CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Data Complexity of Differential Attacks

HGI Cybersec Day, June 5, 2025

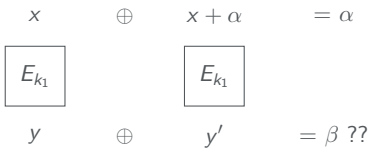
Tim Beyne, Gregor Leander, Mariia Mutkovina, Ricardo Rodriguez
Reveco

Statistical Attacks

A block cipher is a (family of) permutation(s) $\mathrm{F_k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$

- *Real* vs *Ideal* Block Cipher
- *Ideal* is a random uniformly sampled permutation

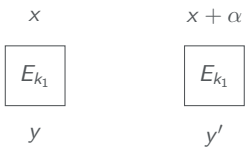
Distinguisher



If $\Pr[y \oplus y' = \beta] = p > \frac{1}{2^n}$ we have a (differential) *distinguisher*

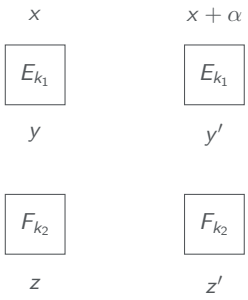
Key Recovery

We split the cipher

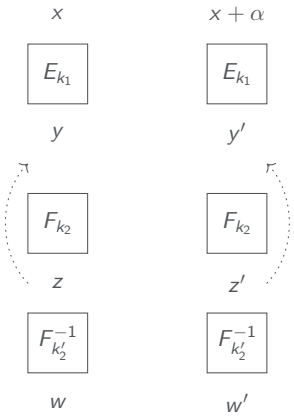


Key Recovery

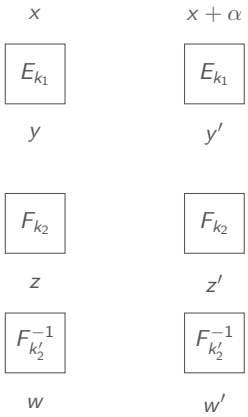
We split the cipher



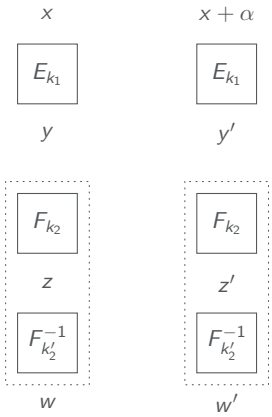
We go back



Right key cancels rounds

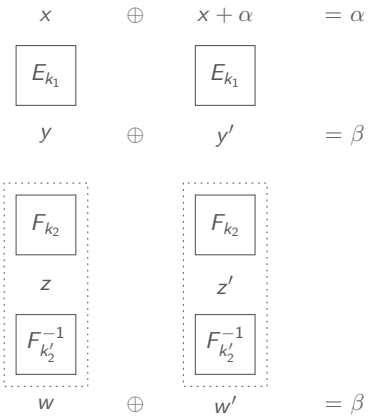


Right key cancels rounds



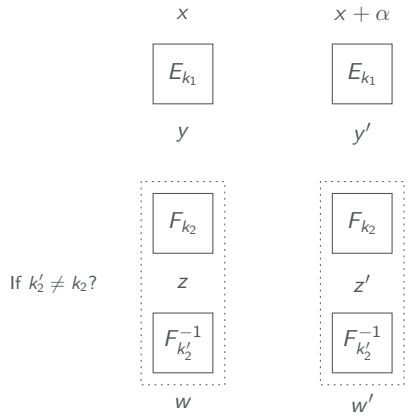
If $k_2' = k_2$,
each dotted box is the identity

Right key cancels rounds

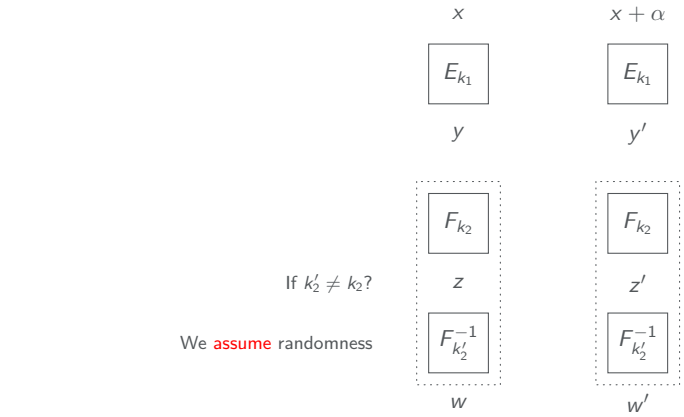


If $k_2' = k_2$,
each dotted box is the identity

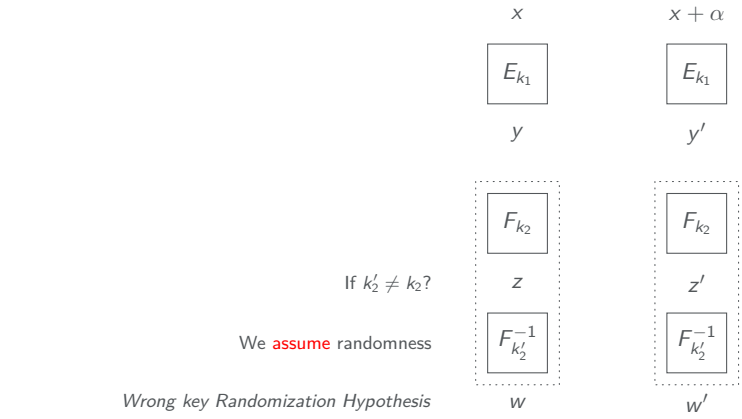
Wrong key?



Wrong key?


x
$x + \alpha$
E_{k_1}
E_{k_1}
y
y'
F_{k_2}
F_{k_2}
If $k_2' \neq k_2$?
z
z'
We assume randomness
$F_{k_2'}^{-1}$
$F_{k_2'}^{-1}$
w
w'

Wrong key?


x
$x + \alpha$
E_{k_1}
E_{k_1}
y
y'
F_{k_2}
F_{k_2}
If $k_2' \neq k_2$?
z
z'
We assume randomness
$F_{k_2'}^{-1}$
$F_{k_2'}^{-1}$
Wrong key Randomization Hypothesis
w
w'

Surprisingly underanalyzed