2023 Rump Session

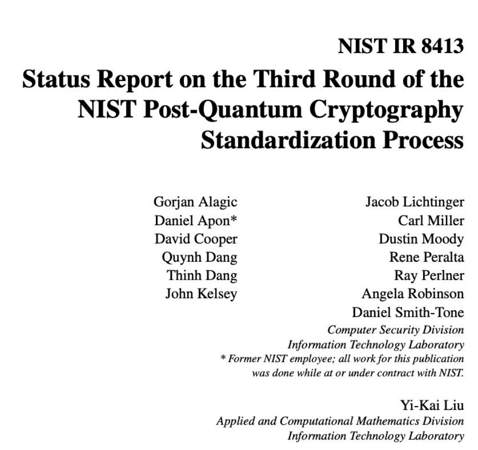
Now presenting: Dustin Moody, NIST Presentation of Plaques

On deck: Po-Chun Kuo, Preon: Digital Signature from zk-SNARK

In the hole: Scott Fluhrer, Signature Limbo

NIST's PQC Selections

- CRYSTALS-KYBER
- CRYSTALS-DILITHIUM
- FALCON
- SPHINCS+



NIST IR 8413

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Daniel Apon*
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone
Computer Security Division
Information Technology Laboratory
** Former NIST employee; all work for this publication was done while at or under contract with NIST.*

Yi-Kai Liu
Applied and Computational Mathematics Division
Information Technology Laboratory

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Extends its appreciation to

The CRYSTALS-Kyber Team

For outstanding contributions to the

NIST PQC Standardization process

through the design of

ML-KEM

August 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Extends its appreciation to

The CRYSTALS-Dilithium Team

For outstanding contributions to the

NIST PQC Standardization process

through the design of

ML-DSA

August 2023

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Extends its appreciation to

The Falcon Team

For outstanding contributions to the

NIST PQC Standardization process

through the design of

FN-DSA

August 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Extends its appreciation to

The SPHINCS+ Team

For outstanding contributions to the

NIST PQC Standardization process

through the design of

SLH-DSA

August 2023

Now presenting: Po-Chun Kuo, Preon: Digital Signature from zk-SNARK

On deck: Scott Fluhrer, Signature Limbo

In the hole: Varun Maram, Does Post-Quantum Come After Quantum Cryptography preon

Digital Signature from zk-SNARK

Po-Chun Kuo @BTQ

preon: under the hood

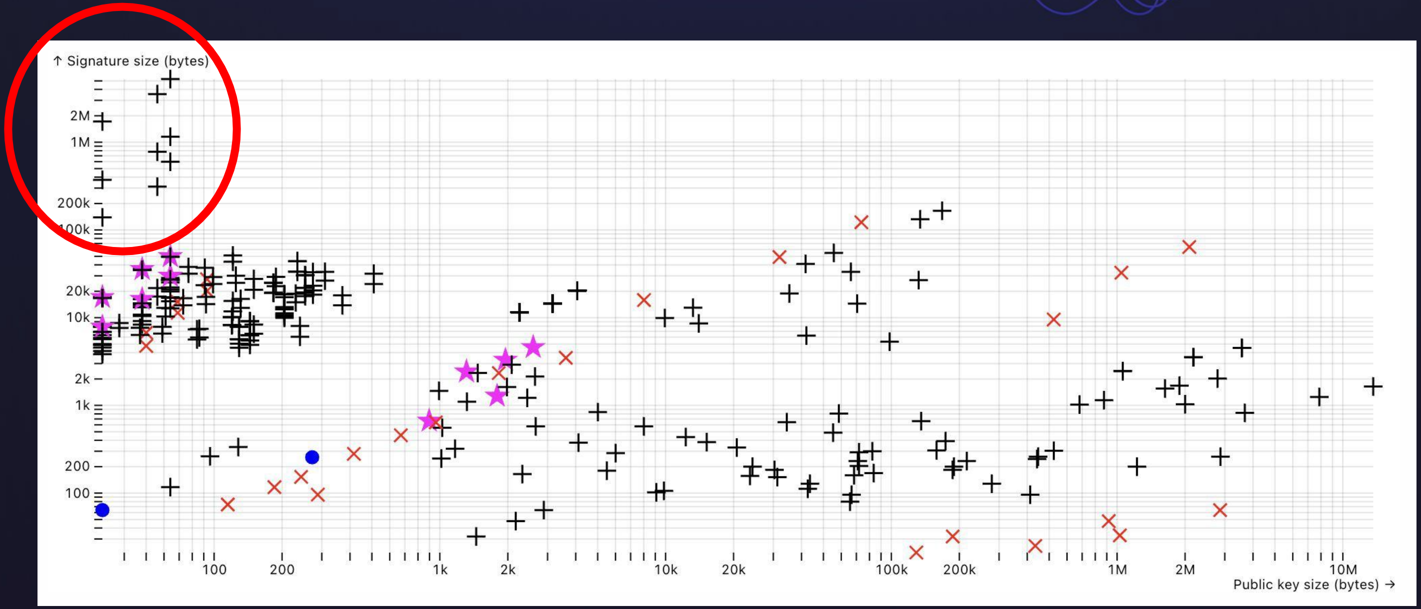
- preon ≈ Aurora + AES
  - Aurora: post-quantum zk-SNARK
  - AES as one-way function

- Optimization: replace prime field with binary field
  - 14240 → 3656 constraints
  - 4x speedup, with additional 2–3x via Additive FFT
  - About 20% smaller signature

preon:beyond digital signature

- Selective Reveal: let $m = m_0 \| m_1$
  - Public m_0
  - Private m_1
    - As a witness in Aurora
    - Prove $f(m_1)$ in Aurora
- R1CS format for f()
  - Friendly to developer
  - Relatively easy to verify the circuit
  - Various compilers support languages such as C++/Rust/Haskell

preon



↑ Signature size (bytes)
2M
1M
200k
100k
20k
10k
2k
1k
200
100
100
200
1k
2k
10k
20k
100k
200k
1M
2M
10M
Public key size (bytes) →

BTQ

Thank You

preon@btq.li

pk@btq.li

Now presenting: Scott Fluhrer, Signature Limbo

On deck: Varun Maram, Does Post-Quantum Cryptography Come After Quantum Cryptography?

