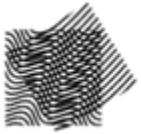
KATHOLIEKE UNIVERSITEIT LEUVEN

Authenticated Encryption and the CAESAR Competition

Elena Andreeva
COSIC, KU Leuven, Belgium

Real World Cryptography Workshop 2015
London, UK
08/01/2015



Security Goal

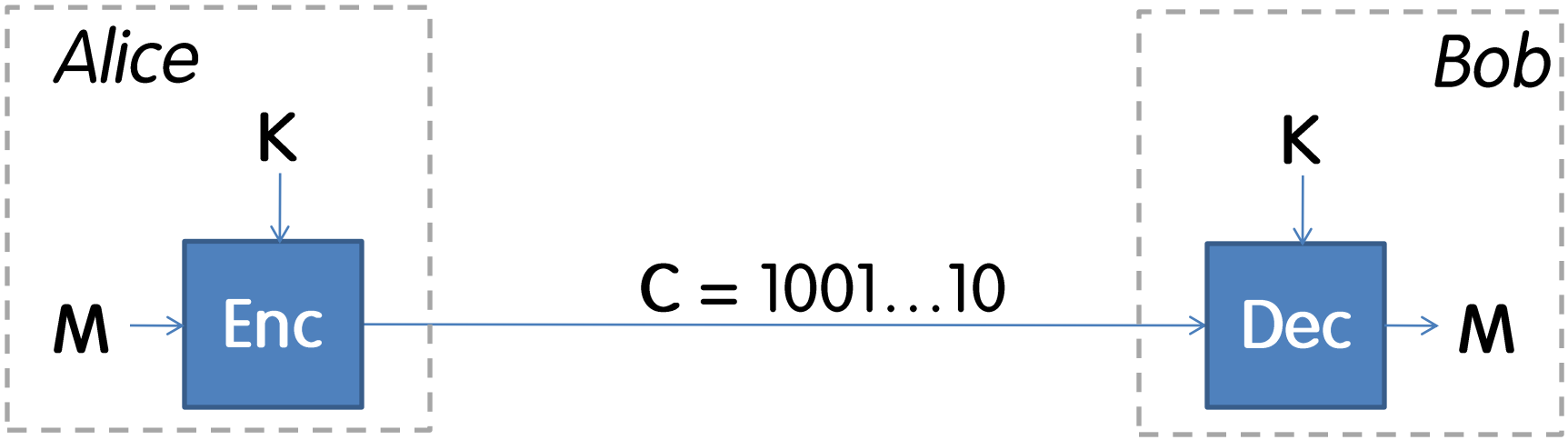
Authenticated Encryption
(AE) Scheme

Confidentiality + Authenticity

Confidentiality

- **Traditionally**

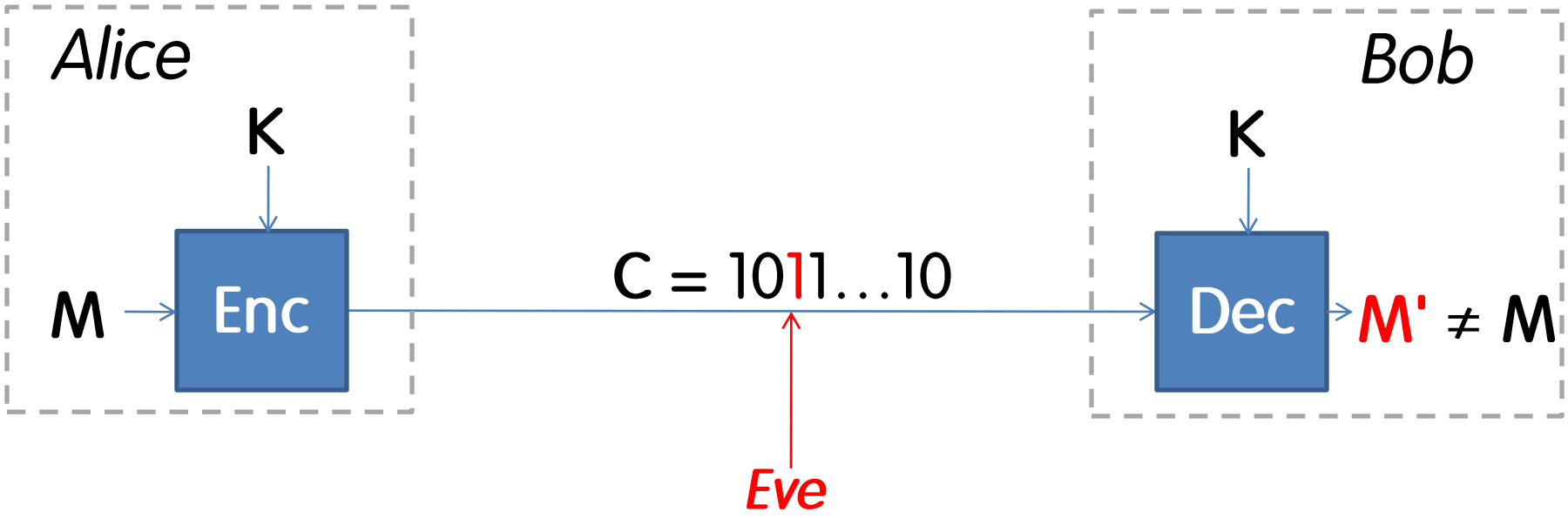
Encryption Scheme ➡ **Confidentiality**: Ind CPA/CCA



