Cryptanalysis of Block Ciphers with Overdefined Systems of Equations

Halil İbrahim Kaplan

TDBY / Kripto Analiz Laboratuvarı

halil.kaplan@tubitak.gov.tr

2021

Overview

1. **Introduction**
2. **Overdefined Equations on the Rijndael S-box**
3. **The XSL Attack**
4. **T method**
5. **Attack results on AES**

By definition, an XSL-cipher is a composition of N_r similar rounds:

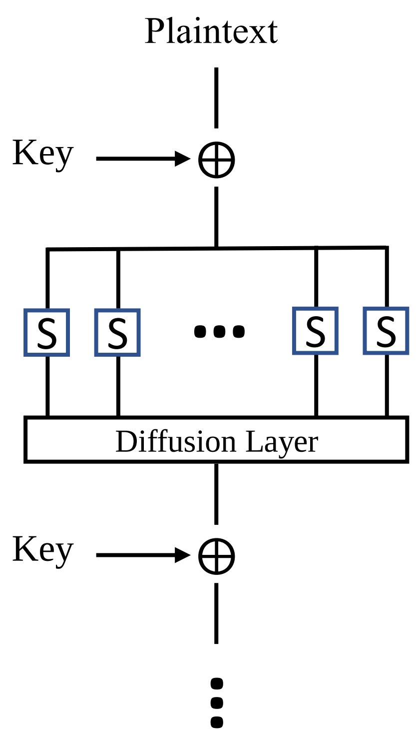
X The first round starts with a XOR with the session key K_i-1.

S Then we apply a layer of B bijective S-boxes in parallel, each on s bits,

L Then we apply a linear diffusion layer,

X Then we XOR with another session key K_i.

Then if i = N_r we finish, otherwise we increment i and go back to step S



Step:		X	S	L	X	...	...	S	L	X	
Values:	Z_0	X_1	Y_1	Z_1	X_2	...	X_{N_r}	Y_{N_r}	Z_{N_r}	X_{N_r+1}	

Let,

r = # of equations.
s = # of variables in equation.
t = # of monomials.
d = degree of equations.

In general,

$$t \approx \binom{s}{d}$$

If ,

$$t << \binom{s}{d}$$

Then

Equations are called **sparse(rare)**

Let,

r = # of equations.
s = # of variables in equation.
t = # of monomials.
d = degree of equations.

When,

$r >> s$

system is **overdefined.**

When

$$\# \text{ of equations} \approx \# \text{ of monomials}$$

we may eliminate most of the terms by linear elimination, and obtain simpler equations that are sparse and maybe even linear.

Good S-box : # of monomials >> # of equations

Overdefined Equations on the Rijndael S-box

AES S-box consist of 2 transformations:

1.

$$g : GF(2^8) \longrightarrow GF(2^8)$$

$$x \longrightarrow \frac{1}{x} \quad \text{(0 mapped on itself)}$$

2.

$$f : GF(2^8) \longrightarrow GF(2^8)$$

$$y = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

S-box = f o g

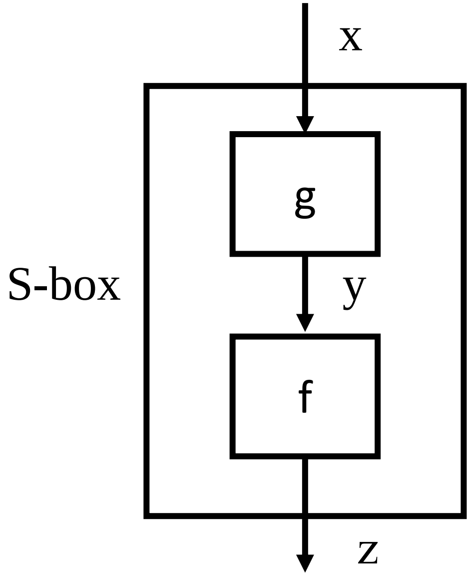
Let

$$y = g(x)$$

$$z = \text{S-box}(x) = f(y) = f(g(x))$$

Then

$$x * y = 1 \text{ when } x \neq 0$$



Overdefined Equations on the Rijndael S-box

$$x * y = 1 \iff [(\sum_{i=0}^{7} x_i * t^i)(\sum_{j=0}^{7} y_j * t^j)]_{m(t)} = \sum_{k=1}^{7} 0 * t^k + 1$$

We can rearrange equation

$$\sum_{i=0}^{7}\sum_{j=0}^{7}[(x_i * t^i)(y_j * t^j)]_{m(t)} = \sum_{k=1}^{7} 0 * t^k + 1$$

$$where\ m(t) = t^8 + t^4 + t^3 + \mathrm{t} + 1$$

If we make the multiplication, we will get

$$
\begin{gathered}
x \otimes y = x_7y_7 \bullet t^{14} + (x_7y_6 + x_6y_7) \bullet t_{13} + (x_7y_5 + x_6y_6 + x_5y_7) \bullet t_{12} + \\
(x_7y_4 + x_6y_5 + x_5y_6 + x_4y_7) \bullet t^{11} + (x_7y_3 + x_6y_4 + x_5y_5 + x_4y_6 + x_3y_7) \\
\bullet t^{10} + (x_7y_2 + x_6y_3 + x_5y_4 + x_4y_5 + x_3y_6 + x_2y_7) \bullet t^9 + \\
(x_7y_1 + x_6y_2 + x_5y_3 + x_4y_4 + x_3y_5 + x_2y_6 + x_1y_7) \bullet t^8 + \\
(x_7y_0 + x_6y_1 + x_5y_2 + x_4y_3 + x_3y_4 + x_2y_5 + x_1y_6 + x_0y_7) \bullet t^7 + \\
(x_6y_0 + x_5y_1 + x_4y_2 + x_3y_3 + x_2y_4 + x_1y_5 + x_0y_6) \\
\bullet t^6 + (x_5y_0 + x_4y_1 + x_3y_2 + x_2y_3 + x_1y_4 + x_0y_5) \bullet t^5 + \\
(x_4y_0 + x_3y_1 + x_2y_2 + x_1y_3 + x_0y_4) \bullet t^4 + (x_3y_0 + x_2y_1 + x_1y_2 + x_0y_3) \\
\bullet t^3 + (x_2y_0 + x_1y_1 + x_0y_2) \bullet t^2 + (x_1y_0 + x_0y_1) \bullet t + x_0y_0
\end{gathered}
$$

then we apply modulo m(t)= $t^8 + t^4 + t^3 + t + 1$

Overdefined Equations on the Rijndael S-box

$$x_7 y_7 * t^{14} \quad = x_7 y_7 * \underbrace{t^8}_{t^4 + t^3 + t + 1} * t^6$$

$$= x_7 y_7 * (t^4 + t^3 + t + 1) * t^6$$

$$= x_7 y_7 * t^{10} + x_7 y_7 * t^9 + x_7 y_7 * t^7 + x_7 y_7 * t^6$$

$$(x_7y_6 + x_6y_7) * t^{13} = (x_7y_6 + x_6y_7) * \underbrace{t^8}_{t^4 + t^3 + \mathrm{t} + 1} * t^5$$

$$= (x_7y_6 + x_6y_7) * (t^4 + t^3 + \mathrm{t} + 1) * t^5$$

$$= (x_7y_6 + x_6y_7) * t^9 + (x_7y_6 + x_6y_7) * t^8$$
$$+ (x_7y_6 + x_6y_7) * t^7 + (x_7y_6 + x_6y_7) * t^5$$

