Cryptographic Side-Channel Signaling and Authentication via Fingerprint Embedding

*Brian M. Sadler*
*ARL*

Ack: P. Yu, G. Verma (ARL), R. Blum, J. Perazzone (Lehigh)

GlobalSIP’18
27 Nov 2018
Introduction

Fingerprinting & Data Hiding
Fingerprinting

Intrinsic Fingerprint

- A characteristic that identifies
- Uniqueness as a realization of a random process

Exploit inherent randomness to develop measures of uniqueness

- Biometrics:
  - fingerprints, iris scan, DNA, voice, behavioral patterns, ...
- Devices:
  - Printers, cameras, scanners, microphones, recorders
  - Radios, emitters, amplifiers, waveforms
- Media:
  - Paper, canvass

Desired Fingerprint Properties

- Unique, measurable (convenient & technically feasible)
- Robust to measurement noise
- Develop modeling to assess statistical reliability of ID
Fingerprint Embedding by Design

**Purposefully embed fingerprint** for unique ID
• Defeat cloning (impersonation), tampering

**Device Manufacturing**
• Many forms for devices
• Intrinsic to randomness inherent in manufacturing
  Example: transparent material doped with light scattering particles
  Laser illumination yields unique speckle pattern
• Physically Clonable Function (PUF)
  • Challenge-response paradigm for authentication

**Steganography (data hiding)**
• Convey hidden messages (Greek: concealed writing)
• Typically binary data: watermark, copyright
Message Authentication

Classical & PHY-Based
Wireless Communications Authentication

Eavesdropper Problem
- *Encryption* for secrecy
- *Authentication* to verify sender ID

Why Authenticate Messages?
- Verify identity of sender and safeguards message integrity
- Thwart impersonation and substitution attacks

![Diagram showing Alice, Bob, and Eve with shared key and wireless signals]
Classical Authentication

Cryptographic HMAC (Hash-based Message Authentication Codes)

Data $\rightarrow$ Hash Function $\rightarrow$ Tag $\rightarrow$ Append $\rightarrow$ Message

Issues

- Requires additional bandwidth
- Provides data and tag to Eve
- Only provides computational security

Crypto-Hash Properties

• “One-way function” infeasible to invert: requires brute force search

• Deterministic and efficient

• Resistant to collisions: behaves like a random function

• Model: Changing data or key yields random tag
Physical Layer Authentication

Exploit intrinsic physical layer features

• **Device fingerprint ID**
  • ADC, power amplifiers, ...

• **Channel state information (CSI)**
  • Typically: independent time-varying fading provides unique Alice-to-Bob CSI
  • Common source of randomness: Can also provide new secret key
    • Requires reconciliation protocol

• **Issues**
  • Non-tunable
  • Requires favorable channel conditions
  • Uniqueness assumptions

Fingerprint Embedding Authentication

Tag Embedding
Our Approach:

• **Design & Embed cryptographic fingerprint in wireless communications physical layer**

• **Goals:**
  • Secrecy – difficult to detect
  • Security – difficult to estimate and exploit fingerprint
  • Self interference – minimal impact on communications
  • Low complexity – easy to implement

• **Enhances information theoretic security (manage key leakage)**

• **Enhances computational security (raises Eve’s complexity)**

Does not assume:
  Eve’s channel has lower SNR
  Alice knows Eve’s channel
Tag Embedding

Transmitter

Generate Data

Generate Tag

Superimpose

Data

Hash Function

Tag

Receiver

Channel Equalization

Estimate Data

Compare to Received Tag

Key

Generate Expected Tag

Authenticity

\[ X = p_s S + p_t T \]

where \( p_s^2 + p_t^2 = 1 \)

\( p_t \ll p_s \)
Authentication Hypothesis Test

Neyman-Pearson hypothesis test
Authentication via Fingerprint Embedding

- No additional bandwidth
- Symbol synchronous, low complexity

- Many variations possible, e.g.,
  - Coupling with other security methods
  - Nonlinear embedding
SDR SISO Experiment

- Minimal impact of ~1% tag power on receiver BER
SDR SISO Experiment

- Tag power tradeoffs
  - Enhances authentication performance
  - Higher SNR for Eve’s tag estimate
  - Small decrease in Bob’s SNR

![Graph showing probability of authentication versus SNR for various tag powers.](image-url)
MIMO Authentication

• Known channel state info (CSI)

Pre-coding \( X = \gamma_S \mathbf{F}_S \mathbf{P}_S^{\frac{1}{2}} \mathbf{S} + \gamma_T \mathbf{F}_T \mathbf{P}_T^{\frac{1}{2}} \mathbf{T} \)

Received \( Y = \sqrt{g} \mathbf{H} X + \mathbf{W} \)

Residual
\( \hat{Q} = \sqrt{g} \gamma_T \hat{\mathbf{H}} \mathbf{F}_T \mathbf{P}_T^{\frac{1}{2}} \tilde{\mathbf{T}} \)

Test Statistic
\( \tau = \Re \left[ \text{Tr}(\hat{Q}^\dagger Q) \right] \)

Strongest mode only

All modes proportionally

\[ \begin{array}{cccc}
\gamma_T^2 \mathbf{P}_T(1) & \gamma_T^2 \mathbf{P}_T(2) & \gamma_T^2 \mathbf{P}_T(3) & \gamma_T^2 \mathbf{P}_T(4) \\
\gamma_S^2 \mathbf{P}_S(1) & \gamma_S^2 \mathbf{P}_S(2) & \gamma_S^2 \mathbf{P}_S(3) & \gamma_S^2 \mathbf{P}_S(4) \\
n(1) & n(2) & n(3) & n(4) \\
\end{array} \]
MIMO Authentication

