Protecting Obfuscation Against Arithmetic Attacks

Mor Weiss

Based on joint work with Eric Miles and Amit Sahai

CRYPTO 2015

August 16-20, 2015

DATE

Santa Barbara, CA, USA

LOCATION

CRYPTO 2015

August 16-20, 2015

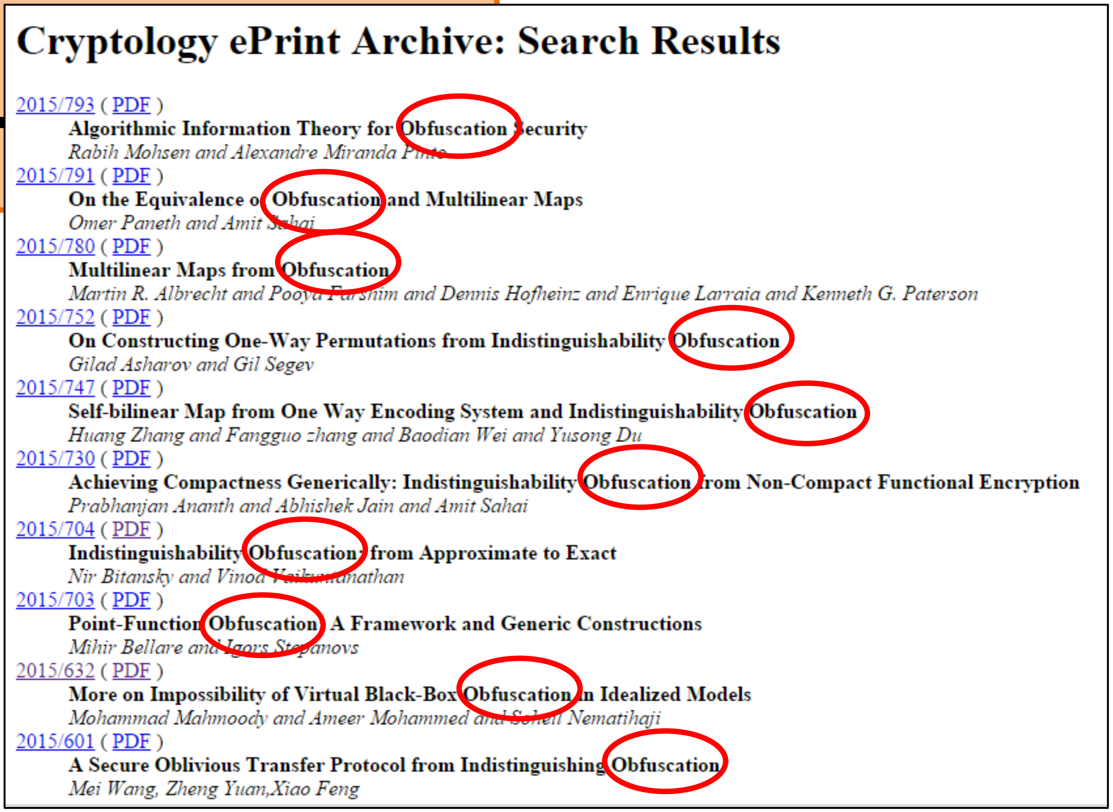
DATE

Santa Barbara, CA, USA

LOCATION

Hey!
What's new on earth?

Hey!
What's
ear



Cryptology ePrint Archive: Search Results

2015/793 (PDF)
Algorithmic Information Theory for Obfuscation Security
Rabih Mohsen and Alexandre Miranda Pinto

2015/791 (PDF)
On the Equivalence of Obfuscation and Multilinear Maps
Omer Paneth and Amit Sahai

2015/780 (PDF)
Multilinear Maps from Obfuscation
Martin R. Albrecht and Pooya Farshim and Dennis Hofheinz and Enrique Larraia and Kenneth G. Paterson

2015/752 (PDF)
On Constructing One-Way Permutations from Indistinguishability Obfuscation
Gilad Asharov and Gil Segev

2015/747 (PDF)
Self-bilinear Map from One Way Encoding System and Indistinguishability Obfuscation
Huang Zhang and Fangguo zhang and Baodian Wei and Yusong Du

2015/730 (PDF)
Achieving Compactness Generically: Indistinguishability Obfuscation from Non-Compact Functional Encryption
Prabhanjan Ananth and Abhishek Jain and Amit Sahai

2015/704 (PDF)
Indistinguishability Obfuscation: from Approximate to Exact
Nir Bitansky and Vinod Vaikuntanathan

