

# Physical-Layer Security and EXIT Analysis for Fast-Correlation Attacks on LFSR-Based Stream Ciphers

*Willie K Harrison*  
*Steven W. McLaughlin*

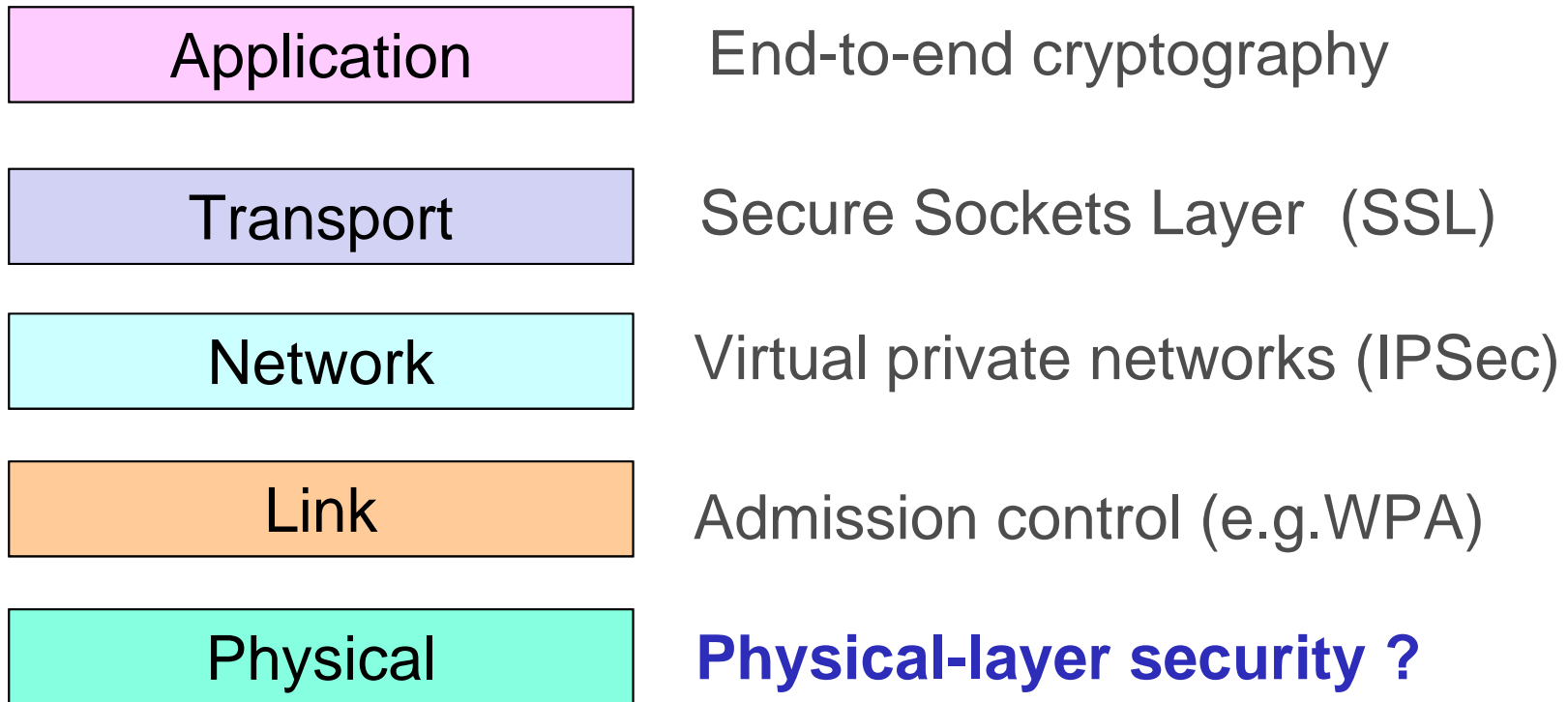
*School of Electrical and Computer Engineering*  
*Georgia Institute of Technology*  
*Atlanta, GA USA*

**[harrison.willie@gatech.edu](mailto:harrison.willie@gatech.edu)**  
**[steven.mclaughlin@provost.gatech.edu](mailto:steven.mclaughlin@provost.gatech.edu)**

