Hash-based Signatures

IETF/IRTF CFRG Draft on XMSS

Fraunhofer Workshop Series 01 – Post-Quantum Cryptography in Practice

Speaker: Dr. Bernhard Jungk

Fraunhofer SINGAPORE

eXtended Merkle Signature Scheme

Fraunhofer SINGAPORE

eXtended Merkle Signature Scheme

Why should we look into XMSS?

Hash-based signatures have many advantages:

- Based on well understood security notions
  - Cryptographic hash functions are hard to invert, **also for quantum computers**
  - Merkle trees well studied since the 1980ies
- Hash functions are well understood (especially after SHA-3 competition)
- Fast signing and verification operations possible
- Relatively easy to understand and implement

eXtended Merkle Signature Scheme

Why should we look into XMSS?

XMSS is a promising candidate for

- Applications with relatively low amount of signatures
- One- or many-times firmware updates
- Digital signatures for documents (e.g. contracts, email)
- Long-term archival of important digital assets
- PKI Certificates (e.g. Root CA)

eXtended Merkle Signature Scheme

Why should we look into XMSS?

IRTF is part of IETF

- Oriented towards research and long-term trends

Important trend – PQC

- Quantum computer attacks are likely
- Design of replacements for traditional public key crypto

Standardization needed

- Interoperability
- Implementation Guidelines

eXtended Merkle Signature Scheme

Our Contribution

Implementation experience

- Benchmarking against other schemes
- Learn good trade-offs for different application scenarios, cost reductions, side-channels, etc.

Target Platform: Hardware, i.e. FPGAs and ASICs

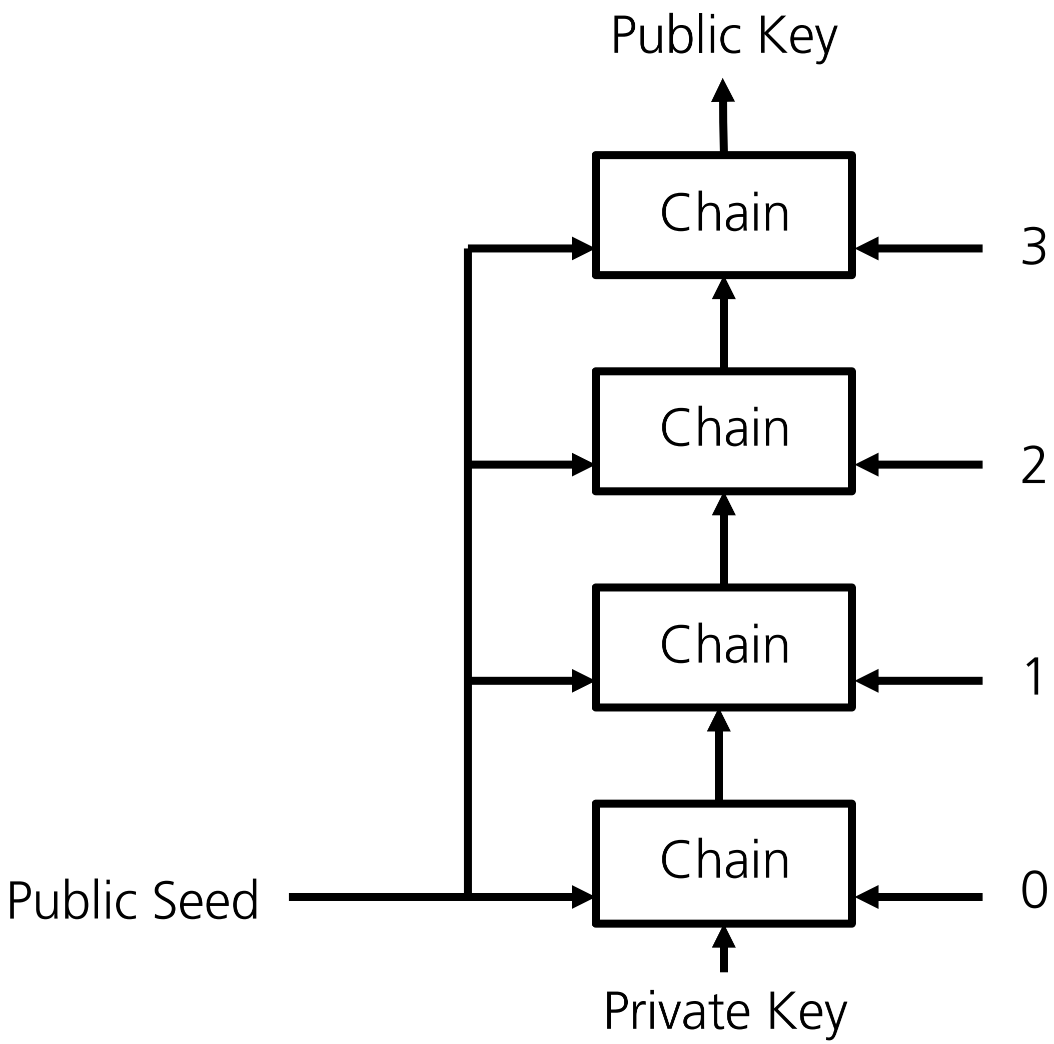
Cooperation:

- Yale University in New Haven, US
- Fraunhofer SIT in Darmstadt, Germany
- Fraunhofer Singapore

