Linking OAE and Blockwise Attack Models

Fast Software Encryption 2017

Guillaume Endignoux[1,2], Damian Vizár[1]

[1]EPFL, Switzerland
[2]Kudelski Security

Wednesday 8th March, 2017

This work was partially supported by Microsoft Research.

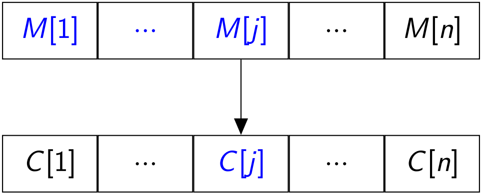
Introduction

Authenticated encryption: confidentiality & authentication in one primitive.

Ongoing CAESAR competition on authenticated encryption (2014 – 2017)

Authenticated encryption: confidentiality & authentication in one primitive.

Ongoing CAESAR competition on authenticated encryption (2014 – 2017)
$\Rightarrow$ most proposed schemes are *online*.



Online authenticated encryption: computable on the fly, constant memory.

Introduction

Security notions to capture AE:

- AE with associated data (AEAD) [Rogaway, 2002]
- Nonce-misuse resistant AE (MRAE) [Rogaway et al., 2006] $\Rightarrow$ cannot be online!
- Online nonce-misuse resistant AE (OAE) [Fleischmann et al., 2012]
- Older notions for *blockwise-adaptive* adversaries [Fouque et al., 2003]

$\Rightarrow$ What are the relations between these notions?

Security notions to capture AE:

- AE with associated data (AEAD) [Rogaway, 2002]
- Nonce-misuse resistant AE (MRAE) [Rogaway et al., 2006] ⇒ cannot be online!
- Online nonce-misuse resistant AE (OAE) [Fleischmann et al., 2012]
- Older notions for *blockwise-adaptive* adversaries [Fouque et al., 2003]

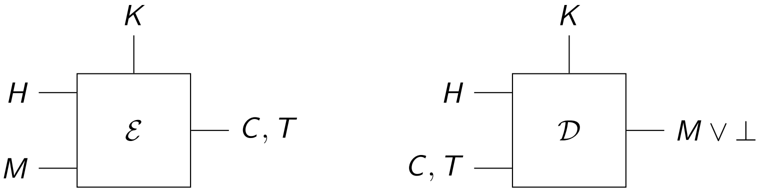
⇒ What are the relations between these notions?

Main contribution: we prove equivalence between OAE and blockwise notions, modulo new PR-TAG notion.

We consider the setting of [Fleischmann et al., 2012]

Online authenticated encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

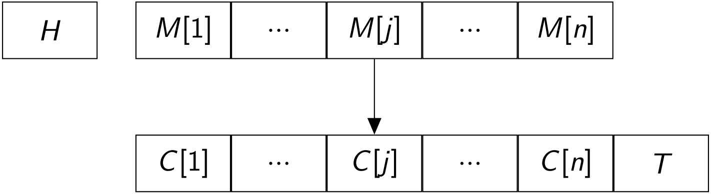
- finite key space $\mathcal{K}$
- deterministic algorithms $\mathcal{E}$ and $\mathcal{D}$



Required properties:

- correctness: $\mathcal{D}(K, H, \mathcal{E}(K, H, M)) = M$
- onlineness: $\mathrm{Core} \circ \mathcal{E}(K, H, \cdot) \in \mathrm{OPerm}[n]$

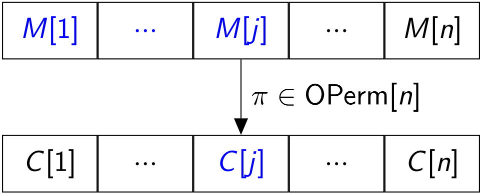
Online authenticated encryption



- blocks of n bits $B_n = \{0,1\}^n$
- message space B_n^*
- header space $\mathcal{H}$ (e.g. $\{0,1\}^*$) = nonce + associated data
- tag space $\mathcal{T} = B_\tau$ (τ bits)
- ciphertext space $\mathcal{C} = B_n^* \times \mathcal{T}$ (core ciphertext blocks + authentication tag)

Online authenticated encryption

We model encryption by *online permutations* of B_n^*.



