Attacks in the multi-user setting: Discrete logarithm, Even-Mansour and PRINCE

Pierre-Alain Fouque[1], Antoine Joux[2], Chrysanthi Mavromati[3]

[1] Université Rennes 1 and Institut Universitaire de France
[2] CryptoExperts and Chaire de Cryptologie de la Fondation de l'UPMC
[3] Sogeti/ESEC R&D Lab and UVSQ Laboratoire PRiSM

ASIACRYPT 2014

The multi-user setting

Cryptographers prove the security of their schemes in a single-user model.

In real world: There are many users, each with a different key, sending each other encrypted data.

Multi-user setting

Main ideas

- Graph of key relations
- New variant of memory-less collision attacks

Generic discrete logarithm

- Single-user discrete log: time $\sqrt{N}$ (generic group)

- Multi-user discrete log (L logs):
  - studied by Kuhn and Struik
  - use of the parallel version of the Pollard rho technique with distinguished points
  - time $\sqrt{NL}$, $L \leq N^{1/4}$

Distinguished points for discrete logarithms

- Define a random function $f : \mathcal{G} \to \mathcal{G}$

$$f(z) = \begin{cases} z^2 & \text{if } z \in \mathcal{G}_1, \\ gz & \text{if } z \in \mathcal{G}_2, \end{cases}$$

  where $\mathcal{G}_1 \cup \mathcal{G}_2 = \mathcal{G}$.
- Define a distinguished subset S_0
- Build chains from random startpoints: $y_{i+1} = f(y_i)$
- Stop chain when $y_\ell = d \in S_0$

$$g^{x_1} = y_1 \xrightarrow{f} y_2 \xrightarrow{f} y_3 \xrightarrow{f} y_4 \xrightarrow{f} \qquad log_g d = Ax_1 + B$$

$$d = d^{'}$$

$$g^{x_1^{'}} = y_1^{'} \xrightarrow{f} y_2^{'} \xrightarrow{f} y_3^{'} \xrightarrow{f} y_4^{'} \xrightarrow{f} \qquad log_g d^{'} = A^{'} x_1^{'} + B^{'}$$

New method

$$g^{x^{(0)}} = Y_0 \xrightarrow{f} \cdots \xrightarrow{f} \cdots$$

$$g^{x^{(1)}} = Y_1 \xrightarrow{f} \cdots \xrightarrow{f} \cdots$$

$$\xrightarrow{f} \cdots \xrightarrow{f}$$

$$\vdots$$

$$\xrightarrow{f} \cdots \xrightarrow{f}$$

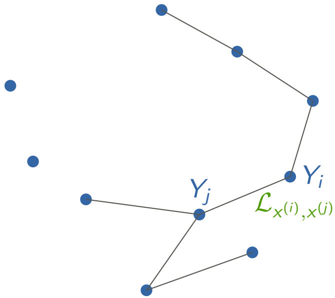
linear relation between $x^{(i)}$ and $x^{(j)}$

$$g^{x^{(L-1)}} = Y_{L-1} \xrightarrow{f} \cdots \xrightarrow{f} \cdots$$

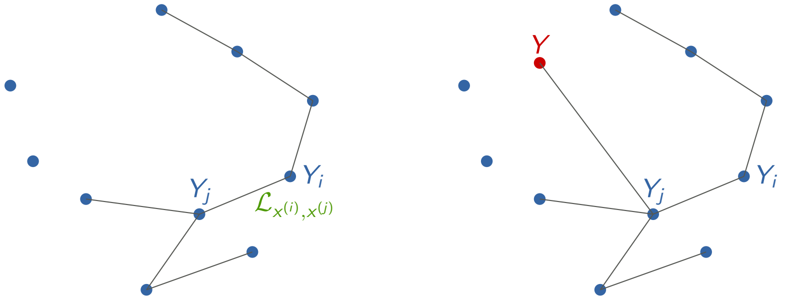
Average length of chains: $\sqrt{N/L}$

Expected number of collisions: $\mathbb{E}[\mathrm{Coll}] = \frac{(L\sqrt{N/|S_0|})^2}{N} = L$

New method - Construct the graph

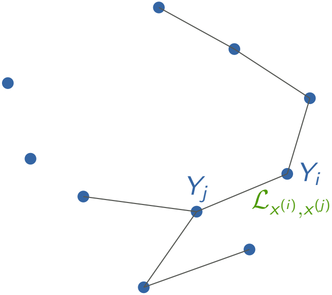


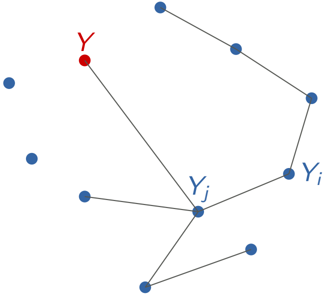
New method - Construct the graph



$\rightarrow$ learn all keys in
connected component

New method - Construct the graph





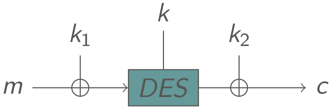
$\rightarrow$ learn all keys in connected component

Overall complexity of the attack: $\sqrt{NL}$

Description of Even-Mansour

Introduced by Even and Mansour at [Asiacrypt '91].

