



**RSA**<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center

**BETTER.**

SESSION ID: CRYPT-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

## 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
- 

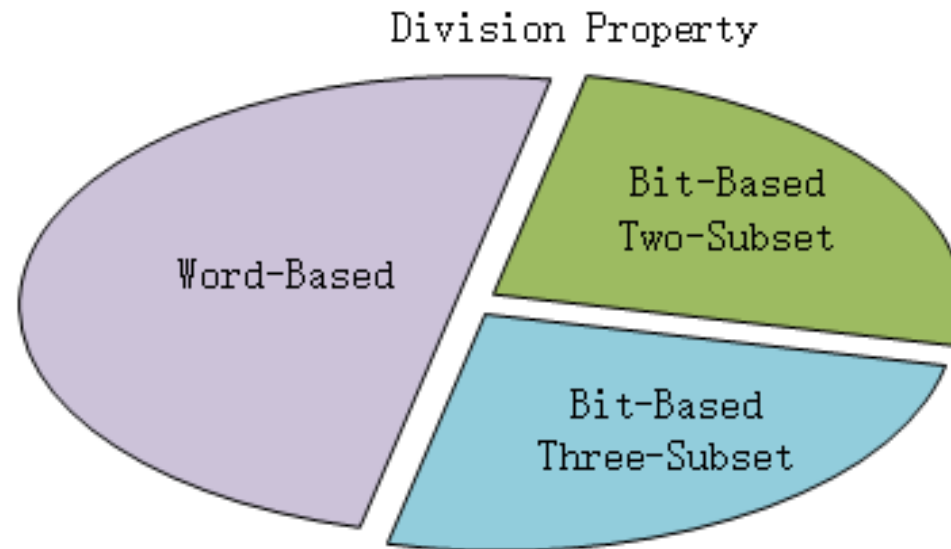
## OUTLINE

- ***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
- 
- An abstract graphic in the bottom right corner consisting of numerous thin, curved blue lines and small dots, creating a sense of motion and complexity.



# What is Division Property (DP)?

- Proposed by **Yosuke Todo** at **Eurocrypt'15**
- A technique to find **integral distinguishers** easily and efficiently
- 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 ?*

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

0                      Unknown

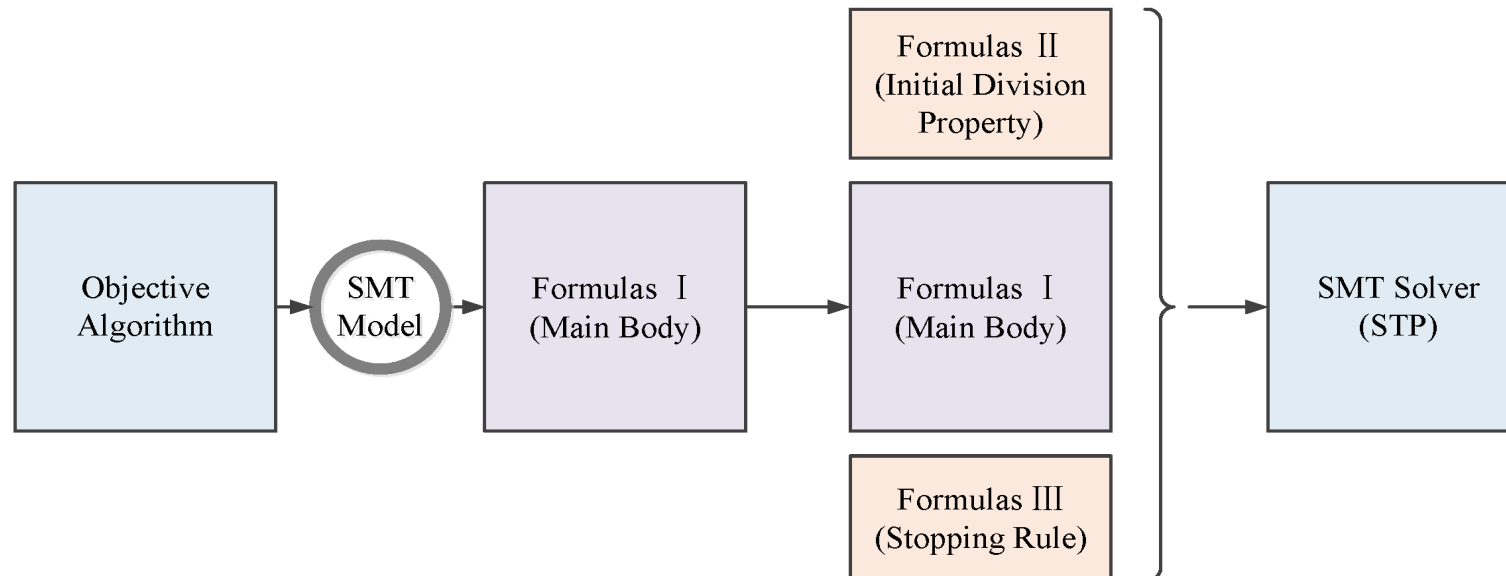
- Three-Subset DP **indicate** the sum of one bit of all the ciphertexts is