Recap Winternitz One-Time Signatures

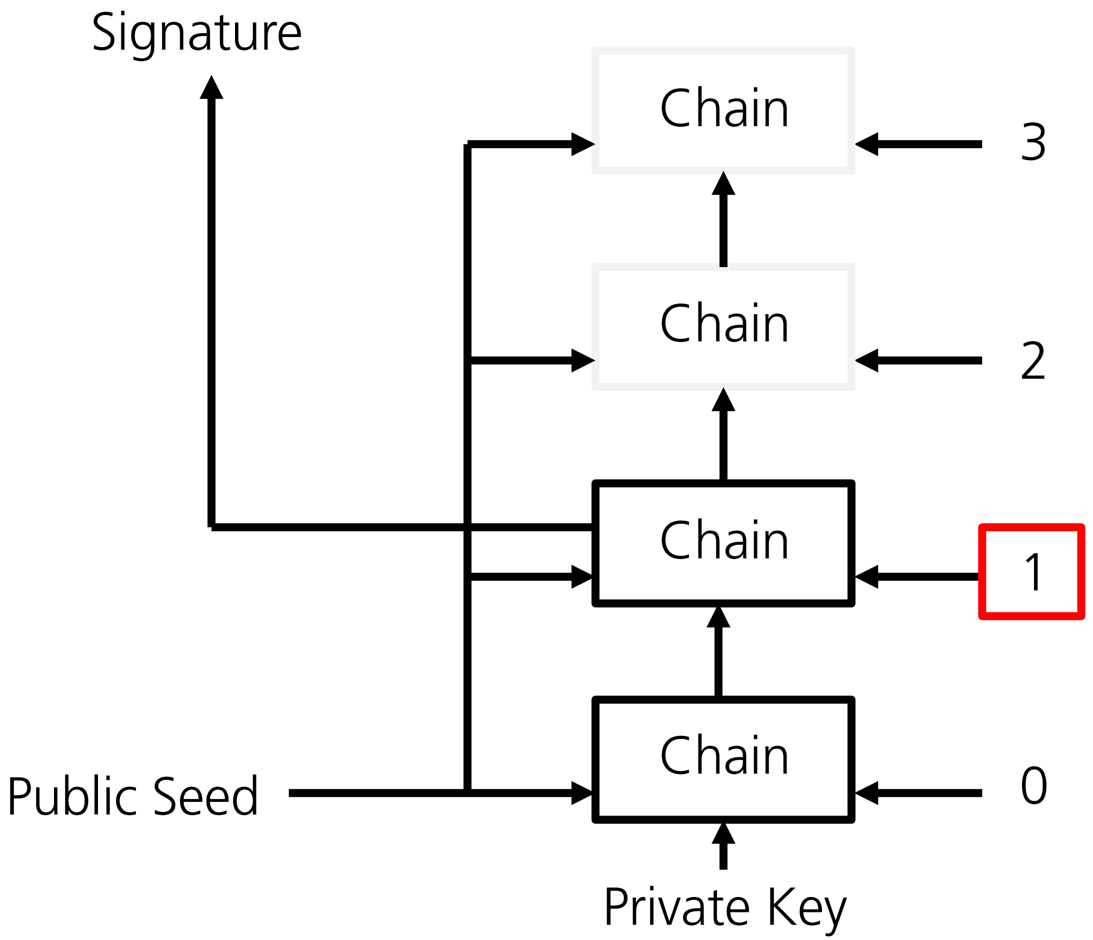
Winternitz One-Time Scheme+

Basic Principle – Public Key Generation



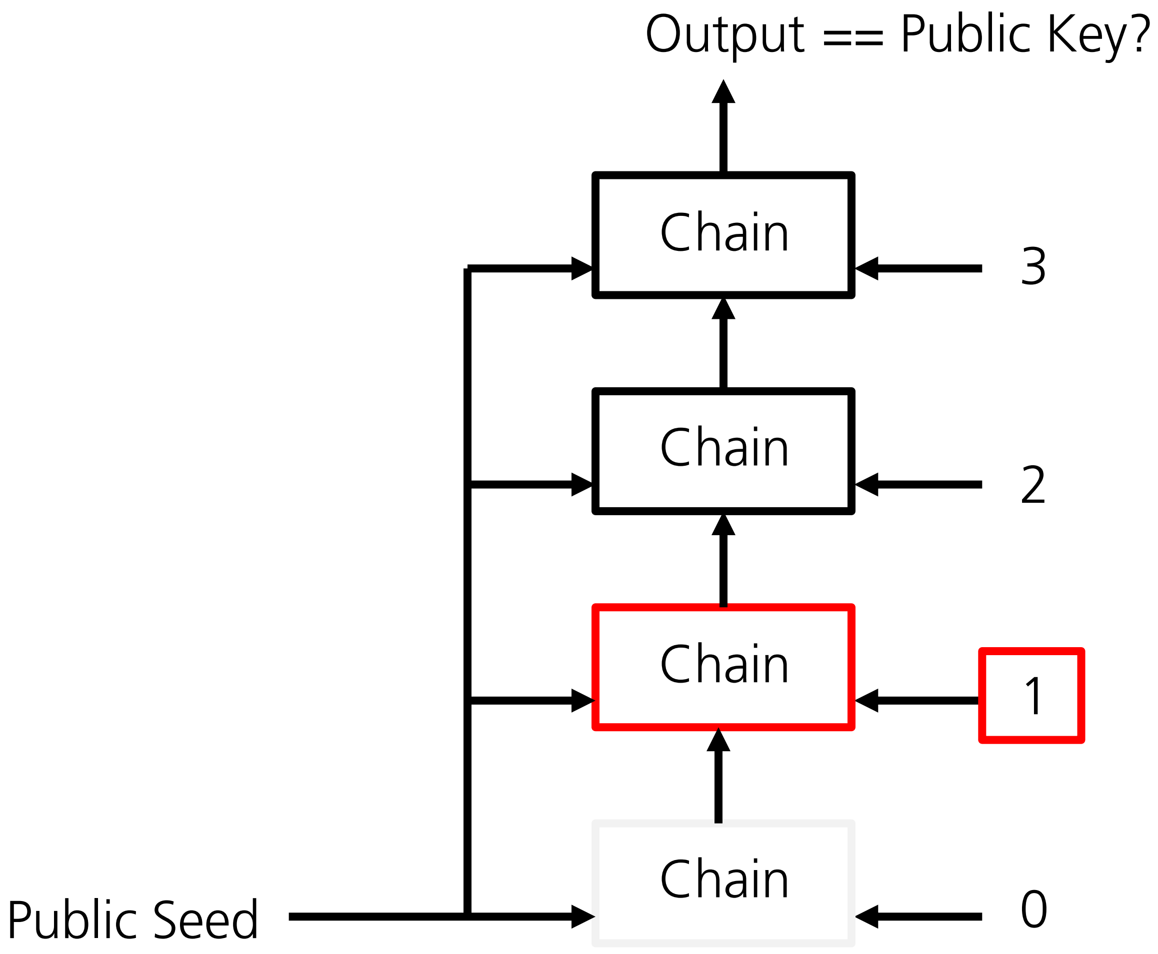
Winternitz One-Time Scheme+

Basic Principle – Signature Generation



Winternitz One-Time Scheme+

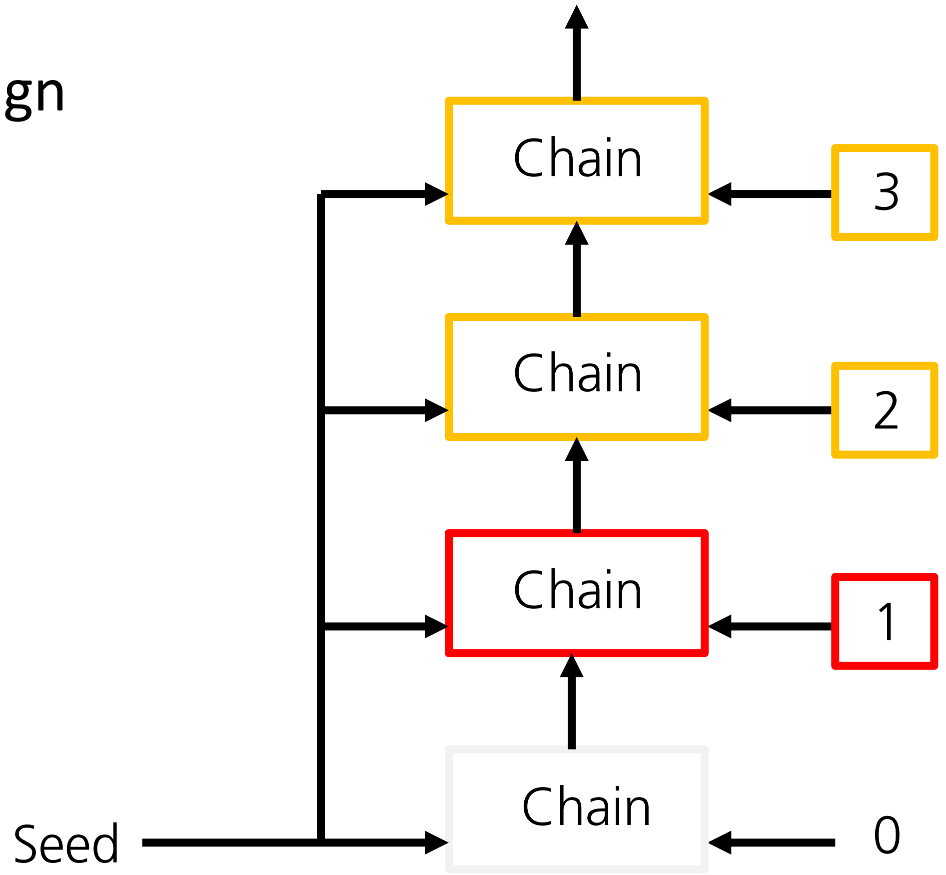
Basic Principle – Signature Verification