2015/703 (PDF)
Point-Function Obfuscation: A Framework and Generic Constructions
Mihir Bellare and Igors Stepanovs

2015/632 (PDF)
More on Impossibility of Virtual Black-Box Obfuscation in Idealized Models
Mohammad Mahmoody and Ameer Mohammed and Soheil Nematihaji

2015/601 (PDF)
A Secure Oblivious Transfer Protocol from Indistinguishing Obfuscation
Mei Wang, Zheng Yuan,Xiao Feng

CRYPTO 2015

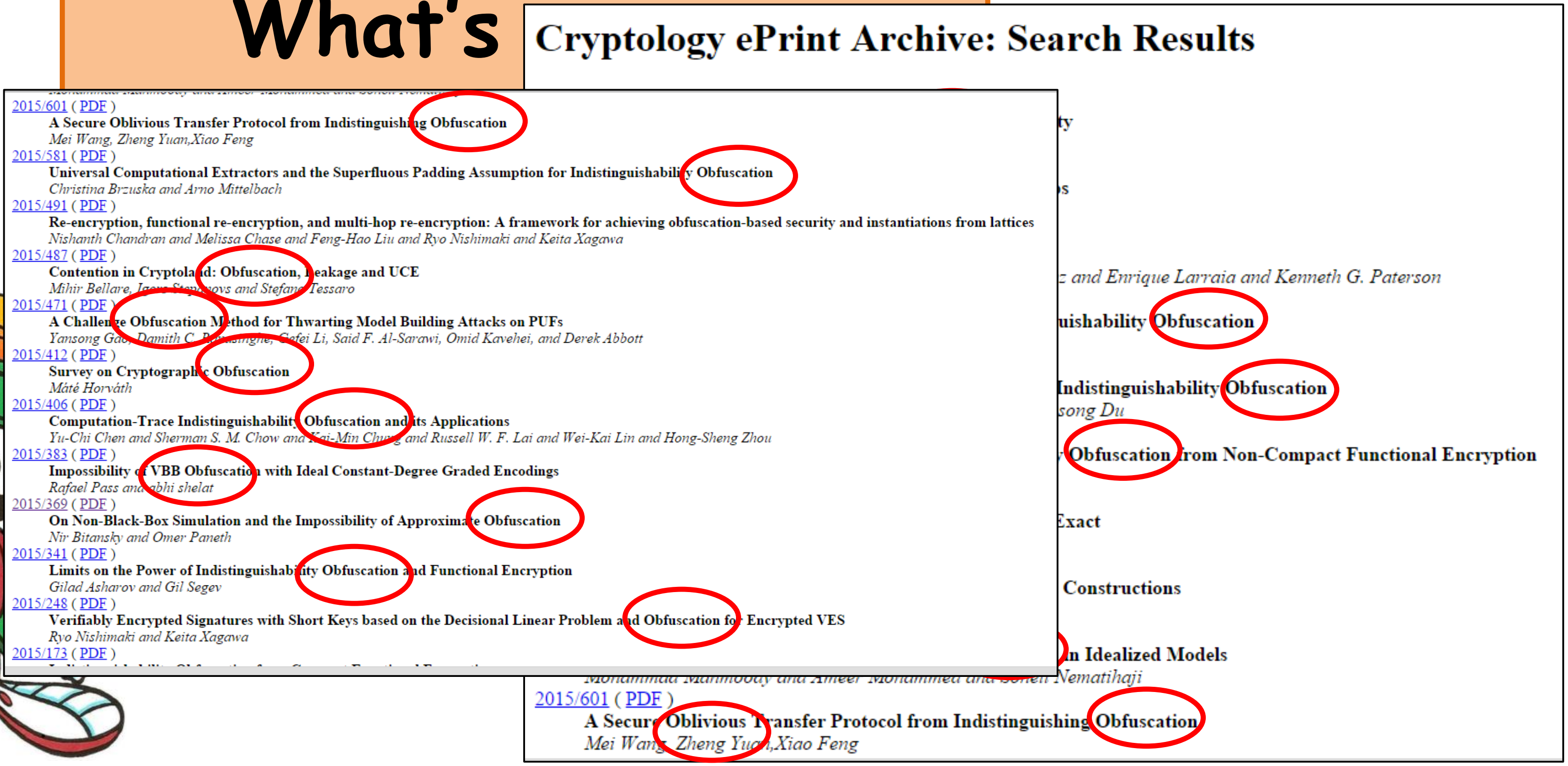
August 16-20, 2015

DATE

Santa Barbara, CA, USA

LOCATION

Hey! What's



Cryptology ePrint Archive: Search Results

Mohammad Mahmoody and Ameer Mohammed and Soheil Nematihaji

2015/601 (PDF)
A Secure Oblivious Transfer Protocol from Indistinguishing Obfuscation
Mei Wang, Zheng Yuan,Xiao Feng

