Punctured bent function sequences for watermarked DS-CDMA

Hong-Yeop Song

Yonsei University, Seoul, Korea

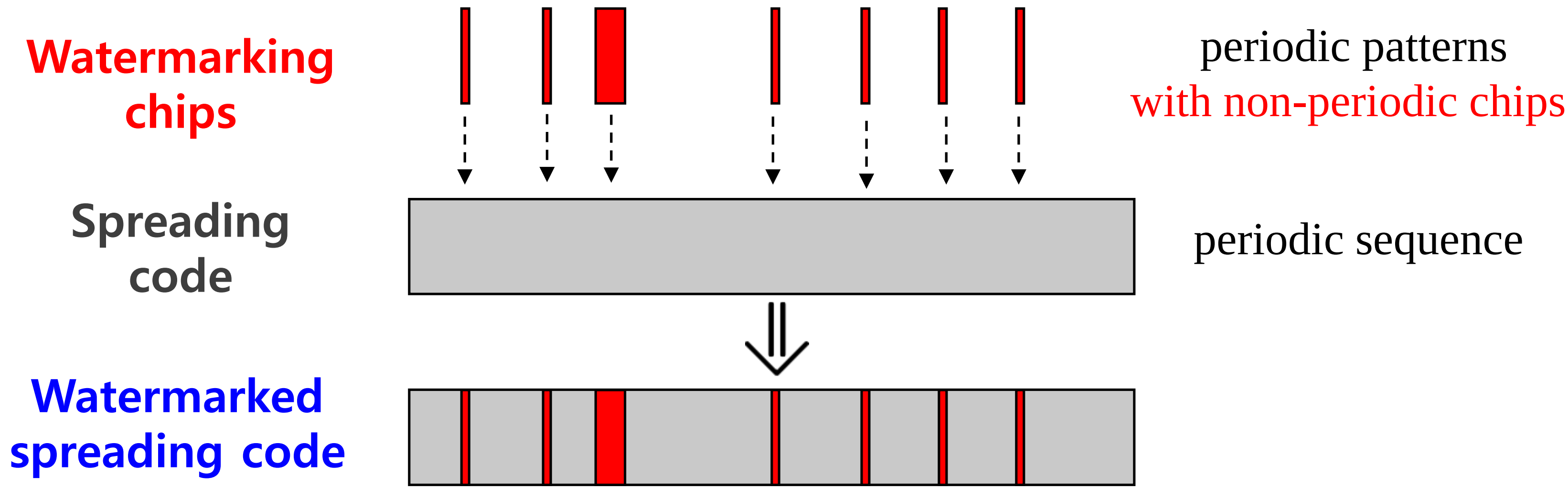
hysong@yonsei.ac.kr

July 5, 2019
Aachen, Germany

Based on the paper with the same title,
IEEE Communications Letters, **2019**, to appear soon.

Table of Contents

Introduction: Watermarked DS-CDMA



- Insert some watermarking chips into spreading code
- Any two watermarks at different time are different

Introduction: advantage/disadvantage

Watermarked DS-CDMA have been considered
to provide security at the signal level

- Steganography
  - Watermark conveys some "secret" information which can be extracted after synchronized.
- Authentication of GNSS open signals
  - Watermark is used to provide where a signal comes from
  - Protect from spoofing attacks

at the price of degrading the correlation performance (communication performance) of spreading sequences for multiple access, for example.

Introduction: Summary

- Investigate **the effect of inserting** some randomly generated **watermarking chips** into known (**set of**) **spreading sequences**
  - In terms of periodic correlations
- Propose two design criteria for **"good" watermarked sequences** in the sense of
  1) Reducing the average correlation value
  2) Minimizing the variance of correlations

  for the best performance of **multiple-access**
- Specifically, we propose, for $n = 2m$ with even m, **an optimal set of 2^{m-1} punctured bent function sequences of length $2^n - 1$ in the sense of the above two criteria** such that
  - all of which are punctured by the **single pattern** obtained by the **Singer difference set**, (Criteria 2)
    - Hence, half the bits are punctured in one period of the sequence
  - the **max non-trivial correlation** magnitude maintains $2^m + 1$, (Criteria 1)
    - which is the same value as those for un-punctured bent function sequences
    - but is in fact **twice of the Welch bound**

Introduction: (selected) References

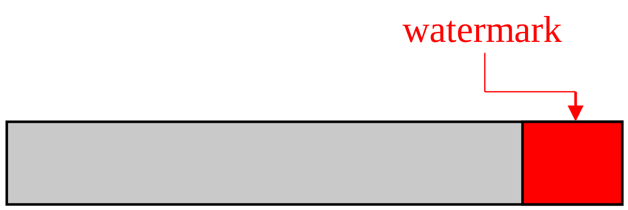
- S. W. Golomb and G. Gong, Signal design for good correlation: for wireless communications, cryptography, and radar, New York, NY, USA: Cambridge University Press, 2005. — DS-CDMA for communications
- Global Positioning Systems Directorate Systems Engineering & Integration Interface Specification, document IS-GPS-200H, Mar. 2014. — DS-CDMA for navigations
- G. Caparra and J. T. Curran, ``On the achievable equivalent security of GNSS ranging code encryption,'' in Proc. 2018 IEEE/ION Positions, Location and Navigation Symposium (PLANS), Monterey, USA, pp. 956-966, Apr. 2018. — W-DS-CDMA for authentication
- X. Li, C. Yu, M. Hizlan, W.-T. Kim, and S. Park, ``Physical layer watermarking of direct sequence spread spectrum signals,'' in Proc. IEEE MILCOM 2013, San Diego, USA. pp. 476-481, Nov. 2013. — W-DS-CDMA for steganography
- C. Yang, ``FFT acquisition of periodic, aperiodic, puncture, and overlaid code sequences in GPS,'' in Proc. ION GPS 2001, Salt Lake City, USA, pp. 137-147, Sep. 2001. — W-DS-CDMA for fast acquisition
- M. Villanti, M. Iubatti, A. Vanelli-Coralli, and G. E. Corazza, ``Design of distributed unique words for enhanced frame synchronization,'' IEEE Trans. Commun., vol. 57, no. 8, pp. 2430-2440, Aug. 2009. — Effect of watermarking on single spreading sequence only in terms of aperiodic autocorrelation
- J. D. Olsen, R. A. Scholtz, and L. R. Welch, ``Bent-function sequences,'' IEEE Trans. Inf. Theory, vol. 28, no. 6, pp.858-864, Nov. 1982. — Bent function sequences
- L. R. Welch, "Lower bounds on the maximum cross correlation of signals (Corresp.)," IEEE Trans. Inf. Theory, vol. 20, no. 3, pp. 397-399, May 1974. — Welch Bound
- L. D. Baumert, Cyclic difference sets, New York, NY, USA: Springer-Verlag, 1972. — Cyclic difference sets
- J. Singer, "A theorem in finite projective geometry and some applications to number theory," Trans. Amer. Math. Soc., vol. 43, pp. 377-385, 1938. — Singer difference sets

Proposed model of W-DS-CDMA

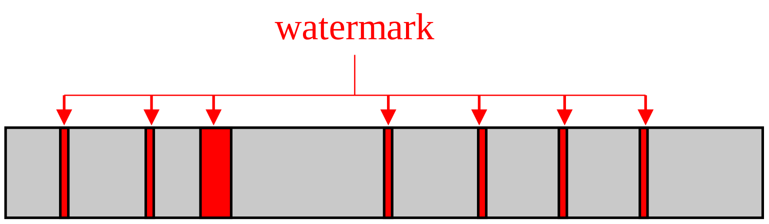
How to insert watermark?

- Previous results are focused on how to use watermarks for security.
- Usually assume the aggregated insertion

Why not



Case 1. aggregated

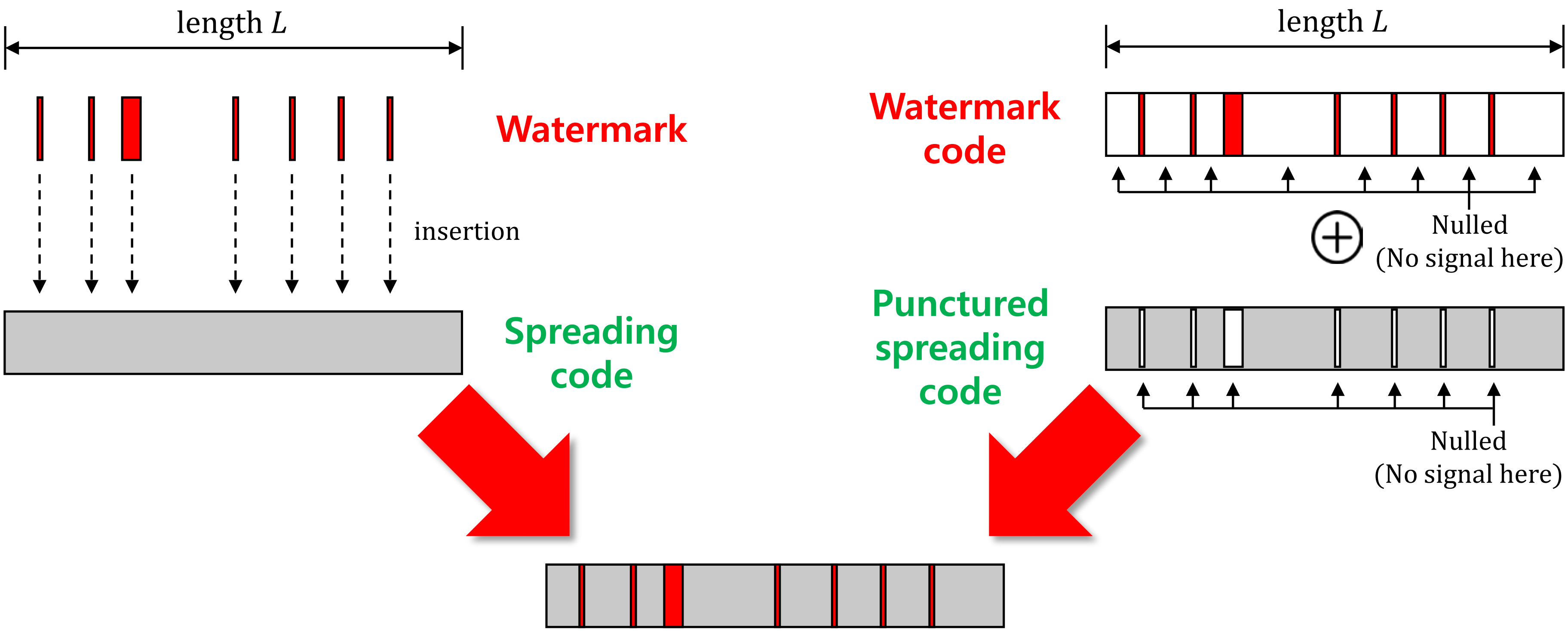


Case 2. spread

- The watermark insertion affects on auto- and cross-correlation of spreading code
- Question:

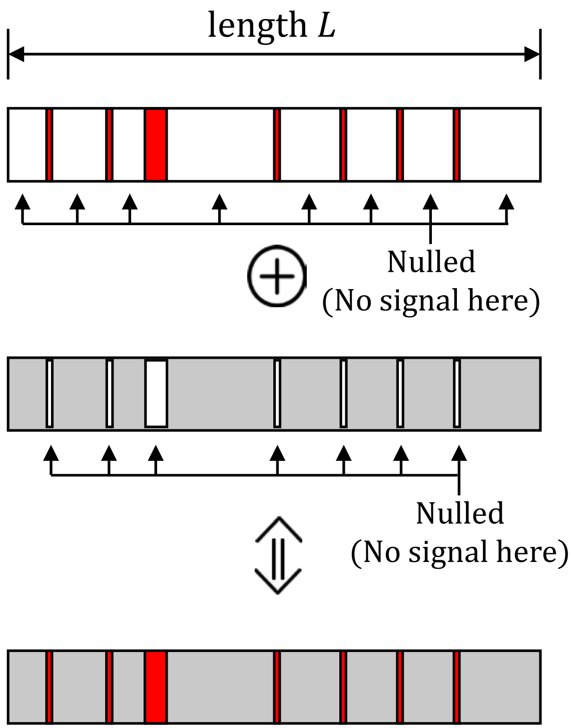
What insertion is better in the sense of acquisition performance?