0                      1                      Unknown

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

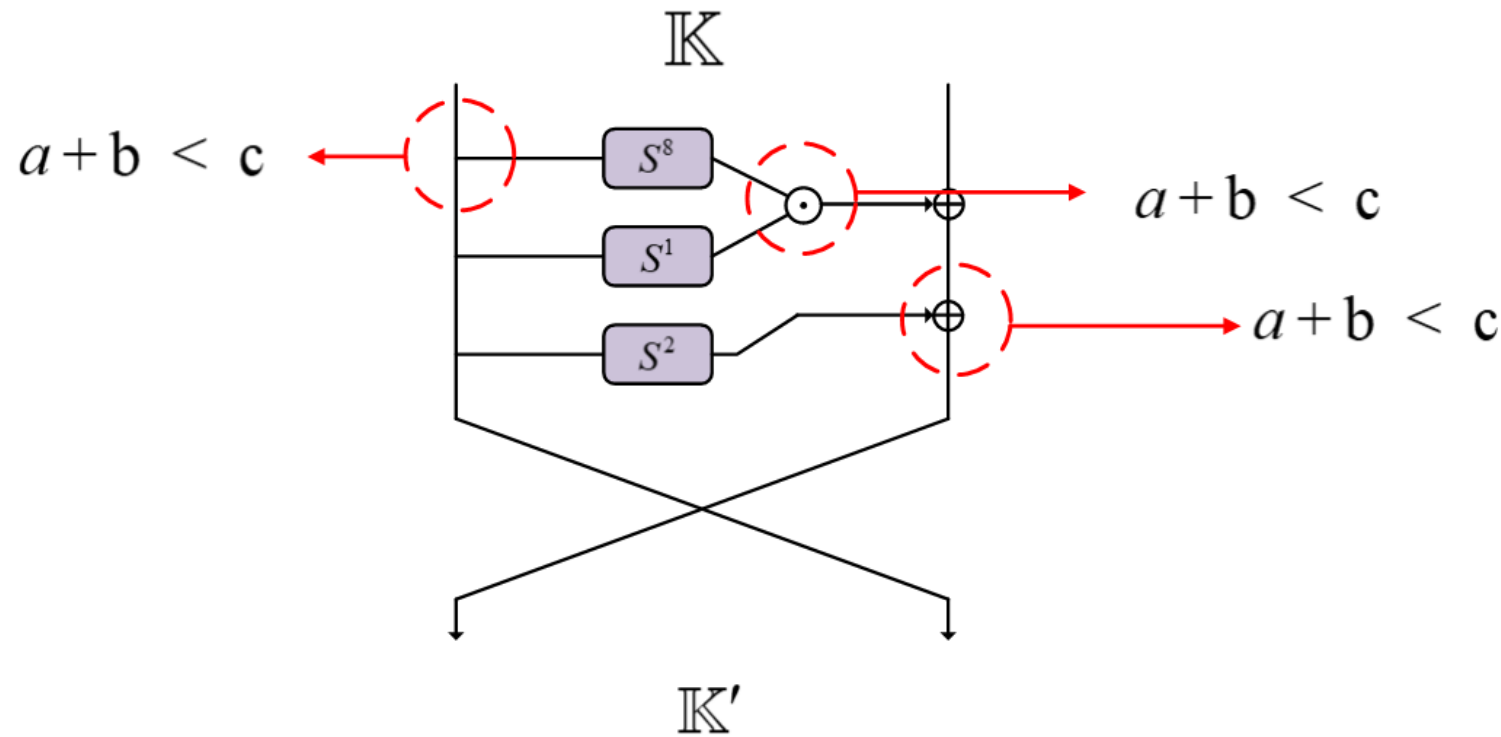
# What is Automatic Search?