Winternitz One-Time Scheme+

Basic Principle

Problem:
Signer reveals how to sign other messages with the same key

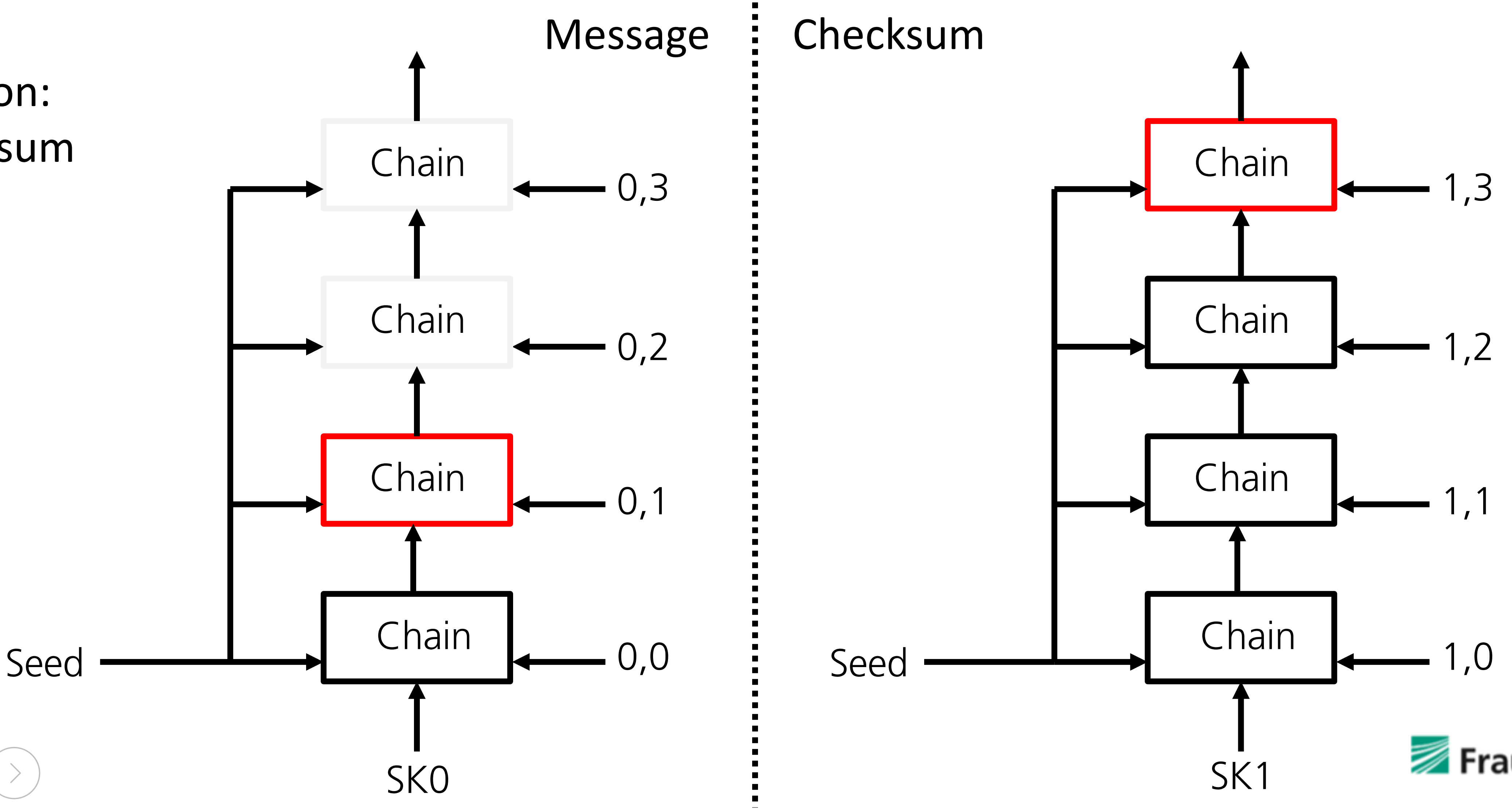


Fraunhofer SINGAPORE

Winternitz One-Time Scheme+

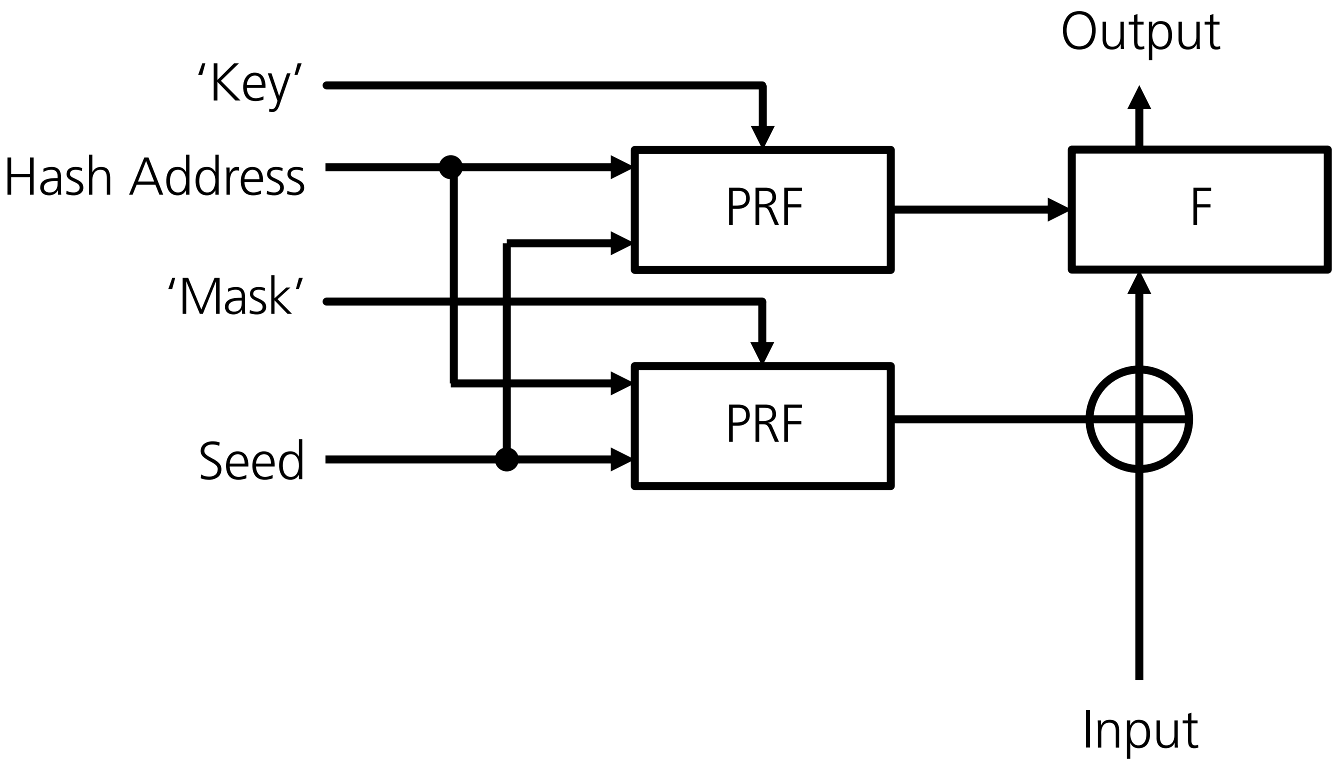
Basic Principle

Solution: Checksum



Winternitz One-Time Scheme+

Chaining Function for XMSS



PRF – Pseudorandom function

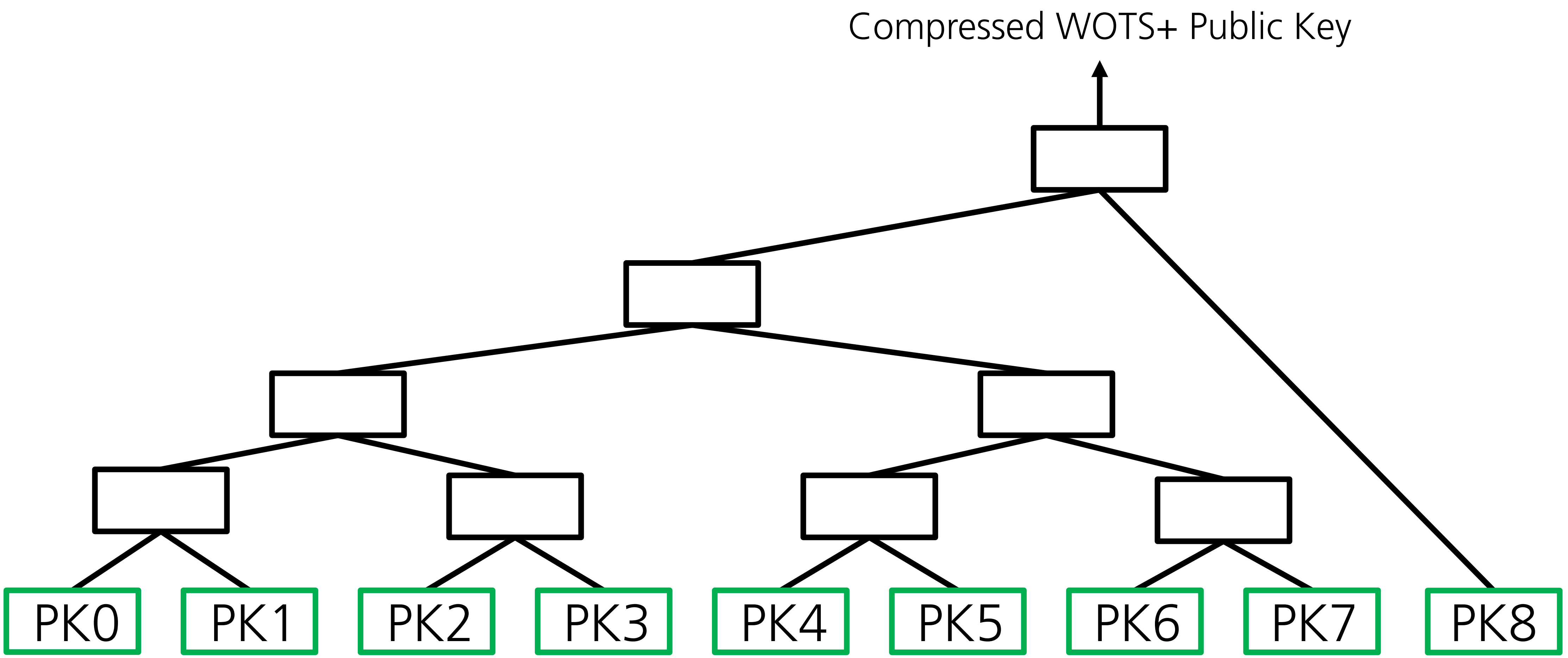
F – Keyed hash function

Fraunhofer SINGAPORE

eXtended Merkle Signature Scheme

eXtended Merkle Signature Scheme

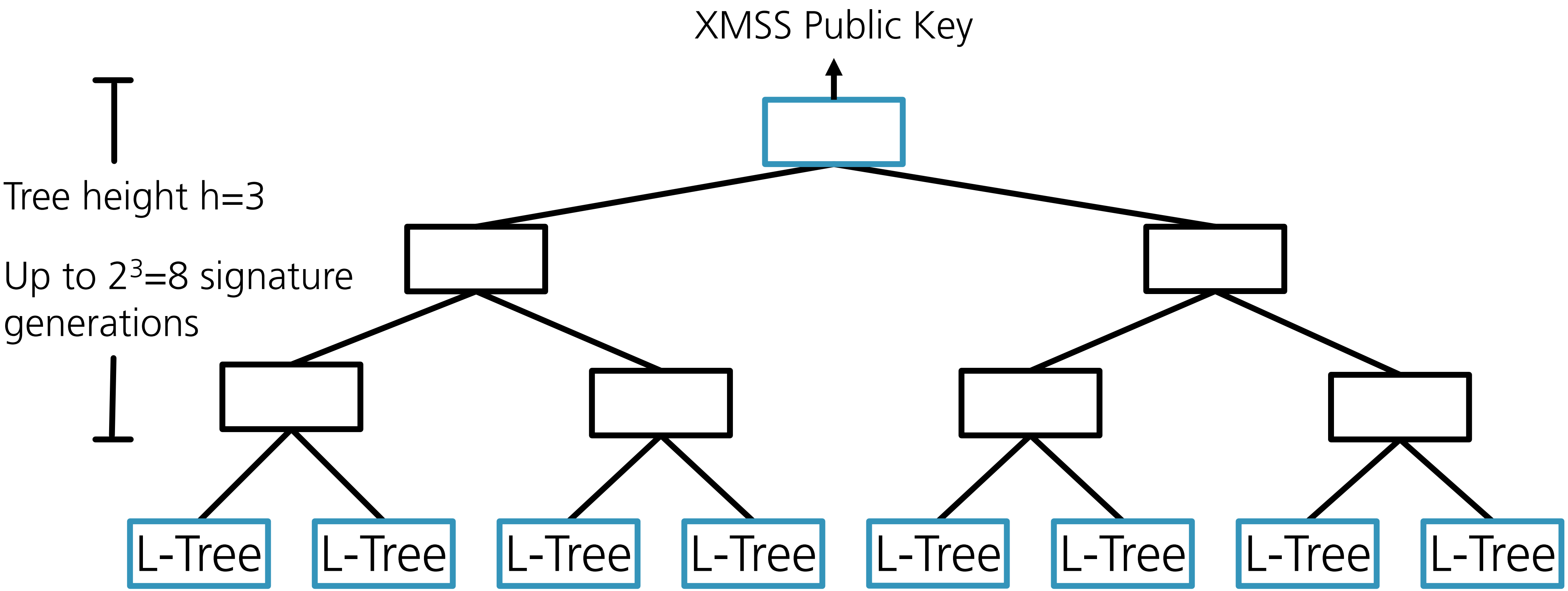
L-Tree – Public Key Generation



