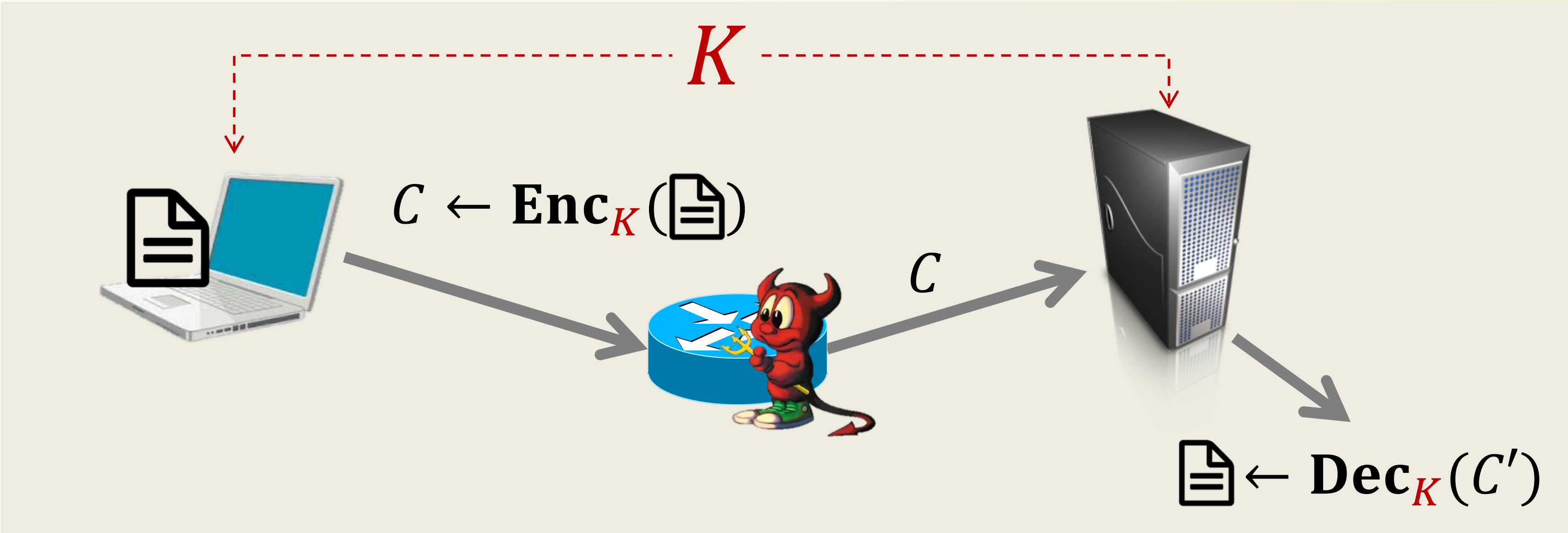
Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds

Priyanka Bose
UCSB

Viet Tung Hoang
FSU

Stefano Tessaro
UCSB

EUROCRYPT 2018

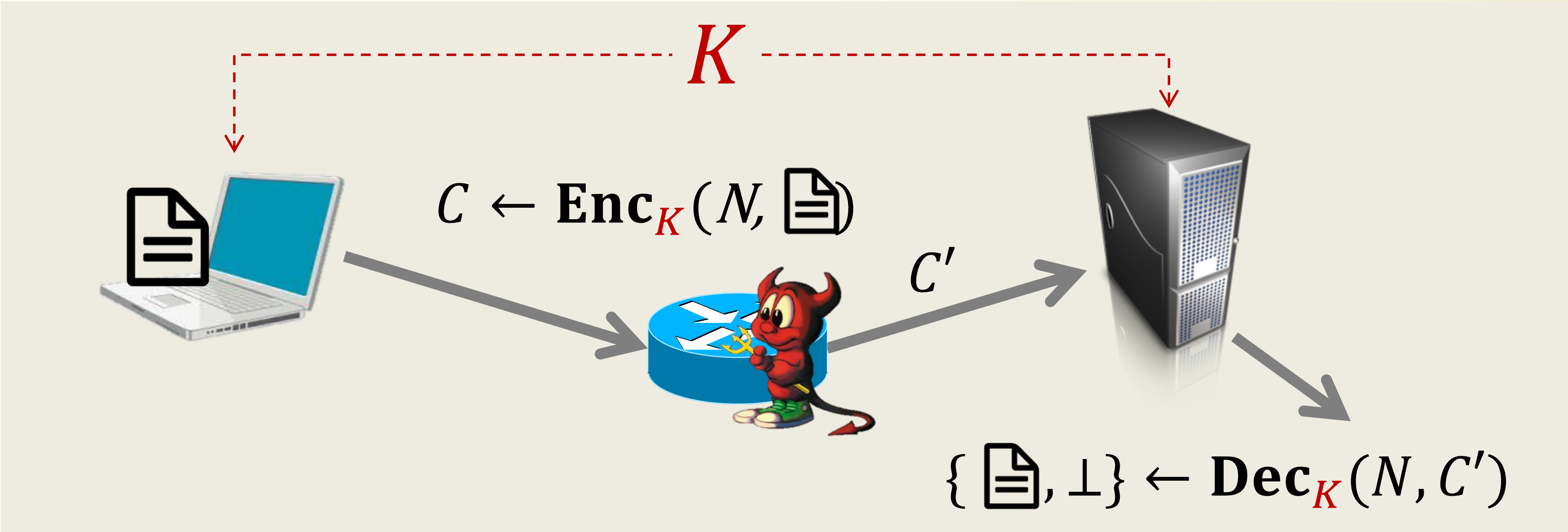


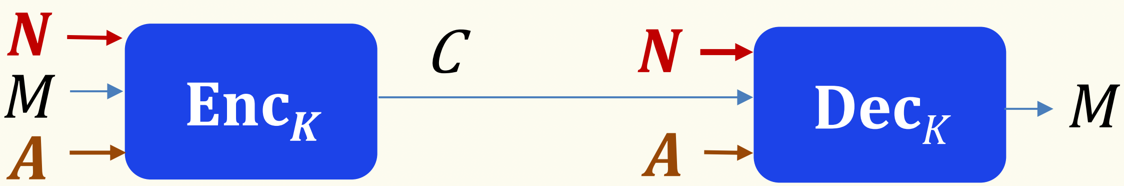
Security Goals

Confidentiality **Integrity**

Authenticated Encryption (AE) achieves *both* of these!

This talk: Multi-user security of AE





Every message encrypted with <u>distinct</u> nonce

Authenticated Encryption (AE)
(*with associated data*)

