Modelling Ciphers with Overdefined Systems of Quadratic Equations: Application to Friday, Vision, RAIN and Biscuit

Fukang Liu, Mairon Mahzoun, Willi Meier

東京工業大学
Tokyo Institute of Technology

3MI LABS

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

n|w University of Applied Sciences and Arts Northwestern Switzerland

Motivation

Algebraic Attacks

- Model the primitive with n variables and $m \geq n$ equations.
- Find information about secrets by solving the system.
    - Gröbner Basis

$$O\left(\binom{n+D}{D}^{\omega}\right)$$

$$D_{m,n} = \left[\frac{\prod_{i=1}^{m}\left(1-x^{d_i}\right)}{(1-x)^n}\right]_+$$

Larger m (more equations) $\Rightarrow$ Smaller $D_{m,n}$ (easier to solve)

Example: AES

State:

$$\mathbf{S} = \begin{bmatrix} M_0 & M_1 & M_2 & M_3 \\ M_4 & M_5 & M_6 & M_7 \\ M_8 & M_9 & M_{10} & M_{11} \\ M_{12} & M_{13} & M_{14} & M_{15} \end{bmatrix}$$

Round Function:

SubBytes:

$$\text{S-box}(M_i) = \begin{cases} \mathcal{A}_8(0) & \text{if } M_i = 0, \\ \mathcal{A}_8\left(M_i^{-1}\right) & \text{otherwise.} \end{cases}$$

MixColumns:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} M_i \\ M_{i+4} \\ M_{i+8} \\ M_{i+12} \end{bmatrix} = \begin{bmatrix} M'_i \\ M'_{i+4} \\ M'_{i+8} \\ M'_{i+12} \end{bmatrix} \qquad 0 \leq i \leq 3$$

ShiftRows:

$$\begin{bmatrix} M_0 & M_1 & M_2 & M_3 \\ M_4 & M_5 & M_6 & M_7 \\ M_8 & M_9 & M_{10} & M_{11} \\ M_{12} & M_{13} & M_{14} & M_{15} \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} M_0 & M_1 & M_2 & M_3 \\ M_5 & M_6 & M_7 & M_4 \\ M_{10} & M_{11} & M_8 & M_9 \\ M_{15} & M_{12} & M_{13} & M_{14} \end{bmatrix}$$

AddRoundKey

$$\begin{bmatrix} M_0 & M_1 & M_2 & M_3 \\ M_4 & M_5 & M_6 & M_7 \\ M_8 & M_9 & M_{10} & M_{11} \\ M_{12} & M_{13} & M_{14} & M_{15} \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} M_0 \oplus K_0 & M_1 \oplus K_1 & M_2 \oplus K_2 & M_3 \oplus K_3 \\ M_4 \oplus K_4 & M_5 \oplus K_5 & M_6 \oplus K_6 & M_7 \oplus K_7 \\ M_8 \oplus K_8 & M_9 \oplus K_9 & M_{10} \oplus K_{10} & M_{11} \oplus K_{11} \\ M_{12} \oplus K_{12} & M_{13} \oplus K_{13} & M_{14} \oplus K_{14} & M_{15} \oplus K_{15} \end{bmatrix}$$

Over-determine AES

Courtois-Pieprzyk's Algebraic Modelling

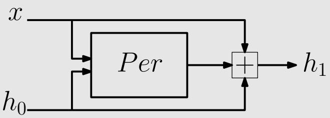
$$x = y^{-1} \quad \Rightarrow \quad xy = 1,\ x^2y = x,\ xy^2 = y,\ x^4y = x^3,\ xy^4 = y^3$$

