



Practical Authentication and Access Control for Software-Defined Networking over Optical Networks

SecSoN 2018

Joo Yeon Cho and Thomas Szyrkowiec

24 August 2018

Security in Optical Transmission

Tapping of Optical Fiber is Reality

The screenshot shows the Guardian website's header with navigation links for 'UK', 'world', 'politics', 'sport', 'football', 'opinion', 'culture', 'business', 'lifestyle', 'fashion', 'environment', 'tech', and 'travel'. The main headline reads 'GCHQ taps fibre-optic cables for secret access to world's communications'. Below the headline, it states 'Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them with NSA, latest documents from Edward Snowden reveal'. The article is attributed to Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, dated Friday 21 June 2013. Social media sharing options for Facebook, Twitter, and LinkedIn are visible, along with 882 shares and 3,404 comments. The GCHQ logo and the title 'MASTERING THE INTERNET (MTI)' are also present.

UK Government Communications Headquarter
– GCHQ –



“The Guardian” Report:

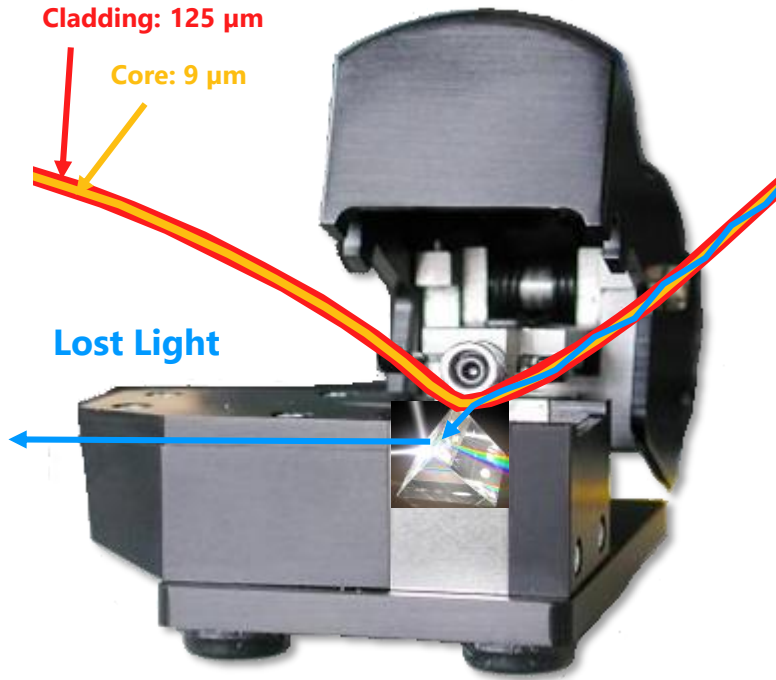
... GCHQ was ... tapping in to 200 fiber-optic cables to give it the ability to monitor up to 600 million communications every day ...

... the GCHQ operation codenamed “Tempora” has been running for 18 months ...

... information from Internet and phone use was stored for up to 30 days to be shifted and analyzed ...