Confidentiality

- **Traditionally**

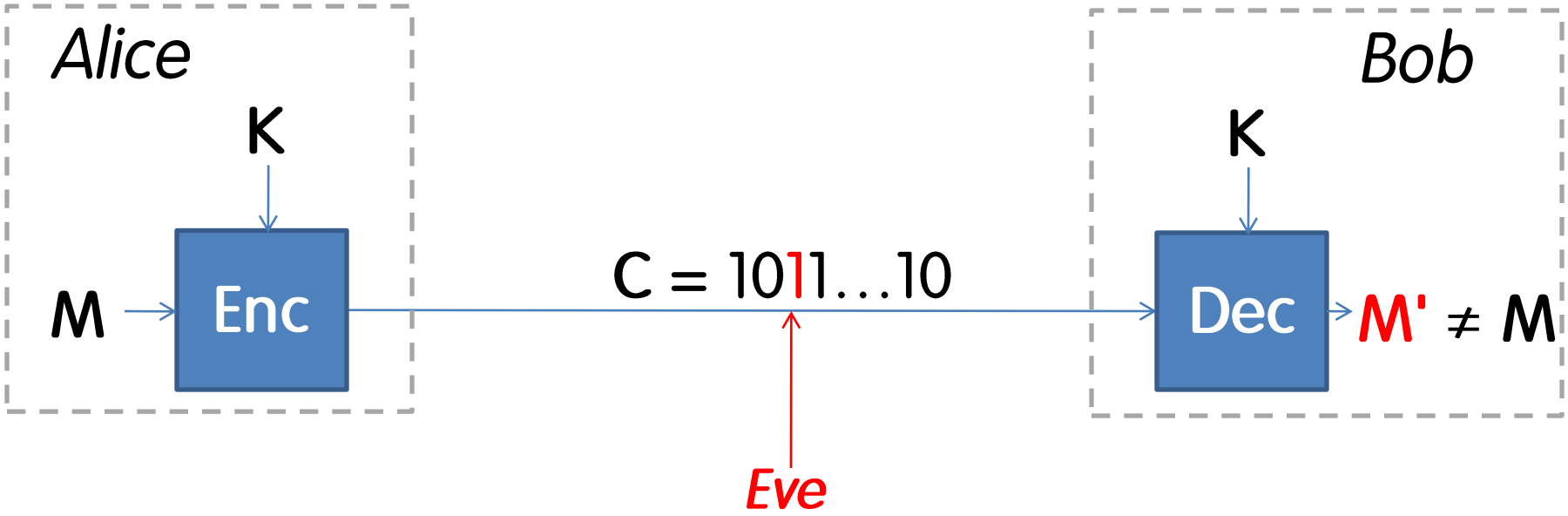
Encryption Scheme ⇒ **Confidentiality**: Ind CPA/CCA



