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

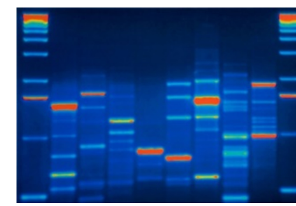
Fingerprinting

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

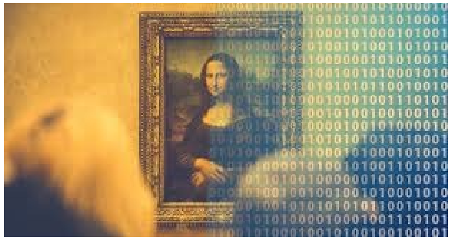
- Defeat cloning (impersonation), tampering

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

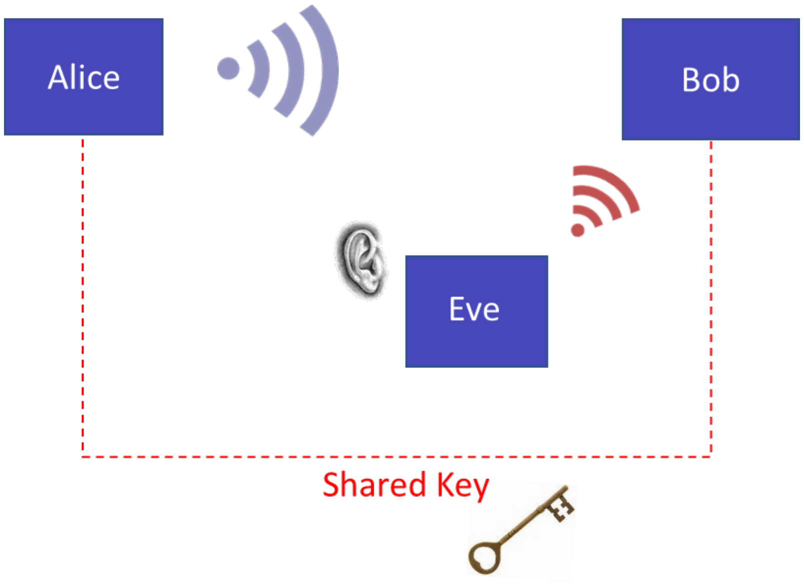
Wireless Communications Authentication

Eavesdropper Problem

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

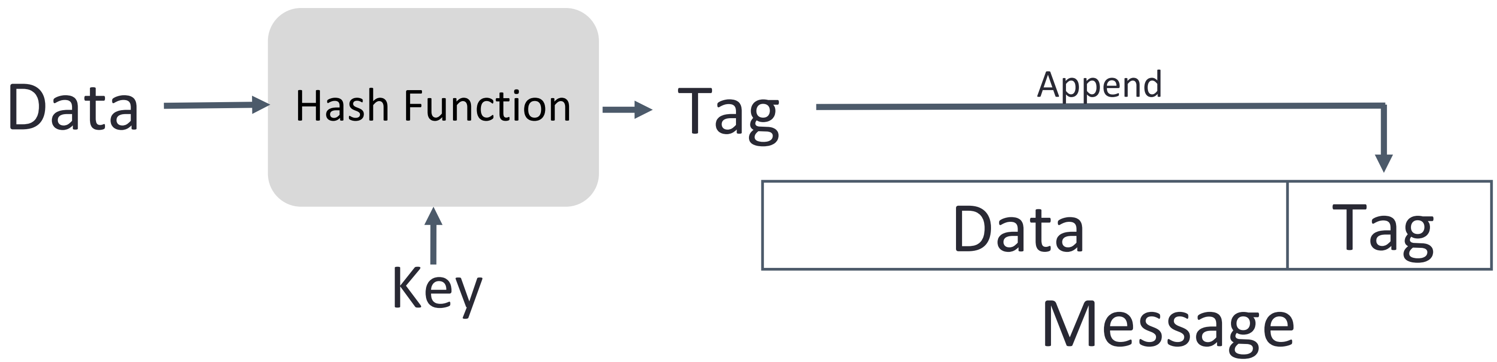
Why Authenticate Messages?

- Verify identity of sender and safeguards message integrity
- Thwart impersonation and substitution attacks



Classical Authentication

Cryptographic HMAC (Hash-based Message Authentication Codes)



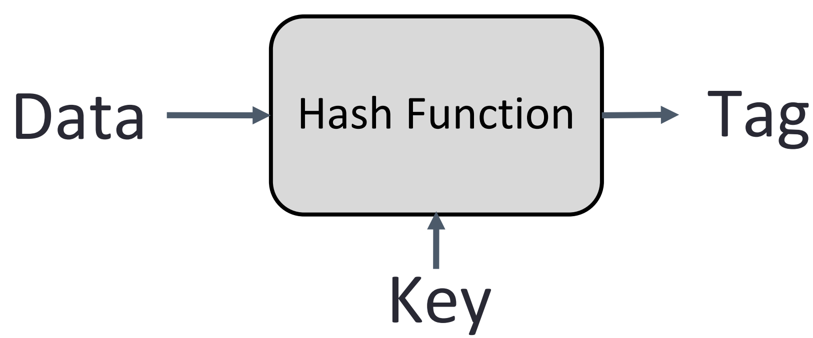
Issues

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

A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

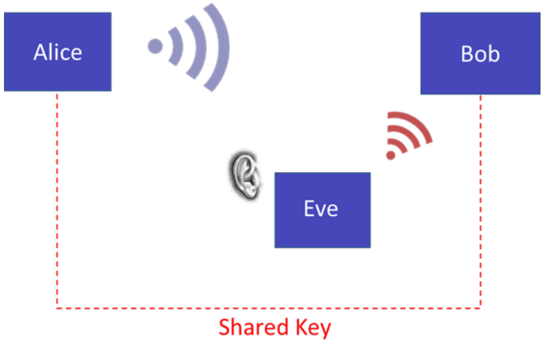
Crypto-Hash Properties

- "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

Polak, Dolatshahi, Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE JSAC*, 2011.
Xiao, Greenstein, Mandayam, Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE TWC*, 2008.
Wang, Hao, Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Comm Mag*, 2016.

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)

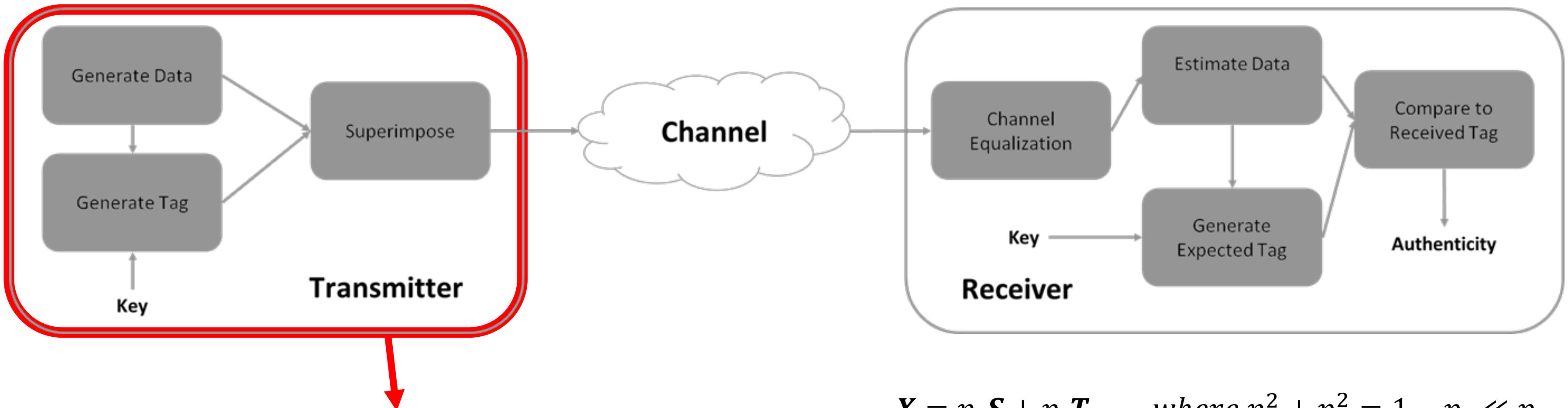
- Enhances computational security (raises Eve’s complexity)