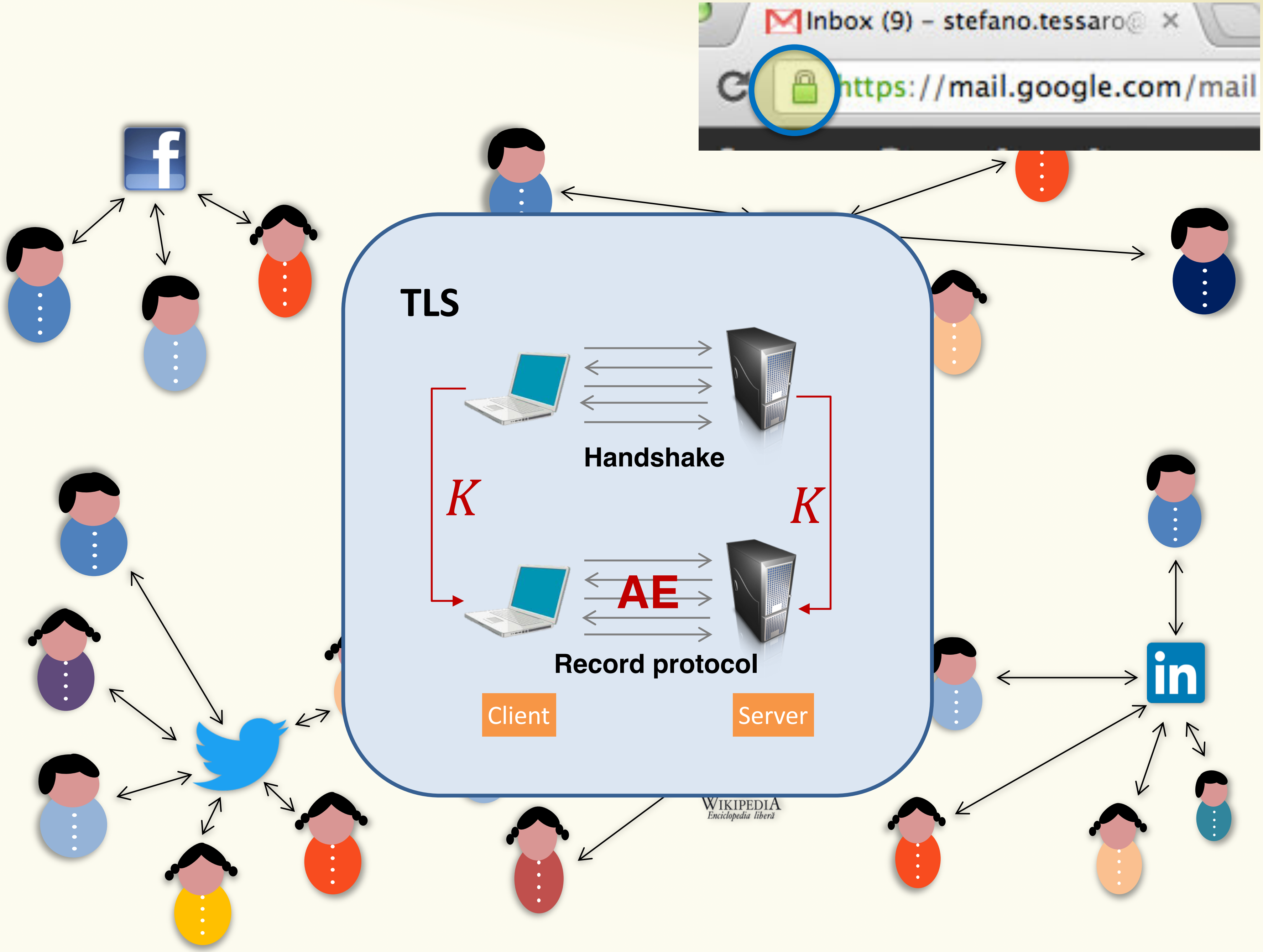
e.g. **nonce = counter**

"Conventional" AE (e.g., GCM)

Nonce repeat = total break

Nonce-misuse resistant AE (MRAE) [RS06]

Nonce repeat only leaks message equality



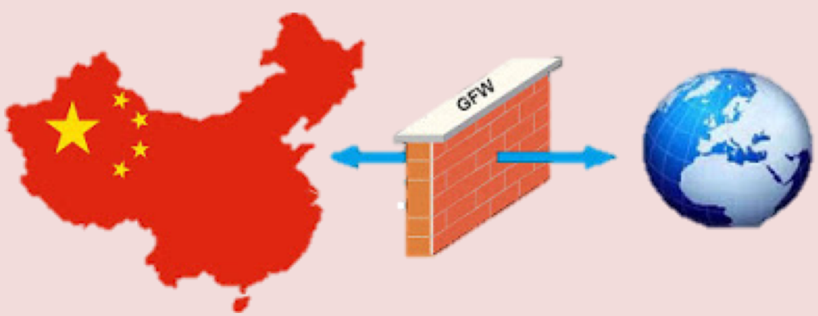
Inbox (9) - stefano.tessaro
https://mail.google.com/mail
TLS
Handshake
K
K
AE
Record protocol
Client
Server
WIKIPEDIA
Enciclopedia liberă

Powerful adversaries can collect vast amounts of Internet traffic: State actors, botnets, …

NSA's Room 641A at AT&T
~ 86 TB/day*

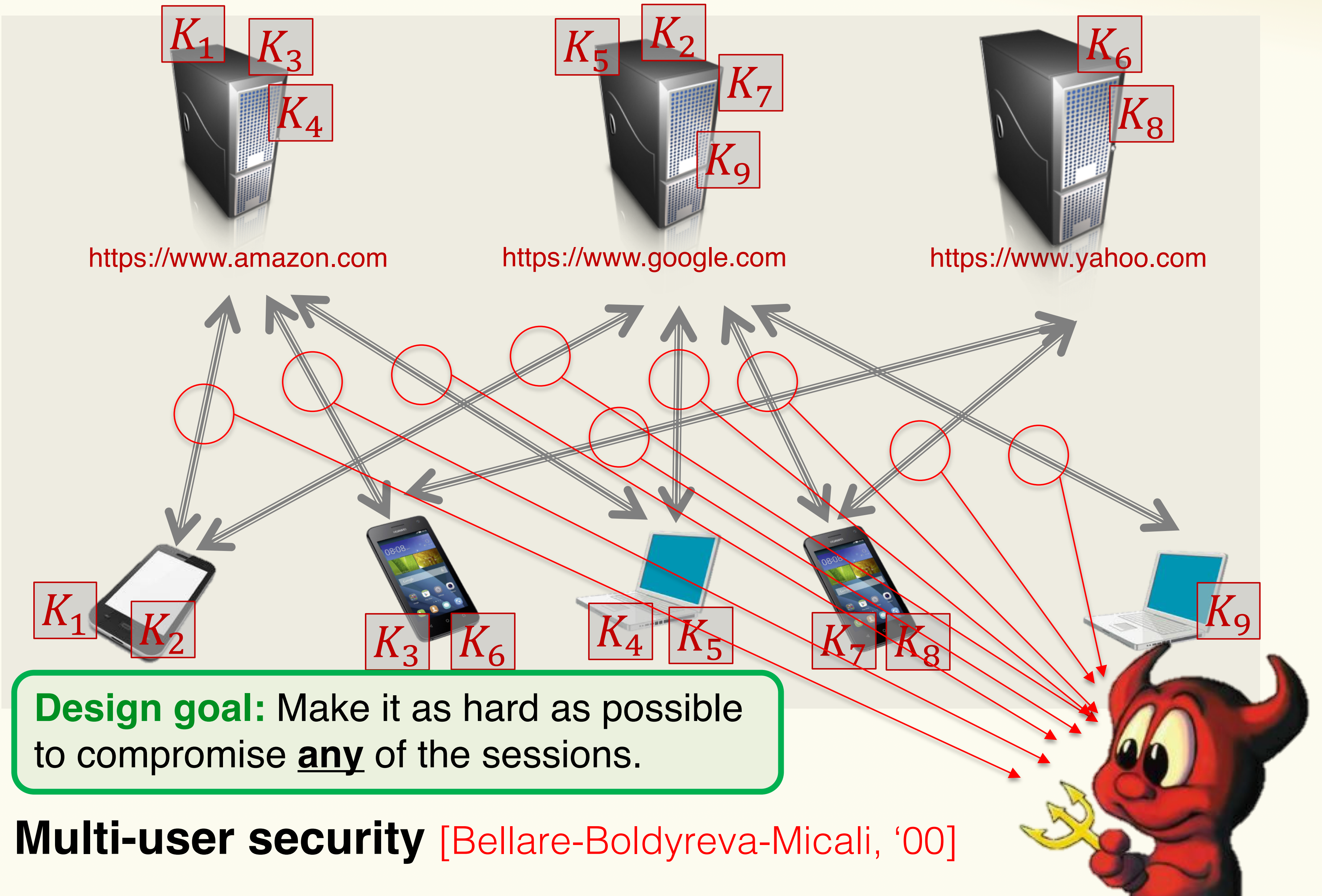
Golden Shield Project
Aka "The Great Firewall"

