10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

# 저피탐 항법신호 설계를 위한 암호화된 확산부호의 상관 특성 분석

## 제 4회 감시-정찰-정보 학술 대회

박기현, 송홍엽, 이장용

Channel Coding and Crypto Lab
**Yonsei University, Seoul, Korea**

August 28, 2014

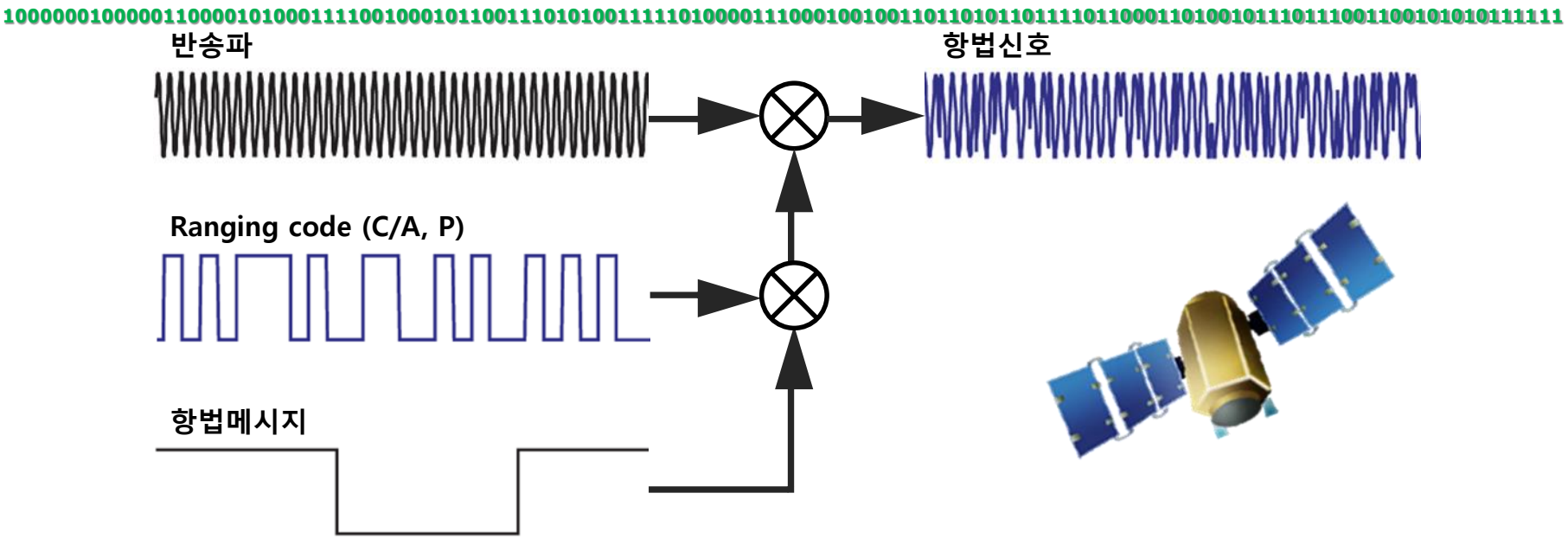
10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

# 발표 순서

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- 위성항법신호에서의 확산부호
- 공격 모델 및 암호화의 특성: 저피탐의 의미
- 이론적 상관특성 분석
- 시뮬레이션 및 결론

