PIMRC 2016: Practical Examples of Physical Layer Security

Arsenia Chorti, Univ. Essex

4 September 2016, Valencia

How it looks from outside

"All you need to make a movie is a girl and a gun"

Jean-Luc Godard

How it looks from outside

"All you need to make a movie is a girl and a gun"

Jean-Luc Godard

"All you need to do crypto is a XOR and a key"

(crypto joke)

How it looks from outside

"All you need to make a movie is a girl and a gun"

Jean-Luc Godard

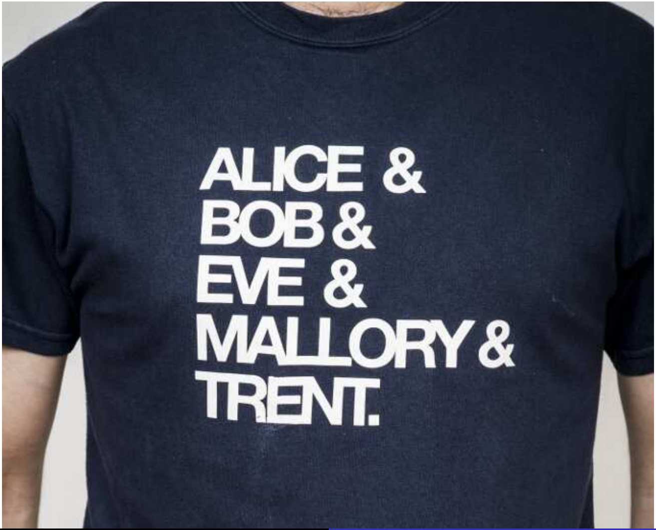
"All you need to do crypto is a XOR and a key"

(crypto joke)

"All you need to do information theory is a log and a lim"

Serio Verdú

The usual suspects



The usual suspects

Openness of wireless channel: security more challenging

- Eavesdropping
- Denial of service attacks (jamming)

Two flavors of PLS

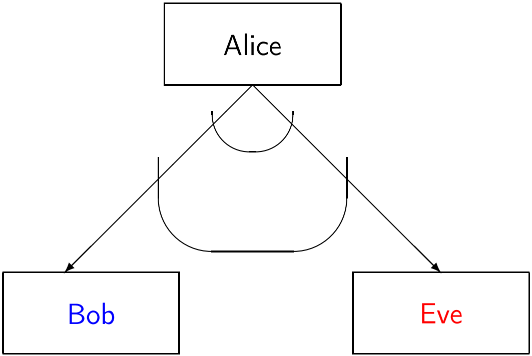
1. Generate keys from correlated sources through public discussion

Two flavors of PLS

1. Generate keys from correlated sources through public discussion
2. Build encoders for degraded adversarial links: "hide" part of the message in noise

What are the hurdles for PLS to gain trust?

1. The adversaries are not powerful enough (passive)



What real systems look like!

Sport US election Daily Edition

Lifestyle › Tech › News

There are officially more mobile devices than people in the world

The world is home to 7.2 billion gadgets, and they're multiplying five times faster than we are

Zachary Davies Boren | @zdboren | Tuesday 7 October 2014 | 0 comments

1K shares

2. The adversary does not have enough observations / diversity

Although infinite computational power is granted at the eavesdropper

2. The adversary does not have enough observations / diversity

Although infinite computational power is granted at the eavesdropper
... often only a single antenna (or limited diversity) is assumed!

2. The adversary does not have enough observations / diversity

Although infinite computational power is granted at the eavesdropper
... often only a single antenna (or limited diversity) is assumed!

Antenna vs. cost survey: gains from 7 dBi to 20 dBi for $25- $200! [1]

2. The adversary does not have enough observations / diversity

Although infinite computational power is granted at the eavesdropper
... often only a single antenna (or limited diversity) is assumed!

Antenna vs. cost survey: gains from 7 dBi to 20 dBi for $25- $200! [1]

What about colluding eavesdroppers?

3. Practical issues: Gaussian signalling, long-length encoders

3. Practical issues: Gaussian signalling, long-length encoders

What about QAM systems?

3. Practical issues: Gaussian signalling, long-length encoders

What about QAM systems?
What about the short codelength regime?

3. Practical issues: Gaussian signalling, long-length encoders

What about QAM systems?
What about the short codelength regime?
What about resource constrained devices?

