UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Inherent Vulnerabilities in Hybrid CDMA & Cryptographic Spread Spectrum for Space Systems

Edd Salkield, Sebastian Köhler, Simon Birnbach, Ivan Martinovic

Systems Security Lab

Security for Space Systems 2025

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter

Receiver

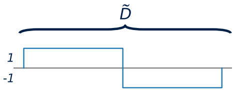
UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter

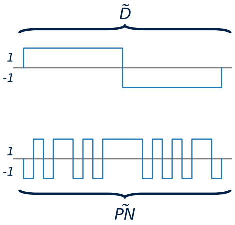


Receiver

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter

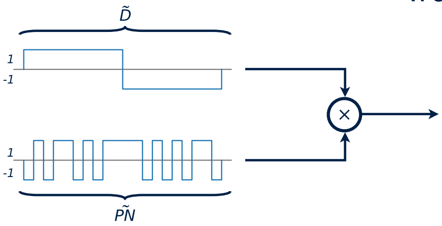


Receiver

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter

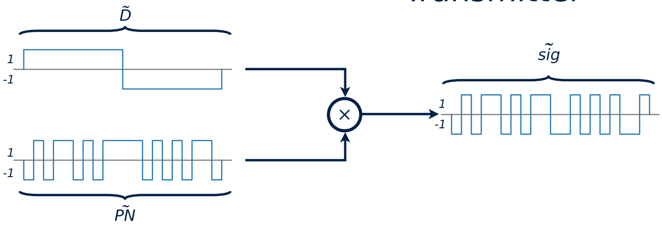


Receiver

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter

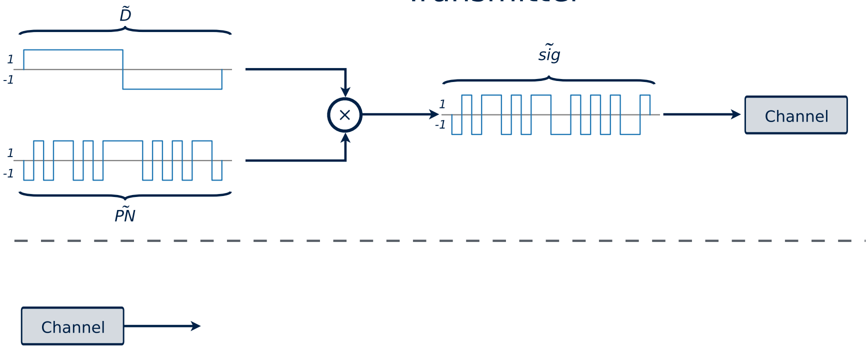


Receiver

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter



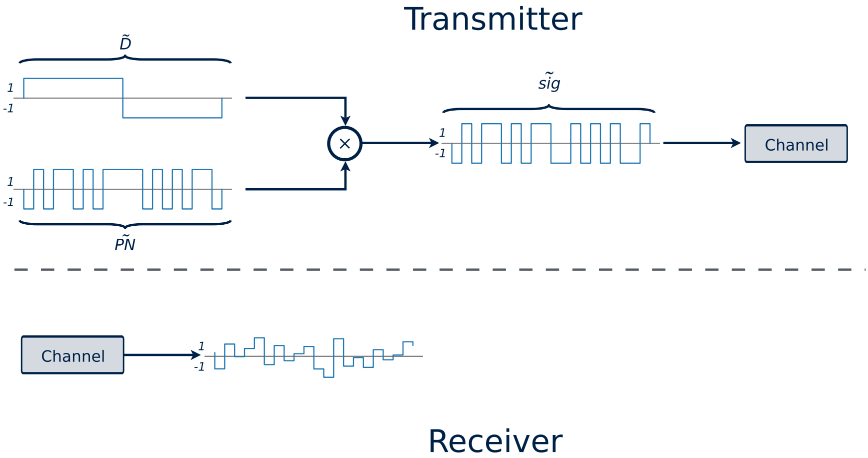
Receiver

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

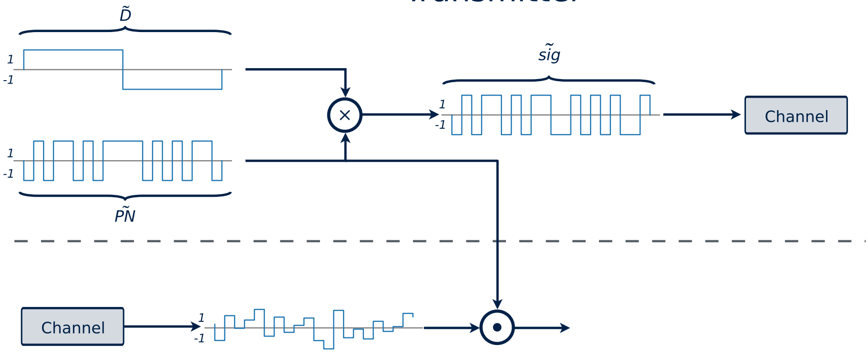


Crypto Spread Spectrum
Direct Sequence
Security
Multiple Access
Hybrid System
Overview
PN Reuse
Attack
Eavesdropping
Spoofing
Jamming
Evaluation
Threat Model
Results
Next Steps
Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

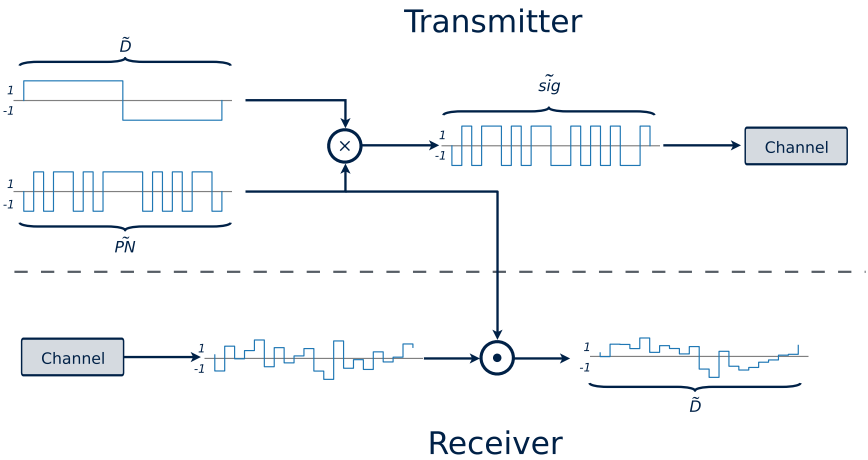
Transmitter



Receiver

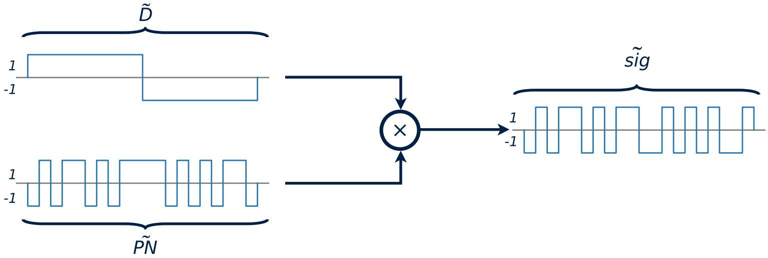
Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading



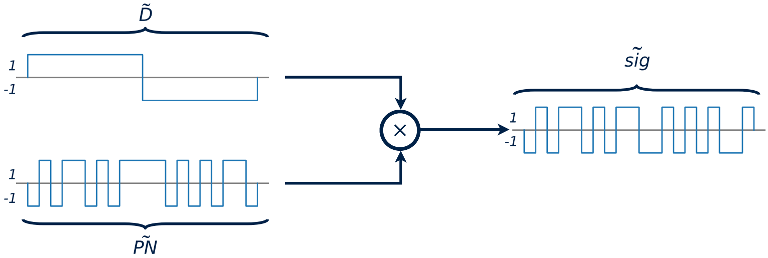
Effect of DSSS

Security Properties: Secrecy/Authenticity



Effect of DSSS

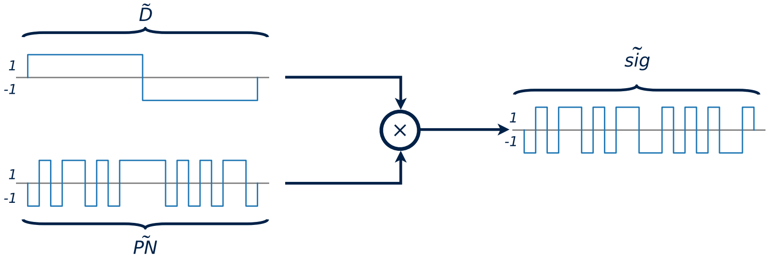
Security Properties: Secrecy/Authenticity



Cryptographic $\tilde{PN}$ is equivalent to PHY-layer XOR

Effect of DSSS

Security Properties: Secrecy/Authenticity

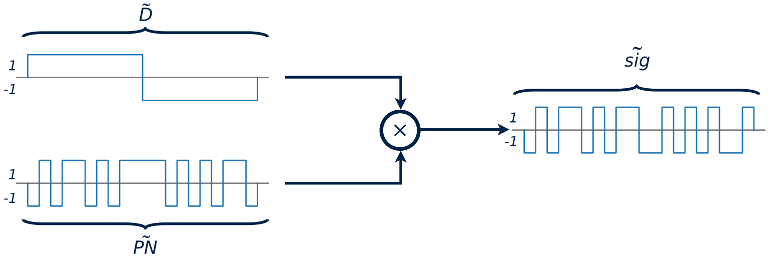


Cryptographic $\tilde{PN}$ is equivalent to PHY-layer XOR

- **Secrecy** – data is encrypted at PHY-layer

Effect of DSSS

Security Properties: Secrecy/Authenticity

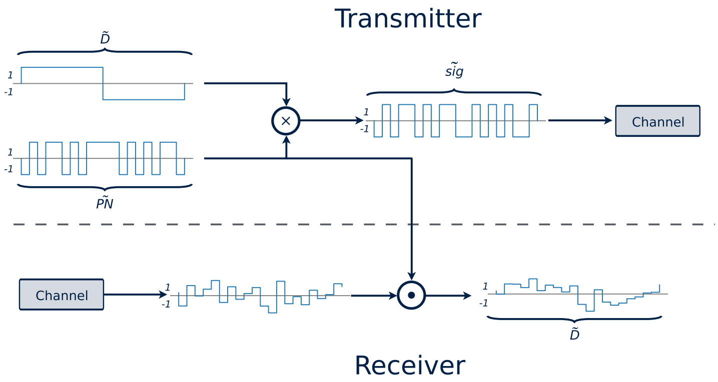


Cryptographic $\tilde{PN}$ is equivalent to PHY-layer XOR

- **Secrecy** – data is encrypted at PHY-layer
- (Authenticity) – as much as provided by XOR with random sequence

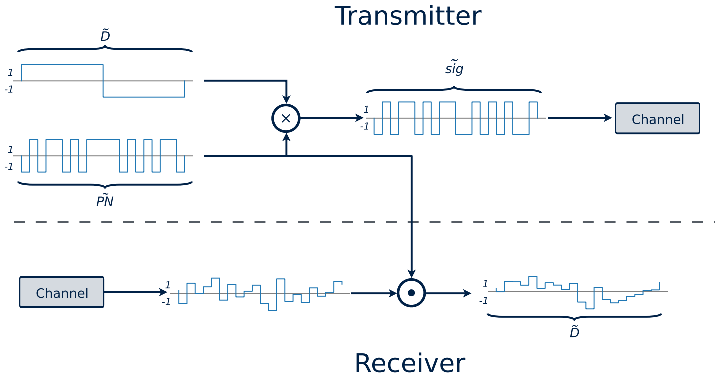
Effect of DSSS

Security Properties: Availability



Effect of DSSS

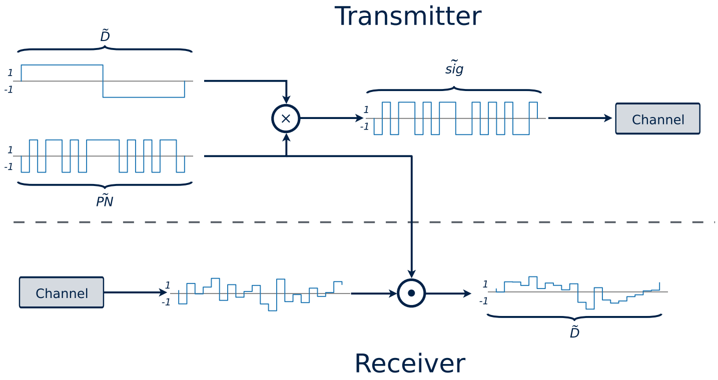
Security Properties: Availability



- Increasing chips per bit improves bit detection

Effect of DSSS

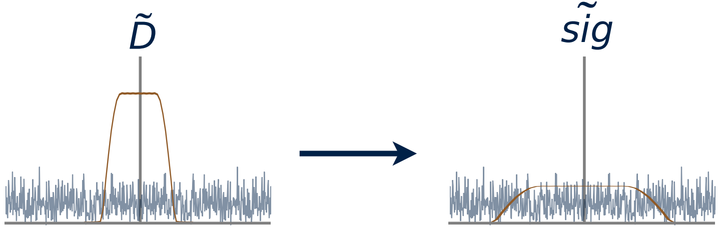
Security Properties: Availability



- Increasing chips per bit improves bit detection
- **Availability** – chips per bit can be scaled to provide required jammer tolerance