$C[j]$ depends only on $M[1], \ldots, M[j]$.

We consider the following notions:

- OAE [Fleischmann et al., 2012]
- blockwise privacy [Fouque et al., 2003-2004]
- blockwise integrity [Fouque et al., 2003]

Security notions

We consider the following notions:

- OAE [Fleischmann et al., 2012] $\Rightarrow$ indistinguishability from idealized primitive
- blockwise privacy [Fouque et al., 2003-2004] $\Rightarrow$ left-or-right sequential blockwise CPA
- blockwise integrity [Fouque et al., 2003] $\Rightarrow$ existential forgery of ciphertext

Game OAE-REAL

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

proc Enc(H, M)

return $\mathcal{E}(K, H, M)$

proc Dec(H, C)

return $\mathcal{D}(K, H, C)$

OAE security

Game OAE-REAL

proc Initialize

$K \stackrel{\$}{\leftarrow} \mathcal{K}$

proc Enc(H, M)

return $\mathcal{E}(K, H, M)$

proc Dec(H, C)

return $\mathcal{D}(K, H, C)$

Game OAE-IDEAL

proc Initialize

for all $H \in \mathcal{H}$ **do**

$\pi_H \stackrel{\$}{\leftarrow} \mathrm{OPerm}[n]$

for all $(H, M) \in \mathcal{H} \times B_n^*$ **do**

$T_{H,M} \stackrel{\$}{\leftarrow} \mathcal{T}$

proc Enc(H, M)

return $(\pi_H(M), T_{H,M})$

proc Dec(H, C)

return $\perp$

OAE security

Game OAE-REAL

proc Initialize
$K \xleftarrow{\$} \mathcal{K}$

proc Enc(H, M)
return $\mathcal{E}(K, H, M)$

proc Dec(H, C)
return $\mathcal{D}(K, H, C)$

Game OAE-IDEAL

proc Initialize
for all $H \in \mathcal{H}$ **do**
$\pi_H \xleftarrow{\$} \mathrm{OPerm}[n]$
for all $(H, M) \in \mathcal{H} \times B_n^*$ **do**
$T_{H,M} \xleftarrow{\$} \mathcal{T}$

proc Enc(H, M)
return $(\pi_H(M), T_{H,M})$

proc Dec(H, C)
return $\bot$

$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE}}(\mathscr{A}) = Pr[\mathscr{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1]$$

Blockwise privacy

Game LORS-BCPA

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

$b \xleftarrow{\$} \{0, 1\}$

$\widetilde{H} \leftarrow \perp; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

proc LR(H, P_0, P_1)

if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$

$\widetilde{M} \leftarrow \widetilde{M} || P_b$

$C \leftarrow \mathrm{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$

$j \leftarrow j + 1$

return $C[j]$

Game LORS-BCPA

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

$b \xleftarrow{\$} \{0, 1\}$

$\widetilde{H} \leftarrow \bot; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

proc LR(H, P_0, P_1)

if $\widetilde{H} = \bot$ **then** $\widetilde{H} \leftarrow H$

$\widetilde{M} \leftarrow \widetilde{M} || P_b$

$C \leftarrow \text{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$

$j \leftarrow j + 1$

return $C[j]$

proc GetTag(H)

if $\widetilde{H} = \bot$ **then** $\widetilde{H} \leftarrow H$

$T \leftarrow \text{Tag}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$

$\widetilde{H} \leftarrow \bot; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

return T

proc Finalize(d)

return $d = b$

Game LORS-BCPA

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

$b \xleftarrow{\$} \{0, 1\}$

$\widetilde{H} \leftarrow \perp; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

