Algebraic-differential cryptanalysis and addition modulo 2^n

Oleksandr Kazymyrov, Roman Oliynykov and Håvard Raddum

September 5, 2014
Boolean Functions and Their Applications
Rosendal, Norway

Algebraic Attacks

Goal

- Describe an encryption primitive by a system of equations.
- Find all variables including keys.

Algebraic Attacks

Goal

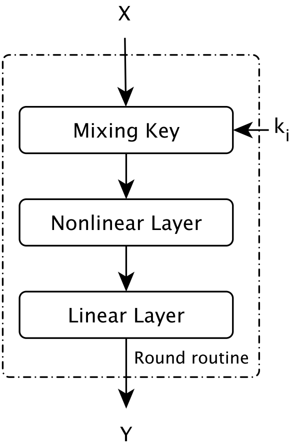
- Describe an encryption primitive by an equation system with maximal number of equations and minimal number of variables.
- Find all variables including keys.

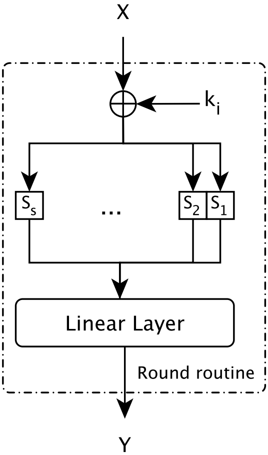
Algebraic Attacks

Goal

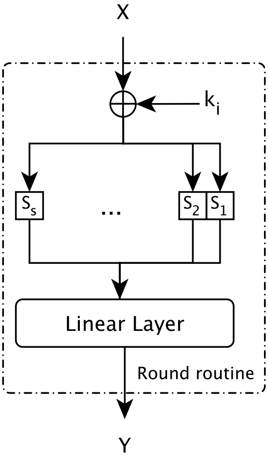
- Describe an encryption primitive by an equation system with the minimal algebraic degree, maximal number of linear independent equations and minimal number of variables.
- Find all variables including keys.

A round routine of an SP network



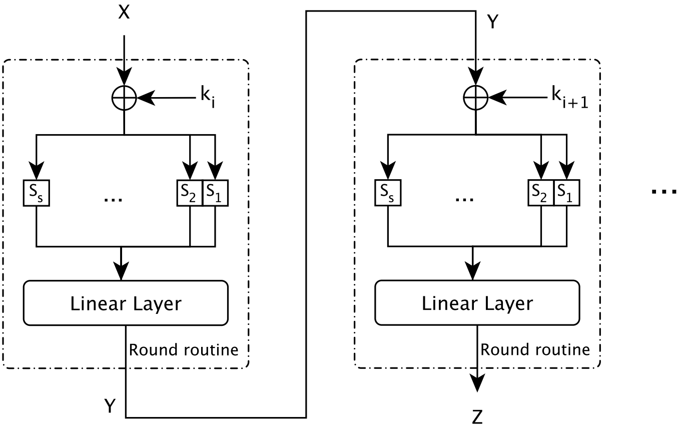


A round routine of an SP network

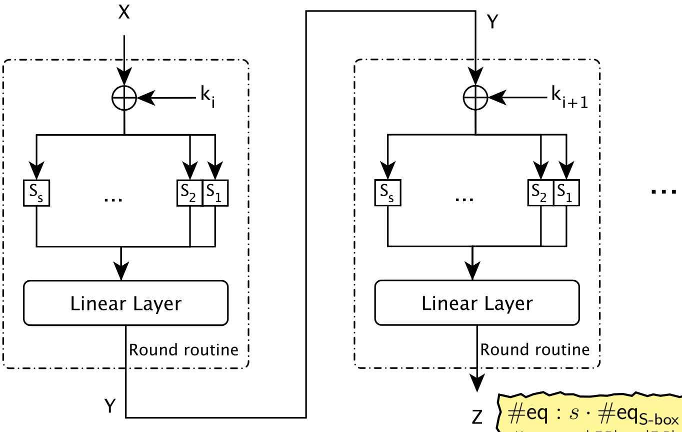


$$
\begin{cases}
x_0x_1 + x_1y_0 + y_1 + 1 = 0 \\
x_0x_1 + x_1y_0 + x_1 = 0 \\
x_0x_1 + x_0 + y_0y_1 = 0 \\
x_1y_0 + y_0y_1 + y_0 = 0 \\
x_1y_1 = 0 \\
x_0y_1 + y_0y_1 = 0 \\
x_0y_0 + y_0y_1 = 0
\end{cases}
$$

