RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CRYP-R11

Automatic Search for A Variant of Division Property Using Three Subsets

Kai Hu* and Meiqin Wang

Key Lab of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University

#RSAC

RSAConference2019

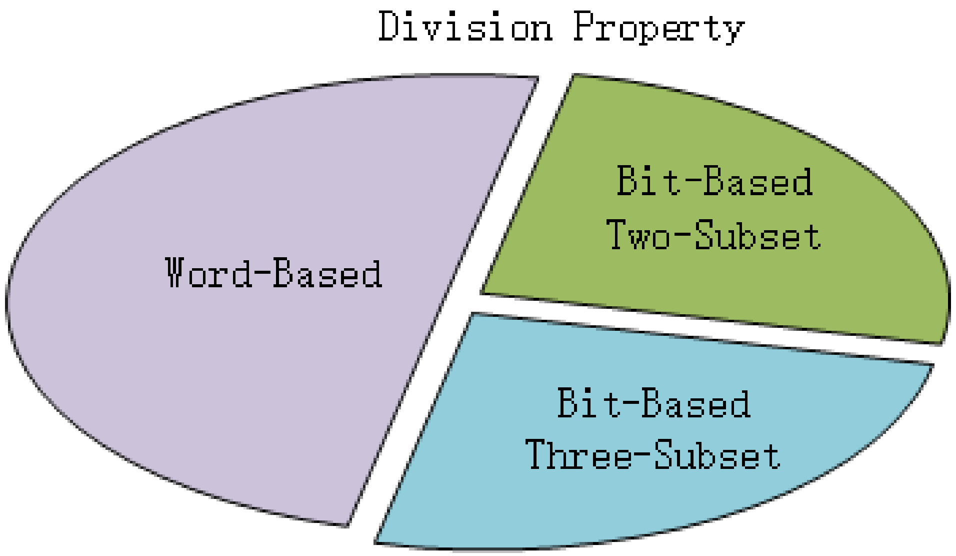
OUTLINE

OUTLINE

- ***1. Background of Division Property and Automatic Search***
- 2. Motivation and Contribution
- 3. A Variant of Three-Subset Division Property (VTDP)
- 4. Automatic Search for VTDP
- 5. Applications
- 6. Summary

What is Division Property (DP)?

- **A technique** to find **integral distinguishers** easily and efficiently
- Proposed by **Yosuke Todo** at **Eurocrypt'15**
- Divided into **Word-based DP** and **Bit-Based DP**
- **Bit-Based DP** is divided into **Two-Subset** and **Three-Subset**



What is Three-Subset Bit-Based Division Property ?