Effect of DSSS

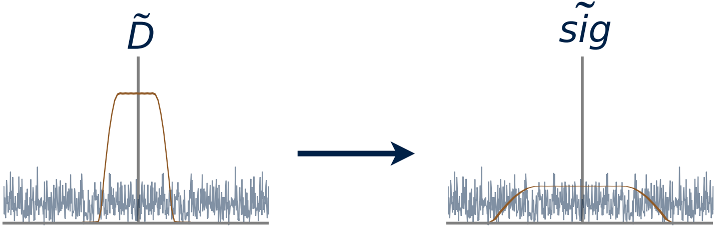
Security Properties: Unobservability



- Increasing the chip rate increases the bandwidth

Effect of DSSS

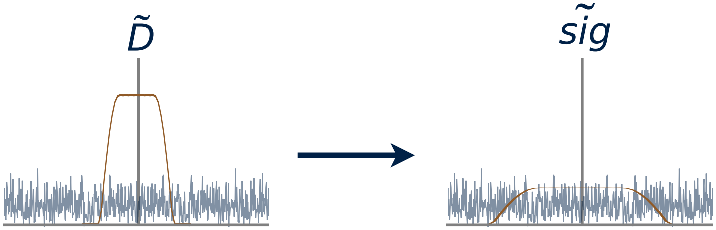
Security Properties: Unobservability



- Increasing the chip rate increases the bandwidth
- Select *chips per bit* to detect signal beneath noise floor

Effect of DSSS

Security Properties: Unobservability



- Increasing the chip rate increases the bandwidth
- Select *chips per bit* to detect signal beneath noise floor
- **Unobservability** – adversaries without knowledge of $\tilde{PN}$ cannot detect presence of signal

Effect of DSSS

Security Properties

- **Secrecy** – data is encrypted at PHY-layer
    - **Unobservability** – adversaries without knowledge of $\tilde{PN}$ cannot detect presence of signal
- **Availability** – chips per bit can be scaled to provide required jammer tolerance
- Authenticity – as much as provided by XOR with random sequence

Effect of DSSS

Security Properties

- **Secrecy** – data is encrypted at PHY-layer
  - **Unobservability** – adversaries without knowledge of $\tilde{PN}$ cannot detect presence of signal
- **Availability** – chips per bit can be scaled to provide required jammer tolerance
- Authenticity – as much as provided by XOR with random sequence

Each depends on *secrecy of spreading sequence* $\tilde{PN}$

Effect of DSSS

Security Properties

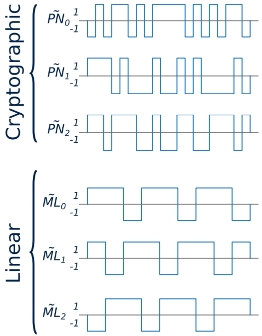
- **Secrecy** – data is encrypted at PHY-layer
  - **Unobservability** – adversaries without knowledge of $\tilde{PN}$ cannot detect presence of signal
- **Availability** – chips per bit can be scaled to provide required jammer tolerance
- Authenticity – as much as provided by XOR with random sequence

Each depends on *secrecy of spreading sequence* $\tilde{PN}$

Therefore $\tilde{PN}$ should be a **cryptographic random sequence**

Effect of DSSS

Multiple Access Properties

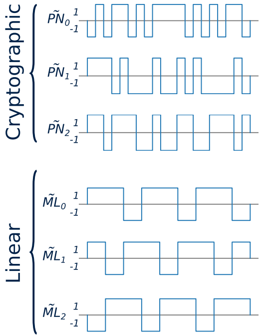


Cryptographic sequences have up to 30 dB higher interfering power[1]

[1] "Fittipaldi et al. (2011, renewed 2021) *Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders*"

Effect of DSSS

Multiple Access Properties



Cryptographic sequences have up to 30 dB higher interfering power[1]

Q: Can security and multiple access be supported simultaneously?

[1] "Fittipaldi et al. (2011, renewed 2021) *Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders*"

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

ThalesAlenia Space

Reference : RPT-RFP-ESA-00013-AASI
Date : 13/07/2021
Issue : 3 **Page :** 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Final Report

Written by	Responsibility
G. Fittipaldi	
Verified by	
L.Simone	
Approved by	
R. Giangreco	Program Manager

[a] Garello et al. (2025) "*AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing*"

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

ThalesAlenia Space

Reference : RPT-RFP-ESA-00013-AASI
Date : 13/07/2021
Issue : 3 Page : 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Final Report

Written by	Responsibility
G. Fittipaldi	
Verified by	
L.Simone	
Approved by	
R. Giangreco	Program Manager

- Developed in 2011, renewed in 2021

[a] Garello et al. (2025) "*AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing*"

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

ThalesAlenia Space

Reference : RPT-RFP-ESA-00013-AASI
Date : 13/07/2021
Issue : 3 Page : 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Final Report

Written by	Responsibility
G. Fittipaldi	
Verified by	
L.Simone	
Approved by	
R. Giangreco	Program Manager

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards

[a] Garello et al. (2025) "*AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing*"

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

ThalesAlenia Space

Reference : RPT-RFP-ESA-00013-AASI
Date : 13/07/2021
Issue : 3 Page : 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Final Report

Written by	Responsibility
G. Fittipaldi	
Verified by	
L.Simone	
Approved by	
R. Giangreco	Program Manager

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards
- Designed for multiple satellite uplink relays e.g. TDRS

[a] Garello et al. (2025) "*AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing*"

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

ThalesAlenia Space

Reference : RPT-RFP-ESA-00013-AASI
Date : 13/07/2021
Issue : 3 **Page :** 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Final Report

Written by	Responsibility
G. Fittipaldi	
Verified by	
L.Simone	
Approved by	
R. Giangreco	Program Manager

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards
- Designed for multiple satellite uplink relays e.g. TDRS
- No security analysis conducted so far

[a] Garello et al. (2025) "*AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing*"

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

ThalesAlenia Space

Reference : RPT-RFP-ESA-00013-AASI
Date : 13/07/2021
Issue : 3 Page : 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Final Report

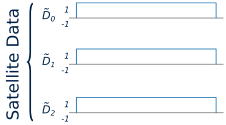
Written by	Responsibility
G. Fittipaldi	
Verified by	
L.Simone	
Approved by	
R. Giangreco	Program Manager

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards
- Designed for multiple satellite uplink relays e.g. TDRS
- No security analysis conducted so far
- Other hybrid systems designed under similar construction[a]

[a] Garello et al. (2025) "*AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing*"

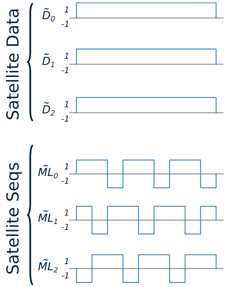
Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



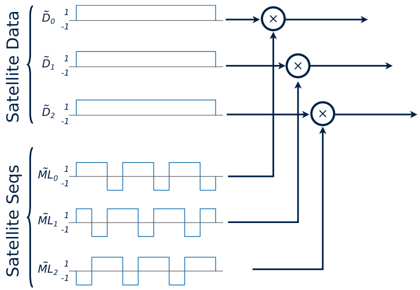
Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

