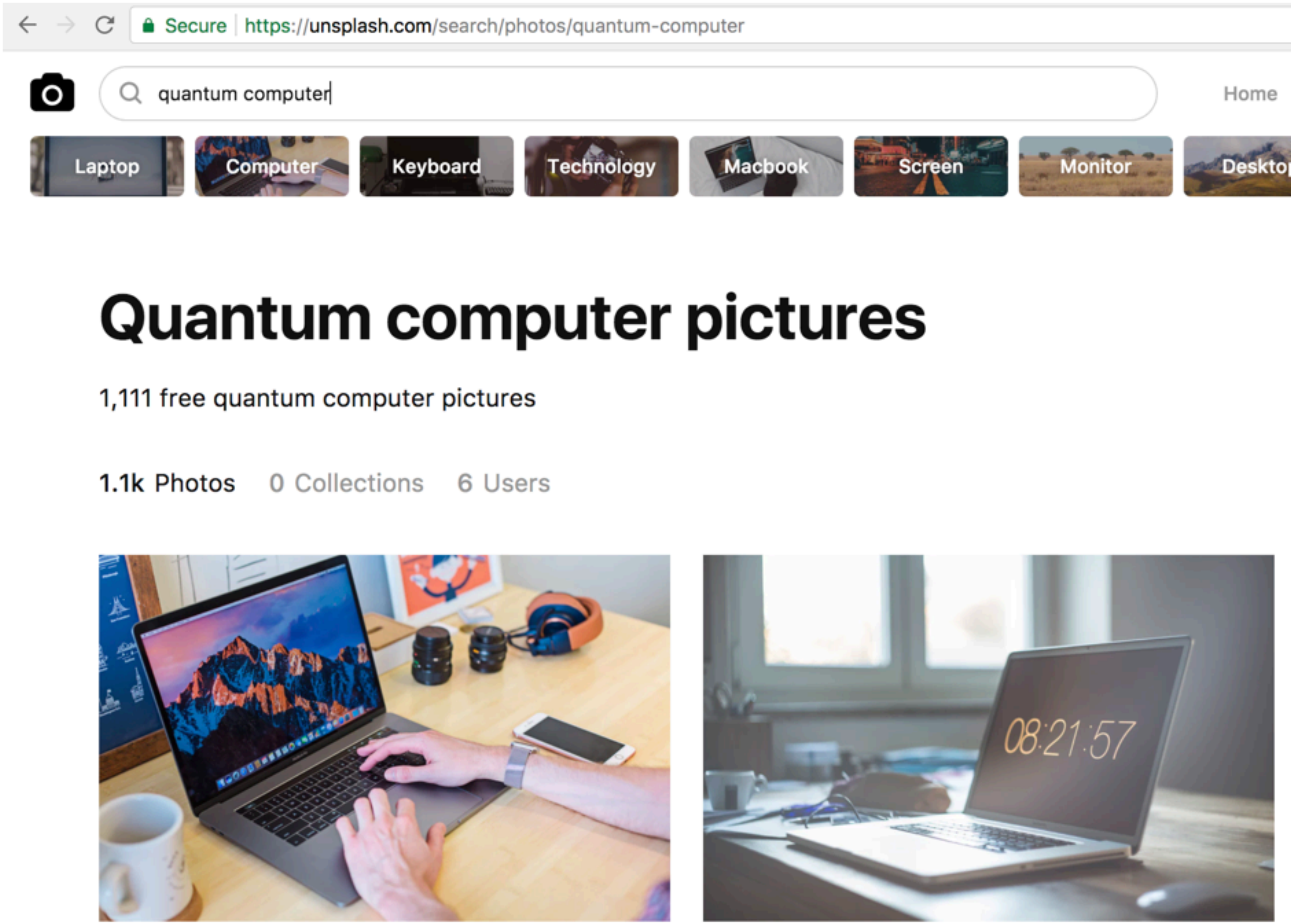
POST-QUANTUM CRYPTO

JP AUMASSON

KUDELSKI SECURITY


Secure https://unsplash.com/search/photos/quantum-computer
quantum computer
Home
Laptop
Computer
Keyboard
Technology
Macbook
Screen
Monitor
Deskto
Quantum computer pictures
1,111 free quantum computer pictures
1.1k Photos
0 Collections
6 Users
08:21:57

⚠ **Sorry, this product is no longer available!**

See larger image

100 pcs lot Lava pendants Energy quantum scalar pendant energy card and Resist radiation JHE0151

Price: **US $263.72 - 341.67** / Lot (US $2.64 - 3.42 / Piece) Reference Currency

100 Pieces / Lot

Wholesale Price (Lot):	1 +	3 +	15 +	16 +	32 +
	US $341.67	US $334.70	US $317.96	US $314.75	US $313.17

Quantity: 1 Lot

Shipping Cost: **US $0.95** to Switzerland Via China Post Air Mail

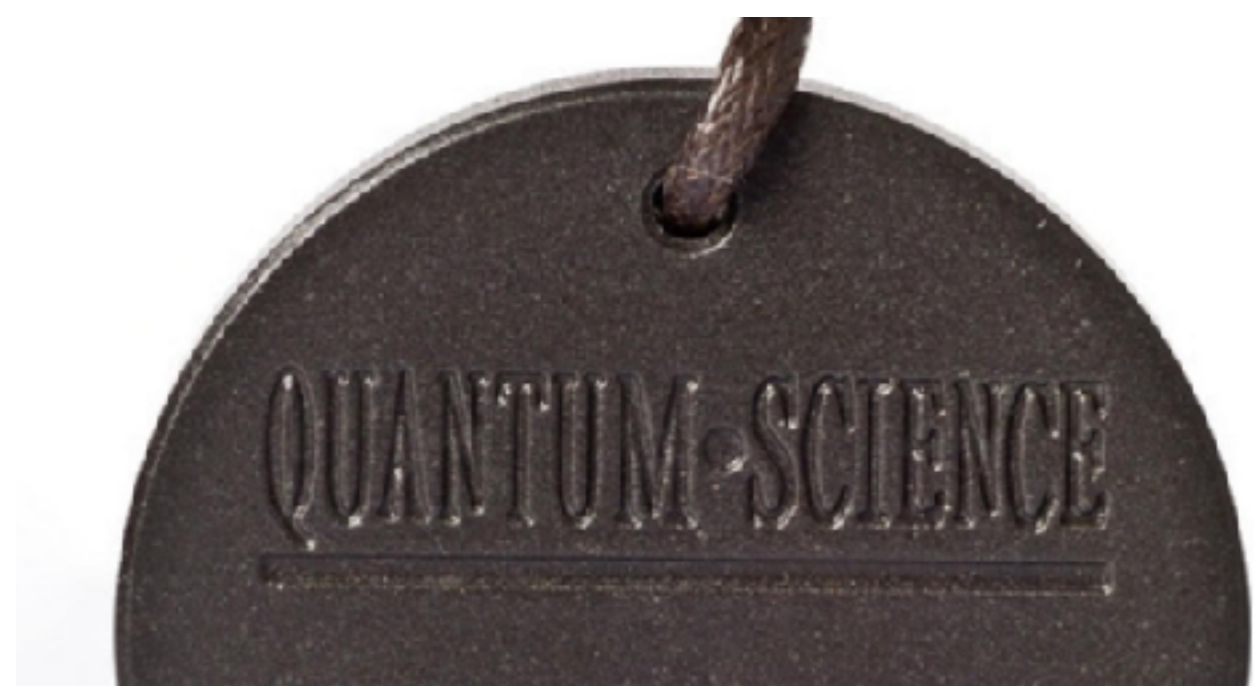
Estimated delivery time: Dec 26 and Jan 5, ships out within 7 business days ?