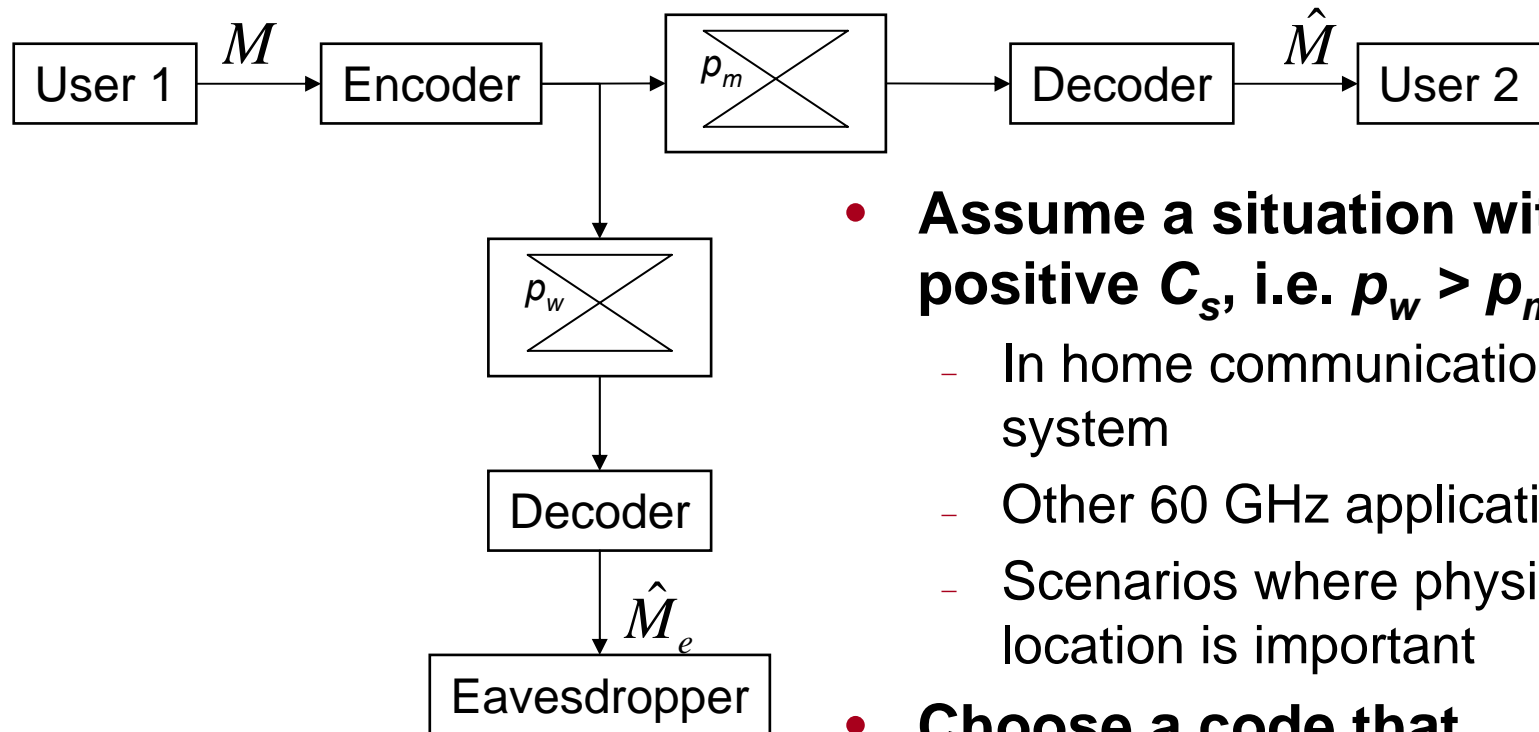


# Layered Communication Architecture

---



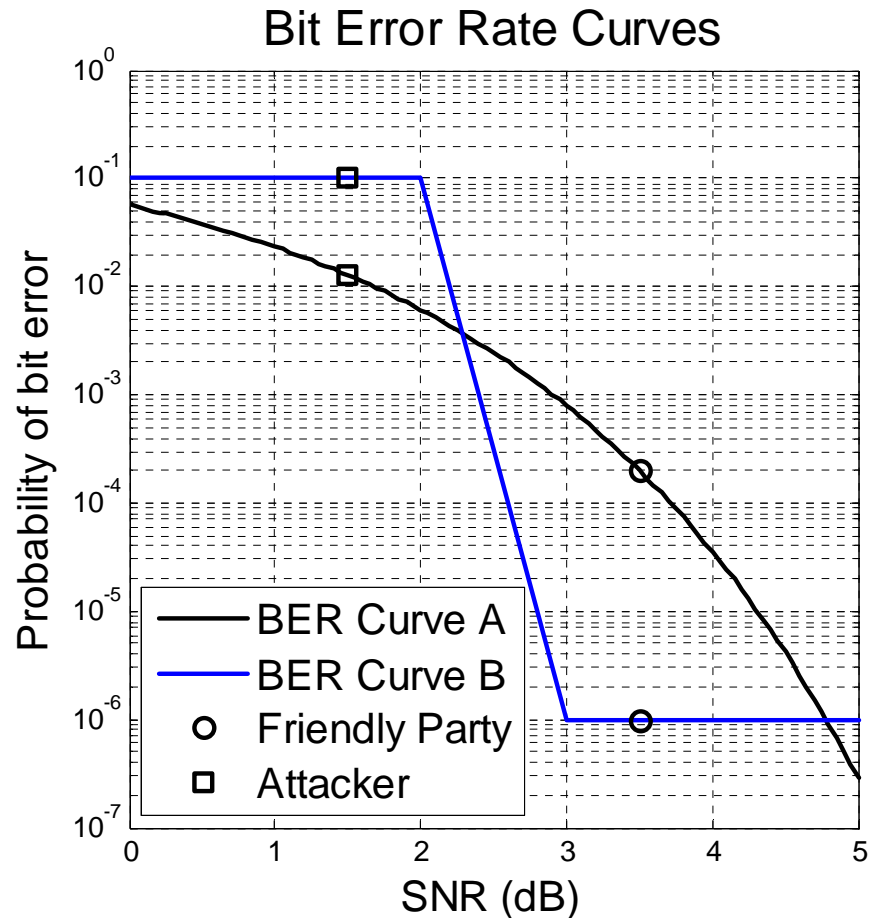
# Wire-tap Channel Model



- **Assume a situation with positive  $C_s$ , i.e.  $p_w > p_m$** 
  - In home communication system
  - Other 60 GHz applications
  - Scenarios where physical location is important
- **Choose a code that exploits this advantage over the eavesdropper.**

