Hash-Based Signatures draft-mcgrew-hash-sigs-07

Scott Fluhrer, Michael Curcio, *David McGrew*

IETF 99 Crypto Forum Research Group

What's New

- Updated draft with security tweak
  https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs
- Proof of security
  Further Analysis of a Proposed Hash-Based Signature Standard, Scott Fluhrer, June, 2017, http://eprint.iacr.org/2017/553.pdf
- Comparison with XMSS
  LMS vs XMSS: A comparison of the Stateful Hash-Based Signature Proposed Standards, Panos Kampanakis, Scott Fluhrer, April 2017, http://eprint.iacr.org/2017/349.pdf
- Full-featured C implementation
  https://github.com/cisco/hash-sigs

Security

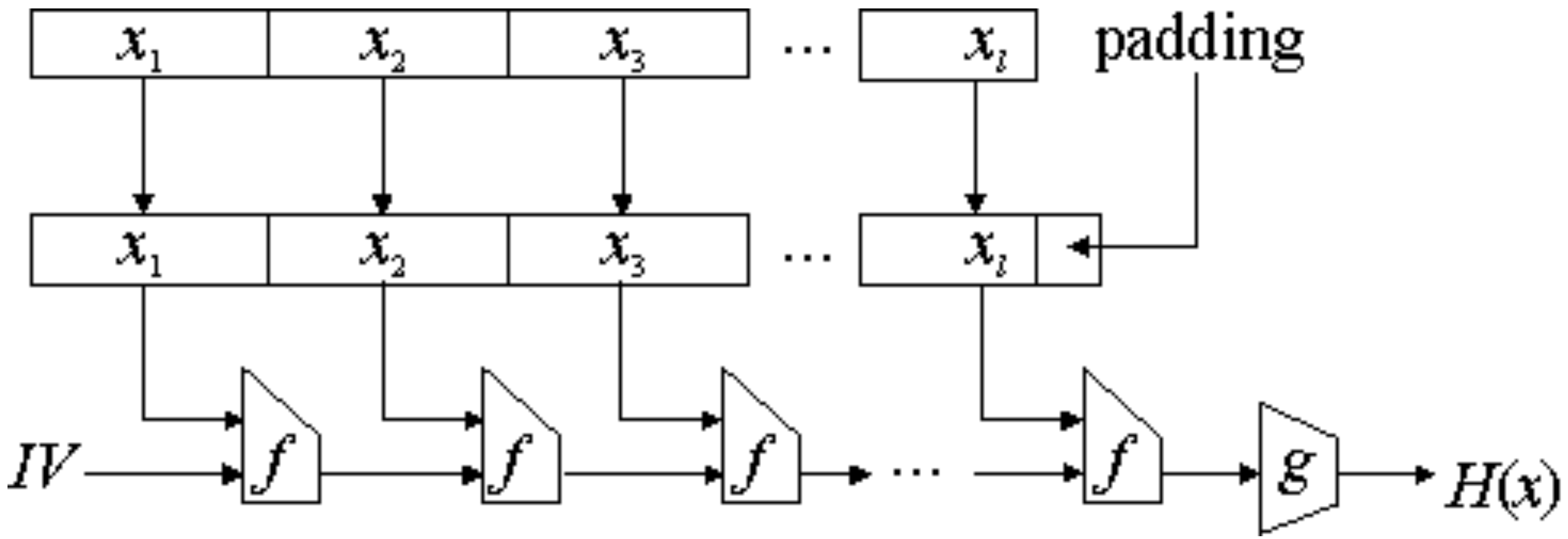
Further Analysis of a Proposed Hash-Based Signature Standard