Does not assume:

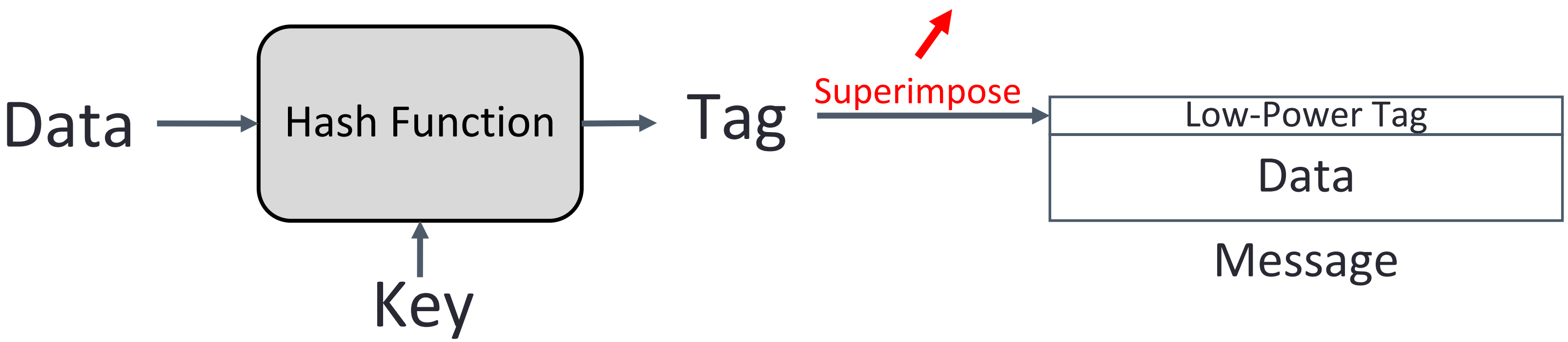
Eve’s channel has lower SNR

Alice knows Eve’s channel

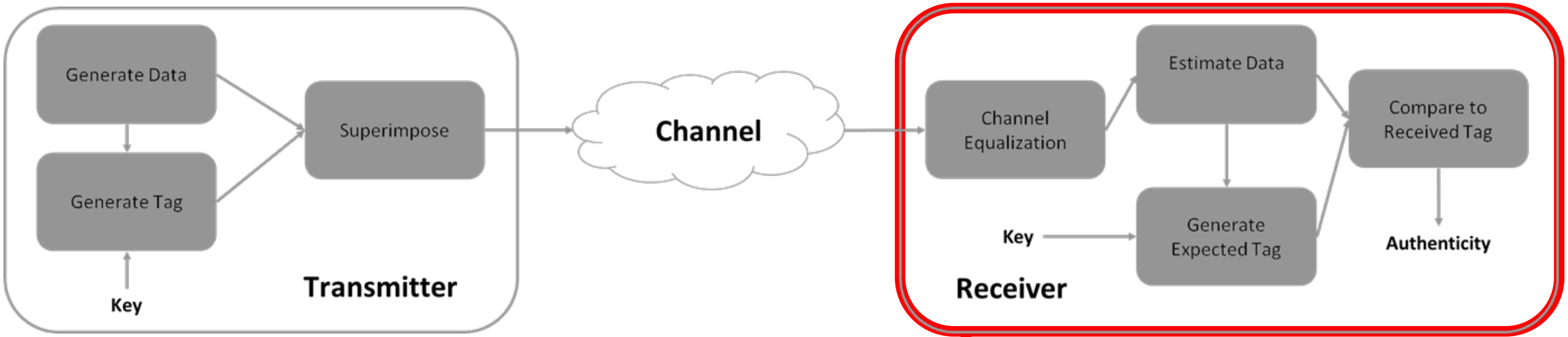
Tag Embedding

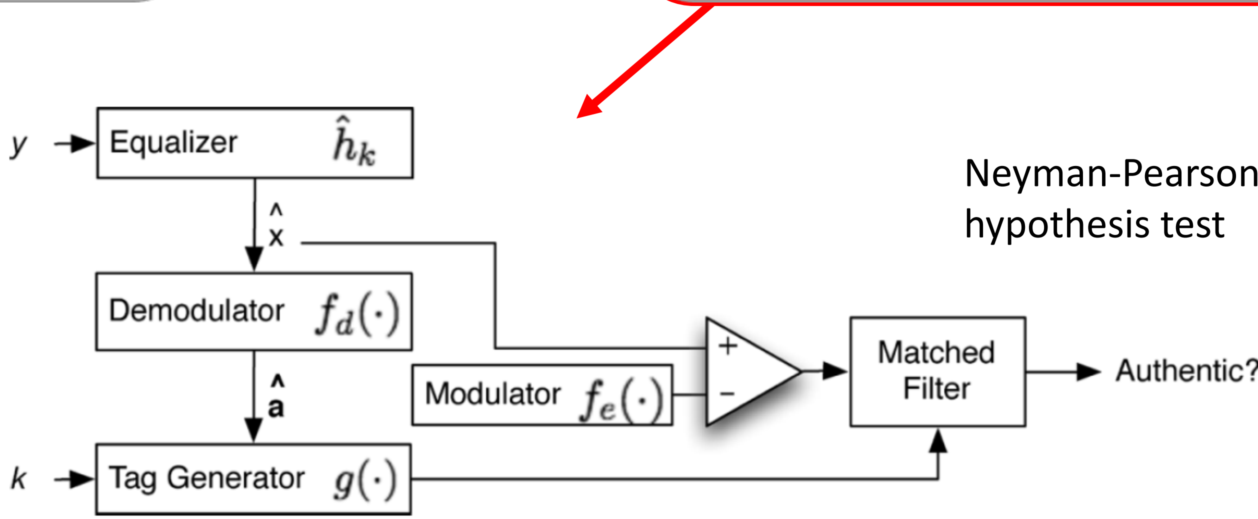


$$\boldsymbol{X} = p_s\boldsymbol{S} + p_t\boldsymbol{T} \qquad where\ p_s^2 + p_t^2 = 1 \quad p_t \ll p_s$$