Two and more rounds

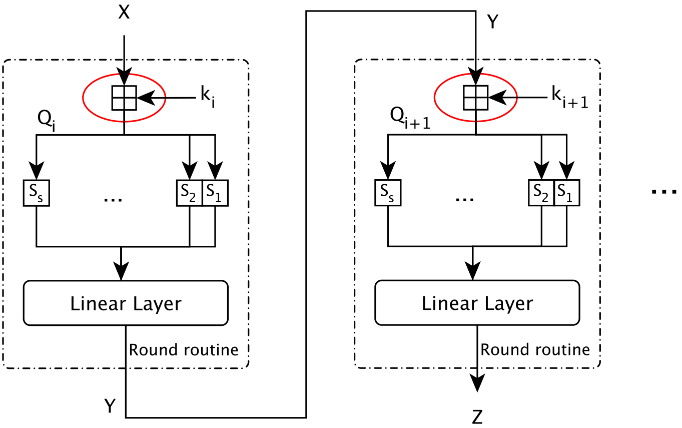


Two and more rounds



#eq : $s \cdot$ #eq$_{\text{S-box}}$
#vars : $|X| + |Y| + |k_i|$

Cryptoprimitives with addition modulo 2^n



Cryptoprimitives with addition mod 2^n

- IDEA
- ARX (Skein, Theefish, ...)
- SNOW 2.0
- GOST 28147-89
- STB 34.101.31-2011
- Kalyna
- GOST 34.11-2012
- ...

Addition modulo 2^n

- Nonlinear
- Widespread values are $n = 32$ and $n = 64$
- Reduced performance comparing to XOR
- Mostly used in ARX constructions
- CCZ-equivalent to a quadratic function
- Described by a system of quadratic equations

Description of mod 2^n by a system of equations

$$\begin{cases} a_i + a_i r_i + a_i r_{i+1} + a_i a_{i+1} + a_i b_{i+1} + r_i r_{i+1} + r_i a_{i+1} + r_i b_{i+1} = 0 \\ b_i + b_i r_i + b_i r_{i+1} + b_i a_{i+1} + b_i b_{i+1} + r_i r_{i+1} + r_i a_{i+1} + r_i b_{i+1} = 0 \\ a_i r_i + b_i r_i + a_i b_i + a_i + b_i + r_{i+1} + a_{i+1} + b_{i+1} = 0 \end{cases}$$

$$\begin{array}{cccccc} & \boxed{a_n} & \boxed{a_{n-1}} & \dots & \boxed{a_2} & \boxed{a_1} \\ + & & & & & \\ & \boxed{b_n} & \boxed{b_{n-1}} & \dots & \boxed{b_2} & \boxed{b_1} \\ \hline & \boxed{r_n} & \boxed{r_{n-1}} & \dots & \boxed{r_2} & \boxed{r_1} \end{array}$$

