확산코드 내 워터마크 삽입에 관한 연구

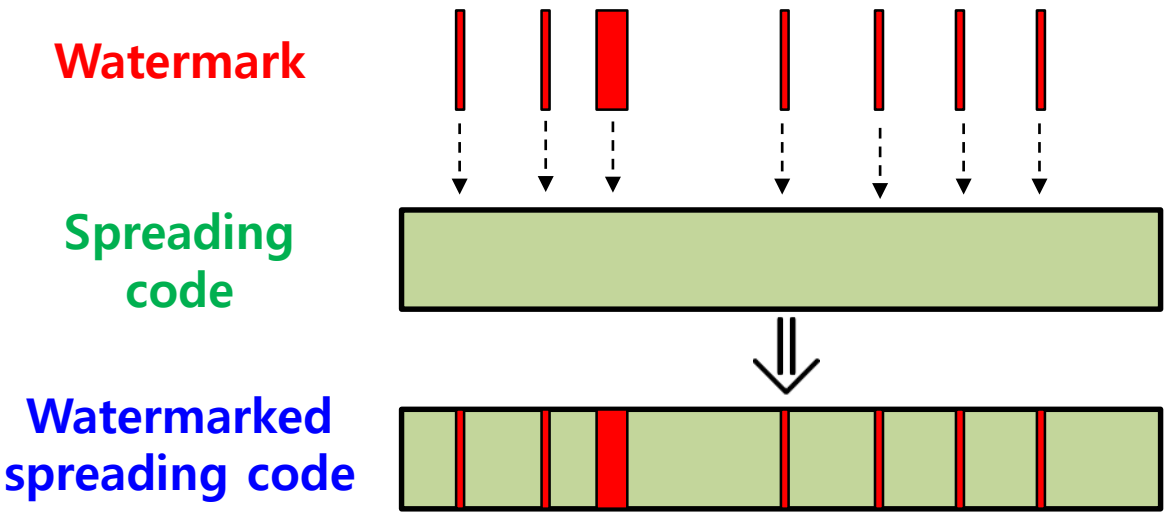
(On the Insertion of a Watermark in Spreading Codes)

송민규, 송홍엽 (연세대학교)
이장용 (국방과학연구소)

2018 항법시스템학회 정기학술대회

2018. 11. 08

Watermarked DSSS



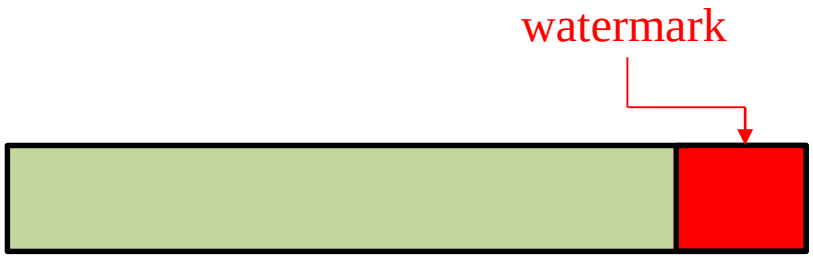
- Inserting some watermark into a spreading code
- Any two watermarks at different time are different.
- Each watermarked chip is either $+1$ or -1.

Why we consider?

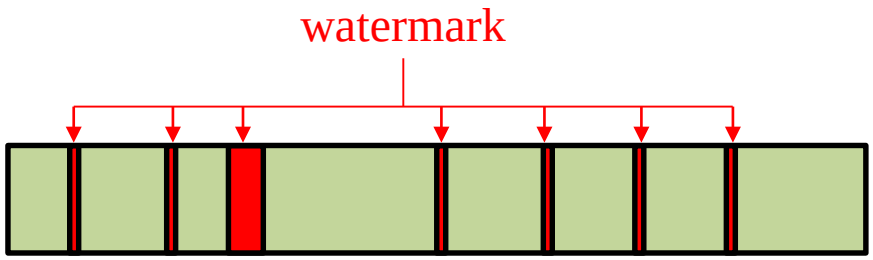
- Watermarked DSSS have been considered to provide security at the signal level
  - Steganography
    - Watermark conveys some information which can be extracted after synchronized.
  - Authentication of GNSS open signals
    - Watermark is used to provide where a signal comes from
    - Protect from spoofing attacks
  - An option of GPS M signal for fast acquisition

How to insert watermark?