Equivalent model



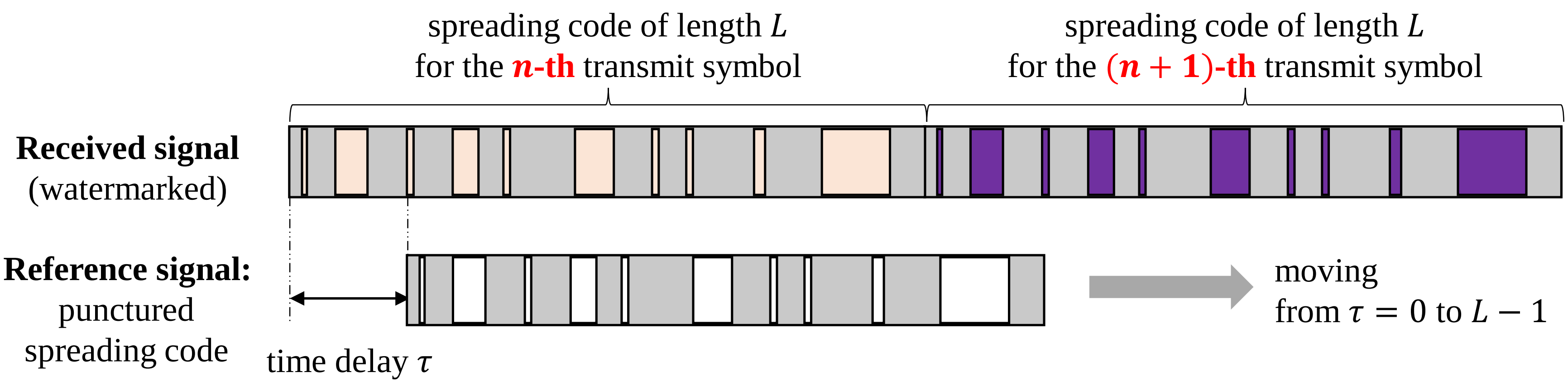
Watermarked spreading code

Some properties



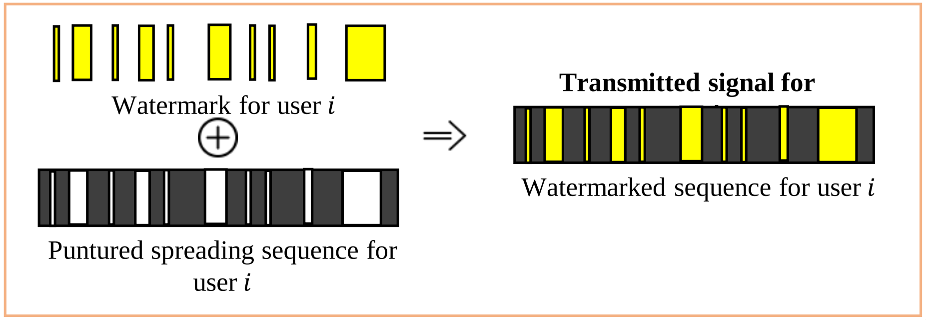
	Alphabet?	Repeated?
watermark	Ternary $\{0, +1, -1\}$	Not repeated
Punctured spreading code	Ternary $\{0, +1, -1\}$	Repeated periodically
Watermarked spreading code	Binary $\{+1, -1\}$	Partially repeated

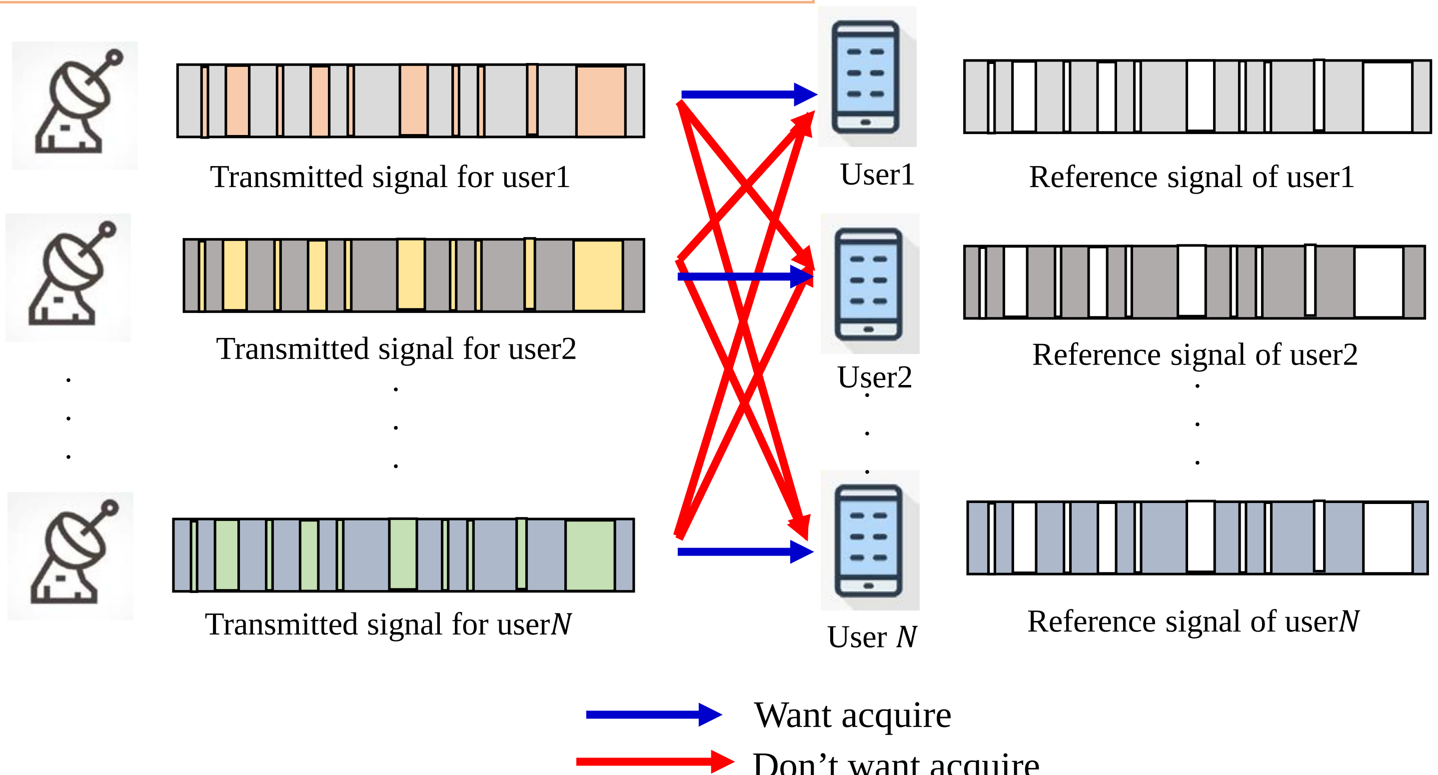
Acquisition for watermarked DS-CDMA



- **During the acquisition process**,
  - ✓ the receiver **knows which chips are watermarked** (only the position information)
  - ✓ but has **no information about what each value is**. (no idea on its value)
  - ✓ Therefore, the receiver can only use **the punctured spreading code**, which is repeated, periodically.
- **Watermark chips** will be extracted **after the signal is obtained/acquired**
  - ✓ the receiver **will use these chips for some other purpose** (steganography/authentication/extra security, etc)
- Our goal is to find **BEST watermarking chips (position) PLUS spreading codes** so that the **multiple-access performance** is **NOT MUCH degraded** compared with **the conventional DS-CDMA systems without watermarks**.