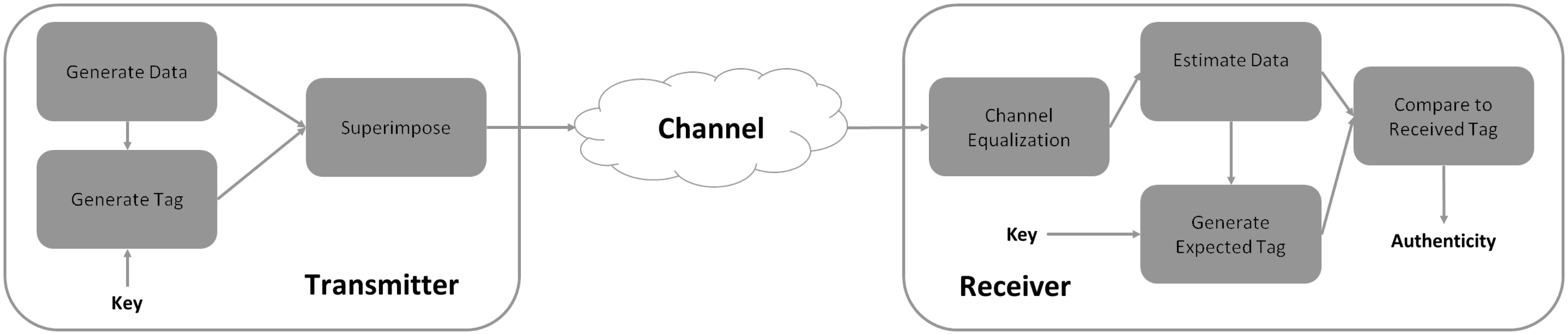
Authentication Hypothesis Test





Neyman-Pearson hypothesis test

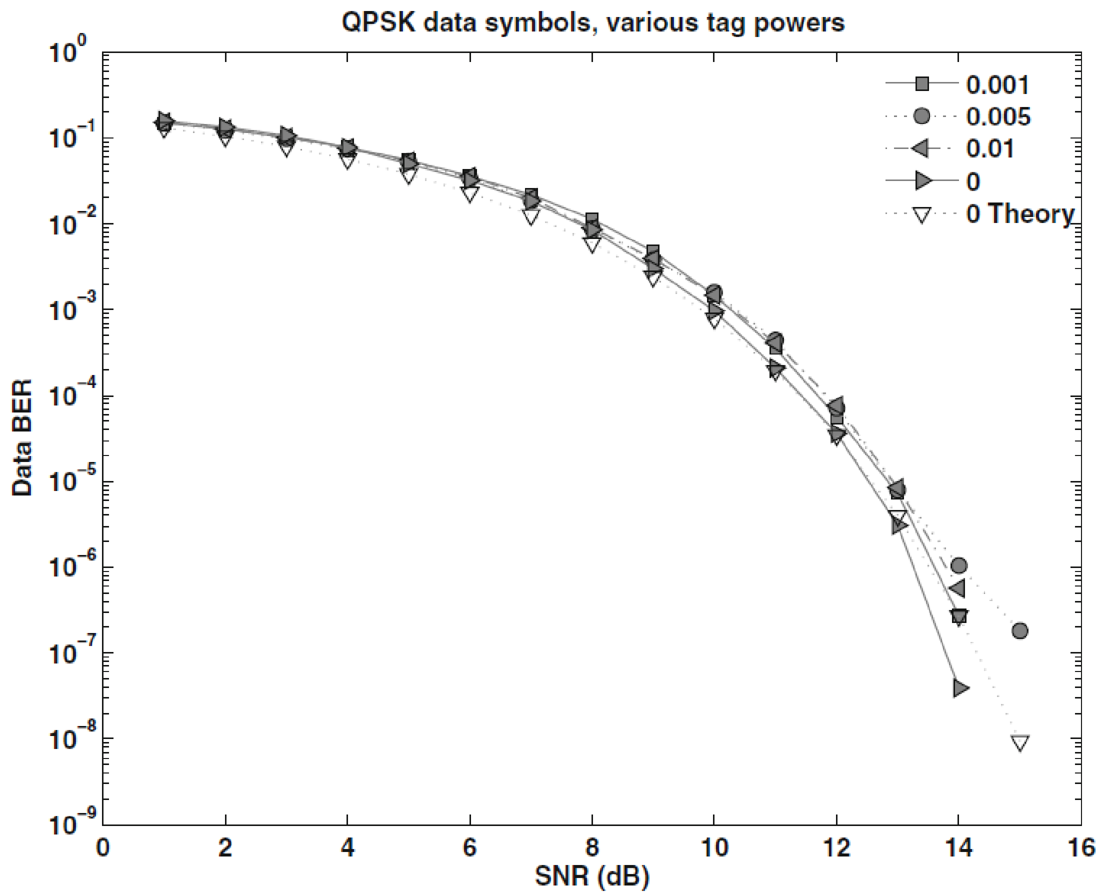
Authentication via Fingerprint Embedding