Fiber Optic Networks

Optical Tapping Method



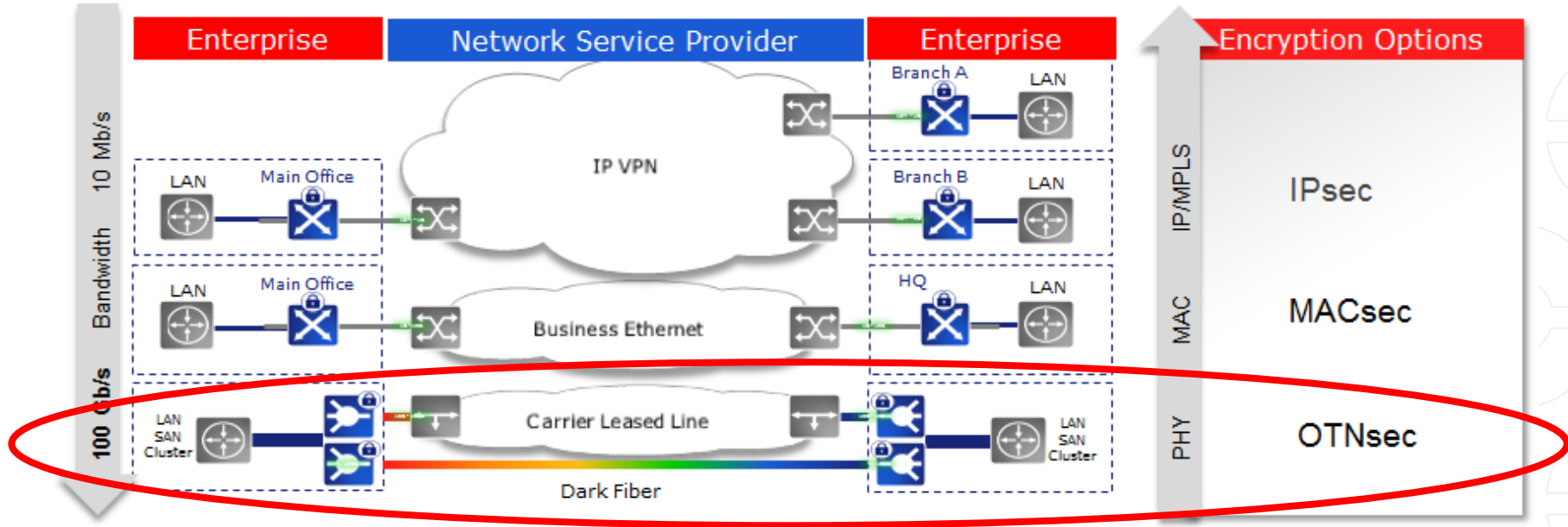
NETWORKWORLD
THE CONNECTED ENTERPRISE

“For both public and private networks, optical taps and analytic devices are required and inexpensive maintenance equipment in common use worldwide today. **Various types of optical taps [...] are also used for corporate espionage...**”

„Clearly, **physical protection** of optical transmission media and junction boxes is **essential**; in addition, **data encryption plays a role in protecting sensitive data.**” [5]

