Summer Project: Side Channel Attacks

Diclehan Erdal
Katrina Falkner, Yuval Yarom, Naomi Benger

October 7, 2013

Preliminary Research

Week 1

Learning goals:

- Set up GitHub.
- Learn how to use LaTeX.
- Commence reading/research.

Reading list:

- The Montgomery Powering Ladder

Progress/Tasks completed:

- 26/09/13 Set up GitHub on my computer. Cloned the project repository and added additional resources to it. Learned how the GUI worked.
- 26/09/13 Attempted to read The Montgomery Powering Ladder. Looked up what Abelian Groups and Lucas Chains are. Need to complete reading paper.
- 26/09/13 Started a (rough) bibliography.
- 26/09/13 Installed TexMaker and watched YouTube videos on tex document basics. Attempted to modify progress report, but couldn't view changes in the PDF, or create my own tex files.

Week 2

Learning goals:

- Create bibliography on TexMaker. i.e. work out/learn how bib files work
- Establish some cryptography basics to ensure better understanding of further reading.
- Reattempt The Montgomery Powering Ladder paper.

Reading list:

- The Montgomery Powering Ladder.
- Sections 19.7 McEliece, 19.8 Elliptic Curve Cryptosystems from Applied Cryptography.
- The following sections of An Introduction to Mathematical Cryptography: 1.1 Simple substitution ciphers, 1.2 Divisibility and greatest common divisors, 1.3 Modular arithmetic, 1.4 Prime numbers, unique factorization, and finite fields, 1.7 Symmetric and asymmetric ciphers, 5.1 Elliptic curves and 5.2 Elliptic curves over finite fields.

Progress/Tasks completed:

- 30/09/10 Upon some web troubleshoot searches, discovered that installing MikTex and running TexMaker as admin solved the problem.
- 02/10/13 Read sections 19.7 and 19.8 of Applied Cryptography. Didn't understand some of the notation in 19.7. The proceeding section was easy to understand, however I'm not familar with how the Diffie-Hellman, ElGamal, or Schnorr algorithms work. ElGamal will be looked into (I believe there is something related to it in 20.1). Will look further into "RSA" as well as I've come across that before.
- 02/10/13 Read the abstracts and introductions of the three papers on Side-Channel attacks analysis.
- 05/10/13 Simple substitution ciphers: Simple, as the title suggests. Nothing new or immensely enlightening but a nice way to start the book.
  Divisibility and greatest common divisors: The Euclidean Algorithm was interesting. I was not familiar with it before unlike the other content of the section. I don't yet see how GCDs are directly relevant to Cryptography, but it was a fun read. Also, I learnt the concept of "relatively prime".
  Modular arithmetic: "Z/mZ is the ring of integers modulo m". I recognise this notation and now know what it means! I was introduced to Eulers phi function and The fast powering algorithm in addition to that.
  Prime numbers, unique factorization, and finite fields: The Fundamental Theorem of Arithmetic was something I used to simplify surds but did not know of formally. Came across a written definition of a field. Learnt that that hollow F is used to represent fields, along with a value; that is equivalent to "Z/pZ, and that the equality relationship between two elements belonging to each is different.

- 06/10/13 With the aid of online resources, created LaTeX bibliography.
- 07/10/13 Symmetric and asymmetric ciphers:
  Elliptic curves:
  Elliptic curves over finite fields:
- 07/10/13 Read The Montgomery Powering Ladder.

Week 3

Learning goals:

- Digital Signatures (DSA)
- Side Channel Attacks (analysis, countermeasures).

Reading list:

- 20.1 Digital Signature Algorithm from Applied Cryptography.
- (if required)Relevant sections from Chapter 7 of An Introduction to Mathematical Cryptography
- Side Channel Attacks on Implementations of Curve-Based Cryptographic Primitives
- Countermeasures against Side-Channel Attacks for EC Cryptosystems
- Low-Cost Solutions for Preventing Simple Side-Channel Analysis Side-Channel Atomicity

Progress/Tasks completed:

-

Week 4

Learning goals:

-

Reading list:

-

Progress/Tasks completed:

-

Week 5

Week 6

Week 7

Week 8

Week 9

Week 10