Watermarked DS-CDMA system



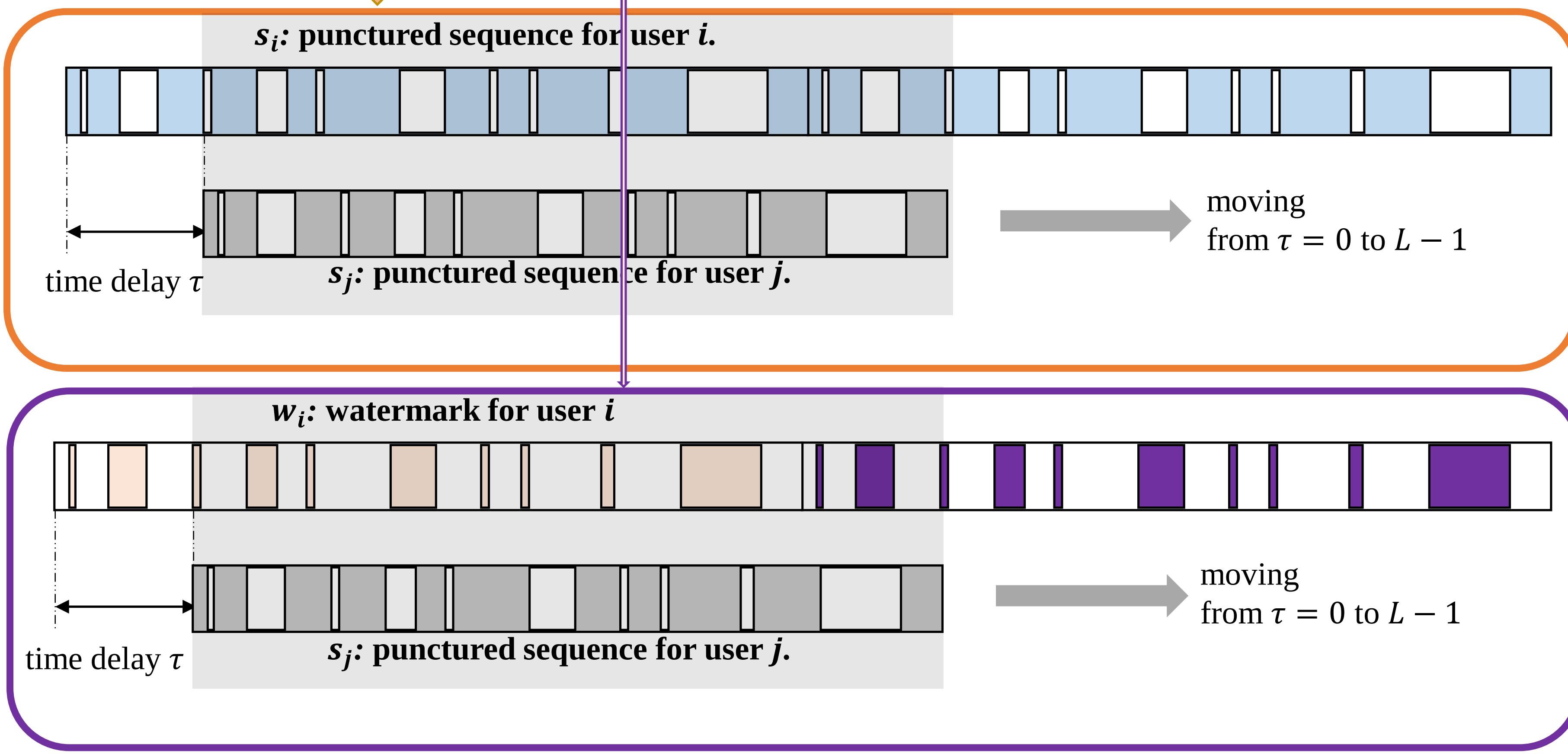


Analysis on Watermarks and Design Criteria

Crosscorrelation of watermarked sequence and punctured sequence

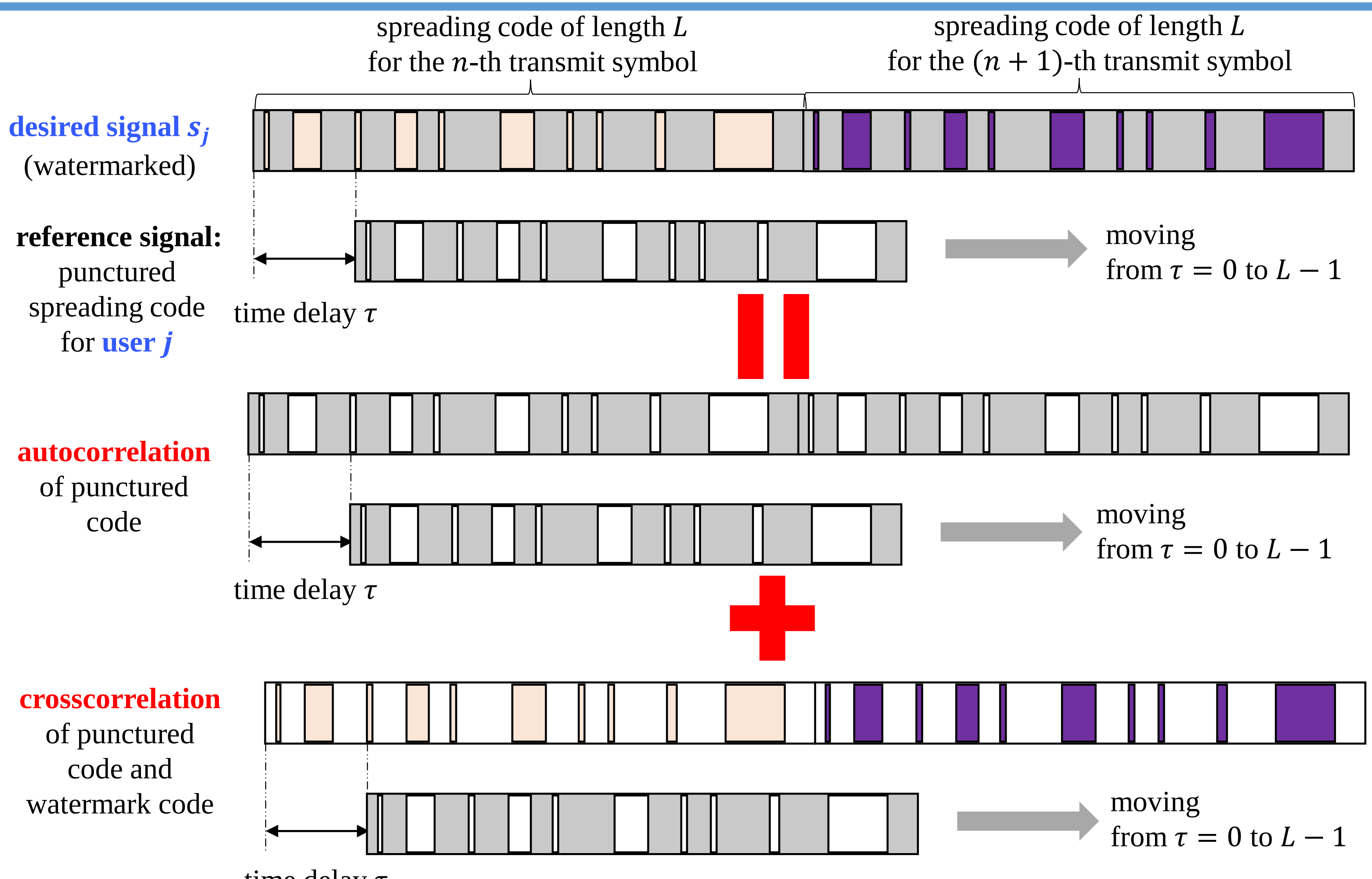
$$\theta_{c_i, s_j}(\tau) = \theta_{s_i, s_j}(\tau) + \theta_{w_i, s_j}(\tau)$$

※ c_i : watermarked sequence for user i.
s_i: punctured sequence for user i.
w_i: watermark for user i



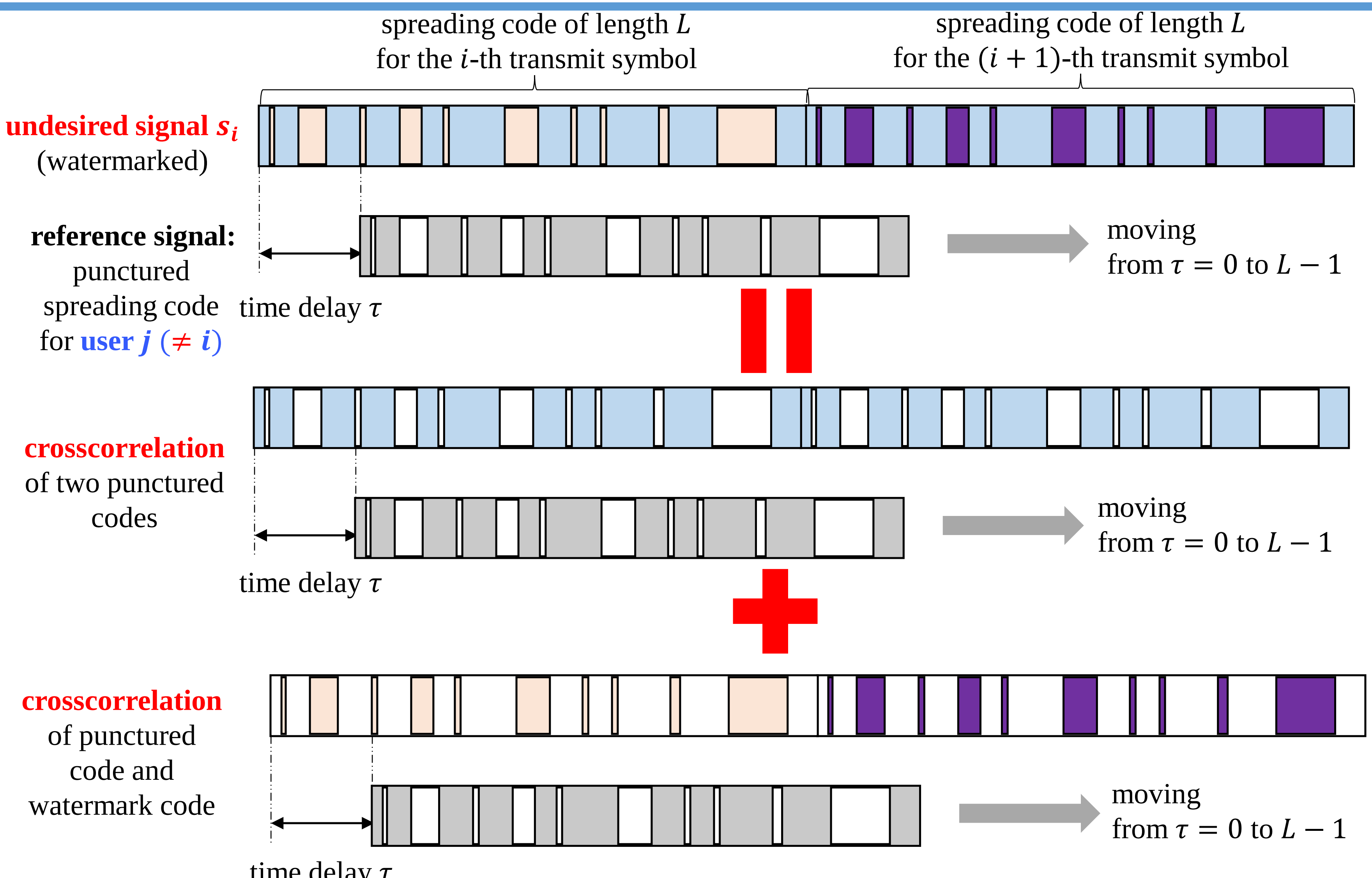
For desired signal (when $i = j$)

$$\theta_{c_j, s_j}(\tau) = \theta_{s_j, s_j}(\tau) + \boldsymbol{\theta}_{\boldsymbol{w}_j, \boldsymbol{s}_j}(\boldsymbol{\tau})$$



For undesired signal (when $i \neq j$)

$$\theta_{c_i, s_j}(\tau) = \theta_{s_i, s_j}(\tau) + \boldsymbol{\theta_{w_i, s_j}(\tau)}$$



What is required

undesired signal

- $\theta_{c_i, s_j}(\tau) = \theta_{s_i, s_j}(\tau) + \boldsymbol{\theta_{w_i, s_j}(\tau)}$

as small as possible for all $\boldsymbol{\tau}$

desired signal

- $\theta_{c_j, s_j}(\tau) = \theta_{s_j, s_j}(\tau) + \boldsymbol{\theta_{w_j, s_j}(\tau)}$

as small as possible for all $\boldsymbol{\tau \neq 0}$

deterministic **random (?)**

as small as possible for all $\boldsymbol{\tau}$

- $\boldsymbol{w_i}$ is a **watermark**, which have values ± 1 at positions indicated by the **puncturing pattern** $\mathcal{p}$, which is a k-subset of $\mathbb{Z}_L$ to be OPTIMIZED
- It turned out that it is enough to assume that all the users have **the same** $\mathcal{p}$.
- Assume that the **watermarking chips are i.i.d. random variables** with ± 1 equally likely

Crosscorrelation $\boldsymbol{\theta_{w,s_j}(\tau)}$ of watermarking chips and punctured sequence

the non-zero values of $\boldsymbol{w}$ are i.i.d. random with ± 1 equally likely, hence, **mean-zero**

$$\boldsymbol{\theta_{w,s_j}(\tau)} = \sum_l \boldsymbol{w}(l+\tau)\boldsymbol{s_j}(l)$$

- Watermarking chip sequence $\boldsymbol{w}$ has a non-zero value ONLY at index $l+\tau \in \wp$ or at index $l \in \wp - \tau$.
- Punctured sequence $\boldsymbol{s_j}$ has a non-zero value ONLY at index $l \notin \wp$ or at $l \in Z_L \backslash \wp$
- Therefore, $\boldsymbol{w}(l+\tau)\boldsymbol{s_j}(l)$ has a non-zero value ONLY at

$$l \in (\wp - \tau) \cap Z_L \backslash \wp = (\wp - \tau) \backslash \wp$$

- Therefore, the number of non-zeros will be

$$\begin{aligned} &= |(\wp - \tau)\backslash \wp| \\ &= |\wp| - |\wp \cap (\wp - \tau)| \\ &= k - D_\wp(\tau) \end{aligned}$$

✓This must be the **variance** of $\boldsymbol{\theta_{w,s_j}(\tau)}$.

