Authenticated Encryption (AE)

Part 1: 14:00 –15:00
Part 2: 15:00 – 16:00

Phillip Rogaway
University of California, Davis, USA

Kind thanks to the organizers of this lovely summer school for the invitation to come talk.

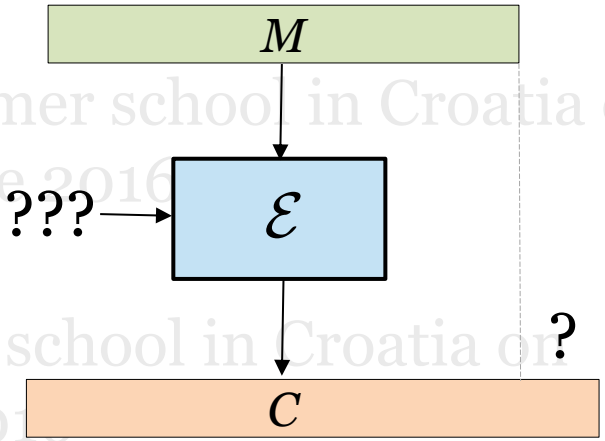
Today:
Definitions and **techniques** for AE

1. **pE** – prob enc achieving semantic security
2. **pAE** – prob AE
3. **nAE**– nonce-based AE with associated data (AEAD)
4. **MRAE** – misuse-resistant AE
5. **RAE** – robust AE

Summer school on Real-World Crypto and Privacy

Tuesday, 7 Jun 2016
Šibenik, Croatia

Symmetric encryption scheme



1. What **security notion** should a symmetric encryption scheme aim to satisfy?

This **is** a pragmatic question

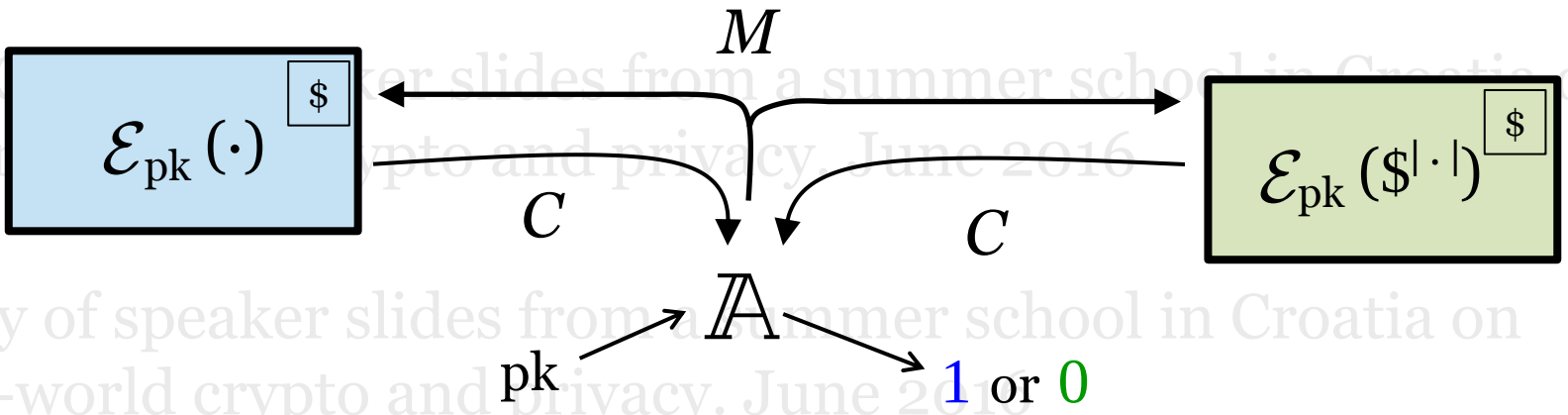
2. How can we **make** efficient schemes we believe to satisfy our chosen notion?

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Secure asymmetric encryption: IND-CPA

Classical view

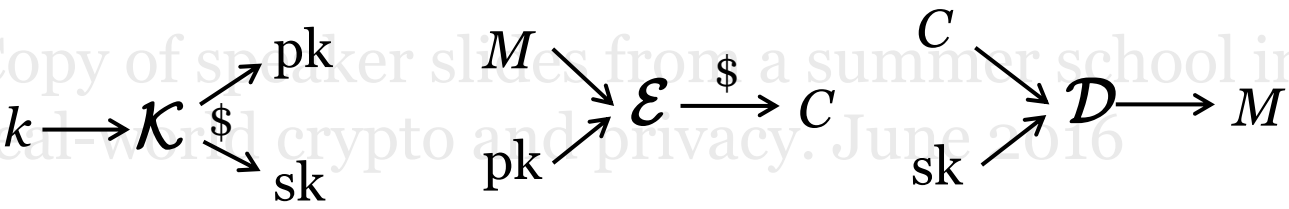
[Goldwasser-Micali 1982]



$$\mathbf{Adv}^{\text{PRIV}}_{\Pi}(\mathbb{A}, k) = \Pr[\mathbb{A}^{\text{Real}}(\text{pk}) \rightarrow 1] \quad - \quad \Pr[\mathbb{A}^{\text{Fake}}(\text{pk}) \rightarrow 1]$$

$\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
a probabilistic
public-key encryption scheme

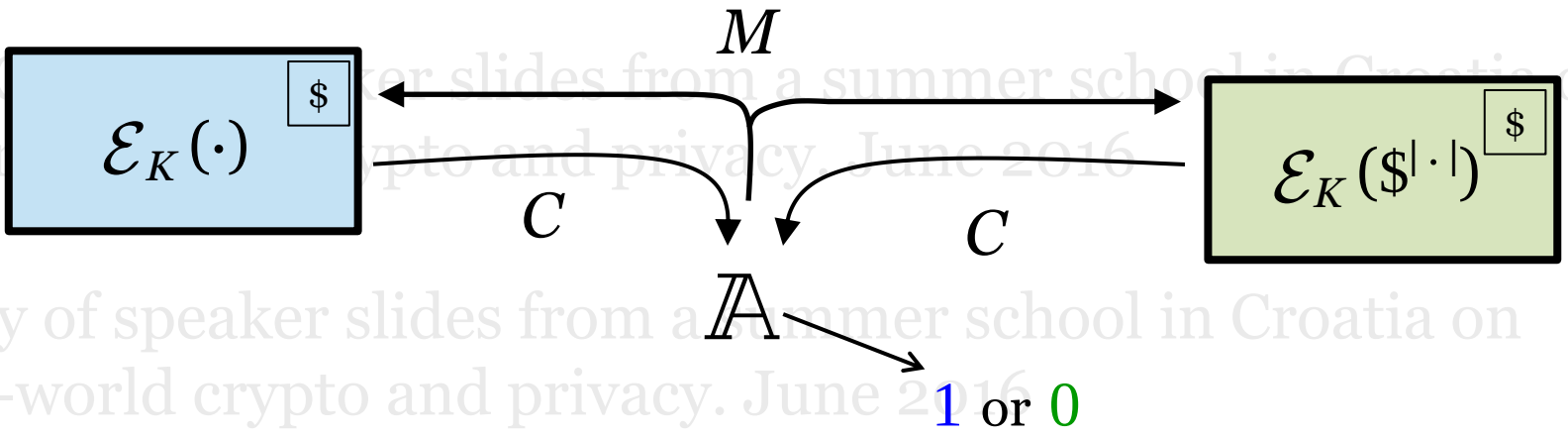
A public-key encryption scheme Π is **secure** if for all **PPT** $\mathbb{A}$, the advantage above is **negligible**.



Secure symmetric encryption: pE

Classical view

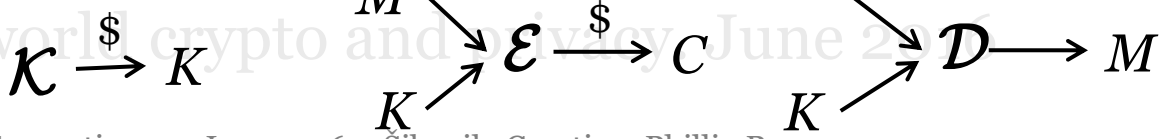
[Bellare-Desai-Jokippi-Rogaway 1997]
Following [GM82]



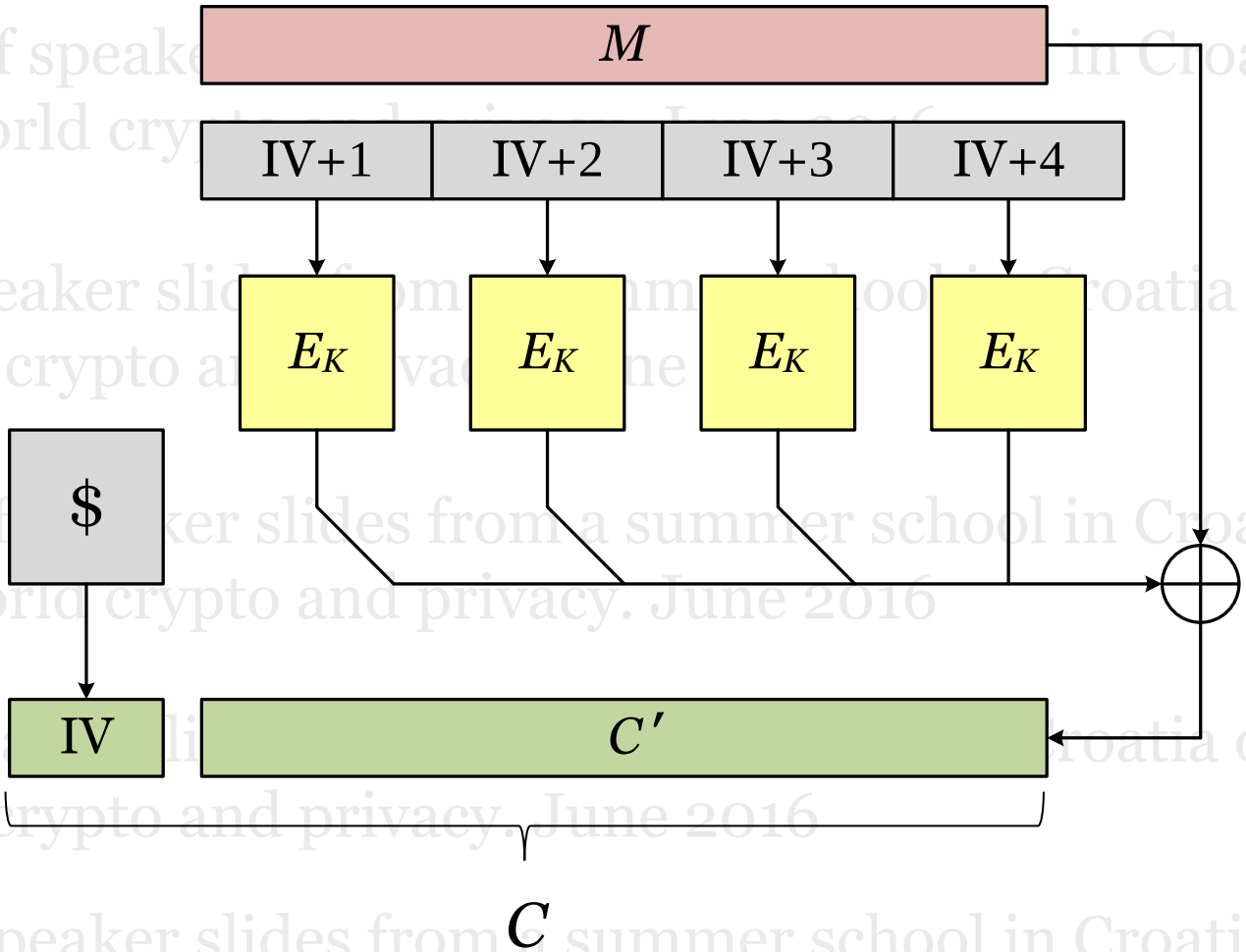
$$\mathbf{Adv}^{\mathrm{pE}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathrm{Real}} \to 1] \quad - \quad \Pr[\mathbb{A}^{\mathrm{Fake}} \to 1]$$

~~A symmetric encryption scheme Π is **secure** if for all **PPT** $\mathbb{A}$, the advantage above is **negligible**.~~

$\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
a probabilistic
symmetric encryption scheme



Achieving pE: CTR$



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

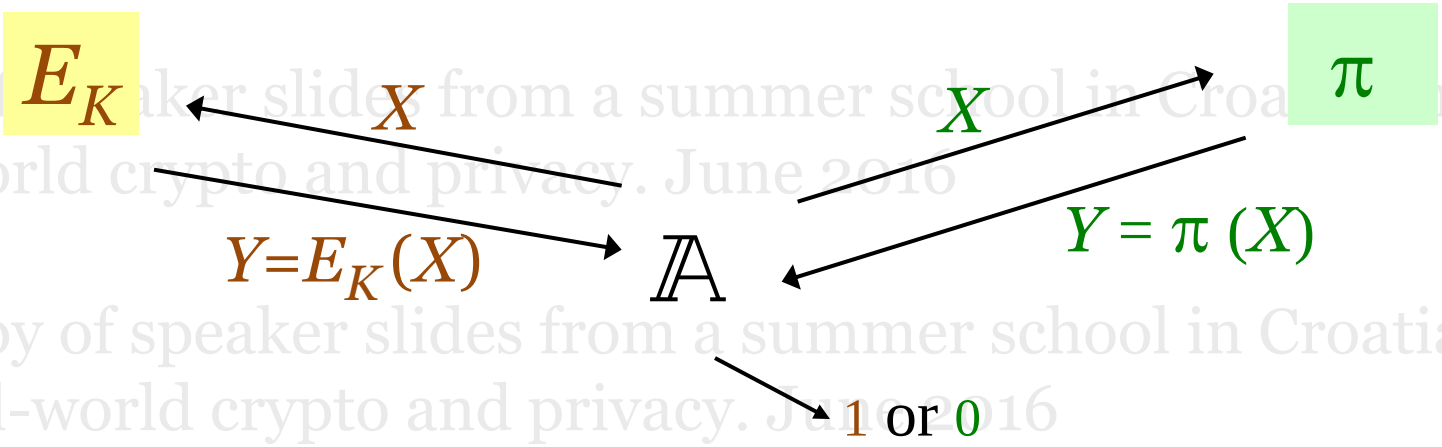
Formalizing Blockciphers

[GGM84,LR95,BKR04]

$E: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$

each $E_K(\cdot) = E(K, \cdot)$ a **permutation**

A random permutation on n bits

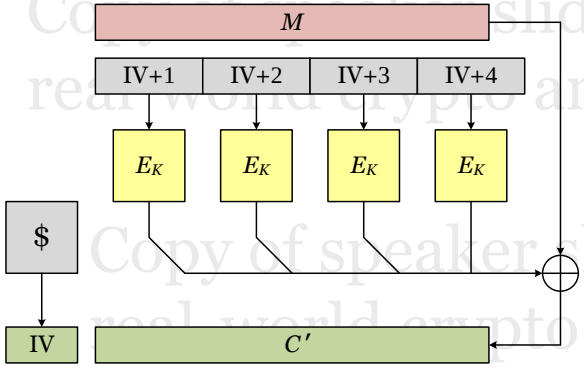


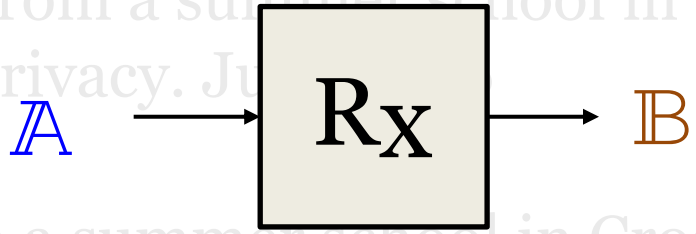
$$\mathbf{Adv}^{\text{prp}}_{E}(\mathbb{A}) = \Pr[\mathbb{A}^{E_K} \Rightarrow 1] - \Pr[\mathbb{A}^{\pi} \Rightarrow 1]$$

$$\mathbf{Adv}^{\pm\text{prp}}_{E}(\mathbb{A}) = \Pr[\mathbb{A}^{E_K, E_K^{-1}} \Rightarrow 1] - \Pr[\mathbb{A}^{\pi, \pi^{-1}} \Rightarrow 1]$$

[Bellare-Desai-Jokippi-Rogaway 1997]

Security of CTR$





Adversary attacking CTR$[$E$]

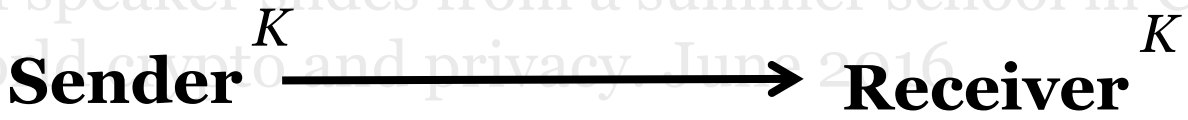
Breaks it with advantage δ *in the pE-sense*

Adversary attacking E

Breaks it with advantage $f($*Resources*, $\delta)$ *in the PRP-sense*

Thm. There exists a reduction Rx with the following property.
Let $E\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher and let $\mathbb{A}$ be an adversary using σ blocks attacking Π = CTR$[$E$]$ with pE-advantage δ.
Then $\mathbb{B}$ = Rx $(\mathbb{A}, E)$ breaks E with PRP-advantage $\geq \delta - \sigma^2\, 2^{-n}$
using resources comparable to $\mathbb{A}$'s.

Traditional view of shared-key cryptography
(until ~2000)



Privacy
(confidentiality)

Authenticity
(data-origin authentication)

Encryption scheme

Authenticated Encryption
Achieve both of these aims

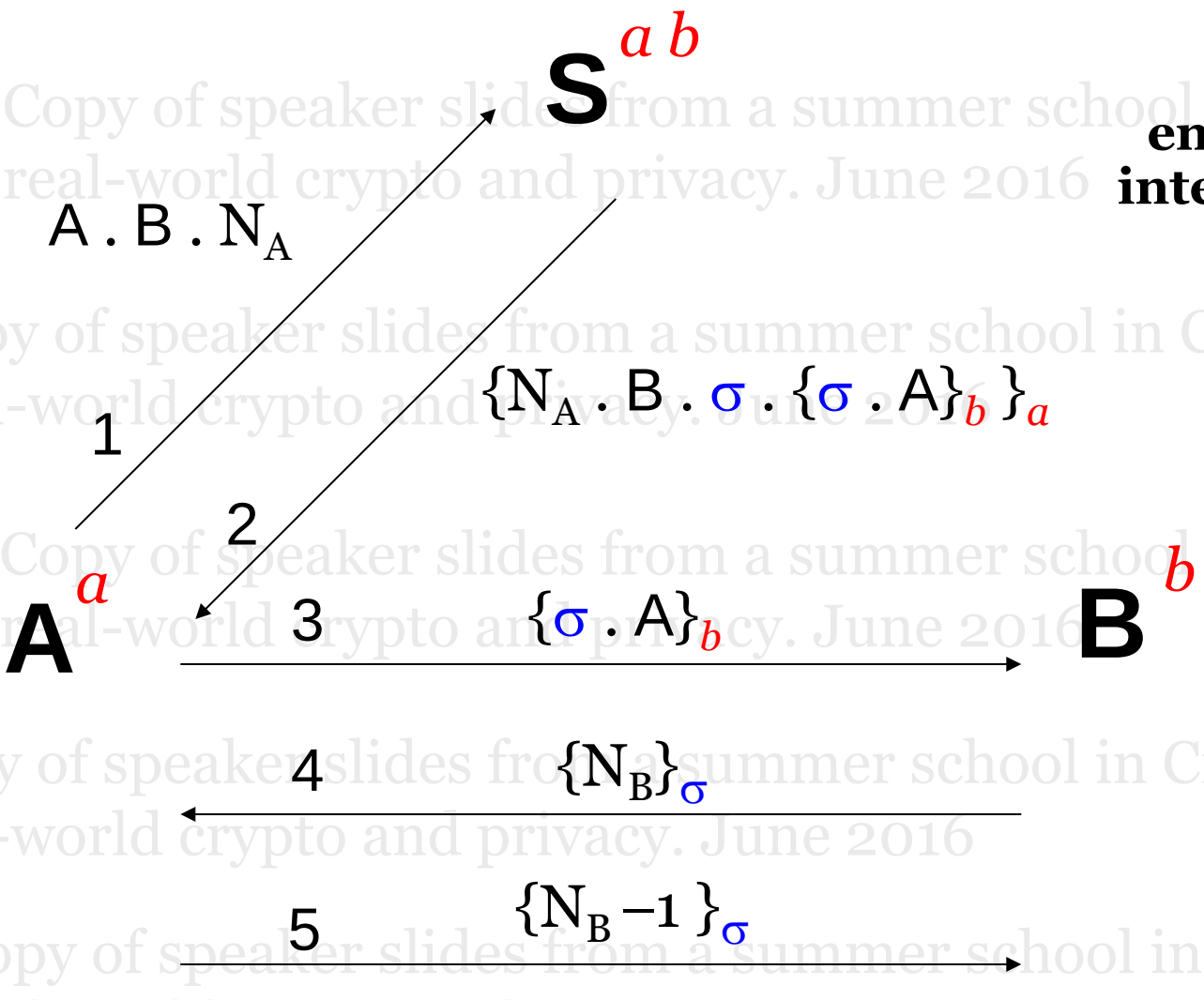
Message Authentication Code (MAC)

IND-CPA
[Goldwasser, Micali 1982]
[Bellare, Desai, Jokipii, R 1997]

Existential-unforgeability under ACMA
[Goldwasser, Micali, Rivest 1984/1988],
[Bellare, Kilian, R 1994], [Bellare, Guerin, R 1995]

Needham-Schroeder Protocol (1978)
Attacked by Denning-Saco (1981)

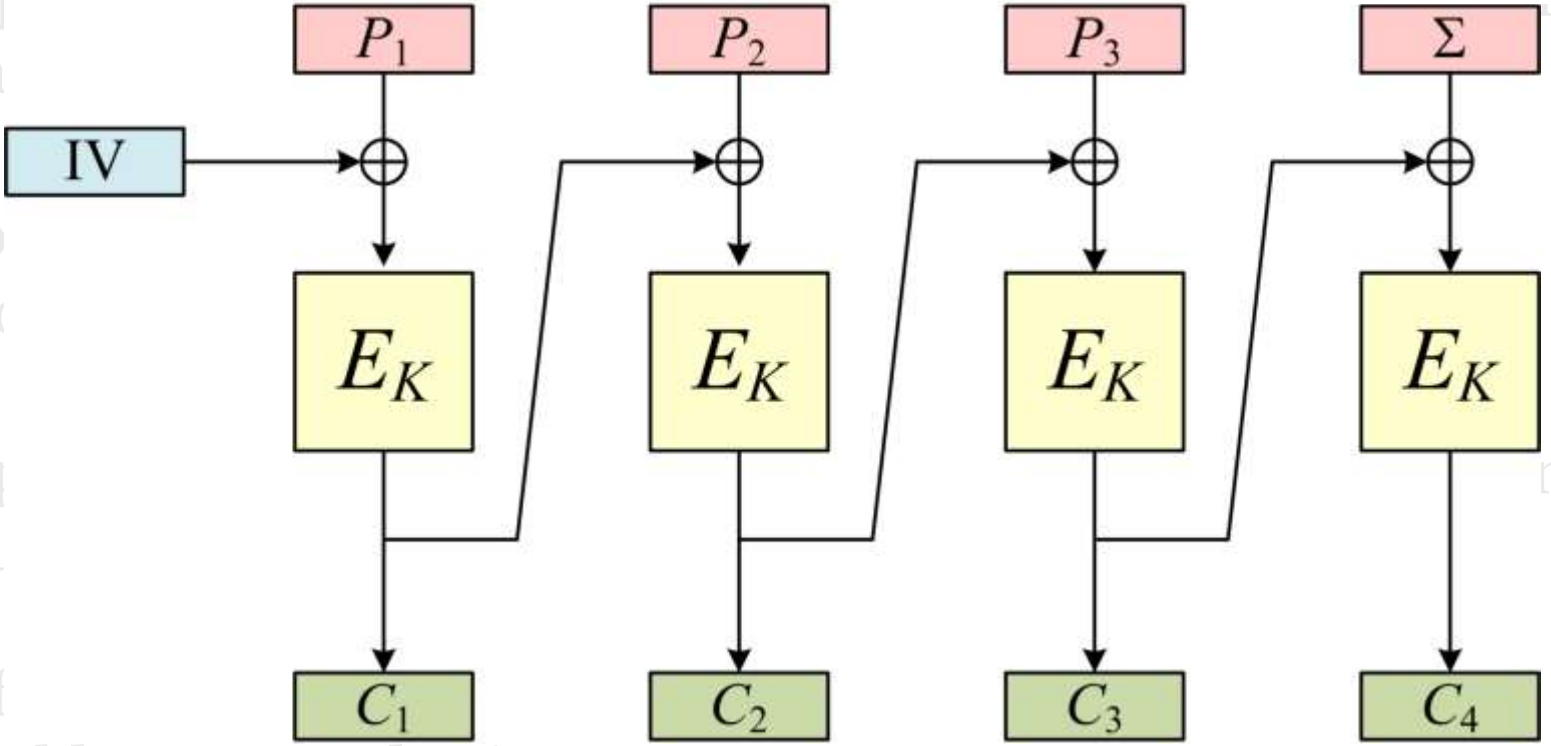
Practioners never saw ind-cpa as encryption's intended goal