# Codes that Yield Physical-Layer Security

- Choose a code with a sharp waterfall or cliff region in BER curve.
- Attempt to force some percentage of bit errors in an eavesdropper's data stream following channel decoding.
- For examples of such codes, see [1], [2], and [3] as well as Demijan Klinc's presentation on Thursday.



[1] V. K. Wei. Generalized Hamming weights for linear codes. *Information Theory, IEEE Transactions on*, 37(5):1412–1418, Sep 1991.

[2] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J-M. Merolla. Applications of LDPC codes to the wiretap channel. *Information Theory, IEEE Transactions on*, 53(8):2933–2945, Aug 2007.

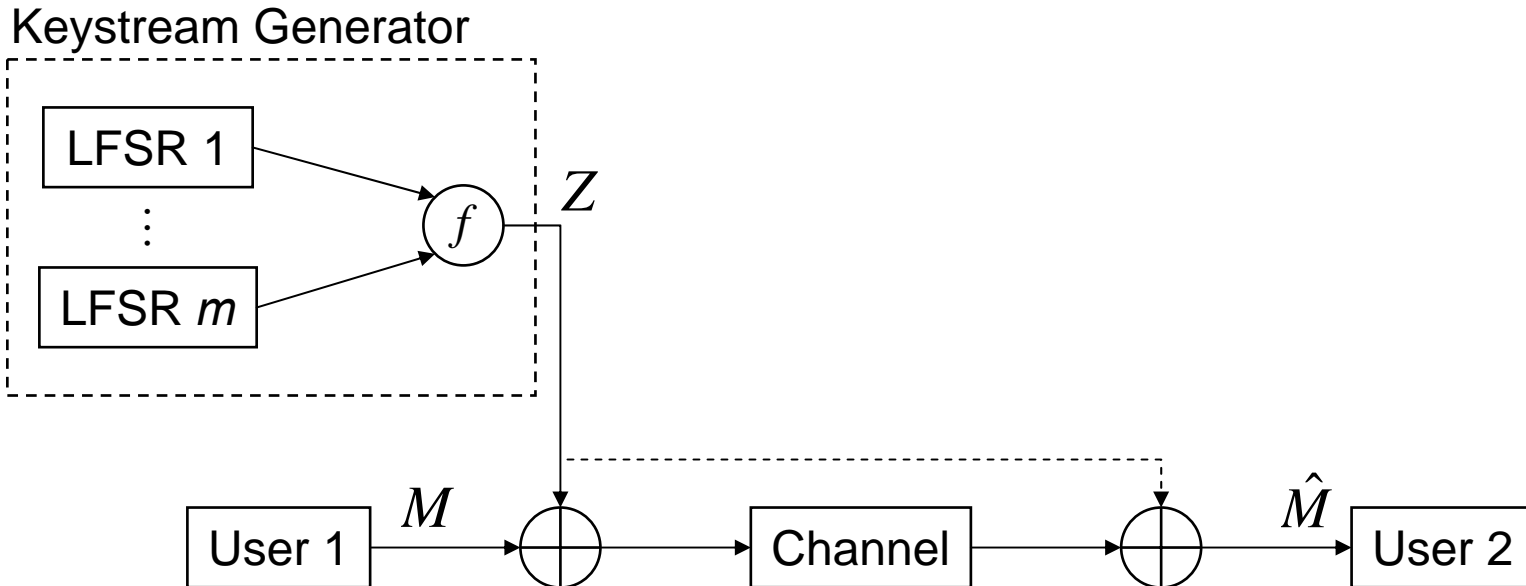
[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *Information Theory, IEEE Transactions on*, 54(6):2515–2534, June 2008.

# Problem Statement & Previous Work

---

- **The problems we want to solve**
  - How do channel errors translate to additional complexity requirements for an eavesdropper to crack cryptographic systems?
  - How do we characterize or quantify additional security due to the physical layer?
  - What can we learn from mutual information in a cryptographic attack?
- **Previous Work**
  - André Zúquete and João Barros, “Physical-Layer Encryption with Stream Ciphers”, in *Proc. Of the IEEE Int. Symp. On Inf. Theory (ISIT’08)*, Toronto, Canada, July 2008.
    - Interchanged encoding and encryption for physical-layer security.
  - Typically cryptographic systems are analyzed assuming the eavesdropper knows the ciphertext exactly.