4. Combining secure systems systems does not guarantee security!

4. Combining secure systems systems does not guarantee security!

One time pad (OTP) is secure

4. Combining secure systems systems does not guarantee security!

One time pad (OTP) is secure
Quantum key distribution (QKD) is secure

4. Combining secure systems systems does not guarantee security!

One time pad (OTP) is secure
Quantum key distribution (QKD) is secure
OTP+QKD should be secure

4. Combining secure systems systems does not guarantee security!

One time pad (OTP) is secure
Quantum key distribution (QKD) is secure
OTP+QKD should be secure

It is not! [2]

Relevance of PLS in Future Networks (5G, IoT, M2M)

Relevance of PLS in Future Networks (5G, IoT, M2M)

- 1000-fold increase in throughput (peak)
- Reduced latency < 1 ms (especially for tactile internet)
- Advanced services (smart*),
- Energy efficiency ...

Relevance of PLS in Future Networks (5G, IoT, M2M)

- 1000-fold increase in throughput (peak)
- Reduced latency < 1 ms (especially for tactile internet)
- Advanced services (smart*),
- Energy efficiency ...

- Massive multi-antenna systems (MIMO), BF and AN
- Small cells: natural PLS setting
- Full duplex: existence of structured interference
- Ad hoc networks, IoT, D2D: secret keys on the fly

Generating secret key from fading coefficients in the presence of active adversaries

Generating keys from correlated sequences

Wireless shared randomness techniques:

Generating keys from correlated sequences

Wireless shared randomness techniques:
Generate purely random keys in 3 steps

Generating keys from correlated sequences

Wireless shared randomness techniques:
Generate purely random keys in 3 steps

1. Advantage distillation

Generating keys from correlated sequences

Wireless shared randomness techniques:
Generate purely random keys in 3 steps

1. Advantage distillation
2. Information reconcilliation

Generating keys from correlated sequences

Wireless shared randomness techniques:
Generate purely random keys in 3 steps

1. Advantage distillation
2. Information reconcilliation
3. Privacy amplification

How good are the PLS keys?

NIST TEST	P-Value
Monobit Frequency	0.739918
Block Frequency	0.739918
Cumulative Sums	0.534146
Runs	0.739918
Longest Run	0.350485
Binary Matrix Rank	0.213309
FFT	0.911413
Non-overlapping Template	0.911413
Overlapping Template	0.534146
Maurer's Universal Test	0.122325
Approximate Entropy	0.739918
Serial	0.739918
Linear Complexity	0.122325

Physical layer authenticated encryption

Replace RSA by PLS key generation in ISO PKE protocol

Physical layer authenticated encryption

Replace RSA by PLS key generation in ISO PKE protocol

1. PLS key seed SeedGen : $\mathbb{R}^+ \rightarrow (0,1)^L \times (0,1)^l$ with (seed,coset) $=$ SeedGen($\mathbf{H}_0$)
2. Sem. sec. hash function G : $(0,1)^L \times (0,1)^l \rightarrow (0,1)^{\lfloor H(\text{seed}) \rfloor}$ with output key K=G(seed, coset), K={Ke, Ki}
3. Sem. sec. A.E.(encrypt-then-MAC): enc. alg. cipher=E(Ke, m), dec. alg. m=D(Ke, cipher), sign alg. t=Sign(Ki, c), ver. alg. v=Ver(Ki, c, t), v $\in \{$ c, $\perp\}$

Physical layer authenticated encryption

Replace RSA by PLS key generation in ISO PKE protocol

1. PLS key seed SeedGen : $\mathbb{R}^+ \rightarrow (0,1)^L \times (0,1)^l$ with (seed,coset) $=$ SeedGen($\mathbf{H}_0$)
2. Sem. sec. hash function G : $(0,1)^L \times (0,1)^l \rightarrow (0,1)^{\lfloor H(\text{seed}) \rfloor}$ with output key K=G(seed, coset), K={Ke, Ki}
3. Sem. sec. A.E.(encrypt-then-MAC): enc. alg. cipher=E(Ke, m), dec. alg. m=D(Ke, cipher), sign alg. t=Sign(Ki, c), ver. alg. v=Ver(Ki, c, t), v $\in \{$ c, $\perp\}$

Alice transmits extended ciphertext C $=$ [coset||cipher||t]

What about spoofing and jamming?

[3]: received signal strength (RSS) key extraction is malleable!

What about spoofing and jamming?

[3]: received signal strength (RSS) key extraction is malleable!
Revisit the SKG model:

What about spoofing and jamming?

[3]: received signal strength (RSS) key extraction is malleable!
Revisit the SKG model: do not rely on simplistic RSS

What about spoofing and jamming?

[3]: received signal strength (RSS) key extraction is malleable!
Revisit the SKG model: do not rely on simplistic RSS

[4]: increasing jamming power diminishes key rates

What about spoofing and jamming?

