

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

| *postdate*

b : behind : posterior : following after

| *postlude*

| *postconsonantal*

2 a : subsequent to : later than

| *postoperative*

b : posterior to

| *postorbital*

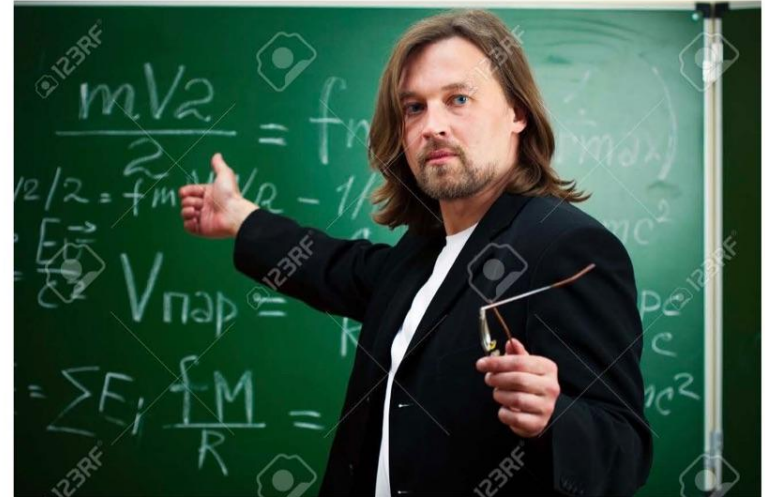
Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



Yes.

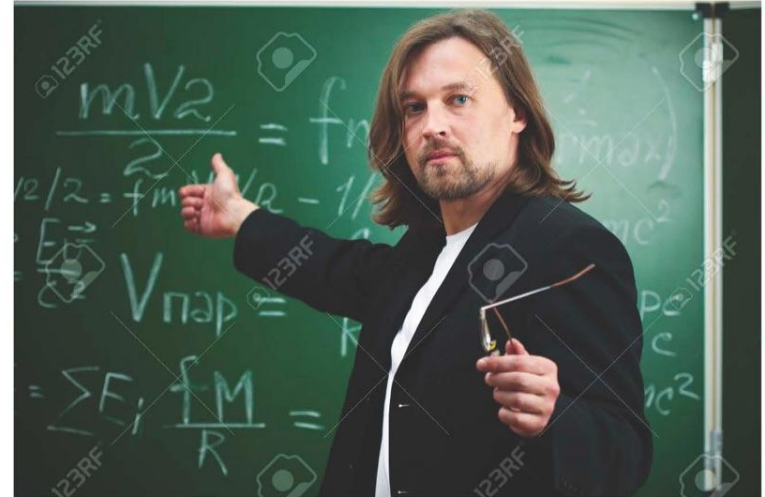
That's all Folks!

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



Using “classical”
against “quantum”.

Does Post-Quantum Cryptography Come After Quantum Cryptography?

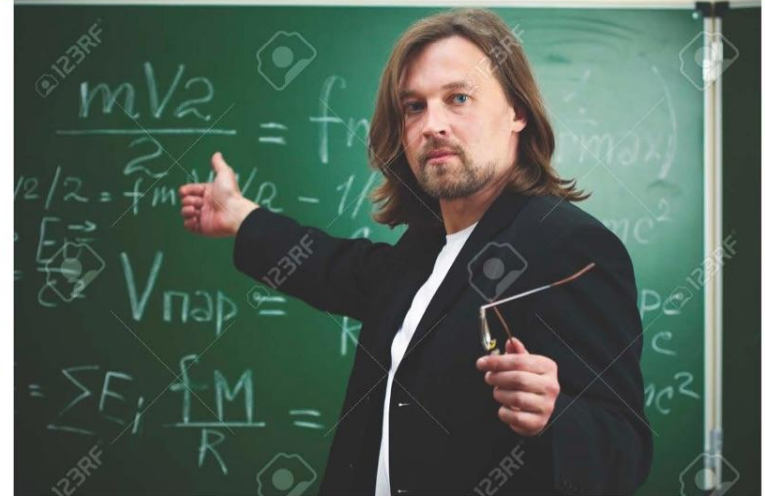


Using “classical”
against “quantum”.

