Structural Evaluation by Generalized Integral Property

Yosuke Todo

NTT Secure Platform Laboratories

For Eurocrypt 2015 (@Sofia)

Overview

Integral Distinguisher (Daemen 97, Knudsen and Wagner 02)

- Exploit the set of chosen plaintexts that the XOR of the corresponding ciphertexts always becomes 0.
- Already have two methods to create distinguisher.

1. Integral property	mainly exploit the diffusion part.
2. Degree estimation	mainly exploit the confusion part.

Propose a new method to create integral distinguisher

- Propose a new property called “Division Property.”
- This property can exploit both confusion and diffusion.

Summarization of Structural Evaluation

Innovative R&D by NTT

Structural Evaluation (Generic Attack)

Exploit only the feature of the network.
It is applicable to large classes of block ciphers.

Add some natural assumptions.

(ℓ, d)-Feistel ℓ-bit F-function with degree d.
(ℓ, d, m)-SPN m concatenating ℓ-bit S-boxes with degree d.

Structure	F-function	vulnerable rounds		Example
(16,2)-Feistel	Non-bijection	9R	2^{31} CPs	Simon 32
(64,2)-Feistel	Non-bijection	14R	2^{127} CPs	Simon 128
(4,3,32)-SPN	-	7R	2^{124} CPs	Serpent
(5,2,320)-SPN	-	15R	2^{1595} CPs	Keccak-f[1600]

NTT

Outline

1. **Background**
   - **What's Integral Attack?**
   - **Higher-Order Differential?**
2. Division Property
3. Vectorial and Collective Division Properties
4. Application to Feistel Cipher
5. Conclusion

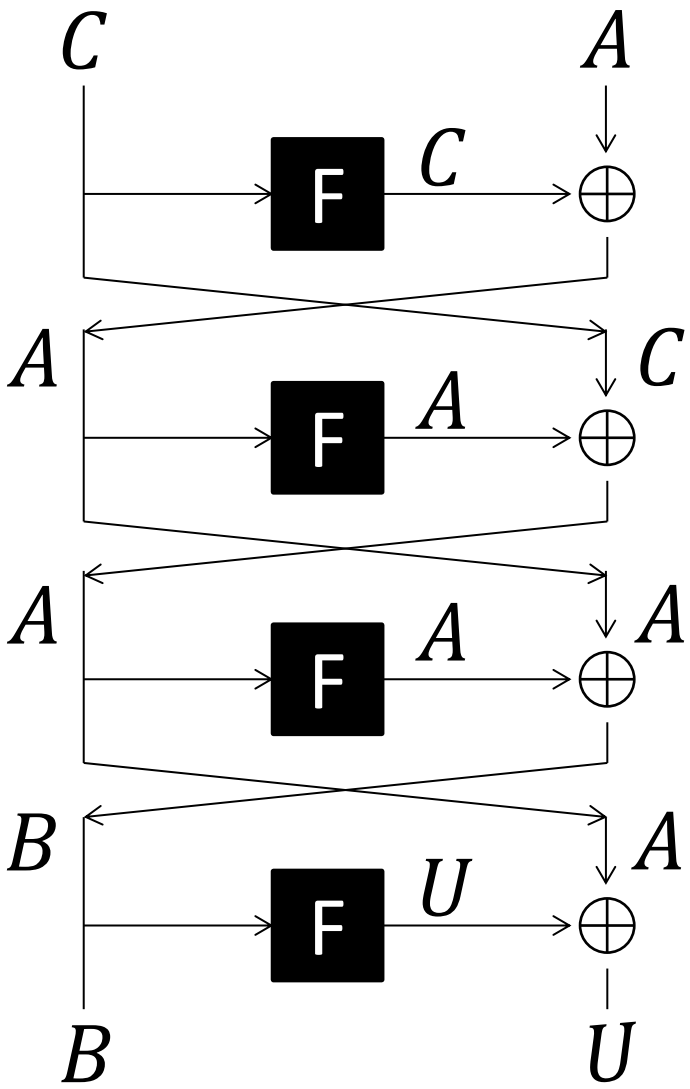
What's Integral Attack?

- Classical differential attack observes the propagation of differences between two values.
- Integral attack treats the propagation of the sum of many values.
- History.
  - It has several names,
    - Higher-Order Differential attack [Lai, 94]
    - Square attack [Daemen et al., FSE97],
    - Saturation attack [Lucks, FSE01],
    - Integral attack [Knudsen, FSE02].
  - We use "integral attack" in my talk.

Integral Property

- When we search for the integral distinguisher, we often use the propagation of the integral property.
- Integral property.
  - A : Every value appears the same number.
  - B : The XOR of all texts is 0.
  - C : The value is fixed to a constant.
  - U : The set does not have useful property.

Propagation of Integral Property



Higher-Order Differential?

- Outline is the same as that of integral attack.
- Exploit the algebraic degree of a function.
  - Choose a set of chosen plaintexts whose (d+1) bits of the input are active.
  - If the algebraic degree is at most d, the sum of the output is always 0.
- How estimate the accurate degree?
  - It is very difficult to estimate the accurate algebraic degree.

Outline

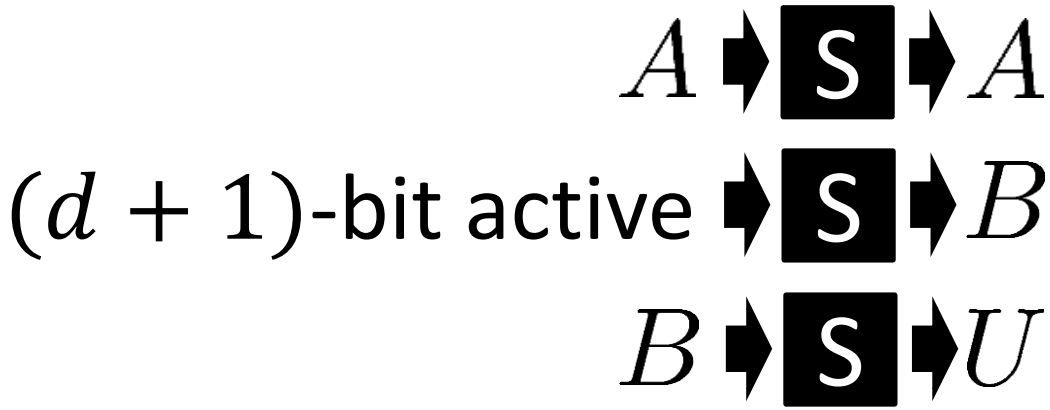
1. Background
2. **Division Property**
   - **Concept**
   - **How to evaluate multi-set by using π_u**
   - **Redefinition of integral property**
   - **Propagation characteristic**
3. Vectorial and Collective Division Properties
4. Application to Feistel Cipher
5. Conclusion

Concept

- Intuition.
  - Integral property.
    - It treats S-box as a black box.
    - It does not clearly exploit the degree of S-box.
    - It mainly exploits the **diffusion** of block cipher.
  - Degree estimation.
    - It treats the algebraic degree of S-box.
    - It is very difficult to estimate accurate degree.
    - It mainly exploits the **confusion** of block cipher.
- Motivation.
  - How can we exploit both confusion and diffusion?