[5] Security Strategies Alert, M.E. Kabay, already in March 2003

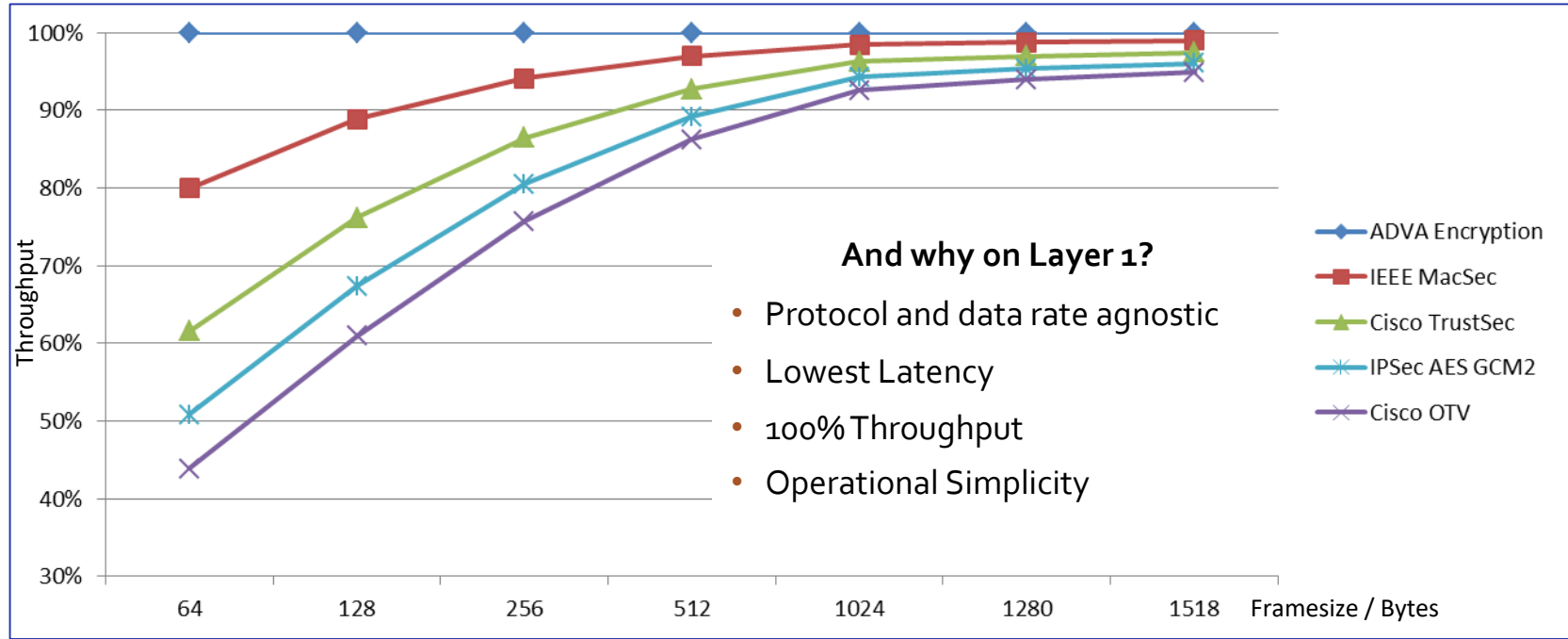
OTN (Layer 1) Security



High throughput, low latency and cost-effective trust model

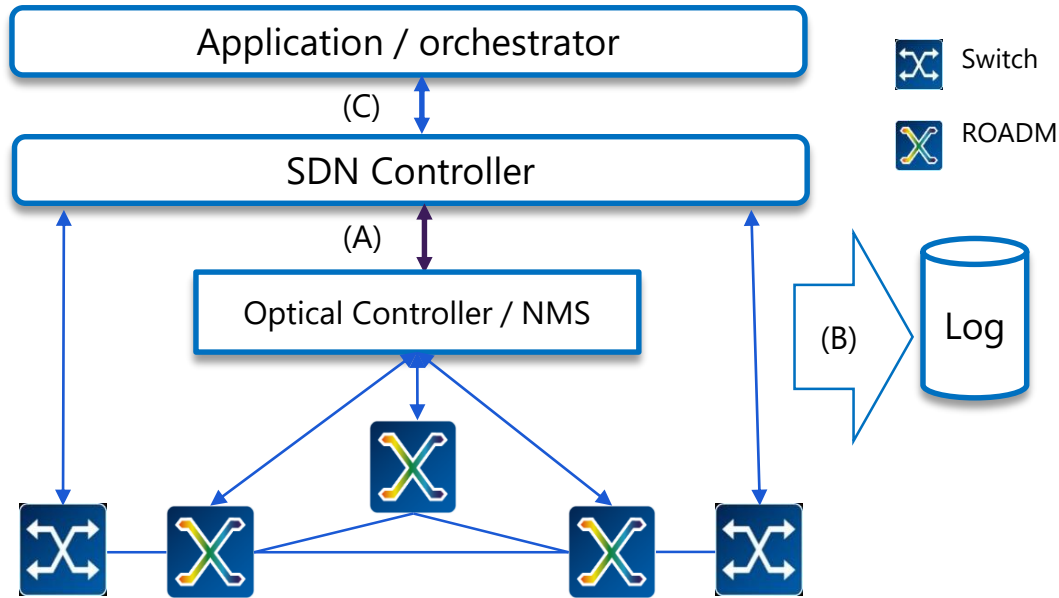
Encryption Performance

Comparison of Maximum Throughput

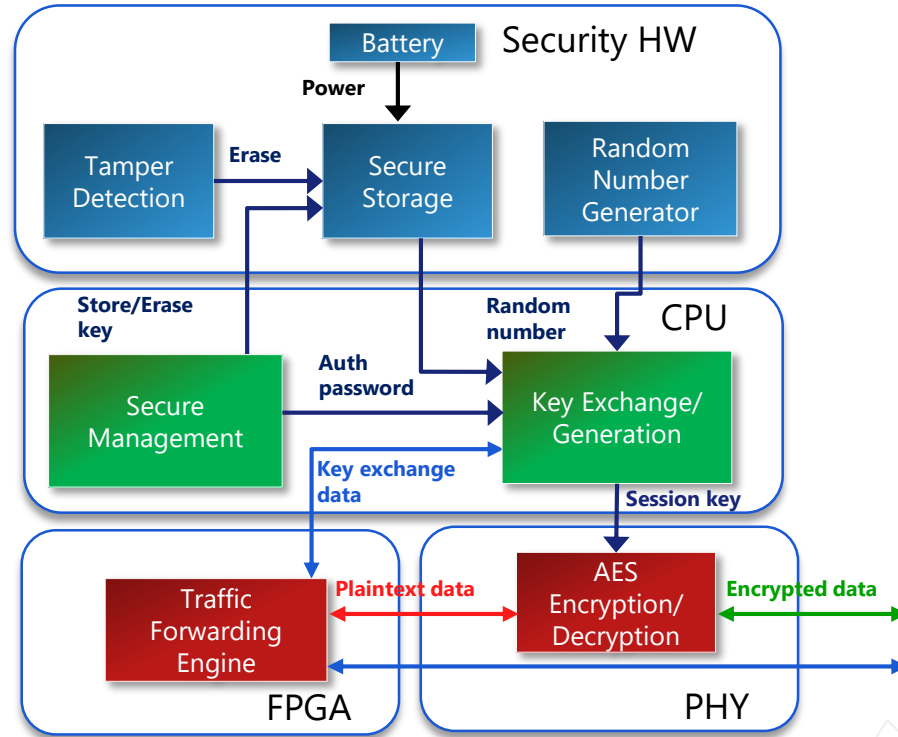


SDN over Optical Network