proc LR(H, P_0, P_1)

if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$

$\widetilde{M} \leftarrow \widetilde{M} || P_b$

$C \leftarrow \text{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$

$j \leftarrow j + 1$

return $C[j]$

proc GetTag(H)

if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$

$T \leftarrow \text{Tag}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$

$\widetilde{H} \leftarrow \perp; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

return T

proc Finalize(d)

return $d = b$

$$\mathbf{Adv}_{\Pi}^{\text{D-LORS-BCPA}}(\mathscr{A}) = 2 \cdot Pr[\mathscr{A}_{\Pi}^{\text{LORS-BCPA}} \Rightarrow 1] - 1$$

Blockwise privacy: deterministic schemes?

Issue with *deterministic* left-or-right indistinguishability: trivial attacks possible.

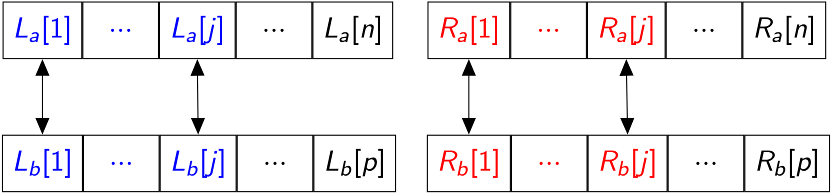
Query a	L_0	L_1	R_0	R_1
Query b	L_0	L_2	R_2	R_3

$\Rightarrow$ Compare $C_a[0]$ and $C_b[0]$ to distinguish between left and right.

Blockwise privacy: deterministic schemes?

We define the *online-respecting* condition to avoid these attacks. Valid adversaries must respect it.

$$LLCP(L_a, L_b)^1 = LLCP(R_a, R_b) \text{ if } H_a = H_b$$



Equivalently (Proposition 1): $\exists \sigma_H \in \mathrm{OPerm}[n]$ s.t. $L_i = \sigma_{H_i}(R_i)$

[1] length of longest common prefix

Blockwise integrity

Game B-INT-CTXT

proc Initialize

win $\leftarrow 0$

$K \xleftarrow{\$} \mathcal{K}$

$\mathcal{X} \leftarrow \emptyset$

$\widetilde{H} \leftarrow \perp; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

proc Enc(H, P)

if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$

$\widetilde{M} \leftarrow \widetilde{M} || P$

$C \leftarrow \text{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$

$j \leftarrow j + 1$

return $C[j]$

Blockwise integrity

Game B-INT-CTXT

proc Initialize

$\text{win} \leftarrow 0$
$K \xleftarrow{\$} \mathcal{K}$
$\mathcal{X} \leftarrow \emptyset$
$\widetilde{H} \leftarrow \bot; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

proc Enc(H, P)

if $\widetilde{H} = \bot$ **then** $\widetilde{H} \leftarrow H$
$\widetilde{M} \leftarrow \widetilde{M} || P$
$C \leftarrow \text{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$
$j \leftarrow j + 1$
return $C[j]$

proc GetTag(H)

if $\widetilde{H} = \bot$ **then** $\widetilde{H} \leftarrow H$
$C \leftarrow \mathcal{E}(K, \widetilde{H}, \widetilde{M})$
$\mathcal{X} \leftarrow \mathcal{X} \cup \{(\widetilde{H}, C)\}$
$\widetilde{H} \leftarrow \bot; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$
return $\text{Tag}(C)$

proc Dec(H, C)

$M \leftarrow \mathcal{D}(K, H, C)$
if $(H, C) \in \mathcal{X}$ **then** $M \leftarrow \bot$
if $M \neq \bot$ **then** $\text{win} \leftarrow 1$
return M

proc Finalize()

return win

Blockwise integrity

Game B-INT-CTXT

proc Initialize
$\text{win} \leftarrow 0$
$K \stackrel{\$}{\leftarrow} \mathcal{K}$
$\mathcal{X} \leftarrow \emptyset$
$\widetilde{H} \leftarrow \perp; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$

proc Enc(H, P)
if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
$\widetilde{M} \leftarrow \widetilde{M} || P$
$C \leftarrow \text{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$
$j \leftarrow j + 1$
return $C[j]$