- **Sum all the ciphertexts together**

- Two-Subset DP **indicates** the sum of one bit of all the ciphertexts is

0 or Unknown

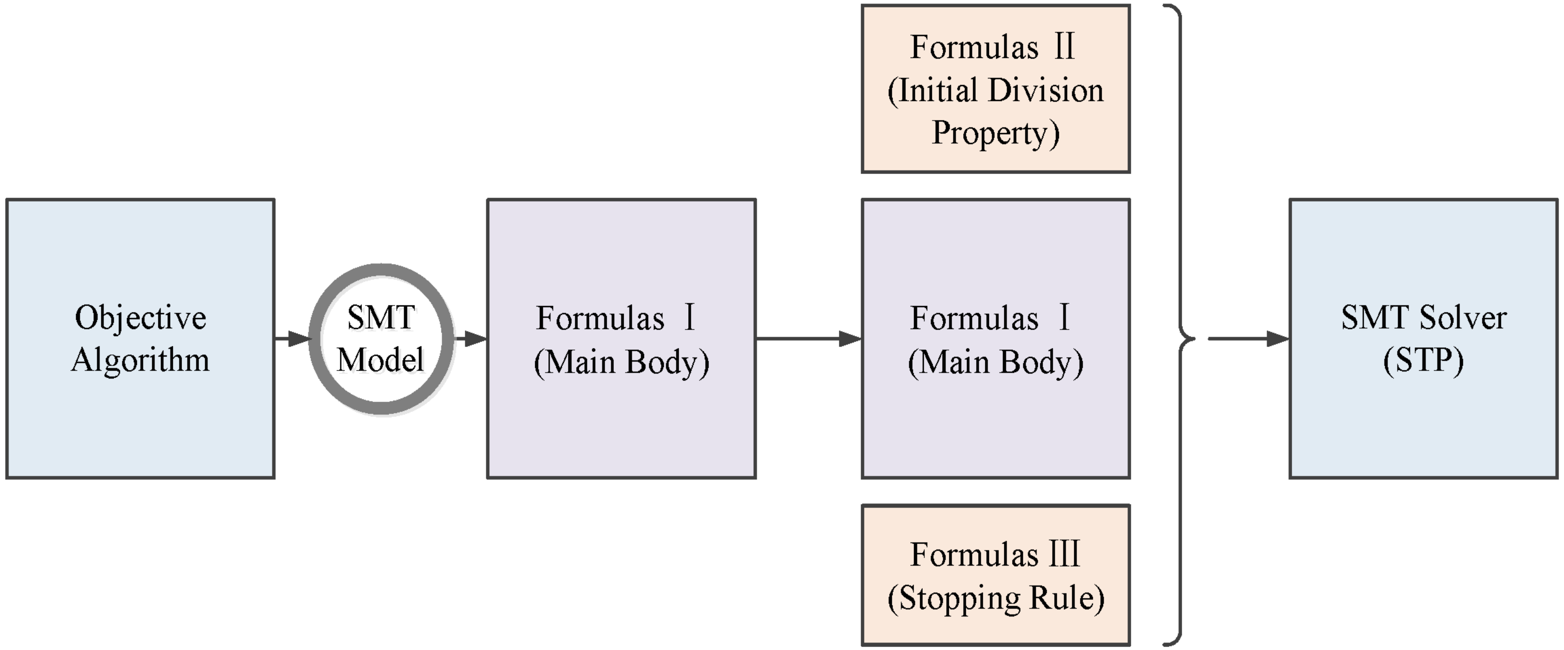
- Three-Subset DP **indicates** the sum of one bit of all the ciphertexts is

0 or 1 or Unknown

- Three-Subset DP is **more accurate** than any other division property

What is Automatic Search?

- **Tools** from **graph theory** can solve **constraint problems**
- Transform **cryptologic problems** into **constraint problems**
- **Solve** the constraint problems