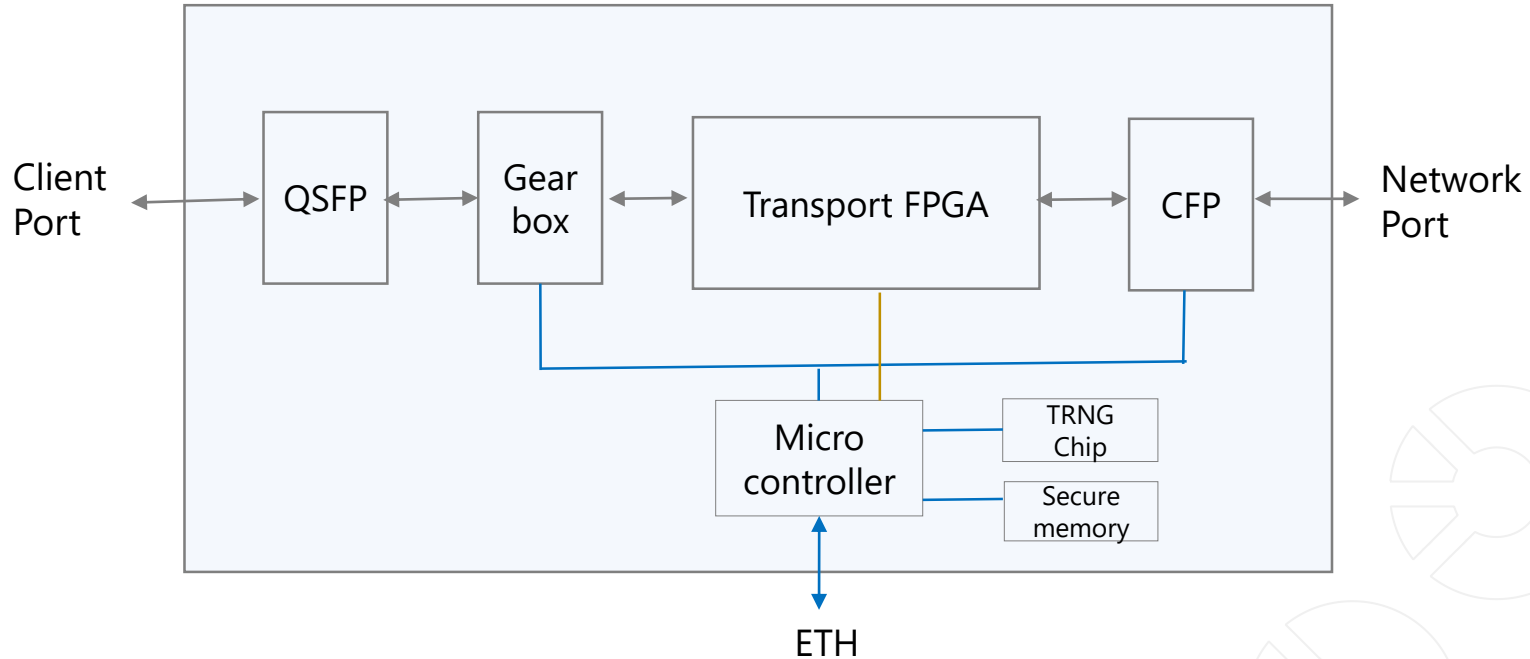
Software-Defined Networking over Optical Networks



System Architecture: Example



Example: HW block diagram



Security Requirements for SDN

- Encryption: AES-256
- Authentication: password-based, certificate-based
- Integrity: GCM
- Key exchange: Diffie-Hellman, PKI
- Access control
- Accountability
- Etc.

