Post-Quantum Cryptography

Johannes Buchmann, Nina Bindel, Denis Butin

CROSSING

http://www.crossing.tu-darmstadt.de

Outline

- What is public-key cryptography? PK encryption, signatures
- Cybersecurity requires PKC
- Current PKC
  - RSA
  - Hardness of factoring
  - Hardness of DL
- Quantum computer threat
- Post quantum strategy

Outline

- Multivariate PKC
- Code-based PKC
- The idea of lattice-based PKC
- State-of-the art lattice-based signatures
  - overview
  - LWE: simplify explanation?
  - SIS: simplify explanation?
- Tesla
  - Tesla: improve explanation, compare with RSA with parameters shown earlier

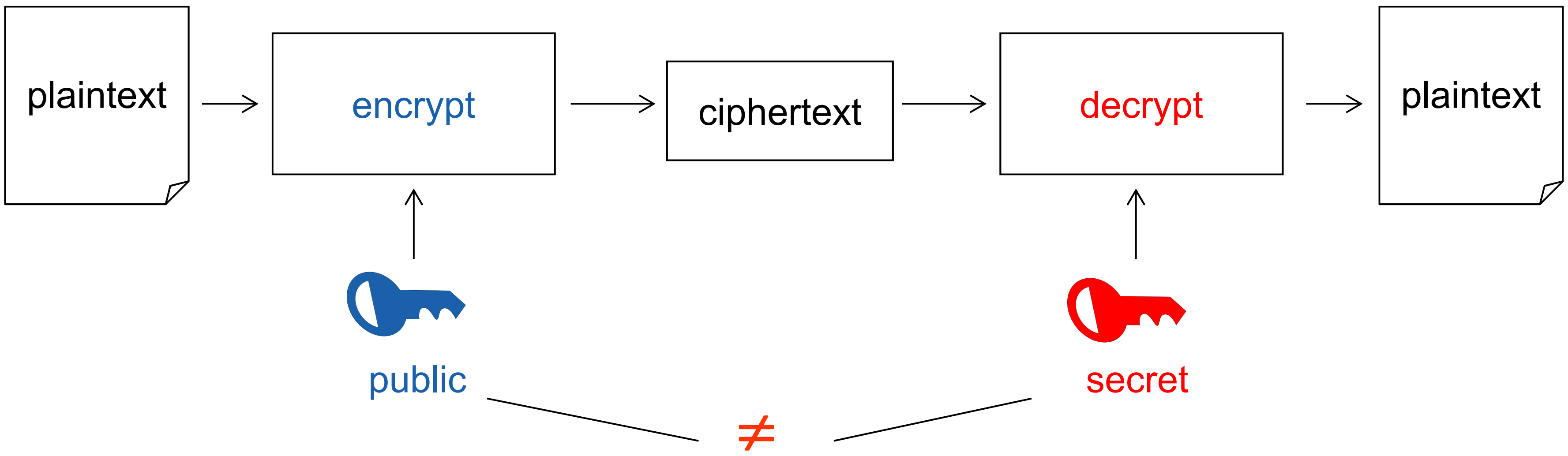
Outline

- State-of-the art lattice-based PK encryption
  - overview
- Lara
  - Improve explanation, compare with RSA with parameters shown earlier
- Hash-based signatures
  - The paradigm
  - Security
  - How it works: please add more
  - Performance
- Conclusion

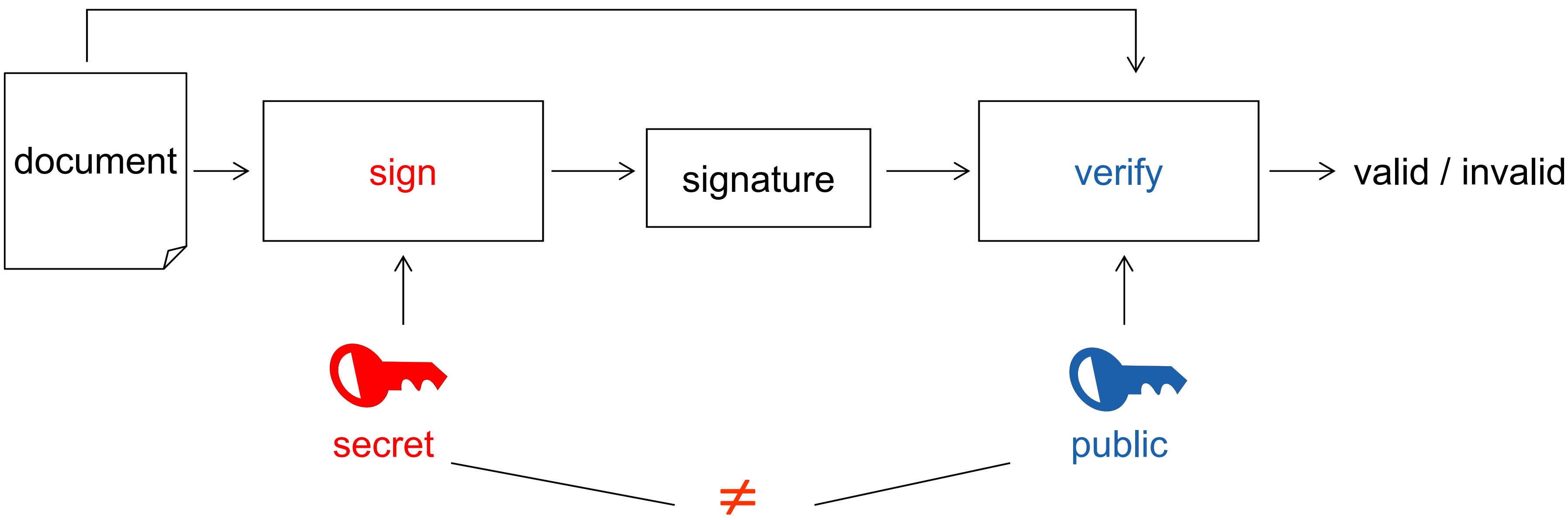
TECHNISCHE UNIVERSITÄT DARMSTADT

Public-key cryptography

Public-key encryption



Digital signatures



TECHNISCHE UNIVERSITÄT DARMSTADT

IT-security requires public-key cryptography

CROSSING

Communication on the Internet

TECHNISCHE UNIVERSITÄT DARMSTADT

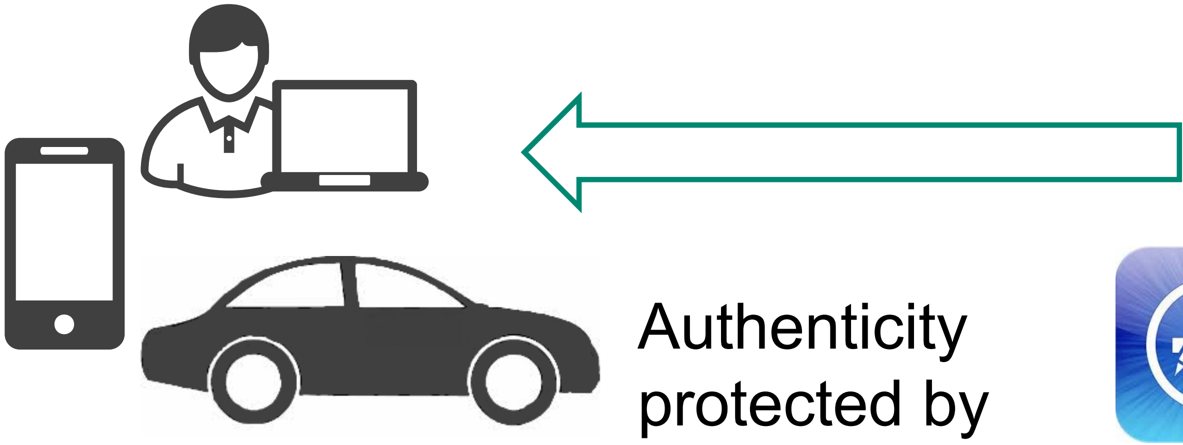
Protected by TLS

Public-key encryption
Digital signatures

Billions daily
e.g., 1.23 billion Facebook log ons daily

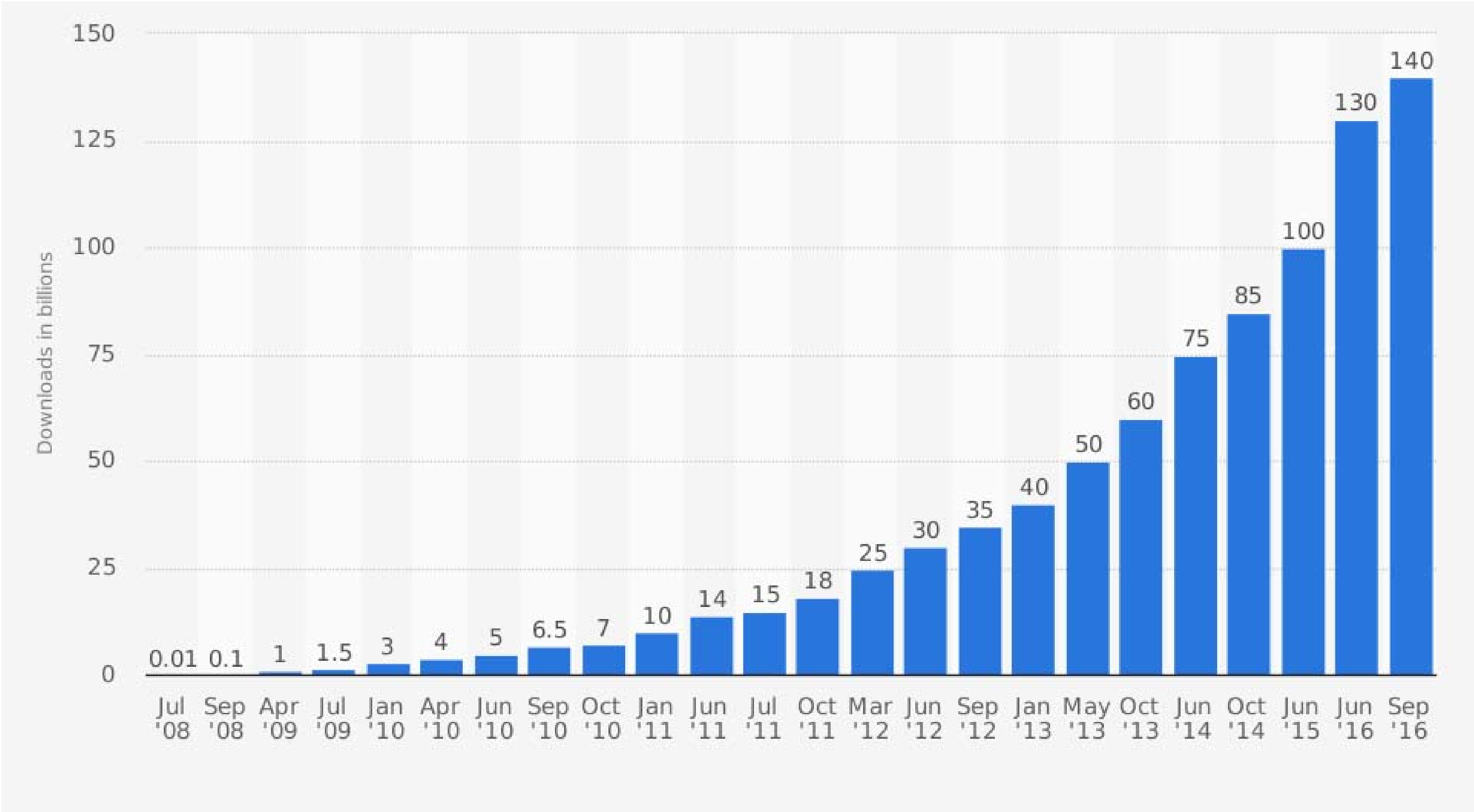
CROSSING

Software downloads



Authenticity protected by **digital signatures**

Cumulative number of apps downloaded from the Apple App Store from July 2008 to September 2016 (in billions)



Source: Apple, TechCrunch; © Statista 2017

Current public-key cryptography

“Generic” RSA

Public key: finite Group G, exponent e, $\gcd(\mathrm{e}, |\mathrm{G}|) = 1$

Secret key: $|\mathrm{G}|$

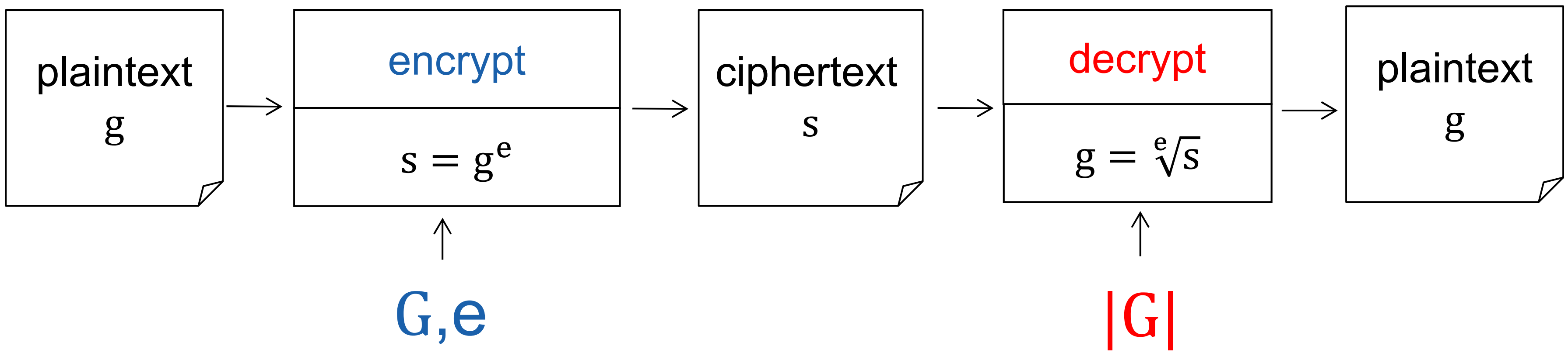
Allows to compute: $\sqrt[\mathrm{e}]{\mathrm{g}} = \mathrm{g}^{\mathrm{e}^{-1} \bmod |\mathrm{G}|}, \mathrm{g} \in \mathrm{G}$

"Generic" RSA encryption

Public key: finite Group G, exponent e, $\gcd(\mathrm{e}, |\mathrm{G}|) = 1$

Secret key: $|\mathrm{G}|$

Allows to compute: $\sqrt[\mathrm{e}]{\mathrm{g}} = \mathrm{g}^{\mathrm{e}^{-1} \bmod |\mathrm{G}|}, \mathrm{g} \in \mathrm{G}$



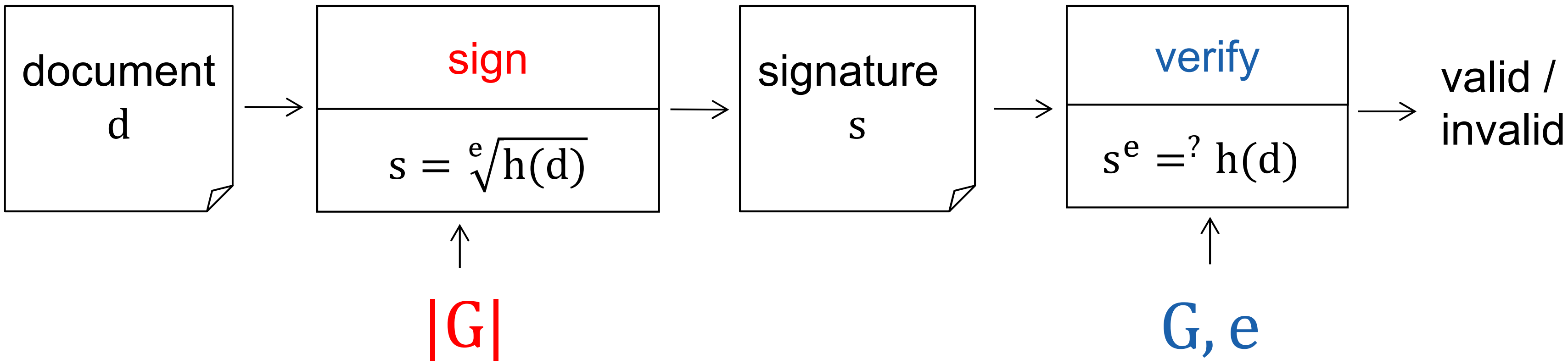
"Generic" RSA signature

Public key: finite Group G, exponent e, $\gcd(\mathrm{e}, |\mathrm{G}|) = 1$

Secret key: $|\mathrm{G}|$

Allows to compute: $\sqrt[\mathrm{e}]{\mathrm{g}} = \mathrm{g}^{\mathrm{e}^{-1} \bmod |\mathrm{G}|}, \mathrm{g} \in \mathrm{G}$

Hash function $\mathrm{h}\colon \{0,1\}^* \rightarrow \mathrm{G}$



RSA: How to keep $|G|$ secret?

Set up: p, q primes, $n = pq$, $G = (\mathbb{Z}/n\mathbb{Z})^*$, e, $\gcd(e, |G|) = 1$

$|G| = (p-1)(q-1)$,

Public key: (n, e)

Secret key: $d = e^{-1} \bmod (p-1)(q-1)$

Security relies on hardness of integer factorization

Only known method to keep $|G|$ secret

Public RSA key of PayPal

TECHNISCHE UNIVERSITÄT DARMSTADT

31795268810366627125473790859797098391197908286525435077364011285
90510438382632507968446475666470736765037698350040734989120408350
36111984436982786965149879673665411793622083038631384645332380078
74977706229020370398442691648609936395220964249973923183224282326
24293883124379061631765073423204610042801378799675461282344132598
82008909669991881742777224061960485068828406517329900151157317659
33488273881059259173651847367586007177868818486949631199170802343
43393438632241104852580095512302299147769809327477605192706038053
13338263751205344637414772085776930403119514835209366439467587236
52946961075123119618309889468210461323294360350311459316891189249

ElGamal encryption and signatures

TECHNISCHE UNIVERSITÄT DARMSTADT

Rely on the **Discrete Logarithm** Problem:

Given: Group $G = \langle g \rangle$, $h \in G$

Find: $x \in \mathbb{N}$ with $h = g^x$

Choices for G: $GF(p^n)^*$

Group of points of elliptic curves over $GF(p^n)$

CROSSING

How difficult is factoring and DL?

Shor's algorithm 1997

TECHNISCHE UNIVERSITÄT DARMSTADT

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

RSA and ElGamal insecure

A digital computer is g
device; that is, it is believ
an increase in computatio
true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

CROSSING

Quantum computer realistic


www.datacenterdynamics.com/content-tracks/servers-storage/google-may-unveil-a-powerful-quantum-computer-by-end-of-2017/96880.fullarticle

Welcome visitor | Sign in | Register | Magazine | Advertise

DatacenterDynamics
The Business of Data Centers.

News | Webinars | Opinion | Videos | Magazine | Content Tracks | Events | Awards

HOME › CONTENT TRACKS › SERVERS + STORAGE

Google may unveil a powerful quantum computer by end of 2017

2 September 2016 | By Sebastian Moss

Post-quantum cryptography

Performance requirements

TECHNISCHE UNIVERSITÄT DARMSTADT

Secure from-until	Security level	RSA modulus/finite field size	Elliptic curve
2017-2020	96	1776	192
2017-2030	112	2432	224
2017-2040	128	3248	256
2017- ?	256	15424	512

Ecrypt recommendations

- Space for keys and signatures: a few kilobytes
- Times: milliseconds

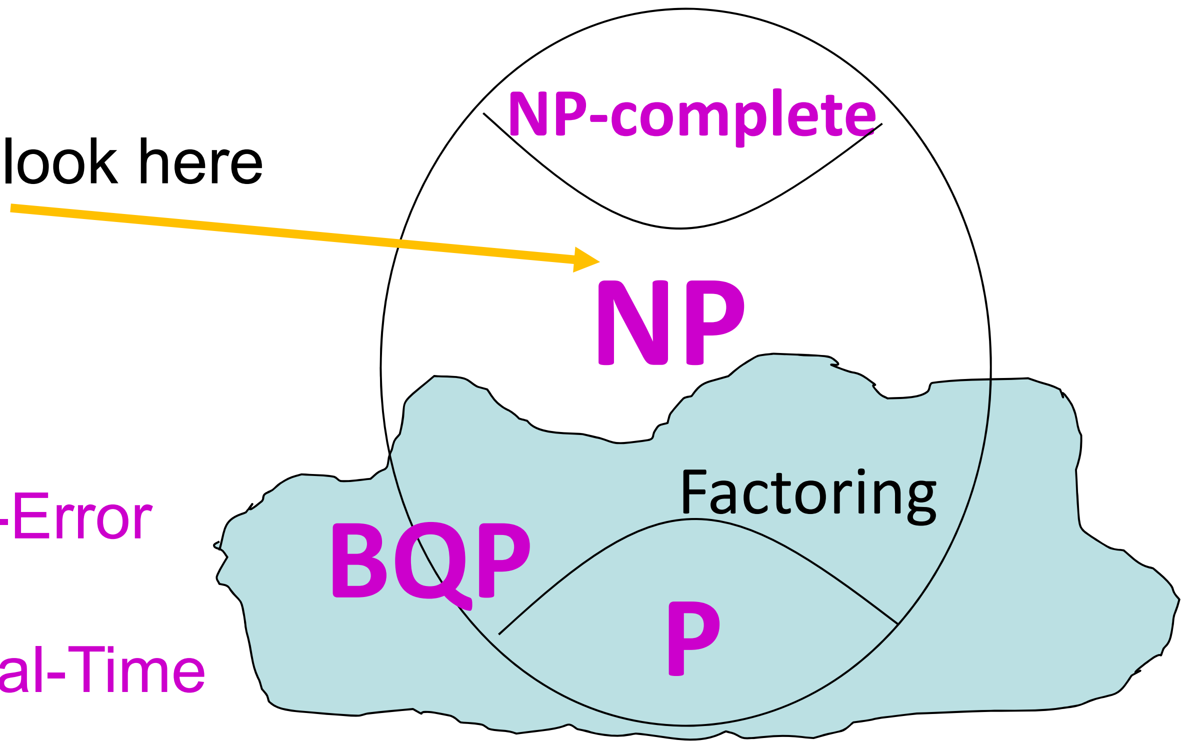
CROSSING

Post-quantum problems?

