Exploiting the Non-Commutativity of Nonlinear Operators for Information-theoretic security in Disadvantaged Wireless Environments

Azadeh Sheikholeslami, Dennis Goeckel, Hossein Pishro-Nik

University of Massachusetts, Amherst
Motivation:
Motivation:
Motivation:
Cryptography:

Standard way to achieve secrecy:
Cryptography
Cryptography:

Standard way to achieve secrecy: Cryptography

- Pro: No assumption on the channels
Cryptography:

**Standard way to achieve secrecy: Cryptography**

- **Pro:** No assumption on the channels
- **Cons:**
  - Assumption on computational capabilities of the eavesdropper
  - The eavesdropper obtains the key after transmission
  - Breaking the encryption system later
Information-theoretic security:

**Perfect Secrecy [Shannon]:**
- Unconditional secrecy
Information-theoretic security:

**Perfect Secrecy [Shannon]:**
- Unconditional secrecy

**Wiretap Channel [Wyner]:**
- Eve’s channel degraded with respect to Bob’s channel
Information-theoretic security:

**Perfect Secrecy [Shannon]:**
- Unconditional secrecy

**Wiretap Channel [Wyner]:**
- Eve’s channel degraded with respect to Bob’s channel

**General Wiretap channel:**
- Eve’s channel “more noisy” or “less capable” than Bob’s channel
Information-theoretic security:

Perfect Secrecy [Shannon]:
- Unconditional secrecy

Wiretap Channel [Wyner]:
- Eve’s channel degraded with respect to Bob’s channel

General Wiretap channel:
- Eve’s channel “more noisy” or “less capable” than Bob’s channel

“The key to achieve positive secrecy rates is to have an advantage over the eavesdropper channel”
Challenges of IT security in wireless networks:
Challenges of IT security in wireless networks:

- Near Eve or Eve with directional antenna
Challenges of IT security in wireless networks:

- Near Eve or Eve with directional antenna
- Eve with unknown location or channel gain
Challenges of IT security in wireless networks:

- Near Eve or Eve with directional antenna
- Eve with unknown location or channel gain
- Eve with perfect access to the output of the transmitter radio, e.g., Eve able to pick up the chip (RFID)
Challenges of IT security in wireless networks:

- Near Eve or Eve with directional antenna
- Eve with unknown location or channel gain
- Eve with perfect access to the output of the transmitter radio, e.g., Eve able to pick up the chip (RFID)

**Cooperative jamming:**

- Needs helper nodes or multiple antennas
- Eve with perfect access to the signal
Challenges of IT security in wireless networks:

- Near Eve or Eve with directional antenna
- Eve with unknown location or channel gain
- Eve with perfect access to the output of the transmitter radio, e.g., Eve able to pick up the chip (RFID)

Cooperative jamming:

- Needs helper nodes or multiple antennas
- Eve with perfect access to the signal

Public discussion:

- It needs a public authenticated channel
- Low data rate if used in one-time-pad (Secret-key agreement for cryptography)
- Eve with perfect access to the signal
Solution?

- Cachin and Maurer introduced the “bounded memory model” to achieve everlasting secrecy [1997].
Solution?

- Cachin and Maurer introduced the “bounded memory model” to achieve everlasting secrecy [1997].
- However, it is hard to pick a memory size that Eve cannot use beyond:
  - Density of memories grows quickly and they can be stacked arbitrarily.
Solution?

- Cachin and Maurer introduced the “bounded memory model” to achieve everlasting secrecy [1997].
- However, it is hard to pick a memory size that Eve cannot use beyond:
  - Density of memories grows quickly and they can be stacked arbitrarily.

Attack the frond-end instead of memory in the back-end.
- Pre-share a cryptographic key between Alice and Bob.
- Distort the signal at transmitter rapidly.
- Follow distortion at receiver.
- Eve gets lost.
System model and approach:
Alice and Bob pre-share an “ephemeral” cryptographic key to choose $g(.)$ from $\mathcal{G}$. 
System model and approach:

- Alice and Bob pre-share an “ephemeral” cryptographic key to choose $g(.)$ from $\mathcal{G}$.
- Key can be handed to Eve after completion of transmission.
System model and approach:

- Alice and Bob pre-share an “ephemeral” cryptographic key to choose $g(.)$ from $\mathcal{G}$.
- Key can be handed to Eve after completion of transmission.
- A/D is a non-linear element, non-commutativity of non-linear operations can lead to: Potential security.
System model and approach:

- Alice and Bob pre-share an “ephemeral” cryptographic key to choose \( g(.) \) from \( \mathcal{G} \).
- Key can be handed to Eve after completion of transmission.
- A/D is a non-linear element, non-commutativity of non-linear operations can lead to: Potential security.
- Secrecy rate is due to the shaping gain:
  \[
  R_s \approx E_g[h(X) - h(g(X))], g(.) \in \mathcal{G}
  \]
System model and approach:

- Alice and Bob pre-share an “ephemeral” cryptographic key to choose $g(.)$ from $\mathcal{G}$.
- Key can be handed to Eve after completion of transmission.
- A/D is a non-linear element, non-commutativity of non-linear operations can lead to: Potential security.
- Secrecy rate is due to the shaping gain:
  \[ R_s \approx E_{\mathcal{G}}[h(X) - h(g(X))], g(.) \in \mathcal{G} \]
- It can be very large by choosing “severely distorting” gains.
System model and approach:

- Alice and Bob pre-share an “ephemeral” cryptographic key to choose $g(.)$ from $\mathcal{G}$.
- Key can be handed to Eve after completion of transmission.
- A/D is a non-linear element, non-commutivity of non-linear operations can lead to: Potential security.
- Secrecy rate is due to the shaping gain:
  \[ R_s \approx E_g[h(X) - h(g(X))], \quad g(.) \in \mathcal{G} \]
- It can be very large by choosing “severely distorting” gains.
- More distorting $g(.)$ can also cause significant “noise enhancement”.

![Diagram of system model with D/A, g(.), A/D, n_B, n_E, X, Y, Z, and Eve.]
Rapid power modulation for secrecy:

Alice

\[ X \xrightarrow{k} A \xrightarrow{n_B} Y \xrightarrow{k} \frac{1}{A} \xrightarrow{n_E} \hat{Z} \xrightarrow{1/G} \frac{A}{D} \xrightarrow{Z} \]

Bob

\[ Y \xrightarrow{A/D} \]

Eve

\[ \hat{Z} \xrightarrow{A/D} \]

6/12
Rapid power modulation for secrecy:

Alice

\[ A = \begin{cases} A_1, & \text{w.p. } p \\ A_2, & \text{w.p. } 1-p \end{cases} \]

Bob

\[ A/D \]

Eve

\[ A/D \]

\[ k \]

\[ n_B \]

\[ 1/A \]

\[ k \]

\[ n_E \]

\[ 1/G \]

\[ \hat{Y} \]

\[ Y \]

\[ \hat{Z} \]

\[ Z \]

\[ X \]
Rapid power modulation for secrecy:

\[ A = \{A_1, A_2, \text{w.p. } 1-p \} \]

\[ A_1, \text{w.p. } p \]

Alice \rightarrow \frac{k}{A} \rightarrow n_B \rightarrow \frac{1}{A} \rightarrow \dot{Y} \rightarrow \frac{k}{1/A} \rightarrow \dot{Y} \rightarrow \text{A/D} \rightarrow Y

Bob

Eve \rightarrow \frac{1}{A} \rightarrow \frac{k}{1/A} \rightarrow \dot{Z} \rightarrow \frac{1}{G} \rightarrow \text{A/D} \rightarrow Z
Rapid power modulation for secrecy:

$$A = \begin{cases} A_1, & \text{w. p. } p \\ A_2, & \text{w. p. } 1 - p \end{cases}$$

1. \( \frac{A_1}{A_2} = r \)
2. \( pA_1^2 + (1 - p)A_2^2 = 1 \)
Rapid power modulation for secrecy:

\[ A = \begin{cases} A_1, & \text{w. p. } p \\ A_2, & \text{w. p. } 1 - p \end{cases} \]

1. \( \frac{A_1}{A_2} = r \)
2. \( p A_1^2 + (1 - p) A_2^2 = 1 \)
Rapid power modulation for secrecy:

\[ A = \begin{cases} A_1, & \text{w.p. } p \\ A_2, & \text{w.p. } 1 - p \end{cases} \]

1. \[ \frac{A_1}{A_2} = r \]
2. \[ pA_1^2 + (1 - p)A_2^2 = 1 \]
Rapid power modulation for secrecy:

\[ A = \begin{cases} A_1, \quad \text{w.p. } p \\ A_2, \quad \text{w.p. } 1 - p \end{cases} \]

1. \( \frac{A_1}{A_2} = r \)
2. \( p A_1^2 + (1 - p) A_2^2 = 1 \)
Rapid power modulation for secrecy:

\[ A = \begin{cases} A_1, & \text{w.p. } p \\ A_2, & \text{w.p. } 1-p \end{cases} \]

1. \( \frac{A_1}{A_2} = r \)
2. \( pA_1^2 + (1-p)A_2^2 = 1 \)
Rapid power modulation for secrecy:

Lemma:
The gain $\frac{1}{G}$ that Eve applies before her A/D should take a single value with probability one to minimize the secrecy rate.