- 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

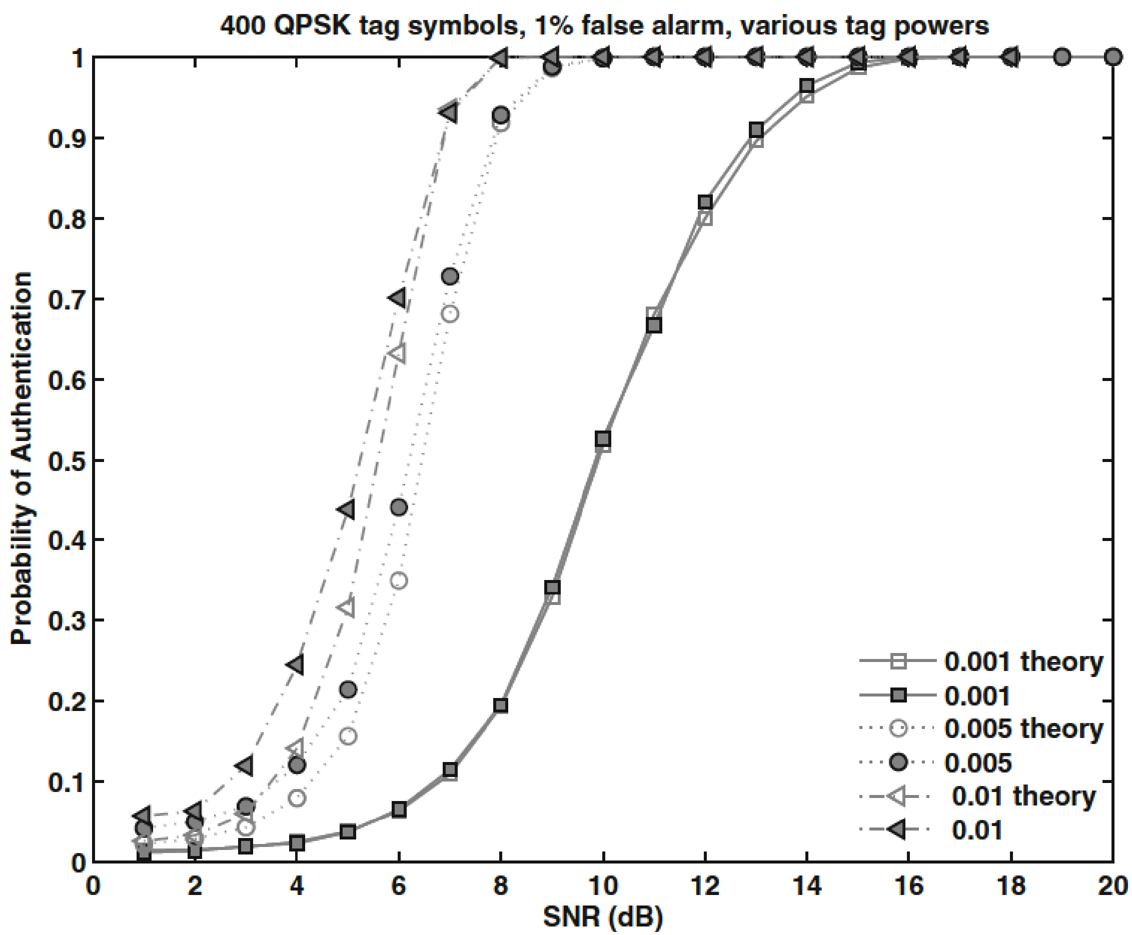


SDR SISO Experiment

- Tag power tradeoffs
  - Enhances authentication performance

  versus

  - Higher SNR for Eve's tag estimate
  - Small decrease in Bob's SNR



MIMO Authentication

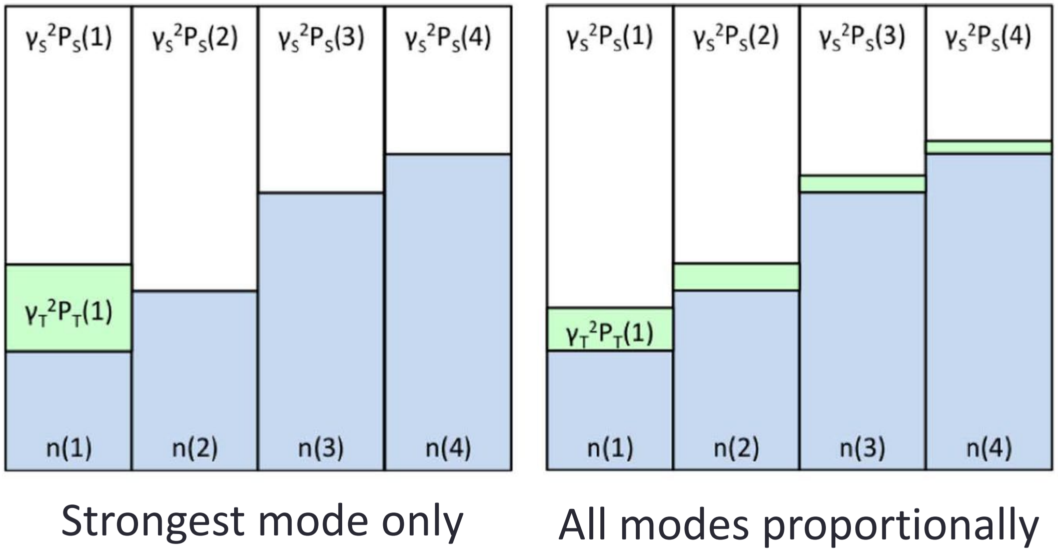
- Known channel state info (CSI)

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

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

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

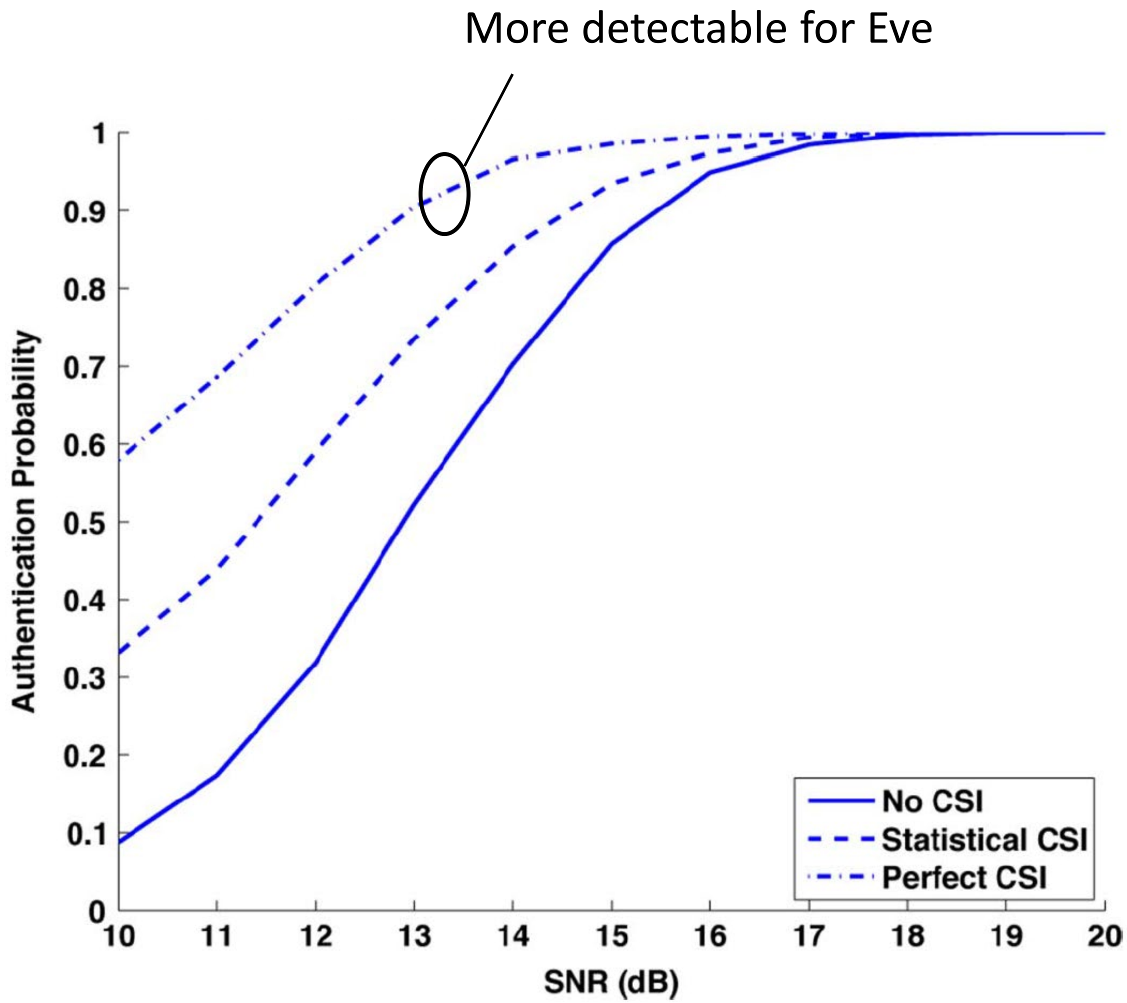
Test Statistic
$$\tau = \Re[\mathrm{Tr}(\hat{\mathbf{Q}}^\dagger \mathbf{Q})]$$



MIMO Authentication

4x4 MIMO Simulation:

- 4 x 256 symbols
- Rayleigh fading
- Multi-mode tagging



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

$$H(\boldsymbol{k}|\boldsymbol{Y},\theta) = \sum_{s\in\mathcal{S},t\in\mathcal{T}} p(\boldsymbol{s},\boldsymbol{t})H(\boldsymbol{k}|\boldsymbol{s},\boldsymbol{t})$$

