

Linking OAE and Blockwise Attack Models

Fast Software Encryption 2017

Guillaume Endignoux, Damian Vizár

EPFL, Switzerland

Wednesday 8th March, 2017

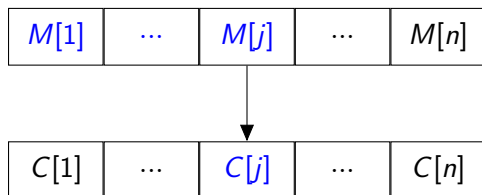
This work was partially supported by Microsoft Research.

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)
⇒ most proposed schemes are *online*.



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

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] \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?

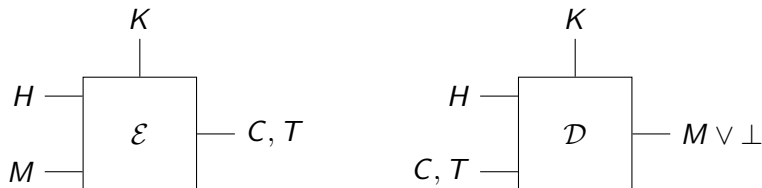
Main contribution: we prove equivalence between OAE and blockwise notions, modulo new PR-TAG notion.

Online authenticated encryption

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

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

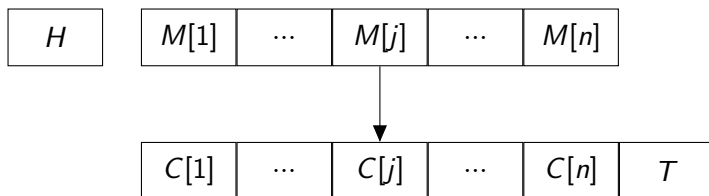
- finite key space \mathcal{K}
- deterministic algorithms \mathcal{E} and \mathcal{D}



Required properties:

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

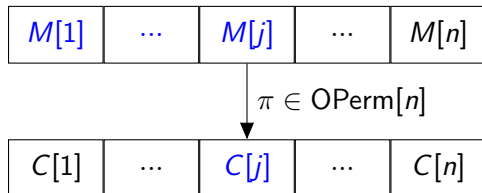
Online authenticated encryption



- 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 $M[1], \dots, M[j]$.

We consider the following notions:

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

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

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

proc Enc(H, M)

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

proc Dec(H, C)

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

Game OAE-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

$\pi_H \xleftarrow{\$} \text{OPerm}[n]$

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 \perp

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

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

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

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

Game LORS-BCPA

proc Initialize

$$K \xleftarrow{\$} \mathcal{K}$$
$$b \xleftarrow{\$} \{0, 1\}$$
$$\tilde{H} \leftarrow \perp; \quad \tilde{M} \leftarrow \varepsilon; \quad j \leftarrow 0$$

proc LR(H, P_0, P_1)

$$\text{if } \tilde{H} = \perp \text{ then } \tilde{H} \leftarrow H$$
$$\tilde{M} \leftarrow \tilde{M} || P_b$$
$$C \leftarrow \text{Core}(\mathcal{E}(K, \tilde{H}, \tilde{M}))$$
$$j \leftarrow j + 1$$
$$\text{return } C[j]$$

Game LORS-BCPA

proc Initialize

```
 $K \xleftarrow{\$} \mathcal{K}$   
 $b \xleftarrow{\$} \{0, 1\}$   
 $\tilde{H} \leftarrow \perp; \tilde{M} \leftarrow \varepsilon; j \leftarrow 0$ 
```

proc LR(H, P_0, P_1)

```
if  $\tilde{H} = \perp$  then  $\tilde{H} \leftarrow H$   
 $\tilde{M} \leftarrow \tilde{M} || P_b$   
 $C \leftarrow \text{Core}(\mathcal{E}(K, \tilde{H}, \tilde{M}))$   
 $j \leftarrow j + 1$   
return  $C[j]$ 
```

