

# Design of LPI Signals Using Optimal Families of Perfect Polyphase Sequences

Inseon Kim, Ki-Hyeon  
Park, Min Kyu Song and  
**Hong-Yeop Song**  
**Yonsei University**

Jang Yong Lee  
**Agency for Defense  
Development**

ISITA 2016, October 30- November 2



# Contents



- Introduction
  - Motivation
  - Low-Probability Interception(LPI)
  - Direct Sequence Spread Spectrm(DSSS)
- Construction of Sequence Family
- Proposed LPI Communication System
- Summary

Modern physical attack are considered to be jamming attack or spoofing attack. Many attacks for GPS are reported. Even some people use GPS spoofing for Pokemon Go!

**PHYS.ORG** Nanotechnology ▾ Physics ▾ Earth ▾ Astronomy & Space ▾ Technology ▾ Chemistry ▾

**US reconnaissance plane emergency landings during a major**

A US military reconnaissance plane emergency landing during a major r

Ad closed by Google

on March 4, forced the plane to mak quoted the report as saying.

They also affected South Korean na Seoul's Gimpo area, according to th

Seoul mobile users also complained malfunctioning as the South and the

The communist state has about 20 t developing a new device with a rang Yonhap news agency has said.

**boingboing** / CORY DOCTOROW / 8:24 AM THU AUG 4, 2015

**Spoofing GPS is surprisingly easy; de-hard**

False GPS signals transmitted by attacker

GPS security is increasingly implicated in both physical and inform security: from steering a super-yacht (or a super-tanker) into pirate-waters to diverting self-driving cars or even unlocking geo-tagged to and AR game objectives.

**BGR** TECH ENTERTAINMENT SOCIAL LIFESTYLE BUSINESS DEALS PODCAST + TIP US SEARCH

**Pokemon Go cheat that lets you walk anywhere without jailbreaking still works after update**

By Chris Smith on Sep 15, 2016 at 5:35 PM

SHARE THIS STORY Tweet Like Share Submit Shop

Niantic released a Pokemon Go update for iPhone and Android that brings over the new Buddy feature, but also prevents rooted/jailbroken devices from playing the game. Niantic's thinking here is that most Pokemon Go cheat apps will require a rooted device, so blocking rooted users would weed out cheaters. However, the best Pokemon Go cheat available on the iPhone still works following the 1.7.0 update. And the best part about it is that you don't even need to jailbreak your iPhone to make use of it.

RELATED ARTICLES



# Low-Probability of Interception(LPI)



An LPI signal is a communication signal having the following characteristics:

- 1) It is hard to understand (or capture) the meaning of the communication with LPI signals by any invalid users.
- 2) It is hard to disturb (or interrupt) the communication with LPI signals by any invalid users.
- 3) It is hard to determine (or detect) whether the communication with LPI signals is operated in specific time/frequencies by any invalid users. In other words, an invalid user cannot decide the existence of LPI signals in the air.

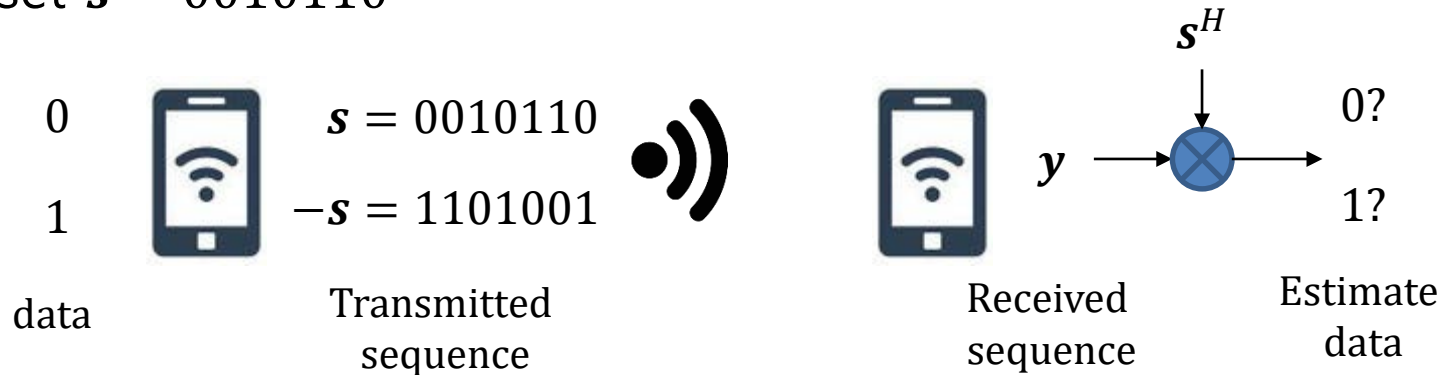


# Direct-Sequence Spread Spectrum(DSSS)

A sequence  $s$  of sufficient length is shared with both transmitter and receiver