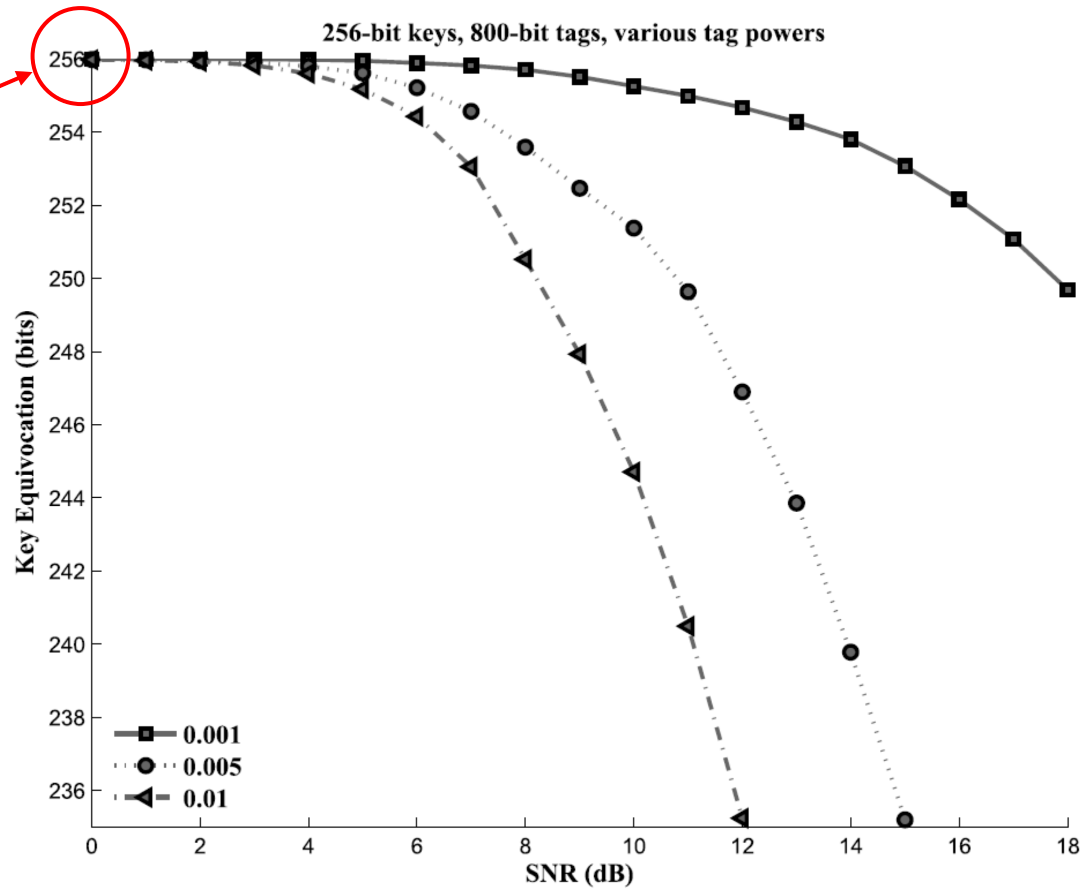
$$H(k|Y) \approx \frac{|\mathcal{K}|}{|\mathcal{T}|} \sum_{i=0}^{\log|\mathcal{T}|} \binom{\log|\mathcal{T}|}{i} H\left(\frac{|\mathcal{T}|}{|\mathcal{K}|} p_e^i (1-p_e)^{\log|\mathcal{T}|-i}\right)$$

Randomness through Eve's bit error probability

Key Information Leakage

- SISO Conditional Entropy (single Tx)
  Provides insight into key update strategy

Key entropy

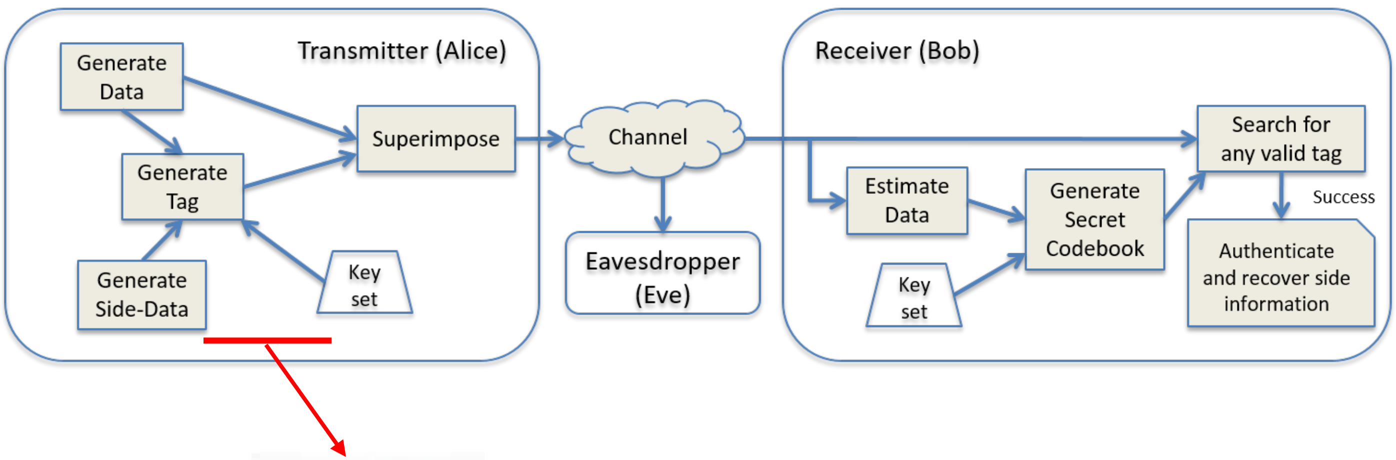


Communications in the Side-Channel

Creating a Secret Codebook of Tags

Authentication + Side-Channel Comms

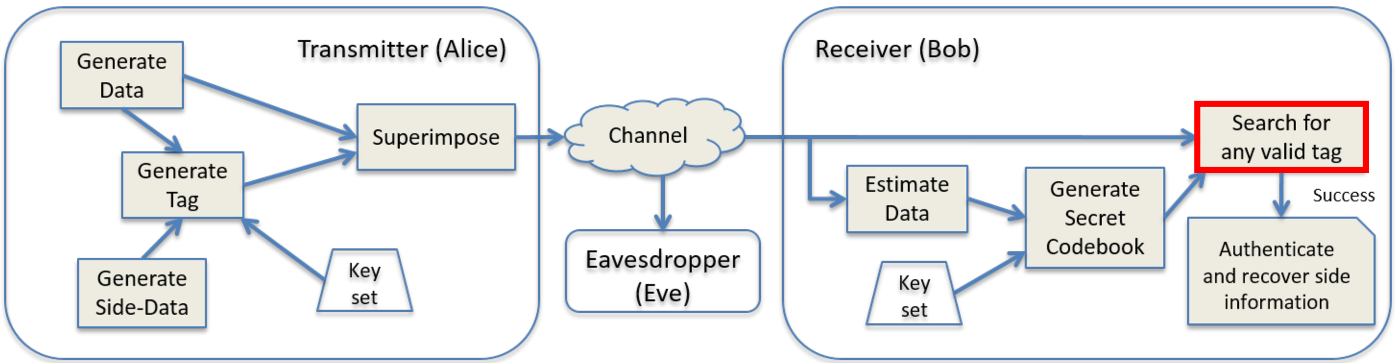
Block Diagram of Multi-Key Authentication System