✓The **mean** of $\boldsymbol{\theta_{w,s_j}(\tau)}$ becomes 0 since $E[w] = 0$

DESIGN CRITERIA

$$\theta_{c_i, s_j}(\tau) = \theta_{s_i, s_j}(\tau) + \boldsymbol{\theta_{w_i,s_j}(\tau)}$$

It is a random variable with mean-zero and variance $k - D_{\wp}(\tau) = |\wp| - |\wp \cap (\wp - \tau)|$ where $\wp$ is a puncturing pattern of size k.

This is a random variable with

mean = $\theta_{s_i, s_j}(\tau)$

variance = $k - D_{\wp}(\tau) = |\wp| - |\wp \cap (\wp - \tau)|$

$\boldsymbol{C_1}$**: Minimize the mean of** $\boldsymbol{\theta_{c_i,s_j}(\tau)}$

$\equiv$ Minimize $\theta_{s_i, s_j}(\tau)$ the non-trivial correlation magnitude of punctured sequences s_i, s_j for all possible i, j.

$\boldsymbol{C_2}$**: Minimize the variance of** $\boldsymbol{\theta_{c_i,s_j}(\tau)}$

$$\equiv \text{ Maximize } \min_{\tau\neq 0} D_{\wp}(\tau) = \min_{\tau\neq 0} |\wp \cap (\wp - \tau)| \triangleq \boldsymbol{D_{min}(\wp)}$$

Upper bound of min of $|\mathcal{p} \cap (\mathcal{p} - \tau)|$

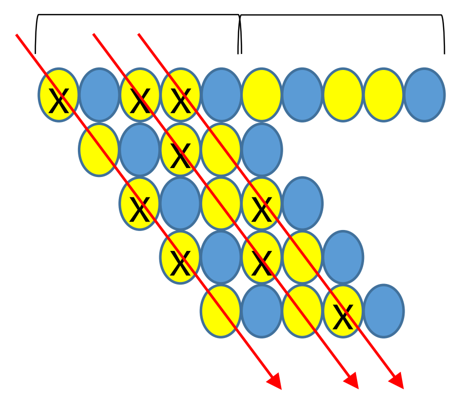
Lemma (C_2). Assume that k watermarking chips are inserted in a watermarked spreading code of length L, according to a puncturing pattern $\mathcal{p}$. Then,

$$\min_{1 \le \tau \le L-1} |\mathcal{p} \cap (\mathcal{p} - \tau)| \le \left\lfloor \frac{k^2 - k}{L - 1} \right\rfloor.$$

Proof: Recall that $\mathcal{p}$ is a k-subset of $\mathbb{Z}_L$.
Therefore, for any such $\mathcal{p}$ of size k, we have

$$\sum_{\tau=0}^{L-1} D_{\mathcal{p}}(\tau) = k^2$$

since each member in $\mathcal{p}$ will match every member of $\mathcal{p}$ (including itself) exactly once as τ runs from 0 to $L-1$.



Since $D_{\mathcal{p}}(0) = k$, we have

$$\frac{1}{L-1} \sum_{\tau=1}^{L-1} D_{\mathcal{p}}(\tau) = \frac{k^2 - k}{L - 1} \qquad \square$$

Proposed Optimal Watermarked Spreading Sequences Set

puncturing pattern **optimization**

which spreading sequence is **best** with the selected puncturing?

We consider $\boldsymbol{C_2}$ first, and then consider $\boldsymbol{C_1}$.

Does there any spreading sequence that is **good** with this puncturing?

or that can be proved to be good with this puncturing?

(Almost) Cyclic Difference Sets

Definition. Let $\mathcal{P}$ be a k-subset of $\mathbb{Z}_L$. Then,

① $\mathcal{P}$ is called a (L, k, λ, t)-**almost cyclic difference set** if, for $\tau = 1, 2, \ldots, L-1$,

$$|\mathcal{P} \cap (\mathcal{P} - \tau)| = \begin{cases} \lambda & t \quad \text{times} \\ \lambda + 1 & L - 1 - t \quad \text{times.} \end{cases}$$

② $\mathcal{P}$ is called a (L, k, λ)-**cyclic difference set** if, for $\tau = 1, 2, \ldots, L-1$,

$$|\mathcal{P} \cap (\mathcal{P} - \tau)| = \lambda.$$

This is equivalent to almost cyclic difference set with $t = L - 1$.

Optimal Puncturing Pattern

Well-known Lemma on the existence:

① If an (L, k, λ, t)-almost cyclic difference set $\mathcal{P}$ exists, then we have

$$k(k-1) = (L-1)\lambda + (L-1-t)$$

② If an (L, k, λ)-cyclic difference set $\mathcal{P}$ exists, then we have

$$k(k-1) = (L-1)\lambda$$

For both cases, we have

$$\left\lfloor \frac{k^2-k}{L-1} \right\rfloor = \lambda$$

Theorem. (ACDS ⇒ C_2 optimal)

Let $\mathcal{P}$ be a k-subset of $\mathbb{Z}_L$. Then $\mathcal{P}$ is an **optimal** puncturing pattern if it is an (L, k, λ, t)-ACDS in the sense of

$$\min_{1 \le \tau \le L-1} |\mathcal{P} \cap (\mathcal{P} - \tau)|$$ **attains its maximum value** $\lambda = \left\lfloor \frac{k^2-k}{L-1} \right\rfloor$

Singer Difference Sets (J. Singer 1938)

- $L = 2^n - 1$ with $n = 0 \pmod 4$
- $k = 2^{n/2} - 1$ and $\lambda = 2^{n/4} - 1$
- $\alpha \in \mathbb{F}_{2^n}$ be a primitive element
- $\mathrm{tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace of $x \in \mathbb{F}_{2^n}$ to $\mathbb{F}_2$

Then, a k-subset $\wp$ of $\mathbb{Z}_L$ is an (L, k, λ)-CDS if, for each $l \in \mathbb{Z}_L$,

$$l \in \wp \text{ iff } \mathrm{tr}_1^n\left(\alpha^l\right) = 0$$

We will use **the puncturing pattern** $\wp$ from the Singer difference set constructed above.

- This is **optimal** $(\boldsymbol{C_2})$
- It punctures about **half the bits** in one period of the sequence of length $L = 2^n - 1$

Is it too much?

Bent Function Sequences

- $n = 2m$ be a positive integer with **even** m.
- f be a bent function over $\mathbb{F}_{2^m}$.
- $\alpha \in \mathbb{F}_{2^n}$ be a primitive element and a constant $\sigma \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$.

The set $\boldsymbol{\mathcal{B}}$ of 2^m binary sequences of length $2^n - 1$ for each constant $\mu \in \mathbb{F}_{2^m}$ given as, for $l = 0,1,\dots,2^n-2$,

$$\boldsymbol{b}_\mu[l] = (-1)^{f\left(\mathrm{tr}_m^n(\alpha^l)\right) + \mathrm{tr}_1^n\left((\mu+\sigma)\alpha^l\right)}$$

is called <u>**bent function sequence family**</u>

and

$$\theta_{max}(\boldsymbol{\mathcal{B}}) \le 2^m + 1.$$

Hence, it is **optimal** in terms of the ***Welch bound***.

Original Contribution: J. D. Olsen, R. A. Scholtz, and L. R. Welch (1982)
Above formulation by traces: Golomb and Gong (2005) Chapter 10

MAIN Contribution

Punctured bent function sequences

- $n = 2m$ be a positive integer with **even** m.
- f be a bent function over $\mathbb{F}_{2^m}$.
- $\alpha \in \mathbb{F}_{2^n}$ be a primitive element and a constant $\sigma \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$.
- $\boldsymbol{b}_\mu[l] = (-1)^{f\left(\mathrm{tr}_m^n(\alpha^l)\right) + \mathrm{tr}_1^n\left((\mu+\sigma)\alpha^l\right)}$ be the bent function sequences of length $2^n - 1$ for each $\mu \in \mathbb{F}_{2^m}$, constructed earlier **in previous page**.

- **Γ be a subset of $\mathbb{F}_{2^m}$ such that $\boldsymbol{\mu} + \boldsymbol{\nu} \neq 1$ for any $\boldsymbol{\mu}, \boldsymbol{\nu} \in \Gamma$.**
- **$\wp$ is the puncturing pattern from the Singer difference set, i.e.,**

$$\boldsymbol{l} \in \wp \text{ iff } \boldsymbol{tr_1^n(\alpha^l) = 0}$$

Consider the set of **punctured bent function sequences** $S = \{s_\mu : \mu \in \Gamma\}$ where

$$s_\mu[l] = \begin{cases} \boldsymbol{b}_\mu[l] & \text{if } l \notin \wp \Leftrightarrow \mathrm{tr}_1^n(\alpha^l) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Main Theorem

Let $S = \{s_\mu : \mu \in \Gamma\}$ be the set of **punctured bent function sequences** in previous page, with puncturing pattern $\wp$ from **Singer difference set**. Then,

$$\theta_{\max}(S) \le 2^m + 1.$$

Proof of correlation bound

First observation:

$$s_\mu[l] = \begin{cases} \boldsymbol{b}_\mu[l] & \text{if } \operatorname{tr}_1^n(\alpha^l) = 1 \\ 0 & \text{if } \operatorname{tr}_1^n(\alpha^l) = 0 \end{cases}$$

$$= \frac{1}{2}\left(1 - (-1)^{\operatorname{tr}_1^n(\alpha^l)}\right)\boldsymbol{b}_\mu[l]$$

Proof of correlation bound

Second observation:

$$s_\mu[l] = \frac{1}{2}\left(1 - (-1)^{\mathrm{tr}_1^n(\alpha^l)}\right) b_\mu[l]$$

$$= \frac{1}{2}\left(b_\mu[l] - \underline{(-1)^{\mathrm{tr}_1^n(\alpha^l)} b_\mu[l]}\right) = \frac{1}{2}\left(b_\mu[l] - \underline{b_{\mu+1}[l]}\right)$$

Since

$$(-1)^{\mathrm{tr}_1^n(\alpha^l)} b_\mu[l] = (-1)^{\mathrm{tr}_1^n(\alpha^l)} (-1)^{f\left(\mathrm{tr}_m^n(\alpha^l)\right) + \mathrm{tr}_1^n((\mu+\sigma)\alpha^l)}$$

$$= (-1)^{f\left(\mathrm{tr}_m^n(\alpha^l)\right) + \mathrm{tr}_1^n((\mu+1+\sigma)\alpha^l)}$$

$$= b_{\mu+1}[l]$$

Proof of correlation bound

For $\mu, \nu \in \Gamma$, the correlation of s_μ and s_ν at time shift τ is given by

$$\theta_{s_\mu,s_\nu}(\tau) = \sum_{l=0}^{L-1} s_\mu[l+\tau]s_\nu[l]$$

$$= \frac{1}{4}\sum_{l=0}^{L-1}\big(b_\mu[l+\tau] - b_{\mu+1}[l+\tau]\big)\big(b_\nu[l] - b_{\nu+1}[l]\big).$$

$$= \frac{1}{4}\Big(\theta_{b_\mu,b_\nu}(\tau) + \theta_{b_{\mu+1},b_{\nu+1}}(\tau) - \theta_{b_{\mu+1},b_\nu}(\tau) - \theta_{b_\mu,b_{\nu+1}}(\tau)\Big)$$