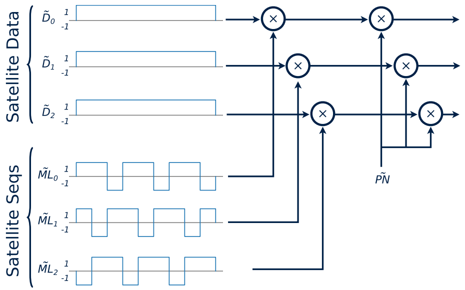


UNIVERSITY OF OXFORD

SSL Systems Security Lab

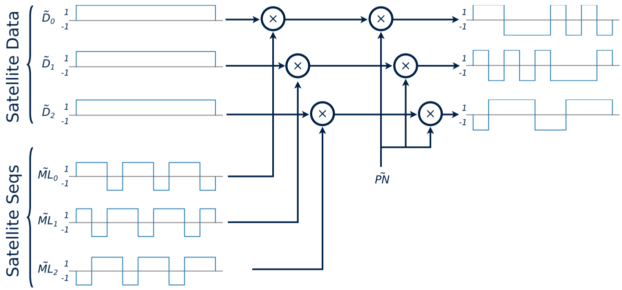
Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

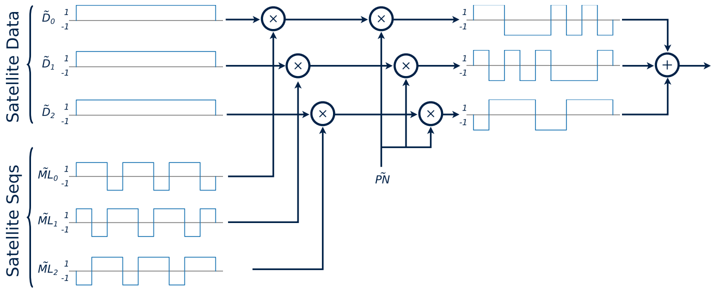


UNIVERSITY OF OXFORD

SSL Systems Security Lab

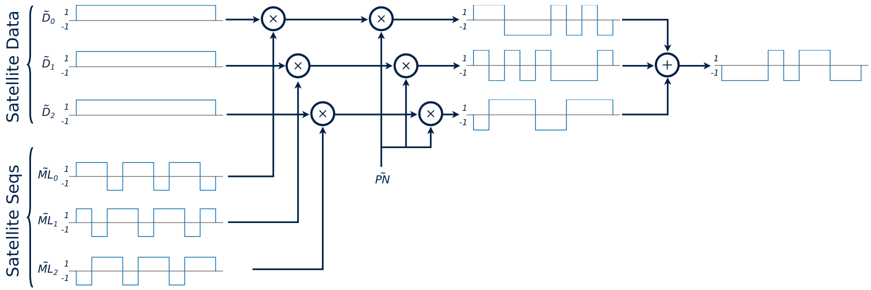
Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



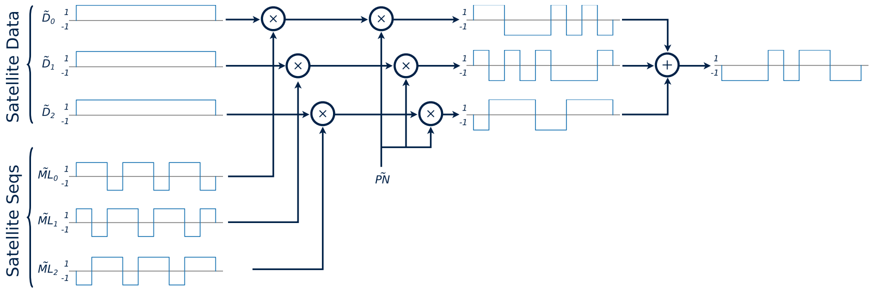
Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



Hybrid Cryptographic/CDMA Spread Spectrum

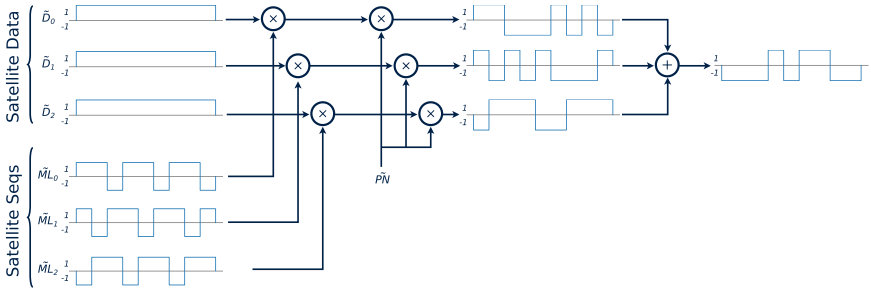
Mechanism Overview



- Spreading sequence cryptographically random since XORed with $\tilde{PN}$

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



- Spreading sequence cryptographically random since XORed with $\tilde{PN}$
- Receivers undo $\tilde{PN}$, reducing to per-satellite linear spreading codes $\tilde{ML}$

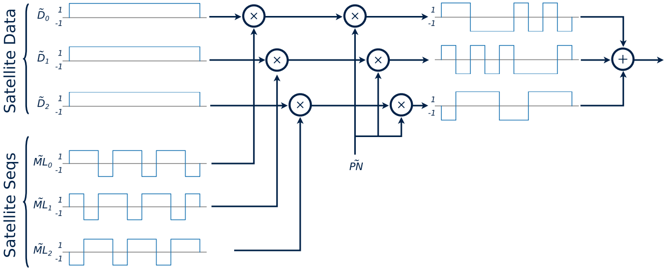
UNIVERSITY OF OXFORD

SSL Systems Security Lab

Key Security Issue

Reuse of Cryptographic Sequence

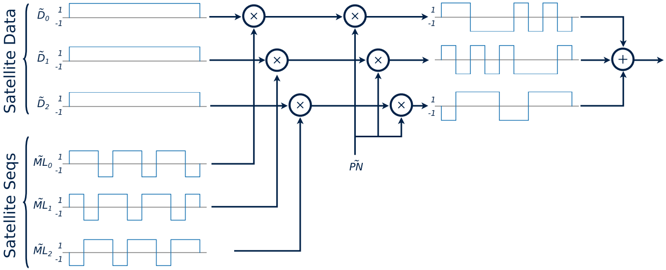
NB: Same cryptographic sequence $\tilde{PN}$ reused across all data sequences