Total Cost: **US $342.62**

Item sold out Add to Favorite Items (0)

Health Benefits:

1. Reduces inflammation.
2. Promotes unclamping of cells.
3. Enhances immune and endocrine systems.
4. Helps to protect DNA from damage.
5. Improves stamina, endurance and strength.
6. Alleviates soreness, aches and pains, and improves flexibility.
7. Helps to retard the ageing process.
8. Helps to fight cancer cells.
9. Has the ability to destroy viruses and bacteria.
10. Enhances cellular nutrition and detoxification.
11. Enhances cellular permeability.
12. Increases energy.
13. Strengthens the body's biofield preventing electro-magnetic waves from affecting one's health.
14. Increases focus and concentration.
15. Improves blood Circulation.
16. Energizes block cells and reduces "stickiness".



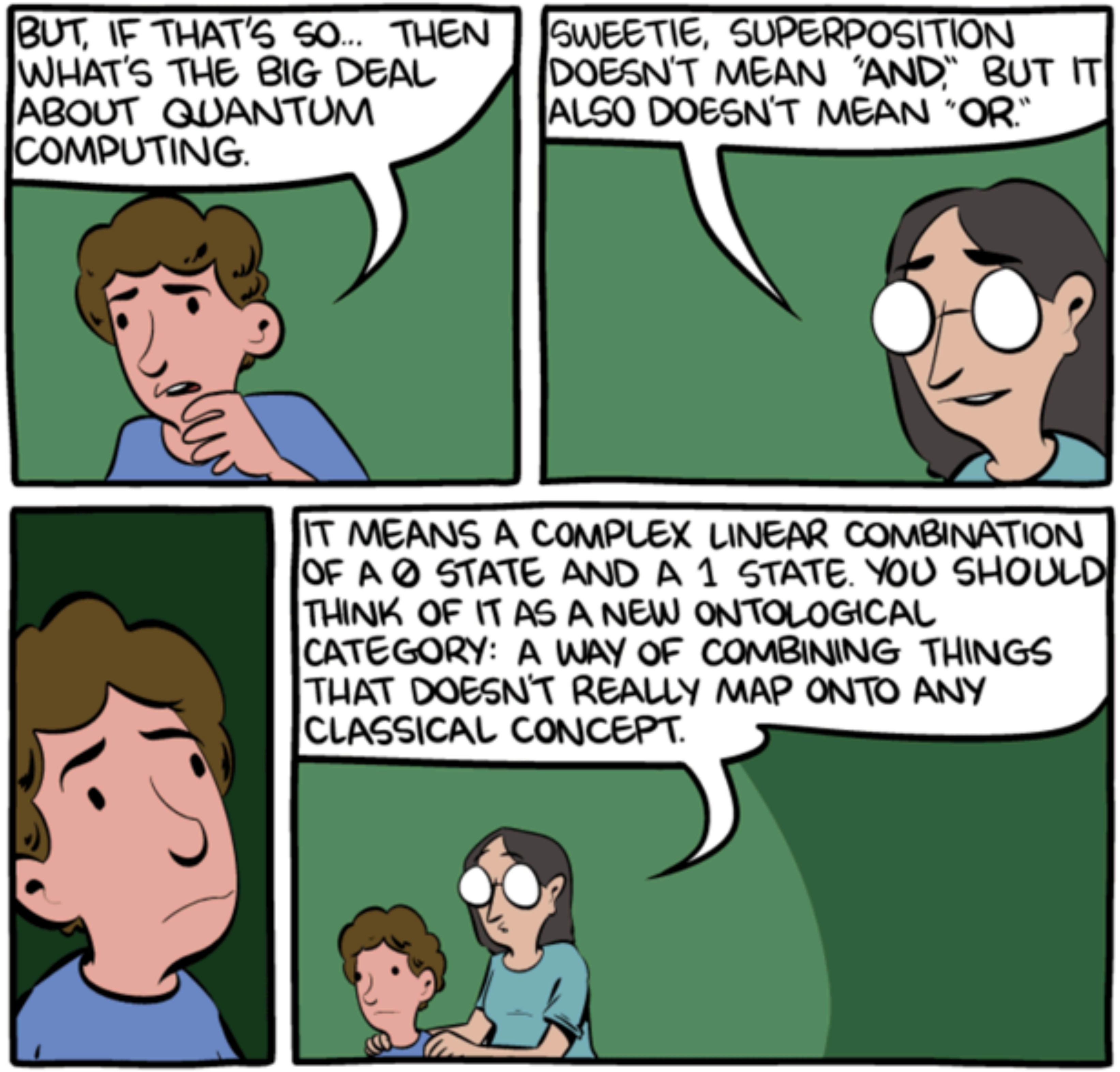
QUBIT

$$\alpha|0\rangle + \beta|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\underbrace{\alpha, \beta} \in \mathbb{C}$$

= "AMPLITUDES"

≈ QUANTUM PROBABILITIES



Credit: Aaronson & Weinersmith, full comic at http://www.smbc-comics.com/comic/the-talk-3

CLASSIC

0  1

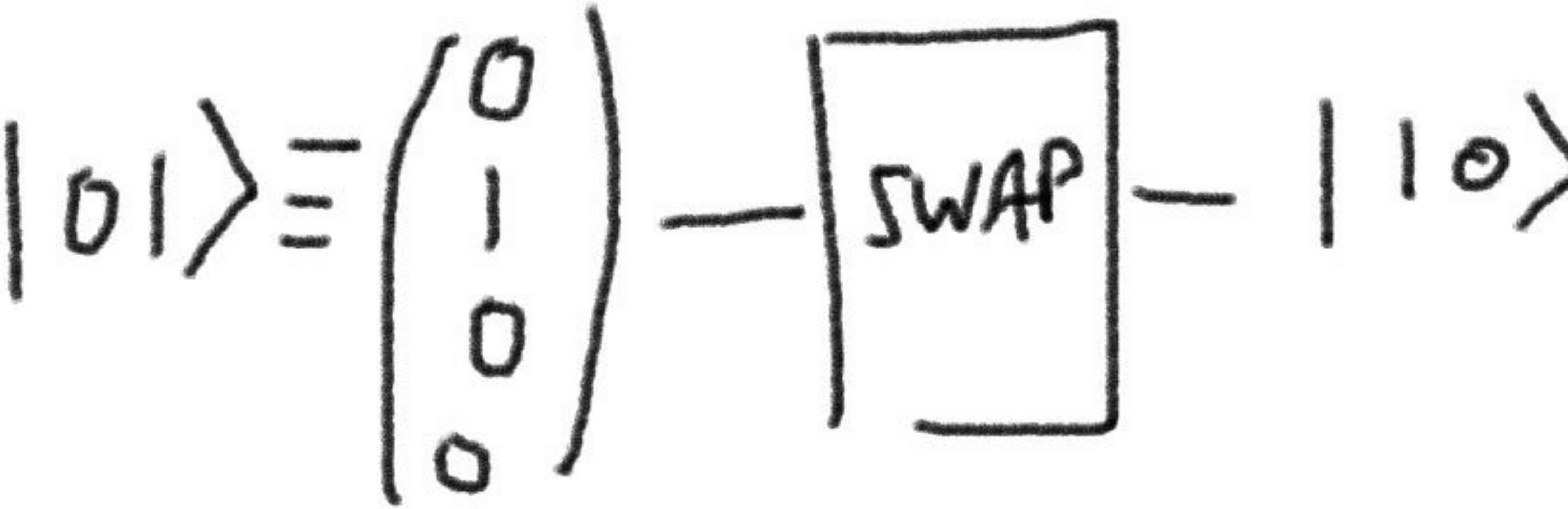
QUANTUM

$$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix} \;—\!\!\boxed{H}\!\!—\; \begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}$$