No provably quantum resistant problems

We must look here

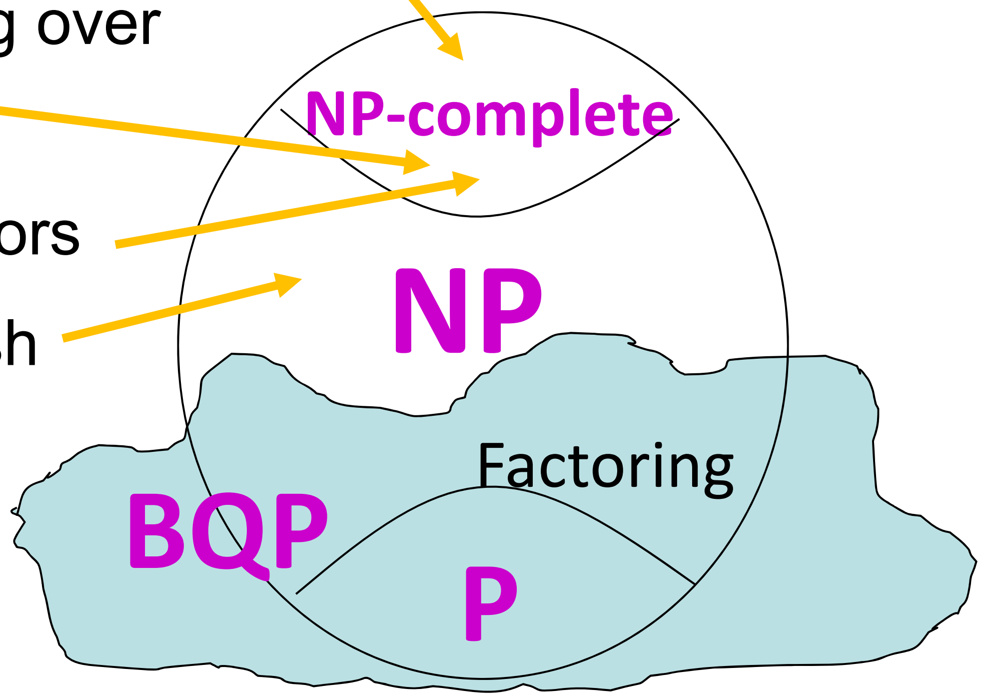
Bounded-Error Quantum Polynomial-Time



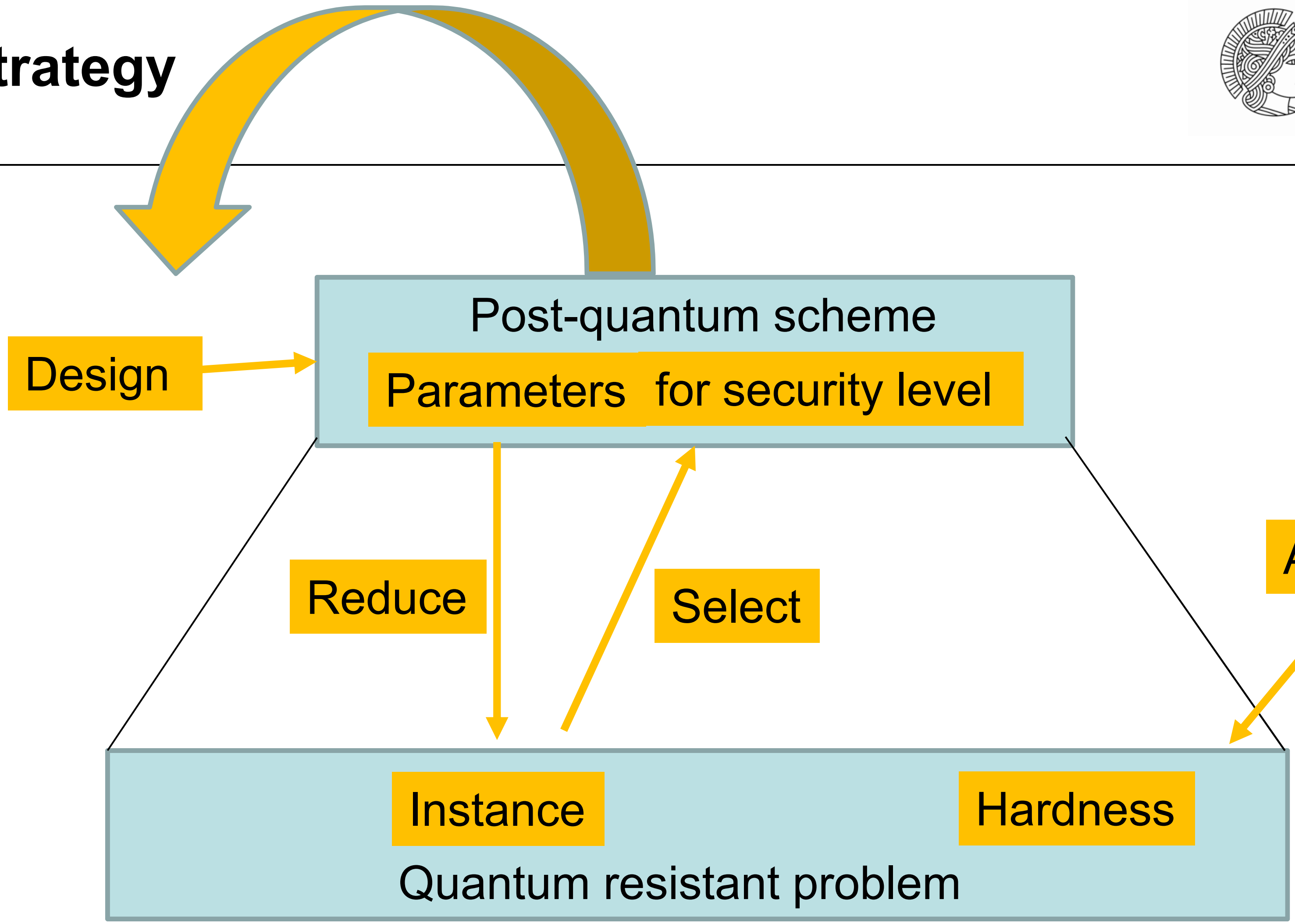
CROSSING

Candidates

- Solving non-linear equation systems over finite fields
- Bounded distance decoding over finite fields
- Short and close lattice vectors
- Breaking cryptographic hash functions



Strategy


Post-quantum scheme
Parameters for security level
Design
Reduce
Select
Assess
Instance
Hardness
Quantum resistant problem

Strategy - Methodology

Task	Goal	Method
Design	Efficient crypto with (tight)reduction proof to hard algorithmic problem	Algorithmics, quantum complexity theory
Assess	Quantum resistant problems, quantum time-space complexity, worst-to-average-case reduction	Quantum algorithmics, quantum complexity theory, parallel computing
Select	Parameter sets for given security level	Explicit complexity analysis

Multivariate cryptography

MQ problem

TECHNISCHE UNIVERSITÄT DARMSTADT

$$4x + x^2 + y^2z \equiv 1 \mod 13$$

$$7y^2 + 2xz^2 \equiv 12 \mod 13$$

$$x + y^2 + 12xz^2 \equiv 4 \mod 13$$

Solution: $x = 15,\ y = 29,\ z = 45$

CROSSING

MQ-Problem

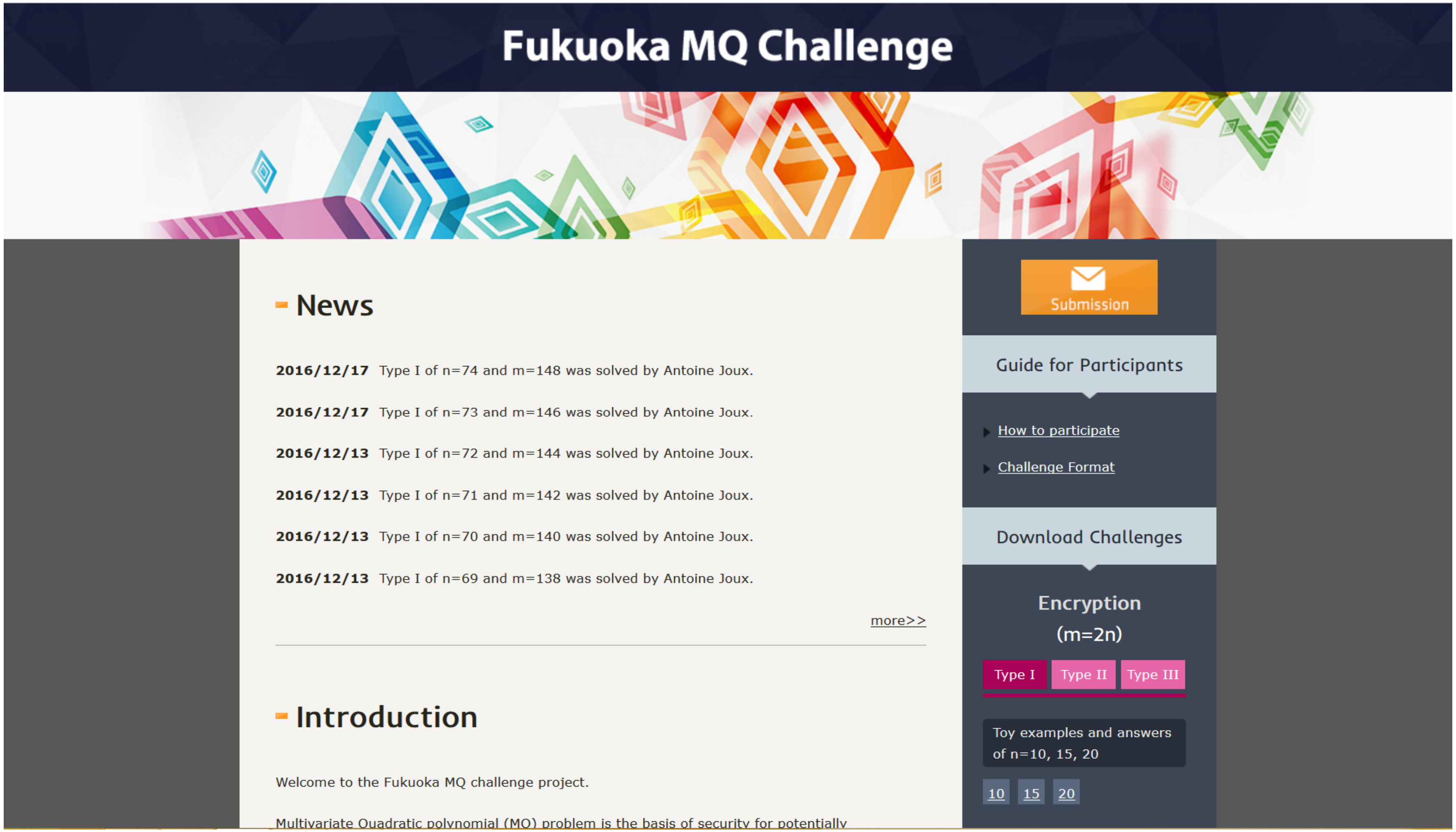
Given: $n, m, p_1, \dots, p_m \in F[x_1, \dots, x_n]$ quadratic, F finite field

Find: $y_1, \dots, y_n \in F$, such that

$$p_1(y_1, \dots, y_n) = \dots = p_m(y_1, \dots, y_n) = 0$$

MQ is NP-complete (Garey, Johnson 1979) (decision version)

MQ Challenge



CROSSING

Multivariate signatures

TECHNISCHE UNIVERSITÄT DARMSTADT

$P: F^n \to F^m$, easily invertible non-linear

$S: F^n \to F^n$, $T: F^m \to F^m$, affine linear

Public key: $G = S \circ P \circ T$, hard to invert

Secret Key: S, P,T allows to find G^{-1}

$$G^{-1} = T^{-1} \circ P^{-1} \circ S^{-1}$$

Signing: $s = T^{-1} \circ P^{-1} \circ S^{-1}(m)$

Verifying: $G(s) \stackrel{?}{=} m$

- UOV , Goubin et al., 1999
- Rainbow, Ding, et al. 2005
- pFlash, Cheng, 2007
- Gui, Ding, Petzoldt, 2015
- QUARTZ, Patarin, Courtois, 2001

Forging signature: Solve $G(s) - m = 0$

Performance of multivariate signature schemes (80-bit security)

TECHNISCHE UNIVERSITÄT DARMSTADT

Scheme	Cyclecounts [k-cycles]		Sizes		
	Sign	Verify	pk [kB]	sk [kB]	sig. [bit]
Gui-96	596	70	62	3	126
Gui-95	1,441	60	30	3	120
Rainbow	4,740	350	25	19	344
UOV	11,201	230	14	96	672
QUARTZ	315,716	84	72	3	128
RSA-1024	1,058	74	0.125	0.125	1024
ECDSA P160	558	635	0.039	0.059	320

Hardware implementations of multivariate signature schemes

First approaches:

- Rainbow:
  Fast Multivariate Signature Generation in Hardware: The Case of Rainbow; Balasubramanian, Bogdanov, Rupp, Ding, Carter
  2008

- UOV:
  *High-Speed Hardware Implementation of Rainbow Signature on FPGAs; T*ang, Yi, Ding, Chen, Chen
  2011

- Gui: no approaches yet

Code-based cryptography

Bounded distance decoding problem

Given:
- Linear code $C \subseteq F_2^n$
- $y \in F_2^n$
- $t \in \mathbb{N}$

Find:
- $x \in C$: $\mathrm{dist}(x, y) \leq t$

BDD is NP-complete (Berlekamp et al. 1978) (Decisional version)

McEliece cryptosystem (1978)

S, G, P matrices over F

G generator matrix for Goppa code ← Allows to solve BDD

Public key: $G' = S \circ G \circ P,\ t$

Secret Key: P, S, G

Encryption: $c = mG' + z \in F^n$

Decryption: $x = cP^{-1} = mSG + zP^{-1}$

solve BDD to get $y = mSG$

decode to obtain m

Performance of code-based encryption schemes (80-bit security)

TECHNISCHE UNIVERSITÄT DARMSTADT

Scheme	Cyclecounts [k-cycles]		Size		Expansion factor
	Encryption	Decryption	pk [kB]	sk [kB]	
McEliece QC-MDPC [vMG14]	7,018	42,130	0.586	0.180	2
RSA-1024 [GPWES04]	3,440	87,920	0.125	0.125	1
ECC-ecp160r1 [GPWES04]	6,480	6,480	0.039	0.059	1

[vMG14]: von Maurich and Güneysu: Towards side-channel resistant implementations of QC-MDPC McEliece encryption on constrained devices, PQCrypto 2014

[GPWES04]: Gura, Patel, Wander, Eberle, Shantz: Comparing elliptic curve cryptography and RSA on 8-bit cpus, CHES 2004

Lattice-based cryptography

Why lattice-based cryptography?

TECHNISCHE UNIVERSITÄT DARMSTADT

- Expected to resist quantum computer attacks
- Worst-to-average-case reduction
- Permits fully homomorphic encryption and many other applications

CROSSING

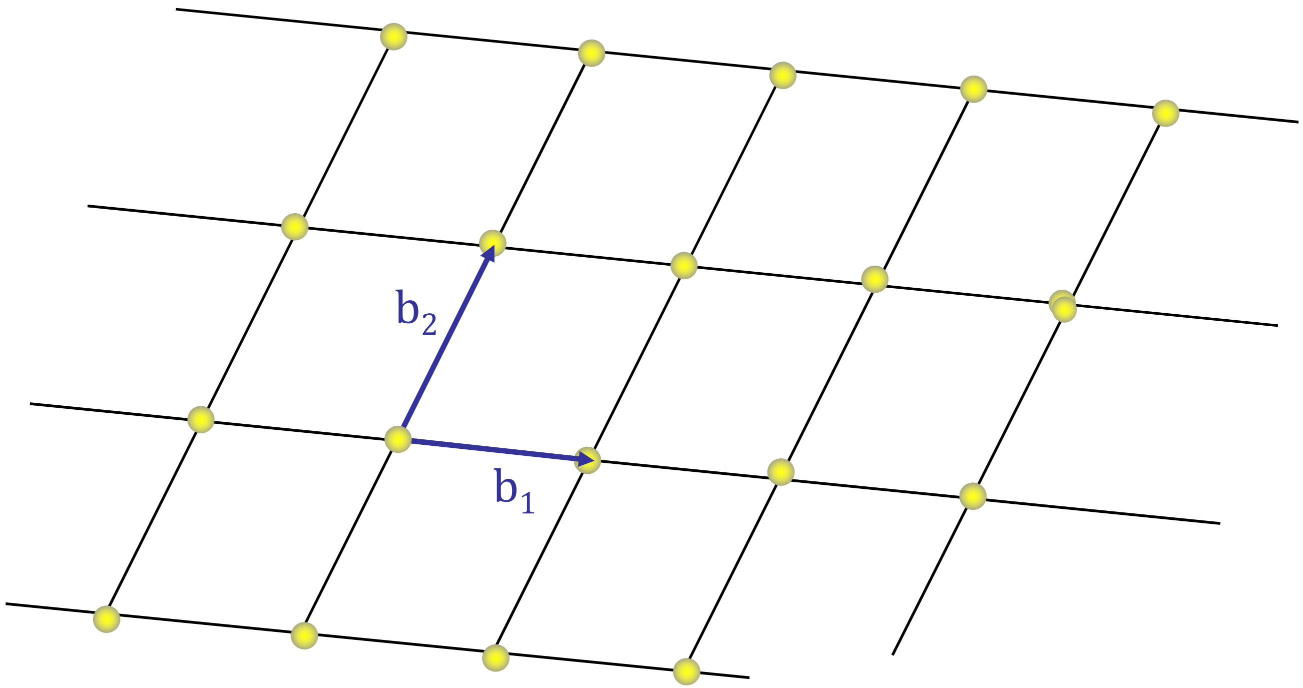
TECHNISCHE UNIVERSITÄT DARMSTADT

The idea of lattice-based cryptography

CROSSING

2-dimensional lattice

$B = (b_1, b_2), L(B) = \mathbb{Z}b_1 + \mathbb{Z}b_2$

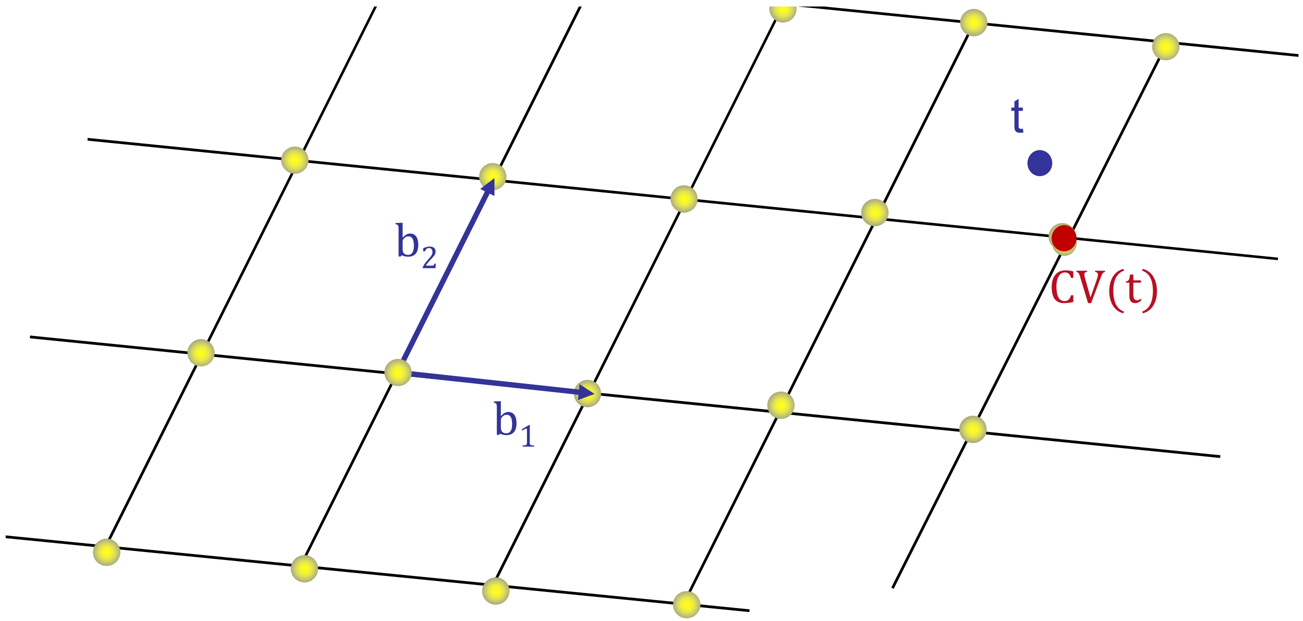


CROSSING

2-dimensional CVP

Given: $B = (b_1, b_2),\ t, \alpha$

Find: $CV(t) \in L(B)\colon\ \left|\left|t - CV(t)\right|\right| \leq \min_{w \in L} ||t - w||$