In the hole: Hyungrok Jo, IWSEC2023 CFPa

Let's Play Signature Limbo

How low can you go (RAM needed during signing)

Falcon	14k RAM used
Dilithium	5k RAM used
Sphincs+	1k RAM used

https://github.com/sphincs/low-ram-sphincsplus

Now presenting: Varun Maram, Does Post-Quantum Cryptography Come After Quantum Cryptography?

On deck: Hyungrok Jo, IWSEC2023 CFPa

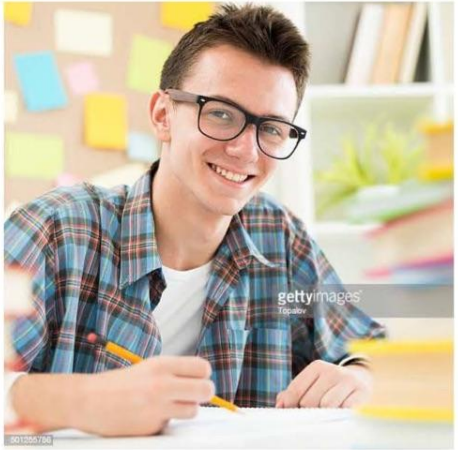
In the hole: Daniel Smith-Tone, Breaking SCRAP

Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

Varun Maram

ETH Zurich

Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

post- 8 of 8 **prefix**

1 **a** **:** after **:** subsequent **:** later

*post*date

b **:** behind **:** posterior **:** following after

*post*lude

*post*consonantal

2 **a** **:** subsequent to **:** later than

*post*operative

b **:** posterior to

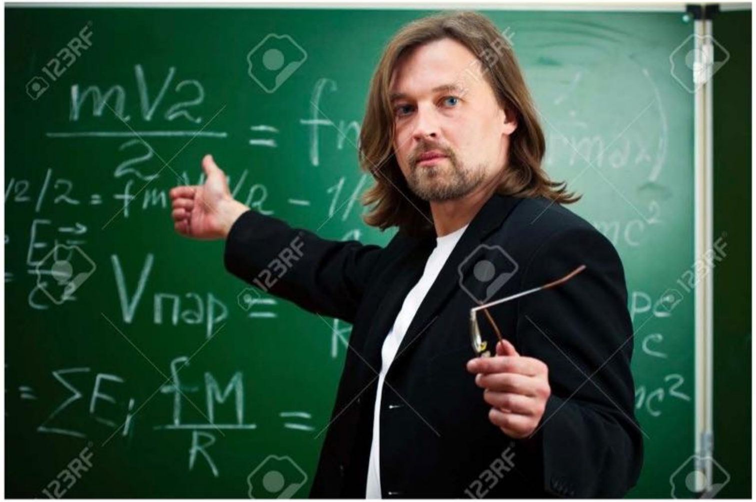
*post*orbital

Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

Yes.

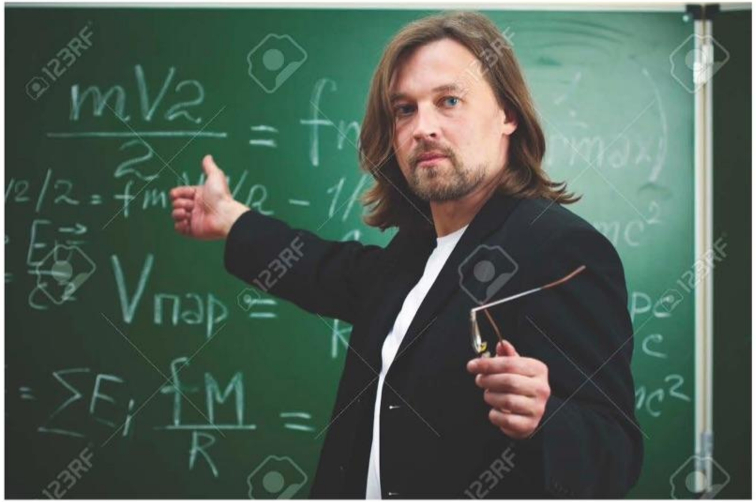

That's all Folks!

Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



Using “classical” against “quantum”.