# 위성항법신호에서의 확산부호



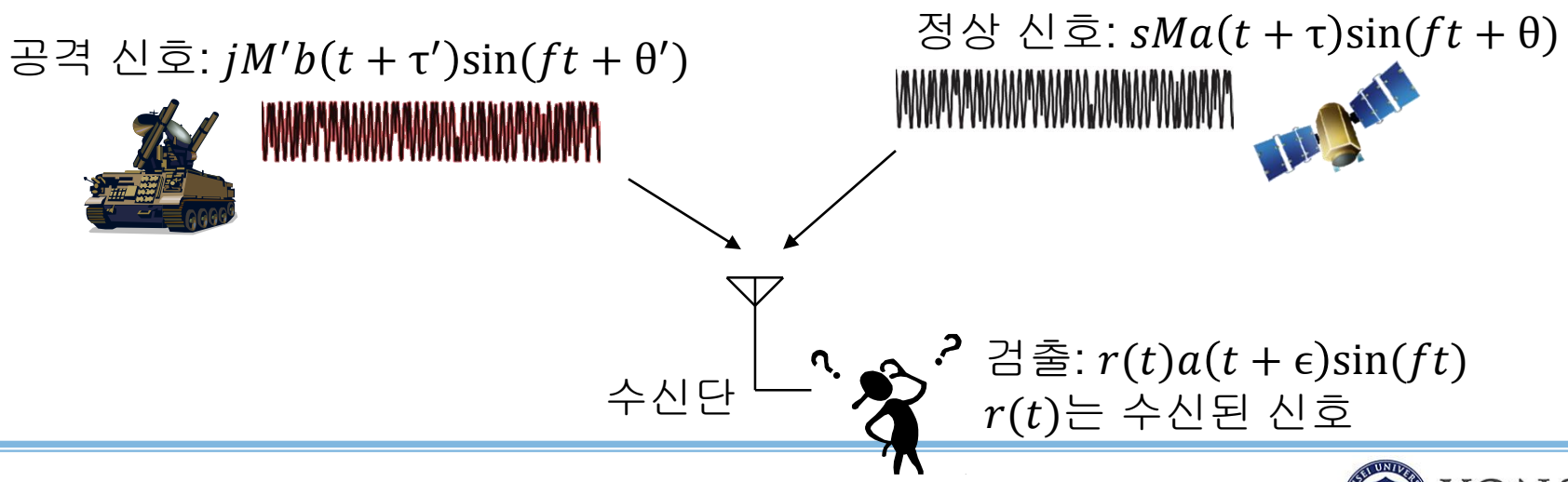

- 메시지보다 훨씬 큰 비트레이트를 가지며, 송수신단 모두 알고 있음
- 측위 정확도를 위하여 자기상관특성이, 상호간섭 억제를 위하여 상호상관특성이 중요함
- GPS C/A 부호는 자기상관/상호상관특성이 좋은 Gold Code를 사용

# 공격 모델

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- **공격자는 반송파 주파수 $f$를 알고 있음**

- **공격자는 수신자의 신호수신을 억제/방해하려고 함**
  - 정상 메시지 $M$ 을 수신하지 못하게/대신 $M'$을 수신시키려 함
  - 공격자는 $a(t)$로 정의된 확산부호를 사용하는 시스템을 공격하기 위해 $b(t)$를 확산부호로 사용
  - 정상 신호 파워 레벨 $s$에 대하여, 재밍 파워 레벨 $j$로 송출



# 저피탐

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- **저피탐의 의미: 공격자의 신호 탐지(Detection) 및 손상(Jamming) 공격에 대한 신호의 내성에 대한 지표**
  - Low Probability of Interception, LPI
  - 저피탐 신호: 공격내성이 높은 신호
  - 동일 수준의 공격을 수행하기 위한 공격자의 비용으로 정량화됨

- **공격 모델에서의 분석**
  - 수신단이 $M$ 을 수신하지 못하게 하는 최소 파워 $j$가 공격자의 재밍 비용이 됨
  - 두 신호 모두 $a(t)$의 MF를 통과하므로, 수신단에서 느끼는 재밍 파워는 $j|R_{a,b}|$가 됨
  - 즉, 공격자가 사용하는 $b(t)$ 가 $a(t)$와 비슷할수록 (상호상관 값이 높을수록) 비용을 낮출 수 있음

# 암호화의 효과

- 저피탐 신호는 공격자가 $a(t)$, 혹은 그와 유사한 확산부호를 쉽게 추정할 수 없게 하여야 함

- 후보군의 범위가 전수 조사가 가능할 만큼 좁은 Gold Code 등은 부적합
  - 공격자는 자신이 수신한 신호를 가정한 코드에 대입시켜 수신레벨을 확인함으로써 신호검출 가능

- 암호화는 확산부호를 랜덤수열로 변환시켜 후보군의 범위를 키 스페이스까지 확장시킴

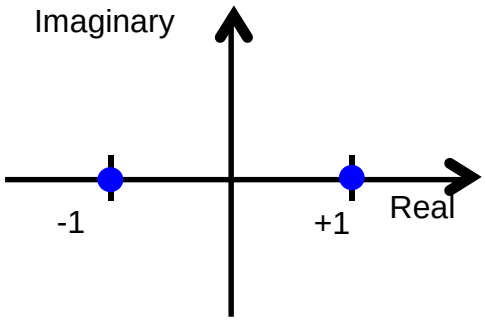
  ➔ 전수 조사를 통한 후보군 대입이 불가능

- Gold Code등이 가지고 있던 상관 특성의 유지가 불가능
  → 얼마나 안 좋아질 것인가?