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



Case 1. aggregated

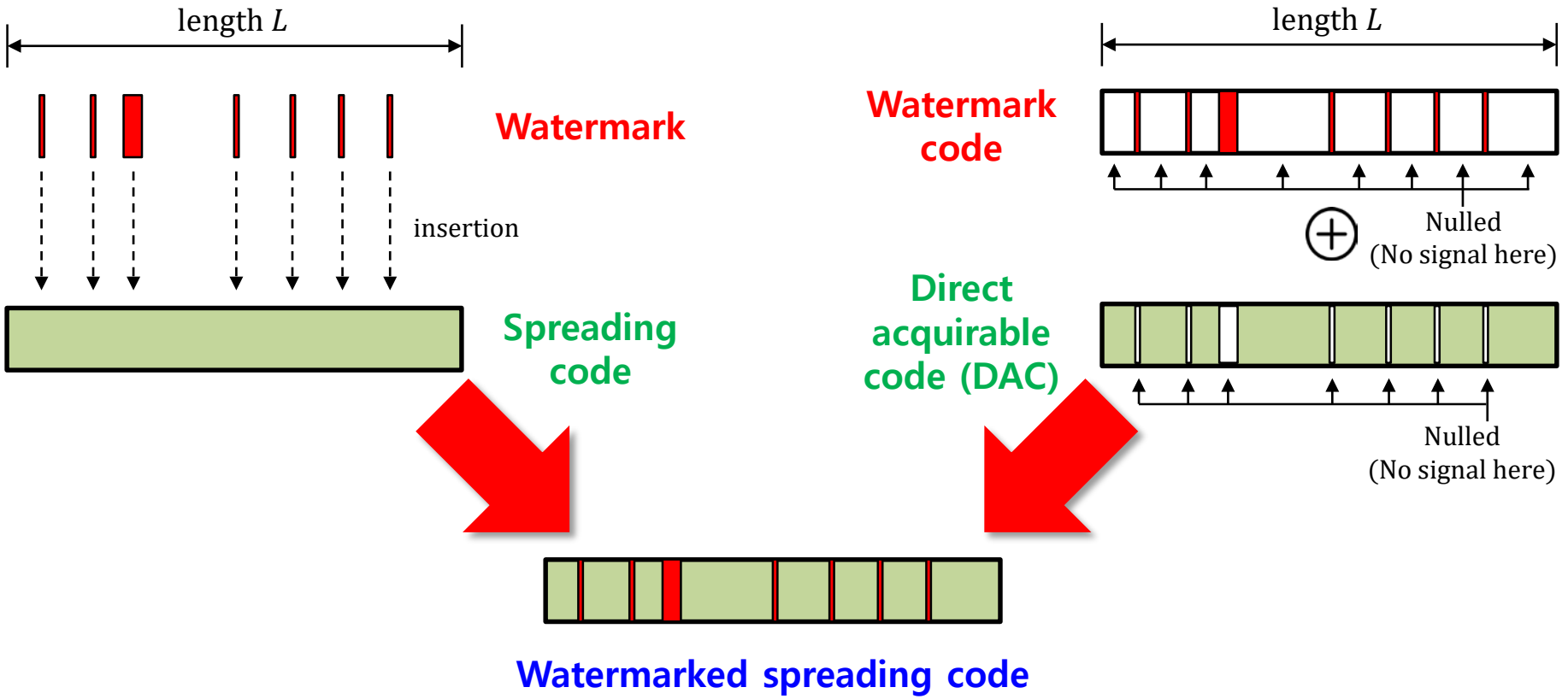


Case 2. spread

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

What insertion is better in the sense of acquisition performance?

