RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: CRYP-R03

Symmetric Key Constructions Full Disk Encryption: Bridging Theory and Practice

Louiza Khati, Nicky Mouha and Damien Vergnaud
ENS and Oppida, France

Disk storage principle/Overview

Logical Block Address (LBA)

Physical Block Address (PBA)

(LBA,PBA, data)

LBA

Read a sector

Write a sector

OS

LBA = sector number s

Disk Volume

Full Disk Encryption (FDE)

Encryption

p

C, LBA

DETERMINISTIC

C, LBA

(LBA,PBA, C)

~~IV, Nonce~~

~~Tags/MAC~~

~~Authentication~~

OS

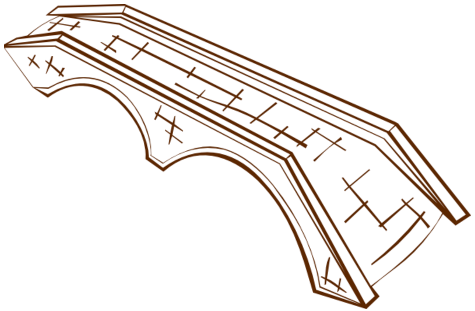
Disk Volume

Goal

FDE deterministic so ...

What level of security can we obtain in this context ?

Databases
SSD

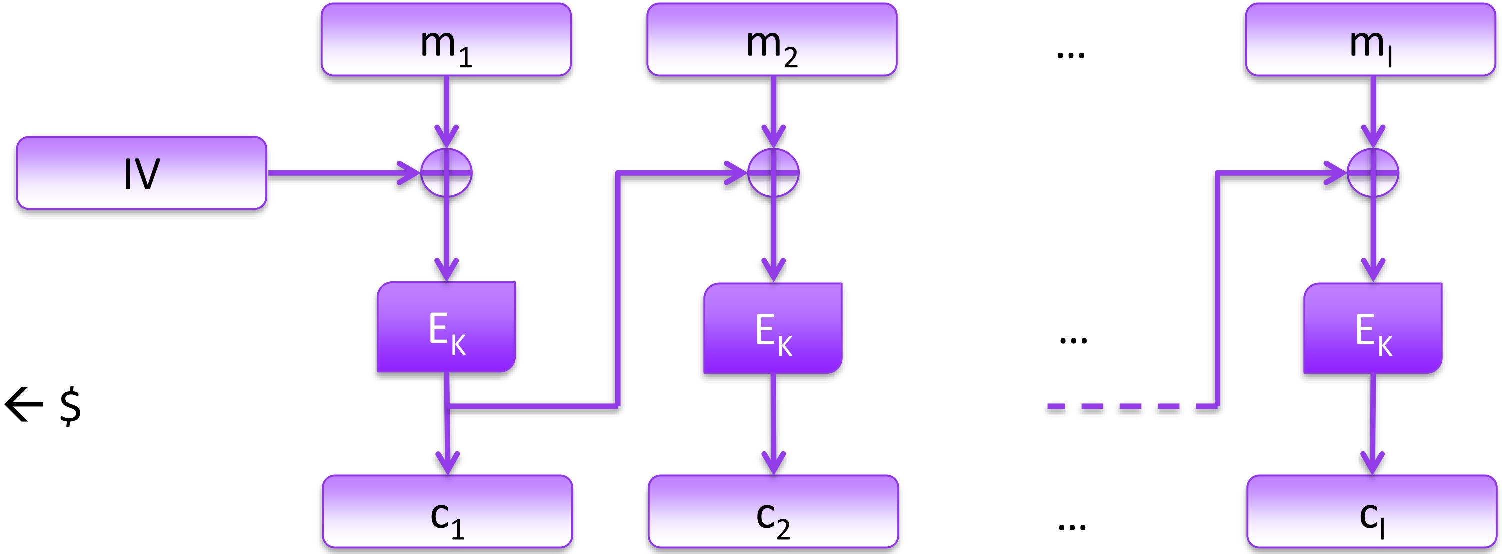


Security models
Security proofs

Outline

- Modes of operation used in FDE
- FDE security notions
- New security models :
  - The Unique First Block (UFB) model
  - The diversifier model
- A diversifier in SSD technology

