Recovering the S-boxes of 24-Round Reduced GOST
(or How to Combine the Cycle Structure with Slide Attacks)

Eli Biham, Orr Dunkelman, Nathan Keller

Computer Science Dept. Technion, Israel
Computer Science Dept. Technion, Israel
Einstein Institute of Mathematics, Hebrew University, Israel

Topics of the Talk

- Short Description of Slide Attacks
- New idea: studying the cycle structure
- Attacking 24-round GOST with unknown S-boxes
- Attacking 30-round GOST with known S-boxes

Slide Attacks [BW99]

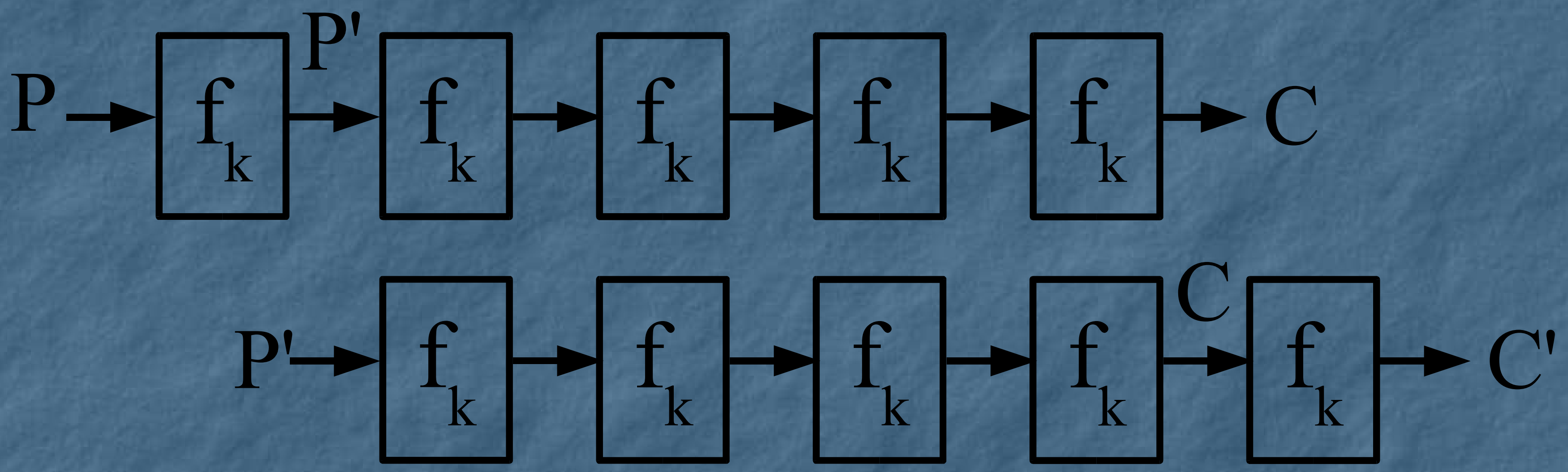
- Applied to ciphers with the same applied keyed permutation

$$\rightarrow \boxed{f_k} \rightarrow \boxed{f_k} \rightarrow \boxed{f_k} \rightarrow \boxed{f_k} \rightarrow$$

Slide Attacks

- **Seeks slid pairs (P,P') s.t.**

$$f_k(P) = P' \Rightarrow f_k(C) = C'$$



Slide Attacks

- If f_k is "simple" enough, given one slid pair the key k can be found

- The attack is independent of the number of times f_k is applied

Genreating Slid Pairs

- Using birthday paradox (requires $\sim 2^{n/2}$ KP)
- Identification can be done by treating <u>each</u> pair as a slid pair and analyzing it

- For Feistel block ciphers it can be reduced to $\sim 2^{n/4}$ CP
- Identification is also easier

Making Simple More Complex

- In [BW00] some advanced slide techniques were presented
- Most interesting property observed:
  - If (P,P') is a slid pair, then so does (E_k(P),E_k(P'))

Allowing More Complex "Simple" Functions

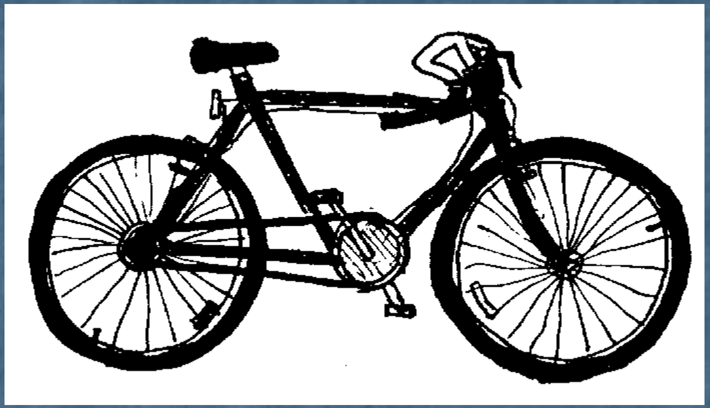
- [BW00,F01]: It is possible to use the observation to attack f_k using a KP attack (that uses *m* KP)
- Take ~$2^{n/2}$ KP, and iteratively encrypt each of them *m* times
- Try all pairs among the $2^{n/2}$ starting points
- Apply the KP attack with *m* pairs for each candidate slid pair (T.C. = $m2^n$)