$$\vdots$$

$$
\begin{aligned}
c_7 = {} & x_7y_0 + x_6y_1 + x_5y_2 + x_4y_3 + x_3y_4 + x_2y_5 + x_1y_6 + x_0y_7 \\
& + x_7y_7 + x_7y_5 + x_6y_6 + x_5y_7 + x_7y_4 + x_6y_5 + x_5y_6 + x_4y_7 \\
c_6 = {} & x_6y_0 + x_5y_1 + x_4y_2 + x_3y_3 + x_2y_4 + x_1y_5 + x_0y_6 + x_7y_6 \\
& + x_6y_7 + x_7y_4 + x_6y_5 + x_5y_6 + x_4y_7 + x_7y_3 + x_6y_4 + \\
& x_5y_5 + x_4y_6 + x_3y_7 \\
c_5 = {} & x_5y_0 + x_4y_1 + x_3y_2 + x_2y_3 + x_1y_4 + x_0y_5 + x_7y_5 + x_6y_6 \\
& + x_5y_7 + x_7y_3 + x_6y_4 + x_5y_5 + x_4y_6 + x_3y_7 + x_7y_2 + x_6y_3 \\
& + x_5y_4 + x_4y_5 + x_3y_6 + x_2y_7 \\
c_4 = {} & x_4y_0 + x_3y_1 + x_2y_2 + x_1y_3 + x_0y_4 + x_7y_4 + x_6y_5 + x_5y_6 + \\
& x_4y_7 + x_7y_2 + x_6y_3 + x_5y_4 + x_4y_5 + x_3y_6 + x_2y_7 + x_7y_7 + \\
& x_7y_1 + x_6y_2 + x_5y_3 + x_4y_4 + x_3y_5 + x_2y_6 + x_1y_7 \\
c_3 = {} & x_3y_0 + x_2y_1 + x_1y_2 + x_0y_3 + x_7y_4 + x_6y_5 + x_5y_6 + x_4y_7 + \\
& x_7y_3 + x_6y_4 + x_5y_5 + x_4y_6 + x_3y_7 + x_7y_7 + x_7y_1 + x_6y_2 + \\
& x_5y_3 + x_4y_4 + x_3y_5 + x_2y_6 + x_1y_7 + x_7y_6 + x_6y_7 + x_7y_5 + \\
& x_6y_6 + x_5y_7 \\
c_2 = {} & x_2y_0 + x_1y_1 + x_0y_2 + x_7y_3 + x_6y_4 + x_5y_5 + x_4y_6 + x_3y_7 + \\
& x_7y_2 + x_6y_3 + x_5y_4 + x_4y_5 + x_3y_6 + x_2y_7 + x_7y_6 + x_6y_7 \\
c_1 = {} & x_1y_0 + x_0y_1 + x_7y_2 + x_6y_3 + x_5y_4 + x_4y_5 + x_3y_6 + x_2y_7 + \\
& x_7y_7 + x_7y_1 + x_6y_2 + x_5y_3 + x_4y_4 + x_3y_5 + x_2y_6 + x_1y_7 + \\
& x_7y_5 + x_6y_6 + x_5y_7 \\
c_0 = {} & x_0y_0 + x_7y_1 + x_6y_2 + x_5y_3 + x_4y_4 + x_3y_5 + x_2y_6 + x_1y_7 + \\
& x_7y_6 + x_6y_7 + x_7y_5 + x_6y_6 + x_5y_7
\end{aligned}
$$

Overdefined Equations on the Rijndael S-box

$$z = A * y + 63 \quad \Longrightarrow \quad y = A^{-1} * z + 05$$

Where:

$$A = \begin{bmatrix} 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \\ 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \end{bmatrix} \quad A^{-1} = \begin{bmatrix} 0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&0&0&1 \\ 1&0&0&1&0&1&0&0 \\ 0&1&0&0&1&0&1&0 \\ 0&0&1&0&0&1&0&1 \\ 1&0&0&1&0&0&1&0 \\ 0&1&0&0&1&0&0&1 \\ 1&0&1&0&0&1&0&0 \end{bmatrix}$$

We can get :

$$y_7 = z_6 + z_4 + z_1$$
$$y_6 = z_5 + z_3 + z_0$$
$$y_5 = z_7 + z_4 + z_2$$
$$y_4 = z_6 + z_3 + z_1$$
$$y_3 = z_5 + z_2 + z_0$$
$$y_2 = z_7 + z_4 + z_1 + 1$$
$$y_1 = z_6 + z_3 + z_0$$
$$y_0 = z_7 + z_5 + z_2 + 1$$

Overdefined Equations on the Rijndael S-box

$$P=1\quad\left\{\begin{aligned}
0 = {} & z_0x_4 + z_0x_5 + z_0x_1 + x_0z_6 + x_0z_4 + x_0z_1 + x_2z_7 + x_2z_4 + x_2z_2 + x_3z_6 + x_3z_3 + x_3z_1 + \\
& x_4z_6 + x_4z_5 + x_4z_4 + x_4z_2 + x_4z_1 + x_5z_6 + x_5z_7 + x_5z_5 + x_5z_3 + x_6z_6 + x_6z_7 + x_6z_5 + \\
& x_6z_4 + x_6z_2 + x_7z_5 + x_7z_3 + x_1z_5 + x_1z_3 + x_5 + x_7 \\
0 = {} & z_0x_0 + z_0x_3 + z_0x_4 + x_0z_5 + x_0z_3 + x_2z_6 + x_2z_3 + x_2z_1 + x_3z_6 + x_3z_5 + x_3z_4 + x_3z_2 + \\
& x_3z_1 + x_4z_6 + x_4z_7 + x_4z_5 + x_4z_3 + x_5z_6 + x_5z_7 + x_5z_5 + x_5z_4 + x_5z_2 + x_6z_5 + x_6z_3 + \\
& x_7z_6 + x_7z_2 + x_7z_1 + x_1z_7 + x_1z_4 + x_1z_2 + x_4 + x_6 \\
0 = {} & z_0x_2 + z_0x_3 + z_0x_7 + x_0z_7 + x_0z_4 + x_0z_2 + x_2z_6 + x_2z_5 + x_2z_4 + x_2z_2 + x_2z_1 + x_3z_6 + \\
& x_3z_7 + x_3z_5 + x_3z_3 + x_4z_6 + x_4z_7 + x_4z_5 + x_4z_4 + x_4z_2 + x_5z_5 + x_5z_3 + x_6z_6 + x_6z_2 + \\
& x_6z_1 + x_7z_5 + x_7z_1 + x_1z_6 + x_1z_3 + x_1z_1 + x_3 + x_5 + x_7 \\
0 = {} & z_0x_2 + z_0x_6 + z_0x_7 + z_0x_1 + x_0z_6 + x_0z_3 + x_0z_1 + x_2z_6 + x_2z_7 + x_2z_5 + x_2z_3 + x_3z_6 + \\
& x_3z_7 + x_3z_5 + x_3z_4 + x_3z_2 + x_4z_5 + x_4z_3 + x_5z_6 + x_5z_2 + x_5z_1 + x_6z_5 + x_6z_1 + x_7z_6 + \\
& x_7z_7 + x_7z_1 + x_1z_6 + x_1z_5 + x_1z_4 + x_1z_2 + x_1z_1 + x_2 + x_4 + x_6 + x_7 \\
0 = {} & z_0x_0 + z_0x_4 + z_0x_6 + z_0x_7 + x_0z_5 + x_0z_2 + x_2z_6 + x_2z_5 + x_3z_6 + x_3z_5 + x_3z_1 + x_4z_5 + \\
& x_4z_4 + x_5z_6 + x_5z_7 + x_5z_3 + x_5z_1 + x_6z_5 + x_6z_4 + x_6z_2 + x_6z_1 + x_7z_6 + x_7z_7 + x_7z_3 + \\
& x_1z_6 + x_1z_7 + x_3 + x_6 + x_1 \\
0 = {} & z_0x_3 + z_0x_4 + z_0x_6 + z_0x_1 + x_0z_7 + x_0z_4 + x_0z_1 + x_2z_6 + x_2z_7 + x_2z_5 + x_2z_4 + x_2z_2 + \\
& x_2z_1 + x_3z_6 + x_3z_5 + x_3z_4 + x_3z_3 + x_3z_1 + x_4z_7 + x_4z_5 + x_4z_4 + x_4z_3 + x_4z_2 + x_5z_6 + \\
& x_5z_7 + x_5z_4 + x_5z_3 + x_5z_2 + x_5z_1 + x_6z_5 + x_6z_4 + x_6z_3 + x_6z_2 + x_7z_7 + x_7z_4 + x_7z_3 + \\
& x_7z_2 + x_7z_1 + x_1z_6 + x_1z_3 + x_0 + x_2 + x_7 \\
0 = {} & z_0x_0 + z_0x_2 + z_0x_3 + z_0x_5 + z_0x_7 + x_0z_6 + x_0z_3 + x_2z_6 + x_2z_5 + x_2z_4 + x_2z_3 + x_2z_1 + \\
& x_3z_7 + x_3z_5 + x_3z_4 + x_3z_3 + x_3z_2 + x_4z_6 + x_4z_7 + x_4z_4 + x_4z_3 + x_4z_2 + x_4z_1 + x_5z_5 + \\
& x_5z_4 + x_5z_3 + x_5z_2 + x_6z_7 + x_6z_4 + x_6z_3 + x_6z_2 + x_6z_1 + x_7z_4 + x_7z_3 + x_7z_2 + x_1z_6 + \\
& x_1z_7 + x_1z_5 + x_1z_4 + x_1z_2 + x_1z_1 + x_6 + x_7 + x_1
\end{aligned}\right.$$

