Iterated Even-Mansour Schemes with Involutions

Itai Dinur[1], Orr Dunkelman[2,4], Nathan Keller[3] and Adi Shamir[4]

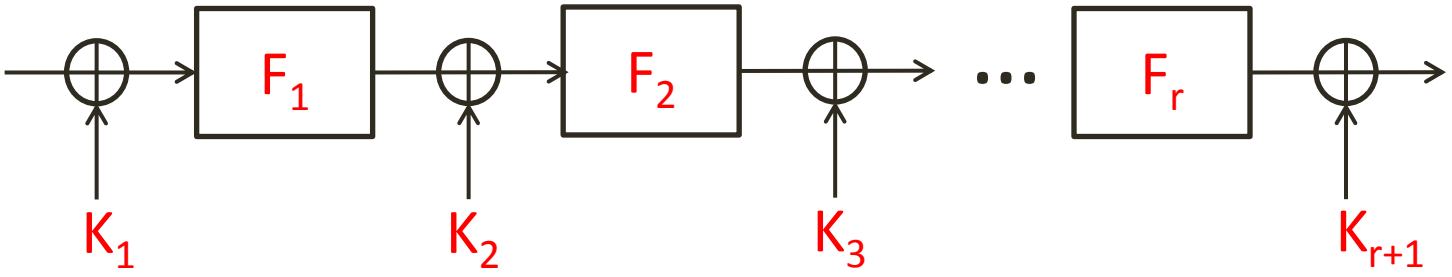
[1]École normale supérieure, France

[2]University of Haifa, Israel

[3]Bar-Ilan University, Israel

[4]The Weizmann Institute, Israel

The Iterated EM Scheme

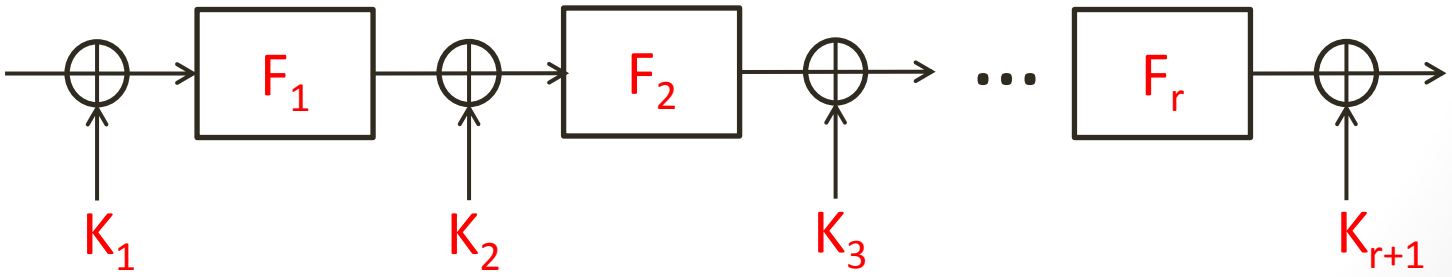


- EM-based schemes are a **very hot** research area
- There are many possible **key schedules**

Involutions

- In practice the permutations F_i can be constructed using a block cipher without the **key schedule**
- Many of these constructions have the property that they are **equal to their inverses**

- A permutation F is called an **involution** if $F=F^{-1}$

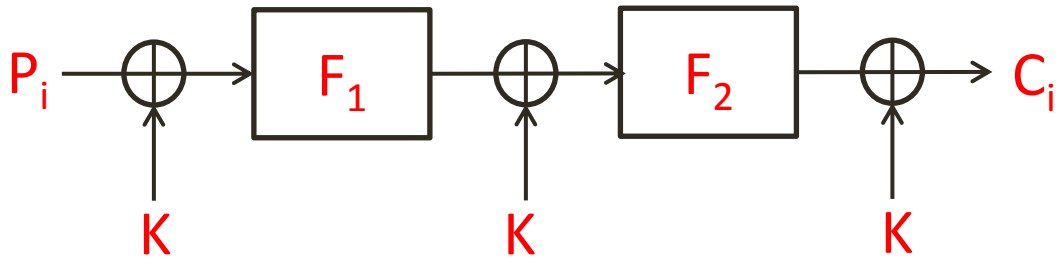


Fixed Points of Involutions

- A **random** involution has an expected number of $2^{n/2}$ **fixed-points**
- $x=F(x) \rightarrow F'(x)=x+F(x)=0 \rightarrow$ the 0 output value in $F'(x)$ has an expected number of $2^{n/2}$ preimages
- When F is a random **permutation** the number of preimages of the **most likely** output is $O(n) << 2^{n/2}$