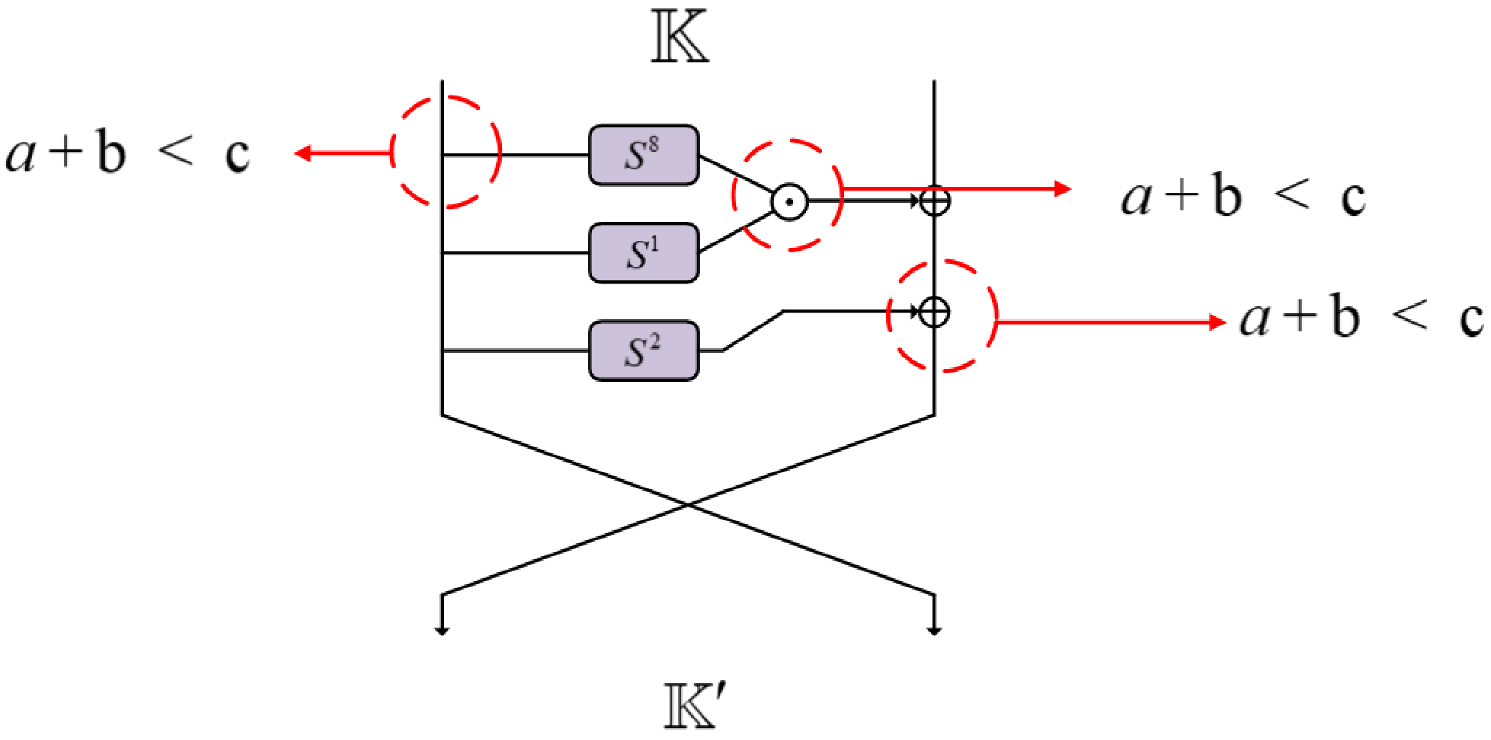


Why Automatic Search is Needed?

- C(python, etc.)-programming will cost **too much** time to write
- **Not easy** to optimize for the efficiency
- Concentration can be focused on the **problem itself**
- …

Automatic Search for Two-Subset Division Property

- Xiang et al. modeled **two-subset DP based MILP@Asiacrypt16**



Difficult to Model Three-Subset Division Property

- Propagation Rules of XOR for Two-Subset and Three-Subset DP are

ESSENTIALLY DIFFERENT!

- Two-Subset Division Property

$$\mathbb{K}' \leftarrow (\boldsymbol{k}_1 + \boldsymbol{k}_2, \boldsymbol{k}_3, \boldsymbol{k}_4, \ldots, \boldsymbol{k}_m)$$

