Cryptanalysis Using Constraint Programming

Hosein Hadipour

TU Wien - Vienna, Austria

› hossein.hadipour@iaik.tugraz.at

Outline

1 Background
- Cryptanalysis
- Constraint Programming (CP)

2 Autoguess
- Guess-and-Determine (GD)
- Converting GD to a CP Problem
- Some Applications of Autoguess

3 Conclusion and Our Other Contributions

Background

Hosein Hadipour
TU Wien - Vienna, Austria

Cryptanalysis

- Complexity-theoretic approach (Public-Key primitives)
- Cryptanalytic approach (Symmetric-Key primitives)
  - Differential attack [BS90]
  - Linear attack [Mat93]
  - Boomerang attack [Wag99]
  - Differential-Linear attack [LH94]
  - Impossible-Differential attack [Knu98; BBS99]
  - Integral attack [Lai94; DKR97]
  - Cube attack [DS09]

Cryptanalysis

- Complexity-theoretic approach (Public-Key primitives)
- Cryptanalytic approach (Symmetric-Key primitives)
  - Differential attack [BS90]
  - Linear attack [Mat93]
  - Boomerang attack [Wag99]
  - Differential-Linear attack [LH94]
  - Impossible-Differential attack [Knu98; BBS99]
  - Integral attack [Lai94; DKR97]
  - Cube attack [DS09]

Automated Methods in Cryptanalysis

Mounting cryptanalytic attacks against symmetric-key primitives:

- requires tracing the propagation of a certain property at the bit-level
- implies solving a hard combinatorial optimization problem
- is very time-consuming
- is potentially an error-prone process

Automated Methods in Cryptanalysis

Getting the help or using of machines to find, build or optimize the attacks

Hosein Hadipour
TU Wien - Vienna, Austria

Different Approaches for Automatic Cryptanalysis

- Dedicated algorithms
- Constraint Programming (CP)
  - CP
  - MILP
  - SAT
  - SMT
- Artificial Intelligence (AI)

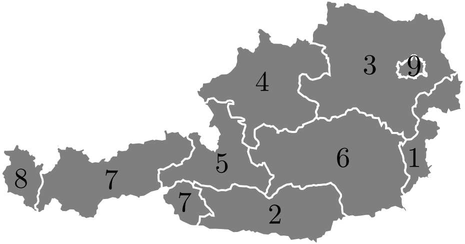
Hosein Hadipour
TU Wien - Vienna, Austria

Constraint Programming (CP)

- Constraint Satisfaction/Optimization Problem (CSP/COP):
  - We define a set of variables: $\mathcal{X} = \{\mathcal{X}_1, \ldots, \mathcal{X}_n\}$
  - We specify the domain of each variable: $\mathbb{F}_2, \mathbb{Z}, \mathbb{R}, \ldots$
  - We define a set of constraints: $\mathcal{C} = \{\mathcal{C}_1, \ldots, \mathcal{C}_2\}$
  - We define an objective function (if it is required)
- Constraint Programming (CP): Searching for a solution for a CSP/COP
- MILP and SAT are special cases of CP

Hosein Hadipour
TU Wien - Vienna, Austria

Constraint Programming – Example

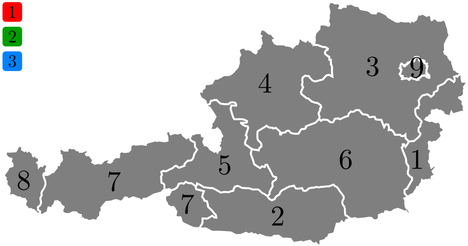



```
int: nc = 3;
array[1..9] of var 1..nc: r;
constraint r[1] != r[3]; constraint r[1] != r[6];
constraint r[2] != r[5]; constraint r[2] != r[6];
constraint r[2] != r[7]; constraint r[3] != r[9];
constraint r[3] != r[6]; constraint r[3] != r[4];
constraint r[4] != r[6]; constraint r[4] != r[5];
constraint r[5] != r[6]; constraint r[5] != r[7];
constraint r[7] != r[8];
solve satisfy;

r = [3, 3, 2, 3, 2, 1, 1, 2, 1];
```


Hosein Hadipour
TU Wien - Vienna, Austria

Constraint Programming – Example

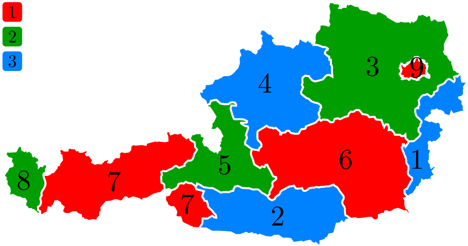



```
int: nc = 3;
array[1..9] of var 1..nc: r;
constraint r[1] != r[3]; constraint r[1] != r[6];
constraint r[2] != r[5]; constraint r[2] != r[6];
constraint r[2] != r[7]; constraint r[3] != r[9];
constraint r[3] != r[6]; constraint r[3] != r[4];
constraint r[4] != r[6]; constraint r[4] != r[5];
constraint r[5] != r[6]; constraint r[5] != r[7];
constraint r[7] != r[8];
solve satisfy;
```

```
r = [3, 3, 2, 3, 2, 1, 1, 2, 1];
```


Hosein Hadipour
TU Wien - Vienna, Austria

Constraint Programming – Example




```
int: nc = 3;
array[1..9] of var 1..nc: r;
constraint r[1] != r[3]; constraint r[1] != r[6];
constraint r[2] != r[5]; constraint r[2] != r[6];
constraint r[2] != r[7]; constraint r[3] != r[9];
constraint r[3] != r[6]; constraint r[3] != r[4];
constraint r[4] != r[6]; constraint r[4] != r[5];
constraint r[5] != r[6]; constraint r[5] != r[7];
constraint r[7] != r[8];
solve satisfy;

r = [3, 3, 2, 3, 2, 1, 1, 2, 1];
```


Hosein Hadipour
TU Wien - Vienna, Austria

Autoguess

Guess-and-Determine (GD)

Guess-and-Determine

Given a set of variables and a set of relations between them, find the smallest subset of variables guessing the value of which uniquely determines the value of the remaining variables.

Hosein Hadipour
TU Wien - Vienna, Austria

Guess-and-Determine (GD)

Guess-and-Determine

Given a set of variables and a set of relations between them, find the smallest subset of variables guessing the value of which uniquely determines the value of the remaining variables.

