Automatic Cryptanalysis Tools

Paper Read Report: MILP II

Tan Jun Xiong
jtan570@e.ntu.edu.sg

School of Physical and Mathematical Sciences

Nanyang Technological University

June 2, 2022

Paper of Interest

- Zhang, Y., Sun, S., Cai, J., & Hu, L. (2018). Speeding up MILP Aided Differential Characteristic Search with Matsui's Strategy.

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- Motivation
- Matsui's Algorithm
- MILP Aided Characteristic Search
- Integrating Matsui's Bounding Condition into MILP Search
- Application to PRESENT, SIMON, and SPECK
- Potential Considerations

NANYANG TECHNOLOGICAL UNIVERSITY

Motivation

- MILP model can be solved with generic MILP
- Inconvenience in implementing Matsui’s algoritm
- Many new ciphers designed for lightweight devices or dedicated use cases

- MILP: sets up R-round model directly
- Matsui’s Algo: Uses probability of optimal characteristics in lower rounds

NANYANG TECHNOLOGICAL UNIVERSITY

Matsui's Algorithm

- Continuously branch down each valid trail (DFS)
- Update the probability of reaching some round i from the previous round; $P_{Rd(i)}$
- If the probability of reaching this round (from the start) is less than some specified bound, break the algo for this trail
- Improve efficiency by (i) using a larger, valid initial probability, and (ii) updating the current best probability found

NANYANG TECHNOLOGICAL UNIVERSITY

Matsui's Algorithm

Algorithm 1. Matsui's Algorithm

Input: $R \in \mathbb{Z}^*$, $R \geq 2$; $q > 0$; $P_{Best}(1)$, $P_{Best}(2)$, $\ldots$, $P_{Best}(R-1)$

Output: differential characteristic $\mathcal{T} = (\alpha_0, \alpha_1, \ldots, \alpha_{R-1}) \in \mathbb{F}_2^n$ where probability $\mathbb{P}(\mathcal{T}) = P_{Estim}$

Algorithm `OptimalTrail`$(R, q, P_{Best}(1), \ldots, P_{Best}(R-1))$ `// Entry Point`

    for *each non-zero* α_1 **do**

        $\mathcal{T} = ()$, $P_{Estim} \leftarrow q$

        Call `FirstRound()`

    end

    if $\mathcal{T} \neq ()$ **then**

        return $\mathcal{T}$, $P_{Estim} = \mathbb{P}(\mathcal{T})$

    end

end

Function `FirstRound()` `// Subroutine`

    $P_{Rd(1)} \leftarrow \max_\alpha \mathbb{P}(\alpha \rightarrow \alpha_1)$

    $\alpha_0 \leftarrow \alpha$, $s.t\ \mathbb{P}(\alpha \rightarrow \alpha_1) = P_{Rd(1)}$

    if $R > 2$ **then**

        Call `Round(2)`

    else

        Call `LastRound()`

    end

end

Matsui's Algorithm

Function Round(r)($2 \leq r \leq R-1$) // Subroutine

  for *each candidate* α *for* α_{r-1} **do**

    $P_{Rd(r)} \leftarrow \mathbb{P}(\alpha_{r-1} \rightarrow \alpha)$

    if $\prod_{i=1}^{r} P_{Rd(i)} \cdot P_{Best}(R-r) \geq P_{Estim}$ **then**

      // Matsui's bounding condition

      $\alpha_r \leftarrow \alpha$

      if $r+1 < R$ **then**

        Call Round(r+1)

      else

        Call LastRound()

      end

    end

  end

end

Function LastRound() // Subroutine

  for *each candidate* α *for* α_{r-1} **do**

    $P_{Rd(R)} \leftarrow \max_{\alpha} \mathbb{P}(\alpha_{R-1} \rightarrow \alpha)$

    $\alpha_R \leftarrow \alpha, \ s.t \ \mathbb{P}(\alpha_{R-1} \rightarrow \alpha) = P_{Rd(R)}$

  end

  if $\prod_{i=1}^{R} P_{Rd(i)} > P_{Estim}$ **then** // A strictly better trail is found