proc GetTag(H)

```
if  $\tilde{H} = \perp$  then  $\tilde{H} \leftarrow H$   
 $T \leftarrow \text{Tag}(\mathcal{E}(K, \tilde{H}, \tilde{M}))$   
 $\tilde{H} \leftarrow \perp; \tilde{M} \leftarrow \varepsilon; j \leftarrow 0$   
return  $T$ 
```

proc Finalize(d)

```
return  $d = b$ 
```

Game LORS-BCPA

proc Initialize

```
 $K \xleftarrow{\$} \mathcal{K}$   
 $b \xleftarrow{\$} \{0, 1\}$   
 $\tilde{H} \leftarrow \perp; \tilde{M} \leftarrow \varepsilon; j \leftarrow 0$ 
```

proc LR(H, P_0, P_1)

```
if  $\tilde{H} = \perp$  then  $\tilde{H} \leftarrow H$   
 $\tilde{M} \leftarrow \tilde{M} || P_b$   
 $C \leftarrow \text{Core}(\mathcal{E}(K, \tilde{H}, \tilde{M}))$   
 $j \leftarrow j + 1$   
return  $C[j]$ 
```

proc GetTag(H)

```
if  $\tilde{H} = \perp$  then  $\tilde{H} \leftarrow H$   
 $T \leftarrow \text{Tag}(\mathcal{E}(K, \tilde{H}, \tilde{M}))$   
 $\tilde{H} \leftarrow \perp; \tilde{M} \leftarrow \varepsilon; j \leftarrow 0$   
return  $T$ 
```

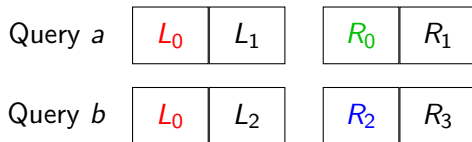
proc Finalize(d)

```
return  $d = b$ 
```

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

Blockwise privacy: deterministic schemes?

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

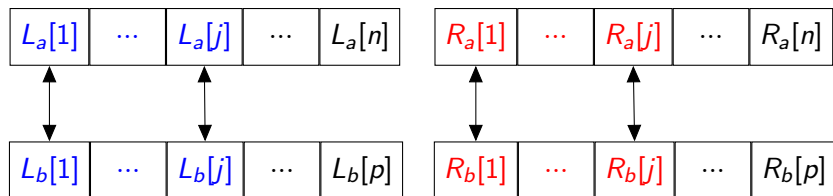


\Rightarrow Compare $C_a[0]$ and $C_b[0]$ to distinguish between left and right.

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

¹length of longest common prefix

Game B-INT-CTXT

proc Initialize

$\text{win} \leftarrow 0$

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

$\mathcal{X} \leftarrow \emptyset$

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

proc Enc(H, P)

if $\tilde{H} = \perp$ then $\tilde{H} \leftarrow H$

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

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

$j \leftarrow j + 1$

return $C[j]$

Game B-INT-CTXT

proc Initialize

```
win  $\leftarrow$  0  
 $K \xleftarrow{\$}$   $\mathcal{K}$   
 $\mathcal{X} \leftarrow \emptyset$   
 $\tilde{H} \leftarrow \perp$ ;  $\tilde{M} \leftarrow \varepsilon$ ;  $j \leftarrow 0$ 
```

proc Enc(H, P)

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

proc GetTag(H)

```
if  $\tilde{H} = \perp$  then  $\tilde{H} \leftarrow H$   
 $C \leftarrow \mathcal{E}(K, \tilde{H}, \tilde{M})$   
 $\mathcal{X} \leftarrow \mathcal{X} \cup \{(\tilde{H}, C)\}$   
 $\tilde{H} \leftarrow \perp$ ;  $\tilde{M} \leftarrow \varepsilon$ ;  $j \leftarrow 0$   
return 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 win  $\leftarrow$  1  
return  $M$ 
```

proc Finalize()

```
return win
```

Game B-INT-CTXT

proc Initialize

```

win  $\leftarrow$  0
 $K \xleftarrow{\$}$   $\mathcal{K}$ 
 $\mathcal{X} \leftarrow \emptyset$ 
 $\tilde{H} \leftarrow \perp$ ;  $\tilde{M} \leftarrow \varepsilon$ ;  $j \leftarrow 0$ 
    
```

proc Enc(H, P)

```

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

proc GetTag(H)