All Internet traffic to/from China



*http://bit-player.org/2006/room-641a

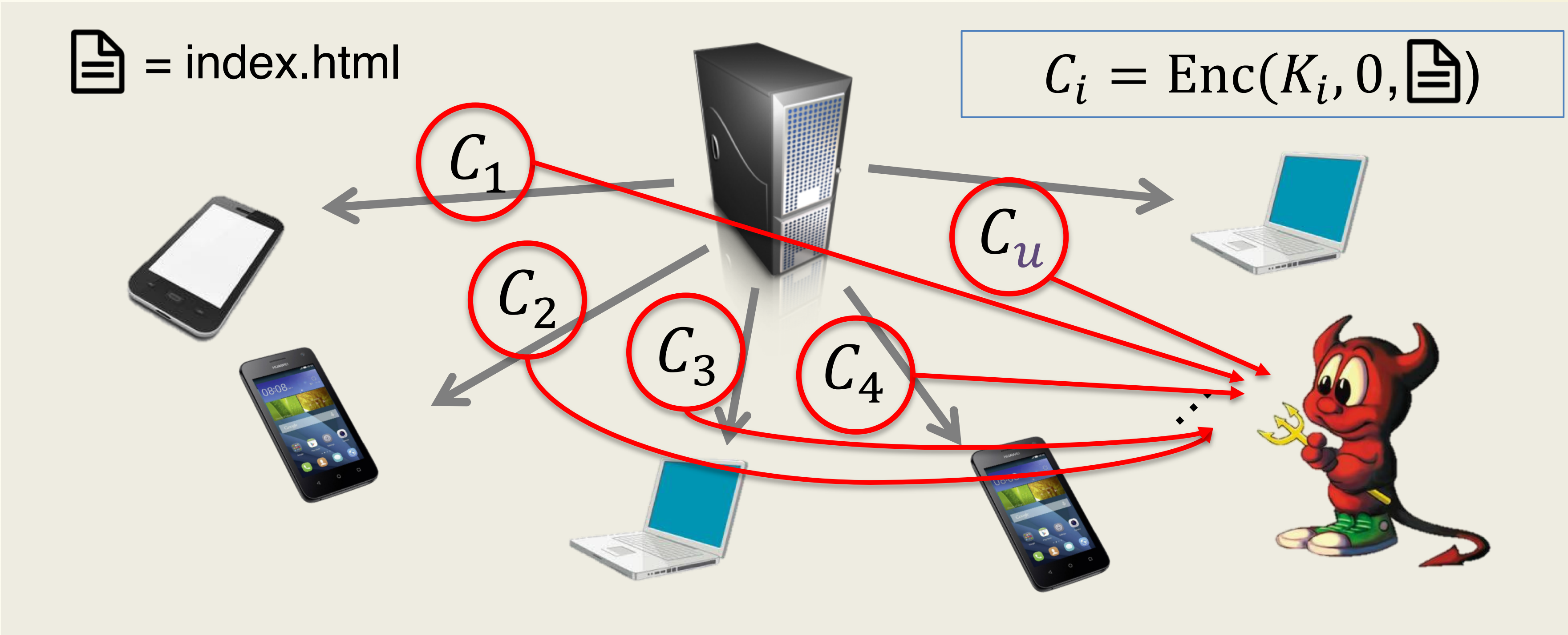
Large-scale attacks



Design goal: Make it as hard as possible to compromise **any** of the sessions.

Multi-user security [Bellare-Boldyreva-Micali, '00]

One-out-of-many **key-recovery attack** [Biham '96]



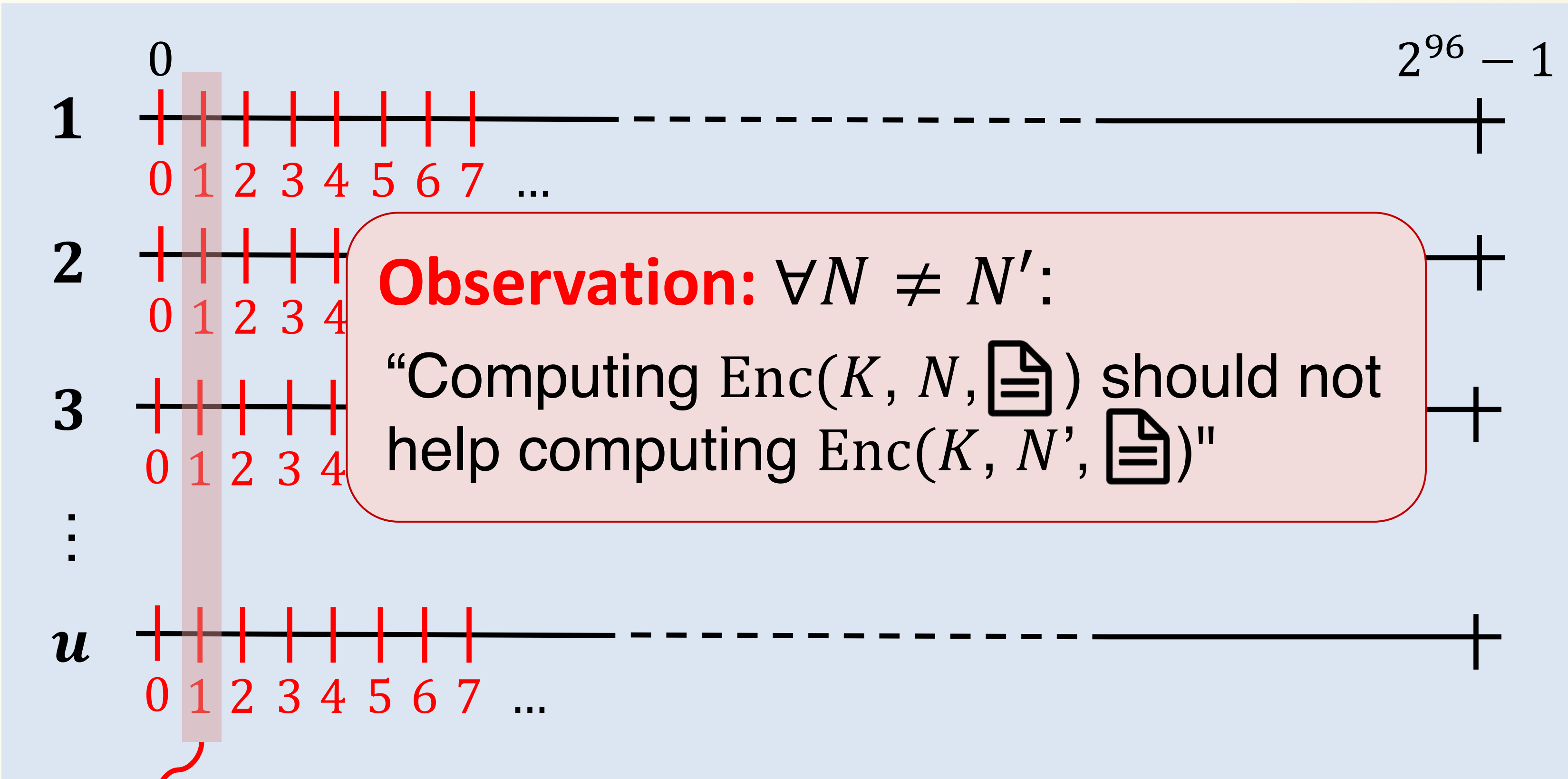
For p different K's:
Is $\mathrm{Enc}(K, 0, 🗎) \in \{C_1, \ldots, C_u\}$?

