


Design a block cipher



Design a block cipher

- Round function
- Key schedule



A cartoon illustration of a woman with blonde hair tied up, green eyes, and a sad expression. She is wearing a purple dress with a yellow belt and a yellow cardigan. She stands in the center of the frame, flanked by two yellow boxes with blue borders. The background is a crumpled, light gray paper texture.

“strong”
key schedule

“weak”
key schedule

Related-Key Attacks

$$E_{K_i}(P_i), K_i = \Phi_i(K)$$



Related-Key Attacks

$$E_{K_i}(P_i), K_i = \Phi_i(K)$$



Related-Key Attacks

$$E_{K_i}(P_i), K_i = \Phi_i(K)$$

Avoid by choosing
keys at random



Multi-Key Attacks

$$E_{K_1}(P), E_{K_2}(P), \dots, E_{K_D}(P)$$



Multi-Key Attacks

$$E_{K_1}(P), E_{K_2}(P), \dots, E_{K_D}(P)$$

Always leads to
security erosion!

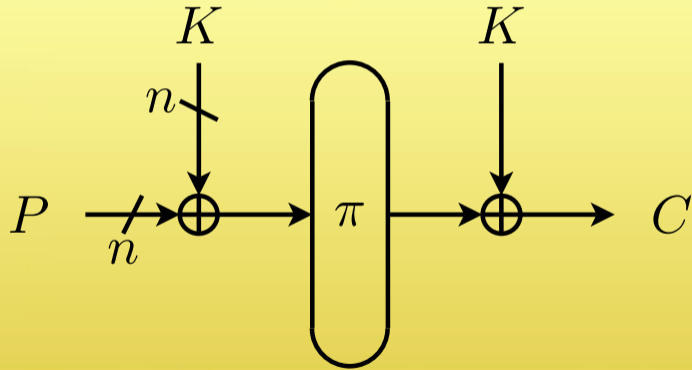


Simplest Fully-Secure Cipher



?

Even-Mansour





Multi-key Even-Mansour: $(D^2 + 2DT)/2^n$



Multi-key Even-Mansour: $(D^2 + 2DT)/2^n$

Ideal block cipher: same bound if $D = \ell$



Multi-key Even-Mansour: $(D^2 + 2DT)/2^n$

Ideal block cipher: same bound if $D = \ell$



Multi-key Even-Mansour: $(D^2 + 2DT)/2^n$

Ideal block cipher: same bound if $D = \ell$

Tight bounds: matching attacks



Multi-key Even-Mansour: $(D^2 + 2DT)/2^n$

Ideal block cipher: same bound if $D = \ell$

Tight bounds: matching attacks

Fast and secure implementation: much easier!



Multi-key Even-Mansour: $(D^2 + 2DT)/2^n$

Ideal block cipher: same bound if $D = \ell$

Tight bounds: matching attacks

Fast and secure implementation: much easier!



Multi-key Even-Mansour: $(D^2 + 2DT)/2^n$

Ideal block cipher: same bound if $D = \ell$

Tight bounds: matching attacks

Fast and secure implementation: much easier!





ePrint 2015/101