$$P=\frac{255}{256}\quad\left\{\begin{aligned}
1 = {} & x_0 + x_6 + z_0x_2 + z_0x_5 + z_0x_6 + x_0z_7 + x_0z_5 + x_0z_2 + x_2z_5 + x_2z_3 + x_3z_7 + x_3z_4 + x_3z_2 + \\
& x_4z_6 + x_4z_3 + x_4z_1 + x_5z_6 + x_5z_5 + x_5z_4 + x_5z_2 + x_5z_1 + x_6z_6 + x_6z_7 + x_6z_5 + x_6z_3 + \\
& x_7z_6 + x_7z_7 + x_7z_5 + x_7z_4 + x_7z_2 + x_1z_6 + x_1z_4 + x_1z_1
\end{aligned}\right.$$

$$x * y = 1$$

$$\Downarrow$$

$$x^2 * y = x$$

$$\Downarrow$$

$$x^4 * y^2 = x^2$$

$$\vdots$$

$$\Downarrow$$

$$x^{256} * y^{128} = x * y^{128} = x^{128}$$

It is symmetric wrt. the exchange of x and y.

So we have :

$$x^{128} = y^{128} * x$$

$$y^{128} = x^{128} * y$$

We have 16 more equations with same technique from:

$$x^{128} = y^{128} * x$$

$$y^{128} = x^{128} * y$$

$$0 = x_3+x_5+x_6+x_1+x_2z_2+x_5z_7+x_7z_4+x_7z_1+x_7z_3+x_0z_1+x_6z_5+x_6z_3+x_7z_7+x_4z_6+x_4z_1+x_4z_5+x_4z_0+x_4z_2+x_1z_5+x_1z_3+x_5z_5+x_5z_3+x_5z_0+x_3z_1+x_3z_3+x_6z_6+x_3z_4+x_2z_3+x_2z_6+x_4z_7+x_0z_5+x_0z_3+x_1z_4+x_1z_7+x_6z_1+x_3z_0+x_4z_3+x_0z_7+x_1z_6+x_2z_5$$

$$0 = x_3+x_6+x_1+x_2z_4+x_5z_1+x_7z_1+x_5z_6+x_0z_6+x_0z_4+x_6z_3+x_6z_4+x_6z_7+x_7z_7+x_7z_5+x_7z_2+x_4z_5+x_4z_0+x_1z_5+x_1z_3+x_5z_5+x_5z_3+x_3z_1+x_3z_3+x_3z_6+x_2z_1+x_2z_3+x_4z_7+x_0z_5+x_0z_3+x_1z_2+x_6z_1+x_3z_5+x_3z_0+x_3z_2+x_4z_3+x_0z_7+x_3z_7+x_1z_6+x_2z_0$$

$$0 = x_3+x_4+x_5+x_1+x_2z_2+x_2z_7+x_5z_1+x_5z_4+x_5z_7+x_7z_6+x_7z_4+x_7z_1+x_0z_6+x_6z_5+x_6z_2+x_6z_7+x_7z_7+x_4z_6+x_4z_1+x_4z_5+x_1z_3+x_1z_0+x_5z_3+x_3z_3+x_2z_1+x_2z_3+x_2z_6+x_0z_5+x_0z_3+x_1z_4+x_6z_1+x_3z_5+x_3z_0+x_4z_3+x_0z_2+x_3z_7+x_1z_1+x_2z_5+x_2z_0$$

$$0 = x_3+x_4+x_1+x_2z_7+x_5z_1+x_5z_7+x_7z_4+x_0z_4+x_0z_1+x_6z_4+x_6z_7+x_7z_7+x_7z_5+x_7z_2+x_4z_4+x_4z_1+x_1z_5+x_1z_3+x_1z_0+x_5z_5+x_3z_1+x_3z_3+x_3z_6+x_6z_6+x_5z_2+x_2z_3+x_4z_7+x_0z_3+x_0z_0+x_1z_2+x_1z_7+x_6z_1+x_3z_5+x_4z_3+x_1z_1+x_1z_6+x_2z_5+x_2z_0$$

$$0 = x_2+x_6+x_7+x_1+x_2z_2+x_5z_1+x_5z_4+x_7z_4+x_7z_1+x_5z_6+x_7z_3+x_0z_6+x_6z_3+x_6z_2+x_6z_4+x_6z_7+x_7z_7+x_7z_2+x_4z_6+x_4z_0+x_1z_0+x_5z_5+x_5z_3+x_5z_0+x_6z_6+x_2z_1+x_0z_0+x_1z_4+x_6z_1+x_3z_0+x_4z_3+x_0z_2+x_3z_7+x_1z_6$$

$$0 = x_2+x_3+x_4+x_5+x_1+x_2z_2+x_2z_7+x_5z_1+x_5z_4+x_7z_6+x_7z_1+x_5z_6+x_0z_6+x_0z_4+x_0z_1+x_6z_5+x_6z_2+x_6z_4+x_6z_7+x_7z_2+x_4z_4+x_4z_2+x_1z_5+x_1z_3+x_5z_5+x_5z_0+x_3z_1+x_3z_6+x_6z_6+x_5z_2+x_3z_4+x_2z_3+x_2z_6+x_4z_7+x_0z_5+x_0z_3+x_0z_0+x_1z_2+x_1z_4+x_1z_7+x_0z_7+x_1z_1+x_1z_6+x_2z_5+x_2z_0$$