→ Advantage = $\dfrac{p \times u}{2^k}$

e.g.: $p = 2^{64}$
$k = 128$

→
- $u = 1$: Adv. $= 2^{-64}$
- $u = 2^{64}$: Adv. ≈ 1

Typical nonce choice: **Counters!** (e.g., RFC 5116)



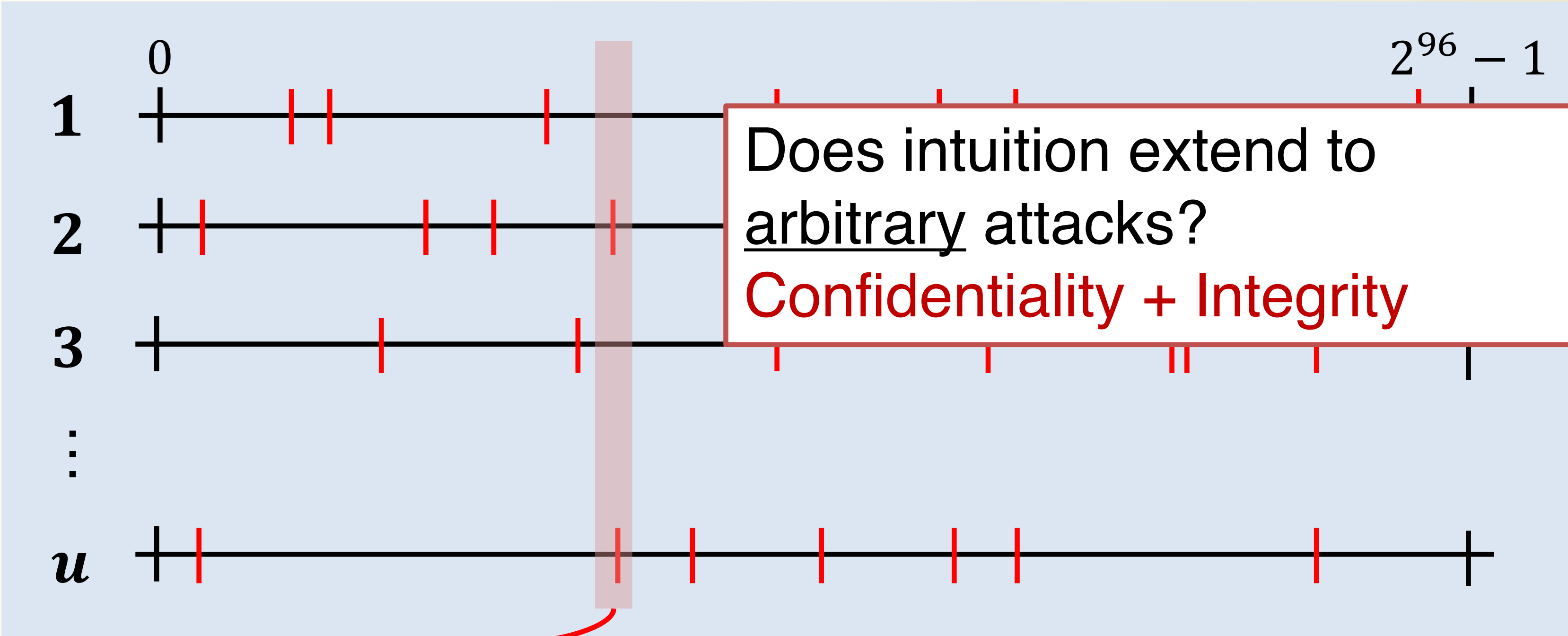
Observation: $\forall N \neq N'$:

"Computing $\mathrm{Enc}(K, N, \ )$ should not help computing $\mathrm{Enc}(K, N', \ )$"

Same nonce for all users!

For p different K's:
Is $\mathrm{Enc}(K, 1, \ ) \in \{C_1, \dots, C_u\}$?

Advantage = $\dfrac{p \times u}{2^k}$



Here: d-bounded model:
Same nonce reused by $\le d$ users when encrypting.

Advantage $= \dfrac{p \times d}{2^k}$

Random nonces $N_0, N_1, N_2, \ldots$	d = small const
Random N_0, then $N_i = N_0 + i$ e.g., RGCM (TLS 1.3) [BT16]	d = small const
Arbitrary nonces	$d = u$

Our Work

Multi-user security of AE in the d-bounded model

Here, we focus on **AES-GCM-SIV** [Gueron-Langley-Lindell, '17]

Main message: "Security degrades linearly in d"

On the way: New techniques for mu analysis of AE

- Nonce-misuse resistant AE secure beyond birthday bound
- Candidate RFC standard
- Implemented in Google's BoringSSL and QUIC
- No mu security analysis

CFRG — S. Gueron
Internet-Draft — University of Haifa and Amazon Web Services
Intended status: Informational — A. Langley
Expires: August 14, 2018 — Google
Y. Lindell
Bar Ilan University
February 10, 2018

AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption
draft-irtf-cfrg-gcmsiv-08

Abstract

This memo specifies two authenticated encryption algorithms that are nonce misuse-resistant - that is that they do not fail catastrophically if a nonce is repeated.

