiat-Shamir [FS86] transform

Digital Signatures from Σ-Protocols

Often used methodology

One-way function $f_x : K \to R$ with $x \in D$

- $sk \xleftarrow{R} K$
- $y \leftarrow f_x(sk)$, $pk \leftarrow (x, y)$

Signature

- Σ-protocol to prove knowledge of sk so that $y = f_x(sk)$
- Use Fiat-Shamir transform to bind message to proof $e \leftarrow H(a \| m)$

Σ-protocols for Arithmetic Circuits

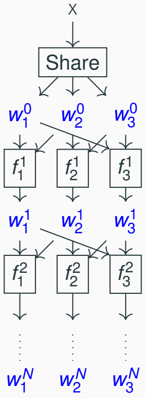
ZKBoo [GMO16]

Efficient Σ-protocols for arithmetic circuits

- generalization, simplification, implementation of "MPC-in-the-head" [IKOS07]

Idea

1. Decompose circuit into 3 shares
2. Revealing 2 parts reveals no information
3. Evaluate decomposed circuit per share
4. Commit to each evaluation
5. Challenger requests to open 2 of 3
6. Verifies consistency



Efficiency

- Heavily depends on #multiplications

ZKB++

Improved version of ZKBoo:

- Reduced proof to **less than half the size** without extra computational cost

Signatures from OWFs

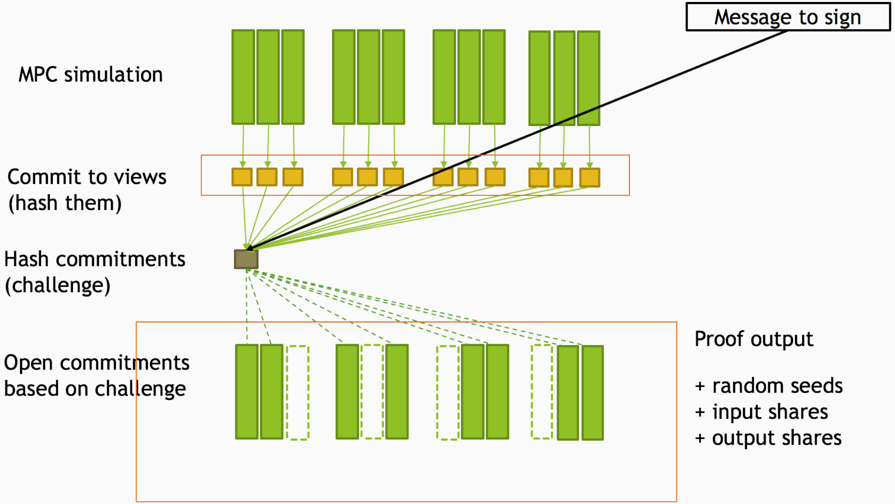
Security in QROM

Proving Fiat-Shamir transform secure in QROM faces problems

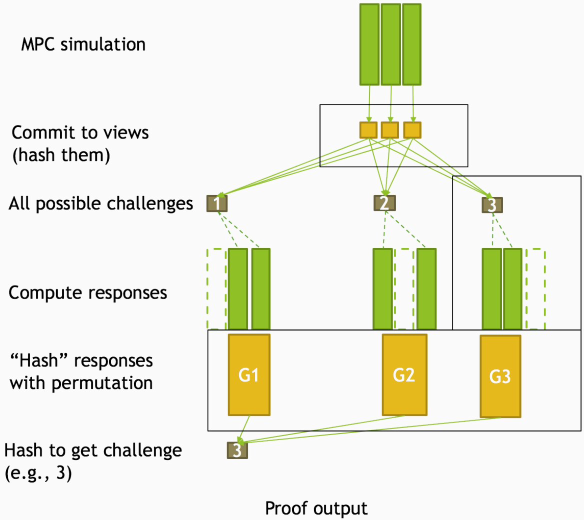
- Proof requires rewinding
- Unclear how to translate

Use Unruh Transform [Unr15]