$$0 = x_0+x_2+x_3+x_7+x_2z_4+x_5z_4+x_5z_7+x_7z_6+x_7z_1+x_5z_6+x_0z_6+x_0z_4+x_0z_1+x_6z_2+x_7z_7+x_4z_6+x_4z_4+x_4z_1+x_4z_5+x_4z_0+x_4z_2+x_1z_5+x_1z_3+x_1z_0+x_5z_5+x_6z_6+x_5z_2+x_3z_4+x_2z_1+x_2z_6+x_7z_0+x_0z_5+x_0z_3+x_1z_2+x_1z_7+x_6z_1+x_3z_2+x_0z_2+x_0z_7+x_3z_7+x_1z_6$$

$$0 = x_3+x_5+x_2z_4+x_2z_7+x_5z_1+x_5z_7+x_7z_6+x_7z_1+x_5z_6+x_7z_3+x_0z_6+x_0z_1+x_6z_5+x_6z_3+x_6z_0+x_6z_7+x_7z_5+x_4z_4+x_4z_1+x_4z_0+x_1z_5+x_1z_3+x_5z_5+x_5z_3+x_5z_0+x_3z_3+x_3z_6+x_5z_2+x_2z_3+x_2z_6+x_0z_0+x_1z_7+x_3z_5+x_3z_2+x_4z_3+x_0z_2+x_1z_1+x_2z_5$$

$$0 = x_5+x_7+z_7+z_5+z_3+z_1+x_5z_1+x_5z_4+x_7z_3+x_0z_6+x_0z_4+x_0z_1+x_6z_3+x_7z_2+x_4z_4+x_4z_2+x_1z_5+x_1z_0+x_5z_3+x_6z_6+x_3z_4+x_2z_3+x_4z_7+x_7z_0+x_6z_1+x_3z_7+x_2z_5+x_2z_0$$

$$0 = x_3+x_5+x_7+z_6+z_7+z_5+z_4+z_3+x_2z_2+x_2z_4+x_2z_7+x_7z_1+x_6z_5+x_6z_0+x_6z_2+x_6z_4+x_7z_7+x_7z_2+x_4z_6+x_4z_1+x_5z_3+x_5z_0+x_3z_1+x_3z_3+x_6z_6+x_5z_2+x_3z_4+x_0z_5+x_0z_3+x_0z_0+x_1z_4+x_1z_7+x_6z_1+x_4z_3$$

$$0 = x_3+x_5+x_6+x_7+x_1+z_6+z_5+z_3+z_2+x_5z_1+x_5z_7+x_7z_6+x_7z_1+x_0z_4+x_6z_5+x_6z_3+x_6z_0+x_6z_7+x_4z_6+x_4z_4+x_4z_1+x_4z_5+x_4z_0+x_4z_2+x_1z_3+x_3z_3+x_6z_6+x_5z_2+x_2z_1+x_2z_3+x_2z_6+x_7z_0+x_1z_4+x_3z_0+x_3z_2+x_0z_2+x_0z_7+x_1z_1$$

$$0 = x_3+x_4+x_5+x_1+z_4+z_3+z_1+z_0+x_2z_2+x_2z_4+x_5z_1+x_5z_6+x_0z_6+x_0z_1+x_6z_5+x_6z_2+x_6z_4+x_6z_7+x_7z_7+x_7z_5+x_4z_6+x_4z_5+x_4z_0+x_1z_3+x_1z_0+x_5z_0+x_3z_1+x_6z_6+x_2z_1+x_2z_6+x_4z_7+x_7z_0+x_0z_3+x_1z_2+x_3z_2+x_4z_3+x_3z_7+x_2z_5+x_2z_0$$

$$0 = x_2+x_3+x_5+x_6+x_1+z_6+z_2+z_0+x_2z_7+x_5z_1+x_5z_4+x_5z_7+x_7z_6+x_7z_4+x_7z_3+x_6z_5+x_7z_7+x_7z_2+x_4z_6+x_4z_5+x_1z_5+x_1z_0+x_5z_5+x_5z_3+x_5z_0+x_3z_1+x_3z_6+x_6z_6+x_3z_4+x_2z_6+x_7z_0+x_0z_5+x_0z_0+x_1z_2+x_1z_7+x_6z_1+x_3z_0+x_0z_2+x_3z_7+x_1z_1$$

$$0 = x_0+x_3+x_4+x_5+x_1+z_6+z_7+z_5+z_4+z_3+z_1+z_0+x_5z_1+x_5z_7+x_7z_4+x_5z_6+x_0z_4+x_0z_1+x_6z_5+x_6z_3+x_6z_0+x_6z_4+x_7z_7+x_7z_5+x_4z_6+x_4z_4+x_4z_1+x_4z_5+x_4z_2+x_1z_5+x_5z_0+x_3z_1+x_3z_3+x_6z_6+x_5z_2+x_2z_3+x_2z_6+x_4z_7+x_7z_0+x_1z_4+x_1z_7+x_6z_1+x_3z_5+x_3z_0+x_0z_7+x_1z_1+x_1z_6+x_2z_0$$

$$0 = x_2+x_3+x_7+x_1+z_6+z_7+z_5+z_4+z_3+z_2+z_1+1+x_2z_2+x_2z_4+x_2z_7+x_5z_4+x_5z_7+x_7z_1+x_7z_3+x_0z_6+x_6z_5+x_6z_3+x_6z_0+x_6z_2+x_6z_4+x_6z_7+x_7z_7+x_4z_6+x_4z_4+x_4z_1+x_4z_5+x_4z_0+x_1z_5+x_1z_3+x_1z_0+x_5z_5+x_5z_0+x_3z_1+x_3z_6+x_2z_1+x_2z_6+x_0z_3+x_0z_0+x_3z_0+x_3z_2+x_4z_3+x_3z_7+x_1z_1+x_2z_5$$

$$0 = x_0+x_7+x_1+z_6+z_2+z_1+z_0+1+x_2z_4+x_5z_4+x_5z_7+x_7z_4+x_7z_1+x_7z_3+x_6z_2+x_6z_4+x_6z_7+x_4z_5+x_4z_0+x_1z_5+x_2z_1+x_2z_6+x_0z_5+x_1z_2+x_1z_7+x_3z_5+x_3z_0+x_4z_3+x_0z_2+x_0z_7+x_1z_1+x_1z_6$$

The XSL Attack

The XSL Attack

For each S-box in cipher,

$\boxed{\text{S-box}}$ r equations
t terms

we will write a set of quadratic equations that will completely define the secret key of the cipher

We will extend # of equations using XSL and T method.

$$R \geq T \implies$$ System can be solved by Linearization.