Fraunhofer SINGAPORE

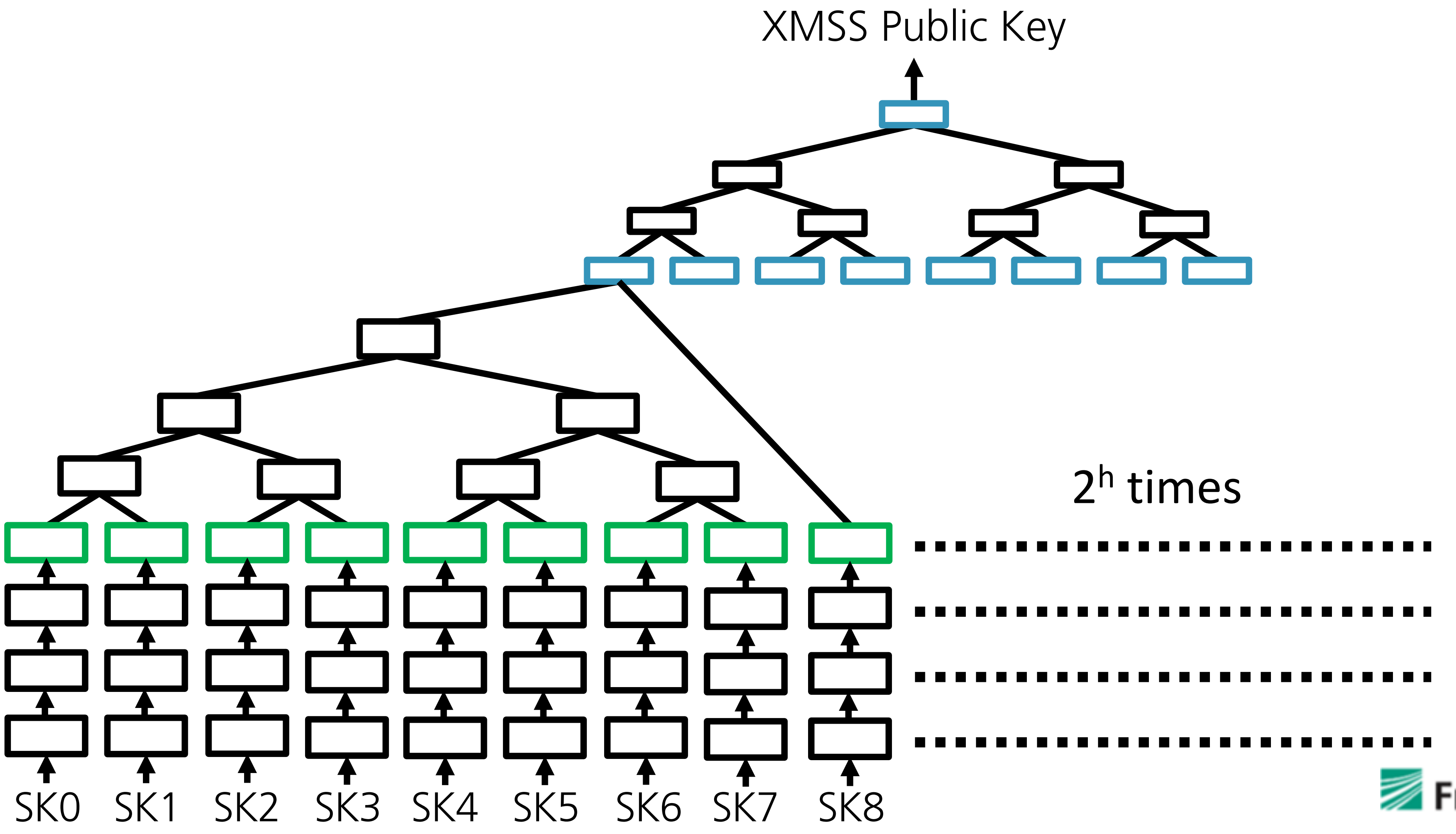
eXtended Merkle Signature Scheme

XMSS Tree – Public Key Generation



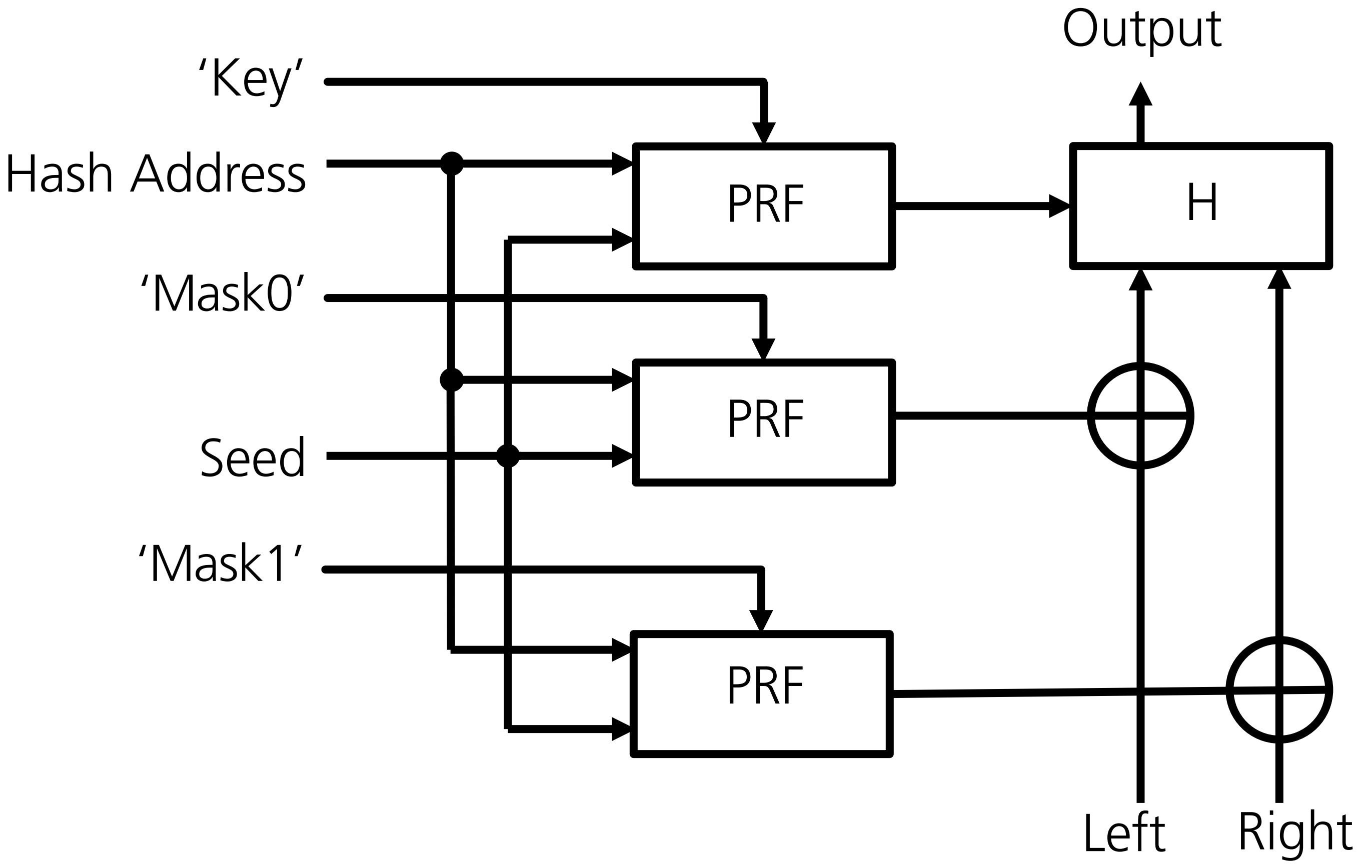
eXtended Merkle Signature Scheme

The Complete Picture – Public Key Generation



eXtended Merkle Signature Scheme

rand_hash



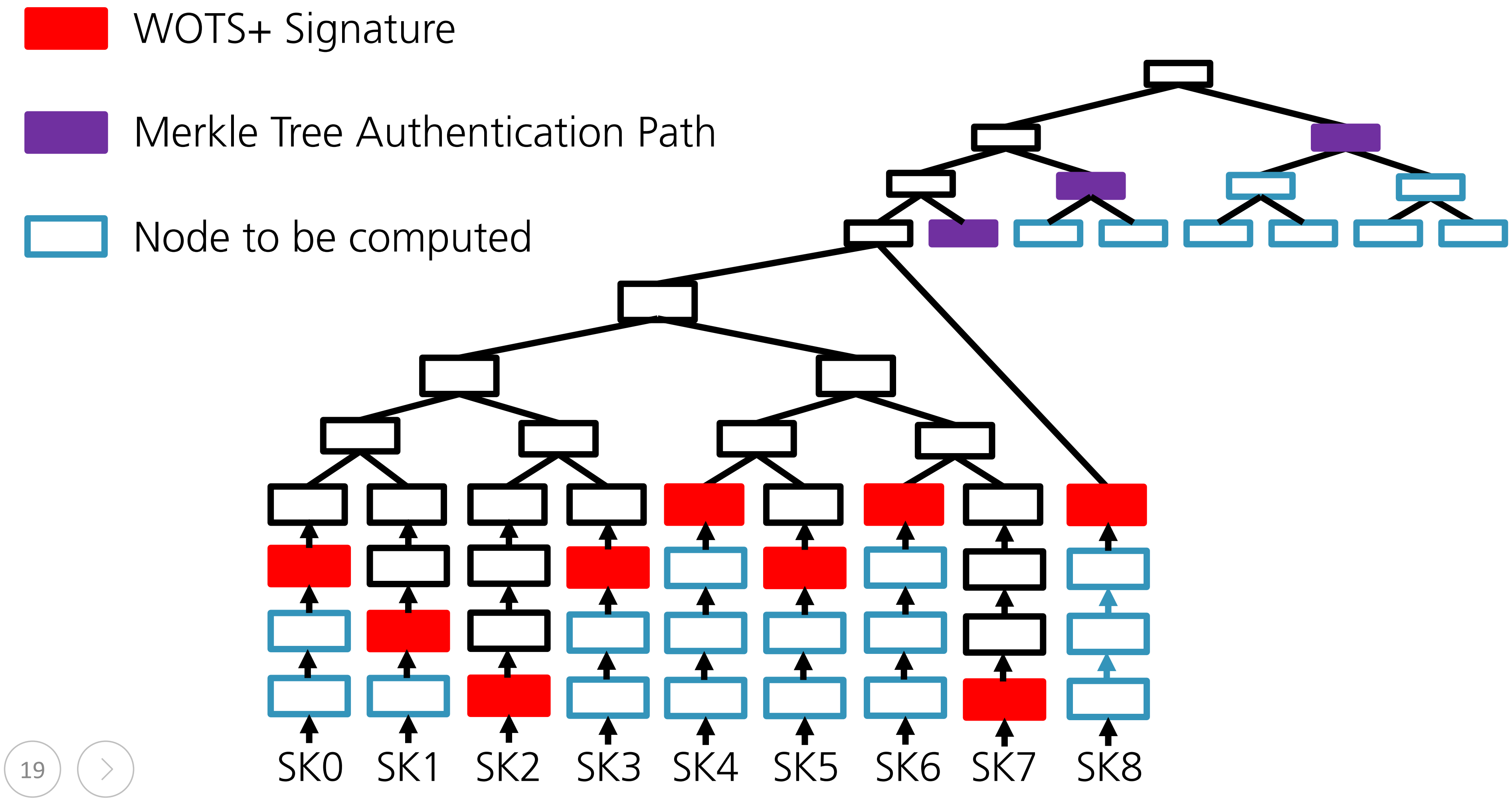
PRF – Pseudorandom function

H – Keyed hash function

Fraunhofer SINGAPORE

eXtended Merkle Signature Scheme

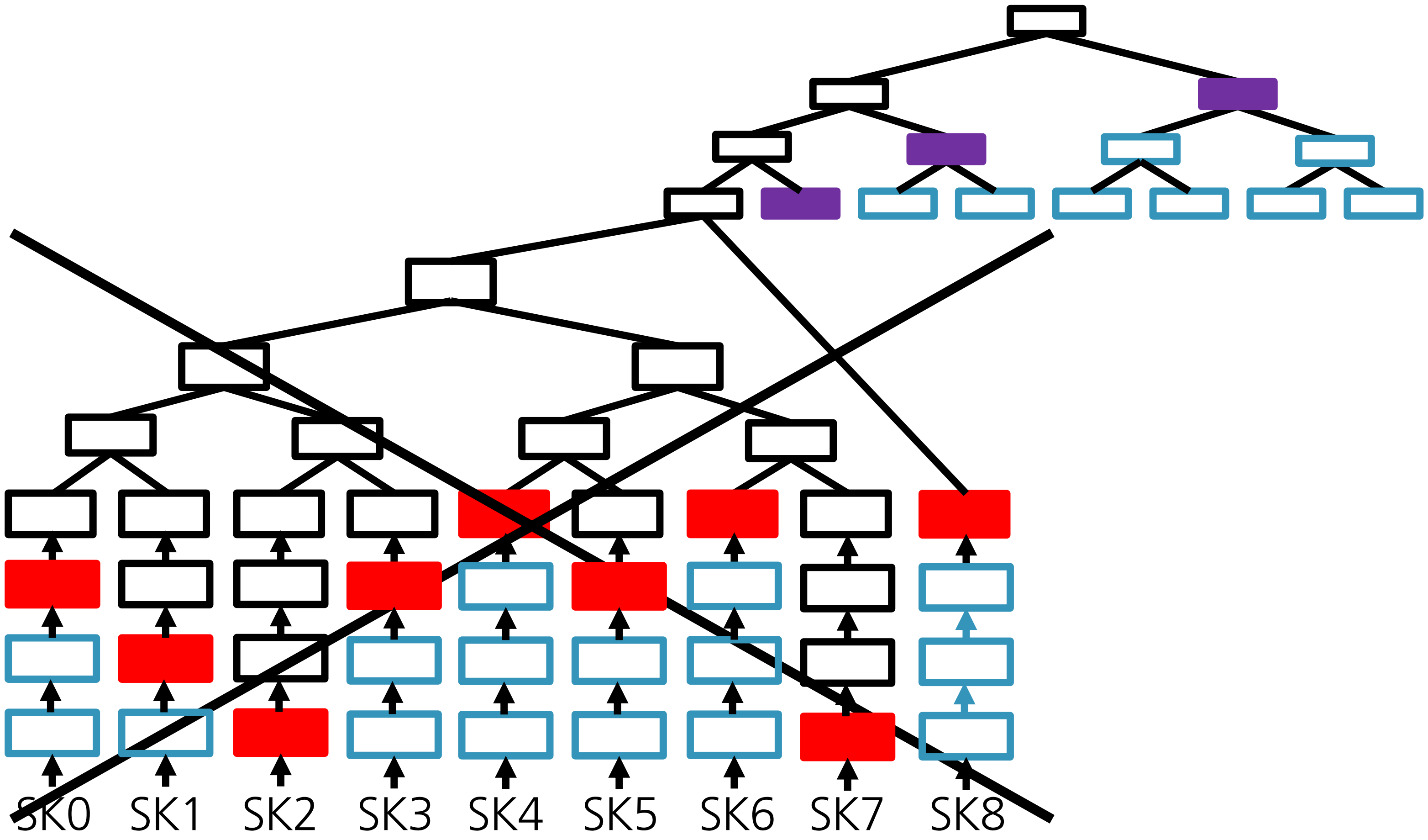
Signature Generation – Message 1



Fraunhofer SINGAPORE

eXtended Merkle Signature Scheme

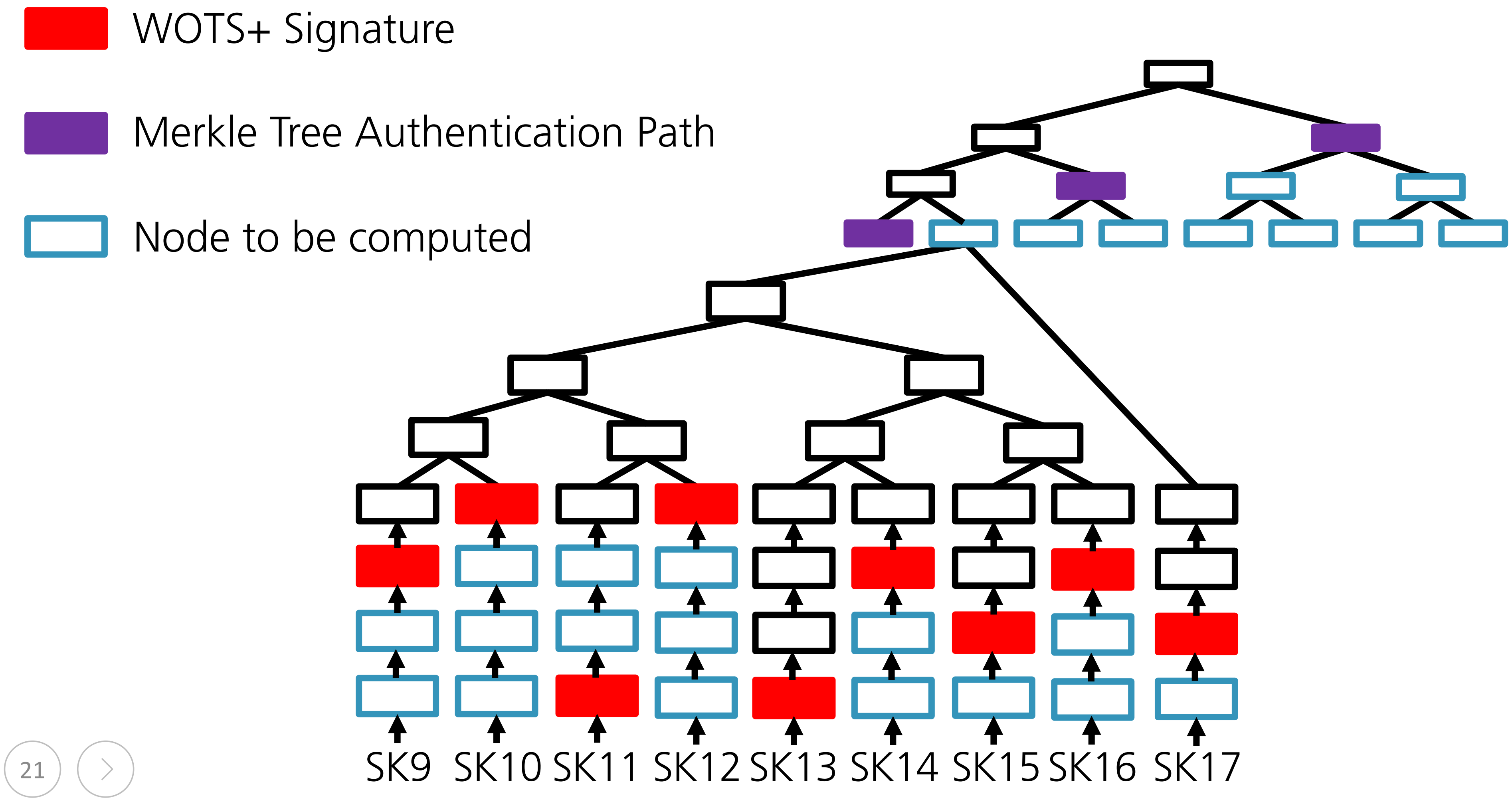
