Non-Profiled Side-Channel Attacks Against GIFT Lightweight Block Cipher

Alexander Benjamin, Jack Herzoff, Dr. Liljana Babinkostova, Dr. Edoardo Serra
Brown University, Boise State University, Boise State University, Boise State University

INTRODUCTION

In 2016, the National Institute of Standards and Technology (NIST) initiated a call for lightweight cryptographic proposals to strengthen the defense of networked devices and their data against cyberattacks.[1] These proposals need to balance security, execution and resource needs within environments with constraints such as limits on power or storage.

Our research applies machine learning techniques to side channel attacks.

SIDE-CHANNEL ATTACKS

Devices conducting encryption algorithms release other data as they encrypt a message. These other data sources, such as timing, heat, or power consumption, can provide insight into the encryption key. Side-Channel Attacks use this insight to reveal encryption keys.[2]

GIFT - Lightweight Block Cipher

GIFT is a block cipher and a finalists in the NIST lightweight cryptography standardization process. Over **28 rounds** it repeatedly shuffles a block of data in permutation or P boxes, switches 4 bit section values in S boxes, then incorporates part of an encryption key.[3]

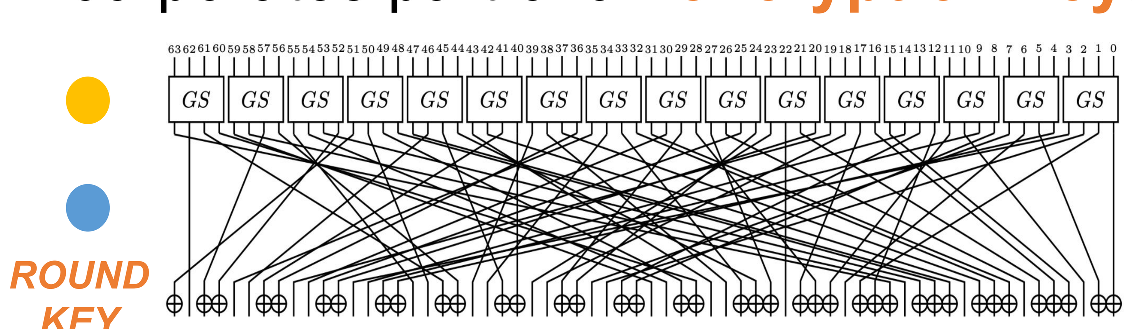
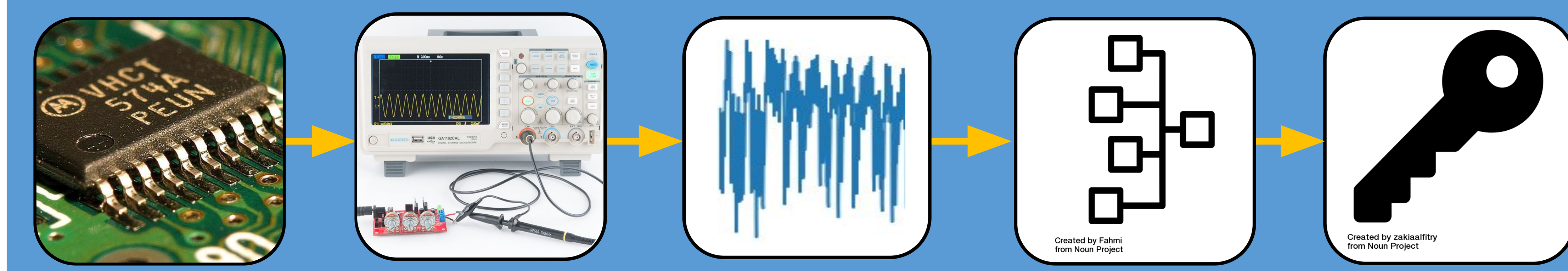


Figure 1: structural diagram of one round of GIFT

Deep Learning

Neural Networks are Machine Learning models made of nodes called perceptrons.[4] A **Multi Layer Perceptron** (MLP) takes in an input layer and feeds it through many **layers of perceptrons** trained over time to improve accuracy. **Convolutional Neural Networks** (CNN) include filtering and compressing layers

METHODOLOGY



Run GIFT	Measure Power Consumption	Attack Model	Power Traces	Predict Round Key

Leakage Model — Hamming Weight

- The leakage model connects subkeys and power traces by **estimating power usage for each subkey guess**
- Converting a 0 to a 1, or a 1 to a 0 requires different amounts of power so **Hamming Weight** can estimate power usage by counting 1s in a byte [5]
- The subkey based estimate best predicted by the power traces will be selected as correct

Correlation Power Analysis [CPA]