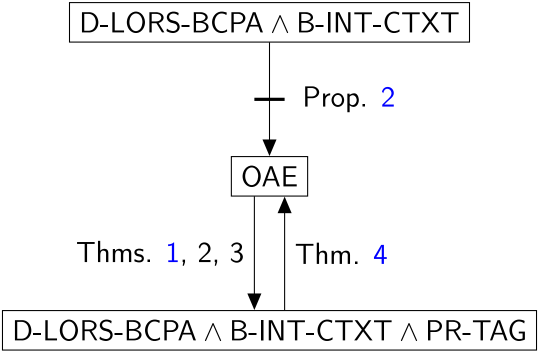
proc GetTag(H)
if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
$C \leftarrow \mathcal{E}(K, \widetilde{H}, \widetilde{M})$
$\mathcal{X} \leftarrow \mathcal{X} \cup \{(\widetilde{H}, C)\}$
$\widetilde{H} \leftarrow \perp; \quad \widetilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$
return $\text{Tag}(C)$

proc Dec(H, C)
$M \leftarrow \mathcal{D}(K, H, C)$
if $(H, C) \in \mathcal{X}$ **then** $M \leftarrow \perp$
if $M \neq \perp$ **then** $\text{win} \leftarrow 1$
return M

proc Finalize$()$
return win

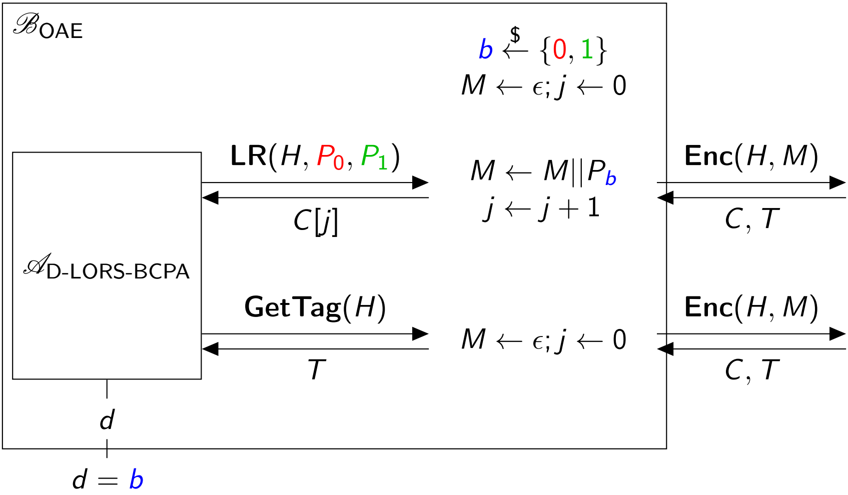
$$\mathbf{Adv}_{\Pi}^{\text{B-INT-CTXT}}(\mathscr{A}) = Pr[\mathscr{A}_{\Pi}^{\text{B-INT-CTXT}} \Rightarrow 1]$$

Main results



Relations between notions shown in the paper.

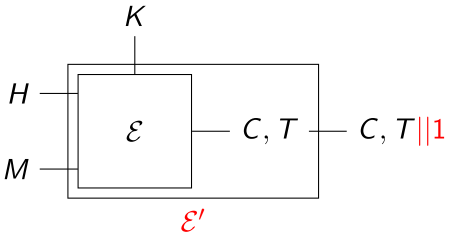
Theorem 1: OAE → D-LORS-BCPA



Advantage: $\mathbf{Adv}_{\Pi}^{\text{D-LORS-BCPA}}(\mathscr{A}) = 2 \cdot \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$

