Security of Even-Mansour Ciphers under Key-dependent Messages

Pooya Farshim, **Louiza Khati**, Damien Vergnaud

ENS, Paris

ANSSI, Oppida

Wednesday, March 7th, 2018

KDM Security

- KDM for "Key Dependent Message" [BRS03]
  - Encryption Scheme Security in Presence of Key Dependent Message
- Disk Encryption [BHHO08]
  - Circular-Secure Encryption from Decision Diffie-Hellman

KDM Security

- KDM for "Key Dependent Message" [BRS03]
  - Encryption Scheme Security in Presence of Key Dependent Message

$\hookrightarrow$ $E_k(k)$ secure ?

- Disk Encryption [BHHO08]
  - Circular-Secure Encryption from Decision Diffie-Hellman

KDM Security

- KDM for "Key Dependent Message" [BRS03]
  - Encryption Scheme Security in Presence of Key Dependent Message

    ↳ $E_k(k)$ secure ?

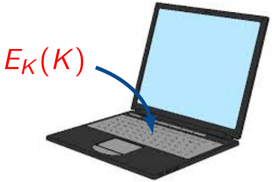
- Disk Encryption [BHHO08]
  - Circular-Secure Encryption from Decision Diffie-Hellman

KDM Security

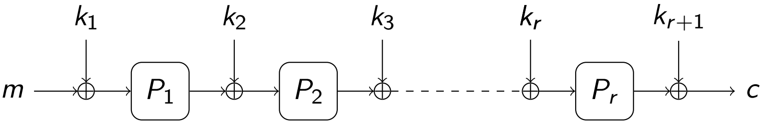
- KDM for "Key Dependent Message" [BRS03]
  - Encryption Scheme Security in Presence of Key Dependent Message

$\hookrightarrow E_k(k)$ secure ?

- Disk Encryption [BHHO08]
  - Circular-Secure Encryption from Decision Diffie-Hellman



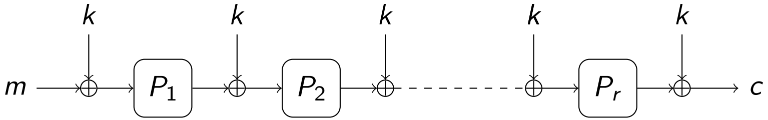
Even-Mansour r rounds



Many configurations for r rounds:

- r public random permutations: equal; **independent;** related.
- $r + 1$ keys: equal; **independent;** key schedule.

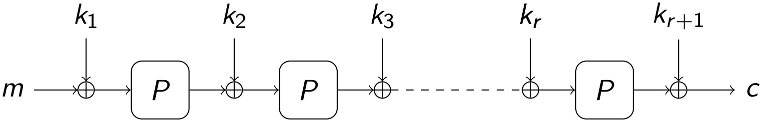
Even-Mansour r rounds



Many configurations for r rounds:

- r public random permutations: equal; **independent;** related.
- $r + 1$ keys: **equal;** independent; key schedule.

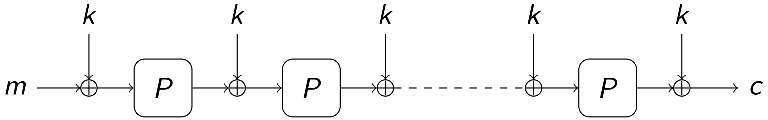
Even-Mansour r rounds



Many configurations for r rounds:

- r public random permutations: **equal;** independent; related.
- $r+1$ keys: equal; **independent;** key schedule.

Even-Mansour r rounds



Many configurations for r rounds:

- r public random permutations: **equal;** independent; related.
- $r + 1$ keys: **equal;** independent; key schedule.

Even-Mansour: Previous works

- Even-Mansour [EM97]
  - 1-r: SPRP up to the birthday bound
- 2-r Even Mansour [CLL$^+$14]
  - Master key, $P_1 = P_2$, 2-r EM secure beyond BB in RPM.
- Related Key Attack security [CS15], [FP15]
  - $\mathcal{A}$ can apply offset Δ to keys: $k_i \oplus \Delta$,
  - Single key, 2-r EM is xor-RKA CPA secure,
  - Single key, 3-r EM is xor-RKA CCA secure.
- Indifferentiability from an Ideal Cipher [DSST17]
  - 5-r EM necessary and sufficient.
- KDM security ?