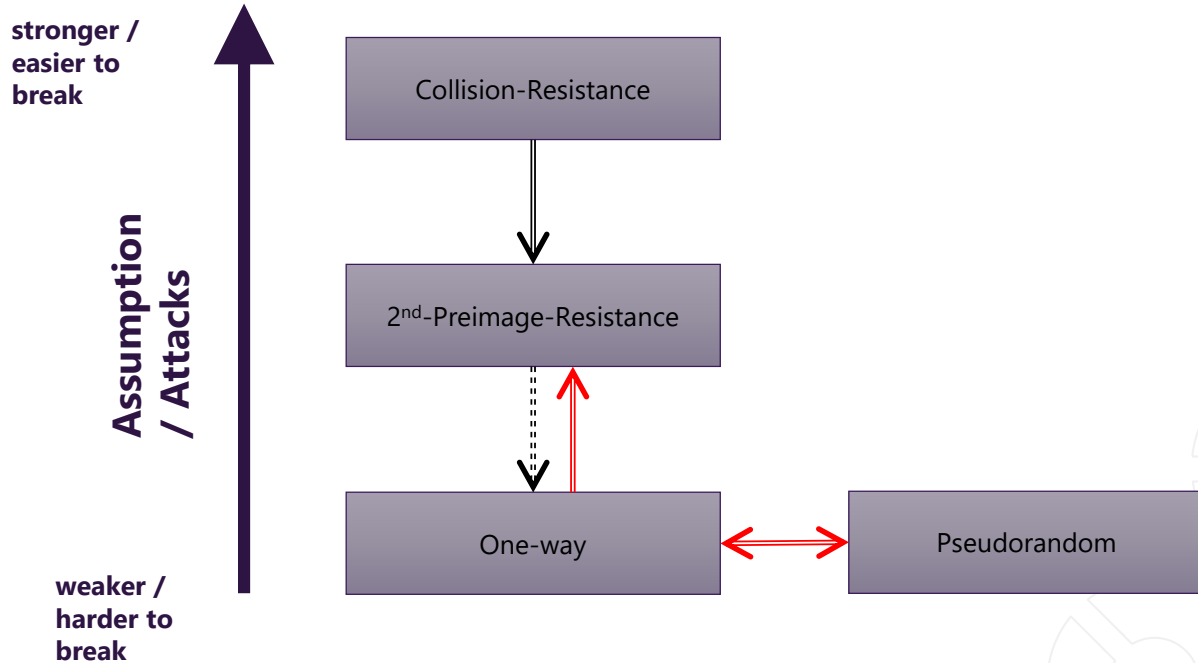
Lightweight AAA solution

- SSL/TLS is a bit heavy.
=> it should be cross-compiled and installed, depending on CPU and OS.
 - Traditional signature scheme: vulnerable to the quantum attacks?
- => A lightweight/quantum-secure AAA solution is preferred for optical devices.

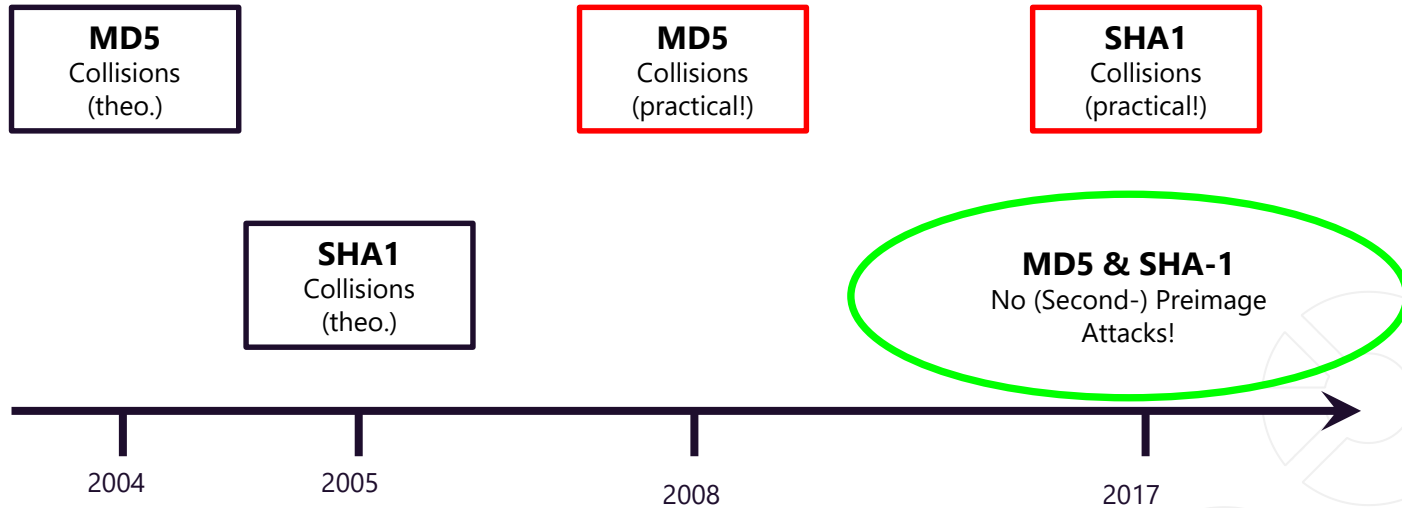
Hash-based Signature



Hash-function properties



Attacks on Hash Functions



Lamport-Diffie OTS (one time signature) [Lam79]