[3]: received signal strength (RSS) key extraction is malleable!
Revisit the SKG model: do not rely on simplistic RSS

[4]: increasing jamming power diminishes key rates
Anti-jamming zero-sum game over N parallel subchannels

What about spoofing and jamming?

[3]: received signal strength (RSS) key extraction is malleable!
Revisit the SKG model: do not rely on simplistic RSS

[4]: increasing jamming power diminishes key rates
Anti-jamming zero-sum game over N parallel subchannels

$$\begin{aligned}
Y_{A,i} &= \sqrt{p_i}H_i + \sqrt{\gamma_i}G_{A,i} + Z_{A,i}, i = 1, \ldots, N \\
Y_{B,i} &= \sqrt{p_i}H_i + \sqrt{\gamma_i}G_{B,i} + Z_{B,i}, i = 1, \ldots, N, \;\; i = 1, \ldots, N
\end{aligned}$$

What about spoofing and jamming?

[3]: received signal strength (RSS) key extraction is malleable!
Revisit the SKG model: do not rely on simplistic RSS

[4]: increasing jamming power diminishes key rates
Anti-jamming zero-sum game over N parallel subchannels

$$\begin{aligned} Y_{A,i} &= \sqrt{p_i} H_i + \sqrt{\gamma_i} G_{A,i} + Z_{A,i}, i = 1, \ldots, N \\ Y_{B,i} &= \sqrt{p_i} H_i + \sqrt{\gamma_i} G_{B,i} + Z_{B,i}, i = 1, \ldots, N, \;\; i = 1, \ldots, N \end{aligned}$$

$$C(p_i, \gamma_i) = I(Y_{A,i}; Y_{B,i}) = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_H^2 p_i}{N_{A,i} + N_{B,i} + \frac{N_{A,i} N_{B,i}}{\sigma_H^2 p_i}} \right),$$

with $\quad N_{A,i} = 1 + \sigma_A^2 \gamma_i, \quad N_{B,i} = 1 + \sigma_B^2 \gamma_i$

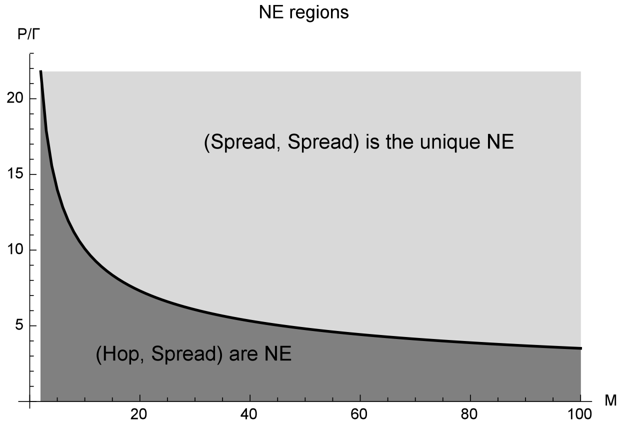
Probabilities $\alpha_i, \beta_i, i \leq N$ for legitimate users and jammer respectively to hop on channel i for
Probabilities $\alpha_{N+1}, \beta_{N+1}$ to spread

$$u(\alpha, \beta) = \sum_{i=1}^{N} \{\alpha_i(1 - \beta_i - \beta_{N+1})C(NP, 0) + \alpha_i\beta_i C(NP, N\Gamma)$$
$$+\alpha_i\beta_{N+1}C(NP, \Gamma) + \alpha_{N+1}(1 - \beta_i - \beta_{N+1})C(P, 0)$$
$$+ \alpha_{N+1}\beta_i C(P, N\Gamma) + \alpha_{N+1}\beta_{N+1}C(P, \Gamma)\} .$$

- Jammer should always spread

- Jammer should always spread
- Frequency hopping not always optimal for legitimate users! When unfavorable conditions hop, when favorable conditions spread

- Jammer should always spread
- Frequency hopping not always optimal for legitimate users! When unfavorable conditions hop, when favorable conditions spread



MQAM encoders for the $x + y$ channel

$x + y$ channels

- Wireless network coding systems
- Full duplex

$x + y$ channels

- Wireless network coding systems
- Full duplex

Creating channel advantage

$x + y$ channels

- Wireless network coding systems
- Full duplex

Creating channel advantage
... using structured interference

$x + y$ channels

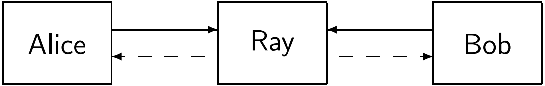
- Wireless network coding systems
- Full duplex

Creating channel advantage
... using structured interference

Gaussian signalling does not offer this opportunity

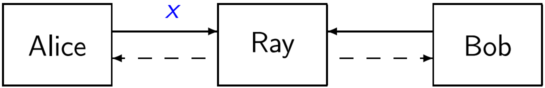
Wireless network coding

In standard relay channels we need 4 cycles to exchange x, y.