Security Model: KDM security

$$K \xleftarrow{\$} \{0,1\}^k$$
$$b \xleftarrow{\$} \{0,1\}$$

Encryption: ϕ is a function
(including constants)

(b=1) Ideal world 

 π_E, π_D

Adversary

Oracle

(b=0) Real world 

EM_K, EM_K^-

Security Model: KDM security

Encryption: ϕ is a function
(including constants)

$$K \xleftarrow{\$} \{0,1\}^k$$
$$b \xleftarrow{\$} \{0,1\}$$

$\phi(.)$

Adversary

c

Oracle

(b=1) Ideal world 

 π_E, π_D

$$c = \pi_E(\phi(K))$$

(b=0) Real world 

EM_K, EM_K^{-}

$$c = EM_K(\phi(K))$$

Security Model: KDM security

Decryption: c is **constant**

$$K \xleftarrow{\$} \{0,1\}^k$$
$$b \xleftarrow{\$} \{0,1\}$$

c

Adversary

Oracle

m

(b=1) Ideal world 

 π_E, π_D

$$m = \pi_D(c)$$

(b=0) Real world 

EM_K, EM_K^-

$$m = EM_K^-(c)$$

Decrypting c **such that** $c = O(\phi(.))$
with $\phi(.) \neq$ **constant is forbidden!!**

KDM security requires Claw-Freeness

No restriction on set Φ

KDM security requires Claw-Freeness

No restriction on set Φ

Example: $\phi_i(.)$ = Set the i-th bit of K to 0 and Id

KDM security requires Claw-Freeness

No restriction on set Φ

Example: $\phi_i(.) =$ Set the i-th bit of K to 0 and Id

$\mathcal{A}$ makes two queries: Id and ϕ_i for a chosen i.

KDM security requires Claw-Freeness

No restriction on set Φ

Example: $\phi_i(.) =$ Set the i-th bit of K to 0 and Id

$\mathcal{A}$ makes two queries: Id and ϕ_i for a chosen i.

If $\mathrm{Enc}(Id(K)) = \mathrm{Enc}(\phi_i(K))$ then the i-th bit of K is 0

KDM security requires Claw-Freeness

No restriction on set Φ

Example: $\phi_i(.) =$ Set the i-th bit of K to 0 and Id

$\mathcal{A}$ makes two queries: Id and ϕ_i for a chosen i.

If $\mathrm{Enc}(Id(K)) = \mathrm{Enc}(\phi_i(K))$ then the i-th bit of K is 0

Key Recovery Attack!

KDM security requires Claw-Freeness

No restriction on set Φ

Example: $\phi_i(.)$ = Set the i-th bit of K to 0 and Id

$\mathcal{A}$ makes two queries: Id and ϕ_i for a chosen i.

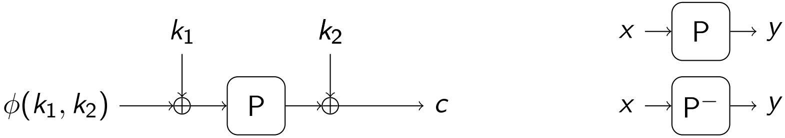
If $\text{Enc}(Id(K)) = \text{Enc}(\phi_i(K))$ then the i-th bit of K is 0

Key Recovery Attack!

Φ must be Claw-Free: It is hard to find $\phi_1 \neq \phi_2$ such that $\Pr[\phi_1(K) = \phi_2(K)]$ "is high".

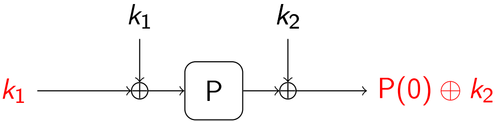
KDM security: Even-Mansour 1 round

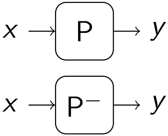
Key extraction with a claw-free set Φ



KDM Attack on 1-r Even-Mansour

Key extraction with a claw-free set Φ





k_2 extraction:

$\phi_1(k) = k_1$; $c_1 = P(0) \oplus k_2$

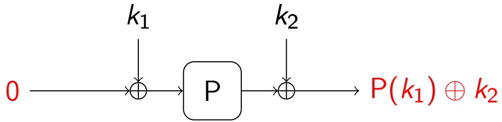
A computes $c_1 \oplus y_1 \rightarrow k_2$

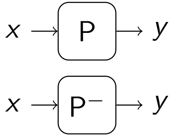
P

$x_1 = 0; y_1 = P(0)$

KDM Attack on 1-r Even-Mansour

Key extraction with a claw-free set Φ





k_2 extraction:
$\phi_1(k) = k_1;\ c_1 = P(0) \oplus k_2$
A computes $c_1 \oplus y_1 \rightarrow k_2$