# Approximating the One-Time Pad



- **Key length is fixed regardless of  $M$ .**
- **Structure of keystream can be exploited by attacker.**
- **LFSR generator polynomials assumed to be primitive in physical-layer security setting.**

# Attacks on LFSR-Based Crypto

---

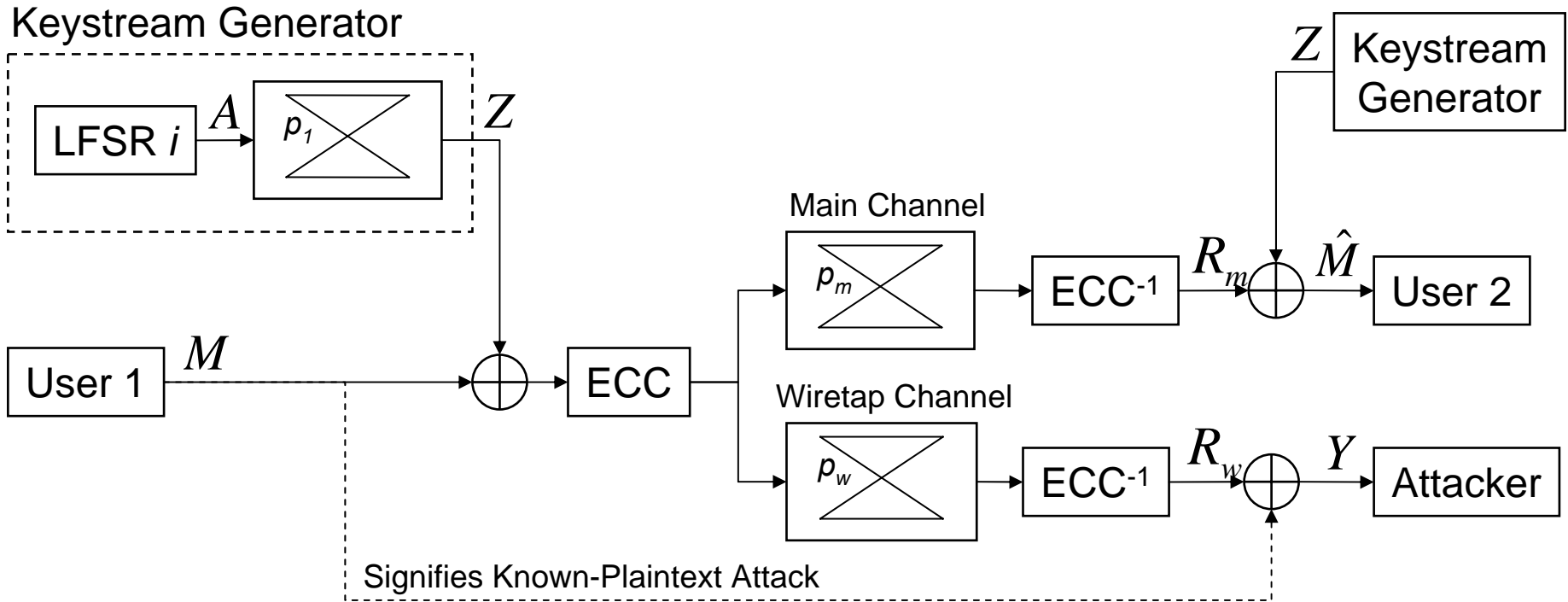
- **Goal of Attackers: Find the initial contents of each LFSR (secret key)**
- **Assumptions made in well-known attacks:**
  - LFSR structure is known by the attacker.
  - All LFSR connection polynomials are primitive.
  - Output of the  $i$ th LFSR  $A$  is correlated with output of keystream generator  $Z$  (correlation attacks).
  - The first  $N$  bits of plaintext are known to an attacker (not necessary, see [4]).
- **Two fast correlation attacks from [5] are analyzed.**
  - Attack 1: noniterative attack.
  - Attack 2: iterative attack similar to LDPC decoding [6].

[4] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. Computers, IEEE Transactions on, C-34(1):81–85, Jan 1985.

[5] W. Meier and O. Staffelbach. Fast correlation attacks on certain stream ciphers. Journal of Cryptology, 1:159–176, 1989.

[6] R. G. Gallager. Low-Density Parity-Check Codes. MIT Press, Cambridge, MA, 1963.