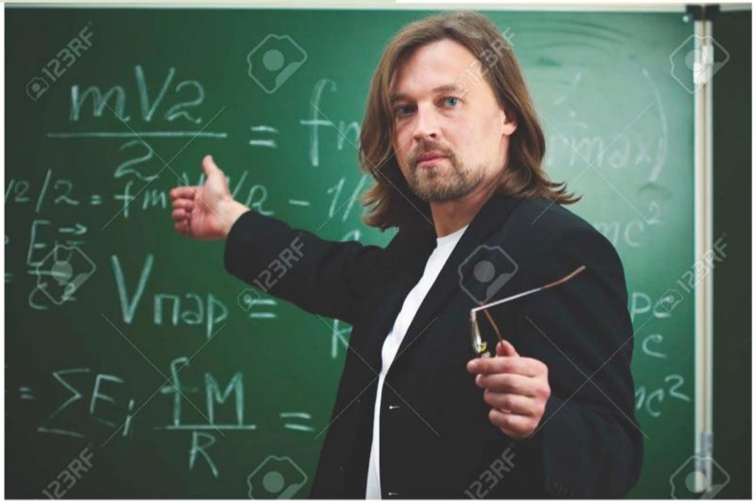
Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



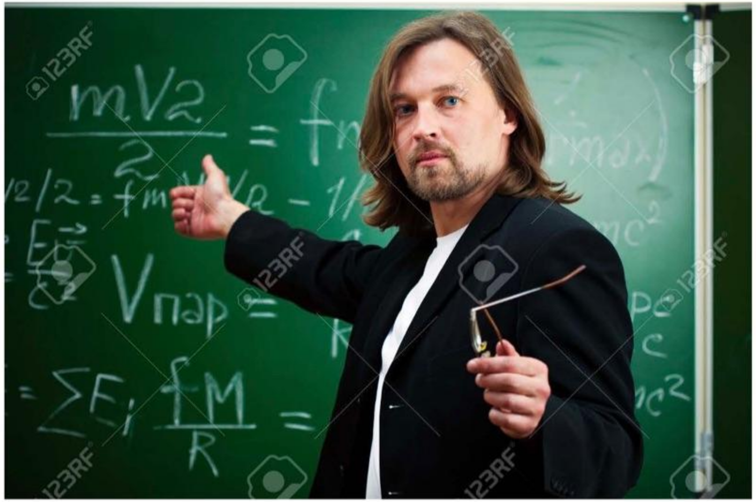
Using "classical" against "quantum".

Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

Using "quantum" against "quantum".

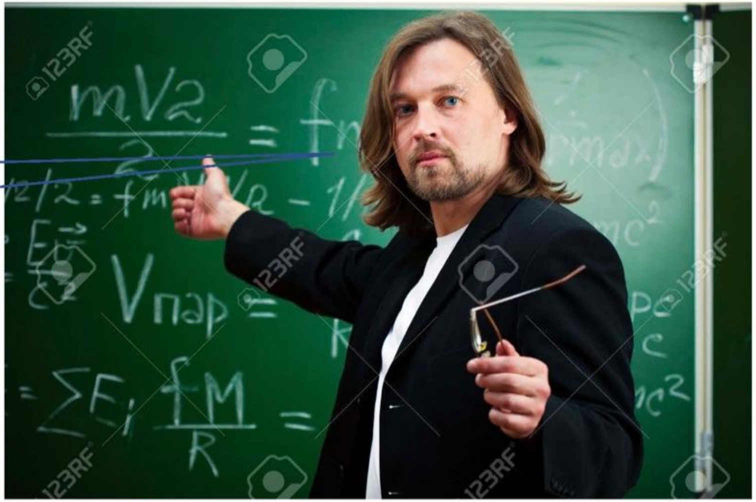


Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

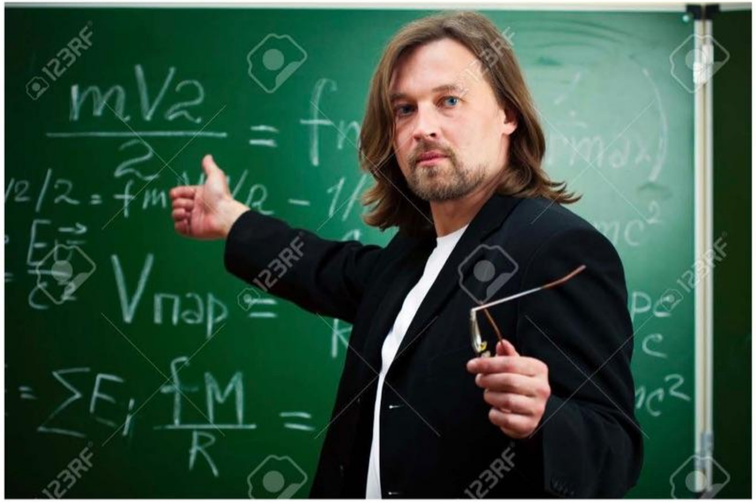


Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

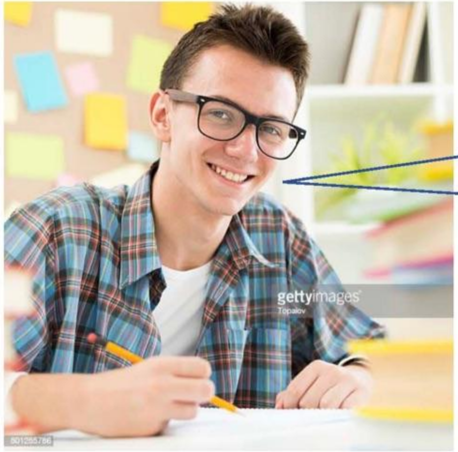
No.