$\hookrightarrow$ 2 Numbers

CLASSIC

2 BITS



QUANTUM 2 QUBITS

→ 4 numbers to simulate

2 - QUBIT GATE

$\simeq 4 \times 4$ matrix

$$\boxed{\text{SWAP}} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

N QUBITS

→ State ~ 2^N numbers

Gate ~ 2^{2N} numbers

⇒ CAN'T SIMULATE CLASSICALLY FOR $N \gtrsim 50$

QUANTUM <u>CIRCUITS</u> CAN SOLVE CERTAIN PROBLEMS FASTER

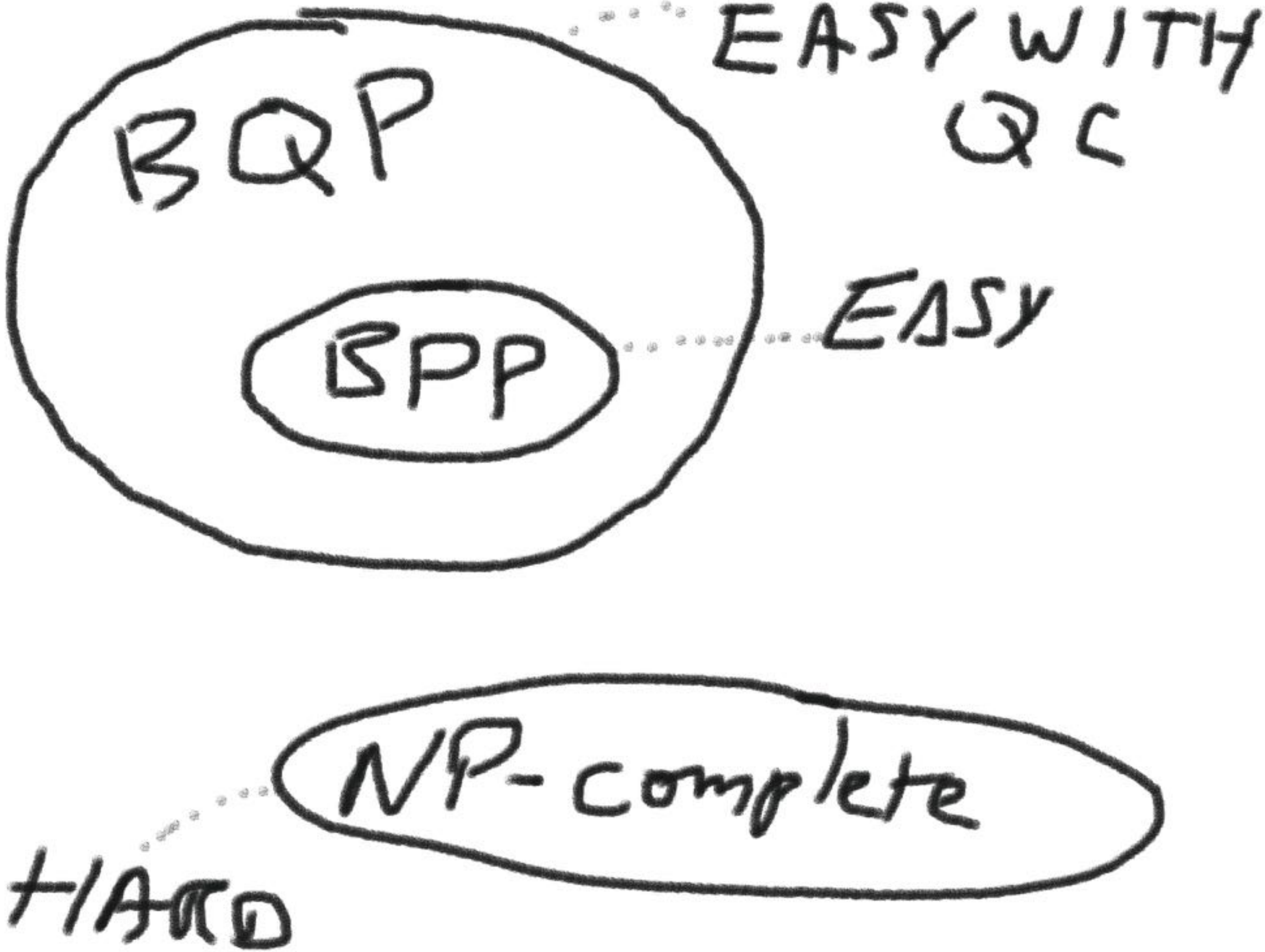
<u>Ex</u> $O(2^{n/2}) \to O(n)$

EXPONENTIAL SPEEDUP

~~IM~~POSSIBLE

QC IS **NOT**

- SUPERFAST COMPUTER
- FREE PARALLELISM
- SOLVING NP-HARD PBS


BQP
EASY WITH QC
BPP
EASY
NP-complete
HARD

QC is **NOT**

SHOR

$N = pq \longrightarrow (p, q)$

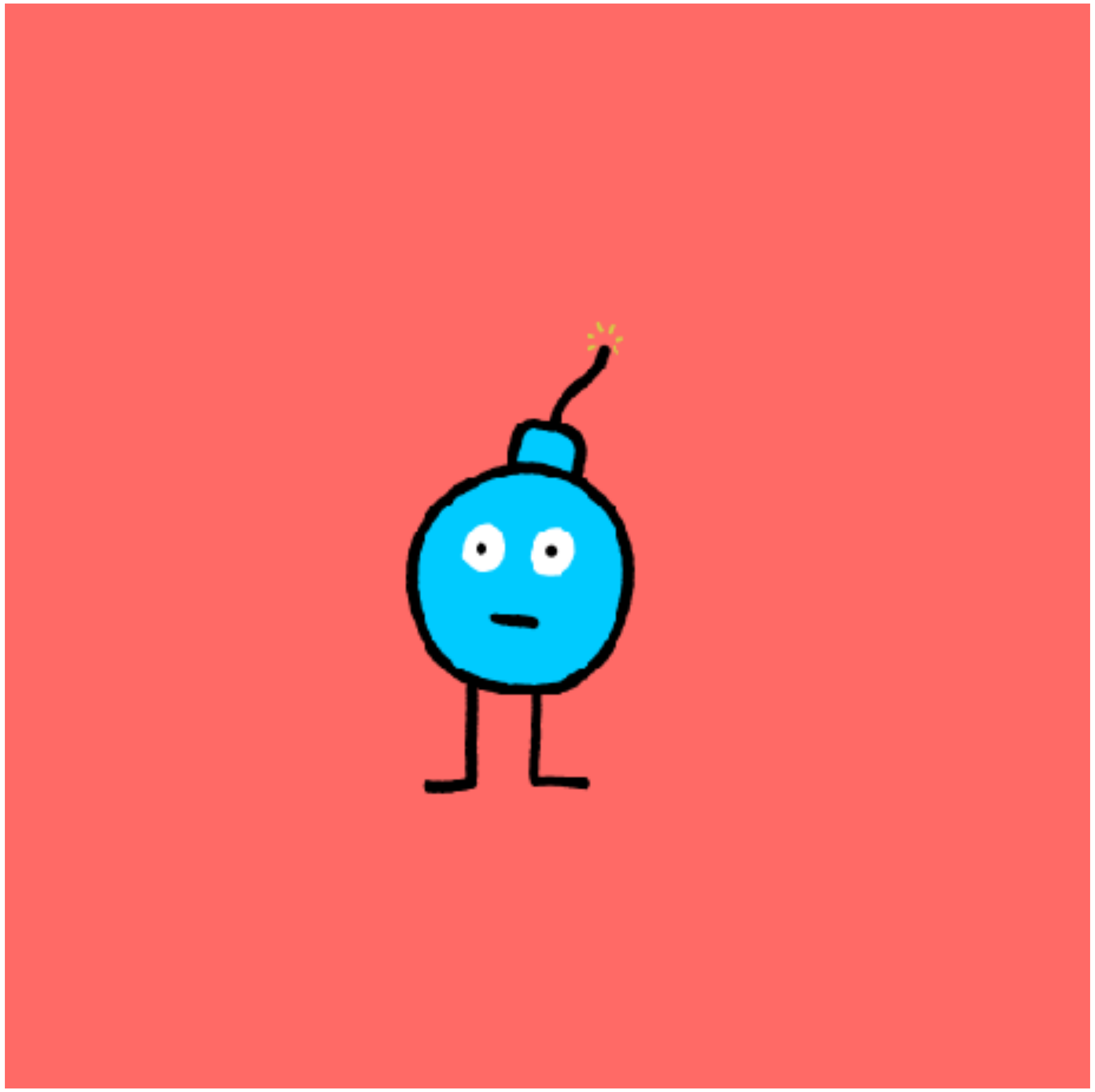
$x^d \bmod p \longrightarrow d$

in $O(n^3)$

~~RSA~~

~~DH~~

~~ECC~~

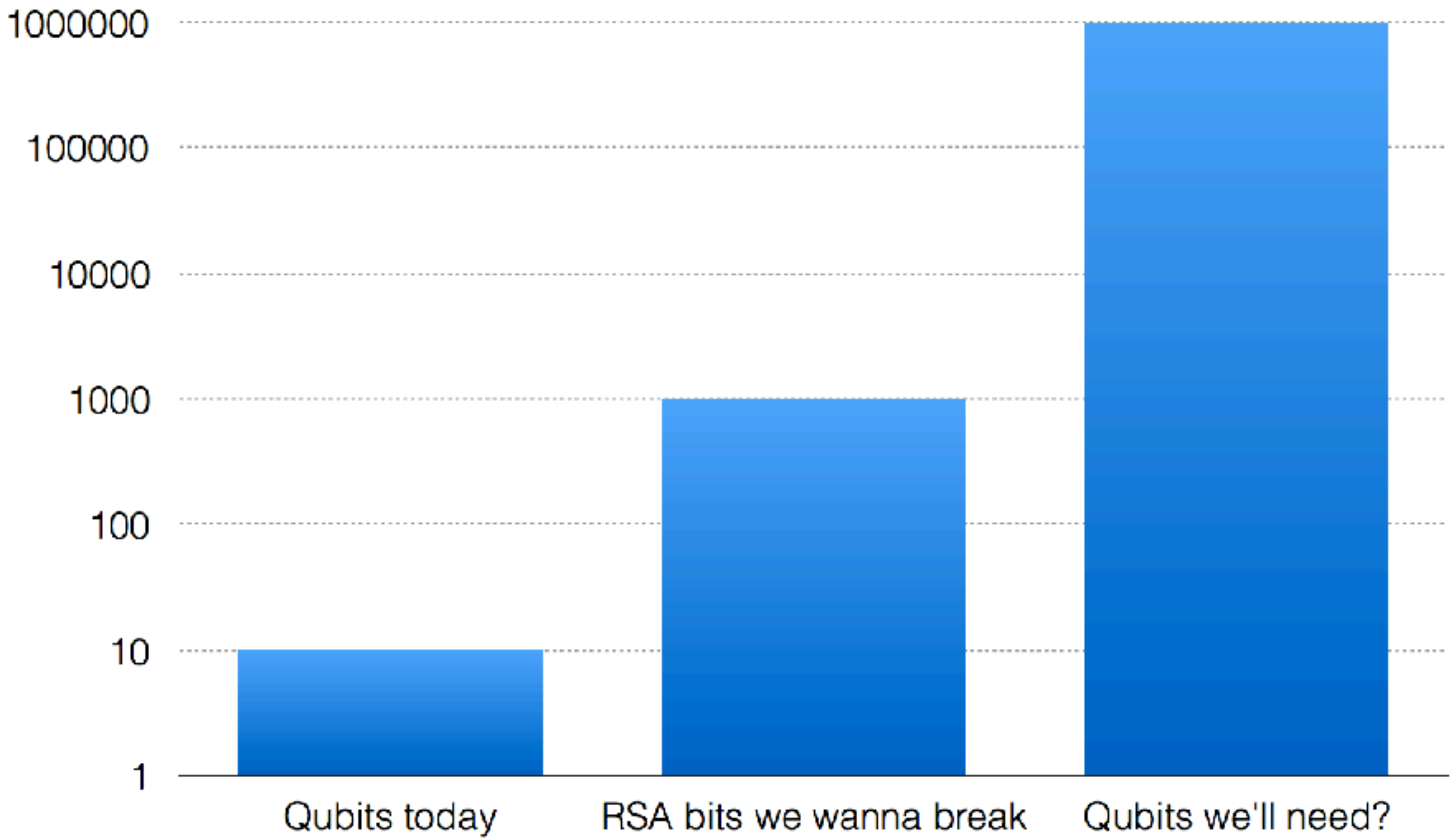


Designing a Million-Qubit Quantum Computer Using Resource Performance Simulator

Muhammad Ahsan, Rodney Van Meter, Jungsang Kim

(Submitted on 2 Dec 2015)

The optimal design of a fault-tolerant quantum computer involves finding an appropriate balance between the burden of large-scale integration of noisy components and the load of improving the reliability of hardware technology. This balance can be evaluated by quantitatively modeling the execution of quantum logic operations on a realistic quantum hardware containing limited computational resources. In this work, we report a complete performance simulation software tool capable of (1) searching the hardware