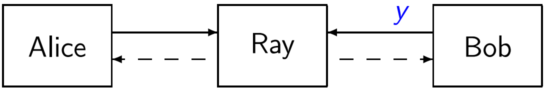
Wireless network coding

In standard relay channels we need 4 cycles to exchange x, y.



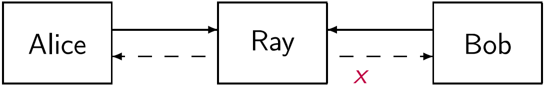
Wireless network coding

In standard relay channels we need 4 cycles to exchange x, y.



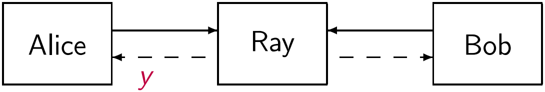
Wireless network coding

In standard relay channels we need 4 cycles to exchange x, y.



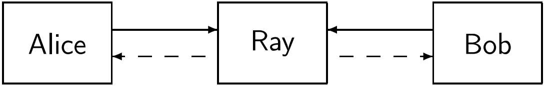
Wireless network coding

In standard relay channels we need 4 cycles to exchange x, y.



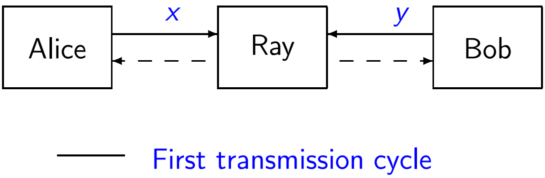
Physical layer network coding ctd'

In PNC we need 2 cycles



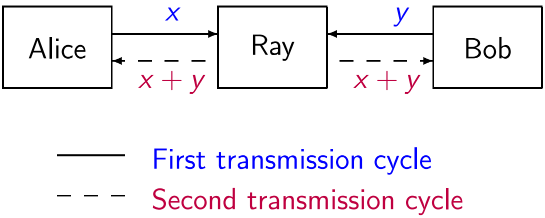
Physical layer network coding ctd'

In PNC we need 2 cycles

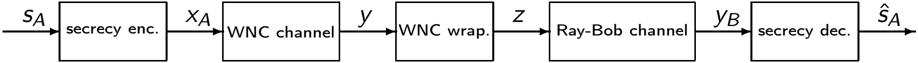


Physical layer network coding ctd'

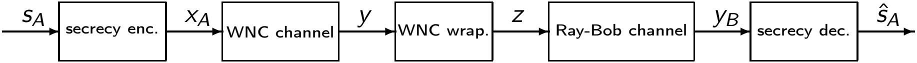
In PNC we need 2 cycles



Untrusted (but honest) relay



Untrusted (but honest) relay

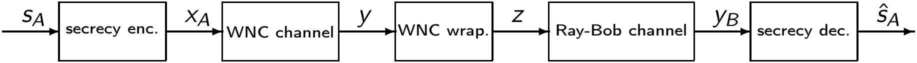


- Finite alphabets $\mathcal{S}_A$, $\mathcal{S}_B$ of secret messages to be transmitted by Alice and Bob

Untrusted (but honest) relay

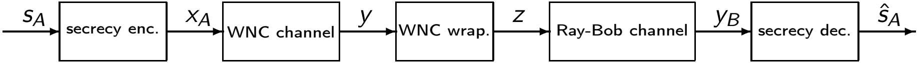
- Finite alphabets $\mathcal{S}_A$, $\mathcal{S}_B$ of secret messages to be transmitted by Alice and Bob
- Codewords $\in \mathcal{X}_A, \mathcal{X}_B \subset \mathcal{C}$ with $M_A = |\mathcal{X}_A|$, $M_B = |\mathcal{X}_B|$, $m_A = \log_2 M_A$, $m_B = \log_2 M_B$

Untrusted (but honest) relay



- Finite alphabets $\mathcal{S}_A$, $\mathcal{S}_B$ of secret messages to be transmitted by Alice and Bob
- Codewords $\in \mathcal{X}_A, \mathcal{X}_B \subset \mathcal{C}$ with $M_A = |\mathcal{X}_A|$, $M_B = |\mathcal{X}_B|$, $m_A = \log_2 M_A$, $m_B = \log_2 M_B$
- Labeling functions $b_A : \mathcal{X}_A \rightarrow \mathcal{S}_A \cup \{\varepsilon\}$, $b_B : \mathcal{X}_B \rightarrow \mathcal{S}_B \cup \{\varepsilon\}$ where ε represents the empty string

