The Iterated Random Permutation Problem with Applications to Cascade Encryption

Brice Minaud[1,2], Yannick Seurin[1]

[1] ANSSI, France
[2] Université Rennes 1, France

CRYPTO 2015

Plan

1. Motivation.
2. The Iterated Permutation Problem.
3. Main theorem.
4. Matching attack.
5. Conclusion.

A Simple Question

Assume you do not trust $\mathbf{AES_k}$ as is.

A simple heuristic strengthening: $\mathbf{AES_k} \circ \mathbf{AES_k}$.

Assuming $\mathbf{AES_k}$ is secure, *is this secure?*

Can we prove it?

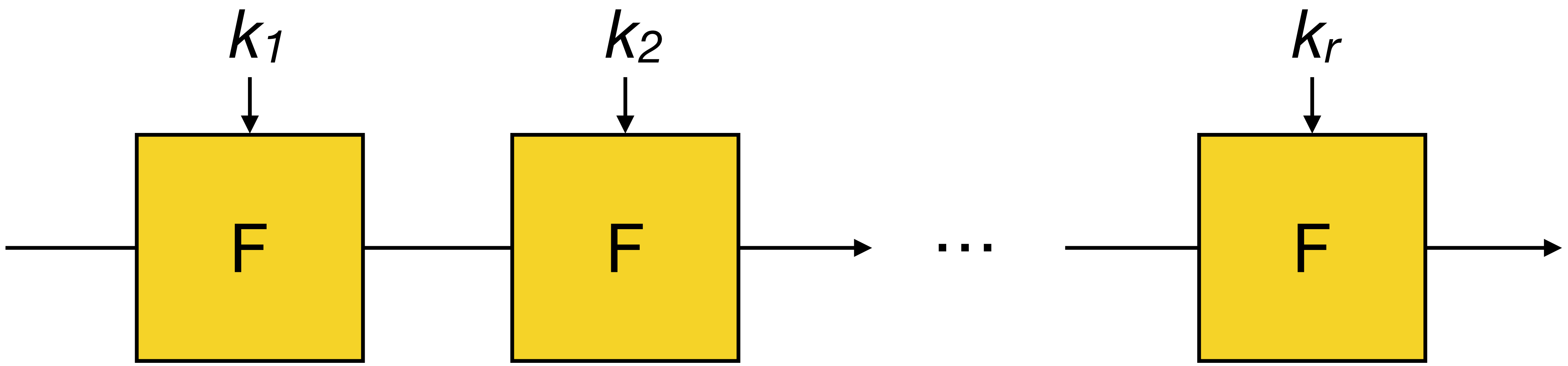
Strong Pseudo-Randomness

We measure "security" by the strong pseudo-randomness notion:

$$\mathbf{Adv}_E^{\mathsf{sprp}}(\mathcal{D}) = \Big|\Pr\Big[P \leftarrow_\$ \mathsf{Perm}(S) : \mathcal{D}^{P,P^{-1}} = 1\Big] - \Pr\Big[k \leftarrow_\$ K : \mathcal{D}^{E_k,(E_k)^{-1}=1}\Big]\Big|$$

→ standard adaptive, two-sided adversary trying to distinguish E_k from a random permutation.