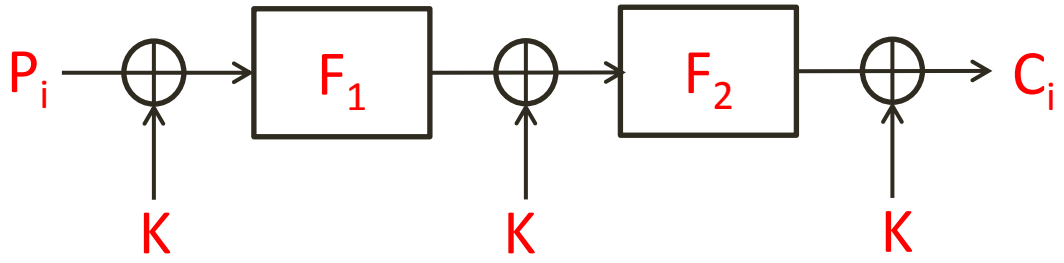
Applications to Iterated EM

- A 2-round iterated EM scheme with 1 key can be attacked in $T \approx 2^n/t$ [DDKS'13]
  - t is the number of **preimages** of the **most likely** output of $F'(x)=x+F(x)$
- When F_1 and F_2 are random permutations $T \approx 2^n/n$



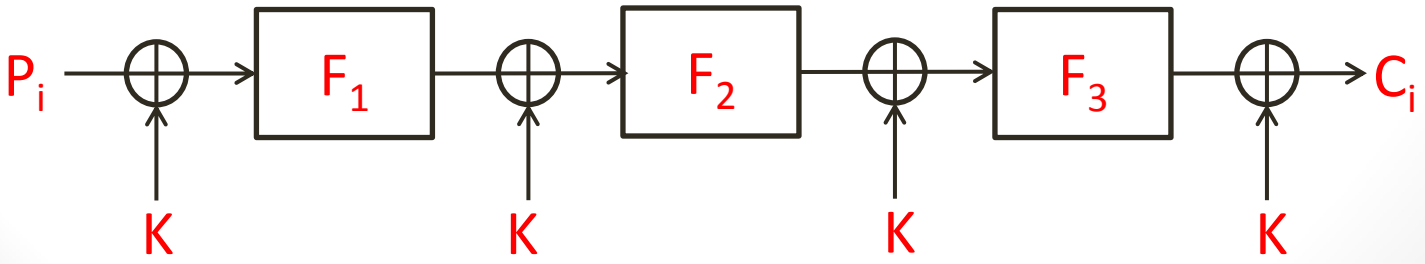
Applications to Iterated EM

- A 2-round iterated EM scheme with 1 key can be attacked in $T \approx 2^n/t$ [DDKS'13]
  - t is the number of **preimages** of the **most likely** output of $F'(x)=x+F(x)$
- When F_1 and F_2 are random permutations $T \approx 2^n/n$
- When F_1 (or F_2) is a **random involution** $T \approx 2^{n/2}$
  - The memory and data complexities are also significantly reduced



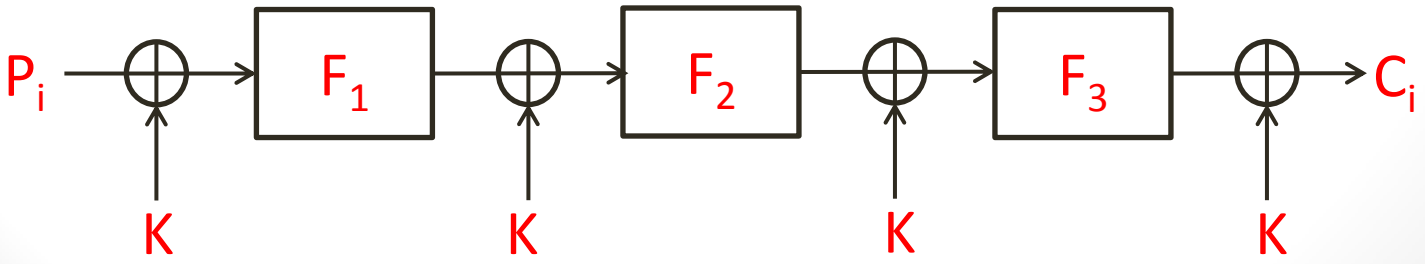
Applications to Iterated EM

- A 3-round iterated EM scheme with 1 key can be attacked in $T \approx 2^n/\sqrt{t}$ [DDKS'13]
- When all permutations are random $T \approx 2^n/\sqrt{n}$