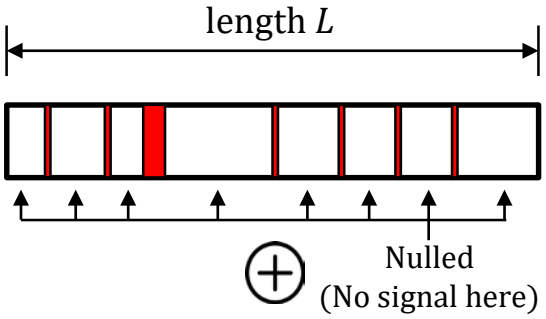
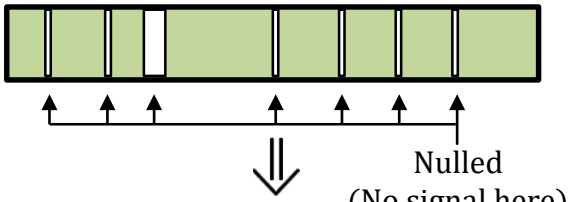
Equivalent model



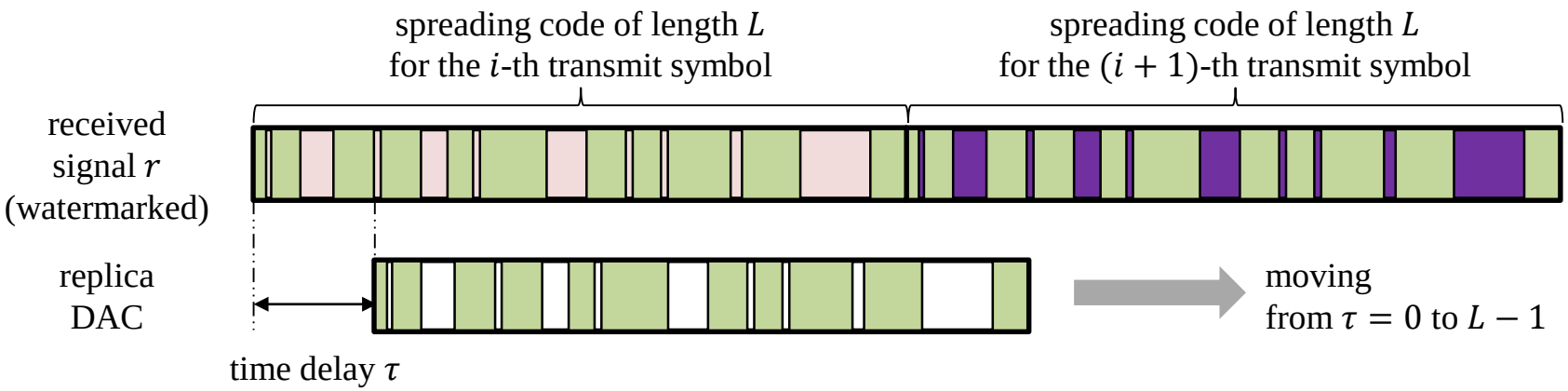
Assume that watermarked chip is a random variable over $\{+1, -1\}$