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Trying to get cheap authenticity

CBC
with redundancy
~ 1980



Doesn't work

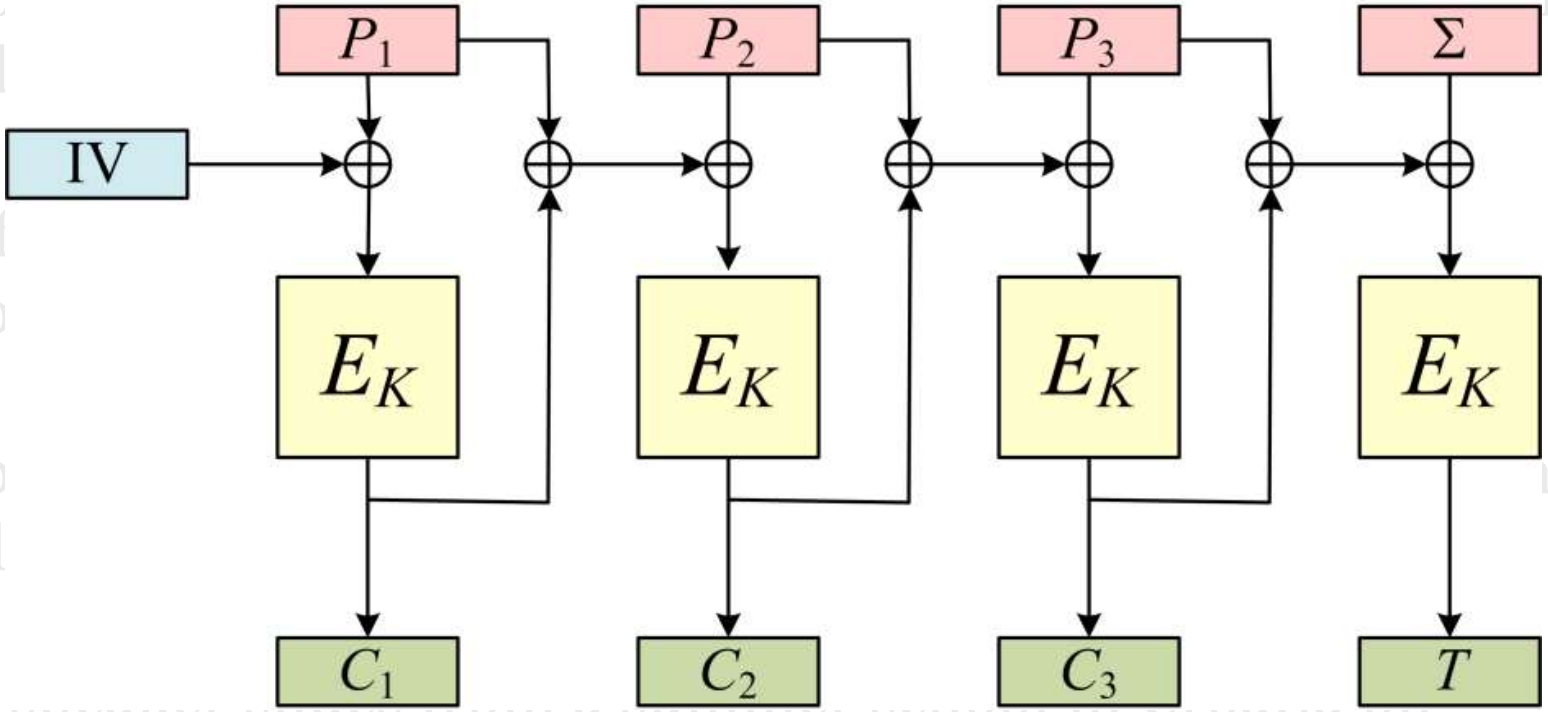
regardless of how you compute the (unkeyed) checksum $\Sigma = R(P_1, \ldots, P_n)$ (Wagner)

Unkeyed checksums don't work even with IND-CCA or NM-CPA sym enc schemes [An, Bellare 2001]

Kerberos' attempt

PCBC

≤ 1982



Doesn't work

See **[Yu, Hartman, Raeburn 2004]**

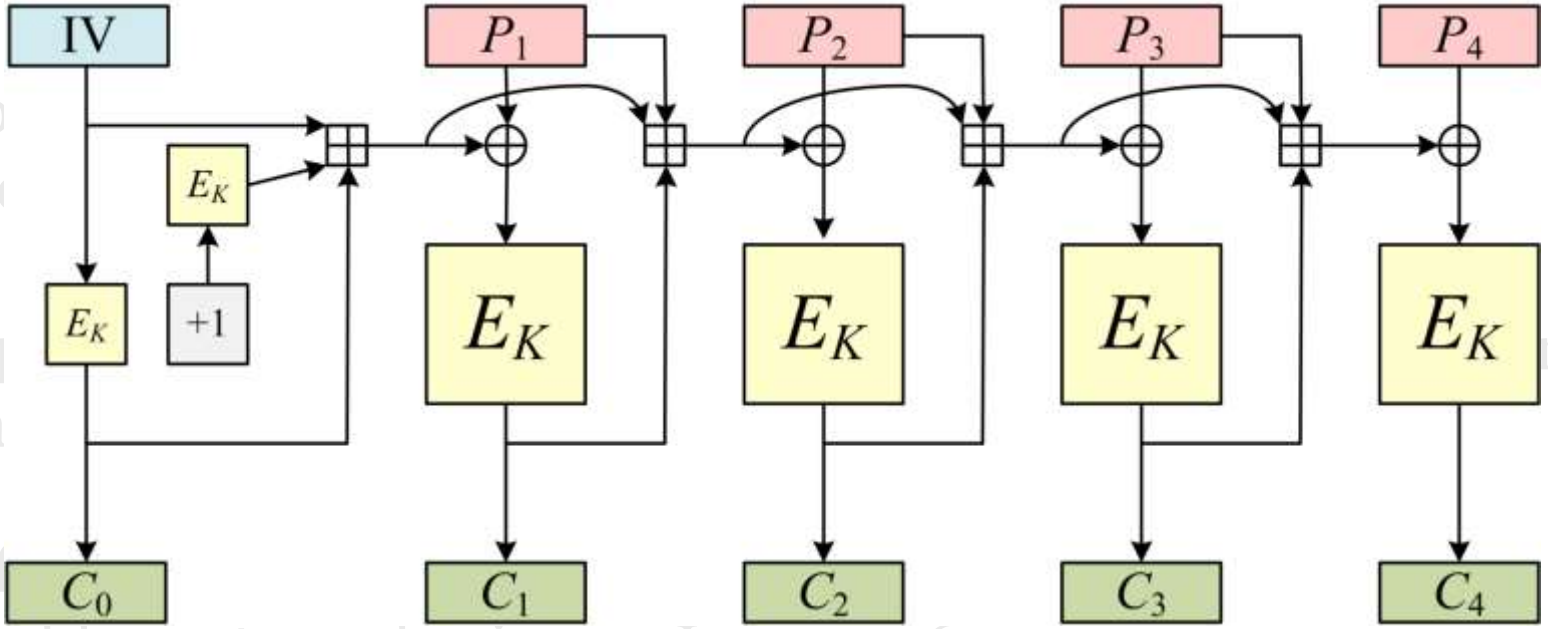
The Perils of Unauthenticated Encryption: Kerberos Version 4

for real-world attacks

Maybe we need more arrows

iaPCBC

[Gligor, Donescu 1999]



Doesn't work

Promptly broken by Jutla (1999)
& Ferguson, Whiting, Kelsey, Wagner (1999)

By 2000:

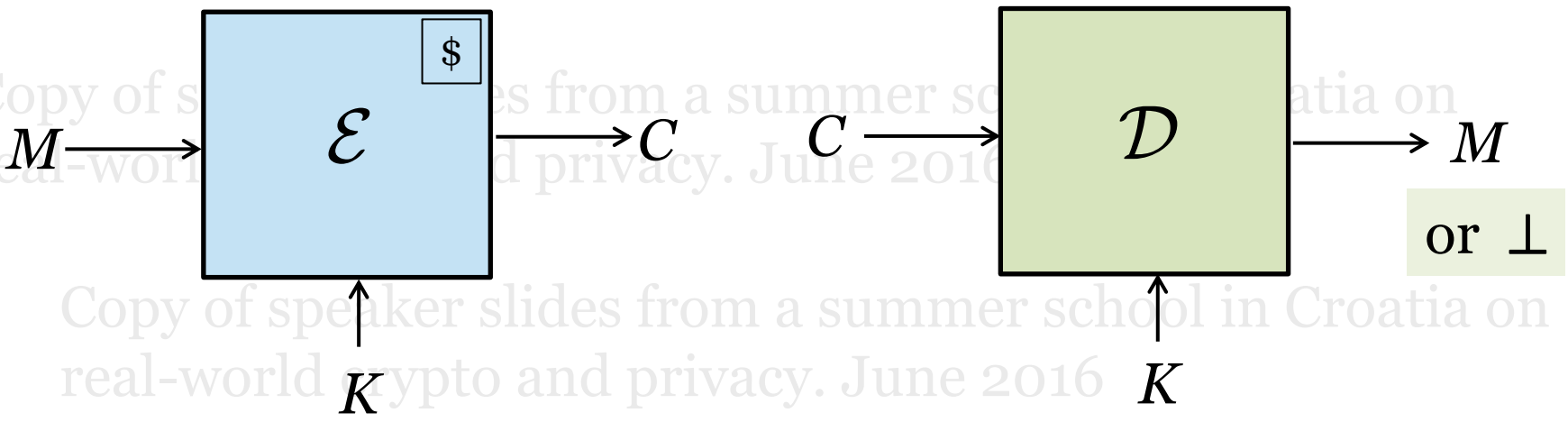
- It was clear that there was a **disconnect** in the way theory and practical people saw symmetric encryption
- Practical people **wanted** to get authenticity and privacy by one conceptual tool
- **Ad hoc** ways to try to do this efficiently **didn't work**

Previously realized for the PK setting

- **[Bleichenbacher 1998]** – Attack on PKCS #1
- Reaction: IND-CPA security **not enough**
  - **CCA1** security [Naor-Yung 1990]
  - **CCA2** security [Rackoff-Simon 1991]
  - **Non-malleability** [Dolev-Dwork-Naor 1991]
- **Signcryption** [Zheng 1997] (very different motivation)

pAE – Probabilistic Authenticated Encryption

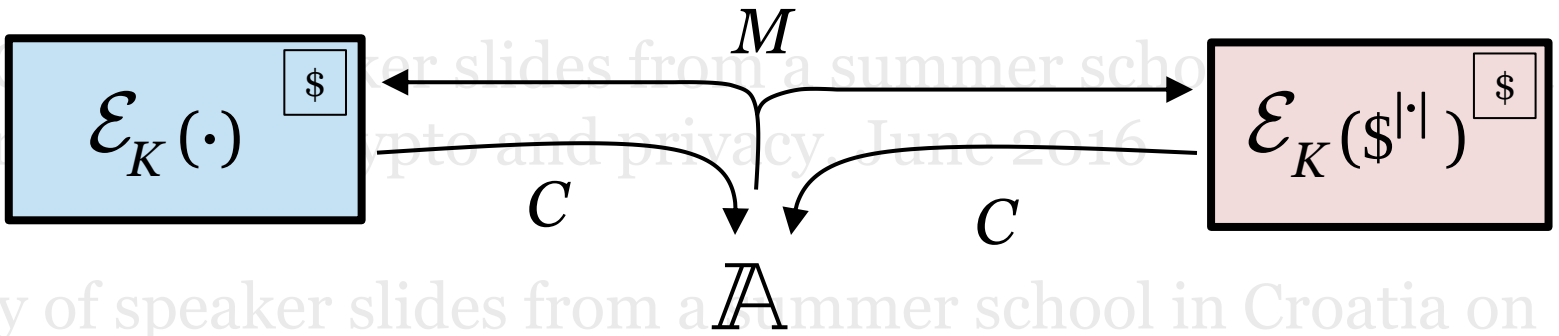
[Bellare, Rogaway 2000]
[Katz, Yung 2000]



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

pAE – Probabilistic AE

[Bellare, Rogaway 2000]
[Katz, Yung 2000]

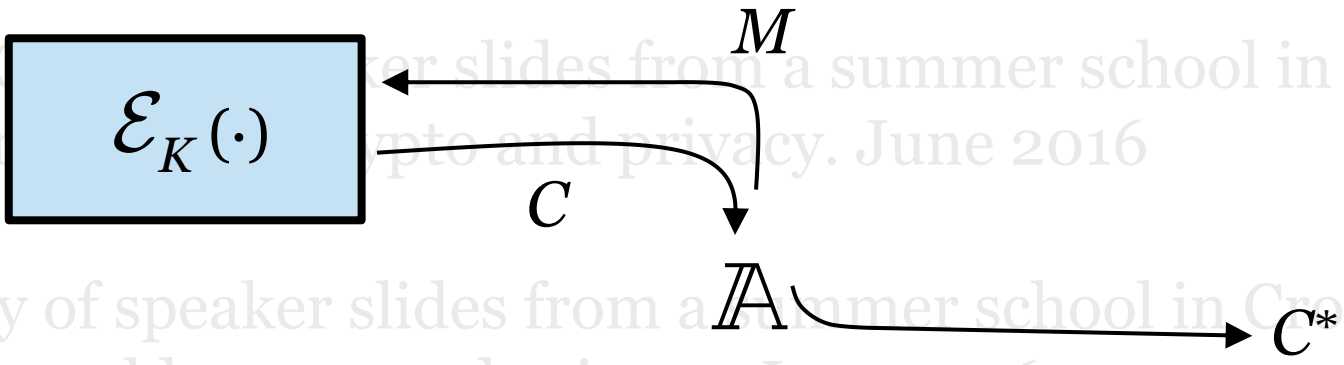


$$\mathbf{Adv}^{\text{priv}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K(\cdot)} \rightarrow 1] \;-\; \Pr[A^{\mathcal{E}_K(\$^{|\cdot|})} \rightarrow 1]$$

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

pAE – Probabilistic AE

[Bellare, Rogaway 2000]
[Katz, Yung 2000]

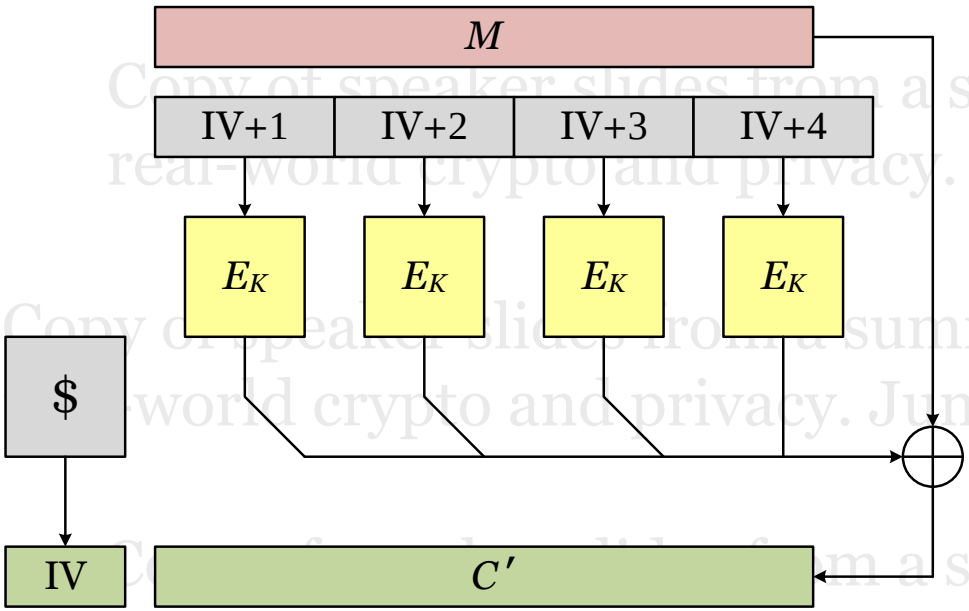


$$\mathbf{Adv}^{\text{priv}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K(\cdot)} \rightarrow 1] - \Pr[A^{\mathcal{E}_K(\$|\cdot|)} \rightarrow 1]$$

$$\mathbf{Adv}^{\text{auth}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K(\cdot)} \rightarrow C^*\text{: no query returned } C^* \text{ and } \mathcal{D}_K(C^*) \neq \perp]$$

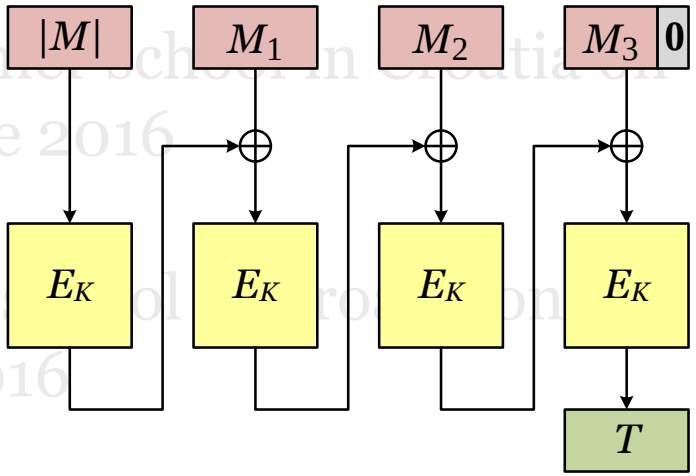
"$\mathbb{A}$ forges"

How to achieve pAE? Combine known tools. Eg:



CBC$

- pE scheme



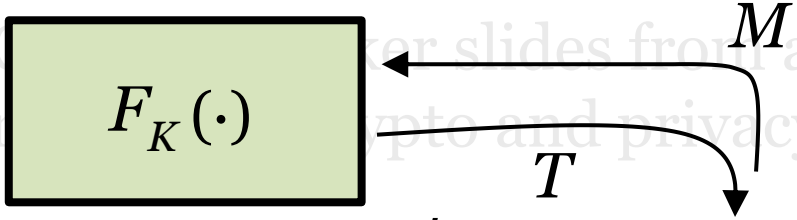
length-prepend CBC MAC

- a MAC
- a PRF

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Message authentication codes
MACs

[Bellare-Guerin-Rogaway 1994, Bellare-Kilian-Rogaway 1995] following [Goldwasser-Micali-Rivest 1984]



$F: \mathcal{K} \times \mathcal{M} \to \{0,1\}^t$

Existential unforgeability under an ACMA

$$\mathbf{Adv}^{\text{mac}}_{F}(\mathbb{A}) = \Pr[\mathbb{A}^{F_K} \text{ forges}]$$

$\mathbb{A}$ outputs a pair $(\tilde{M}, \tilde{T})$ where:

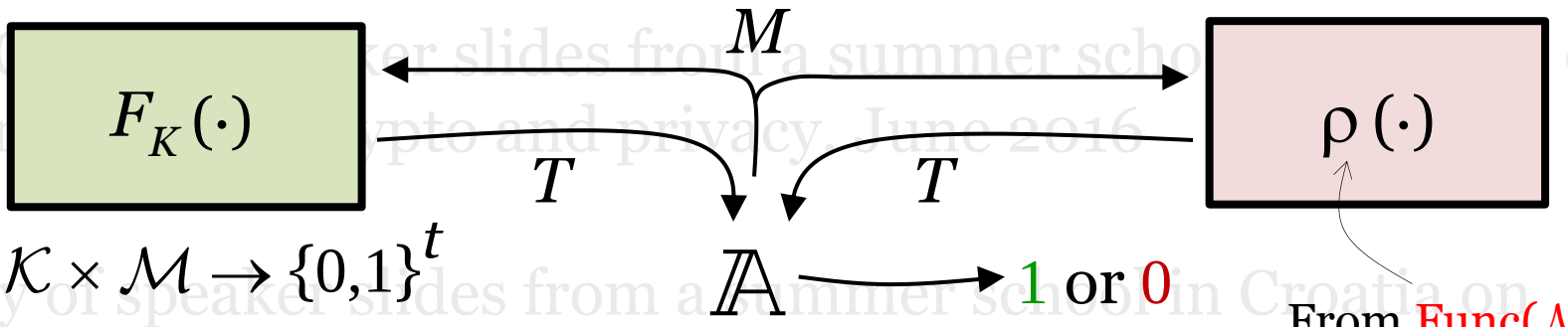
- $\mathbb{A}$ never asked $\tilde{M}$
- $\tilde{T} = F_K(\tilde{M})$

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Message authentication codes

MACs

[Bellare-Guerin-Rogaway 1994, Bellare-Kilian-Rogaway 1995] following [Goldwasser-Micali-Rivest 1984]

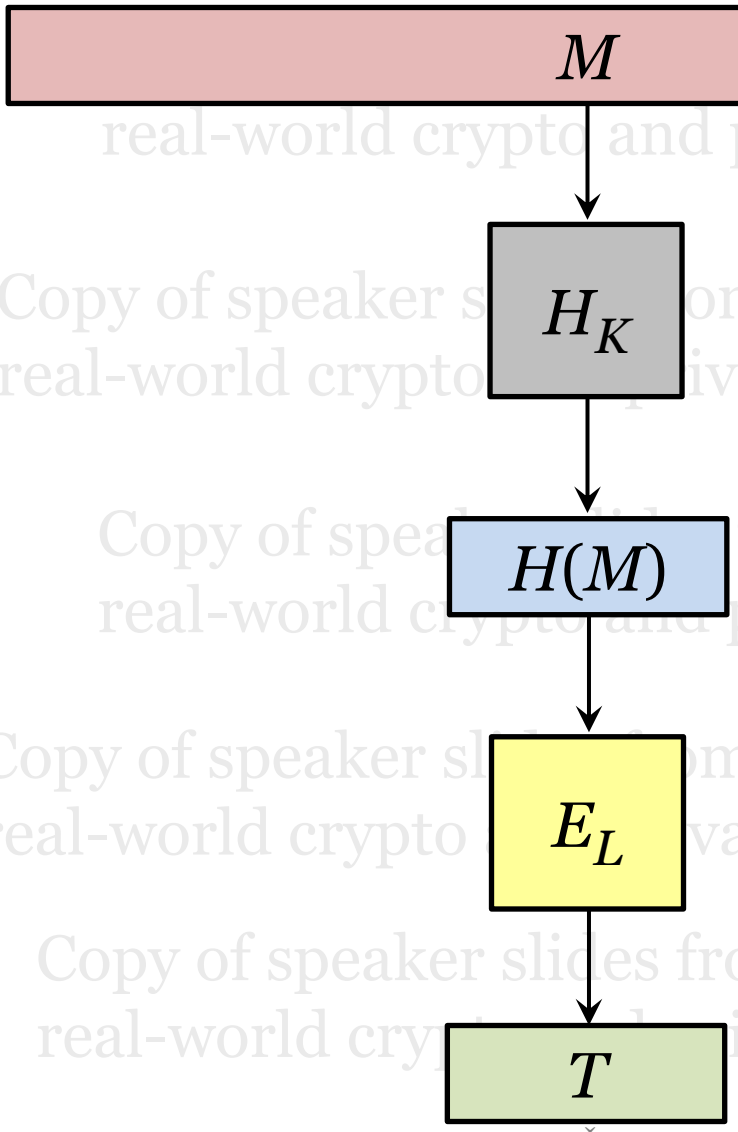


From Func($\mathcal{M}$, n), all functions from $\mathcal{M}$ to n-bit strings

$$\mathbf{Adv}^{\mathrm{prf}}_{F}(\mathbb{A}) = \Pr[\mathbb{A}^{F_K} \to 1] - \Pr[\mathbb{A}^{\rho} \to 1]$$