Message $M = b_1, \dots, b_m$

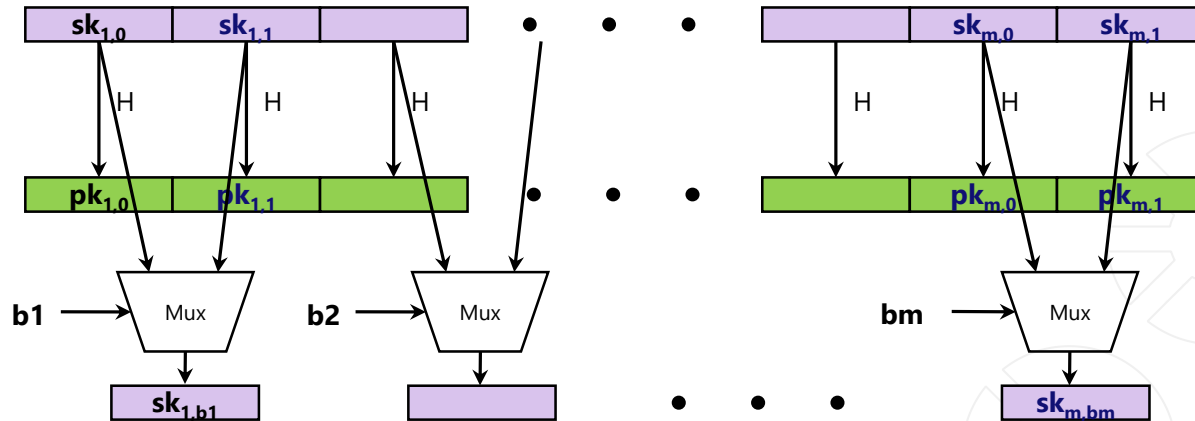
* = n bit

H: one-way function

SK

PK

Sig

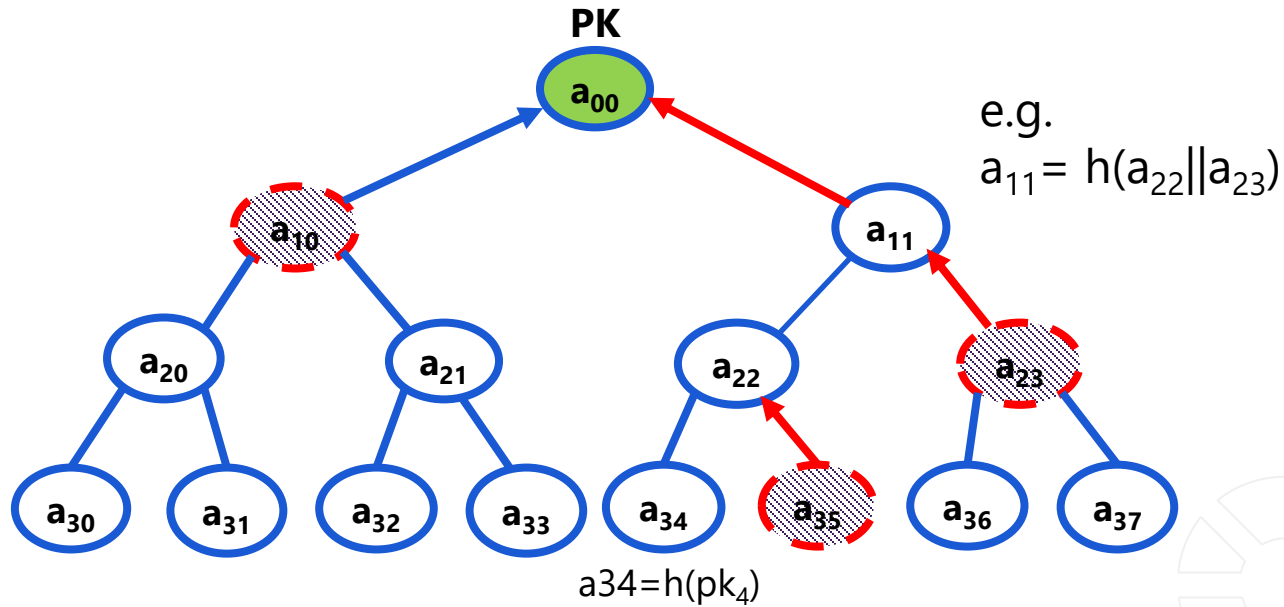


Security

Theorem:

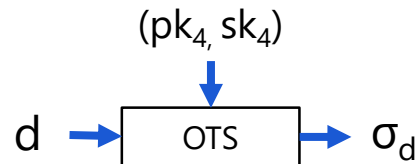
If H is one-way then LD-OTS is one-time eu-cma-secure.