```

if  $\tilde{H} = \perp$  then  $\tilde{H} \leftarrow H$ 
 $C \leftarrow \mathcal{E}(K, \tilde{H}, \tilde{M})$ 
 $\mathcal{X} \leftarrow \mathcal{X} \cup \{(\tilde{H}, C)\}$ 
 $\tilde{H} \leftarrow \perp$ ;  $\tilde{M} \leftarrow \varepsilon$ ;  $j \leftarrow 0$ 
return Tag( $C$ )
    
```

proc Dec(H, C)

```

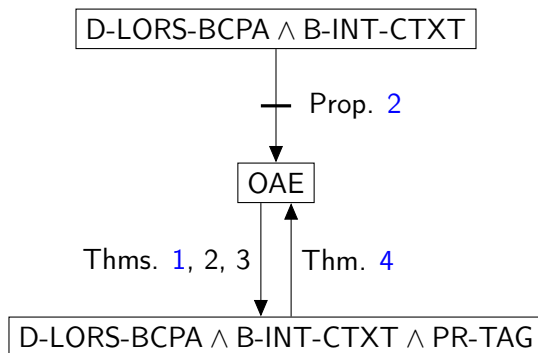
 $M \leftarrow \mathcal{D}(K, H, C)$ 
if  $(H, C) \in \mathcal{X}$  then  $M \leftarrow \perp$ 
if  $M \neq \perp$  then win  $\leftarrow$  1
return  $M$ 
    
```

proc Finalize()