- CPA is a statistical model that finds connects estimated power usage and power traces using the **Pearson Correlation Coefficient** [5]

Pearson Coefficient: $r = \sum(x_i - \bar{x})(y_i - \bar{y}) \,/\, \sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}$

- The subkey with the highest correlation between estimated power usage and power traces is selected

Deep Learning Power Analysis [DLPA]

- Neural Networks predict estimated power usage for each subkey using the power traces [6]
- As our DLPA models based on [TIMON 19] train to predict estimated power usage, loss, an accuracy metric, decreases. Loss should decrease fastest for the correct round key, and the key with lowest loss is selected.
- Our power trace data used for all our models comes from [UNGER 21]. [7]

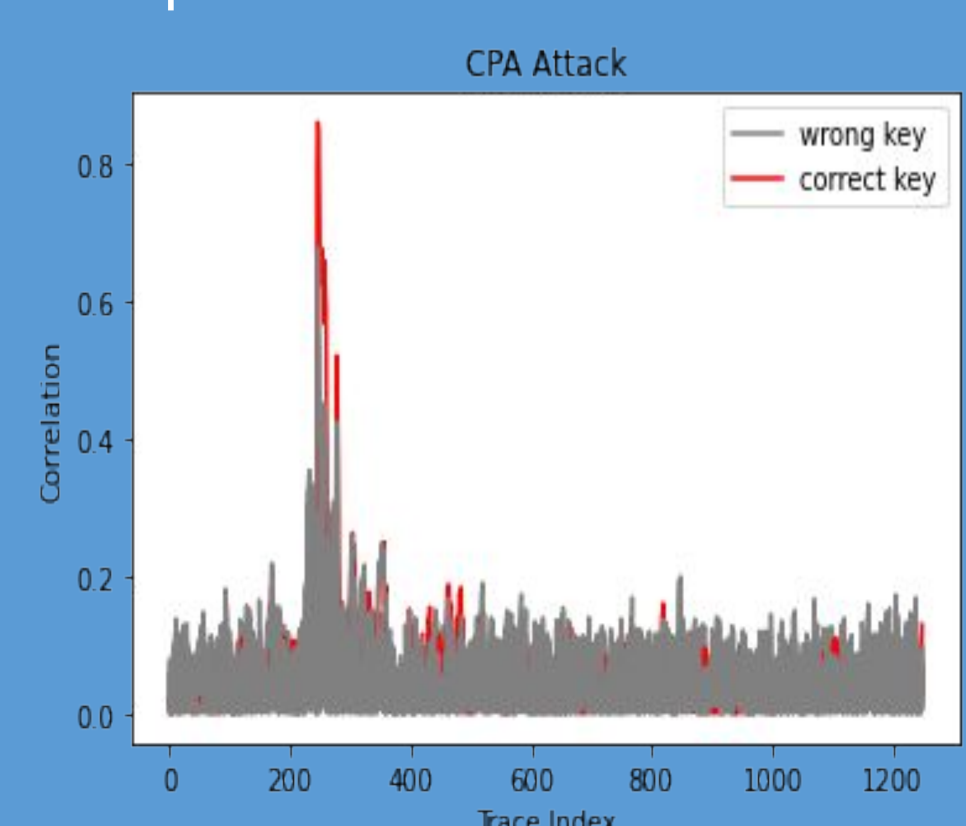


Figure 2: Correlation shown between each power trace measurement and Sbox output (after XOR of subkey) for 16 possible subkeys. To find the correct key, we calculate the maximum correlation for all 16 possible subkey values and select the subkey with the highest correlation.