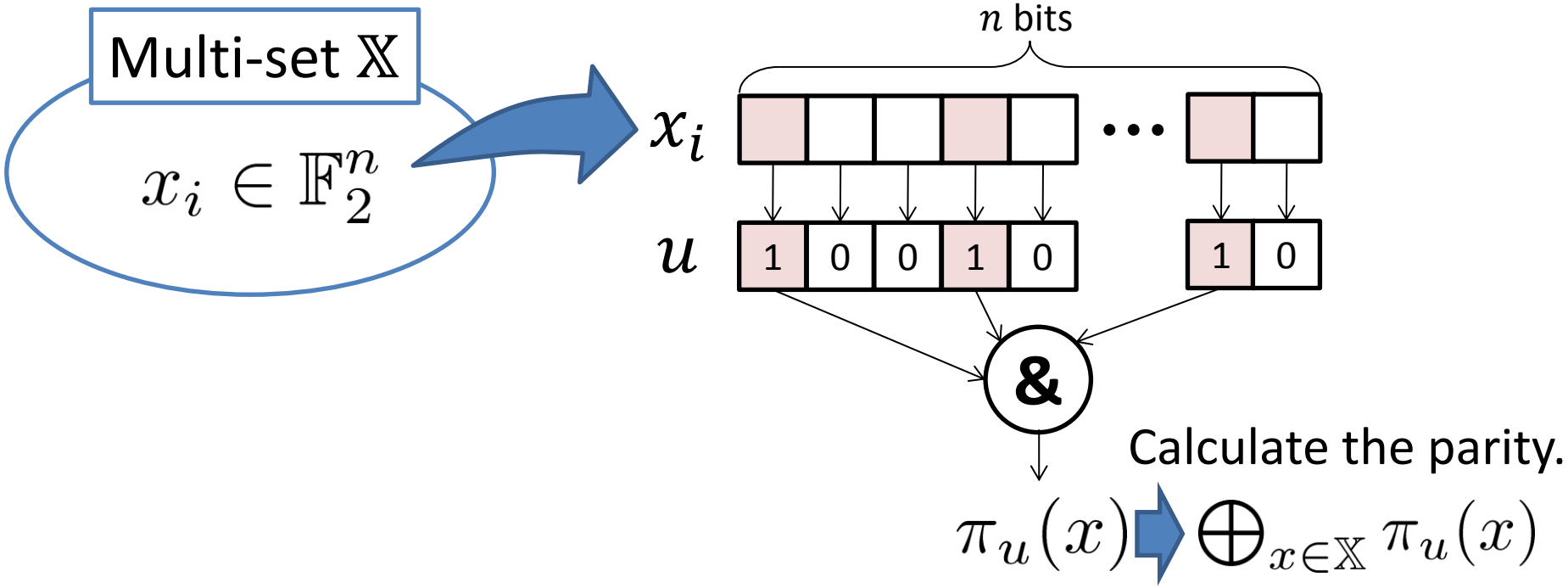
How do we exploit both properties?

- Assume that the degree of S-box is at most d.



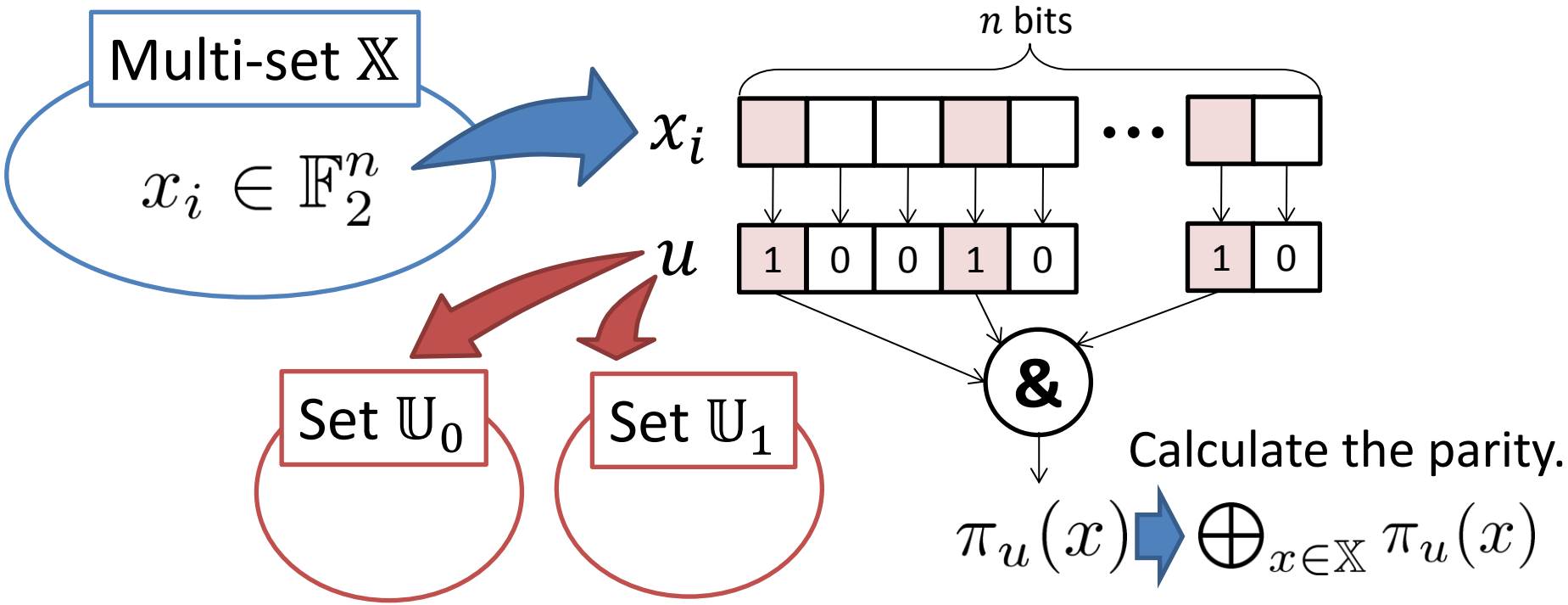
- Believe that some useful properties are hidden between "A" and "B".
- To exploit the useful property, we redefine each property by the same statement, and reveal the useful property.

Bit Product Function π_u



- Choose bits that corresponding bits of u are 1, and output the AND.
- Evaluate the parity of $\pi_u(x)$ for all elements.

Bit Product Function π_u



- Evaluate whether the parity becomes 0 or 1.
- If the parity is 0, the value of u belongs to $\mathbb{U}_0$.
- If the parity is 1, the value of u belongs to $\mathbb{U}_1$.

Example

- Assume that elements of $\mathbb{X}$ take 3-bit value.

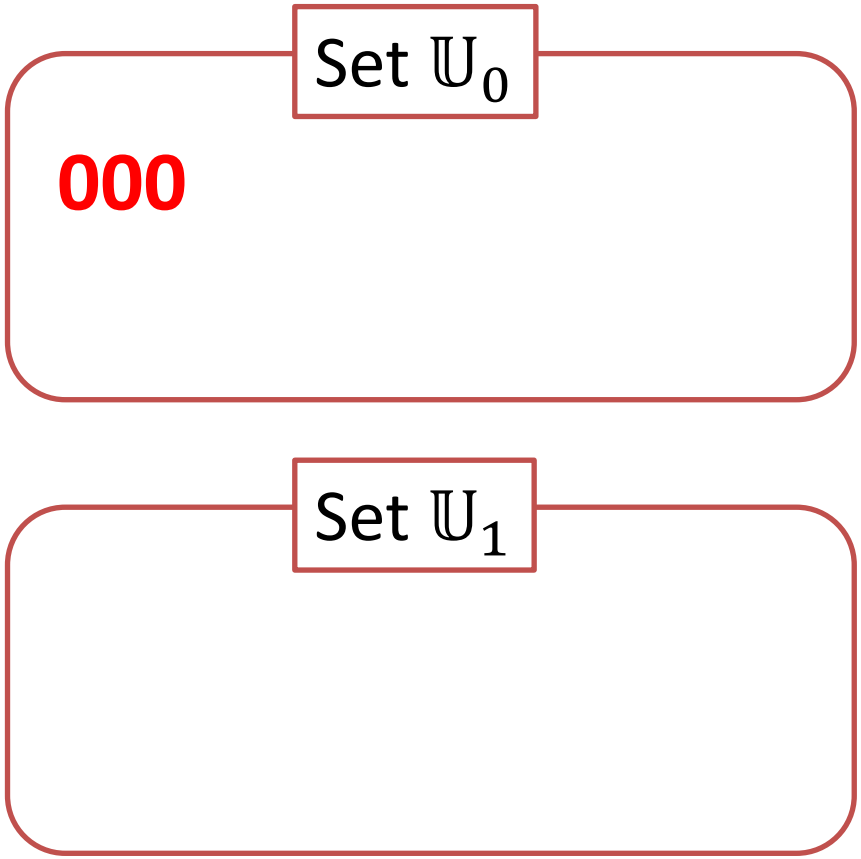
Set $\mathbb{X}$	$\pi_u(x)$
000	
001	
010	
011	
100	
101	
110	
111	
Parity	

- All values appear only once in the set $\mathbb{X}$.
- The set $\mathbb{X}$ has the integral property A.
- Calculate the parity of $\pi_u(x)$, and evaluate whether u belongs to $\mathbb{U}_0$ or $\mathbb{U}_1$.

Example

When u of π_u is equal to **000**.

Set $\mathbb{X}$	$\pi_{000}(x)$
000	0
001	0
010	0
011	0
100	0
101	0
110	0
111	0
Parity	**0**



Example

When u of π_u is equal to **001**.