```

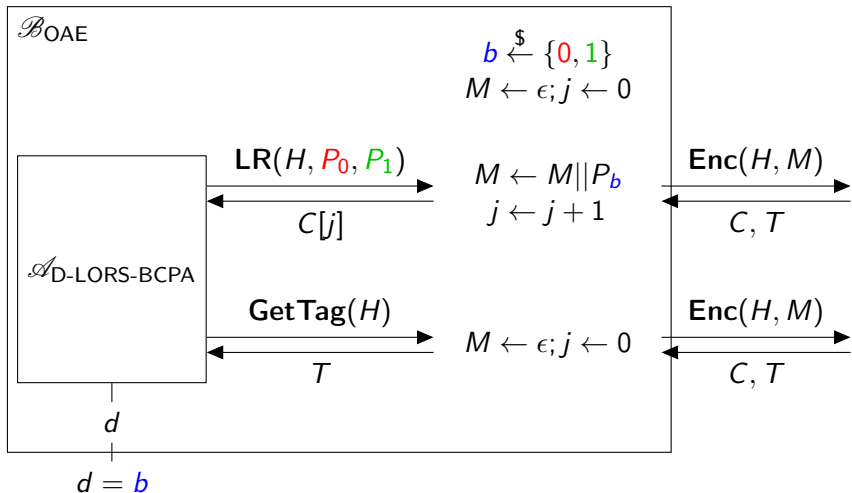
return win
    
```

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



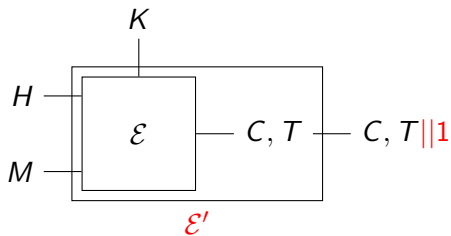
Relations between notions shown in the paper.

Theorem 1: OAE \rightarrow D-LORS-BCPA

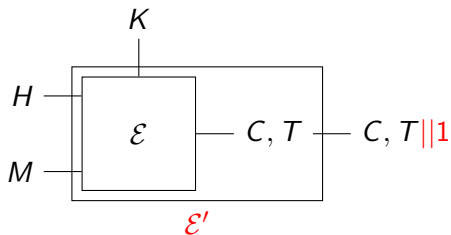


Advantage: $\text{Adv}_{\Pi}^{\text{D-LORS-BCPA}}(\mathcal{A}) = 2 \cdot \text{Adv}_{\Pi}^{\text{OAE}}(\mathcal{B})$

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

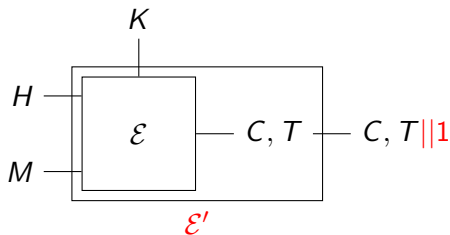


We construct a counter-example \mathcal{E}'



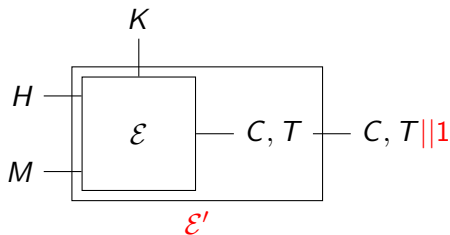
- \mathcal{E}' is as secure as \mathcal{E} for D-LORS-BCPA and B-INT-CTXT.

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 $\frac{1}{2}$.

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)

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

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)

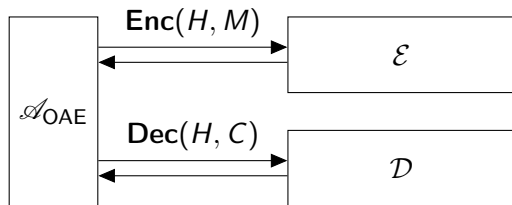
$C \leftarrow \text{Core}(\mathcal{E}(K, H, M))$

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

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

Theorem 4:

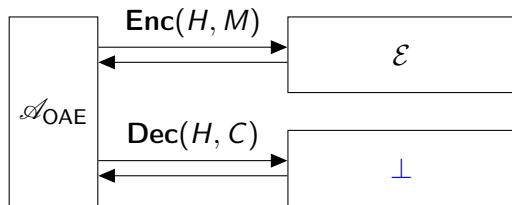
D-LORS-BCPA \wedge B-INT-CTXT \wedge PR-TAG \rightarrow OAE



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

Theorem 4:

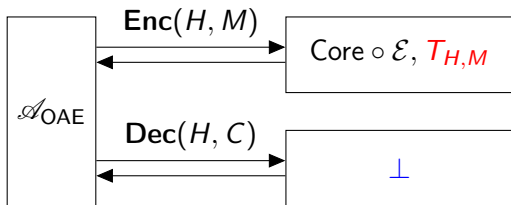
D-LORS-BCPA \wedge B-INT-CTXT \wedge PR-TAG \rightarrow OAE