Key Security Issue

Reuse of Cryptographic Sequence

NB: Same cryptographic sequence $\tilde{PN}$ reused across all data sequences

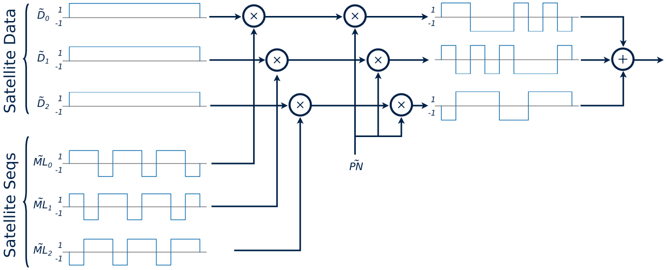


- Intuition: insufficient entropy entering the system to protect the data

Key Security Issue

Reuse of Cryptographic Sequence

NB: Same cryptographic sequence $\tilde{PN}$ reused across all data sequences

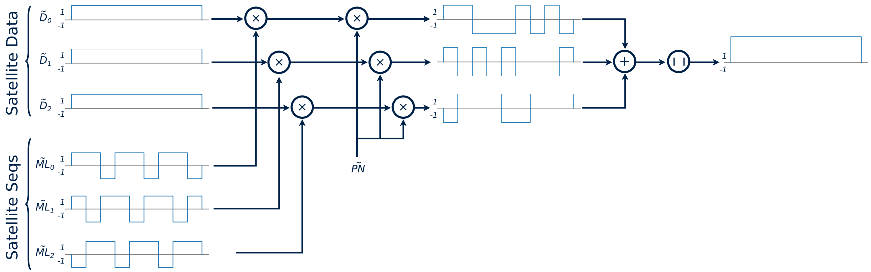


- Intuition: insufficient entropy entering the system to protect the data
- $\tilde{PN}$ has effect of randomising *sign* of aggregate chip, but not *magnitude*

Key Security Issue

Reuse of Cryptographic Sequence

NB: Same cryptographic sequence $\tilde{PN}$ reused across all data sequences

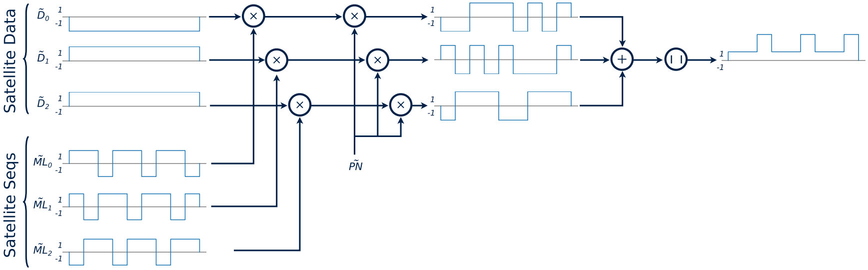


- Intuition: insufficient entropy entering the system to protect the data
- $\tilde{PN}$ has effect of randomising *sign* of aggregate chip, but not *magnitude*

Key Security Issue

Reuse of Cryptographic Sequence

NB: Same cryptographic sequence $\tilde{PN}$ reused across all data sequences

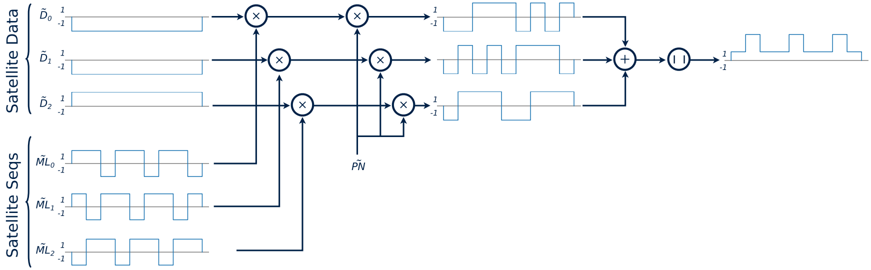


- Intuition: insufficient entropy entering the system to protect the data
- $\tilde{PN}$ has effect of randomising *sign* of aggregate chip, but not *magnitude*

Key Security Issue

Reuse of Cryptographic Sequence

NB: Same cryptographic sequence $\tilde{PN}$ reused across all data sequences

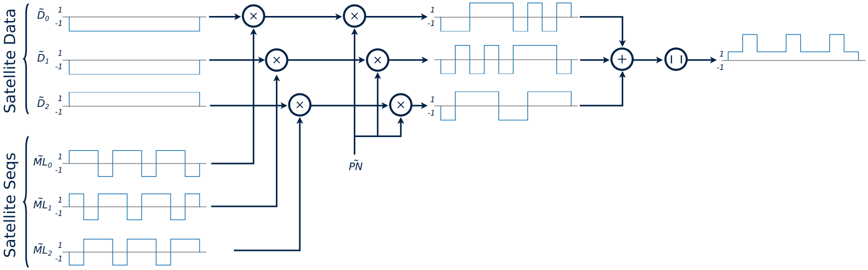


- Intuition: insufficient entropy entering the system to protect the data
- $\tilde{PN}$ has effect of randomising *sign* of aggregate chip, but not *magnitude*

Key Security Issue

Reuse of Cryptographic Sequence

NB: Same cryptographic sequence $\tilde{PN}$ reused across all data sequences



- Intuition: insufficient entropy entering the system to protect the data
- $\tilde{PN}$ has effect of randomising *sign* of aggregate chip, but not *magnitude*
- Aggregate chip magnitudes repeat many times, leaking information about the data

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:

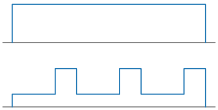
D_0	D_1	D_2
0	*0*	*0*
1	*1*	*1*

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:

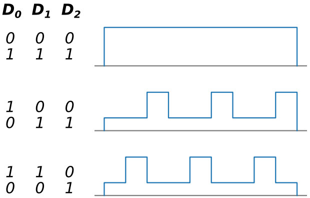
D_0	D_1	D_2
0	0	0
1	1	1
1	0	0
0	1	1



Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:

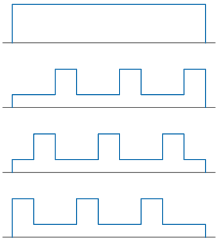


Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:

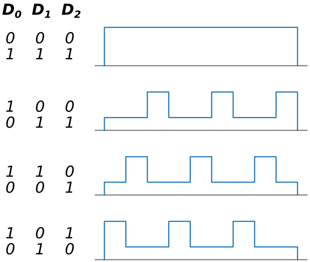
D_0	D_1	D_2
0 1	0 1	0 1
1 0	0 1	0 1
1 0	1 0	0 1
1 0	0 1	1 0



Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:



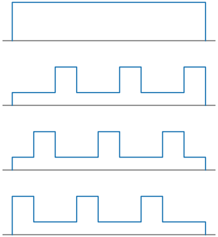
Unobservability broken by correlating for known, repeating aggregate sequences

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:

D_0	D_1	D_2
0 1	0 1	0 1
1 0	0 1	0 1
1 0	1 0	0 1
1 0	0 1	1 0



Unobservability broken by correlating for known, repeating aggregate sequences

Q: In general case, how can the original data sequence be determined given a noisy waveform?