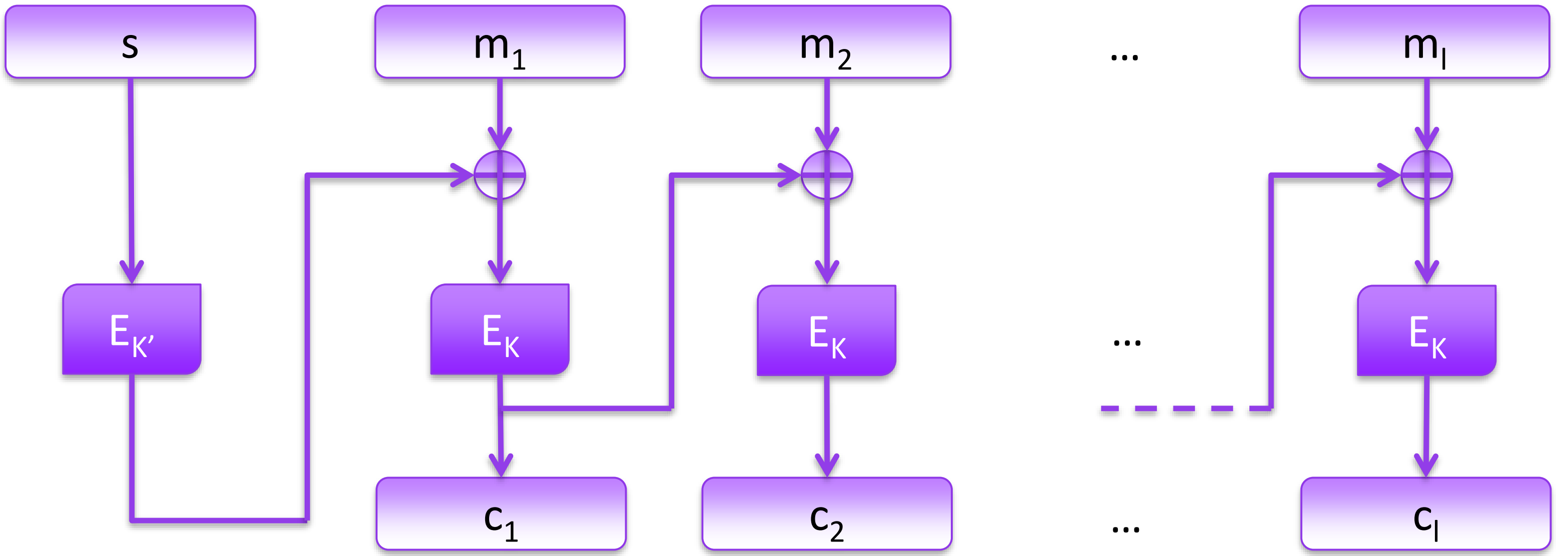
CBC mode



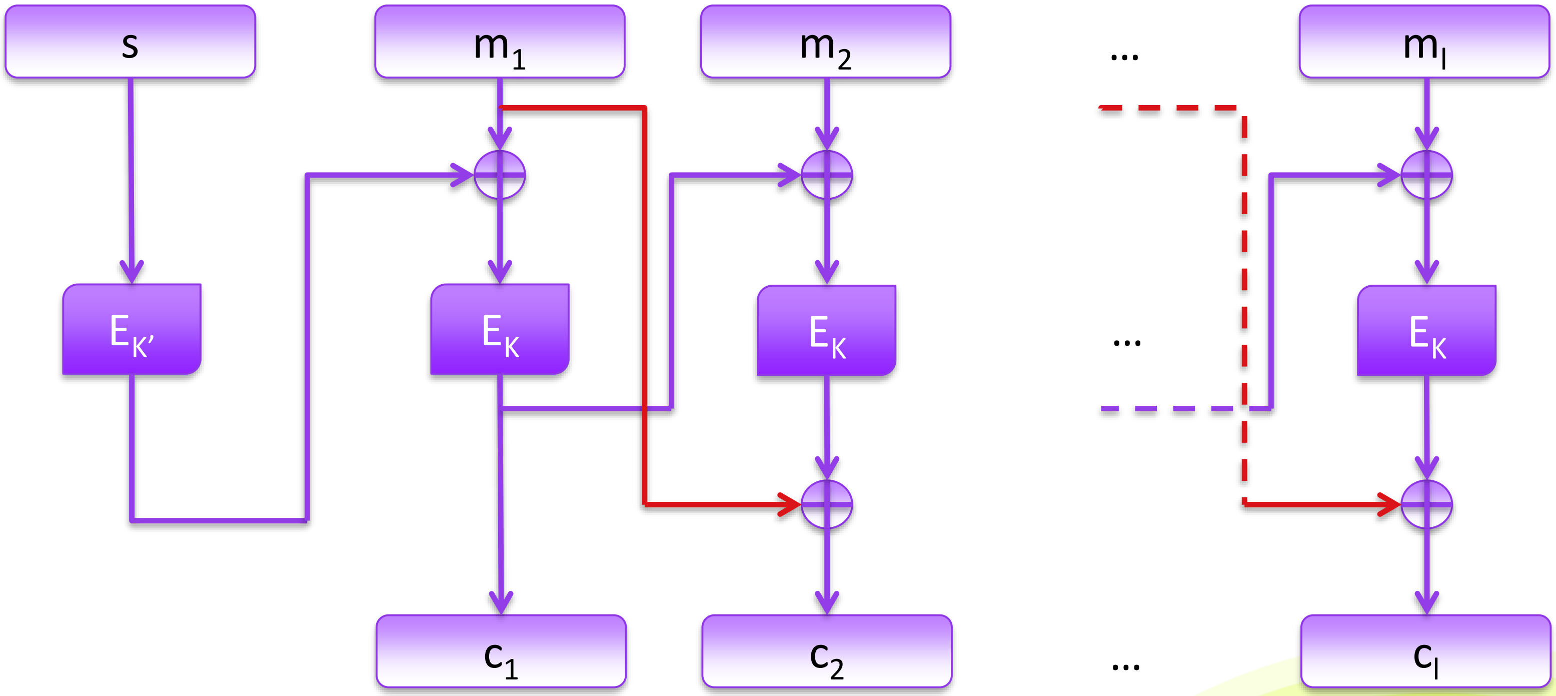
IV ← $

Sector size = multiple of block size

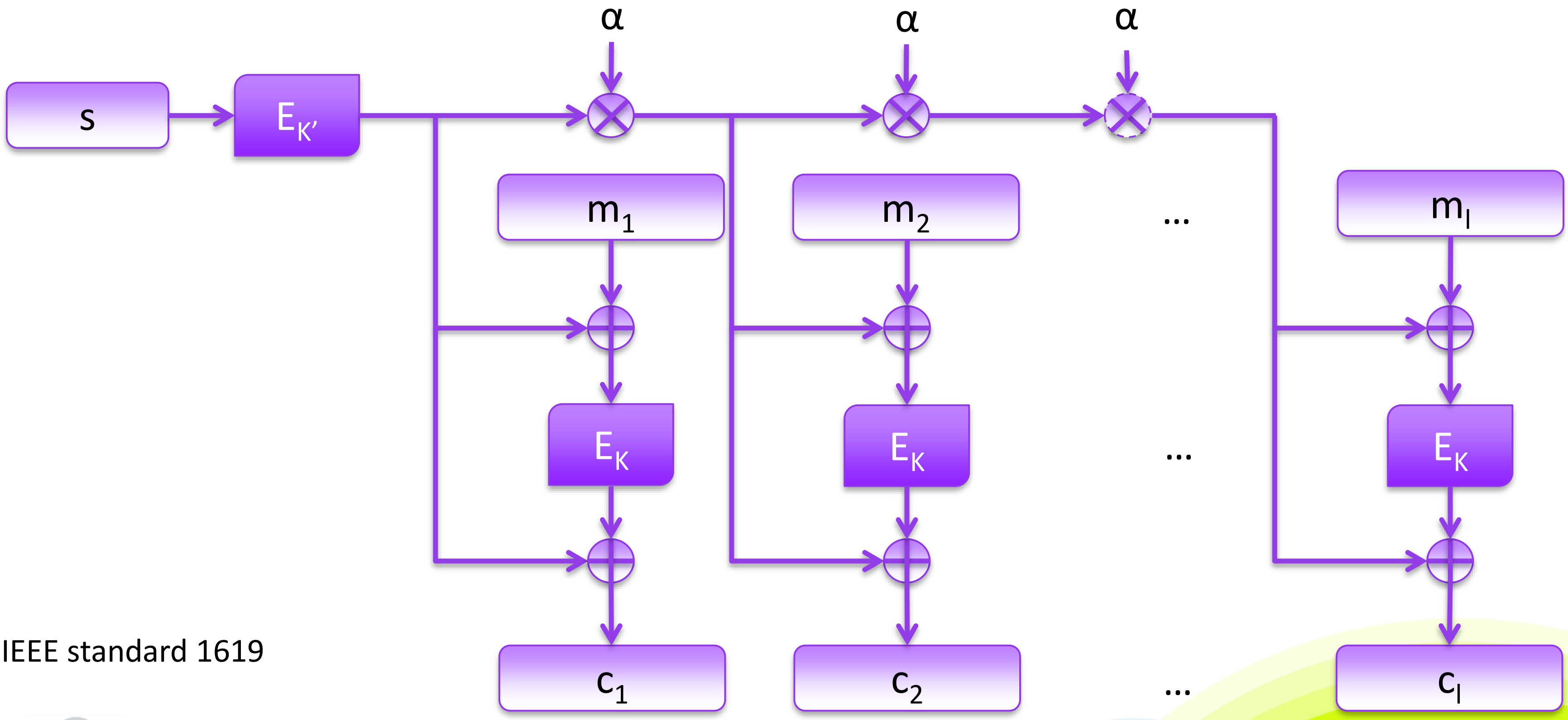
CBC-essiv mode



IGE-essiv mode

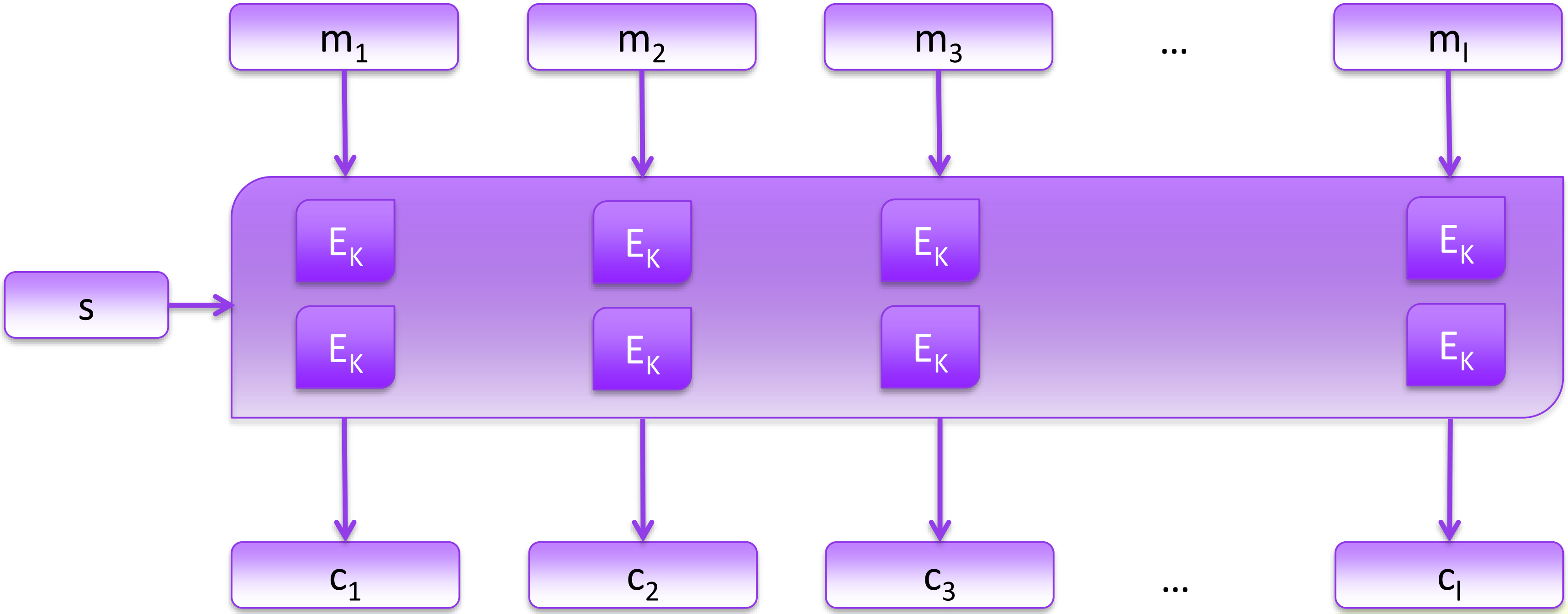


XTS mode



IEEE standard 1619

Wide Tweakable Block Cipher (WTBC)



Ex : EME2 (IEEE standard 1619.2)

FDE security notions : IND-CPA

i = 1 i = 2 i = 3 i = 4

s = 3 p_1 p_2 p_3 p_4

↓ encryption

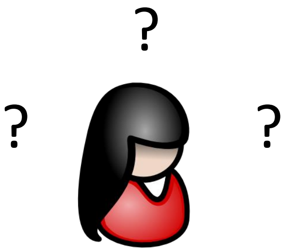
c_1 c_2 c_3 c_4

i = 1 i = 2 i = 3 i = 4