The system is performed by encoding the messages with  $s$  and decoding with matched filter

Ex) set  $s = 0010110$



- In this system, the performance is determined by the correlation of sequences
- If unintended users **know the information of sequence  $s$** , then we can say **LPI characteristic is broken**
- GPS P(Y) or GPS M codes use these technique for LPI characteristics

## Definition 1

- 1) Two sequences  $\mathbf{u} = \{u(t) | t \in \mathbb{Z}\}$  and  $\mathbf{v} = \{v(t) | t \in \mathbb{Z}\}$  are **cyclically equivalent** if there exists an integer  $\tau$  that satisfies  $u(t) = v(t + \tau)$
- 2) Two families of sequences  $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$  and  $\mathcal{G} = \{g_1, g_2, \dots, g_n\}$  are **cyclically equivalent** if  $g_i \in \mathcal{G}$  is cyclically equivalent with some  $f_j \in \mathcal{F}$
- 3) Two families of sequences  $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$  and  $\mathcal{G} = \{g_1, g_2, \dots, g_n\}$  are **completely distinct** if there is no cyclically equivalent sequence pair  $f_i$  and  $g_j$

## Example

$$\begin{array}{l}
 \mathcal{F} = \{(0,0,0,1), (1,1,2,3), (0,1,2,1)\} \\
 \mathcal{G} = \{(0,1,0,0), (1,2,1,0), (2,3,1,1)\} \\
 \mathcal{H} = \{(0,1,0,0), (1,2,1,0), (2,3,3,3)\} \\
 \mathcal{J} = \{(0,1,0,1), (1,1,1,1), (2,1,0,0)\}
 \end{array}
 \begin{array}{l}
 \left. \begin{array}{l} \curvearrowright \\ \curvearrowright \end{array} \right\} \text{cyclically equivalent} \\
 \left. \begin{array}{l} \curvearrowright \\ \curvearrowright \end{array} \right\} \text{cyclically inequivalent \&} \\
 \left. \begin{array}{l} \curvearrowright \\ \curvearrowright \end{array} \right\} \text{not completely distinct} \\
 \left. \begin{array}{l} \curvearrowright \\ \curvearrowright \end{array} \right\} \text{completely distinct}
 \end{array}$$

Let  $\mathbf{g} = \{g(t) | t \in \mathbb{Z}\}$  be a  $p$ -ary sequence of length  $p$

$\mathcal{S}(\mathbf{g})$  : set of all  $p$ -ary sequence of length  $p^2$  s.t. any sequence  $\mathbf{s} = \{s(t) | t \in \mathbb{Z}\} \in \mathcal{S}(\mathbf{g})$  satisfies  $s(t) = s(j + pi) \equiv s(j) + i \cdot g(j) \pmod{p}$

for given  $s(j)$  for  $j = 0, 1, \dots, p - 1$

## Theorem (Park16)

If  $\mathbf{g}$  is a permutation, then all the sequences in  $\mathcal{S}(\mathbf{g})$  have the perfect auto-correlation property

Let's consider an example when  $p = 3$ . If we set  $\mathbf{g} = (0, 1, 2)$ , then  $\mathcal{S}(\mathbf{g})$  is

$$\begin{array}{cccccccccc}
 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & 2 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 2 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, & \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}, & \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}, & \begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 2 & 2 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 2 \\ 1 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}, & \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 2 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \\
 \begin{pmatrix} 2 & 0 & 0 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}, & \begin{pmatrix} 2 & 0 & 1 \\ 2 & 1 & 0 \\ 2 & 2 & 2 \end{pmatrix}, & \begin{pmatrix} 2 & 0 & 2 \\ 2 & 1 & 1 \\ 2 & 2 & 0 \end{pmatrix}, & \begin{pmatrix} 2 & 1 & 0 \\ 2 & 2 & 2 \\ 2 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 2 & 1 & 1 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}, & \begin{pmatrix} 2 & 1 & 2 \\ 2 & 2 & 1 \\ 2 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 2 & 2 & 0 \\ 2 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix}, & \begin{pmatrix} 2 & 2 & 1 \\ 2 & 0 & 0 \\ 2 & 1 & 2 \end{pmatrix}, & \begin{pmatrix} 2 & 2 & 2 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}.
 \end{array}$$