P
$x_1 = 0; y_1 = P(0)$

k_1 extraction:
$\phi_2(k) = 0;\ c_2 = P(k_1) \oplus k_2;$
A computes $z = k_2 \oplus c_2$
$y_2 \rightarrow k_1$

P^-
$x_2 = z; y_2 = P^-(z)$

Even-Mansour KDM security under a set Φ

r	Perm	Keys	Set Φ ind. P_i
1	P	K_1, K_2	cf, offset-free*
2	P, P	K, K, K	cf, offset-free*
2	P, P	K_1, K_2, K_3	cf, ox-free
2	P_1, P_2	K_1, K_2, K_3	cf
3	P, P, P	K, K, K, K	cf, offset-free*
3	P, P, P	K_1, K_2, K_3, K_4	cf
3	P_1, P_2, P_3	K, K, K, K	cf
n	P, P, ..., P	$K, K, \ldots, K$	cf, offset-free*

offset: (ϕ, X) such that $\phi(K_1, K_2) = K_1 \oplus X$.
ox: (ϕ, X) such that $\phi(K_1, K_2, K_3) = K_1 \oplus K_2 \oplus X$.

* Sliding attack if the set Φ is not offset-free.

Security proof

KDM security of Even-Mansour 2 rounds

- Independent random permutations: $\mathsf{P}_1^{\pm}, \mathsf{P}_2^{\pm}$
- Independent random keys: K_1, K_2, K_3

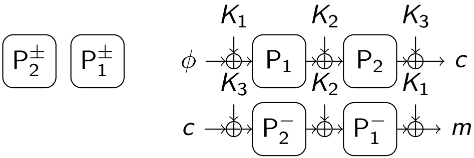
KDM rules:

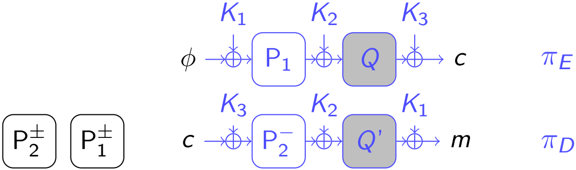
- Encryption/Decryption of oracle answers
- No repeat queries
  - $\phi_1 \neq \phi_2$
  - $c_1 \neq c_2$

The set Φ is:

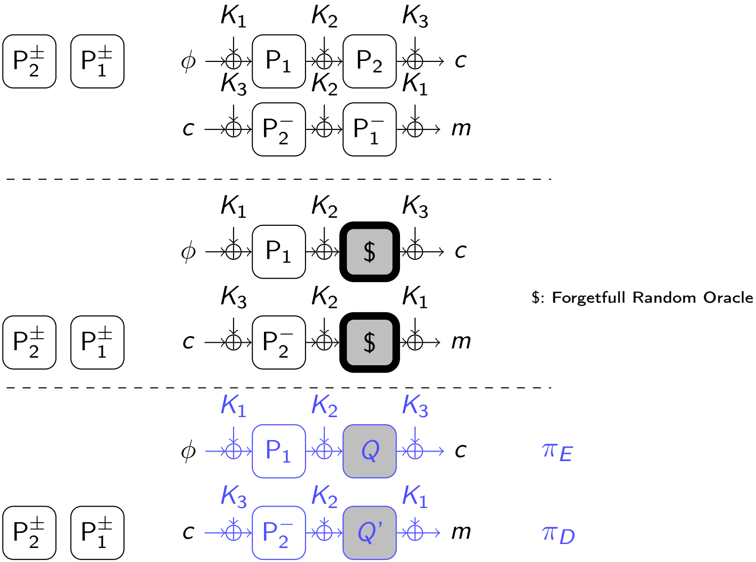
- Claw-Free
- Functions ϕ independent of $\mathsf{P}_i^{\pm}$