s = 3 p_1 p_2 p_3 p_4

↓ encryption

c'_1 c'_2 c'_3 c'_4



FDE security notions : IND-CPA-repetition

Twice the same (s, p) → same c

	i = 1	i = 2	i = 3	i = 4
s = 3	p_1	p_2	p_3	p_4

↓ encryption

c_1	c_2	c_3	c_4

	i = 1	i = 2	i = 3	i = 4
s = 3	p_1	p_2	p'_3	p_4

↓ encryption

c'_1	c'_2	c'_3	c'_4

?

?

FDE security notions : IND-CPA-block

Twice the same $(s, i, p_i) \rightarrow$ same c_i

	i = 1	i = 2	i = 3	i = 4
s = 3	p_1	p_2	p_3	p_4

↓ encryption

c_1	c_2	c_3	c_4

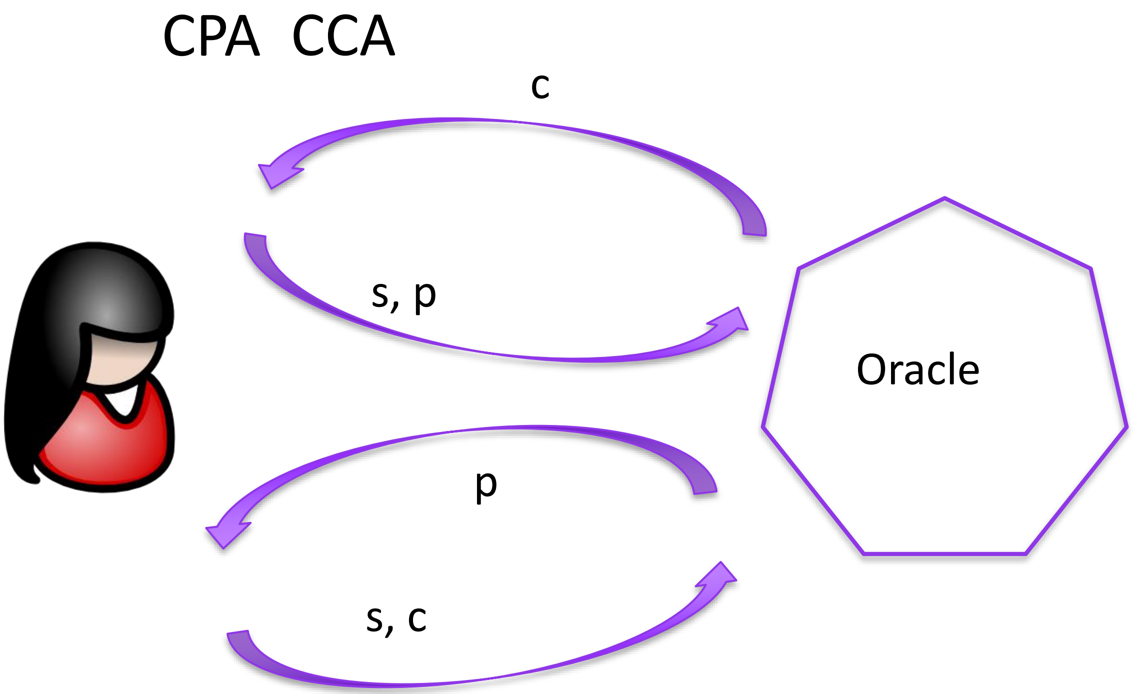
	i = 1	i = 2	i = 3	i = 4
s = 3	p_1	p_2	p'_3	p_4