Confidentiality

- **Traditionally**

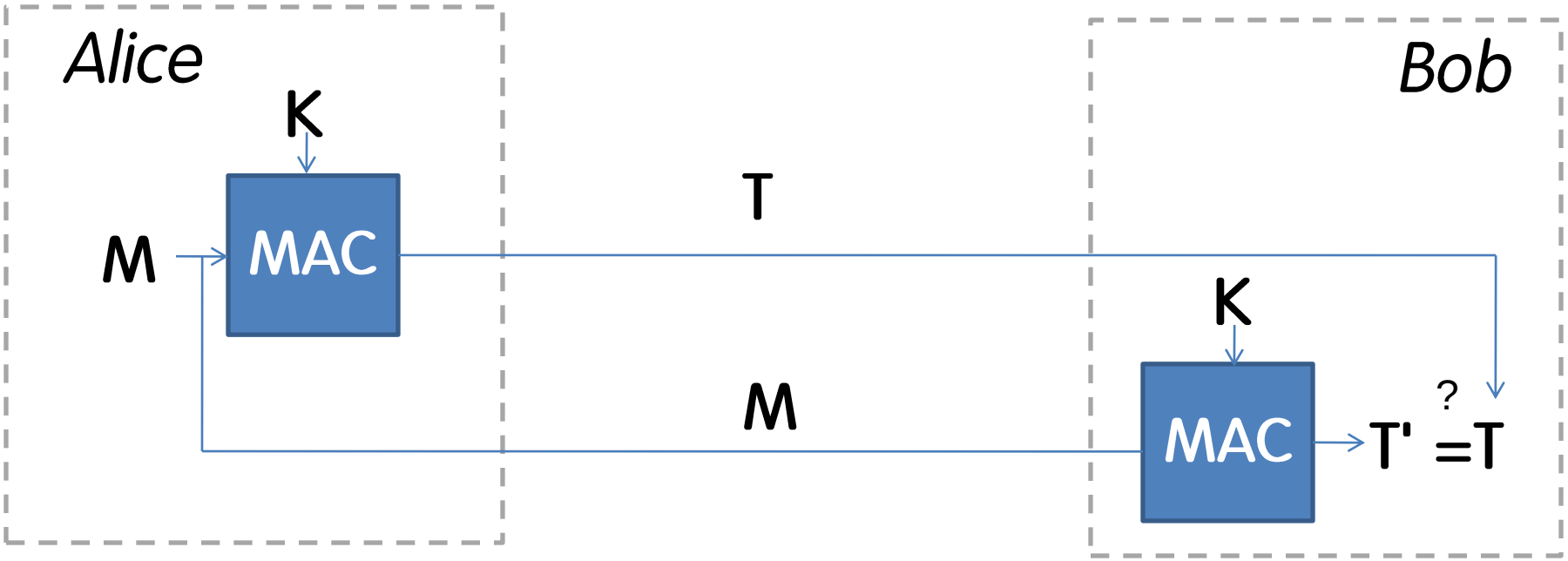
Encryption Scheme ⇒ **Confidentiality ≠ Authenticity**



Authenticity

- **Traditionally**

Message Authentication Code (MAC) → **Authenticity**: UF-CMA



Security Goal

- **Traditionally**

Encryption Scheme → **Confidentiality**: Ind CPA/CCA

Message Authentication Code (MAC) → **Authenticity**: UF-CMA

- **Nowadays**

Authenticated Encryption (AE) Scheme → **Confidentiality + Authenticity**
Ind CPA + Int-Ctxt

Main Question

How to achieve secure AE?

1. **Combine Enc + MAC**

   Generic composition:

   Bellare, Namprempre (2000), Namprempre et al. (2014)

2. **Dedicated AE schemes ≈ Inbetweeners ☺**

   State of the art

Generic Composition
Bellare, Namprempre (2000), Krawczyk (2001)

1. Encrypt and MAC Insecure

2. MAC then Encrypt Insecure

3. Encrypt then MAC Secure

Build probabilistic AE from probabilistic Enc

- Enc IV is random/state
- IV/state is communicated in-band

Generic Composition

1. **Encrypt and MAC** SSH
   [APW'09] OpenSSH attack: bad Enc and MAC interaction
   Timing attacks, …

2. **MAC then Encrypt** TLS
   In-model attack: BEAST [DR'11]! (SSL 3.0,TLS 1.0) CBC chaining IV
   Repair: TLS 1.1 and 1.2: random IV-CBC [K'01]
   Out-of-model attacks: Padding oracle [V02,CHVV03],
   Lucky 13 [AP'13]: SSLv3.0, TLS 1.0, 1.1, 1.2., DTLS

3. **Encrypt then MAC** IPsec, ISO/IEC 19772:2009

ISO 19772 Enc then MAC?