(1) when $\mu = \nu$, we are checking the values $\theta_{s_\mu,s_\mu}(\tau \neq 0)$

$$= \frac{1}{4}\Big(\theta_{b_\mu,b_\mu}(\tau \neq 0) + \theta_{b_{\mu+1},b_{\mu+1}}(\tau \neq 0) - \theta_{b_{\mu+1},b_\mu}(\tau \neq 0) - \theta_{b_\mu,b_{\mu+1}}(\tau \neq 0)\Big)$$

autocorrelations   crosscorrelations

Therefore, by triangular inequality, we get

$$\left|\theta_{s_\mu,s_\mu}(\tau \neq 0)\right| \leq \frac{1}{4}\big(\theta_{\max}(\mathcal{B}) + \theta_{\max}(\mathcal{B}) + \theta_{\max}(\mathcal{B}) + \theta_{\max}(\mathcal{B})\big)$$

$$= \theta_{\max}(\mathcal{B}) \leq 2^m + 1$$

Proof of correlation bound

For $\mu, \nu \in \Gamma$, the correlation of s_μ and s_ν at time shift τ is given by

$$\theta_{s_\mu,s_\nu}(\tau) = \sum_{l=0}^{L-1} s_\mu[l+\tau] s_\nu[l]$$
$$= \frac{1}{4}\sum_{l=0}^{L-1}\big(b_\mu[l+\tau] - b_{\mu+1}[l+\tau]\big)\big(b_\nu[l] - b_{\nu+1}[l]\big).$$
$$= \frac{1}{4}\Big(\theta_{b_\mu,b_\nu}(\tau) + \theta_{b_{\mu+1},b_{\nu+1}}(\tau) - \theta_{b_{\mu+1},b_\nu}(\tau) - \theta_{b_\mu,b_{\nu+1}}(\tau)\Big)$$

(2) when $\mu \neq \nu$, we are checking the values $\theta_{s_\mu,s_\mu}(\tau)$ for all τ including 0,

$$= \frac{1}{4}\Big(\theta_{b_\mu,b_\nu}(\tau) + \theta_{b_{\mu+1},b_{\nu+1}}(\tau) - \theta_{b_{\mu+1},b_\nu}(\tau) - \theta_{b_\mu,b_{\nu+1}}(\tau)\Big)$$

crosscorrelations

crosscorrelations
since $\mu + \nu \neq 1$ implies $\mu \neq \nu + 1$ and $\mu + 1 \neq \nu$

Without the condition that $\mu + \nu \neq 1$, it may happen that $\mu = \nu + 1$ and $\mu + 1 = \nu$. Then these become autocorrelations and the values at $\tau = 0$ matters!

Therefore, similarly,

$$\left|\theta_{s_\mu,s_\nu}(\tau)\right| \leq \frac{1}{4}\big(\theta_{\max}(\mathcal{B}) + \theta_{\max}(\mathcal{B}) + \theta_{\max}(\mathcal{B}) + \theta_{\max}(\mathcal{B})\big)$$
$$= \theta_{\max}(\mathcal{B}) \leq 2^m + 1 \qquad \square$$

Example: $n = 4$
Punctured bent function sequences

- $\alpha \in \mathbb{F}_{2^4}$ be a primitive element, a root of $x^4 + x + 1$
- Let $f(x) = x^3$ over $\mathbb{F}_{2^2}$
- **Walsh-Hadamard Transform** of f :

$$\hat{f}(\eta)=\sum_{x\in\mathbb{F}_{2^2}}(-1)^{f(x)+\mathrm{Tr}_1^2(\eta x)} \text{ over } \mathbb{F}_{2^2}$$

x	$f(x)$	$\mathrm{Tr}_1^2(0\cdot x)$	$\mathrm{Tr}_1^2(1\cdot x)$	$\mathrm{Tr}_1^2(\alpha\cdot x)$	$\mathrm{Tr}_1^2(\alpha^2\cdot x)$
0	0	0	0	0	0
1	1	0	0	1	1
α	1	0	1	1	0
α^2	1	0	1	0	1

$\hat{f}(0) = 1 - 1 - 1 - 1 = -2$

$\hat{f}(1) = 1 - 1 + 1 + 1 = +2$

$\hat{f}(\alpha) = 1 + 1 + 1 - 1 = +2$

$\hat{f}(\alpha^2) = 1 + 1 - 1 + 1 = +2$

$|\hat{f}(\eta)|=2$ for all $\eta \in \mathbb{F}_{2^2}$

$f(x) = x^3$ is a **bent function** over $\mathbb{F}_{2^2}$

Example: $n = 4$
Punctured bent function sequences

- $m = 2$ and $n = 4$
- $\alpha \in \mathbb{F}_{2^4}$ be a primitive element, a root of $x^4 + x + 1$
- $f(x) = x^3$ is a bent function over $\mathbb{F}_{2^2}$
- Choose a constant $\sigma = \alpha \in \mathbb{F}_{2^4} \backslash \mathbb{F}_{2^2}$.
- For any $\mu \in \mathbb{F}_{2^2}$, the sequence

$$\boldsymbol{b}_\mu[l] = (-1)^{f\left(\mathrm{tr}_2^4(\alpha^l)\right) + \mathrm{tr}_1^4\left((\mu+\alpha)\alpha^l\right)}$$

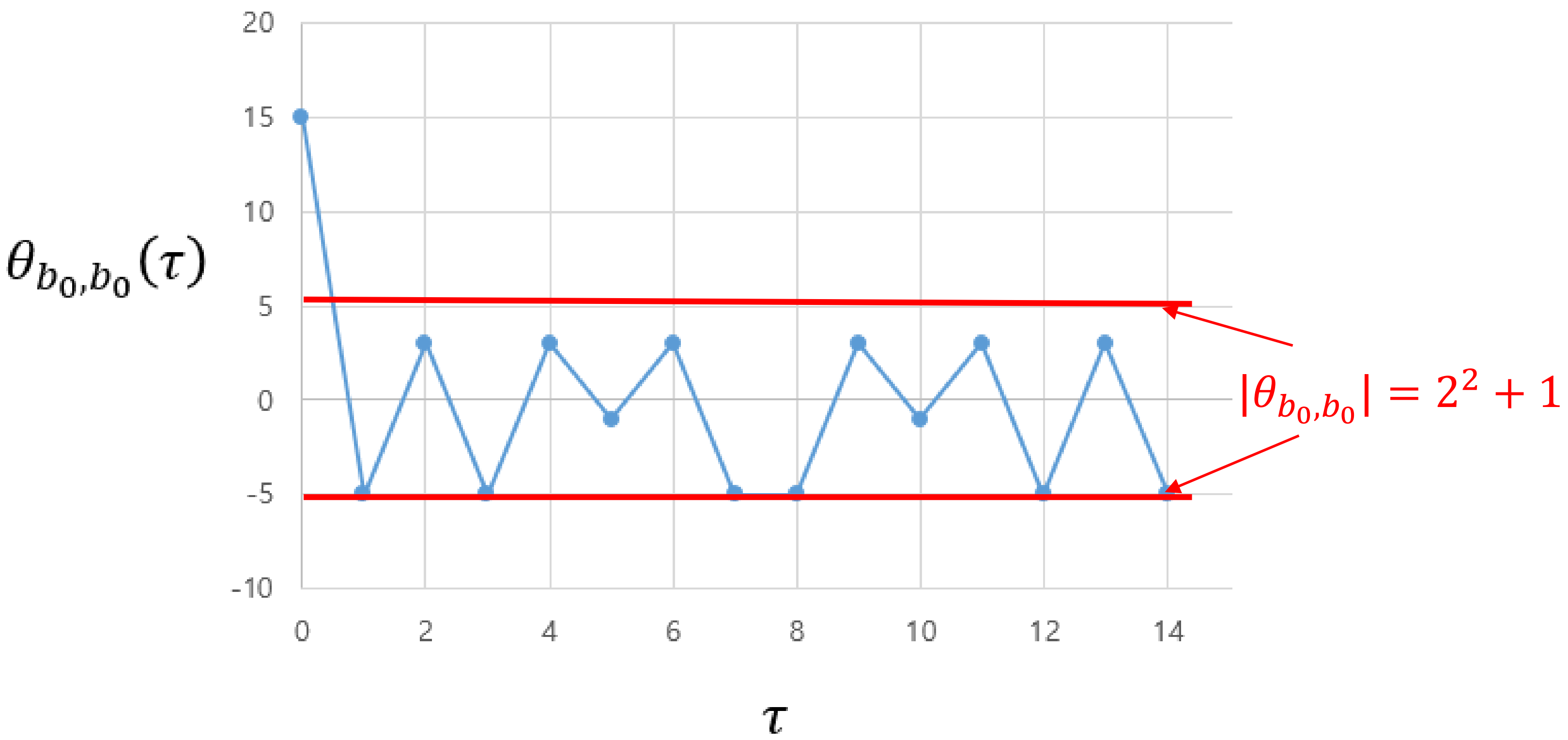
is a **bent function sequence** of length $2^4 - 1 = 15$

There are 4 of them:

- μ=0: + − + − − − + − + − − + + + −
- μ=1: + − + + − − − + + + − − − − +
- $\mu=\alpha^5$: + + − − + − − + − + − + + − −
- $\mu=\alpha^{10}$: + + − + + − + − − − − − − + +