    $\mathcal{T} \leftarrow (\alpha_0, \alpha_1, \ldots, \alpha_{R-1})$

    $P_{Estim} \leftarrow \prod_{i=1}^{R} P_{Rd(i)}$

  end

end

NANYANG TECHNOLOGICAL UNIVERSITY

MILP Aided Characteristic Search

- Objective Function

- Modelling XOR [MILP 1]
- Modelling S-Box [MILP 1]
- Modelling Modular Addition

NANYANG TECHNOLOGICAL UNIVERSITY

Objective Function

- To minimize the *probability weight* of the underlying differential characteristic
- Recall: (Matsui's Bounding Condition)

$$\prod_{i=1}^{r} P_{Rd(i)} \cdot P_{Best}(R-r) \geq P_{Estim}$$

- For simplicity, WLOG, assume the condition can be represented (linearly) by:

$$\sum_{i=1}^{R} \sum_{j=1}^{k} A_{i,j}\,,$$

where $A_{i,j}$'s are *probability weight variables* for $j \in [1, k]$ in some round i in an iterative cipher

→Probability weight contributed by round i is

$$\sum_{j=1}^{k} A_{i,j}$$

NANYANG TECHNOLOGICAL UNIVERSITY

Modular Addition in ARX construct

- ARX= add-rotate-xor
- Addition in $(\text{mod } 2^n)$

- Ex. $1 + 1 \equiv 0\ (mod\ 2)\ [XOR]$
- Ex. $F(1111) + F(1111) = E(1110)\ (mod\ F)$

Setting up the MILP Model

- $d_{\oplus}$ is 0-1 dummy variable
- s_i for $i \in [1, n-2]$ is 0-1 active markers

$$
\begin{cases}
a_{n-1} + b_{n-1} + c_{n-1} \leq 2 \\
a_{n-1} + b_{n-1} + c_{n-1} - 2d_{\oplus} \geq 0 \\
d_{\oplus} - a_{n-1} \geq 0 \\
d_{\oplus} - b_{n-1} \geq 0 \\
d_{\oplus} - c_{n-1} \geq 0 \\
-a_i + b_i + s_i \geq 0 \\
-b_i + c_i + s_i \geq 0 \\
a_i - c_i + s_i \geq 0 \\
a_i + b_i + c_i - s_i \geq 0 \\
-a_i - b_i - c_i - s_i \geq -3 \\
c_i + a_{i-1} + b_{i-1} - c_{i-1} + s_i \geq 0 \\
-a_i - b_i - c_i + 3a_{i-1} + 3b_{i-1} + 3c_{i-1} + 2s_i \geq 0 \\
a_i + b_i + c_i - 3a_{i-1} - 3b_{i-1} - 3c_{i-1} + 2s_i \geq -6 \\
-b_i + a_{i-1} - b_{i-1} - c_{i-1} + s_i \geq -2 \\
c_i + a_{i-1} - b_{i-1} + c_{i-1} + s_i \geq 0 \\
-a_i - b_i - c_i - 3a_{i-1} + 3b_{i-1} - 3c_{i-1} + 2s_i \geq -6 \\
-a_i - a_{i-1} - b_{i-1} + c_{i-1} + s_i \geq -2 \\
a_i + b_i + c_i - 3a_{i-1} + 3b_{i-1} + 3c_{i-1} + 2s_i \geq 0 \\
(i = 1, \ldots, n-2)
\end{cases}
$$

NANYANG TECHNOLOGICAL UNIVERSITY

Setting up the MILP Model

- $d_{\oplus}$ is 0-1 dummy variable
- s_i for $i \in [1, n-2]$ is 0-1 active markers