Communicate via Key Choice

Authentication + Side-Channel Comms

Block Diagram of Multi-Key Authentication System



Test over codebook entries

$$\begin{cases} H_0 & \text{No valid tag was sent} \\ H_1 & t_1^{\text{valid}} \text{ was sent}, m = 1 \\ \vdots & \\ H_{N_k} & t_{N_k}^{\text{valid}} \text{ was sent}, m = N_k \end{cases}$$

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**

$$\overline{\mathbf{G}} = \begin{bmatrix} \mathbf{t}_1^{\text{valid}} \\ \mathbf{t}_2^{\text{valid}} \\ \vdots \\ \mathbf{t}_{N_k}^{\text{valid}} \end{bmatrix}$$

$$t^{\text{xmit}} = \mathbf{m}\overline{\mathbf{G}} = \sum_{j=1}^{N_k} \mathbf{m}_j \mathbf{t}_j^{\text{valid}}$$

Perazzone, Yu, Sadler,Blum "Cryptographic Side-Channel Signaling and Authentication via Fingerprint Embedding," *IEEE TIFS, 2018.*

Authentication Performance

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

WLOG assumes H1 true

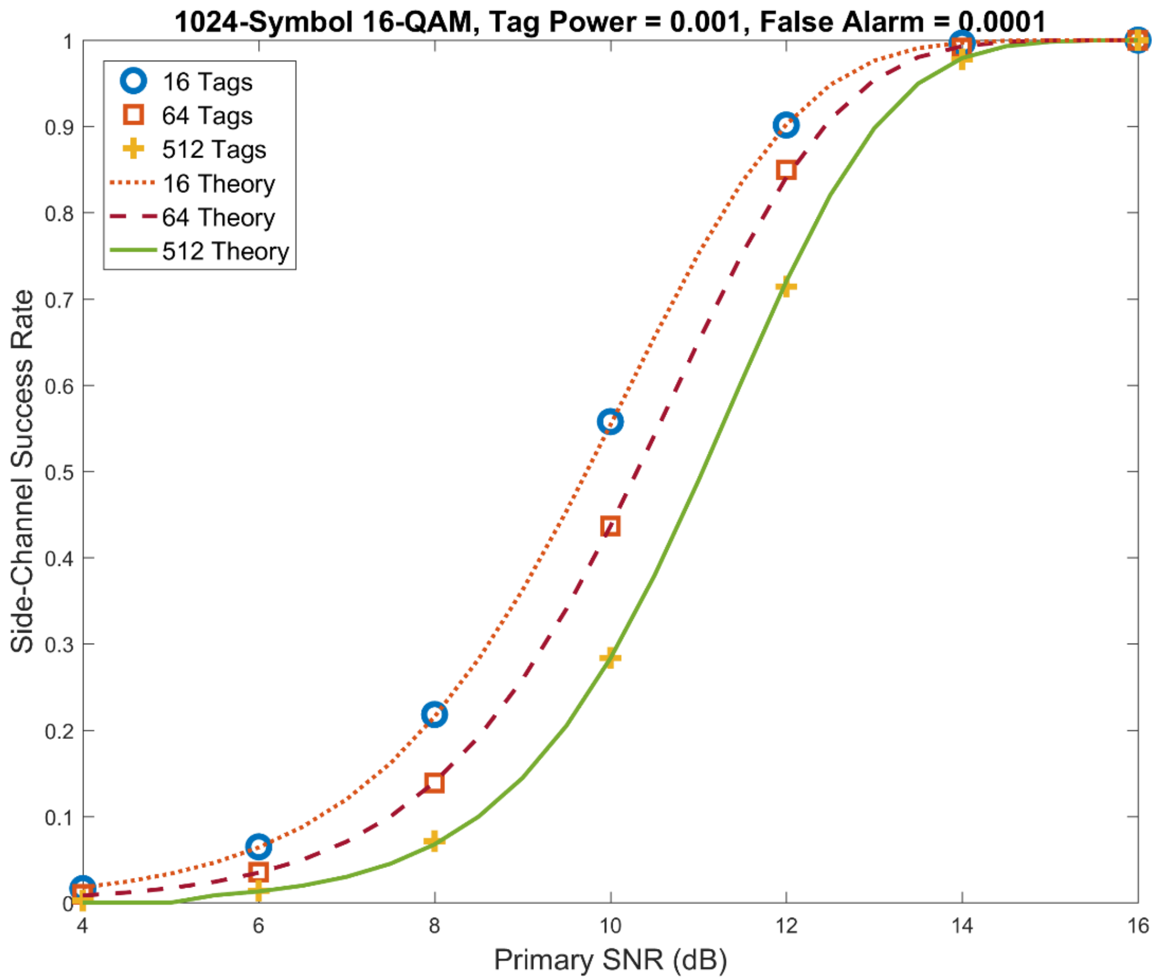
$$\tau_{1,0} \triangleq \tau_1 | H_0 \text{ and } F_{\tau_1}(z) = \Pr \tau_1 < z \text{ is the CDF of } \tau_1$$

Threshold under
H0 is constant

$$\tau_i | H_{j(\neq i)} = \min_{\tau} \text{ s.t. } \Pr Z_i(R|H_j) > \tau < \alpha$$