↓ encryption

c_1	c_2	c'_3	c_4

? ?

Adversary power : Classical model



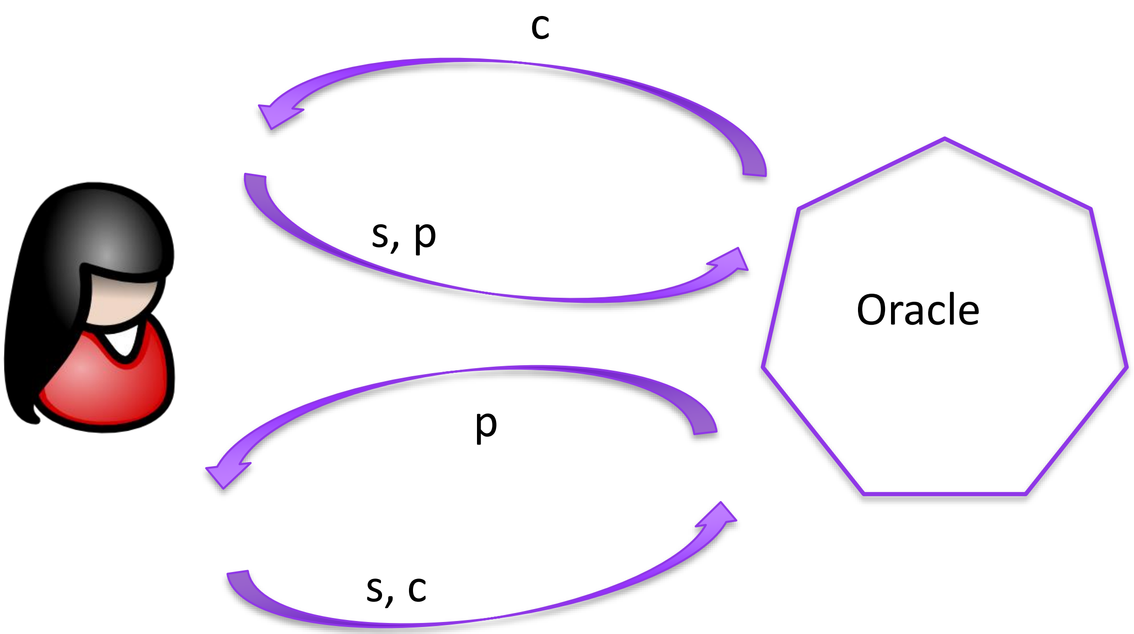
Decrypt/encrypt
Oracle answers

Classical Attack model

IV →	CBC s	CBC $E_{K'}(s)$	IGE $E_{K'}(s)$	XTS s	WTBC s
IND-CPA-block	X	X	X	✓	X
IND-CPA-repetition	X	X	X	X	✓
IND-CPA	X	X	X	X	X
IND-CCA-block	X	X	X	✓	X
IND-CCA-repetition	X	X	X	X	✓
IND-CCA	X	X	X	X	X

Adversary power : UFB model

CPA CCA



Decrypt (s, c)
St c Oracle answer

UFB constraint

Encrypt two (s, p)
With same p_1

UFB Model applications

- Database applications
  - Encryption at application level too slow,
  - At least 8 bytes of padding added = wastage
- Solution :
  - Use 8-bytes timestamp in the first block (→UFB)
  - Encryption at sector level (CBC-essiv)
- Rogaway's Encode-then-Encipher [5]

UFB attack model

IV →	CBC s	CBC $E_{K'}(s)$	IGE $E_{K'}(s)$	XTS s	WTBC s
IND-CPA-block	X	X	X	✓	X
IND-CPA-repetition	X	✓	✓	X	✓
IND-CPA	X	✓	✓	X	✓
IND-CCA-block	X	X	X	✓	X
IND-CCA-repetition	X	X	X	X	✓
IND-CCA	X	X	X	X	✓