Example

- $u, \ldots, z \in \mathbb{F}_2^{32}$
- F, G, H: bijective functions
- $c_1, \ldots, c_5$: constants

$$
\begin{cases}
F(u + v) \oplus G(x) \oplus y \oplus (z \lll 7) & = c_1 \\
G(u \oplus w) + (y \lll 3) + z & = c_2 \\
F(w \oplus x) + y \oplus z & = c_3 \\
F(u) \oplus G(w + z) & = c_4 \\
(F(u) \times G(w \lll 7)) + H(z \oplus v) & = c_5
\end{cases}
$$

Hosein Hadipour
TU Wien - Vienna, Austria

Guess-and-Determine (GD)

Guess-and-Determine

Given a set of variables and a set of relations between them, find the smallest subset of variables guessing the value of which uniquely determines the value of the remaining variables.

Example

- Guess w, z
- Determine u (4), y (2)
- Determine x (3), v (5)

$$
\begin{cases}
F(u + v) \oplus G(x) \oplus y \oplus (z \lll 7) & = c_1 \\
G(u \oplus w) + (y \lll 3) + z & = c_2 \\
F(w \oplus x) + y \oplus z & = c_3 \\
F(u) \oplus G(w + z) & = c_4 \\
(F(u) \times G(w \lll 7)) + H(z \oplus v) & = c_5
\end{cases}
$$

Hosein Hadipour
TU Wien - Vienna, Austria

Symmetric and Implication Relations

Assumption: Relations are symmetric or implication

- **Implication relations**: $x_1, \ldots, x_n \Rightarrow y$
- **Symmetric relations**: $[x_1, \ldots, x_n]$

Example

Assume that $x, y, z, k \in \mathbb{F}_2^{32}$, and $F : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$ is bijective:

$z = x \times y$	$z = F(x + k) \oplus y$
$x, y \Rightarrow z$	$[x, y, z, k]$

Hosein Hadipour
TU Wien - Vienna, Austria

System of Equations

$$E : \begin{cases} e_1 : F(u + v) \oplus G(x) \oplus y \oplus (z \lll 7) & = c_1 \\ e_2 : G(u \oplus w) + (y \lll 3) + z & = c_2 \\ e_3 : F(w \oplus x) + y \oplus z & = c_3 \\ e_4 : F(u) \oplus G(w + z) & = c_4 \\ e_5 : (F(u) \times G(w \lll 7)) + H(z \oplus v) & = c_5 \end{cases}$$

$$X = \{u, v, w, x, y, z\}, \;\; E = \{e_1, \ldots, e_5\}$$

$$\mathcal{R} : \begin{cases} r_1 : [u, v, x, y, z], & r_2 : [u, w, y, z] \\ r_3 : [w, x, y, z], & r_4 : [u, w, z] \\ r_5 : u, w \Rightarrow t, & r_6 : [t, z, v] \end{cases}$$

$$\mathcal{X} = \{u, v, w, x, y, z, t\}, \;\; \mathcal{R} = \{r_1, \ldots, r_6\}$$

Hosein Hadipour
TU Wien - Vienna, Austria

System of Equations $\Rightarrow$ System of Relations

$$
E : \begin{cases}
e_1 : F(u+v) \oplus G(x) \oplus y \oplus (z \lll 7) & = c_1 \\
e_2 : G(u \oplus w) + (y \lll 3) + z & = c_2 \\
e_3 : F(w \oplus x) + y \oplus z & = c_3 \\
e_4 : F(u) \oplus G(w+z) & = c_4 \\
e_5 : (F(u) \times G(w \lll 7)) + H(z \oplus v) & = c_5
\end{cases}
$$

$$X = \{u, v, w, x, y, z\},\ E = \{e_1, \ldots, e_5\}$$

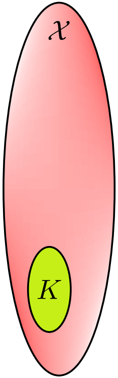
$$
\mathcal{R} : \begin{cases}
r_1 : [u, v, x, y, z], & r_2 : [u, w, y, z] \\
r_3 : [w, x, y, z], & r_4 : [u, w, z] \\
r_5 : u, w \Rightarrow t, & r_6 : [t, z, v]
\end{cases}
$$

$$\mathcal{X} = \{u, v, w, x, y, z, t\},\ \mathcal{R} = \{r_1, \ldots, r_6\}$$

Hosein Hadipour
TU Wien - Vienna, Austria

Knowledge Propagation

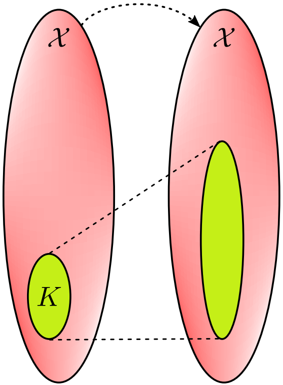
- $(\mathcal{X}, \mathcal{R})$
- $K \subseteq \mathcal{X}$
- K is initially known
- K is known



Hosein Hadipour
TU Wien - Vienna, Austria

Knowledge Propagation

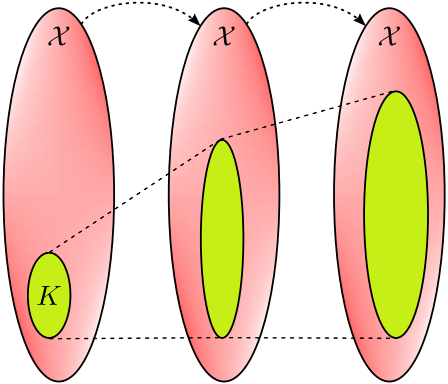
- $(\mathcal{X}, \mathcal{R})$
- $K \subseteq \mathcal{X}$
- K is initially known
- K is known



Hosein Hadipour
TU Wien - Vienna, Austria

Knowledge Propagation

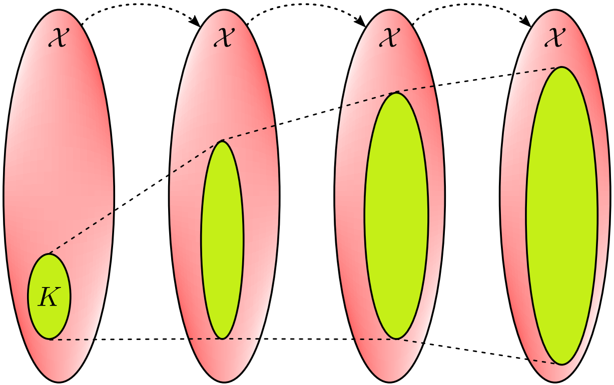
- $(\mathcal{X}, \mathcal{R})$
- $K \subseteq \mathcal{X}$
- K is initially known
- K is known