Untrusted (but honest) relay



- Finite alphabets $\mathcal{S}_A$, $\mathcal{S}_B$ of secret messages to be transmitted by Alice and Bob
- Codewords $\in \mathcal{X}_A, \mathcal{X}_B \subset \mathcal{C}$ with $M_A = |\mathcal{X}_A|$, $M_B = |\mathcal{X}_B|$, $m_A = \log_2 M_A$, $m_B = \log_2 M_B$
- Labeling functions $b_A : \mathcal{X}_A \to \mathcal{S}_A \cup \{\varepsilon\}$, $b_B : \mathcal{X}_B \to \mathcal{S}_B \cup \{\varepsilon\}$ where ε represents the empty string
- $\forall s_A \in \mathcal{S}_A \cup \{\varepsilon\}$ we set $b_A^{-1}(s_A) = \{x_A \mid b_A(x_A) = s_A\}$ and $\forall s_B \in \mathcal{S}_B \cup \{\varepsilon\}$ we set $b_B^{-1}(s_B) = \{x_B \mid b_B(x_B) = s_B\}$

Transmission cycles

1. First Transmission Cycle

Transmission cycles

1. First Transmission Cycle
   - Stochastic encoders $\varphi_A(s_A), \varphi_B(s_B)$ uniformly distributed over $b_A^{-1}(s_A)$ and $b_B^{-1}(s_A)$

Transmission cycles

1. First Transmission Cycle
   - Stochastic encoders $\varphi_A(s_A), \varphi_B(s_B)$ uniformly distributed over $b_A^{-1}(s_A)$ and $b_B^{-1}(s_A)$
   - Ray observes
$$Y = X_A + X_B + W$$

Transmission cycles

1. First Transmission Cycle
    - Stochastic encoders $\varphi_A(s_A), \varphi_B(s_B)$ uniformly distributed over $b_A^{-1}(s_A)$ and $b_B^{-1}(s_A)$
    - Ray observes

$$Y = X_A + X_B + W$$

2. Second Transmission Cycle

Transmission cycles

1. First Transmission Cycle
   - Stochastic encoders $\varphi_A(s_A), \varphi_B(s_B)$ uniformly distributed over $b_A^{-1}(s_A)$ and $b_B^{-1}(s_A)$
   - Ray observes

$$Y = X_A + X_B + W$$

2. Second Transmission Cycle
   - Ray transmits Z, Alice and Bob observe

$$Y_A = Z + W_A,$$
$$Y_B = Z + W_B,$$

W, W_A, W_B AWGN noise

Upper Bounds on Secrecy Rates

Perfect Secrecy w.r.t. Ray if

- $I(Y; S_A) = 0$, perfect secrecy condition for Alice
- $I(Y; S_B) = 0$, perfect secrecy condition for Bob

Upper Bounds on Secrecy Rates

Perfect Secrecy w.r.t. Ray if

- $I(Y; S_A) = 0$, perfect secrecy condition for Alice
- $I(Y; S_B) = 0$, perfect secrecy condition for Bob

Proposition 1

The perfect secrecy rates are bounded by $R_A^s \leq \widehat{R}_A^s$ and $R_B^s \leq \widehat{R}_B^s$,

$$\widehat{R}_A^s = I(X_A; Y_B|X_B) - I(X_A; Y) + \delta_A$$
$$\widehat{R}_B^s = I(X_B; Y_A|X_A) - I(X_B; Y) + \delta_B$$

with $\delta_A = H(X_A|Y_B, X_B)$ and $\delta_B = H(X_B|Y_A, X_A)$

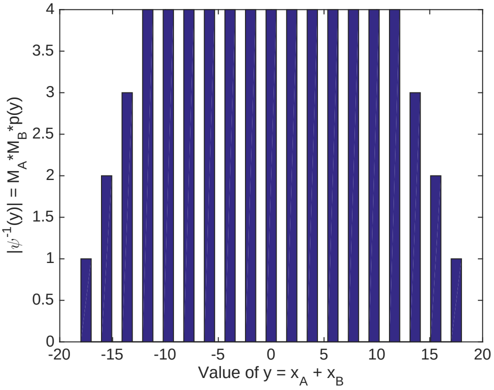


Figure: Pmf of Ray's observation $y = x_A + x_B$ in the noiseless scenario for a 4-PAM modulator and a 16-PAM modulator.