Addition modulo 2^n and XOR

- Approximation by XOR

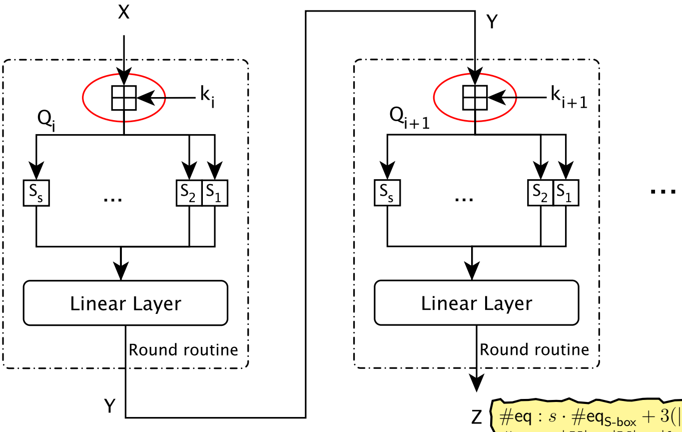
$$Pr(x \boxplus y = x \oplus y) = \frac{4 \cdot 3^{n-1}}{2^{2n}}$$

n	4	6	8	32	64
Pr	0.422	0.237	0.133	$10^{-3.87}$	$10^{-7.87}$

- Probability of a carry bit

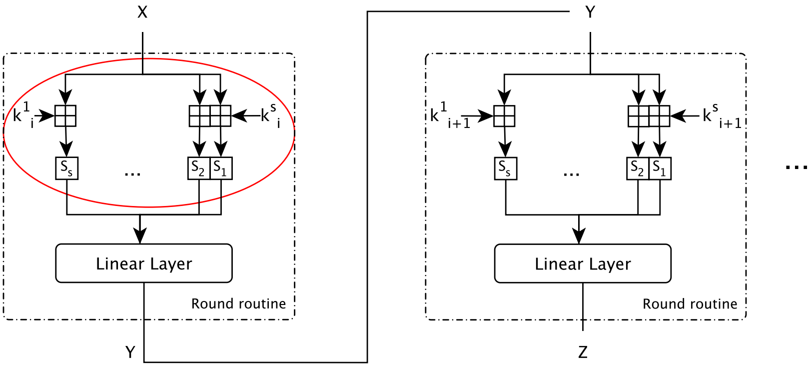
$$Pr(carry) = \frac{1}{2} - \frac{1}{2^{n+1}}$$

Representations of routines with ⊞ (I)

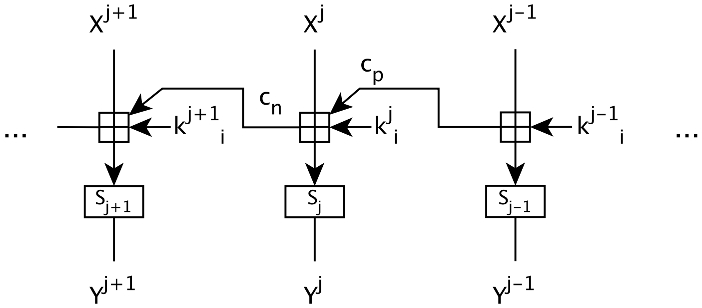


#eq : $s \cdot$ #eq$_{\text{S-box}}$ $+ 3(|X| - 1)$
#vars : $|X| + |Y| + |k_i| + |Q|$

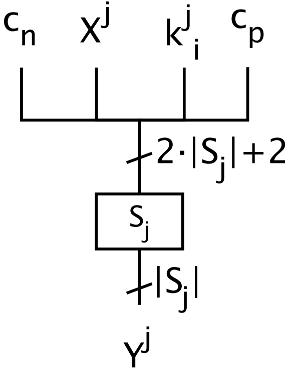
Representations of routines with ⊞ (II)



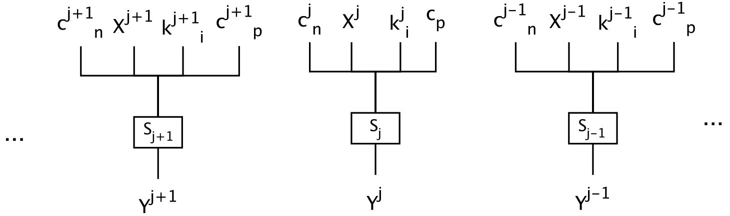
Addition plus substitution (II)