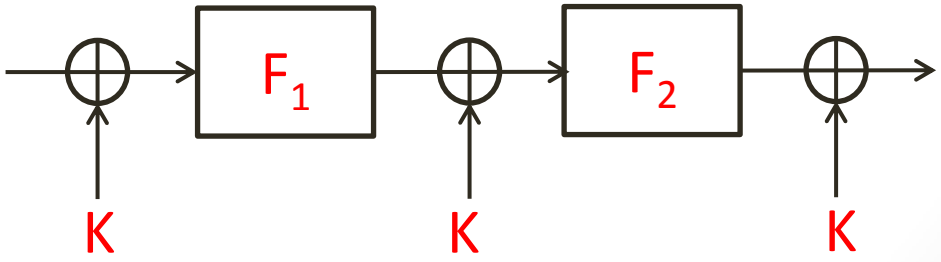
Applications to Iterated EM

- A 3-round iterated EM scheme with 1 key can be attacked in $T \approx 2^n/\sqrt{t}$ [DDKS'13]
- When all permutations are random $T \approx 2^n/\sqrt{n}$
- When F_1 (or F_2 or F_3) is a **random involution** $T \approx 2^{3n/4}$
  - The memory and data complexities are also significantly reduced



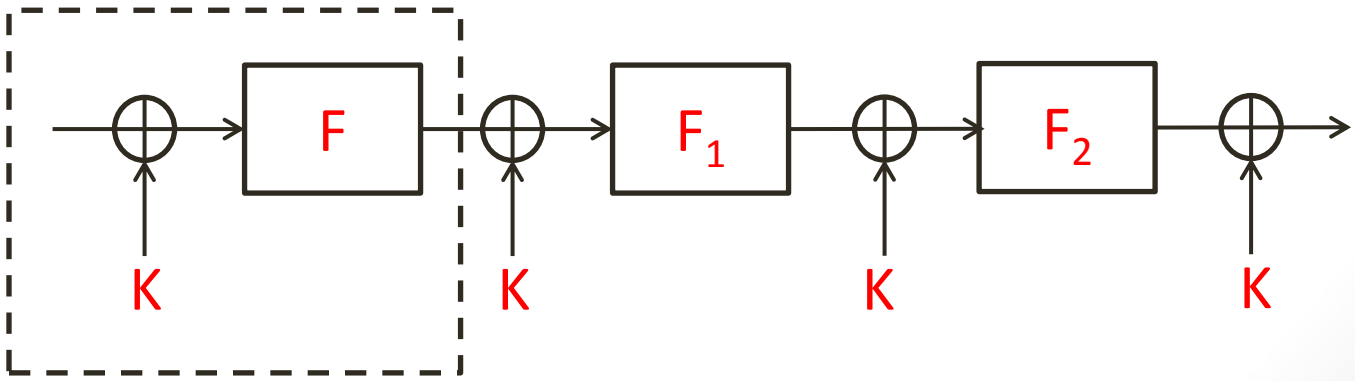
A Surprising Application

- A 2-round iterated EM scheme with 1 key with **random permutations** can be attacked in $T \approx 2^n/n$



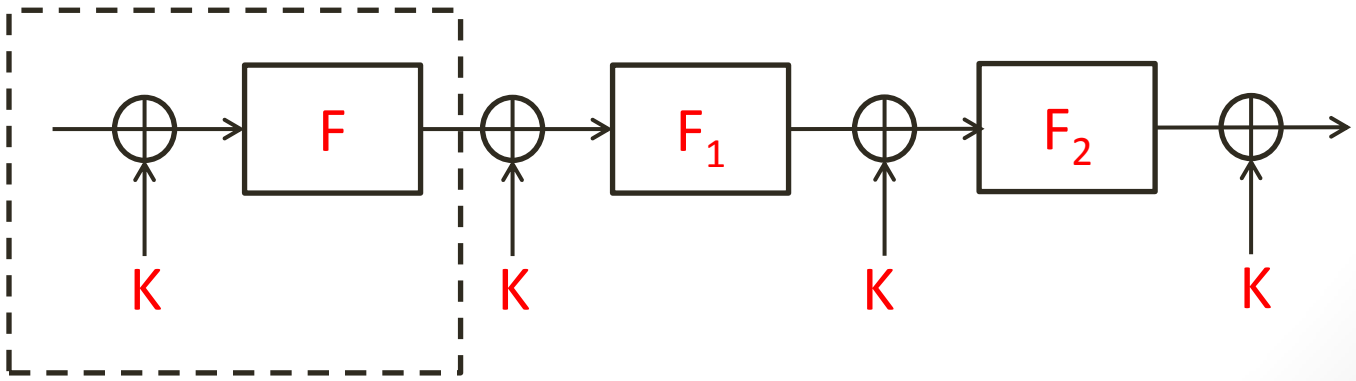
A Surprising Application

- A 2-round iterated EM scheme with 1 key with **random permutations** can be attacked in $T \approx 2^n/n$
- Add an **arbitrary involutional round** (unrelated to the original permutations)



A Surprising Application

- A 2-round iterated EM scheme with 1 key with **random permutations** can be attacked in $T \approx 2^n/n$
- Add an **arbitrary involutional round** (unrelated to the original permutations)
- This **significantly reduces** the security to $T \approx 2^{3n/4}$!!
  - Also significantly reduces the data and memory complexities of the attack



Thank you for your attention!