# 이론적 특성 분석: BPSK Real Signal

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- BPSK에서 확산부호는 [+1, -1]의 신호값으로 모델링됨




- 암호화된 확산부호는 각각의 값을 균등한 확률분포 (50%)로 가짐

- 암호화된 서로 다른 두 $a[n]$, $b[n]$ 확산부호의 임의의 위치에서의 곱 $a[n]b^*[n+\tau]$ 또한 [+1, -1] 각각의 값을 균등한 확률분포 (50%)로 가짐

# 이론적 특성 분석: BPSK Real Signal

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- 길이 $N$ 인 두 확산부호 $a[n], b[n]$ 의 상호상관값 $R_{a,b}(\tau)$는 다음과 같이 정의됨

$$R_{a,b}(\tau) = \sum_{i=0}^{N-1} a[i]b^*[i+\tau]$$

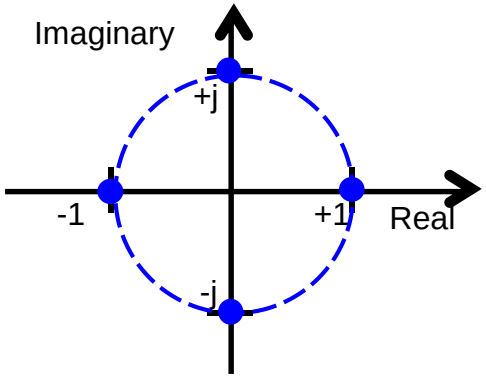
- 상호상관값의 절대값이 $h$일 확률 $p_{BPSK}(|R_{a,b}(\tau)| = h)$는 $N$개 위치에서 +1의 개수가 $\frac{N-h}{2}$ 혹은 $\frac{N+h}{2}$일 때이므로, 다음과 같음

$$p_{BPSK}(|R_{a,b}(\tau)| = h) \triangleq P(N,h) = \begin{cases} \binom{N}{\frac{N+h}{2}} 0.5^N + \binom{N}{\frac{N-h}{2}} 0.5^N & N \geq h > 0,\ N-h \text{ even} \\ \binom{N}{\frac{N}{2}} 0.5^N & N \text{ even},\ h = 0 \\ 0 & \text{otherwise} \end{cases}$$

# 이론적 특성 분석: QPSK Complex Signal

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- QPSK에서 확산부호는 [+1, -1, +j, -j]의 신호값으로 모델링됨




- 암호화된 확산부호는 각각의 값을 균등한 확률분포 (25%)로 가짐

- 암호화된 서로 다른 두 $a[n]$, $b[n]$ 확산부호의 임의의 위치에서의 곱 $a[n]b^*[n+\tau]$ 또한 [+1, -1, +j, -j] 각각의 값을 균등한 확률분포 (25%)로 가짐

# 이론적 특성 분석: QPSK Complex Signal



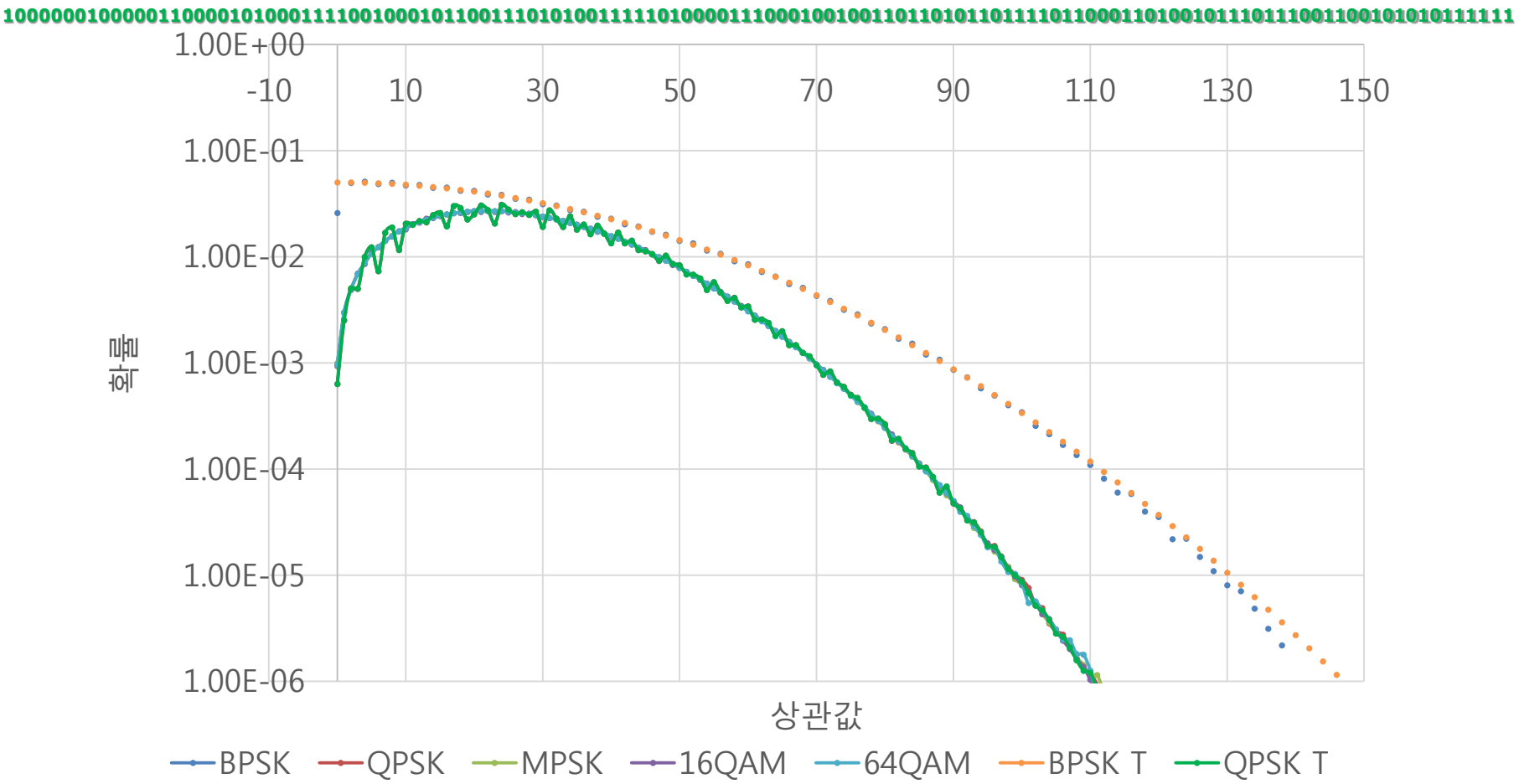
- $R_{a,b}(\tau) = a + jb$ 라고 했을 때 상호상관값의 절대값이 $h$일 확률 $p_{QPSK}(|R_{a,b}(\tau)| = h)$는 모든 가능한 $a$에서 리얼값이 $a$일 확률과 $b = \sqrt{h^2 - a^2}$ 가 될 확률의 곱의 합으로 표현됨