Status of This Memo

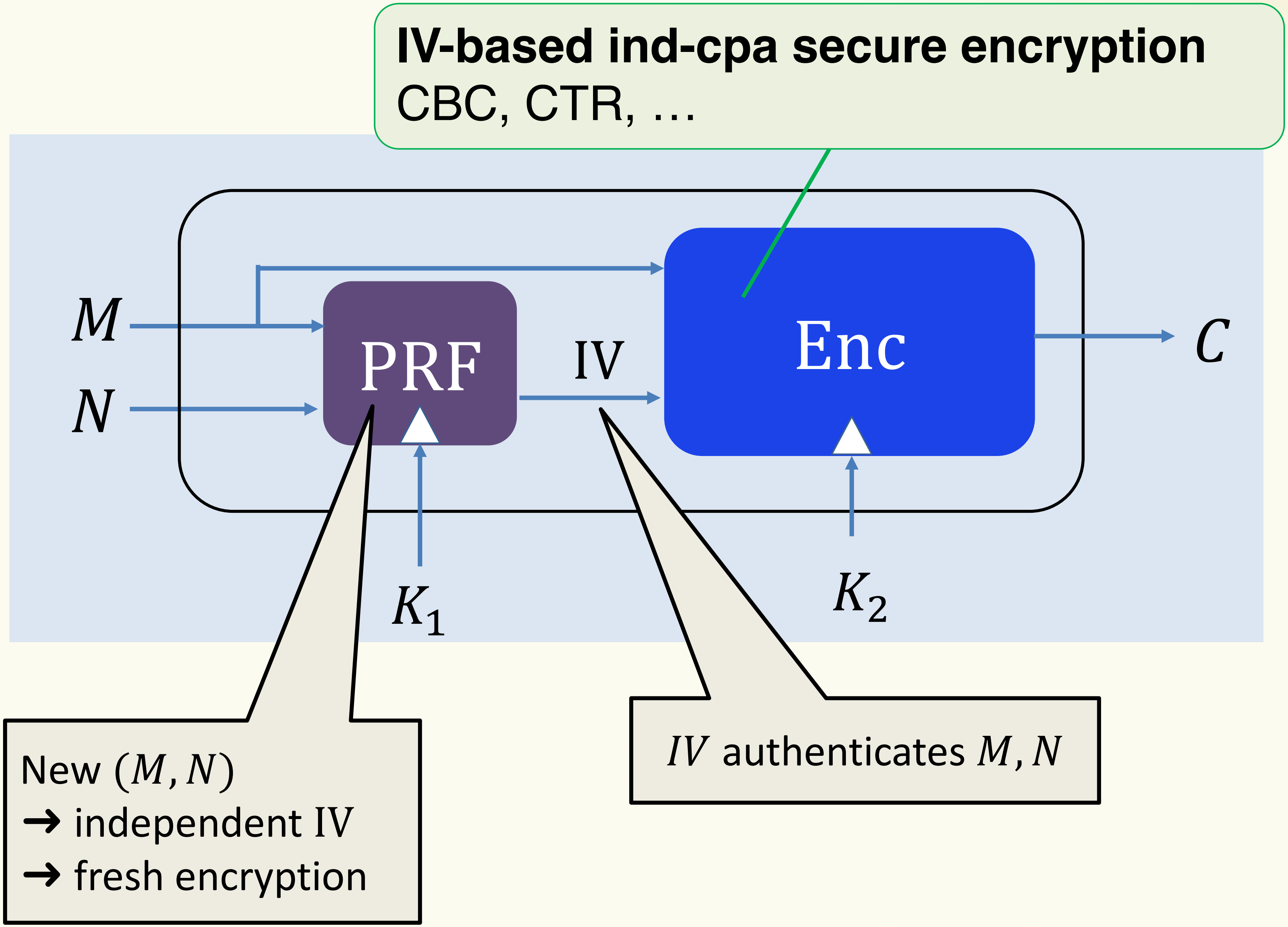
Roadmap

1. **AES-GCM-SIV: Overview & results**

2. **Proof ideas**

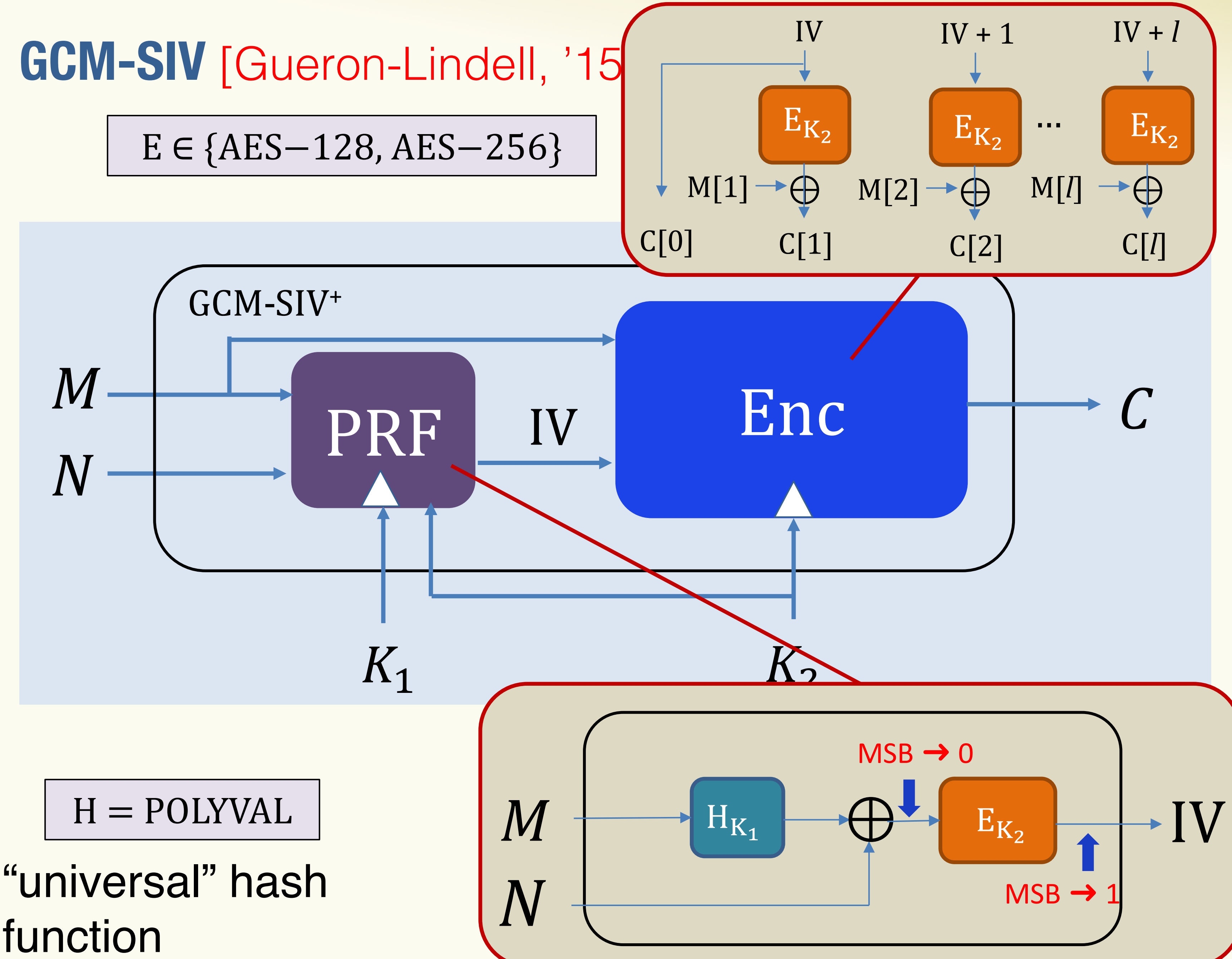
3. **Lessons learned & conclusions**

SIV mode [Rogaway-Shrimpton, '06]



GCM-SIV [Gueron-Lindell, '15

$E \in \{AES-128, AES-256\}$



$H = POLYVAL$

“universal” hash function

# of encrypted 128-bit blocks

Problem: Security of GCM-SIV is inherently affected by the <u>Birthday Bound</u> $\sim \frac{L^2}{2^{128}}$

AES-GCM-SIV [Gueron-Langley-Lindell, ’17]