2015/581 (PDF)
Universal Computational Extractors and the Superfluous Padding Assumption for Indistinguishability Obfuscation
Christina Brzuska and Arno Mittelbach

2015/491 (PDF)
Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achieving obfuscation-based security and instantiations from lattices
Nishanth Chandran and Melissa Chase and Feng-Hao Liu and Ryo Nishimaki and Keita Xagawa

2015/487 (PDF)
Contention in Cryptoland: Obfuscation, Leakage and UCE
Mihir Bellare, Igors Stepanovs and Stefano Tessaro

2015/471 (PDF)
A Challenge Obfuscation Method for Thwarting Model Building Attacks on PUFs
Yansong Gao, Damith C. Ranasinghe, Gefei Li, Said F. Al-Sarawi, Omid Kavehei, and Derek Abbott

2015/412 (PDF)
Survey on Cryptographic Obfuscation
Máté Horváth

2015/406 (PDF)
Computation-Trace Indistinguishability Obfuscation and its Applications
Yu-Chi Chen and Sherman S. M. Chow and Kai-Min Chung and Russell W. F. Lai and Wei-Kai Lin and Hong-Sheng Zhou

2015/383 (PDF)
Impossibility of VBB Obfuscation with Ideal Constant-Degree Graded Encodings
Rafael Pass and abhi shelat

2015/369 (PDF)
On Non-Black-Box Simulation and the Impossibility of Approximate Obfuscation
Nir Bitansky and Omer Paneth

2015/341 (PDF)
Limits on the Power of Indistinguishability Obfuscation and Functional Encryption
Gilad Asharov and Gil Segev

2015/248 (PDF)
Verifiably Encrypted Signatures with Short Keys based on the Decisional Linear Problem and Obfuscation for Encrypted VES
Ryo Nishimaki and Keita Xagawa

2015/173 (PDF)

ty

s

z and Enrique Larraia and Kenneth G. Paterson

uishability Obfuscation

Indistinguishability Obfuscation
song Du

Obfuscation from Non-Compact Functional Encryption

Exact

Constructions

n Idealized Models
Mohammad Mahmoody and Ameer Mohammed and Soheil Nematihaji

2015/601 (PDF)
A Secure Oblivious Transfer Protocol from Indistinguishing Obfuscation
Mei Wang, Zheng Yuan,Xiao Feng