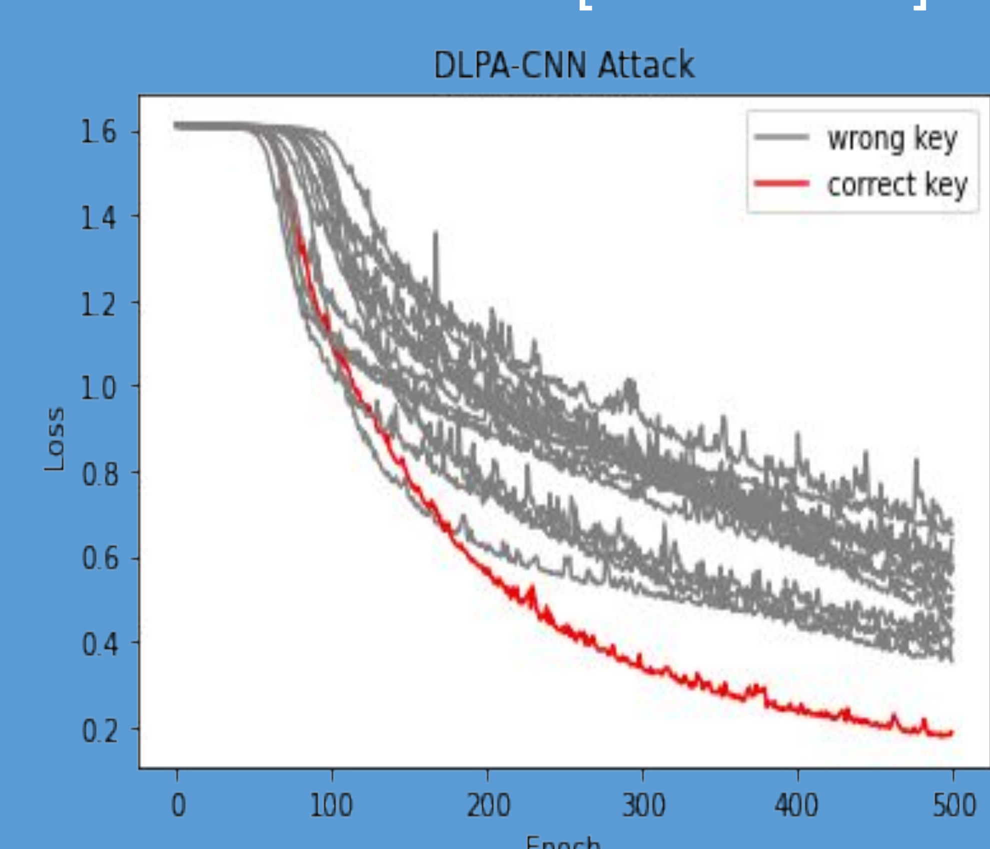


Figure 3: This shows 16 DLPA-CNN loss metrics plotted over 500 epochs. The model trained on the correct sub-key leads to the lowest training loss and is selected. We repeat for all 16 subkeys of the round.

Grant: CCF-1950599

BROWN

SCAN FOR FURTHER REFERENCES, RESOURCES, AND ABSTRACT

RESULTS

Attack Model	Key Prediction Accuracy
CPA	100%
DLPA-CNN	100%
DLPA-MLP	60%
Logistic Regression	0%
Random Forest	0%
Support Vector Machine	0%

Figure 4: Attacks performed on 10 datasets, each with a different fixed key and 345 traces. CPA and DLPA-CNN attacks recovers the key 100% of the time while the DLPA-MLP attack were only able to recover the key 60% of the time.

Conclusion

Unprotected GIFT is **vulnerable to side channel attacks against both CPA and DLPA**. In particular, the Sbox leaks information that SCA can leverage to recover the key. Machine Learning models such as Logistic Regression, Random Forest, and Support Vector Machine are unable to predict GIFT subkeys using power trace data.

Future Work

Further masked data should show the strength of DLPA against CPA. The Masking countermeasure adds randomness by splitting up processes into shares.[8] Share number relates directly to the degree of security but has a computational cost. We have implemented masking on GIFT but have not conducted attacks on it

References

[1] Computer Security Resource Center. Lightweight Cryptography. National Institute of Standards and Technology, Jan. 2017.
[2] V. Arribas. "Design and Verification of Side-Channel and Fault Attacks Countermeasures". Svetla Nikova and Vincent Rijmen (promotors). PhD thesis. Katholieke Universiteit Leuven, 2020.
[3] S. Banik et al. "GIFT: A Small Present – Towards Reaching the Limit of Lightweight Encryption". In: IACR-CHES. ePrint Arch. (Aug. 2017), pp. 321–345.
[4] E. Prouff, R. Strullu, R. Benadjila, E. Cagli, C. Dumas, Study of Deep Learning Techniques for Side-Channel Analysis and Introduction to ASCAD Database. IACR Cryptol. ePrint Arch. 2018: 53 (2018)
[5] O. Lo, W. J. Buchanan, and D. Carson. "Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)". In: Journal of Cyber Security Technology 1.2 (2017), pp. 88–107.
[6] B. Timon. "Non-Profiled Deep Learning-based Side-Channel attacks with Sensitivity Analysis". In: IACR Transactions on Cryptographic Hardware and Embedded Systems (2019), pp. 107–131.
[7] W. Unger, L. Babinkostova, M. Borowczak, and R. Erbes, Side-Channel Leakage Assessment Metrics: A Case Study of GIFT Block Ciphers, IEEE Computer Society Annual Symposium on VLSI, July 7-9, 2021, Tampa, Florida.
[8] L. De Meyer. "Cryptography in the Presence of Physical Attacks: Design, Implementation and Analysis". Begul Bilgin and Vincent Rijmen (promotors). PhD thesis. KU Leuven, 2020.