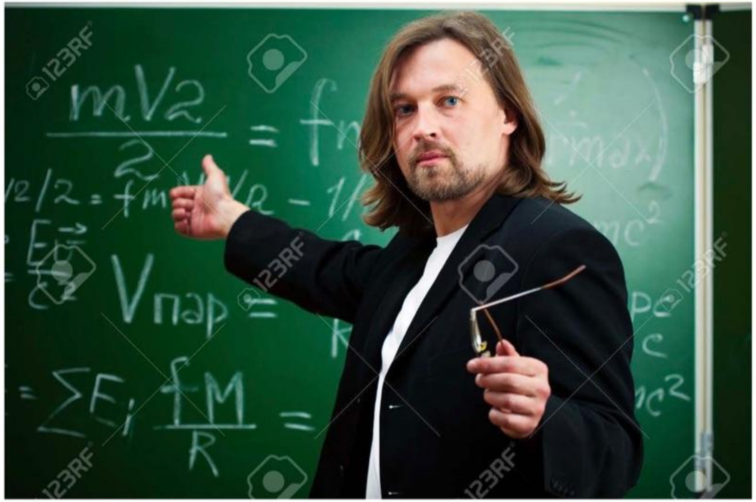
Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



What are you even talking about?




How to not confuse Jimmy?


He'll get used to it.


He'll get used to it.
Change PQ instead.


He'll get used to it.
Change PQ instead.
Rename our field to post-post-quantum crypto?


imgflip.com


Change PQ instead.

Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

Does Pre-Quantum Cryptography Come **After** Quantum Cryptography?

Does Pre-Quantum Cryptography Come **After** Quantum Cryptography?

PQCrypto 2023

The 14th International Conference on Post-Quantum Cryptography

August 16-18, 2023

College Park, MD, USA

Does Pre-Quantum Cryptography Come **After** Quantum Cryptography?

PQCrypto 2023

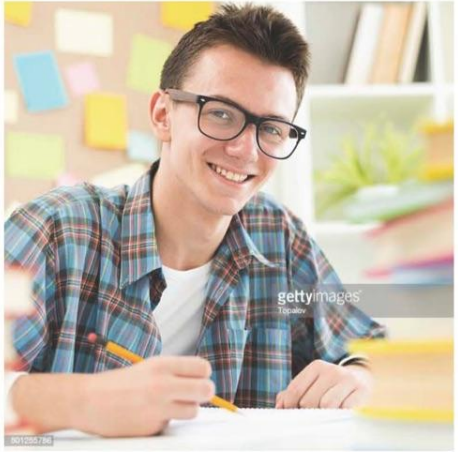
The 14th International Conference on Pre-Quantum Cryptography

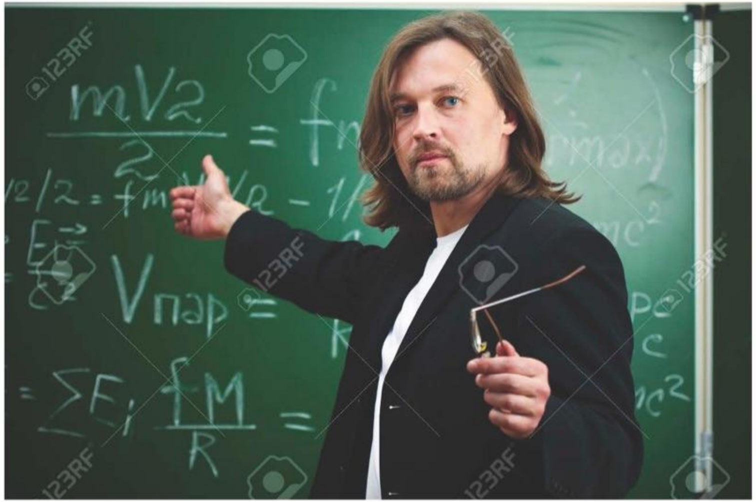
August 16-18, 2023

College Park, MD, USA

Using “classical” against “classical”.

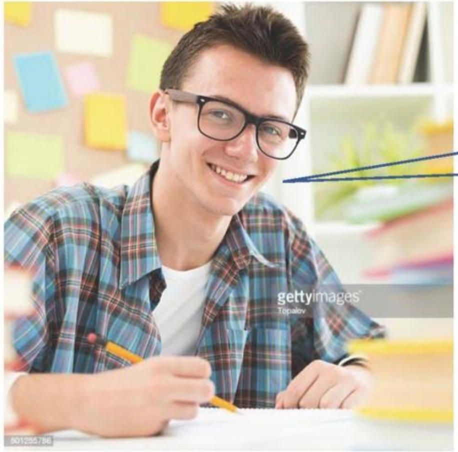
Does Pre-Quantum Cryptography Come **After** Quantum Cryptography?



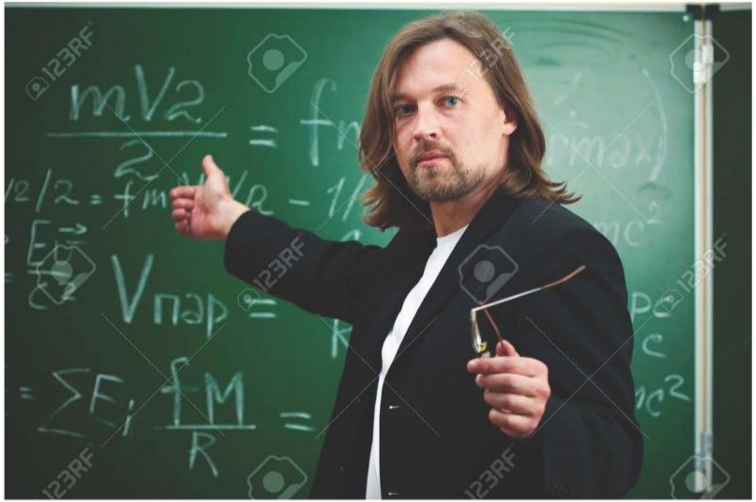


Using “classical” against “classical”.