Merkle's Hash-based Signature [MSS 1970s]



h : hash func.

OTS: one time signature



Security

Theorem:

MSS is eu-cma-secure if OTS is a one-time eu-cma secure signature scheme and H is a random element from a family of collision resistant hash functions.

XMSS: eXtended Merkle Signature Scheme (2018)

- Internet draft: RFC 8391
- Several tricks are applied.
 - signature size halved
 - OTS: WOTS+
 - function families based on SHA2 / SHA3
- Small public key (2n bit)

Internet Research Task Force (IRTF)
Request for Comments: 8391
Category: Informational
ISSN: 2070-1721

A. Huelsing
TU Eindhoven
D. Butin
TU Darmstadt
S. Gazdag
genua GmbH
J. Rijnveld
Radboud University
A. Mohaisen
University of Central Florida
May 2018

XMSS: eXtended Merkle Signature Scheme

Abstract

This note describes the eXtended Merkle Signature Scheme (XMSS), a hash-based digital signature system that is based on existing descriptions in scientific literature. This note specifies Winternitz One-Time Signature Plus (WOTS+), a one-time signature scheme; XMSS, a single-tree scheme; and XMSS^{MT}, a multi-tree variant of XMSS. Both XMSS and XMSS^{MT} use WOTS+ as a main building block. XMSS provides cryptographic digital signatures without relying on the conjectured hardness of mathematical problems. Instead, it is proven that it only relies on the properties of cryptographic hash functions. XMSS provides strong security guarantees and is even secure when the collision resistance of the underlying hash function is broken. It is suitable for compact implementations, is relatively simple to implement, and naturally resists side-channel attacks. Unlike most other signature systems, hash-based signatures can so far withstand known attacks using quantum computers.

XMSS Implementation [HRS16]

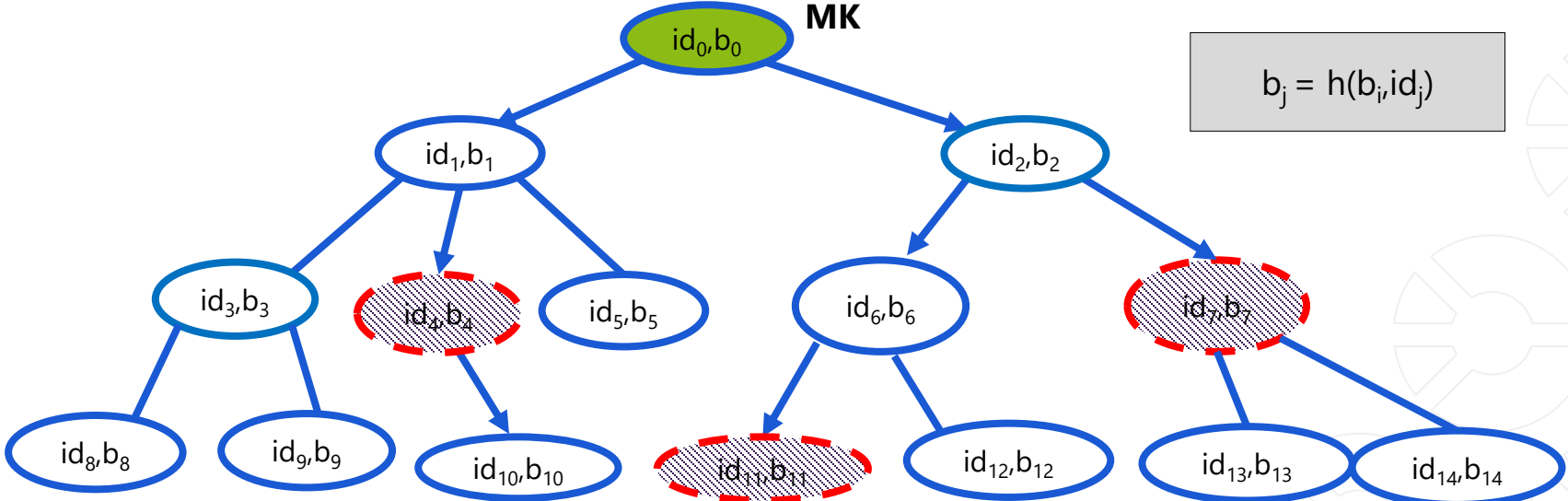
[HRS16] Huelsing, A., Rijneveld, J., and F. Song, "Mitigating Multi-Target Attacks in Hash-based Signatures", Public-Key Cryptography - PKC, 2016.