- Motivated by the DESX construction [Rivest, 1984]

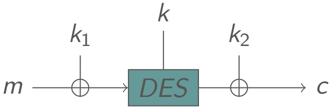


DES key k, whitening keys k_1, k_2

Description of Even-Mansour

Introduced by Even and Mansour at [Asiacrypt '91].

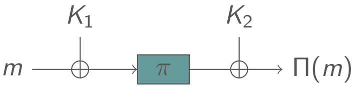
- Motivated by the DESX construction [Rivest, 1984]



DES key k, whitening keys k_1, k_2

- Minimal construction of a blockcipher

$$\Pi_{K_1,K_2}(m) = \pi(m \oplus K_1) \oplus K_2$$



- Keyed permutation family Π_{K_1,K_2}
- π is a public permutation on n-bit values ($N = 2^n$)
- Two whitening keys K_1, K_2 of n-bits

Known results in the single-user model

Main result: Any attack with D queries to Π and T off-line computation (queries to the public permutation π) has an upper bound of $O(DT/2^n)$ on probability of success.

Single-Key EM: Proved secure with the same bound [Dunkelman *et al.*]

Slide attacks and variants - Two key case

[Dunkelman *et al.*, 2012]

Define $F(P) = \Pi(P) \oplus \Pi(P \oplus \delta)$
$f(P) = \pi(P) \oplus \pi(P \oplus \delta)$

Fix $\delta \in \{0,1\}^n$: Assume $(P, P^{'})$ satisfy $P \oplus P^{'} = K_1$ (slid pair)

Slide attacks and variants - Two key case

[Dunkelman *et al.*, 2012]

$$\text{Define } F(P) = \Pi(P) \oplus \Pi(P \oplus \delta)$$
$$f(P) = \pi(P) \oplus \pi(P \oplus \delta)$$

Fix $\delta \in \{0,1\}^n$: Assume $(P, P^{'})$ satisfy $P \oplus P^{'} = K_1$ (slid pair)

Then,

$$\begin{aligned} F(P^{'}) &= \Pi(P^{'}) \oplus \Pi(P^{'} \oplus \delta) \\ &= \pi(P^{'} \oplus K_1) \oplus \cancel{K_2} \oplus \pi(P^{'} \oplus \delta \oplus K_1) \oplus \cancel{K_2} \\ &= \pi(P) \oplus \pi(P \oplus \delta) = f(P) \end{aligned}$$

So, if $F(P^{'})$ and $f(P)$ collide then:

$P \oplus P^{'}$ is a good key candidate.

Slide attacks and variants - Two key case

[Dunkelman *et al.*, 2012]

Define $F(P) = \Pi(P) \oplus \Pi(P \oplus \delta)$
$f(P) = \pi(P) \oplus \pi(P \oplus \delta)$

Fix $\delta \in \{0,1\}^n$: Assume $(P, P^{'})$ satisfy $P \oplus P^{'} = K_1$ (slid pair)

Then,

$$\begin{aligned} F(P^{'}) &= \Pi(P^{'}) \oplus \Pi(P^{'} \oplus \delta) \\ &= \pi(P^{'} \oplus K_1) \oplus \cancel{K_2} \oplus \pi(P^{'} \oplus \delta \oplus K_1) \oplus \cancel{K_2} \\ &= \pi(P) \oplus \pi(P \oplus \delta) = f(P) \end{aligned}$$

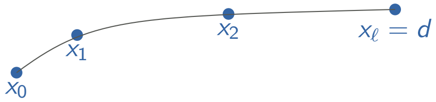
So, if $F(P^{'})$ and $f(P)$ collide then:

$P \oplus P^{'}$ is a good key candidate.

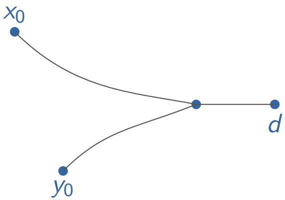
Note that if $P \oplus P^{'} = K_1 \oplus \delta$ yields the same property then $P \oplus P^{'} \oplus \delta$ is also a key candidate.