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



# Automatic Search for Two-Subset Division Property

- Xiang et al. first model **two-subset DP based MILP@Asiacrypt**



# *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

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

- Three-Subset Division Property

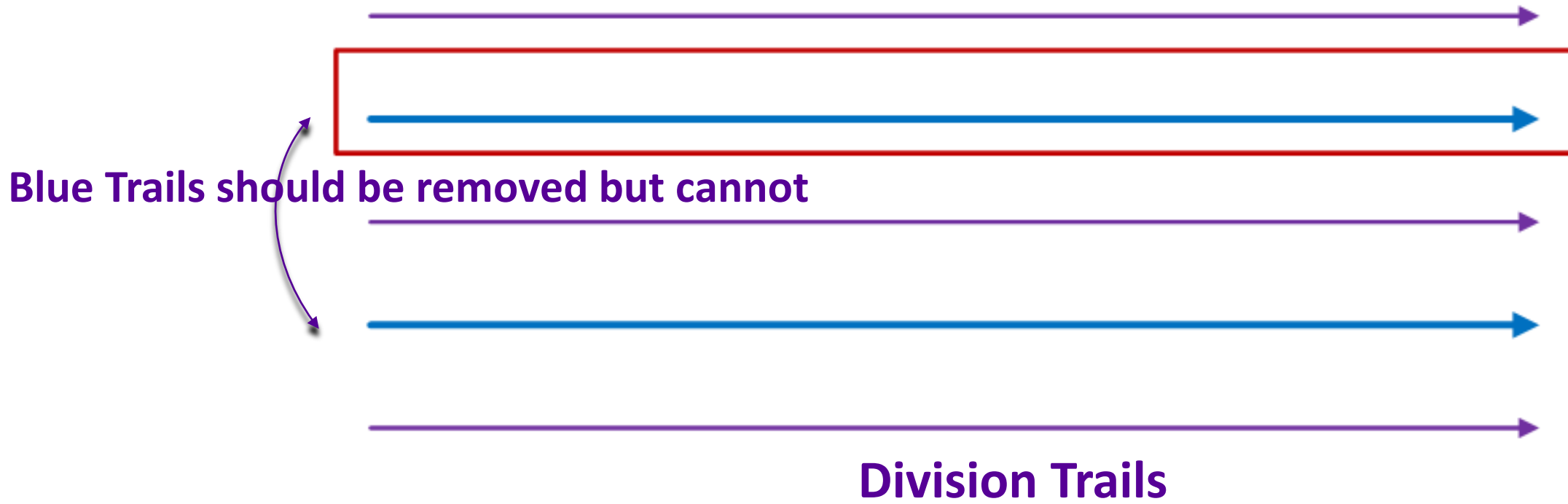
$$\mathbb{L}' \overset{x}{\leftarrow} (l_1 + l_2, l_3, l_4, \dots, l_m)$$

Removed if exits




## Why Is It So Difficult?

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



## 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
- 
- An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, light blue lines that form a complex web of overlapping circles and arcs. Small blue dots are scattered along these lines, creating a sense of motion or a network structure. The overall effect is a modern, technical-looking design element.