CRYPTO 2015

August 16-20, 2015

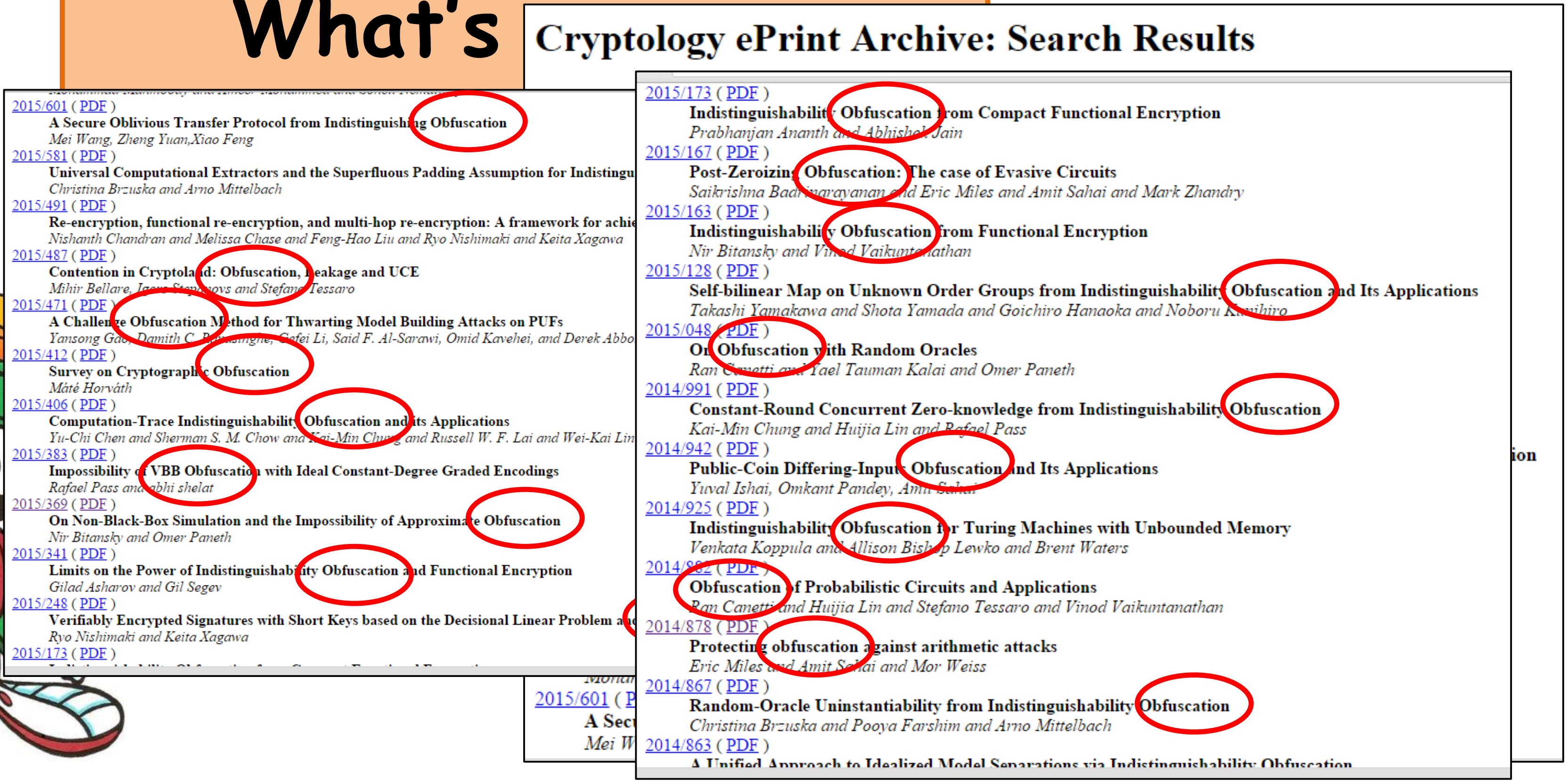
DATE

Santa Barbara, CA, USA

LOCATION

Hey!

What's



Cryptology ePrint Archive: Search Results

2015/601 (PDF)
A Secure Oblivious Transfer Protocol from Indistinguishing Obfuscation
Mei Wang, Zheng Yuan,Xiao Feng

2015/581 (PDF)
Universal Computational Extractors and the Superfluous Padding Assumption for Indistingu
Christina Brzuska and Arno Mittelbach

2015/491 (PDF)
Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achie
Nishanth Chandran and Melissa Chase and Feng-Hao Liu and Ryo Nishimaki and Keita Xagawa

2015/487 (PDF)
Contention in Cryptoland: Obfuscation, Leakage and UCE
Mihir Bellare, Igors Stepanovs and Stefano Tessaro

2015/471 (PDF)
A Challenge Obfuscation Method for Thwarting Model Building Attacks on PUFs
Yansong Gao, Damith C. Ranasinghe, Gefei Li, Said F. Al-Sarawi, Omid Kavehei, and Derek Abbo

2015/412 (PDF)
Survey on Cryptographic Obfuscation
Máté Horváth

2015/406 (PDF)
Computation-Trace Indistinguishability Obfuscation and its Applications
Yu-Chi Chen and Sherman S. M. Chow and Kai-Min Chung and Russell W. F. Lai and Wei-Kai Lin

2015/383 (PDF)
Impossibility of VBB Obfuscation with Ideal Constant-Degree Graded Encodings
Rafael Pass and abhi shelat

2015/369 (PDF)
On Non-Black-Box Simulation and the Impossibility of Approximate Obfuscation
Nir Bitansky and Omer Paneth

2015/341 (PDF)
Limits on the Power of Indistinguishability Obfuscation and Functional Encryption
Gilad Asharov and Gil Segev

2015/248 (PDF)
Verifiably Encrypted Signatures with Short Keys based on the Decisional Linear Problem a
Ryo Nishimaki and Keita Xagawa

2015/173 (PDF)

2015/173 (PDF)
Indistinguishability Obfuscation from Compact Functional Encryption
Prabhanjan Ananth and Abhishek Jain

2015/167 (PDF)
Post-Zeroizing Obfuscation: The case of Evasive Circuits
Saikrishna Badrinarayanan and Eric Miles and Amit Sahai and Mark Zhandry

2015/163 (PDF)
Indistinguishability Obfuscation from Functional Encryption
Nir Bitansky and Vinod Vaikuntanathan

2015/128 (PDF)
Self-bilinear Map on Unknown Order Groups from Indistinguishability Obfuscation and Its Applications
Takashi Yamakawa and Shota Yamada and Goichiro Hanaoka and Noboru Kunihiro

