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

Sebastian Ramacher

Joint work with Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Christian Rechberger, Daniel Slamanig, Greg Zaverucha

March 28, 2017

IAIK, Graz University of Technology

Overview

Digital Signatures in a post-quantum world

- RSA and DLOG based schemes insecure

New schemes

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

Other alternatives only relying on symmetric primitives?

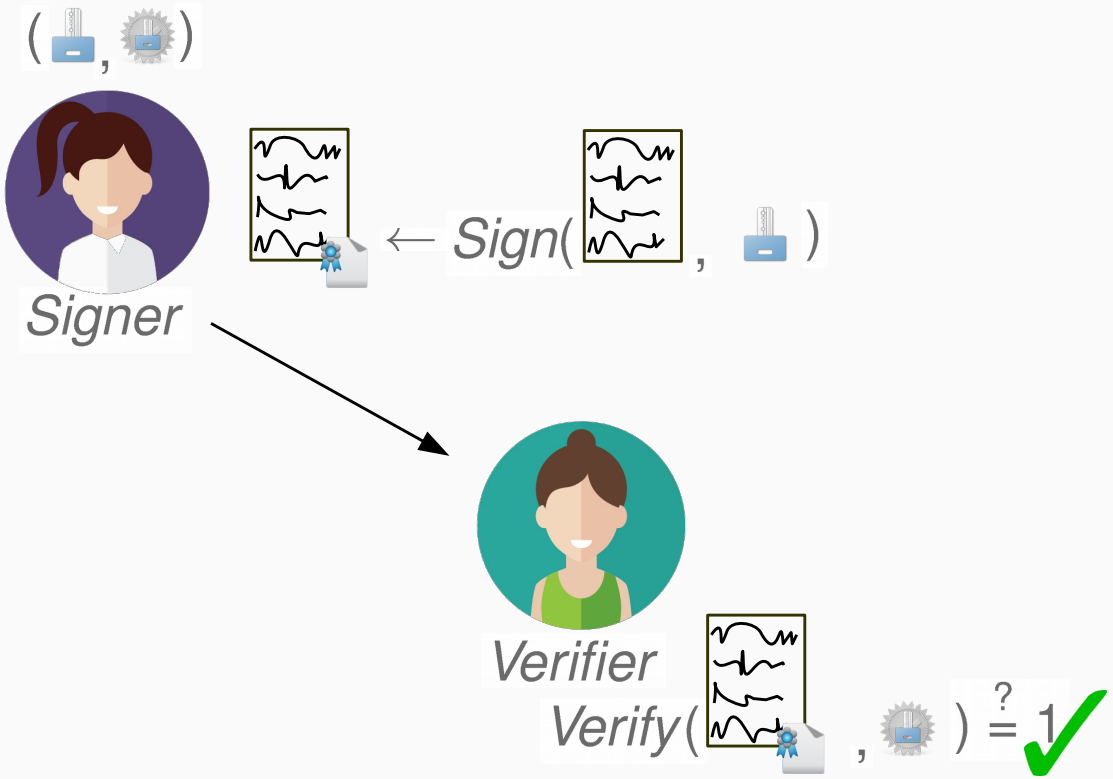
High-level View

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

Digital Signatures

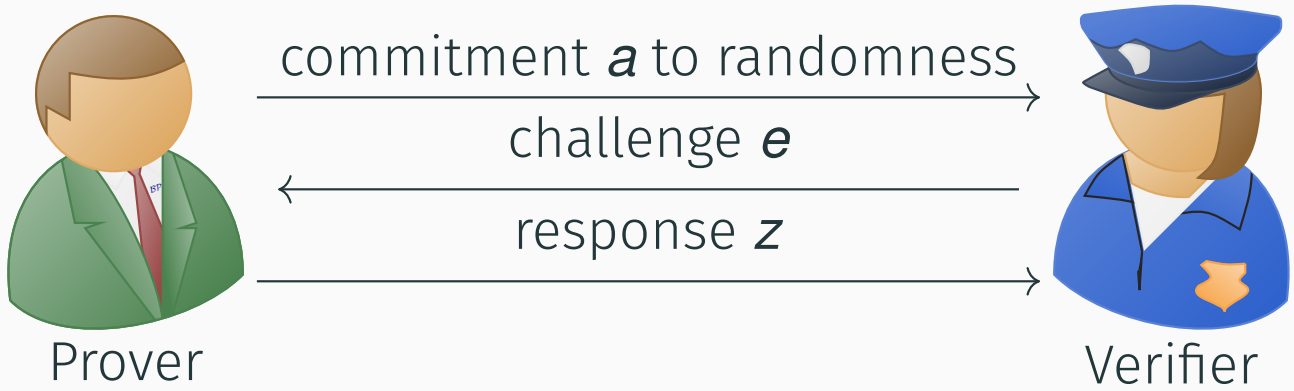


Existential Unforgeability under Chosen-Message Attacks

- Adversary may see signatures on arbitrary messages
- Still intractable to output signature for new message

Σ-Protocols

Three move protocol:



- Important that e unpredictable before sending a
- aka (Interactive) Honest-Verifier Zero-Knowledge Proofs

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

Digital Signatures from Σ-Protocols

Well known methodology

One-way function $f_k : D \to R$ with $k \in K$

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

Signature

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

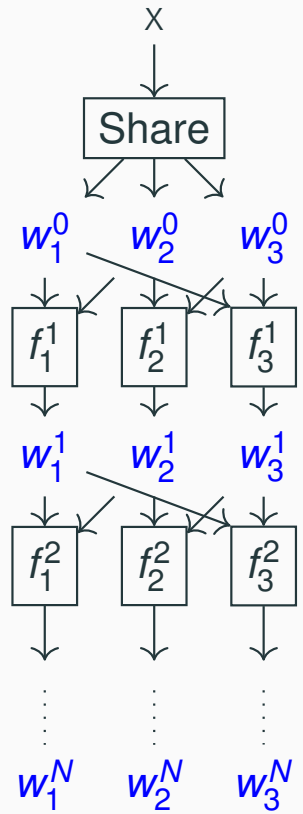
ZKBoo [GMO16]

Efficient Σ-protocols for arithmetic circuits

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

Idea

1. (2,3)-decompose circuit into three 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:

- Remove redundant information from views
- Remove redundant checks
- Proof size reduction to less than half the size
- But without extra computational cost

Optimizations

Optimization 1: Share Function and Input Shares

- Use PRNGs R_i keyed with k_i
- Share as $x_1 \leftarrow R_1(0)$, $x_2 \leftarrow R_2(0)$ and $x_3 \leftarrow x - x_1 - x_2$
- x_1 and x_2 deterministically computable by the verifier from k_1 and k_2
- Only need to include k_i in View_1 and View_2
- Expected proof size reduction: $4r \cdot |x|/3$ bits

Optimizations (cont.)

Optimization 2: Not Including Commitments

- For opened views, verifier can re-compute commitment
- Only one commitment needs to be sent
- View e as a "commitment to the commitments"
- Proof size reduction: $2r \cdot |c|$ bits

Optimizations (cont.)

Optimization 3: Not Including the Output Shares

- Output shares y_i for opened views can be re-computed
- Third output share reconstructable from y and re-computed output shares
- Unnecessary to include any output shares in proof
- Proof size reduction: $3r \cdot |y|$ bits

Optimizations (cont.)

Optimization 4: No Additional Randomness for Commitments

- First input to the commitment is seed k_i
- Protocol input to commitment doubles as randomization values
- No additional randomness for commitments necessary
- ROM is needed here, but we already need it for non-interactivity

Optimizations (cont.)

Optimization 5: Not Including View_e

- Verifier can re-compute View_e given k_e, k_{e+1} and wire values of View_{e+1}
- By binding of the commitment, commitment verifies only if View_e re-computed correctly
- Only need to store input wires of View_e
- Proof size reduction: $r \cdot |\mathsf{View}|$ bits

LowMC [ARS+15, ARS+16]

Substitution-permutation-network design

- Very lightweight S-box with one AND gate per bit
- S-box layer is only partial
- Very expensive affine layer with $n/2$ XOR gates per bit.
- Allows selection of instances minimizing, e.g.
  - 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

Fish

Fish:

- Turn ZKB++ and OWF into signature scheme
- via Fiat-Shamir Transform
- Instantiate OWF with LowMC v2
- $\Rightarrow$ EUF-CMA security in the ROM

Security in QROM

Proving Fiat-Shamir transform secure in QROM faces problems

- Proof requires rewinding
- Unclear how to translate

Use Unruh Transform [Unr15]

Take random permutation G and random oracle H

- Produce multiple proofs $(c_i, G(resp_{i,1}), \ldots, G(resp_{i,n}))$
- Hash all of them with H
- Use the result of hashing to indicate which response of each c_i should be revealed

Picnic

Picnic:

- Turn ZKB++ and OWF into signature scheme
- via Unruh Transform
- Instantiate OWF with LowMC v2
- $\Rightarrow$ EUF-CMA security in the QROM

Unruh Transform incurs overhead in signature size

- But careful tweaking reduces overhead to factor 1.6

Signature Size

- Recall: OWF $f_k : D \to R$, $sk \xleftarrow{R} K$, $pk \leftarrow (x, f_{sk}(x))$
- Security parameter κ

OWF represented by arithmetic circuit with

- ring size λ
- multiplication count a

Signature size: $|\sigma| = c_1 + c_2 \cdot (c_3 + \lambda \cdot a)$ where c_i are polynomial in κ

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 v2	128	< 800	
LowMC v2	256	< 1400	
Kreyvium	128	1536	
FLIP	128	> 100000	
MIMC	128	10337	
MIMC	256	41349	

Signature Size Comparison

name	security	$\lvert\sigma\rvert$
AES	128	339998
AES	256	473149
SHA-2	256	1331629
SHA-3	256	2158573
LowMC v2	256	108013