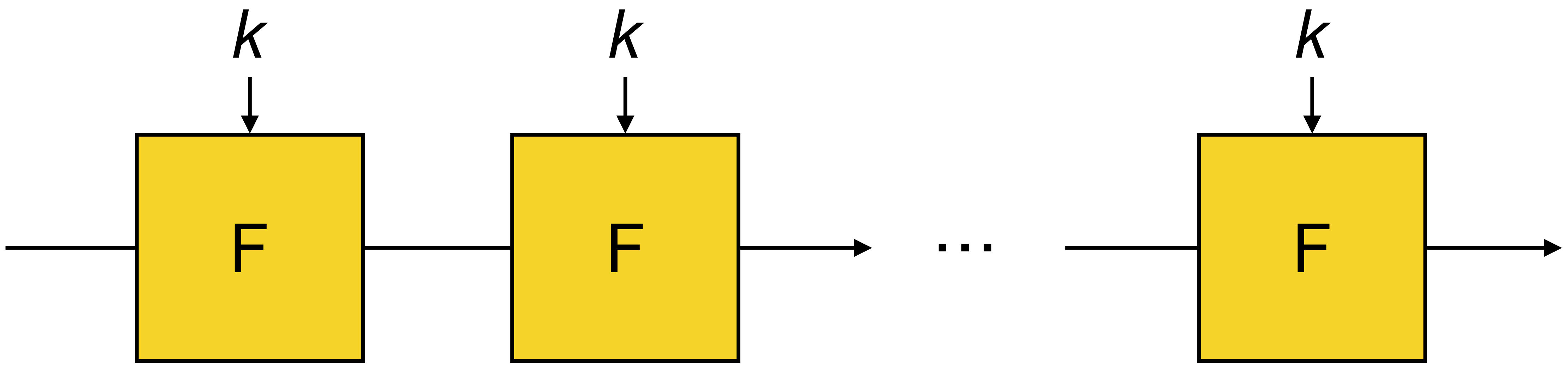
Cascade encryption



Independent keys ⇒ security amplification.

Many results in the