Set $\mathbb{X}$	$\pi_{001}(x)$
000	0
001	1
010	0
011	1
100	0
101	1
110	0
111	1
Parity	**0**

Set $\mathbb{U}_0$

000, **001**

Set $\mathbb{U}_1$

Example

When u of π_u is equal to **111**.

Set $\mathbb{X}$	$\pi_{111}(x)$
000	0
001	0
010	0
011	0
100	0
101	0
110	0
111	1
Parity	**1**

Set $\mathbb{U}_0$

000, 001, 010, 011,
100, 101, 110

Set $\mathbb{U}_1$

111

Another Example

Similarly, divide the set of u into $\mathbb{U}_0$ and $\mathbb{U}_1$.

Set $\mathbb{X}$	$\pi_{110}(x)$
000	0
001	0
001	0
011	0
100	0
110	1
110	1
111	1
Parity	**1**

Set $\mathbb{U}_0$

000, 001, 010, 011, 100,

Set $\mathbb{U}_1$

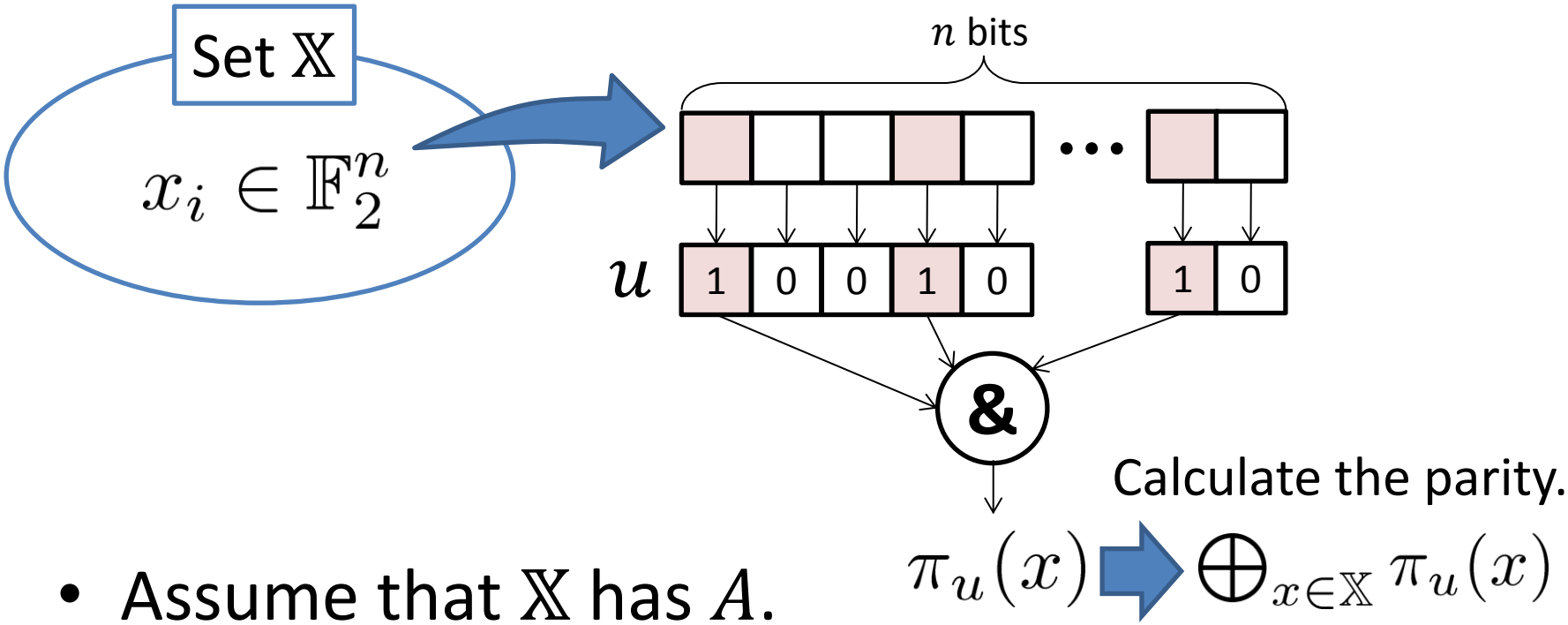
101, 110, 111

How to Evaluate Multi-Set with Unknown Elements

- In previous simple example, we know all elements of the multi-set.
- However, attackers can't know elements, but they can only know the property of the multi-set.
  - Every value appears the same number.
  - The XOR of all values becomes 0.
- We use a set $\mathbb{U}_?$ instead of $\mathbb{U}_1$.
  - If attackers can know that the parity is always 0, u belongs to $\mathbb{U}_0$.
  - Otherwise, u belongs to $\mathbb{U}_?$.

Redefinition of ALL

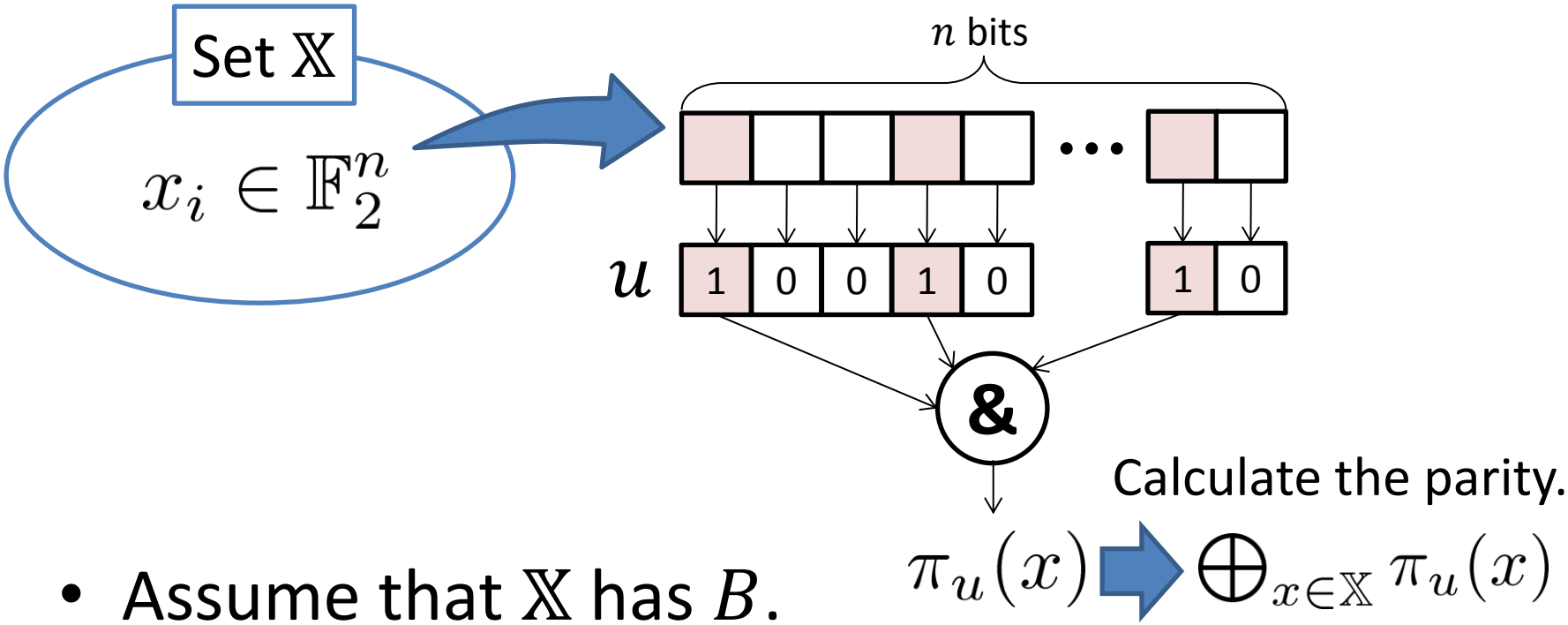
Evaluate the set by a bit product function π_u.



- Assume that $\mathbb{X}$ has A.
  - If $\boldsymbol{wt(u) < n}$, the parity is always **0**.
  - If $\boldsymbol{wt(u) = n}$, the parity becomes **unknown**.

Redefinition of BALANCE

Evaluate the set by a bit product function π_u.