Example of Exploration of Variation of LowMC Instances

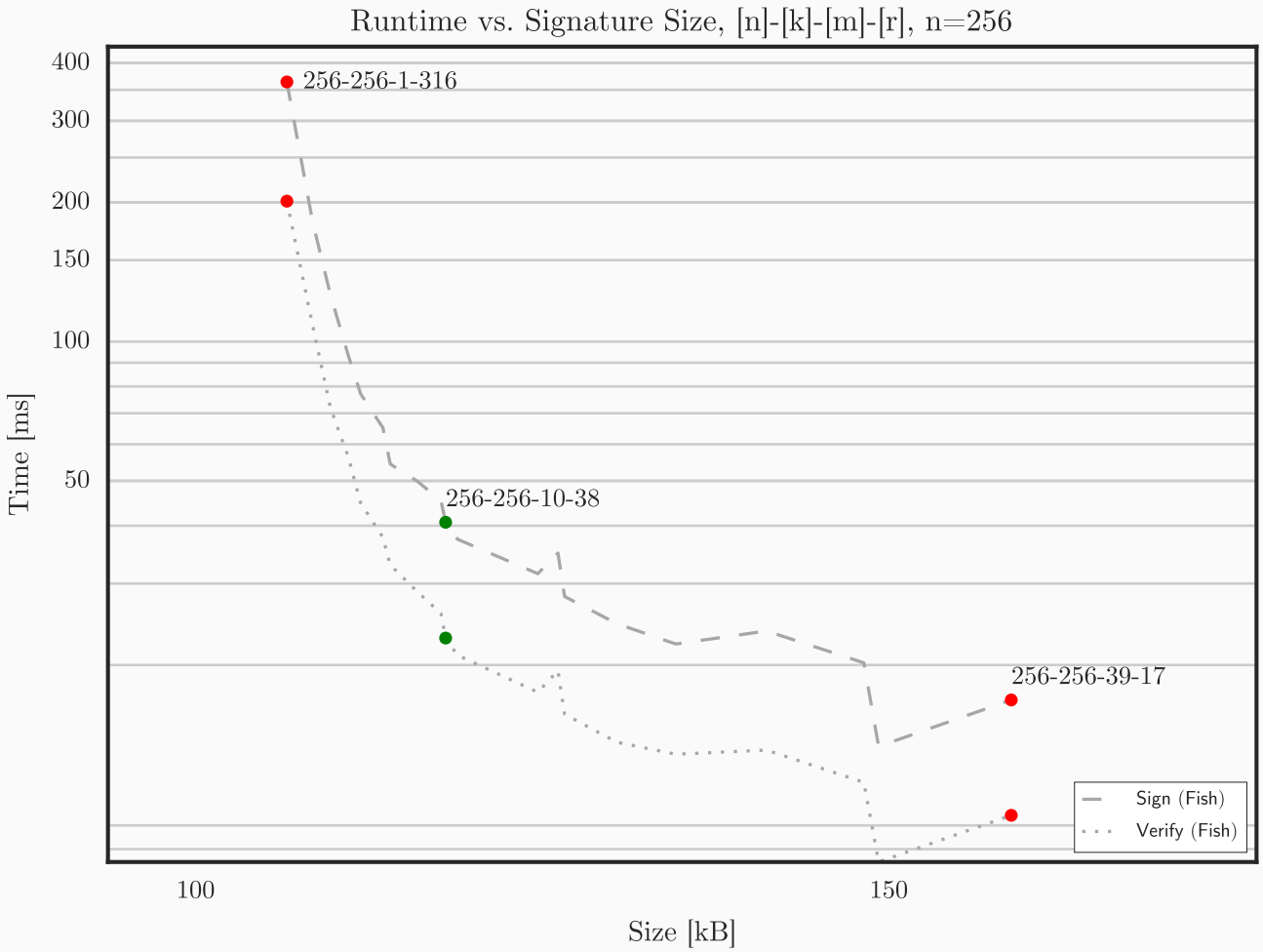


Figure 1: Measurements for instance selection (128-bit PQ-security).

Comparison with other recent proposals

Scheme	Gen	Sign	Verify	$\lvert sk \rvert$	$\lvert pk \rvert$	$\lvert \sigma \rvert$	M
Fish-10-38	0.01	29.73	17.46	32	32/64	116K	ROM
Picnic-10-38	0.01	31.31	16.30	32	32/64	191K	QROM
MQ 5pass	1.0	7.2	5.0	32	74	40K	ROM
SPHINCS-256	0.8	1.0	0.6	1K	1K	40K	SM
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)

Conclusion

ZKB++: Improved ZK proofs for arithmetic circuits

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

- Alternative symmetric primitives with few multiplications
  - Something new with even less multiplications than LowMC?
  - 256-bit secure variant of Trivium/Kreyvium?
- More LowMC cryptanalysis
  - More aggressive LowMC parameters with very low allowable data complexity, e.g. only 2 plaintexts.
- Analysis regarding side-channels
- Unruh Transform with constant overhead?

Thank you.

- Preprint will soon appear on eprint.
  - Merge of `https://ia.cr/2016/1085` and `https://ia.cr/2016/1110`.

Supported by: prisma cloud, CryptoAction, 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.

References iii

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