$+1$ with probability 0.5

Some properties

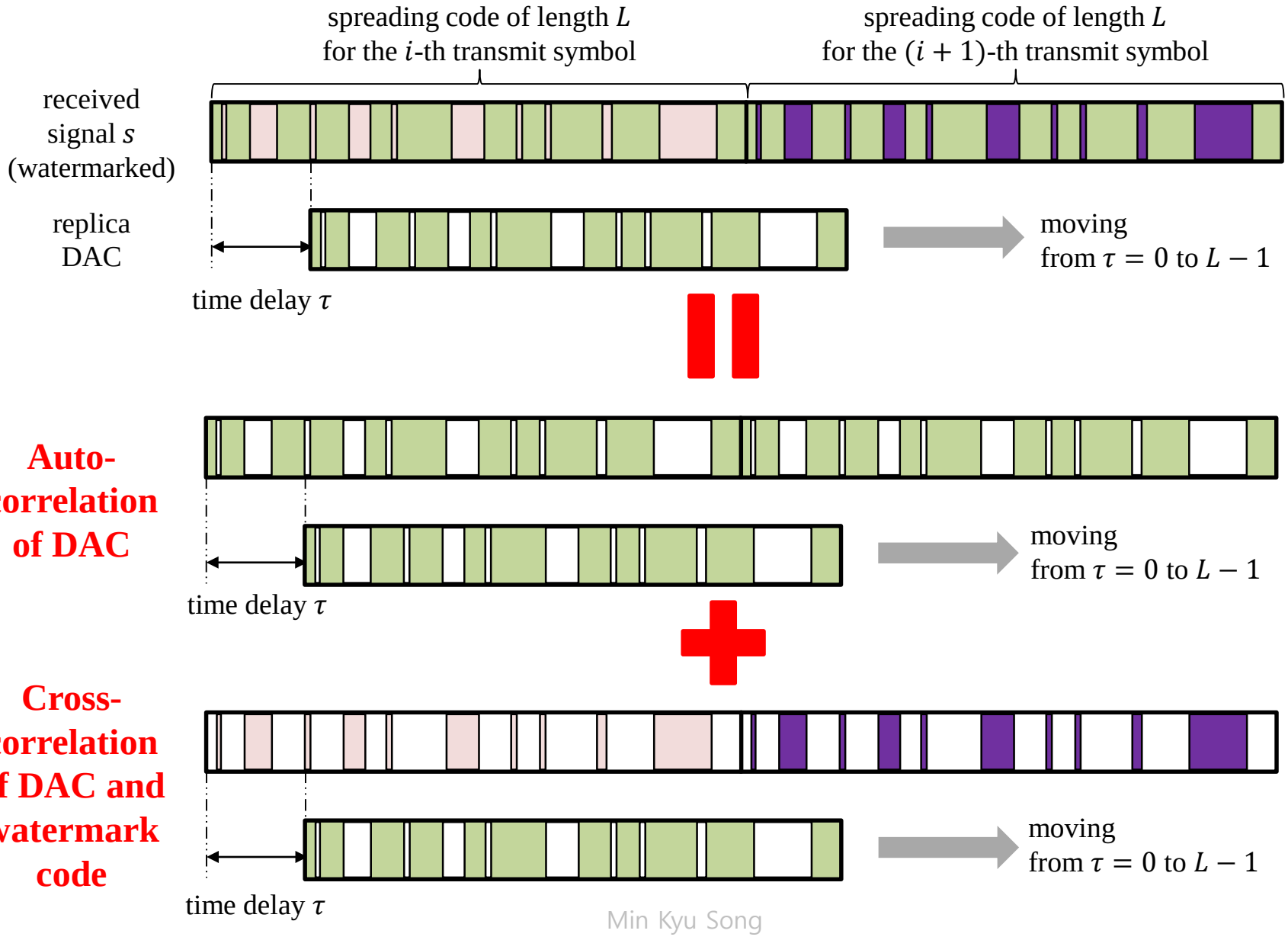
		Alphabet?	Repeated?
watermark		Ternary $\{0, +1, -1\}$	Not repeated
Spreading code		Ternary $\{0, +1, -1\}$	Repeated periodically
Watermarked spreading code		Binary $\{+1, -1\}$	Partially repeated