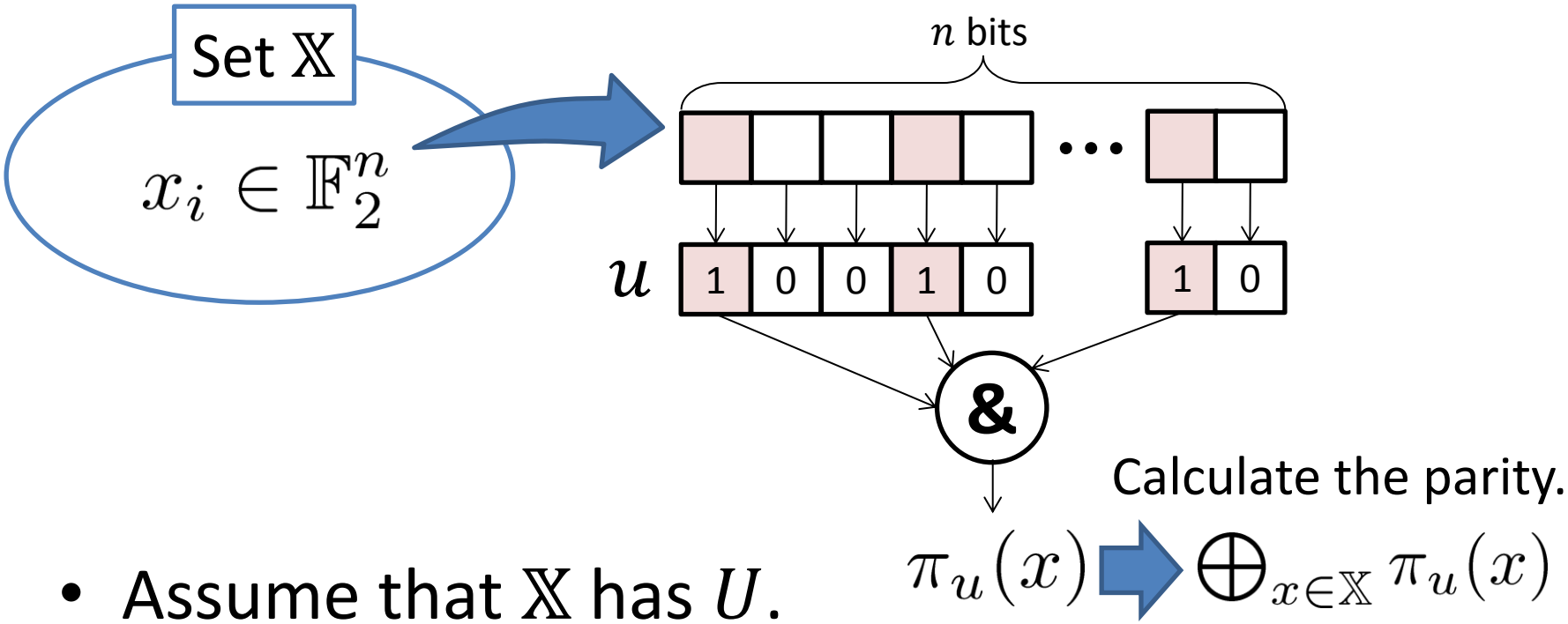


- Assume that $\mathbb{X}$ has B.
  - If $\boldsymbol{wt(u) < 2}$, the parity is always **0**.
  - If $\boldsymbol{wt(u) \geq 2}$, the parity becomes **unknown**.

Redefinition of UNKNOWN

Innovative R&D by NTT

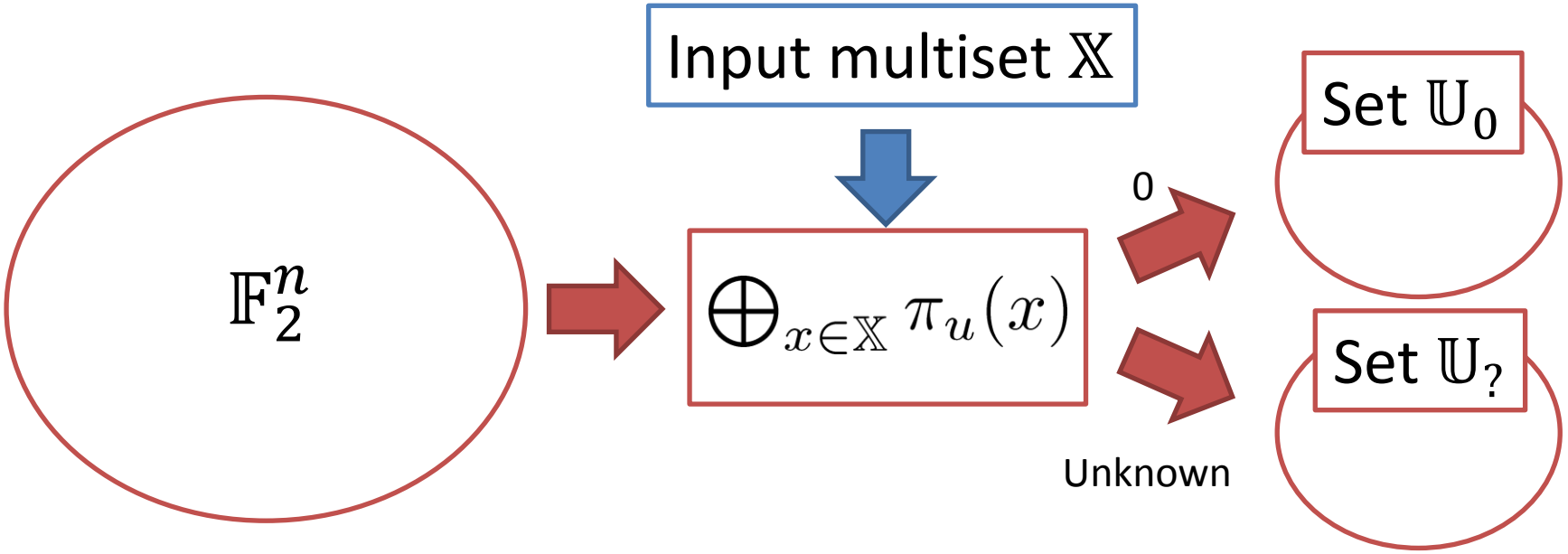
Evaluate the set by a bit product function π_u.



- Assume that $\mathbb{X}$ has U.
  - If $\boldsymbol{wt(u) < 1}$, the parity is always **0**.
  - If $\boldsymbol{wt(u) \geq 1}$, the parity becomes **unknown**.

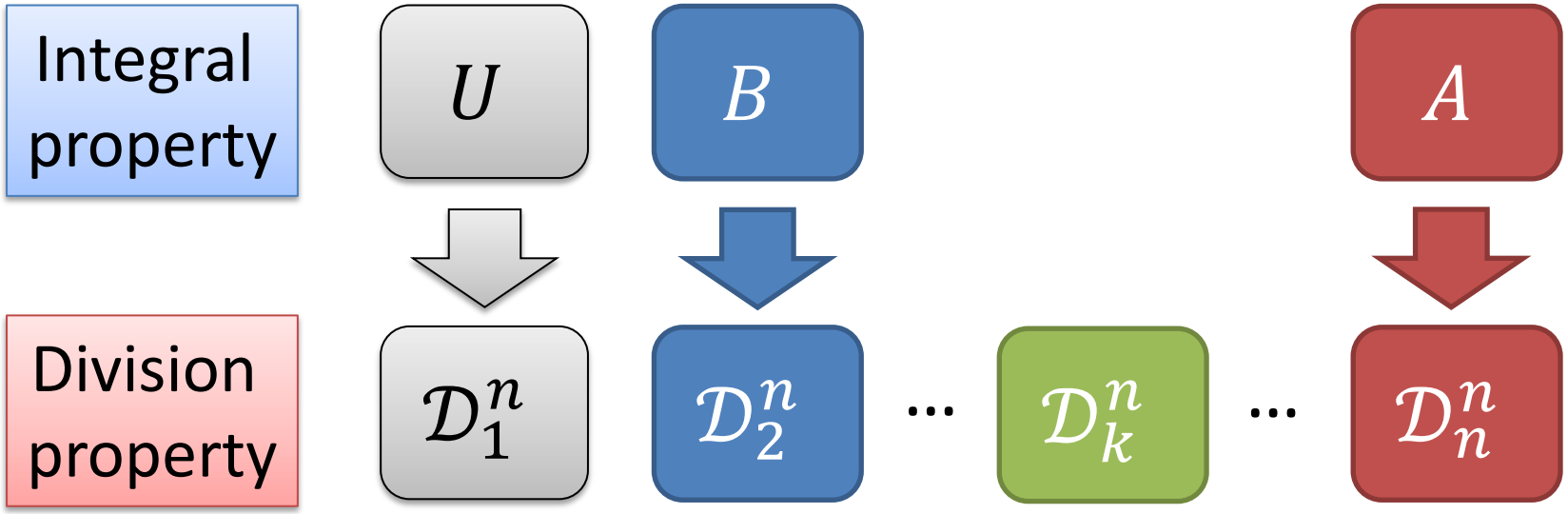
Division Property

- Division property $\mathcal{D}_k^n$
  - All n-bit values are divided into elements of the set $\mathbb{U}_0$ and those of the set $\mathbb{U}_?$.