An Approach for Building PRFs
Hash-then-encipher

[Wegman, Carter 1977]
[Carter, Wegman 1981]
[Rogaway 1995]



$H: \mathcal{K} \times \mathcal{M} \to \{0,1\}^n$

is ε-AU (almost universal) if

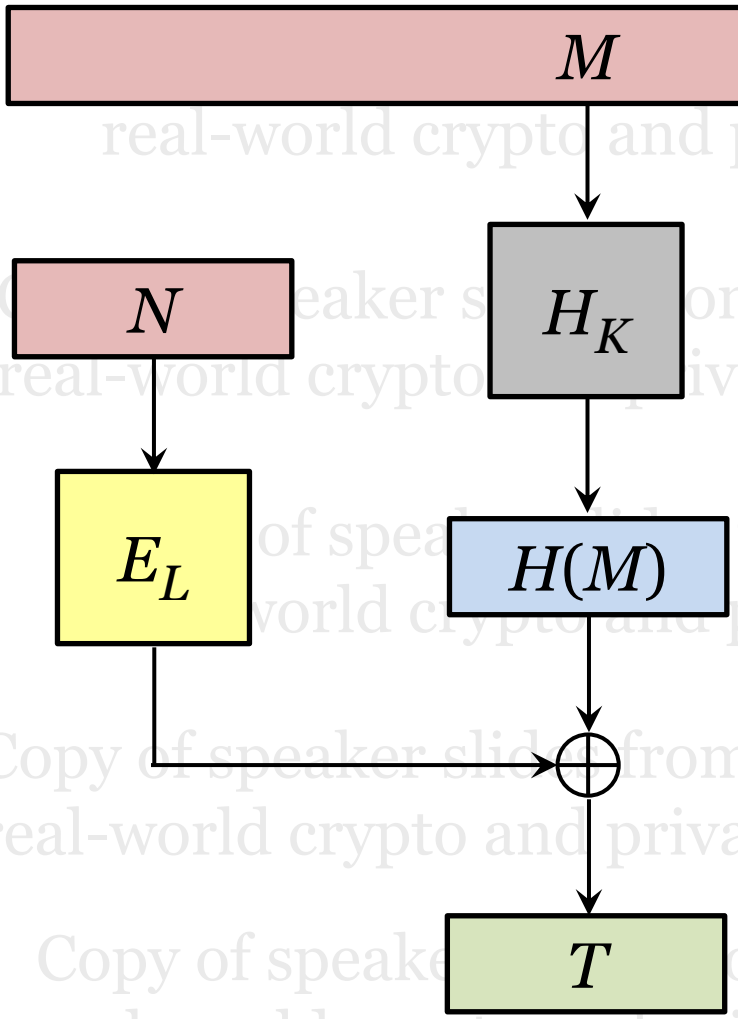
$\forall\ M, M' \in \mathcal{M},\ M \neq M',$

$\Pr[\ H(M) = H(M')] \leq \varepsilon$

If E is a good PRP and
H *is* ε-AU for small ε
then $F_{KL} = E_L \circ H_K$
is a good PRF

An Approach for Building PRFs
Hash-then-mask

[Wegman, Carter 1977]
[Carter, Wegman 1981]
[Rogaway 1995]



$H: \mathcal{K} \times \mathcal{M} \to \{0,1\}^n$

is ε-AXU (almost-xor universal)

$\forall M, M' \in \mathcal{M}, M \neq M', \ \forall C \in \{0,1\}^n,$

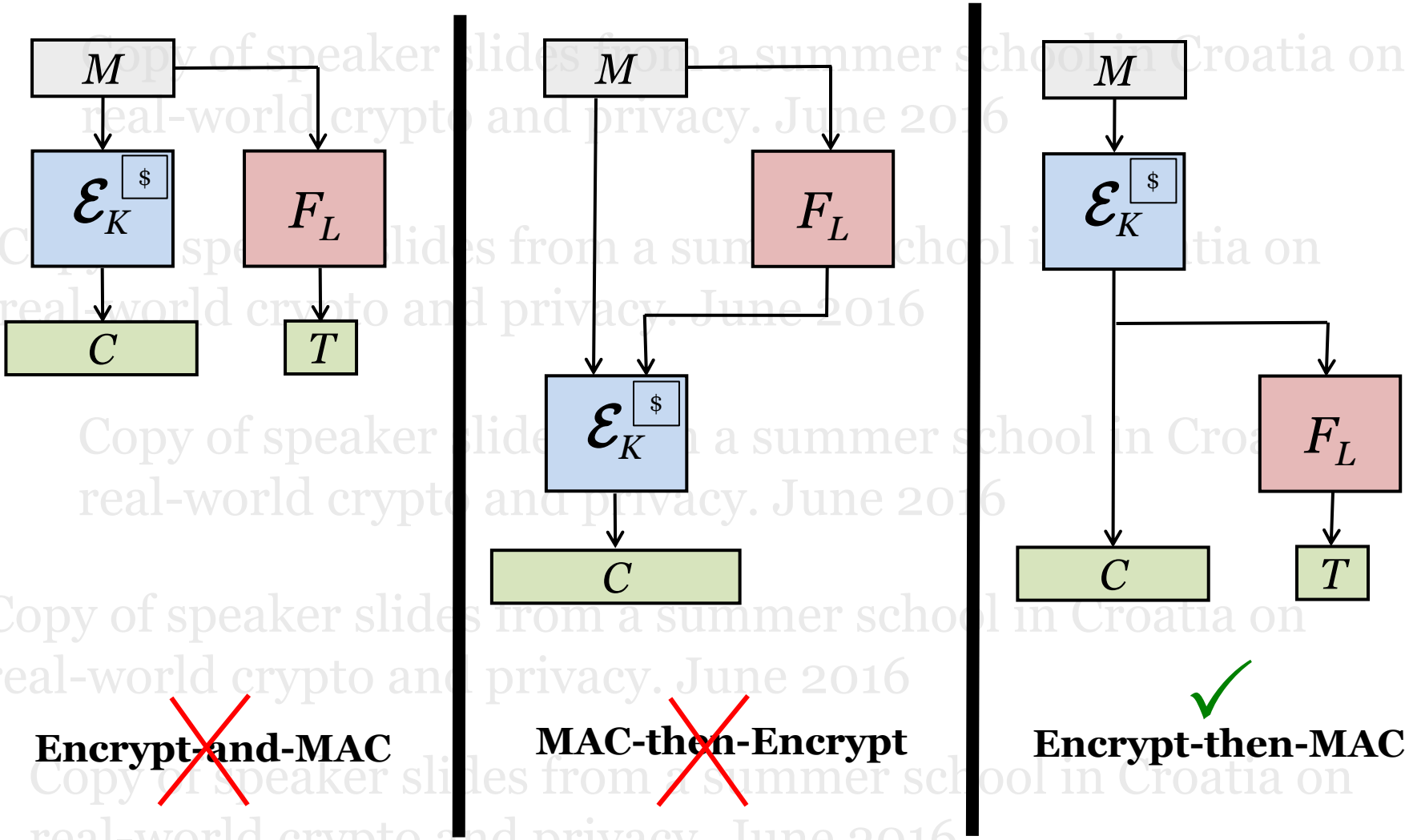
$\Pr[\, H(M) \oplus H(M') = C] \leq \varepsilon$

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Generic composition

of a pE scheme and a PRF

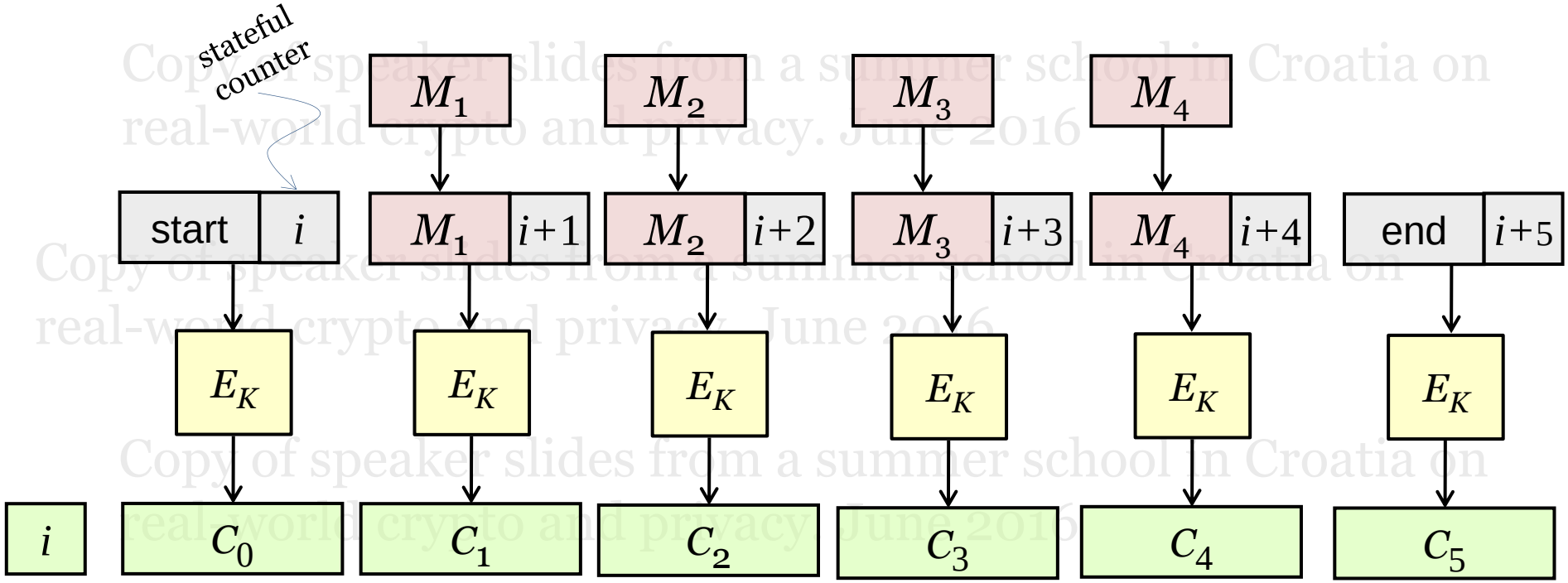
[Bellare, Namprempre 2000]



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

RPC mode

[Katz, Yung 2000]



- Blockcipher-based AE using ~1.33 m + 2 calls
- Fully parallelizable

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

IAPM mode

[Jutla 2001]

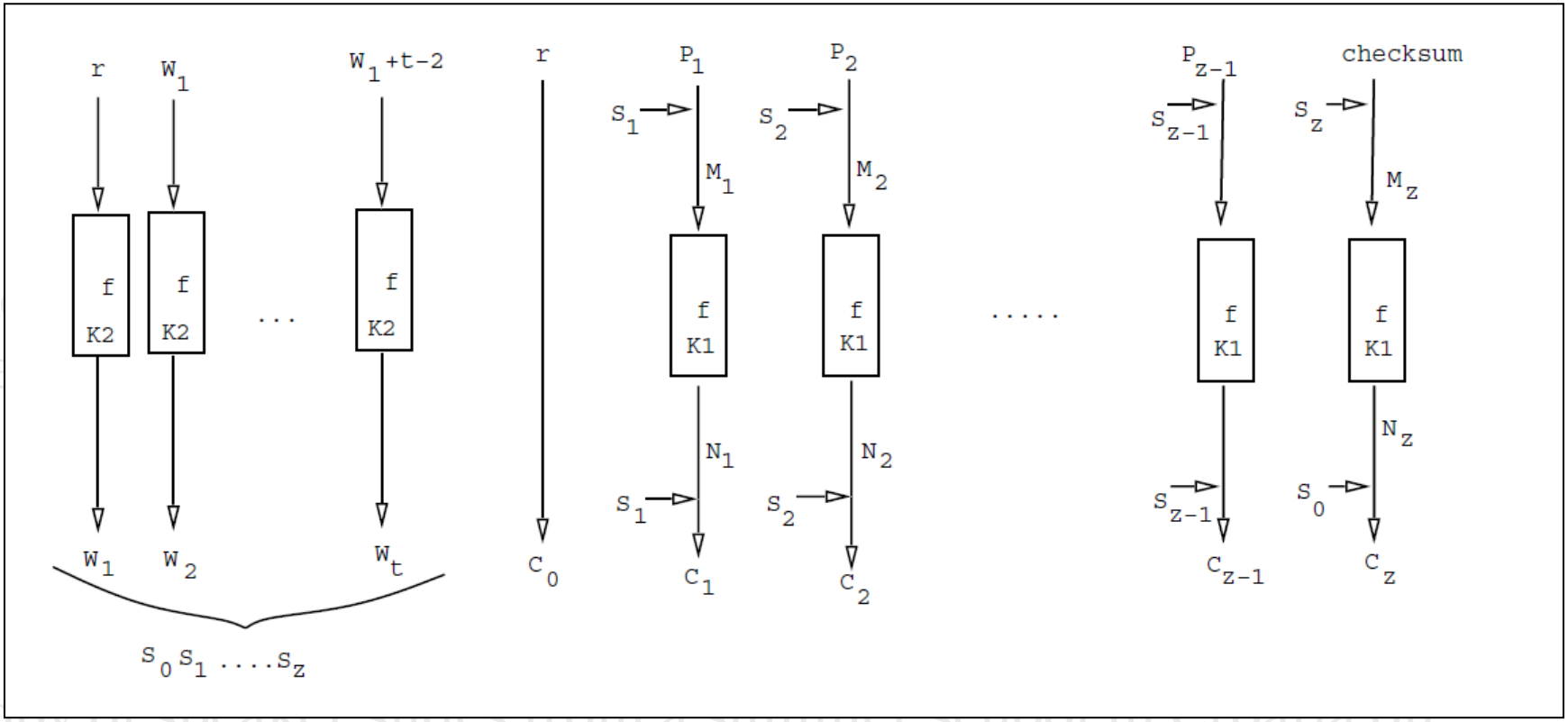


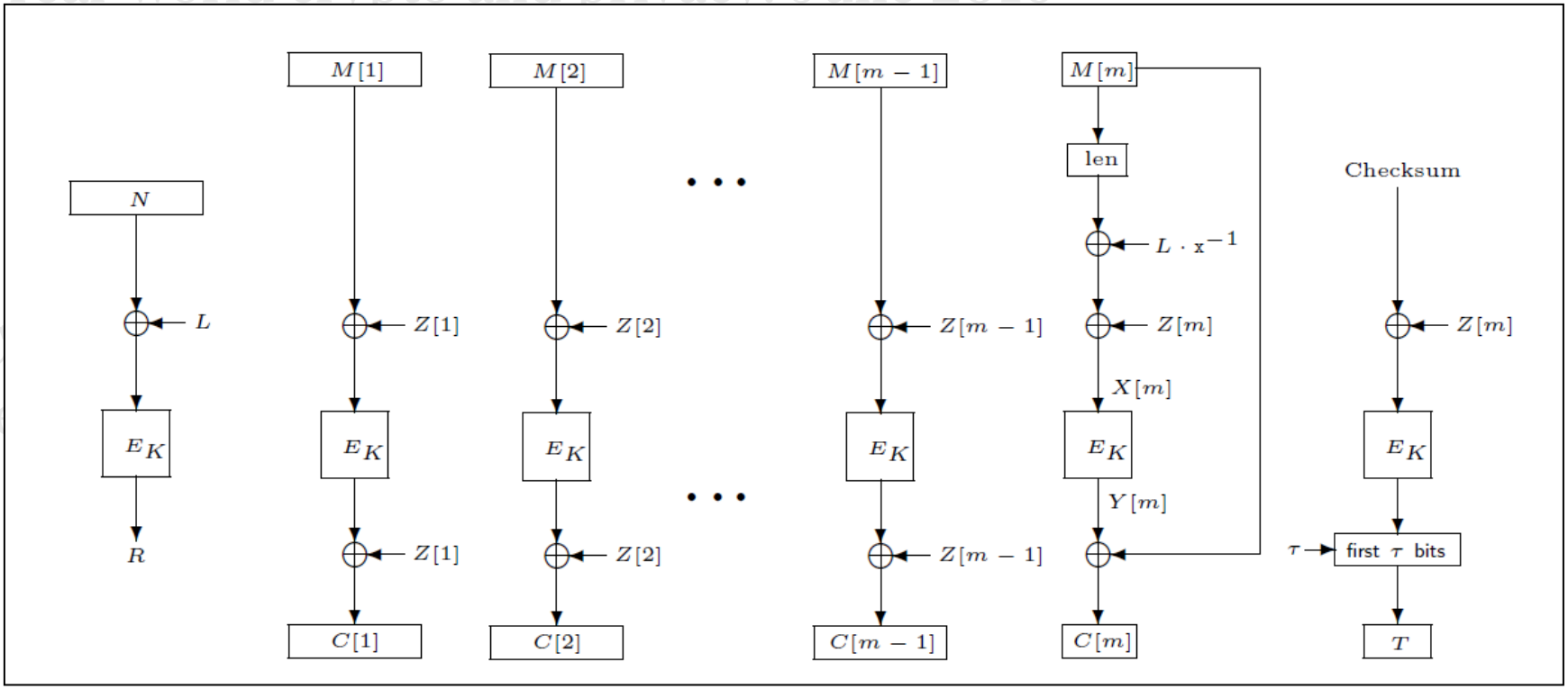
Illustration from **[Jutla 2001]**

See **[Gligor, Donescu 2001]** for similar AE designs

- Blockcipher-based AE using $m + \lg(m)$ calls
- Fully parallelizable
- Plaintext a multiple of blocksize. Padding will increases $|C|$
- Multiple blockcipher keys
- Need for random r

OCB mode ("OCB1")

[Rogaway, Bellare, Black, Krovetz 2001]



$Z[i] = R \oplus \gamma_i \cdot L$

Checksum = $M[1] \oplus \cdots \oplus M[m\text{-}1] \oplus C[m]0^* \oplus Y[m]$

- Arbitrary-length messages; no padding
- Efficient offset calculations
- Single blockcipher key
- Cheap key setup (one blockcipher call)
- $m + 2$ blockcipher calls

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

AE quickly became real

Urgent need

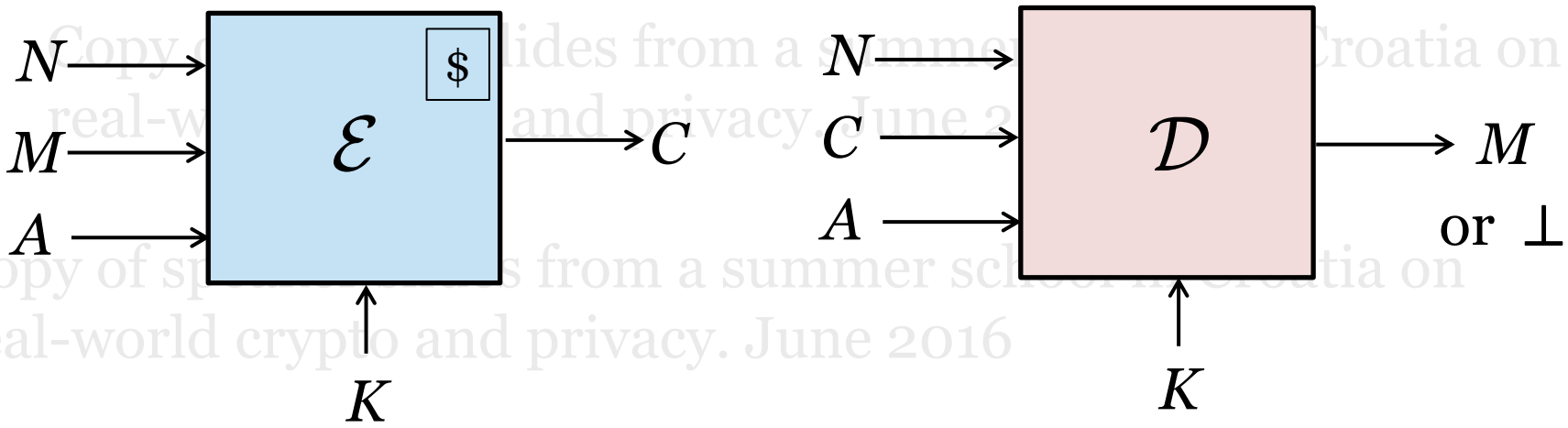
- **802.11** standard ratified in 1999
  Uses **WEP** security – RC4 with a CRC-32 checksum for integrity

- **Fatal attacks** soon emerge:
  - [Fluhrer, Mantin, Shamir 2001]
    Weaknesses in the key scheduling algorithm of RC4
  - [Stubblefield, Ioannidis, Rubin 2001]
    Using the Fluhrer, Mantin, Shamir attack to break WEP
  - [Borisov, Goldberg, Wagner 2001]
    Intercepting mobile communications: the insecurity of 802.11
  - [Cam-Winget, Housley, Wagner, Walker 2003]
    Security flaws in 802.11 data links protocols

- **WEP → WPA** (uses **TKIP**) **→ WPA2** (uses **CCM**)
  - Draft solutions based on **OCB**
  - Politics +patent-avoidance:
    CCM developed **[Whiting, Housley, Ferguson 2002]**
  - Standardized in **IEEE 802.11** [2004] , **NIST 800-38C** [2004]

But before it could become real …

Definitional issues in the basic syntax



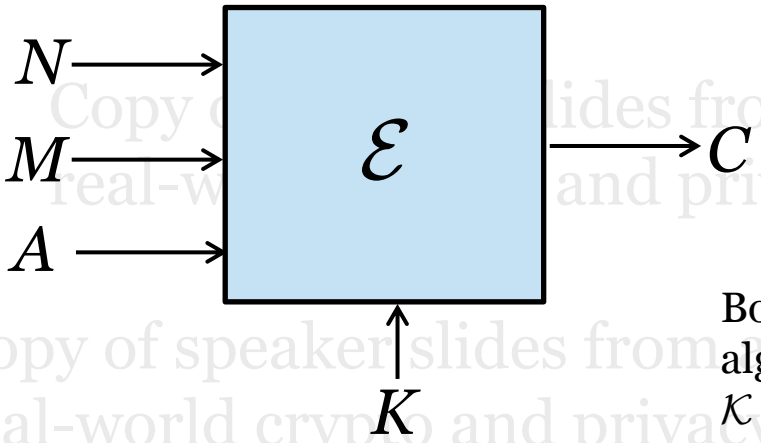
1) Move the coins out of $\mathcal{E}$ — make it deterministic **[RBBK01]**

Need to design cryptosystems resilient
to random-number generation problems
& to architect to existing abstraction boundaries

2) Add in "associated data" **[R02]**

Jesse Walker, Nancy Cam-Winget, Burt Kaliski all "requested" this functionality for their standardization-related work

Formalizing the Syntax
For AEAD



One approach:
An AE scheme is a 3-tuple of algorithms
$\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ …

Both $\mathcal{E}$ and $\mathcal{D}$ should be efficiently computable by algorithms that take in 4-tuples of binary strings; $\mathcal{K}$ should be efficiently sampleable.