2015/048 (PDF)
On Obfuscation with Random Oracles
Ran Canetti and Yael Tauman Kalai and Omer Paneth

2014/991 (PDF)
Constant-Round Concurrent Zero-knowledge from Indistinguishability Obfuscation
Kai-Min Chung and Huijia Lin and Rafael Pass

2014/942 (PDF)
Public-Coin Differing-Inputs Obfuscation and Its Applications
Yuval Ishai, Omkant Pandey, Amit Sahai

2014/925 (PDF)
Indistinguishability Obfuscation for Turing Machines with Unbounded Memory
Venkata Koppula and Allison Bishop Lewko and Brent Waters

2014/882 (PDF)
Obfuscation of Probabilistic Circuits and Applications
Ran Canetti and Huijia Lin and Stefano Tessaro and Vinod Vaikuntanathan

2014/878 (PDF)
Protecting obfuscation against arithmetic attacks
Eric Miles and Amit Sahai and Mor Weiss

2014/867 (PDF)
Random-Oracle Uninstantiability from Indistinguishability Obfuscation
Christina Brzuska and Pooya Farshim and Arno Mittelbach

2014/863 (PDF)
A Unified Approach to Idealized Model Separations via Indistinguishability Obfuscation

2015/601 (P
A Sec
Mei W

CRYPTO 2015

August 16-20, 2015

DATE

Santa Barbara, CA, USA

LOCATION

Hey!
What's new on
earth?

In one word:

Obfuscation!

signatures

Functional encryption

NIZK

Deniable encryption

KEM

OT

Obfuscation*

*Adapted from Amit's slides

STOP

Is it even secure?

candidate obfuscators

multilinear maps

*Adapted from Amit's slides

are these even secure?

Yes!

are these even secure?

Yes!

…assuming multilinear maps are

are these even secure?

Yes!

…assuming multilinear maps are

Multilinear Maps

[GGH13,CLT13
GGH15,CLT15]

Ideal Multilinear Maps

[BR13,BR14
BGKPS14,AGIS14
AB15]

Multilinear Maps

Ideal Multilinear Maps

Multilinear Maps

Add
Multiply
Is zero?

Ideal Multilinear Maps

Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Ideal Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Ideal Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Invalid ops

Invalid Add
Invalid Multiply
Invalid Is zero?

Ideal Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Invalid ops

Ideal Multilinear Maps

Add
Multiply
Is zero?

