An Improved Attack on 4-Round Even-Mansour with 2 Alternating Keys

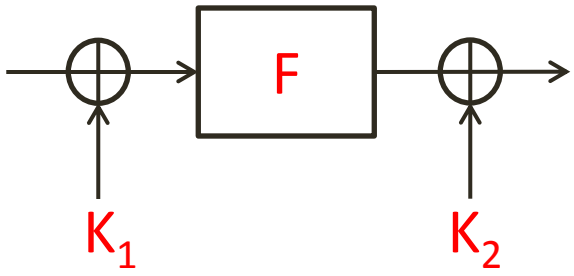
Itai Dinur[1], Orr Dunkelman[1,2], Nathan Keller[3] and Adi Shamir[1]

[1]The Weizmann Institute, Israel

[2]University of Haifa, Israel

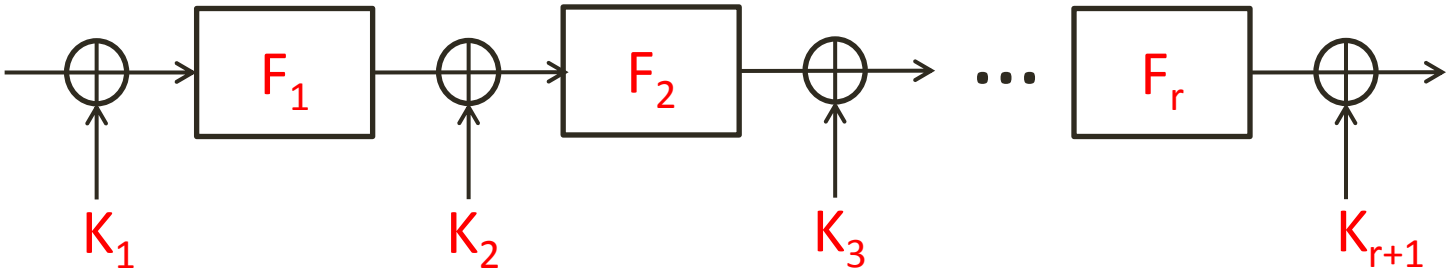
[3]Bar-Ilan University, Israel

The Even-Mansour Scheme (1991)



- Security: $TD=2^n$ using the **slidex** attack (Dunkelman, Keller and Shamir Eurocrypt '12)

