Łukasz Chmielewski,
Faculty of Informatics,
Masaryk University,
Botanická 68a, 602 00 Brno

BACHELOR THESIS REVIEW

Date: 12.6.2026

Student: Jozef Sabo, UČO 536644
Supervisor: Marek Sýs
Reader: Łukasz Chmielewski
Title: Correcting errors in the side-channel attacks
Report:

The work analyzes and improves upon the study "Side-channel Attacks on Blinded Scalar Multiplications Revisited" by Roche, Imbert, and Lomné (that work analyzed side-channel attacks on blinded scalar multiplications used in elliptic-curve cryptography). The objective was to reproduce and extend the results of the original paper. The student's goal was to first implement and verify the published attack, confirming its correctness and success rates under various parameters (such as noise level, bit error rate, and the number of observed traces). Secondly, the student was supposed to propose modifications that improve the success rate or minimize the number of traces. The results should have been experimentally verified and discussed in terms of accuracy, performance, and robustness.

I believe that this thesis fulfills all the goals of the assignment very well. The results presented are very interesting and go beyond what is expected of a bachelor's thesis. In particular, the thesis presents clear improvements over published research. The analysis of how significant the improvement is for higher error rates (>=20%) is missing from the thesis, but this does not diminish the value of the presented results.

This thesis is organized as follows. Chapter 1 introduces the mathematical foundations of elliptic curve cryptography, side-channel analysis, and scalar blinding. Chapter 2 describes the baseline attack algorithm. Chapter 3 presents the methodology and an implementation used to simulate the attack environment and execute the attack. Chapter 4 provides a detailed structural analysis of the algorithm and formulates optimization hypotheses. Finally, Chapter 5 reports the empirical results of these modifications and evaluates their impact on the algorithm's accuracy, time complexity, and practical robustness.

The main weakness of the thesis is readability. The thesis is mathematically dense, and I think that some parts are difficult for a reader who is not already familiar with the original attack. Sometimes it is not fully clear what comes from prior work, what was reproduced, what discrepancy was found, and what is genuinely new. In terms of writing, the thesis is generally clear and precise, but it could use some polishing.

While I am impressed with the results from the thesis, I would like to ask the following question:

- For error rates 20% and 25%, Figure 5.5 suggests that the success rate of the algorithms might still slowly grow beyond the 10000 mark. Could you comment on

whether it would ever reach 64 and how many traces it would require?
If the proposed method could achieve a success rate of 64 in a feasible time while maintaining an error rate >20%, I believe it would be an interesting scientific contribution.

- Would the presented method work well against data obtained from Algorithm 1 in https://tches.iacr.org/index.php/TCHES/article/view/9962/9465 ?
  Here, the issue might be that the information obtained by the attacker concerns the XOR of scalar bits and not the scalar bits directly.

Evaluation:

Based on the discussion above, I recommend the manuscript as a bachelor's thesis. Despite presentation issues, the analysis and the technical work presented in the manuscript justify marking the thesis as having **passed with exceptional results**.

Brno 12.6.2026 **Łukasz Chmielewski**