... choose appropriate "starting variable" (SV = IV) for Enc
C' = C || T where C = $Enc_{K1}(M)$ and T = $f_{K2}(C)$ ...

1. **Appropriate?**
- distinct for every M during the lifetime of a key
  Nonce? ➔Attack
- Chosen statistically unique SV is recommended
  Random? ➔OK

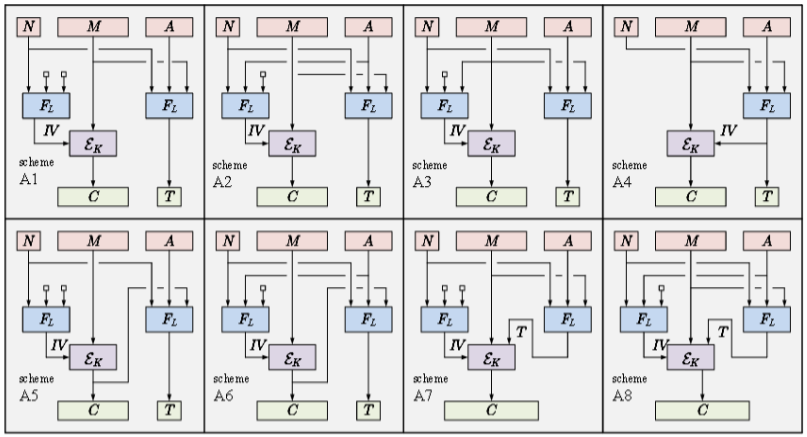
2. **Is SV part of C?**
- no ➔ Attack (for any SV choice)

Generic Composition Reconsidered
Namprempre et al. (2014)

1. IV (random)-Enc + MAC

Nonce-based AE from IV-Enc

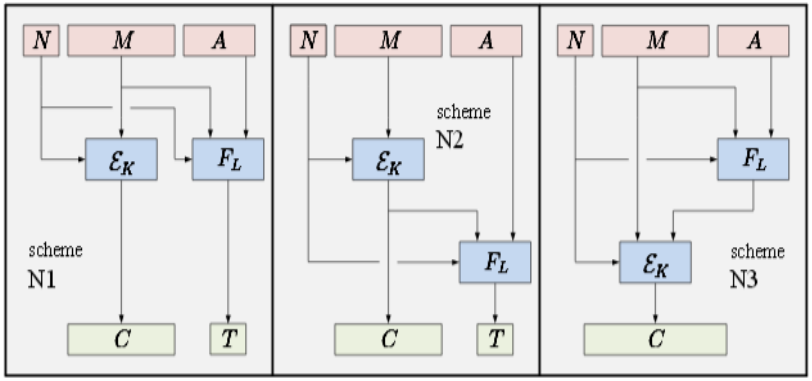
- IV is random (externally generated)
- IV is communicated in-band



2. N (Nonce)-Enc + MAC

Nonce-based AE from N-Enc

- IV is an unique number
- IV is communicated in-band



Other Ways to Build AE Schemes?