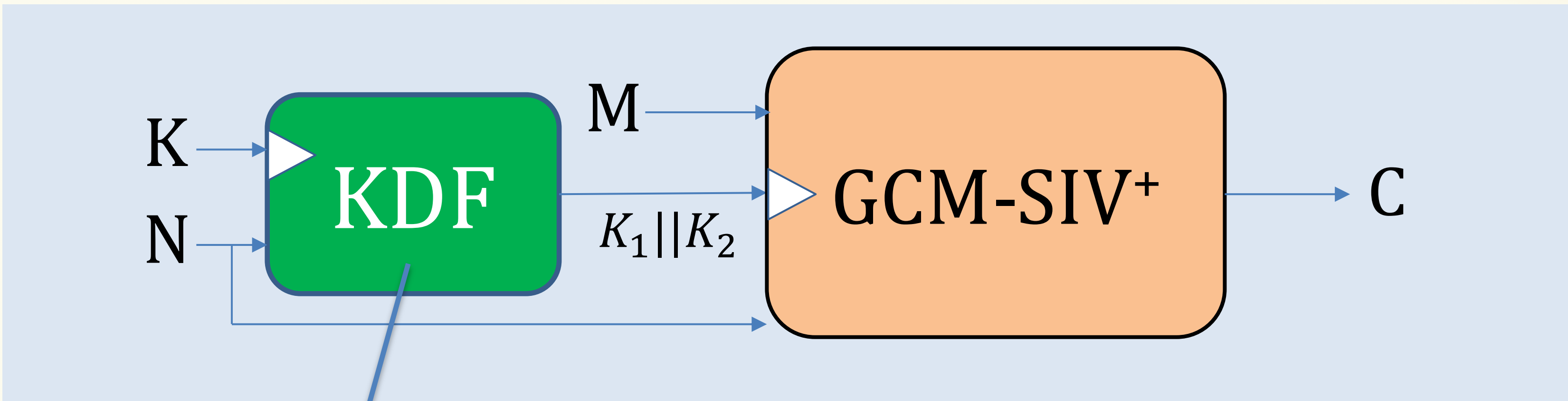
“Nonce-based key derivation”

# of encrypted 128-bit blocks <u>per nonce</u>

$= 1$ $\quad \frac{L^2}{2^{128}} \longrightarrow \frac{L \times B}{2^{128}}$ $\quad = 2^{-48}$

Example. $B = 2^{16}, L = 2^{64}$

AES-GCM-SIV

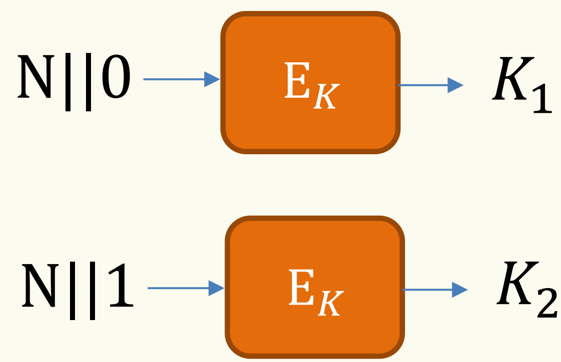


Beyond-birthday secure PRF

- Truncation based → RFC
- CENC [I06]
- XOR [BKR98, BI99, Luc00, DHT16]

[IS17]

Original proposal:



More efficient, but not a good PRF!

This work – main result

\# ideal-cipher queries

MRAE single-user Adv. $\approx \frac{L \cdot B}{2^{128}} + \frac{p}{2^k} + \frac{Q}{2^{96}}$

Truncation-based KDF

[GL17, IS17] $k \in \{128, 256\}$

\# blocks encrypted per user-nonce pair

MRAE multi-user Adv. $\approx \frac{L \cdot B}{2^{128}} + \frac{d(p+L)}{2^k}$

[This work]

General class of natural KDFs (includes original proposal)

This work – main result

Arbitrary nonces: $d = L$ → 256-bit keys

If $d \approx$ const (e.g., random nonces)
→ su security = mu security

$$\text{MRAE } \underline{\text{multi-user}} \text{ Adv.} \approx \frac{L \cdot B}{2^{128}} + \frac{d(p+L)}{2^k}$$

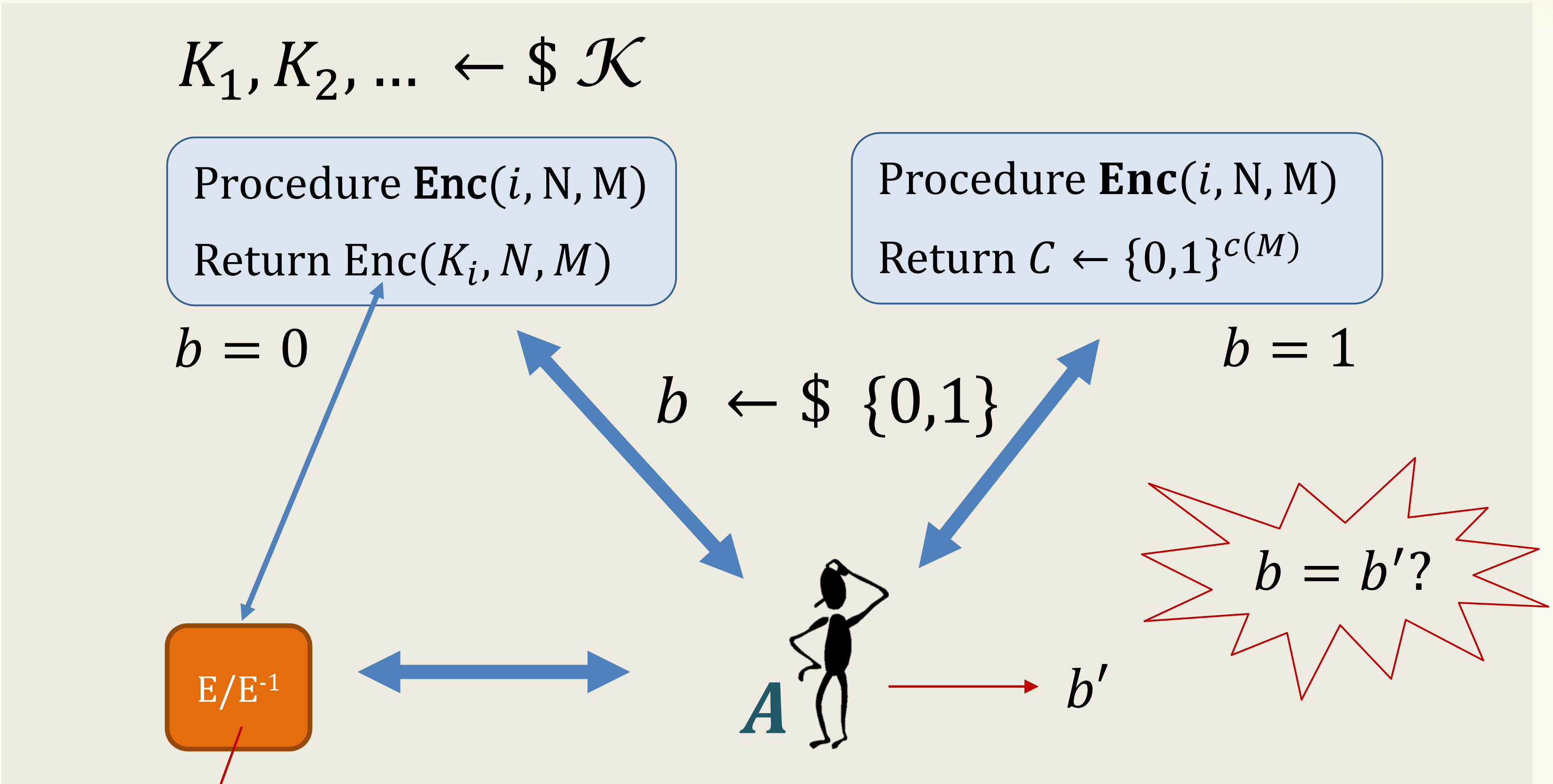
Roadmap

1. AES-GCM-SIV: Overview & results

2. <u>Proof ideas</u>

3. Lessons learned & conclusions

Modeling mu security



ideal cipher

$\forall i$ and any two queries:
$(i, N, M) \neq (i, N', M')$

MRAE security

Unless: C previously returned by $\mathbf{Enc}(i, \mathrm{N}, \mathrm{M})$

$K_1, K_2, \ldots \leftarrow \$ \ \mathcal{K}$

Procedure $\mathbf{Enc}(i, \mathrm{N}, \mathrm{M})$

Ret $\mathrm{Enc}(K_i, N, M)$

Procedure $\mathbf{Ver}(i, \mathrm{N}, \mathrm{C})$

Ret $\mathrm{Dec}(K_i, N, C) \neq \perp$

$b = 0$

Procedure $\mathbf{Enc}(i, \mathrm{N}, \mathrm{M})$

Ret $C \leftarrow \{0,1\}^{c(M)}$

Procedure $\mathbf{Ver}(i, \mathrm{N}, \mathrm{C})$

Ret False

$b = 1$

$$\mathrm{Adv}_{AE}^{\mathrm{mu-mrae}}(\boldsymbol{A}) = 2 \times (\Pr[b = b'] - \tfrac{1}{2})$$

$b = b'$?