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP($\mathbf{b}, \mathbf{ML}, \mathbf{g}$) $\rightarrow$ ($\mathbf{D}^*, \mathbf{PN}^*$)

Constants

$b_1, \ldots, b_N$	Received aggregate chips
$ML_1, \ldots, ML_n$	Satellite ML sequences
$g_1, \ldots, g_n$	Satellite gains

Variables

$D_1, D_2, \ldots, D_n$	Data chip values
$PN_1, \ldots, PN_N$	Cryptographic pseudo-noise
$e_1^+, e_1^-, \ldots, e_N^+, e_N^-$	Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize $Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$

Key Constraints:

$g_1 ML_1[1] D_1 PN_1 + \ldots + g_n ML_n[1] D_n PN_1 + e_1^+ - e_1^- = b_1$

$\ldots$

$g_1 ML_1[N] D_1 PN_N + \ldots + g_n ML_n[N] D_n PN_N + e_N^+ - e_N^- = b_N$

Bounding Constraints:

$-1 \leq D_1, \ldots, D_n, PN_1, \ldots, PN_N \leq 1$

$e_1^+, e_1^-, e_2^+, e_2^- \geq 0$

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP($\mathbf{b}, \mathbf{ML}, \mathbf{g}$) $\rightarrow (\mathbf{D}^*, \mathbf{PN}^*)$

Constants

$b_1, \ldots, b_N$	Received aggregate chips
$ML_1, \ldots, ML_n$	Satellite ML sequences
$g_1, \ldots, g_n$	Satellite gains

Variables

$D_1, D_2, \ldots, D_n$	Data chip values
$PN_1, \ldots, PN_N$	Cryptographic pseudo-noise
$e_1^+, e_1^-, \ldots, e_N^+, e_N^-$	Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize $Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$

Key Constraints:

$g_1 ML_1[1] D_1 PN_1 + \ldots + g_n ML_n[1] D_n PN_1 + e_1^+ - e_1^- = b_1$

$\ldots$

$g_1 ML_1[N] D_1 PN_N + \ldots + g_n ML_n[N] D_n PN_N + e_N^+ - e_N^- = b_N$

Bounding Constraints:

$-1 \leq D_1, \ldots, D_n, PN_1, \ldots, PN_N \leq 1$

$e_1^+, e_1^-, e_2^+, e_2^- \geq 0$

- Solve optimisation problem by *Maximum Likelihood* decoding

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP$(\mathbf{b}, \mathbf{ML}, \mathbf{g}) \rightarrow (\mathbf{D}^*, \mathbf{PN}^*)$

Constants

$b_1, \ldots, b_N$	Received aggregate chips
$ML_1, \ldots, ML_n$	Satellite ML sequences
$g_1, \ldots, g_n$	Satellite gains

Variables

$D_1, D_2, \ldots, D_n$	Data chip values
$PN_1, \ldots, PN_N$	Cryptographic pseudo-noise
$e_1^+, e_1^-, \ldots, e_N^+, e_N^-$	Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize $Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$

Key Constraints:

$g_1 ML_1[1] D_1 PN_1 + \ldots + g_n ML_n[1] D_n PN_1 + e_1^+ - e_1^- = b_1$

$\ldots$

$g_1 ML_1[N] D_1 PN_N + \ldots + g_n ML_n[N] D_n PN_N + e_N^+ - e_N^- = b_N$

Bounding Constraints:

$-1 \leq D_1, \ldots, D_n, PN_1, \ldots, PN_N \leq 1$

$e_1^+, e_1^-, e_2^+, e_2^- \geq 0$

- Solve optimisation problem by *Maximum Likelihood* decoding
- "What was the most likely transmitted data sequence given the waveform?"

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

$\textsc{Eavesdrop}(\mathbf{b}, \mathbf{ML}, \mathbf{g}) \rightarrow (\mathbf{D}^*, \mathbf{PN}^*)$

Constants

$b_1, \ldots, b_N$	Received aggregate chips
$ML_1, \ldots, ML_n$	Satellite ML sequences
$g_1, \ldots, g_n$	Satellite gains

Variables

$D_1, D_2, \ldots, D_n$	Data chip values
$PN_1, \ldots, PN_N$	Cryptographic pseudo-noise
$e_1^+, e_1^-, \ldots, e_N^+, e_N^-$	Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize $Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$

Key Constraints:

$g_1 ML_1[1] D_1 PN_1 + \ldots + g_n ML_n[1] D_n PN_1 + e_1^+ - e_1^- = b_1$

$\ldots$

$g_1 ML_1[N] D_1 PN_N + \ldots + g_n ML_n[N] D_n PN_N + e_N^+ - e_N^- = b_N$

Bounding Constraints:

$-1 \leq D_1, \ldots, D_n, PN_1, \ldots, PN_N \leq 1$

$e_1^+, e_1^-, e_2^+, e_2^- \geq 0$

- Solve optimisation problem by *Maximum Likelihood* decoding
- “What was the most likely transmitted data sequence given the waveform?”
- Takes into account many repeating chip magnitudes

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP($\mathbf{b}, \mathbf{ML}, \mathbf{g}$) $\rightarrow$ ($\mathbf{D}^*, \mathbf{PN}^*$)

Constants

$b_1, \ldots, b_N$	Received aggregate chips
$ML_1, \ldots, ML_n$	Satellite ML sequences
$g_1, \ldots, g_n$	Satellite gains

Variables

$D_1, D_2, \ldots, D_n$	Data chip values
$PN_1, \ldots, PN_N$	Cryptographic pseudo-noise
$e_1^+, e_1^-, \ldots, e_N^+, e_N^-$	Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize $Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$

Key Constraints:

$g_1 ML_1[1] D_1 PN_1 + \ldots + g_n ML_n[1] D_n PN_1 + e_1^+ - e_1^- = b_1$

$\ldots$

$g_1 ML_1[N] D_1 PN_N + \ldots + g_n ML_n[N] D_n PN_N + e_N^+ - e_N^- = b_N$

Bounding Constraints:

$-1 \leq D_1, \ldots, D_n, PN_1, \ldots, PN_N \leq 1$

$e_1^+, e_1^-, e_2^+, e_2^- \geq 0$

- Solve optimisation problem by *Maximum Likelihood* decoding
- "What was the most likely transmitted data sequence given the waveform?"
- Takes into account many repeating chip magnitudes
- Catastrophic outcome: almost always reduces to 2 bits of entropy

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

$\text{EAVESDROP}(\mathbf{b}, \mathbf{ML}, \mathbf{g}) \rightarrow (\mathbf{D}^*, \mathbf{PN}^*)$

Constants

$b_1, \ldots, b_N$	Received aggregate chips
$ML_1, \ldots, ML_n$	Satellite ML sequences
$g_1, \ldots, g_n$	Satellite gains

Variables

$D_1, D_2, \ldots, D_n$	Data chip values
$PN_1, \ldots, PN_N$	Cryptographic pseudo-noise
$e_1^+, e_1^-, \ldots, e_N^+, e_N^-$	Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize $Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$

Key Constraints:

$g_1 ML_1[1] D_1 PN_1 + \ldots + g_n ML_n[1] D_n PN_1 + e_1^+ - e_1^- = b_1$

$\ldots$

$g_1 ML_1[N] D_1 PN_N + \ldots + g_n ML_n[N] D_n PN_N + e_N^+ - e_N^- = b_N$

Bounding Constraints:

$-1 \leq D_1, \ldots, D_n, PN_1, \ldots, PN_N \leq 1$

$e_1^+, e_1^-, e_2^+, e_2^- \geq 0$

- Solve optimisation problem by *Maximum Likelihood* decoding
- "What was the most likely transmitted data sequence given the waveform?"
- Takes into account many repeating chip magnitudes
- Catastrophic outcome: almost always reduces to 2 bits of entropy
- **Any** satellite's data sequence is sufficient to recover **all** other satellites' data

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

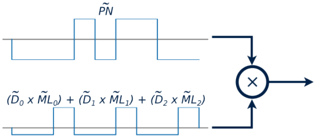
To create new messages, the attacker must know $\tilde{PN}$.

Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

To create new messages, the attacker must know $\tilde{PN}$.

Q: How can $\tilde{PN}$ be recovered?

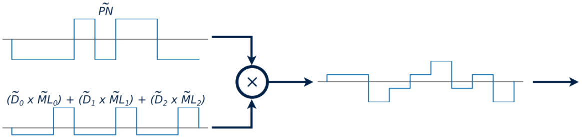


Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

To create new messages, the attacker must know $\tilde{PN}$.

Q: How can $\tilde{PN}$ be recovered?



UNIVERSITY OF OXFORD

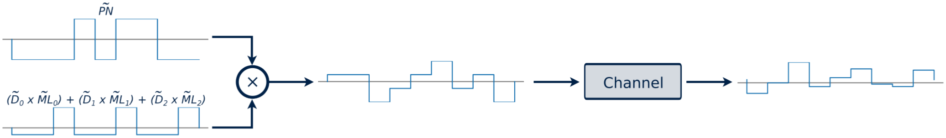
SSL
Systems Security Lab

Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

To create new messages, the attacker must know $\tilde{PN}$.

Q: How can $\tilde{PN}$ be recovered?

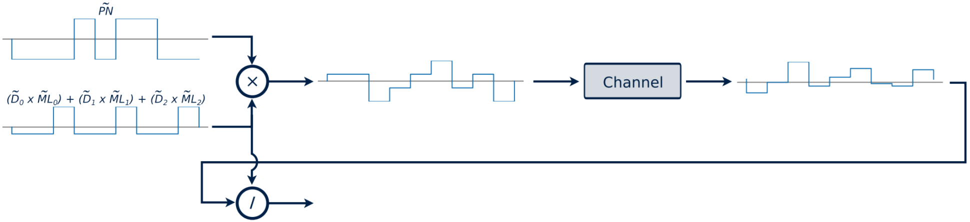


Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

To create new messages, the attacker must know $\tilde{PN}$.

Q: How can $\tilde{PN}$ be recovered?

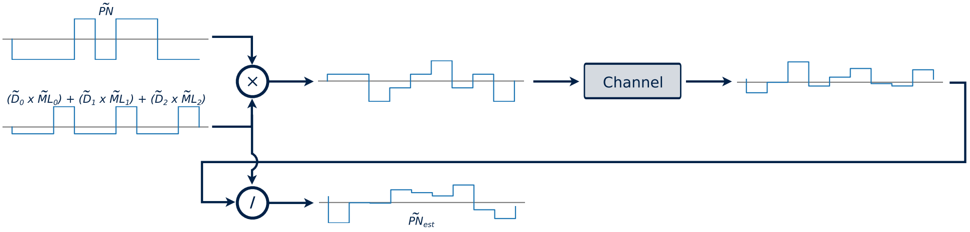


Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

To create new messages, the attacker must know $\tilde{PN}$.

Q: How can $\tilde{PN}$ be recovered?

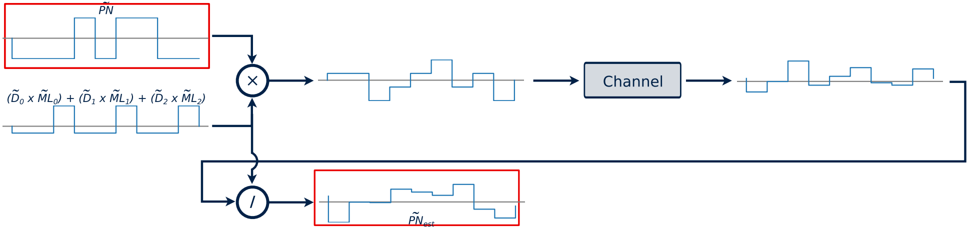


Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

To create new messages, the attacker must know $\tilde{PN}$.

Q: How can $\tilde{PN}$ be recovered?

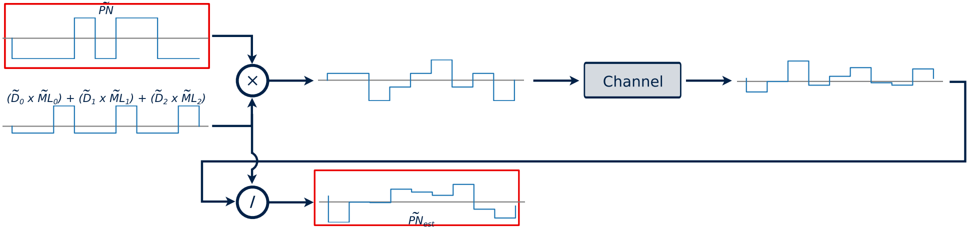


Attack: Spoofing

$\tilde{PN}$ Spreading Sequence Recovery

To create new messages, the attacker must know $\tilde{PN}$.

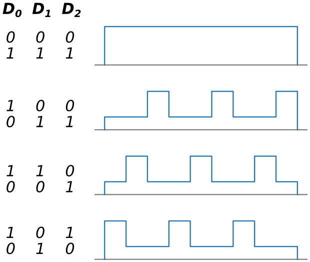
Q: How can $\tilde{PN}$ be recovered?



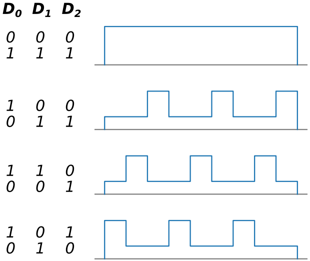
This recovers a noisy estimate of the spreading sequence

$$\tilde{PN} = \tilde{PN}_{est} + noise$$

Attack: Jamming

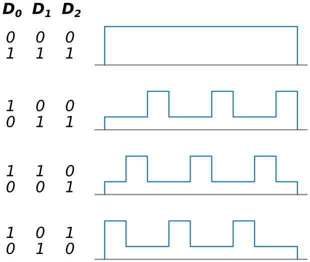


Attack: Jamming



- During each bit period, the jammer…

Attack: Jamming

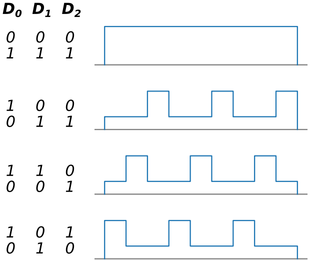


- During each bit period, the jammer...
  - detects the current aggregate bit sequence