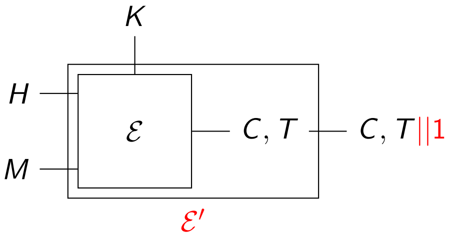
Proposition 2: D-LORS-BCPA $\wedge$ B-INT-CTXT $\not\to$ OAE

We construct a counter-example $\mathcal{E}'$



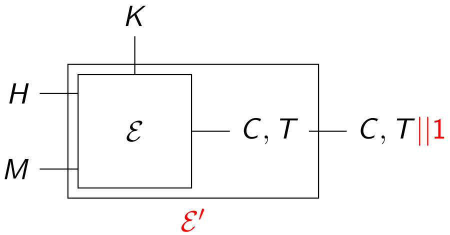
Proposition 2: D-LORS-BCPA $\wedge$ B-INT-CTXT $\not\rightarrow$ OAE

We construct a counter-example $\mathcal{E}'$



- $\mathcal{E}'$ is as secure as $\mathcal{E}$ for D-LORS-BCPA and B-INT-CTXT.

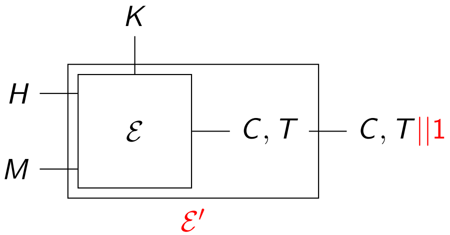
We construct a counter-example $\mathcal{E}'$



- $\mathcal{E}'$ is as secure as $\mathcal{E}$ for D-LORS-BCPA and B-INT-CTXT.
- The tag allows to distinguish real scheme from ideal scheme with probability $\frac{1}{2}$.

Proposition 2: D-LORS-BCPA $\wedge$ B-INT-CTXT $\not\rightarrow$ OAE

We construct a counter-example $\mathcal{E}'$



- $\mathcal{E}'$ is as secure as $\mathcal{E}$ for D-LORS-BCPA and B-INT-CTXT.
- The tag allows to distinguish real scheme from ideal scheme with probability $\frac{1}{2}$.
- Neither D-LORS-BCPA nor B-INT-CTXT enforce uniformly distributed tag.

A novel notion: pseudo-random tag

PR-TAG = indistinguishability from real encryption + random tag

A novel notion: pseudo-random tag

PR-TAG = indistinguishability from real encryption + random tag

Game PR-TAG-REAL

proc Initialize
$K \xleftarrow{\$} \mathcal{K}$

proc Enc(H, M)
return $\mathcal{E}(K, H, M)$

A novel notion: pseudo-random tag

PR-TAG = indistinguishability from real encryption + random tag

Game PR-TAG-REAL

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

proc Enc(H, M)

return $\mathcal{E}(K, H, M)$

Game PR-TAG-IDEAL

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

for all $(H, M) \in \mathcal{H} \times B_n^*$ **do**

$T_{H,M} \xleftarrow{\$} \mathcal{T}$

proc Enc(H, M)

$C \leftarrow \mathrm{Core}(\mathcal{E}(K, H, M))$

return $(C, T_{H,M})$

A novel notion: pseudo-random tag

PR-TAG = indistinguishability from real encryption + random tag

Game PR-TAG-REAL

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

proc Enc(H, M)

return $\mathcal{E}(K, H, M)$

Game PR-TAG-IDEAL

proc Initialize

$K \xleftarrow{\$} \mathcal{K}$

for all $(H, M) \in \mathcal{H} \times B_n^*$ **do**

$T_{H,M} \xleftarrow{\$} \mathcal{T}$

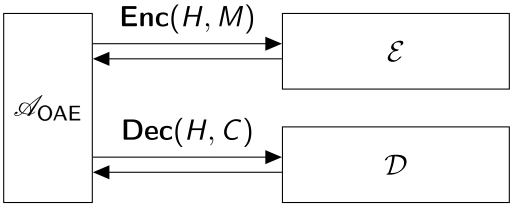
proc Enc(H, M)