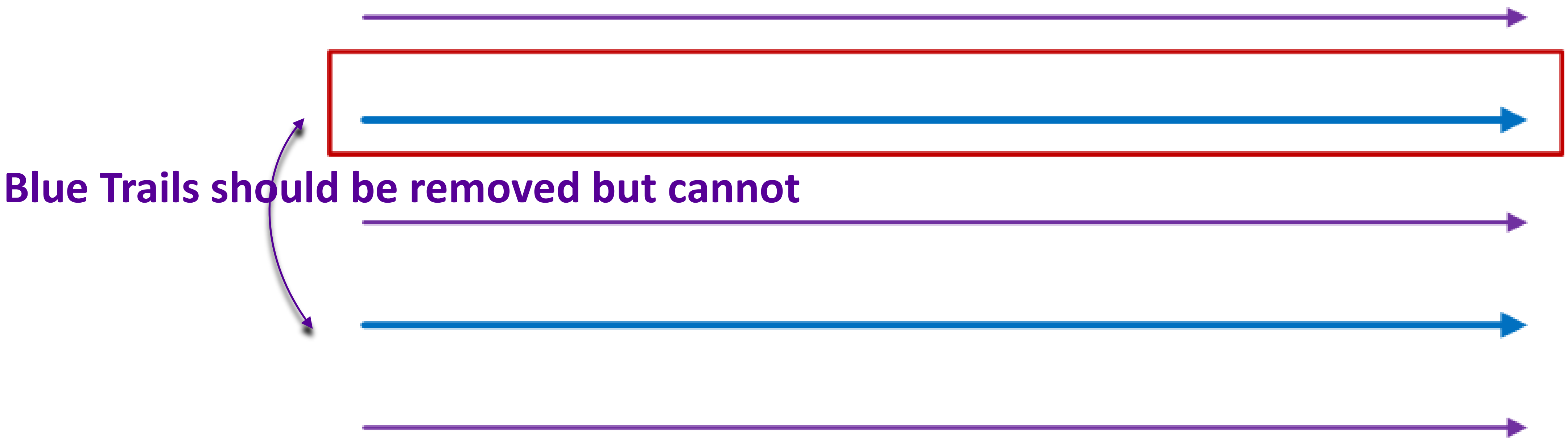
- Three-Subset Division Property

$$\mathbb{L}' \xleftarrow{\boldsymbol{x}} (\boldsymbol{l}_1 + \boldsymbol{l}_2, \boldsymbol{l}_3, \boldsymbol{l}_4, \ldots, \boldsymbol{l}_m)$$

Removed if exits

Why Is It So Difficult?

At any time, the automatic search tool can process only one trial



Division Trails

RSAConference2019

OUTLINE

1. Background of Division Property and Automatic Search
2. ***Motivation and Contribution***
3. A Variant of Three-Subset Division Property (VTDP)
4. Automatic Search for VTDP
5. Applications
6. Summary

Motivations

- Three-Subset Division Property can **find more distinguishers**
- It still **cannot be modeled** by automatic search methods

Contributions

- A **new division property** is proposed
- **More** integral distinguishers than two-subset division property
- **Improvement** of the results of SIMON, SPECK and KATAN

OUTLINE

1. Background of Division Property and Automatic Search
2. Motivation and Contribution
3. ***A Variant of Three-Subset Division Property (VTDP)***
4. Automatic Search for VTDP
5. Applications
6. Summary

Variant Three-Subset Division Property

Rule (Variant XOR)

Let F be a function compressed by an XOR, where the input $(x_1, x_2, \ldots, x_m)$ takes values of $(\mathbb{F}_2)^m$, and the output is calculated as $(x_1 \oplus x_2, x_3, \ldots, x_m)$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input and output multiset, respectively. Assuming that $\mathbb{X}$ has $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$, $\mathbb{Y}$ has $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$, where $\mathbb{K}'$ is computed from $\boldsymbol{k} \in \mathbb{K}$ s.t. $(k_1, k_2) = (0,0), (1,0),$ or $(0,1)$ as

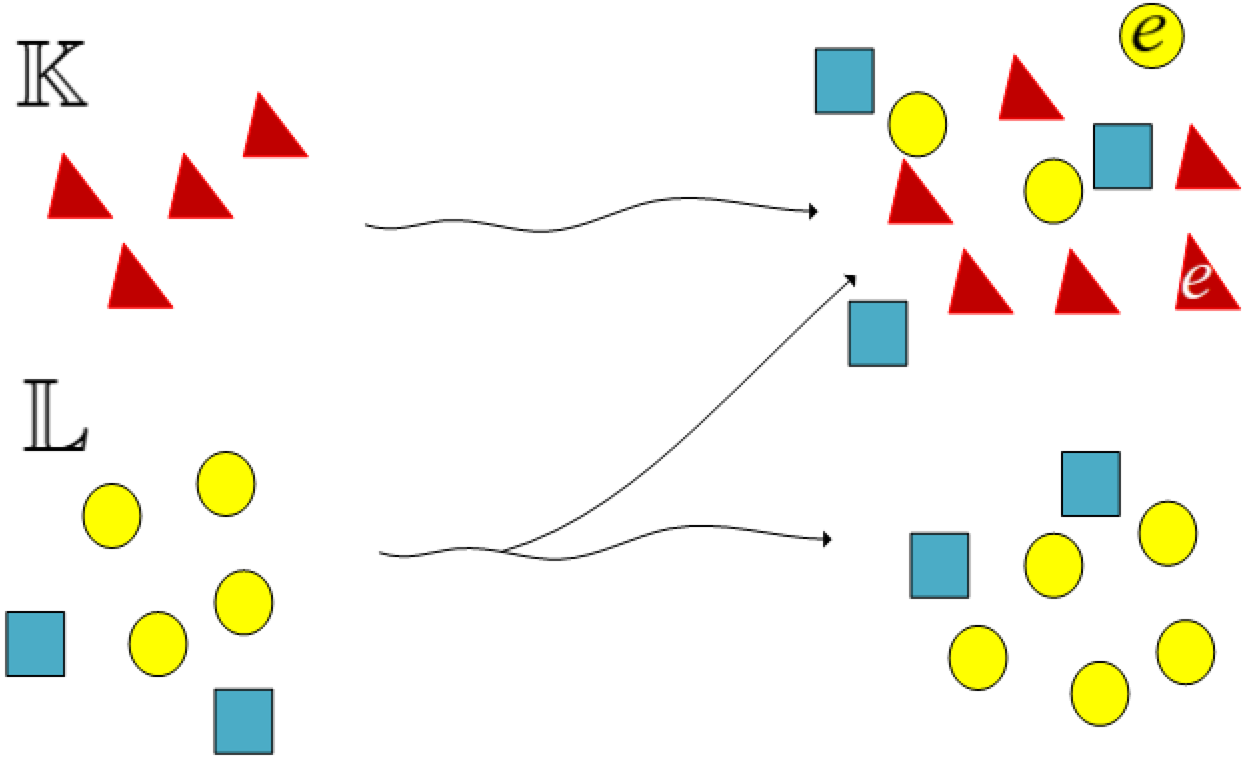
$$\mathbb{K}' \leftarrow (k_1 + k_2, k_3, k_4, \ldots, k_m).$$