1. $\frac{A_1}{A_2} = r$
2. $pA_1^2 + (1 - p)A_2^2 = 1$
Rapid power modulation for secrecy:

Alice

\[ A = \begin{cases} A_1, & \text{w.p. } p \\ A_2, & \text{w.p. } 1 - p \end{cases} \]

1. \[ \frac{A_1}{A_2} = r \]
2. \[ p A_1^2 + (1 - p) A_2^2 = 1 \]

- Eve tries to find a gain \( G \) that minimizes the secrecy rate \( R_s \); On the other hand, Alice sets the parameter \( p \) to maximize \( R_s \).
Rapid power modulation for secrecy:

- Eve tries to find a gain $G$ that minimizes the secrecy rate $R_s$; On the other hand, Alice sets the parameter $p$ to maximize $R_s$.

**Secrecy rate:** $R_s = \max_p \min_G R_s(G, p)$
Rapid power modulation for secrecy:

- Eve tries to find a gain \( G \) that minimizes the secrecy rate \( R_s \); On the other hand, Alice sets the parameter \( p \) to maximize \( R_s \).

**Secrecy rate:** \( R_s = \max_p \min_G R_s(G, p) \)

- Alice chooses \( p = \Pr(A = A_1) \) such that no matter what \( G \) Eve chooses, some secrecy rate \( R_s \) is always guaranteed, and she tries to maximize \( R_s \).

\[ A = \begin{cases} A_1, & \text{w.p. } p \\ A_2, & \text{w.p. } 1 - p \end{cases} \]

1. \( \frac{A_1}{A_2} = r \)
2. \( pA_1^2 + (1 - p)A_2^2 = 1 \)
Rapid power modulation for secrecy:

Effect of A/D on the signal:
- Clipping (due to overflow)
Rapid power modulation for secrecy:

Effect of A/D on the signal:
- Clipping (due to overflow)
- Quantization noise (uniformly distributed)
Rapid power modulation for secrecy:

**Effect of A/D on the signal:**
- Clipping (due to overflow)
- Quantization noise (uniformly distributed)

**Trade-off between choosing a large gain and a small gain:**
- Eve needs to compromise between more A/D overflows or less resolution.
Numerical results:

Secrecy rate vs. $p$ and $G$:
Identical 10-bit A/D’s.

The ratio between the two power levels at the transmitter is $r = 10^3 (30 \text{ dB})$, and the average transmitting power is $P = 1$. A maximin secrecy rate of $R_s = 3.1372$ is achieved.
Numerical results:

Secrecy rate vs. $p$ and $G$:
Identical 10-bit A/D’s.

The ratio between the two power levels at the transmitter is $r = 10^3 (30 \text{ dB})$, and the average transmitting power is $P = 1$. A maximin secrecy rate of $R_s = 3.1372$ is achieved.
Numerical results:

Secrecy rate vs. $p$ and $G$:
Identical 10-bit A/D’s.

The ratio between the two power levels at the transmitter is $r = 10^{3}(30 \text{ dB})$, and the average transmitting power is $P = 1$. A maximin secrecy rate of $R_s = 3.1372$ is achieved.

Eve with better A/D than Bob

Upper curve: both Bob and Eve have 10-bit A/D’s. Lower curve: Bob has 10-bit A/D while Eve has 14-bit A/D (Eve’s A/D is 24 dB better). A maximin secrecy rate of $R_s = 1.2478$ is achieved ($p = 0.4$).
Numerical results:

Secrecy rate vs. $p$ and $G$:
Identical 10-bit A/D’s.

The ratio between the two power levels at the transmitter is $r = 10^3 (30 \text{ dB})$, and the average transmitting power is $P = 1$. A maximin secrecy rate of $R_s = 3.1372$ is achieved.