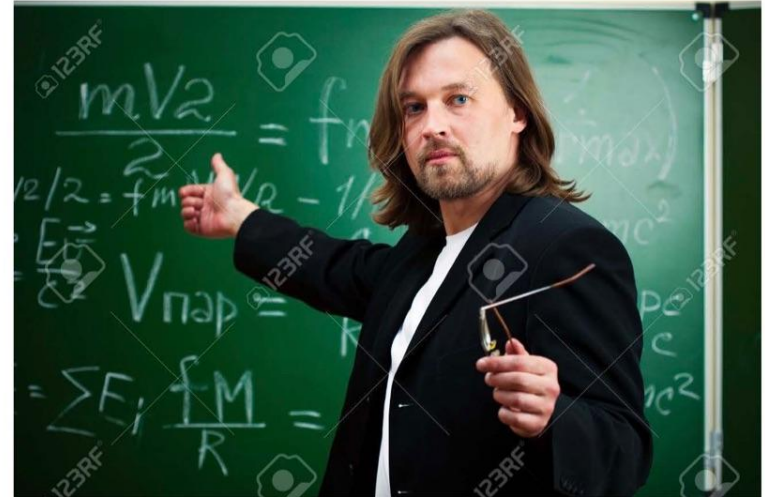
Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



Using “quantum”
against “quantum”.



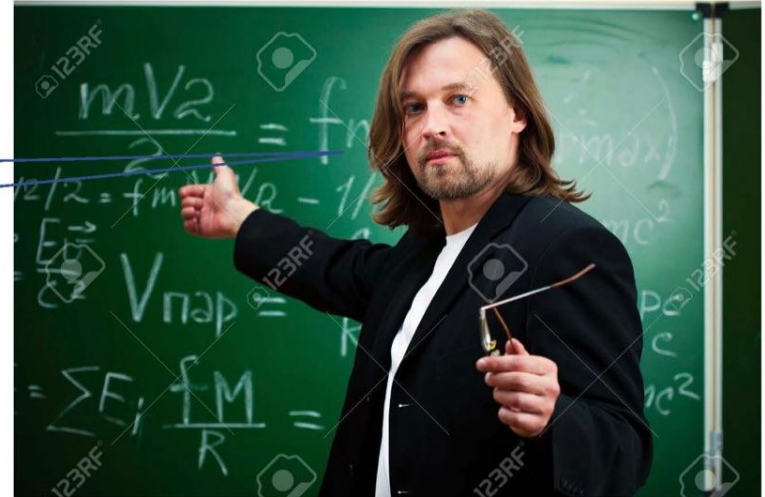
Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



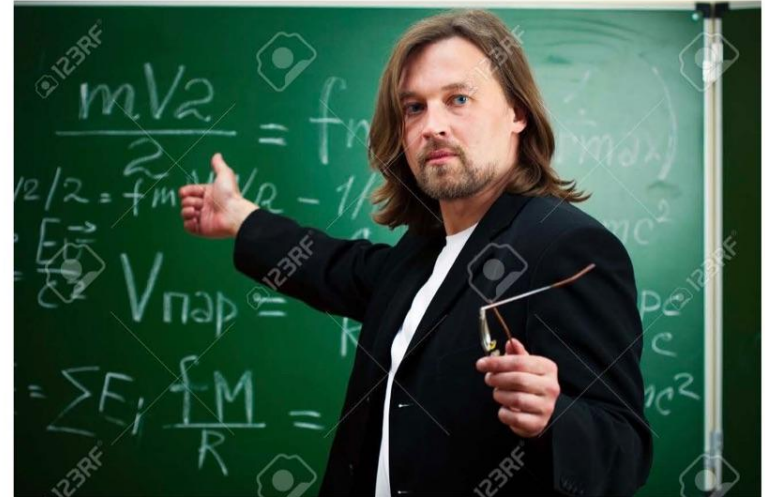
Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



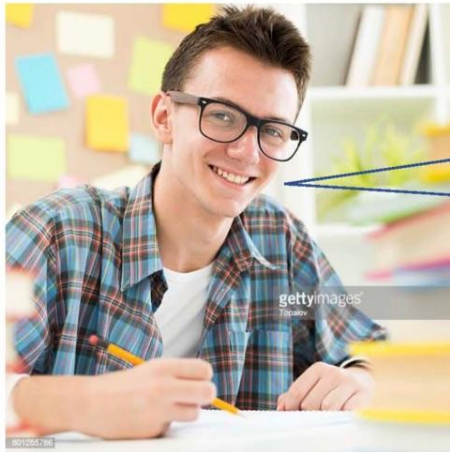
No.