# Motivations


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

# Contributions

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

# RSA<sup>®</sup>Conference2019

## 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
- 

# Variant Three-Subset Division Property

## Rule (Variant XOR)

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

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

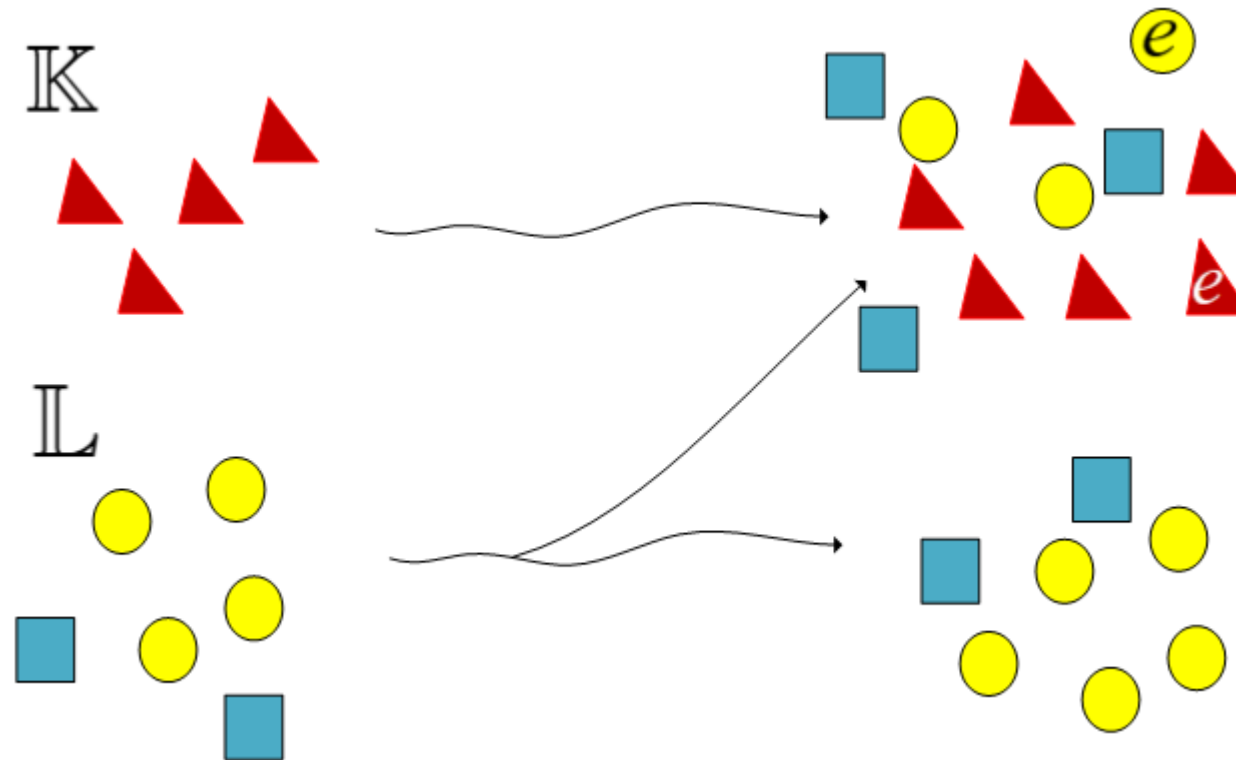
Moreover,  $\mathbb{L}'$  is computed from  $\mathbf{l} \in \mathbb{L}$  s.t.  $(l_1, l_2) = (0, 0), (1, 0)$ , or  $(0, 1)$  as

