1

Deep Learning Techniques for Side Channel Analysis

Nimar Blume

***Abstract*—Put the abstract here. The abstract should be 200-300 words long and must answer the following questions:**

- **Why is this topic important and interesting?**
- **What is the topic?**

It's a good writing style to answer the "why" question first by putting the topic in a broader context.

I. Introduction

To protect data against tampering and inspection by 3rd parties, encryption is commonly used to make data only accessible to people possessing the relevant credentials to access said data. Encryption provides in many cases privacy, integrity and authenticity of data exchanged by two or more parties.

A. The Advanced Encryption Standard

There are many encryption algorithms available to use for data encryption, this paper focuses on the use of the block cipher Advanced Encryption Standard (henceforth AES) with a 128bit key. AES expands a single 128bit key to 11 round keys which are then used to encrypt the given data. It is important to note, that a compromise of any of the 11 round keys enables an attacker to reconstruct the initial 128bit key and thus decrypt the whole data set. The AES algorithm encrypts data in batches of 128bits or 16bytes. Should a block be smaller than 16bytes, padding will be appended to it.

What is side channel analysis with regard to cryptography?

II. State of the Art

Where can SCA be applied?

A. The state of Side Channel Analysis

Current state of SCA: Simple power analysis, differential power analysis, template attacks How do they work/what is the difference between the three?

B. Where Machine Learning used in Template Attacks

Machine learning used in template attacks -> path to using deep learning techniques?

III. HAUPTTEIL

Regular research papers need at least two additional sections here. One section for contributions and methods and one section for the results. For seminar papers these sections can be omitted.

Fabrizio Desantis, Chair of Security in Information Technology of the Technical University of Munich

IV. Conclusion

Put the conclusions of the work here. The conclusion is like the abstract with an additional discussion of open points.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.