EM Side-Channel Analysis of ECC Scalar Multiplication

Sebastian Verschoor, Alvin Cai Kunming

Technische Universiteit Eindhoven, Eindhoven, The Netherlands

Abstract. The aim of the project is to successfully run an electromagnetic side channel attack on the Lim-Lee ECC scalar multiplication algorithm implemented on a smart card.

1 Introduction

The electric current that flows through a conductor induces Electromagnetic (EM) emanations which can be used for side channel analysis. The advantage of this technique is that it (a) allows the measurement of local EM radiations from selected points on the chip [1] and (b) attacks can be mounted from a distance of several feet away [2] e.g. against mobile devices.

In this paper, we attempt a practical attack on a smartcard performing ECC scalar multiplication using EM analysis. This attack targets the Lim-Lee scalar multiplication algorithm on Riscure's training card 8. In this report, we will not go into details of the Lim-Lee algorithm and associated attack, but will focus instead on the EM aspects which can be generalised to any scalar multiplication algorithm.

2 Methodology and Practical Results

In our attack, we first try to identify the specific location where cryptographic operations are carried out on the smartcard. We can then position the EM probe very close to this region so as to increase the chances of capturing data-dependent signals. The EM traces we obtained were very noisy and required signal processing to reduce noise to levels at which the data dependencies are revealed. The final step is to perform a simple side channel analysis to recover the secret key bits.

2.1 Spatial Positioning

1. how to identify 30.8MHz crypto core frequency from the power trace
2. how to find this point on the chip.
3. How we efficiently to iteratively measure and narrow down the region.
4. ...

2.2 Signal Processing

1. Remove harmonics
2. Sync resample
3. Filter
4. Can also average many traces
5. ...

2.3 Simple Side Channel Analysis

1. just provide a brief description as anyway we did not do this completely.
2. I think its more interesting to talk about how we can perform a proper attack given the limitations (i.e. can only measure short sections each time.)
3. ...

3 Conclusion

1. Talk about how practical?

References

1. Gandolfi, Karine, Christophe Mourtel, and Francis Olivier. "Electromagnetic analysis: Concrete results." Cryptographic Hardware and Embedded SystemsCHES 2001. Springer Berlin Heidelberg, 2001.
2. Gary Kenworthy and Pankaj Rohatgi. "Mobile Device Security: The case for side channel resistance." Cryptography Research Inc, 2012.