The set of u whose $wt(u) < k$ belongs the set $\mathbb{U}_0$.

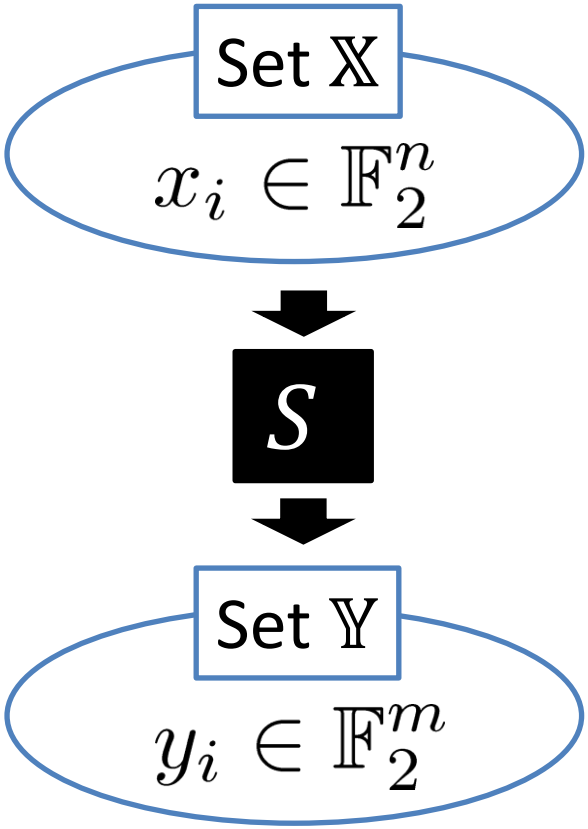
Relation between Integral and Division



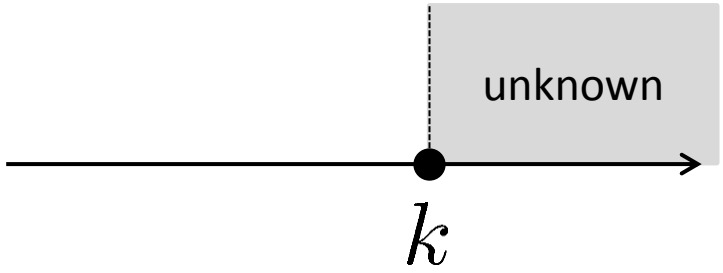
- The division property can treat the hidden property between A and B by using from $\mathcal{D}_3^n$ to $\mathcal{D}_{n-1}^n$.

Propagation

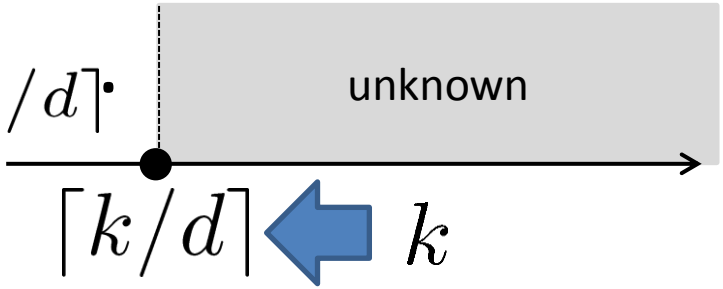
Let S be a functions from n bits to m bits, and the algebraic degree is d.



$\mathbb{X}$ has $\mathcal{D}_k^n$.

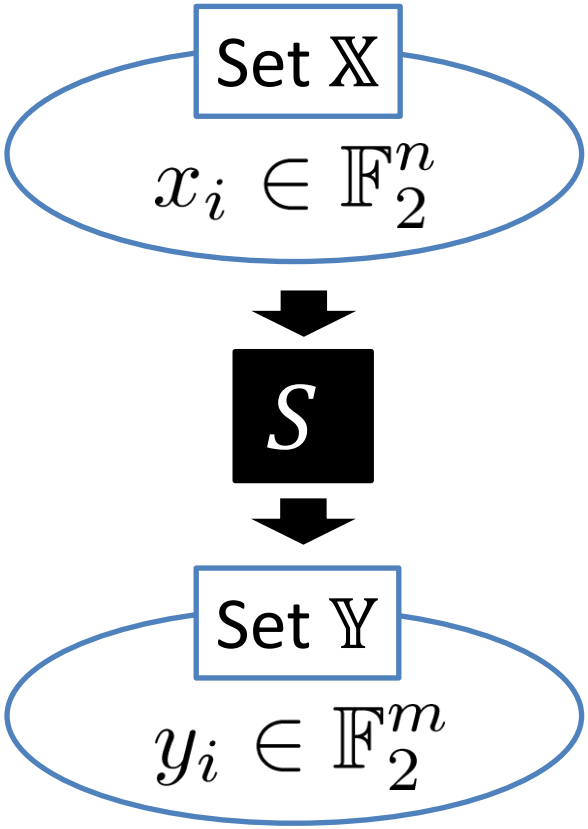


$\mathbb{Y}$ has $\mathcal{D}_{\lceil k/d \rceil}^m$.

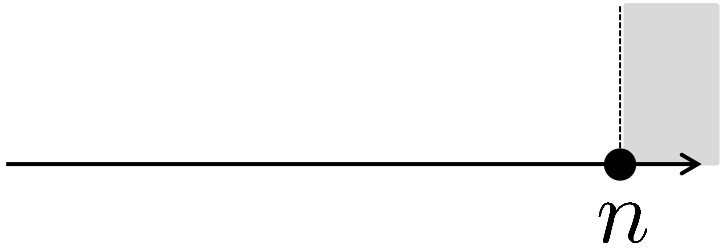


Propagation – Special Case

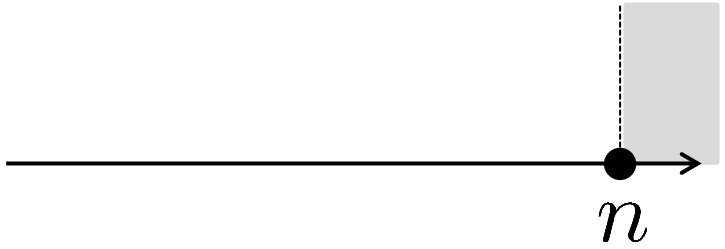
Moreover, if the function S is bijective,



$\mathbb{X}$ has $\mathcal{D}_n^n$.



$\mathbb{Y}$ has $\mathcal{D}_n^n$.