- $a[n]b^*[n+\tau]$ 표현됨가 real일 확률은 50%이므로, 전체 $N$개 위치에서 real값이 나오는 위치가 $Z$개일 확률은 $\binom{N}{Z} 0.5^N$ 이 됨

- 즉, $p_{QPSK}(|R_{a,b}(\tau)| = h)$는 모든 가능한 $Z$에서 $Z$ 일 확률과 $Z$ 일때 모든 가능한 $a$에서 리얼값이 $a$일 확률과 $b = \sqrt{h^2 - a^2}$ 가 될 확률의 곱의 합의 곱의 합이 됨, 즉

$$p_{QPSK}(|R_{a,b}(\tau)| = h) = \sum_{Z=0}^{N} \binom{N}{Z} 0.5^N \sum_{a=0}^{Z} P(Z,a) P\left(N - Z, \sqrt{h^2 - a^2}\right)$$

# 플로팅 및 시뮬레이션




- 길이 1000에서 함수 플로팅 및 시뮬레이션 조사
- 같은 복소신호는 <u>모듈레이션이 바뀌어도 상관값 통계는 동일</u>

# 암호화에 따른 성능열화 분석

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

| 길이 | Gold | BPSK Random |
|---|---|---|
| 127 | 17 | 31 |
| 511 | 33 | 75 |
| 1023 | 65 | 109 |
| 16383 | 257 | 529 |

| 길이 | Zadoff-Chu | MPSK Random |
|---|---|---|
| 31 | 5.6 | 10.7 |
| 127 | 11.3 | 25.2 |
| 1021 | 32 | 84.3 |
| 16381 | 128 | 395 |

- **각 길이에 따른 주기내 최대 상호 상관값**
  - 랜덤의 경우 1만 회 반복 시뮬레이션으로 구한 평균
- **BPSK의 경우, 암호화된 코드 사용시 Gold Code에 비해 대략 2배 정도의 상관성능 열화를 보임**
- **MPSK의 경우, Zadoff-Chu 코드에 비해 대략 3배 정도의 상관성능 열화를 보임**
- **MPSK 를 사용한 경우에 비해 BPSK가 대략 1.5배 정도 상관성능이 나쁨**

# 결 론

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **암호화된 확산부호의 장점: 공격자의 확산부호 추정이 어렵기 때문에 신호에 대한 탐지 및 재밍 공격이 어려워짐**
- **암호화된 확산부호의 단점: 상관특성이 최적화된 확산부호를 사용하는 기존 시스템에 비해 열화된 측위성능을 보임**

- **본 논문의 결과**
  - 암호화된 확산부호의 실제 측위 성능 열화 정도를 상관도 분석을 통해 이론적/실험적으로 확인
  - 기존의 BPSK가 아닌 복소 신호를 사용하여 암호화된 수열의 상관특성을 개선 가능함을 보이고, 이 때의 기대 성능을 도식
  - 통신의 모듈레이션을 바꾸어도 암호화된 확산부호를 거의 측위성능의 차이 없이 사용할 수 있음을 확인

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

# 감사합니다

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111