1. **Generic AE composition**

   + combines off the shelf primitives

   - prone to implementation errors

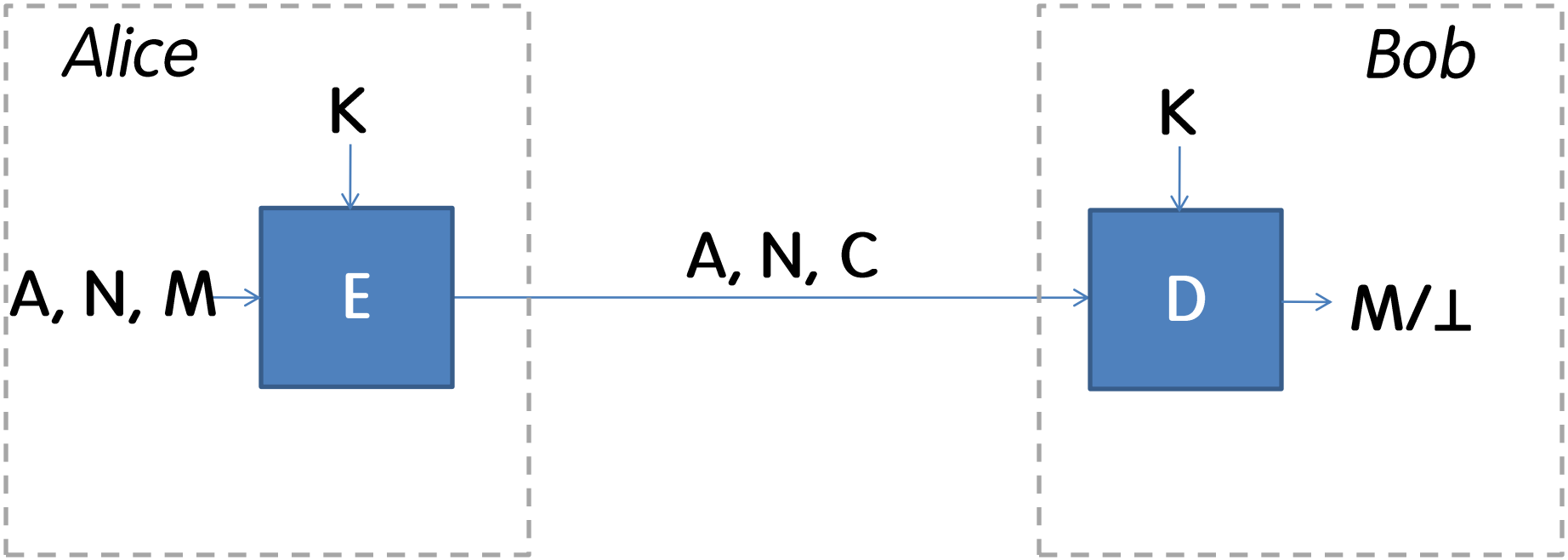
   - 2 data passes

   - 2 keys

2. **Dedicated AE schemes**

   nonce-based (randomness is not required)

Nonce-based AE



Nonce dependent AE: Security fails when N repeats
Nonce MR AE: Provide security when N repeats

Dedicated AE (Prior to CAESAR)

Primitive	Nonce dependent	Nonce MR
Block cipher	IAPM*, OCB*, XECB*, CCM, **GCM**, OTR*, CLOC	SIV, BTM, McOE-G, POET, COPA
Permutation	Sponge Wrap Ketje&Keyak, NORX	APE

Green ISO/IEC 19772:2009 (NIST recommended: CCM, GCM)
Blue part of the CAESAR competition (+OCB)
* hold a patent

AE Characteristics

Security	Efficiency
+ Nonce misuse resistant **NMR** + Secure against release of unverified plaintext **RUP** + Side-channel resistant	+ Online + Parallelizable + Inverse free + Low # data passes + Incrementality + Static AD

Underlying primitive ?

Target security levels?

Target platform?

Nonce Misuse

- Flawed implementations
- Bad user management
- Backup reset of virtual machine clones

Not all security should be lost
if N is misused!

Nonce Misuse

1. MAX security up to M repetitions
SIV, BTM, HBS but two passes over the data

2. LCP security up to longest common prefix
McOE-G, COPA, APE, POET

Release of Unverified Plaintext RUP

Andreeva et al. (2014)

- Insecure memory
- Small buffer
- Real-time requirements

Attacker gets ciphertext decryptions before verification completed!