Hosein Hadipour
TU Wien - Vienna, Austria

Knowledge Propagation

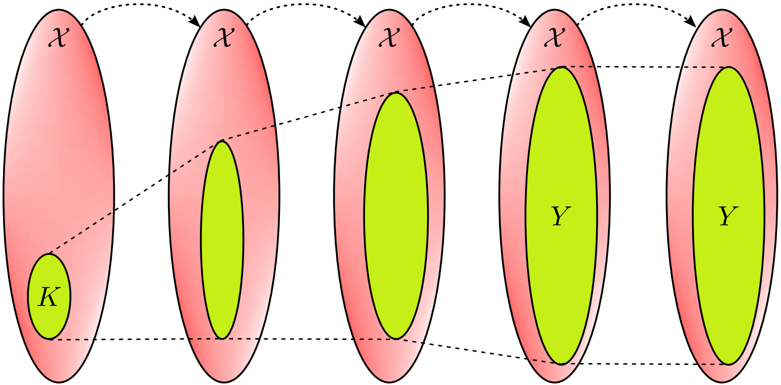
- $(\mathcal{X}, \mathcal{R})$
- $K \subseteq \mathcal{X}$
- K is initially known
- K is known



Hosein Hadipour
TU Wien - Vienna, Austria

Knowledge Propagation

- $(\mathcal{X}, \mathcal{R})$
- $K \subseteq \mathcal{X}$
- K is initially known
- K is known

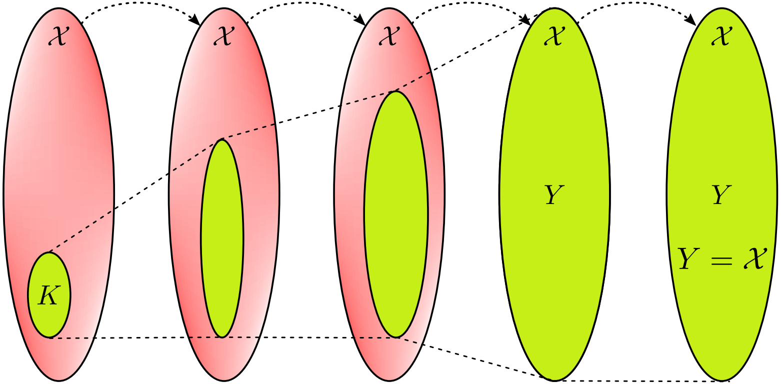


$Y = \texttt{Propagate}(K)$

Hosein Hadipour
TU Wien - Vienna, Austria

Knowledge Propagation

- $(\mathcal{X}, \mathcal{R})$
- $K \subseteq \mathcal{X}$
- K is initially known
- K is known



If $\mathcal{X} = \texttt{Propagate}(K)$, then K is a *Guess Basis*

Hosein Hadipour
TU Wien - Vienna, Austria

Naive Approach for GD

Given a system of relations $(\mathcal{X}, \mathcal{R})$, where $|\mathcal{X}| = n$, is there any guess basis of size $\leq m$?

Brute-force

- For $k = 1 \to m$
  - For each subset $K \subseteq \mathcal{X}$, where $|K| = k$:
    - If $\texttt{Propagate(K)} = \mathcal{X}$ then return K

- Time complexity $\approx \sum_{k=1}^{m} \binom{n}{k}$
- Exponential with respect to both n and m

Hosein Hadipour
TU Wien - Vienna, Austria

Naive Approach for GD

Given a system of relations $(\mathcal{X}, \mathcal{R})$, where $|\mathcal{X}| = n$, is there any guess basis of size $\leq m$?

Brute-force

- For $k = 1 \to m$
  - For each subset $K \subseteq \mathcal{X}$, where $|K| = k$:
    - If $\texttt{Propagate(K)} = \mathcal{X}$ then return K

- Time complexity $\approx \sum_{k=1}^{m} \binom{n}{k}$
- Exponential with respect to both n and m

Hosein Hadipour
TU Wien - Vienna, Austria

Naive Approach for GD

Given a system of relations $(\mathcal{X}, \mathcal{R})$, where $|\mathcal{X}| = n$, is there any guess basis of size $\leq m$?

Brute-force

- For $k = 1 \to m$
  - For each subset $K \subseteq \mathcal{X}$, where $|K| = k$:
    - If $\texttt{Propagate(K)} = \mathcal{X}$ then return K

- Time complexity $\approx \sum_{k=1}^{m} \binom{n}{k}$
- Exponential with respect to both n and m

Hosein Hadipour
TU Wien - Vienna, Austria

CP-Based Approach to Solve GD Problem

1. Convert the system of equations to a system of relations
   - We can apply a preprocessing step here (Gaussian elimination)
2. Convert the problem of finding a minimal guess basis to a CP problem
3. Employ the state-of-the-art CP solvers to solve the problem

Hosein Hadipour
TU Wien - Vienna, Austria

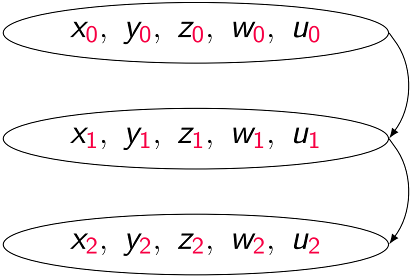
Convert GD to a CP Problem

$$r_0 : [\ x, y, z]$$
$$r_1 : [z, w, y]$$
$$r_2 : [w, x, u]$$

Hosein Hadipour
TU Wien - Vienna, Austria

Convert GD to a CP Problem

$$r_0 : [\,x, y, z]$$
$$r_1 : [z, w, y]$$
$$r_2 : [w, x, u]$$



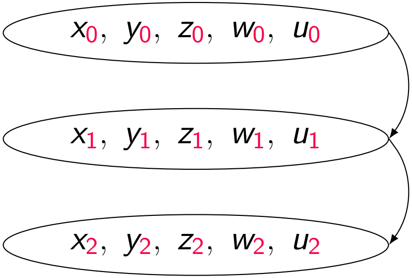
- Fix the number of steps in knowledge propagation
- $X = \{\, x_i, y_i, z_i, w_i, u_i : 0 \leq i \leq 2\}$
- $x_i = 1$ iff x is known after the ith step of knowledge propagation, otherwise $x_i = 0$
- Initialize the set of constraints: $\mathcal{C} \leftarrow \emptyset$

Hosein Hadipour
TU Wien - Vienna, Austria

Convert GD to a CP Problem

$$r_0 : [x, y, z]$$
$$r_1 : [z, w, y]$$
$$r_2 : [w, x, u]$$

$$X \leftarrow X \cup \{x_{0,0}, x_{0,1}\}$$
$$\mathcal{C} \leftarrow \mathcal{C} \cup \{x_{0,0} = y_0 \wedge z_0\}$$
$$\mathcal{C} \leftarrow \mathcal{C} \cup \{x_{0,1} = w_0 \wedge u_0\}$$
$$\mathcal{C} \leftarrow \mathcal{C} \cup \{x_1 = x_{0,0} \vee x_{0,1}\}$$