$$\begin{aligned} \text{Adv}_{\Pi}^{\text{OAE}}(\mathcal{A}) &= \Pr[\mathcal{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - \Pr[\mathcal{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] \\ &\leq \text{Adv}_{\Pi}^{\text{B-INT-CTXT}}(\mathcal{A}_C) \end{aligned}$$

Theorem 4:

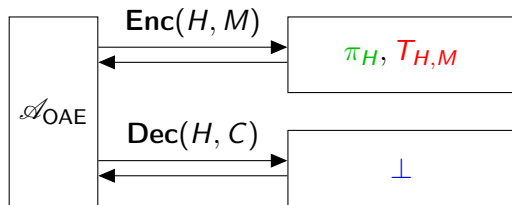
D-LORS-BCPA \wedge B-INT-CTXT \wedge PR-TAG \rightarrow OAE



$$\begin{aligned} \text{Adv}_{\Pi}^{\text{OAE}}(\mathcal{A}) &= \Pr[\mathcal{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - \Pr[\mathcal{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] \\ &\leq \text{Adv}_{\Pi}^{\text{B-INT-CTXT}}(\mathcal{A}_c) + \text{Adv}_{\Pi}^{\text{PR-TAG}}(\mathcal{A}_t) \end{aligned}$$

Theorem 4:

D-LORS-BCPA \wedge B-INT-CTXT \wedge PR-TAG \rightarrow OAE



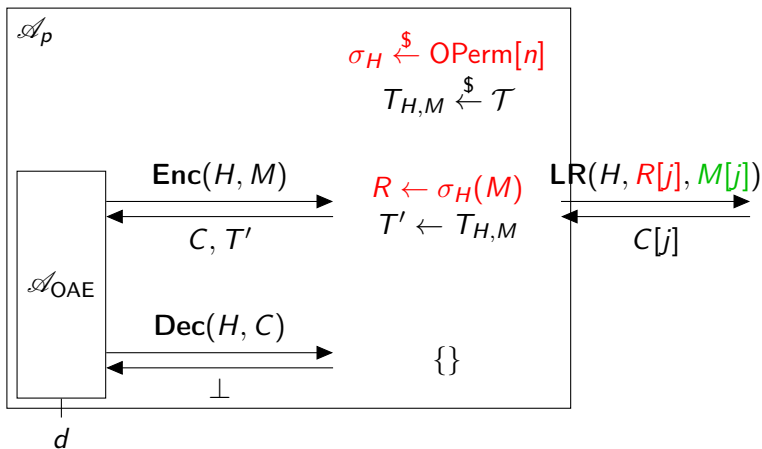
$$\begin{aligned} \text{Adv}_{\Pi}^{\text{OAE}}(\mathcal{A}) &= \Pr[\mathcal{A}_{\Pi}^{\text{OAE-REAL}} \Rightarrow 1] - \Pr[\mathcal{A}_{\Pi}^{\text{OAE-IDEAL}} \Rightarrow 1] \\ &\leq \text{Adv}_{\Pi}^{\text{B-INT-CTXT}}(\mathcal{A}_c) + \text{Adv}_{\Pi}^{\text{PR-TAG}}(\mathcal{A}_t) + \text{Adv}_{\Pi}^{\text{D-LORS-BCPA}}(\mathcal{A}_p) \end{aligned}$$

Theorem 4: reduction of D-LORS-BCPA

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

Theorem 4: reduction of D-LORS-BCPA

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



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

- 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:
 $\text{OAE} \leftrightarrow \text{D-LORS-BCPA} \wedge \text{B-INT-CTXT} \wedge \text{PR-TAG}$

- 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:
 $\text{OAE} \leftrightarrow \text{D-LORS-BCPA} \wedge \text{B-INT-CTXT} \wedge \text{PR-TAG}$

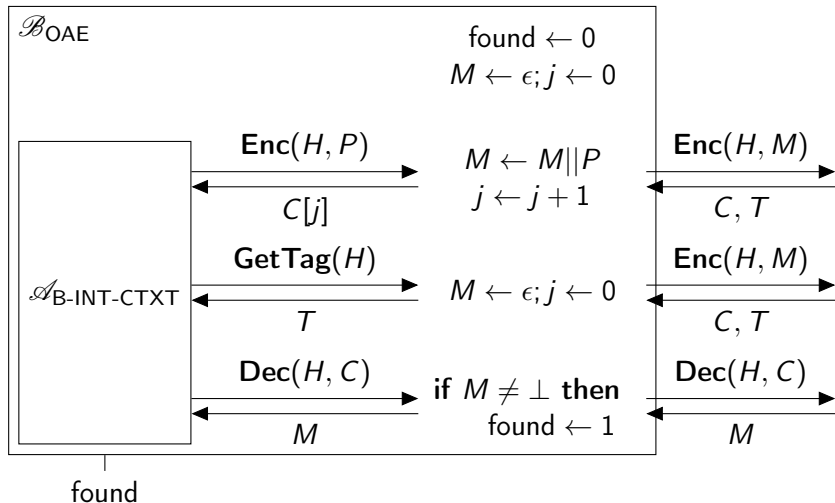
Open questions:

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

Thank you for your attention!

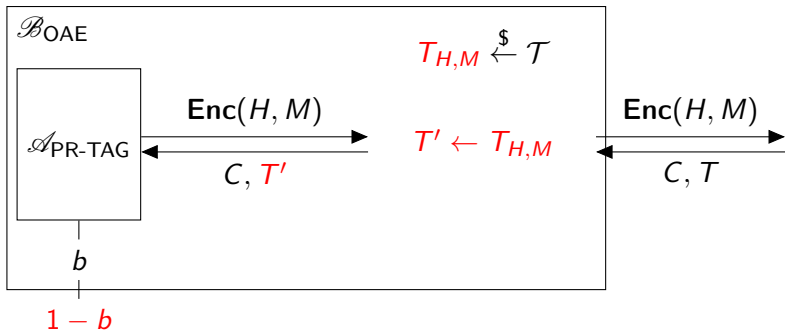
Bonus slides

Theorem 2: OAE \rightarrow B-INT-CTXT



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

Theorem 3: OAE \rightarrow PR-TAG

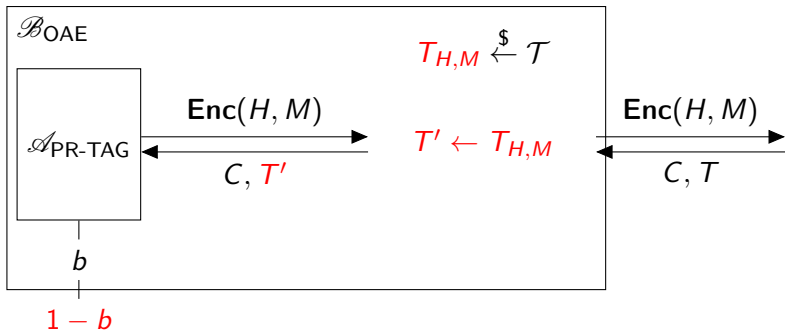


Advantage: $\text{Adv}_{\Pi}^{\text{PR-TAG}}(\mathcal{A}) = \text{Adv}_{\Pi}^{\text{OAE}}(\mathcal{A}) + \text{Adv}_{\Pi}^{\text{OAE}}(\mathcal{B})$

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

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

Theorem 3: OAE \rightarrow PR-TAG

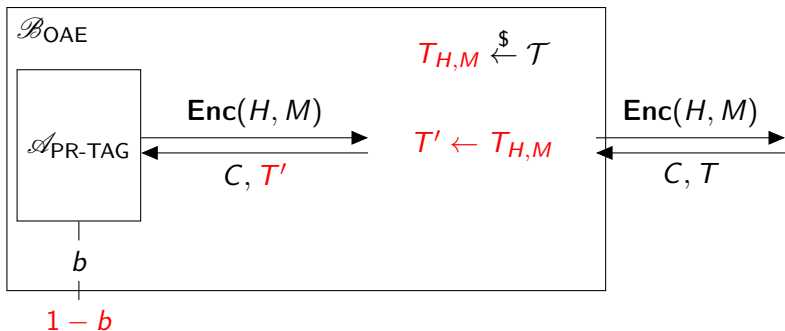


Advantage: $\mathbf{Adv}_{\Pi}^{\text{PR-TAG}}(\mathcal{A}) = \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathcal{A}) + \mathbf{Adv}_{\Pi}^{\text{OAE}}(\mathcal{B})$

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

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

Theorem 3: OAE \rightarrow PR-TAG



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

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

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