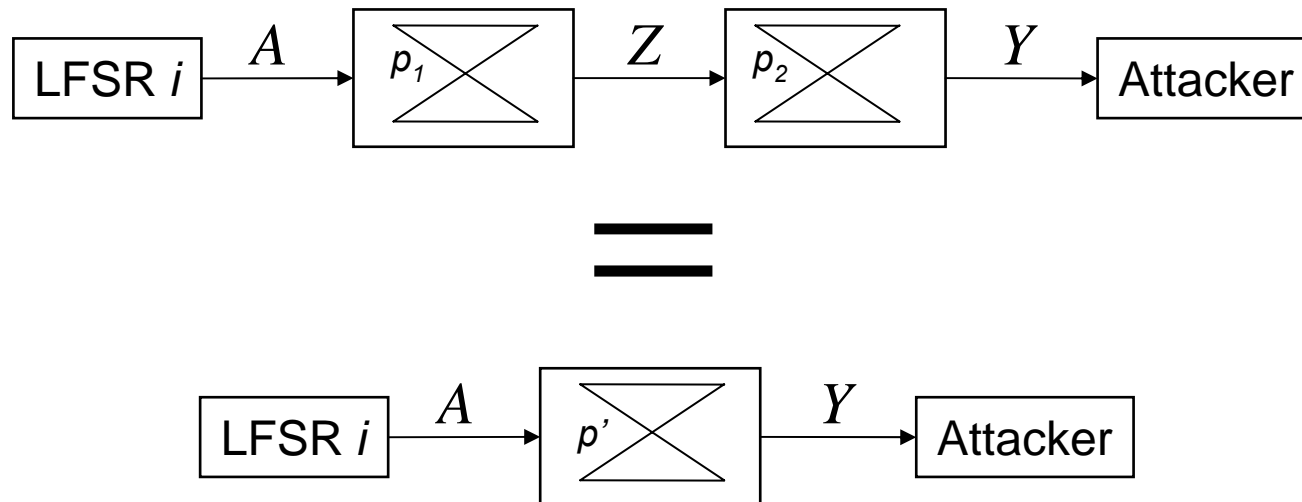
# Combined System



$$Y = R_w + M = Z + E_w + 2M = Z + E_w = A + E_1 + E_w.$$

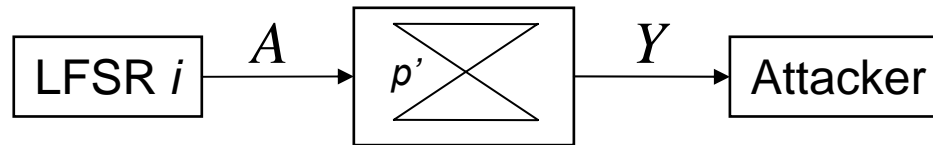
# Eavesdropper's Perspective

- $Y = A + E_1$ : gives traditional noise-free attack model.
- $Y = A + E_1 + E_w = A + E$ , where  $E = E_1 + E_w$ : gives model assuming errors due to the physical layer.



