DLPA on a Hardware Implementation of GIFT-COFB

Abstract

With the expansion of the Internet of Things (IoT), concerns about security measures on resource-constrained devices susceptible to side-channel attacks (SCA) have been raised. In 2016, The National Institute for Standard and Technology (NIST) initiated a process to evaluate lightweight cryptographic (LWC) algorithms for lightweight devices where current NIST cryptographic standards perform poorly. This research investigates side-channel vulnerabilities of unmasked and masked versions of GIFT, one of the ten NIST lightweight cryptographic algorithms finalists. To test the resilience of GIFT against SCA, we apply Deep Learning Power Analysis (DLPA) to its hardware implementation.

Introduction

With the expansion of the IoT, classical cryptographic standards do not hold up in lightweight devices due to resource constraints. In 2016, NIST started a standardization competition for **Lightweight Cryptography**. At the time of our research, NIST has reached the final stage of selecting an LWC algorithm. We investigate the side-channel resilience of a finalist, GIFT, using DLPA. To our knowledge, this is the first SCA on a hardware implementation of GIFT.

GIFT-COFB is a lightweight block cipher that uses a 128-bit key [Banik et al., 2017]. It has an initialization phase, loading a 128-bit plaintext into four 32-bit segments, and a round function, which includes a substitution box, permutation layer, and add round key function.

DLPA combines **Deep Learning (DL)** trainings and **Correlation Power Analysis (CPA)**-like hypotheses in a non-profiled context. We follow the DLPA algorithm provided in [Timon, 2018] on GIFT.

DLPA on GIFT-COFB

We apply DLPA on GIFT-COFB to 13 different data sets containing 10,000 plaintexts using CNN and MLP neural networks on synchronized and desynchronized power traces for each nibble of the key. We use the output of the first round key function as the hypothetical values for DLPA with the loss and accuracy model. The percentages indicate the probability that a key nibble was guessed correctly on average.

Table 1: Percentage of full round key recovered with CNN.

DLPA-CNN	Synchronized	Desynchronized
Loss	24.8%	24.3%
Accuracy	26.7%	25.7%

Table 2: Percentage of full round key recovered with MLP.

DLPA-MLP	Synchronized	Desynchronized
Loss	24.8%	24.0%
Accuracy	24.5%	25.2%

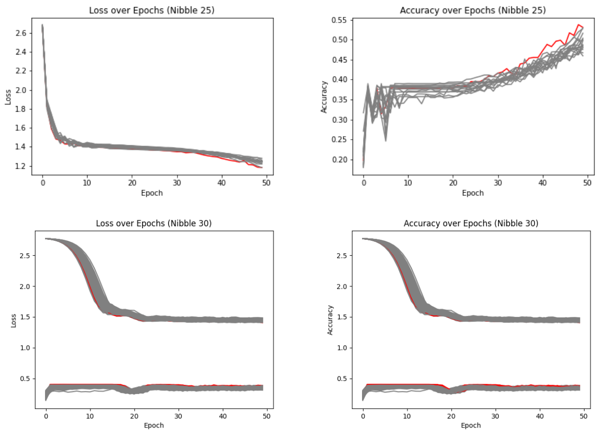

Figure 1: Nibble with the best metrics using loss and accuracy. Top: DLPA-CNN Bottom: DLPA-MLP

We pick the nibble with the highest accuracy and lowest loss metric, shown in Figure 1. DLPA-CNN and DLPA-MLP on synchronized and desynchronized traces recovered one-fourth of the key correctly, making it a partially effective DLPA attack. Table 1 and Table 2 show the portions of the key guessed correctly ranging from 24.0% to 26.7% for CNN and MLP, respectively.

Conclusion

GIFT-COFB is a lightweight block cipher selected as a NIST finalist, but only software implementations of it have been investigated. We applied DLPA to a hardware implementation of GIFT by targeting the first-round key function of GIFT-128. DLPA-CNN and DLPA-MLP were only able to recover about one-fourth of the key, showing that GIFT is not fully secure against DLPA attacks. One direction of focus in the future could be to apply other countermeasures to GIFT in order to prevent any portion of the key from being discovered.

Acknowledgements

This research was supported by the National Science Foundation under award #1950599.

References

[Banik et al., 2017] Banik, S., Pandey, S., Peyrin, T., Sasaki, Y., Sim, S. M., and Todo, Y. (2017). Gift: A small present – towards reaching the limit of lightweight encryption. *IACR-CHES. ePrint Arch.*, pages 321–345.

[Timon, 2018] Timon, B. (2018). Non-profiled deep learning-based side-channel attacks. *Cryptology ePrint Archive.*