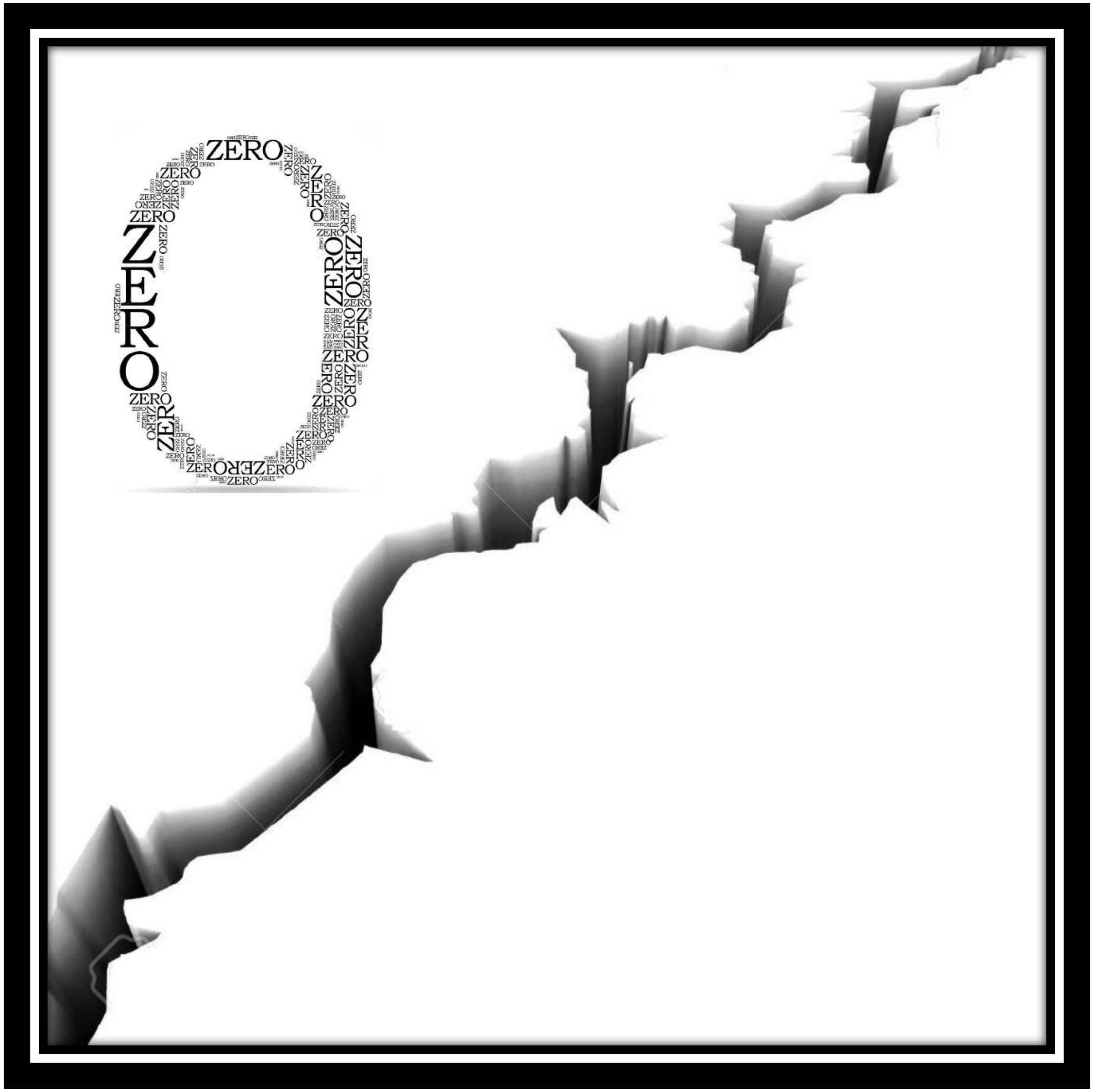
Valid ops

Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Invalid ops


ZERO

Ideal Multilinear Maps

Add
Multiply
Is zero?

Valid ops

Multilinear Maps

Add
Multiply
Is zero?