Another approach: An AEAD scheme is a function

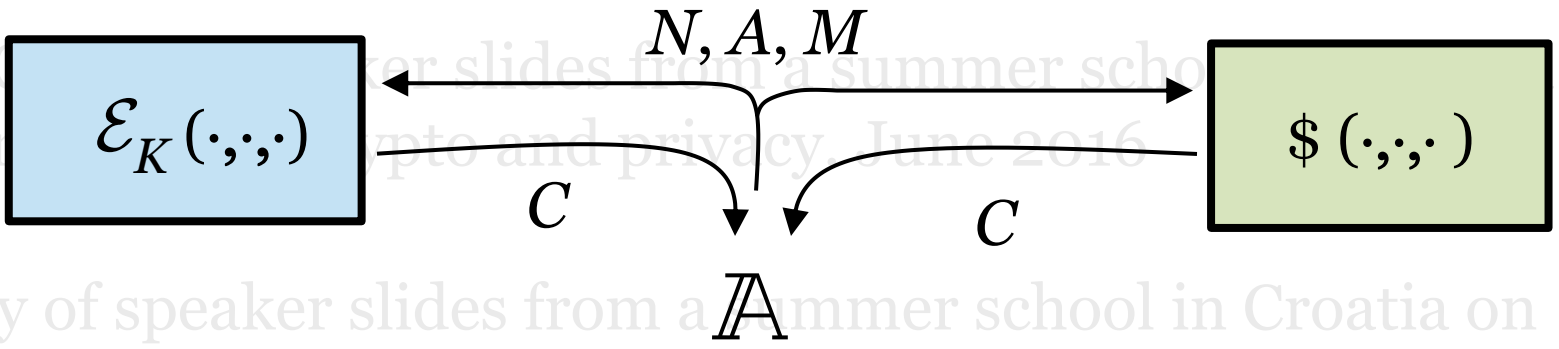
$\mathcal{E}: \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \{0,1\}^*$ where

- $\mathcal{K}$ is a set with a distribution; $\mathcal{N}$, $\mathcal{A}$, $\mathcal{M}$ are nonempty sets of strings; $\mathcal{M}$ contains a string x iff it contains all strings of length $|x|$
- Each $\mathcal{E}(K, N, A, \cdot)$ is an injection
- For some λ, $|\mathcal{E}(K, N, A, M)| = |M| + \lambda$

Let $\mathcal{D} = \mathcal{E}^{-1}$ be the map $\mathcal{D}: \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$ defined by $\mathcal{D}(K, N, A, C) = M$ if $\mathcal{E}(K, N, A, M) = C$ for some M, and $\perp$ otherwise

nAE – nonce-based AEAD

Two-part definition, as in **[RBBK00]**, **[R02]**



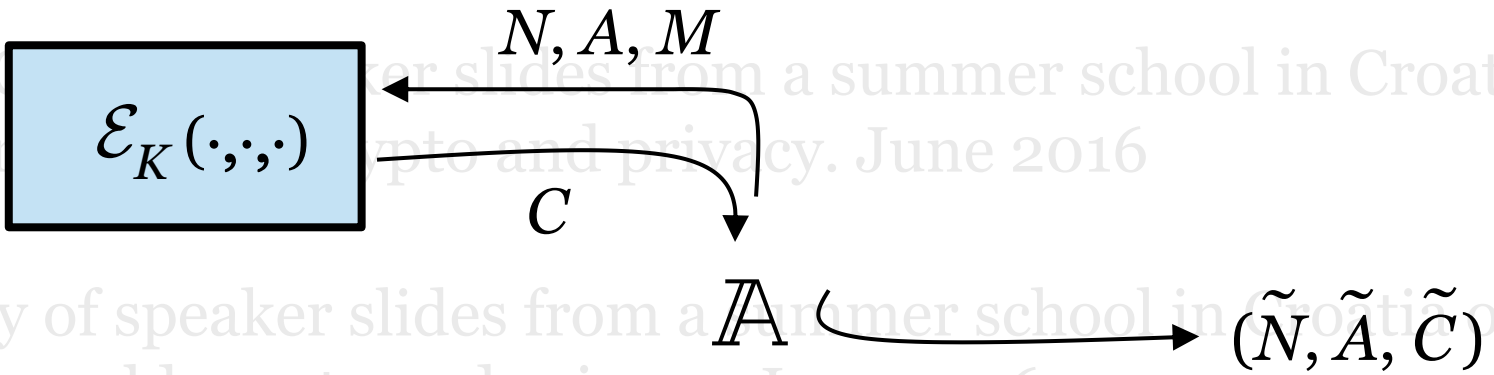
𝔸 may not repeat an *N*-value

$$\mathbf{Adv}^{\text{priv}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K} \rightarrow 1] - \Pr[\mathbb{A}^{\$} \rightarrow 1]$$

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

nAE – nonce-based AEAD

Two-part definition, as in **[RBBKoo]**, **[Ro2]**



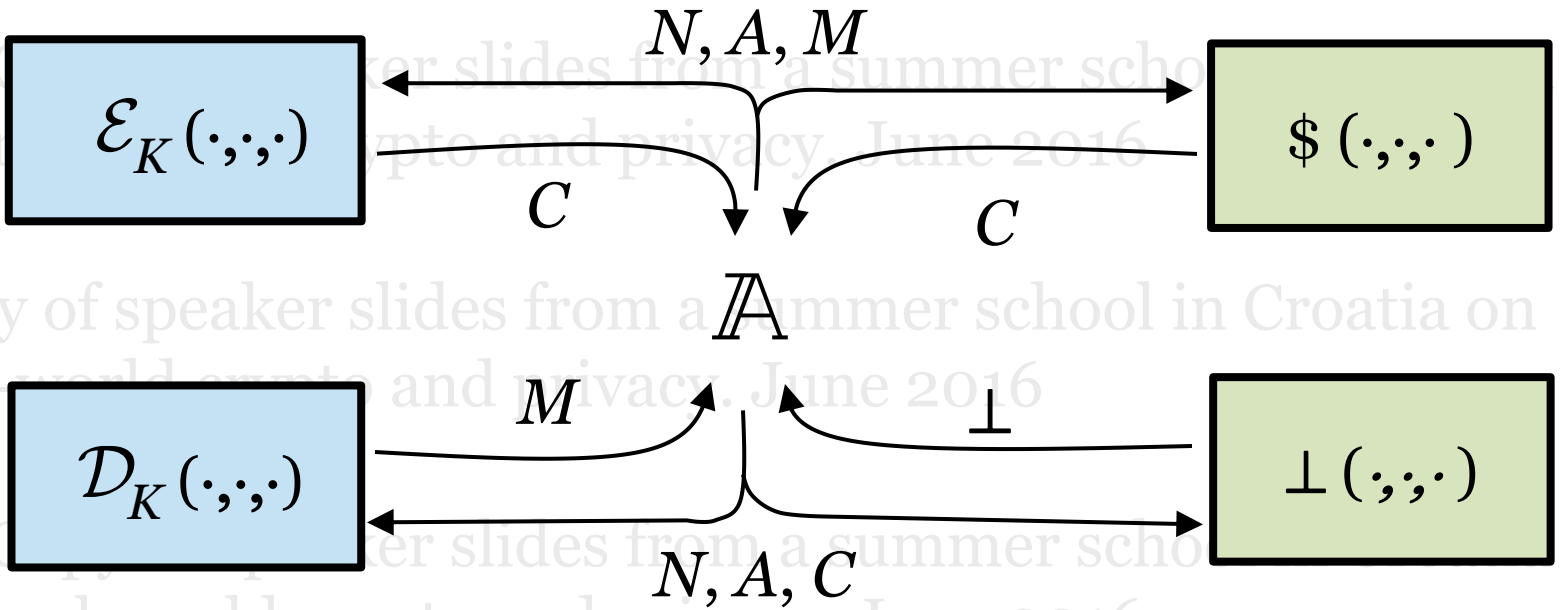
$$\mathbf{Adv}^{\text{priv}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K} \rightarrow 1] \quad - \quad \Pr[\mathbb{A}^{\$} \rightarrow 1]$$

$$\mathbf{Adv}^{\text{auth}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\text{Real}} \text{ forges}]$$

- A never asked $(\tilde{N}, \tilde{A}, \cdot) \rightarrow \tilde{C}$
- $\mathcal{D}(\tilde{N}, \tilde{A}, \tilde{C}) \neq \perp$

nAE – nonce-based AEAD

All-in-one definition **[Rogaway, Shrimpton 2006]**
Uses ind from random bits **[RBBK00]**



$$\mathbf{Adv}^{\text{aead}}_{\Pi}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K, \mathcal{D}_K} \rightarrow 1] - \Pr[\mathbb{A}^{\$, \perp} \rightarrow 1]$$

$\mathbb{A}$ may not:
- Repeat an N in an enc query
- Ask a dec query (N, A, C) after C is returned by an $(N, A, \cdot)$ enc query

(

New contribution in today's talk!

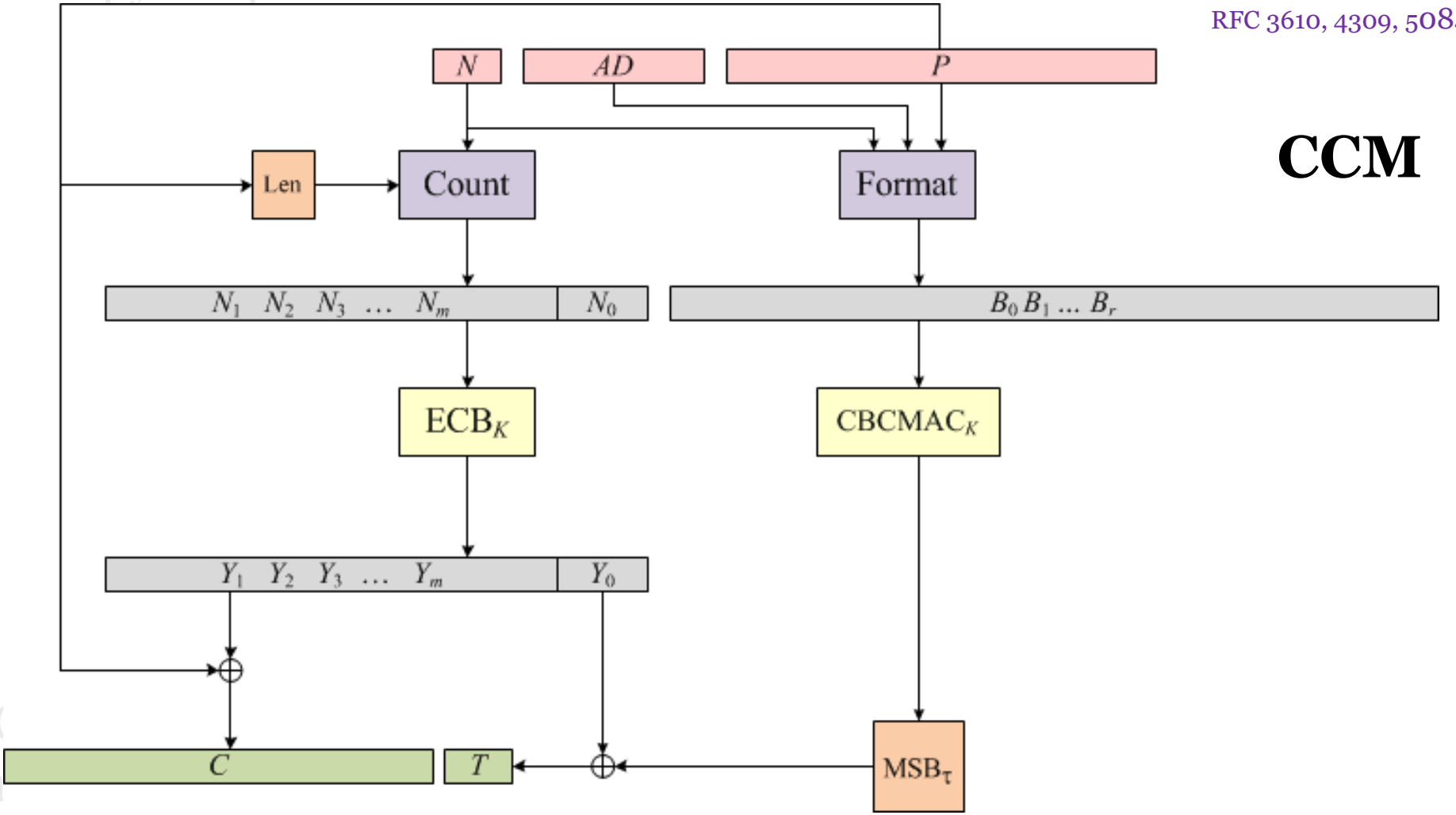
- A – an entity, "Alice". Rarely needed.
- A – capitalized English article. Change to "An" before a vowel.
- A – associated data. A string. $a = |A|$
- $\mathcal{A}$ – space of associated-data values. A set of strings.
- $\mathbb{A}$ – an adversary.

)

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

[Whiting, Housley, Ferguson 2002]
NIST SP 800-38C
RFC 3610, 4309, 5084

CCM



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Functions FORMAT and COUNT

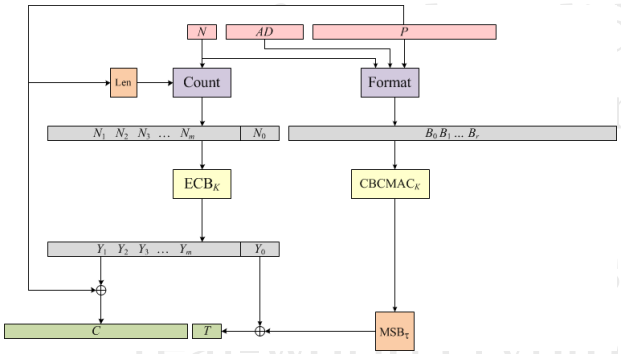
CCM

$\textsc{Count}_q(N, m) = N_1 \,\|\, N_2 \,\|\, \cdots \,\|\, N_m$ where

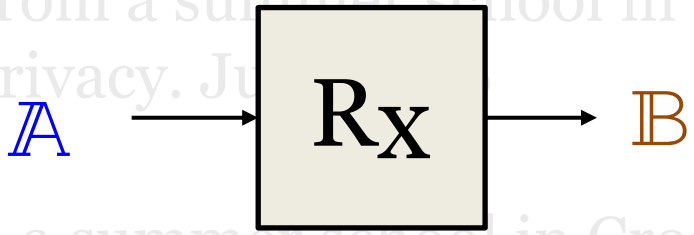
$N_i = 0^5 \,\|\, [\, q-1 \,]_3 \,\|\, N \,\|\, [\, i \,]_{8q}$

$\textsc{Format}_{q,t}(N, A, P) =$

$0 \,\|\, \textbf{if } A = \varepsilon \textbf{ then } 0 \textbf{ else } 1 \textbf{ endif} \,\|\, [\, t/2-1 \,]_3 \,\|\, [\, q-1 \,]_3 \,\|$
$N \,\|\, [\, |P|_8 \,]_{8q} \,\|$
$\textbf{if } A = \varepsilon \textbf{ then } \varepsilon \textbf{ elseif}$
$|A|_8 < 2^{16} - 2^8 \textbf{ then } [\, |A|_8 \,]_{16}$
$\textbf{elseif } |A|_8 < 2^{32} \textbf{ then } \texttt{0xFFFE} \,\|\, [\, |A|_8 \,]_{32} \textbf{ else } \texttt{0xFFFF} \,\|\, [\, |A|_8 \,]_{64} \textbf{ endif} \,\|$
$A \,\|$
$\textbf{if } A = \varepsilon \textbf{ then } \varepsilon \textbf{ elseif } |A|_8 < 2^{16} - 2^8 \textbf{ then } (\texttt{0x00})^{(14-|A|_8) \bmod 16}$
$\textbf{elseif } |A|_8 < 2^{32} \textbf{ then } (\texttt{0x00})^{(10-|A|_8) \bmod 16} \textbf{ else } (\texttt{0x00})^{(6-|A|_8) \bmod 16} \textbf{ endif} \,\|$
$P \,\|$
$(\texttt{0x00})^{(-|M|_8) \bmod 16}$



CCM



Adversary attacking CCM[E]

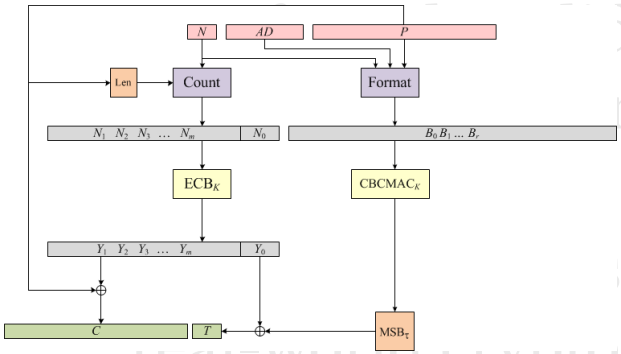
Breaks it with advantage δ in the aead-sense

Adversary attacking E

Breaks it with advantage f(Resources, δ) in the PRP-sense

Thm. There exists a reduction Rx with the following property.
Let E: $\mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a blockcipher and let $\mathbb{A}$ be an adversary using σ blocks in attacking Π = CCM[E] with nAE-advantage δ.
Then $\mathbb{B}$ = Rx ($\mathbb{A}$,E) breaks E with PRP-advantage $\geq \delta - \sigma^2 \, 2^{-n}$ and resources comparable to $\mathbb{A}$'s.

CCM



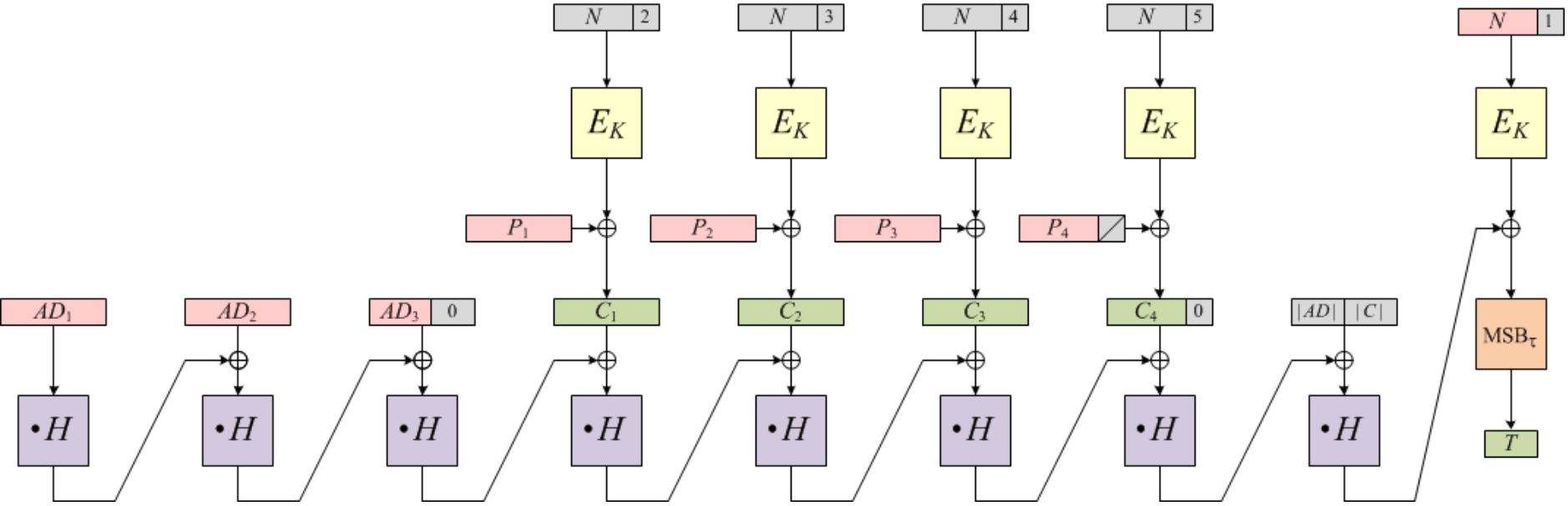
- Provably secure **[Jonsson 2002]**
- Widely standardized & used
- Simple to implement
- Only forward direction of cipher used

- About $2m+2$ blockcipher calls
- Half non-parallelizable
- Word alignment disrupted
- Can't preprocess static AD
- Not online
- Parameter $q \in \{2,3,4,5,6,7,8\}$ (byte length of byte length of longest message) determines nonce length of $\tau = 15-q$
- Full of *ad hoc* conventions

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

[McGrew, Viega 2004]
(Follows **CWC**
[Kohno, Viega, Whiting 2004])
NIST SP 800-38D:2007
RFC 4106, 5084, 5116, 5288, 5647
ISO 19772:2009

GCM



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

GCM

- Provably secure
- Widely standardized & used
- Parallelizable, online
- About $m+1$ blockcipher calls
- Efficient in HW
- Good in SW with AES-NI, PCMULDQ, or tables
- Static *AD* can be preprocessed
- Only forward direction of blockcipher used

- Poor key agility (table-based implementation)
- Can't use short tags **[Ferguson 05]**
- Not so good in SW without HW support
- Timing attacks if table-based
- "Reflected-bit" convention
- $|N| \neq 96$ not handled well
- Published proof buggy [Iwata, 2012]

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

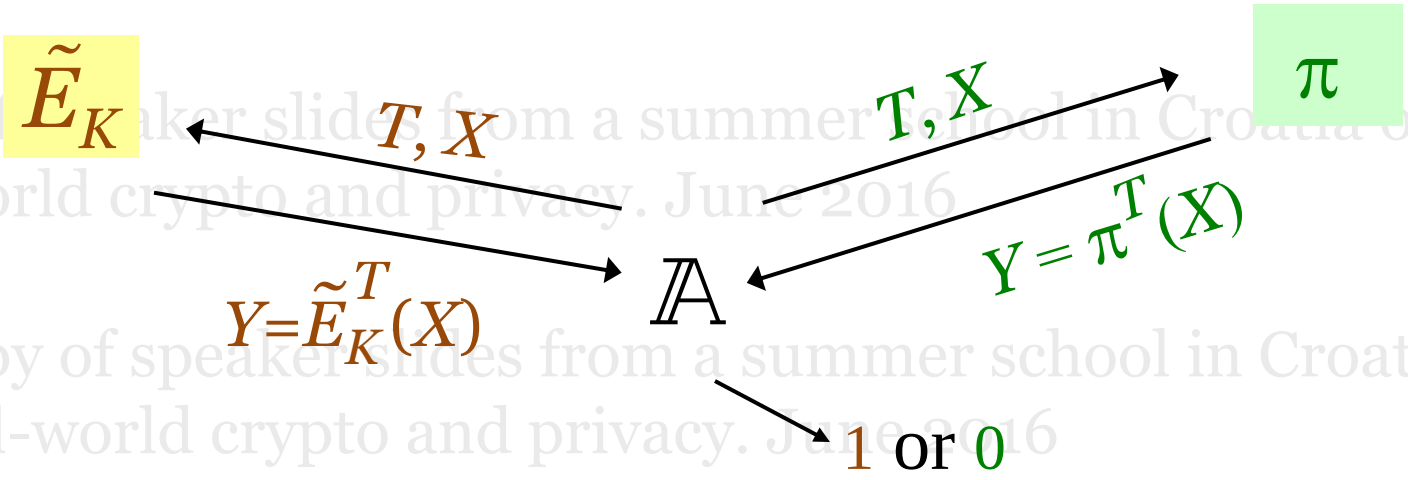
Tweakable Blockciphers

[Liskov, Rivest, Wagner 2002]