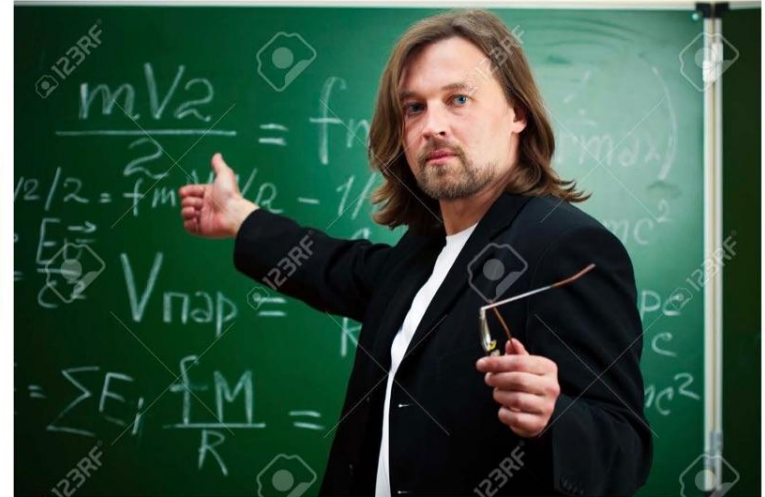
Does Post-Quantum Cryptography Come **After** Quantum Cryptography?



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



What are you even talking about?













imgflip.com



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

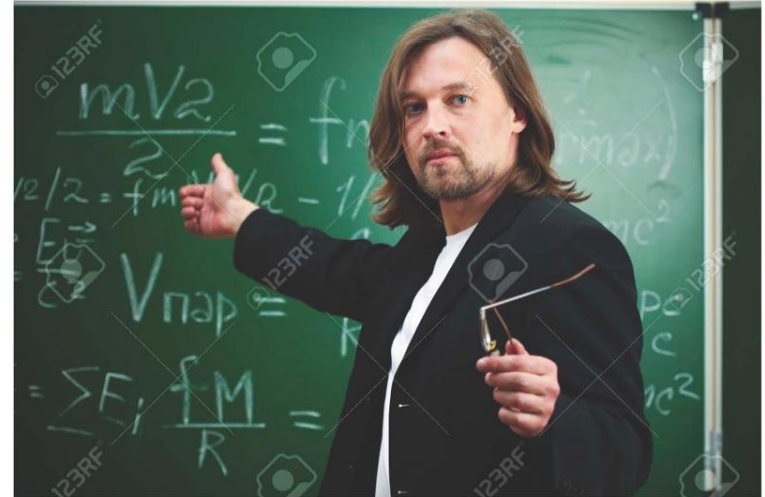
The 14th International Conference on **Pre**-Quantum Cryptography

August 16-18, 2023

College Park, MD, USA

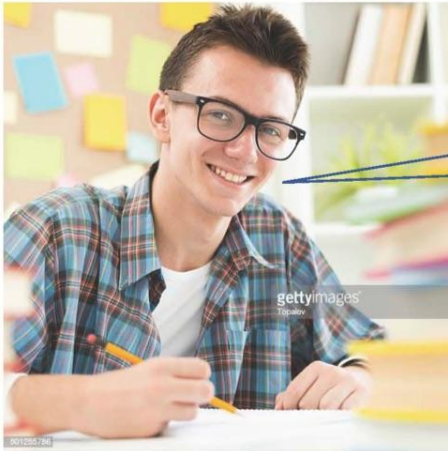
Using “classical”
against “classical”.

Does Pre-Quantum Cryptography Come After Quantum Cryptography?

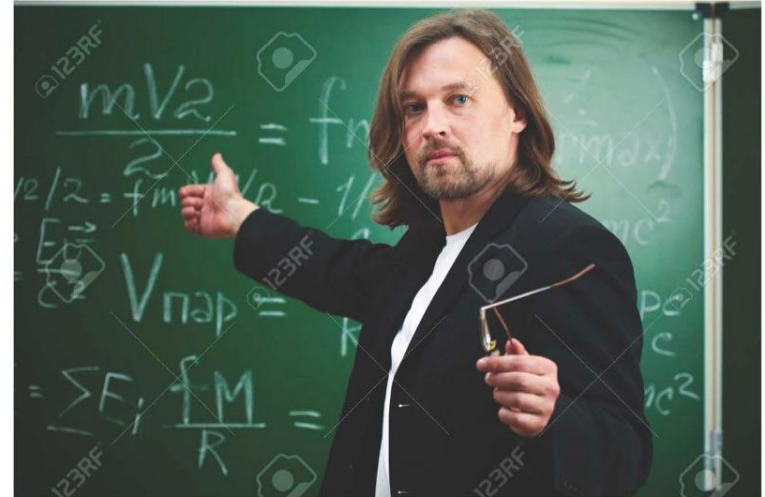


Using “classical”
against “classical”.