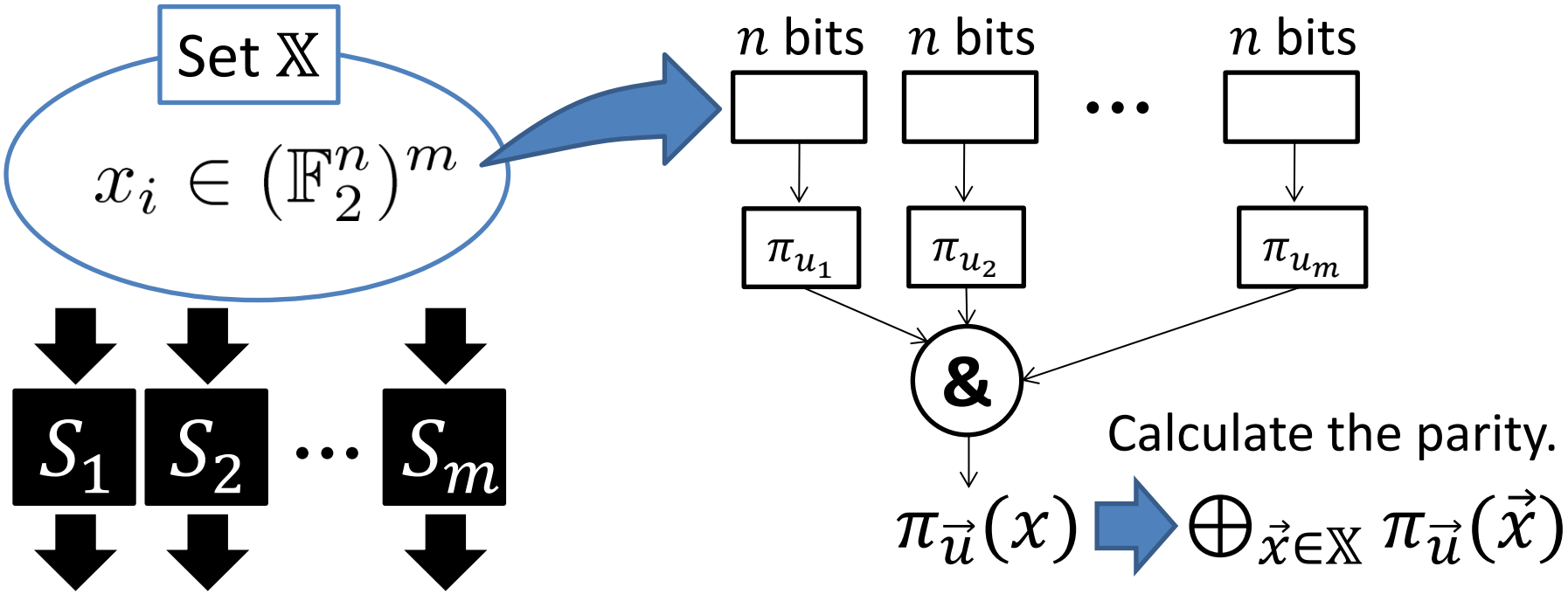


Outline

1. Background
2. Division Property
3. **Vectorial and Collective Division Properties**
   - **Definition of vectorial and collective ones**
   - **Simple example for vectorial division property**
   - **Simple example for collective division property**
4. Application to Feistel Cipher
5. Conclusion

Vectorial and collective Division Property

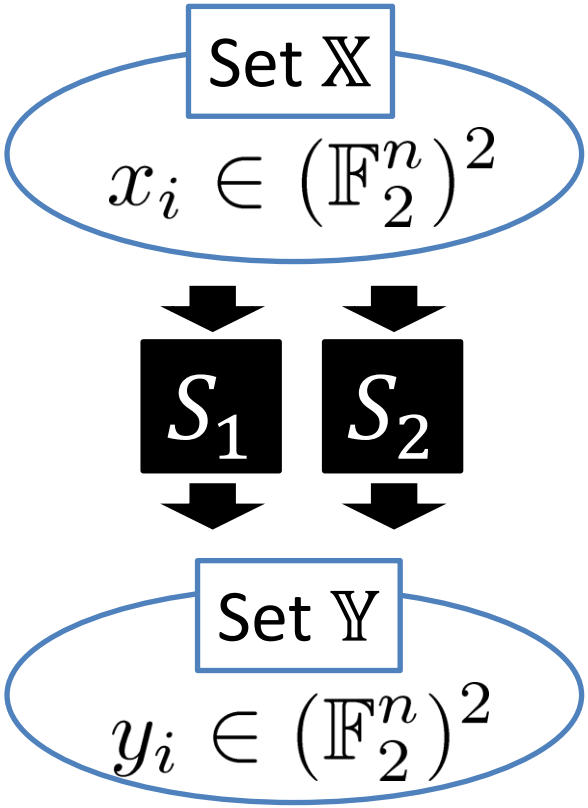
Evaluate the set by the bit product function $\pi_{\vec{u}}$.



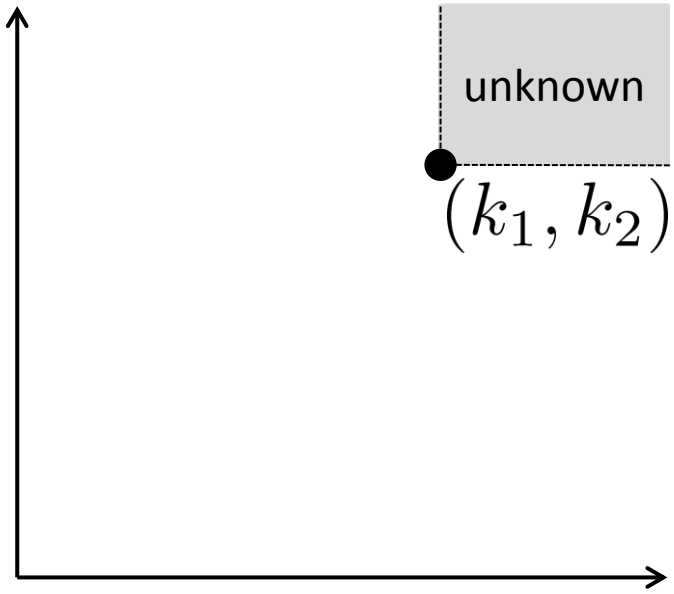
Vectorial and collective Division Properties are a little complicated, so we only explain them by two dimensions.

Vectorial Division Property

The parity becomes unknown when $\pi_{\vec{u}}$ is applied such that $u_1 \geq k_1$ and $u_2 \geq k_2$.

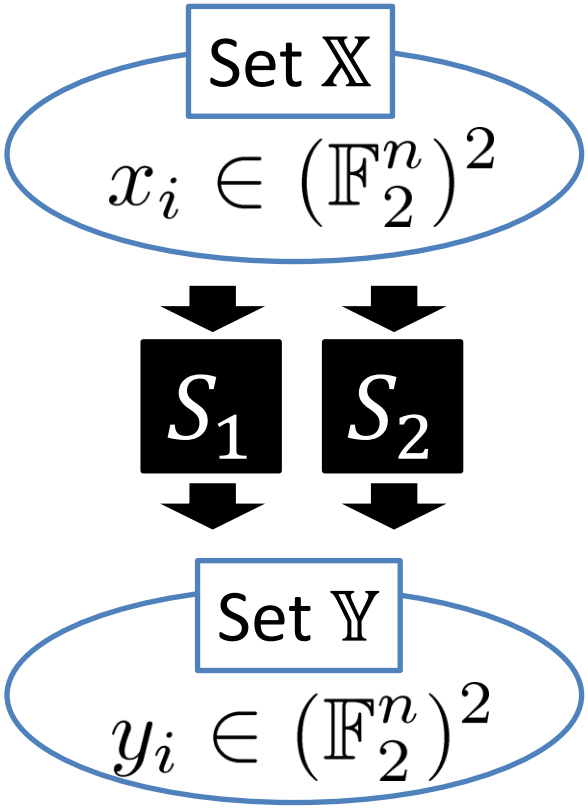


$\mathbb{X}$ has $\mathcal{D}^{n,2}_{[k_1,k_2]}$.

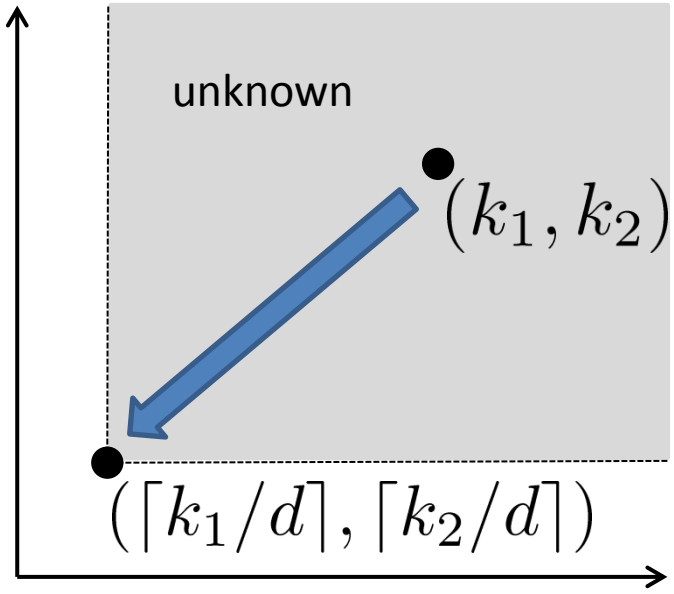


Propagation of Vectorial Division Property

When 2 S-boxes are applied, we evaluate the propagation of each element of vector $[k_1, k_2]$.