Security proof

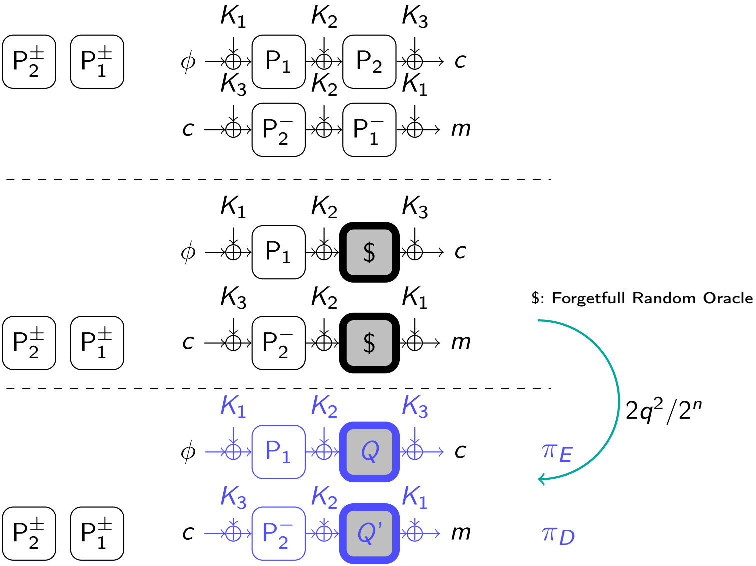




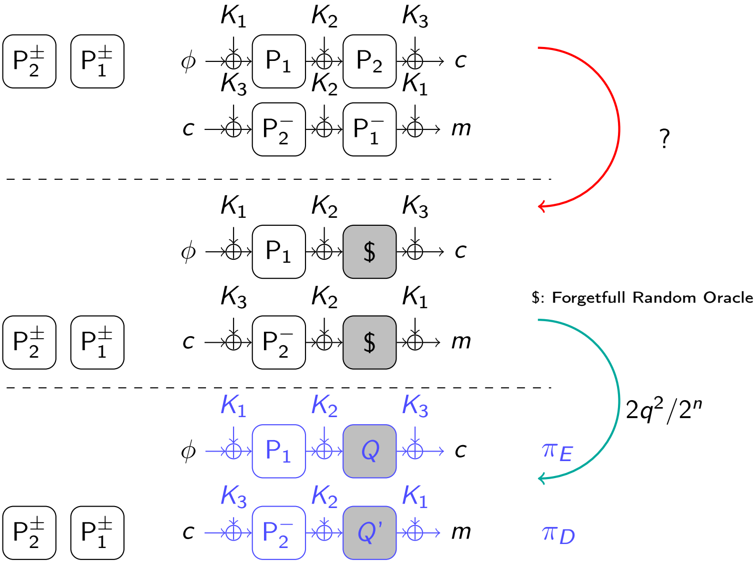
Security proof



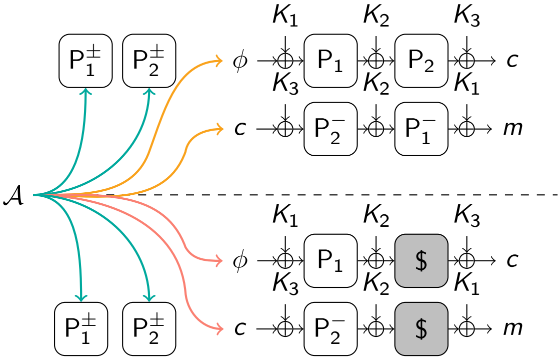
Security proof



Security proof

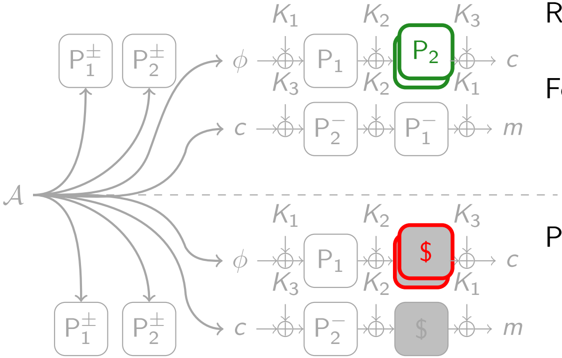


Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



Inconsistencies ?

Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



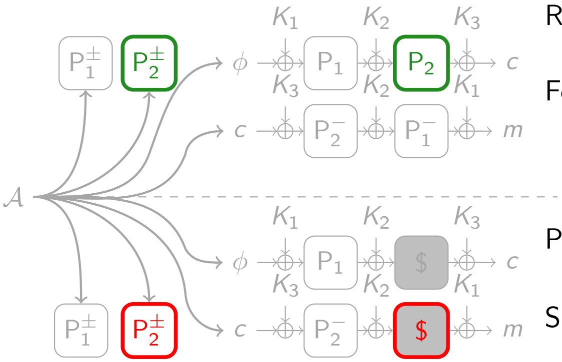
Reductions

Forgetfull game:

- no repeated queries on \$
- no "circular queries"

PRF/PRP switching lemma

Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



Reductions

Forgetfull game:

- no repeated queries on \$
- no "circular queries"

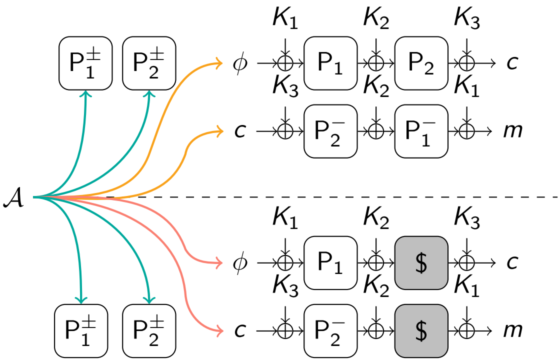
PRF/PRP switching lemma

Splitting game:

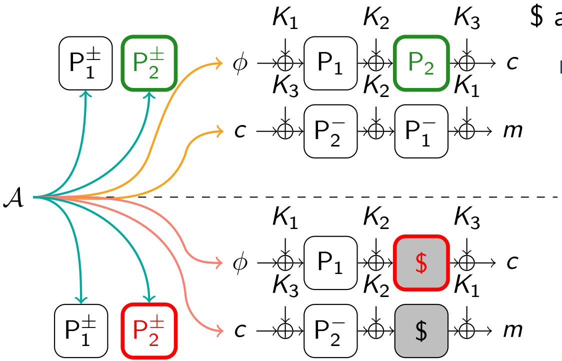
- no repeated queries on \$
- no "circular queries"

PRF/PRP switching lemma

Security proof: 2-r $\mathrm{EM}^{\mathrm{P}_1,\mathrm{P}_2}[K_1, K_2, K_3]$



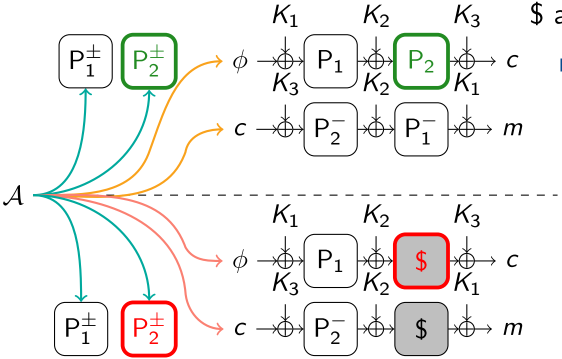
Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



\$ and direct accessed P_i

- $Enc(\phi)$ and $P_2^{+}(X)$
  - $X = P_1(\phi(K) \oplus K_1) \oplus K_2$
  - $P_2(X) = c \oplus K_3$

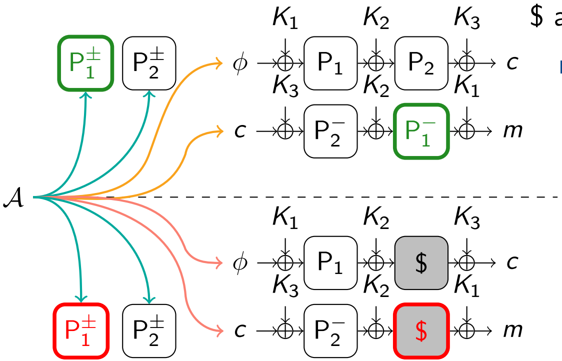
Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



\$ and direct accessed P_i

- $Enc(\phi)$ and $P_2^+(X)$
  - $X = P_1(\phi(K) \oplus K_1) \oplus K_2$
  - $P_2(X) = c \oplus K_3$
- $Enc(\phi), P_2^-(Y)$
  - $Y = c \oplus K_3$
  - $X = P_1(\phi(K) \oplus K_1) \oplus K_2$

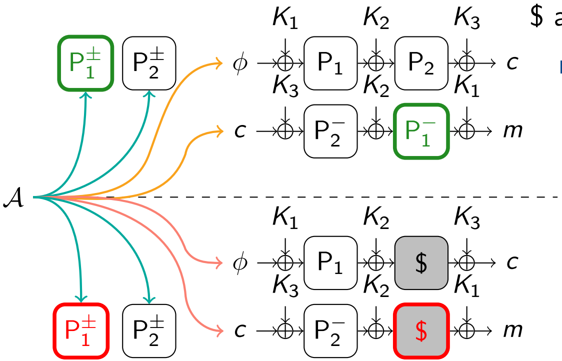
Security proof: 2-r $\mathrm{EM}^{\mathrm{P}_1,\mathrm{P}_2}[K_1, K_2, K_3]$