(not in current AE security models)

Release of Unverified Plaintext

Andreeva et al. (2014)

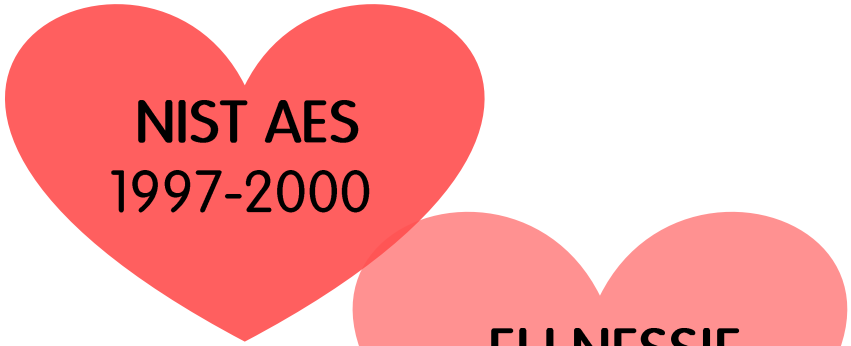
Nonce	AE scheme	RUP confidentiality
Nonce dependent	OCB, CCM, GCM SpongeWrap	No No
Nonce MR	COPA, McOE-G APE SIV, BTM, HBS	No Yes Yes

In Summary …

Multiple AE security and efficiency objectives
More analysis and trust in AE
before deployment

Cryptographic competition

Cryptographers Affairs

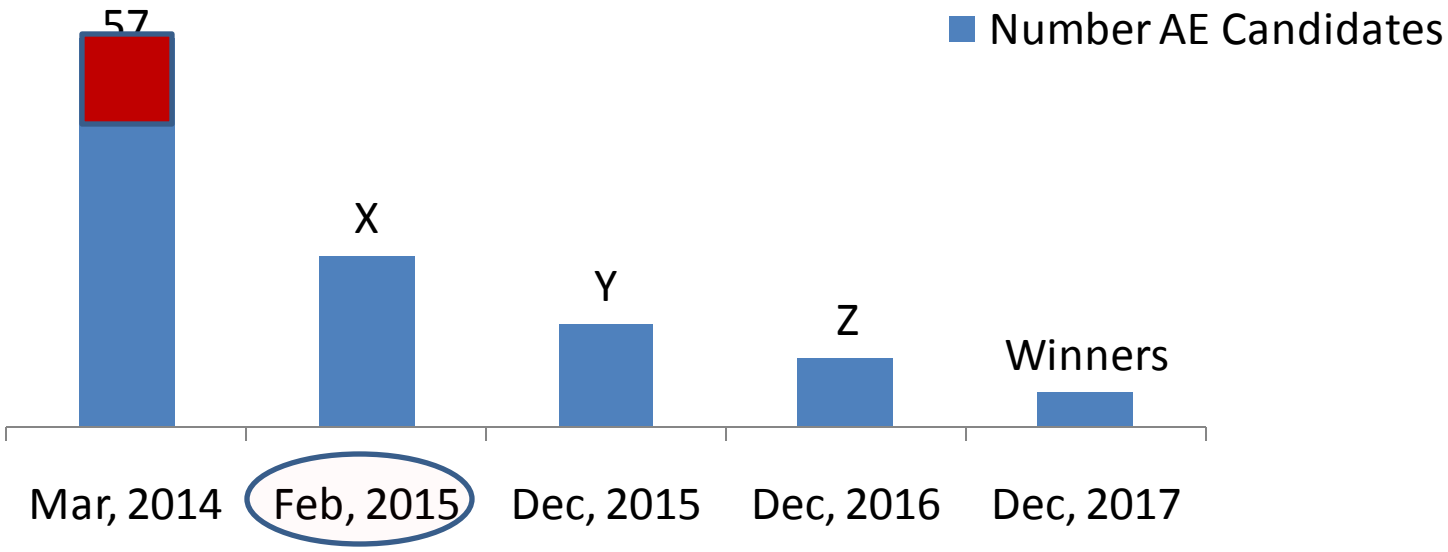


VS

CAESAR

Competition for Authenticated Encryption: Security, Applicability, and Robustness