computational, information-theoretic and ideal cipher models.

Cascade encryption



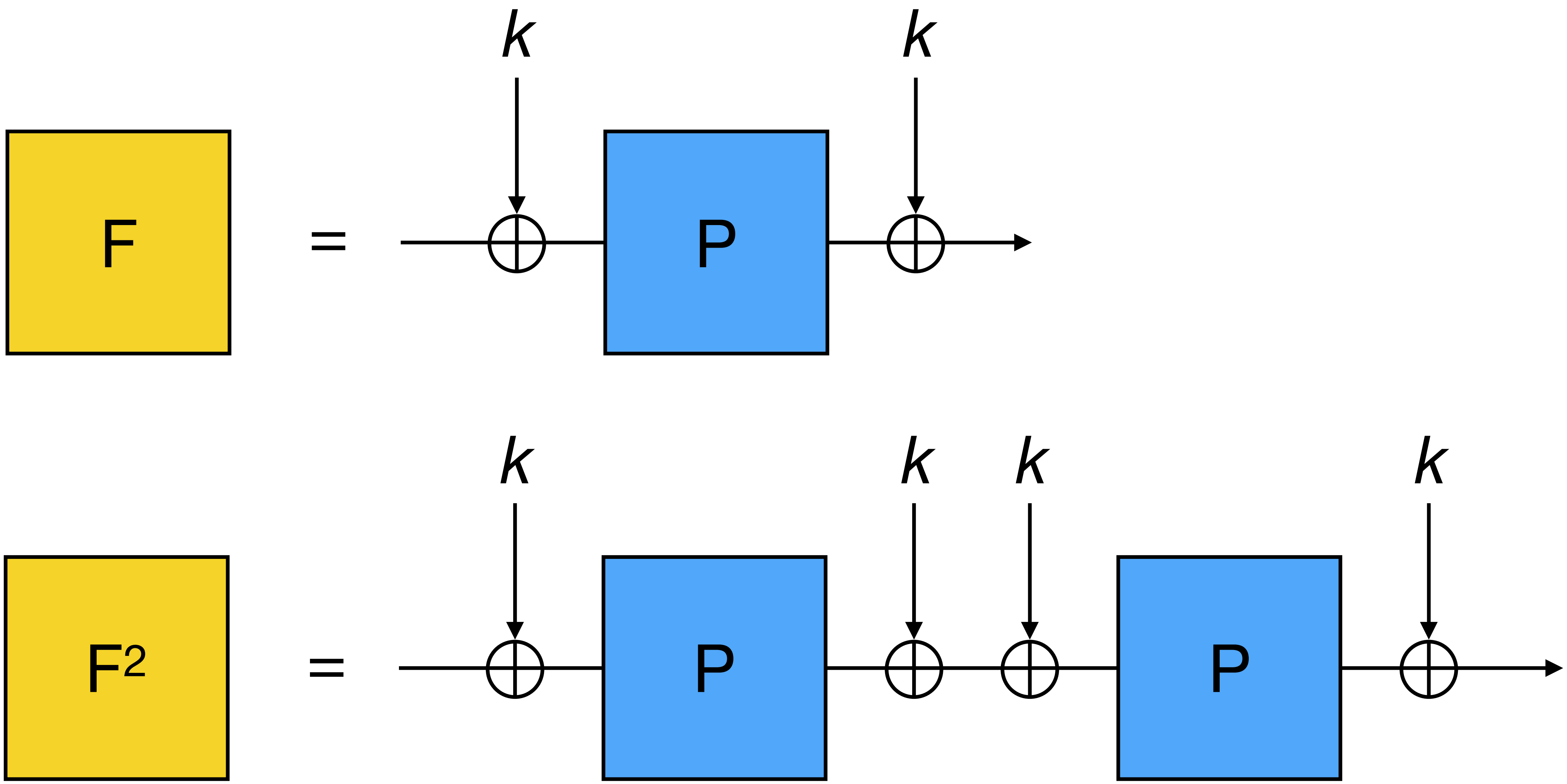
Non-independent keys ⇒ ?