Moreover, $\mathbb{L}'$ is computed from $\boldsymbol{l} \in \mathbb{L}$ s.t. $(l_1, l_2) = (0,0), (1,0),$ or $(0,1)$ as

$$\mathbb{L}' \leftarrow (l_1 + l_2, l_3, l_4, \ldots, l_m),$$

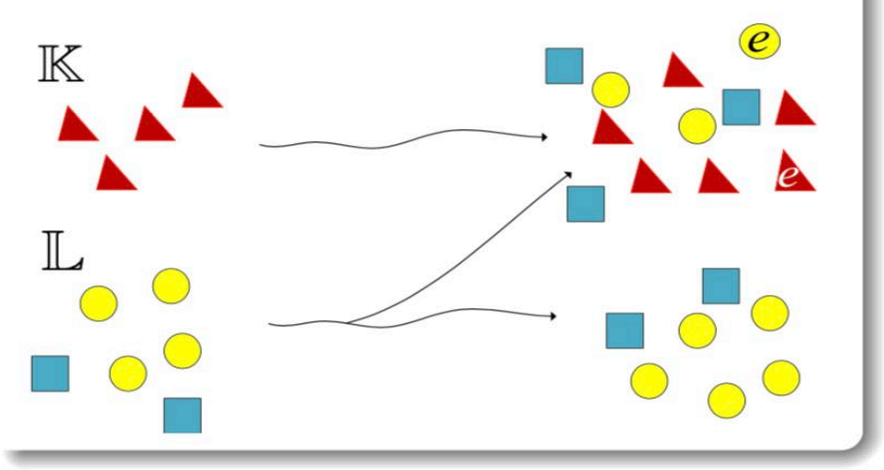
Variant XOR Propagation Rules

- Duplicated vectors will not be removed
- $\mathbb{L}' \overset{x}{\leftarrow} (l_1 + l_2, l_3, l_4, \dots, l_m) \longrightarrow \mathbb{L}' \leftarrow (l_1 + l_2, l_3, l_4, \dots, l_m)$