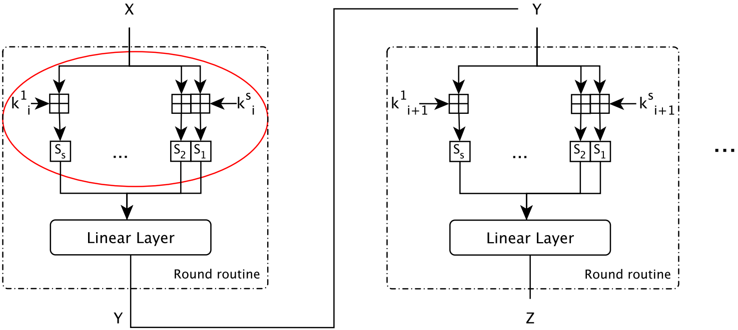
Algebraic description (II)



Addition plus substitution (II)

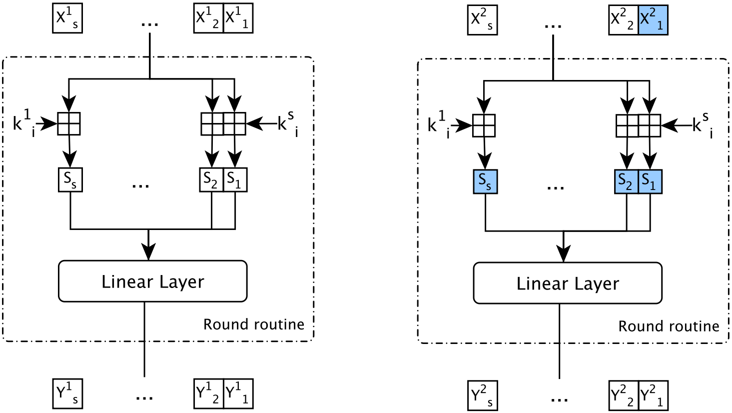


Representations of routines with ⊞ (II)