$\tilde{E}: \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \rightarrow \{0,1\}^n$

each $\tilde{E}_K^T(\cdot) = \tilde{E}(K, T, \cdot)$ a **permutation**

A $\mathcal{T}$-indexed family of random permutations on n bits

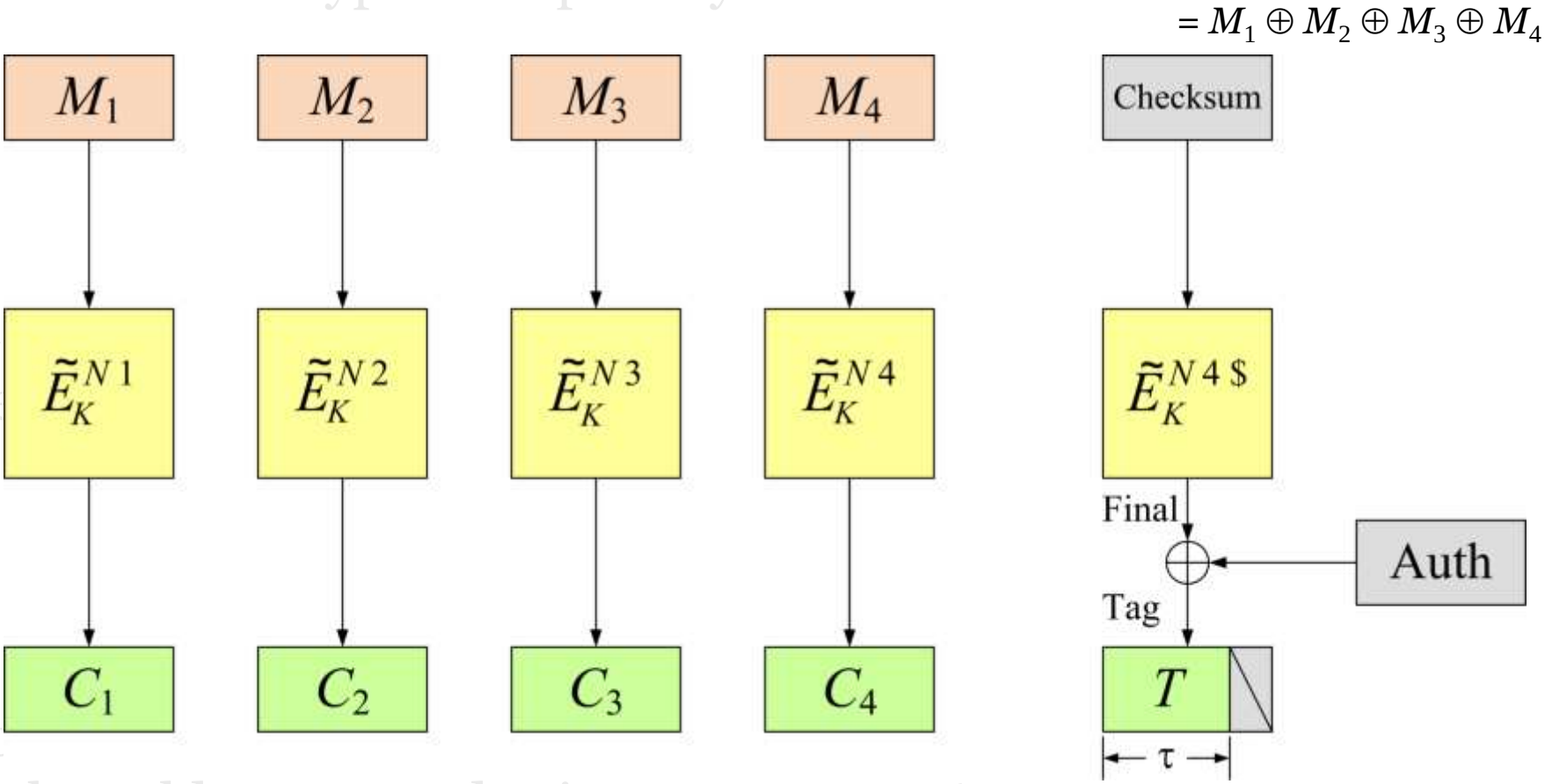


$$\mathbf{Adv}^{\mathrm{prp}}_{\tilde{E}}(\mathbb{A}) = \Pr[\mathbb{A}^{\tilde{E}_K} \Rightarrow 1] - \Pr[\mathbb{A}^{\pi} \Rightarrow 1]$$

$$\mathbf{Adv}^{\pm\mathrm{prp}}_{\tilde{E}}(\mathbb{A}) = \Pr[\mathbb{A}^{\tilde{E}_K\, \tilde{E}_K^{-1}} \Rightarrow 1] - \Pr[\mathbb{A}^{\pi\, \pi^{-1}} \Rightarrow 1]$$

In terms of tweakable blockcipher **[LRW02]**

OCB

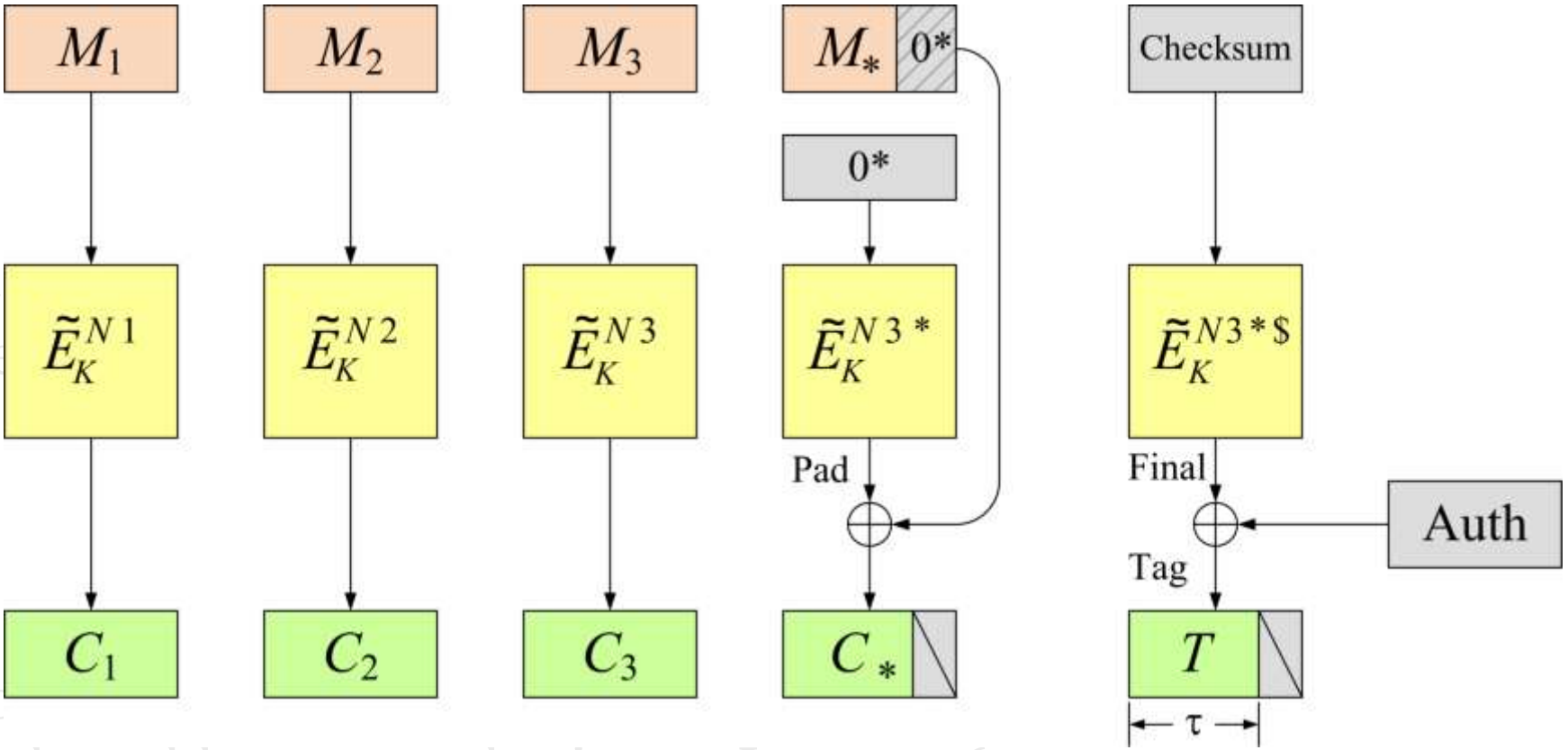


[KR11], following
[RBBK01,LRW02,R04]
RFC 7253 ISO 19772

In terms of tweakable blockcipher **[LRW02]**

OCB

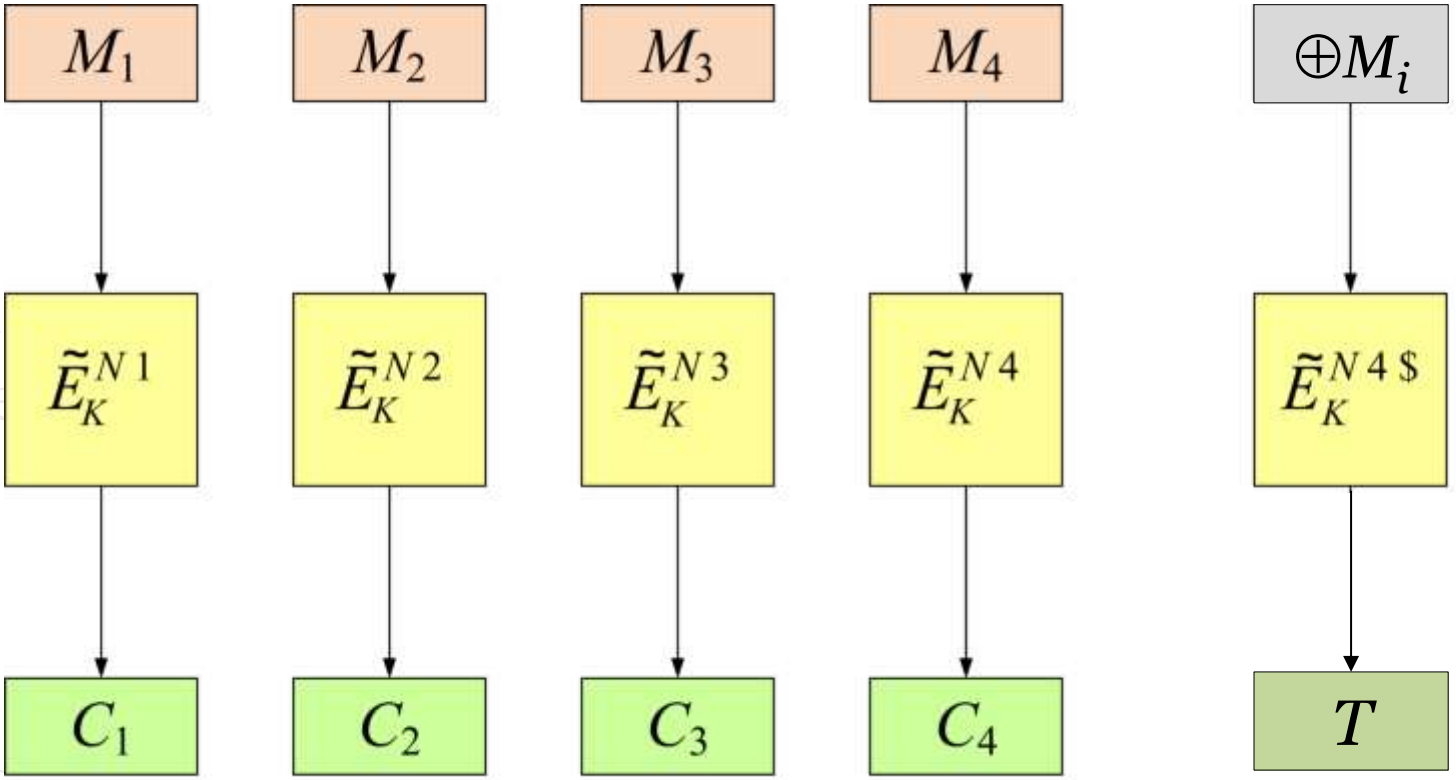
$= M_1 \oplus M_2 \oplus M_3 \oplus M_4 10^*$



[KR11], following
[RBBK01,LRW02,R04]
RFC 7253 ISO 19772

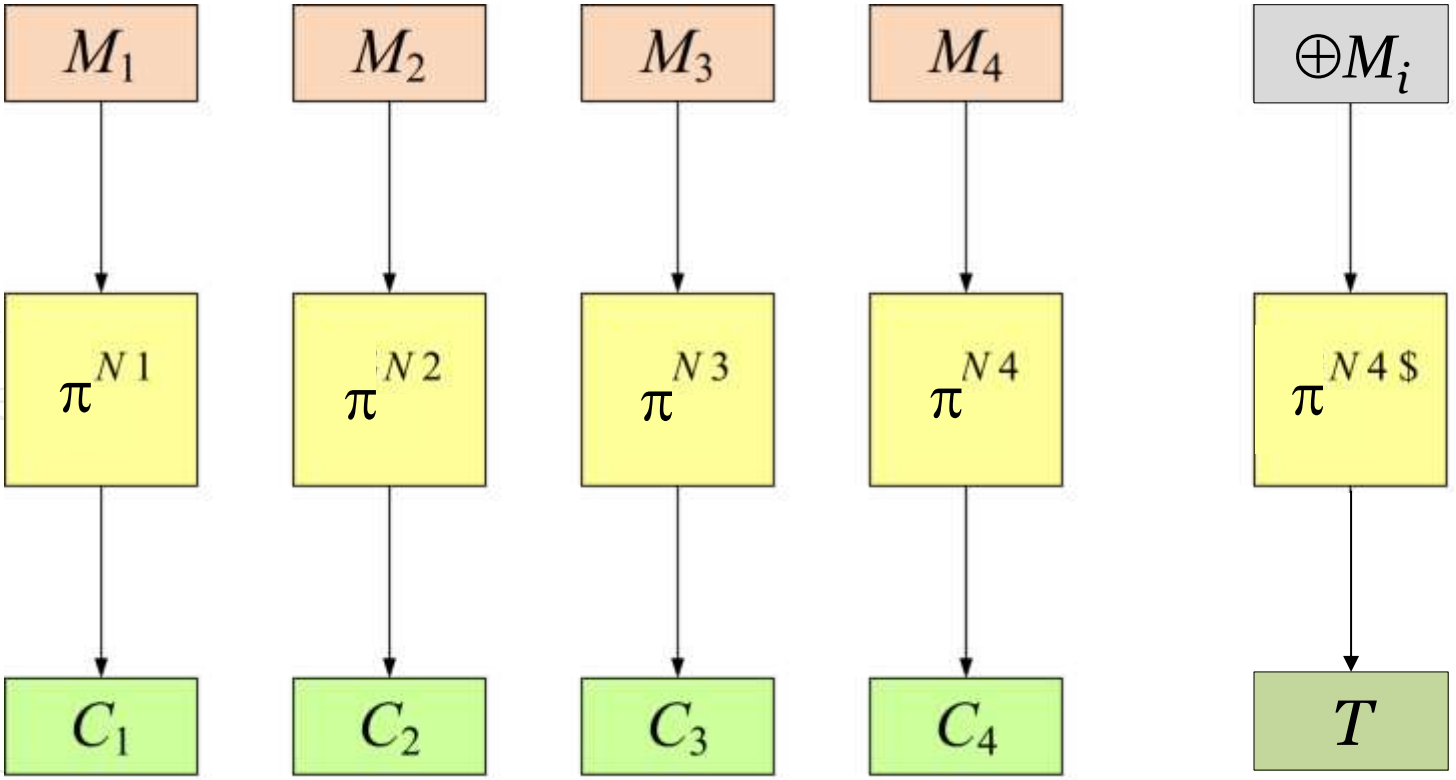
In terms of tweakable blockcipher **[LRW02]**

OCB



[KR11], following **[RBBK01,LRW02,R04]**
RFC 7253 ISO 19772

OCB



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Making OCB's Tweakable Blockcipher

$$\widetilde{E}_K^{N\,i}(X) = E_K(X \oplus \Delta) \oplus \Delta \quad \text{with} \quad \Delta = \text{Initial} + \lambda_i L$$

$$\widetilde{E}_K^{N\,i^*}(X) = E_K(X \oplus \Delta) \quad \text{with} \quad \Delta = \text{Initial} + \lambda_i^* L$$

$$\widetilde{E}_K^{N\,i\,\$}(X) = E_K(X \oplus \Delta) \quad \text{with} \quad \Delta = \text{Initial} + \lambda_i^\$ L$$

$$\widetilde{E}_K^{N\,i^*\,\$}(X) = E_K(X \oplus \Delta) \quad \text{with} \quad \Delta = \text{Initial} + \lambda_i^{*\$} L$$

$$\widetilde{E}_K^{i}(X) = E_K(X \oplus \Delta) \quad \text{with} \quad \Delta = \lambda_i L$$

$$\widetilde{E}_K^{i^*}(X) = E_K(X \oplus \Delta) \quad \text{with} \quad \Delta = \lambda_i^* L$$

$$\text{Nonce} = 0^{127-|N|}\,1\,N$$
$$\text{Top} = \text{Nonce} \;\&\; 1^{122}\,0^6$$
$$\text{Bottom} = \text{Nonce} \;\&\; 1^{122}\,1^6$$
$$\text{Ktop} = E_K(\text{Top})$$
$$\text{Stretch} = \text{Ktop} \;\|\; (\text{Ktop} \oplus (\text{Ktop} \ll 8))$$
$$\text{Initial} = (\text{Stretch} \ll \text{Bottom})\;[1..128]$$

$$L = E_K(0^{128})$$
$$\lambda_i = 4\,a(i)$$
$$\lambda_i^* = 4\,a(i)+1$$
$$\lambda_i^\$ = 4\,a(i)+2$$
$$\lambda_i^{*\$} = 4\,a(i)+3$$

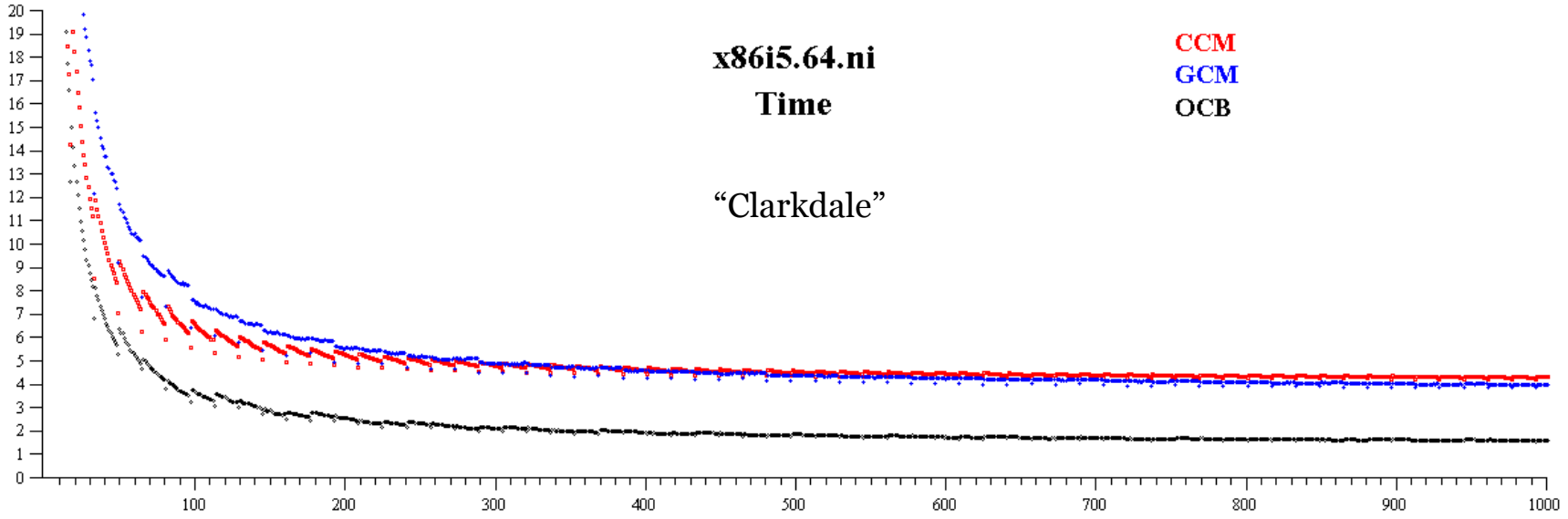
$$a(0) = 0$$
$$a(i) = a(i-1) \oplus 2^{\mathbf{ntz}(i)}$$

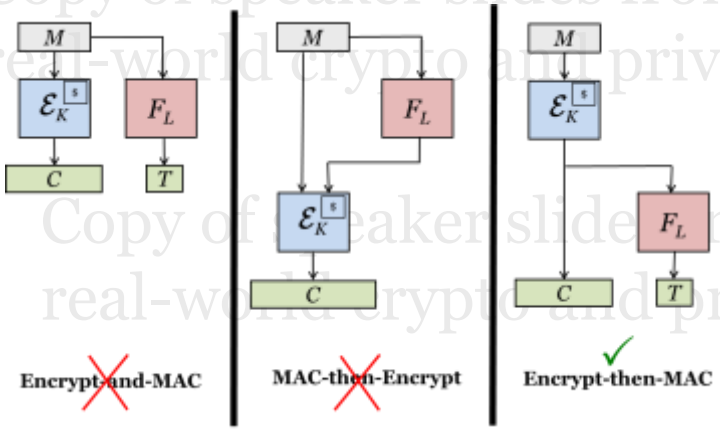
OCB

[KR11], following
[RBBK01,LRW02,R04]
RFC 7253 ISO 19772

- Fastest provably-secure AES-based construction for SW: eg, 0.69 cpb on Haswell
- Parallelizable, online, ~ m+1.02 blockcipher calls

- Blockcipher used in backward direction
- There are faster *de novo* approaches
- Security only to the birthday bound
- Patents from multiple parties
- Nonce-reuse destroys security





Back to generic composition

What did people learn from BN?

1. There are **three ways** to glue together a (privacy-only) **encryption scheme** and a **MAC** to make an AE scheme

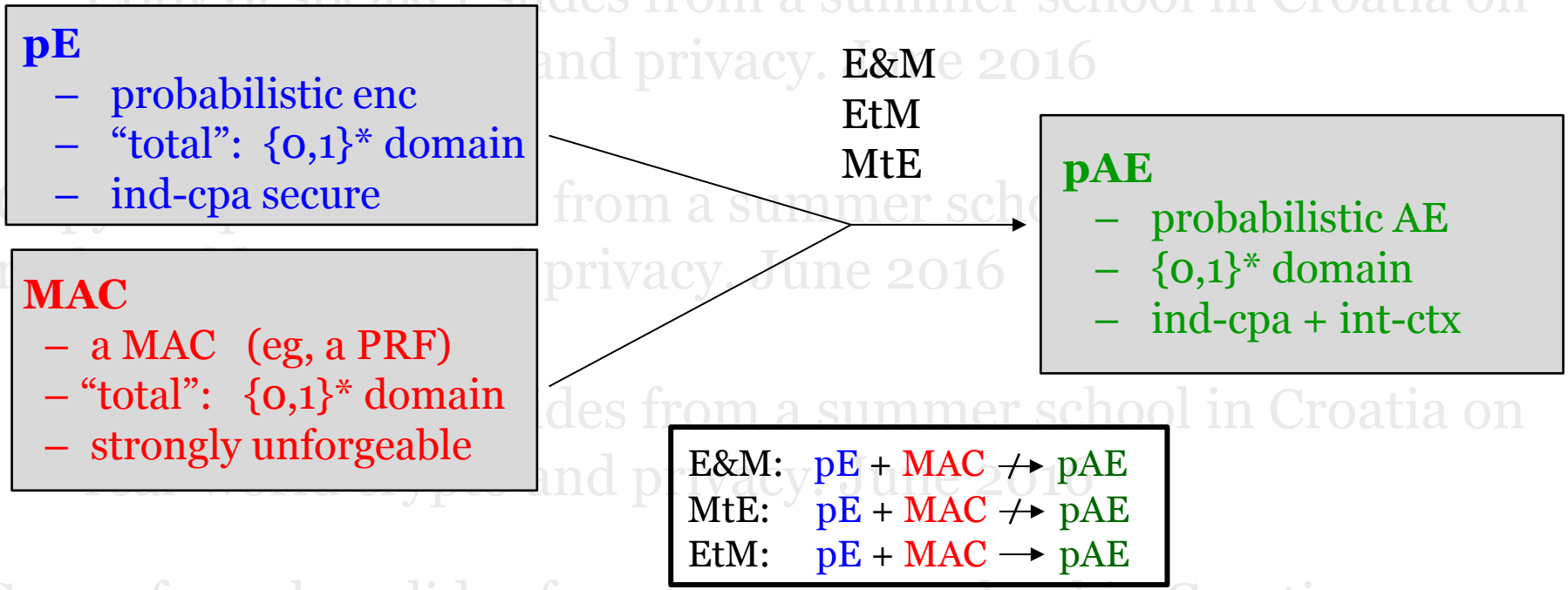
   Encrypt-and-MAC **Encrypt-then-MAC** **MAC-then-Encrypt**

2. Of these, only **Encrypt-then-MAC** works well.

Not the right lesson.

Why not?

It doesn't mention **what definitions** BN use.



If you **change** the definitions, the **results might change** *(duh…)*

*And **they do.*** EtM: ivE + MAC ↛ nAE

[Namprempre, Rogaway, Shrimpton 2014]

ISO/IEC 19772: 2009 (Mechanism 5, Encrypt-then-MAC)

The originator shall perform the following sequence of steps to protext a data string D.

a) A Starting Variable S for use with the selected block cipher mode of operation shall be selected. This variable shall be distinct for every message to be protected during the lifetime of the key, and must be made available to the recipient of the message. Further possible requirements for S are described in the appropriate clauses of ISO/IEC 10116.

b) Let $C' = \varepsilon_{K_1}(D)$.

c) Let $T = f_{K_2}(C')$.