Acquisition for watermarked DSSS

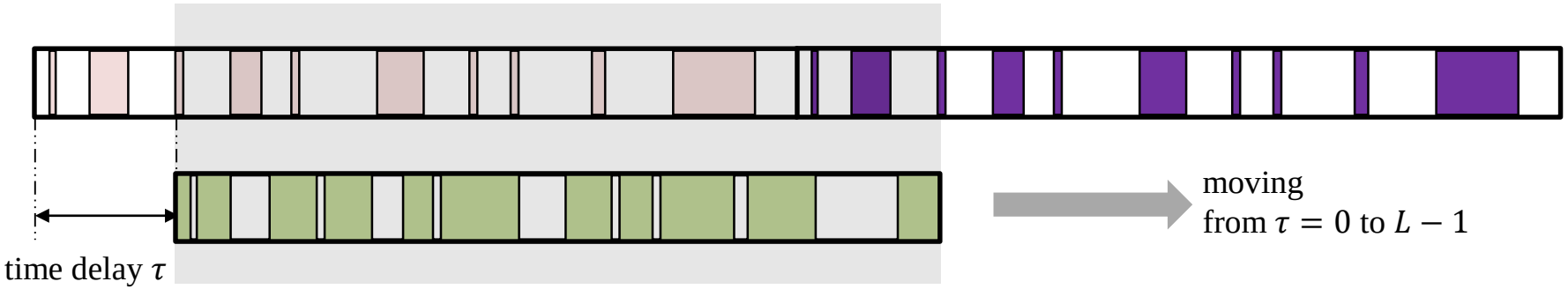


- At the acquisition process,
  the receiver **know which chips are watermarked**.
  - But has **no information about what the watermark is**.
- Therefore, It can only use the direct acquirable code (DAC), which is repeated, periodically.