Scott Fluhrer

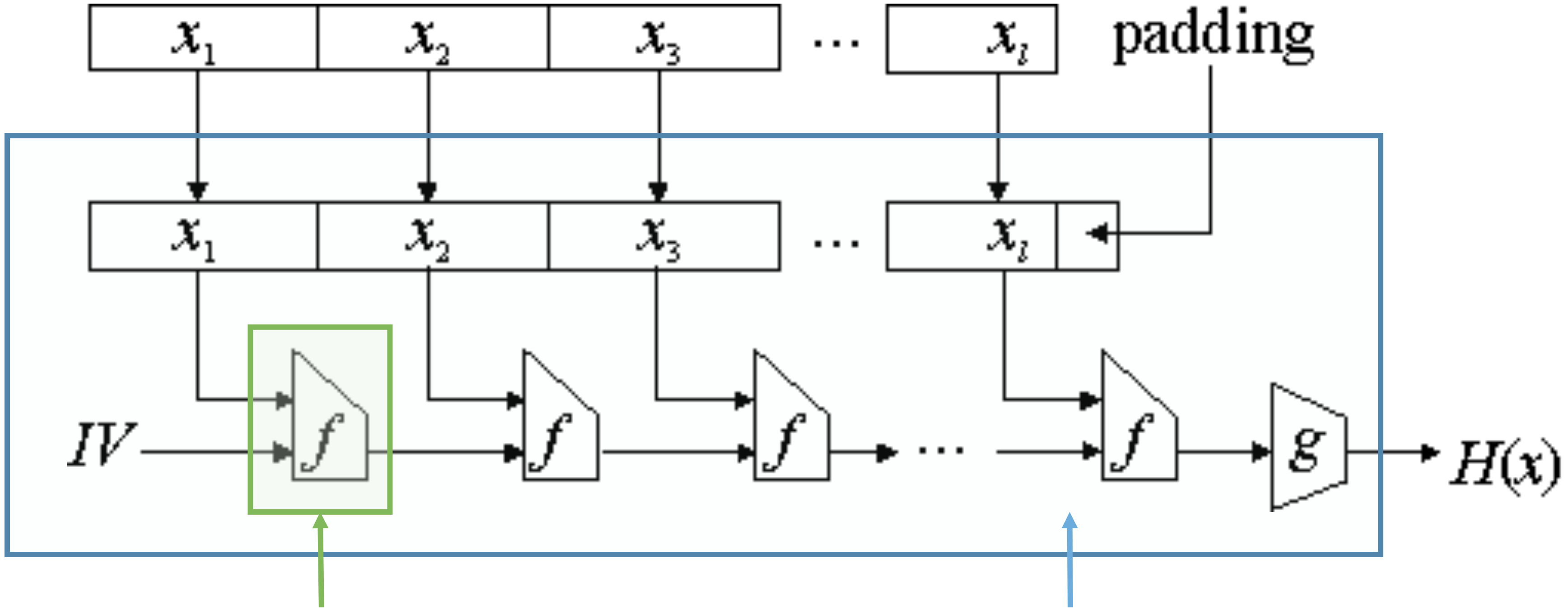
Cisco Systems, USA
sfluhrer@cisco.com

Abstract. We analyze the concrete security of a hash-based signature scheme described in the most recent Internet Draft by McGrew, Fluhrer and Curcio. We perform this analysis in the random-oracle model, where the Merkle-Damgård hash compression function is models as the random oracle. We show that, even with a large number of different keys the attacker can choose from, and a huge computational budget, the attacker succeeds in creating a forgery with negligible probability ($< 2^{-129}$).

MD Hash Security Assumptions



MD Hash Security Assumptions



Compression Function
is a Random Oracle

Hash is a Random Oracle

Post Quantum Security

Leighton-Micali Hash-Based Signatures in the Quantum Random-Oracle Model

Edward Eaton

ISARA Corporation <ted.eaton@isara.com>
and University of Waterloo, Canada

Abstract. Digital signatures constructed solely from hash functions offer competitive signature sizes and fast signing and verifying times. Moreover, the security of hash functions against a quantum adversary is believed to be well understood. This means that hash-based signatures are strong candidates for standard use in a post-quantum world. The Leighton-Micali signature scheme (LMS) is one such scheme being considered for standardization. However all systematic analyses of LMS have only considered a classical adversary. In this work we close this gap by showing a proof of the security of LMS in the quantum random-oracle model. Our results match the bounds imposed by Grover's search algorithm within a constant factor, and remain tight in the multi-user setting.

From https://eprint.iacr.org/2017/607.pdf

Performance

Operation	LMS	XMSS	XMSS / LMS ratio
	XMSSMT_SHA2-256_W16_H20_D2		
PK Gen	0.89 s	3.26 s	3.66
Sign	1.21 ms	4.72 ms	3.90
Verify	0.339 ms	1.76 ms	5.19
	XMSSMT_SHA2-256_W16_H40_D2		
PK Gen	720 s	3340 s	4.64
Sign	1.91 ms	7.70 ms	4.03
Verify	0.350 ms	1.75 ms	5.00

Table 6: Measured time per operation for LMS and XMSS

LMS is over
3X Faster

From http://eprint.iacr.org/2017/349.pdf

Next Steps

- Please review draft-07, security analysis, and comparison
- Request CFRG last call for RFC
  - Diversity of HBS mechanisms is good for security
  - Feedback from many reviewers
  - Multiple implementations
  - Attractive performance
  - Based on well established techniques

Thank You