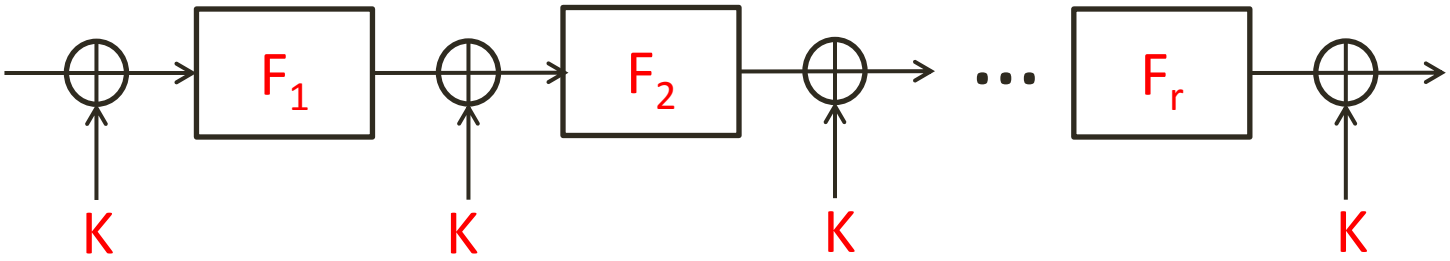
The Iterated EM Scheme



- There are many possible key schedules

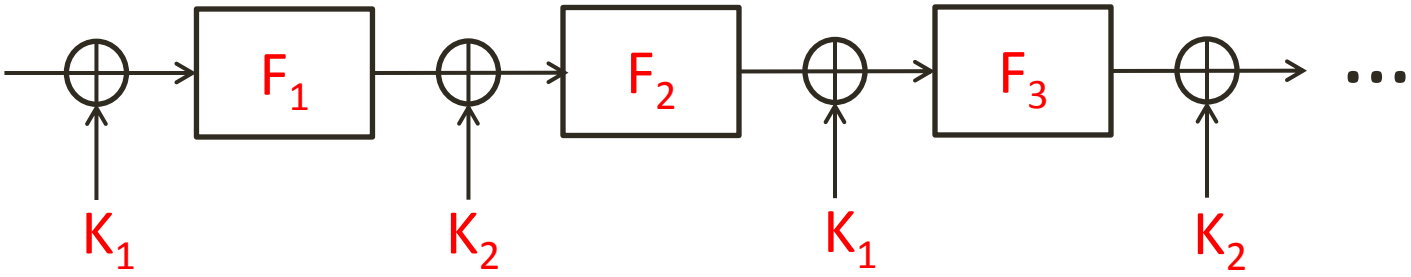
The Iterated EM Scheme

- The simplest key schedule uses only one key
- Concrete constructions: **LED-64**, **Zorro**



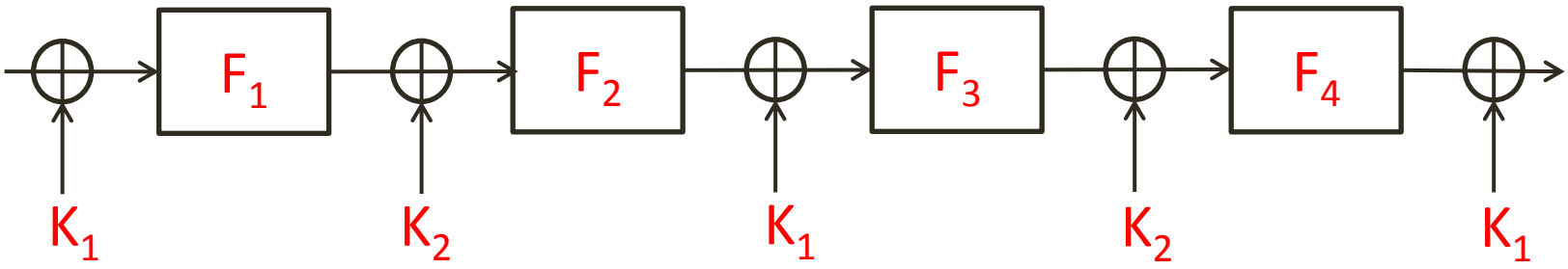
EM with 2 Alternating Keys

- We concentrate on the construction in which K_1 and K_2 alternate
- Concrete construction: **LED-128** (12 steps)