Virtually no result when keys are *not* independent.

We consider the case where a single key is repeated.

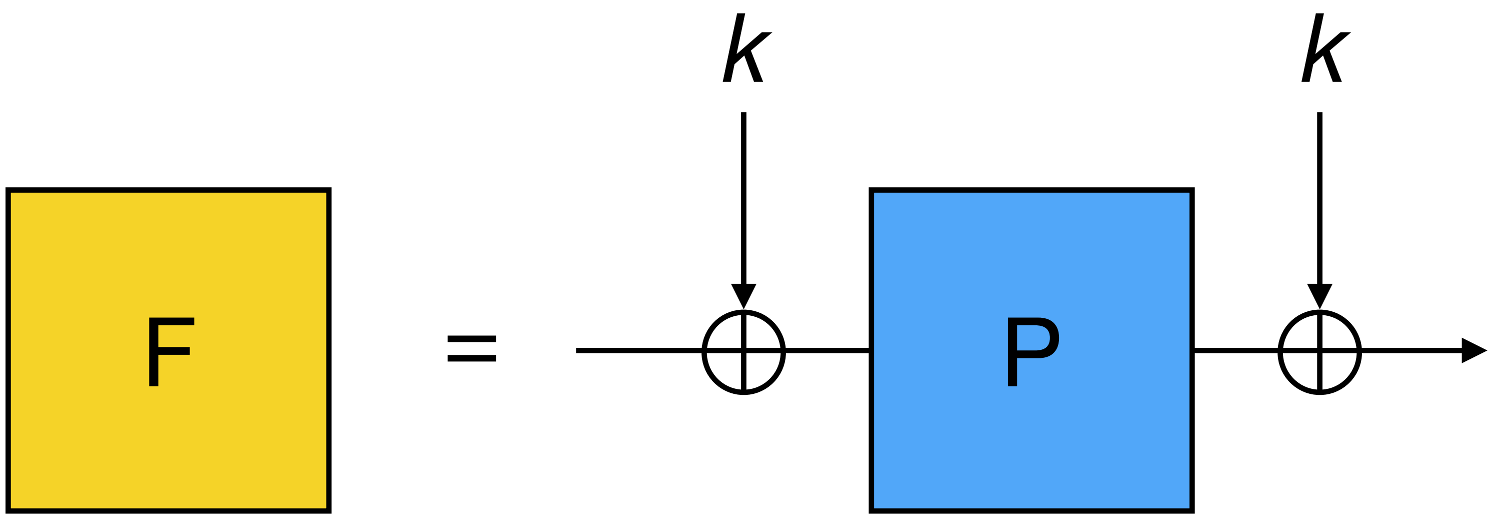
Cascade encryption

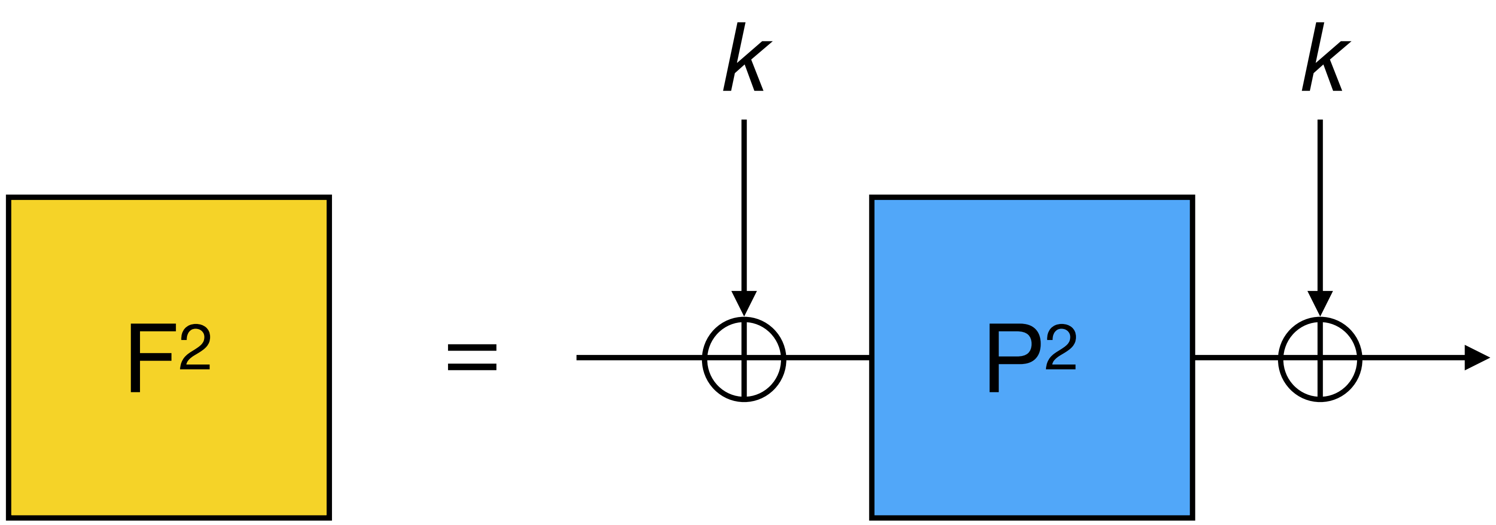
If F is an Even-Mansour construction…



Cascade encryption

If F is an Even-Mansour construction…





⇒ no security amplification

Main result

Iterating a block cipher a *constant* number of times has a negligible effect on its SPRP security:

$$\mathbf{Adv}_{E^r}^{\mathrm{sprp}}(q, t) \leq \mathbf{Adv}_{E}^{\mathrm{sprp}}(rq, t') + \frac{(2r+1)q}{N}$$