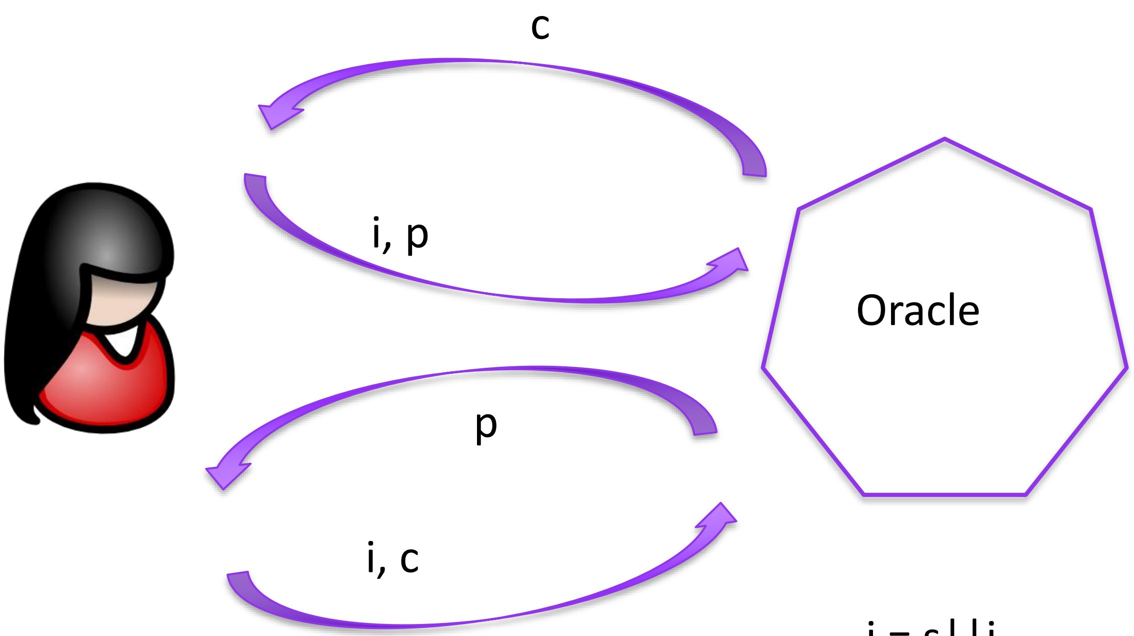
Security proofs in the paper

Introduction of a diversifier

- No additional data (no storage)
  - Not an IV, Not a Nonce
- A non stored value j in the system different for each encryption
- Now s is replaced by $i = s||j$
- Even same (s, p) → different j → different c

Adversary power : Diversifier model

CPA CCA



$i = s||j$

Same (s, p)

Decrypt (i, c)
St c Oracle answer

Diversifier :

Same (i, p)

Diversifier model

IV →	CBC s	CBC $E_{K'}(s)$	IGE $E_{K'}(s)$	XTS s	WTBC s
IND-CPA-block	X	✓	✓	✓	✓
IND-CPA-repetition	X	✓	✓	✓	✓
IND-CPA	X	✓	✓	✓	✓
IND-CCA-block	X	X	X	✓	X
IND-CCA-repetition	X	X	X	X	✓
IND-CCA	X	X	X	X	✓

SSD technology

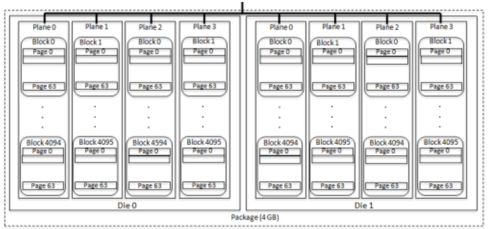
LBA	PBA
0	Block : 2 Page : 7
1	
2	
…	…

Flash Translation Layer
FTL

Wear leveling

Garbage collection

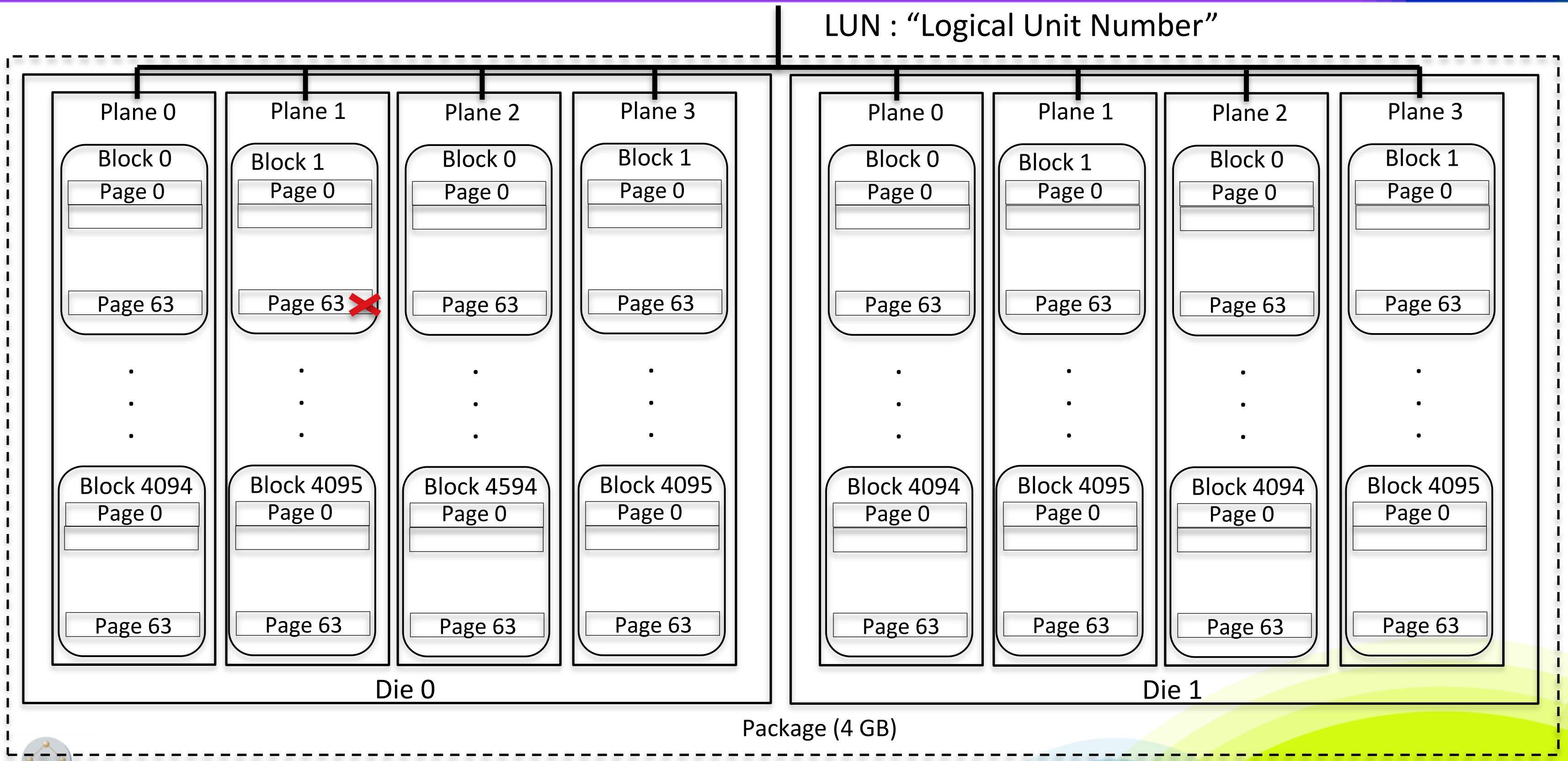
Firmware



Memory

Flash Memory organisation

PBA



SSD constraints

- PBA can be overwritten only a **limited** number of times

  →Wear leveling : distribution of writes (extend SSD lifetime)

- Rewriting individual sectors is not possible → invalidated sector
  - Smallest unit that can be **written** : a page.
  - Smallest unit that can be **erased** : a block.