# of quadratic eq. # of terms.

Eq_1
Eq_2
.
.
Eq_r

Equations defines key of the cipher

XSL

Eq_1
Eq_2
.
.
Eq_{r+m}

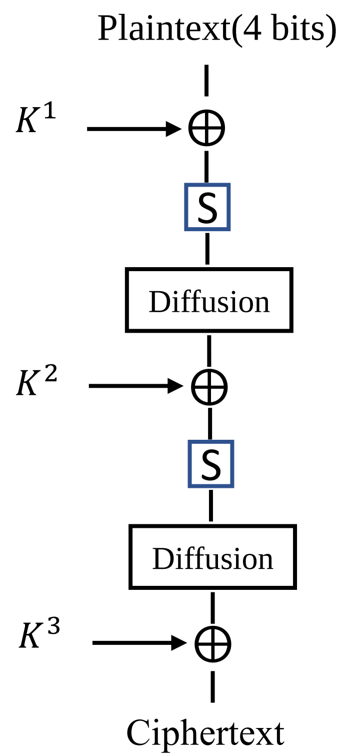
T method

Eq_1
Eq_2
.
.
Eq_{r+m+n}

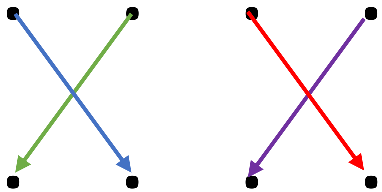
Linearisation

Gaussian elimination

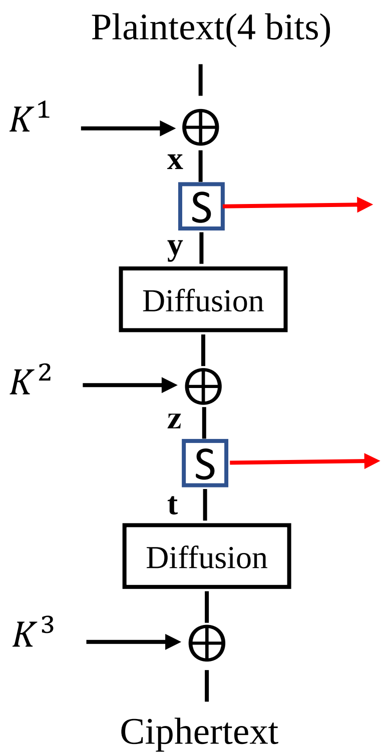
2 ROUND BABY XSL



DIFFUSION



2 ROUND BABY XSL



$$x_1 + x_2 + x_1 y_2 = 0 \longrightarrow P_1 \oplus k_1^1 + P_2 \oplus k_2^1 + P_1 y_2 \oplus k_1^1 y_2 = 0$$

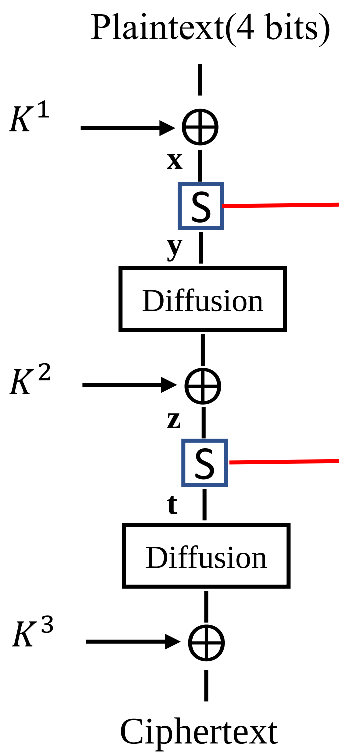
$\vdots$

$$z_1 + z_2 + z_1 t_2 = 0 \longrightarrow y_2 \oplus k_1^2 + y_1 \oplus k_2^2 + (y_2 \oplus k_1^2) * (c_1 \oplus k_2^3) = 0$$

$\vdots$

ROUND $\uparrow$ $\Longrightarrow$ # of monomials, # of variables $\uparrow$

2 ROUND BABY XSL



$x_1 + x_2 + x_1 y_2 = 0 \quad \longrightarrow \quad P_1 \oplus k_1^1 + P_2 \oplus k_2^1 + P_1 y_2 \oplus k_1^1 y_2 = 0$

$\vdots \qquad\qquad \vdots$

$z_1 + z_2 + z_1 t_2 = 0 \quad \longrightarrow \quad y_2 \oplus k_1^2 + y_1 \oplus k_2^2 + (y_2 \oplus k_1^2) * (c_1 \oplus k_2^3) = 0$

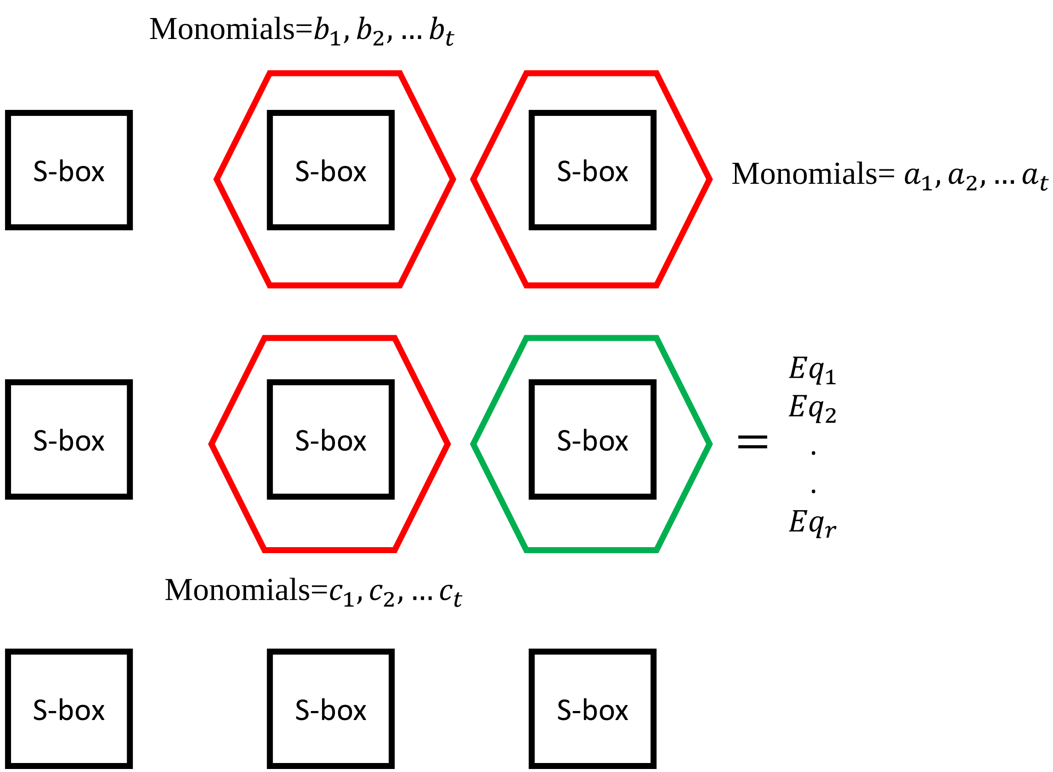
$\vdots \qquad\qquad \vdots$

2 ROUND UNKNOWS : K^1, K^2, K^3, y

3 ROUND UNKNOWS : K^1, K^2, K^3, K^4, y , t

Choose P s.t $\frac{R}{T} > 1$

Let P = 4 and S = 9



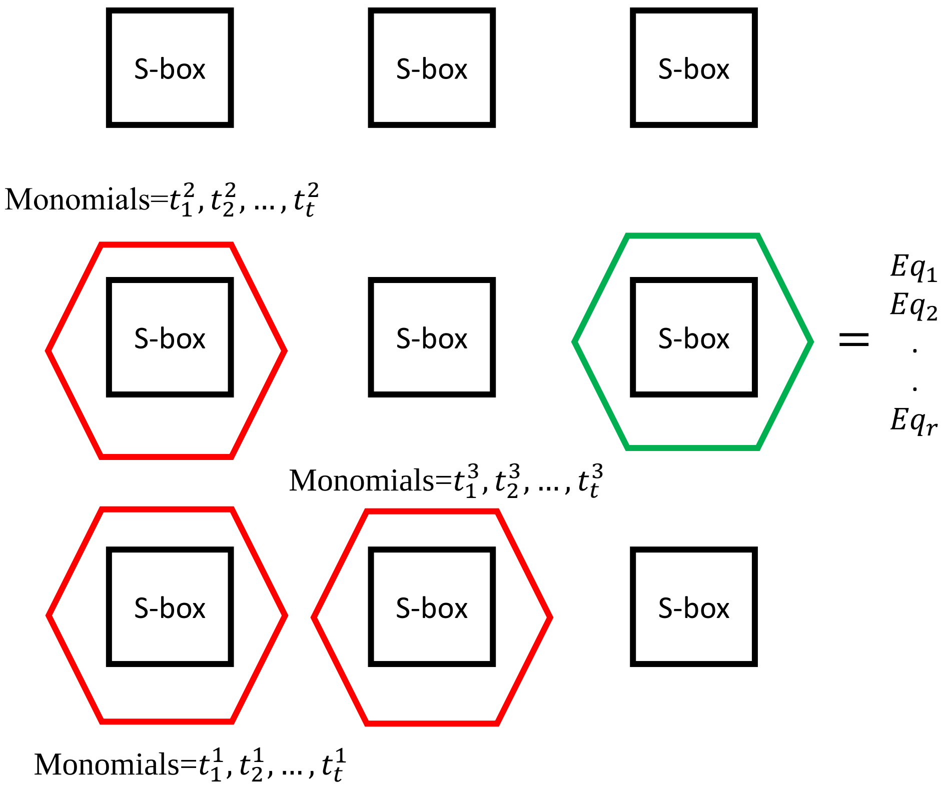
We will get:

$$Eq_1 * a_1 * b_1 * c_1$$
$$Eq_1 * a_1 * b_1 * c_2$$
$$\vdots$$
$$Eq_2 * a_1 * b_1 * c_1$$
$$\vdots$$
$$Eq_r * a_r * b_r * c_r$$

\# of equations = $r * t^{P-1}$

The XSL Attack

Let P = 4 and S = 9

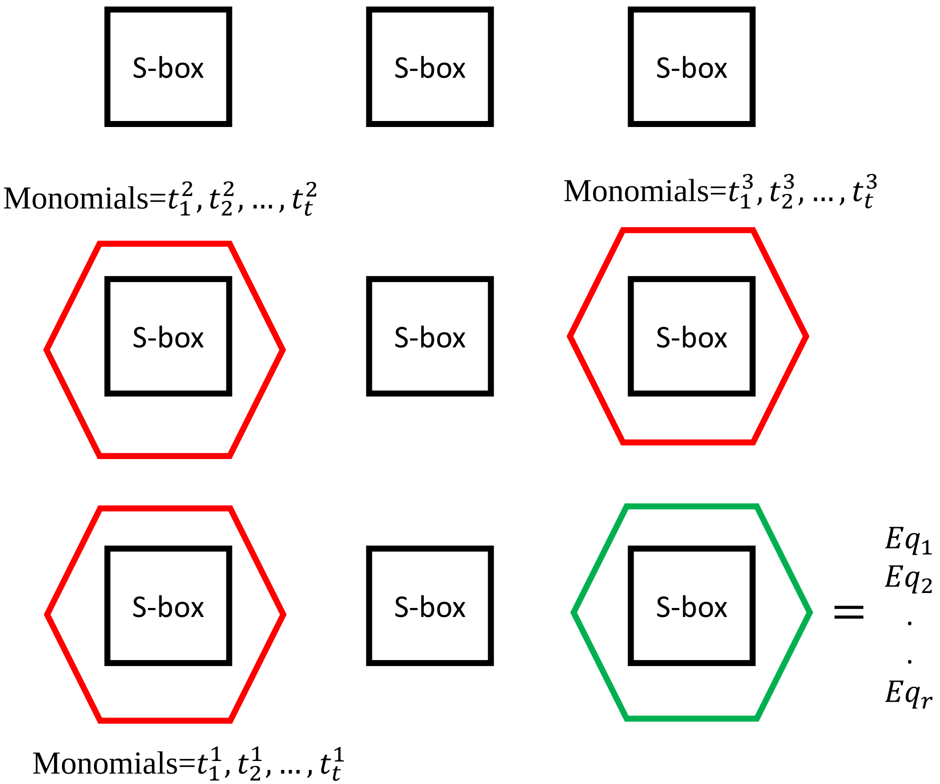


We will do for all possible P-1 passive S-box

# of equations = $r * t^{P-1}\binom{S-1}{P-1}$

The XSL Attack

Let P = 4 and S = 9



<u>We will do above process for all possible active S-box</u>

# of equations = $S * r * t^{P-1}\binom{S-1}{P-1}$

$$\mathrm{R} \approx \underbrace{\mathrm{r}}_{\text{\# of eq.}} * \underbrace{S}_{\text{\# of S-boxes}} * \underbrace{t}_{\text{\# of monomials}}^{P-1} * \binom{S-1}{P-1}$$

<u>Too much linear dependencies</u>

The XSL Attack

Let P = 2

Multiply each equation with (t-r) monomials and r equations.

$$\boxed{\text{S-box}} = \begin{matrix} Eq'_1 \\ Eq'_2 \\ \vdots \\ Eq'_r \end{matrix} \qquad \boxed{\text{S-box}} = \begin{matrix} Eq_1 \\ Eq_2 \\ \vdots \\ Eq_r \end{matrix}$$

$\longrightarrow$ Monomials = T_1 , T_2 , ... T_{t-r} ... T_t

Instead of

$$T_1 * Eq'_1 \,, T_2 * Eq'_1 \ldots \,, T_t * Eq'_1$$

Write:

$$T_1 * Eq'_1 \,, T_2 * Eq'_1 \ldots \,, T_{t-r} * Eq'_1$$

and complete with

$$Eq_1 * Eq'_1 \,, Eq_2 * Eq'_1 \ldots \,, Eq_r * Eq'_1$$

Let P = 2

Multiply each equation with (t-r) monomials and r equations.

$$\boxed{\text{S-box}} = \begin{matrix} Eq'_1 \\ Eq'_2 \\ \cdot \\ \cdot \\ Eq'_r \end{matrix} \qquad \boxed{\text{S-box}} = \begin{matrix} Eq_1 \\ Eq_2 \\ \cdot \\ \cdot \\ Eq_r \end{matrix} \rightarrow \text{Monomials} = \underbrace{T_1\,,\ T_2\,, \ldots\, T_{t-r}}_{\text{t-r}}\ \underbrace{\ldots\ T_t}_{\text{r}}$$

PROBLEM = $Eq_1 * Eq'_1$ occurs twice.

We restrict to multiplying an ”active” equation only by one of the monomials $T_1..T_{t-r}$ for some ”passive” S-box of our system, and on the other hand we also add the equations containing products of several ”active” S-boxes.

$$R \approx \sum_{i=1..P} \binom{S}{i} r^i * \binom{S-i}{P-i} (t-r)^{P-i} = \binom{S}{P} \left(t^P - (t-r)^P\right)$$

Choose i S-boxes out of S S-boxes

Multiply active S-box equations.

From remaining S-boxes, choose P-i passive S-boxes

Multiply t-r monomial of P-i passive S-boxes

For P=2 :

$$R \approx \binom{S}{1} * r * \binom{S-1}{P-1} * (t-r)^{\,p-1} + \binom{S}{2} r^2$$

For P=3 :

$$R \approx \binom{S}{1} * r * \binom{S-1}{P-1} * (t-r)^{\,p-1} + \binom{S}{2} r^2 * \binom{S-2}{P-2} * (t-r)^{\,p-2} + \binom{S}{3} r^3$$

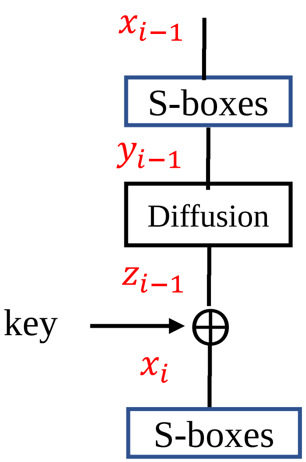
“ It seems that there are no other obvious linear dependencies”

The equations on the Diffusion Layers

We have $\boldsymbol{N_r}$**+1** known plaintexts.