Lattice problems

$n \in \mathbb{N}, L = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n \subseteq \mathbb{R}^n$ lattice; $B = (b_1, \ldots, b_n)$ basis

α-Closest Vector Problem (CVP)

Given: $\alpha > 1$, lattice $L = L(B)$ basis B, t

Find: $v \in L$ such that $||t - v|| \leq \alpha \min_{w \in L} ||t - w||$

α-Shortest Vector Problem (SVP)

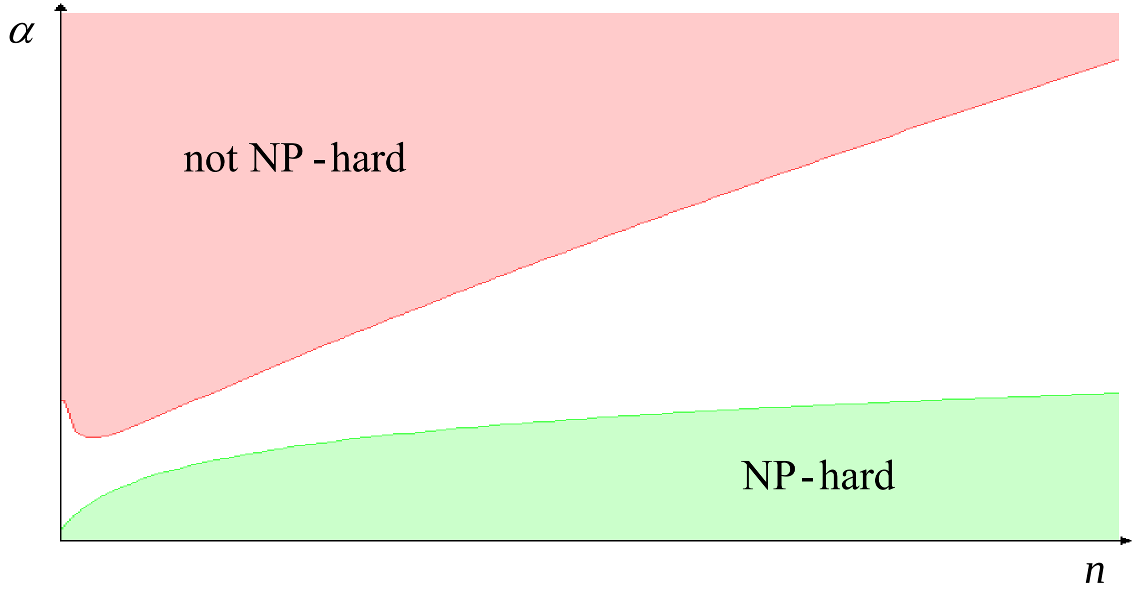
Given: $\alpha > 1$, lattice $L = L(B)$ in terms of basis B

Find: $v \in L$ nonzero such that $||v|| \leq \alpha \lambda_1(L)$

Complexity of α-CVP/SVP

Arora et al. (1997):

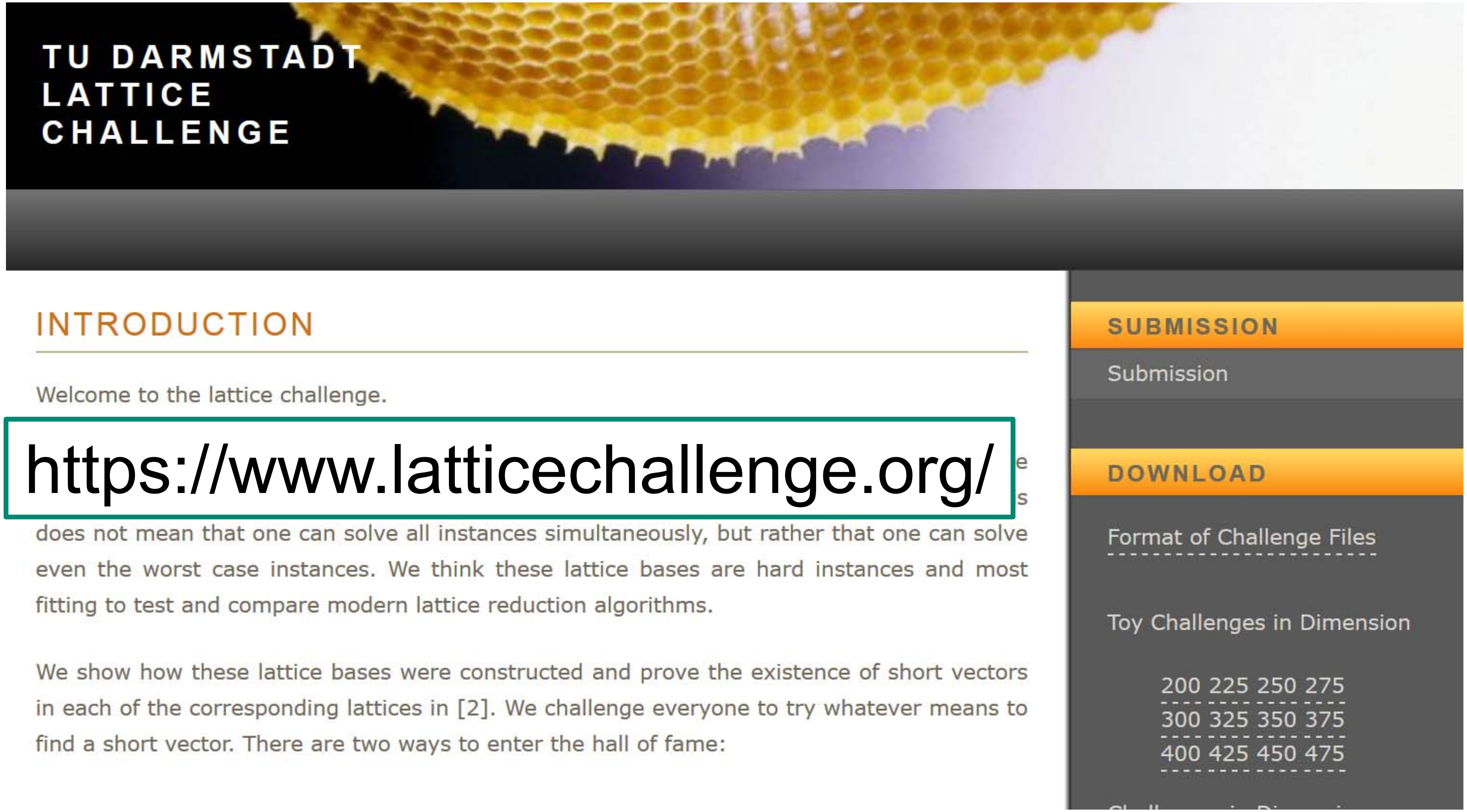
$$\log(n)^c\text{-CVP/SVP is NP-hard for all } c$$



Goldreich, Goldwasser (2000):

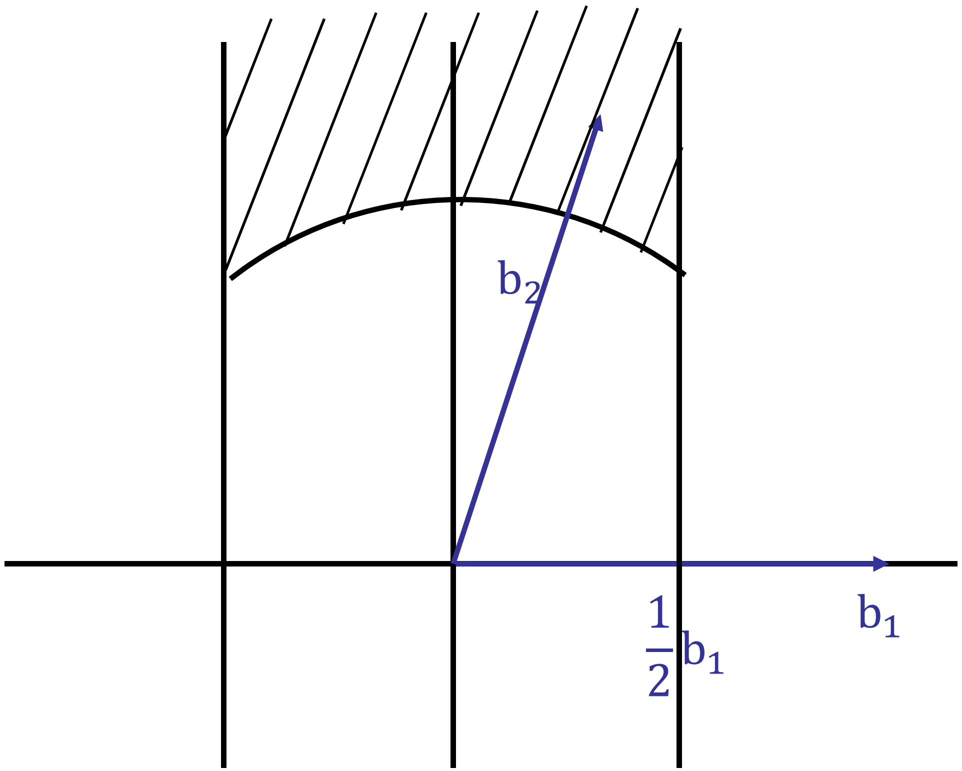
$$\Omega\left(\sqrt{n}/\log(n)\right)\text{-CVP/SVP is not NP-hard or } \mathbf{coNP} \subseteq \mathbf{AM}$$

Practical complexity



https://www.latticechallenge.org/

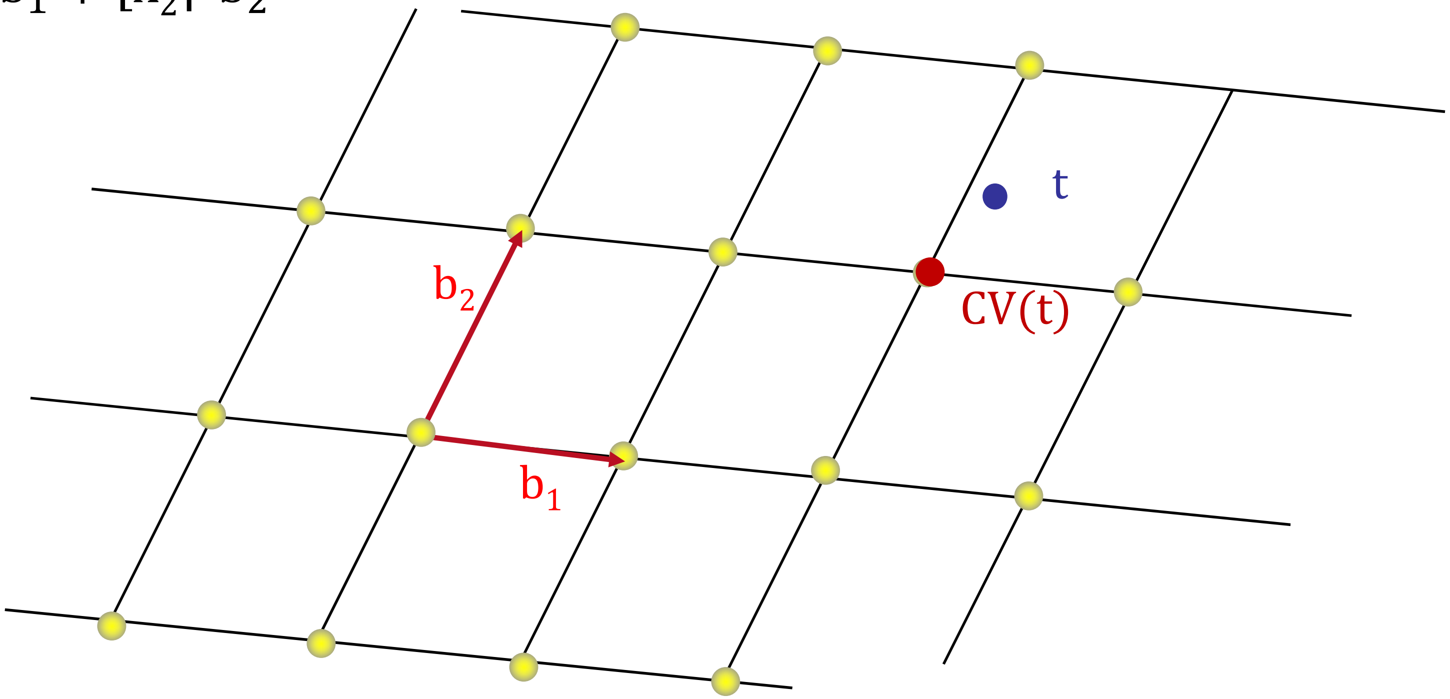
Reduced bases (Gauß 1801)



$(\mathbf{b_1}, \mathbf{b_2})$ reduced
Gauss: CVP easy

$\mathrm{t} = \mathrm{x_1 b_1} + \mathrm{x_2 b_2}$

$\mathrm{CV(t)} = \lfloor \mathrm{x_1} \rceil \mathrm{b_1} + \lfloor \mathrm{x_2} \rceil \ \mathrm{b_2}$



$\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$ not reduced ⇒ CVP hard

TECHNISCHE UNIVERSITÄT DARMSTADT

$L = \mathbb{Z}^2$, $B = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$, $t = \begin{pmatrix} 3.4 \\ -2.3 \end{pmatrix}$, $\mathrm{CVP}(t) = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$

Another basis $B' = \left(\begin{pmatrix} 100 \\ 99 \end{pmatrix}, \begin{pmatrix} 99 \\ 98 \end{pmatrix} \right)$

$t = \begin{pmatrix} 3.4 \\ -2.3 \end{pmatrix} = -560.9 \cdot \begin{pmatrix} 100 \\ 99 \end{pmatrix} + 566.6 \cdot \begin{pmatrix} 99 \\ 98 \end{pmatrix}$

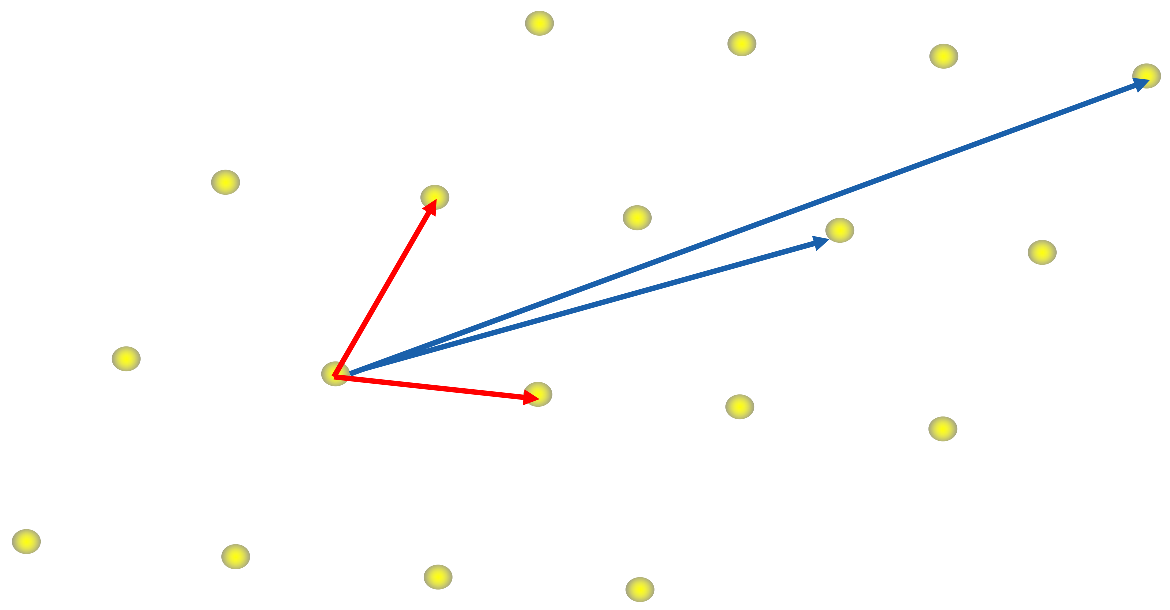
$-561 \cdot \begin{pmatrix} 100 \\ 99 \end{pmatrix} + 567 \cdot \begin{pmatrix} 99 \\ 98 \end{pmatrix} = \begin{pmatrix} 33 \\ 27 \end{pmatrix} \neq \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \mathrm{CVP}(t)$

Key generation

Key generation: $n \in \mathbb{N}, L \subseteq \mathbb{R}^n$ lattice

Secret key: „reduced“ basis B of L. (Allows to efficiently solve CVP.)

Public key: „bad” basis B' of L. (Does not.)



Public-key encryption

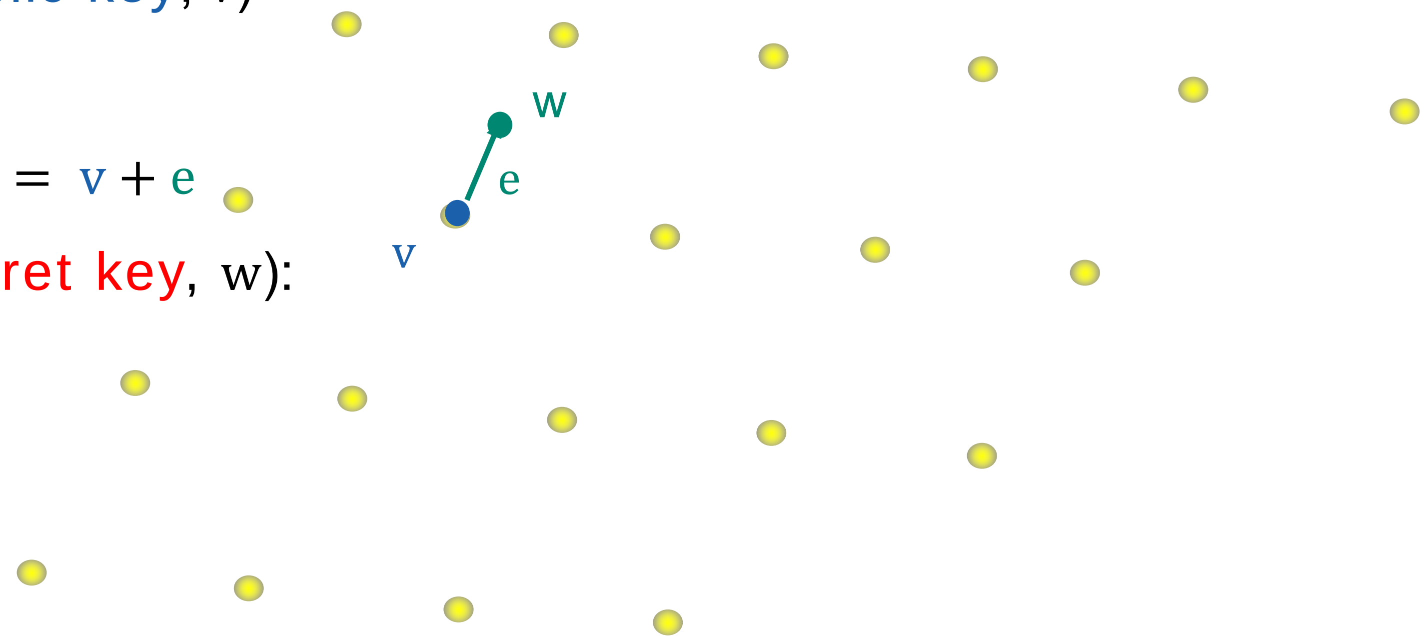
Plaintext $v \in L$

Encryption(public key, v)

- small $e \in \mathbb{R}^n$
- ciphertext $w = v + e$

Decryption(secret key, w):

- $v = CV(w)$



Digital signature

Public: Cryptographic hash function $h: \{0,1\} \to \mathbb{R}^n$

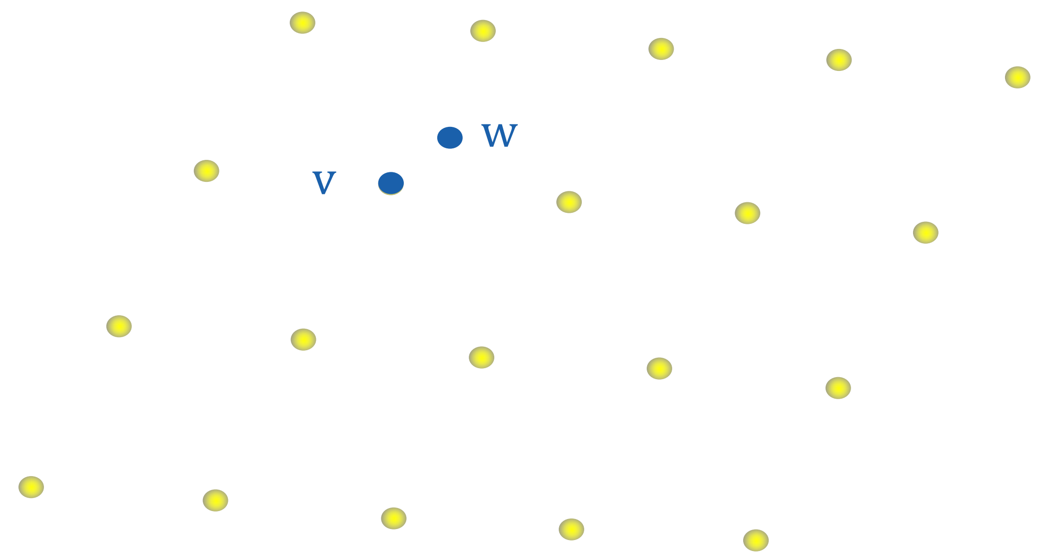
Sign(secret key, document d):

$$w = h(d)$$
$$v = CV(w)$$

Verify(public key, v, w):

v lattice vector?