E : block cipher

N : size of the message space

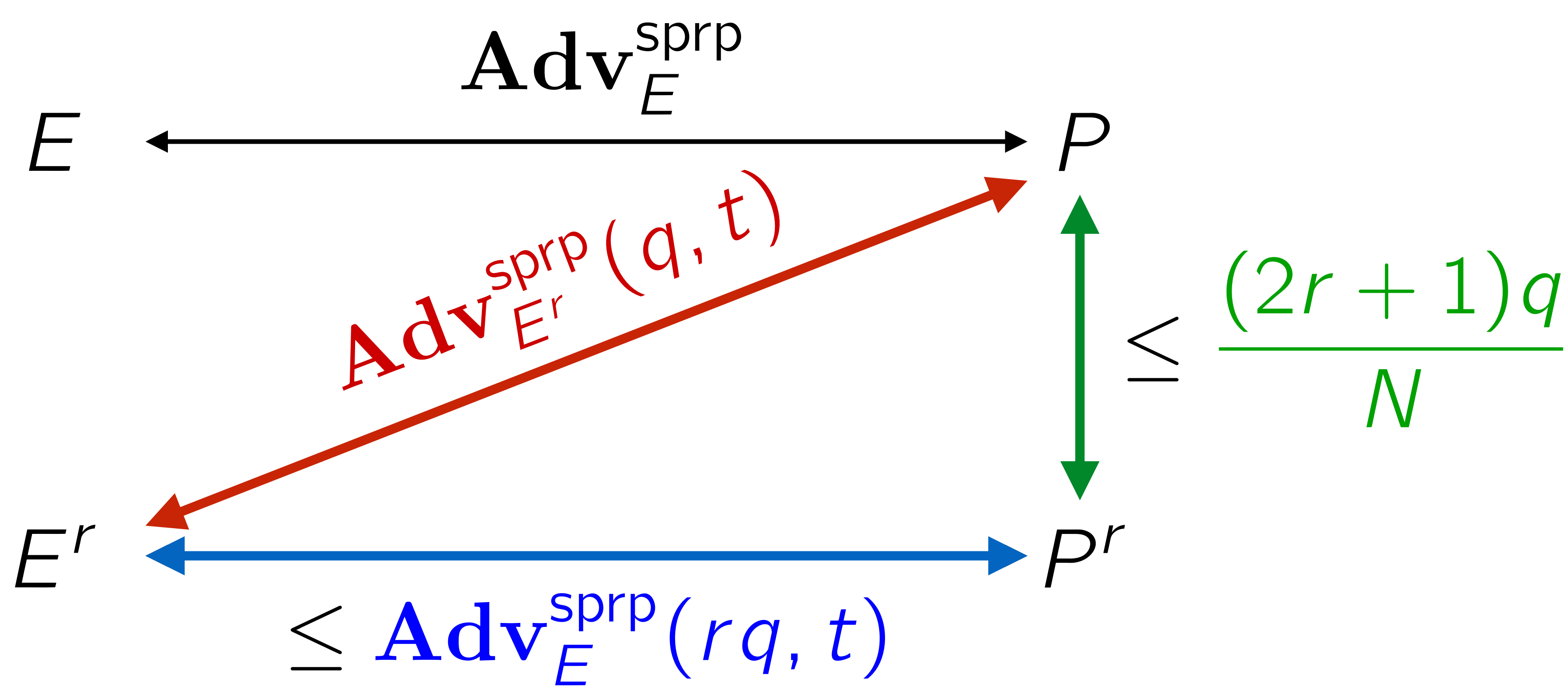
r : number of rounds

q : number of queries

Main result

Iterating a block cipher a *constant* number of times has a negligible effect on its SPRP security:

$$\mathbf{Adv}^{\mathsf{sprp}}_{E^r}(q,t) \le \mathbf{Adv}^{\mathsf{sprp}}_{E}(rq,t') + \frac{(2r+1)q}{N}$$



Iterated Random Permutation Problem

Iterated Random Permutation Problem:

Number of queries to distinguish P from P^r?

I.e. bound $\mathbf{Adv}_{P,P^r}(q)$.

This problem shows up in a few places [CLLSS14] [BAC12] [GJMN15].

This is really a problem about unlabeled permutations. I.e. only cycle structure matters.

Iterated Random Permutation Problem

Main theorem

$$\mathbf{Adv}_{P,P^r}(q) \leq \frac{(2r+1)q}{N}$$

$$\mathbf{Adv}_{P,P^r}(q) = \Theta\left(\frac{q}{N}\right)$$

E.g. for r = 2:

$$0.5\frac{q}{N} - \frac{2}{N} \leq \mathbf{Adv}_{P,P^2}(q) \leq 5\frac{q}{N}$$

Iterated permutations

Core result: $\mathbf{Adv}_{P,P^r}(q) \leq \dfrac{(2r+1)q}{N}$

$$
\begin{tikzcd}
G(\mathbf{P}) \arrow[d, leftrightarrow, "\mathbf{Adv} \leq \frac{q}{N}"'] & & G(\mathbf{P}^{\mathbf{r}}) \arrow[d, leftrightarrow, "\mathbf{Adv} \leq \frac{rq}{N}"] \\
G(\mathbf{C}) \arrow[rr, leftrightarrow, "\mathbf{Adv} \leq \frac{rq}{N}"] & & G(\mathbf{C}^{\mathbf{r}})
\end{tikzcd}
$$