Hosein Hadipour
TU Wien - Vienna, Austria

Convert GD to a CP Problem

$r_0 : [\,x, y, z]$

$r_1 : [z, w, y]$

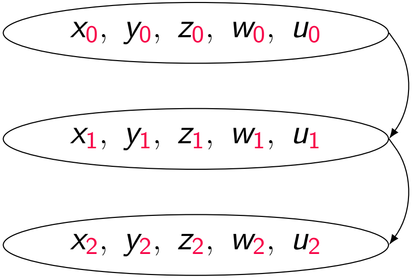
$r_2 : [w, x, u]$

$X \leftarrow X \cup \{\, y_{0,0}, \; y_{0,1} \}$

$\mathcal{C} \leftarrow \mathcal{C} \cup \{ y_{0,0} = x_0 \wedge z_0 \}$

$\mathcal{C} \leftarrow \mathcal{C} \cup \{ y_{0,1} = z_0 \wedge w_0 \}$

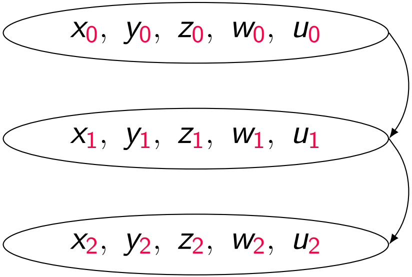
$\mathcal{C} \leftarrow \mathcal{C} \cup \{ y_1 = y_{0,0} \vee y_{0,1} \}$



Hosein Hadipour
TU Wien - Vienna, Austria

Convert GD to a CP Problem

$$r_0 : [\, x, y, z]$$
$$r_1 : [z, w, y]$$
$$r_2 : [w, x, u]$$



- Do it for all variables and in each step
- All variables should be known at the last step:

$$\mathcal{C} \leftarrow \mathcal{C} \cup \{x_2 \wedge y_2 \wedge z_2 \wedge w_2 \wedge u_2 = 1\}$$

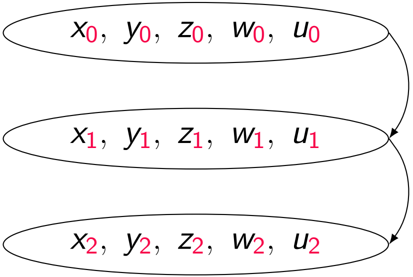
Hosein Hadipour
TU Wien - Vienna, Austria

Convert GD to a CP Problem

$r_0 : [\, x, y, z]$

$r_1 : [z, w, y]$

$r_2 : [w, x, u]$



$$\min \; x_0 + y_0 + z_0 + w_0 + u_0$$
$$s.t. \text{ all constraints in } \mathcal{C} \text{ are satisfied}$$

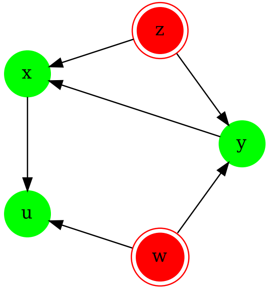
Hosein Hadipour
TU Wien - Vienna, Austria

Convert GD to a CP Problem

$r_0 : [\, x, y, z]$

$r_1 : [z, w, y]$

$r_2 : [w, x, u]$

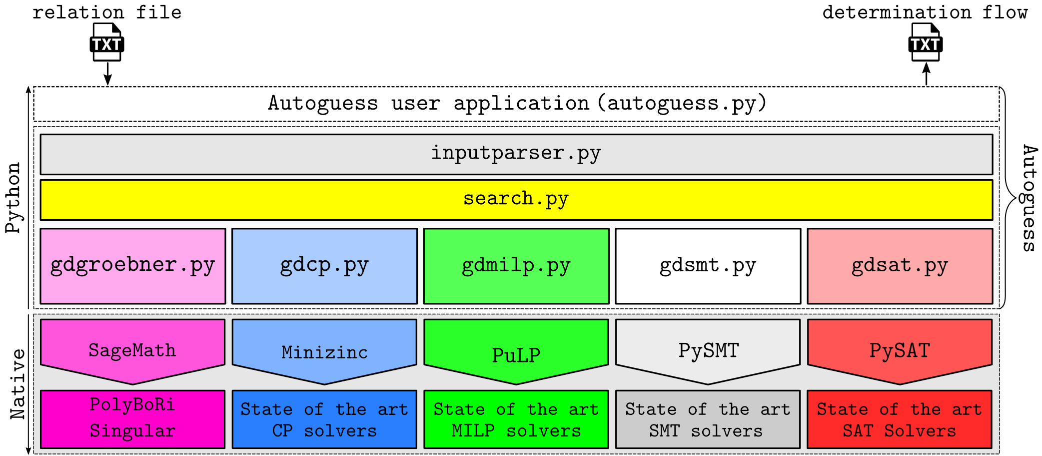


$$\min\ x_0 + y_0 + z_0 + w_0 + u_0$$

$s.t.$ all constraints in $\mathcal{C}$ are satisfied

Hosein Hadipour
TU Wien - Vienna, Austria

Autoguess



: https://github.com/hadipourh/autoguess

Hosein Hadipour
TU Wien - Vienna, Austria

Autoguess - Simple User Interface

$$\begin{cases} F(u+v) \oplus G(x) \oplus y \oplus (z \lll 7) & = c_1 \\ G(u \oplus w) + (y \lll 3) + z & = c_2 \\ F(w \oplus x) + y \oplus z & = c_3 \\ F(u) \oplus G(w+z) & = c_4 \\ (F(u) \times G(w \lll 7)) + H(z \oplus v) & = c_5 \end{cases}$$

Hosein Hadipour
TU Wien - Vienna, Austria

Autoguess - Simple User Interface

Input file (`relations.txt`):

```
# Comments
connection relations
u, v, x, y, z
u, w, y, z
w, x, y, z
u, w, z
u, w => t
t, z, v
end
```

Run Autoguess:

```
python3 autoguess.py -i relations.txt --maxsteps 5 --solver cp
```

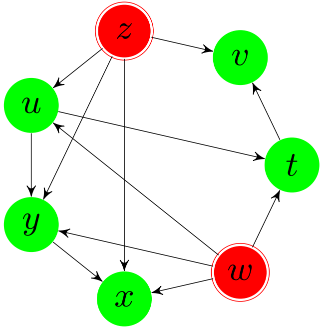

Hosein Hadipour
TU Wien - Vienna, Austria

Autoguess - Simple User Interface

Input file (`relations.txt`):

```
# Comments
connection relations
u, v, x, y, z
u, w, y, z
w, x, y, z
u, w, z
u, w => t
t, z, v
end
```

Output:

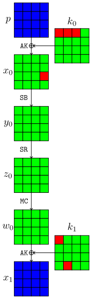


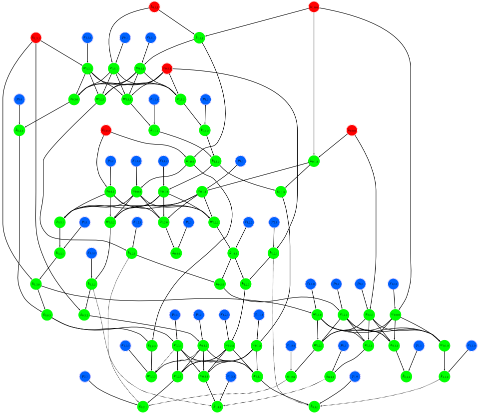
Run Autoguess:

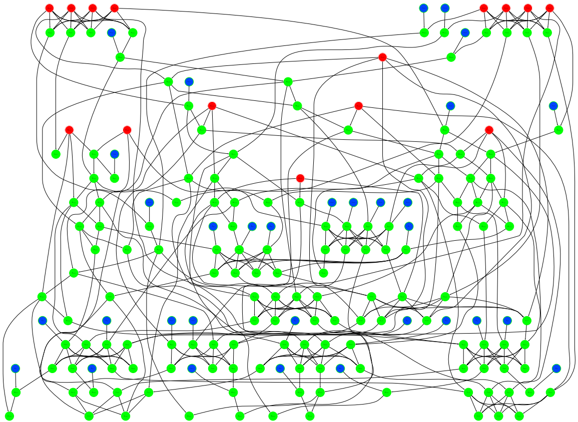
```
python3 autoguess.py -i relations.txt --maxsteps 5 --solver cp
```


Hosein Hadipour
TU Wien - Vienna, Austria

GD Attack on 1 to 3 Rounds of AES





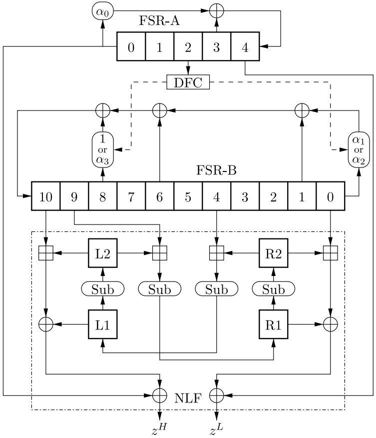


Found in 0.02 seconds on a standard laptop

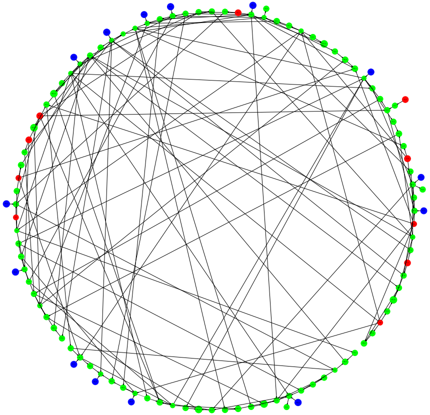
Found in 34.51 seconds on a standard laptop

Hosein Hadipour
TU Wien - Vienna, Austria

GD Attack on KCipher-2



ISO/IEC 18033-4



Found in 7 seconds on a standard laptop

Hosein Hadipour
TU Wien - Vienna, Austria

Conclusion and Our Other Contributions

Hosein Hadipour
TU Wien - Vienna, Austria

Our Contributions – I

- Hosein Hadipour, Sadegh Sadeghi, and Maria Eichlseder. **Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks**. **EUROCRYPT 2023**. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. LNCS. Springer, 2023, pp. 128–157. DOI: 10.1007/978-3-031-30634-1_5
- Hosein Hadipour, Marcel Nageler, and Maria Eichlseder. **Throwing Boomerangs into Feistel Structures Application to CLEFIA, WARP, LBlock, LBlock-s and TWINE**. **IACR Trans. Symmetric Cryptol.** 2022.3 (2022), pp. 271–302. DOI: 10.46586/TOSC.V2022.I3.271-302
- Hosein Hadipour and Maria Eichlseder. **Integral Cryptanalysis of WARP based on Monomial Prediction**. **IACR Trans. Symmetric Cryptol.** 2022.2 (2022), pp. 92–112. DOI: 10.46586/TOSC.V2022.I2.92-112

Hosein Hadipour
TU Wien - Vienna, Austria

Our Contributions – II

- Hosein Hadipour and Maria Eichlseder. **Autoguess: A Tool for Finding Guess-and-Determine Attacks and Key Bridges**. ACNS 2022. Ed. by Giuseppe Ateniese and Daniele Venturi. Vol. 13269. LNCS. Springer, 2022, pp. 230–250. DOI: 10.1007/978-3-031-09234-3_12
- Hosein Hadipour et al. **Improved Search for Integral, Impossible-Differential and Zero-Correlation Attacks: Application to Ascon, ForkSKINNY, SKINNY, MANTIS, PRESENT and QARMAv2**. **IACR Trans. Symmetric Cryptol.** 2024.1 (2024)
- Hosein Hadipour and Yosuke Todo. **Cryptanalysis of QARMAv2**. **IACR Trans. Symmetric Cryptol.** 2024.1 (2024)

Future Works

- Future works
  - Improving the accuracy and performance of the existing automated methods
  - Many cryptanalytic methods are not automated yet
  - New cryptanalytic methods require new automated tools

Thanks for your attention!

: https://github.com/hadipourh/talks

Bibliography I

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. **Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials**. EUROCRYPT 1999. Vol. 1592. LNCS. Springer, 1999, pp. 12–23. DOI: 10.1007/3-540-48910-X_2.

[BS90] Eli Biham and Adi Shamir. **Differential Cryptanalysis of DES-like Cryptosystems**. CRYPTO '90. Ed. by Alfred Menezes and Scott A. Vanstone. Vol. 537. LNCS. Springer, 1990, pp. 2–21. DOI: 10.1007/3-540-38424-3_1.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. **The Block Cipher Square**. FSE 1997. Vol. 1267. LNCS. Springer, 1997, pp. 149–165. DOI: 10.1007/BFb0052343.

[DR99] Joan Daemen and Vincent Rijmen. **AES proposal: Rijndael**. (1999).

Hosein Hadipour
TU Wien - Vienna, Austria

Bibliography II

[DS09] Itai Dinur and Adi Shamir. **Cube Attacks on Tweakable Black Box Polynomials**. EUROCRYPT 2009. Ed. by Antoine Joux. Vol. 5479. LNCS. Springer, 2009, pp. 278–299. DOI: 10.1007/978-3-642-01001-9_16.

[Had+24] Hosein Hadipour et al. **Improved Search for Integral, Impossible-Differential and Zero-Correlation Attacks: Application to Ascon, ForkSKINNY, SKINNY, MANTIS, PRESENT and QARMAv2**. **IACR Trans. Symmetric Cryptol.** 2024.1 (2024).