$$
\begin{cases}
a_{n-1} + b_{n-1} + c_{n-1} \le 2 \\
a_{n-1} + b_{n-1} + c_{n-1} - 2d_{\oplus} \ge 0 \\
d_{\oplus} - a_{n-1} \ge 0 \\
d_{\oplus} - b_{n-1} \ge 0 \\
d_{\oplus} - c_{n-1} \ge 0 \\
-a_i + b_i + s_i \ge 0 \\
-b_i + c_i + s_i \ge 0 \\
a_i - c_i + s_i \ge 0 \\
a_i + b_i + c_i - s_i \ge 0 \\
-a_i - b_i - c_i - s_i \ge -3 \\
c_i + a_{i-1} + b_{i-1} - c_{i-1} + s_i \ge 0 \\
-a_i - b_i - c_i + 3a_{i-1} + 3b_{i-1} + 3c_{i-1} + 2s_i \ge 0 \\
a_i + b_i + c_i - 3a_{i-1} - 3b_{i-1} - 3c_{i-1} + 2s_i \ge -6 \\
-b_i + a_{i-1} - b_{i-1} - c_{i-1} + s_i \ge -2 \\
c_i + a_{i-1} - b_{i-1} + c_{i-1} + s_i \ge 0 \\
-a_i - b_i - c_i - 3a_{i-1} + 3b_{i-1} - 3c_{i-1} + 2s_i \ge -6 \\
-a_i - a_{i-1} - b_{i-1} + c_{i-1} + s_i \ge -2 \\
a_i + b_i + c_i - 3a_{i-1} + 3b_{i-1} + 3c_{i-1} + 2s_i \ge 0 \\
(i = 1, \ldots, n-2)
\end{cases}
$$

Integrating Matsui's Bounding Condition into MILP Search

- Define $xobj$ as the linear representation of P_{Estim}, and let [Minimize $xobj$] be the objective function of the model.

$$xobj = \sum_{i=1}^{R}\sum_{j=1}^{k} A_{i,j}$$

Integrating Matsui's Bounding Condition into MILP Search

- Obtaining more constraints:
- $$\sum_{t=1}^{i}\sum_{j=1}^{k} A_{t,j} + wt\left(P_{Best}(R-i)\right) \leq xobj, \qquad i \in [1, R-1]$$
- $$\sum_{t=i+1}^{R}\sum_{j=1}^{k} A_{t,j} + wt\left(P_{Best}(i)\right) \leq xobj, \qquad i \in [1, R-1]$$

*$2R-2$ more constraints

NANYANG TECHNOLOGICAL UNIVERSITY

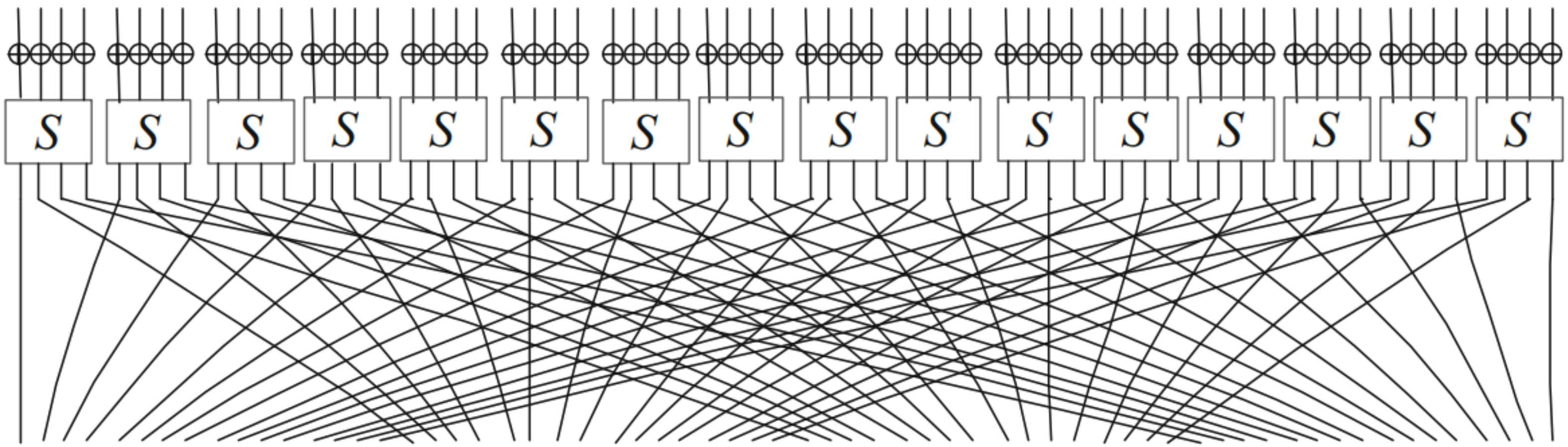
Applications to PRESENT, SIMON, and SPECK