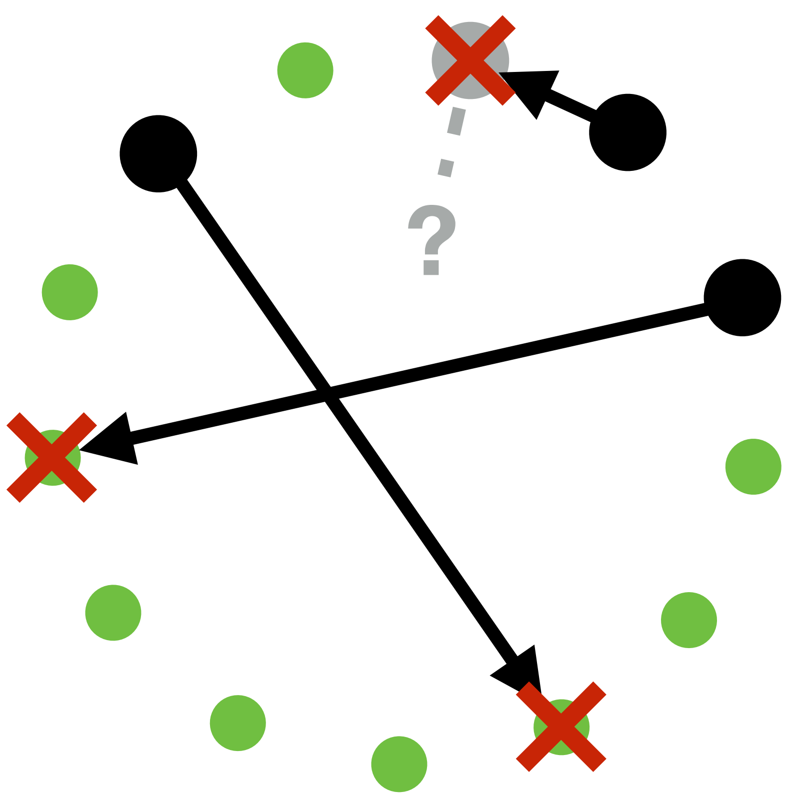
$G(\mathbf{P})$:	access to P, P^{-1}	for $P \leftarrow_{\$}$ *Permutations(N)*
$G(\mathbf{P}^{\mathbf{r}})$:	access to P^r, $(P^{-1})^r$	for $P \leftarrow_{\$}$ *Permutations(N)*
$G(\mathbf{C})$:	access to C, C^{-1}	for $C \leftarrow_{\$}$ *Cycles(N)*
$G(\mathbf{C}^{\mathbf{r}})$:	access to C^r, $(C^{-1})^r$	for $C \leftarrow_{\$}$ *Cycles(N)*

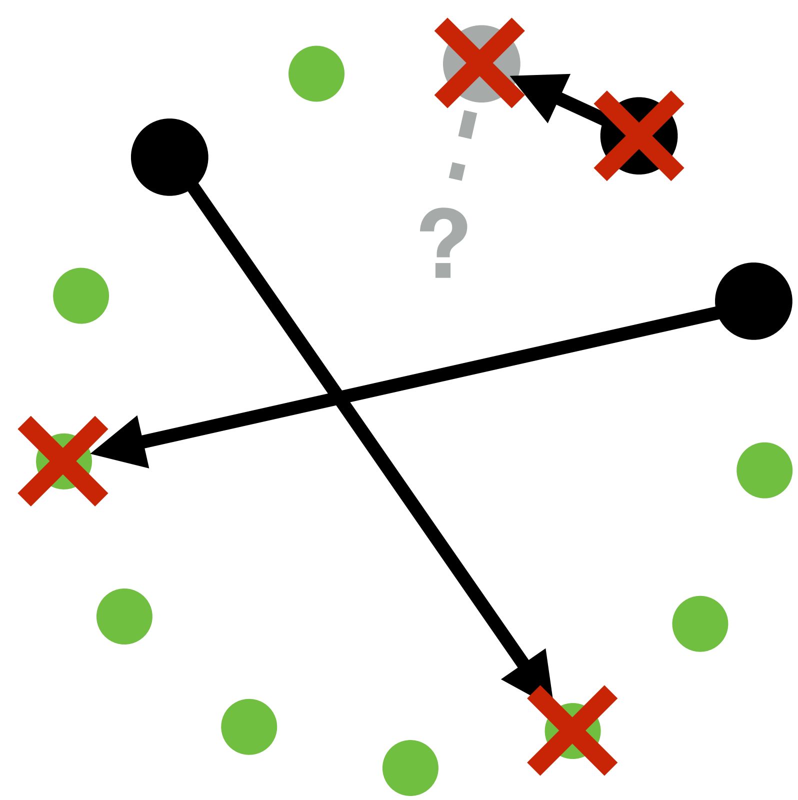
From P to C

G(P) ⟷ G(C) ⟷ G(C^r) ⟷ G(P^r)

$$\mathbf{Adv} \leq \frac{q}{N}$$

- Game G(P) ⇔ picking unif. random unpicked point
- Game G(C) ⇔ same + source point is forbidden