Upper bound in M-PAM systems

Theorem 1

In the noiseless setting with unit channel gains when Alice and Bob employ M_A-PAM and M_B-PAM modulators with $M_B \geq M_A$, we have

$$\widehat{R}^s = m_A \frac{M_B - M_A + 1}{M_B} + \frac{2}{M_A M_B} \sum_{a=1}^{M_A - 1} a \log_2(a).$$

In particular, for fixed M_A we have $\lim_{M_B \to \infty} \widehat{R}^s = m_A$.

Encoder Construction at Bob

Bob's Secret Subset

- Define a subset $\mathcal{X}_B^s$ of $\mathcal{X}_B$ on which Bob will transmit secret bits

Encoder Construction at Bob

Bob's Secret Subset

- Define a subset $\mathcal{X}_B^s$ of $\mathcal{X}_B$ on which Bob will transmit secret bits

$$\mathcal{X}_B^s = \{x_B \in \mathcal{X}_B \mid |x_B| \leq M_B - 2M_A - 1\}$$

Encoder Construction at Bob

Bob's Secret Subset

- Define a subset $\mathcal{X}_B^s$ of $\mathcal{X}_B$ on which Bob will transmit secret bits

$$\mathcal{X}_B^s = \{x_B \in \mathcal{X}_B \mid |x_B| \leq M_B - 2M_A - 1\}$$

- $\forall x_B \in \mathcal{X}_B^s$ we have $|\psi^{-1}(x_A + x_B)| = M_A$ for all $x_A \in \mathcal{X}_A$

Encoder Construction at Bob

Bob's Secret Subset

- Define a subset $\mathcal{X}_B^s$ of $\mathcal{X}_B$ on which Bob will transmit secret bits

$$\mathcal{X}_B^s = \{x_B \in \mathcal{X}_B \mid |x_B| \leq M_B - 2M_A - 1\}$$

- $\forall x_B \in \mathcal{X}_B^s$ we have $|\psi^{-1}(x_A + x_B)| = M_A$ for all $x_A \in \mathcal{X}_A$
- $|\mathcal{X}_B^s| = M_B - 2M_A$

Encoder Construction at Bob cnt'd

Bit Labeling

- Bit labeling for $\mathcal{X}_B$: perfect binary tree with edges alternately labeled

Encoder Construction at Bob cnt'd

Bit Labeling

- Bit labeling for $\mathcal{X}_B$: perfect binary tree with edges alternately labeled
- x_B given bit labeling $l(x_B)$ tracing the tree downwards

Encoder Construction at Bob cnt'd

Bit Labeling

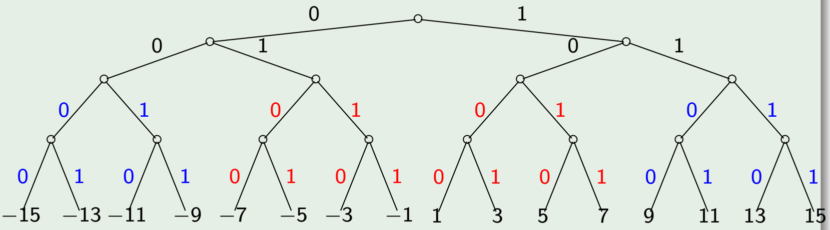
- Bit labeling for $\mathcal{X}_B$: perfect binary tree with edges alternately labeled
- x_B given bit labeling $l(x_B)$ tracing the tree downwards
- Bob's labeling function $b_B : \mathcal{X}_B \to \mathcal{S}_B \cup \{\varepsilon\}$ defined by

$$b_B(x_B) = \begin{cases} \text{the last } m_A \text{ bits of } l(x_B) & x_B \in \mathcal{X}_B^s \\ \varepsilon & x_B \notin \mathcal{X}_B^s \end{cases}$$

Bob's Encoder Example

Example: $M_A = 4$, $M_B = 16$, $\mathcal{X}_B^s = \{-7, \ldots, +7\}$, $\mathcal{X}_B = \{-15, \ldots, +15\}$

Bob transmits $m_A = 2$ bits on $\mathcal{X}_B^s$ with rate $R_B^s = m_A \frac{M_B - 2M_A}{M_B}$



Bob's Transmission Example

$M_A = 4$ and $M_B = 16$

Bob has public and secret bit queues
$\mathcal{Q}_B^p = 10110101, \quad \mathcal{Q}_B^s = 1111$

Bob's Transmission Example

$M_A = 4$ and $M_B = 16$

Bob has public and secret bit queues
$\mathcal{Q}_B^p = 10110101, \quad \mathcal{Q}_B^s = 1111$