For every known plaintexts

Eliminate key variables and write equations of the form:



$$X_{i\ j} \oplus \sum \alpha_j Y_{i-1\ j} = X'_{i\ j} \oplus \sum \alpha_j Y'_{i-1\ j} = X''_{i\ j} \oplus \sum \alpha_j Y''_{i-1\ j} = \ldots$$

We have $N_r * (N_r + 1) * (sB)$ such equations.

# of round

# of plaintext

Variables in each S-box of cipher round

The equations on the Diffusion Layers

Multiply these equations by products of terms for some (P-1) S-boxes.

$$X_{i\ j} \oplus \sum \alpha_j Y_{i-1\ j} = X'_{i\ j} \oplus \sum \alpha_j Y'_{i-1\ j} = X''_{i\ j} \oplus \sum \alpha_j Y''_{i-1\ j} = \ldots$$

# of new equations :

$$\boldsymbol{R' \approx N_r * (N_r + 1) * (\mathbf{sB}) * t^{P-1} * \binom{S}{P-1}}$$

# of equations after XSL

We expect that : $$\frac{R + R'}{T} > 1$$

# of monomials after XSL

IF NOT:

T method

T method

T = # of terms.

T′ = # of terms can be multiply by x_i and still belong to the set of T.

Assume we have system of 8 equations and 5 variables x_1, x_2, x_3, x_4, x_5
T' wrt. x_1
T'' wrt. x_2

Then,

$$T = \{1, x_1, x_2, x_3, x_4, x_5, x_1x_2, x_1x_3, x_1x_4, x_1x_5, x_2x_3, x_2x_4, x_2x_5, x_3x_4, x_3x_5, x_4x_5\} = 16$$

$$T' = \{1, x_1, x_2, x_3, x_4, x_5, x_1x_2, x_1x_3, x_1x_4, x_1x_5\} = 10$$

$$T'' = \{1, x_1, x_2, x_3, x_4, x_5, x_1x_2, x_2x_3, x_2x_4, x_2x_5\} = 10$$

T method

The equations from Gaussian elimination with respect to T' will be:

$$
\begin{aligned}
x_2x_3 &= x_1x_4 + x_5 + x_3 \\
x_2x_4 &= x_1x_5 + x_4 + 1 \\
x_2x_5 &= x_1x_4 + x_1x_5 + x_1 + x_3 + x_4 \\
x_3x_4 &= x_1 + x_2 + x_3 + x_4 \\
x_3x_5 &= x_1x_4 + x_2 + 1 \\
x_4x_5 &= x_1x_5 + x1 + x_2 + x_3
\end{aligned}
$$

Contains only terms in T'

$$
\left\{
\begin{aligned}
0 &= x_1x_3 + x_1x_5 + x_1 + x_2 + x_3 + x_4 \\
1 &= x_1x_2 + x_1 + x_2 + x_3 + x_4 + x_5
\end{aligned}
\right.
$$

T method

The equations from Gaussian elimination with respect to T'' will be:

$$\begin{aligned}
x_3x_4 &= x_1 + x_2 + x_3 + x_4 \\
x_3x_5 &= x_2x_4 + x_2x_5 + x_1 + x_2 + x_3 \\
x_4x_5 &= x_2x_4 + x_1 + x_2 + x_3 + x_4 + 1 \\
x_1x_3 &= x_2x_4 + x_1 + x_2 + x_3 + 1 \\
x_1x_4 &= x_2x_4 + x_2x_5 + x_1 + x_3 + 1 \\
x_1x_5 &= x_2x_4 + x_4 + 1
\end{aligned}$$

Contains only terms in T''

$$\left\{\begin{aligned}
1 &= x_1x_2 + x_1 + x_2 + x_3 + x_4 + x_5 \\
1 &= x_2x_3 + x_2x_4 + x_2x_5 + x_1 + x_5
\end{aligned}\right.$$

T method

$$0 = x_1x_3 + x_1x_5 + x_1 + x_2 + x_3 + x_4$$

$$1 = x_1x_2 + x_1 + x_2 + x_3 + x_4 + x_5$$

Multiply them with x_1:

Terms of the new eq. will be still in T.

$$0 = x_1x_2 + x_1x_4 + x_1x_5 + x_1$$

$$0 = x_1x_3 + x_1x_4 + x_1x_5$$

We have 10 linearly independent equation.

T method

$$
\begin{aligned}
0 &= x_1x_2 + x_1x_4 + x_1x_5 + x_1 \\
0 &= x_1x_3 + x_1x_4 + x_1x_5
\end{aligned}
$$

Write these 2 equations wrt. equations in T'' :

$$
\begin{aligned}
1 &= x_2x_4 + x_2x_5 + x_2 + x_4 \\
0 &= x_1x_2 + x_2x_5 + x_3 + x_4
\end{aligned}
$$

Add these equations to the equations contains only terms in T'' :

$$
\begin{aligned}
1 &= x_2x_4 + x_2x_5 + x_2 + x_4 \\
0 &= x_1x_2 + x_2x_5 + x_3 + x_4 \\
1 &= x_1x_2 + x_1 + x_2 + x_3 + x_4 + x_5 \\
1 &= x_2x_3 + x_2x_4 + x_2x_5 + x_1 + x_5
\end{aligned}
$$

$$
\begin{aligned}
1 &= x_2x_4 + x_2x_5 + x_2 + x_4 \\
0 &= x_1x_2 + x_2x_5 + x_3 + x_4 \\
1 &= x_1x_2 + x_1 + x_2 + x_3 + x_4 + x_5 \\
1 &= x_2x_3 + x_2x_4 + x_2x_5 + x_1 + x_5
\end{aligned}
$$

Multiply them with x_2:

$$
\begin{aligned}
0 &= x_2x_5 \\
0 &= x_1x_2 + x_2x_3 + x_2x_4 + x_2x_5 \\
0 &= x_2x_3 + x_2x_4 + x_2x_5 \\
0 &= x_2x_3 + x_1x_2 + x_2x_4 + x_2
\end{aligned}
$$

T method

$$
\begin{aligned}
0 &= x_2x_5 \\
0 &= x_1x_2 + x_2x_3 + x_2x_4 + x_2x_5 \\
0 &= x_2x_3 + x_2x_4 + x_2x_5 \\
0 &= x_2x_3 + x_1x_2 + x_2x_4 + x_2
\end{aligned}
$$

We have 13 equations linearly independent equation, we drop last equation it is not linearly independent.

Write these 3 equations wrt. equations in T'

T method

We will get :

$$
\begin{aligned}
1 &= x_1 + x_5 \\
1 &= x_1x_2 + x_1 + x_5 \\
0 &= x_1x_4 + x_1x_5 + x_1 + x_3 + x_4
\end{aligned}
$$

Multiply them with x_1:

$$
\begin{aligned}
0 &= x_1x_5 \\
0 &= x_1x_2 + x_1x_5 \\
0 &= x_1x_3 + x_1x_5 + x_1
\end{aligned}
$$

Unfortunately, all the new equations we get are linearly dependent with the old equations.

We stay with only 13 equations.