Murphy-Robshaw's Algebraic Modelling

$$\begin{cases} (xy)^{2^i} = 1, \rightarrow x_i y_i = 1 \\ (x^2y)^{2^i} = x^{2^i} \rightarrow x_{(i+1)\%\ell} y_i = x_i, \\ (xy^2)^{2^i} = y^{2^i} \rightarrow x_i y_{(i+1)\%\ell} = y_i,, \\ (x^4y)^{2^i} = (x^3)^{2^i} \rightarrow x_{(i+2)\%\ell} y_i = x_i x_{(i+1)\%\ell}, \\ (xy^4)^{2^i} = (y^3)^{2^i} \rightarrow x_i y_{(i+2)\%\ell} = y_i y_{(i+1)\%\ell}, \end{cases} \quad \text{for } \forall i \in [0, \ell - 1]. \qquad (1)$$

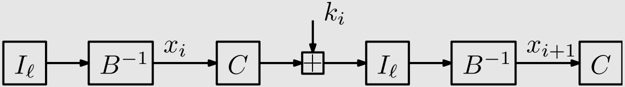
Friday

Goal



Goal: Given (h_0, h_1), find x such that $Per(x, h_0) + x + h_0$.

Per



$$
\begin{aligned}
\forall i \in [1, r-1] : (C(x_i) + k_i) \cdot B(x_{i+1}) &= 1, \\
B(x_1) \cdot (C(x_r) + k_r + h_1 + h_0) &= 1,
\end{aligned}
$$

$$\xrightarrow{\text{Expanding } B, C}$$

$$(y^4 + c_2 y^2 + c_1 y + \beta_1)(z^4 + b_2 z^2 + b_1 z + \beta_2) = 1,$$

Friday

Polynomial System

New variables:

$$\forall i \in [0, i_\ell] : \; y_i = y^{2^i}, \; z_i = z^{2^i}.$$

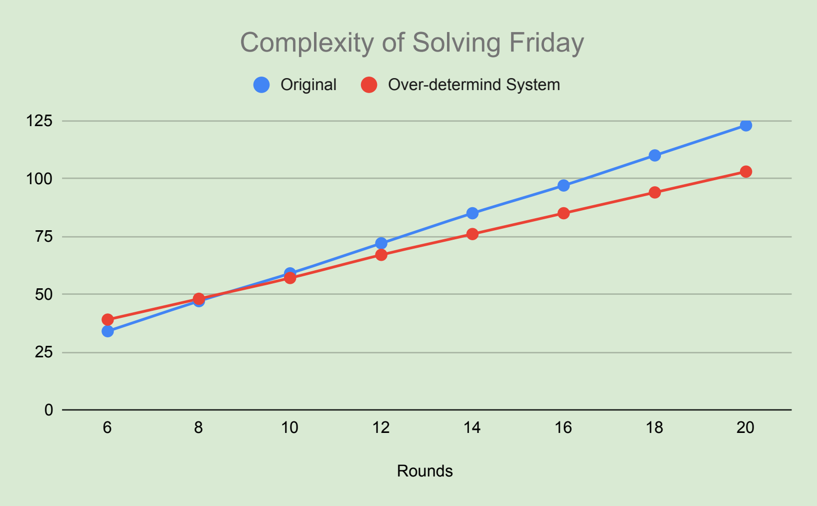
New system:

$(y_2 + c_2 y_1 + c_1 y_0 + \beta_1)(z_2 + b_2 z_1 + b_1 z_0 + \beta_2)$ $= 1$	$(y_2 + c_2 y_1 + c_1 y_0 + \beta_1)^2 (z_2 + b_2 z_1 + b_1 z_0 + \beta_2)$ $= (y_3 + c_2^2 y_2 + c_1^2 y_1 + \beta_1^2)(z_2 + b_2 z_1 + b_1 z_0 + \beta_2)$ $= (y_2 + c_2 y_1 + c_1 y_0 + \beta_1)$
$(y_2 + c_2 y_1 + c_1 y_0 + \beta_1)(z_2 + b_2 z_1 + b_1 z_0 + \beta_2)^2$ $= (y_2 + c_2 y_1 + c_1 y_0 + \beta_1)(z_3 + b_2^2 z_2 + b_1^2 z_1 + \beta_2^2)$ $= (z_2 + b_2 z_1 + b_1 z_0 + \beta_2)$	$(y_2 + c_2 y_1 + c_1 y_0 + \beta_1)^2 (z_2 + b_2 z_1 + b_1 z_0 + \beta_2)^2$ $= (y_3 + c_2^2 y_2 + c_1^2 y_1 + \beta_1^2)(z_3 + b_2^2 z_2 + b_1^2 z_1 + \beta_2^2)$ $= 1$