Eve with better A/D than Bob

Upper curve: both Bob and Eve have 10-bit A/D’s. Lower curve: Bob has 10-bit A/D while Eve has 14-bit A/D (Eve’s A/D is 24 dB better). A maximin secrecy rate of $R_s = 1.2478$ is achieved ($p = 0.4$).
Numerical results:

Secret rate vs. SNR at Bob, Eve has perfect access to the signal

Noisy main channel, noiseless eavesdropper’s channel:
Both use 10-bit A/D’s, the ratio between the two power levels at the transmitter is $r = 10^3$, and the average transmitting power $P = 1$. 
The proposed method vs. public discussion:

SNR at Bob’s receiver is 60 dB, Both use 10-bit A/D’s, the ratio between the two power levels at the transmitter is $r = 10^3$, and the average transmitting power $P = 1$. 
The proposed method vs. public discussion:

SNR at Bob’s receiver is 60 dB, Both use 10-bit A/D’s, the ratio between the two power levels at the transmitter is \( r = 10^3 \), and the average transmitting power \( P = 1 \).
The proposed method vs. public discussion:

SNR at Bob’s receiver is 60 dB. Both use 10-bit A/D’s, the ratio between the two power levels at the transmitter is $r = 10^3$, and the average transmitting power $P = 1$. SNR at Bob’s receiver is 80 dB.
Conclusion and future work:
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.
- A simple power modulation instantiation of the approach is investigated.
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.

- A simple power modulation instantiation of the approach is investigated.

- In the case of an advantaged eavesdropper, the secrecy rates that can be achieved using our proposed method are substantially higher than public discussion.
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.
- A simple power modulation instantiation of the approach is investigated.
- In the case of an advantaged eavesdropper, the secrecy rates that can be achieved using our proposed method are substantially higher than public discussion.
- Even in the case that the adversary is able to pick up the transmitter’s radio (i.e. Eve has perfect access to the output of the transmitter), a positive secrecy rate is achievable at high SNRs.
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.

- A simple power modulation instantiation of the approach is investigated.

- In the case of an advantaged eavesdropper, the secrecy rates that can be achieved using our proposed method are substantially higher than public discussion.

- Even in the case that the adversary is able to pick up the transmitter’s radio (i.e. Eve has perfect access to the output of the transmitter), a positive secrecy rate is achievable at high SNRs.

- Risk: asymmetric capabilities at the receivers.
  - Applying a gain with a continuous pdf.
  - Drawing the signal warping from a class of nonlinearities.
  - Adding memory to the signal warping process.
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.

- A simple power modulation instantiation of the approach is investigated.

- In the case of an advantaged eavesdropper, the secrecy rates that can be achieved using our proposed method are substantially higher than public discussion.

- Even in the case that the adversary is able to pick up the transmitter’s radio (i.e. Eve has perfect access to the output of the transmitter), a positive secrecy rate is achievable at high SNRs.

- Risk: asymmetric capabilities at the receivers.
  - Applying a gain with a continuous pdf.
  - Drawing the signal warping from a class of nonlinearities.
  - Adding memory to the signal warping process.
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.

- A simple power modulation instantiation of the approach is investigated.

- In the case of an advantaged eavesdropper, the secrecy rates that can be achieved using our proposed method are substantially higher than public discussion.

- Even in the case that the adversary is able to pick up the transmitter’s radio (i.e. Eve has perfect access to the output of the transmitter), a positive secrecy rate is achievable at high SNRs.

- Risk: asymmetric capabilities at the receivers.
  - Applying a gain with a continuous pdf.
  - Drawing the signal warping from a class of nonlinearities.
  - Adding memory to the signal warping process.

Cryptography: hardness of the problem and the current/future computational capabilities of Eve.

Information-theoretic security: Quality of the channel to Eve (limitations on her location).
Conclusion and future work:

- Exploiting a short-term cryptographic key to force different orderings of two operators at Bob and Eve (one is necessarily non-linear) to obtain secrecy.

- A simple power modulation instantiation of the approach is investigated.

- In the case of an advantaged eavesdropper, the secrecy rates that can be achieved using our proposed method are substantially higher than public discussion.

- Even in the case that the adversary is able to pick up the transmitter’s radio (i.e. Eve has perfect access to the output of the transmitter), a positive secrecy rate is achievable at high SNRs.

- Risk: asymmetric capabilities at the receivers.

- Cryptography: hardness of the problem and the current/future computational capabilities of Eve.

- Information-theoretic security: Quality of the channel to Eve (limitations on her location).

- In the proposed method: Eve’s current conversion hardware capabilities.
  - Applying a gain with a continuous pdf.
  - Drawing the signal warping from a class of nonlinearities.
  - Adding memory to the signal warping process.