  → garbage collection

- Wear leveling + Garbage collection = SSD performance

Find a diversifier in SSD technology

- Minimal modifications of the SSD firmware :
  - wear leveling and garbage collection,
  - SATA exchanges.
- Our solution : d = LUN
- Proof of concept with Eagle Tree (Open Source Simulator)
  - 2-bits diversifier → Decrease of IOPS = 4%
  - 3-bits diversifier → Decrease of IOPS = 14%

Conclusion

- Classification of modes of operation in FDE context
- Security proofs in UFB model (CBC-essiv, IGE-essiv)
- Introduction of a diversifier (non deterministic FDE) + benchmark
- Open question:
  - Performance and diversifier size for industrial firmware?

RSAConference2017

Thank you for your attention!

Revisiting Full-PRF-Secure PMAC and Using It for Beyond-Birthday Authenticated Encryption

Eik List[1], Mridul Nandi[2]

[1] Bauhaus-Universität Weimar, Germany
[2] Applied Statistics Unit, Indian Statistical Institute, Kolkatta, India

Cryptographers' Track at the RSA Conference
February 2017

Section 1

Motivation

Motivation

- DIAC2016: Bernstein announced community's work on Future Directions in Authenticated Encryption:
  - One important aspect: Robustness and beyond-birthday-bound (BBB) security
- **BBB-secure block-cipher-based designs (Focus)**
  - SCT [Peyrin, Seurin'15]
  - CAESAR candidates: Deoxys, Joltik [Jean et al.'15]
- BBB-secure streamcipher-based designs
  - TriviA-ck [Nandi,Chakraborty'14], HS1-SIV [Krovetz'14], ...
- Highly secure permutation-based designs:
  - Ascon [Dobraunig et al.'14], Ketje and Keyak [Bertoni et al.'14], NORX [Aumasson et al.'14], StriBob [Saarinen'14], ...
- BBB-secure designs from primitives with $> n$-bit security:
  - PIV [Shrimpton, Terashima'13]
  - DCT [Forler et al.'16]

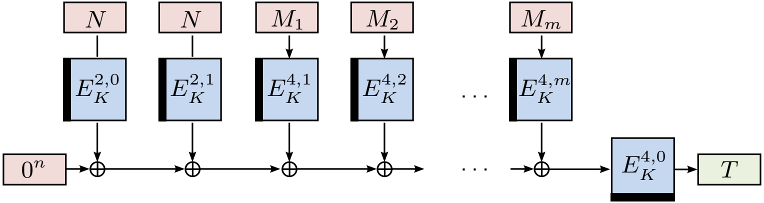
Synthetic Counter in Tweak (SCT)

Peyrin, Seurin'16

- Mac-then-Encrypt composition: EPWC + CTRT
- Based on tweakable block cipher

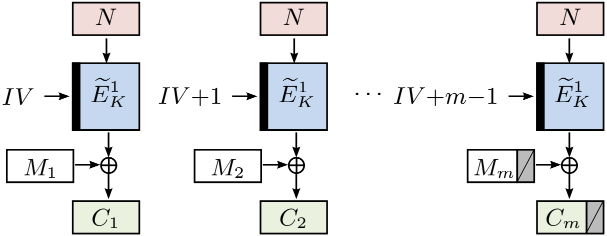
- Encrypted Parallel Wegman-Carter MAC (EPWC):

  (here: empty associated data)
  - BBB security if nonces unique
  - **Falls back to birthday security if any nonce repeats once**



Synthetic Counter in Tweak (cont'd)

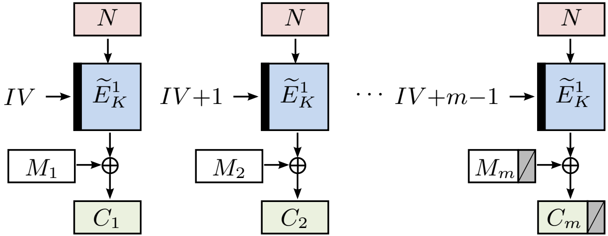
Peyrin, Seurin'16



- CTR-in-Tweak (CTRT) mode:
  - BBB security independent also for random 2n-bit inputs
  - Graceful security degradation with #nonce repetitions

Synthetic Counter in Tweak (cont'd)

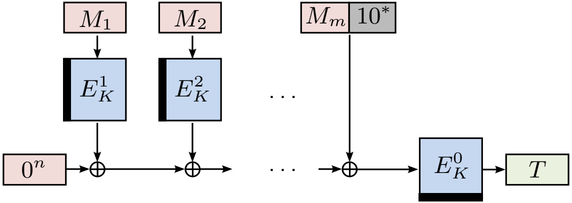
Peyrin, Seurin'16



- CTR-in-Tweak (CTRT) mode:
  - BBB security independent also for random 2n-bit inputs
  - Graceful security degradation with #nonce repetitions
- **Our Goal:**
  - BBB security without nonces
  - Applications: Deterministic AE, key wrap

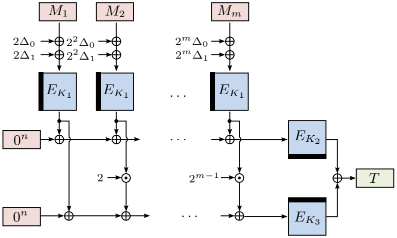
PMAC as Base

Rogaway and Krovetz'11

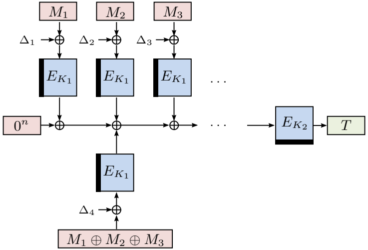


- Many desirable properties:
  - Incremental, parallelizable, single-key, single-primitive
- Variants used in various block-cipher-based CAESAR candidates
  - COLM [Andreeva et al.'16] (COPA, ELmD), Marble [Guo'14], POET [Abed et al.'14], AEZ [Hoang et al.'14] ...