The output of the above process, i.e., the authenticated-encrypted version of D, shall be the bit string

$C = C' \| T$.

CBC, CFB, OFB, CTR (ISO 9797)

CBC MAC variants (ISO 10116)

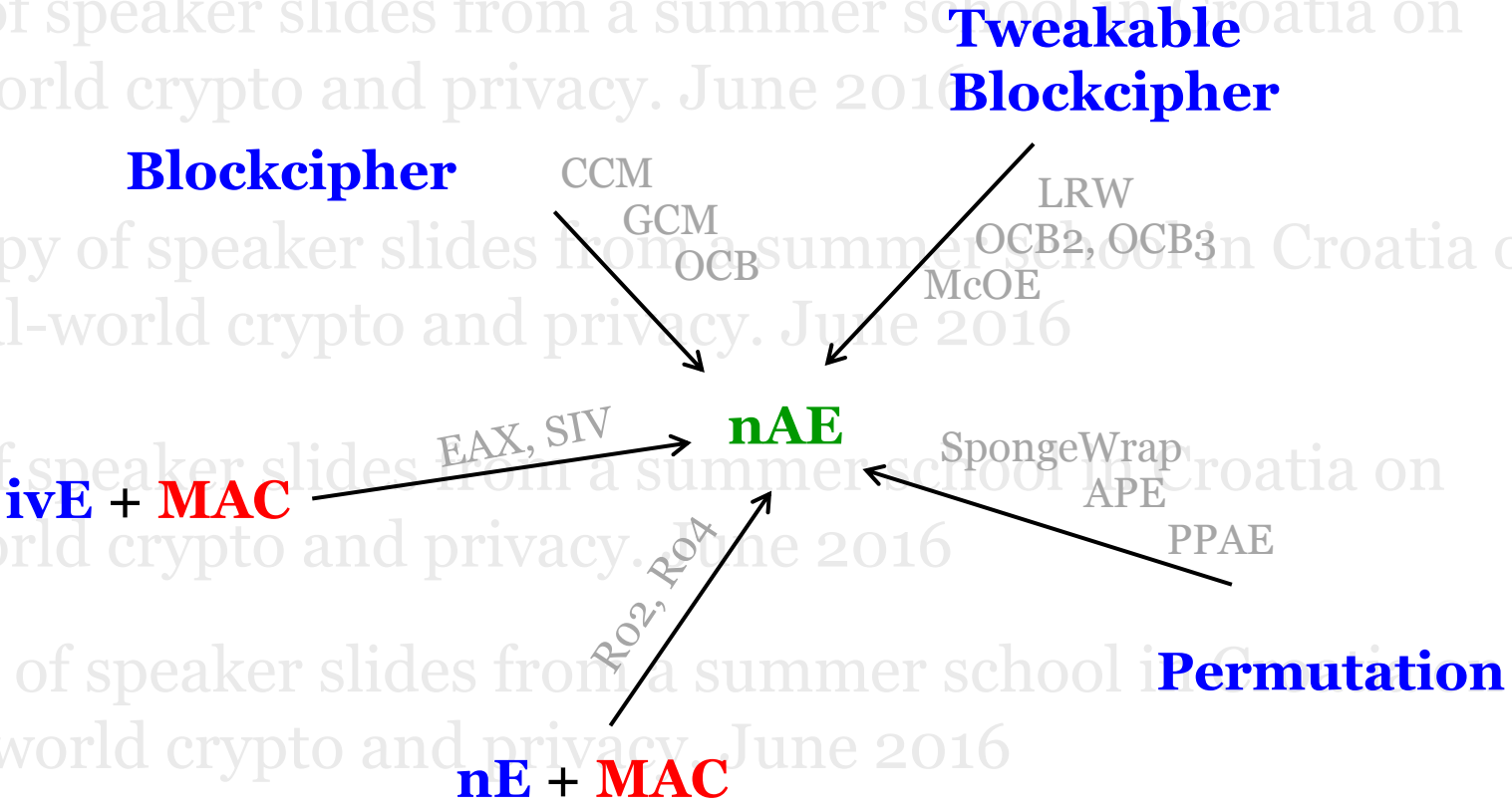
All wrong.

- The IV is not included in the MAC
- The IV is not required to be random
- The underlying encryption modes and MACs aren't total

Modern view of BN

pE + MAC → (BN) → pAE

Multiple starting points and ending points are possible

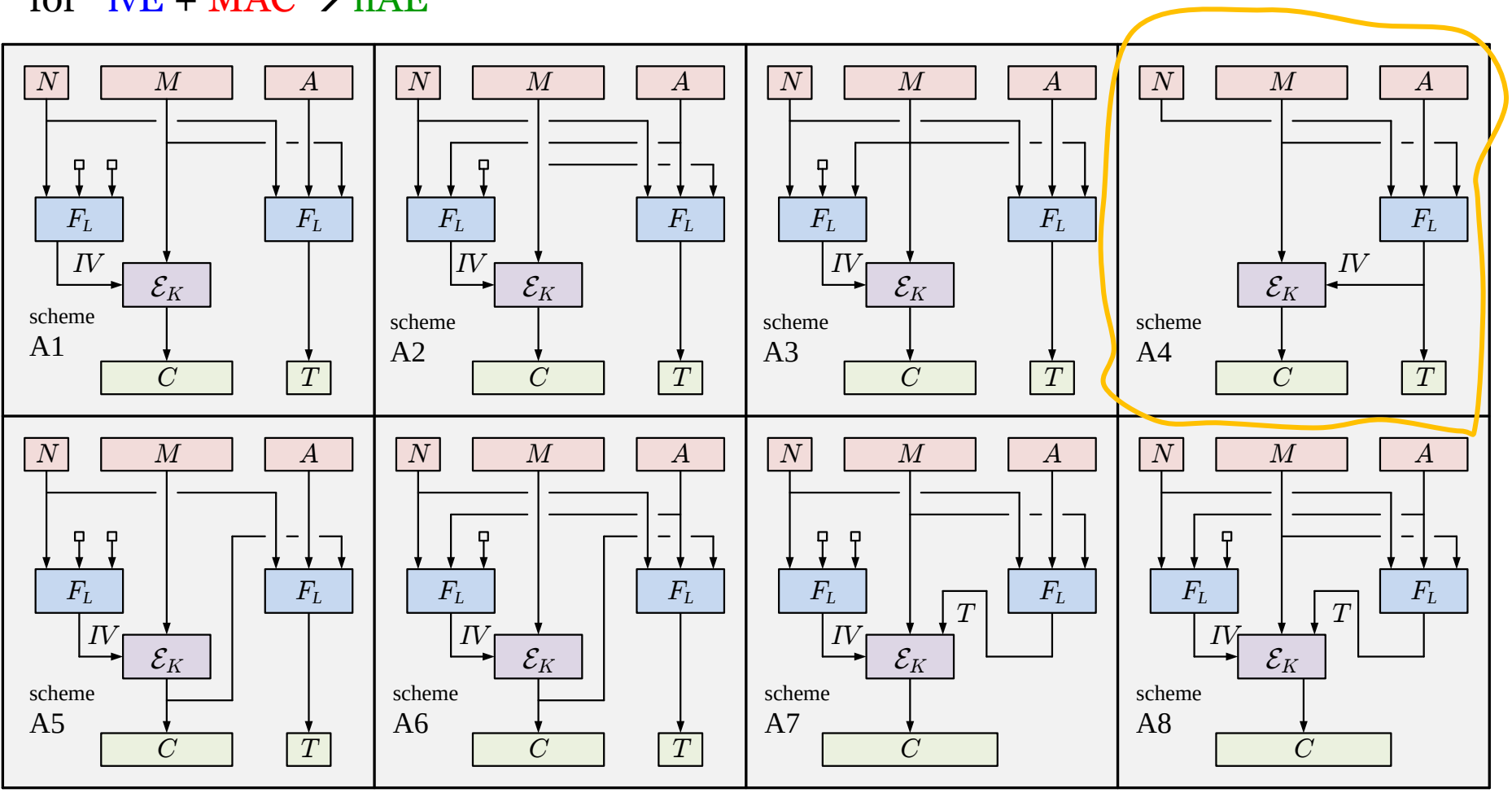


Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Eight "favored" schemes (of 160)

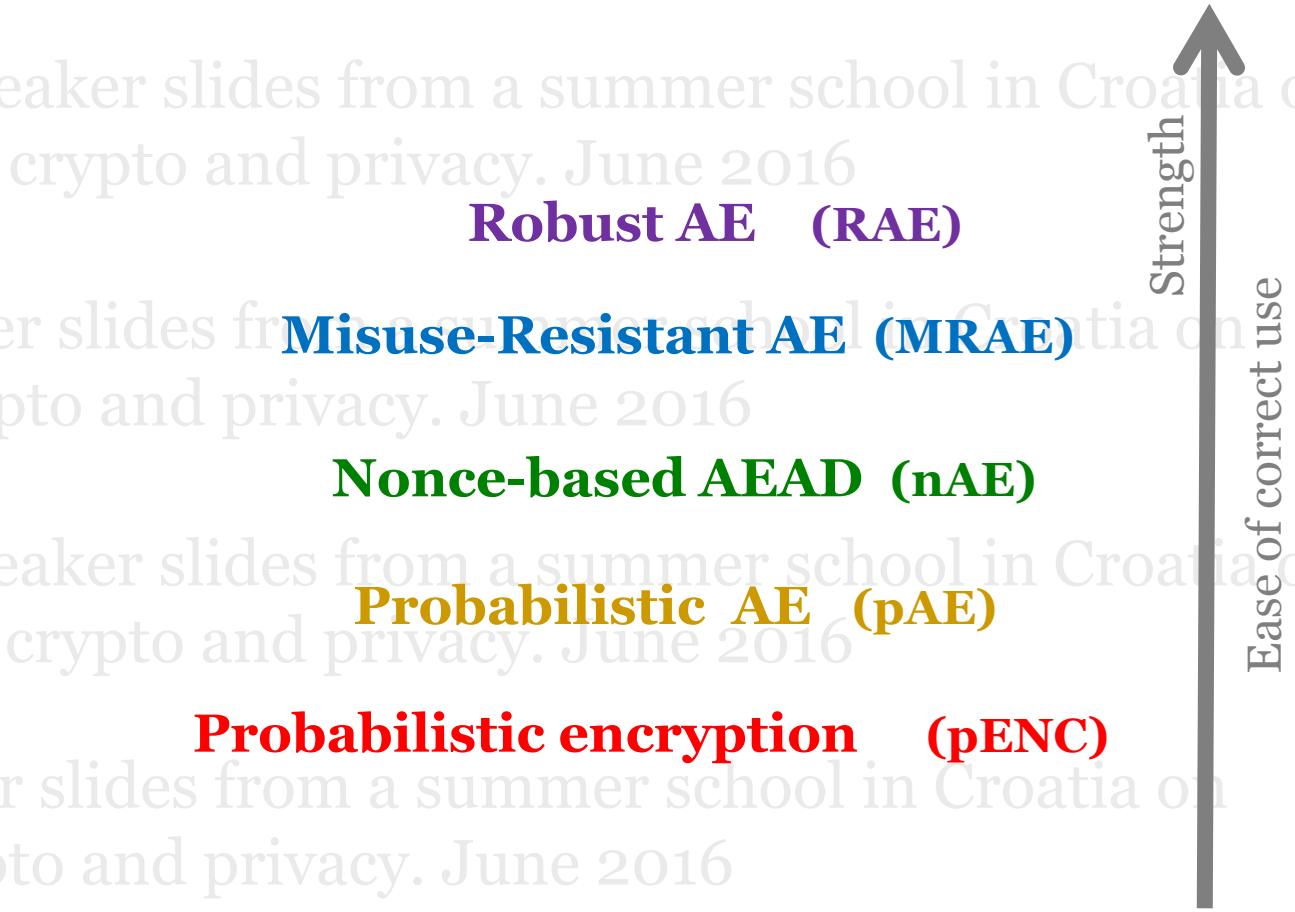
[Namprempre, Rogaway, Shrimpton 2014]

for ivE + MAC → nAE



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

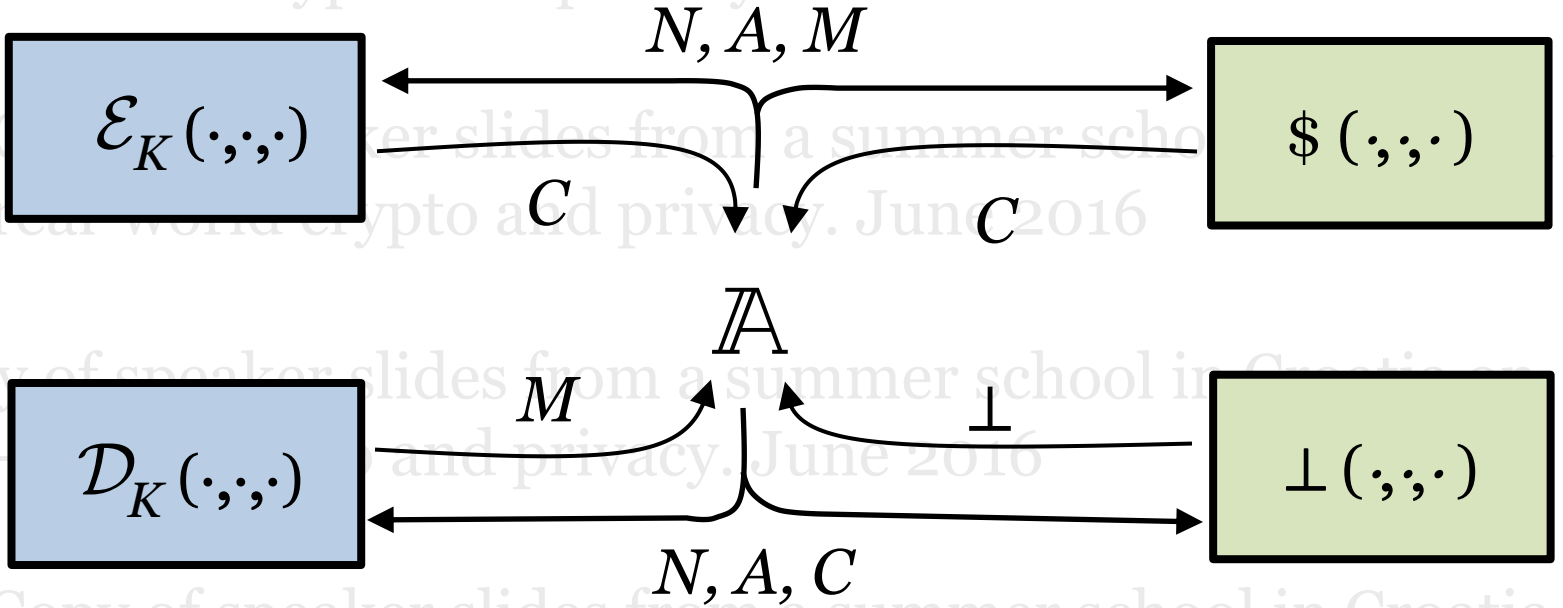
AE works by strengthening definitions



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

MRAE

[Rogaway, Shrimpton 2006]



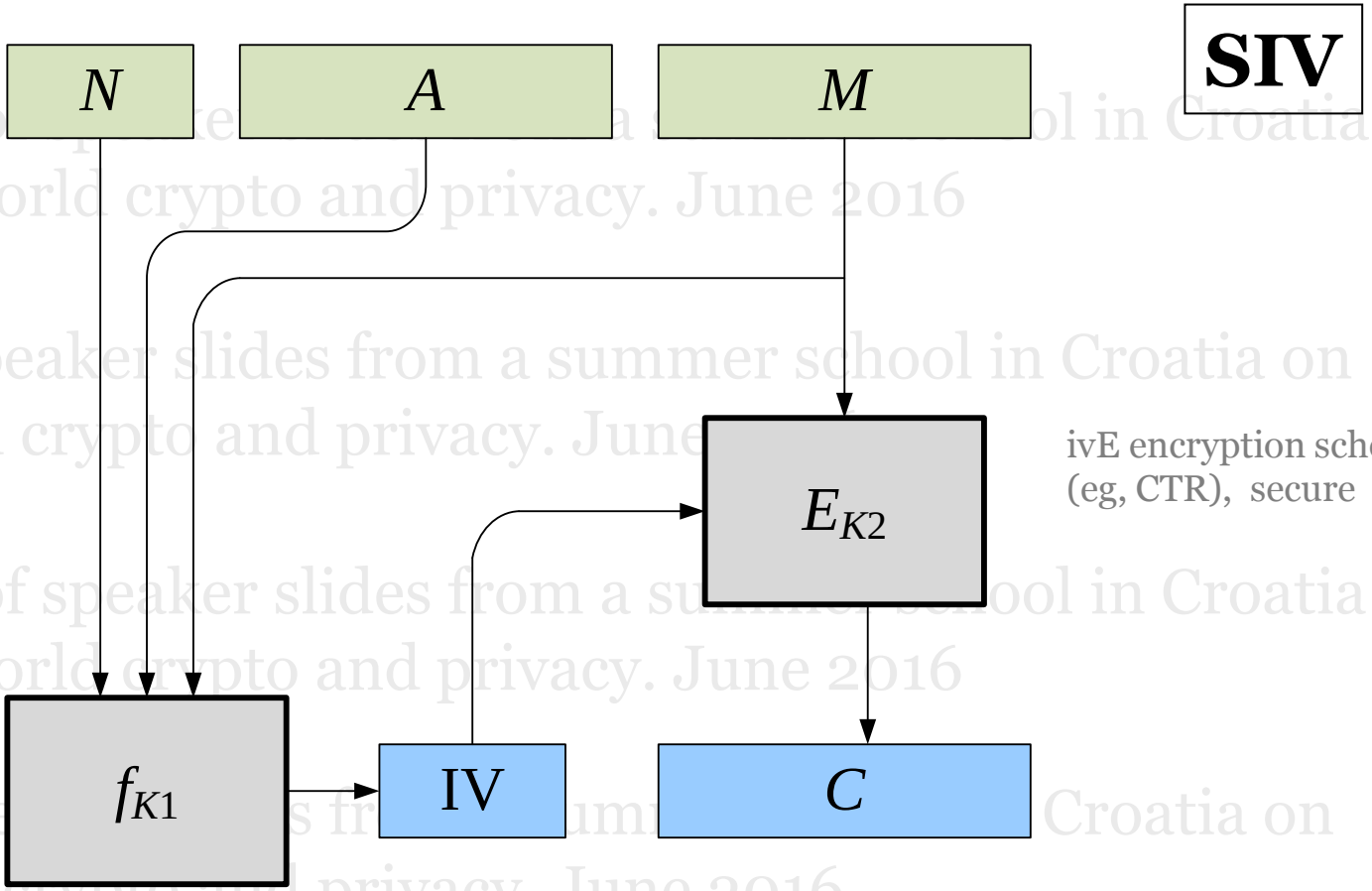
1. **Nonce-reuse security**: A repeated N **shouldn't** be cataclysmic
2. **Novelty exploitation**: Uniqueness of (N, A, M) **should** suffice

$\mathbb{A}$ may not ask queries that would trivially result in a win. It may not:

- Repeat an (N, A, M) enc query
- Ask a dec query (N, A, C) after C is returned by an $(N, A, \cdot)$ enc query

MRAE

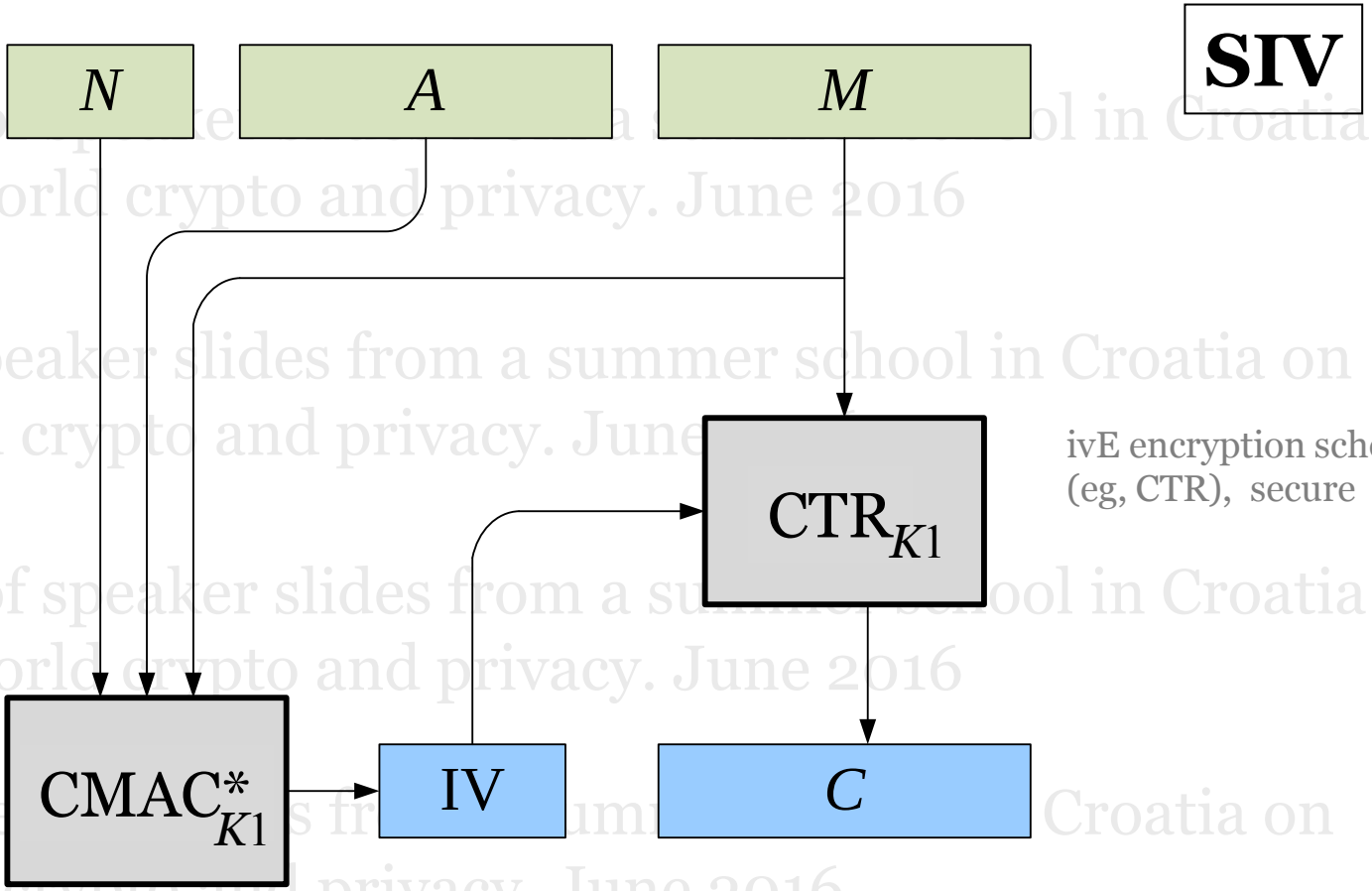
[Rogaway, Shrimpton 2006]