$C \leftarrow \mathrm{Core}(\mathcal{E}(K, H, M))$

return $(C, T_{H,M})$

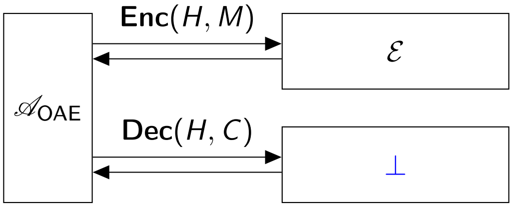
$$\mathbf{Adv}_{\Pi}^{\text{PR-TAG}}(\mathscr{A}) = Pr[\mathscr{A}_{\Pi}^{\text{PR-TAG-REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{PR-TAG-IDEAL}} \Rightarrow 1]$$

Theorem 4: D-LORS-BCPA $\wedge$ B-INT-CTXT $\wedge$ PR-TAG $\rightarrow$ OAE



$$\mathbf{Adv}_{\Pi}^{\mathsf{OAE}}(\mathscr{A}) = Pr[\mathscr{A}_{\Pi}^{\mathsf{OAE\text{-}REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\mathsf{OAE\text{-}IDEAL}} \Rightarrow 1]$$

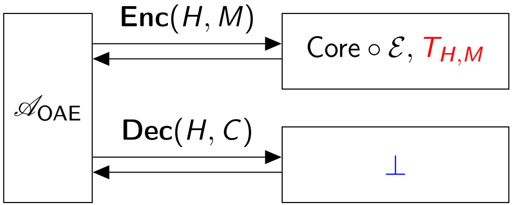
Theorem 4: D-LORS-BCPA $\wedge$ B-INT-CTXT $\wedge$ PR-TAG $\rightarrow$ OAE



$$\mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A}) = Pr[\mathscr{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1]$$

$$\leq \mathbf{Adv}_{\Pi}^{\text{B-INT-CTXT}}(\mathscr{A}_c)$$

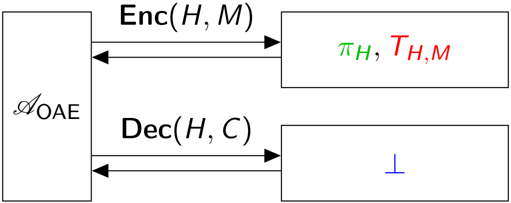
Theorem 4: D-LORS-BCPA $\wedge$ B-INT-CTXT $\wedge$ PR-TAG $\rightarrow$ OAE



$$\mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A}) = Pr[\mathscr{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1]$$

$$\leq \mathbf{Adv}_{\Pi}^{\text{B-INT-CTXT}}(\mathscr{A}_c) + \mathbf{Adv}_{\Pi}^{\text{PR-TAG}}(\mathscr{A}_t)$$