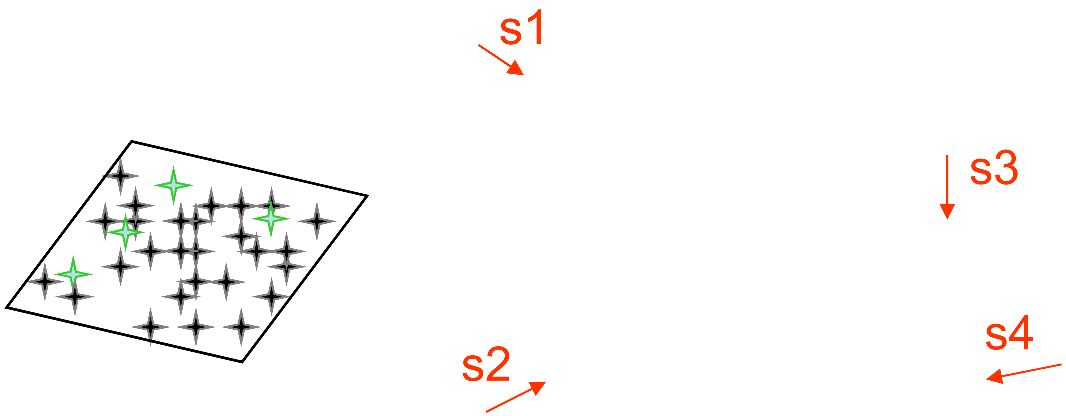
v close to w ?



Early lattiice-based schemes

- GGH Sign 1995
- NTRU Encrypt 1996
- NTRU Sign 2003

Learning the secret key
Nguyen and Regev 2006



NTRU-251 broken using ≈ 400 signatures

GGH-400 broken using ≈ 160.000 signatures

State-of-the-art lattice-based signatures

Lattice-based signature schemes

Signature scheme	Year	Computational Assumption	ROM?	Tight?	QROM?	Tight?
GPV	2008	SIS	✓	✓	✓	✓
BG	2014	SIS, LWE	✓	✗	-	-
TESLA	2017	LWE	✓	✓	✓	✓
GPV-poly	2013	R-SIS	✓	✓	✓	✓
GLP	2012	DCK	✓	✗	-	-
BLISS	2013	R-SIS, NTRU	✓	✗	-	-

SIS and LWE

Small Integer Solutions Problem (SIS)

TECHNISCHE UNIVERSITÄT DARMSTADT

$$\begin{pmatrix} 3 & 1 & 2 & 4 & 2 & 4 \\ 0 & 3 & 6 & 2 & 0 & 3 \\ 2 & 0 & 4 & 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \\ ? \\ ? \\ ? \\ ? \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \mod 7$$

Small Integer Solutions Problem (SIS)

$$\begin{pmatrix} 3 & 1 & 2 & 4 & 2 & 4 \\ 0 & 3 & 6 & 2 & 0 & 3 \\ 2 & 0 & 4 & 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \mod 7$$

SIS - general

Given:

$A \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$ $\cdot$? $=$ 0 mod q

Bound β

Find:

$s \in \mathbb{Z}_q^{m}$ with $||s|| < \beta$ and

$A \cdot s = 0 \mod q$

Learning with errors problem (LWE)

$$\begin{pmatrix} 3 & 1 & 2 \\ 0 & 3 & 6 \\ 2 & 0 & 4 \\ 4 & 2 & 4 \\ 2 & 0 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \\ ? \end{pmatrix} + \begin{pmatrix} ? \\ ? \\ ? \\ ? \\ ? \\ ? \end{pmatrix} = \begin{pmatrix} 6 \\ 1 \\ 6 \\ 2 \\ 5 \\ 3 \end{pmatrix} \mod 7$$

$$A \cdot s + e = b \mod q$$

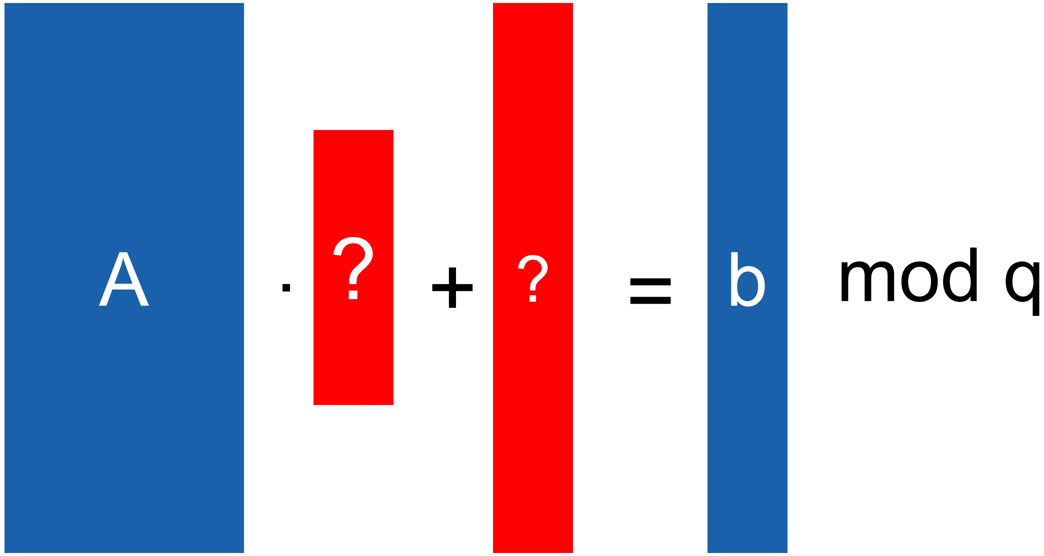
Learning with errors problem (LWE)

$$\begin{pmatrix}3&1&2\\0&3&6\\2&0&4\\4&2&4\\2&0&3\\1&3&2\end{pmatrix} \cdot \begin{pmatrix}1\\0\\1\end{pmatrix} + \begin{pmatrix}1\\2\\0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}6\\1\\6\\2\\5\\3\end{pmatrix} \mod 7$$

$$A \cdot s + e = b \mod q$$

LWE - general

Given:



$A \leftarrow_{\$} \mathbb{Z}_q^{m \times n}$

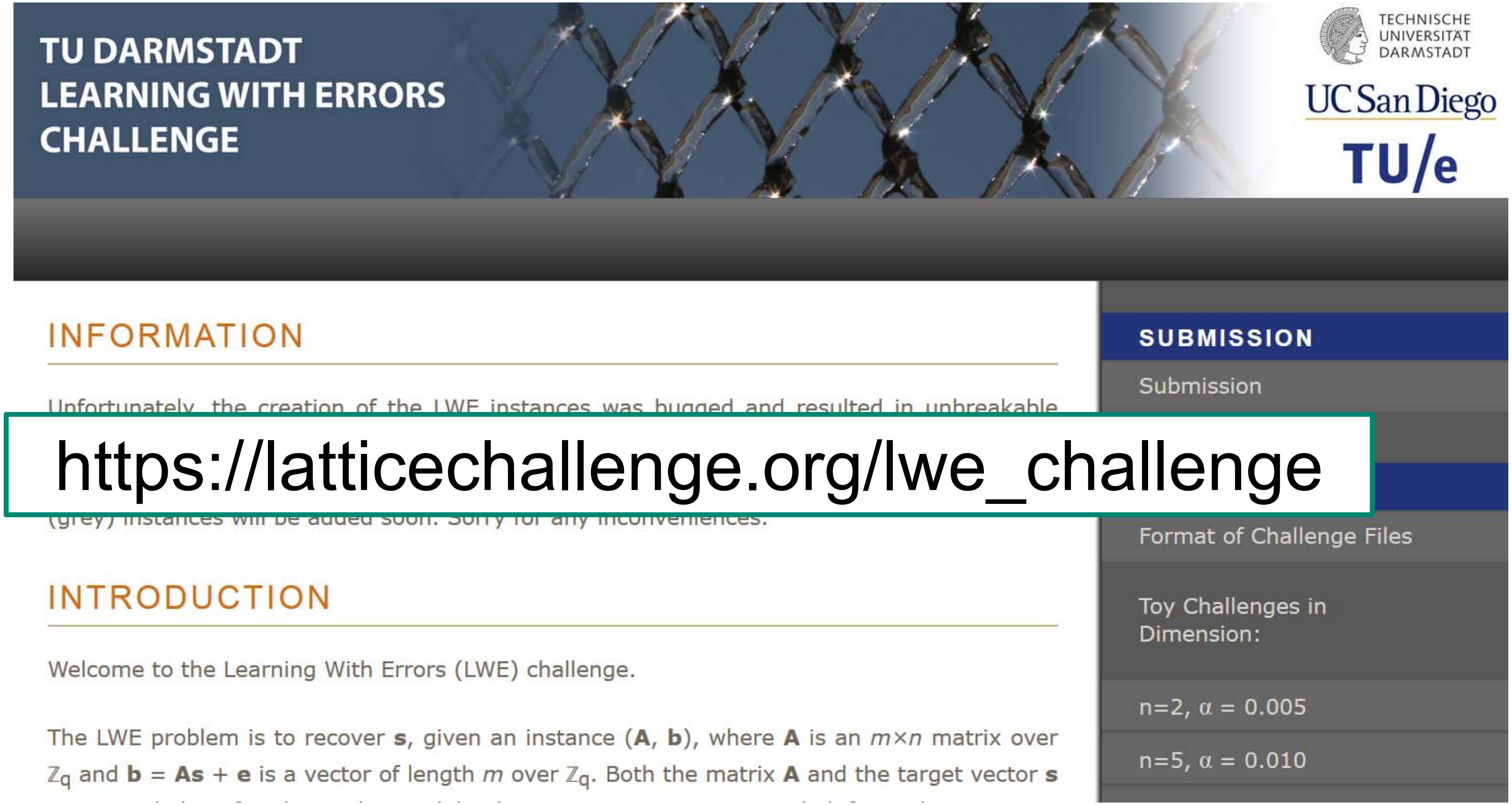
$b \leftarrow \mathbb{Z}_q^{m}$

Find:

$A \cdot s + e = b \bmod q \qquad (s,e) \leftarrow D_\sigma^n \times D_\sigma^m$

Practical complexity of LWE

TECHNISCHE UNIVERSITÄT DARMSTADT



https://latticechallenge.org/lwe_challenge

CROSSING

Selecting secure parameters

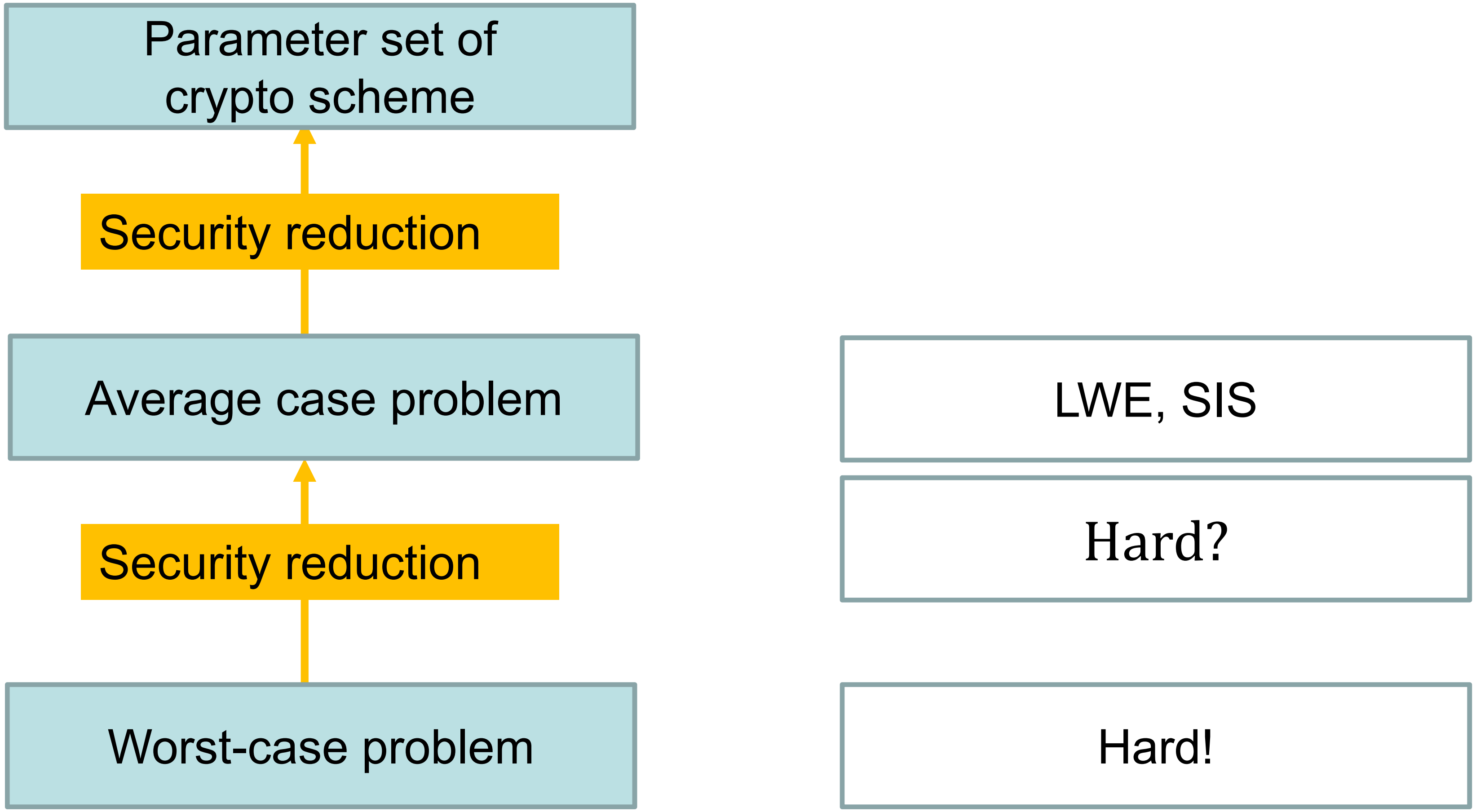
Selecting secure RSA parameters

TECHNISCHE UNIVERSITÄT DARMSTADT

Parameters of RSA	$p, q, \; n = pq$
↑	
Average case factoring problem	p, q random large primes
Hard in classical setting	

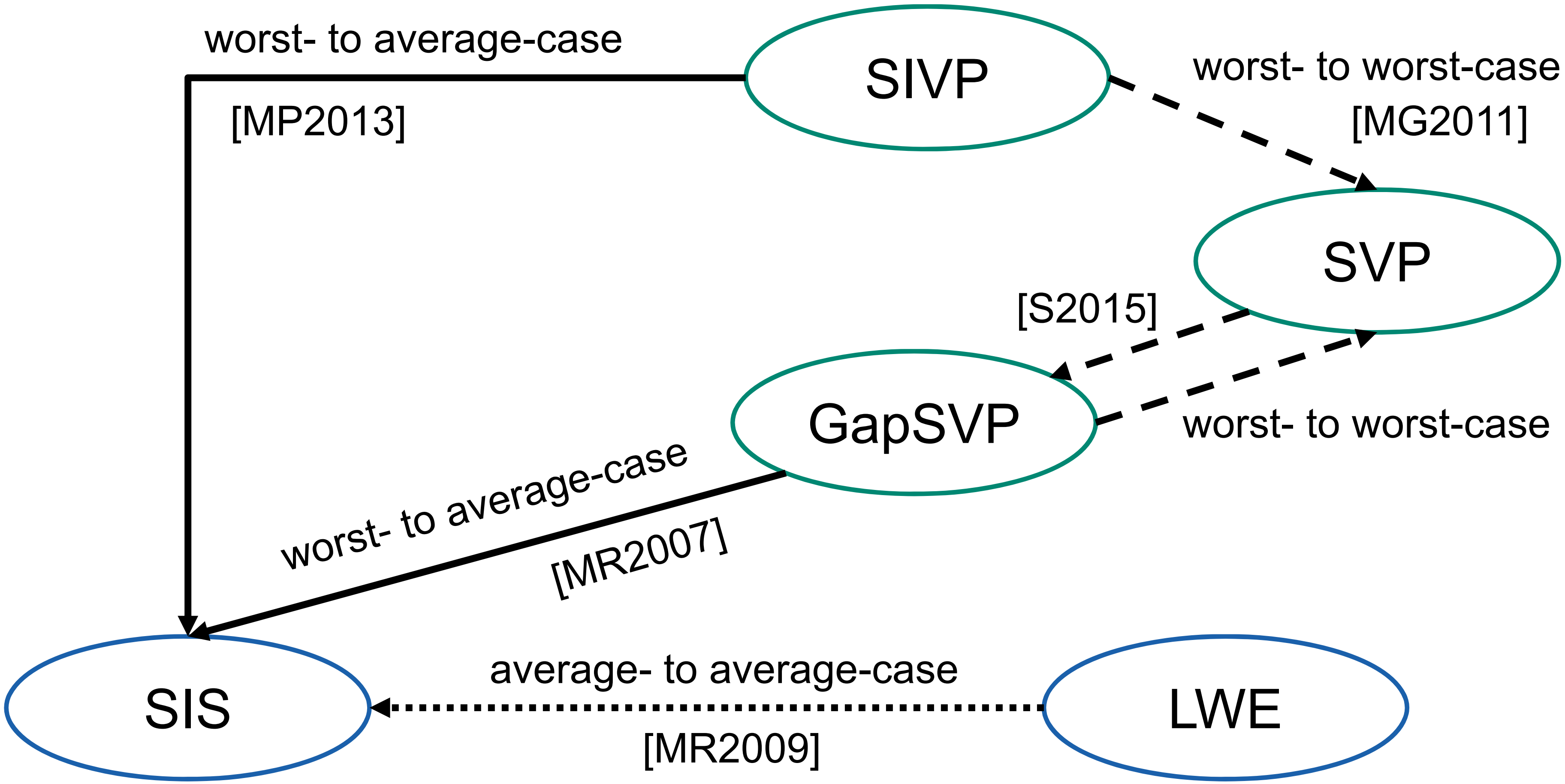
CROSSING

Secure parameters for lattice-based schemes



CROSSING

Reductions between lattice problems



TESLA

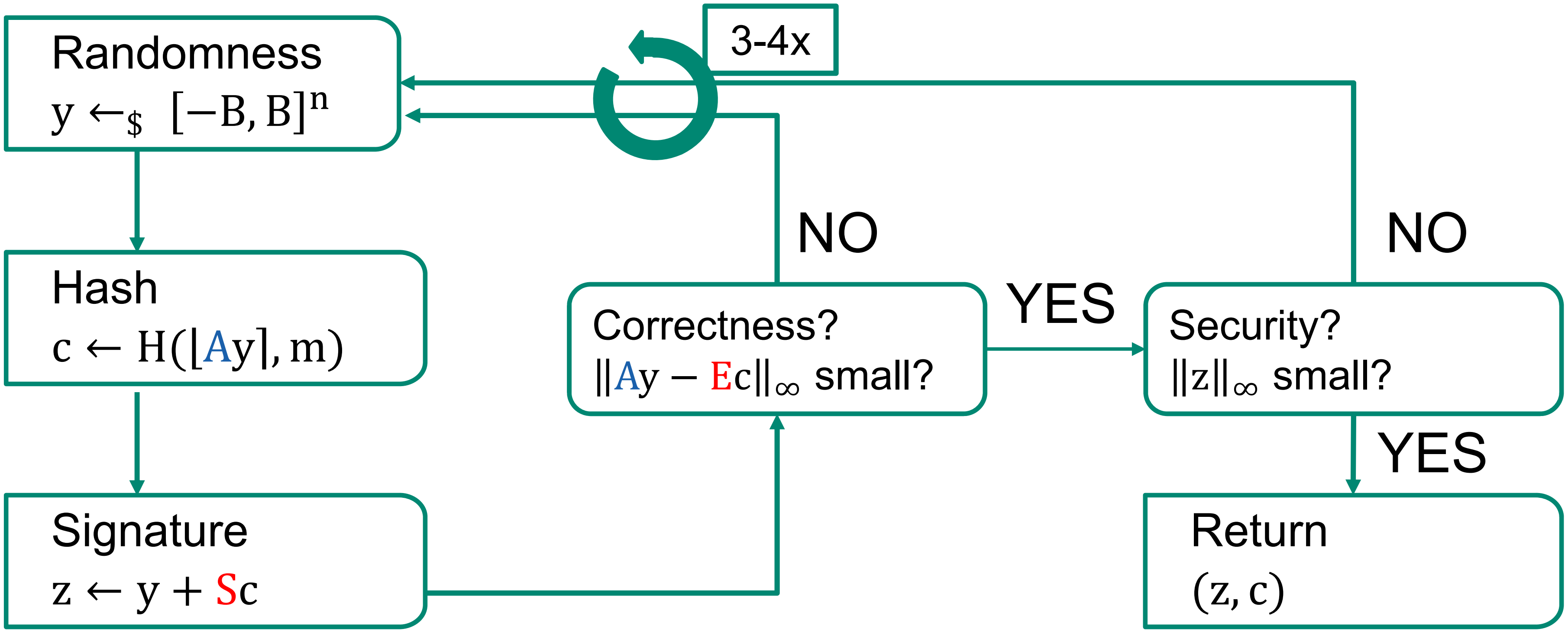
TESLA signature scheme

$A \leftarrow_{\$} \mathbb{Z}_q^{m \times n}$

$sk = (S, E) \leftarrow_{\sigma} \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^{m \times n}$