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

MRAE

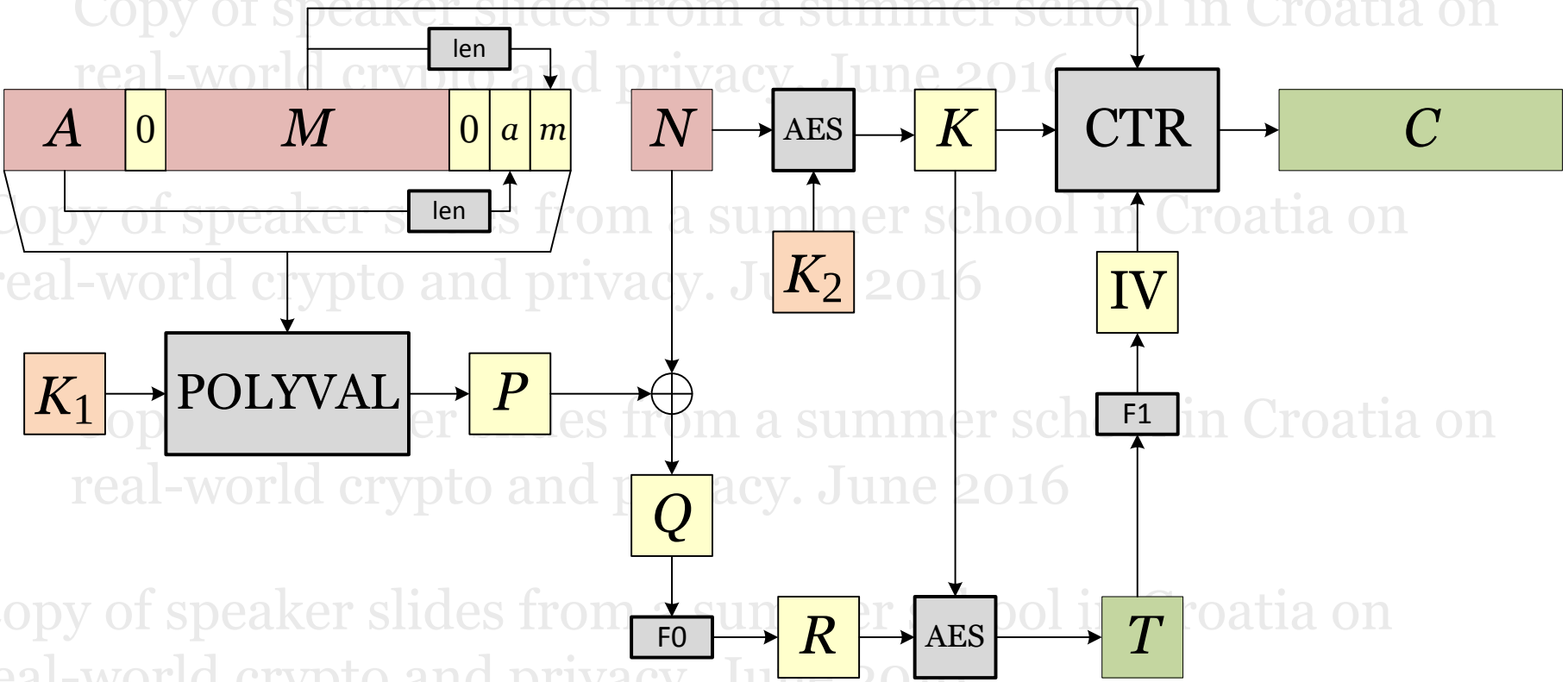
[Rogaway, Shrimpton 2006]



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

MRAE by GCM-SIV

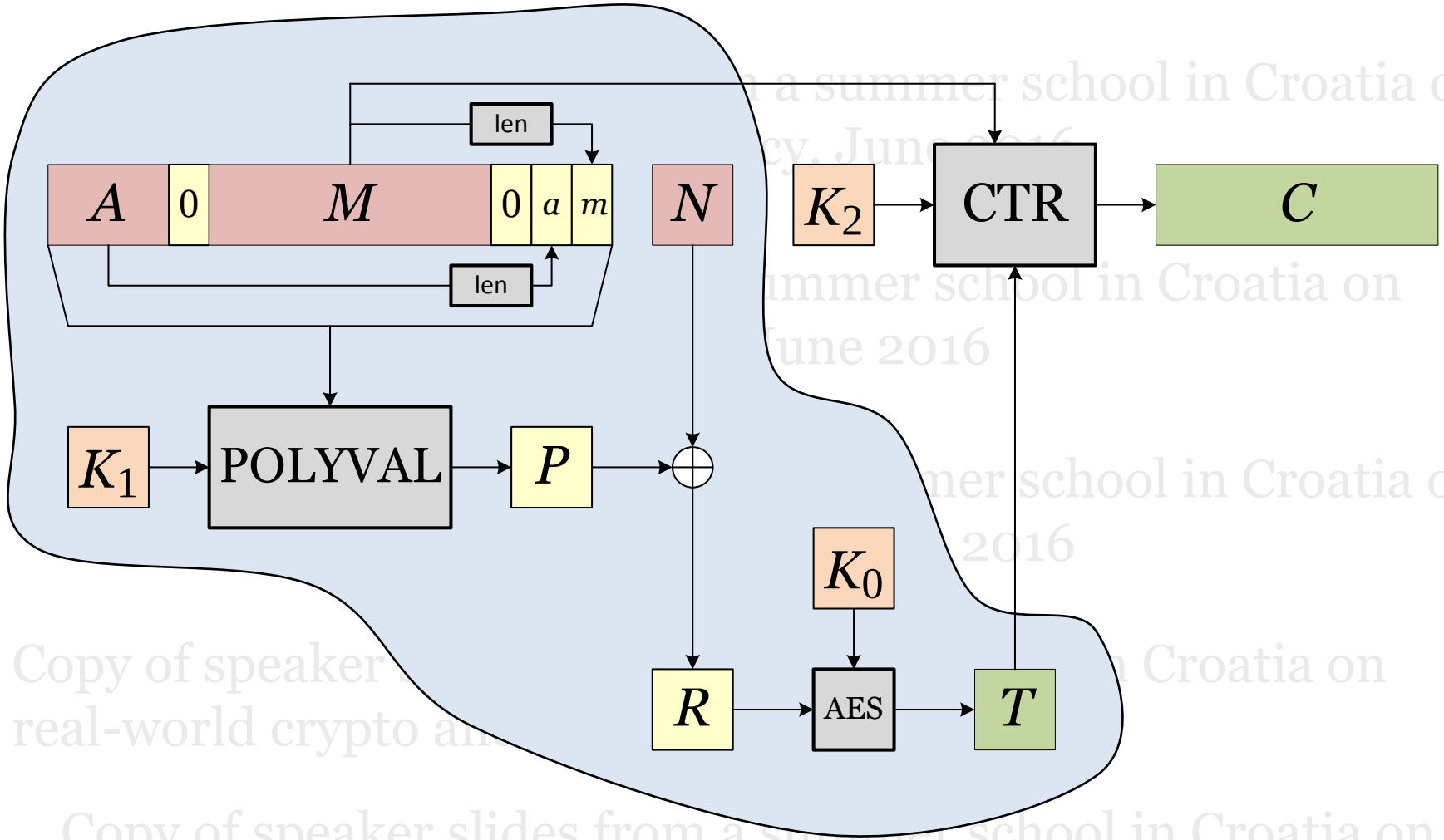
[Gueron, Langley, Lindell 2016]
[Gueron, Lindell 2015]



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

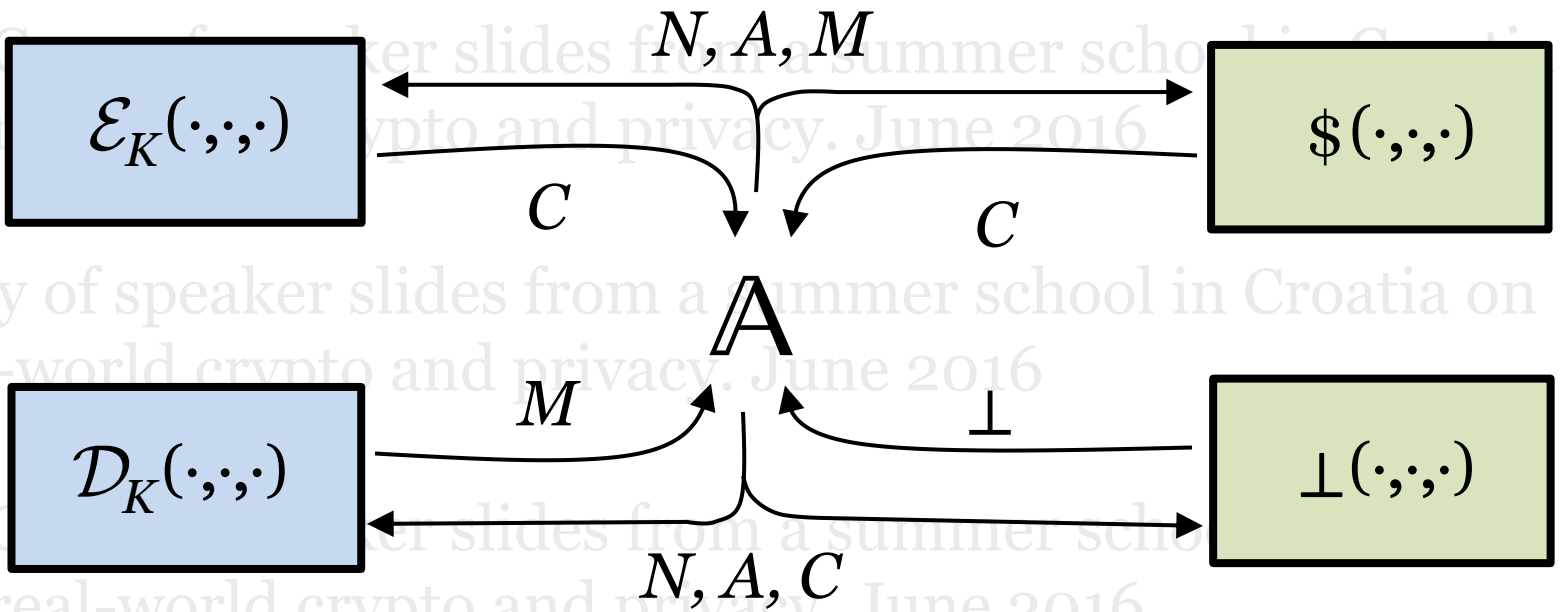
MRAE by GCM-SIV-simplified

[Gueron, Langley, Lindell 2016]
[Gueron, Lindell 2015]



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

A limitation of MRAE

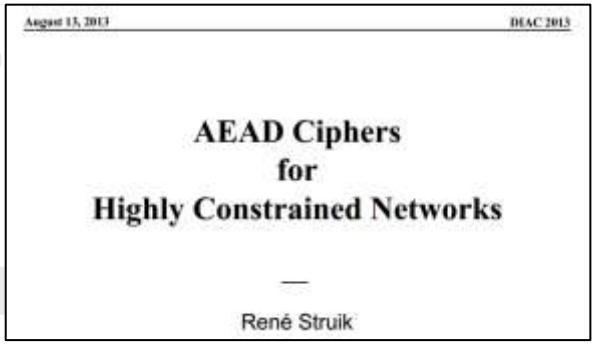


Effectively **requires**

$|C| = |M| + \lambda$

for **reasonably large** λ

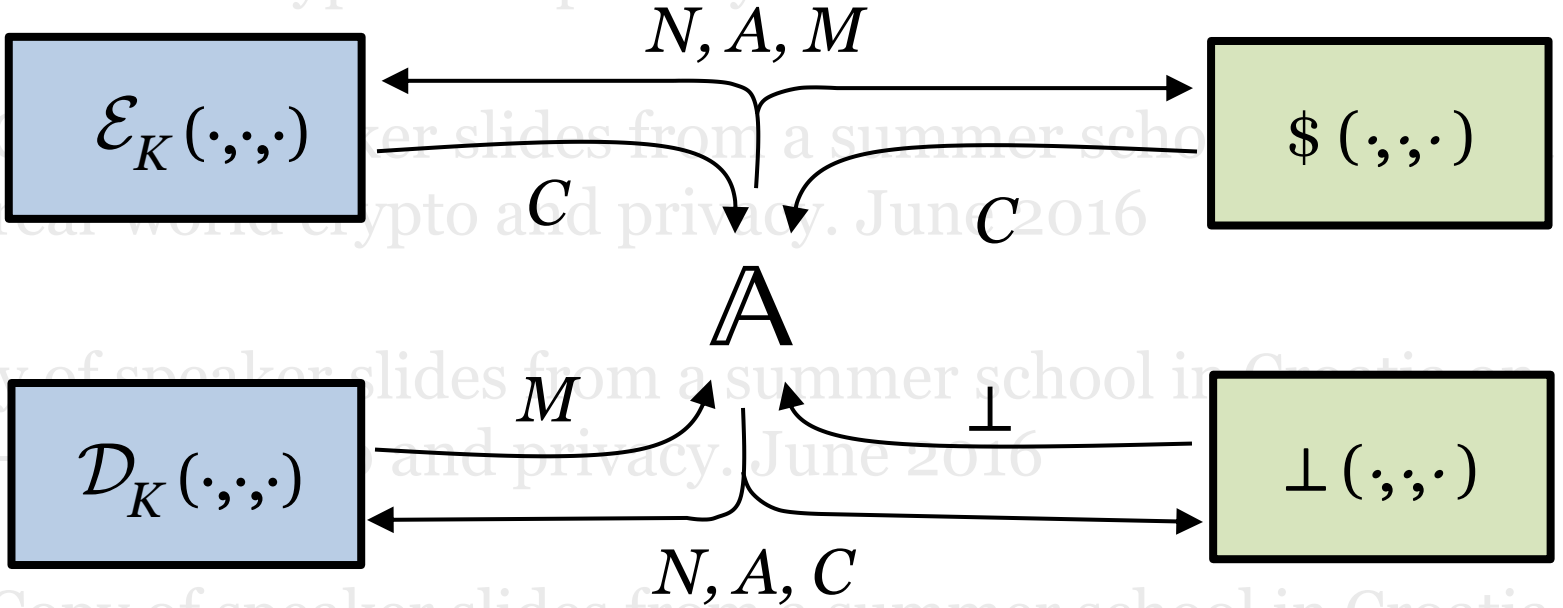
The utility of short authenticated ciphertexts



- Looked at "internet of things" settings – IEC 62951, ZigBee, …
- *Shaving off 8 octets may justify making symmetric-key crypto 10× more expensive* [slide 12]
- Following [BR2000], wanted to exploit authenticity already present in messages.
- These messages may be short
- *Authentication tags may be "evil" (authenticity is <u>not</u>)* [slide 29]

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

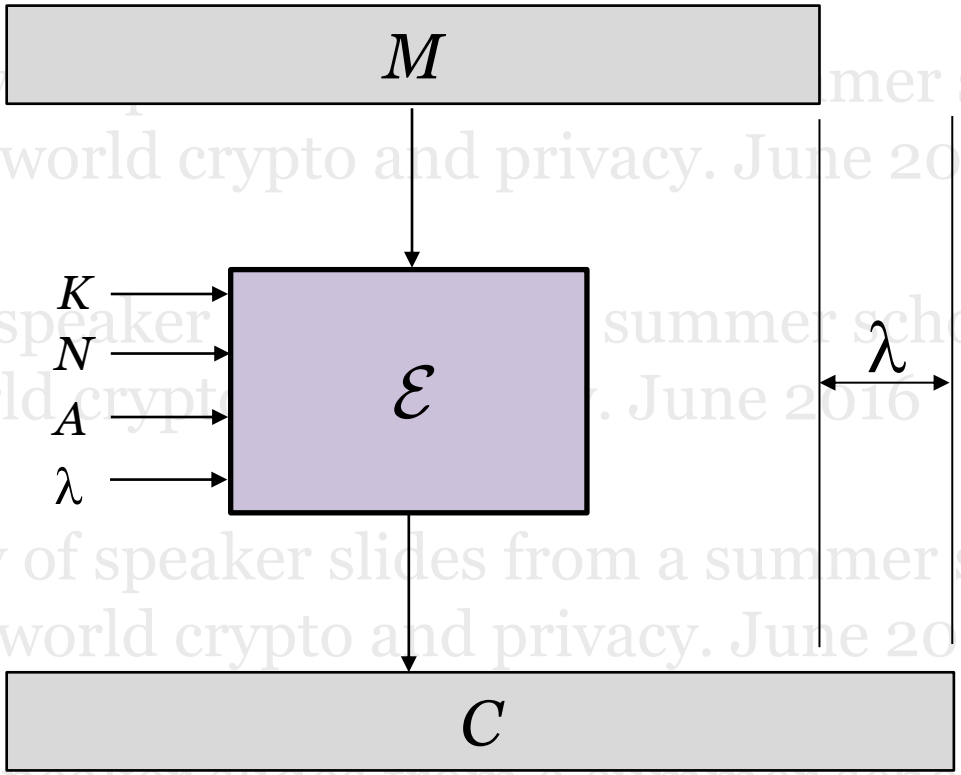
Robust AE



1. **Nonce-reuse security**: A repeated N **shouldn't** be cataclysmic
2. **Novelty exploitation**: Uniqueness of (N, A, M) **should** suffice
3. **Low ciphertext expansion possible** – even **no** expansion
4. **Redundancy exploitation**: Message-validity checks should **help**
   If valid messages have density ρ then having the decrypting party verify validity should enhance authenticity by -lg(ρ) bits
5. **Decryption-leakage security**: Divulging an **invalid** M shouldn't hurt
   The **caller** determines validity of M, and we can't control what it does

[Hoang, Krovetz, Rogaway 2014]

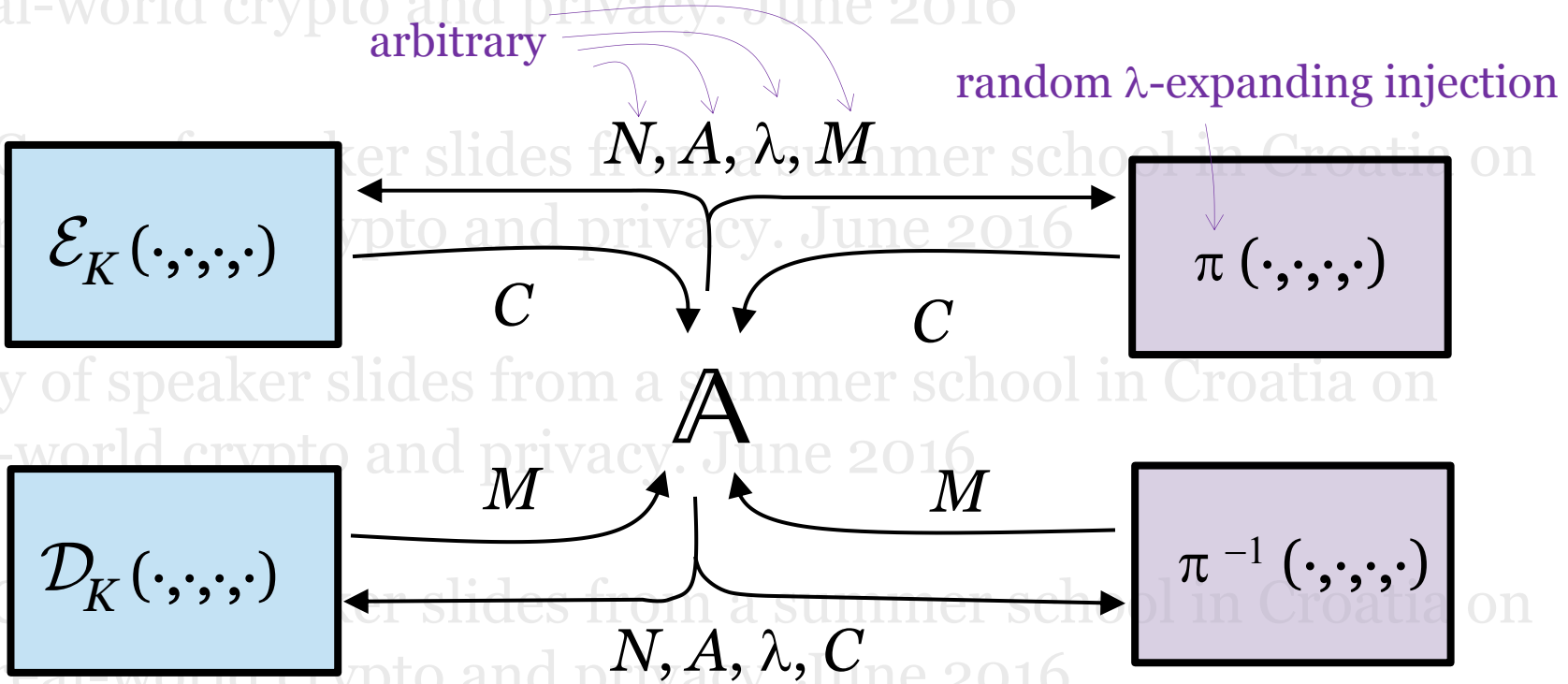
Robust AE



$|K|, |N|, |A|, |M|, \lambda$ **arbitrary**

User chooses the signature —
"expand by $\lambda \geq 0$ bits"
Gets best possible security for λ

Robust AE

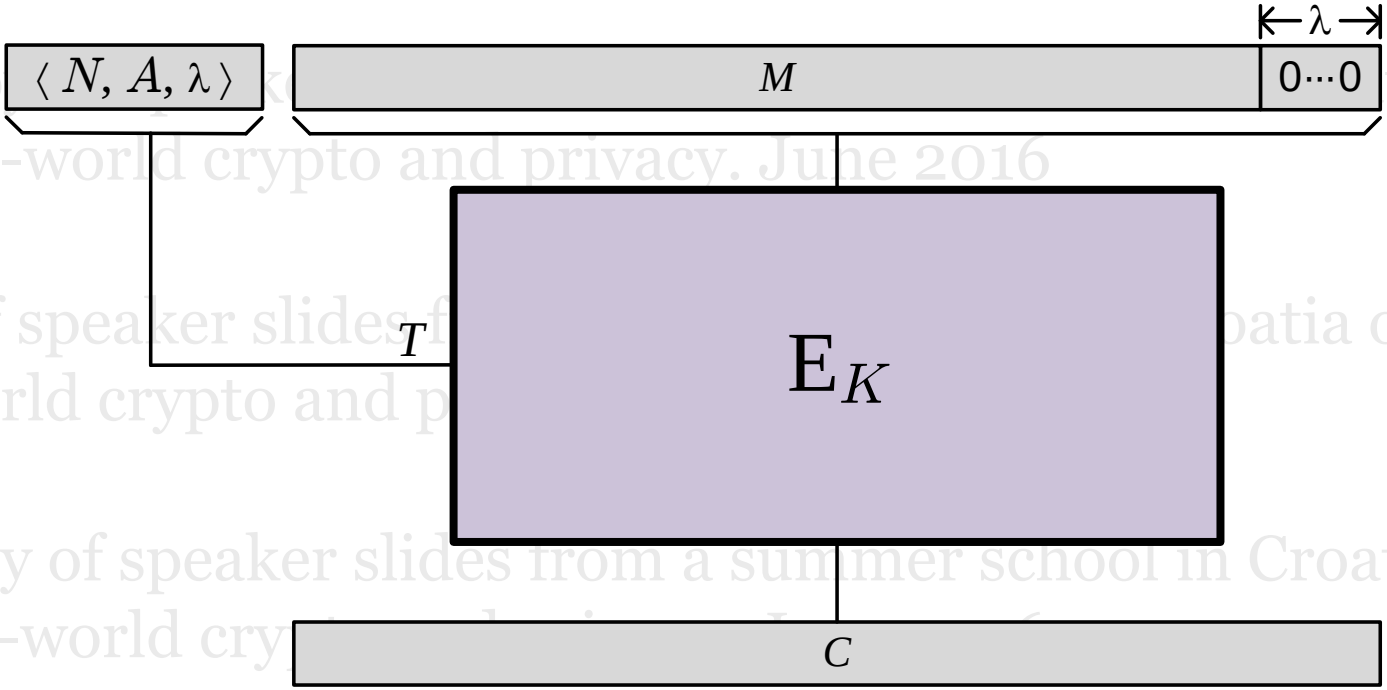


$$\mathbf{Adv}^{\mathrm{rae}}_{\Pi}(\mathbb{A}, k) = \Pr[\mathbb{A}^{\text{Real}} \to 1] - \Pr[\mathbb{A}^{\text{Fake}} \to 1]$$

Like a **pseudorandom injection** [R, Shrimpton 2006] but now understood **prescriptively**, for all λ — not just an alternative characterization of an MRAE scheme