[HE22a] Hosein Hadipour and Maria Eichlseder. **Autoguess: A Tool for Finding Guess-and-Determine Attacks and Key Bridges**. ACNS 2022. Ed. by Giuseppe Ateniese and Daniele Venturi. Vol. 13269. LNCS. Springer, 2022, pp. 230–250. DOI: 10.1007/978-3-031-09234-3_12.

Bibliography III

[HE22b] Hosein Hadipour and Maria Eichlseder. **Integral Cryptanalysis of WARP based on Monomial Prediction**. **IACR Trans. Symmetric Cryptol.** 2022.2 (2022), pp. 92–112. DOI: 10.46586/TOSC.V2022.I2.92-112.

[HNE22] Hosein Hadipour, Marcel Nageler, and Maria Eichlseder. **Throwing Boomerangs into Feistel Structures Application to CLEFIA, WARP, LBlock, LBlock-s and TWINE**. **IACR Trans. Symmetric Cryptol.** 2022.3 (2022), pp. 271–302. DOI: 10.46586/TOSC.V2022.I3.271-302.

[HSE23] Hosein Hadipour, Sadegh Sadeghi, and Maria Eichlseder. **Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks**. **EUROCRYPT 2023**. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. LNCS. Springer, 2023, pp. 128–157. DOI: 10.1007/978-3-031-30634-1_5.

Bibliography IV

[HT24] Hosein Hadipour and Yosuke Todo. **Cryptanalysis of QARMAv2**. **IACR Trans. Symmetric Cryptol.** 2024.1 (2024).

[Knu98] Lars Knudsen. **DEAL-a 128-bit block cipher**. *complexity* 258.2 (1998), p. 216.

[Lai94] Xuejia Lai. **Higher Order Derivatives and Differential Cryptanalysis**. (1994), pp. 227–233. DOI: 10.1007/978-1-4615-2694-0_23.

[LH94] Susan K. Langford and Martin E. Hellman. **Differential-Linear Cryptanalysis**. CRYPTO '94. Vol. 839. Springer, 1994, pp. 17–25. DOI: 10.1007/3-540-48658-5_3.

[Mat93] Mitsuru Matsui. **Linear Cryptanalysis Method for DES Cipher**. EUROCRYPT '93. Ed. by Tor Helleseth. Vol. 765. LNCS. Springer, 1993, pp. 386–397. DOI: 10.1007/3-540-48285-7_33.

Bibliography V

[Wag99] David A. Wagner. **The Boomerang Attack**. FSE 1999. Vol. 1636. LNCS. Springer, 1999, pp. 156–170. DOI: 10.1007/3-540-48519-8_12.

Hosein Hadipour
TU Wien - Vienna, Austria

AES [DR99]

- Block size $n = 128$ bits, Key size $k \in \{128, 192, 256\}$ bits
- 3 Block ciphers named after their key size: AES-128, AES-192, AES-256
- The 16-byte input block $M = s_{00} \| s_{10} \| s_{20} \| s_{30} \| s_{01} \| \dots \| s_{33}$ is written as a 4×4 matrix of bytes, the $\{16, 24, 32\}$-*byte* key K as a $4 \times \{4, 6, 8\}$ matrix:

$$M = \begin{array}{|c|c|c|c|}\hline s_{00} & s_{01} & s_{02} & s_{03} \\ \hline s_{10} & s_{11} & s_{12} & s_{13} \\ \hline s_{20} & s_{21} & s_{22} & s_{23} \\ \hline s_{30} & s_{31} & s_{32} & s_{33} \\ \hline\end{array}, \qquad K = \begin{array}{|c|c|c|c|c|c|c|c|}\hline k_{00} & k_{01} & k_{02} & k_{03} & k_{04} & k_{05} & k_{06} & k_{07} \\ \hline k_{10} & k_{11} & k_{12} & k_{13} & k_{14} & k_{15} & k_{16} & k_{17} \\ \hline k_{20} & k_{21} & k_{22} & k_{23} & k_{24} & k_{25} & k_{26} & k_{27} \\ \hline k_{30} & k_{31} & k_{32} & k_{33} & k_{34} & k_{35} & k_{36} & k_{37} \\ \hline\end{array}$$

- The state is initialized to M and updated in *10 rounds* (for AES-128) or 12 rounds (AES-192) or 14 rounds (AES-256). The last round is different.

Hosein Hadipour
TU Wien - Vienna, Austria

AES [DR99]

- Block size $n = 128$ bits, Key size $k \in \{128, 192, 256\}$ bits
- 3 Block ciphers named after their key size: AES-128, AES-192, AES-256
- The 16-byte input block $M = s_{00} \| s_{10} \| s_{20} \| s_{30} \| s_{01} \| \ldots \| s_{33}$ is written as a 4×4 matrix of bytes, the $\{16, 24, 32\}$-*byte* key K as a $4 \times \{4, 6, 8\}$ matrix:

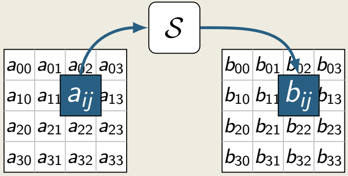
$$M = \begin{array}{|c|c|c|c|} \hline s_{00} & s_{01} & s_{02} & s_{03} \\ \hline s_{10} & s_{11} & s_{12} & s_{13} \\ \hline s_{20} & s_{21} & s_{22} & s_{23} \\ \hline s_{30} & s_{31} & s_{32} & s_{33} \\ \hline \end{array}, \qquad K = \begin{array}{|c|c|c|c|c|c|c|c|} \hline k_{00} & k_{01} & k_{02} & k_{03} & k_{04} & k_{05} & k_{06} & k_{07} \\ \hline k_{10} & k_{11} & k_{12} & k_{13} & k_{14} & k_{15} & k_{16} & k_{17} \\ \hline k_{20} & k_{21} & k_{22} & k_{23} & k_{24} & k_{25} & k_{26} & k_{27} \\ \hline k_{30} & k_{31} & k_{32} & k_{33} & k_{34} & k_{35} & k_{36} & k_{37} \\ \hline \end{array}$$

- The state is initialized to M and updated in *10 rounds* (for AES-128) or 12 rounds (AES-192) or 14 rounds (AES-256). The last round is different.

