

# Hamming correlation property of frequency-hopping sequences from the array structure of Sidelnikov sequences Min Kyu Song<sup>1</sup>, Hong-Yeop Song<sup>1</sup>, and Jang Yong Lee<sup>2</sup> <sup>1</sup>Yonsei University, <sup>2</sup>Agency of Defense Development

International Conference on Electronics, Information, and Communication (ICEIC) 2017

### Motivation

- Sidelnikov sequences are known as not only having good complex correlation, but also optimal frequency-hopping sequences
- Recently, the array structure of a Sidelnikov sequence is analyzed in the sense of complex correlation
- So, we tried to analyze hamming correlation of the

### Simulation result

#### \* optimal, near-optimal

					-	_	-	
q=17 , $d=2$			4	11	12	q = 31, d = 2		
M	CS	CA	3	13	14	M	CS	CA
16	1	2	2	17	18	30	1	2
8	3	4	q = 27, d = 2			15	3	4
4	7	8	M	<b>CS</b>	CA	10	5	6
2	11	12	26	1	2	6	9	10
q = 19, d = 2			13	3	4	5	11	12
M	CS	CA	2	17	18	3	15	16
18	1	2	q = 29, d = 2			2	19	20
9	3	4	М	CS	CA	q = 31, d = 3		
6	5	6	28	1	2	M	CS	CA
3	11	12	14	3	4	30	2	3
2	13	14	7	7	8	15	5	6
q = 23, d = 2			4	13	14	10	8	9
M	CS	CA	2	19	20	6	14	15
22	1	2	q = 29, d = 3			5	15	16
11	3	4	M	CS	CA	3	19	20
2	15	6	28	2	3	2	24	25
q = 25, d = 2			14	5	6	q = 32 d = 2		



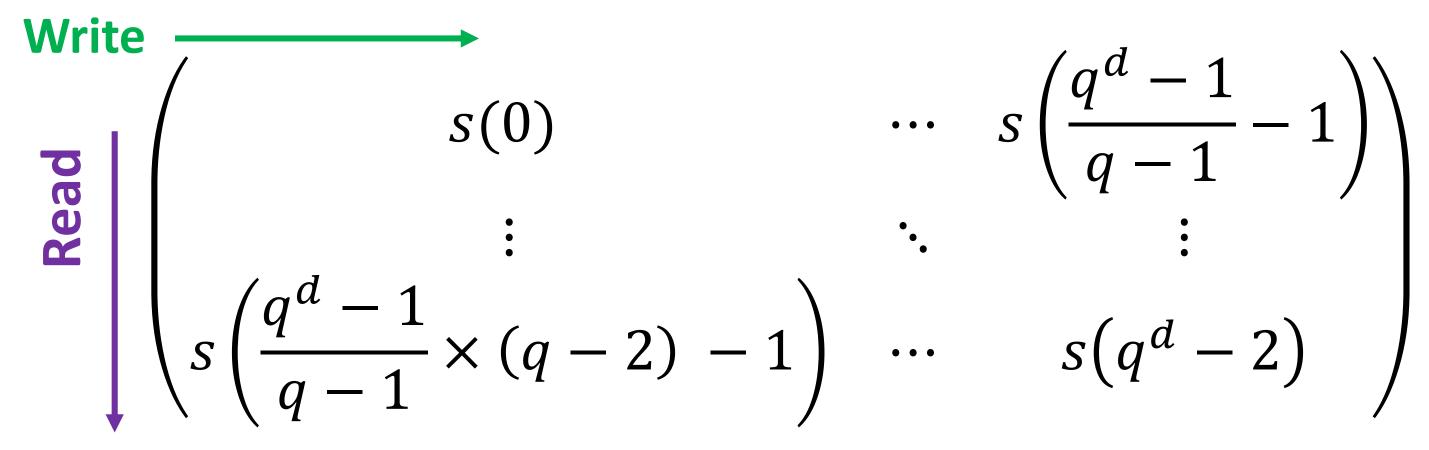
- array structure of a Sidelnikov sequence by using **computer simulation**
- Hamming correlation : the number of same alphabets at same time
- Sidelnikov sequence of period  $q^d 1$

 $s(t) = \log_{\alpha}(\alpha^{t} + 1) \pmod{M}$ 

- q : a prime power
- $\alpha$  : a primitive element of the finite filed of size q
- M : a divisor of  $q^d 1$  with  $M \ge 2$
- $\log_{\alpha}(\cdot)$  : discrete logarithm with  $\log_{\alpha}(0) = 0$ .
- Array structure of a Sidelnikov sequence<sup>[1]</sup>

- Assume that 
$$2 \le d < \frac{1}{2} \left( \sqrt{q} - \frac{2}{\sqrt{q}} + 1 \right)$$

- Set M be smaller than or equal to q-1
- Write row by row, and regard *l*-th column as a sequence, denoted by  $v_l(t)$



- Fig. 2-D array from a Sidelnikov sequence -
- For an integer l, let  $m_l$  be the size of its q-cyclotomic coset modulo  $\frac{q^a-1}{q-1}$
- A set of indices  $\Lambda' = \left\{ l \left| 1 \le l < \frac{q^d 1}{q 1}, m_l = d \right\} \right\}$ - Then, for  $l \neq k \in \Lambda'$ ,  $v_l(t)$  and  $v_k(t)$  are cyclically

CS M **C**A 11 12 M **CS C**A 7 24 16 31 2 17 4 2 1 q = 32, d = 323 24 12 3 4 2 **CS C**A 5 M 8 6 7 6 8 31 2 3 

#### Discussion

- **CS** is a set of one-coincidence sequences<sup>[2]</sup>, which is **optimal**, when M = q - 1, d = 2
- **Near optimal** when
  - 1. CA with M = q 1 and d = 2
  - 2. *CS* with M = q 1 and d = 3
- For the same q, d, and M, the gap between

## distinct.

## New frequency-hopping sequence families

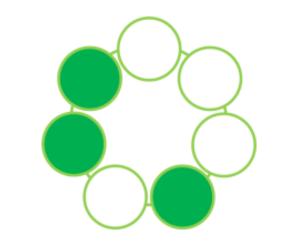
 $CS = \{v_l(t) | l \in \Lambda'\}$ 

$$CA = \{v_l(t) + k | l \in \Lambda', 0 \le k \le M - 1\}$$

maximum non-trivial hamming correlation of CS and CA is always 1.

#### References

[1] Young-Tae Kim, Dae San Kim, and Hong-Yeop Song, "New M-ary sequence families with low correlation from the array structure of Sidelnikov sequences", IEEE Transactions on Information Theory, vol.61, no.1, pp.655-670, 2015. [2] A. A. Shar and P. A. Davis, "A survey of one-coincidence sequences for frequency-hopped spread spectrum systems," IEE Proceedings F, vol. 131, no. 7, pp. 719-724, 1984.



Channel coding and Signal Design Lab CSDL)