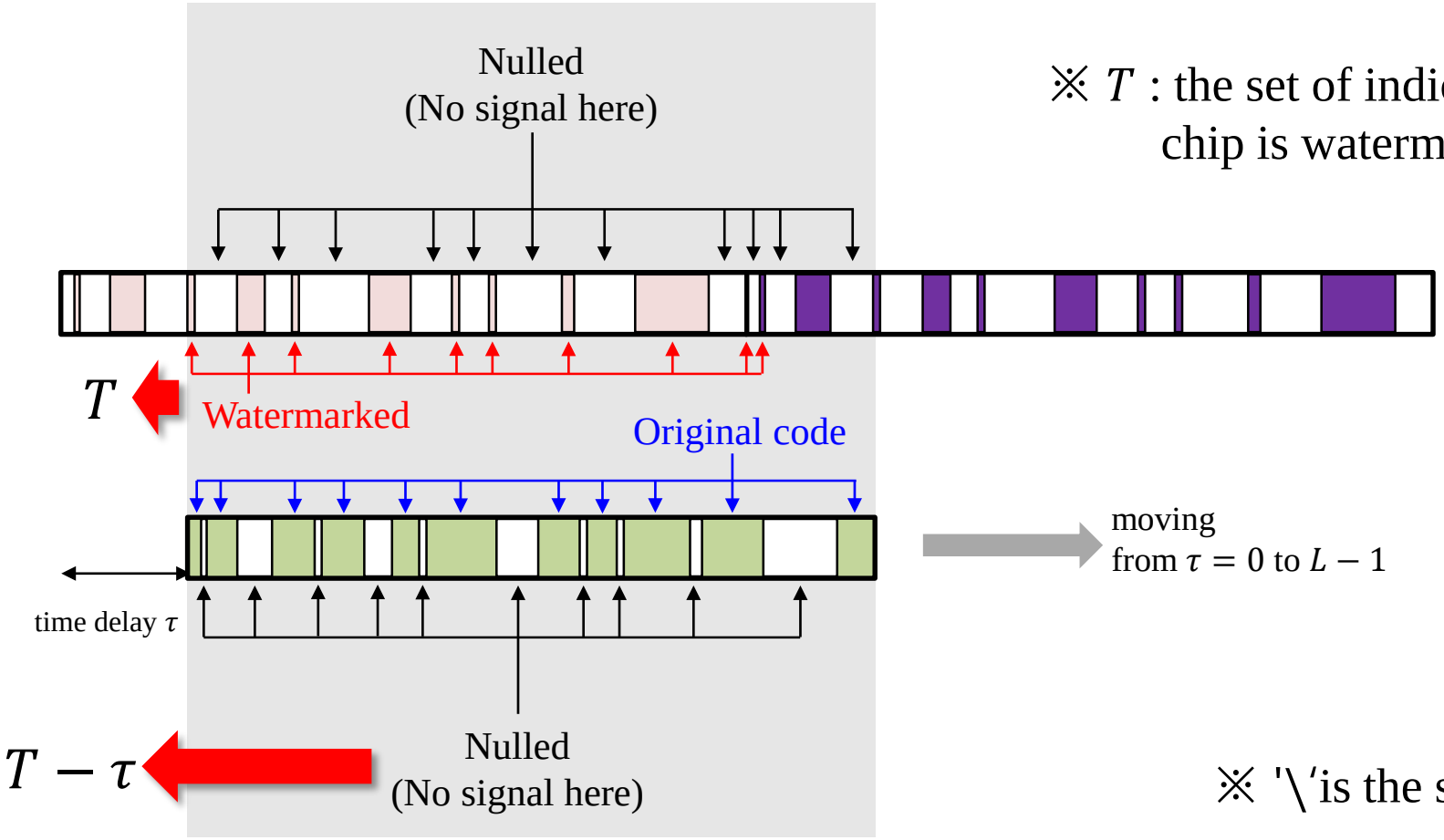
Under ideal channel condition



$$C_{r,\mathrm{DAC}}(\tau) = C_{\mathrm{DAC}}(\tau) + C_{\mathrm{DAC,W}}(\tau)$$



Inner product of two vectors of length L



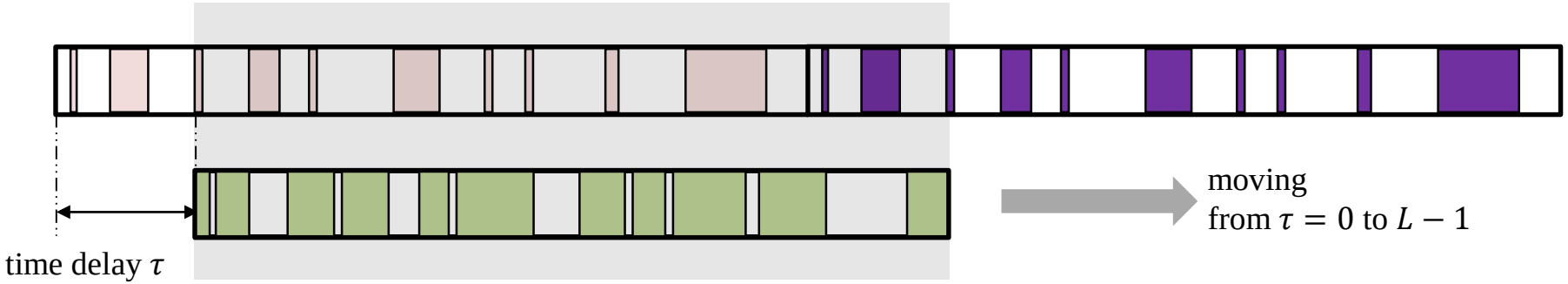
※ T : the set of indices where a chip is watermarked

※ '\'is the set minus

Inner product of two vectors of length L

$$(\#\ \text{Hit of watermark and original}) = |T \setminus (T - \tau)|$$

$$C_{r,\mathrm{DAC}}(\tau) = C_{\mathrm{DAC}}(\tau) + C_{\mathrm{DAC,W}}(\tau)$$



Inner product of two vectors of length L

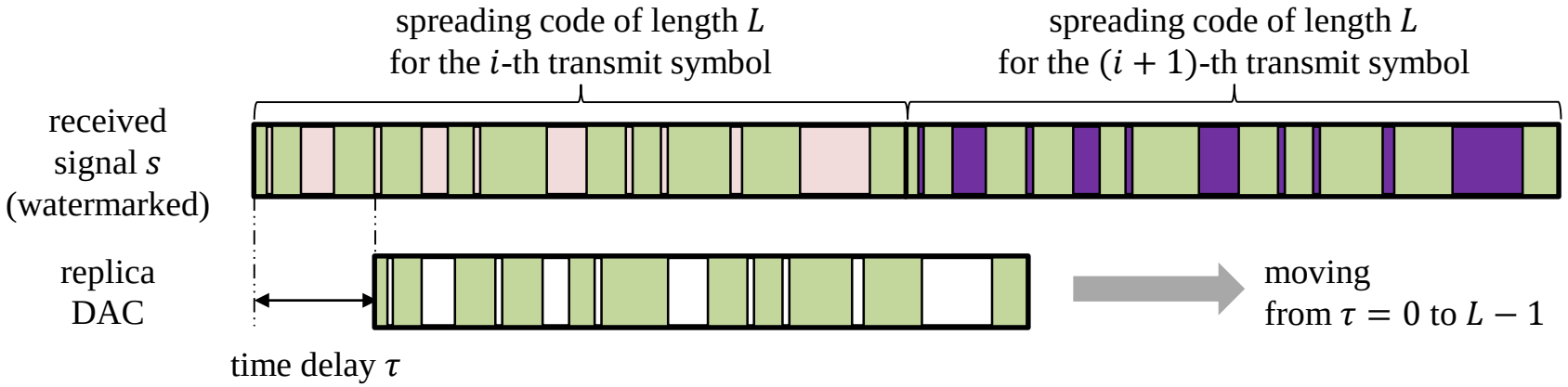
(# Hit of watermark and original) $= T \setminus (T - \tau)$