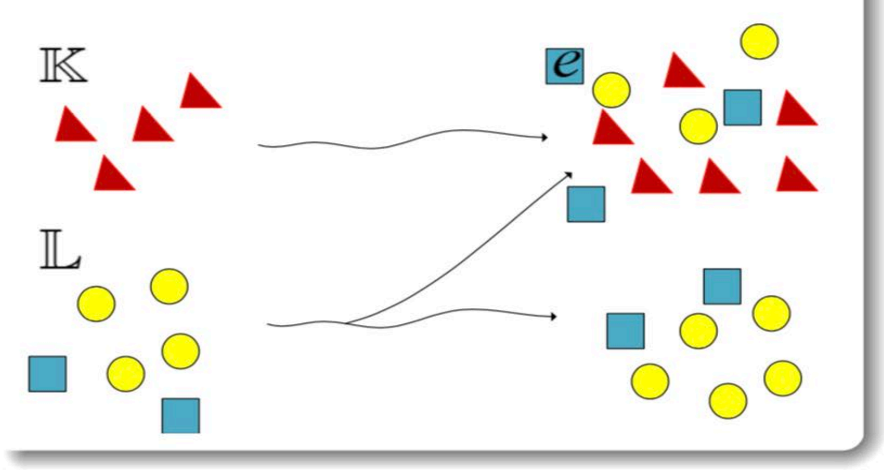


Relationship of OTDP and VTDP

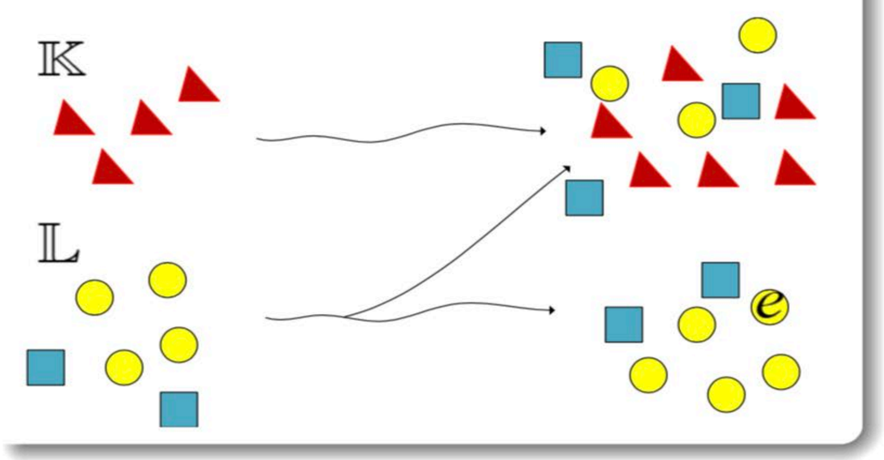
1 OTDP: unknown VTDP: unknown



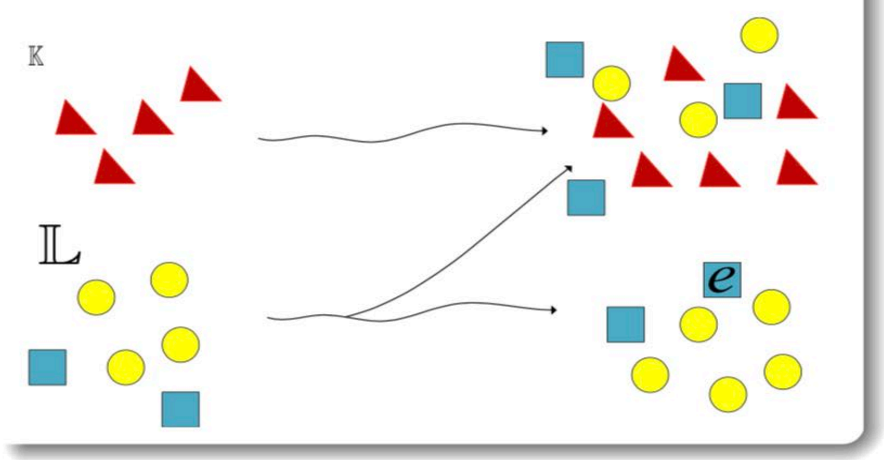
2 OTDP: constant VTDP: unknown



3 OTDP: odd VTDP: odd

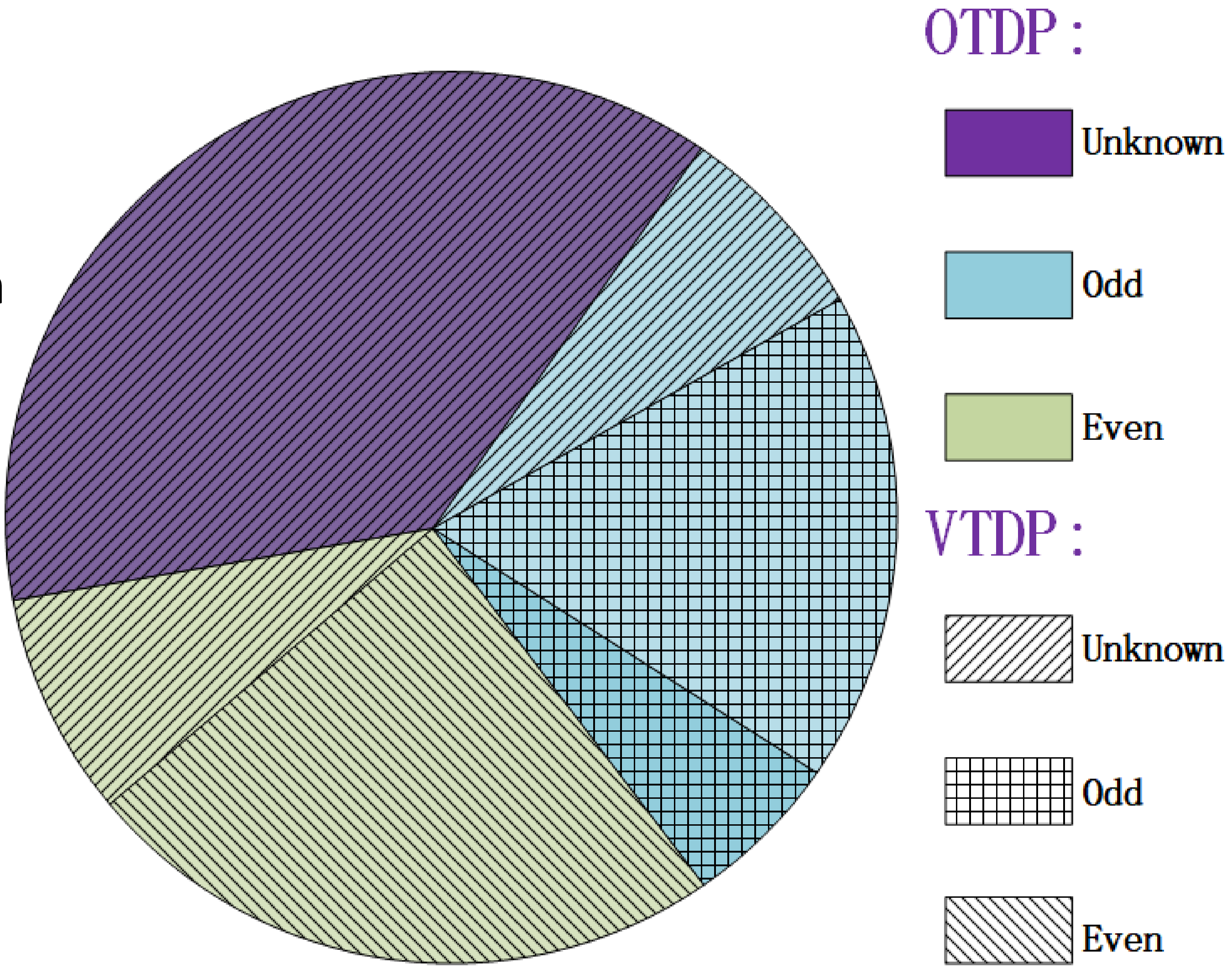


4 OTDP: even VTDP: odd



Relationship between VTDP and OTDP

- More bits are indicated unknown
- Some even-parity bits are indicated Odd-parity



RSAConference2019

OUTLINE

1. Background of Division Property and Automatic Search
2. Motivation and Contribution
3. A Variant of Three-Subset Division Property (VTDP)
4. ***Automatic Search for VTDP***
5. Applications
6. Summary

Propagation Rule of Key-XOR

- Some new vectors are **generated** from $\mathbb{L}$ and **appended** into $\mathbb{K}$
  - $l \in \mathbb{L}$, $l' = (l_0, l_1, \dots, \boldsymbol{l_i} \vee \mathbf{1}, \dots, l_{s-1})$ for $l_i = 0$

$$(\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}) \rightarrow \{(\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}), (\mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{0}), (\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{1})\}$$

- Two problems in **automatic search model**?
  - **How to generate** the new vectors?
  - **How to insert them** into $\mathbb{K}$?