Does Pre-Quantum Cryptography Come **After** Quantum Cryptography?



What?!



Does Post-Quantum Cryptography Come **After** Quantum Cryptography?

Does Quantum-Safe/-Resistant Cryptography Come **After** Quantum Cryptography?

Does Quantum-Safe/-Resistant

Keywords

cryptography; digital signatures; key-encapsulation mechanism (KEM); key-establishment; post-quantum cryptography; public-key encryption; quantum resistant; quantum safe

i

NIST IR 8413-upd1 Third Round Status Report

IBM Research Focus areas

Home
↳ Projects

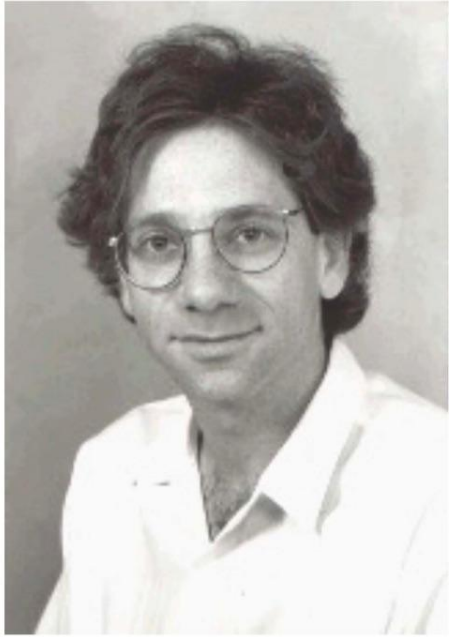
Quantum-safe cryptography algorithms

- Do I want PQC to be eventually replaced by QRC/QSC?

- Do I want PQC to be eventually replaced by QRC/QSC?
    - Yes!

- Do I want PQC to be eventually replaced by QRC/QSC?
    - Yes!

- Will the community actually do it?

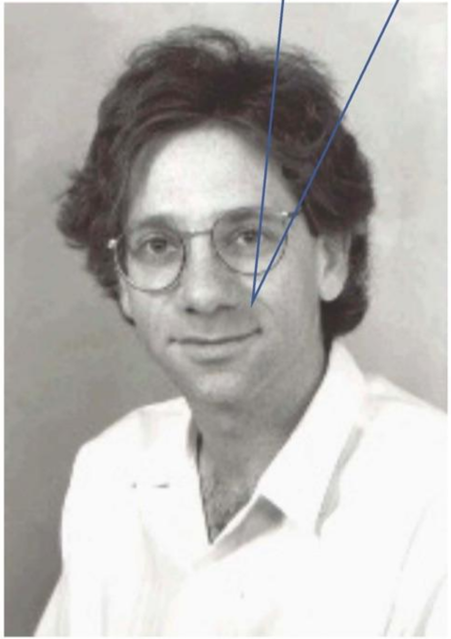


Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC

Phillip Rogaway

Dept. of Computer Science, University of California, Davis CA 95616 USA, and
Dept. of Computer Science, Chiang Mai University, Chiang Mai 50200 Thailand
rogaway@cs.ucdavis.edu   www.cs.ucdavis.edu/~rogaway

Let's use "blockcipher", and not "block cipher" or "block-cipher".
(Asiacrypt'04)



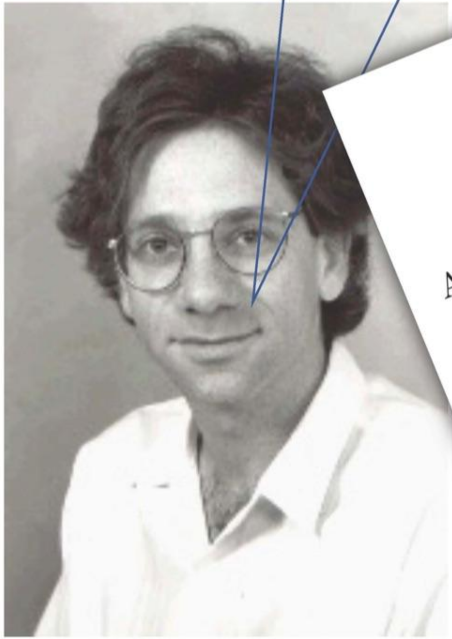
Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC

Phillip Rogaway

Dept. of Computer Science, University of California, Davis CA 95616 USA, and
Dept. of Computer Science, Chiang Mai University, Chiang Mai 50200 Thailand
rogaway@cs.ucdavis.edu www.cs.ucdavis.edu/∼rogaway

I end this paper by acknowledging that everyone writes *block cipher*, not *blockcipher*. Still, the time has come to spell this word solid. I invite you to join me.

Let's use "blockcipher", and not "block cipher" or "block-cipher".
(Asiacrypt'04)



Efficient Instantiati... Refin...