E/E-1

$\boldsymbol{A}$

b'

The proof

Makes p ideal-cipher queries

We show: $\mathrm{Adv}^{\mathrm{mu-mrae}}_{\mathrm{AES\text{-}GCM\text{-}SIV}}(\boldsymbol{A}) \leq \frac{L \cdot B}{2^{128}} + \frac{d(p+L)}{2^k}$

Encrypts + verifies $\leq L$ blocks

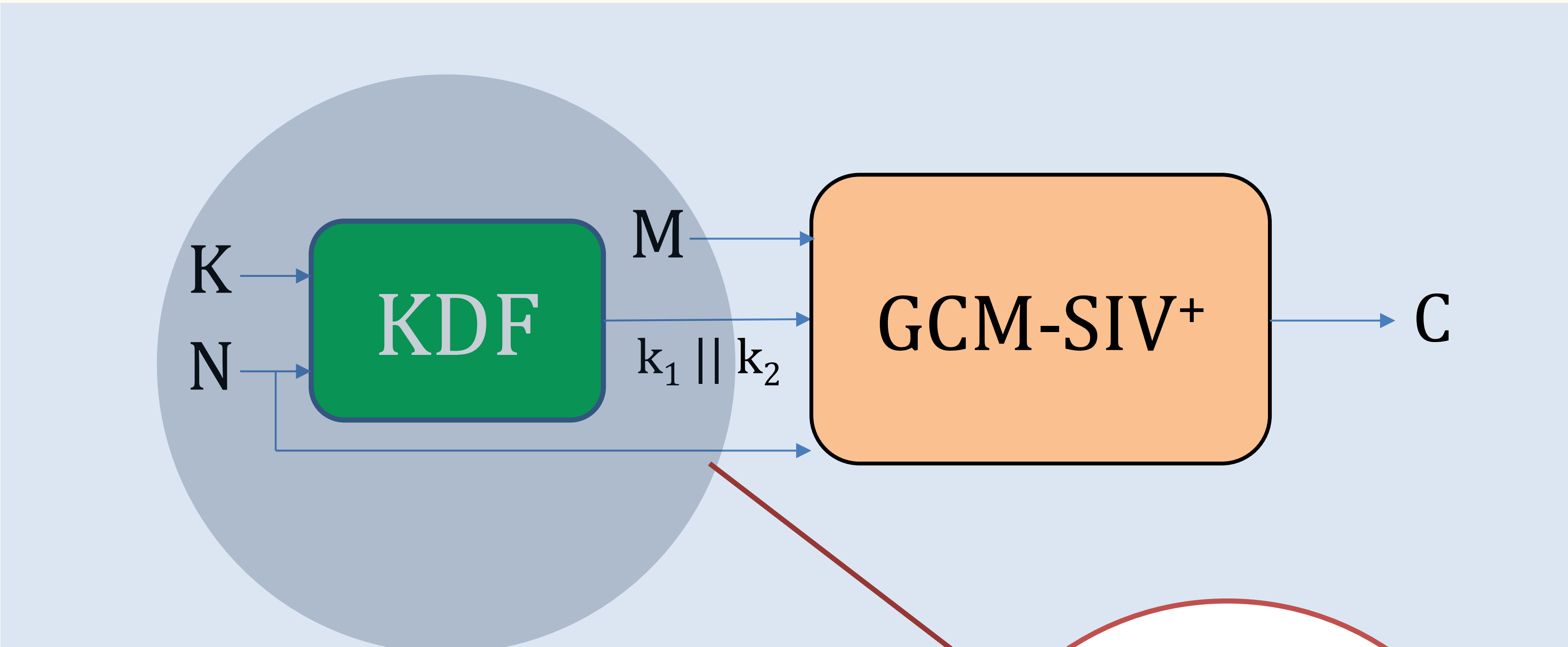
B blocks per nonce-user pair

d-bounded encryption queries

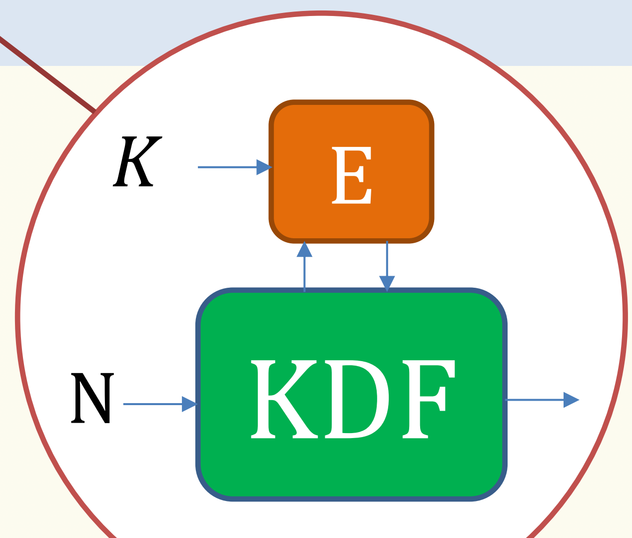
Major challenge: Nonce can be re-used across <u>unbounded</u> number of users in verification queries!

Here: Simplifying assumption: Every nonce re-used by $\leq d$ users in verification queries!