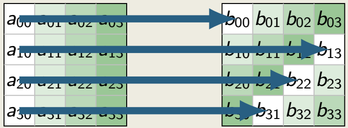
Hosein Hadipour
TU Wien - Vienna, Austria

AES Round Function – Overview

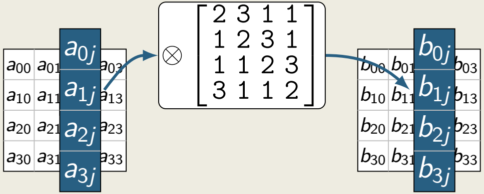
1 SubBytes (SB)



2 ShiftRows (SR)



3 MixColumns (MC)

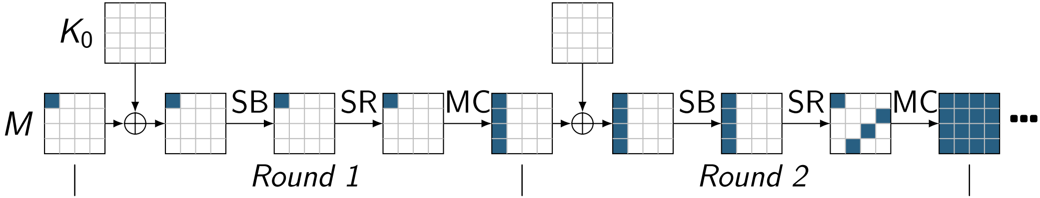


4 AddRoundKey (AK)

$$\begin{array}{|c|c|c|c|} \hline a_{00} & a_{01} & a_{02} & a_{03} \\ \hline a_{10} & a_{11} & a_{12} & a_{13} \\ \hline a_{20} & a_{21} & a_{22} & a_{23} \\ \hline a_{30} & a_{31} & a_{32} & a_{33} \\ \hline \end{array} + \begin{array}{|c|c|c|c|} \hline k_{00} & k_{01} & k_{02} & k_{03} \\ \hline k_{10} & k_{11} & k_{12} & k_{13} \\ \hline k_{20} & k_{21} & k_{22} & k_{23} \\ \hline k_{30} & k_{31} & k_{32} & k_{33} \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline b_{00} & b_{01} & b_{02} & b_{03} \\ \hline b_{10} & b_{11} & b_{12} & b_{13} \\ \hline b_{20} & b_{21} & b_{22} & b_{23} \\ \hline b_{30} & b_{31} & b_{32} & b_{33} \\ \hline \end{array}$$

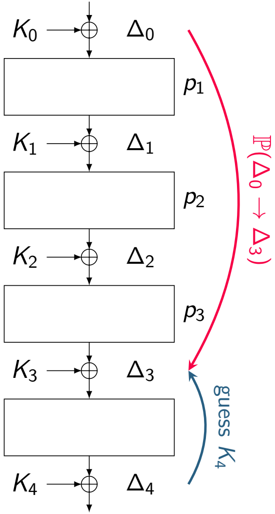
Hosein Hadipour
TU Wien - Vienna, Austria

AES – Diffusion



Hosein Hadipour
TU Wien - Vienna, Austria

Differential Attack [BS90]



1. Find "good" differential characteristic

$$\Delta_{\mathrm{i}} = \Delta_0 \to \Delta_1 \to \Delta_2 \to \Delta_{\mathrm{o}} = \Delta_3$$

2. Guess final key K_4' and determine Δ_3'

3. The right key satisfies $\Delta_3' = \Delta_3$ with probability $\mathbb{P}(\Delta_0 \to \Delta_3) = p_1 \cdot p_2 \cdot p_3$, while a wrong key satisfies $\Delta_3' = \Delta_3$ with probability 2^{-n}

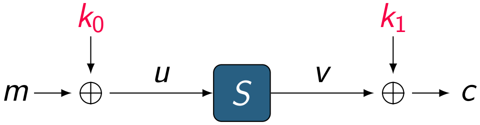
4. *Necessary condition* for the attack: $\mathbb{P} \gg 2^{-n}$.

Hosein Hadipour
TU Wien - Vienna, Austria

A Simple Toy Block Cipher

The block cipher $E_{k_0||k_1}(m)$ encrypts 4 bits of plaintext using two 4-bit keys:

$$c = E_{k_0||k_1}(m) = \mathcal{S}(m \oplus k_0) \oplus k_1$$



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	4	0	a	7	b	e	1	d	9	f	6	8	5	2	c	3

Given $(m_0, c_0) = (\text{a}, 9)$ and $(m_1, c_1) = (5, 6)$, what is the key?

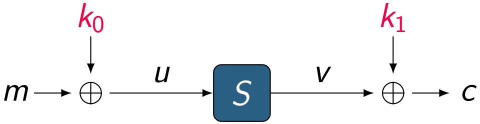
Brute force (exhaustive search): try all $2^4 \cdot 2^4 = 256$ keys.

Hosein Hadipour
TU Wien - Vienna, Austria

A Simple Toy Block Cipher

The block cipher $E_{k_0||k_1}(m)$ encrypts 4 bits of plaintext using two 4-bit keys:

$$c = E_{k_0||k_1}(m) = \mathcal{S}(m \oplus k_0) \oplus k_1$$



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	4	0	a	7	b	e	1	d	9	f	6	8	5	2	c	3

Given $(m_0, c_0) = (\text{a}, 9)$ and $(m_1, c_1) = (5, 6)$, what is the key?

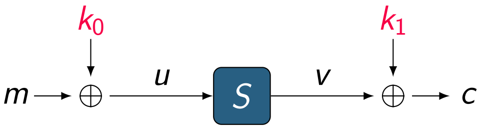
Brute force (exhaustive search): try all $2^4 \cdot 2^4 = 256$ keys.

Hosein Hadipour
TU Wien - Vienna, Austria

A Simple Toy Block Cipher

The block cipher $E_{k_0||k_1}(m)$ encrypts 4 bits of plaintext using two 4-bit keys:

$$c = E_{k_0||k_1}(m) = \mathcal{S}(m \oplus k_0) \oplus k_1$$



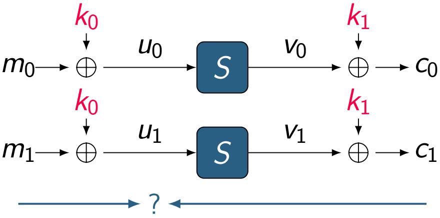
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	4	0	a	7	b	e	1	d	9	f	6	8	5	2	c	3

Given $(m_0, c_0) = (\text{a}, 9)$ and $(m_1, c_1) = (5, 6)$, what is the key?

Brute force (exhaustive search): try all $2^4 \cdot 2^4 = 256$ keys.