These 9 sequences are cyclically inequivalent with each other

## Theorem (Park16)

If  $\mathbf{g}(\kappa, m, \tau) = \{g(t; \kappa, m, \tau) | t \in \mathbb{Z}\}$  satisfies

$$g(t; \kappa, m, \tau) \equiv m(t + \tau)^\kappa \pmod{p}$$

for an integer  $\tau$ , an integer  $m (\neq 0)$ , and an integer  $\kappa$  that is relatively prime to  $p - 1$ , then the family  $\mathcal{F}$  of size  $p - 1$  made by picking up any one member  $s_m$  from  $\mathcal{S}(\mathbf{g}(\kappa, m, \tau))$  for each  $m = 1, 2, \dots, p - 1$  has optimum cross-correlation property

Let's consider an example when  $p = 3$ . The possible parameters are  $\kappa = 1$ ,  $m = 1$  or  $2$ , and  $\tau = 0, 1$  or  $2$ . Now, choose  $\kappa = 1$ ,  $m = 1$  and  $\tau = 0$

$$g(t; 1, 1, 0) \equiv t \pmod{3}$$

We have  $\mathbf{g}(1, 1, 0) = (0, 1, 2)$

$\mathcal{S}(\mathbf{g}(1, 1, 0))$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 2 & 0 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}, \\ \begin{pmatrix} 2 & 0 & 0 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 \\ 2 & 1 & 0 \\ 2 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 2 \\ 2 & 1 & 1 \\ 2 & 2 & 0 \end{pmatrix}.$$

$\mathcal{S}(\mathbf{g}(1, 2, 0))$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 \\ 0 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 2 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \\ \begin{pmatrix} 2 & 0 & 0 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 \\ 2 & 2 & 2 \\ 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 2 \\ 2 & 2 & 0 \\ 2 & 1 & 1 \end{pmatrix}.$$



Optimum  
Cross-correlation





# Construction of Sequence Family



## Definition 2

Let  $p$  be an odd prime. Then, for any  $m = 1, 2, \dots, p - 1$ , the family  $\mathcal{S}_m$  is defined to be  $\mathcal{S}(\mathbf{g}(\kappa, m, \tau))$  for an integer  $\tau$  and an integer  $\kappa$  that is relatively prime to  $p - 1$ . Define a family  $\mathcal{F}$  of size  $p - 1$  by picking up any one member from each  $\mathcal{S}_m$  for  $m = 1, 2, \dots, p - 1$ . The family  $\mathcal{F}$  can be simply written as

$$\mathcal{F} = \{\mathbf{s}_m | m = 1, 2, \dots, p - 1\}$$

## Theorem 1(Park16)

Let  $p$  be an odd prime. Then, for any  $m = 1, 2, \dots, p - 1$ , the family  $\mathcal{S}_m$  in *Definition 2* contains  $p^p$  sequences of period  $p^2$ . The family  $\mathcal{F}$  of size  $p - 1$  in *Definition 2* is an optimum family in the sense that every sequence has the perfect auto-correlation and any pair has the optimum cross-correlation.



# Construction of Sequence Family



## Theorem 2

Let  $p$  be an odd prime. Then, for any  $m = 1, 2, \dots, p - 1$ , the family  $\mathcal{S}_m$  in *Definition 2* contains only  $p^{p-1}$  cyclically inequivalent members with each other. Total number of ways of constructing "**completely distinct**"  $\mathcal{F}$ 's in *Definition 2* is at least  $\varphi(p - 1)p^{p-1}$  where  $\varphi(\cdot)$  denotes the Euler's phi function

### Proof of Theorem 2)

Ways of choosing  $\kappa$  is  $\varphi(p - 1)$  since  $\kappa$  is relatively prime to  $p - 1$

For given  $\kappa$ , each  $\mathcal{S}_m$  contains  $p^p$  sequences by Theorem 1.

Total numbers of constructing the family  $\mathcal{F}$  is  $\varphi(p - 1)p^{p(p-1)}$

