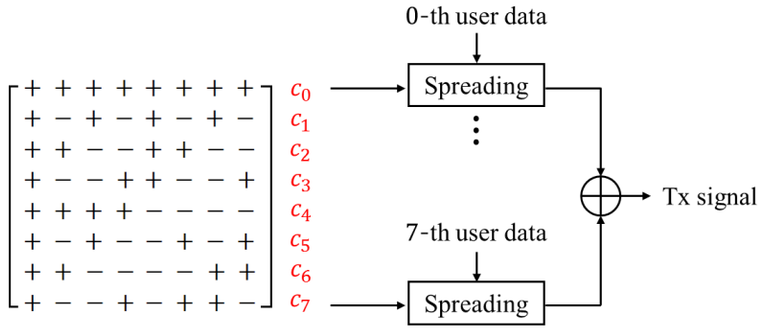
그룹 단위 보안성을 제공하는 동기 DS-CDMA 시스템에 관한 연구

송민규, 김강산, 송홍엽
연세대학교
2018년도 한국통신학회 동계종합학술발표회

1. 연구 배경

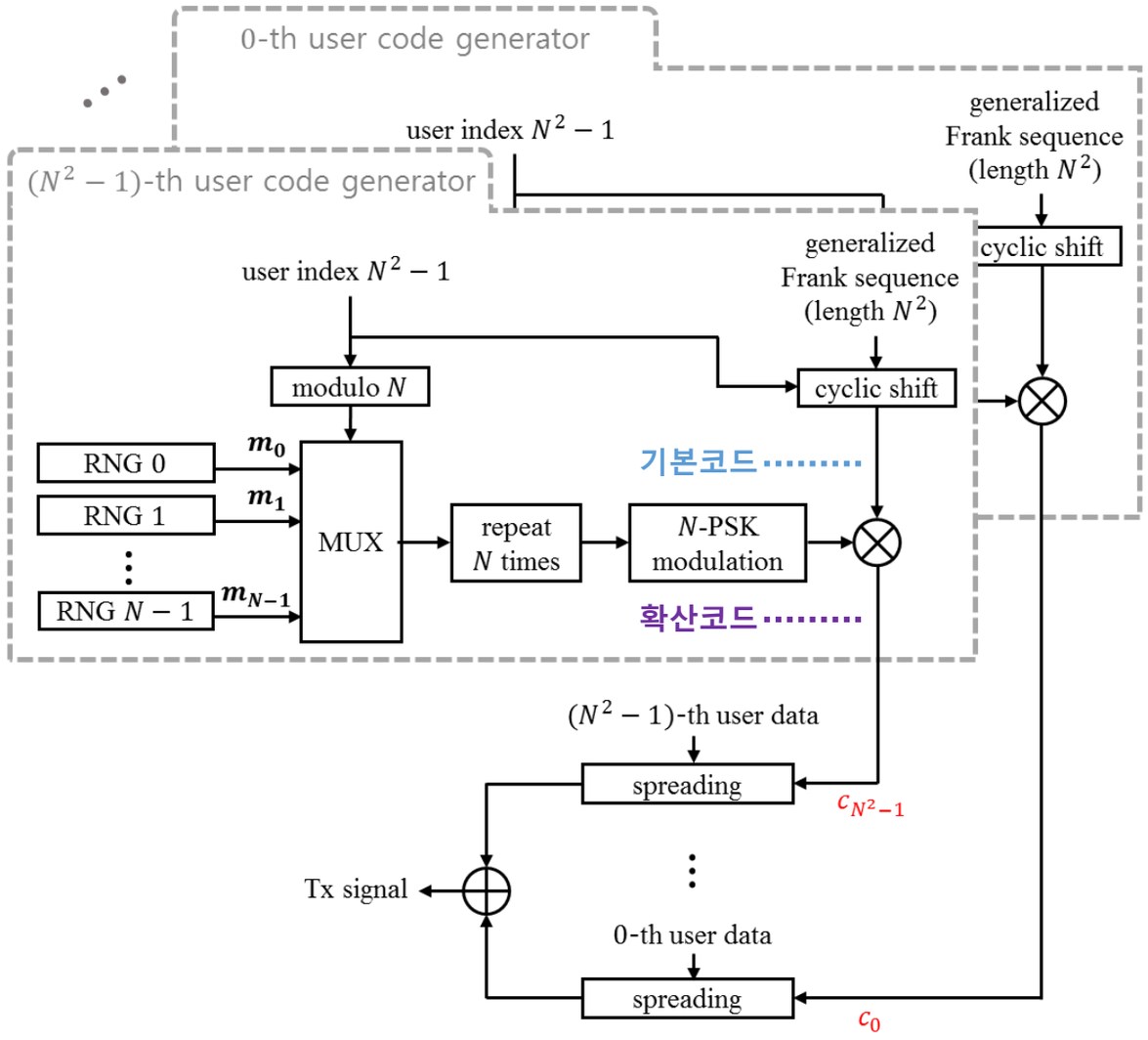
- DS-CDMA는 확산코드(spreading code)를 이용하여 하나의 채널을 다수의 채널로 분할하는 기법으로 신호의 동기화 유무에 따라 동기식과 비동기식으로 구분됨
- 이 기법은 확산코드를 모르면 신호수신이 불가능하다는 특징으로 인해 보안성이 내재된 기법으로 알려짐
- 허나, Berlekamp-Massey 알고리즘을 통해 확산코드를 복원할 수 있다는 사실이 알려진 후, DS-CDMA가 내재하는 보안성을 향상시키기 위한 연구가 진행됨
- 비동기식의 경우, 확산코드를 비주기적이고 무작위한 형태로 변화시키는 발전함 (e.g. [3])
- 동기식의 경우, 위의 방법이 일반적으로 확산코드 간의 직교성을 보장하지 못하기에, scrambling을 통해 향상된 보안성을 얻음 (e.g. [4])
- 본 연구에서는, 직교성을 보장하면서도 특정 확산코드 그룹별로 무작위성을 부여할 수 있는 직교확산코드 생성 방법을 제시함.