From C^r to P^r

$$G(P) \longleftrightarrow G(C) \longleftrightarrow G(C^r) \longleftrightarrow G(P^r)$$

$$\mathbf{Adv} \leq \frac{q}{N} \qquad\qquad \mathbf{Adv} \leq \frac{rq}{N}$$

Querying $G(P^r)$ ⇔ querying $G(P)$ along chain of length r

Querying $G(C^r)$ ⇔ querying $G(C)$ along chain of length r

Distinguisher between $G(P^r)$ and $G(C^r)$

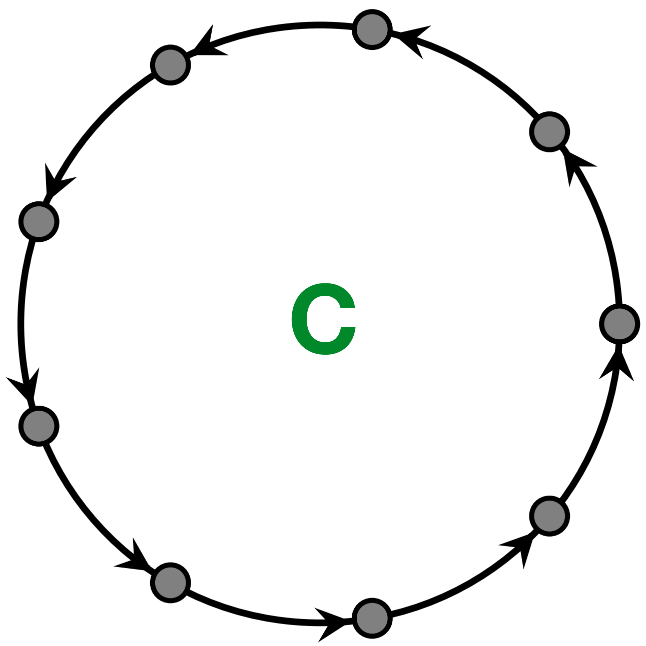
⇒ distinguisher between $G(P)$ and $G(C)$

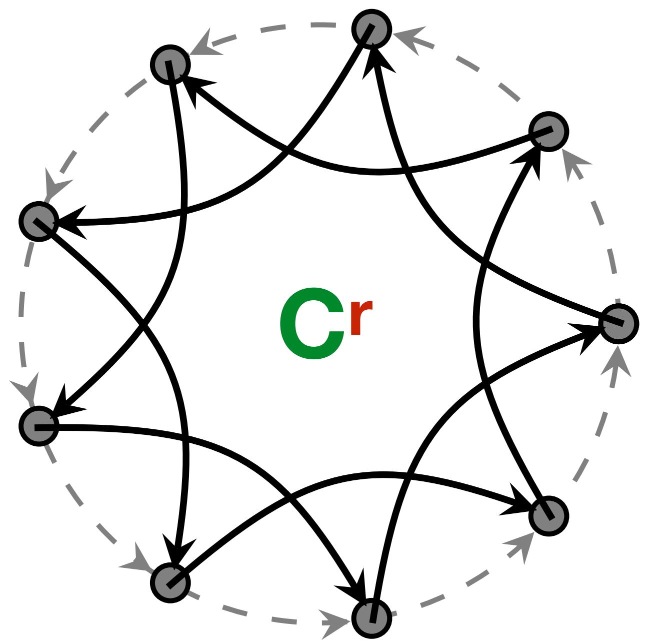
From C to C^r

$$G(P) \longleftrightarrow G(C) \longleftrightarrow G(C^r) \longleftrightarrow G(P^r)$$

$$\mathbf{Adv} \le \frac{q}{N} \qquad\qquad \mathbf{Adv} \le \frac{rq}{N}$$

If gcd(N,r) = 1, C^r still has a single cycle.