$pk = (A, B = AS + E \bmod q)$

Sign(sk, m):



TESLA - verification

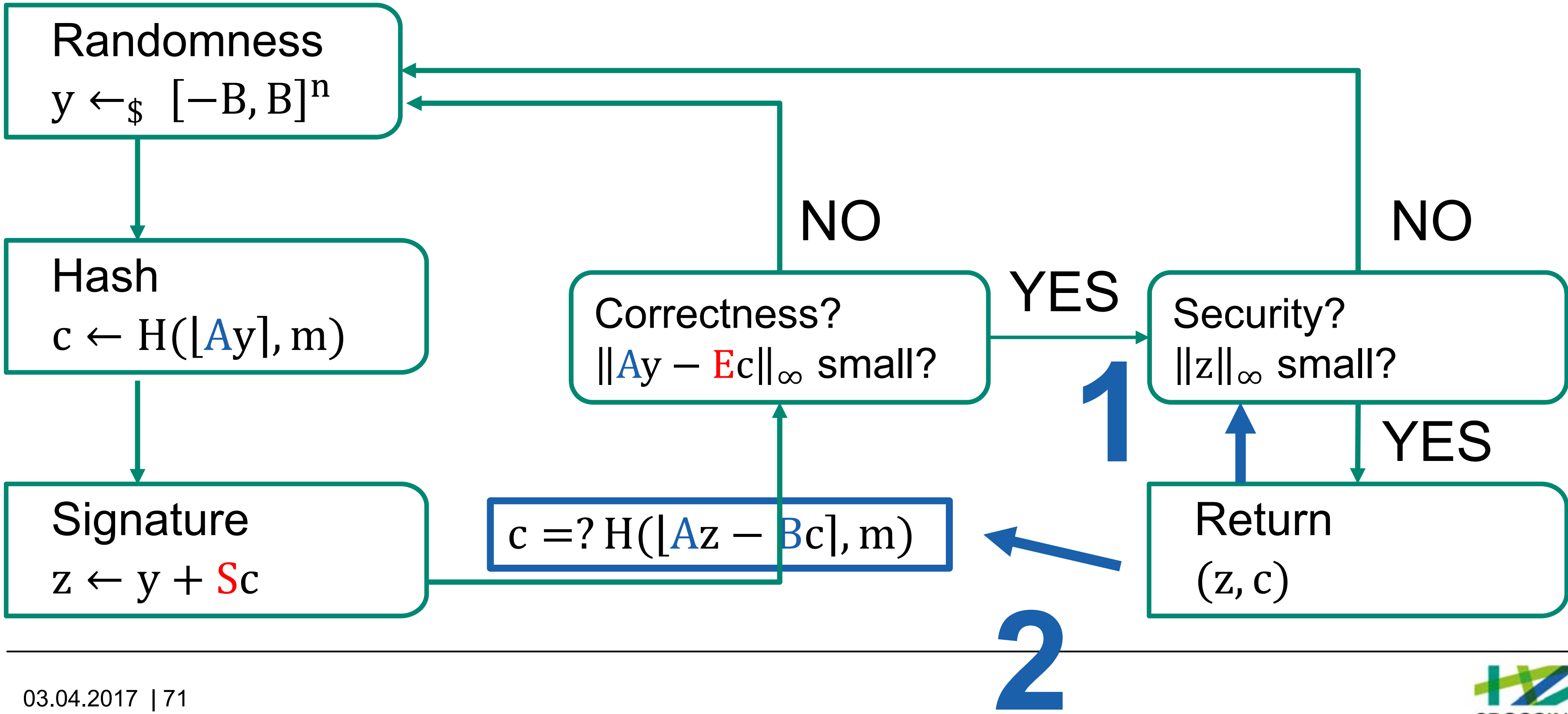
TECHNISCHE UNIVERSITÄT DARMSTADT

$A \leftarrow_{\$} \mathbb{Z}_q^{m\times n}$

$sk = (S, E) \leftarrow_{\sigma} \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{m\times n}$

$pk = (A, B = AS + E \bmod q)$

Sign(sk, m):



CROSSING

ring-TESLA

$A \leftarrow_{\$} \mathbb{Z}_q^{m\times n}$

$sk = (S, E) \leftarrow \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{m\times n}$

$pk = (A, B = AS + E)$

Most expensive operation

$a_1, a_2 \leftarrow \mathbb{Z}_q[x]/\langle x^n + 1\rangle$

$sk = (s, e_1, e_2) \leftarrow \mathbb{Z}_q[x]/\langle x^n + 1\rangle$

$pk = (a_1, a_2, b_1 = a_1 s + e_1, b_2 = a_2 s + e_2)$

TESLA signature scheme – Performance

TECHNISCHE UNIVERSITÄT DARMSTADT

Scheme	Cyclecounts [k-cycles]		Sizes [kB]			Security
	Sign	Verify	pk	sk	sig.	[bit]
GPV	312,800	50,600	27,840	12,064	29	96
BG	1,204	335	1,582	891	1.5	97
TESLA	41,604	5,017	16,406	9,986	1.9	96
GPV-poly	80,500	11,500	55	26	32	96
GLP	452	34	1.5	0.25	1.12	80
BLISS	358	102	0.87	0.25	0.63	128
RSA-2048	5,347	76	0.25	0.25	0.25	112
ECDSA P256	388	920	0.06	0.09	0.06	128

TECHNISCHE UNIVERSITÄT DARMSTADT

State-of-the-art lattice-based PK encryption

CROSSING

Lattice-based PK encryption schemes

Encryption scheme	Year	Computational Assumption	CPA/ CCA?	Security reduction
LWE Regev	2005	LWE	CPA	yes
LARA	2016	(R-)LWE	CPA, CCA1,CCA2	Yes
NTRU	1998	NTRU	CPA (CCA1)	-
LP	2011	(R-)LWE	CPA	Yes
CCA-MP	2012	LWE	CCA1	Yes
CCA-Peikert	2009	LWE	CCA1/2	Yes

LARA – Performance (128-bit Security)

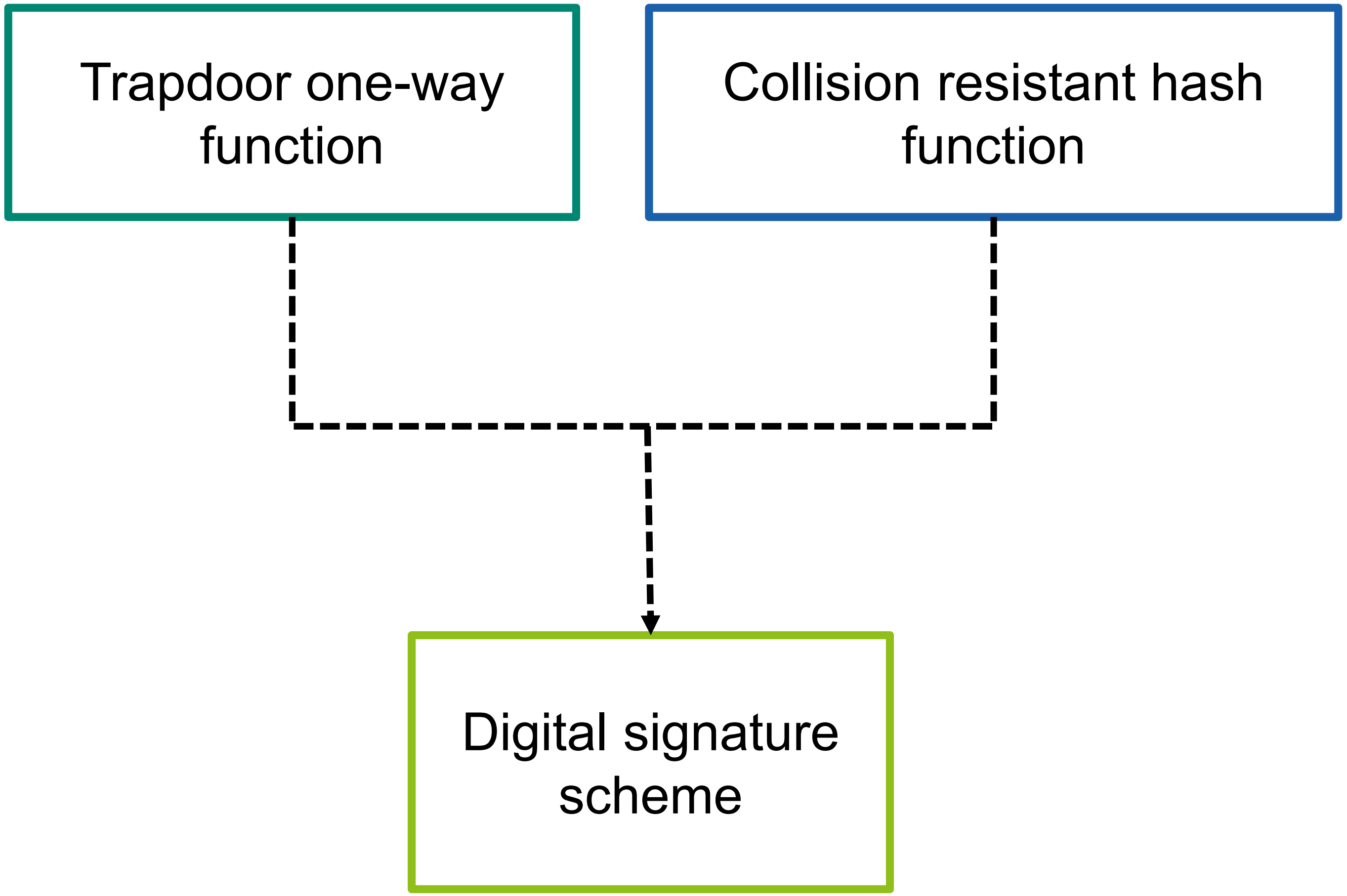
El Bansarkhani et al.

TECHNISCHE UNIVERSITÄT DARMSTADT

Scheme	Cyclecounts/message bit		Sizes [kB]		Ciphertext expansion
	Encrypt	Decrypt	pk	sk	
LARA-CPA	22	15	1.25	0.28	2.8
LARA-CCA1	29	22	1.19	0.28	3.1
LARA-CCA2	50	42	1.19	0.28	3.1
Linder-Peikert-CPA	444	65	1.25	0.28	40
NTRU-CCA2	138	158	0.69	0.64	8
RSA-4096	51	2992	0.25	0.25	1

Hash-based signatures

Typical construction



Trapdoor one-way functions hard to construct but not required

Hash-based Signatures
Merkle (1979/1989)

TECHNISCHE UNIVERSITÄT DARMSTADT

A CERTIFIED DIGITAL SIGNATURE

Ralph C. Merkle
Xerox PARC
3333 Coyote Hill Road,
Palo Alto, Ca. 94304
merkle@xerox.com
(Subtitle: That Antique Paper from 1979)

Abstract
A practical digital signature system based on a conventional encryption function which is as secure as the conventional encryption function is described. Since certified conventional systems are available it can be implemented quickly, without the several years delay required for certification of an untested system.

Key Words and Phrases: Public Key Cryptosystem, Digital Signatures, Cryptography, Electronic Signatures, Receipts, Authentication, Electronic Funds Transfer.

CR categories: 3.56, 3.57, 4.9

Lamport-Diffie OTSS

Lamport, Diffie (1976)

Example:

signing strings

of length 3

$x_1(0)$	$x_1(1)$	$x_2(0)$	$x_2(1)$	$x_3(0)$	$x_3(1)$
0	1	1	0	0	1
1	1	1	0	1	0
0	0	1	1	1	1

$$\downarrow H$$

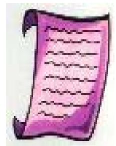
0	1	0	0	1	1
1	1	0	1	0	1
1	1	0	0	0	0
$y_1(0)$	$y_1(1)$	$y_2(0)$	$y_2(1)$	$y_3(0)$	$y_3(1)$

Lamport-Diffie OTSS

Lamport, Diffie (1976)

0 1 1 0 0 1
1 1 1 0 1 0
0 0 1 1 1 1

0 1 0 0 1 1
1 1 0 1 0 1
1 1 0 0 0 0

 = *hello world*

↓ H

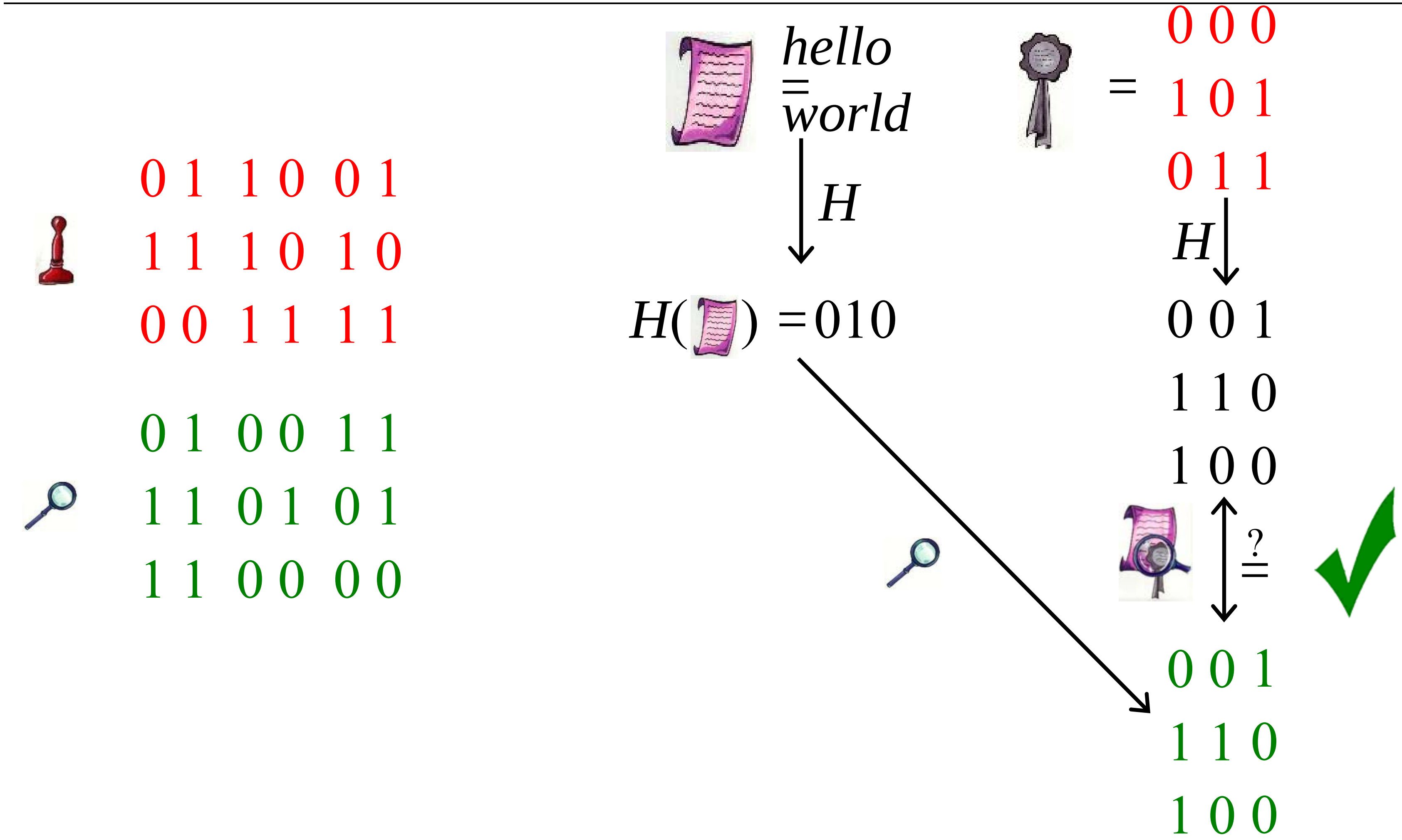
$H($$) = 0\ 1\ 0$

↓ 

 =
0 0 0
1 0 1
0 1 1

Lamport-Diffie OTSS

Lamport, Diffie (1976)



CROSSING

Merkle Signature Scheme

TECHNISCHE UNIVERSITÄT DARMSTADT

Lamport-Diffie OTSS:

One key pair (, ) per signature

Hash tree:

Reduces validity of many verification keys to one public key: root of tree

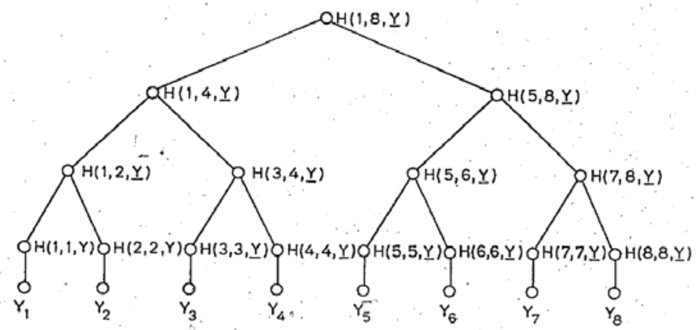


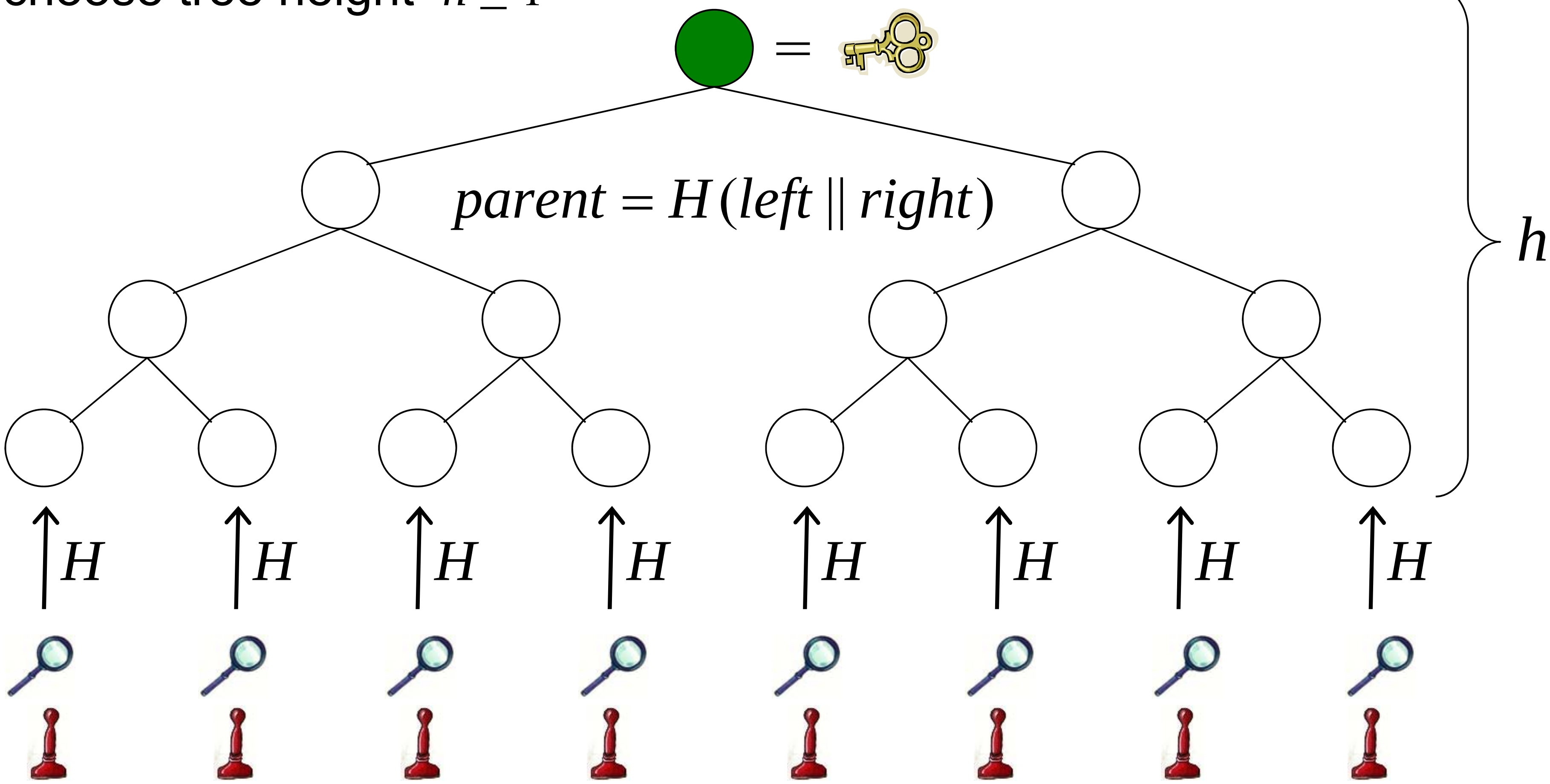
FIG 1

AN AUTHENTICATION TREE WITH N = 8.