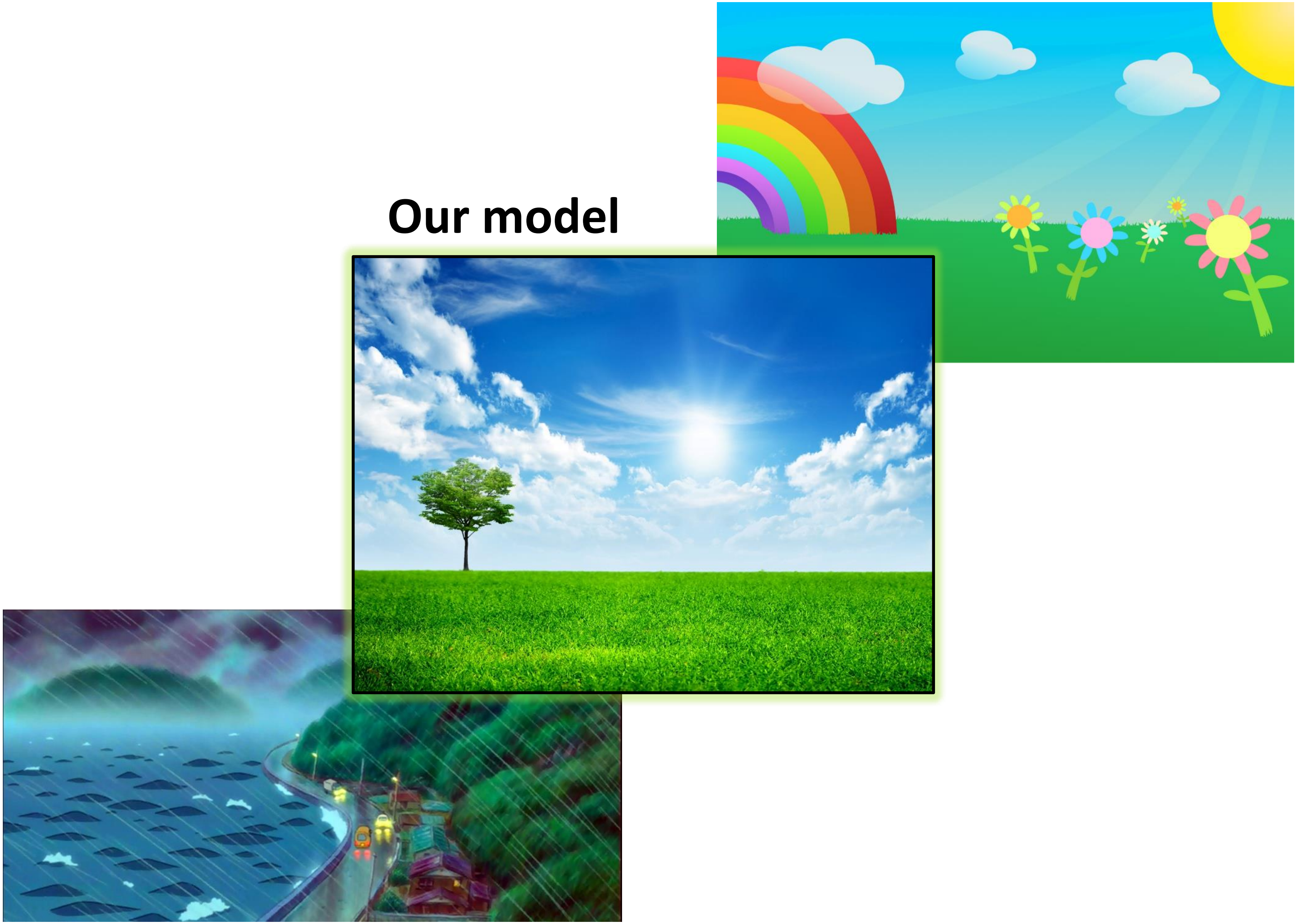
Valid ops

Invalid ops

Ideal Multilinear Maps

Multilinear Maps

Our model



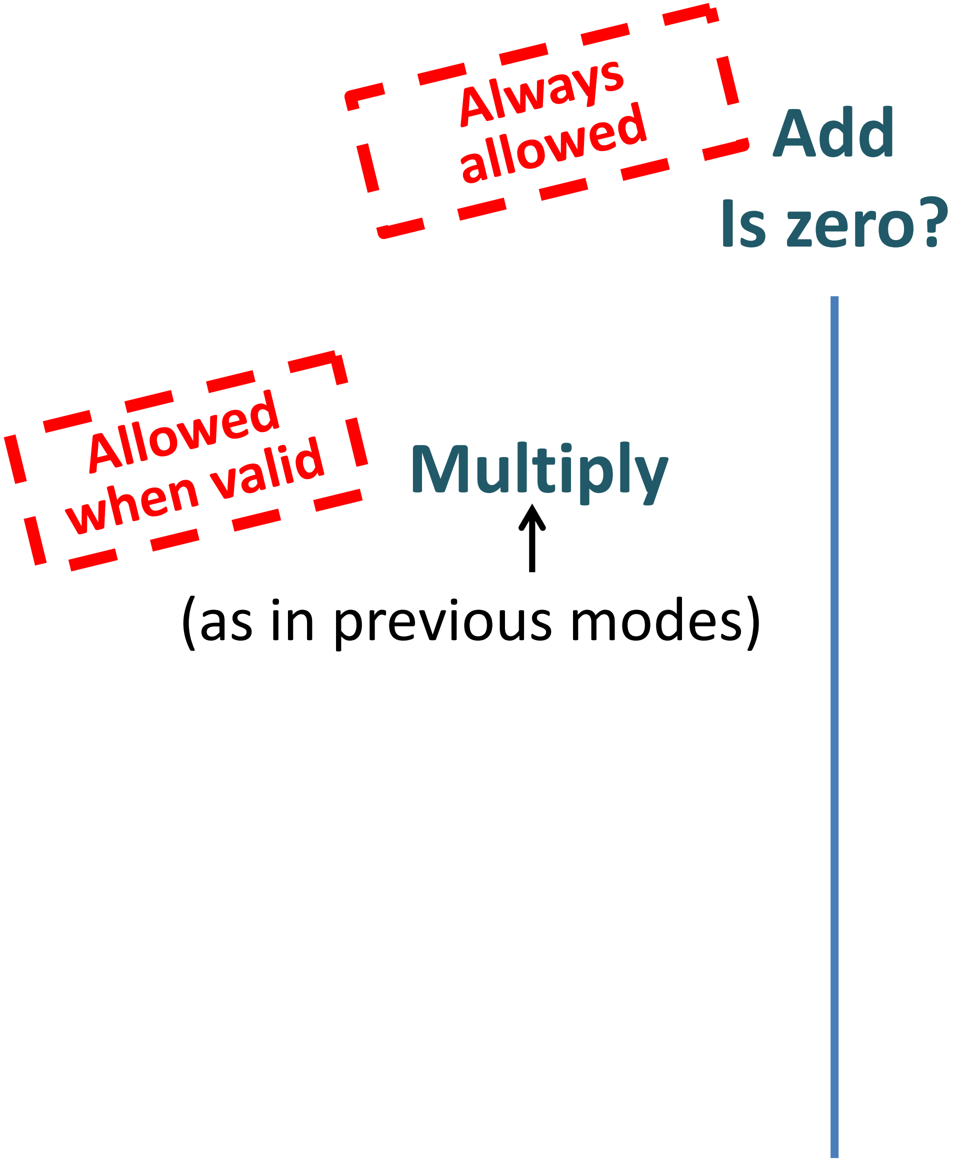
Our model

Always allowed

Add

Is zero?