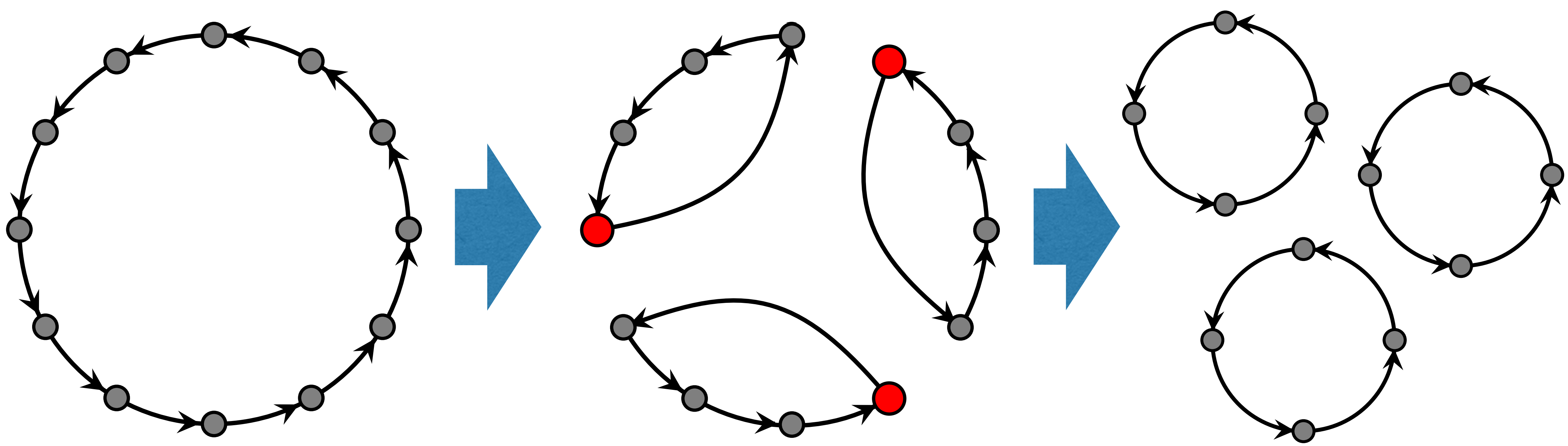


$\Rightarrow$ C $\longmapsto$ C^r is a permutation of *Perm*(N) $\Rightarrow$ $\mathbf{Adv}_{C,C^r} = 0$

From C to C^r

$$G(P) \underset{\mathbf{Adv} \le \frac{q}{N}}{\longleftrightarrow} G(C) \underset{\mathbf{Adv} \le \frac{rq}{N}}{\longleftrightarrow} G(C^r) \underset{\mathbf{Adv} \le \frac{rq}{N}}{\longleftrightarrow} G(P^r)$$

C **C^r**



1 cycle | redirect $d \le r$ points | $d = \gcd(N,r)$ cycles

Summing up

$$G(P) \xleftrightarrow[\mathbf{Adv} \leq \frac{q}{N}]{} G(C) \xleftrightarrow[\mathbf{Adv} \leq \frac{rq}{N}]{} G(C^r) \xleftrightarrow[\mathbf{Adv} \leq \frac{rq}{N}]{} G(P^r)$$

Conclusion: $\mathbf{Adv}_{P,P^r}(q) \leq \dfrac{(2r+1)q}{N}$

Matching Attack

Make q queries along a chain

- If there is a cycle $\to\to\cdots\to$: guess $\boldsymbol{P^r}$
- Otherwise $\to\to\to\cdots\to$: guess $\boldsymbol{P}$

$$\text{Advantage} \approx C(r)\frac{q}{N} \qquad \text{with } C(r) = \sum_{d|r} \frac{\phi(d)}{d} - 1 \geq \frac{1}{2}$$

$$\geq \frac{q}{2N}$$

Conclusion

- Upper bound on the iterated permutation problem

  + matching attack for constant r

  in the end: $\mathbf{Adv}_{P,P^r}(q) = \Theta\left(\frac{q}{N}\right)$

- Direct application to cascade encryption with the same key:

$$\mathbf{Adv}^{\mathsf{sprp}}_{E^r}(q,t) \leq \mathbf{Adv}^{\mathsf{sprp}}_{E}(rq,t') + \frac{(2r+1)q}{N}$$

- Open problem: security amplification under some hypotheses?

Conclusion

Thank you for your attention!

Questions ?