design space by varying resource architecture and technology parameters, (2) synthesizing and scheduling fault-tolerant quantum algorithm within the hardware constraints, (3) quantifying the performance metrics such as the execution time and the failure probability of the algorithm, and (4) analyzing the breakdown of these metrics to highlight the performance bottlenecks and visualizing resource utilization to evaluate the adequacy of the chosen design. Using this tool we investigate a vast design space for implementing key building blocks of Shor's algorithm to factor a 1,024-bit number with a baseline budget of 1.5 million qubits. We show that a trapped-ion quantum computer designed with twice as many qubits and one-tenth of the baseline infidelity of the communication channel can factor a 2,048-bit integer in less than five months.


1000000
100000
10000
1000
100
10
1
Qubits today
RSA bits we wanna break
Qubits we'll need?

(log scale)

GROVER

AKA "QUANTUM SEARCH"

$O(n) \rightarrow O(\sqrt{n})$

$\Rightarrow$ n-bit key search in $\approx 2^{n/2}$ . . .

AES vs. Grover

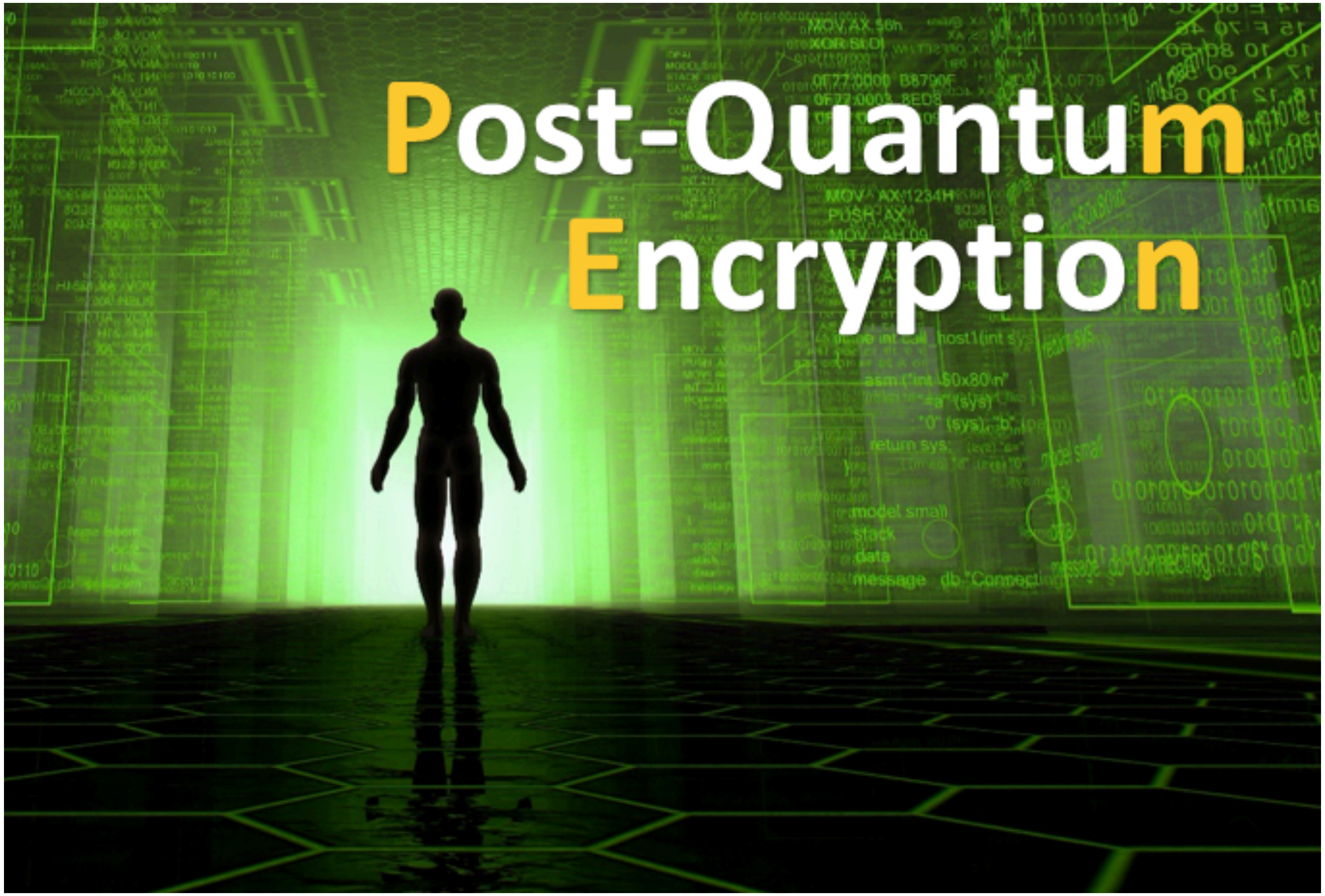
	#gates		depth		#qubits
k	T	Clifford	T	overall	
128	$1.19 \cdot 2^{86}$	$1.55 \cdot 2^{86}$	$1.06 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	$2,953$
192	$1.81 \cdot 2^{118}$	$1.17 \cdot 2^{119}$	$1.21 \cdot 2^{112}$	$1.33 \cdot 2^{113}$	$4,449$
256	$1.41 \cdot 2^{151}$	$1.83 \cdot 2^{151}$	$1.44 \cdot 2^{144}$	$1.57 \cdot 2^{145}$	6,681