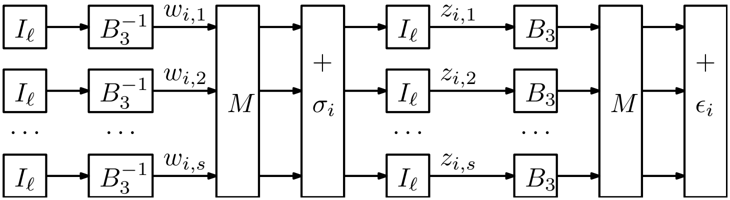
New vs. Old system

$\frac{r}{2}$ variables and equations $\Rightarrow 4r$ variable and $7r$ equtions.

Friday


Complexity of Solving Friday
Original
Over-determind System
125
100
75
50
25
0
6
8
10
12
14
16
18
20
Rounds

Vision



$$B_3(v_1) \cdot \left(\alpha_1 B_3(u_1) + \ldots + \alpha_s B_3(u_s) + \beta_4 \right) = 1, \tag{2}$$

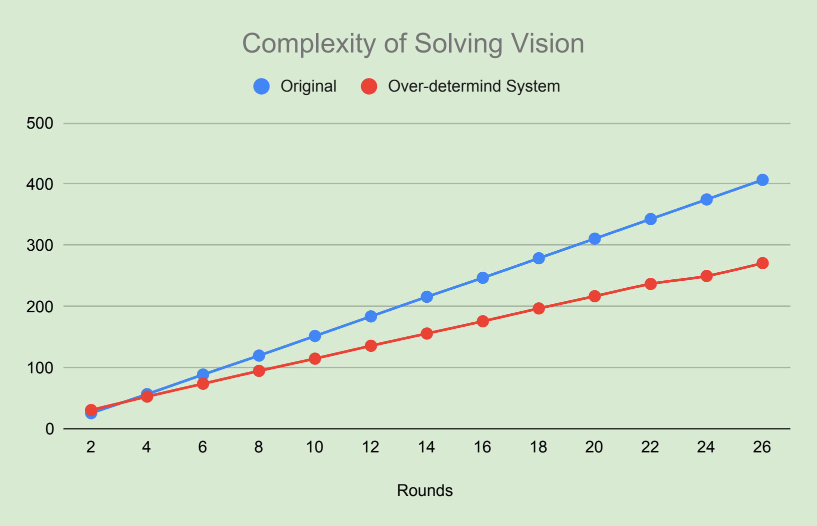
$$(\lambda_3 v_{1,2} + \lambda_2 v_{1,1} + \lambda_1 v_{1,0} + \lambda_0)(\sum_{j=1}^{s} \sum_{i=0}^{2} \lambda_{j,i} u_{j,i} + \beta_5) = 1,$$