Signature Generation – Message 1



Fraunhofer SINGAPORE

eXtended Merkle Signature Scheme

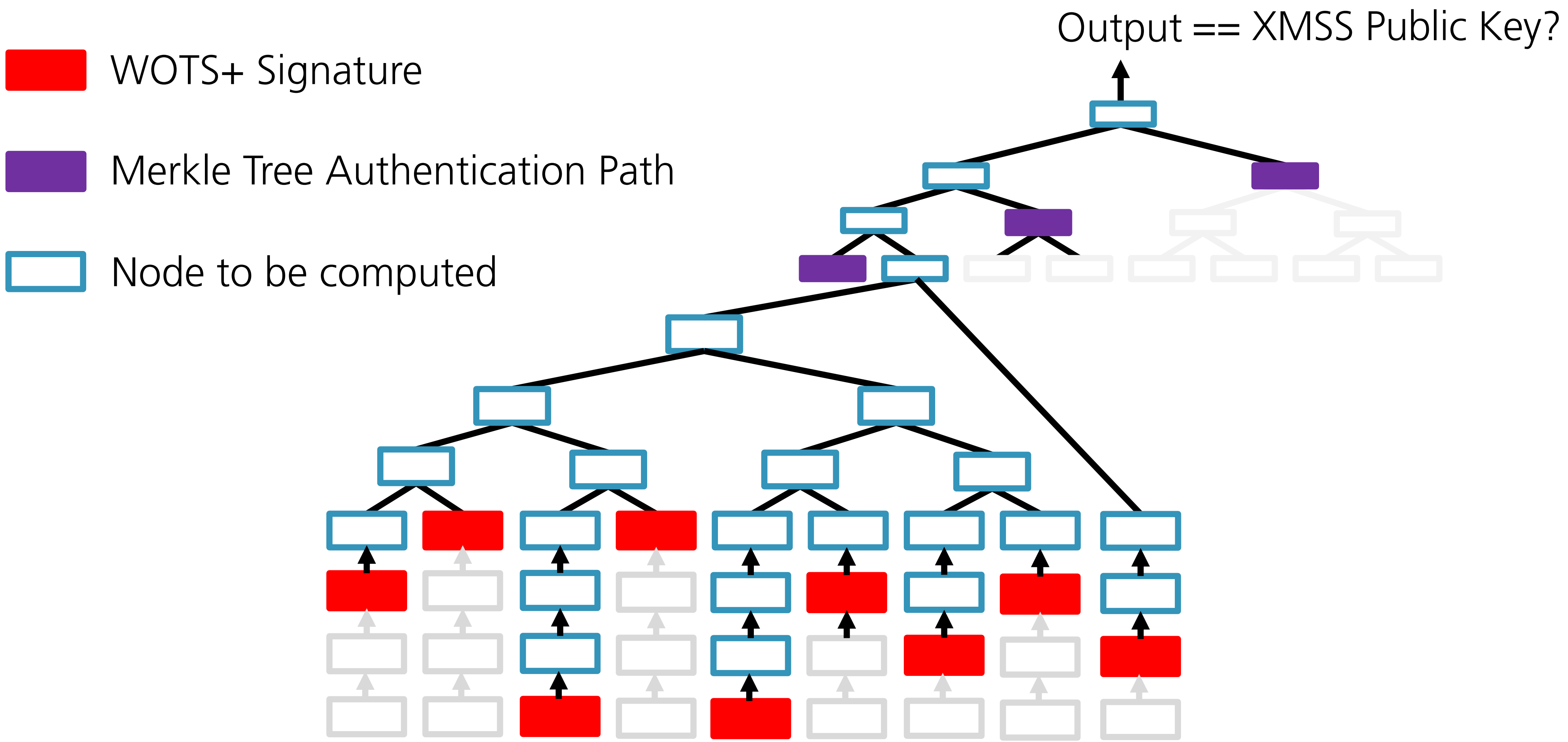
Signature Generation – Message 2



Fraunhofer
SINGAPORE

eXtended Merkle Signature Scheme

Signature Verification – Message 2



Performance Estimates

Performace Consideration

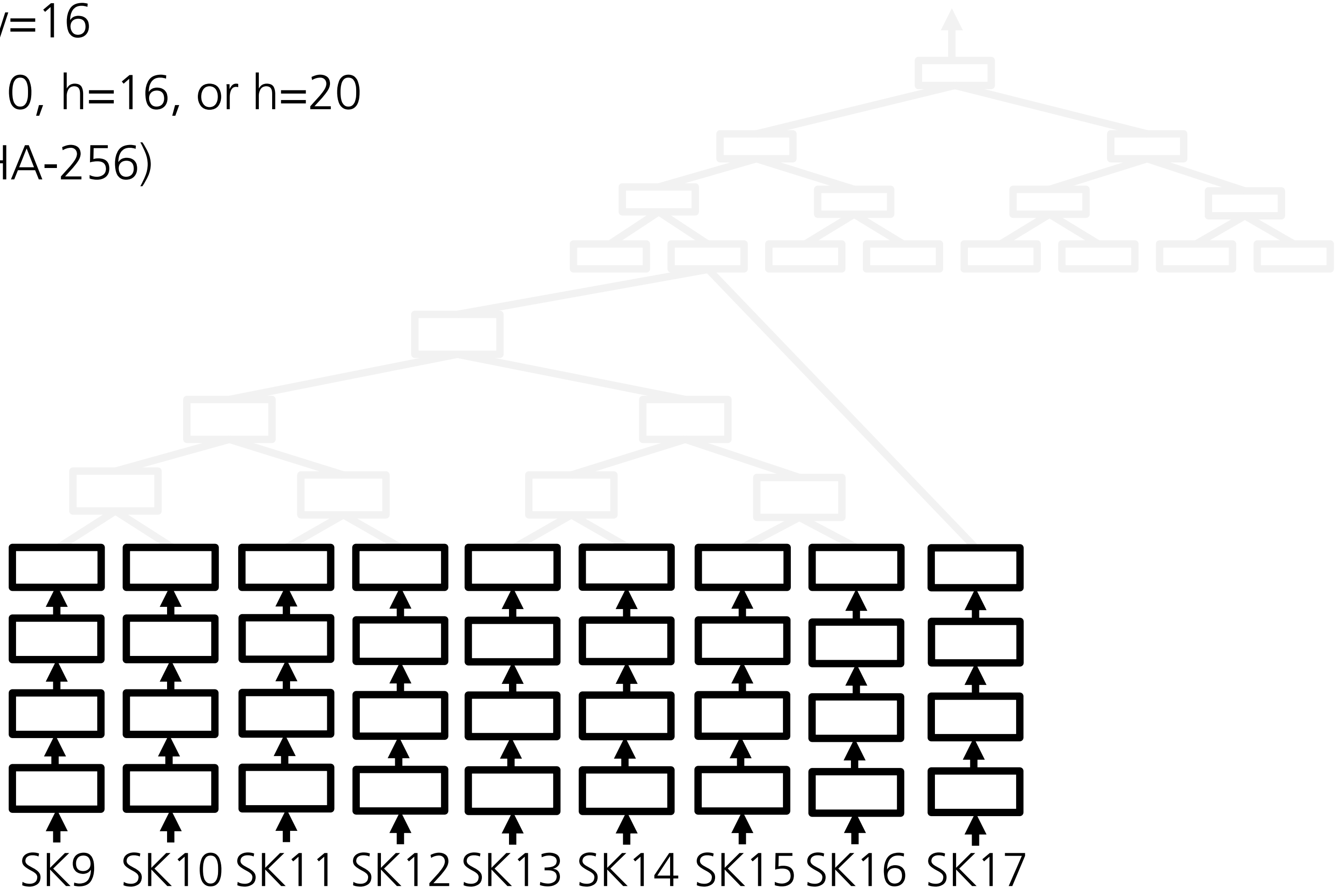
Public Key Generation – WOTS+

IRTF Parameters:

WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)



Fraunhofer
SINGAPORE

Performace Consideration

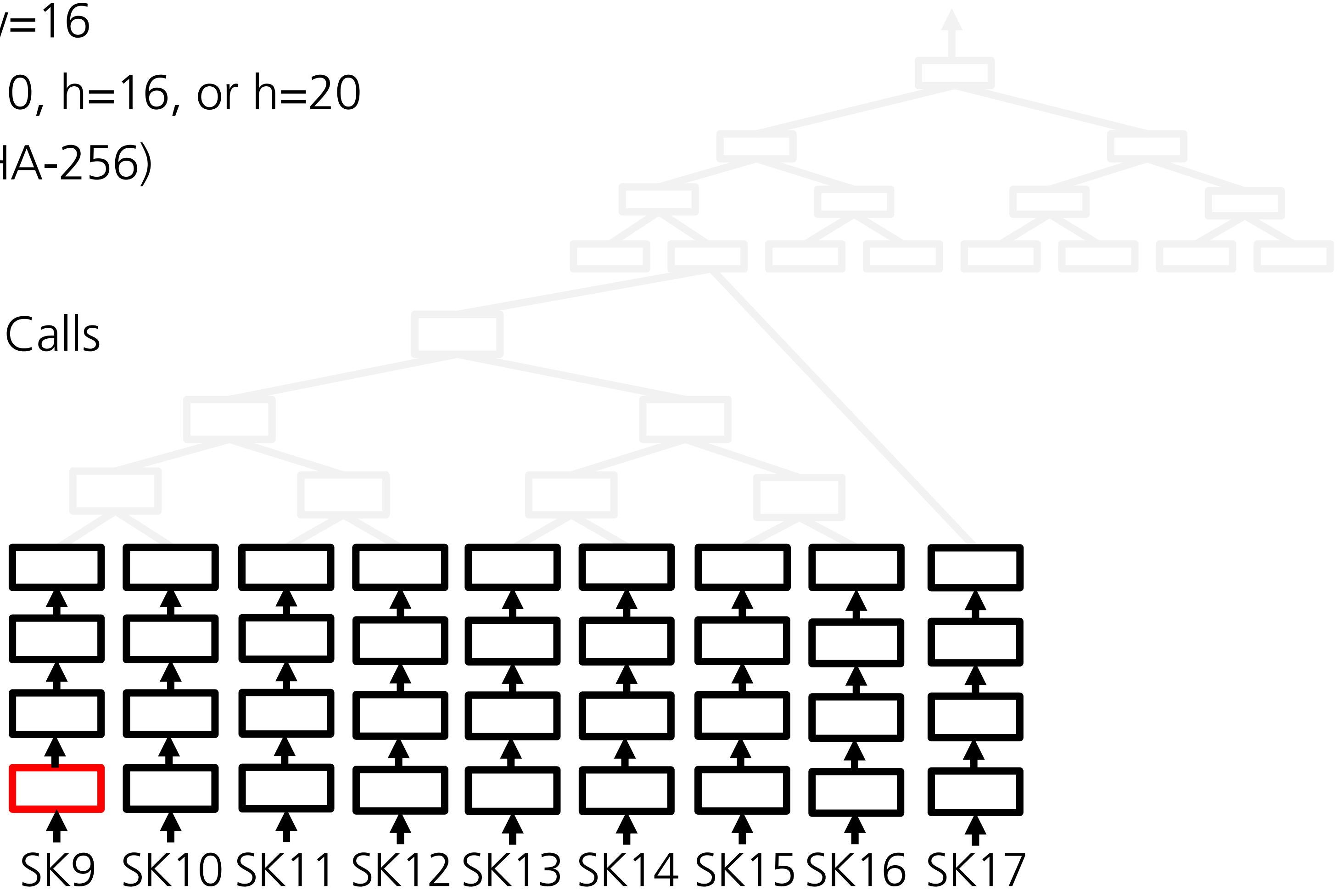
Public Key Generation – WOTS+

IRTF Parameters:

WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)



Performace Consideration

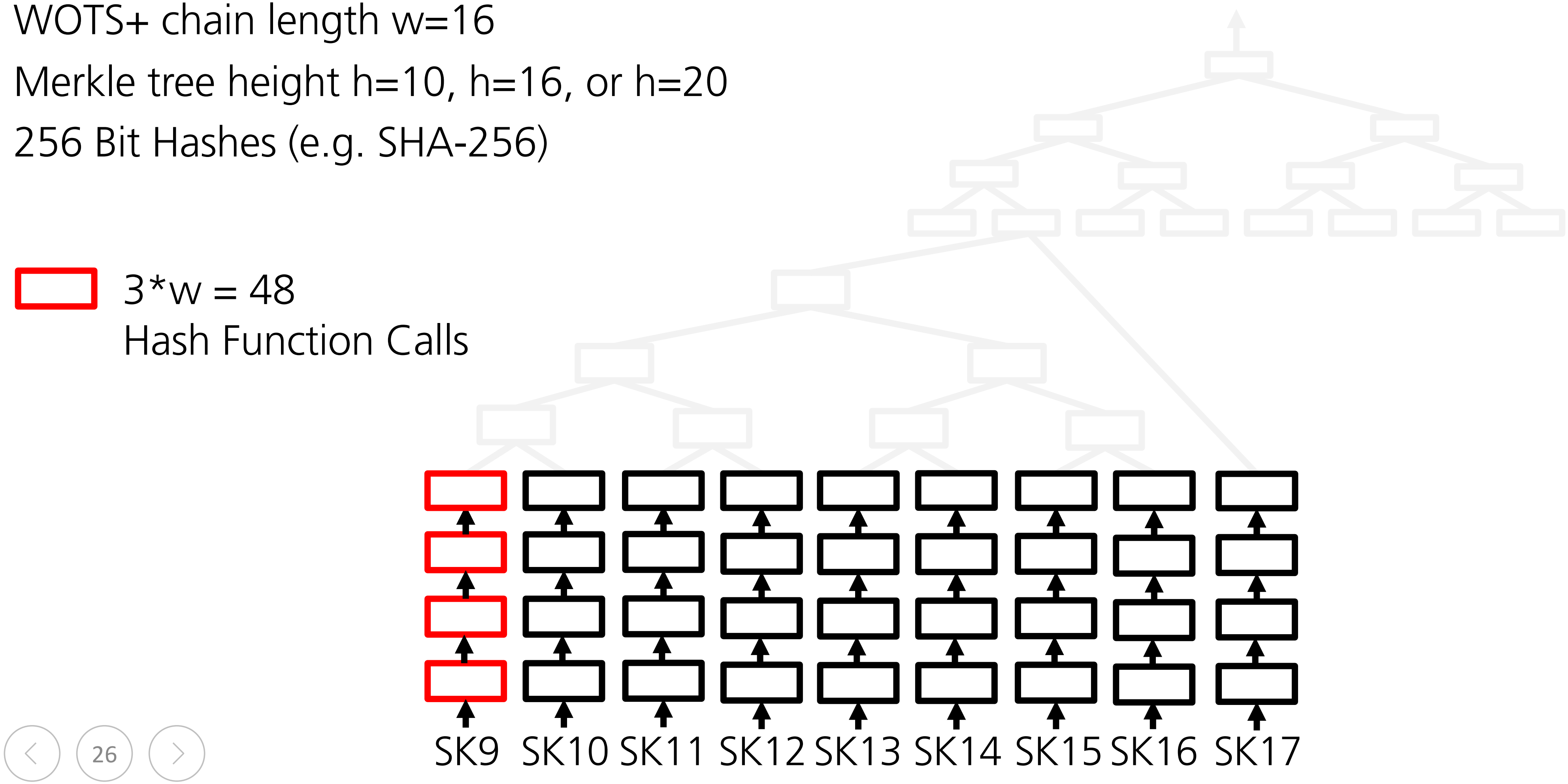
Public Key Generation – WOTS+

IRTF Parameters:

WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)



Performace Consideration

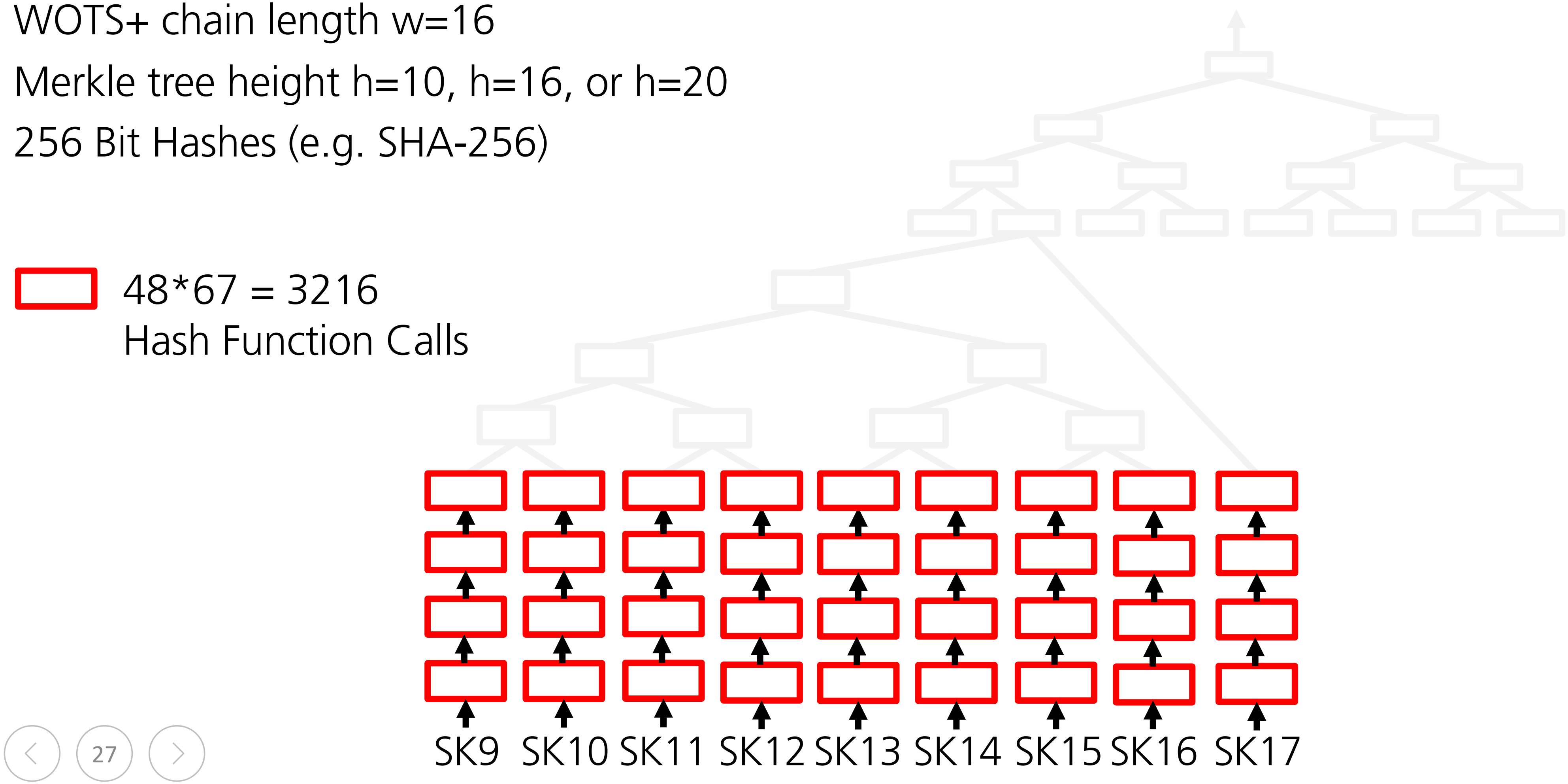
Public Key Generation – WOTS+

IRTF Parameters:

WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)



Performace Consideration

Public Key Generation – WOTS+

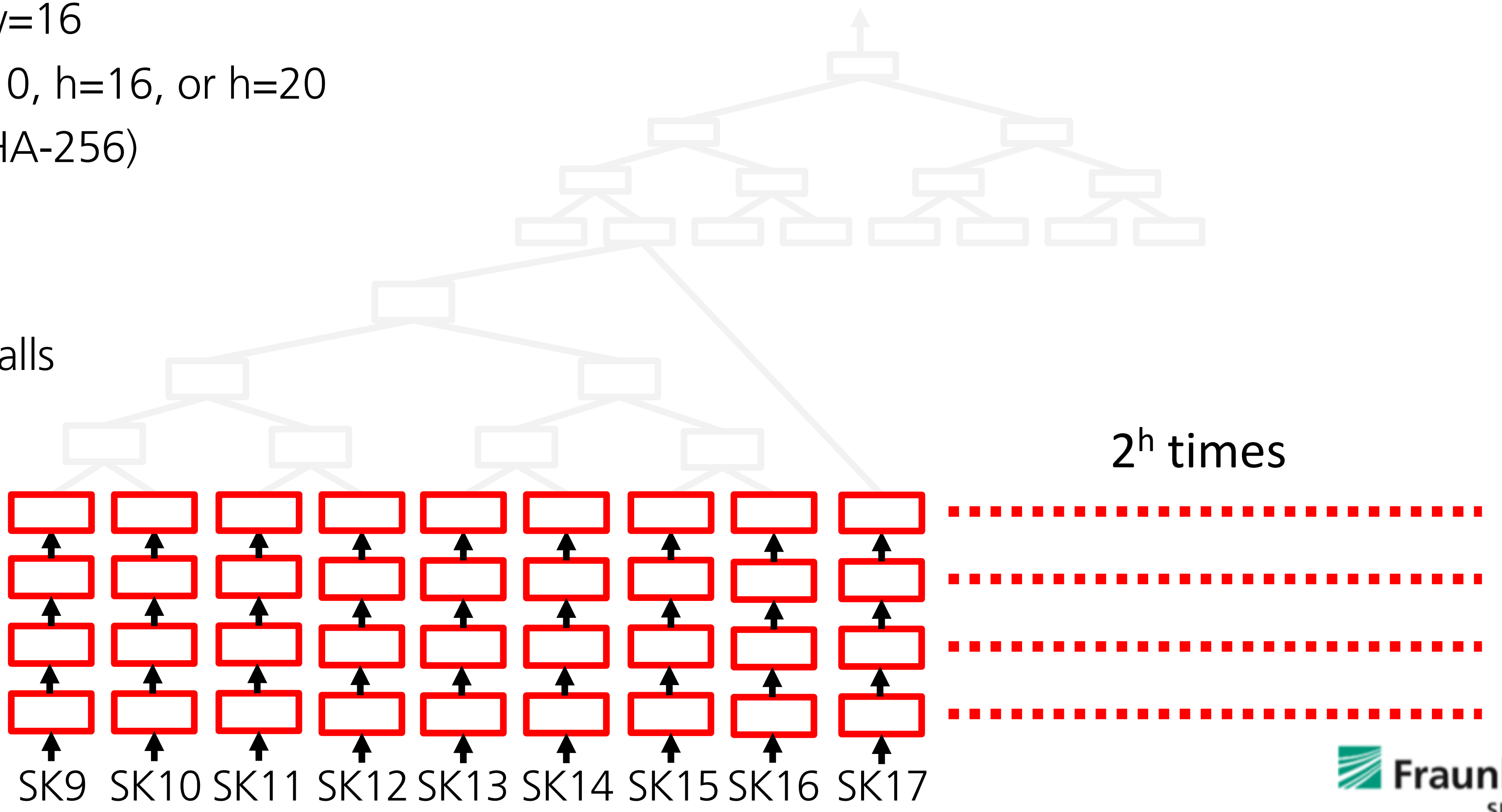
IRTF Parameters:

WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)

$3216*2^h$ Hash Function Calls



Fraunhofer SINGAPORE

Performace Consideration

Public Key Generation – L-Tree

IRTF Parameters:

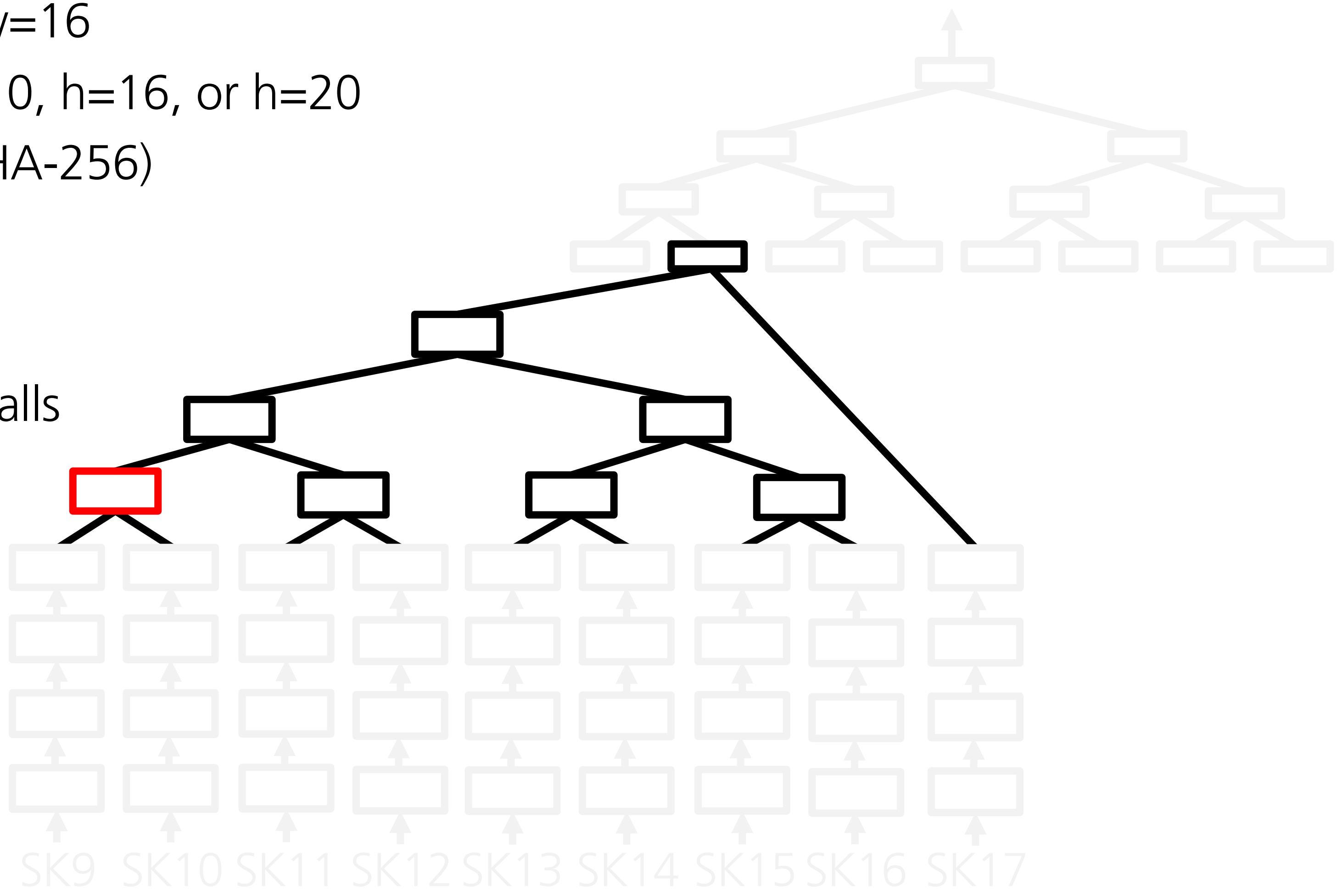
WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)

4

Hash Function Calls



Performace Consideration

Public Key Generation – L-Tree

IRTF Parameters:

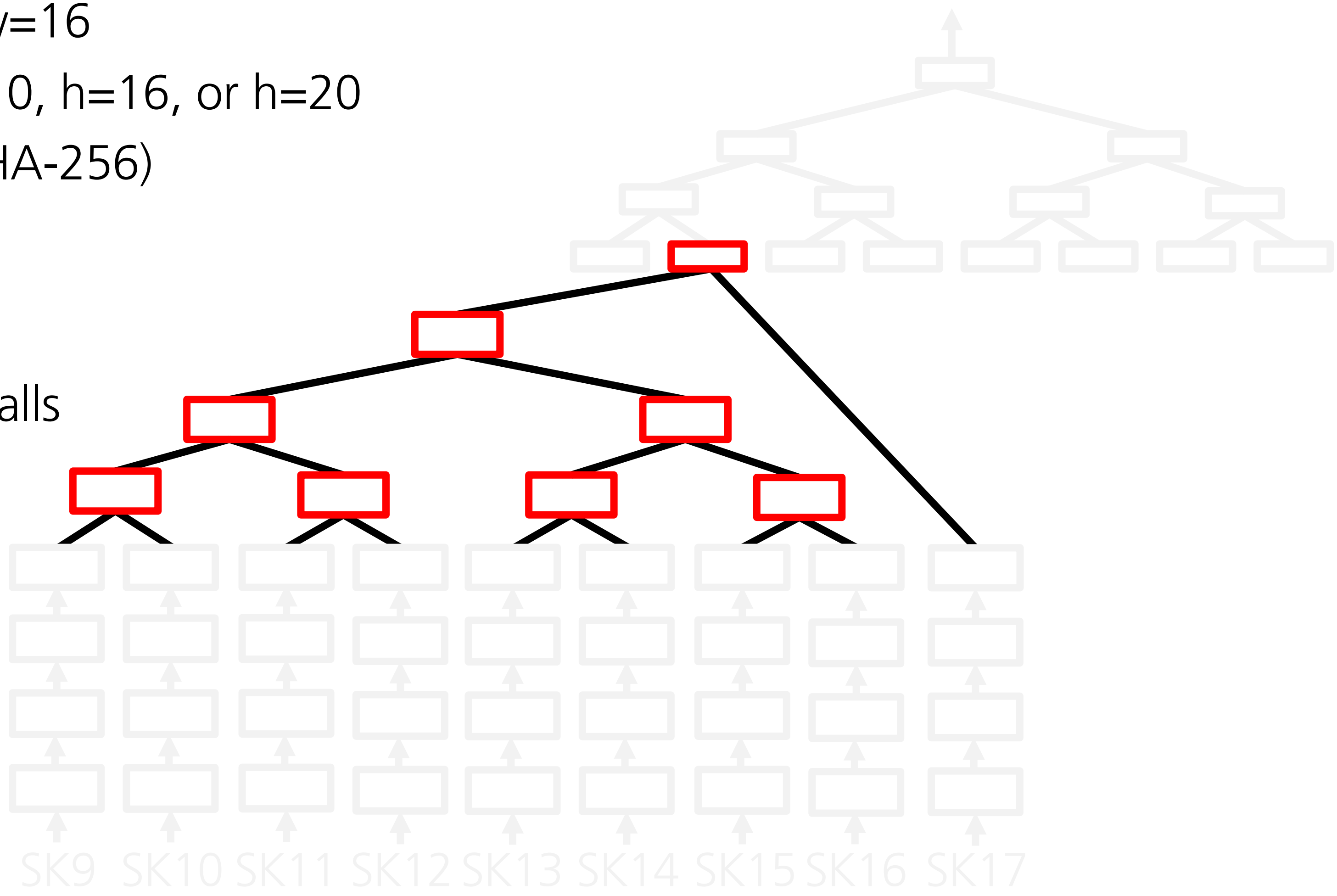
WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)

4*65 = 268

Hash Function Calls



Performace Consideration

Public Key Generation – L-Tree

IRTF Parameters:

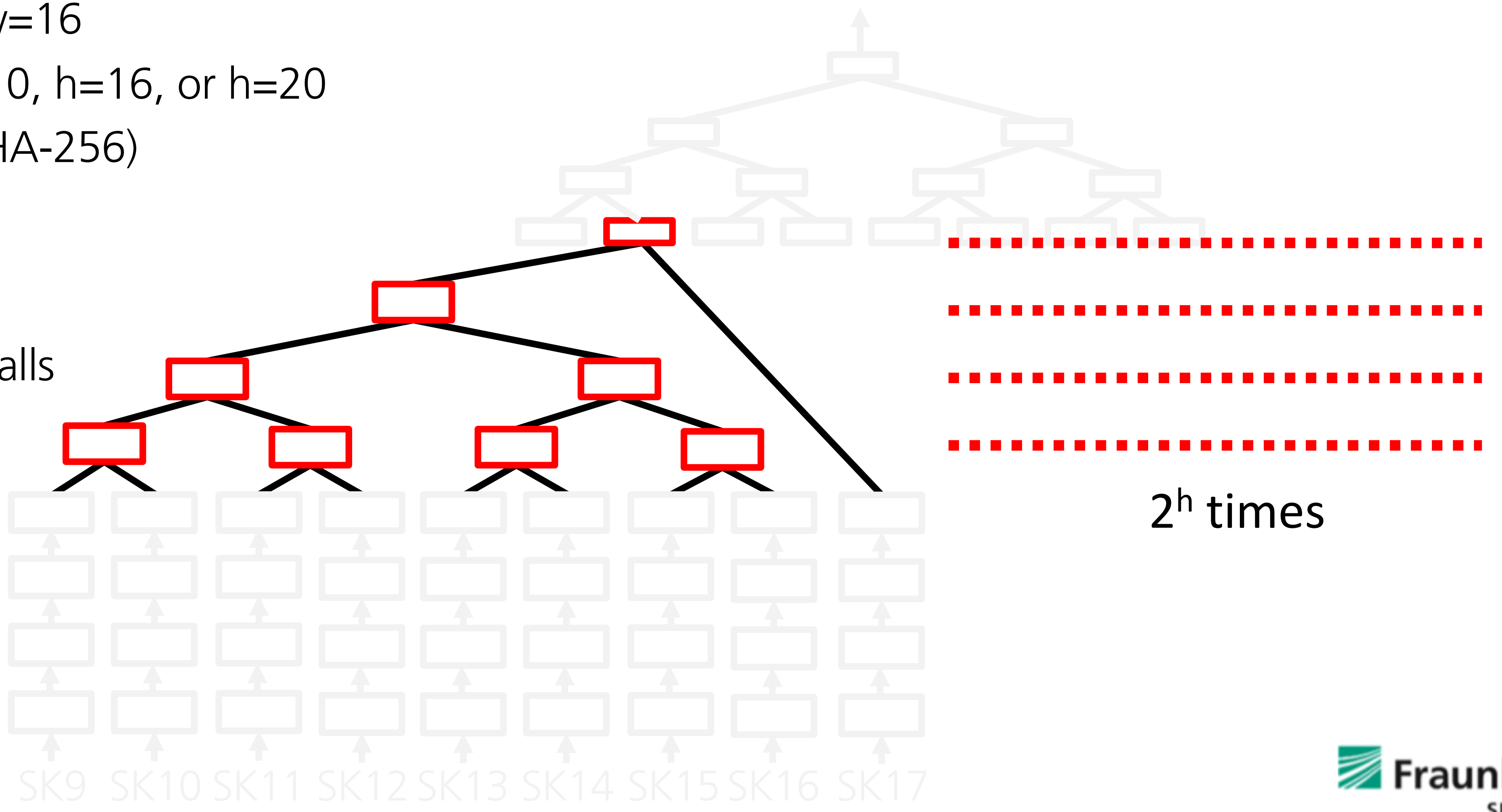
WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)