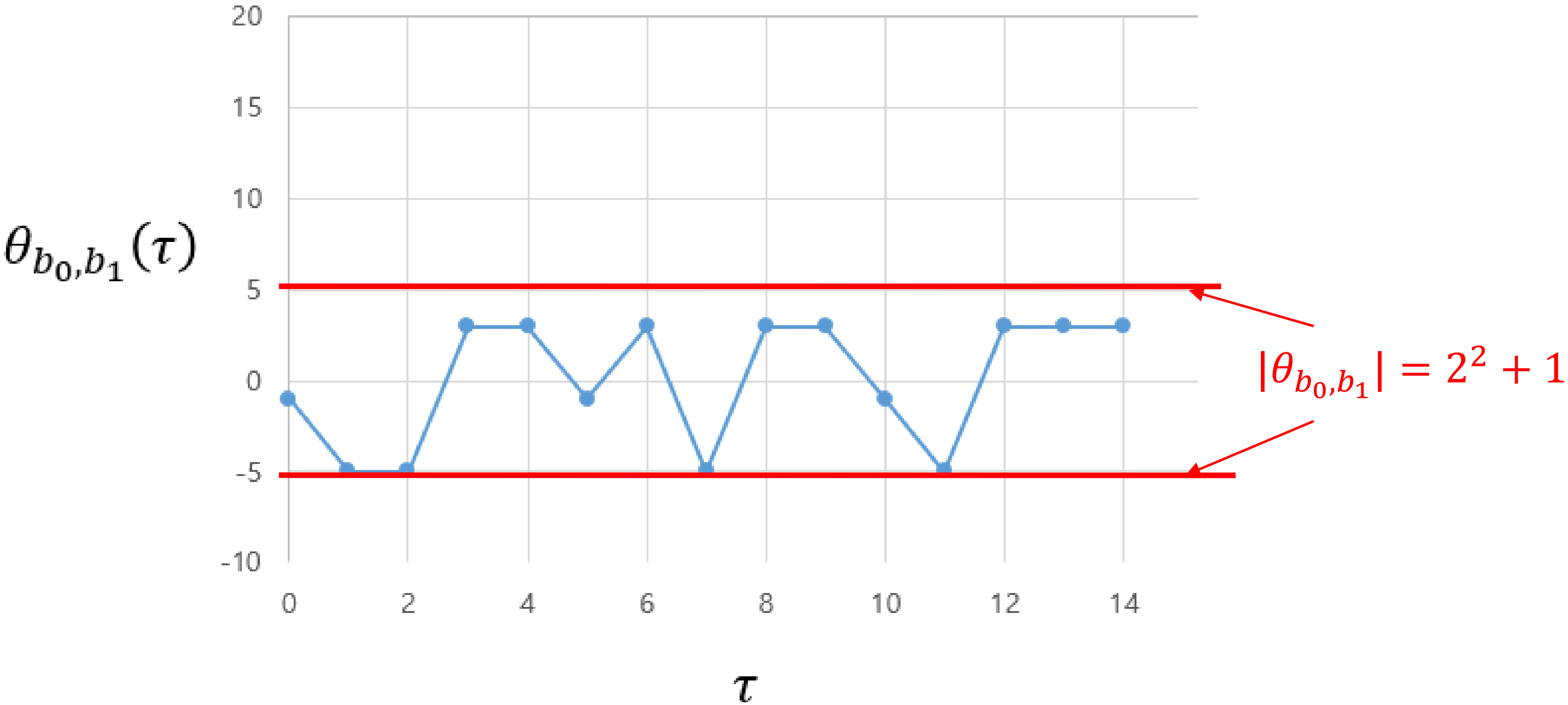
Example: $n = 4$, Continued

- $b_0 = + - + - - - + - + - - + + + -$



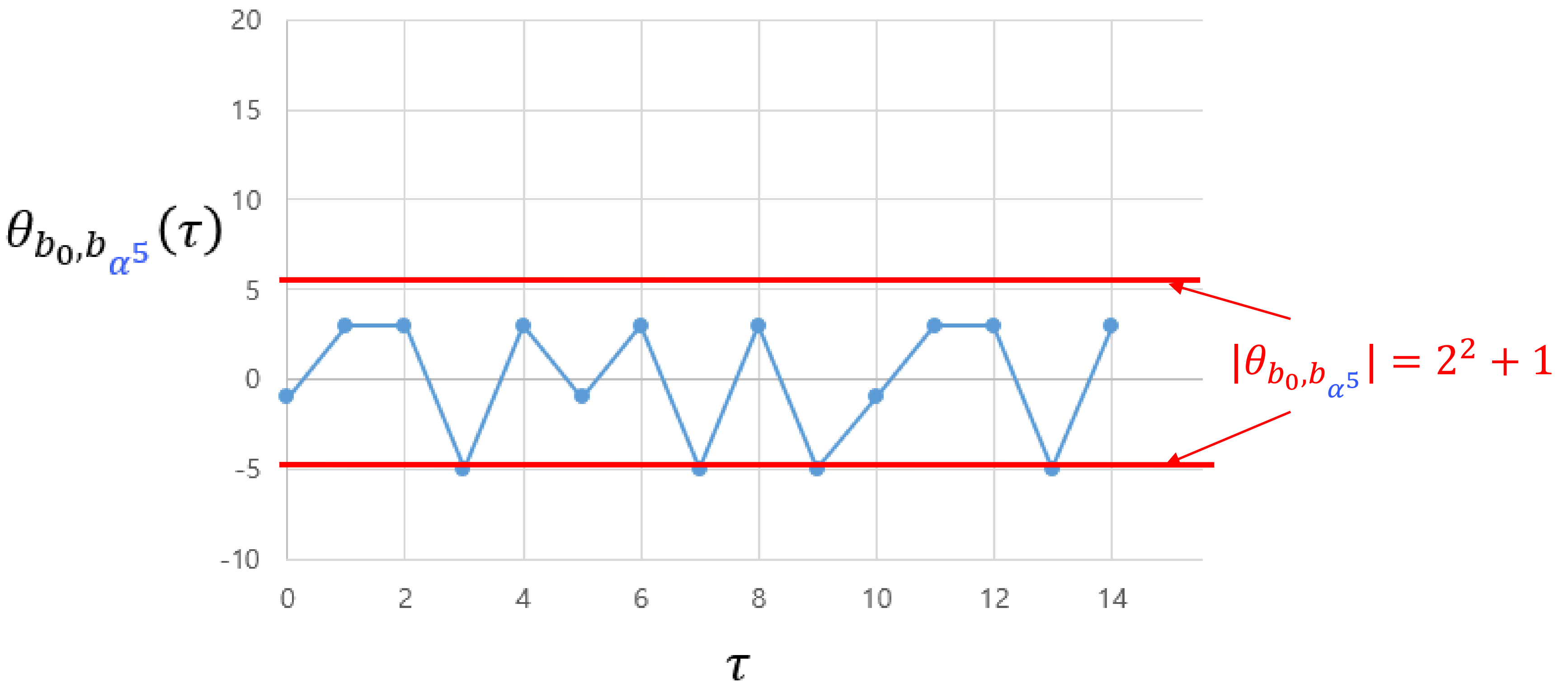
Example: $n = 4$, Continued

- $b_0 = + \ - \ + \ - \ - \ - \ + \ - \ + \ - \ - \ + \ + \ + \ -$
  $b_1 = + \ - \ + \ + \ - \ - \ - \ + \ + \ + \ - \ - \ - \ - \ +$



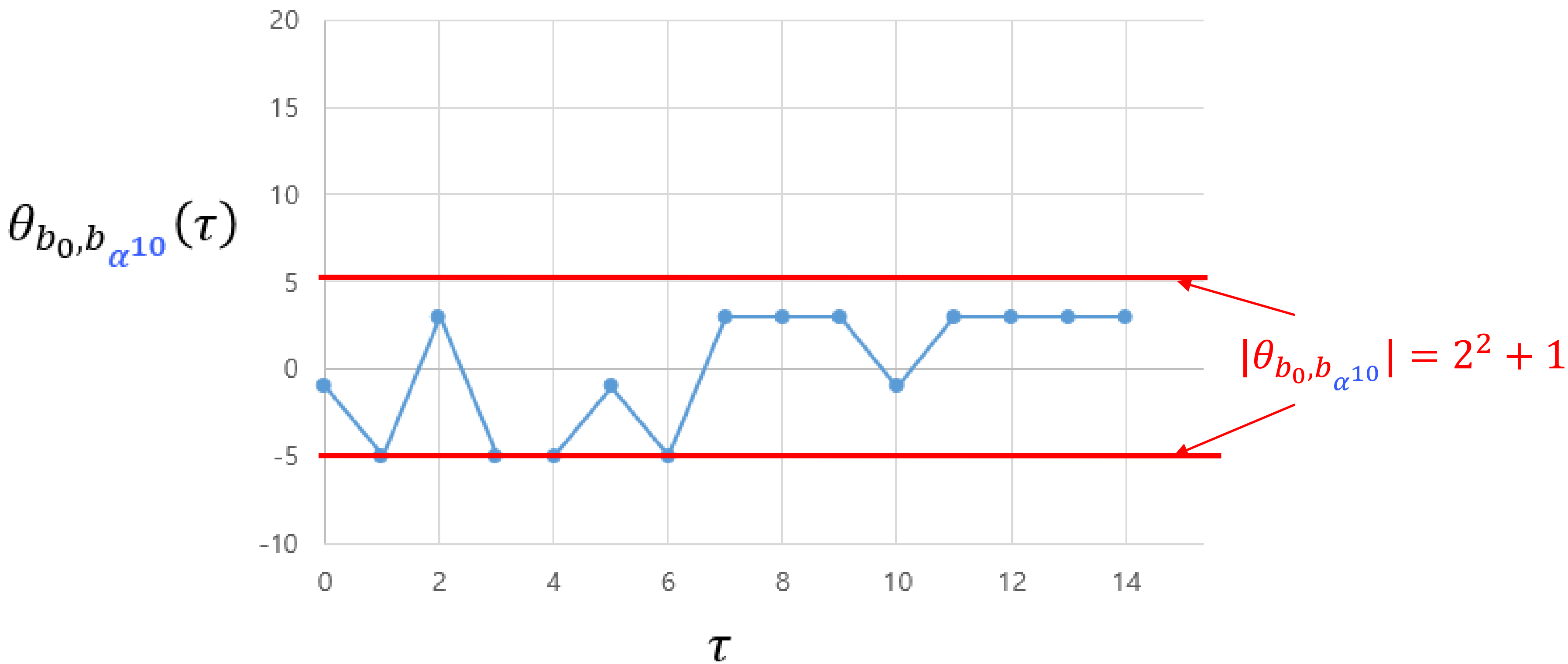
Example: $n = 4$, Continued

- $b_0 = + - + - - - + - + - - + + + -$
  $b_{\alpha^5} = + + - - + - - + - + - + + - -$

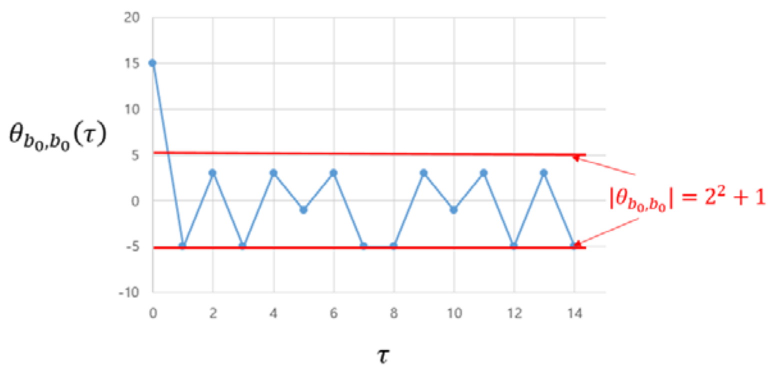


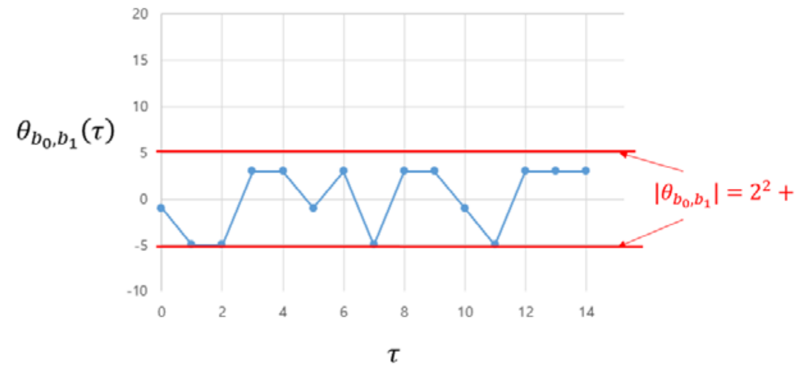
Example: $n = 4$, Continued

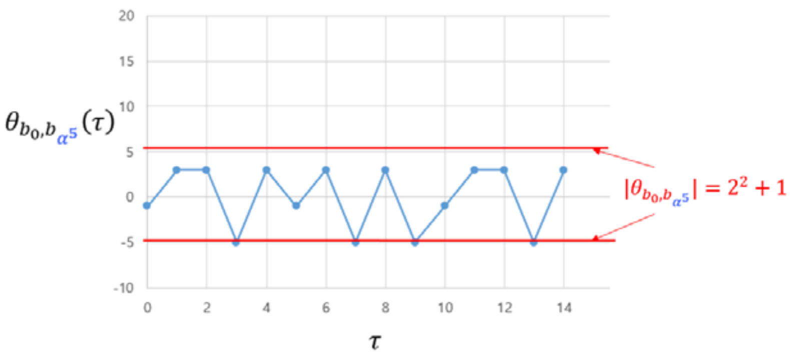
- $b_0 \;= + \; - \; + \; - \; - \; - \; + \; - \; + \; - \; - \; + \; + \; + \; -$
  $b_{\alpha^{10}} = + \; + \; - \; + \; + \; - \; + \; - \; - \; - \; - \; - \; - \; + \; +$