Vision

$$u_1 \cdot \left(\alpha_1 v_1 + \ldots + \alpha_s v_s + \beta_6\right) = 1,$$

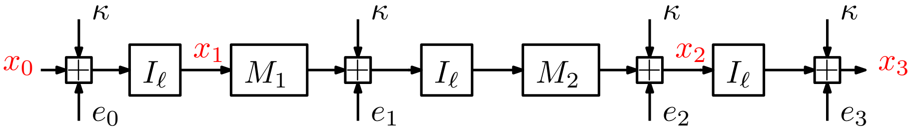
$$\begin{cases} u_1 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6) = 1, \\ {u_1}^2 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^2 = 1, \\ {u_1}^4 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^4 = 1, \\ {u_1}^2 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6) = u_1, \\ {u_1}^4 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^2 = {u_1}^2, \\ u_1 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^2 = \alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6, \\ {u_1}^2 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^4 = (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^2, \\ {u_1}^4 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6) = {u_1}^2 \cdot u_1, \\ u_1 \cdot (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^4 = (\alpha_1 v_{1,0} + \ldots + \alpha_s v_{s,0} + \beta_6)^{2+1}. \end{cases}$$

Vision



Complexity of Solving Vision
Original
Over-determind System
500
400
300
200
100
0
2
4
6
8
10
12
14
16
18
20
22
24
26
Rounds

RAIN



$$\begin{cases} x_1 \cdot (x_0 + \kappa + e_0) = 1, \\ M_2^{-1}(x_2 + \kappa + e_2) \cdot (M_1(x_1) + \kappa + e_1) = 1, \\ x_2 \cdot (x_3 + \kappa + e_3) = 1, \end{cases}$$

Define 3ℓ variables. $15\ell + 3\ell = 18\ell$ equations.

RAIN

Extra 5ℓ equations:

$$\begin{cases} x_1 + x_2 + \theta x_1 x_2 = 0. \\ x_1^2 + x_1 x_2 + \theta x_1^2 x_2 = 0, \\ x_1 x_2 + x_2^2 + \theta x_1 x_2^2 = 0. \\ (\theta x_1^3 + x_1^2)(x_1 + x_2 + \theta x_1 x_2) = \theta x_1^4 + \theta^2 x_1^4 x_2 + x_1^3 + x_1^2 x_2 = 0, \\ (\theta x_2^3 + x_2^2)(x_1 + x_2 + \theta x_1 x_2) = \theta x_2^4 + \theta^2 x_1 x_2^4 + x_1 x_2^2 + x_2^3 = 0. \end{cases}$$

Rounds (N)	ℓ	#variables	#equations	D_{reg}	Complexity
3	128	384	2944	11	139 (195)
	192	576	4416	15	196 (274)
	256	768	5888	19	252 (352)

Biscuit

Problem *PowAff*$_2$

$$f_i(\overline{X}) = d_i + A_i \cdot \overline{X} + B_i \cdot \overline{X} \times C_i \cdot \overline{X}$$

Modeling *PowAff*$_2$

$$\begin{cases} d_i + A_i \cdot \overline{X} + B_i \cdot \overline{X} \times C_i \cdot \overline{X} = 0, \\ B_i \cdot \overline{X} \times \left(d_i + A_i \cdot \overline{X}\right) + B_i^2 \cdot \overline{X} \times C_i \cdot \overline{X} = 0, \\ C_i \cdot \overline{X} \times \left(d_i + A_i \cdot \overline{X}\right) + B_i \cdot \overline{X} \times C_i^2 \cdot \overline{X} = 0, \\ d_i^2 + A_i^2 \cdot \overline{X} + B_i^2 \cdot \overline{X} \times C_i^2 \cdot \overline{X} = 0. \end{cases} \tag{3}$$

Complexity

Security	(n, m)	#variables	#equations	D_{sol}	Complexity
128	$(50, 52)$	100	258	11	98
192	$(89, 92)$	178	457	16	153
256	$(127, 130)$	254	647	22	215

Conclusion

Summary

- Friday: $7r$ equations in $4r$ variables.
- Vision: $5s + 14s(r-1)$ equations in $3s + 6s(r-1)$ variables.
- RAIN: $(5r+5)\ell$ equations in $r\ell$ variables.
- Biscuit: $4m+n$ quadratic equations in $2n$ variables.

Open Problems

- Tighter lower bounds for complexities.
- Effect of syzygy relations of added polynomials in higher degrees.

Thank you for your attention.