$260 * 2^h$

Hash Function Calls



2^h times

Performace Consideration

Public Key Generation – XMSS

IRTF Parameters:

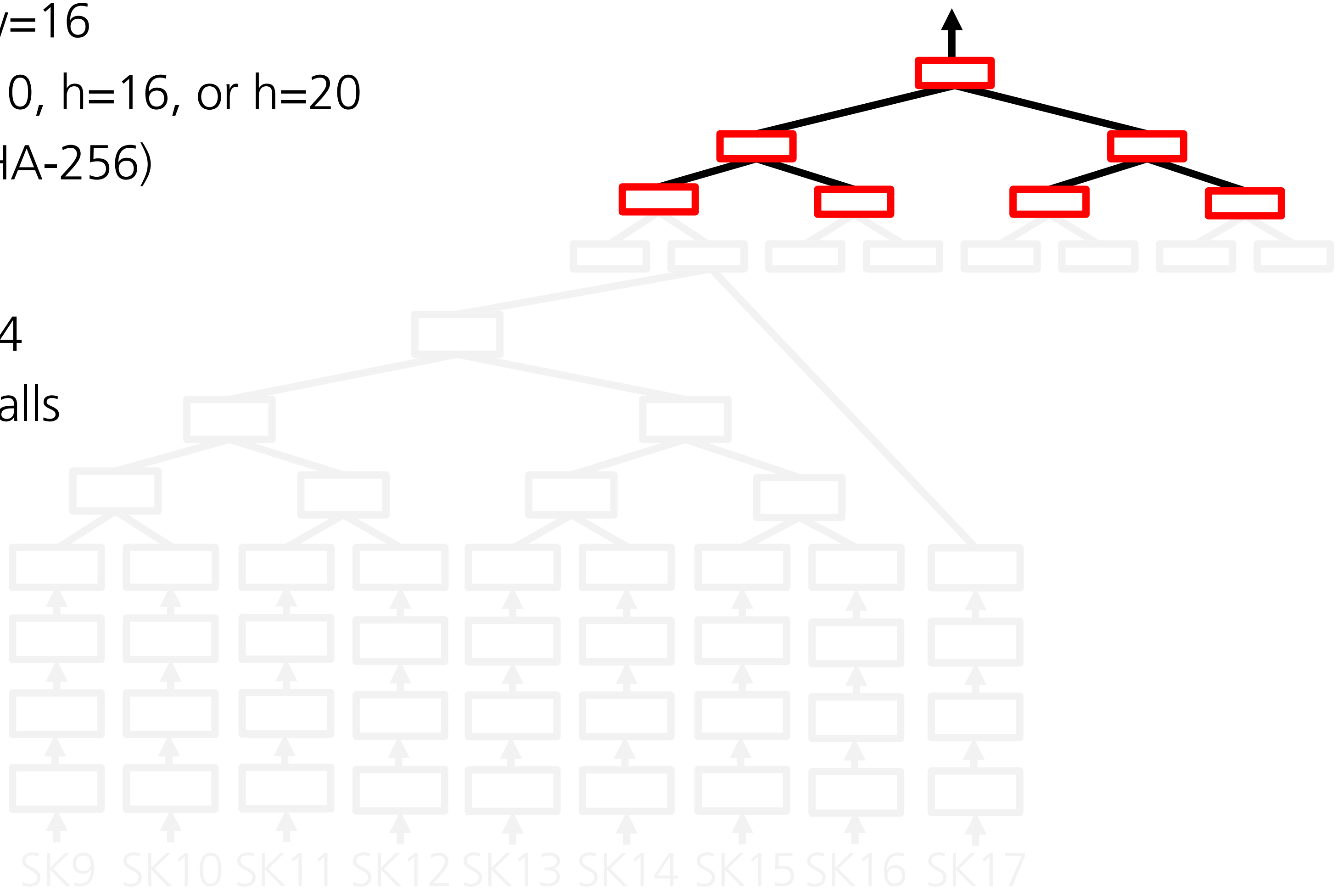
WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)

$4*(2^h-1) = 4*2^h-4$

Hash Function Calls



Fraunhofer SINGAPORE

Performace Consideration

Public Key Generation – XMSS

IRTF Parameters:

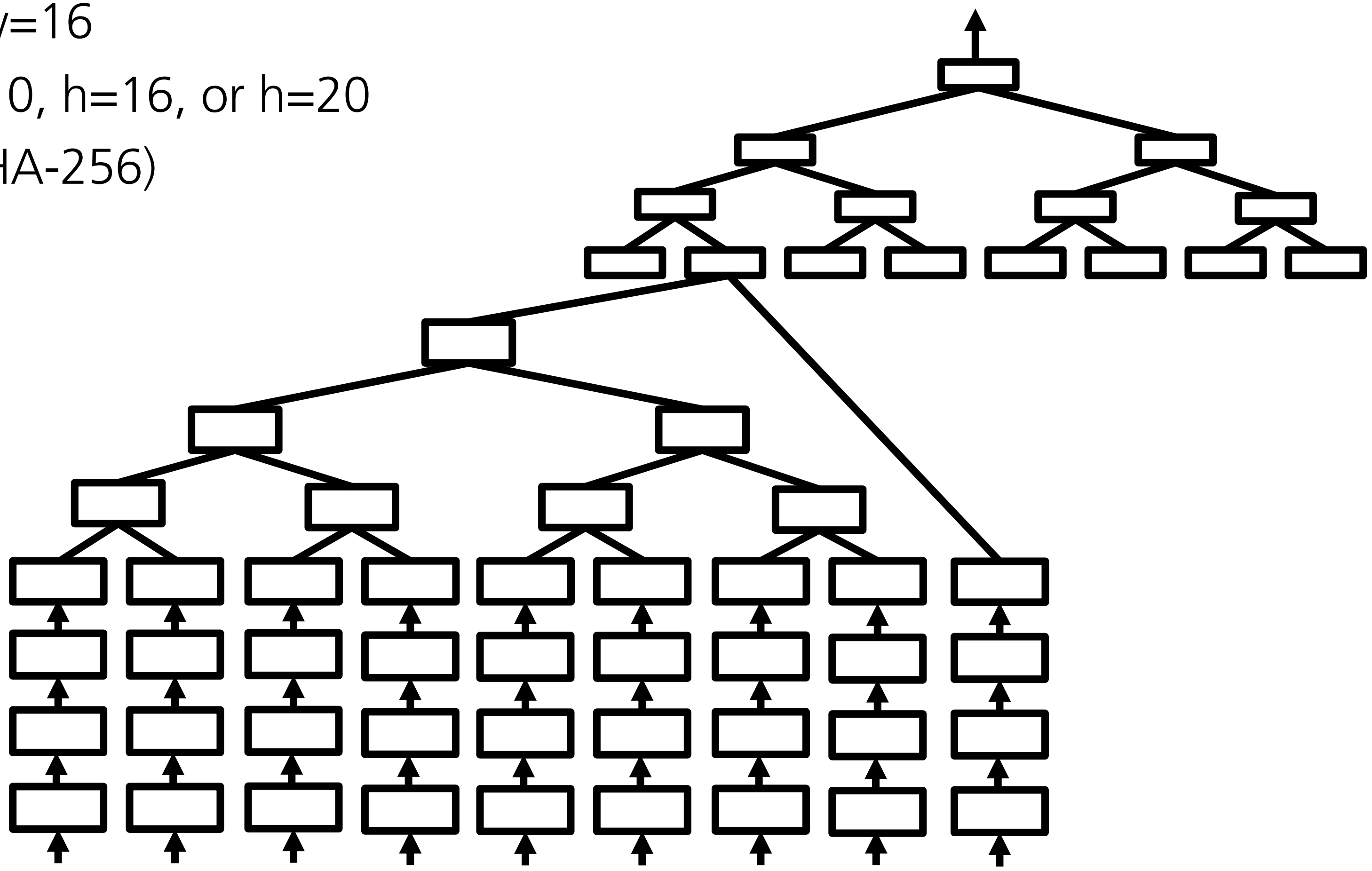
WOTS+ chain length w=16

Merkle tree height h=10, h=16, or h=20

256 Bit Hashes (e.g. SHA-256)

$3480*2^h$ -4

Total Hash Function Calls



Fraunhofer SINGAPORE

Performance Consideration

Hash Function Calls

	h=10	h=16	h=20
Signatures	1024	65,536	1,048,576
Public Key Generation	3,563,520	228,065,280	3,649,044,480
Signature Generation	~5,560	~263,684	~4,195,828
Signature Verification	~1,908	~1,932	~1,948

Performance with SHA-256

	h=10	h=16	h=20
Signatures	1024	65,536	1,048,576
Public Key Generation	423,099,648 clock cycles	$27*10^9$ clock cycles	$434*10^9$ clock cycles
With 400 MHz	<1.1 s	<70 s	<1085 s
Sign	< 2 ms	< 70 ms	< 1 s
Verify	< 1 ms	< 1 ms	< 1 ms

Performance with SHA-3

	h=10	h=16	h=20
Signatures	1024	65,536	1,048,576
Public Key Generation	79,159,200 clock cycles	$5*10^9$ clock cycles	$81*10^9$ clock cycles
With 400 MHz	< 200 ms	<12.5 s	< 203 s
Sign	< 1 ms	< 12.5 ms	< 200 ms
Verify	< 1 ms	< 1 ms	< 1 ms

Comparison with ECC

FPGA Implementation Estimates (Virtex-5)

	Ed25519	XMSS-SHA3 h=10
Public Key Generation	< 1 ms	< 200 ms
Sign	< 1 ms	< 1 ms
Verify	< 2 ms	< 1 ms

Optimisations and Trade-Offs

Parallelization and Caching

- Parallelization
  - WOTS+ trivial to compute in parallel
  - L-Tree and XMSS more difficult to parallelize
- More/Less Caching
  - More caching of XMSS for authentication path (costs more memory)

    → Improves the signing performance
  - Less caching to save memory

    → In the worst case, signing almost as slow as public key generation

    → Useful for lightweight applications with low memory

Thank you for your attention!