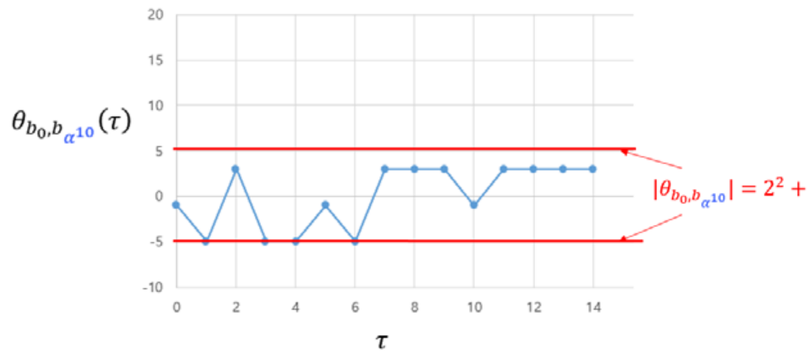


Example: $n = 4$, Continued









- $\theta_{max}(\boldsymbol{\mathcal{B}}) = 2^2 + 1$

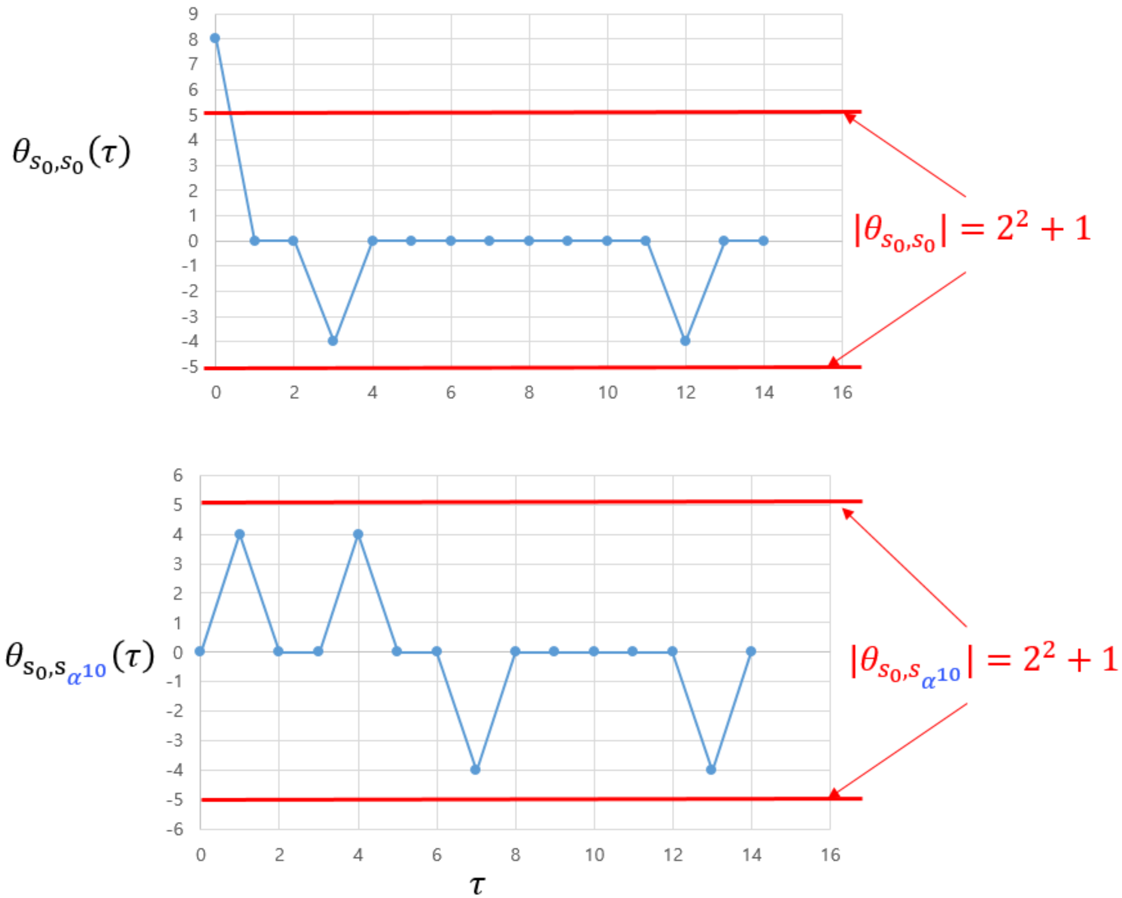
Example: $n = 4$, Continued

- $\boldsymbol{\Gamma} = \{0, \alpha^5\}$ be a subset of $\mathbb{F}_{2^4}$ such that $\boldsymbol{\mu} + \boldsymbol{\nu} \neq \mathbf{1}$ for any $\boldsymbol{\mu}, \boldsymbol{\nu} \in \boldsymbol{\Gamma}$.
- $\wp$ is the puncturing pattern given by $l \in \wp$ iff $tr_1^4(\alpha^l) = 0$.
- Note that, $tr_1^4(\alpha^l) = 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1$.
- Therefore, $\wp = \{0, 1, 2, 4, 5, 8, 10\}$

Finally, the set of **punctured bent function sequences** $S = \{s_\mu : \mu \in \Gamma\}$ contains only two sequences, for μ=0 and $\mu=\alpha^5$. These are

- μ=0: 0 0 0 − 0 0 + − 0 − 0 + + + −
- $\mu=\alpha^5$: 0 0 0 − 0 0 − + 0 + 0 + + − −

Example: $n = 4$, Continued



- $\theta_{max}(\boldsymbol{S}) = 4 \leq 2^2 + 1 = \theta_{max}(\boldsymbol{\mathcal{B}})$

Example: $n = 8$

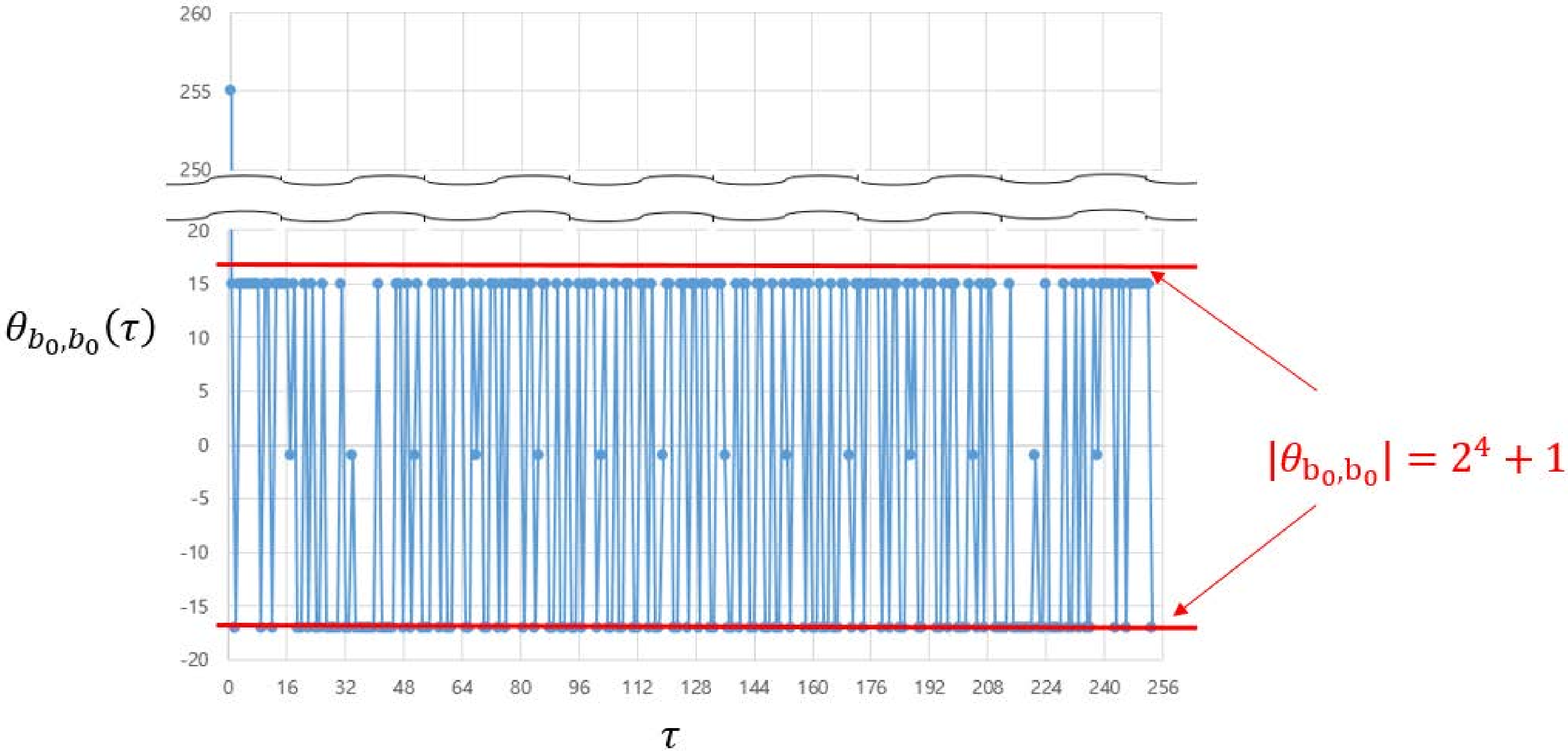
For bent function sequences...

- m =8 and $n = 4$
- $\alpha \in \mathbb{F}_{2^8}$ be a primitive element, a root of $x^8 + x^7 + x^2 + x^1 + 1$
- $f(x) = \mathrm{Tr}_1^4(\alpha^{17}x^3)$ is a bent function over $\mathbb{F}_{2^4}$
- Choose a constant $\sigma = \alpha \in \mathbb{F}_{2^8} \backslash \mathbb{F}_{2^4}$.
- Represent correlation only the case $\boldsymbol{\mu}$=0, $\alpha^{17} \in \mathbb{F}_{2^4}$.

For punctured bent function sequences...