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



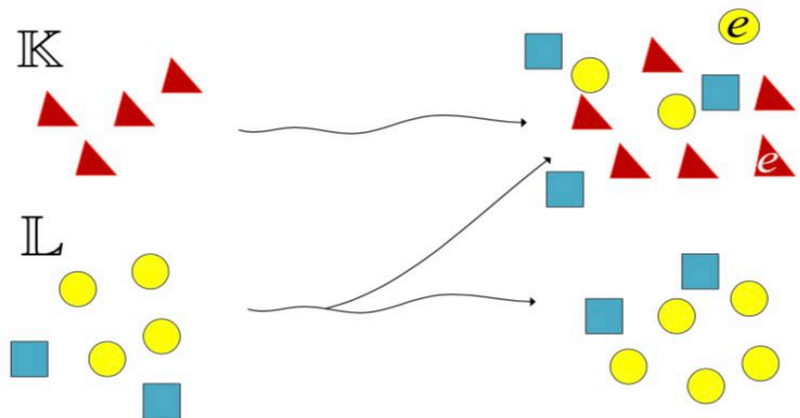
## Variant XOR Propagation Rules

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

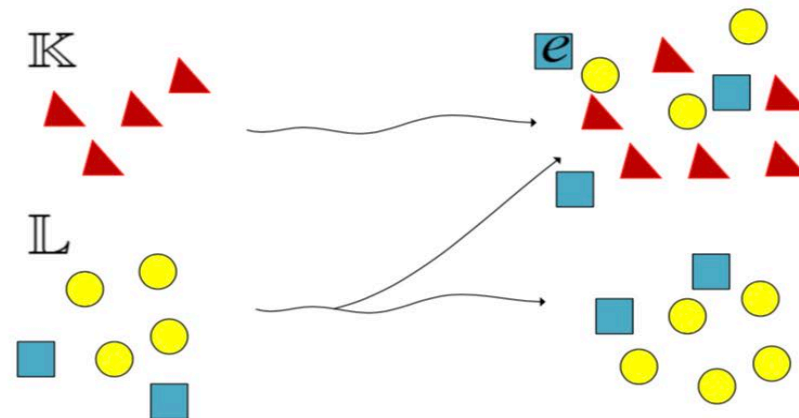


# Relationship of OTDP and VTDP

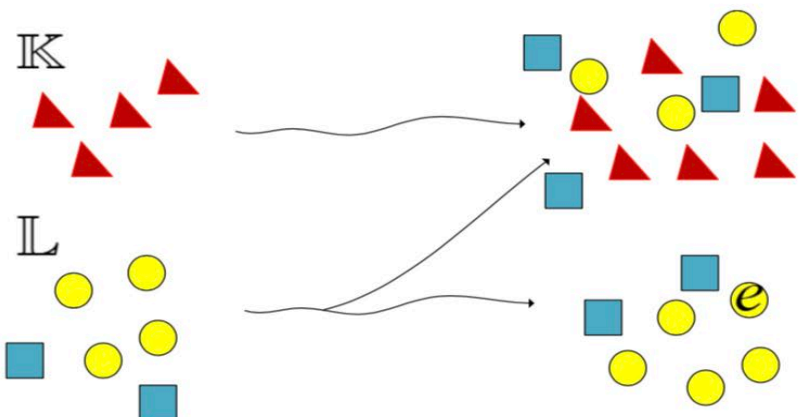
1 OTDP: unknown VTDP: unknown



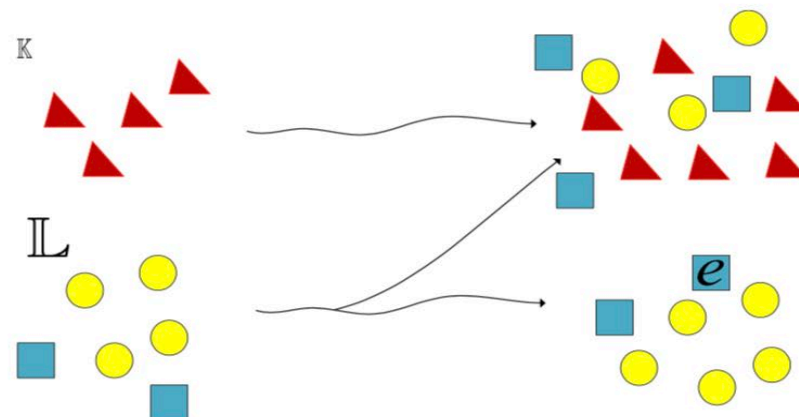
2 OTDP: constant VTDP: unknown



3 OTDP: odd VTDP: odd

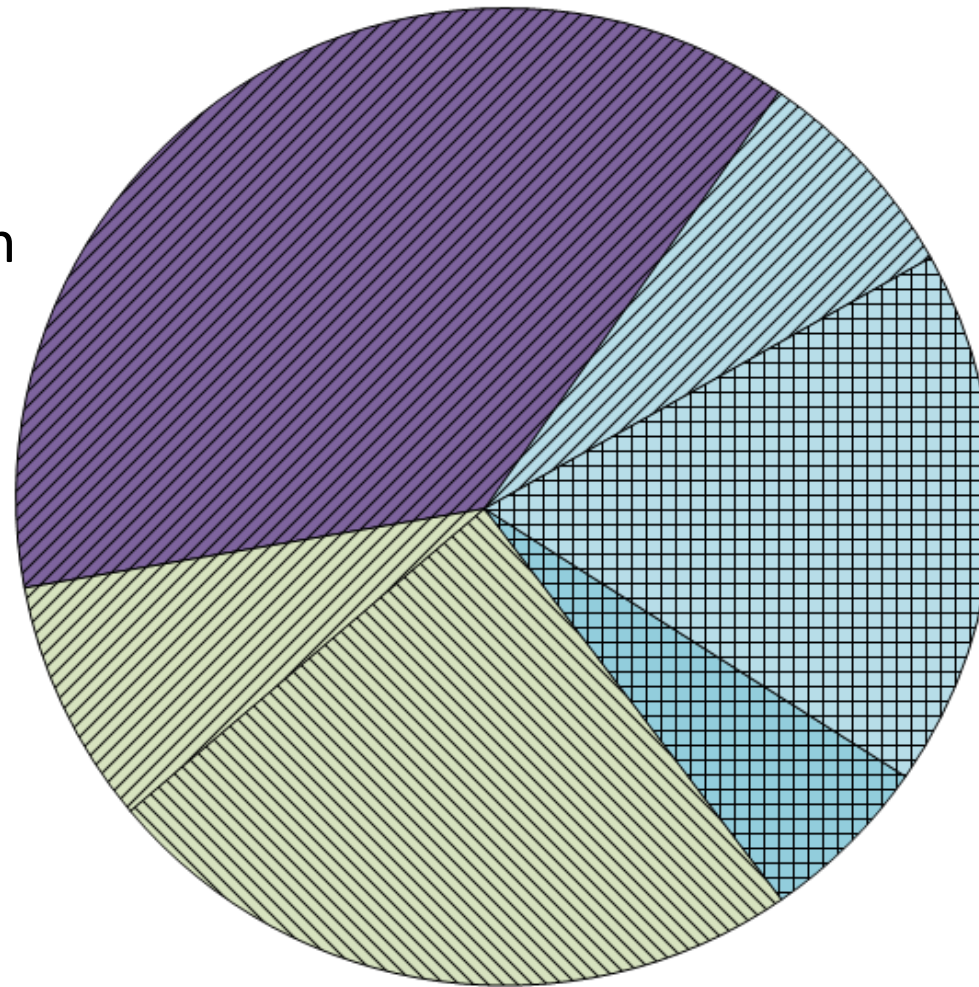


4 OTDP: even VTDP: odd



# Relationship between VTDP and OTDP

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



# RSA<sup>®</sup>Conference2019

## 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
- 
- An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, light blue lines that form a complex web of overlapping circles and arcs. Small blue dots are scattered along these lines, creating a sense of motion or a network structure. The overall effect is a modern, technical-looking design element.



# Models of Key-XOR for Three-subset Division Property

## Model the VTDP for Key-XOR

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

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

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

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

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



# Initial Rules for Three-subset Division Property

## Initial Rules

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

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

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

# 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  $\vec{e}_{i_0} \in \mathbb{L}$ :

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

## 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**

# 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

**RSA**Conference2019

**Thanks for Your Attention!**