Example which T method fails

7 linearly independent equation with 5 variables.

$$x_1x_2 + x_1x_4 + x_2x_3 + x_2x_5 + x_4x_5 + x_1 + x_3 + x_4 + x_5 + 1 = 0$$
$$x_1x_2 + x_1x_3 + x_2x_5 + x_3x_5 + x_4x_5 + x_4 + 1 = 0$$
$$x_2x_3 + x_3x_5 + x_3x_4 + x_2 + x_3 + x_4 + x_5 + 1 = 0$$
$$x_1x_5 + x_1x_3 + x_3x_4 + x_4x_5 + x_5 = 0$$
$$x_1x_5 + x_1x_3 + x_2x_4 + x_2 + x_3 = 0$$
$$x_1x_3 + x_2x_4 + x_3x_5 + x_1 + x_2 + x_5 + 1 = 0$$
$$x_2x_5 + x_2x_3 + x_4x_5 + x_2 + x_3 + x_5 = 0$$

Example which T method fails

Represent system wrt. x_1 :

$$x_2x_3 = x_1x_3 + x_1x_4 + x_1x_5 + 1$$
$$x_2x_4 = x_1x_3 + x_1x_5 + x_2 + x_3$$
$$x_2x_5 = x_1x_3 + x_1 + x_3 + x_4$$
$$x_3x_4 = x_1x_3 + x_1x_4 + x_1 + x_2 + x_4 + 1$$
$$x_3x_5 = x_1x_5 + x_1 + x_3 + x_5 + 1$$
$$x_4x_5 = x_1x_4 + x_1x_5 + x_1 + x_2 + x_4 + x_5 + 1$$

Contains only terms in T'

$$1 = x_1x_2 + x_1x_4 + x_1 + x_2 + x_4.$$

Example which T method fails

Multiply the last equation by x_1 we have:

$$x_1 * (1 + x_1x_2 + x_1x_4 + x_1 + x_2 + x_4) = 0$$

No new equation.

Same is valid for all variables

For x_2:

$$x_1x_3 = x_2x_5 + x_1 + x_3 + x_4$$
$$x_1x_4 = x_2x_3 + x_2x_4 + x_2 + x_3 + 1$$
$$x_1x_5 = x_2x_4 + x_2x_5 + x_1 + x_2 + x_4$$
$$x_3x_4 = x_2x_3 + x_2x_4 + x_2x_5$$
$$x_3x_5 = x_2x_4 + x_2x_5 + x_2 + x_3 + x_4 + x_5 + 1$$
$$x_4x_5 = x_2x_3 + x_2x_5 + x_2 + x_3 + x_5$$

Contains only terms in T'

$$0 = x_1x_2 + x_2x_3 + x_2x_4 + x_1 + x_3 + x_4.$$

Multiply the last equation by x_2 we have:

$$x_2 \cdot (x_1x_2 + x_2x_3 + x_2x_4 + x_1 + x_3 + x_4) = 0.$$

No new equation.

T METHOD WORKING CONDITIONS

If ,

$$\boldsymbol{Free} \approx \%\, \mathbf{99.4}\, \boldsymbol{T}(\#\ \boldsymbol{of\ monomials})$$

Then

T method expected to increase # of equations.

OR

$$We\ have\ Free \geq T - T' + C\ for\ some\ C$$

If ,

$$\boldsymbol{x_i}(\boldsymbol{C}) > \boldsymbol{C}\ \textbf{for any of}\ \boldsymbol{x_i}$$

Then

T method expected to increase # of equations.

T METHOD WORKING CONDITIONS

$$We\ have\ Free\ \geq T - T' + C\ for\ some\ C$$

If ,

$$\boldsymbol{x_i(C) > C} \textbf{ for any of } \boldsymbol{x_i}$$

Then

T method expected to increase # of equations.

EX 1

Free =8
T = 16
T'= 10
For C = 1, eq. Satisfied
$x_1(C)$= 2

Satisfies the condition

EX 2

Free =7
T = 16
T'= 10
For C = 1, eq. Satisfied
$x_1(C)$= 1

Does not satisfies the condition

Attack results on AES

AES-128: The smallest P where $R + R' > T$ is $P = 7$. The parameters are $R = 4.95 \times 10^{25}$, $R' = 4.85 \times 10^{24}$, $T = 5.41 \times 10^{25}$. We have $(R + R')/T = 1.004$ and the complexity of XSL attack is $T^{2.376} \approx 2^{203}$.

AES-192: The smallest P where $R + R' > T$ is $P = 7$. The parameters are $R = 8.65 \times 10^{27}$, $R' = 8.50 \times 10^{26}$, $T = 9.46 \times 10^{27}$. We have $(R + R')/T = 1.004$ and the complexity of XSL attack is $T^{2.376} \approx 2^{221}$.

AES-256: The smallest P where $R + R' > T$ is $P = 7$. The parameters are $R = 3.15 \times 10^{28}$, $R' = 3.02 \times 10^{27}$, $T = 3.45 \times 10^{28}$. We have $(R + R')/T = 1.002$ and the complexity of XSL attack is $T^{2.376} \approx 2^{225}$.

Attack results on AES

S-box		
s	r	t
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22
3	14	22

B	Bs [bits]	N_r	H_k [bits]
4	12	1	12
4	12	2	12
4	12	3	12
4	12	4	12
4	12	5	12
4	12	6	12
4	12	7	12
4	12	8	12
4	12	9	12
4	12	10	12
4	12	11	12
4	12	12	12

Λ	S	R	R'	T	T'	$Free$	The results $\frac{Free}{T}$	$\frac{Free}{T-T'}$
1	5	3192	952	3751	912	3693	0.9845	1.3008
1	9	13104	2384	14545	1920	14184	0.9752	1.1235
1	13	29736	4584	32395	2928	31470	0.9714	1.0680
1	17	53088	7552	57301	3936	55556	0.9695	1.0411
1	21	83160	11288	89263	4944	86442	0.9684	1.0252
1	25	119952	15792	128281	5952	124128	0.9676	1.0147
1	29	163464	21064	174355	6960	168614	0.9670	1.0073
1	33	213696	27104	227485	7968	219900	0.9667	1.0017
1	37	270648	33912	287671	8976	277986	0.9663	0.9975
1	41	334320	41488	354913	9984	342872	0.9661	0.9940
1	45	404712	49832	429211	10992	414558	0.9659	0.9912
1	49	481824	58944	510565	12000	493044	0.9657	0.9889

$$\boldsymbol{\frac{Free}{R+R'}}$$

0.89

0.91

0.91

0.91

Attack results on AES

AES-128: The smallest P where $R + R' > T$ is $P = 7$. The parameters are $R = 4.95 \times 10^{25}$, $R' = 4.85 \times 10^{24}$, $T = 5.41 \times 10^{25}$. We have $(R + R')/T = 1.004$ and the complexity of XSL attack is $T^{2.376} \approx 2^{203}$.

$$\frac{Free}{T} = (4.95 \times 10^{25} + 4.85 \times 10^{24}) \times \frac{0.9}{5.41 \times 10^{25}} \approx 0.904$$

“XSL is not an attack, it is a dream”

Vincent Rijmen, AES designer

“ XSL may be a dream. It may also be a very bad dream and turn into a nightmare”

Nicolas T. Courtois, Founder of XSL

References

1. Courtois, N., Pieprzyk, J.: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Cryptology ePrint Archive, Report 2002/044 (2002)

2. Cid C., Leurent G. (2005) An Analysis of the XSL Algorithm. In: Roy B. (eds) Advances in Cryptology - ASIACRYPT 2005. ASIACRYPT 2005. Lecture Notes in Computer Science, vol 3788. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11593447_18

3. Cui, Jie & Zhong, Hong & Wang, Jiankai & Shi, Run-hua. (2014). Generation and Optimization of Rijndael S-box Equation System. Information Technology Journal. 13. 2482-2488. 10.3923/itj.2014.2482.2488.

4. Lim, C., & Khoo, K. (2007). An Analysis of XSL Applied to BES. FSE.