Theorem 4: D-LORS-BCPA $\wedge$ B-INT-CTXT $\wedge$ PR-TAG $\rightarrow$ OAE



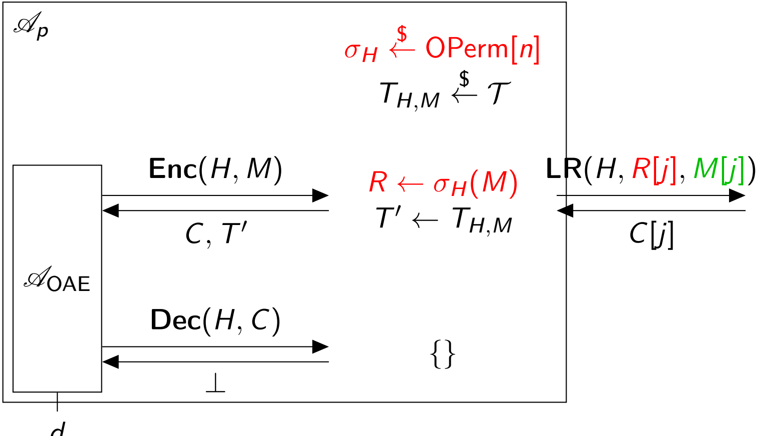
$$\mathbf{Adv}_{\Pi}^{\mathsf{OAE}}(\mathscr{A}) = Pr[\mathscr{A}_{\Pi}^{\mathsf{OAE\text{-}REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\mathsf{OAE\text{-}IDEAL}} \Rightarrow 1]$$

$$\leq \mathbf{Adv}_{\Pi}^{\mathsf{B\text{-}INT\text{-}CTXT}}(\mathscr{A}_c) + \mathbf{Adv}_{\Pi}^{\mathsf{PR\text{-}TAG}}(\mathscr{A}_t) + \mathbf{Adv}_{\Pi}^{\mathsf{D\text{-}LORS\text{-}BCPA}}(\mathscr{A}_p)$$

Theorem 4: reduction of D-LORS-BCPA

Reduction between D-LORS-BCPA adversary $\mathscr{A}_p$ and OAE adversary $\mathscr{A}$?

Reduction between D-LORS-BCPA adversary $\mathscr{A}_p$ and OAE adversary $\mathscr{A}$?



Lemma 5: $\mathrm{Core}(\mathcal{E}(K, H, \sigma_H(\cdot)))$ is equivalent to $\pi_H \xleftarrow{\$} \mathrm{OPerm}[n]$

Conclusion

- Reformulation of blockwise privacy for *deterministic* OAE schemes. Definition of *online-respecting* adversaries.
- Proposition of a new PR-TAG security notion.
- Proof of equivalence between OAE and blockwise notions: OAE $\leftrightarrow$ D-LORS-BCPA $\wedge$ B-INT-CTXT $\wedge$ PR-TAG

Conclusion

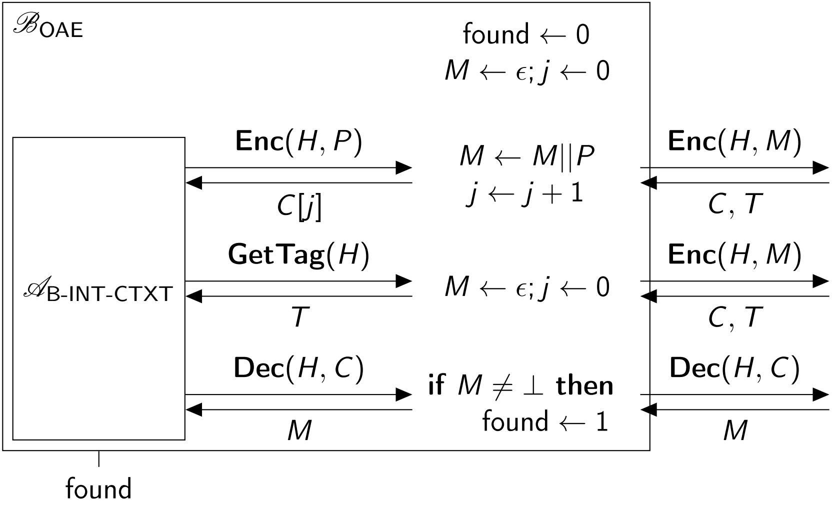
- Reformulation of blockwise privacy for *deterministic* OAE schemes. Definition of *online-respecting* adversaries.
- Proposition of a new PR-TAG security notion.
- Proof of equivalence between OAE and blockwise notions: OAE $\leftrightarrow$ D-LORS-BCPA $\wedge$ B-INT-CTXT $\wedge$ PR-TAG

Open questions:

- Overlap between D-LORS-BCPA and PR-TAG? Minimality of PR-TAG?