- $p' = p_1(1-p_2) + p_2(1-p_1) = p_1 + p_2 - 2p_1p_2.$

# Mutual Information for Attack 1 (noniterative)

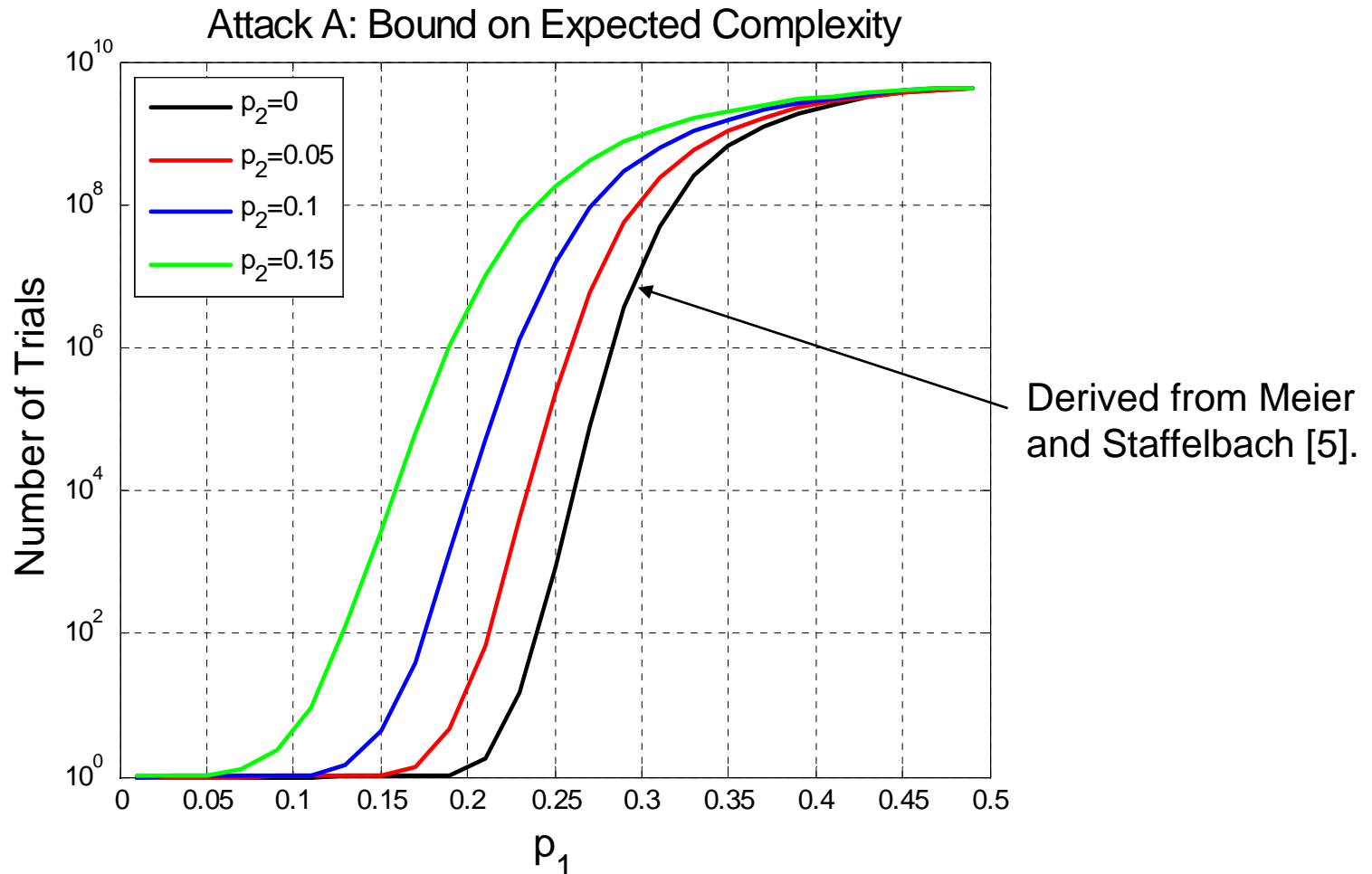


- **Assuming  $A$  and  $Y$  to be random variables**
  - $I(A; Y) = H(Y) - H(Y|A) = H(Y) - H(p') \leq 1 - H(p')$ .
- **As  $p' \rightarrow 0.5$  then  $I(A; Y) \rightarrow 0$ .**
  - This reduces Attack 1 to a brute-force attack.

# Mutual Information for Attack 2 (iterative)

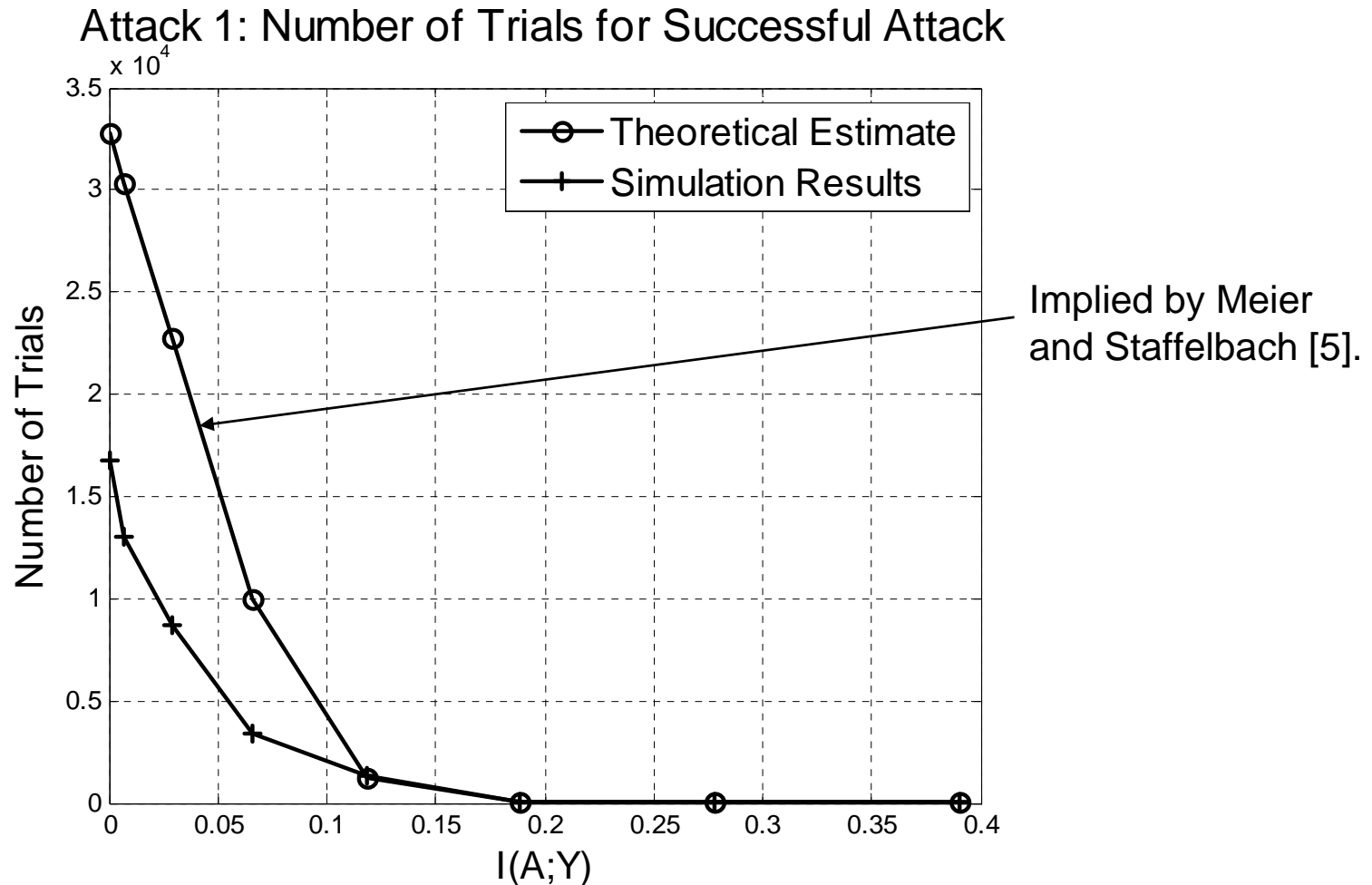
- **Attack 2** modifies the eavesdropper's data sequence  $Y$  each round.
- Thus  $I(A;Y)$  changes throughout the attack.
  - In a successful attack,  $I(A;Y) \rightarrow 1$ .
- Let  $Y^{[l]}$  denote a random variable governing the distribution of the  $Y$  data after the  $l$ th round of the attack.
- **Therefore** 
$$I(A;Y^{[l]}) = \sum_{a,y} p(A = a, Y^{[l]} = y) \log_2 \frac{p(A = a, Y^{[l]} = y)}{p(A = a)p(Y^{[l]} = y)}$$
  - Can be estimated through simulation.
  - Can be graphically presented using EXIT charts.