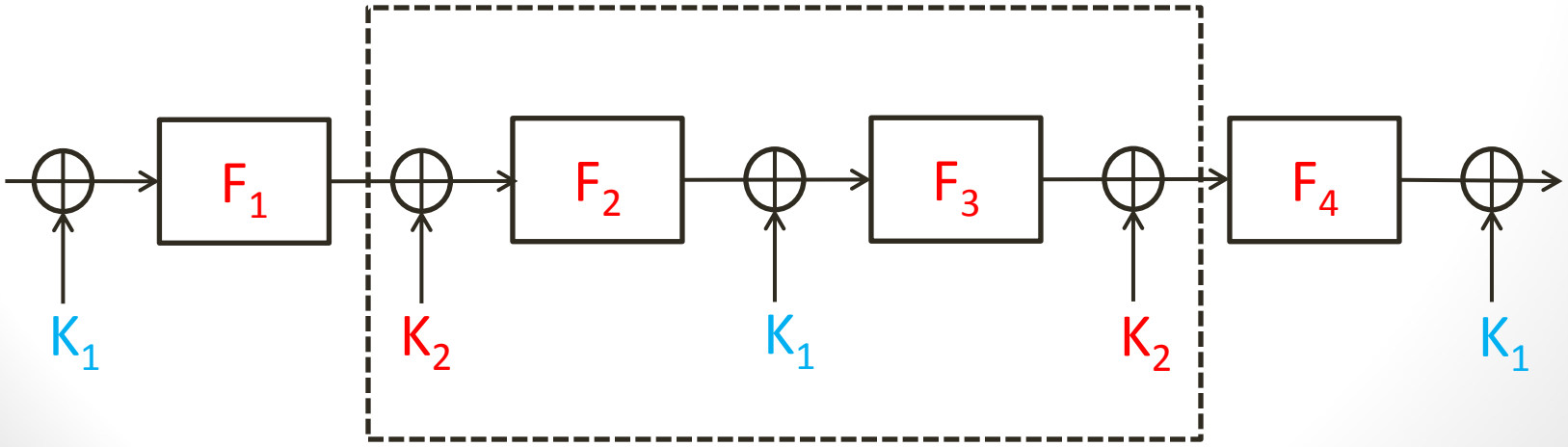
4-Round EM with 2 Alternating Keys

- The best known previous attack on 4 rounds was presented at FSE ‘13 by Nikolic, Wang and Wu



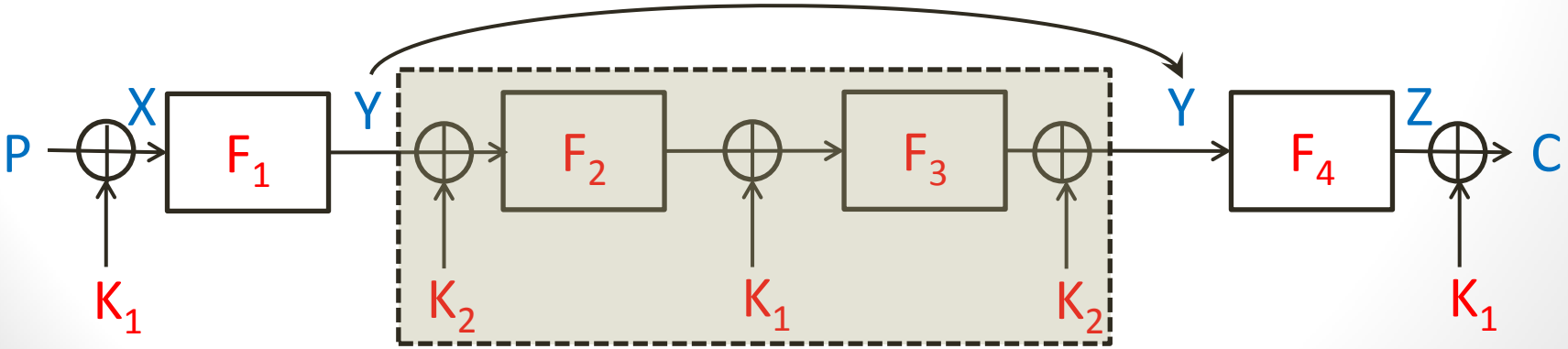
The Previous Attack [NWW13]

- For each value of K_1
  - Partially encrypt the plaintexts through F_1 and partially decrypt the ciphertexts through F_4
  - Apply the **slidex** attack to the remaining EM scheme
- Total time complexity $T=2^n \cdot 2^n/D=2^{2n}/D$
- However $T \geq 2^{1.5n}$