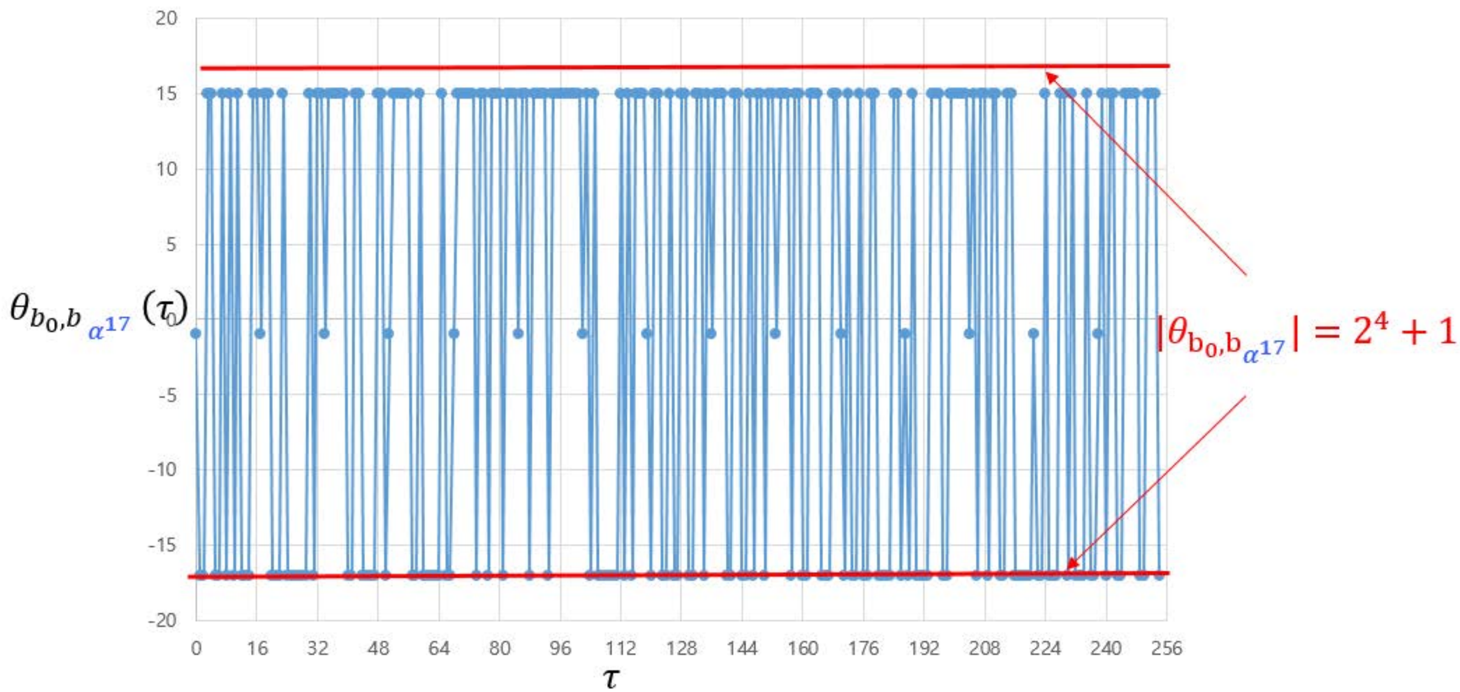
- $\boldsymbol{\Gamma} = \{0, \alpha^{17}\}$ be a subset of $\mathbb{F}_{2^8}$ such that $\boldsymbol{\mu} + \boldsymbol{\nu} \neq \mathbf{1}$ for any $\boldsymbol{\mu}, \boldsymbol{\nu} \in \boldsymbol{\Gamma}$.
- $\wp$ is the puncturing pattern given by $l \in \wp$ iff $tr_1^8(\alpha^l) = 0$.

Example: $n = 8$, Continued



Autocorrelation of bent function sequences

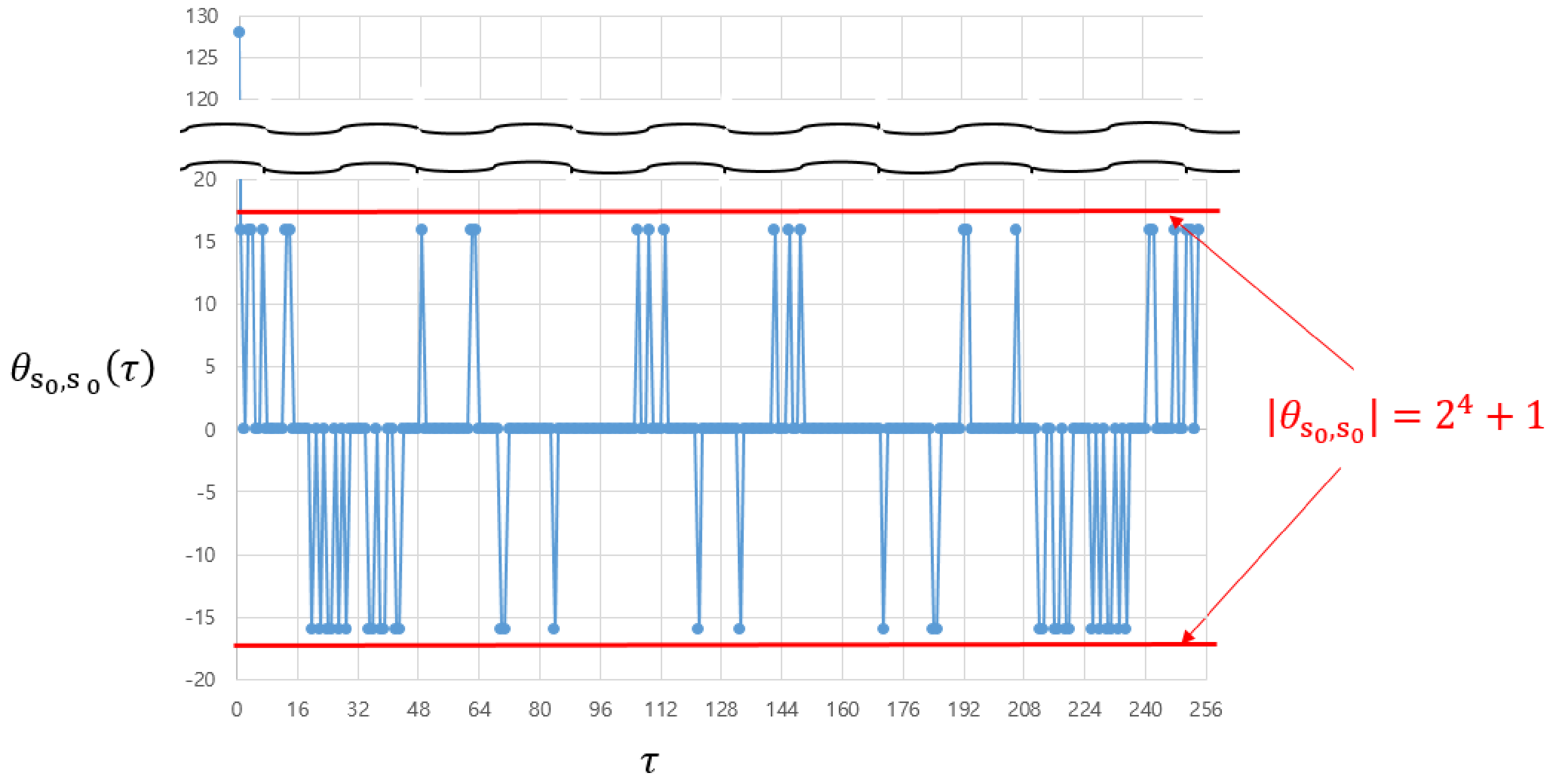
Example: $n = 8$, Continued



Crosscorrelation of bent function sequences

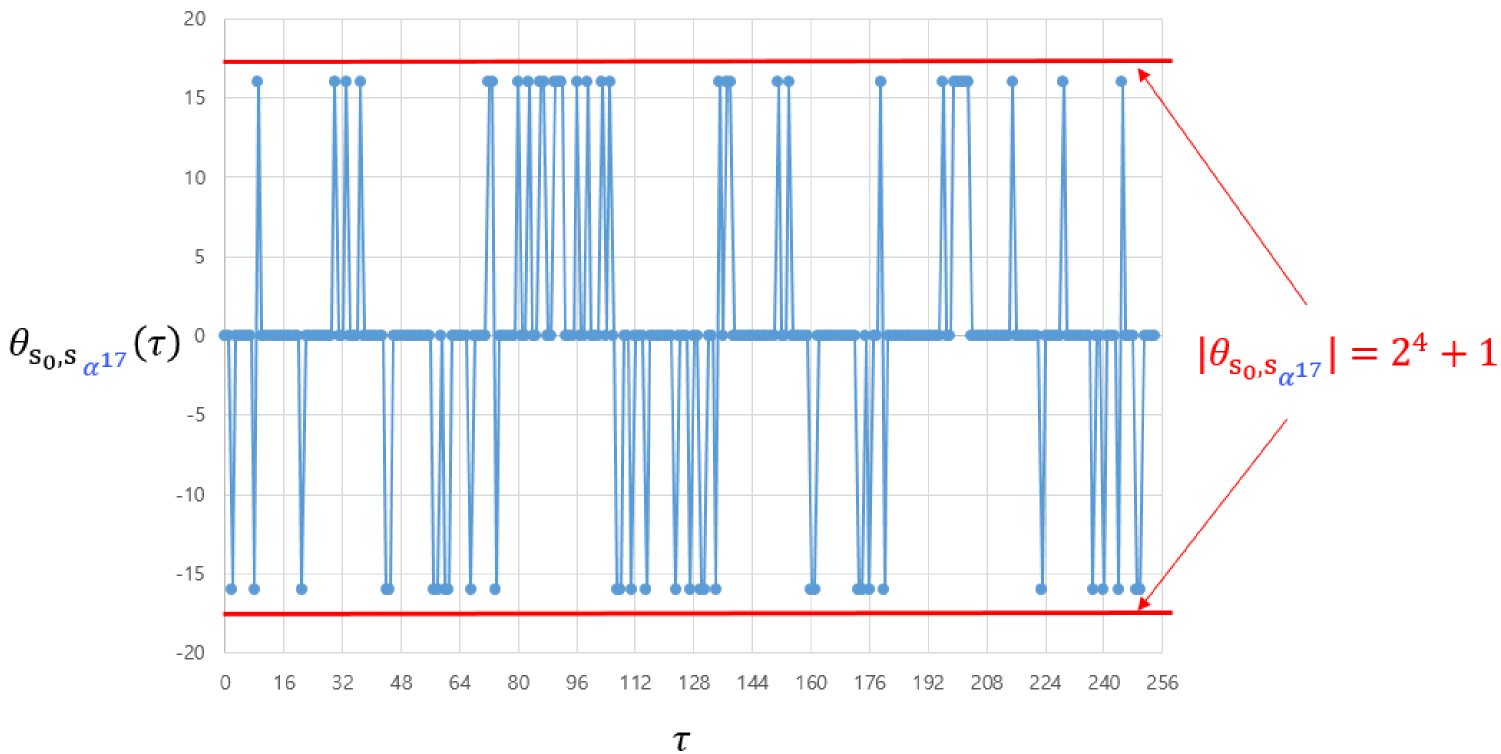
- $\theta_{max}(\mathcal{B}) = 2^4 + 1$

Example: $n = 8$, Continued



Autocorrelation of punctured bent function sequences

Example: $n = 8$, Continued



Crosscorrelation of punctured bent function sequences

- $\theta_{max}(\boldsymbol{S}) = 16 \leq 2^4 + 1 = \theta_{max}(\boldsymbol{\mathcal{B}})$

Properties of Punctured bent function sequences

- The **cardinality** of S is $|\Gamma| = 2^{m-1}$.
  - Because of Γ in which $\mu + \nu \neq 1$
- S is **optimal** in terms of C_2.
  - Because puncturing pattern of S is Singer difference set.
- Any sequence in S has the energy $E = \theta(0) = 2^{n-1}$, which is about **half the energy of the original** bent function sequences.
  - Because $|\wp| = 2^{n-1} - 1$ is about the half the length
- S is asymptotically **optimal** in terms of C_1 also.
  - Both S and the original bent function sequences have **the same upper bound** on the maximum non trivial correlation magnitude
  - Since the energy is reduced by half, this upper bound $\theta_{max}(S)$ asymptotically achieves **TWO times the Welch bound**.

Some open questions

- For the puncturing pattern from the Singer's difference set, **try some other spreading sequences**
  - Gold, Kasami, etc
- Optimal puncturing patterns must be from either ACDS or CDS.
  - They all are optimal but some implications might be different when it applies to some other spreading sequences.
  - Does there **any pair of puncturing pattern and spreading sequences** that can be provable mathematically, **other than** those mentioned in this talk
- **Main theorem implies:** we have constructed a set of 2^{m-1} ternary sequences of length $2^{2m}-1$ such that
  1. Number of **0**'s is $2^{m-1}-1$ in each sequence
  2. Number of non-zeros (either **+1** or **-1**) is 2^{m-1} in each sequence
  3. Max correlation magnitude is upper bounded by **2 times Welch Bound**.

True/False:

this is a set of BEST ternary sequence family in terms of Welch Bound.

Any questions?