# Enhanced Security: Attack 1 (noniterative)



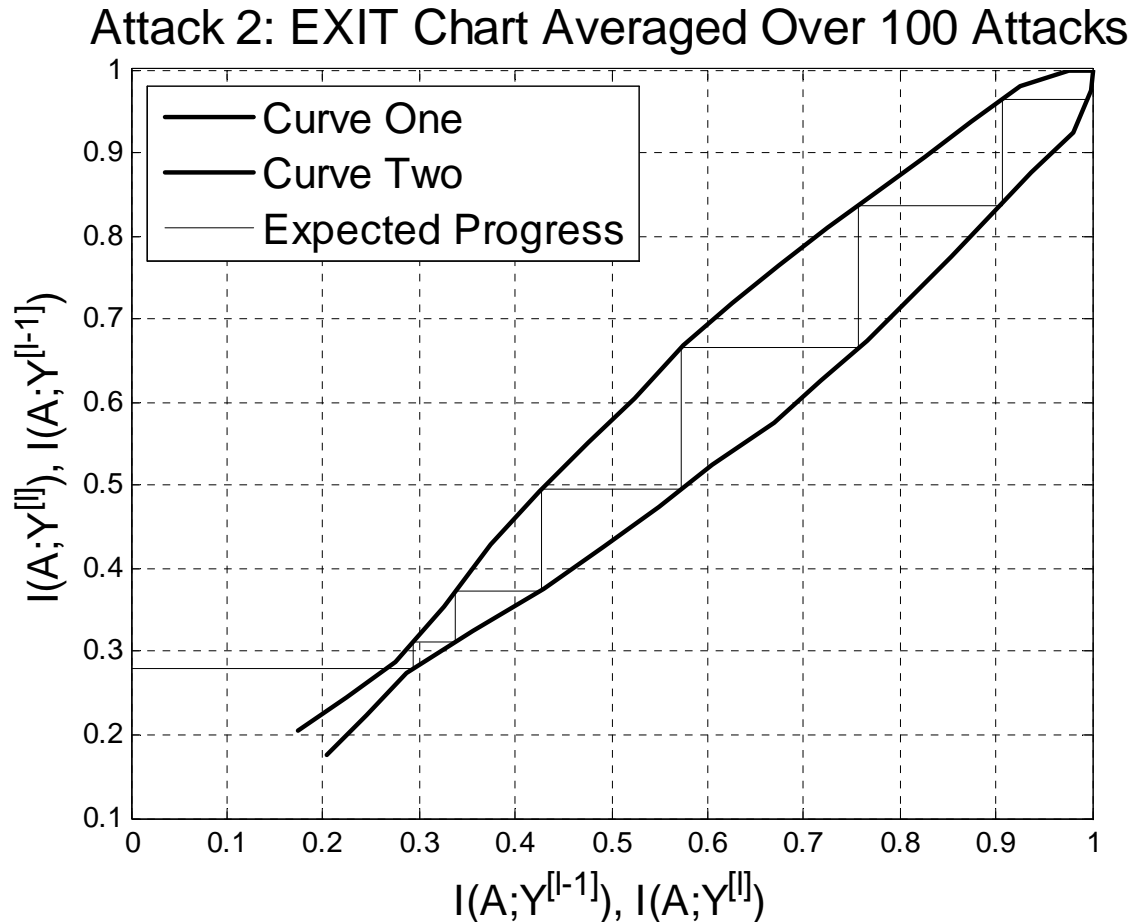
Expected bound on the number of trials required to find the secret key using attack 1 for  $k = 32$ ,  $N = k \times 10^6$ , and  $t = 6$ .