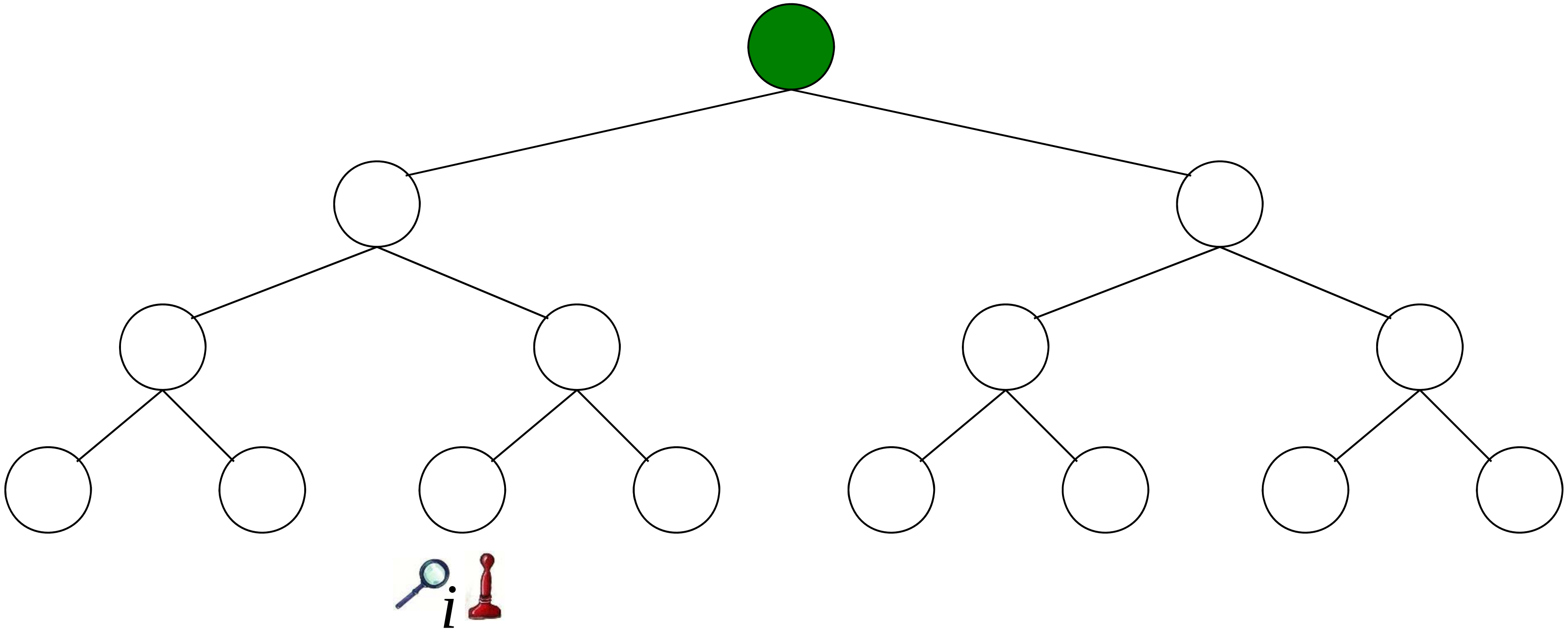
PAGE 41B

Merkle Signature Scheme — Key Generation

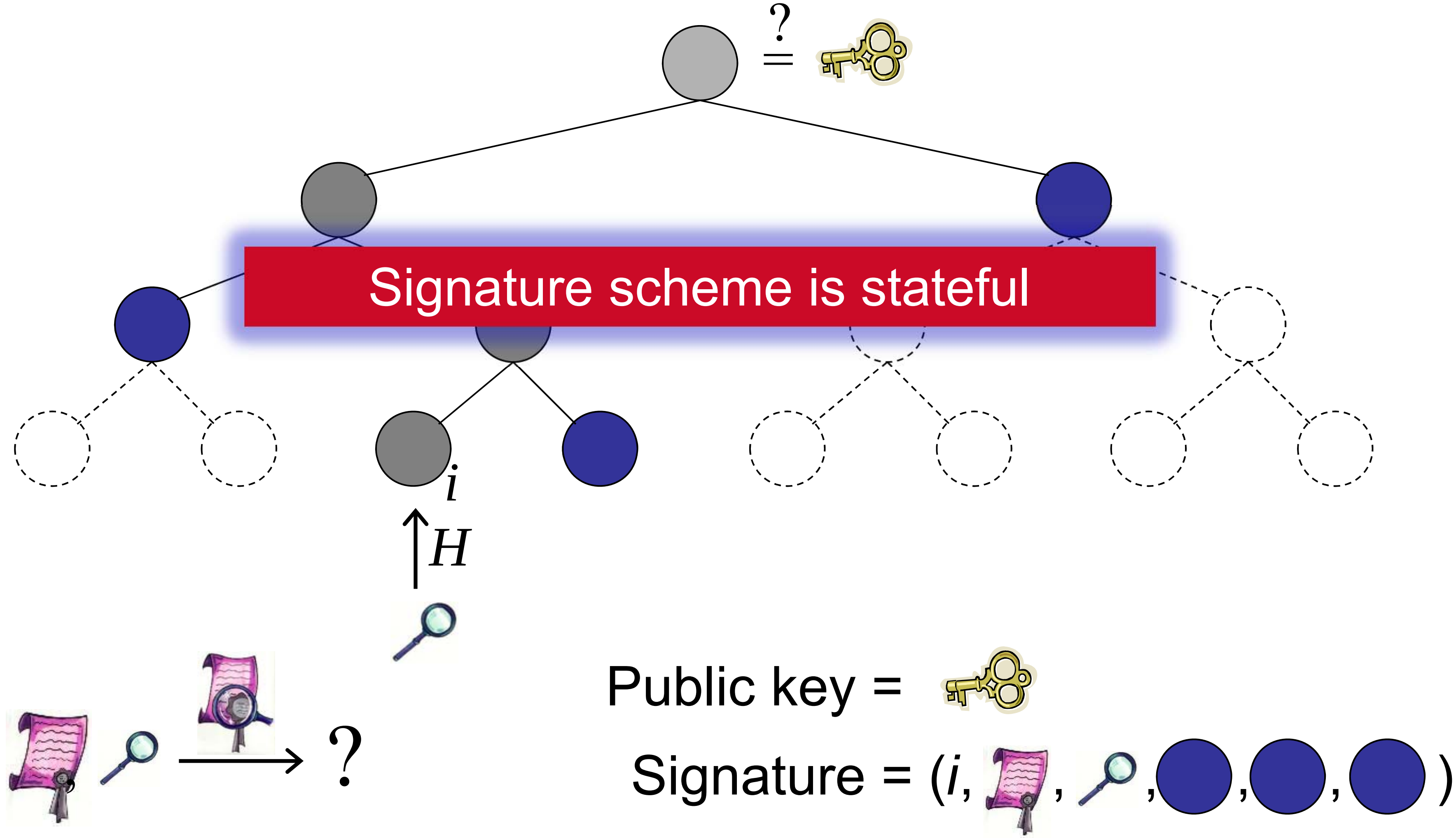
choose tree height $h \geq 1$



Merkle Signature Scheme — Signing



Merkle Signature Scheme — Verifying



XMSS:

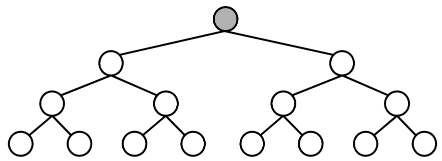
A practical signature template with minimal security assumptions

J.B., Carlos Coronado Garcia, Erik Dahmen, Andreas Hülsing

XMSS improves

TECHNISCHE UNIVERSITÄT DARMSTADT

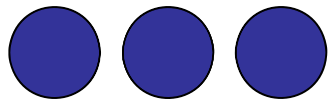
- Public key generation time



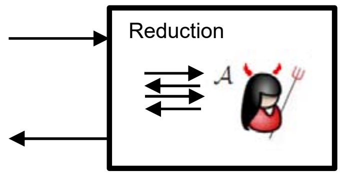
- Private key size

- Signature size

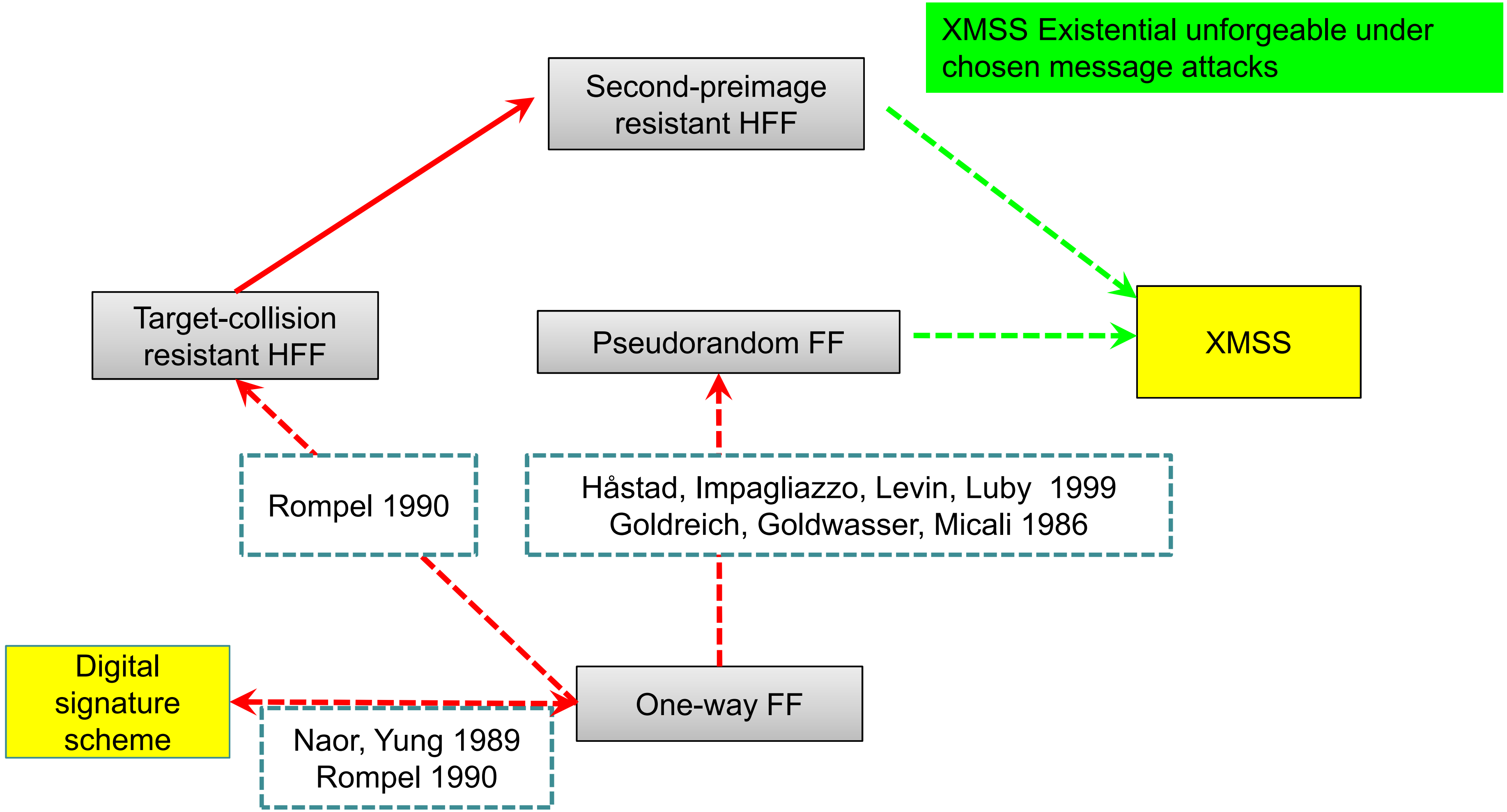
- Authentication path generation time and space



- Provable security

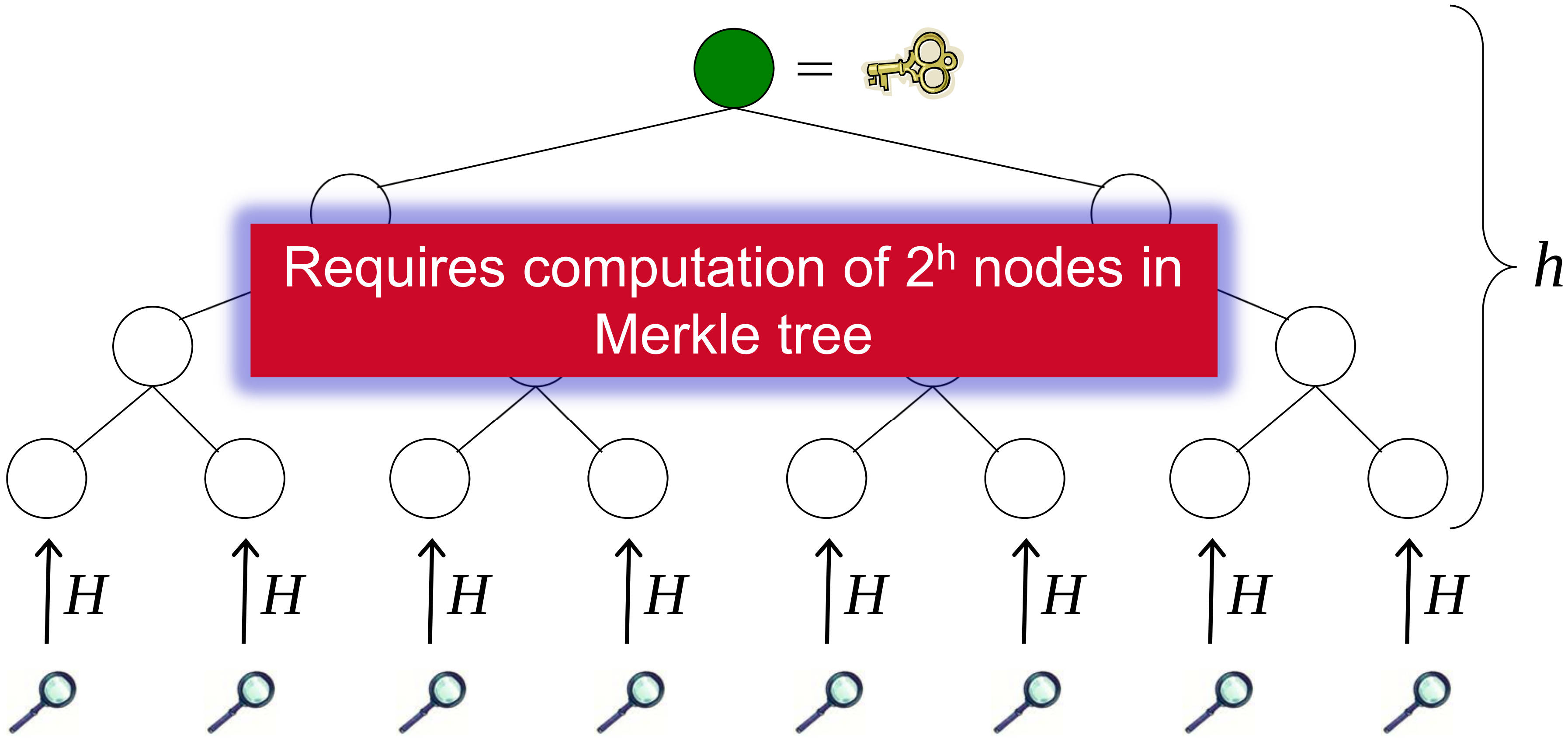


XMSS has minimal security requirements



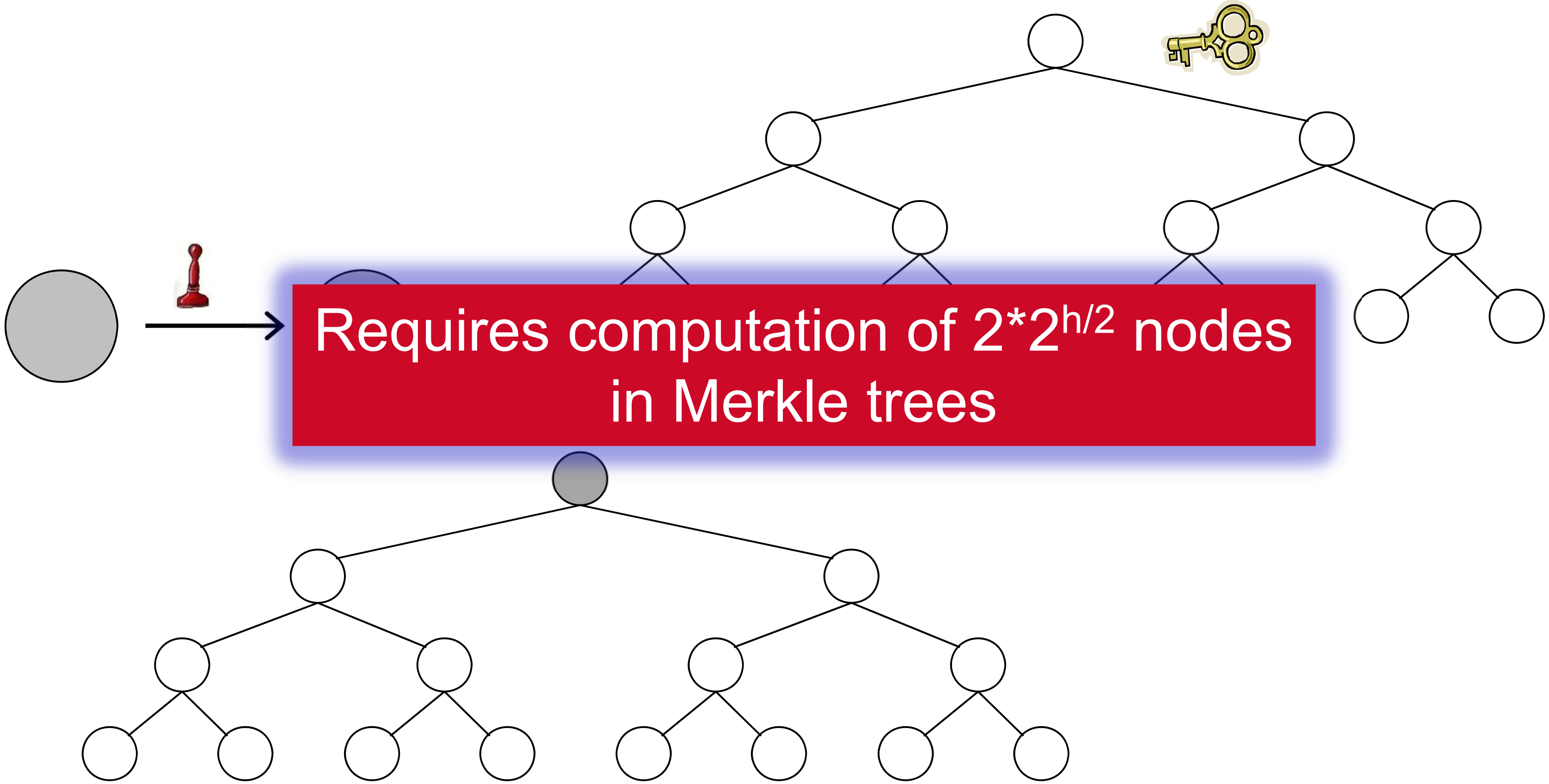
Improved public key generation: tree chaining