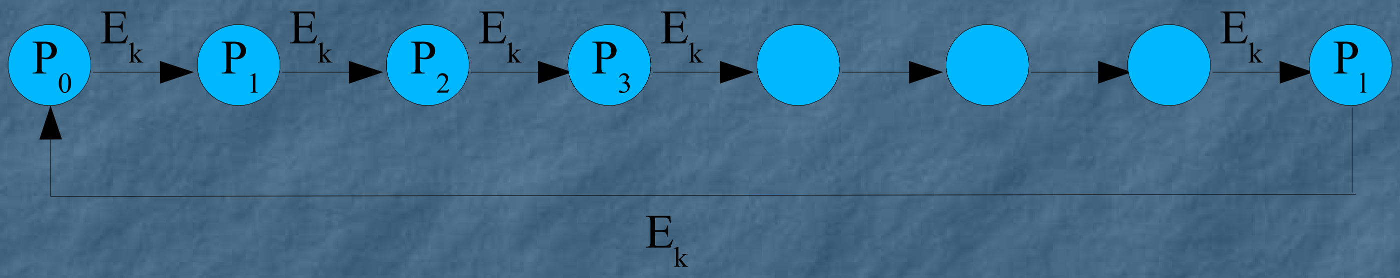
Making the Complex - Real

- Our technique solves two problems:
  - Finding the slid pairs easily
  - Allowing chosen plaintext attacks (even ACPC)
- How?

Making the Complex Become Real – Considering Cycles

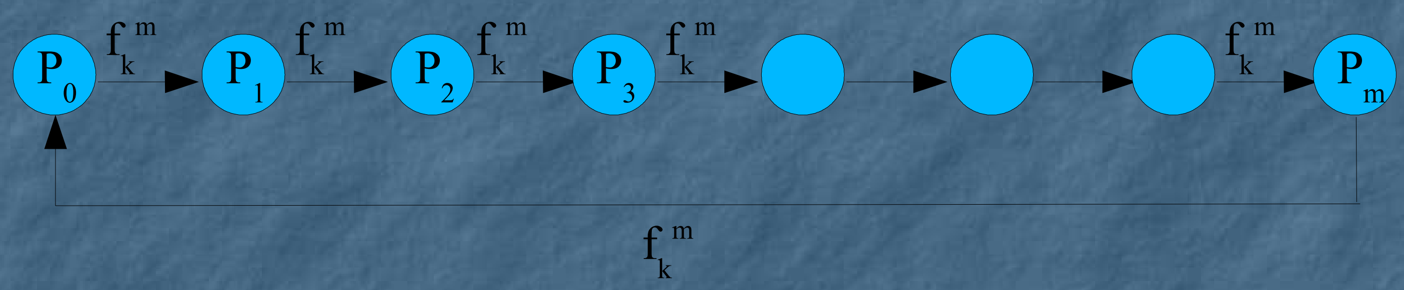
- Let $E_K(P) = f_K^{\,m}(P)$
- Choose P_0 randomly
- Iteratively encrypt P_0 until P_0 is obtained again





Making the Complex Become Real – Considering Cycles

- The cycle is actually also a multiple of the cycle of f_k as well!
- Let *Cycle-*E_k = l, *Cycle-*f_k = r
- Then $l*m = C*r$ for some constant C
- if $gcd(m,r)=1$, then $r=l$



So You Have Cycles... So What?!

- The information on the cycle can be used to find slid pairs
- Once one slid pair is found, we can find as many pairs as there plaintexts in the cycle
- We can use CP attacks (and even ACPC attacks) on f_k

GOST

- Russian encryption standard
- 32-round Feistel construction
- 64-bit block, 256-bit key
- Round function consists of key addition, eight 4x4 S-boxes, rotate to the left by 11
- S-boxes are unknown...

GOST

- **Simple key schedule:**
  - **rounds 1-8:** $k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8$
  - **rounds 9-16:** $k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8$
  - **rounds 17-24:** $k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8$
  - **rounds 25-32:** $k_8\ k_7\ k_6\ k_5\ k_4\ k_3\ k_2\ k_1$

$$GOST_K = g_K \circ f_K^3$$

$$24 - Round\ GOST_K = f_K^3$$

24-Round GOST (Unknown S-boxes)

- Using a 6-round truncated differential (with prob. ~2/3) we attack 8-round GOST
- We find subkey material and unknown S-boxes
- Data Complexity: 2^{63} ACPC or almost 2^{64} KP
- Time Complexity: ~2^{64}

30-Round GOST (Known S-boxes)

- Guess subkey of last six rounds
- Partially decrypt all ciphertexts 6 rounds
- Apply 24-round attack
- Data Complexity: almost 2^{64} KP
- Time Complexity: ~2^{254}

Questions?

Thank you!