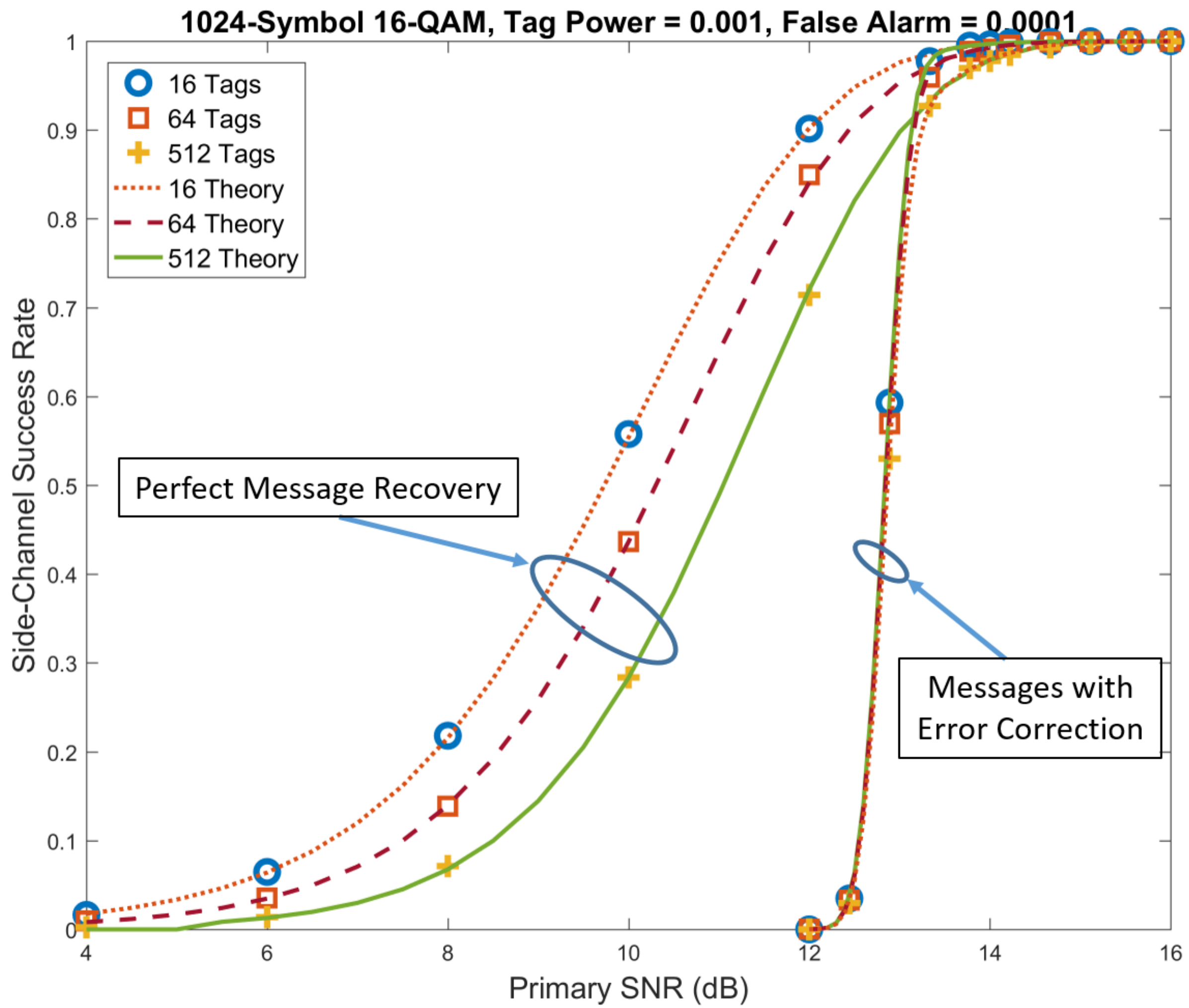
Thresholds are recalculated by Bob for each transmission
(New Random Codebook)

Side Channel Performance: No Data EC Coding



Assumption: Bob correctly reconstructs secret codebook
(Primary message obtained without error)

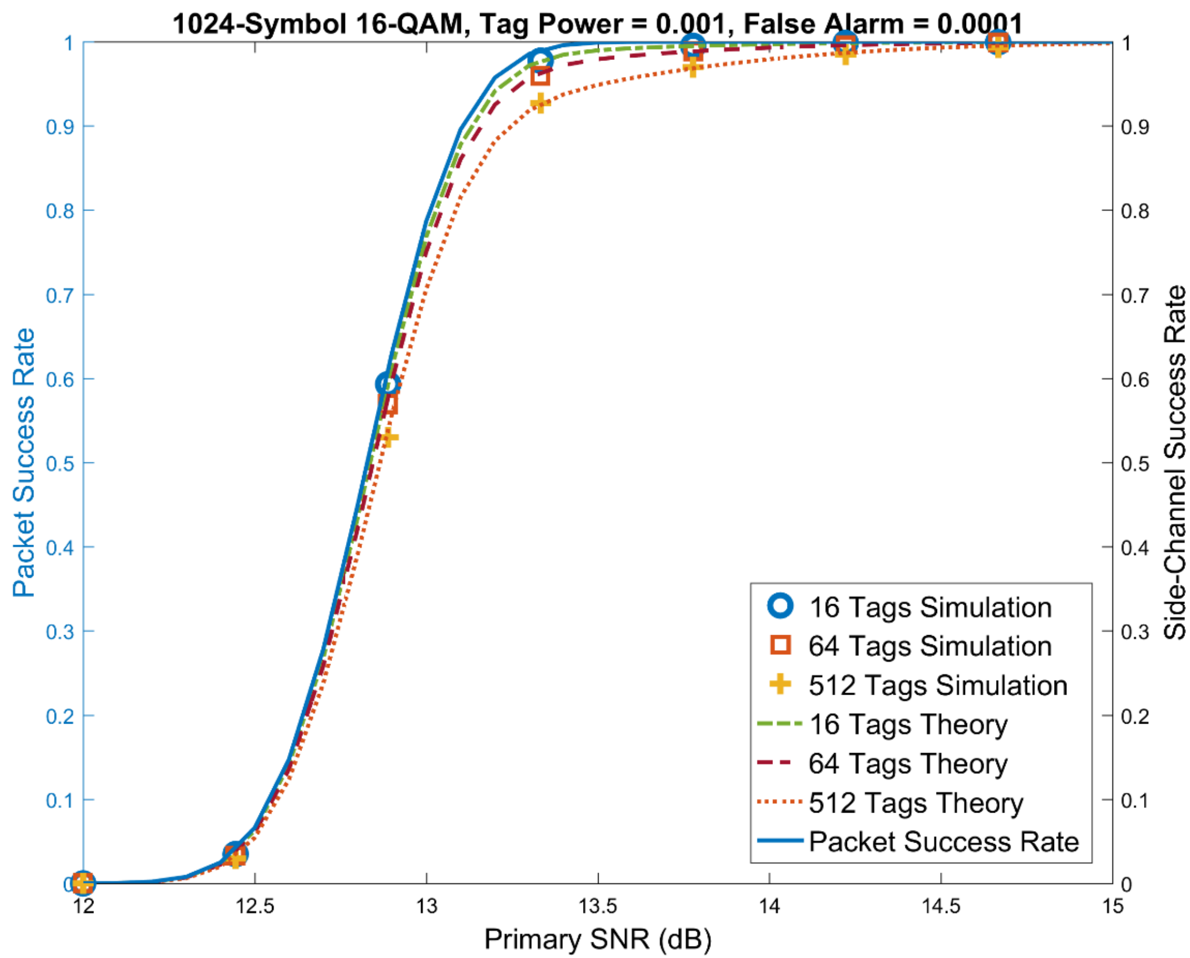
Performance w/ Data Error Correction Coding



BCH: 10 bit EC
512 block

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:

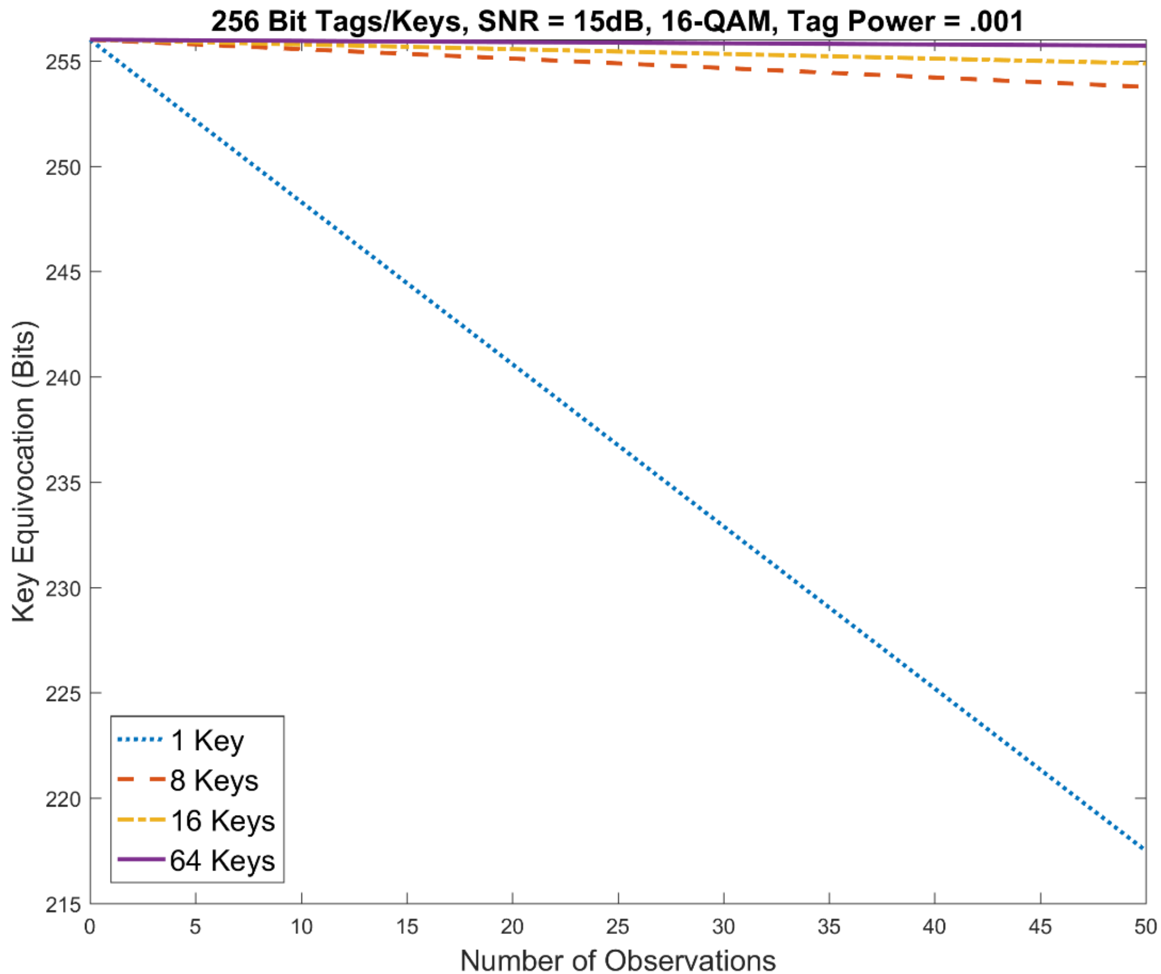
$$H(\boldsymbol{k}|\boldsymbol{Y},\theta) = \sum_{\boldsymbol{s}\in\mathcal{S},\boldsymbol{t}\in\mathcal{T}} p(\boldsymbol{s},\boldsymbol{t})H(\boldsymbol{k}|\boldsymbol{s},\boldsymbol{t})$$

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

Computational Security:

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

Key Leakage

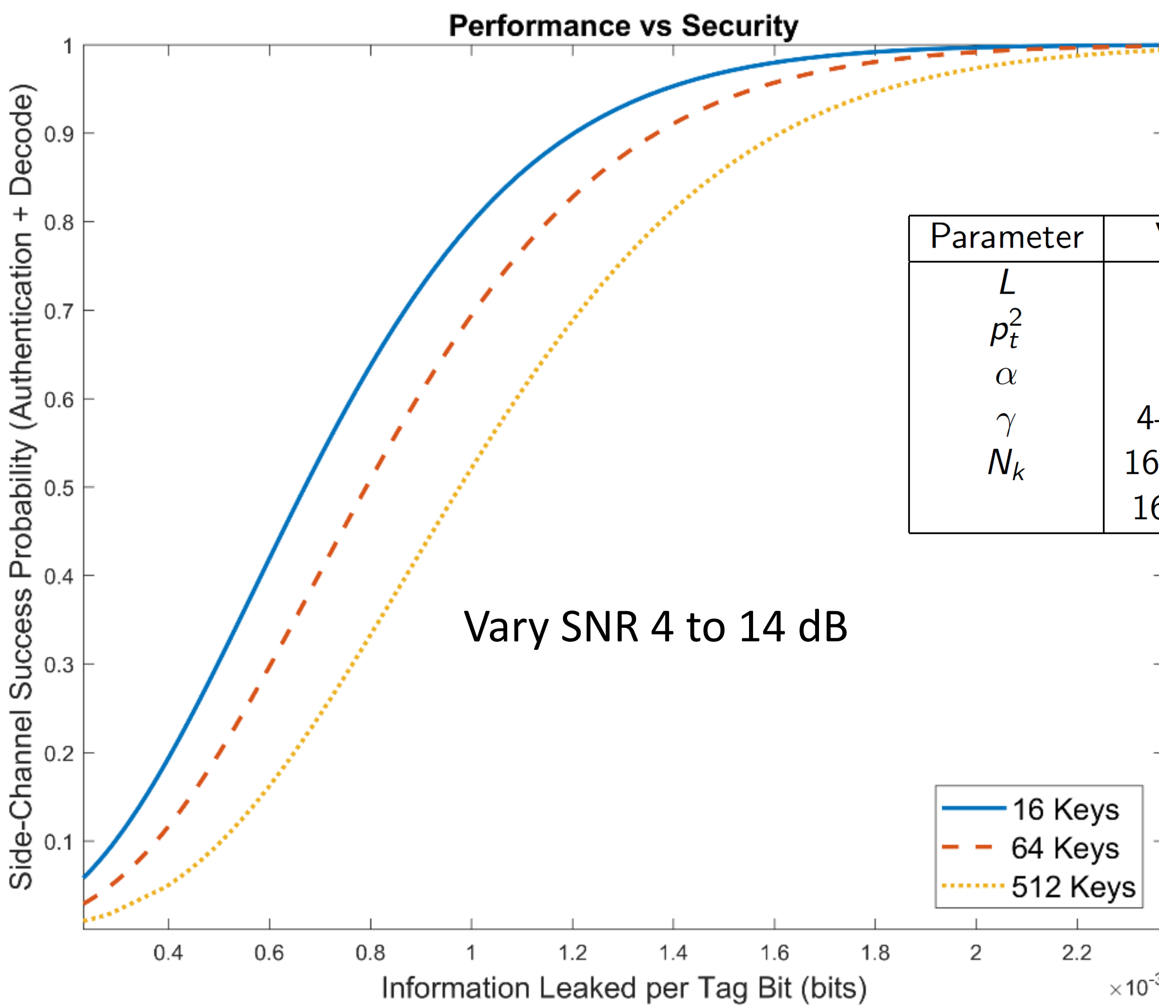


Simple Codebook

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



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

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

- J. B. Perazzone, P. L. Yu, B. M. Sadler, R. S. Blum, “Cryptographic side-channel signaling and authentication via fingerprint embedding,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2216--2225, 2018.
- P. L. Yu, B. M. Sadler, G. Verma, J. S. Baras, “Fingerprinting by design: embedding and authentication,” in Digital Fingerprinting (Springer, 2016), C. Wang, R. M. Gerdes, Y. Guan, S. K. Kasera, editors.
- P. L. Yu, G. Verma, B. M. Sadler, “Wireless physical layer authentication via fingerprint embedding,” *IEEE Communications Magazine, special issue on Wireless Physical Layer Security*, pp. 48--53, June 2015.

END

Contact

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