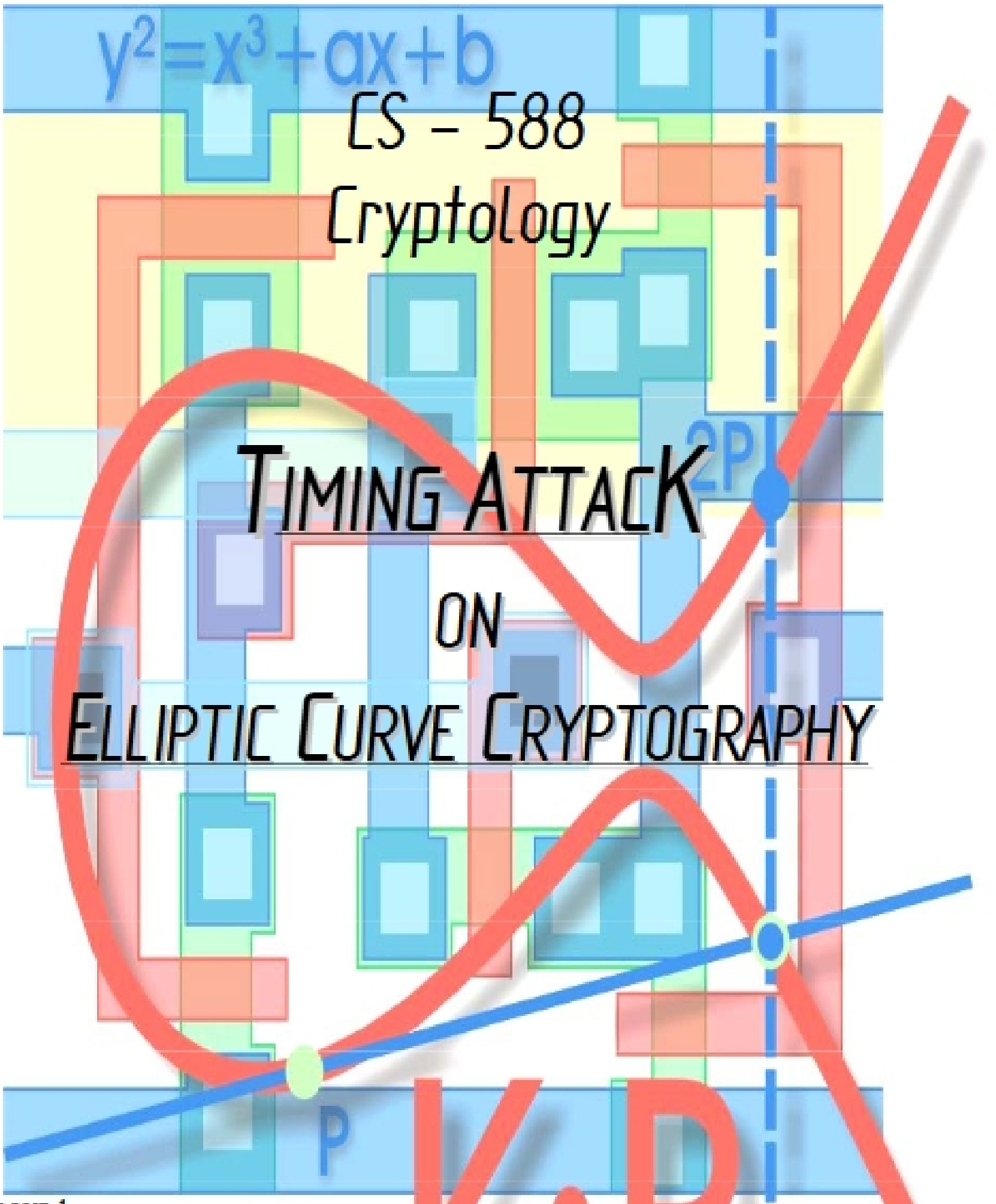

Timing Attack on Elliptic Curve Cryptography

Group 1

Matthew Mah
Michael Neve
Eric Peeters
Zhijan Lu

Professor David Evans

Table of Contents

Introduction

As subject for this project, we first planned to focus upon smart card timing attacks. Smart cards are widely used through Western Europe and will probably appear soon in America. They are used in various application fields and with different levels of complexity and security.

Timing attacks attempt to exploit the variations in computational time for private key operations to guess the private key. This type of attack is primitive in the sense that no specialized equipment is needed. An attacker can break a smart card key by simply measuring the computational time required by the card to respond to user inputs and recording those user inputs. The viability of this attack is important to any smart card implementation using vulnerable cryptosystems. An attacker with prolonged passive eavesdropping ability may be able to break the private key and gain access to the information stored on the card. This will give the attacker access to sensitive information or money.

Later – and after readings – we focused deeper: produce a new timing attack. We have glanced through the Internet to find a cryptosystem not yet analyzed for timing weaknesses. Hence, it appears that the vulnerability of Elliptic Curve Cryptology to timing attacks has not been widely studied. We have thought that this subject could be satisfactory and innovative.

This report is subdivided in three parts: we first start talking about the basics of the timing attacks on a RSA implementation; we then develop a brief presentation of Elliptic Curves and EC Cryptology. The last and major part of the report is dedicated to the timing attacks on an open-source implementation of ECC and our diagnosis about this last point.