Reminder – AES-GCM-SIV

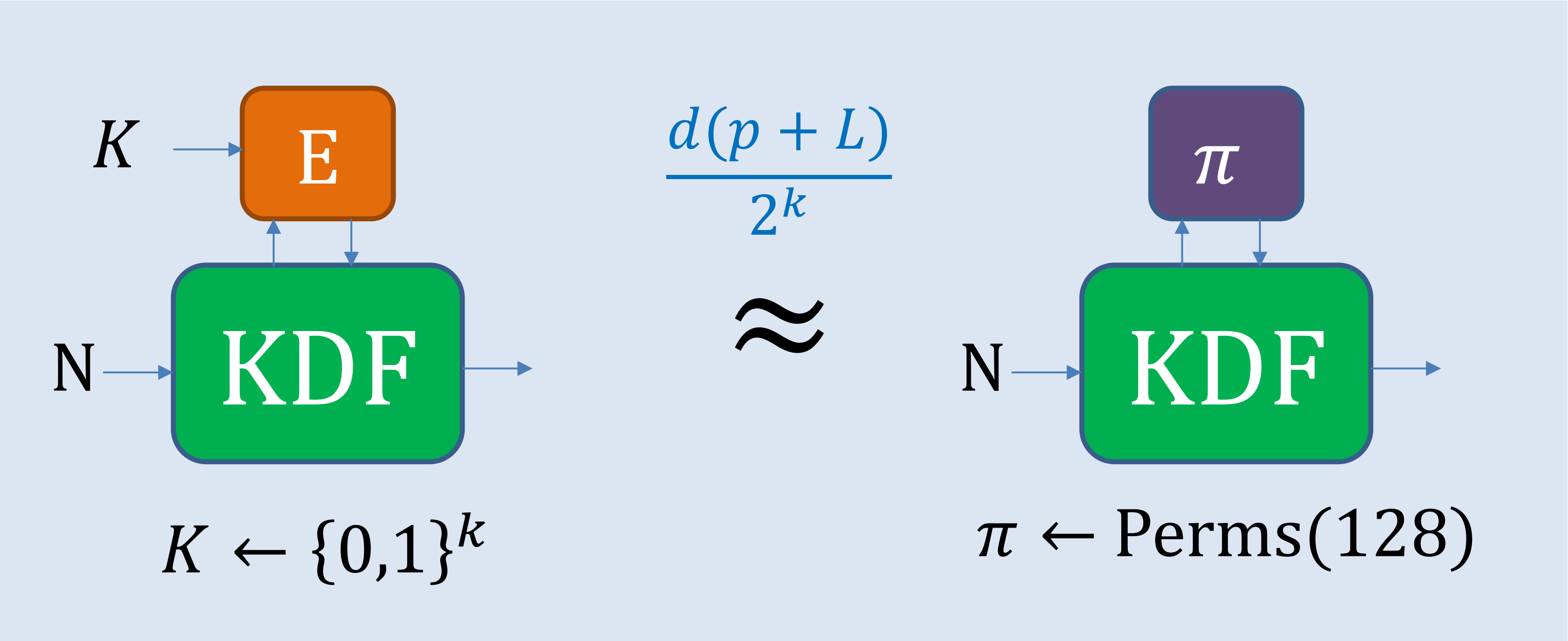


<u>block-cipher based</u> KDFs



Step 1 – Ideal KDFs

“Ideal KDF”

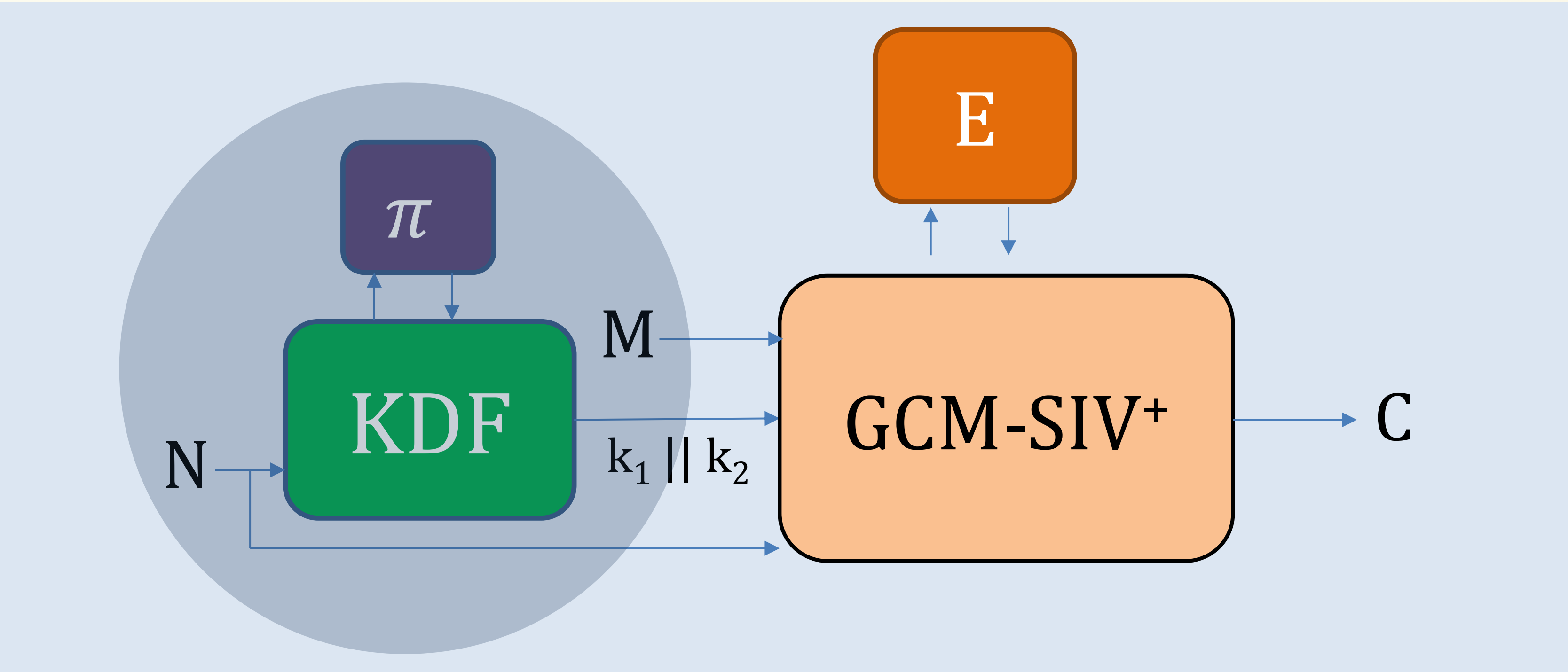


Good KDFs: Ideal KDF produces keys that are (almost) pairwise independent.

$\neq$ **random function**

Step 2 – Ideal AES-GCM-SIV

$(N, i) \rightarrow k_1 \mid\mid k_2$



Mu analysis of GCM-SIV$^+$

- (almost) pairwise independent keys
- $\leq B$ blocks/user

Mu analysis of AES-GCM-SIV

- ideal KDF
- $\leq B$ blocks/(nonce, user)

Roadmap

1. AES-GCM-SIV: Overview & results

2. Proof ideas

3. Lessons learned & conclusions

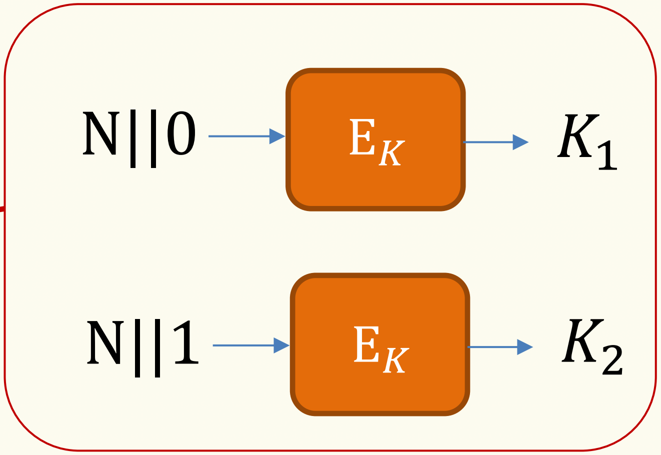
Lessons learned – It's all about the nonces!

- **Random nonces better than counters**
  - mu security = su security
- **Nonces not random → use 256-bit keys**

(AES-)GCM-SIV – Better than advertised!

Refined proof techniques + ideal-cipher model.

- **Tighter bounds** even for su security.
- **More efficient KDFs.**



Minor point: mu security of stand-alone $\mathrm{GCM{-}SIV}^{+}$ **weaker than ideal:**

- $\mathrm{POLYVAL}(K, \varepsilon) = 0^{128}$ for all K.
- Easy to fix through better padding.

Beyond AES-GCM-SIV – General lessons

- d-bounded model.
- Nonce-based key derivation in the mu setting.
- Analysis of integrity in the mu setting.
- First analysis giving guarantees beyond key collisions.

Thank you!

https://eprint.iacr.org/2018/136