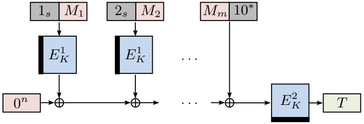
Evolution of PMAC Designs



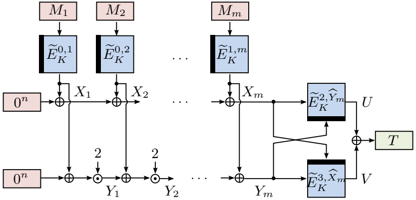
PMAC$^+$ [Yasuda'11]



PMAC/P [Yasuda'12]



LightMAC [Luyckx et al.'16]



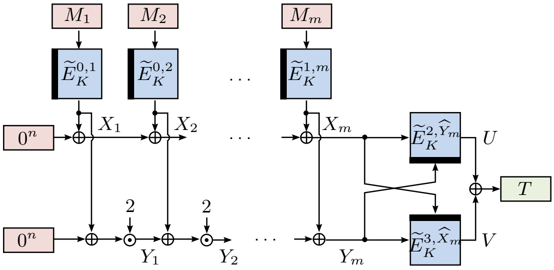
PMAC_TBC1k [Naito'15]

Existing PMAC Designs

Summary

Primitive	Construction	Keys	Size	Advantage	Ref.
BC	PMAC^{+}	3	n	$O(q^3m^3/2^{2n} + qm/2^n)$	[Yasuda'11]
	$1\textsc{k}\_\mathrm{PMAC}^{+}$	1	n	$O(qm^2/2^n + q^3m^4/2^{2n})$	[Datta et al.'15]
	$\mathrm{PMAC/P}$	$r+1$	n	$O(q^2/2^n + qm\ell/2^{2n})$	[Yasuda'12]
	PMACX	2	n	$O(q^2/2^n + qm\ell/2^{2n})$	[Zhang,Zhang'15]
	LightMAC	1	n	$O(q^2/2^n)$	[Luyckx et al.'16]
TBC	$\mathrm{PMAC\_TBC3}\textsc{k}$	3	n	$O(q^2/2^{2n})$	[Naito'15]
	$\mathrm{PMAC\_TBC1}\textsc{k}$	1	n	$O(q/2^n + q^2/2^{2n})$	[Naito'15]
	PMACx	1	n	$O(q^2/2^{2n} + q^3/2^{3n})$	This work
	PMAC2x	1	$2n$	$O(q^2/2^{2n} + q^3/2^{3n})$	This work

Existing PMAC Designs – [Naito'15]



- $\mathrm{PMAC\_TBC3K}$: 3-keys
- $\mathrm{PMAC\_TBC1K}$: 1-key, tweak domain separation at finalization
- Based on tweakable block cipher, full PRF-security

Our purpose:

- Need adaption with $2n$-bit output: For N and IV in CTRT
- Found assumption in proof that does not always hold

Contribution

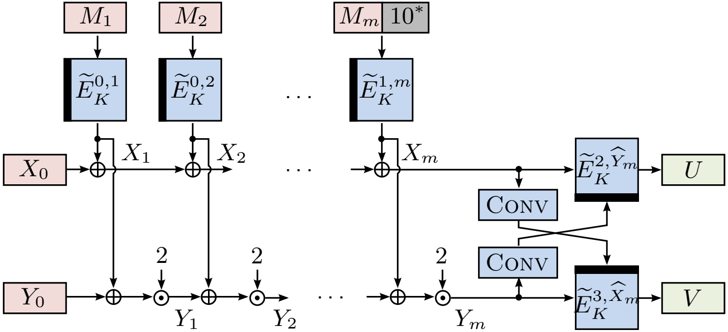
- PMAC2x:
  - BBB-secure parallelizable MAC with $2n$-bit outputs
- PMACx: Variant with n-bit output like PMAC_TBC1k
  - Fix proof
- SIVx: PMAC2x as MAC + Counter-in-Tweak mode
  - BBB-secure 1-primitive, 1-key deterministic AE scheme

Section 2

PMAC2x

PMAC2x

Scheme



Main differences to PMAC_TBC1K:

- $2n$-bit output
- Different proof approach
- Arbitrary-length messages
- General regular function $\textsc{Conv} : \{0,1\}^n \rightarrow \{0,1\}^{n-d}$

PMAC2x

Bound

- $\widetilde{E}$ Tweakable block cipher
- n/t Block/Tweak size
- d Domain size
- q/ℓ #Queries/#Blocks of $\mathbf{A}$

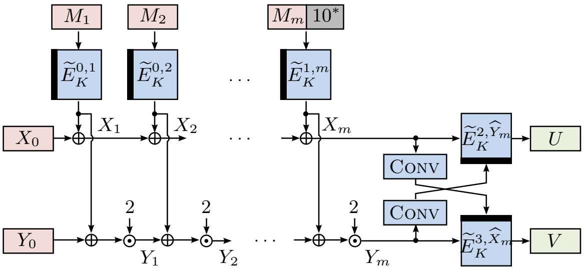
Theorem 1

Let $d + t = n$, and let $m < 2^t$ denote the maximum number of n-bit blocks of any query. Then

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{PMAC2x}[\widetilde{E}]}(q, \ell, \theta) \leq \frac{2^{2d} q^2}{2 \cdot (2^n - q)^2} + \frac{2^d q^3}{3 \cdot 2^{2n}(2^n - q)} + \frac{2^d q^2}{2^n (2^n - q)} + \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\ell + 2q, O(\theta + \ell + 2q)).$$

PMAC2x

Proof Idea



Bad Events:

- **Case1**: $(\widehat{X}_m, \widehat{Y}_m) \in \mathcal{Q}$:

  Resample $U \twoheadleftarrow \{0,1\}^n \setminus \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m})$

  and $V \twoheadleftarrow \{0,1\}^n \setminus \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$

- **Case2**: $U \in \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m}) \wedge$

  $V \in \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$:

  Resample $U \twoheadleftarrow \{0,1\}^n \setminus \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m})$

  and $V \twoheadleftarrow \{0,1\}^n \setminus \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$

- **Case3**: $U \in \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m}) \wedge$

  $V \notin \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$:

  Resample $U \twoheadleftarrow \{0,1\}^n \setminus \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m})$

- **Case4**: $U \notin \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m}) \wedge$

  $V \in \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$:

  Resample $V \twoheadleftarrow \{0,1\}^n \setminus \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$

- **Case1**: $(\widehat{X}_m, \widehat{Y}_m) \in \mathcal{Q}$

$$(i-1) \cdot \frac{2^d}{(2^n - q)} \cdot \frac{2^d}{(2^n - q)} = \frac{2^{2d}(i-1)}{(2^n - q)^2}.$$

- **Case2**: $U \in \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m}) \wedge V \in \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$

$$\frac{i-1}{2^n} \cdot \frac{i-2}{2^n} \cdot \frac{2^d}{2^n - q} \leq \frac{2^d(i-1)^2}{2^{2n}(2^n - q)}.$$