UNIVERSITY OF OXFORD

SSL Systems Security Lab

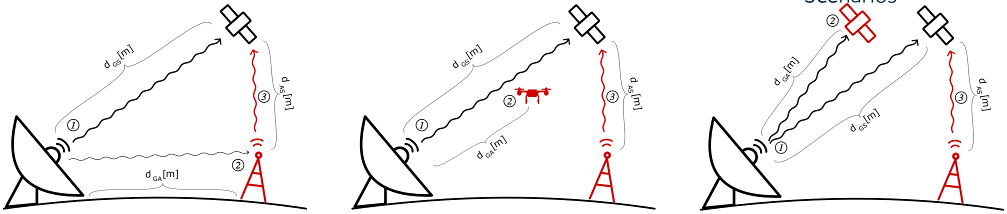
Attack: Jamming



- During each bit period, the jammer...
  - detects the current aggregate bit sequence
  - targets the lowest-power sequences

Threat Model

Scenarios



Ground-based

In-beam

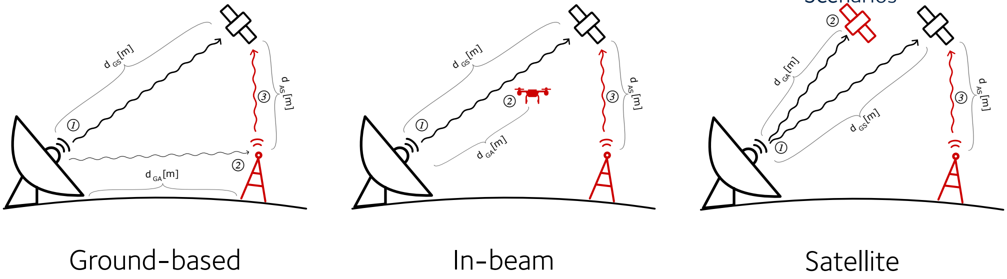
Satellite

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Threat Model

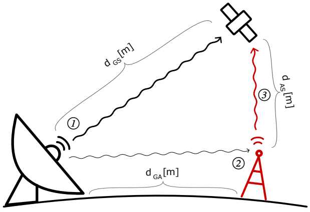
Scenarios



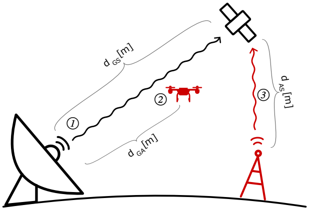
- **Secrecy** – eavesdropping
- **Authenticity** – spoofing
- **Availability** – jamming

Threat Model

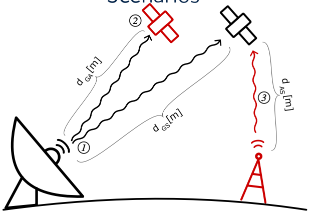
Scenarios



Ground-based



In-beam



Satellite

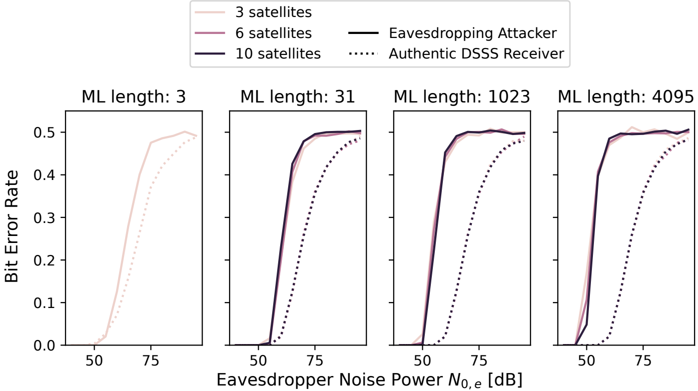
- **Secrecy** – eavesdropping
- **Authenticity** – spoofing
- **Availability** – jamming

Source code available:

https://github.com/ssloxford/hybrid-crypto-spreading-code

Evaluation

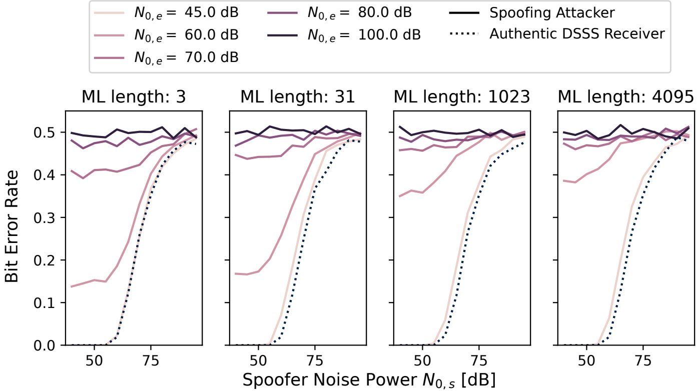
Eavesdropping



Decoding without knowledge of the spreading sequence at only ~ 10 dB less power than with knowledge of the sequence.

Evaluation

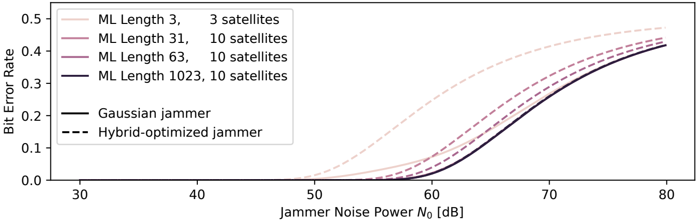
Spoofing



Spoofing depends primarily on the noise in the spreading sequence estimate.
“Lifting” it from the noise floor through e.g. high gain antennas not required.

Evaluation

Jamming



Jammer advantage is high for low ML lengths, and decreases as the length increases.

Countermeasures

UNIVERSITY OF OXFORD

SSL Systems Security Lab

Countermeasures

- Non-hybrid spread spectrum
  - Suffers up to 30 dB performance loss under multiple access
  - Secure hybrid systems for future standardisation must be secure against the presented attacks

Countermeasures

- Non-hybrid spread spectrum
  - Suffers up to $30\,$dB performance loss under multiple access
  - Secure hybrid systems for future standardisation must be secure against the presented attacks
- Preventing synchronization data reuse
  - Initialisation parameters are transmitted in the clear, allowing the adversary to record, modify, and replay as discussed
  - Authenticity protection and freshness guarantees required in session establishment

Countermeasures

- Non-hybrid spread spectrum
  - Suffers up to 30 dB performance loss under multiple access
  - Secure hybrid systems for future standardisation must be secure against the presented attacks
- Preventing synchronization data reuse
  - Initialisation parameters are transmitted in the clear, allowing the adversary to record, modify, and replay as discussed
  - Authenticity protection and freshness guarantees required in session establishment
- Cryptographic scrambling
  - Prevents recovery of the data sequences
  - Does not provide unobservability
  - Does not protect against bit-flipping spoofing attacks

UNIVERSITY OF OXFORD

SSL
Systems Security Lab

Thank you for your attention

Edd Salkield
Systems Security Lab, University of Oxford
https://seclab.cs.ox.ac.uk

edward.salkield@cs.ox.ac.uk
https://edd.salkield.uk