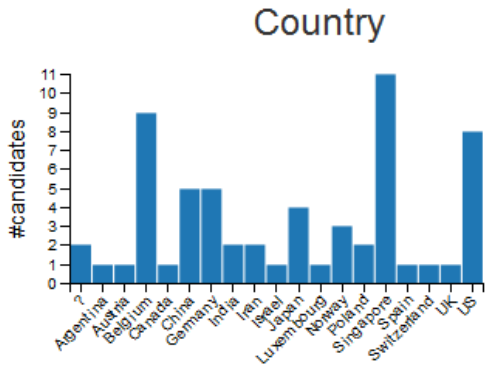
- Easy to use, secure and efficient AE
- Advantageous over AES-GCM and suitable for widespread adoption

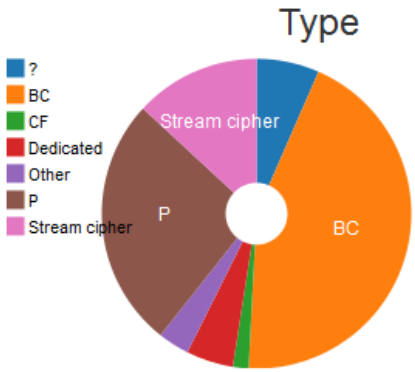


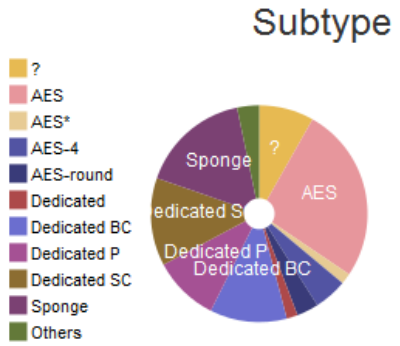
CAESAR Comparison

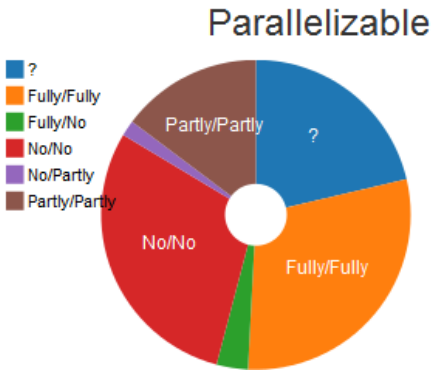
- Properties dataviz by Xavier Dutoit➔

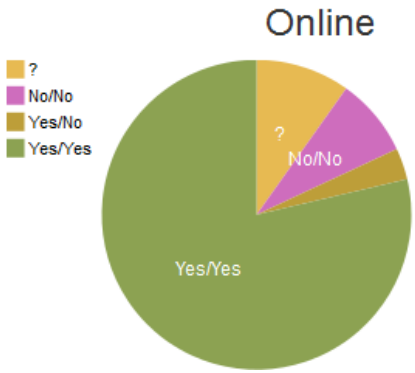
http://homes.esat.kuleuven.be/~eandreev/caesarviz/index.html