...A 95616 USA, and
...hiang Mai 50200 Thailand
...davis.edu/~rogaway

Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality

Akiko Inoue[1], Tetsu Iwata[2], Kazuhiko Minematsu[1], and Bertram Poettering[3]

[1] NEC Corporation, Kawasaki, Japan,
a_inoue@nec.com, k-minematsu@nec.com
[2] Nagoya University, Nagoya, Japan, tetsu.iwata@nagoya-u.jp
[3] IBM Research – Zurich, Switzerland, poe@zurich.ibm.com

... by acknowledging that everyone writes *block cipher*, not
...still, the time has come to spell this word solid. I invite you to join

“blockcipher”

2007	ASIACRYPT	**On Tweaking Luby-Rackoff Blockciphers** *David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, Hakan Seyalioglu*
2016	ASIACRYPT	**How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers** *Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, Dawu Gu*
2016	ASIACRYPT	**Salvaging Weak Security Bounds for Blockcipher-Based Constructions** *Thomas Shrimpton, R. Seth Terashima*
2017	ASIACRYPT	**Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length** *Yusuke Naito*

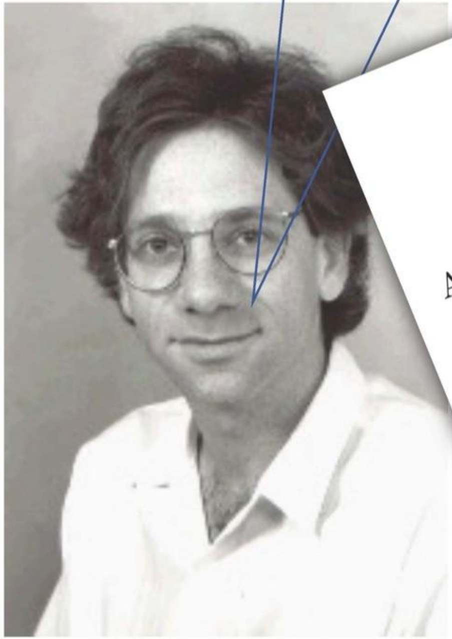
“block-cipher/block cipher”

"block-cipher/block cipher"

2006	ASIACRYPT	Combining Compression Functions and Block Cipher-Based Hash Functions *Thomas Peyrin, Henri Gilbert, Frédéric Muller, Matthew J. B. Robshaw*
2007	ASIACRYPT	Known-Key Distinguishers for Some Block Ciphers *Lars R. Knudsen, Vincent Rijmen*
2007	ASIACRYPT	On Efficient Message Authentication Via Block Cipher Design Techniques *Goce Jakimoski, K. P. Subbalakshmi*
2009	ASIACRYPT	The Key-Dependent Attack on Block Ciphers *Xiaorui Sun, Xuejia Lai*
2012	ASIACRYPT	Differential Analysis of the LED Block Cipher *Florian Mendel, Vincent Rijmen, Deniz Toz, Kerem Varici*
2012	ASIACRYPT	PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract *Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, Tolga Yalçin*
2013	ASIACRYPT	Block ciphers - past and present Invited paper *Lars R. Knudsen*
2013	ASIACRYPT	Key Difference Invariant Bias in Block Ciphers *Andrey Bogdanov, Christina Boura, Vincent Rijmen, Meiqin Wang, Long Wen, Jingyuan Zhao*
2014	ASIACRYPT	Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers *Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, Ling Song*
2014	ASIACRYPT	Tweaks and Keys for Block Ciphers: The TWEAKEY Framework *Jérémy Jean, Ivica Nikolic, Thomas Peyrin*

2015	ASIACRYPT	Midori: A Block Cipher for Low Energy *Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, Francesco Regazzoni*
2015	ASIACRYPT	Optimally Secure Block Ciphers from Ideal Primitives *Stefano Tessaro*
2016	ASIACRYPT	Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers *Zejun Xiang, Wentao Zhang, Zhenzhen Bao, Dongdai Lin*
2018	ASIACRYPT	Block Cipher Invariants as Eigenvectors of Correlation Matrices Best Paper Award *Tim Beyne*
2018	ASIACRYPT	Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions Abstract ▼ *Akinori Hosoyamada, Kan Yasuda*
2018	ASIACRYPT	Tweakable Block Ciphers Secure Beyond the Birthday Bound in the Ideal Cipher Model *ByeongHak Lee, Jooyoung Lee*
2018	ASIACRYPT	ZCZ – Achieving n-bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls *Ritam Bhaumik, Eik List, Mridul Nandi*
2020	ASIACRYPT	How to Build Optimally Secure PRFs Using Block Ciphers *Benoît Cogliati, Ashwin Jha, Mridul Nandi*
2020	ASIACRYPT	Lower Bounds on the Degree of Block Ciphers Abstract ▼ *Phil Hebborn, Baptiste Lambin, Gregor Leander, Yosuke Todo*
2022	ASIACRYPT	A Modular Approach to the Incompressibility of Block-Cipher-Based AEADs *Akinori Hosoyamada, Takanori Isobe, Yosuke Todo, Kan Yasuda*

Let's use "blockcipher", and not "block cipher" or "block-cipher".
(Asiacrypt'04)



Efficient Instantiati... Refin...