Our model



Always allowed

Add

Is zero?

Allowed when valid

Multiply

↑

(as in previous modes)

Our model

Always allowed

Add

Is zero?

Allowed when valid

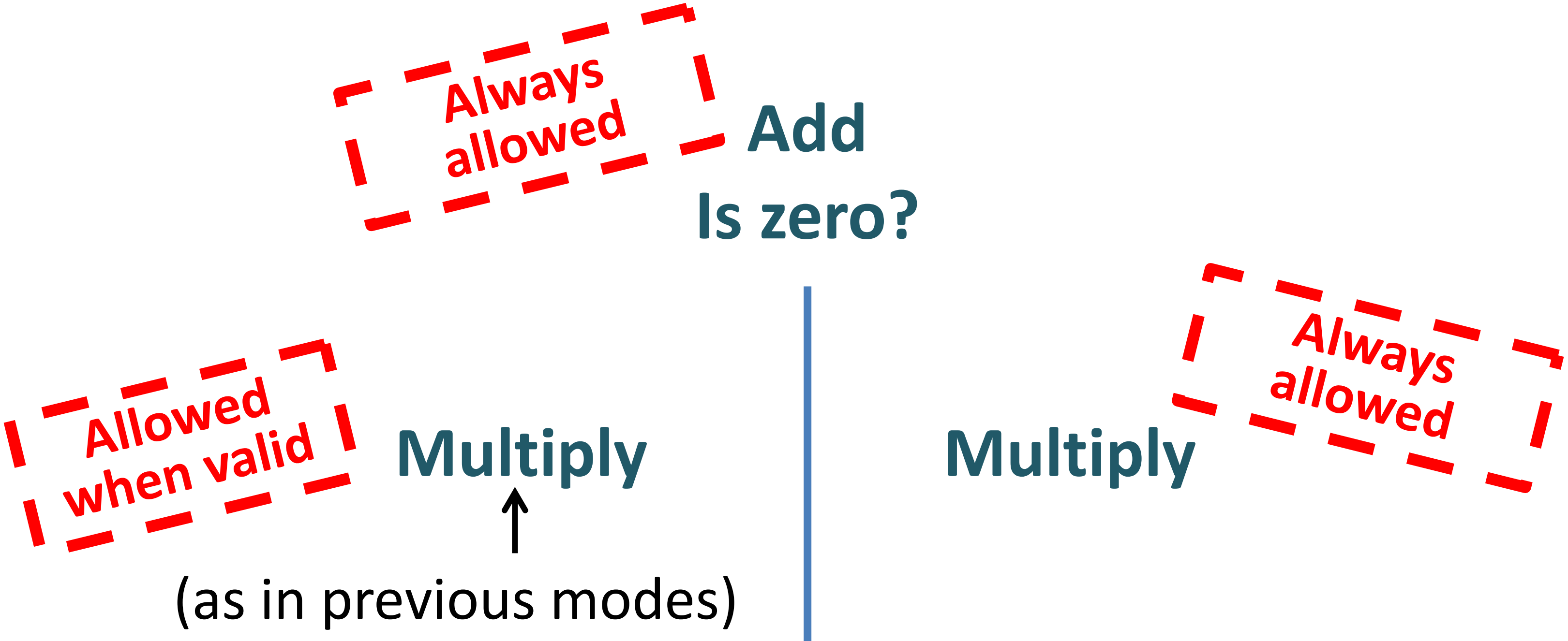
Multiply

↑

(as in previous modes)

Thm: general-purpose VBB obfuscation exists

Our model



Always allowed

Add

Is zero?

Allowed when valid

Multiply

(as in previous modes)

Multiply

Always allowed

Thm:

general-purpose VBB obfuscation exists

Our model

Always allowed

Add

Is zero?

Allowed when valid

Multiply

↑

(as in previous modes)

Thm:
general-purpose VBB obfuscation exists

Always allowed

Multiply

Thm:
Existence of general-purpose VBB obfuscation related to "algebraic P vs. NP" question

https://eprint.iacr.org/2014/878