# Cryptography with Dispensable Backdoors

Kai-Min Chung
Academia Sinica

Marios Georgiou
CUNY

Ching-Yi Lai
Academia Sinica

**Vassilis Zikas**
University of Edinburgh & IOHK

## Eurocrypt 2018 Rump Session

# Apple vs FBI

# Apple vs FBI

Backdoor your locking mechanism so that I can solve crimes

# Apple vs FBI

No

Backdoor your locking mechanism so that I can solve crimes

# Apple vs FBI

No

Backdoor your locking mechanism so that I can solve crimes

why not?

# Apple vs FBI

No

Because leakage of the backdoor allows anyone to unlock every phone. Not worth the risk

Backdoor your locking mechanism so that I can solve crimes

why not?

# Apple vs FBI

No

Because leakage of the backdoor allows anyone to unlock every phone. Not worth the risk

Backdoor your locking mechanism so that I can solve crimes

why not?


Can this be avoided?

# Apple vs FBI

I know how to do this

# Apple vs FBI

# Apple vs FBI

I know how to do this

Ha! I heard it

# Apple vs FBI

I know how to do this

Ha! I heard it

Meeau too!

And it’s the same for all phones

# Apple vs FBI

- Store all (key/phone-ID) pairs
- Upon receiving an ID, output the key and never receive another input

# Apple vs FBI

- Store all (key/phone-ID) pairs
- Upon receiving an ID, output the key and never receive another input

To lock:

- Use key to encrypt state
- Throw away key

# Apple vs FBI

- Store all (key/phone-ID) pairs
- Upon receiving an ID, output the key and never receive another input

To lock:

- Use key to encrypt state
- Throw away key

Yields:

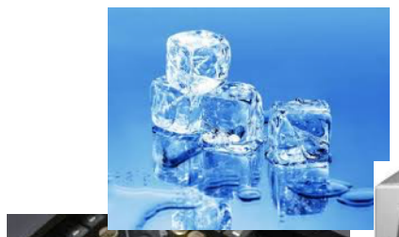
- Encryption where one out of many keys can be recovered
- Only this one! All other keys/encryptions are safe
  - *Dispensable-backdoor encryption.*

# Apple vs FBI

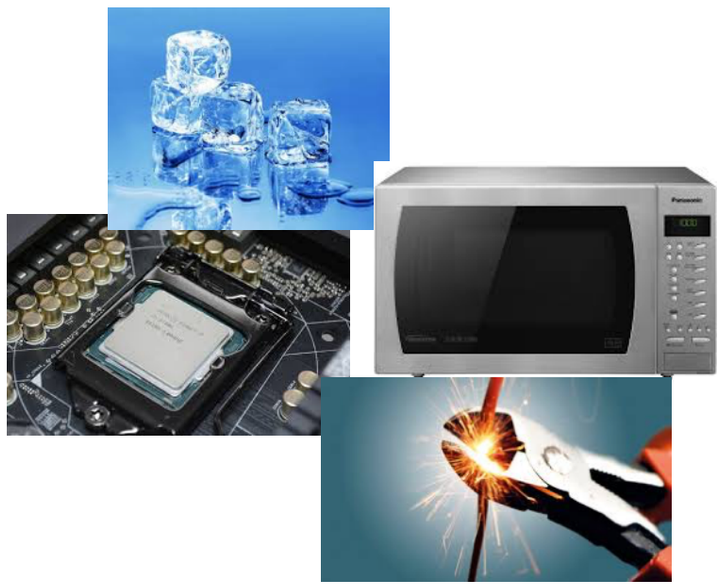
# Apple vs FBI

# Apple vs FBI

# Apple vs FBI



# Apple vs FBI



# Apple vs FBI

# Apple vs FBI

# Apple vs FBI

# Apple vs FBI

Reset the token

# Apple vs FBI

Reset the token

Can we do it from stateless tokens?

# Stateful From Stateless Token

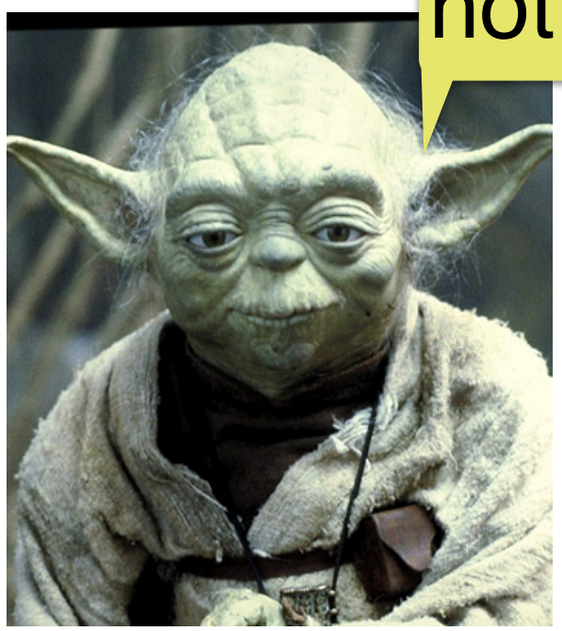
I want to create information that

- Cannot be copied/duplicated
- Can encode a lot of keys
- Once read it “self-destructs”

# Stateful From Stateless Token

I want to create information that

- Cannot be copied/duplicated
- Can encode a lot of keys
- Once read it “self-destructs”



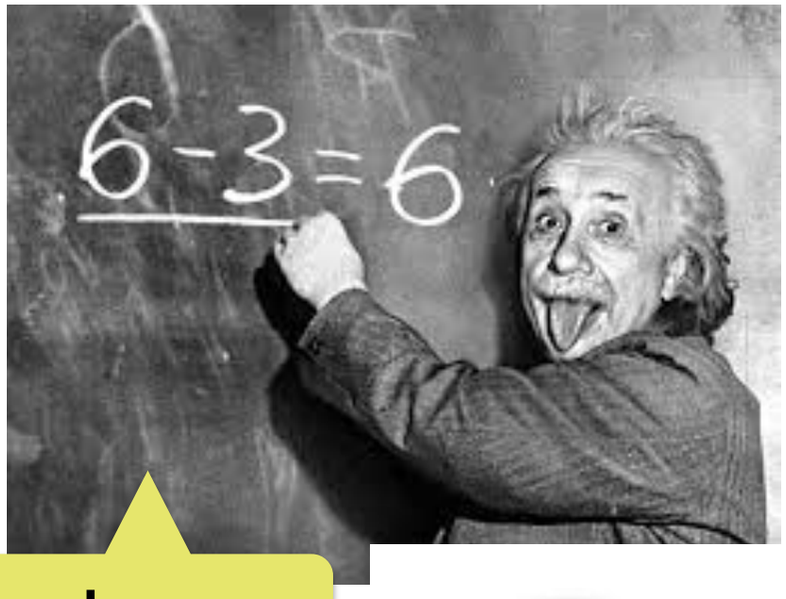
What you seek exists not in the digital world

# Stateful From Stateless Token

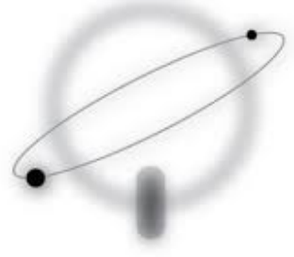
I want to create information that

- Cannot be copied/duplicated
- Can encode a lot of keys
- Once read it “self-destructs”

What you seek exists not in the digital world




I have exactly what you need!



# Cryptography with Dispensable Backdoors

https://eprint.iacr.org/2018/352.pdf

Cryptography with Dispensable Backdoors

https://eprint.iacr.org/2018/352.pdf