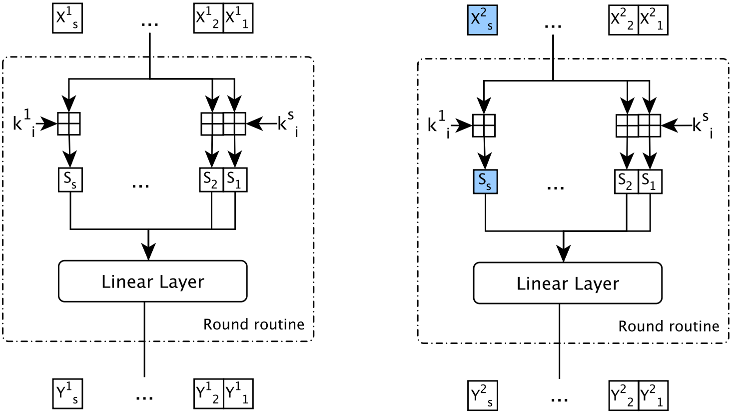


#eq : $s \cdot$ #eq$^*_{\text{S-box}}$
#vars : $|X| + |Y| + |k_i| + s - 1$

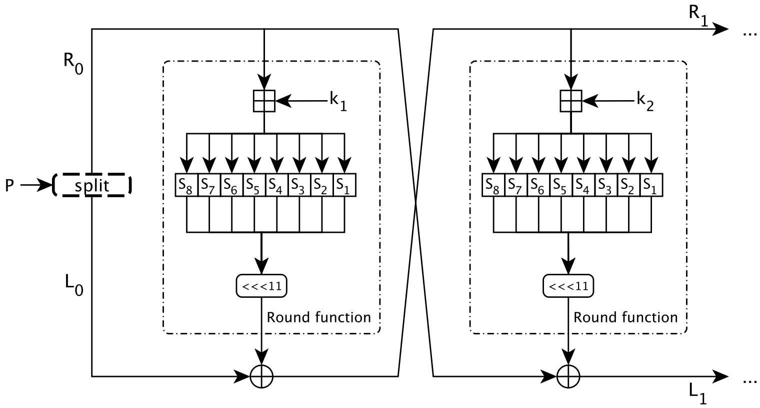
Two rounds with differentials



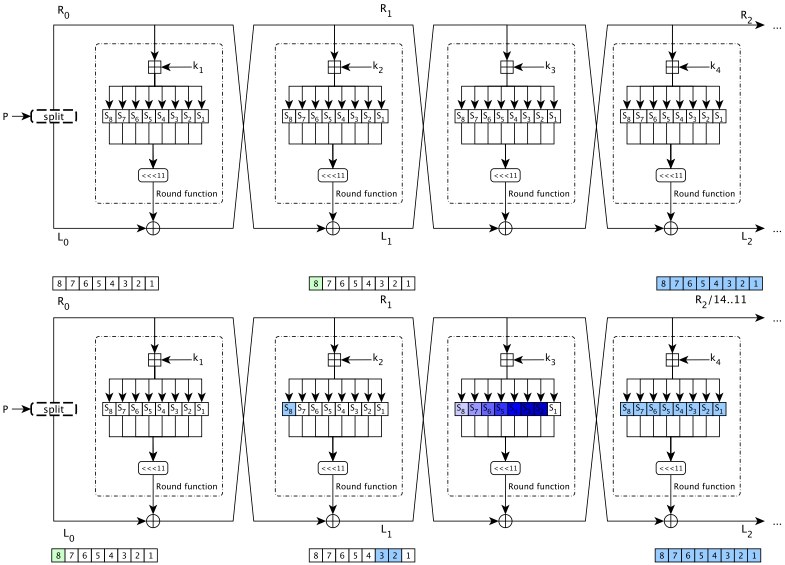
Two rounds with differentials



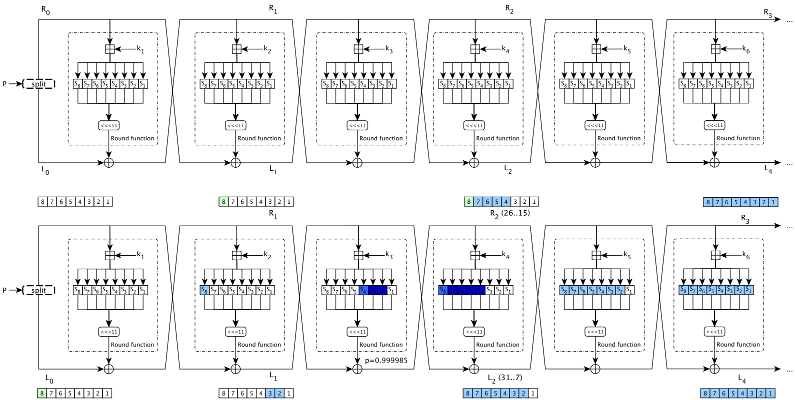
GOST 28147-89



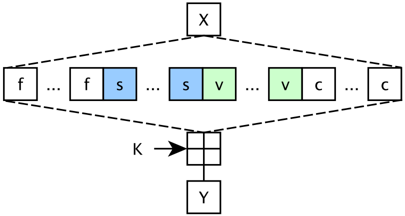
An algebraic-differential attack on GOST 28147-89



An algebraic-differential attack on GOST 28147-89



Number of active S-boxes after $\boxplus$



Theorem

Suppose f, s, v and c are fixed, stop, variable and constant bits, respectively. Then the probability that f-bits are not affected by addition modulo 2^n is

$$Pr(f \text{ are the same}) = 1 - \frac{2^{|v|} - 1}{2^{|s||v|}}$$

Open problems

- How to use the known CCZ-equivalence property of mod 2^n on real ciphers?
- Are there more equations for the description of addition modulo 2^n by a system of equations?
- What about theoretical bounds of $\oplus \mapsto \boxplus$, $\boxplus \mapsto \oplus$ and $\boxplus \mapsto \boxplus$?
- Find a theoretical example of an (n, n) permutation function limited by δ-uniformity, nonlinearity and algebraic immunity.