XMSS Public Key Generation



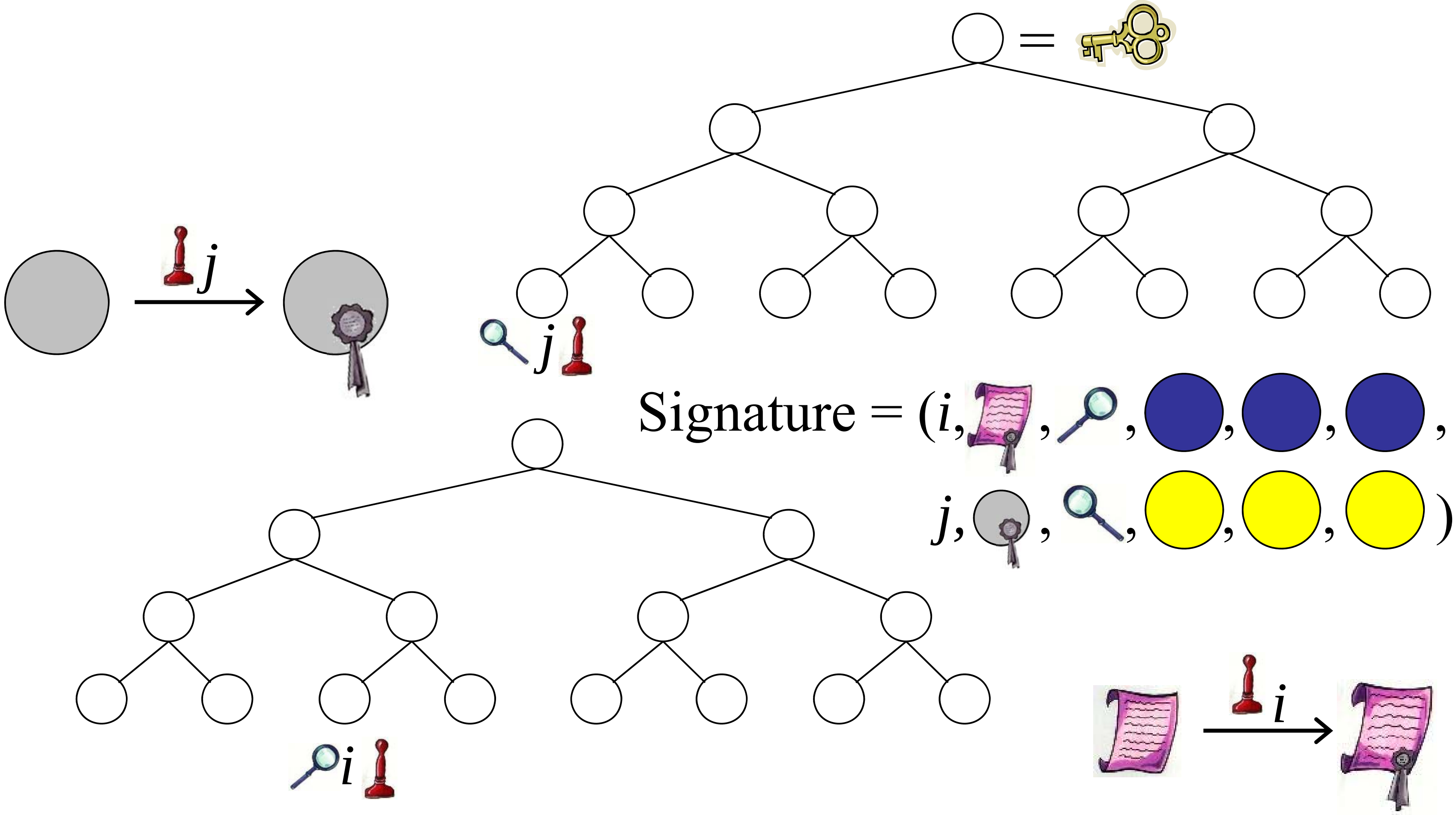
Requires computation of 2^h nodes in Merkle tree

Two Levels
Key generation

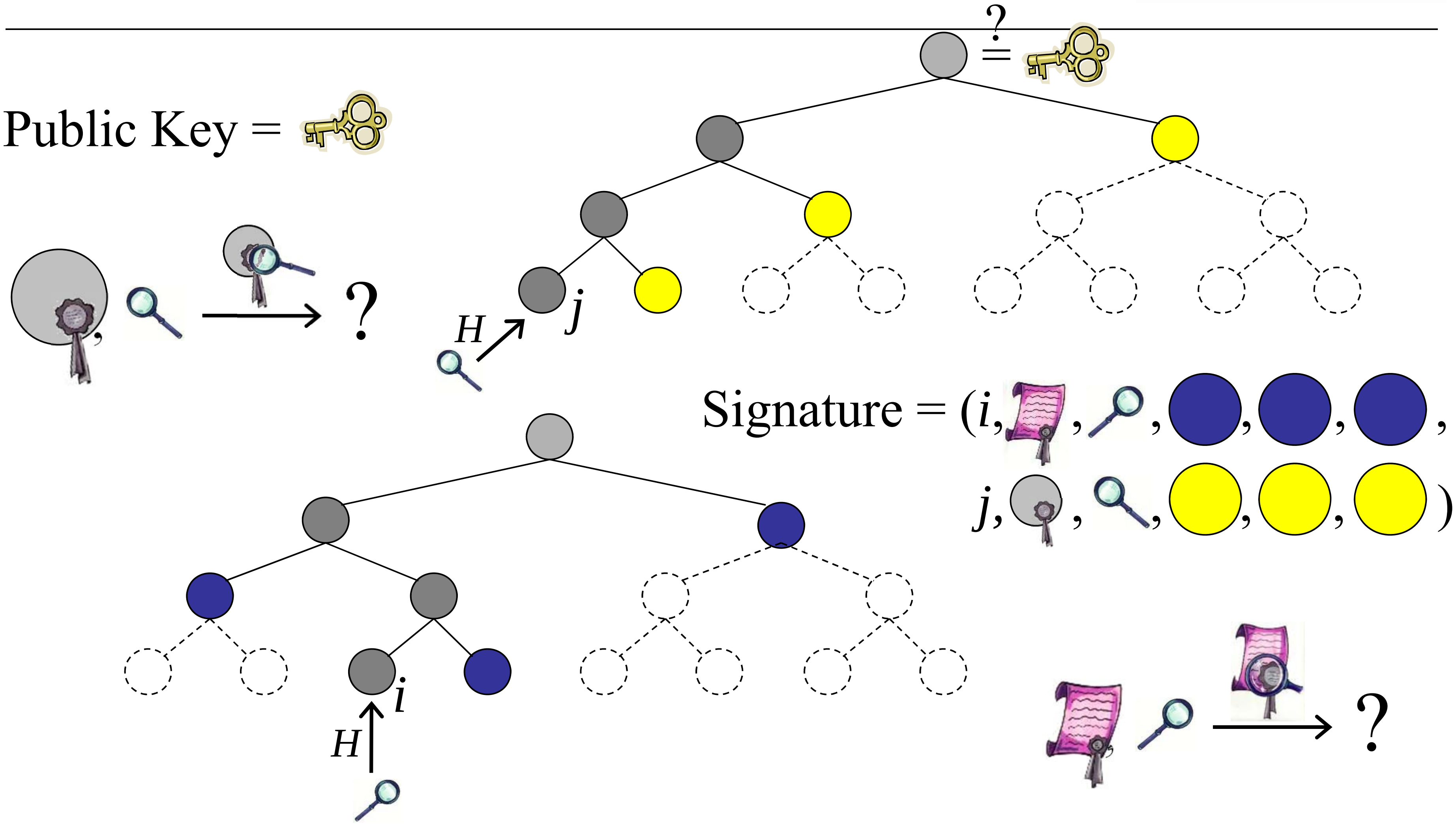


Requires computation of $2*2^{h/2}$ nodes in Merkle trees

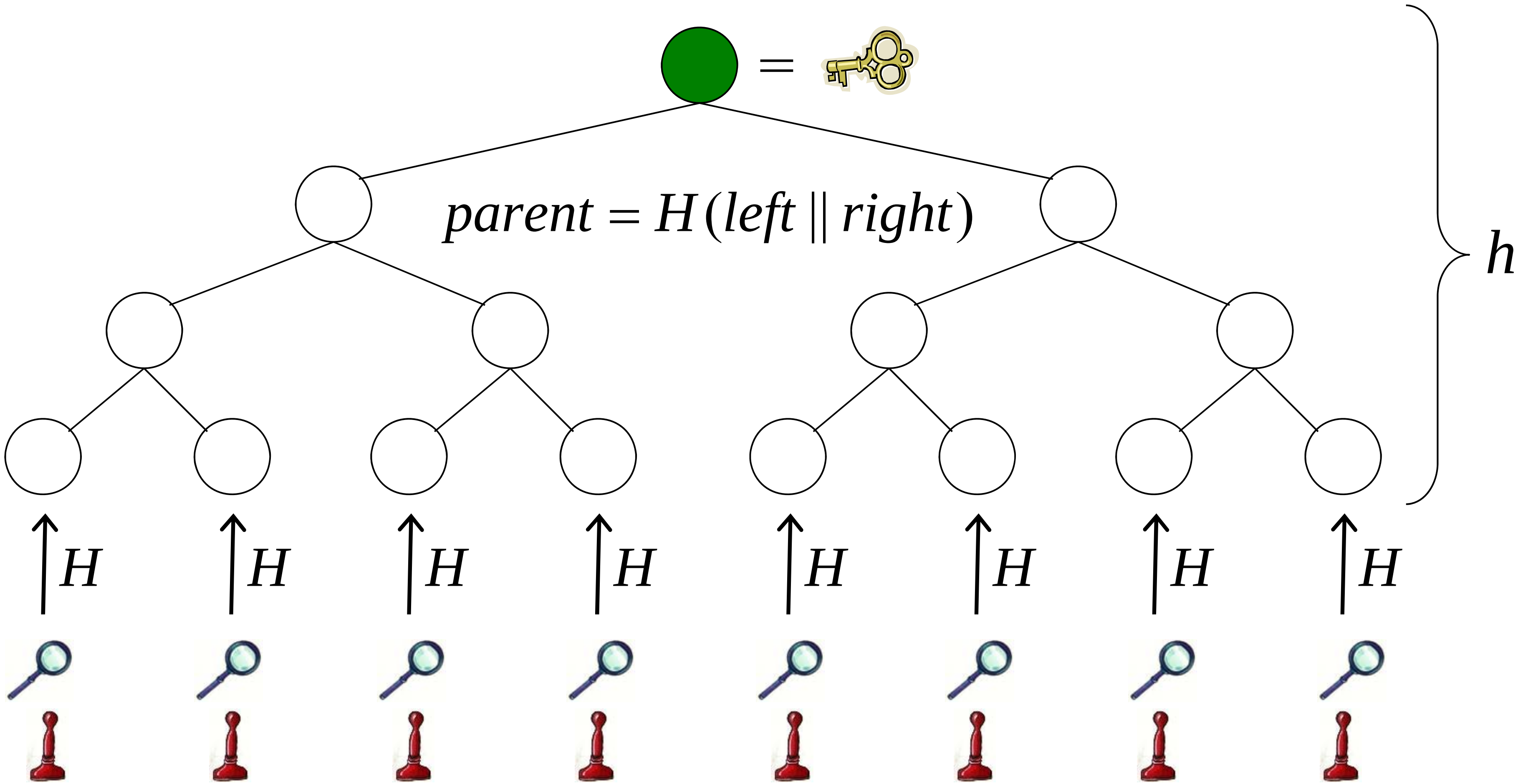
Two Levels
Signing



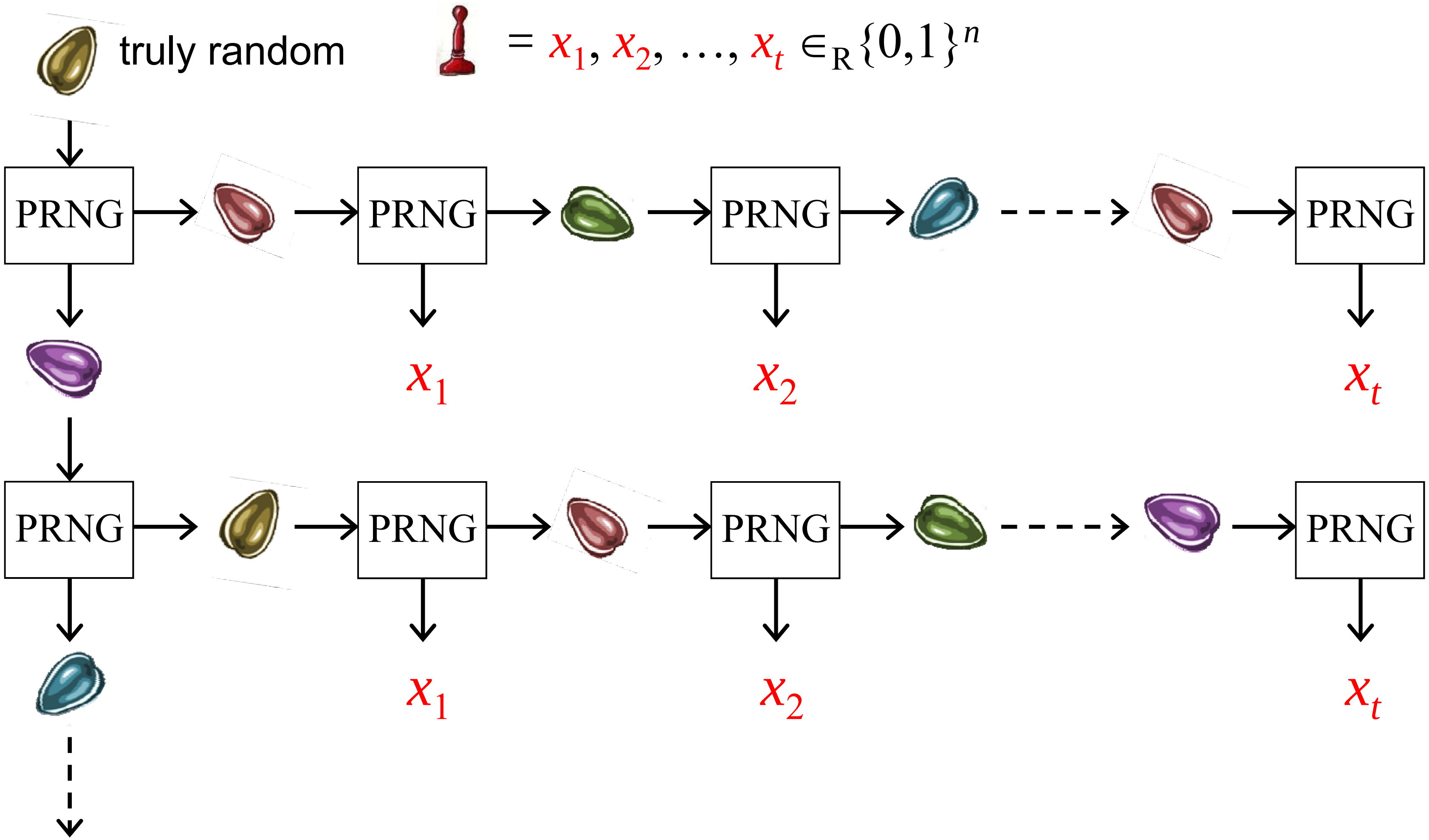
Two Levels
Verifying



Improved secret key size: pseudo-random generation



parent = H(left || right)
h
H
H
H
H
H
H
H
H


truly random
$= x_1, x_2, \ldots, x_t \in_R \{0,1\}^n$
PRNG
PRNG
PRNG
PRNG
x_1
x_2
x_t
PRNG
PRNG
PRNG
PRNG
x_1
x_2
x_t

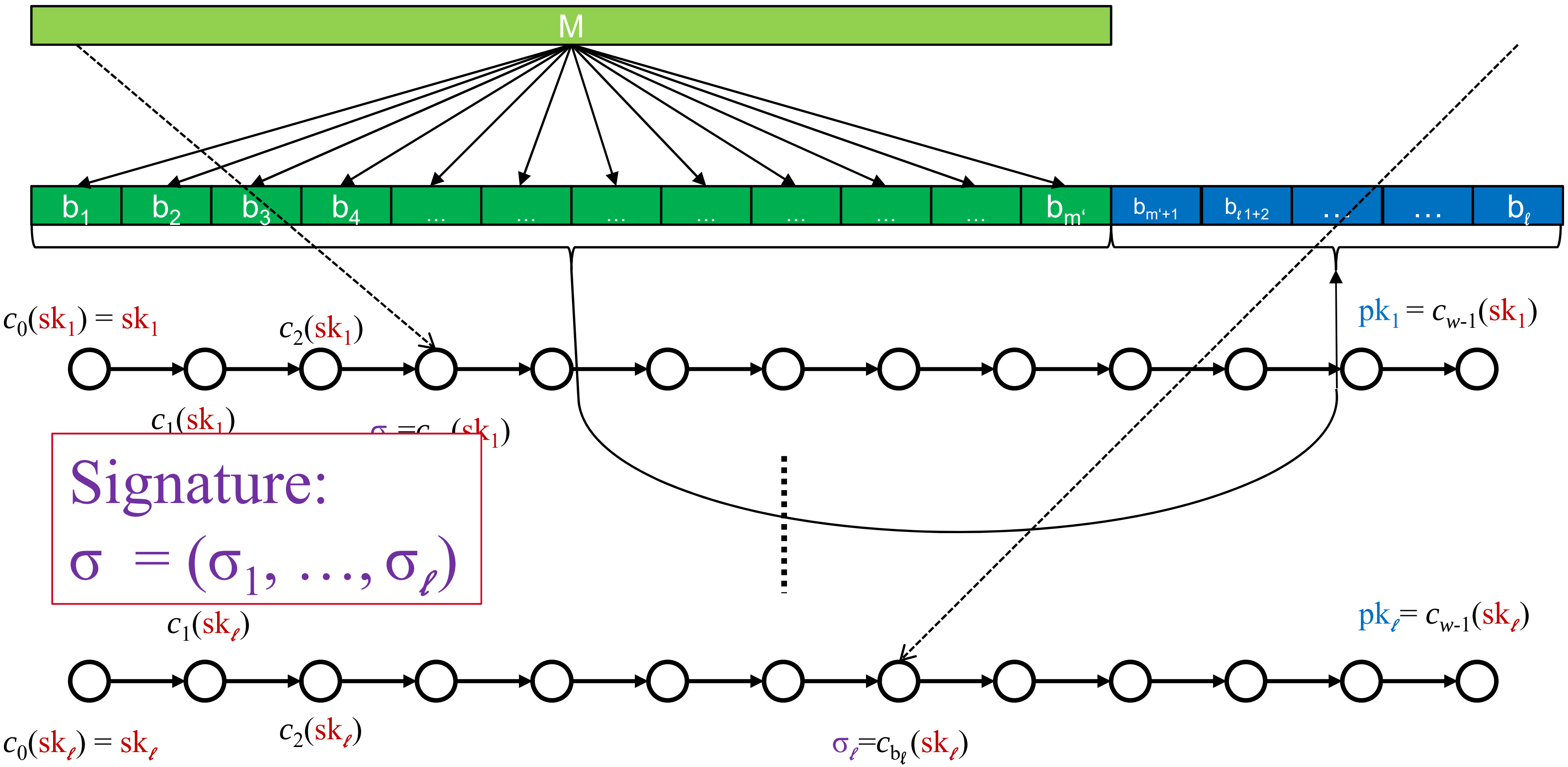
Smaller signatures

Smaller signatures: Winternitz OTS (WOTS) / WOTS⁺

Initial idea: Winternitz (Mer89)

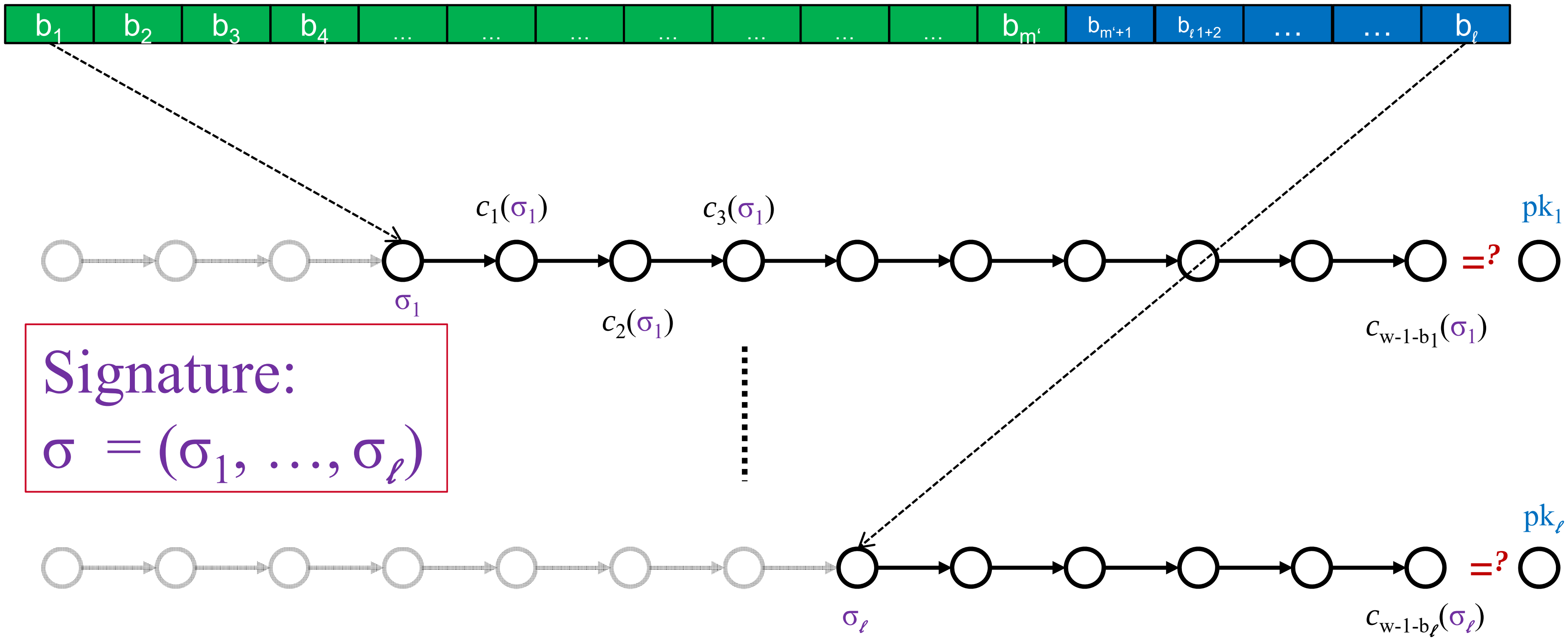
WOTS⁺: Hülsing (Hül13)
Requires second preimage resistant undetectable one-way function family.