C Implementation, using OpenSSL

	Sign (ms)	Signature (kB)	Public Key (kB)	Secret Key (kB)	Bit Security classical/quantum	Comment
XMSS	3.24	2.8	1.3	2.2	236 / 118	$h = 20,$ $d = 1,$
XMSS	3.59	8.3	1.3	14.6	196 / 98	$h = 60,$ $d = 3$

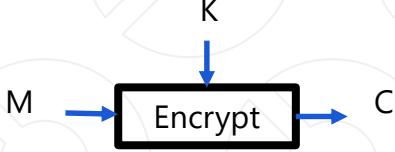
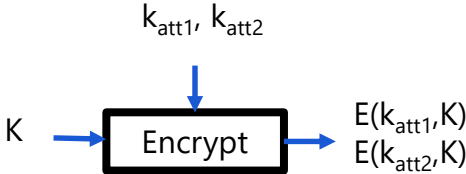
Intel(R) Core(TM) i7 CPU @ 3.50GHz

Attribute-based Access Control

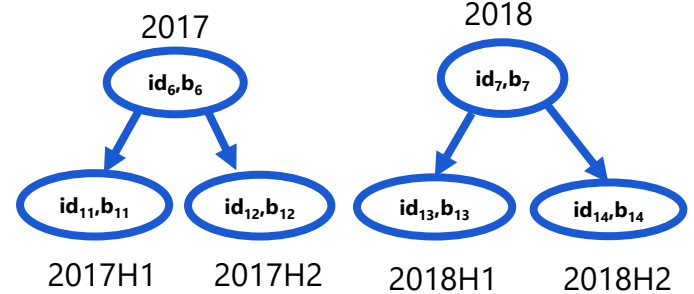


$$k_{att1} = h(b_4, b_{11})$$

$$k_{att2} = h(b_7)$$



Use case: Auditing log data



(1) "Submit the log data from 2017H2-2018."



(2) "Here is b₇ and b₁₂."

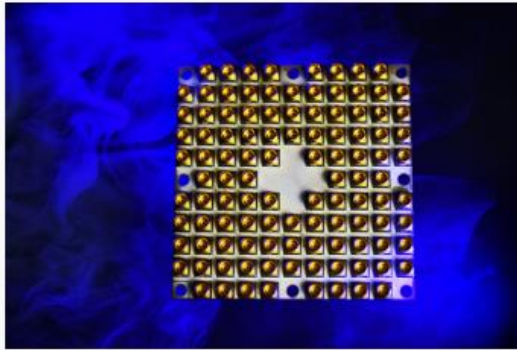


✓ A system admin does not need to search/encrypt/submit the specific log data.

Quantum-safe Security



The Rise of Quantum Computing



Intel's 49-qubit chip
"Tangle-Lake"
January 2018



Google's 72-qubit chip
"Bristlecone"
March 2018



IBM's 50-qubit
quantum computer
November 2017

NIST Post-quantum crypto project

Timeline

- Aug 2016 – Draft submission requirements & evaluation criteria
- Dec 2016 – Final requirements and criteria
- Nov 2017 – Deadline for submissions
- Apr 2018 – NIST PQC Workshop – submitters' presentations
- 2018/2019 – 2nd Round begins (smaller number of submissions)
 - minor changes allowed
- Aug 2019 – 2nd NIST PQC Workshop
- 2020/2021 - Select algorithms or start a 3rd Round
- 2022-2024 - Draft standards available

- NIST will release reports on progress and selection rationale

Submissions

- 37 preliminary submissions (early deadline Sep 2017)
- 82 total submissions received
 - 69 accepted as "complete and proper" (5 since withdrawn)

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric/Hash-based	3		3
Other	2	5	7
Total	19	45	64

Summary and on-going work

- A lightweight / quantum-secure hash-based authentication and an access control mechanism for optical SDN are presented.
- Proposed schemes are flexible and easily-deployable.
- Suitable for relatively small scale of network.
- The proposed mechanisms are based on Merkle hash tree and the security relies only on hash functions.
- We are working on the integration with open source SDN controller such as ONOS or Ryu.
- A python-based mutual authentication will be performed between a SDN controller and network devices.

Acknowledgements

This work has been performed in the framework of the CELTIC EUREKA project SENDATE-Secure-DCI (Project ID C2015/3-4), and it is partly funded by the German BMBF (Project ID 16KIS0477K).



Federal Ministry
of Education
and Research



Thank you

jcho@advaoptical.com



IMPORTANT NOTICE

The content of this presentation is strictly confidential. ADVA Optical Networking is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited.

The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA Optical Networking shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation.

Copyright © for the entire content of this presentation: ADVA Optical Networking.