일반적인 동기 DS-CDMA의 구조
(길이 8인 Walsh-Hadamard code 사용)

3. 그룹 보안성이 향상된 동기 DS-CDMA

- 정리 1로 부터 아래와 같은 동기 DS-CDMA 시스템을 제안함



- 각 가입자 번호의 modulo N이 같은 가입자들이 그룹을 이루며, 그룹 단위로 동일 난수 발생기(RNG)를 사용해 확산코드에 무작위성을 부여함
- 생성된 모든 확산코드는 서로 직교함

2. 일반화된 프랭크 수열의 특성

- **정의. (일반화된 프랭크 수열[2])**
  임의의 자연수 N에 대해서, 함수 $g(x)$와 $m(x)$를 각각 N진 정수환 상의 치환(permutation) 함수와 임의의 함수라 하자. 길이 N^2인 N진 일반화된 프랭크 수열 $\boldsymbol{f} = \{f(n)\}_{n=0}^{N^2-1}$의 n번째 원소는,

$$n = qN + r, \qquad 0 \le r < N$$

  과 같이 표현할 때,

$$f(n) = f(qN + r) = \omega_N^{qg(r)+m(r)}$$

  로 정의한다. 여기서, $\omega_N = e^{-j2\pi/N}$이다.

- **사실. ([2, Theorem 3])**
  모든 $\tau \not\equiv 0 \pmod{N^2}$에서, 일반화된 프랭크 수열 $\boldsymbol{f}\{f(n)\}_{n=0}^{N^2-1}$는,

$$\sum_{n=0}^{N^2-1} f(n) f^*(n+\tau) = 0$$

  를 만족한다.

- **정리 1.**
  함수 $g(x)$를 N진 정수환에서의 임의의 치환 함수라 하자. 두 일반화된 프랭크 수열

$$f_1 = \{f_1(n)\}_{n=0}^{N^2-1} = \left\{f_1(qN + r) = \omega_N^{qg(r)+m_1(r)}\right\}_{n=0}^{N^2-1}$$

$$f_2 = \{f_2(n)\}_{n=0}^{N^2-1} = \left\{f_2(qN + r) = \omega_N^{qg(r)+m_2(r)}\right\}_{n=0}^{N^2-1}$$

  이 각각 동일한 $g(x)$와 임의의 $m_1(x)$, $m_2(x)$로부터 생성되었을 때, $\tau \not\equiv 0 \pmod{N}$에 대해서

$$\sum_{n=0}^{N^2-1} f_1(n) f_2^*(n+\tau) = 0$$

  이다.