- PRESENT: SPN network
- SIMON: Feistel cipher with pure bitwise operations
- SPECK: ARX construction
- Using 3 models for comparison
  - original MILP without modifications
  - MILP with modified objective function, and R-1 constraints from the first inequality
  - MILP with modified objective function, and all 2R-2 constraints

- Measuring time cost for the solution to prove that the solution it identified is optimal
  - less time → tighter bound → more accurate security evaluation

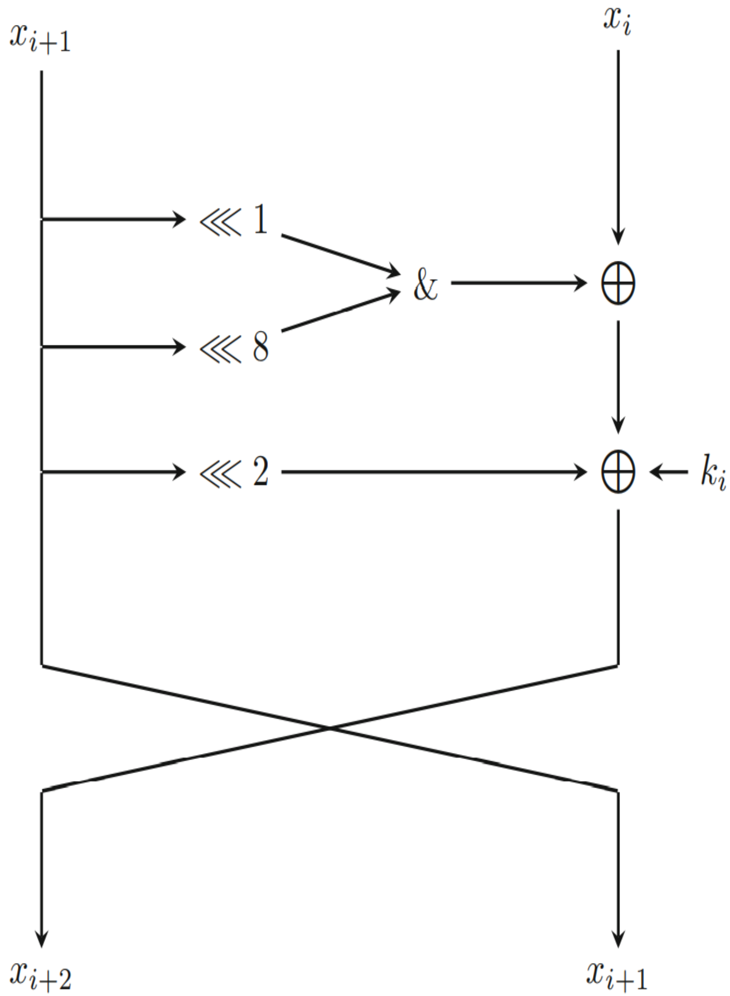
NANYANG TECHNOLOGICAL UNIVERSITY

Applications to PRESENT



R	p	$\mathcal{M}^{I}$	$\mathcal{M}^{II}$	$\mathcal{M}^{III}$
1	2^{-2}	0.01s	0.09s	0.13s
2	2^{-4}	0.95s	0.95s	0.06s
3	2^{-8}	3.70s	2.82s	2.43s
4	2^{-12}	15.78s	10.08s	8.82s
5	2^{-20}	629.83s	114.13s	448.61s
6	2^{-24}	1740.55s	200.03s	74.56s
7	2^{-28}	48638.29s	714.03s	655.36s
8	2^{-32}	>10h	2124.51s	1074.45s