1. First encode left-most bits in $\mathcal{Q}_B^p$ 10

Bob's Transmission Example

$M_A = 4$ and $M_B = 16$

Bob has public and secret bit queues
$\mathcal{Q}_B^p = 10110101, \quad \mathcal{Q}_B^s = 1111$

1. First encode left-most bits in $\mathcal{Q}_B^p$ 10
2. $\in \mathcal{X}_B^s \Rightarrow$ 11 from $\mathcal{Q}_B^s \Rightarrow x_B = +7$ transmitted

Bob's Transmission Example

$M_A = 4$ and $M_B = 16$

Bob has public and secret bit queues
$\mathcal{Q}_B^p = 10110101, \quad \mathcal{Q}_B^s = 1111$

1. First encode left-most bits in $\mathcal{Q}_B^p$ 10
2. $\in \mathcal{X}_B^s \Rightarrow 11$ from $\mathcal{Q}_B^s \Rightarrow x_B = +7$ transmitted
3. and so on...

$$\begin{aligned} &\text{time } t = 1 \quad 1011 \rightarrow +7 = x_B(1) \\ &\text{time } t = 2 \quad 1101 \rightarrow +11 = x_B(2) \\ &\text{time } t = 3 \quad 0111 \rightarrow -1 = x_B(3) \end{aligned}$$

Alice's Bit Labeling

With side info, Alice's bit labeling function

$$b_A : \mathcal{X}_A \times \mathcal{X}_B \to \mathcal{S}_A \cup \{\varepsilon\}$$

where $\mathcal{X}_A$ and $\mathcal{X}_B$ M_A-PAM, M_B-PAM and

$$b_A(x_A, x_B) = \begin{cases} l(x_A) & \text{if } |\psi^{-1}(x_A + x_B)| = M_A \\ \varepsilon & \text{otherwise} \end{cases}$$

Theorem 3

Suppose that $M_B \geq M_A$. For the above encoder, $I(S_A; Y) = 0$, $R_A^s = m_A \frac{M_B - M_A + 1}{M_B}$ and for fixed M_A, $\lim_{M_B \to \infty} R_A^s = m_A$.

Example of Alice's Encoder Construction

$$M_A = 4,\ M_B = 8\ \mathcal{Q}_A^s = 1011,\ x_B(1) = 7,\ x_B(2) = -5,\ x_B(3) = +5$$

x_B

x_A		-7	-5	-3	-1	$+1$	$+3$	$+5$	$+7$
	$+3$	00	00	00	00	00	ε	ε	ε
	$+1$	ε	01	01	01	01	01	ε	ε
	-1	ε	ε	11	11	11	11	11	ε
	-3	ε	ε	ε	10	10	10	10	10

Alice's encoder

time $t = 1$ $\quad x_B(1) = +7, \Rightarrow x_A(1) = -3$

time $t = 2$ $\quad x_B(2) = -5, \Rightarrow x_A(2) = \varepsilon$

time $t = 3$ $\quad x_B(3) = +5, \Rightarrow x_A(3) = -1$

Effect of Synchronization Errors

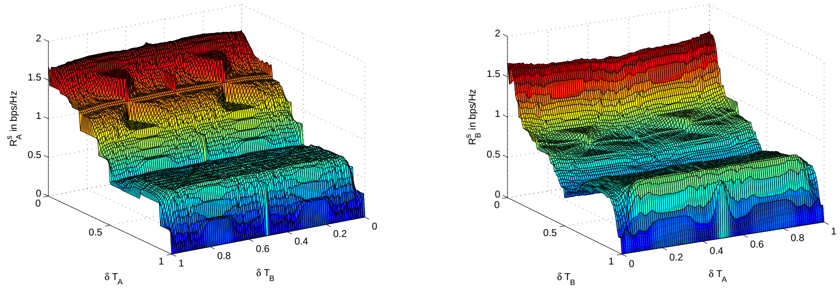
- Synchronization errors $\Rightarrow$ misalignment of Alice's and Bob's symbols at Ray

Effect of Synchronization Errors

- Synchronization errors $\Rightarrow$ misalignment of Alice's and Bob's symbols at Ray
- Interference depends on past codewords

Effect of Synchronization Errors

- Synchronization errors $\Rightarrow$ misalignment of Alice's and Bob's symbols at Ray
- Interference depends on past codewords



Advantage in population size

Cooperative multiuser setting

- Network with M parallel Rayleigh subchannels, K legitimate users and E eavesdroppers

Cooperative multiuser setting

- Network with M parallel Rayleigh subchannels, K legitimate users and E eavesdroppers
- Subchannel allocation according to a max SNR criterion: order statistics come into play

Cooperative multiuser setting

- Network with M parallel Rayleigh subchannels, K legitimate users and E eavesdroppers
- Subchannel allocation according to a max SNR criterion: order statistics come into play