Finding collisions: the distinguished points technique

- Define a function f on a set S of size N.
- Define a distinguished subset S_0 of S
- Build chains from random startpoints: $x_{i+1} = f(x_i)$
- Stop chain when $x_\ell = d \in S_0$
- Store (x_0, d, ℓ)

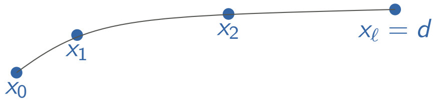


Two paired chains

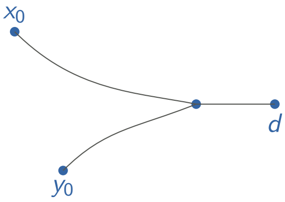


Finding collisions: the distinguished points technique

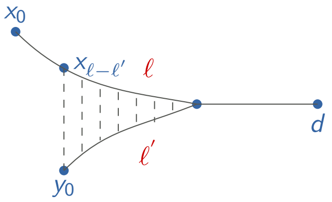
- Define a function f on a set S of size N.
- Define a distinguished subset S_0 of S
- Build chains from random startpoints: $x_{i+1} = f(x_i)$
- Stop chain when $x_\ell = d \in S_0$
- Store (x_0, d, ℓ)



Two paired chains



How do we recover a collision?



Application on Even-Mansour - First trial

Goal: Find a collision between a set of chains using the public permutation π and a chain obtained from the keyed permutation Π

Define $F(P) = \Pi(P) \oplus \Pi(P \oplus \delta)$ and $f(P) = \pi(P) \oplus \pi(P \oplus \delta)$

$\rightarrow$ These chains can cross but not merge

Application on Even-Mansour - First trial

Goal: Find a collision between a set of chains using the public permutation π and a chain obtained from the keyed permutation Π

Define $F(P) = \Pi(P) \oplus \Pi(P \oplus \delta)$ and $f(P) = \pi(P) \oplus \pi(P \oplus \delta)$

$\rightarrow$ These chains can cross but not merge

Another option: use a function that mixes calls to Π and $\pi \Rightarrow$ adaptive attack

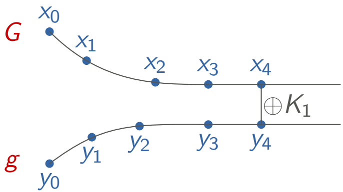
Application on Even-Mansour - New idea

Define new functions:

$$G(P) = P \oplus \Pi(P) \oplus \Pi(P \oplus \delta) = P \oplus F(P) \text{ and}$$
$$g(P) = P \oplus \pi(P) \oplus \pi(P \oplus \delta) = P \oplus f(P)$$

- Assume that two plaintexts $(P, P^{'})$ satisfy: $P^{'} = P \oplus K_1$ or $P^{'} = P \oplus K_1 \oplus \delta$
- Then $G(P^{'}) = g(P) \oplus K_1 (\text{resp.} \ \oplus \delta)$

$\rightarrow$ These chains can become parallel



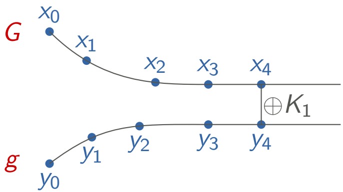
Application on Even-Mansour - New idea

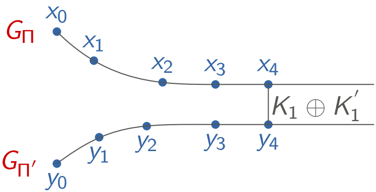
Define new functions:

$$G(P) = P \oplus \Pi(P) \oplus \Pi(P \oplus \delta) = P \oplus F(P) \text{ and}$$
$$g(P) = P \oplus \pi(P) \oplus \pi(P \oplus \delta) = P \oplus f(P)$$

- Assume that two plaintexts $(P, P^{'})$ satisfy: $P^{'} = P \oplus K_1$ or $P^{'} = P \oplus K_1 \oplus \delta$
- Then $G(P^{'}) = g(P) \oplus K_1(\text{resp. } \oplus \delta)$

$\rightarrow$ These chains can become parallel





Detection of parallel chains with distinguished points

- For g chains: P is a distinguished point if $f(P) \in S_0$
- For G chains: $P^{'}$ is a distinguished point if $F(P^{'}) \in S_0$

Detection of parallel chains with distinguished points

- For g chains: P is a distinguished point if $f(P) \in S_0$
- For G chains: $P^{'}$ is a distinguished point if $F(P^{'}) \in S_0$
- If $P^{'} = P \oplus K_1$ and P is a distinguished point in the g chain, then:

$$\begin{aligned} F(P^{'}) = \Pi(P^{'}) \oplus \Pi(P^{'} \oplus \delta) &= \pi(P^{'} \oplus K_1) \oplus \cancel{K_2} \oplus \pi(P^{'} \oplus K_1 \oplus \delta) \oplus \cancel{K_2} \\ &= \pi(P) \oplus \pi(P \oplus \delta) = f(P) \end{aligned}$$