# Mutual Information: Attack 1 (noniterative)



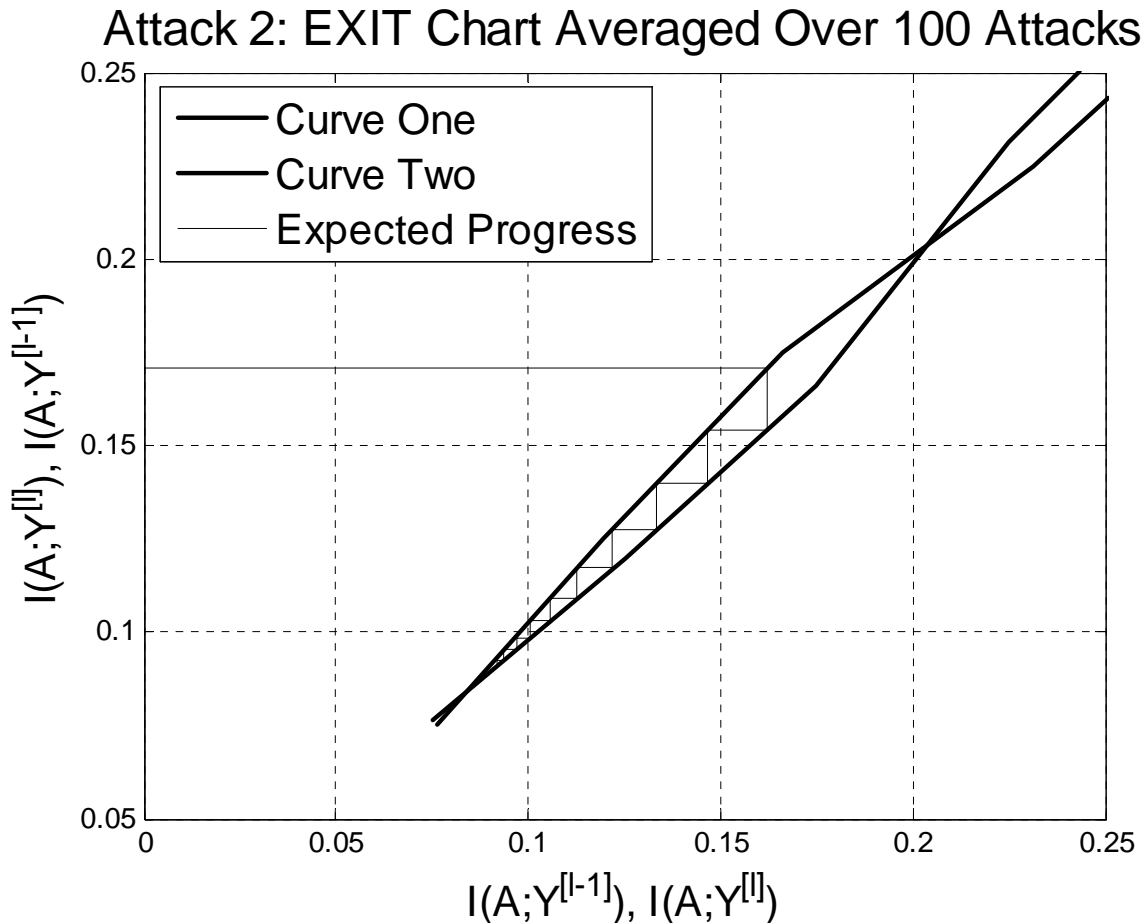
Number of trials required for a successful attack versus  $I(A;Y)$  when  $k = 15$ ,  $N = 1500$ , and  $t = 4$ . (Note that  $t$  is small relative to  $k$  for ease in simulation, but these results extend to larger  $t$ .)

# EXIT Chart: Attack 2 (Successful attack)



EXIT chart formed by averaging the results of 100 simulations of attack 2 with  $k = 31$ ,  $t = 6$ , and  $N = 3100$ , assuming  $p_1 = p' = 0.2$ , i.e. there are no errors from the physical layer.

# EXIT Charts: Attack 2 (Failed attack)



EXIT chart formed by averaging the results of 100 simulations of attack 2 with  $k = 31$ ,  $t = 6$ , and  $N = 3100$ , assuming  $p_1 = 0.2$  and  $p_2 = 0.1$  yielding  $p' = 0.26$ , i.e. there is a 10% error rate due to the physical layer.

# Conclusions

---

- **Wiretap channel model is used to show security enhancements in a system by considering the channel coding problem and the cryptography problem in tandem.**
- **Physical-layer security is characterized in terms of the cryptographic layer metrics and mutual information.**
- **It is verified using mutual information and EXIT charts that fast correlation attacks can be made more difficult or impossible when channel errors at the physical layer are considered.**

**See Related Work:**

[7] W. K. Harrison and S. W. McLaughlin. Physical-layer security: Combining error control coding and cryptography. Presented at ICC 2009 and posted on arXiv.org, arXiv:0901.0275v2 [cs.IT], Apr 2009.

[8] W. K. Harrison and S.W. McLaughlin. Tandem coding and cryptography on wiretap channels: Exit chart analysis. Presented at ISIT 2009 and posted on arXiv.org, arXiv:0905.0440v1 [cs.IT], May 2009.