Table 5. Quantum resource estimates for Grover's algorithm to attack AES-k, where $k \in \{128, 192, 256\}$.

https://arxiv.org/pdf/1512.04965v1.pdf

≈ Solar system diameter!

JUST DOUBLE THE KEY SIZE
→ AES-256



Credit: Dyadic Security

POST-QUANTUM

≃ NOT IN BQP

⇒ RSA IS **NOT** P-Q

AES **IS**

POST-QUANTUM CRYPTO IS AN INSURANCE

(Against an unlikely event)

#Risk Management

WHY CARE?

WHY CARE?

National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

**Commercial National Security Algorithm Suite
and Quantum Computing FAQ**

WHY CARE?

Q: Given the range of algorithm options and sizes to choose from, which is best?
A: CNSS Advisory Memorandum 02-15 alerts NSS developers and operators of the need to transition to quantum resistant algorithms in the future and permits greater flexibility in algorithm choice today than was allowed under the existing CNSSP-15. This flexibility avoids making systems that do not already comply with CNSSP-15 first do an upgrade to comply with

NIST's PQ CONTEST

POST-QUANTUM CRYPTO PROJECT

NEWS -- August 2, 2016: The National Institute of Standards and Technology (NIST) is requesting comments on a new process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Please see the Post-Quantum Cryptography Standardization menu at left.

Fall 2016	Formal Call for Proposals
Nov 2017	Deadline for submissions
Early 2018	Workshop - Submitter's Presentations
3-5 years	Analysis Phase - NIST will report findings *1-2 workshops during this phase*
2 years later	Draft Standards ready

NIST's PQ CONTEST

Announced submissions to NIST's **post-quantum crypto standardization project**:

code-based

- **CAKE**: KEM by Barreto, Gueron, Güneysu, Misoczki, Persichetti, Sendrier, Tillich
- **RLCE**: KEM by Wang

hash-based

- **Gravity-SPHINCS**: signature by Aumasson, Endignoux
- **PRUNE-HORST**: signature by Aumasson, Endignoux

lattice-based

- **HILA5**: encryption/KEM by Saarinen
- **Kyber**: KEM by Bos, Ducas, Kiltz, Lepoint, Lyubashevsky, Schanck, Schwabe, Stehlé
- **Dilithium**: signature by Ducas, Lepoint, Lyubashevsky, Schwabe, Seiler, Stehlé
- **ThreeBears**: KEM by Hamburg

Contact

https://post-quantum.ch/ (unofficial)

5 MAIN FAMILIES OF PQ CRYPTO

- CODE-BASED
- HASH-BASED
- LATTICE-BASED
- MULTIVARIATE
- ISOGENY-BASED

HASH-BASED CRYPTO

ONE-TIME SIGNATURES

$$K_0 \longrightarrow H(K_0)$$

$$K_1 \longrightarrow H(K_1)$$

Secret Key	Public Key
K_0, K_1	$H(K_0)$, $H(K_1)$

N keys for N bits

Keys used only once

WINTERNITZ:

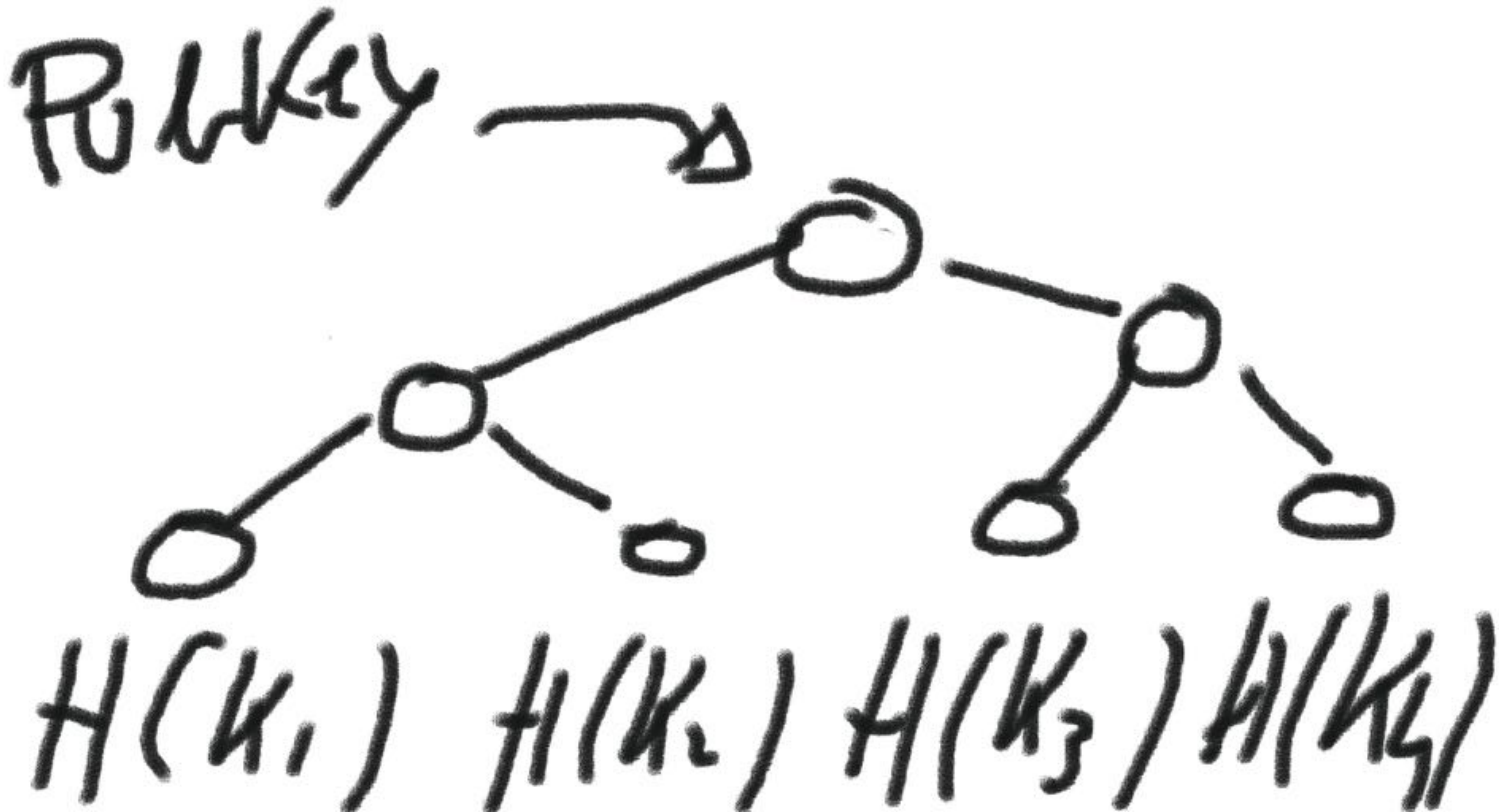
Sign more than 1 bit

$$PubKey = H(H(H(\ldots(K))))$$
$$= H^{N}(K)$$

$$Sig(x) = H^{x}(K)$$

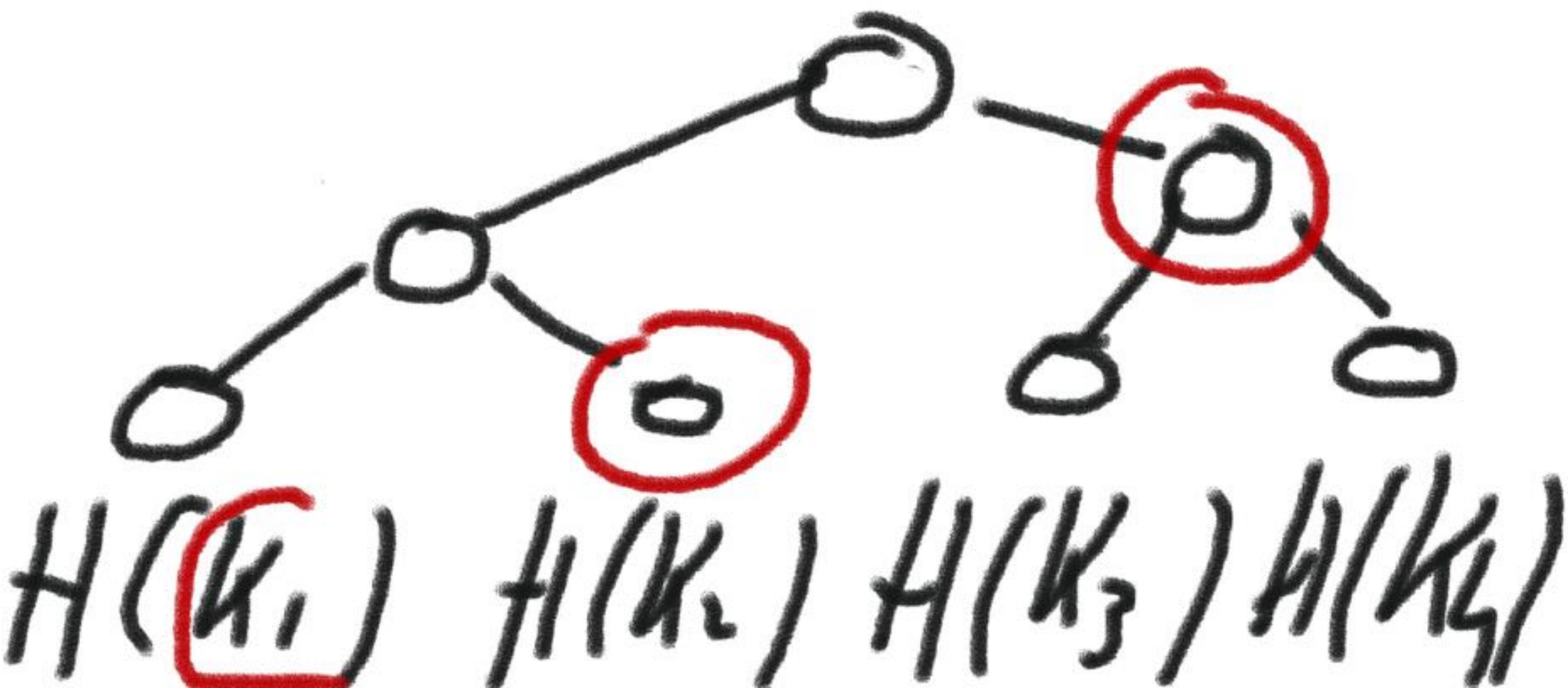
MANY-TIME SIGS

MERKLE TREE FTW!



AUTHENTICATION PATH

OF K_1



Few-time sigs

"HORS", Reyzin[2] (2002)

	0	1		m
sk_0	k_0	k_1	---	k_m
pk_0	$H(k_0)$	$H(k_1)$	---	$H(k_m)$

$H: M \rightarrow$ indexes in $\{0, 1 \ldots m\}$

IF $H(M) = \{1, m\}$

THEN $SIG(M) = (K_1, K_m)$

	0	1		m
SK_0	K_0	K_1	--- ---	K_m
PK_0	$H(K_0)$	$H(K_1)$	--- ---	$H(K_m)$

Too many messages

$\Rightarrow$ All keys revealed, Becomes INSECURE

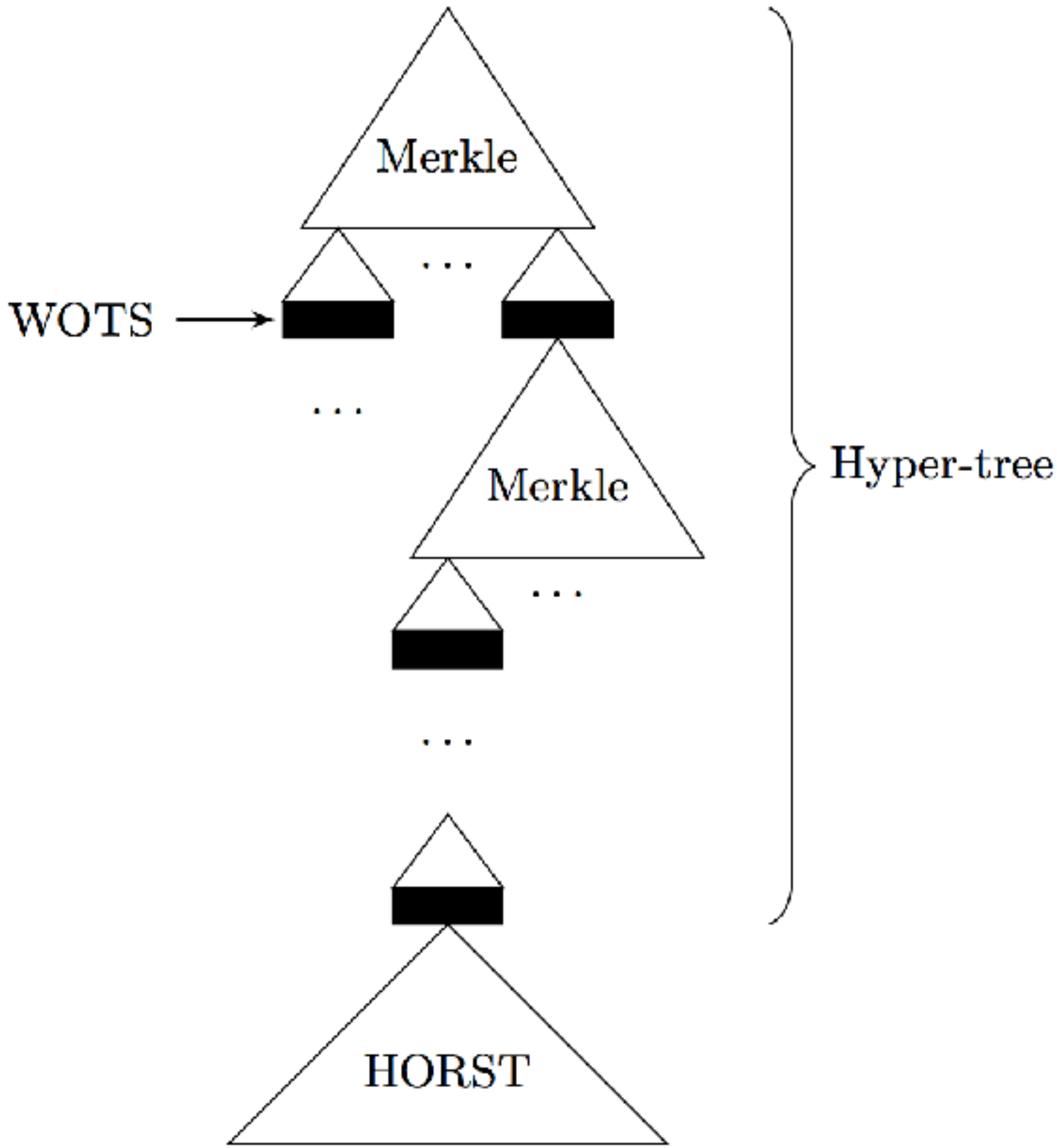
	0	1	---	n
SK_0	K_0	K_1	---	K_n
PK_0	$H(K_0)$	$H(K_1)$	---	$H(K_n)$