Our New Attack

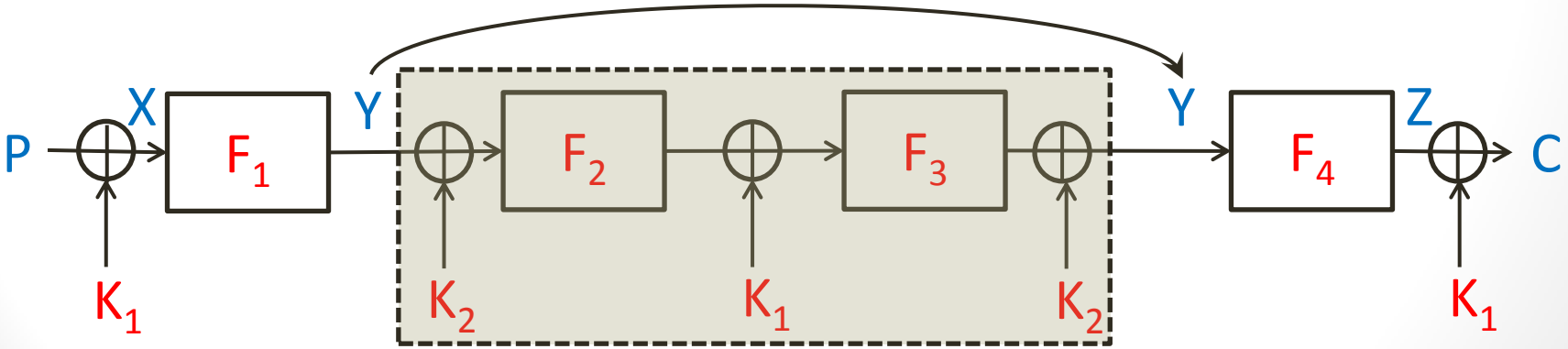
- Assume that we are given the full $D=2^n$ codebook
- With high probability a **magic fixed point** Y->Y occurs for **some magic** (P,C) pair
- For each value of Y
  - Calculate X and Z
  - Since X+Z=P+C, search for this specific (P,C), calculate a suggestion for K_1=P+X and store the quartet K_1,Y,(P,C)



Our New Attack

- We fill a table of size $D=2^n$ in 2^n time

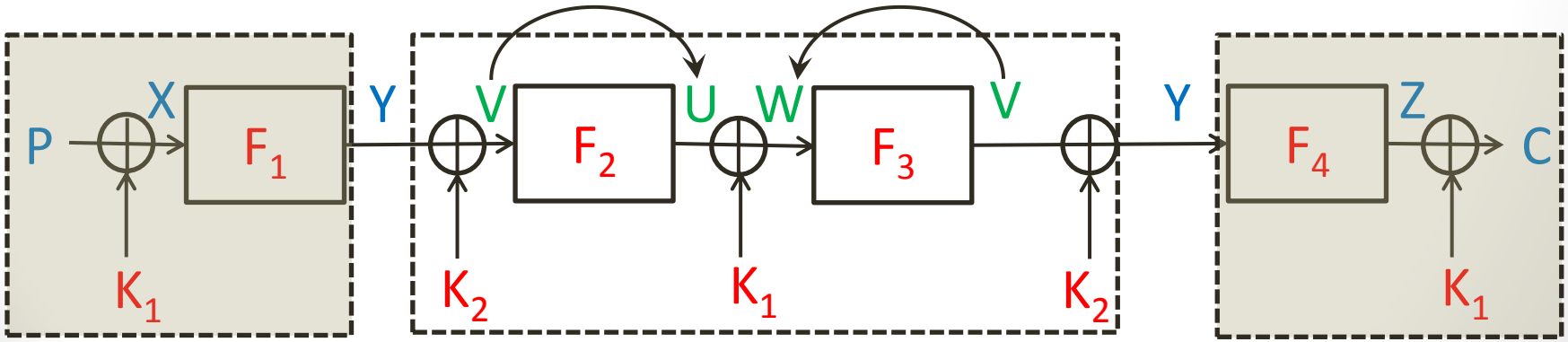
K_1	Y	P,C
⋮	⋮	⋮



Our New Attack

- Independently, for each value of V:
  - Calculate U and W
  - Obtain a suggestion for K_1=U+W
  - Search for K_1 in the table and obtain Y
  - Calculate a suggestion for K_2=Y+V
  - Test the key (K_1,K_2)

K_1	Y	P,C
⋮	⋮	⋮



Our New Attack

- The time complexity is 2^n given $D=2^n$ data
- For $D<2^n$, repeat the attack for $2^n/D$ **magic transitions** $Y \to Y+\Delta$, defined by $2^n/D$ values of the **magical** Δ (generalizing the fixed point where $\Delta=0$)
  - A similar idea was used in the **slidex** attack on 1-round EM to obtain the full tradeoff curve of $TD=2^n$
- Total time complexity is $2^{2n}/D$ for **all** $T \geq 2^n$ (not just $T \geq 2^{1.5n}$)
  - The total memory complexity is D
- The security of the scheme is actually 2^n !
  - The security of 4-step **LED-128** is reduced from 2^{96} to only 2^{64}

Thank you for your attention!