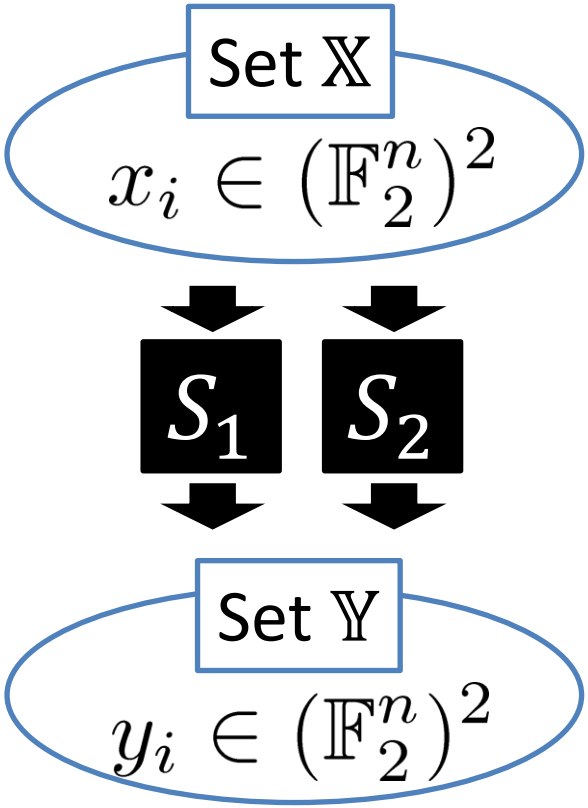


$\mathbb{Y}$ has $\mathcal{D}^{n,2}_{[\lceil \frac{k_1}{d} \rceil, \lceil \frac{k_2}{d} \rceil]}$.

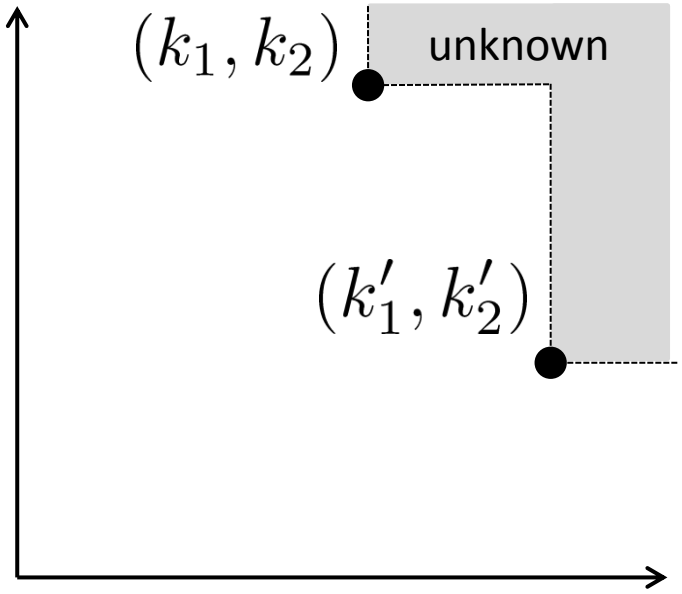


Collective Division Property

When the unknown has to be represented by 2 vectors, we use collective division property.

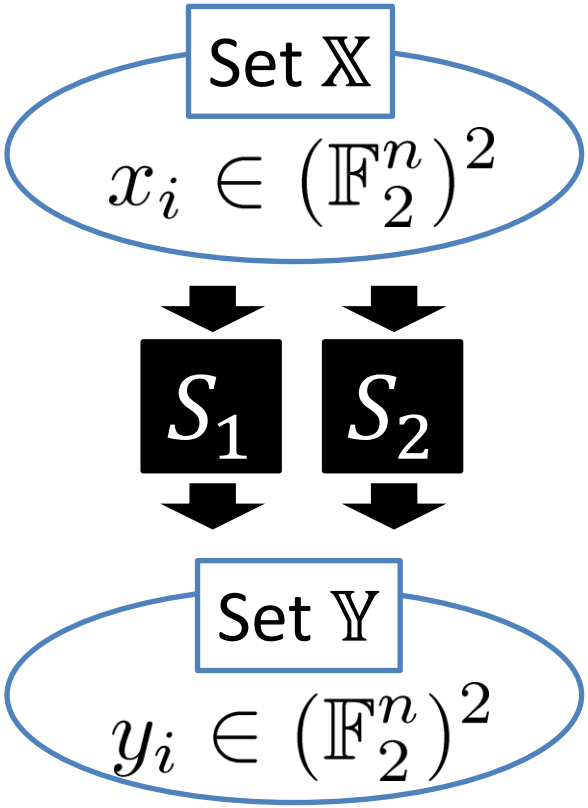


$\mathbb{X}$ has $\mathcal{D}^{n,2}_{[k_1,k_2],[k_1',k_2']}$.

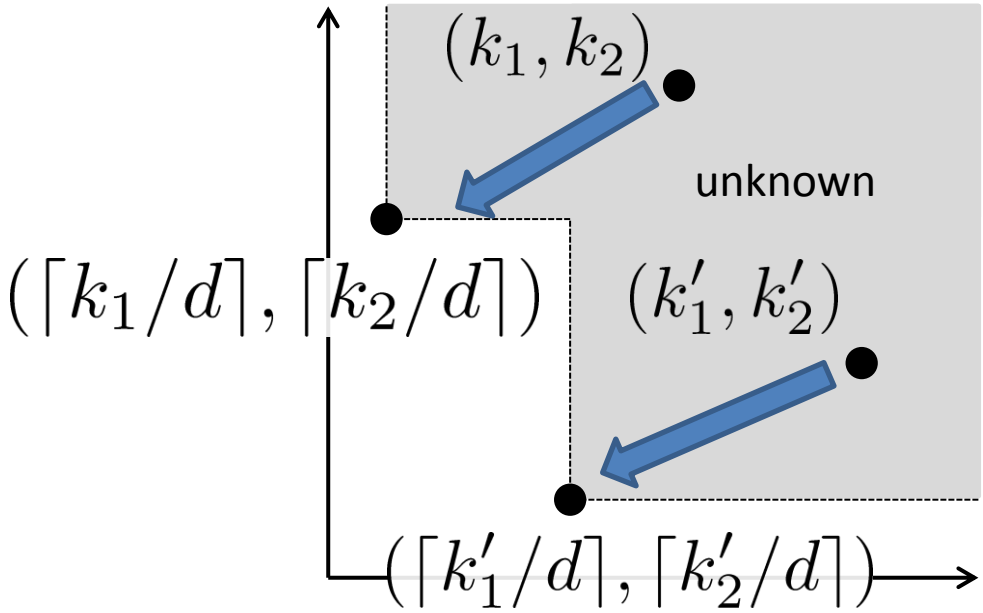


Propagation of Collective Division Property

We evaluate the propagation of the vectorial division property every vector.



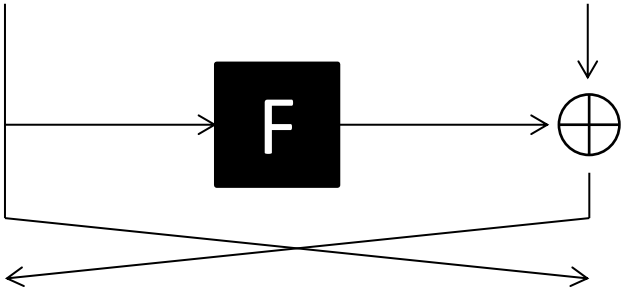
$\mathbb{Y}$ has $\mathcal{D}^{n,2}_{[\lceil \frac{k_1}{d} \rceil, \lceil \frac{k_2}{d} \rceil], [\lceil \frac{k'_1}{d} \rceil, \lceil \frac{k'_2}{d} \rceil]}$.