- **Case3**: $U \in \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m}) \wedge V \notin \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$

$$\frac{2^d}{2^n - q} \cdot \frac{i-1}{2^n} = \frac{2^d(i-1)}{2^n(2^n - q)}.$$

- **Case4**: $U \notin \text{range}(\widetilde{\pi}^{2,\widehat{Y}_m}) \wedge V \in \text{range}(\widetilde{\pi}^{3,\widehat{X}_m})$

$$\frac{2^d(i-1)}{2^n(2^n - q)}.$$

- Our theorem follows from sum and union bound over q queries

PMAC2x

Assumption in Old Proof

- Proof of $\mathrm{PMAC\_TBC1K}$ uses probabiliy of multi-collisions:

$$\mathsf{mcoll}_1 := (\exists\, \widehat{X}_m^1, \ldots, \widehat{X}_m^\rho \in \mathcal{X} \text{ s.t. } \widehat{X}_m^1 = \ldots = \widehat{X}_m^\rho) \vee$$
$$(\exists\, \widehat{Y}_m^1, \ldots, \widehat{Y}_m^\rho \in \mathcal{Y} \text{ s.t. } \widehat{Y}_m^1 = \ldots = \widehat{Y}_m^\rho),$$
$$\mathsf{mcoll}_2 := \exists\, (X_m^1, \widehat{Y}_m^1), \ldots, (X_m^\xi, \widehat{Y}_m^\xi) \in \mathcal{Q} \text{ s.t. } (X_m^1, \widehat{Y}_m^1) = \ldots = (X_m^\xi, \widehat{Y}_m^\xi)$$

- Bounds $\Pr[\mathsf{mcoll}_1]$ (and $\Pr[\mathsf{mcoll}_2]$ similarly) as

$$\Pr[\mathsf{mcoll}_1] \leq 2 \cdot 2^t \cdot \binom{q}{\rho} \cdot \left(\frac{2^{n-t}}{2^n - q}\right)^\rho \leq 2^{t+1} \cdot \left(\frac{2^{n-t} \cdot eq}{\rho(2^n - q)}\right)^\rho$$

  - ρ values are all equal: $(2^{n-t}/(2^n - q))^\rho$
  - 2^t tweak values
  - $\binom{q}{\rho}$ ways to choose ρ out of q values

- Holds **only if** the ρ colliding tweaks stem from ρ linearly independent random variables

PMAC2x

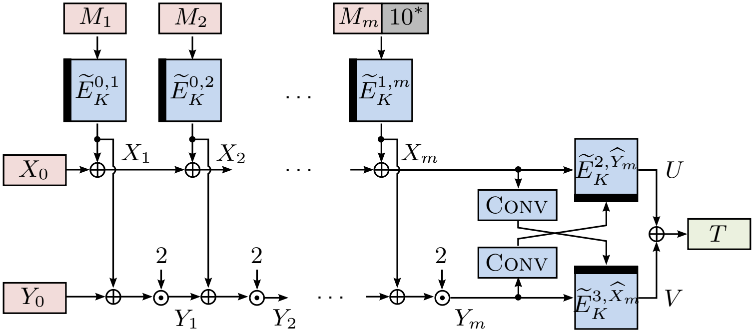
Assumption in Old Proof – Counter Example

- 2^m queries which combine pair-wise distinct blocks $\{M_i, M'_i\}$ with $M_i \neq M'_i$, for $1 \leq i \leq m$ position-wise:

$$\begin{aligned} Q^0 &= (M_1, M_2, M_3, \dots, M_m), \\ Q^1 &= (M'_1, M_2, M_3, \dots, M_m), \\ Q^2 &= (M_1, M'_2, M_3, \dots, M_m), \\ Q^{2^m-1} &= (M'_1, M'_2, M'_3, \dots, M'_m) \end{aligned}$$

- The 2^m resulting values X_m^i, for $0 \leq i \leq 2^m - 1$, depend on the linear combination of only $2m$ random variables

PMACx



Corollary 2

Let $d + t = n$, and let $m < 2^t$ denote the maximum number of n-bit blocks of any query. Then, it holds that $\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{PMACx}[\widetilde{E}]}(q, \ell, \theta) \leq \mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{PMAC2x}[\widetilde{E}]}(q, \ell, \theta)$.

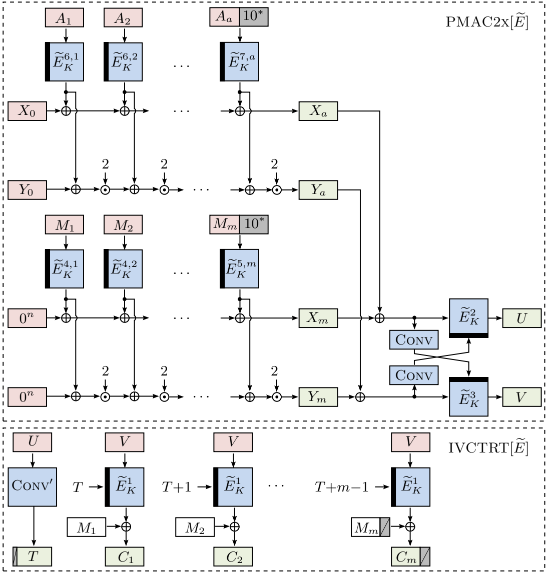
Section 3

SIVx

SIVx

Deterministic AE Scheme

- PMAC2x as MAC
- IVCTRT as mode
- Tweak for domain separation
- $2n$-bit output replaces N, T



SIVx
Bound

Theorem 3 (DAE Security of SIVx)

Let $F : \mathcal{K}_1 \times \mathcal{A} \times \mathcal{M} \to \{0,1\}^{2n}$, and let $\Pi = (\widetilde{\mathcal{E}}, \widetilde{\mathcal{D}})$ be an IV-based encryption scheme with key space $\mathcal{K}_2$ and IV space $\mathcal{IV}$. Let $K_1 \twoheadleftarrow \mathcal{K}_1$ and $K_2 \twoheadleftarrow \mathcal{K}_2$ be independent. Let $\textsc{Conv}' : \{0,1\}^n \to \mathcal{IV}$ be a regular function. Let $\mathbf{A}$ be a DAE adversary running in time at most θ, asking at most q queries of at most $8 \leq \ell < 2^t$ blocks in total. Then, it holds that

$$\mathbf{Adv}^{\mathrm{DAE}}_{\mathrm{SIVx}[F,\Pi]}(\mathbf{A}) \leq \mathbf{Adv}^{\mathrm{IVE}}_{\Pi}(\theta + O(\ell), q, \ell) + \mathbf{Adv}^{\mathrm{PRF}}_{F}(\theta + O(\ell), q, \ell) + \frac{q}{2^n}.$$

- Proof deferred to full version (ePrint)

Section 4

Conclusion

Conclusion

- Revisited the $\mathrm{PMAC\_TBC1K}$ construction
  - Identified critical assumption in proof
- Proposed BBB-secure $\mathrm{PMAC2X}$ with $2n$-bit outputs
- Derived variant PMACX with n-bit outputs
  - Fixed assumption by different proof approach
  - Confirm full-PRF security by Naito
- Derived BBB-secure 1-key, 1-primitive Deterministic AE scheme SIVX
  - Open problem: Reduce transmission overhead $< 2n$ bits

Questions?