Applications to SIMON



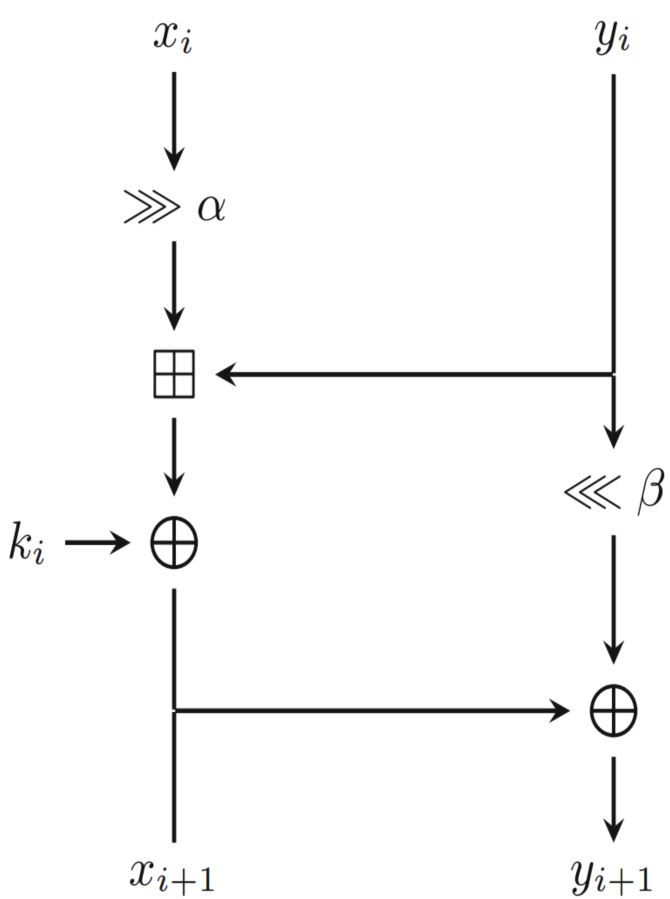
Parameters for SIMON32 and SIMON48

Variant $2n/mn$	Block Size $2n$	Key Size mn	Round r
32/64	32	64	32
48/72	48	72	36
48/96	48	96	36

Block size $2n$	R	p	$\mathcal{M}^I$	$\mathcal{M}^{II}$	$\mathcal{M}^{III}$
32	11	2^{-30}	75.05s	79.22s	67.92s
	12	2^{-34}	657.37s	559.83s	209.09s
48	13	2^{-38}	309.58s	376.33s	109.85s
	14	2^{-44}	4627.26s	3577.05s	2942.85s
	15	2^{-46}	31979.80s	3351.41s	2444.28s
	16	2^{-50}	>20h	>15h	26589.96s

NANYANG TECHNOLOGICAL UNIVERSITY

Applications to SPECK



Parameters for SPECK32 and SPECK48

Variant $2n/mn$	Block Size $2n$	Key Size mn	Round r	α	β
32/64	32	64	22	7	2
48/72	48	72	22	8	3
48/96	48	96	23	8	3

Block size $2n$	R	p	$\mathcal{M}^I$	$\mathcal{M}^{II}$	$\mathcal{M}^{III}$
32	5	2^{-9}	9.78s	17.15s	26.08s
	6	2^{-13}	173.67s	820.82s	390.33s
	7	2^{-18}	7175.87s	>10000s	>10000s
48	5	2^{-10}	32.90s	358.11s	273.98s
	6	2^{-14}	1482.66s	2626.50s	2287.21s
	7	2^{-19}	40860.38s	>100000s	>100000s

NANYANG TECHNOLOGICAL UNIVERSITY

Potential Considerations

- PRESENT: New MILP model *v.* Matsui's Algorithm
- Non-lightweight ciphers
- Integrating cutting-off inequalities (mentioned in MILP 1)

NANYANG TECHNOLOGICAL UNIVERSITY

Related Readings

- Heys, H.: A Tutorial on Linear and Differential Cryptanalysis. Computer Science Department, Boston College. http://www.cs.bc.edu/~straubin/crypto2017/heys.pdf
- Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 57–76. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34704-7_5
- Sun, S., et al.: Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties. Cryptology ePrint Archive, Report 2014/747(2014). http://eprint.iacr.org/2014/747
- Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_9
- Zhang, T.: Cryptology Basics. School of Physical and Mathematical Sciences, Nanyang Technological University.
- Li, H.: Some Basics. School of Physical and Mathematical Sciences, Nanyang Technological University

NANYANG TECHNOLOGICAL UNIVERSITY

Thank you ☺