\$ and direct accessed P_i

- $Enc(\phi)$ and $\mathrm{P}_2^{+}(X)$
  - $X = \mathrm{P}_1(\phi(K) \oplus K_1) \oplus K_2$
  - $\mathrm{P}_2(X) = c \oplus K_3$
- $Enc(\phi), \mathrm{P}_2^{-}(Y)$
  - $Y = c \oplus K_3$
  - $X = \mathrm{P}_1(\phi(K) \oplus K_1) \oplus K_2$
- $Dec(c), \mathrm{P}_1^{-}(Y)$
  - $\mathrm{P}_2^{-}(c \oplus K_3) \oplus K_2 = Y$
  - $m \oplus K_1 = \mathrm{P}_1^{-}(Y)$

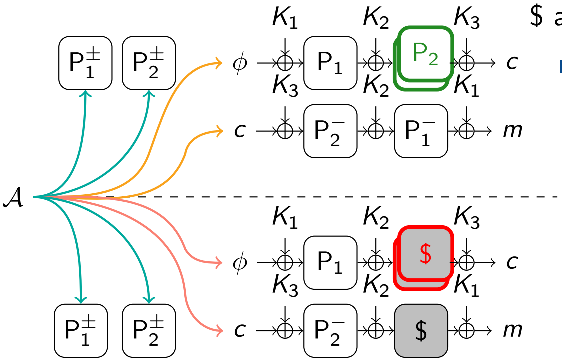
Security proof: 2-r $\mathrm{EM}^{\mathrm{P}_1,\mathrm{P}_2}[K_1, K_2, K_3]$



\$ and direct accessed P_i

- $Enc(\phi)$ and $\mathrm{P}_2^+(X)$
  - $X = \mathrm{P}_1(\phi(K) \oplus K_1) \oplus K_2$
  - $\mathrm{P}_2(X) = c \oplus K_3$
- $Enc(\phi), \mathrm{P}_2^-(Y)$
  - $Y = c \oplus K_3$
  - $X = \mathrm{P}_1(\phi(K) \oplus K_1) \oplus K_2$
- $Dec(c), \mathrm{P}_1^-(Y)$
  - $\mathrm{P}_2^-(c \oplus K_3) \oplus K_2 = Y$
  - $m \oplus K_1 = \mathrm{P}_1^-(Y)$
- $Dec(c), \mathrm{P}_1^+(X)$
  - $\mathrm{P}_2^-(c \oplus K_3) \oplus K_2 = \mathrm{P}_1^+(X)$
  - $m \oplus K_1 = X$

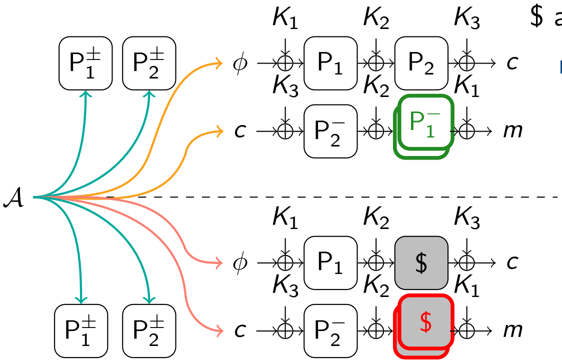
Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



\$ and itself

- $Enc^{+}(\phi_1)$ and $Enc(\phi_2)$
  - $\phi_1(K) = \phi_2(K)$ **Claw-free**

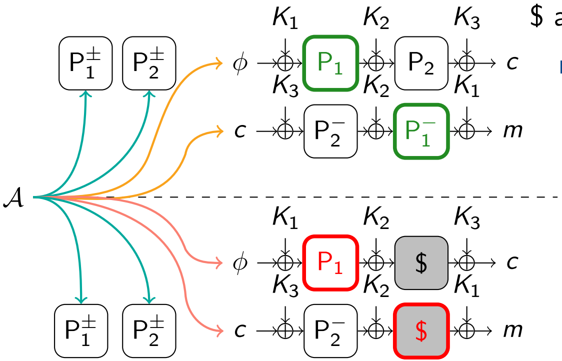
Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



\$ and itself

- $Enc^{+}(\phi_1)$ and $Enc(\phi_2)$
  - $\phi_1(K) = \phi_2(K)$ **Claw-free**
- $Dec(c_1), Dec(c_2)$
  - $c_1 = c_2$ repeat