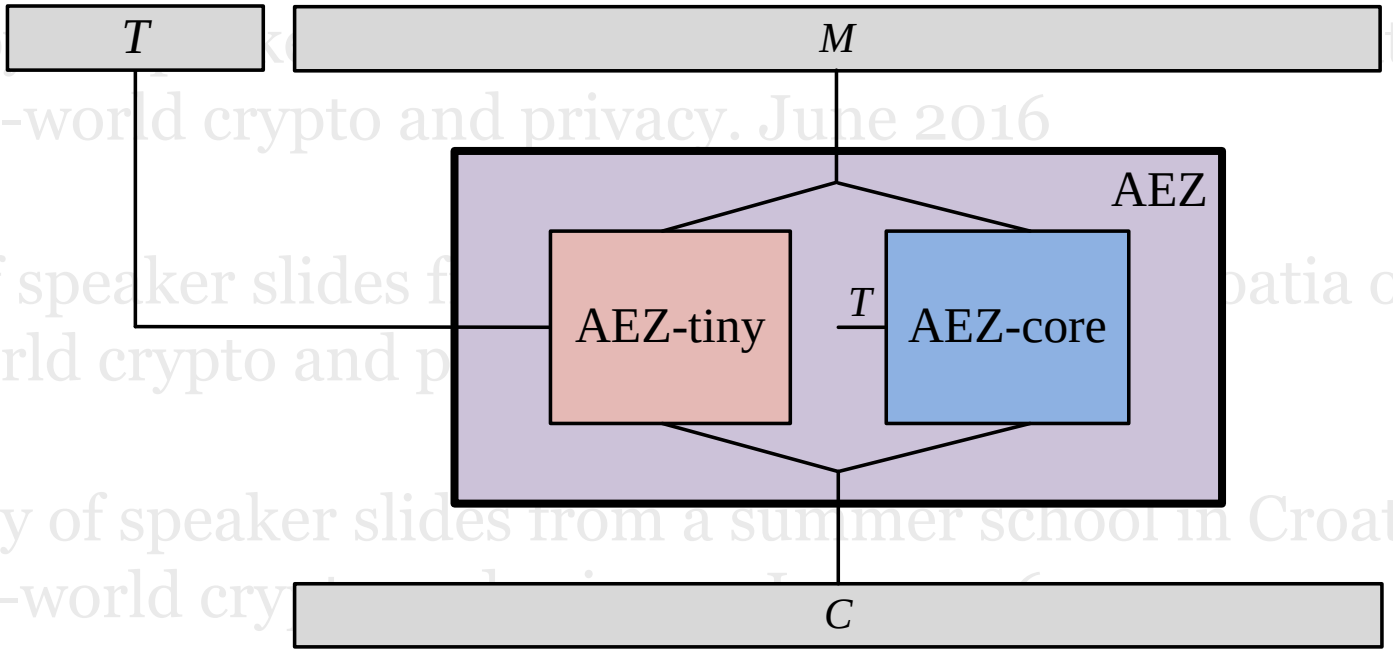
Achieving RAE
Enciphering-based encryption

[Hoang, Krovetz, Rogaway 2014]
following [Bellare, Rogaway 2000]
[Shrimpton, Terashima 2013]



Need E secure as a strong, AIL, VIL, tweakable PRP –
a "**generalized blockcipher**"

Making the enciphering scheme



AEZ-tiny
FFX-like (Feistel)
[NIST SP 800-38G]
AES4-Based

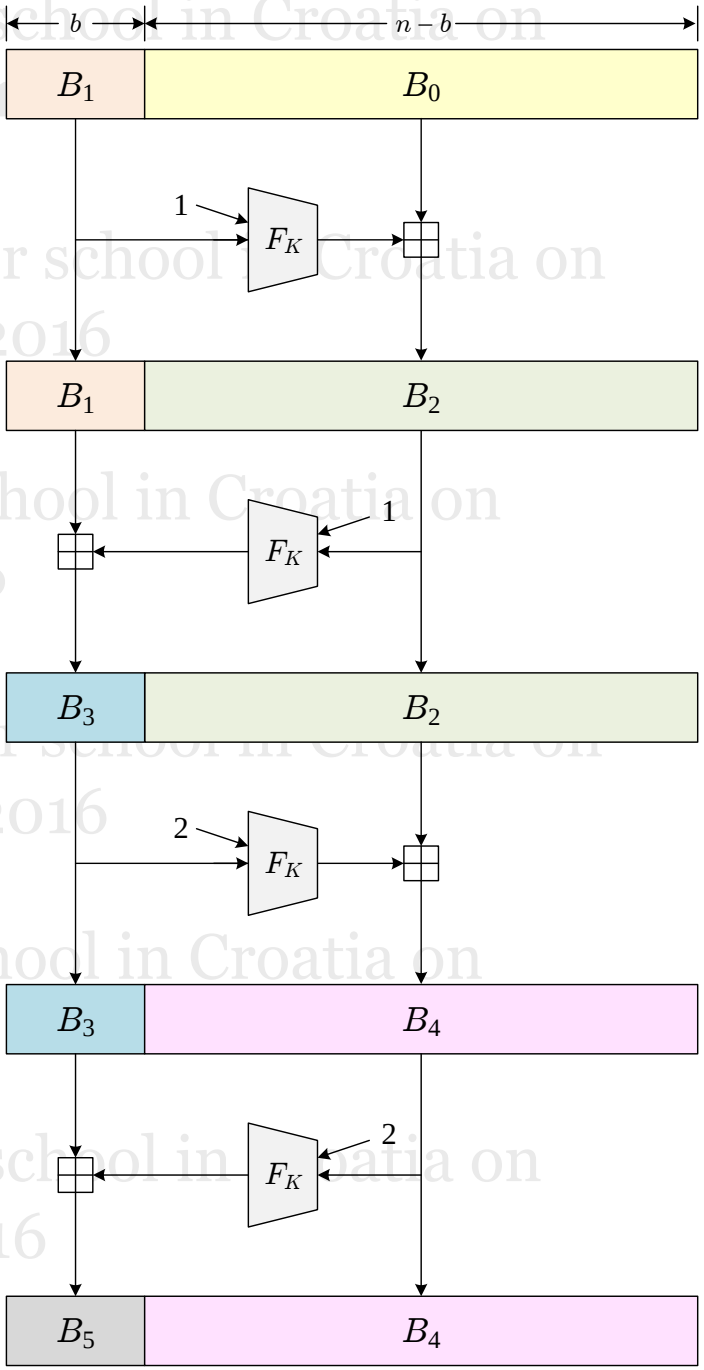
AEZ-core
Builds on EME [Halevi, Rogaway]
and OTR [Minematsu 2014]
AES4 & AES based.

Building the wide-block blockcipher

NR, CMC, EME, EME2,
HCTR, PEP, HCH, TET,
HEH, …

Other recent work

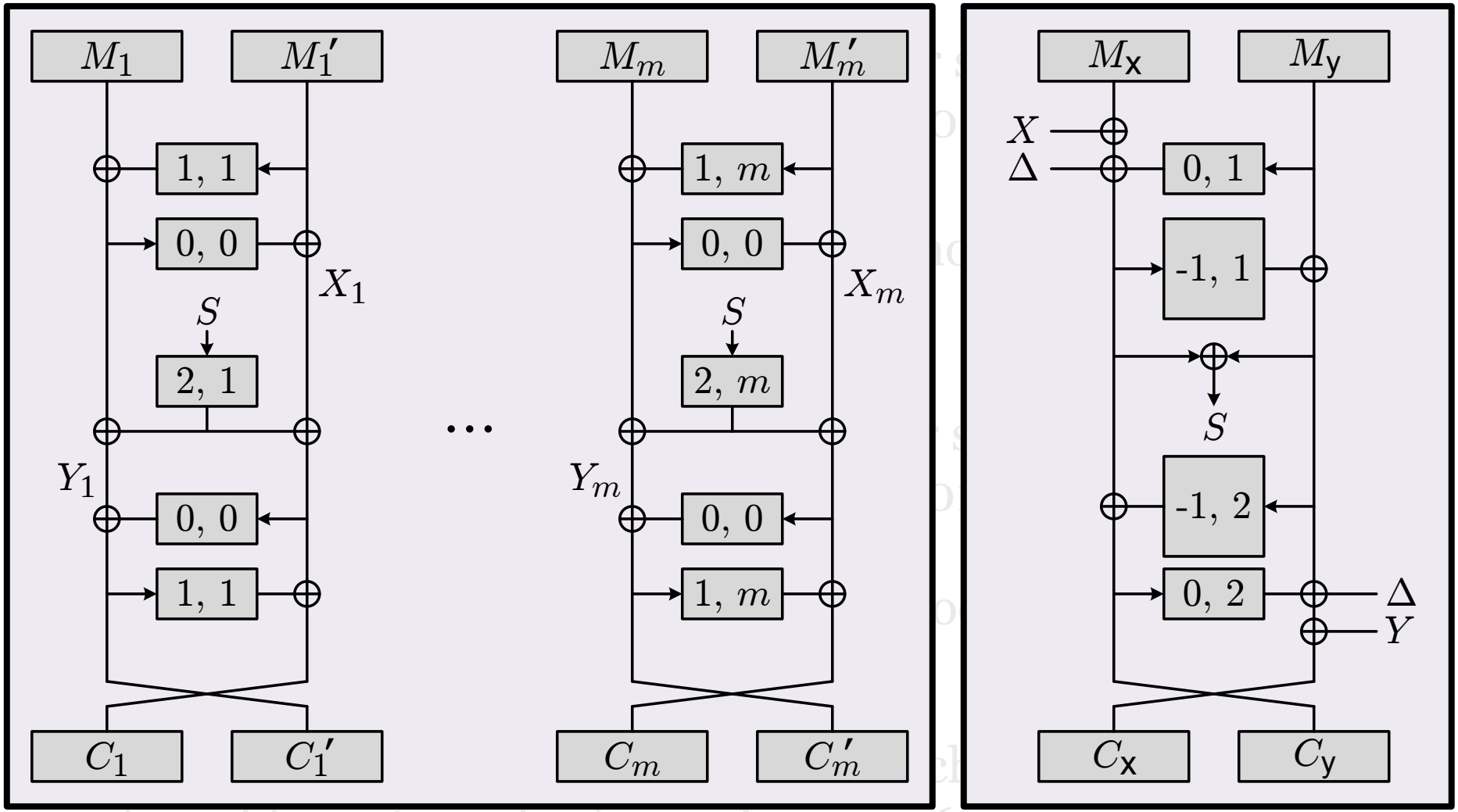
- **Mr. MONSTER BURRITO**
  [Keccak team, 2014]
- **HHFHFH**
  [Bernstein, Nandi, Sarkar 2016]

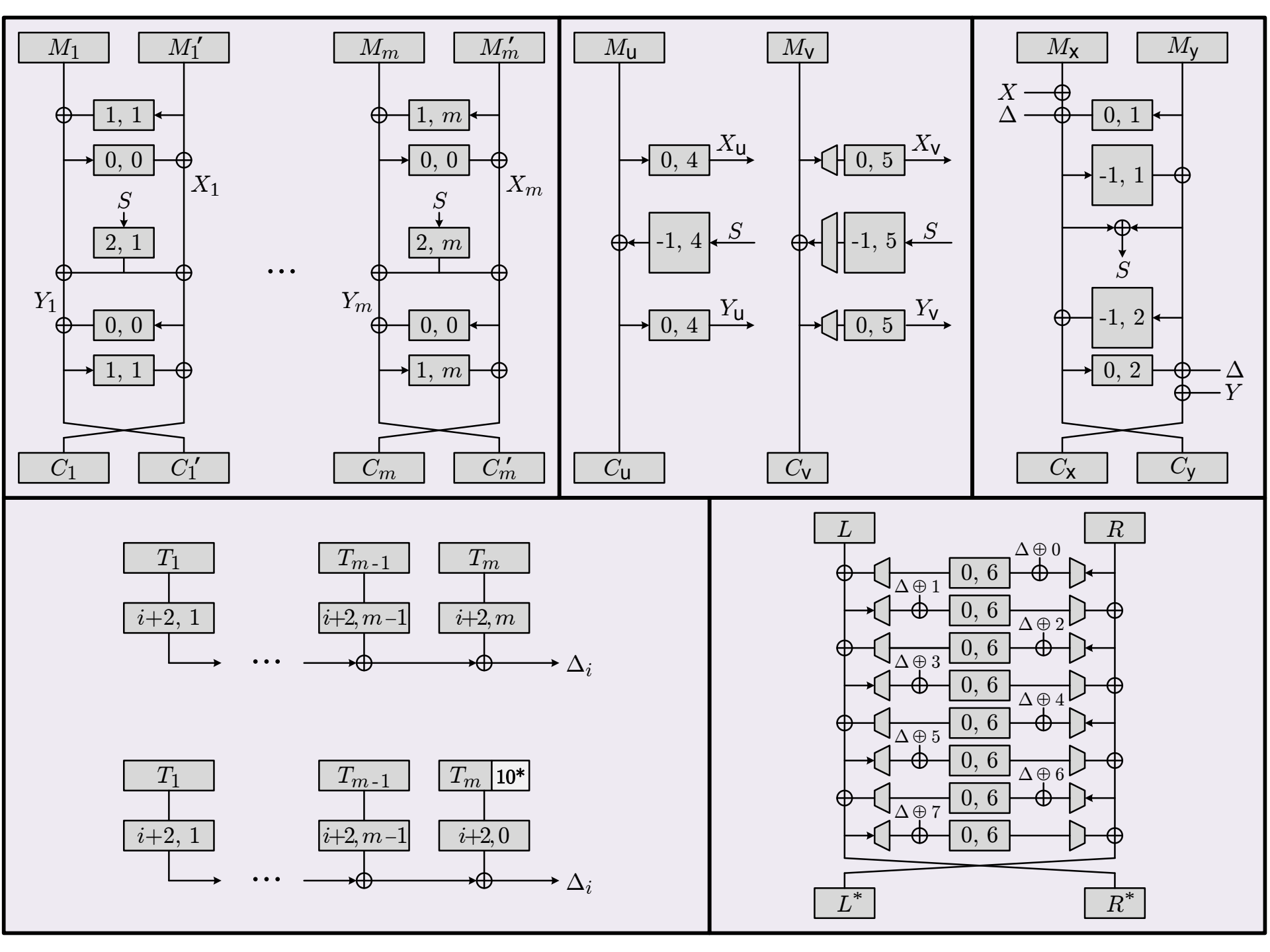


First attempt at AEZ-core →
Inspired by [Luby, Rackoff 1988] and BEAR/LION [Anderson, Biham 2007]

AEZ-core

Messages with an **even** number of blocks, all of them **full**




M_1
M_1'
M_m
M_m'
1, 1
0, 0
1, m
X_1
X_m
S
2, 1
2, m
Y_1
Y_m
1, 1
1, m
C_1
C_1'
C_m
C_m'
M_u
M_v
0, 4
0, 5
X_u
X_v
-1, 4
-1, 5
Y_u
Y_v
C_u
C_v
M_x
M_y
X
Δ
0, 1
-1, 1
-1, 2
0, 2
Y
C_x
C_y
T_1
T_{m-1}
T_m
i+2, 1
i+2, m−1
i+2, m
Δ_i
10*
i+2, 0
L
R
$\Delta \oplus 0$
$\Delta \oplus 1$
$\Delta \oplus 2$
$\Delta \oplus 3$
$\Delta \oplus 4$
$\Delta \oplus 5$
$\Delta \oplus 6$
$\Delta \oplus 7$
0, 6
L^*
R^*

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Theorem. Let E be a TBC and Π = AEZ-core[E].

Then there's explicit and efficient reduction Rx such that

$$\mathbf{Adv}^{\mathrm{rae}}_{\Pi}(\mathbb{A}) \le 3.5\, s^2 / 2^{128} + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathbb{B})$$

where $\mathbb{B}$ = Rx($\mathbb{A}$, E) and s is the total number of blocks asked by $\mathbb{A}$.

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

"Prove-then-prune" design

In general	For AEZ
Assume some primitive	A tweakable blockcipher (TBC) (tweak space $\mathbb{Z} \times \mathbb{Z}$)
Design assuming the primitive meets some standard assumption	The TBC is good as a tweakable PRP
Instantiate with a "standard" primitive: the **scaled-up** design	Not what was done with AEZ
Instantiate with a mix of standard and reduced-round primitives: the **scaled-down** design	What was done with AEZ, using AES + AES4 (apart from their key schedule)

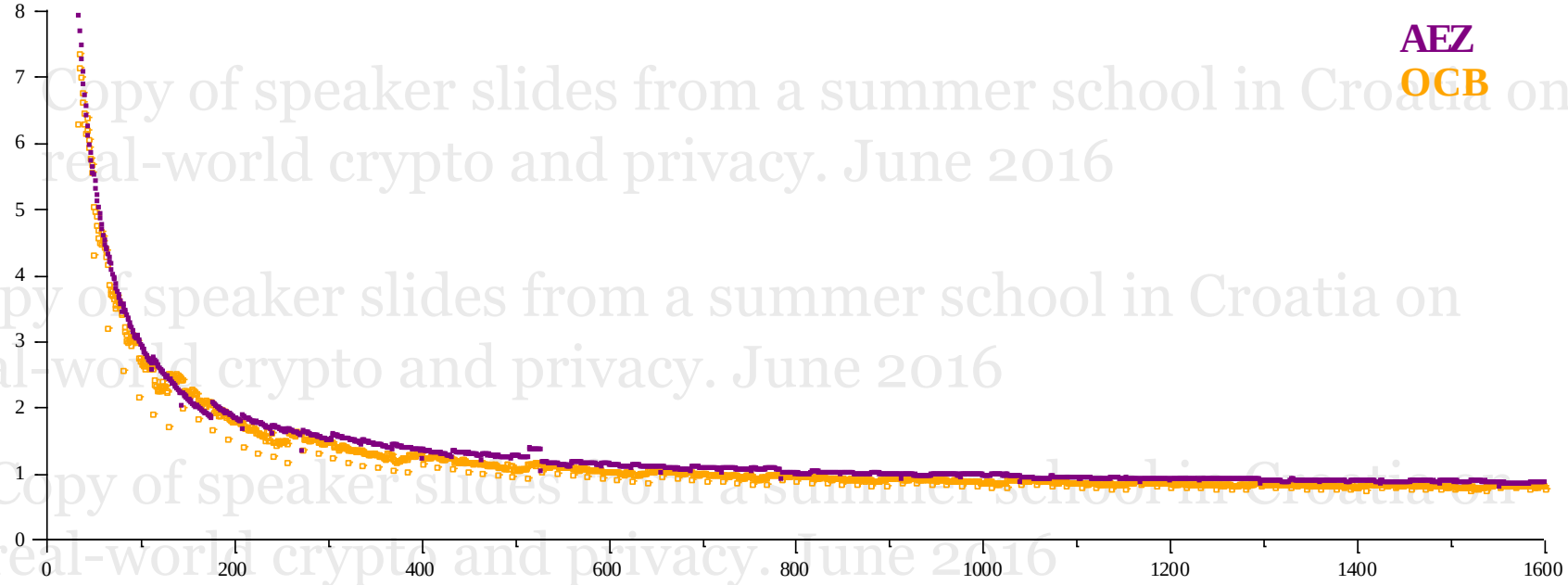
Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

AEZ Performance

Haswell i5-4570S (2.9 GHz), cpb vs bytes,
C with “intrinsic” function calls, GCC 4.9, -marc=native –O3

Not far from AES-CTR
which has **0.63 cpb**
as a theoretical limit

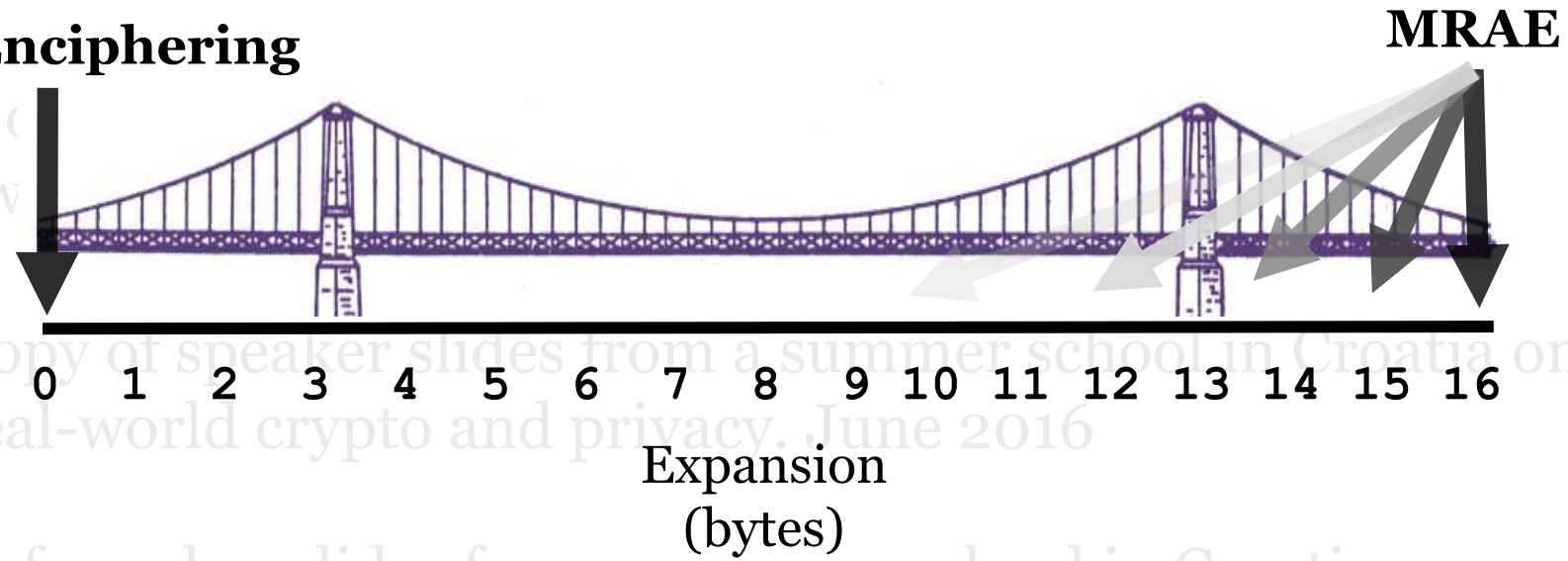
Encrypt/decrypt: **0.64 cpb** on “Skylake”
Reject invalid ciphertext: **0.31 cpb**
MAC: **0.29 cpb**



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

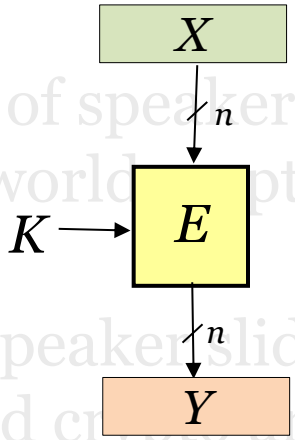
Robust AE

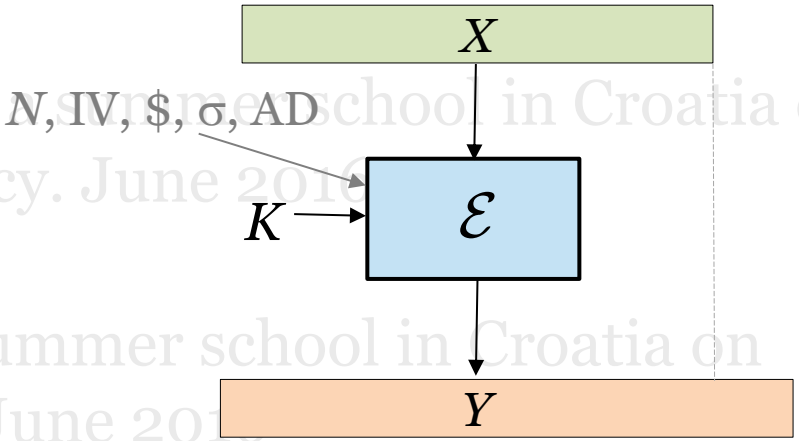
Connects enciphering and AE



Copy of speaker slides from a summer school in Croatia on real-world crypto and privacy. June 2016

Blockcipher | Symmetric encryption scheme





Simple object	Fairly complex object
Stable security notion	Contested security notions
Fixed-length input	Arbitrary-length input
Length-preserving	Possibly length-increasing
Plaintext repetitions revealed	Plaintext repetitions concealed
No nonces, IV, randomness, state	Nonces, IV, randomness, or state
No associated data	Associated data

Maybe **not** so very different.
When defined strongly enough–RAE–the notions and techniques are ultimately similar

Conclusions

Finding useful definitions is quite dialectical.

Need to lose implicit normative sensibilities (encryption is for privacy, encryption must be probabilistic, …)

New definitions & primitives can eclipse old ones and impact practice. Need standards and advocates.

Theory-for-practice can genuinely benefit practice. AE is a domain where this has clearly happened.