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

OPEN QUANTUM SAFE

*software for prototyping
quantum-resistant cryptography*

- 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

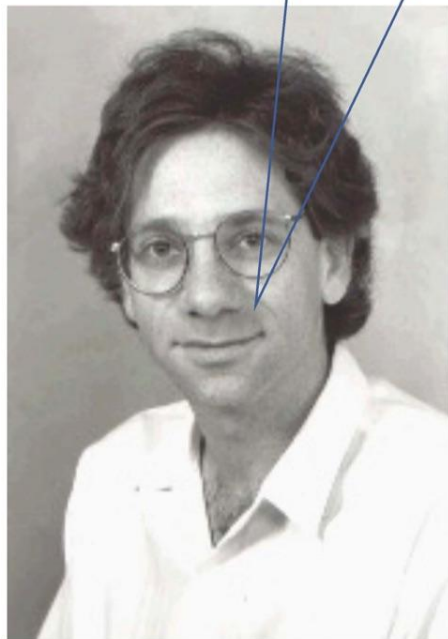
Let's use “**blockcipher**”, and not
“**block cipher**” or “**block-cipher**”.

(Asiacrypt'04)

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

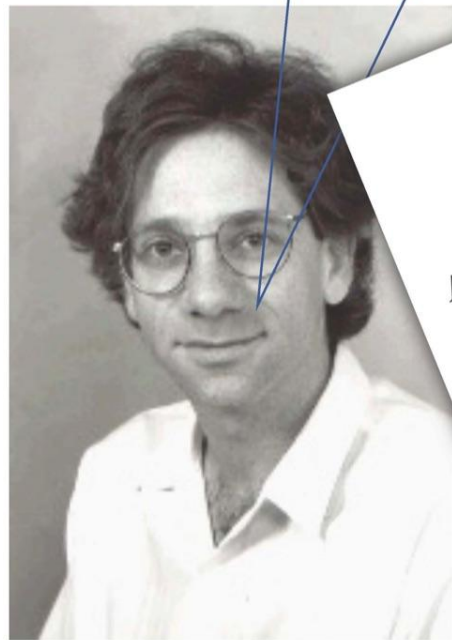
Phillip Rogaway

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 Instantiation of OCB2: Refined Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality

Akiko Inoue¹ , Tetsu Iwata² , Kazuhiko Minematsu¹ , and Bertram Poettering³ 

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

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

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

“blockcipher”

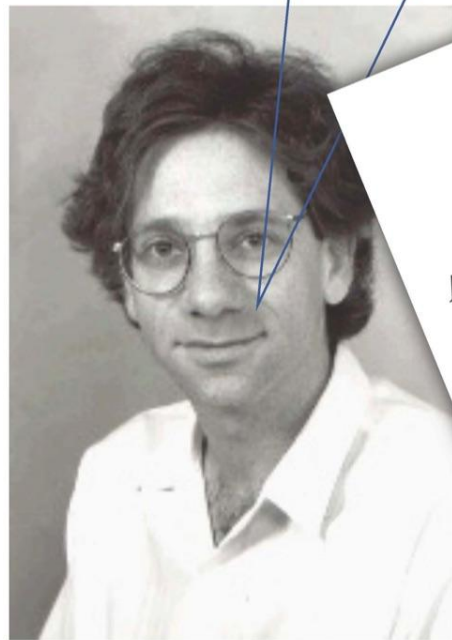
2007	ASIACRYPT	On Tweaking Luby-Rackoff Blockciphers <i>David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, Hakan Seyalioglu</i>
2016	ASIACRYPT	How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers <i>Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, Dawu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

“block-cipher/block cipher”





“block-cipher/block cipher”