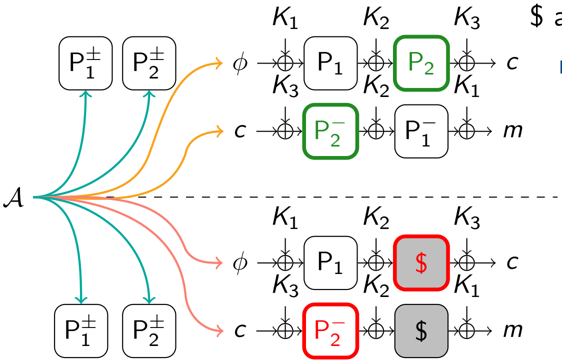
Security proof: 2-r $EM^{P_1,P_2}[K_1, K_2, K_3]$



\$ and internal P_i

- $Dec(c_1)$ then $Enc(\phi_2)$
  - $m_1 \oplus K_1 = \phi_2(K) \oplus K_1$ **Claw-free** or forbidden
  - $P_2^{-}(c_1 \oplus K_3) \oplus K_2 = P_1(\phi_2(K) \oplus K_1)$

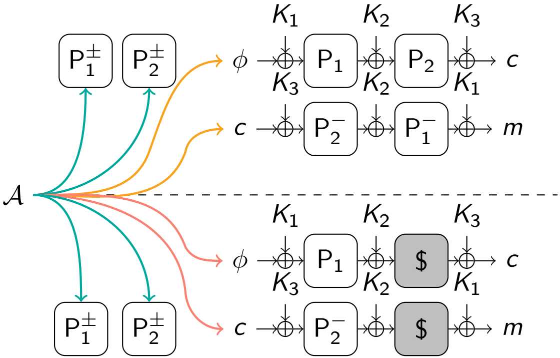
Security proof: 2-r $\mathrm{EM}^{\mathrm{P}_1,\mathrm{P}_2}[K_1, K_2, K_3]$



\$ and internal P_i

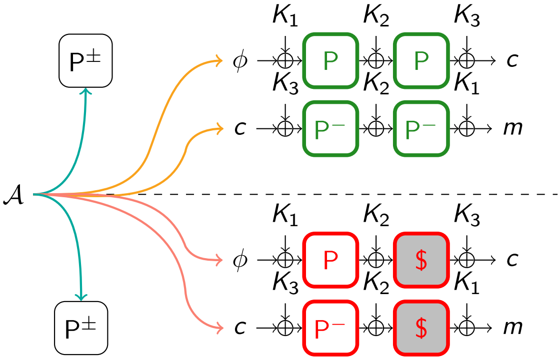
- $Dec(c_1)$ then $Enc(\phi_2)$
  - $m_1 \oplus K_1 = \phi_2(K) \oplus K_1$ **Claw-free** or forbidden
  - $\mathrm{P}_2^{-}(c_1 \oplus K_3) \oplus K_2 = \mathrm{P}_1(\phi_2(K) \oplus K_1)$
- $Enc(\phi_1)$ then $Dec(c_2)$
  - $\mathrm{P}_1(\phi_1(K) \oplus K_1) \oplus K_2 = \mathrm{P}_2^{-}(c_2 \oplus K_3)$
  - $c_1 \oplus K_3 = c_2 \oplus K_3$ forbidden

Security proof: 2-r $\mathsf{EM}^{\mathsf{P}_1,\mathsf{P}_2}[K_1, K_2, K_3]$



Φ-KDM Security up to the birthday bound with a set Φ that is Claw-Free and P_i independent.

Security proof: 2-r $EM^{P,P}[K_1, K_2, K_3]$



$P_1 = P_2 = P$

More collisions !!

Conclusion

To sum up:

- KDM security of 2 rounds Even-Mansour different keys, different permutations

In the paper:

- General framework to analyse with a two stage-adversary
  - KDM security, RKA security,
  - Different block ciphers.
- KDM security for Ideal Cipher;
- Analysis of different Even-Mansour configurations

Even-Mansour KDM security under a set Φ

r	Perm	Keys	Set Φ ind. P_i
1	P	K_1, K_2	cf, offset-free*
2	P, P	K, K, K	cf, offset-free*
2	P, P	K_1, K_2, K_3	cf, ox-free
2	$\mathsf{P}_1, \mathsf{P}_2$	K_1, K_2, K_3	cf
3	$\mathsf{P}, \mathsf{P}, \mathsf{P}$	K, K, K, K	cf, offset-free*
3	$\mathsf{P}, \mathsf{P}, \mathsf{P}$	K_1, K_2, K_3, K_4	cf
3	$\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3$	K, K, K, K	cf
n	$\mathsf{P}, \mathsf{P}, \ldots, \mathsf{P}$	$K, K, \ldots, K$	cf, offset-free*

offset: (ϕ, X) such that $\phi(K_1, K_2) = K_1 \oplus X$.
ox: (ϕ, X) such that $\phi(K_1, K_2, K_3) = K_1 \oplus K_2 \oplus X$.