Hosein Hadipour
TU Wien - Vienna, Austria

Differential Attack



Strategy:

1. compute $\Delta_i = u_0 \oplus u_1$
2. guess k_1 (iterate over all values)
3. compute $u'_0 = \mathcal{S}^{-1}(c_0 \oplus k'_1)$ and $u'_1 = \mathcal{S}^{-1}(c_1 \oplus k'_1)$
4. check if $u_0 \oplus u_1 = u'_0 \oplus u'_1$
5. if not: key guess was definitely wrong! (filtering)

Hosein Hadipour
TU Wien - Vienna, Austria

Difference Distribution Table (DDT) – I

We need a metric to measure the quality of a differential characteristic

Differential Distribution Table (DDT)

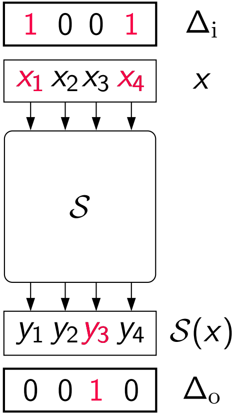
For a vectorial Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the DDT is a $2^n \times 2^m$ table whose rows correspond to the input difference Δ_i to S and whose columns correspond to the output difference Δ_o of S. The entry at index $(\Delta_\mathrm{i}, \Delta_\mathrm{o})$ is

$$\mathtt{DDT}(\Delta_\mathrm{i}, \Delta_\mathrm{o}) = |\{x \in \mathbb{F}_2^n : \; S(x) \oplus S(x \oplus \Delta_\mathrm{i}) = \Delta_\mathrm{o}\}|.$$

$$\mathbb{P}\left(\Delta_\mathrm{i}, \Delta_\mathrm{o}\right) = 2^{-n} \cdot \mathtt{DDT}\left(\Delta_\mathrm{i}, , \Delta_\mathrm{o}\right)$$

Hosein Hadipour
TU Wien - Vienna, Austria

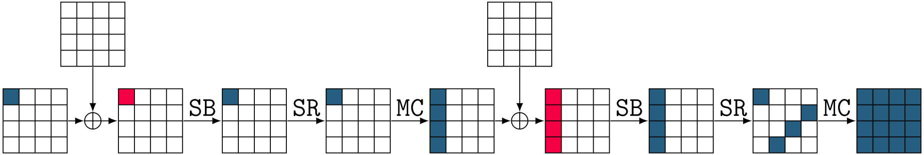
Difference Distribution Table (DDT) – II



$$\mathbb{P}(9, 2) = \frac{4}{16}$$

$\Delta_i \setminus \Delta_o$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
2	0	2	0	2	0	0	0	4	0	2	2	0	0	0	2	2
3	0	2	0	2	0	0	4	0	0	2	2	0	0	0	2	2
4	0	0	0	0	0	0	0	0	0	0	4	4	2	2	2	2
5	0	0	0	0	2	2	2	2	0	0	4	4	0	0	0	0
6	0	2	0	2	0	4	0	0	0	2	2	0	2	2	0	0
7	0	2	0	2	4	0	0	0	0	2	2	0	2	2	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4
9	0	4	4	0	0	0	0	0	0	4	0	4	0	0	0	0
a	0	0	2	2	2	0	0	2	4	0	0	0	0	2	0	2
b	0	0	2	2	0	2	2	0	4	0	0	0	2	0	2	0
c	0	4	4	0	2	2	2	2	0	0	0	0	0	0	0	0
d	0	0	0	0	2	2	2	2	0	4	0	4	0	0	0	0
e	0	0	2	2	0	2	2	0	4	0	0	0	0	2	0	2
f	0	0	2	2	2	0	0	2	4	0	0	0	2	0	2	0

Truncated Differential Trail for AES with Minimum Number of Active S-boxes



Variables:

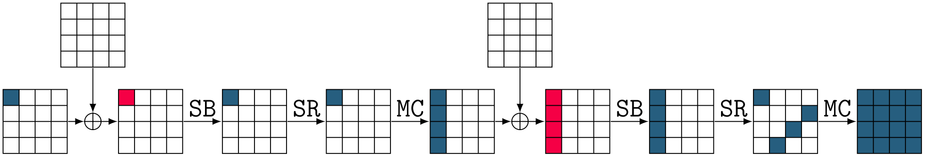
- $s_{r,i,j} \in \{0, 1\}$ is S-box in row i, column j, round r active?
- $m_{r,j} \in \{0, 1\}$ is Mix-columns j in round r active?

Objective function and constraints:

- $5 \cdot M_{r,j} \leq \sum_i s_{r,i,(i+j)\%4} + \sum_i s_{r+1,i,j} \leq 8 \cdot M_{r,j}; \quad \sum_{i,j} s_{0,i,j} \geq 1$
- $\min \sum_{r,i,j} s_{r,i,j}$

Hosein Hadipour
TU Wien - Vienna, Austria

Truncated Differential Trail for AES with Minimum Number of Active S-boxes



Variables:

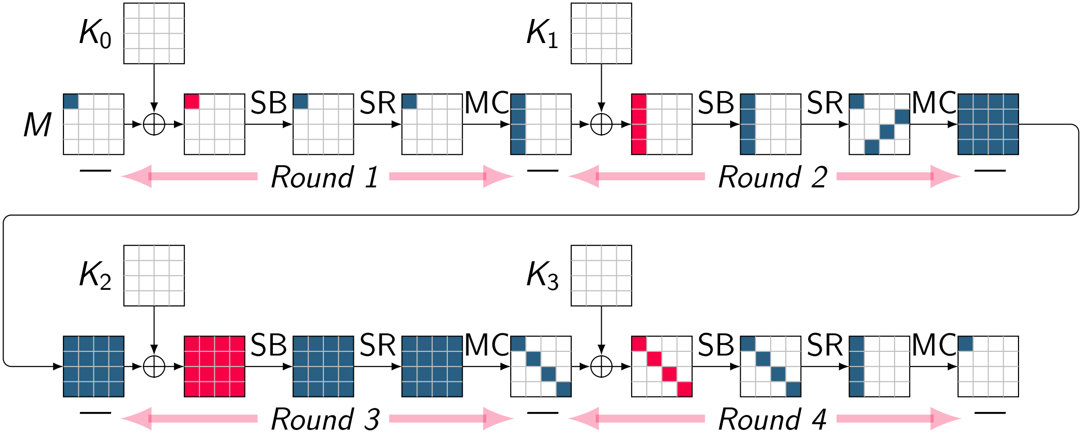
- $s_{r,i,j} \in \{0,1\}$ is S-box in row i, column j, round r active?
- $m_{r,j} \in \{0,1\}$ is Mix-columns j in round r active?

Objective function and constraints:

- $5 \cdot M_{r,j} \leq \sum_i s_{r,i,(i+j)\%4} + \sum_i s_{r+1,i,j} \leq 8 \cdot M_{r,j}; \quad \sum_{i,j} s_{0,i,j} \geq 1$
- $\min \sum_{r,i,j} s_{r,i,j}$

Hosein Hadipour
TU Wien - Vienna, Austria

Security of AES Against Differential/Linear Attacks



$$\mathbb{P}_{4 \text{ rounds}} \leq 2^{-150}, \ \mathbb{C}^2_{4 \text{ rounds}} \leq 2^{-150}$$

Hosein Hadipour
TU Wien - Vienna, Austria