2006	ASIACRYPT	Combining Compression Functions and Block Cipher-Based Hash Functions <i>Thomas Peyrin, Henri Gilbert, Frédéric Muller, Matthew J. B. Robshaw</i>	
2007	ASIACRYPT	Known-Key Distinguishers for Some Block Ciphers <i>Lars R. Knudsen, Vincent Rijmen</i>	
2007	ASIACRYPT	On Efficient Message Authentication Via Block Cipher Design Techniques <i>Goce Jakimoski, K. P. Subbalakshmi</i>	
2009	ASIACRYPT	The Key-Dependent Attack on Block Ciphers <i>Xiaorui Sun, Xuejia Lai</i>	
2012	ASIACRYPT	Differential Analysis of the LED Block Cipher <i>Florian Mendel, Vincent Rijmen, Deniz Toz, Kerem Varici</i>	
2012	ASIACRYPT	PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract <i>Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventsislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, Tolga Yalçın</i>	
2013	ASIACRYPT	Block ciphers - past and present ★ Invited paper <i>Lars R. Knudsen</i>	
2013	ASIACRYPT	Key Difference Invariant Bias in Block Ciphers <i>Andrey Bogdanov, Christina Boura, Vincent Rijmen, Meiqin Wang, Long Wen, Jingyuan Zhao</i>	
2014	ASIACRYPT	Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers <i>Siwei Sun, Lei Hu, Peng Wang, Xexin Qiao, Xiaoshuang Ma, Ling Song</i>	
2014	ASIACRYPT	Tweaks and Keys for Block Ciphers: The TWEAKEY Framework <i>Jérémy Jean, Ivica Nikolic, Thomas Peyrin</i>	
2015	ASIACRYPT	Midori: A Block Cipher for Low Energy <i>Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, Francesco Regazzoni</i>	
2015	ASIACRYPT	Optimally Secure Block Ciphers from Ideal Primitives <i>Stefano Tessaro</i>	
2016	ASIACRYPT	Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers 📄 <i>Zejun Xiang, Wentao Zhang, Zhenzhen Bao, Dongdai Lin</i>	
2018	ASIACRYPT	Block Cipher Invariants as Eigenvectors of Correlation Matrices ★ Best Paper Award <i>Tim Beyne</i>	
2018	ASIACRYPT	Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions Abstract ▼ <i>Akinori Hosoyamada, Kan Yasuda</i>	
2018	ASIACRYPT	Tweakable Block Ciphers Secure Beyond the Birthday Bound in the Ideal Cipher Model <i>ByeongHak Lee, Jooyoung Lee</i>	
2018	ASIACRYPT	ZCZ – Achieving n-bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls <i>Ritam Bhaumik, Eik List, Mridul Nandi</i>	
2020	ASIACRYPT	How to Build Optimally Secure PRFs Using Block Ciphers <i>Benoît Cogliati, Ashwin Jha, Mridul Nandi</i>	
2020	ASIACRYPT	Lower Bounds on the Degree of Block Ciphers 📄 Abstract ▼ <i>Phil Hebborn, Baptiste Lambin, Gregor Leander, Yosuke Todo</i>	
2022	ASIACRYPT	A Modular Approach to the Incompressibility of Block-Cipher-Based AEADs <i>Akinori Hosoyamada, Takanori Isobe, Yosuke Todo, Kan Yasuda</i>	

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



Efficient Instantiation of OCB2: Refined Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality

Akiko Inoue¹ , Tetsu Iwata² , Kazuhiko Minematsu¹ , and Bertram Poettering³ 

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

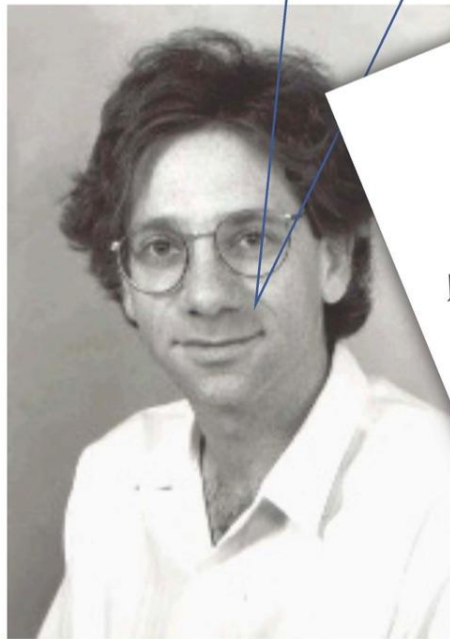
² Nagoya University, Nagoya, Japan, tetsu.iwata@nagoya-u.jp

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





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

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

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



Efficient Instantiation of Refined Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality

Akiko Inoue¹ , Tetsu Iwata² , Kazuhiko Minematsu¹ , and Bertram Poettering³ 

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 *block cipher* 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!