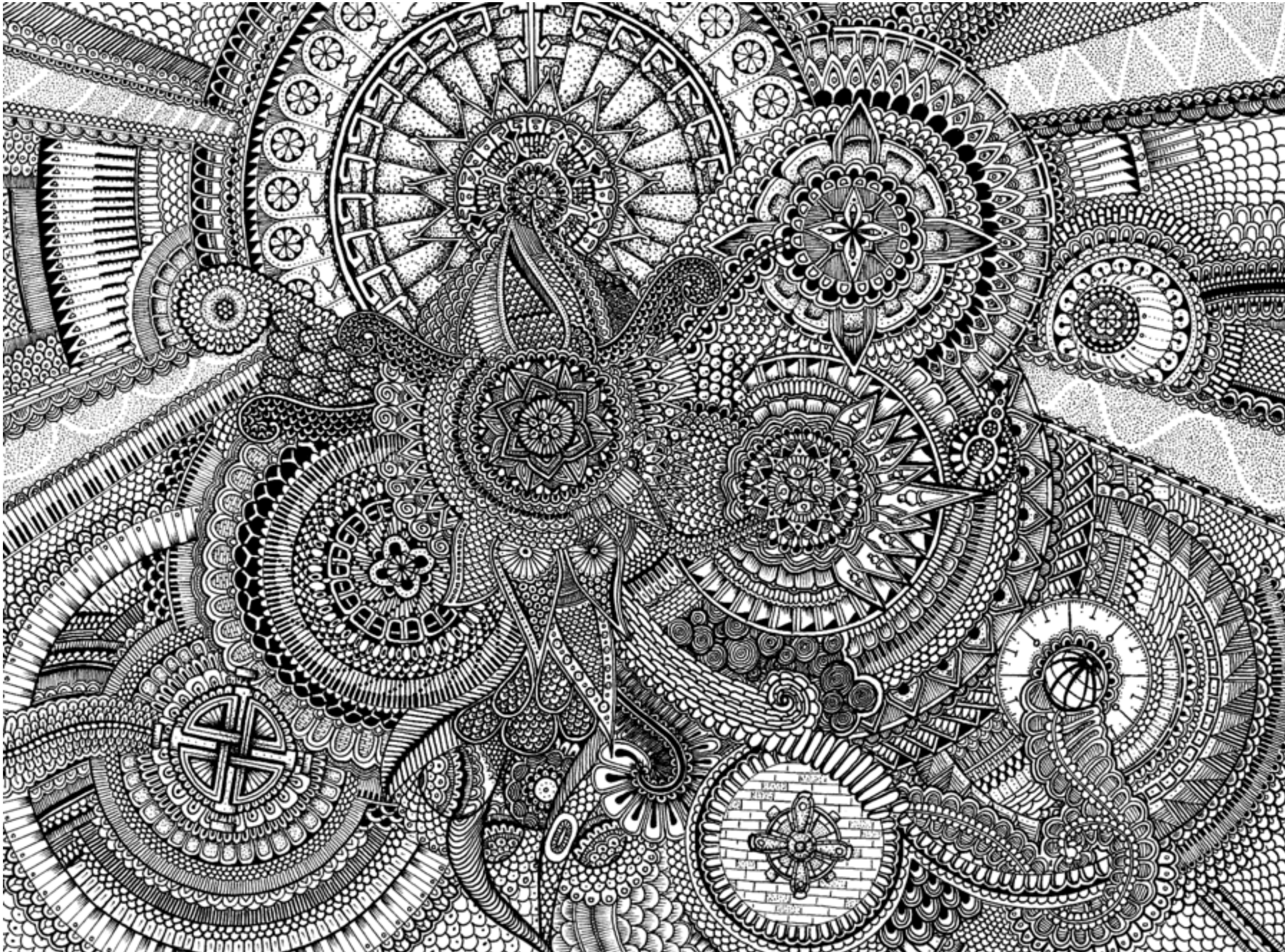
MIX EVERYTHING:

- WINTERNITZ OTS
- HORS FTS
- MERKLE TREES
- MORE TREES!

SPHINCS: practical stateless hash-based signatures

Daniel J. Bernstein[1,3], Daira Hopwood[2], Andreas Hülsing[3], Tanja Lange[3], Ruben Niederhagen[3], Louiza Papachristodoulou[4], Michael Schneider, Peter Schwabe[4], and Zooko Wilcox-O'Hearn[2]


Merkle
WOTS
Merkle
HORST
Hyper-tree



Even more complex?

Improving Stateless Hash-Based Signatures

Jean-Philippe Aumasson[1] and Guillaume Endignoux[2]

[1] Kudelski Security, Switzerland
[2] firstname.surname@m4x.org

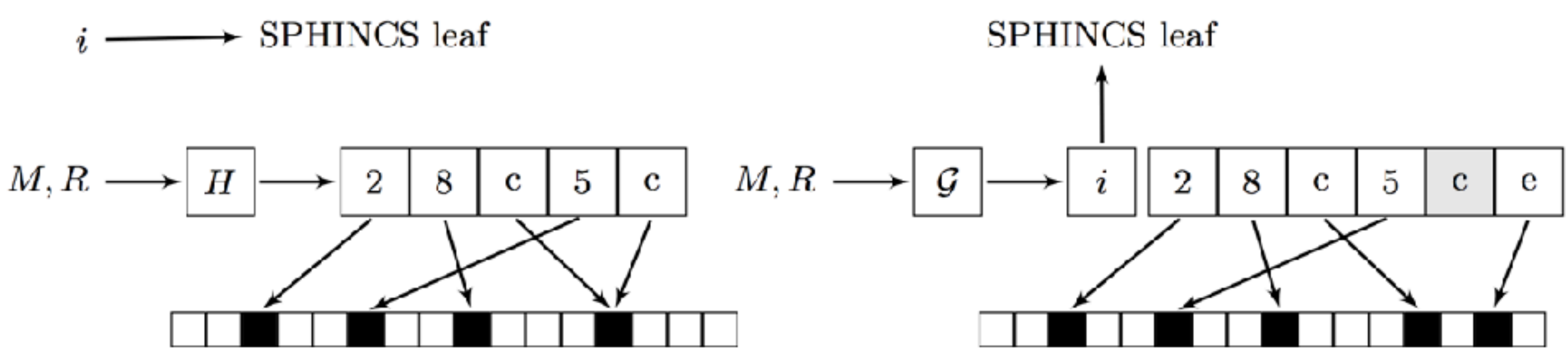
Abstract. We present several optimizations to SPHINCS, a stateless hash-based signature scheme proposed by Bernstein et al. in 2015: PORS, a more secure variant of the HORS few-time signature scheme used in SPHINCS; secret key caching, to speed-up signing and reduce signature size; batch signing, to amortize signature time and reduce signature size when signing multiple messages at once; mask-less constructions to reduce the key size and simplify the scheme; and Octopus, a technique to eliminate redundancies from authentication paths in Merkle trees. Based on a refined analysis of the subset resilience problem, we