Fiat-Shamir Transform

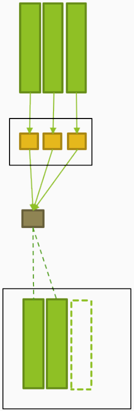


Unruh Transform



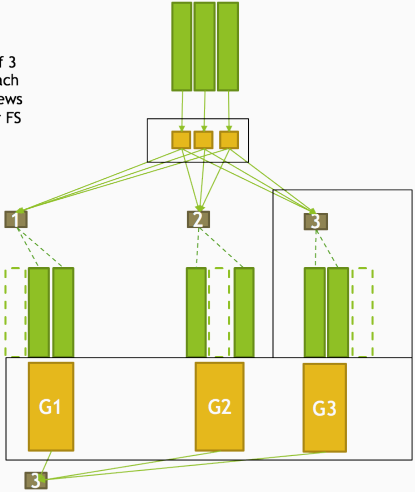
Unruh Transform (cont)

Fiat-Shamir

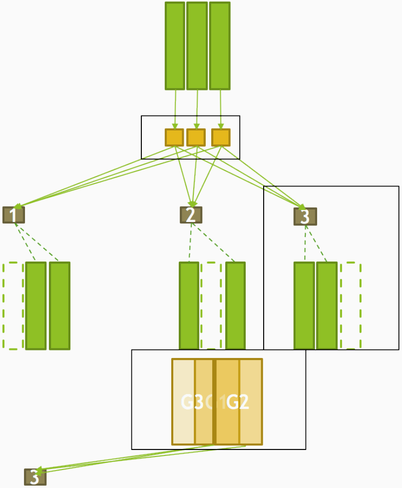


- Send permutation of 3 responses, where each response opens 2 views
- ~300% increase over FS

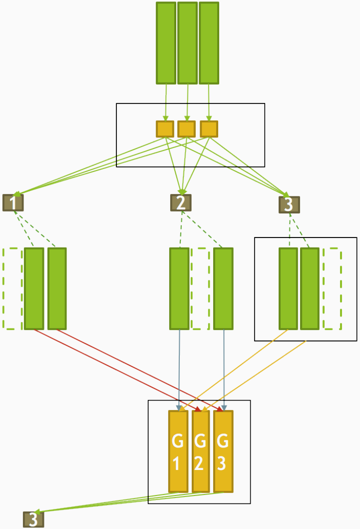
Unruh



Unruh Transform (cont)



Unruh Transform (cont)



Fish

Fish:

- Turn ZKB++ and OWF into signature scheme
- via Fiat-Shamir Transform
- Provable secure in the ROM

Picnic

Picnic:

- Turn ZKB++ and OWF into signature scheme
- via Unruh Transform
- Provable secure in the QROM

Unruh Transform incurs overhead in signature size

- But careful tweaking reduces overhead to factor 1.6

OWF Selection

Signature Size

OWF represented by arithmetic circuit with

- ring size λ
- multiplication count a

Signature size

- $|\sigma| = c_1 + c_2 \cdot (c_3 + \lambda \cdot a)$
- c_i constants polynomial in security parameter

OWF with few multiplications?

Build OWF from

name	security	$\lambda \cdot a$	
AES	128	5440	$\mathbb{F}_2$ approach
AES	128	4000?	$\mathbb{F}_{2^4}$ approach
AES	256	7616	$\mathbb{F}_2$ approach
SHA-2	256	> 25000	
SHA-3	256	38400	
Noekeon	128	2048	
Trivium	80	1536	
PRINCE		1920	
Fantomas	128	2112	
LowMC v3	128	< 800	
LowMC v3	256	< 1400	
Kreyvium	128	1536	
FLIP	128	> 100000	
MIMC	128	10337	
MIMC	256	41349	

Signature Size Comparison

name	security	$\lvert\sigma\rvert$
AES	128	$162K$
AES	256	$475K$
SHA-2	256	$1314K$
SHA-3	256	$2121K$
LowMC v3	128	$33K$
LowMC v3	256	$129K$

LowMC [ARS+15, ARS+16]

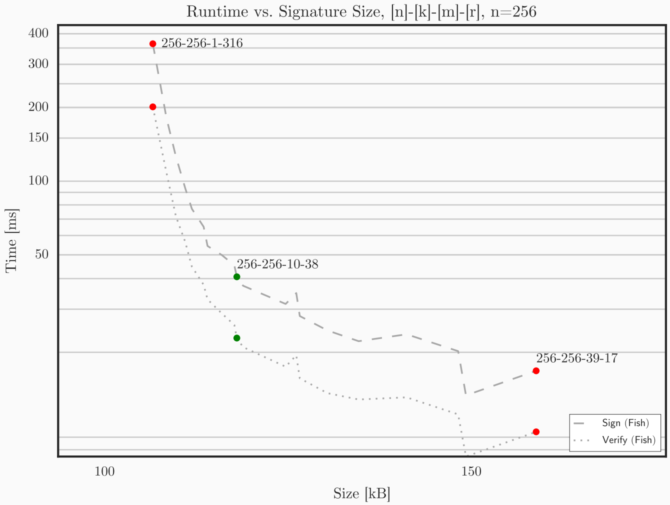
- Lightweight block ciper design
- Allows selection of instances minimizing
  - ANDdepth,
  - number of ANDs, or
  - ANDs / bit