Each hit is +1 with prob. 0.5 and -2 with prob. 0.5

$$C_{\mathrm{DAC,W}}(\tau) \approx \mathcal{N}\left(0, \sigma^2(\tau; T)\right) = \mathcal{N}(0, |T \setminus (T - \tau)|)$$

where T is the set of indices where a chip is watermarked

watermark insert position design



$$C_{\mathrm{s,DAC}}(\tau) = C_{\mathrm{DAC}}(\tau) + C_{\mathrm{DAC,W}}(\tau)$$

1. Minimize auto-correlation magnitude of DAC

   ⇒ For a given spreading code, it is hard to control in general

2. Minimize the variance $\sigma^2(\tau; \mathrm{T})$ of AWGN modeled $\mathrm{C_{DAC,W}}(\tau)$

   ⇒ Minimizing the maximum of $|T \backslash (T-\tau)|$ for any time shift

Sum of all the variances

$$C_{\mathrm{DAC,W}}(\tau) \approx \mathcal{N}\left(0, \sigma^2(\tau; T)\right) = \mathcal{N}(0, |T \backslash (T-\tau)|)$$

Lemma. For given two positive integers k, L with $k < L$, let T be a k-subset of $\mathbb{Z}_L$. Then,

$$\sum_{\tau=0}^{L-1} |T \backslash (T-\tau)| = kL - k^2.$$

If k, L are fixed, then the total amount of the AWGN modeled self-interference $C_{\mathrm{DAC,W}}(\tau)$ is fixed!

Lower bound on the max. variance

It is obvious that $|T \setminus (T - \tau)| = 0$ if $\tau = 0$.

Theorem. Assume that k watermarks are inserted in a watermarked spreading code of length L, according to the insert position T. Then,

$$\max_{0 \le \tau \le L-1} |T \setminus (T - \tau)| \ge \left\lceil \frac{kL - k^2}{L - 1} \right\rceil.$$

How to achieve?

Definition. For given two positive integers k, L with $k < L$, let T be a k-subset of $\mathbb{Z}_L$.
Then, T is called a (L, k, λ)-cyclic difference set if

$$\{d - d' \pmod{L} | d, d' \in T, d \neq d'\}$$

Corollary. For given two positive integers k, L with $k < L$, let T be a k-subset of $\mathbb{Z}_L$.
If T is a (L, k, λ)-cyclic difference set, then

$$|T \setminus (T - \tau)| = k - \lambda$$

for any $1 \leq \tau \leq L - 1$.

binary sequences with two-level autocorrelation function

1-1 correspondence

A CDS ⟺ '0's (or '1's) in a binary sequence with two-level autocorrelation function

Examples:

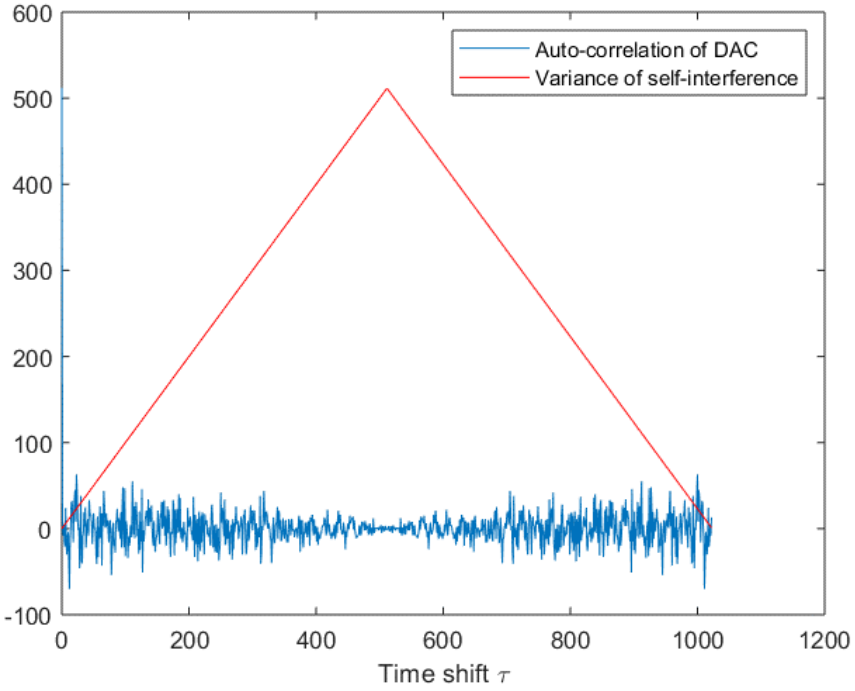
- ✓ M-sequence of length $2^n - 1$
- ✓ Legendre sequence of length p with $p \equiv 3 \pmod 4$
- ✓ Twin prime sequence of length $p(p+2)$
- ✓ Etc.

※ n : a positive integer
$p,\ p+2$: prime numbers

An example: aggregated vs spread

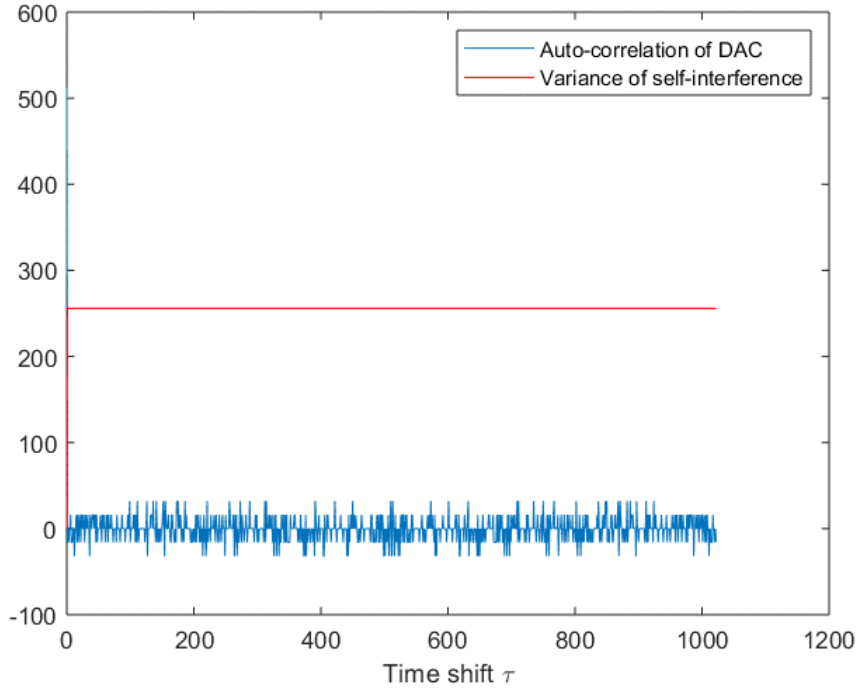
511 watermarked chips inserted into a Gold code of length 1023

aggregated



spread

(based on '0's in an m-sequence)



Auto-correlation side peak : 70
Maximum variance : 511

→

Auto-correlation side peak : 32
Maximum variance : 255

Both are reduced about half

Conclusion & Future work

- We give some analysis on the effect of watermark insertion on the auto-correlation of spreading code
  - We describe a lower bound and how to achieve the bound.
  - Spread insertion can achieve better performance than aggregated insertion.

- We will extend this work to watermarked DS-CDMA
  - It requires multiple spreading codes with good auto- and cross-correlation.