GRAVITY - SPHINCS

= SPHINCS + New TRICKS

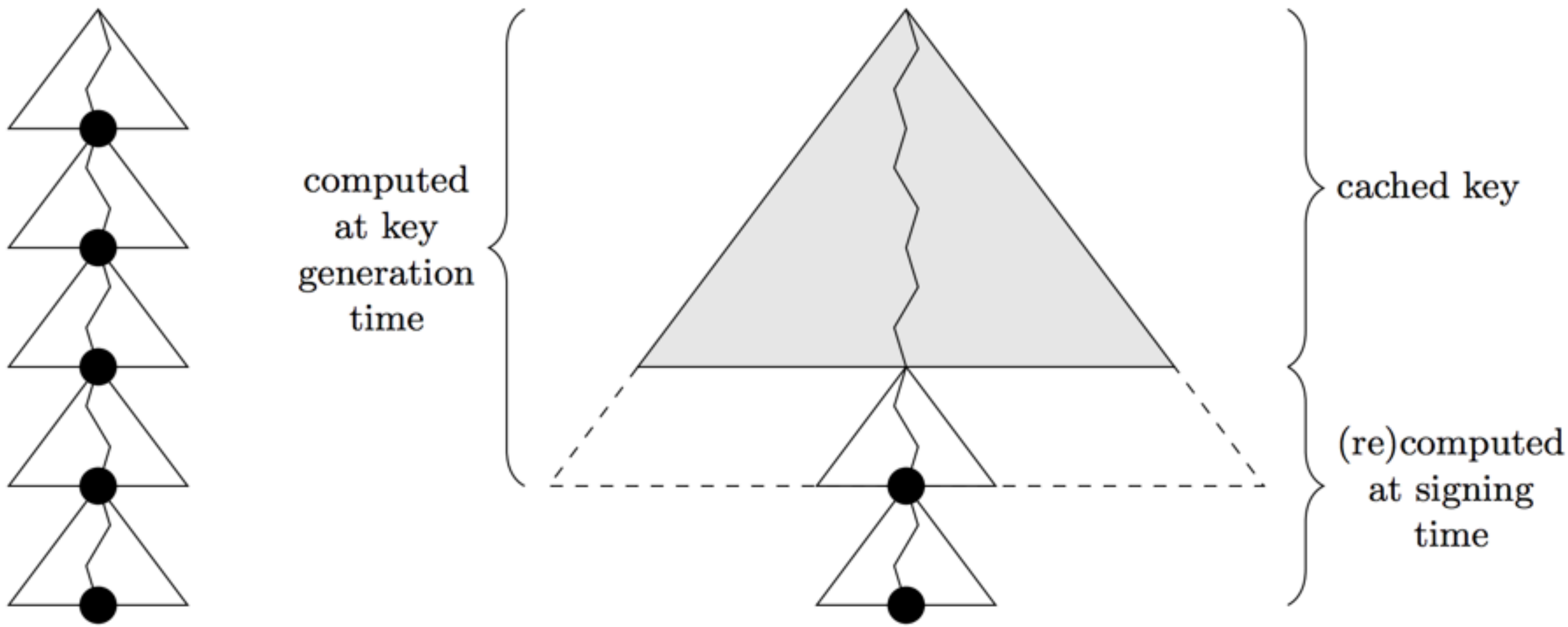
- SHORTER SIGS
- LESS SLOW

COLLISION-FREE HASHING



(a) HORS. (b) PORS.

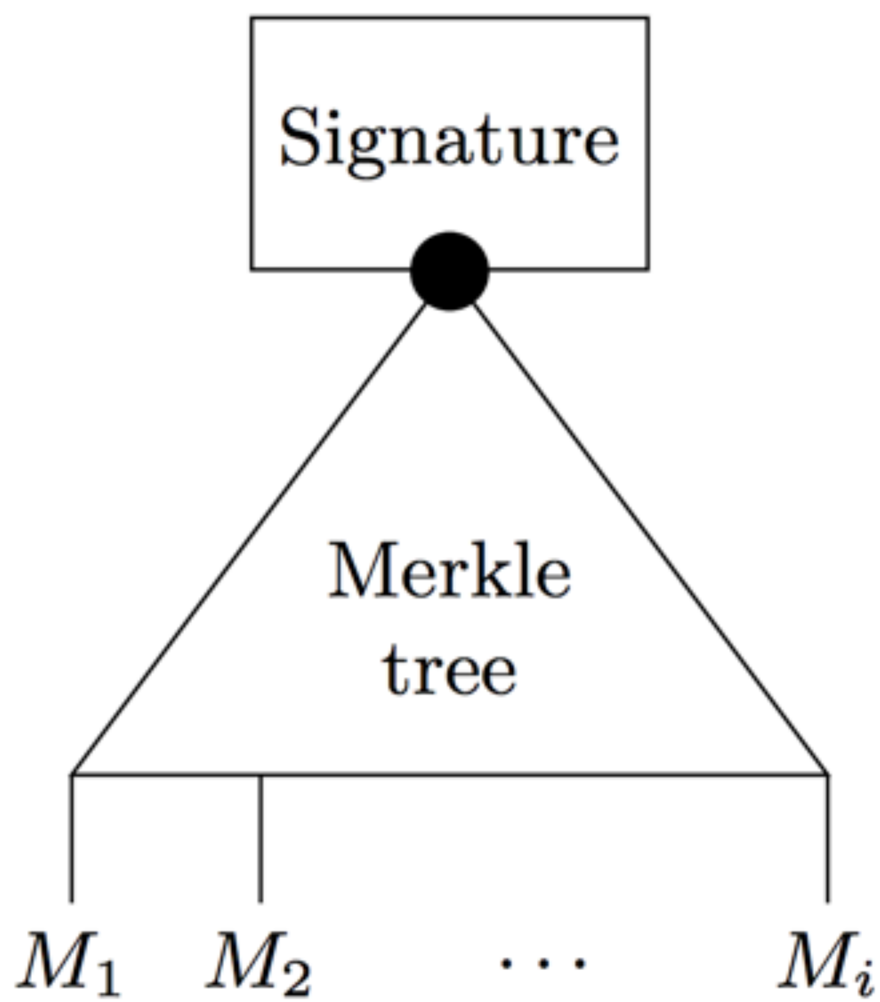
KEY CACHING



(a) SPHINCS.

(b) Secret key caching.

BATCHING



name	$\log_2 t$	k	h	d	c	sigsz	capacity
NIST-fast	16	28	5	10	14	35 168	2^{64}
NIST	16	28	8	6	16	26 592	2^{64}
NIST-slow	16	28	14	4	8	22 304	2^{64}
fast	16	32	5	7	15	28 928	2^{50}
batched	16	32	8	3	16	20 032	2^{40}
small	16	24	5	1	10	12 640	2^{10}

Table 1: Proposed Gravity-SPHINCS parameters for 128-bit quantum security. The capacity is the number of messages (or batches thereof) that can be signed per key pair. The maximal signature size sigsz is in bytes and does not include batching. Public keys are always 32 bytes, secret keys are always 64 bytes.

Hyatt Regency, Pier 66,
Fort Lauderdale, Florida

In Cooperation with IACR

PQCrypto 2018
The Ninth International Conference on Post-Quantum Cryptography
Fort Lauderdale, Florida, April 9-11, 2018

Springer

PQ Crypto Conference

Introduction

The aim of PQCrypto is to serve as a forum for researchers to present results and exchange ideas on the topic of cryptography in an era with large-scale quantum computers.

After eight successful PQCrypto conferences (2006 in Leuven, 2008 in Cincinnati, 2010 in Darmstadt, 2011 in Taipei, 2013 in Limoges, 2014 in Waterloo, 2016 in Fukuoka, and 2017 in Utrecht, the Netherlands), PQCrypto 2018 will take place **April 9-11, 2018** in Fort Lauderdale, Florida.

THANK YOU!

OBRIGADO!

@veorq

https://aumasson.jp

Serious Cryptography

A Practical Introduction to Modern Encryption

Jean-Philippe Aumasson

Foreword by Matthew D. Green

no starch press

Serious Cryptography
A Practical Introduction to Modern Encryption
Aumasson
no starch press