Models of Key-XOR for Three-subset Division Property

Model the VTDP for Key-XOR

1. Allocate n-bit variables $\mathcal{V}_j$ $(j \in \{0, 1, 2, \ldots, s-1\})$. Check each bit of $\mathcal{L}$, i.e., $\mathcal{L}[0], \mathcal{L}[1], \ldots, \mathcal{L}[s-1]$, and assign $\mathcal{V}_j$ as follows,

$$\mathcal{V}_j = \begin{cases} \mathcal{L} \vee \vec{e}_j, & \text{if } \mathcal{L}[j] = 0, \\ \vec{1}, & otherwise, \end{cases}$$

STP ASSERT $\mathcal{L}^j =$ IF $\mathcal{L}[j] = 0$ THEN $\mathcal{L} \vee \vec{e}_j$ ELSE $\vec{1}$ ENDIF;

2. Let $\{\mathcal{K}'\} = \{\mathcal{K}\} \cup \{\mathcal{V}_0\} \cup \{\mathcal{V}_1\} \cup \cdots \cup \{\mathcal{V}_{s-1}\}$.

STP ASSERT $\mathcal{K}' = \mathcal{K}$ OR $\mathcal{K}' = \mathcal{V}_0$ OR $\mathcal{K}' = \mathcal{V}_1$ OR $\ldots$ OR $\mathcal{K}' = \mathcal{V}_{s-1}$;

Initial Rules for Three-subset Division Property

Initial Rules

Let $((\mathcal{K}_0^0, \mathcal{K}_1^0, \ldots, \mathcal{K}_{n-1}^0), (\mathcal{L}_0^0, \mathcal{L}_1^0, \ldots, \mathcal{L}_{n-1}^0))$ denote the initial division property, where n is the block size. The constraints on $\mathcal{K}_i^0$ and $\mathcal{L}_i^0$ are

$$\mathcal{K}_i^0 = 1, \text{for } i = 0, 1, 2, \ldots, n-1.$$

$$\mathcal{L}_i^0 = \begin{cases} 1, & \text{if the } i\text{-th bit is active,} \\ 0, & \text{otherwise.} \end{cases}$$

Stopping Rules for Three-subset Division Property

Stopping Rules

1 examine whether there is a unit vector $\vec{e}_{i_0} \in \mathbb{K}$:

$$\mathcal{K}_i^r = \begin{cases} 1, & \text{if } i = i_0, \\ 0, & \text{otherwise.} \end{cases}$$

2 If not stopped. Check whether there is a unit vector $\vec{e}_{i_0} \in \mathbb{L}$:

$$\mathcal{L}_i^r = \begin{cases} 1, & \text{if } i = i_0, \\ 0, & \text{otherwise.} \end{cases}$$

RSAConference2019

OUTLINE

Applications on Some Ciphers

Cipher	Data	Round	bits	Time	Reference
SIMON32	2^{31}	14	32		TM16@FSE'16, XZBL@Asiacrpt'16
		15	3	27s	TM16@FSE'16, Ours
SIMON32(102)	2^{31}	20	1		XZBL@Asiacrpt'16
		20	3	25s	Ours
SIMON48(102)	2^{47}	28	1		XZBL@Asiacrpt'16
		28	3	9.3s	Ours
SIMON64(102)	2^{63}	36	1		XZBL@Asiacrpt'16
		36	3	1.1h	Ours
KATAN/KTANTAN32	2^{31}	99	1		SWLW@eprint
		101	1	5.6h	Ours
KATAN/KTANTAN48	2^{47}	63.5	1		SWLW@eprint
		64	1	16h	Ours
KATAN/KTANTAN64	2^{63}	72.3	1		SWLW@eprint
		72.3	2	18h	Ours
SPECK32	2^{31}	6	1		SWW@eprint
		6	2	3.5m	Ours

RSAConference2019

OUTLINE

1. Background of Division Property and Automatic Search
2. Motivation and Contribution
3. A Variant of Three-Subset Division Property (VTDP)
4. Automatic Search for VTDP
5. Applications
6. ***Summary***

Summary

- **A new division property** that can find more distinguishers
- **Automatic search model** of the variant division property
- It may bring **some new insights** into bit-based division property

RSA Conference 2019

Thanks for Your Attention!