Digital Signatures from Symmetric-Key Primitives

Christian Rechberger

IAIK, TU Graz and DTU Compute, DTU

March 7, 2017

Based on Joint Work With

David Derler
TU Graz

Claudio Orlandi
Aarhus University

Sebastian Ramacher
TU Graz

Daniel Slamanig
TU Graz

Overview

Most known signature schemes

- Based on structured hardness assumptions
- Except hash-based signatures

Why omit structured hardness assumptions?

- Favorable in post-quantum context

Are there alternatives to hash-based signatures?

High-level view

In recent years there was progress in two very distinct areas

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

We take advantage of both and propose new signature schemes

Digital Signatures from NIZK

One-Way Function $f : D \to R$.

- Easy to evaluate
- Hard to invert
- $sk \xleftarrow{R} D, \quad pk \leftarrow f(sk)$.

Signature

- Proof of knowledge of sk so that $pk = f(sk)$.

\+ Some mechanism to bind message to this proof

Security (informal):

- Can only create proof if I actually know sk.

OWF or PRF with few multiplications?

name	security	$\lambda \cdot a$	
AES	128	5440	GF(2) approach
AES	128	4000?	GF(2^4) approach
AES	256	7616	GF(2) approach
SHA-2	256	$>$ 25000	
SHA-3	256	38400	
Noekeon	128	2048	
Trivium	80	1536	
PRINCE		1920	
Fantomas	128	2112	
LowMCv2	128	$<$ 800	
LowMCv2	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
LowMCv2 (+ 30% security margin)	256	108013

Example of exploration of variation of LowMC instances

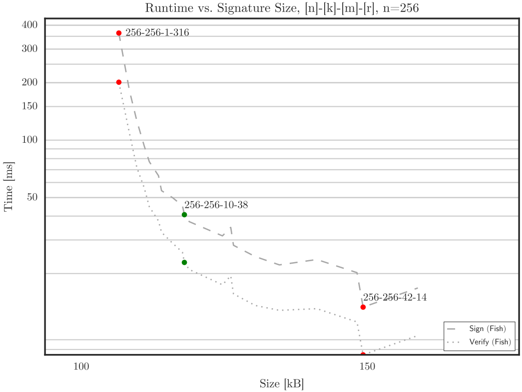

Figure : 128-bit PQ security. Measurements for instance selection (average over 100 runs).

Comparison with other recent proposals

Scheme	Gen	Sign	Verify	$\|sk\|$	$\|pk\|$	$\|\sigma\|$	T	M	PQ
Fish-256-10-38	0.01	29.73	17.46	32	$32/64$	$116K$	$\times$	ROM	✓
MQ 5pass	1.0	7.2	5.0	32	74	$40K$	$\times$	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	$12K$	$8K$	$1.5K$	$\times$	ROM	✓
TESLA-768	$49K$	0.6	0.4	$3.1M$	$4M$	$2.3K$	$\times$	(Q)ROM	✓
FS-Véron	n/a	n/a	n/a	32	160	$126K$	$\times$	ROM	✓
SIHDp751	16	$7K$	$5K$	48	768	$138K$	$\times$	QROM	✓

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

Conclusion and Outlook

Two new efficient post-quantum signature schemes

- Based on LowMC instances

New questions in various directions

- Alternative symmetric primitives with few multiplications
  - Something new, even more crazy than LowMC?
  - 256-bit secure variant of Trivium/Kreyvium?
- More LowMC cryptanalysis
- Analysis regarding side-channels

Thank you.

Preprint: `http://ia.cr/2016/1085`
Full implementations and benchmarking:
`https://github.com/IAIK/fish-begol`

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

Signature Size

Fish

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

OWF represented by arithmetic circuit with

- ringsize λ
- Multiplication-count a

Signaturesize = $c_1 + c_2 \cdot (c_3 + \lambda \cdot a)$ with $c_i = f_i(\kappa)$, reduction of constants using optimizations from ZKB++ [GCZ16]

For Begol: signature size roughly doubles.

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.

[BG89] Mihir Bellare and Shafi Goldwasser.
New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs.
In *CRYPTO*, 1989.

[DOR+16] David Derler, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, and Daniel Slamanig.
Digital signatures from symmetric-key primitives.
IACR Cryptology ePrint Archive, 2016:1085, 2016.

[Fis99] Marc Fischlin.
Pseudorandom function tribe ensembles based on one-way permutations: Improvements and applications.
In *Advances in Cryptology - EUROCRYPT '99*, pages 432–445, 1999.

References II

[FS86] Amos Fiat and Adi Shamir.
How to prove yourself: Practical solutions to identification and signature problems.
In *CRYPTO '86*, 1986.

[GCZ16] Steven Goldfeder, Melissa Chase, and Greg Zaverucha.
Efficient post-quantum zero-knowledge and signatures.
IACR Cryptology ePrint Archive, 2016:1110, 2016.

[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.