WOTS+ Signature Generation

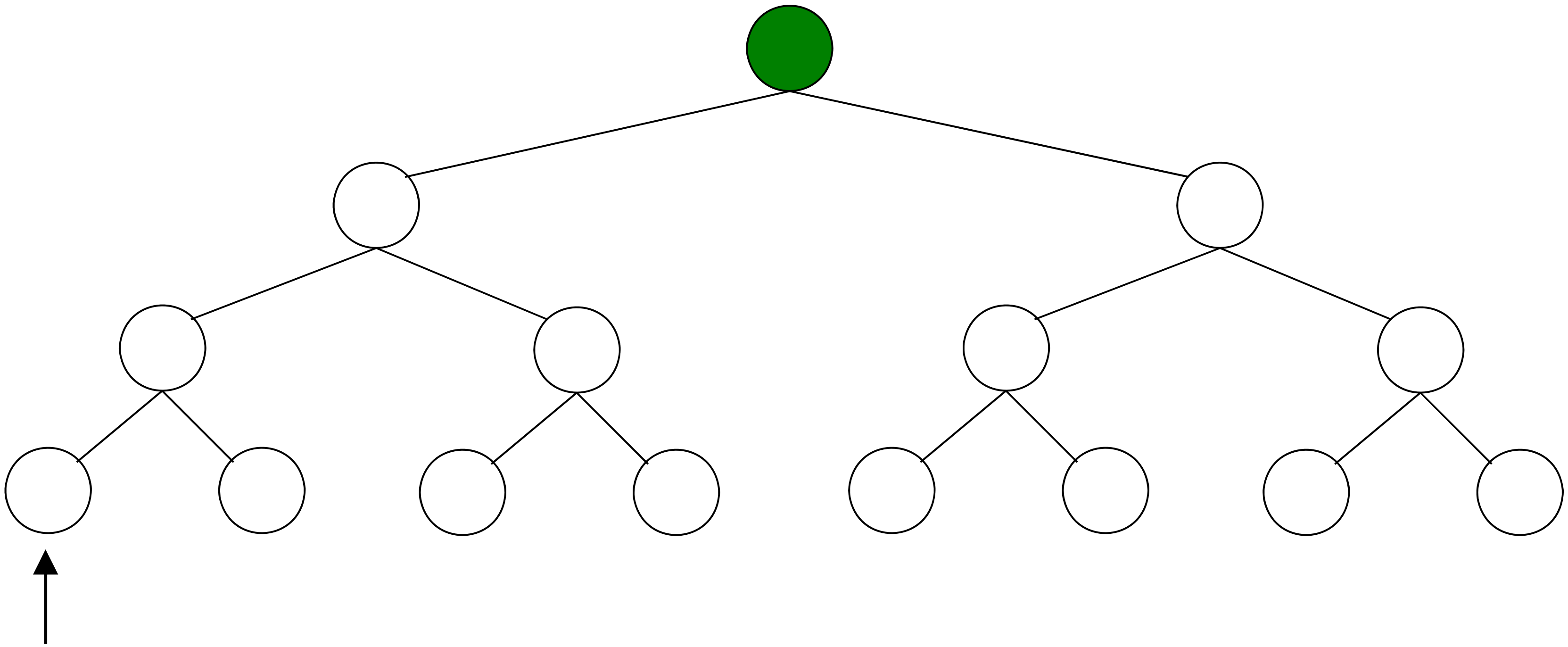


WOTS+ Signature Verification

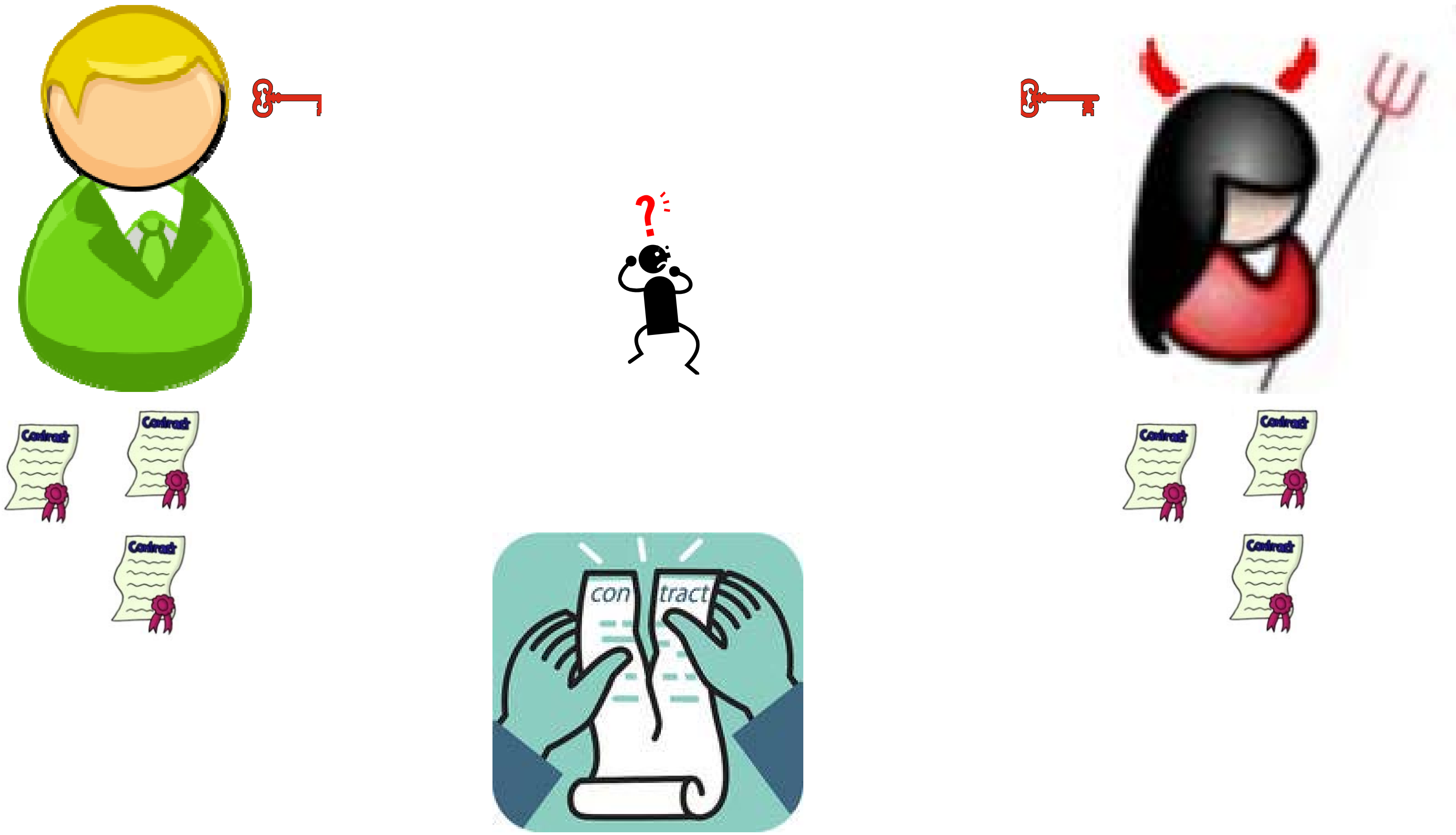
Verifier knows: M, n, w, c



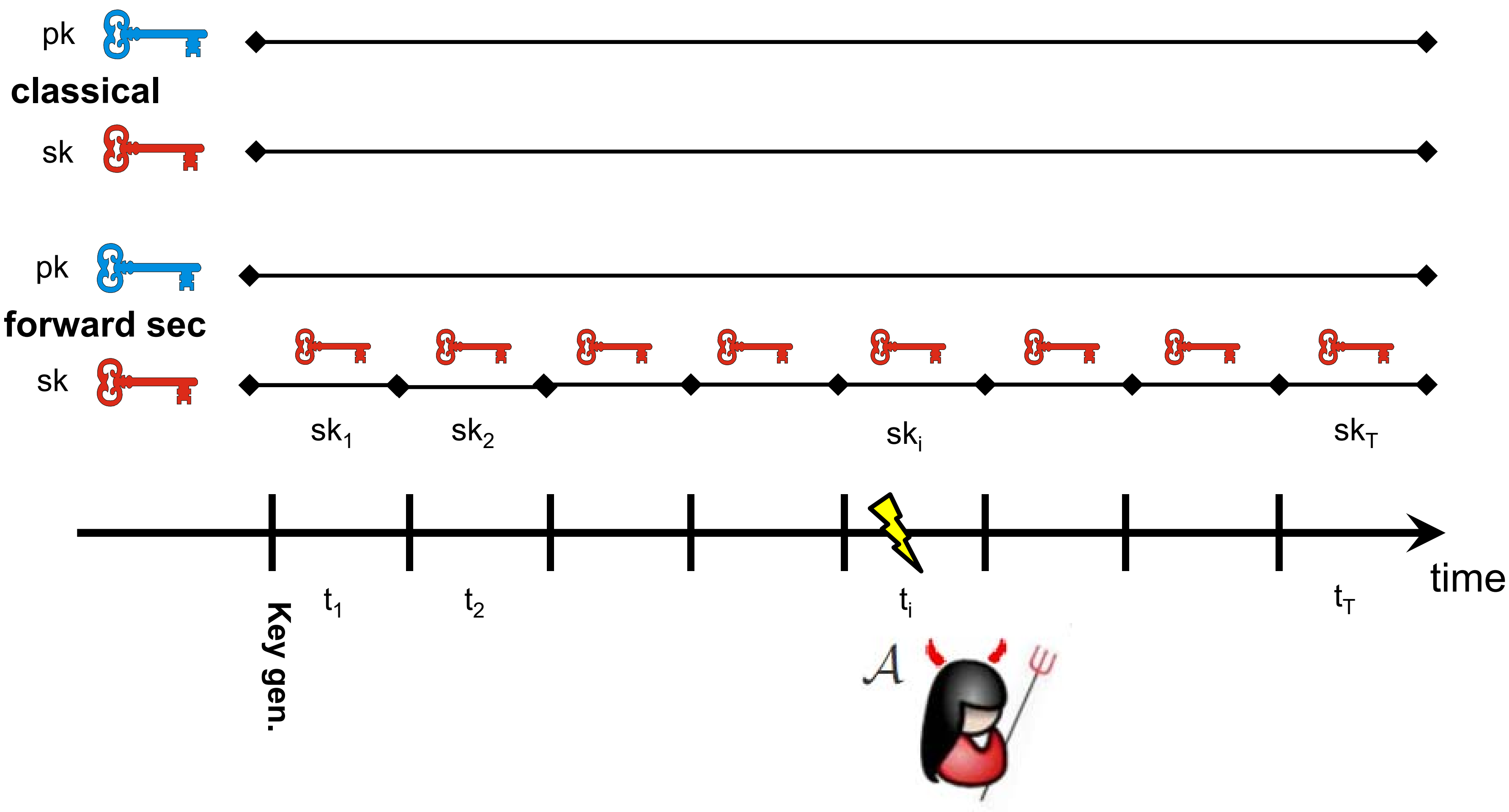
Authentication path computation



Forward security

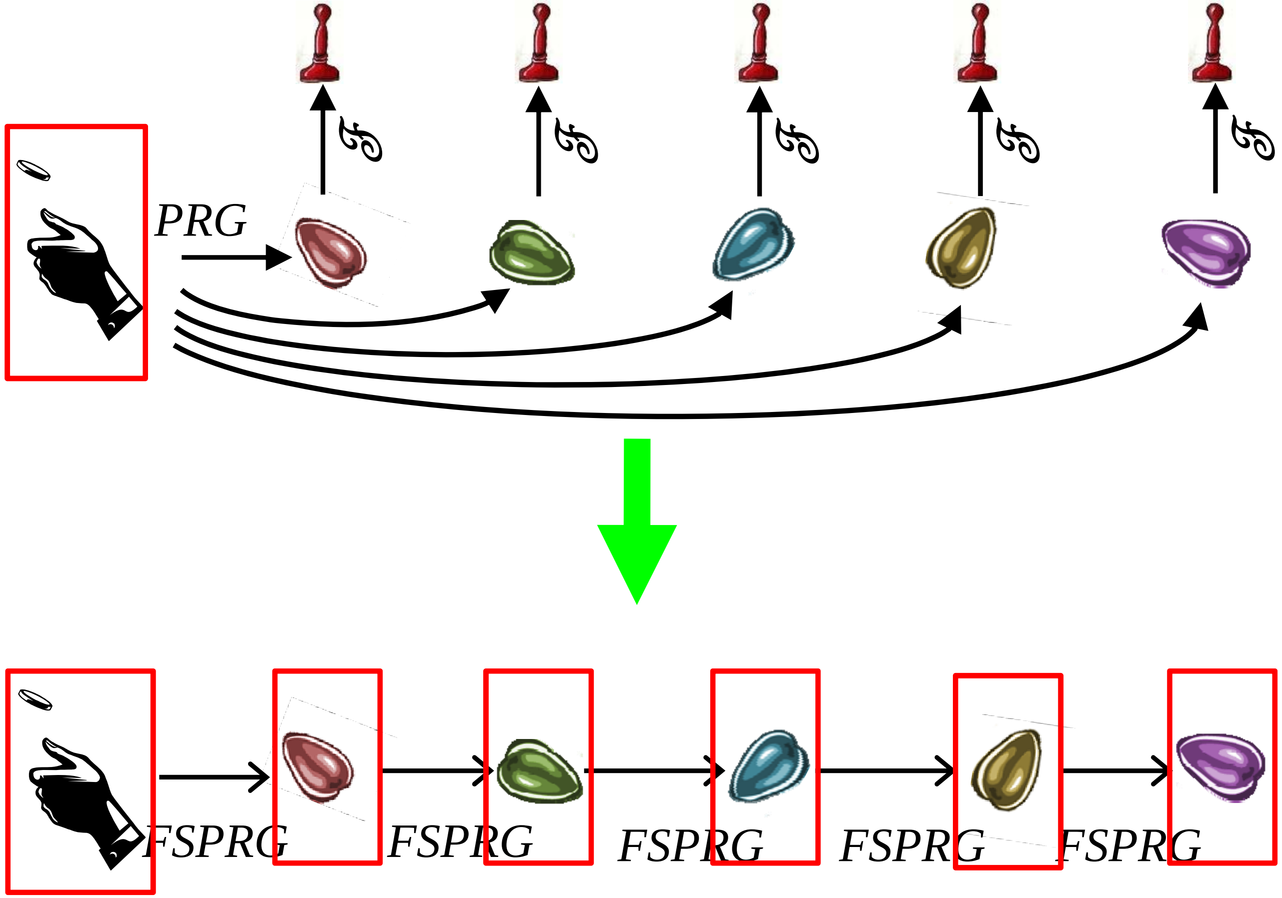

Contract
Contract
Contract
Contract
Contract
Contract
con
tract

Forward Secure Signatures



TECHNISCHE UNIVERSITÄT DARMSTADT

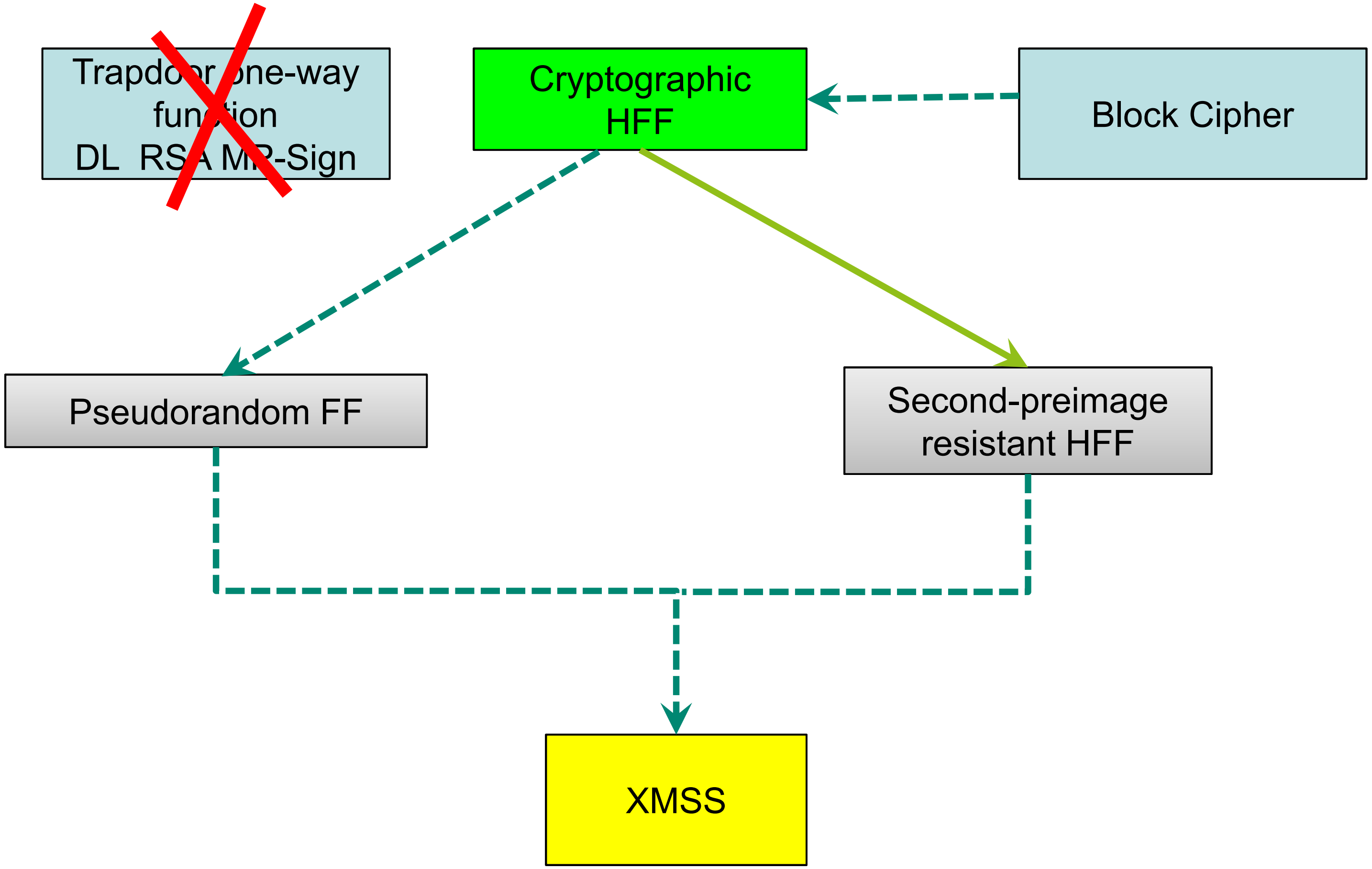
XMSS forward secure



CROSSING

XMSS in practice

XMSS in practice



Hash functions & Blockciphers

AES
Blowfish
3DES
Twofish
Threefish
Serpent
IDEA
RC5
RC6
…

SHA-2
SHA-3
BLAKE
Grøstl
JH
Keccak
Skein
VSH
MCH
MSCQ
SWIFFTX
RFSB
…

XMSS performance (IETF-compliant version)

TECHNISCHE UNIVERSITÄT DARMSTADT

	Parameters				Cyclecounts [k-cycles]	Sizes [kB]		
	m	n	h	d	Signing	Signature	Secret key	Public key
XMSS	276	256	20	1	35 499	2.9	2.2	0.1
XMSS	316	256	60	3	44 882	8.8	14.6	0.1
RSA-15360	/	/	/	/	~ 2 256 000	1.9	1.9	1.9

256 bits classical security

- m: input length (bits)
- n: hash output length (bits)
- h: tree height
- d: # tree layers

XMSS transfer project

Denis Butin, Stefan Gazdag

TECHNISCHE UNIVERSITÄT DARMSTADT

Standardisation underway at IETF/IRTF Crypto Forum Research Group

Internet-Draft *XMSS: Extended Hash-Based Signatures*:
https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/

Includes hierarchical (MT) variant

Shepherding successful, ready for IRTF chair review → RFC soon

http://www.square-up.org/

Practical Hash-based Signatures

TECHNISCHE UNIVERSITÄT DARMSTADT

genua Soviel ist sicher.

PQCrypto 2017

The Eighth International Conference on Post-Quantum Cryptography

Utrecht, the Netherlands, June 26–28, 2017