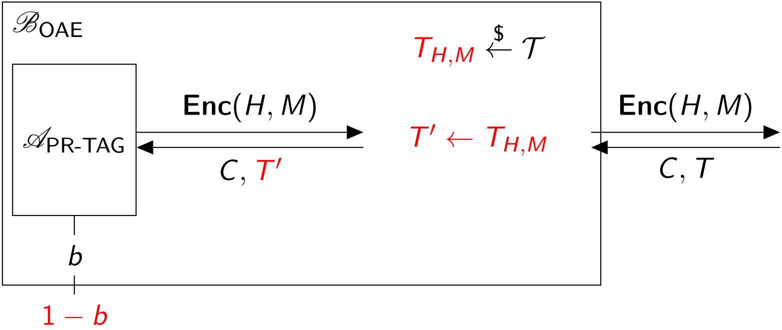
Thank you for your attention!

Bonus slides



Advantage: $\mathbf{Adv}_{\Pi}^{\text{B-INT-CTXT}}(\mathscr{A}) = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$

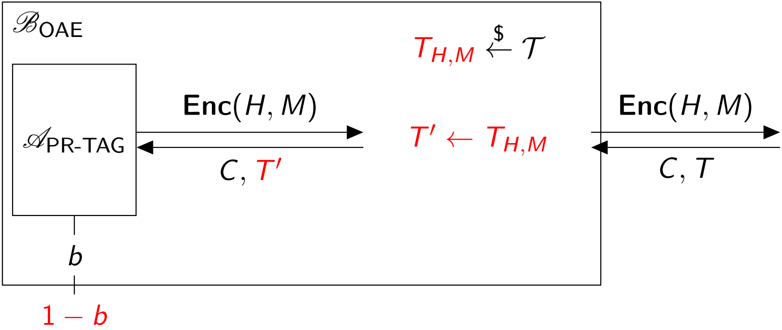
Theorem 3: OAE → PR-TAG



Advantage: $\mathbf{Adv}_{\Pi}^{\text{PR-TAG}}(\mathscr{A}) = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A}) + \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$

$$Pr[\mathscr{A}_{\Pi}^{\text{PR-TAG-REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A})$$
$$Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{PR-TAG-IDEAL}} \Rightarrow 1] = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$$

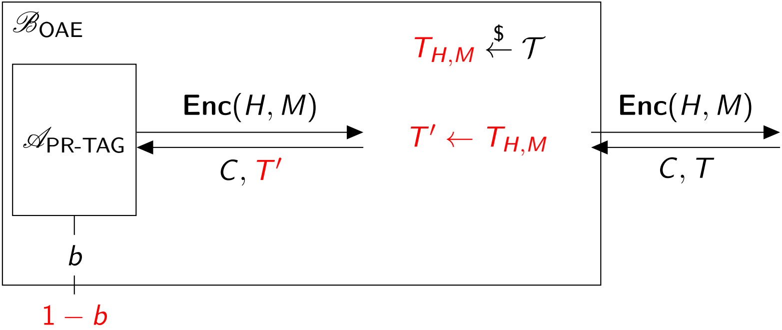
Theorem 3: OAE → PR-TAG



Advantage: $\mathbf{Adv}_{\Pi}^{\text{PR-TAG}}(\mathscr{A}) = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A}) + \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$

$$Pr[\mathscr{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A})$$
$$Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{PR-TAG-IDEAL}} \Rightarrow 1] = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$$

Theorem 3: OAE → PR-TAG



Advantage: $\mathbf{Adv}_{\Pi}^{\text{PR-TAG}}(\mathscr{A}) = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A}) + \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$

$$Pr[\mathscr{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - Pr[\mathscr{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{A})$$
$$Pr[\mathscr{B}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 0] - Pr[\mathscr{B}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 0] = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathscr{B})$$