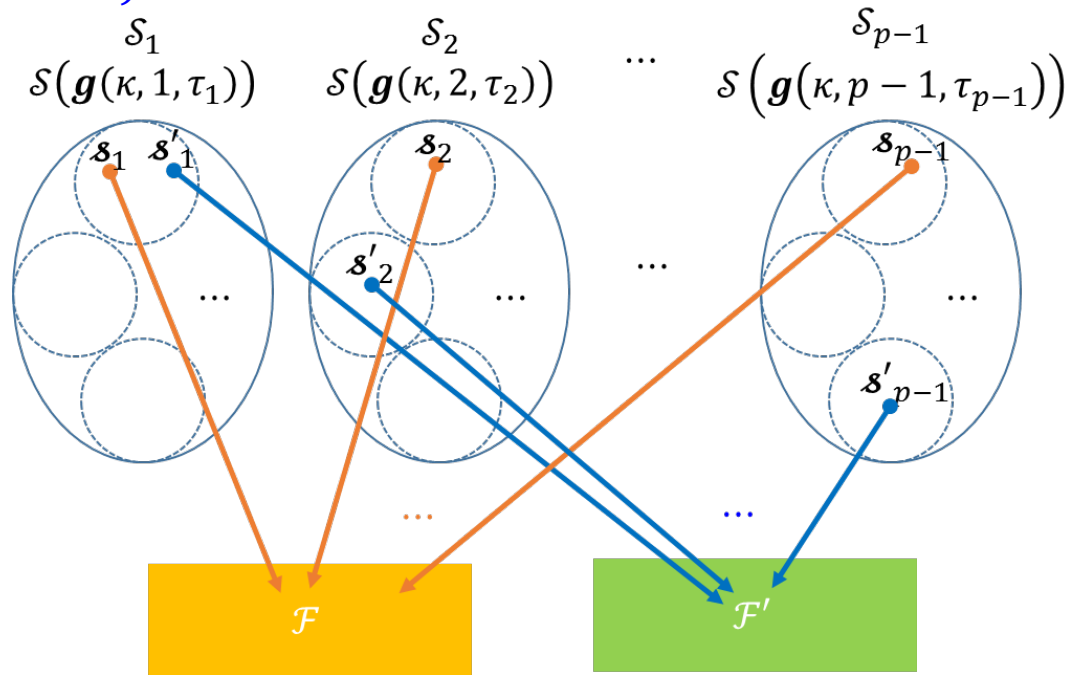
Now, consider two families

$$\mathcal{F} = \{\mathbf{s}_m | m = 1, 2, \dots, p - 1\} \text{ and } \mathcal{F}' = \{\mathbf{s}'_m | m = 1, 2, \dots, p - 1\}$$

are not completely distinct.

It happens when any one pair of  $\mathcal{F}$  and  $\mathcal{F}'$  are cyclically equivalent

Proof of Theorem 2)



Given  $\mathcal{F}$ , the number of constructing  $\mathcal{F}'$ 's is at most  $p \cdot p^{p(p-2)} = p^{(p-1)^2}$

The number of completely distinct families is at least

$$\frac{\varphi(p-1)p^{p(p-1)}}{p^{(p-1)^2}} = \varphi(p-1)p^{p-1}$$

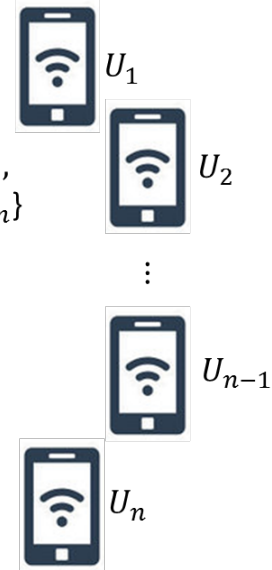
# Proposed LPI Communication System

## Assumptions

- Transmitter  $T$  and  $n$  receivers
- Transmit messages  $m_i$  to each receiver  $U_i$
- Each user  $U_i$  has a private key  $k_i$  shared only with transmitter
- $S_i$  : set of  $p$ -ary sequence of period  $p^2$  ( $p \gg n$  be an odd prime)
- $S_i$  and  $S_j$  ( $i \neq j$ ) have perfect auto- and cross correlation property



$\{m_1 \otimes s_1, m_2 \otimes s_2, \dots, m_{n-1} \otimes s_{n-1}, m_n \otimes s_n\}$



## System Design

- Transmitter  $T$  and all users make an agreement for prime  $p$
- Each user  $U_i$  selects a sequence  $s_i \in S_i$  according to key  $k_i$  and the selection method must be shared only with transmitter
- Transmitter has  $\mathcal{F} = \{s_1, s_2, \dots, s_n\}$  and each user  $U_i$  has  $s_i$  and none of other  $s_j$ 's
- Transmitter sends signals  $\{m_1 \otimes s_1, m_2 \otimes s_2, \dots, m_n \otimes s_n\}$



# Proposed LPI Communication System



## Remark 1

For proposed LPI communication system, an attacker must guess  $s$  from  $\varphi(p-1)p^{p-1}$  candidates to transmit information successfully to valid user  $U_i$  even if he have knowledge of prime  $p$ . If someone select  $p = 31$ , one has  $\varphi(30) \cdot 31^{30} \approx 2^{152}$  candidates of "completely distinct" families of sequences with period  $31^2 = 961$  and size 30. The number of candidates is far larger than the key space of AES-128, that is  $2^{128}$ . This means that the brute-force attack of guessing  $s$  is almost impossible in this case, since it is harder than the brute-force attack against AES-128.



# Summary



- In this talk, we propose a communication system with multiple users requiring LPI properties using the optimal families of polyphase sequences
- We discuss and prove the bound on the key space for candidates, and conclude that our system is more secure than those employing encrypted sequences using AES-128 against brute-force attack.



# Question?