Blocksize n	**S-boxes** m	**Keysize** k	**Data** d	**ANDdepth** r	**# of ANDs**	**ANDs/bit**
256	2	256	256	232	**1392**	5.44
512	66	256	256	**18**	3564	6.96
1024	10	256	256	103	3090	**3.02**

Table 1: LowMC parameters for 128-bit PQ-security

- Choose instances with $n = k$ and $d = 1$

Example Exploration of Variation of LowMC Instances



Comparison and Conclusion

Comparison with Recent Proposals

Scheme	Gen	Sign	Verify	$\|sk\|$	$\|pk\|$	$\|\sigma\|$	M
Fish-256-10-38	0.1	17.22	12.46	$32/64$		$129K$	ROM
Picnic-256-10-38	0.1	17.49	12.70	$32/64$		$204K$	QROM
SPHINCS-256	0.8	13.4	0.6	$1K$	$1K$	$40K$	SM
MQ 5pass	1.0	7.2	5.0	32	74	$40K$	ROM
BLISS-I	44	0.1	0.1	$2K$	$7K$	$5.6K$	ROM
Ring-TESLA	$17K$	0.1	0.1	$12K$	$8K$	$1.5K$	ROM
TESLA-768	$49K$	0.6	0.4	$3.1M$	$4M$	$2.3K$	(Q)ROM
FS-Véron	n/a	n/a	n/a	32	160	$\geq 126K$	ROM
SIDHp751	16	$7K$	$5K$	48	768	$138K$	QROM

Table 2: Timings (ms) and key/signature sizes (bytes)

Security Levels for NIST competition

- Upcoming NIST competition looking for PQ signatures schemes
- Asking for various security levels
  - L1 $\sim$ 64 bit PQ security
  - L5 $\sim$ 128 bit PQ security

Scheme	Gen	Sign	Verify	$\lvert sk\rvert$	$\lvert pk\rvert$	$\lvert\sigma\rvert$	M
Fish-L5	0.1	17.22	12.46	32/64		$129K$	ROM
Picnic-L5	0.1	17.49	12.70	32/64		$204K$	QROM
Fish-L1	0.1	1.99	1.39	16/32		$33K$	ROM
Picnic-L1	0.1	2.69	1.94	16/32		$52K$	QROM

Table 3: Timings (ms) and key/signature sizes (bytes)

Conclusion

- ZKB++: Improved ZK proofs for arithmetic circuits
  - Half the proof size
- Unruh transform: Reduced overhead to factor 1.6
- Fish/Picnic: Two new efficient post-quantum signature schemes in ROM and QROM
- Applications beyond signatures: NIZK proof system for arithmetic circuits in post-quantum setting

Outlook and Future Work

- Submitted to NIST PQ competition.
- Alternative symmetric primitives
  - Even less multiplications than LowMC?
- More LowMC cryptanalysis
  - More aggressive LowMC parameters with very low allowable data complexity, e.g. only 2 plaintexts.
- Analysis regarding side-channels

Thank you.

- Website: `https://microsoft.github.io/Picnic`
- Full version: `https://ia.cr/2017/279`
- Implementations and benchmarking: `https://github.com/IAIK/Picnic` and `https://github.com/Microsoft/Picnic`

Supported by: prisma cloud, Crypto Action, PQCRYPTO ICT-645622

References i

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner.
Ciphers for MPC and FHE.
In EUROCRYPT, 2015.

[ARS+16] Martin Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner.
Ciphers for MPC and FHE.
Cryptology ePrint Archive, Report 2016/687, 2016.

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

References ii

[GMO16] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi.
ZKBoo: Faster zero-knowledge for boolean circuits.
In USENIX Security, 2016.

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai.
Zero-knowledge from secure multiparty computation.
In Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007, pages 21–30, 2007.

[Unr15] Dominique Unruh.
Non-interactive zero-knowledge proofs in the quantum random oracle model.
In EUROCRYPT, 2015.