Power Analysis Attacks on New Hope

A Part III project proposal

T. T. Bui (*ttb29*), Downing College

Project Supervisor: Dr Markus G. Kuhn
Director of Studies: Dr Robert K. Harle

Abstract

In January 2019, NIST announced the Round 2 candidate algorithms of its ongoing call for Post-Quantum Cryptography standardization proposals[1]. Post-quantum cryptography protocols aim to provide secure systems against both quantum and classical computers, and at the same time be compatible with existing security infrastructures. In the past, classical public-key cryptography schemes had been known to be vulnerable to side-channel attacks. Power analysis side-channel attacks have been well-studied and are shown to be effective against the implementations of major algorithms, including AES [1] and RC4 [2]. This project seeks to investigate its effectiveness on post-quantum cryptography protocols by implementing New Hope, one of the NIST Second-round candidates, on a microcontroller and performing power analysis attacks on the implementation.

1 Introduction, approach and outcomes (500 words)

In recent years, a considerable amount of research has been focusing on developing quantum computers—machines that can quickly solve problems that would take normal computers an unreasonable amount of time. In light of the recent news of Google claiming "quantum supremacy" [3], should quantum computers become more practical, existing public-key cryptosystems could be easily broken, as they rely on the computational intractability of one of two number-theoretic problems: large numbers factorisation or the discrete-logarithm problem. Post-quantum cryptography protocols aim to provide public-key functionality without relying on those two assumptions while remaining compatible with existing security infrastructures.

In preparation for the uncertain arrival of the quantum computing era, the study of post-quantum cryptography protocols is of prime importance. In the past, classical public-key cryptography schemes had been known to be vulnerable to side-channel attacks. Side-channel attacks leverage measurements from a target device's unintended channel to extract

[1] https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

secret information, usually the secret key, that the device processes. The channels could range from power consumption to electromagnetic or photon emissions [1]. In particular, power analysis methods such as *Simple power analysis (SPA)*, *Differential power analysis (DPA)* [1] and *Correlation power analysis (CPA)* [4] are effective against implementations of major algorithms.

The main goal of my project is to investigate the effectiveness of the power analysis methods against New Hope, one of the Round 2 candidate algorithms of NIST's ongoing call for Post-Quantum Cryptography standardization proposals. New Hope is a key-establishment protocol. In a basic Diffie-Hellman key-exchange protocol between two parties, Alice and Bob, Alice uses two values g, p and a secret value a, computes $A = g^a \mod p$ and sends (A, g, p) to Bob. Bob uses a secret value b, computes $B = g^b \mod p$ and sends back B to Alice. Alice and Bob now share a secret key $K = B^a \mod p = A^b \mod p$.

To approach the problem, I will first implement a key-exchange scheme using the New Hope algorithm to run on an evaluation board of a microcontroller. Difficulties could arise in working with the evaluation board of the microcontroller due to unfamiliarity, so I have set out some time in the schedule for that purpose. The next step is to generate a tuple (A, g, p) for the application, load them onto the microcontroller and then forget the value a. The high-frequency power consumption fluctuations of the microcontroller during the key computation stage, when it processes the secret value b, are recorded for different tuples. Then, I will instrument different power analysis attacks, possibly DPA and CPA, and/or template attack, to extract the secret value used by the device using the information about the intermediate values leaking out through the power consumption traces during the key computation stage.

The outcome of my project would be to produce an implementation of New Hope key-establishment algorithm on a microcontroller and be able to extract the secret value used in the device during the key computation process of the algorithm. The evaluation will focus on presenting and explaining the results, and comparing the different attacks in terms of timing or the number of power traces required.

2 Workplan (500 words)

1. **Michaelmas vacation weeks 1–2 [5/12–18/12]:** Become familiar with working with an evaluation board of a microcontroller. Understand the New Hope algorithm.
2. **Michaelmas vacation weeks 3–4 [19/12–1/1]:** Write the basic code for the implementation of the New Hope algorithm.
3. **Michaelmas vacation weeks 5–6 [2/1–15/1]:** Start implementing the algorithm onto the microcontroller.
   Milestone: A basic working version of the application using the algorithm

on the microcontroller.

4. **Lent weeks 1–2 [16/1–29/1]:** Buffer weeks for leisure time spent during Michaelmas vacation.
5. **Lent weeks 3–4 [30/1–12/2]:** Record the power consumption fluctuations of the microcontroller. Process the power traces in preparation for the power analysis attacks.
6. **Lent weeks 5–6 [13/2–26/2]:** Perform the power analysis attacks.
7. **Lent weeks 7–8 [27/2–11/3]:** Evaluate the results of the different attacks. Compare the efficiency of different attacks.
   Milestone: **Different power analysis attacks performed and results evaluated.**
8. **Easter vacation weeks 1–2 [12/3–25/3]:** Work on possible extensions (if any). Otherwise, focus on the evaluation and comparison of the attacks.
9. **Easter vacation weeks 3–4 [26/3–8/4]:** Possible overflow from the previous weeks. Clean up codes and repository. Start writing dissertation main chapters.
10. **Easter vacation weeks 5–6 [9/4–22/4]:** Possible overflow from the previous weeks. Clean up codes and repository. Continue writing dissertation.
    Milestone: **Complete working prototype with power analysis performed and results evaluated. First draft of dissertation.**
11. **Easter weeks 1–2 [23/4–6/5]:** Continue writing dissertation. Review cycles and corrections to dissertation.
12. **Easter weeks 3–4 [7/5–20/5]:** Continue writing dissertation. Review cycles and corrections to dissertation.
    Milestone: **Complete dissertation. Proof reading and submission.**
13. **Easter weeks 5 [21/5–27/5]:** Buffer week.

References

[1] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, vol. 1, pp. 5–27, Apr 2011.

[2] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002* (B. S. Kaliski, ç. K. Koç, and C. Paar, eds.), (Berlin, Heidelberg), pp. 13–28, Springer Berlin Heidelberg, 2003.

[3] H. Neven, "Computing takes a quantum leap forward." https://www.blog.google/technology/ai/computing-takes-quantum-leap-forward/. Accessed: 2019-11-21.

[4] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems - CHES 2004* (M. Joye and J.-J. Quisquater, eds.), (Berlin, Heidelberg), pp. 16–29, Springer Berlin Heidelberg, 2004.