(then $P^{'}$ is a distinguished point in the G chain)

Detection of parallel chains with distinguished points

- For g chains: P is a distinguished point if $f(P) \in S_0$
- For G chains: $P^{'}$ is a distinguished point if $F(P^{'}) \in S_0$
- If $P^{'} = P \oplus K_1$ and P is a distinguished point in the g chain, then:

$$\begin{aligned} F(P^{'}) = \Pi(P^{'}) \oplus \Pi(P^{'} \oplus \delta) &= \pi(P^{'} \oplus K_1) \oplus \cancel{K_2} \oplus \pi(P^{'} \oplus K_1 \oplus \delta) \oplus \cancel{K_2} \\ &= \pi(P) \oplus \pi(P \oplus \delta) = f(P) \end{aligned}$$

(then $P^{'}$ is a distinguished point in the G chain)

Detection of parallel chains: for $(P, P^{'})$ distinguished points, test if $F(P^{'}) = f(P)$

New attack on Even-Mansour

- Build chains from $g(P) = P \oplus \pi(P) \oplus \pi(P \oplus \delta) = P \oplus f(P)$
  - Stop if $f(P)$ arrives at a distinguished point
- Build chains from $G(P^{'}) = P^{'} \oplus \Pi(P^{'}) \oplus \Pi(P^{'} \oplus \delta) = P^{'} \oplus F(P^{'})$
  - Stop if $F(P^{'})$ arrives at a distinguished point
- If $F(P^{'}) = f(P)$
  - Then $G(P^{'}) = g(P) \oplus K_1$ (parallel chains)
  - We have a good candidate for K_1

We only need to store endpoints (don't have to recompute chains)

Attack Even-Mansour in the multi-user setting

1. Use of second idea
   - Build chains from g of length ℓ
   - Build chains from G of length ℓ for each user
   - Find parallel chains
2. Use of first idea
   - Construct a graph:
     - Nodes are labelled by the users and the unkeyed user
     - If $G^{(i)} = G^{(j)}$ (for users $(i), (j)$), then add a vertex between the two nodes
     - $K_1^{(i)} \oplus K_1^{(j)} (\oplus \delta)$
     - If we find a single collision between a user and the unkeyed user, then we learn all keys (in the connected component)

Analysis of the attack:

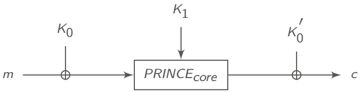
For $2^{n/3}$ users, $2^{n/3}$ queries/user, $2^{n/3}$ unkeyed queries
$\rightarrow$ recover a constant fraction of $2^{n/3}$ keys

Description of PRINCE

PRINCE [Borghoff *et al.*, Asiacrypt 2012]

- 64-bit lightweight block cipher
- 128-bit key k split into equal parts: $k = k_0 \| k_1$
- extension to 192 bit: $k = (k_0 \| k_1) \to (k_0 \| k_0^{'} \| k_1)$
- $k_0^{'}$ derived from k_0 by using the linear function L': $L'(k_0) = (k_0 \ggg 1) \oplus (k_0 \gg 63)$
- α-reflection property

$$\forall (k_0 \| k_0^{'} \| k_1),\ D_{(k_0 \| k_0^{'} \| k_1)}(\cdot) = E_{(k_0^{'} \| k_0 \| k_1 \oplus \alpha)}(\cdot)$$



$$E_k(m) = k_0^{'} \oplus Pcore_{k_1}(m \oplus k_0)$$

Attacks on PRINCE in the single and multi-user setting

Attack in the multi-user setting

Total cost 2^{65} **operations for deducing** k_0 **and** k_1 of 2 users in a set of 2^{32}.

Attack in the single-user setting

$$T_{off} = 2^{96}, T_{on} = 2^{32}, D = 2^{32}$$

$$\mathbf{DT_{off}} = 2^{128}$$
$$\mathbf{DT_{on}} = 2^{64}$$

Conclusion

- Propose two new algorithmic ideas to improve collision based attacks
- Application of the first idea to solve the discrete logarithm problem in the multi-user setting
- Application of both ideas to the Even-Mansour scheme
- Propose two new attacks for PRINCE
  - The attacks were applied to DESX with some differences

Conclusion

- Propose two new algorithmic ideas to improve collision based attacks
- Application of the first idea to solve the discrete logarithm problem in the multi-user setting
- Application of both ideas to the Even-Mansour scheme
- Propose two new attacks for PRINCE
  - The attacks were applied to DESX with some differences

Thank you for your attention!