...A 95616 USA, and
...ang Mai 50200 Thailand
...davis.edu/~rogaway

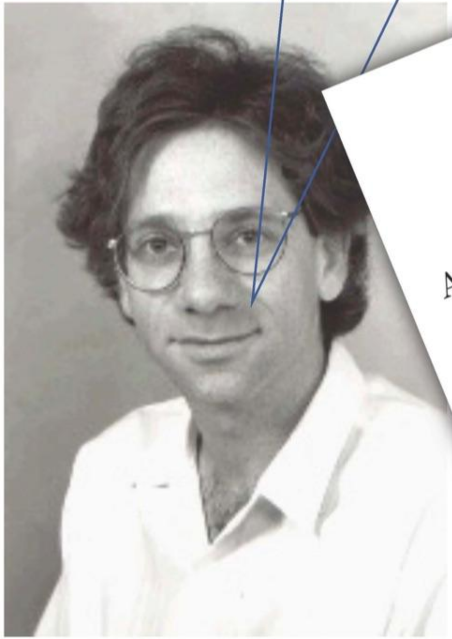
... by acknowledging that everyone writes *block cipher*, not
...till, the time has come to spell this word solid. I invite you to join

Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality

Akiko Inoue[1], Tetsu Iwata[2], Kazuhiko Minematsu[1], and Bertram Poettering[3]

[1] NEC Corporation, Kawasaki, Japan,
a_inoue@nec.com, k-minematsu@nec.com
[2] Nagoya University, Nagoya, Japan, tetsu.iwata@nagoya-u.jp
[3] IBM Research – Zurich, Switzerland, poe@zurich.ibm.com

Let's use "blockcipher", and not "block cipher" or "block-cipher".
(Asiacrypt'04)



Efficient Instantiati... Refin...

Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality

Akiko Inoue[1], Tetsu Iwata[2], Kazuhiko Minematsu[1], and Bertram Poettering[3]

[1] NEC Corporation, Kawasaki, Japan, a_inoue@nec.com, k-minematsu@nec.com

[2] Nagoya University, Nagoya, Japan, tetsu.iwata@nagoya-u.jp

[3] IBM Research – Zurich, Switzerland, poe@zurich.ibm.com

Abstract. We present practical attacks on OCB2. This mode of operation of a blockcipher was designed with the aim to provide particularly efficient and provably-secure authenticated encryption services, and since its proposal about 15 years ago it belongs to the top performers in this realm. OCB2 was included in an ISO standard in 2009.

...one writes *block cipher*, not ...this word solid. I invite you to join

- Do I want PQC to be eventually replaced by QRC/QSC?
  - Yes!

- Will the community actually do it?

- Do I want PQC to be eventually replaced by QRC/QSC?
    - Yes!
- Will the community actually do it?
    - Highly unlikely.

- Do I want PQC to be eventually replaced by QRC/QSC?
  - Yes!
- Will the community actually do it?
  - Highly unlikely.
- So what’s the point of this talk?

- Do I want PQC to be eventually replaced by QRC/QSC?
  - Yes!
- Will the community actually do it?
  - Highly unlikely.
- So what’s the point of this talk?
  - I don’t know.


That's all Folks!

Now presenting: Hyungrok Jo, IWSEC2023 CFPa

On deck: Daniel Smith-Tone, Breaking SCRAP

In the hole: Ryann Cartor, PQCrypto 23 Group Avatar

IWSEC 2023
Call For Participants

IWSEC 2023

IISEC in YOKOHAMA
and *ONLINE*
Aug. 29 - Aug. 31, 2023

IWSEC 2023

IISEC in YOKOHAMA and *ONLINE*

Aug. 29 - Aug. 31, 2023

Accepted papers

A: Cryptography Track (11)

- **Efficient Card-Based Millionaires' Protocols via Non-Binary Input Encoding**
  - Koji Nuida
- **Extractable Witness Encryption for the Homogeneous Linear Equation problem**
  - Bénédikt Tran and Serge Vaudenay
- **Making Classical (Threshold) Signatures Post-Quantum for Single Use on a Public Ledger**
  - Laurane Marco, Abdullah Talayhan and Serge Vaudenay
- **Improved Boomerang Attacks on Deoxys-BC**
  - Jiahao Zhao, Ling Song, Qianqian Yang, Nana Zhang and Lei Hu
- **TENET : Sublogarithmic Proof, Sublinear Verifier Inner Product Argument without a Trusted Setup**
  - Hyeonbum Lee and Jae Hong Seo
- **PMACrx: a vector-input MAC for high-dimensional vectors with BBB security**
  - Isamu Furuya, Hayato Kasahara, Akiko Inoue, Kazuhiko Minematsu and Tetsu Iwata
- **Improved Hybrid Attack via Error-Splitting Method for Finding Quinary Short Lattice Vectors**
  - Haiming Zhu, Shoichi Kamada, Momonari Kudo and Tsuyoshi Takagi
- **A New Security Analysis Against MAYO and QR-UOV Using Rectangular MinRank Attack**
  - Hiroki Furue and Yasuhiko Ikematsu
- **aPlonK : Aggregated PlonK from Multi-Polynomial Commitment Schemes**
  - Miguel Ambrona, Marc Beunardeau, Anne-Laure Schmitt and Raphael Toledo
- **Check Alternating Patterns: A Physical Zero-Knowledge Proof for Moon-or-Sun**
  - Samuel Hand, Alexander Koch, Pascal Lafourcade, Daiki Miyahara and Léo Robert
- **Total Break of a Public Key Cryptosystem Based on a Group of Permutation Polynomials**
  - Max Cartor, Ryann Cartor, Mark Lewis and Daniel Smith-Tone

B: Cybersecurity, Usable Security, and Privacy Track (3)