* Sliding attack if the set Φ is not offset-free.

Thank you for your attention!
Questions?

Security of Even-Mansour Ciphers under Key-dependent Messages

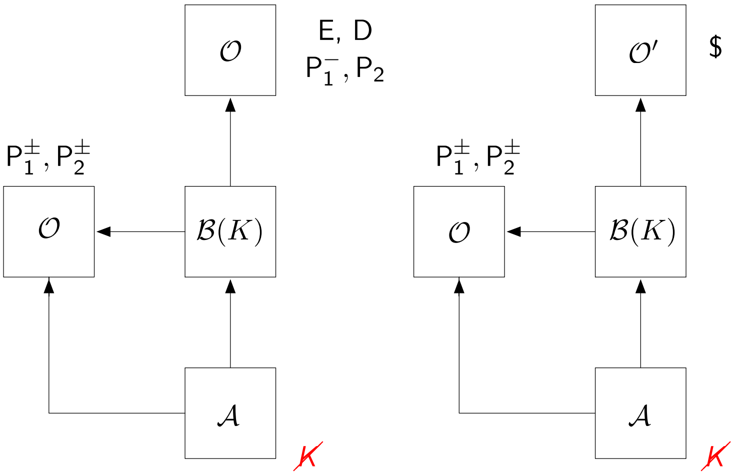
Pooya Farshim, **Louiza Khati**, Damien Vergnaud

ENS, Paris

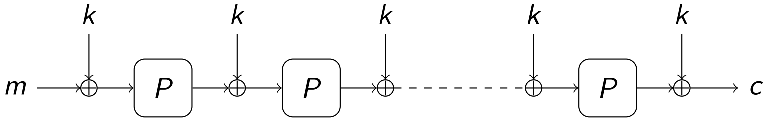
ANSSI, Oppida

Wednesday, March 7th, 2018

General Framework: Two-stage adversary



Sliding attack: Even-Mansour r rounds



$\phi_1 = 0$ then $EM(0) = P(k) \oplus k = c_1$
$\phi_2 = c_1 \oplus k$ then $c_2 = \mathrm{P}(\mathrm{P}(k) \oplus k) \oplus k$
$\mathcal{A}$ asks $x = c_1$ to P then $y = P(c_1) = \mathrm{P}[\mathrm{P}(k) \oplus k]$
$\mathcal{A}$ can computes k: $c_2 \oplus y$

Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky.
Circular-secure encryption from decision Diffie-Hellman.
In David Wagner, editor, CRYPTO 2008, volume 5157 of LNCS, pages 108–125. Springer, Heidelberg, August 2008.

John Black, Phillip Rogaway, and Thomas Shrimpton.
Encryption-scheme security in the presence of key-dependent messages.

In Kaisa Nyberg and Howard M. Heys, editors, SAC 2002, volume 2595 of LNCS, pages 62–75. Springer, Heidelberg, August 2003.

Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger.
Minimizing the two-round Even-Mansour cipher.

In Juan A. Garay and Rosario Gennaro, editors, CRYPTO 2014, Part I, volume 8616 of LNCS, pages 39–56. Springer, Heidelberg, August 2014.

Benoit Cogliati and Yannick Seurin.
On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks.

In Elisabeth Oswald and Marc Fischlin, editors, EUROCRYPT 2015, Part I, volume 9056 of LNCS, pages 584–613. Springer, Heidelberg, April 2015.

Yuanxi Dai, Yannick Seurin, John Steinberger, and Aishwarya Thiruvengadam.
Indifferentiability of iterated Even-Mansour ciphers with non-idealized key-schedules: Five rounds are necessary and sufficient.

Cryptology ePrint Archive, Report 2017/042, 2017.
http://eprint.iacr.org/2017/042.

Shimon Even and Yishay Mansour.
A construction of a cipher from a single pseudorandom permutation.
Journal of Cryptology, 10(3):151–162, 1997.

Pooya Farshim and Gordon Procter.

The related-key security of iterated Even-Mansour ciphers.
In Gregor Leander, editor, FSE 2015, volume 9054 of LNCS, pages 342–363. Springer, Heidelberg, March 2015.