Outline

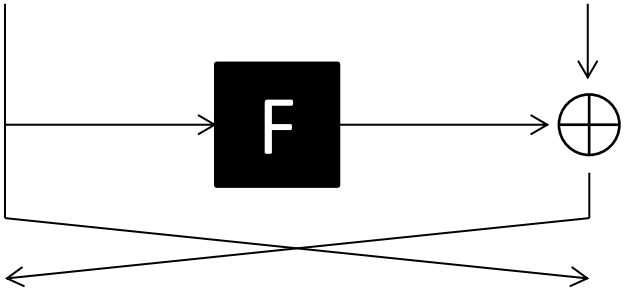
1. Background
2. Division Property
3. Vectorial and Collective Division Properties
4. **Application to Feistel Cipher**
   - **Definition of (ℓ, d)-Feistel**
   - **Propagation characteristic against (ℓ, d)-Feistel**
   - **Integral distinguisher on $(\ell, \ell - 1)$-Feistel**
   - **Integral distinguisher on $(\ell, 2)$-Feistel**
5. Conclusion

Feistel Cipher



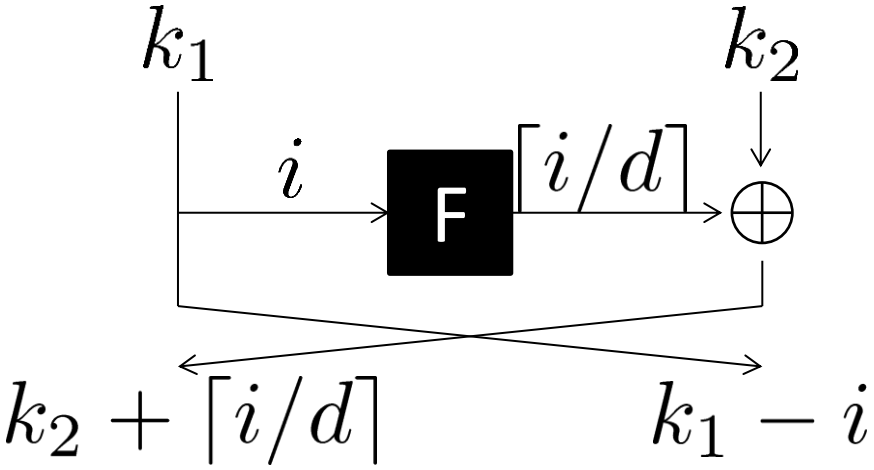
- Famous structure to design block cipher.
- It is widely applied, e.g., DES and Camellia.
- Many results have been known about the structural evaluation.
- Integral attack is strong attack, but previous approach is not effective if F is non-bijective.

(ℓ, d)-Feistel



- The bit length of F-function is ℓ bits.
- The algebraic degree of F-function is at most d.
- The block length is 2ℓ bits.

Propagation on (ℓ, d)-Feistel



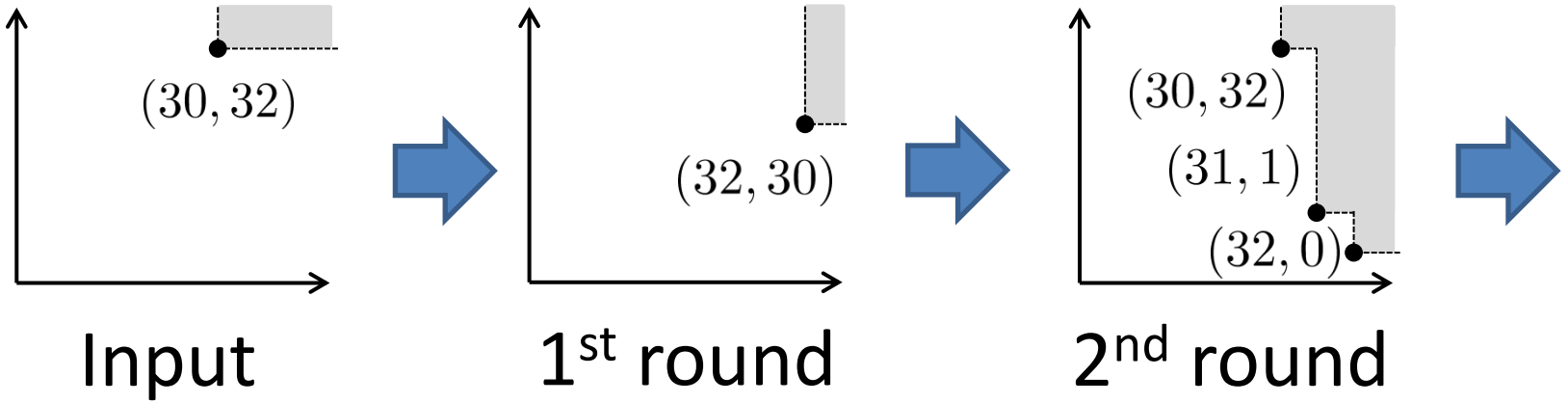
- The division property propagates as follows.

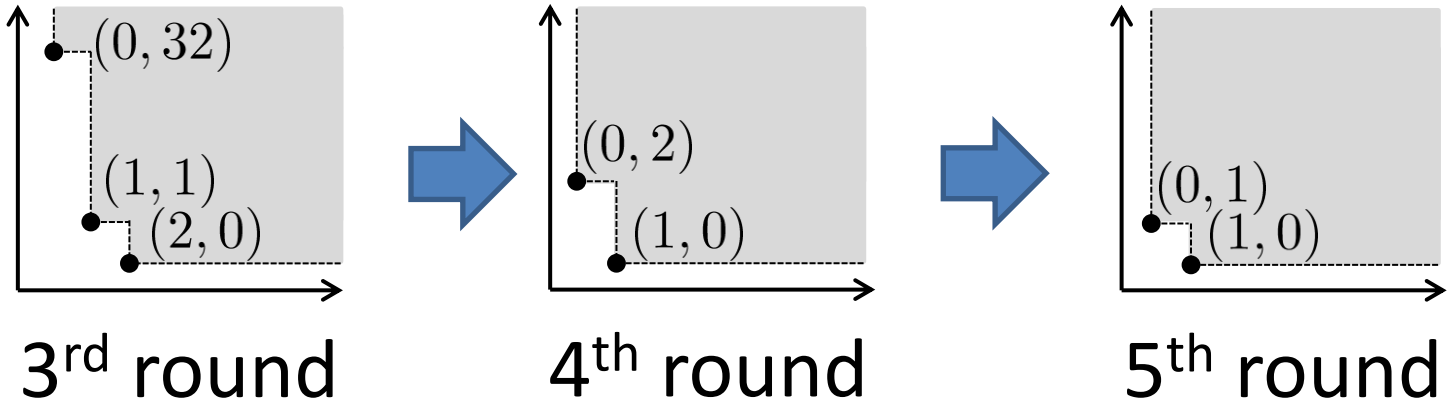
$$\mathcal{D}^{\ell,2}_{[k_1,k_2]} \Rightarrow \mathcal{D}^{\ell,2}_{[k_2,k_1],[k_2+1,k_1-d],\ldots,[k_2+q,k_1-qd]}$$

- Here $k_1 - qd \geq 0$ and $k_2 + q \leq \ell$.

Distinguisher against (32,31)-Feistel

Prepare 2^{62} CPs with left 30 and right 32 bits are active





Distinguisher against $(\ell, 2)$-Feistel

Target [Application]	$\log_2(\#texts)$								Method
	r=6	r=7	r=8	r=9	r=10	r=11	r=12	r=13	
(16,2)-Feistel [Simon 32]	17	25	29	31	-	-	-	-	our
	-	-	-	-	-	-	-	-	degree
(24,2)-Feistel [Simon 48]	17	29	39	44	46	47	-	-	our
	17	-	-	-	-	-	-	-	degree
(32,2)-Feistel [Simon 64]	17	33	49	57	61	63	-	-	our
	17	-	-	-	-	-	-	-	degree
(48,2)-Feistel [Simon 96]	17	33	57	77	87	92	94	95	our
	17	33	-	-	-	-	-	-	degree
(64,2)-Feistel [Simon 128]	17	33	65	97	113	121	125	127	our
	17	33	-	-	-	-	-	-	degree

15-round integral distinguisher against Simon32 were already known, but it was confirmed by experiments and the existence is not proven.

Outline

1. Background
2. Division Property
3. Vectorial and Collective Division Properties
4. Application to Feistel Cipher
5. **Conclusion**

Conclusion

- Propose the division property.
  - It is a generalization of the integral property such that it can also exploit the algebraic degree.
- Application
  - I showed structural evaluations for Feistel and SPN by adding some realistic assumptions.
  - Toward to dedicated cryptanalysis, we also show integral distinguishers of AES-Like ciphers.
- Future works
  - I expect the division property is useful to construct integral characteristic of specific block ciphers.
  - I think that all integral distinguishers are looked again by using the division property.