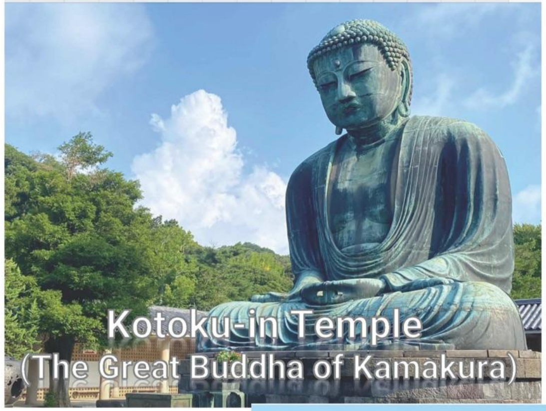
- **Power analysis pushed too far: breaking Android-based isolation with fuel gauges**
  - Vincent Giraud and David Naccache
- **Reliability of Ring Oscillator PUFs with Reduced Helper Data**
  - Julien Béguinot, Jean-Luc Danger, Olivier Rioul, Sylvain Guilley, Wei Cheng and Ville-Oskari Yli-Mayry
- **The Good, the Bad, and the Binary: An LSTM-Based Method for Section Boundary Detection in Firmware Analysis**
  - Riccardo Remigio, Alessandro Bertani, Mario Polino, Michele Carminati and Stefano Zanero

Poster session (10) on DAY 1

Accepted posters will come up soon @https://www.iwsec.org/2023/

Excursion

(**Kamakura Half Day Tour** on the last day)



Registration

- **Standard Rate**
  (On or before August 28, 2023)

- **On-site registration**
  (On or after August 29, 2023)

For more information,

https://www.iwsec.org/2023/

https://twitter.com/iwsec

iwsec2023-inquiry@iwsec.org

Now presenting: Daniel Smith-Tone, Breaking SCRAP

On deck: Ryann Cartor, PQCrypto 23 Group Avatar

SCRAP Dig. Sig. Scheme

Choose positive integers q, n and $\ell < k$.
Let $\mathcal{R} = \mathbb{Z}_q[x_1, \ldots, x_n]$.
Choose matrices $\mathbf{S} \in \mathcal{R}^{\ell \times k}$ and $\mathbf{P} \in \mathcal{R}^{k \times \ell}$ such that

$$\mathbf{SP} = \mathbf{I}_\ell.$$

To sign:
$\mathbf{uS} = \mathbf{v}$.

To verify:
$\mathbf{vP} = \mathbf{uSP} = \mathbf{u}$.

To make it work...

- Need a reasonable way to build **S** and **P**.
- Build a pair **W**, $\mathbf{W}^{-1}$ and use a subset of rows/columns.

To make it reasonable...

- Restrict the degree of entries.
- Make it sparse

To make it efficient...

- Make both **S** and **P** quite sparse and with a low degree bound.
- Build **W** and $\mathbf{W}^{-1}$ from elementary matrices in a special way to balance the sparsity/degree.

To break it...

Notice that $\phi = \mathbf{P}$ is an isomorphism of $\mathcal{R}$-modules, $\mathcal{R}^\ell$ and $\phi(\mathcal{R}^\ell)$. Therefore, both $\mathbf{u}$ and $\mathbf{v}$ generate the same ideal in $\mathcal{R}$.

The sparsity means that there is low probability of elimination of terms from polynomial combinations of the coefficients.

Easy instance of ideal membership where a Gröbner basis is not needed!

If direct depth-first leading term division doesn't break it, start adding S-polynomials.

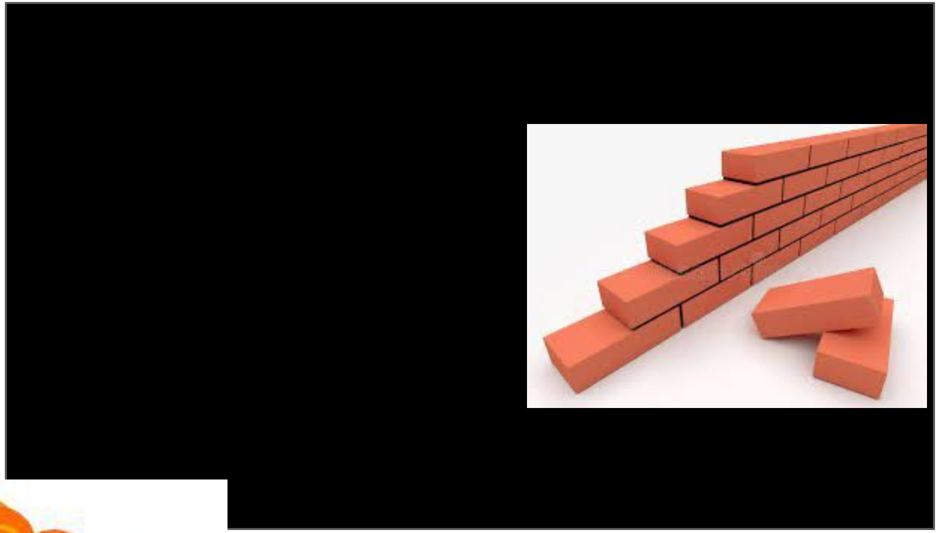
Performance

Table: MAGMA attack timing for 1000 instances of the Scrap digital signature scheme with smaller sparsity bound t and for claimed NIST Security level I, i.e. 143-bit security, parameters.

Scrap(q, n, ℓ, k, t, b)	Least(ms)	Average(ms)	Most(ms)
$Scrap(6, 64, 5, 10, 2, 3)$	20	100	320
$Scrap(6, 64, 5, 10, 3, 3)$	30	1140	4170

Now presenting: Ryann Cartor, PQCrypto 23 Group Avatar

1) What are you using your drink ticket for? (Beer, wine, other)
2) What is more fun? (Cryptanalysis or constructing schemes)
3) What is your main interest? (Code-based, multivariate, lattice based, Isogeny based)
4) Where do you work? (Academia, Government, Industry?)




POLYNOMIALS
#