4x4 MIMO Simulation:
- 4 x 256 symbols
- Rayleigh fading
- Multi-mode tagging

More detectable for Eve
Security

Key Information Leakage
Key Information Leakage

Conditional Entropy:

- *Equivocation* (calling two different things by the same name)
- Assume Eve knows architecture, parameters, and hash function
  - Zero equivocation in noise free case & if hash is uniquely invertible

\[
H(k|Y, \theta) = \sum_{s \in S, t \in T} p(s, t) H(k|s, t)
\]

\[
H(k|Y) \approx \frac{|\mathcal{K}|}{|\mathcal{T}|} \sum_{i=0}^{\log|\mathcal{T}|} \binom{\log|\mathcal{T}|}{i} H\left(\frac{|\mathcal{T}|}{|\mathcal{K}|} p_e^i (1-p_e)^{\log|\mathcal{T}|-i}\right)
\]

Randomness through Eve’s bit error probability
Key Information Leakage

- **SISO Conditional Entropy (single Tx)**
  Provides insight into key update strategy
Communications in the Side-Channel

Creating a Secret Codebook of Tags
Authentication + Side-Channel Comms

Block Diagram of Multi-Key Authentication System

Transmitter (Alice)
- Generate Data
- Generate Tag
- Generate Side-Data

Receiver (Bob)
- Search for any valid tag
- Authenticate and recover side information
- Generate Secret Codebook
- Estimate Data

Eavesdropper (Eve)
- Key set

Channel
- Superimpose

Communicate via Key Choice
Authentication + Side-Channel Comms

Block Diagram of Multi-Key Authentication System

Test over codebook entries

Authenticates & recovers side-channel symbol
Secret Random Codebook: 2 Designs

0. Key is partitioned into $N_k$ sub-keys

1. Simple Codebook Construction
   - One sub-key per symbol
   - $\log_2 N_k$ bits communicated

2. Linear Codebook Construction
   - $N_k$ possible tags are rows in generator matrix $G$
   - Transmit $m$ by linear combination of possible tags
   - $N_k$ bits communicated

\[
\overline{G} = \begin{bmatrix}
t_1^{\text{valid}} \\ t_2^{\text{valid}} \\ \vdots \\ t_{N_k}^{\text{valid}}
\end{bmatrix}
\]

\[
t_{\text{xmit}} = \frac{m \overline{G}}{N_k} = \sum_{j=1}^{N_k} m_j t_j^{\text{valid}}
\]

Authentication Performance

\[ \Pr \, \text{Decide} \, H_1 | H_1 = \int_{\tau_{1,0}}^{\infty} \Phi^{N_k-1} \left( \frac{z}{\sqrt{\frac{L}{2} + \sigma^2_{\tilde{w}}}} \right) \phi \left( \frac{z - L}{\sigma_{\tilde{w}}} \right) F_{\tau_1}(z) \, dz, \]

WLOG assumes H1 true

\[ \tau_{1,0} \triangleq \tau_1 | H_0 \quad \text{and} \quad F_{\tau_1}(z) = \Pr \, \tau_1 < z \quad \text{is the CDF of} \, \tau_1 \]

Threshold under
H0 is constant

\[ \tau_i | H_j (\neq i) = \min_\tau \quad \text{s.t.} \quad \Pr Z_i(R | H_j) > \tau < \alpha \]

Thresholds are recalculated by Bob for each transmission
(New Random Codebook)
Side Channel Performance: No Data EC Coding

Assumption: Bob correctly reconstructs secret codebook (Primary message obtained without error)
Performance w/ Data Error Correction Coding

Bit error causes random codebook mismatch
Performance w/ Data Error Correction Coding

Performance dominated by packet success rate
Security

Multi-Key Codebook Scheme
Key Information Leakage

Conditional Entropy:

\[ H(k|Y, \theta) = \sum_{s \in S, t \in T} p(s, t) H(k|s, t) \]

\[ H(k|Y^n, \theta) \approx \frac{|\mathcal{K}|}{|\mathcal{T}|} \left( \frac{N}{N_k} \log_2 |\mathcal{T}| \right) \sum_{i=0}^{\frac{N}{N_k}} \binom{\frac{N}{N_k}}{i} H \left( \frac{|\mathcal{T}|}{|\mathcal{K}|} p_e^i (1 - p_e)^{\frac{N}{N_k} \log_2 |\mathcal{T}| - i} \right) \]

Computational Security:

Multi-key attribution problem increases Eve’s search space
Much worse for linear codebook
Key Leakage

256 Bit Tags/Keys, SNR = 15dB, 16-QAM, Tag Power = .001

Simple Codebook
Assume Eve knows key assignment

Eve needs more observations to obtain information about a sub-key
Security - Performance Trade-off: Side-Channel Success vs Key Leakage

![Graph showing the relationship between performance and security with varying SNR from 4 to 14 dB.](image)

- **Parameter**
- **Value**
- **Description**
  - $L$
  - 1024
  - Number of Symbols
  - $p_t^2$
  - .001
  - Tag Power
  - $\gamma$
  - $10^{-4}$
  - False Alarm Probability
  - $\gamma$
  - 4-16 dB
  - Receiver SNR
  - $N_k$
  - 16,64,512
  - Number of Keys
  - 16-QAM
  - Modulation Scheme

Vary SNR 4 to 14 dB
Conclusion

• Design framework yields good tradeoffs in secrecy, security, self-interference, and complexity

Going Further:
• Couple approach with PHY layer encryption & jamming, active & passive techniques
  • MIMO, directional modulation, beamforming

• Networking & broadcast authentication
• Key evolution using the side-channel
References


END
Contact

- Brian Sadler, brian.m.sadler6.civ@mail.mil
- Army Research Laboratory, Adelphi, MD 20783
- 301-394-1239