Probability of secrecy outage

- Non-cooperative scenario

$$P_{out}^{(nc)}(K, E, \tau)K\Gamma(K)\sum_{n=1}^{E}(-1)^{n+1}\binom{E}{n}\frac{\Gamma(n2^{-\tau}+1)}{\Gamma(K+n2^{-\tau}+1)}$$

Cooperative multiuser setting

- Network with M parallel Rayleigh subchannels, K legitimate users and E eavesdroppers
- Subchannel allocation according to a max SNR criterion: order statistics come into play

Probability of secrecy outage

- Non-cooperative scenario

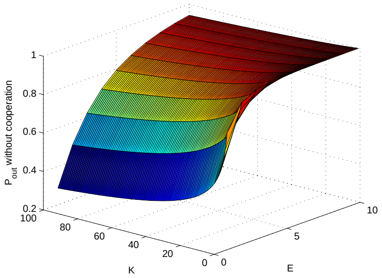
$$P_{out}^{(nc)}(K, E, \tau) K\Gamma(K) \sum_{n=1}^{E} (-1)^{n+1} \binom{E}{n} \frac{\Gamma(n2^{-\tau}+1)}{\Gamma(K+n2^{-\tau}+1)}$$

- Fully cooperative scenario (virtual MIMO)

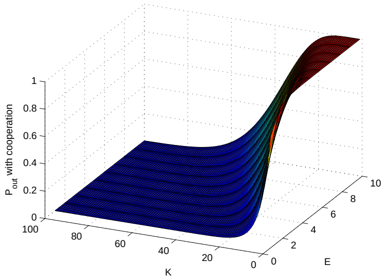
$$P_{out}^{(co)}(K, E, \tau) 1 - \frac{\sum_{n=0}^{K-1} \binom{K+E-1}{n} 2^{n\tau}}{(1+2^{\tau})^{K+E-1}}$$

$\tau = 1$ bit/sec/Hz

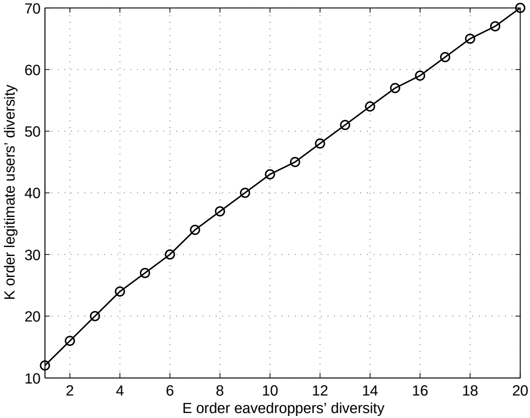
Non-cooperative case $P_{out}^{(nc)}$



Cooperative case $P_{out}^{(co)}$



Required minimum number of K versus E to upper-bound the $P_{out}^{(co)} \leq 1\%$ for $\tau = 1$ bit/sec/Hz



Conclusions

- There exist systems in which PLS might be useful

Conclusions

- There exist systems in which PLS might be useful
- Mature topic: wireless channels can be used to establish secret keys
- Emerging topic: systems with structured interference

Conclusions

- There exist systems in which PLS might be useful
- Mature topic: wireless channels can be used to establish secret keys
- Emerging topic: systems with structured interference

- **Synergy between information theoretic security and crypto necessary**
- **Nested structures?**
- **New opportunities: user centric adaptive security**

[1] W. Trappe, "The Challenges Facing Physical Layer Security", *IEEE Commun. Mag.*, 2015
[2] R. Koenig, R. Renner, A. Bariska, U. Maurer, "Small Accessible Quantum Information Does Not Imply Security", *Phys. R. Let.*, 2007
[3] S. Jana et al., "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," *Proc. 15th ACM Mobile Comp. Netw.*, 2009,
[4] M. Zafer, D. Agrawal,M. Srivatsa, "Limitations of Generating a Secret Key Using Wireless Fading Under Active Adversary", *IEEE/ACM Trans. Netw.*, 2012
[5] V. Belmega and A. Chorti, "Anti-jamming games for secret key generation systems", to be submitted
[6] D. Karpuk and A. Chorti, "Perfect Secrecy in Physical Layer Network Coding Systems from Structured Interference", *IEEE Trans. Inf. Forensics Security*, 2016
[7] A. Chorti, S.M. Perlaza, Z. Han, H.V. Poor, "On the Resilience of Wireless Multiuser Networks to Passive and Active Eavesdroppers", *IEEE J. Sel. Areas Commun.*, 2013"

gracias!

achorti@essex.ac.uk