- 확산코드 생성 예 ($N = 3$)

RNG0 출력: $\{2, 1, 0\}$ RNG1 출력: $\{0, 1, 0\}$ RNG2 출력: $\{0, 0, 2\}$

	기본코드		확산코드	
그룹0	가입자 0	$\{\omega_3^0, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^1, \omega_3^2, \omega_3^0, \omega_3^2, \omega_3^1\}$	가입자 0	$\{\omega_3^2, \omega_3^1, \omega_3^0, \omega_3^2, \omega_3^2, \omega_3^2, \omega_3^2, \omega_3^0, \omega_3^1\}$
	가입자 3	$\{\omega_3^0, \omega_3^2, \omega_3^1, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^1, \omega_3^2\}$	가입자 3	$\{\omega_3^2, \omega_3^0, \omega_3^1, \omega_3^2, \omega_3^1, \omega_3^0, \omega_3^2, \omega_3^2, \omega_3^2\}$
	가입자 6	$\{\omega_3^0, \omega_3^1, \omega_3^2, \omega_3^0, \omega_3^2, \omega_3^1, \omega_3^0, \omega_3^0, \omega_3^0\}$	가입자 6	$\{\omega_3^2, \omega_3^2, \omega_3^2, \omega_3^2, \omega_3^0, \omega_3^1, \omega_3^2, \omega_3^1, \omega_3^0\}$
그룹1	가입자 1	$\{\omega_3^1, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^1, \omega_3^2, \omega_3^0, \omega_3^2\}$	가입자 1	$\{\omega_3^1, \omega_3^1, \omega_3^0, \omega_3^0, \omega_3^1, \omega_3^1, \omega_3^2, \omega_3^1, \omega_3^2\}$
	가입자 4	$\{\omega_3^2, \omega_3^0, \omega_3^2, \omega_3^1, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^1\}$	가입자 4	$\{\omega_3^2, \omega_3^1, \omega_3^2, \omega_3^1, \omega_3^1, \omega_3^0, \omega_3^0, \omega_3^1, \omega_3^1\}$
	가입자 7	$\{\omega_3^0, \omega_3^0, \omega_3^1, \omega_3^2, \omega_3^0, \omega_3^2, \omega_3^1, \omega_3^0, \omega_3^0\}$	가입자 7	$\{\omega_3^0, \omega_3^1, \omega_3^1, \omega_3^2, \omega_3^1, \omega_3^2, \omega_3^1, \omega_3^1, \omega_3^0\}$
그룹2	가입자 2	$\{\omega_3^2, \omega_3^1, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^1, \omega_3^2, \omega_3^0\}$	가입자 2	$\{\omega_3^2, \omega_3^1, \omega_3^2, \omega_3^0, \omega_3^0, \omega_3^2, \omega_3^1, \omega_3^2, \omega_3^2\}$
	가입자 5	$\{\omega_3^1, \omega_3^2, \omega_3^0, \omega_3^2, \omega_3^1, \omega_3^0, \omega_3^0, \omega_3^0, \omega_3^0\}$	가입자 5	$\{\omega_3^1, \omega_3^2, \omega_3^2, \omega_3^2, \omega_3^1, \omega_3^2, \omega_3^0, \omega_3^0, \omega_3^2\}$
	가입자 8	$\{\omega_3^0, \omega_3^0, \omega_3^0, \omega_3^1, \omega_3^2, \omega_3^0, \omega_3^2, \omega_3^1, \omega_3^0\}$	가입자 8	$\{\omega_3^0, \omega_3^0, \omega_3^2, \omega_3^1, \omega_3^2, \omega_3^2, \omega_3^2, \omega_3^1, \omega_3^2\}$

4. 결과 고찰

- 난수 발생기의 영향으로 확산코드의 변화를 예측하는 것이 어려움
- 다른 그룹에 있는 참여자의 확산코드를 알 수 없음.
- 확산코드가 시간에 따라 변화함으로, DS-CDMA 신호의 acquisition 단계에서 확산코드 위상을 효율적으로 찾기 위한 방법에 대한 연구가 필요함.

참고문헌

[1] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, 2005.

[2] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized Bent Functions and Their Properties," *Journal of combinatorial theory, Series A*, vol. 40, pp. 90-107, 1985.

[3] L. Nguyen, "Self-encoded spread spectrum communications," *Proc. of MILCOM 1999*, pp. 182-186, 1999.

[4] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical layer built-in security analysis and enhancement of CDMA systems," *Proc. of MILCOM 2005*, pp. 956-962, 2005.