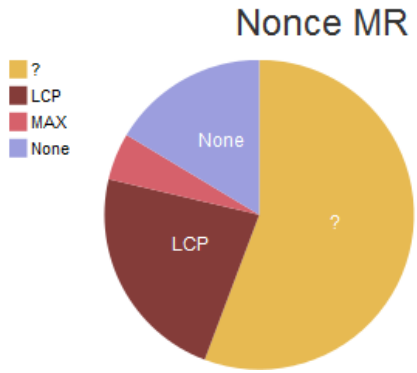








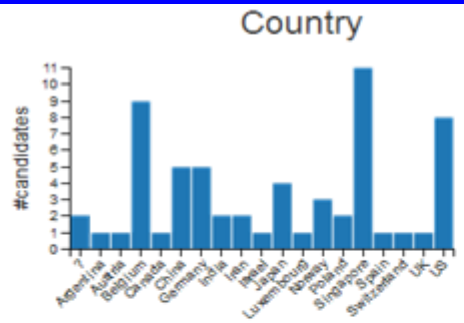


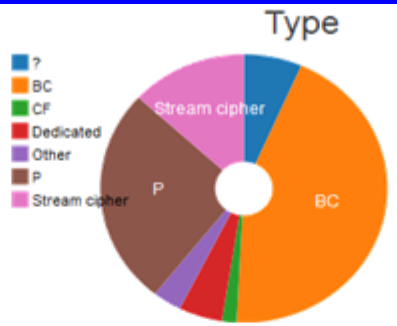


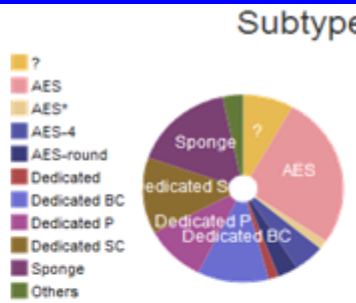
CAESAR Comparison

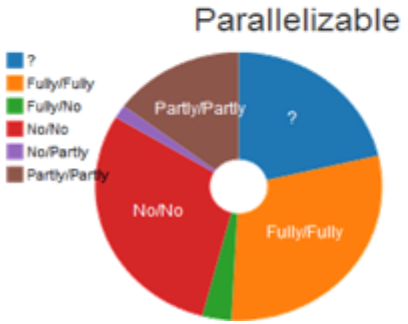
- Properties dataviz by Xavier Dutoit➔

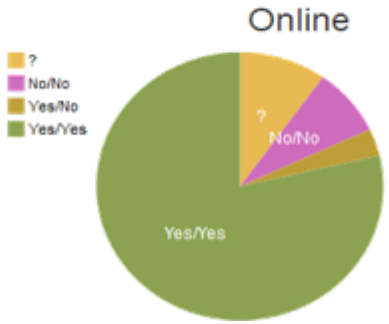
http://homes.esat.kuleuven.be/~eandreev/caesarviz/index.html

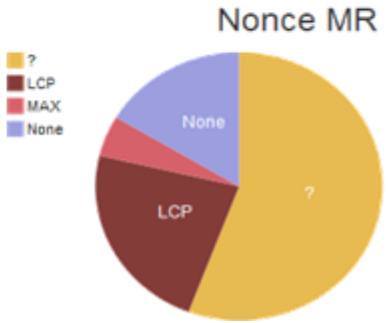


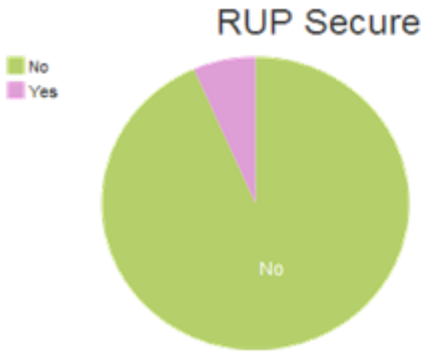


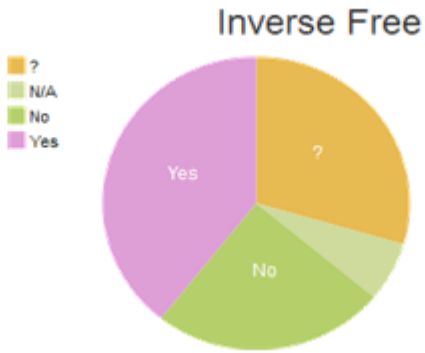


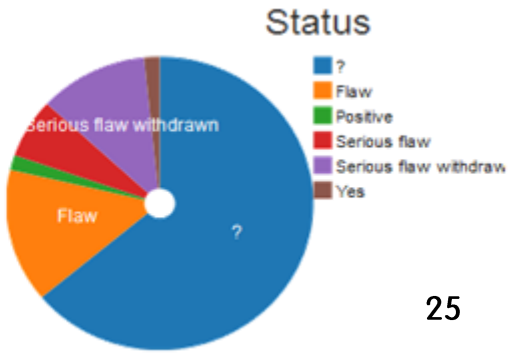












CAESAR
Comparison and Categories

- Properties dataviz by Xavier Dutoit➔

http://homes.esat.kuleuven.be/~eandreev/caesarviz/index.html

- https://mjos.fi/aead_feedback/
- http://www1.spms.ntu.edu.sg/~syllab/speed/
- Categories (speculate ☺ …)

Target platforms and applications

hardware/software/low latency/lightweight/…

Security

high margin/NMR/RUP/side-channel/…

CAESAR

http://competitions.cr.yp.to/caesar.html

Thank you!

Elena.Andreeva@esat.kuleuven.be