COMP90043: Cryptography and Security

Project Proposal: Digital Signature Scheme Evaluation

1 Introduction

Digital signatures indicate mathematical techniques used to validate the authenticity of a message, document or software, which can ensure that the signer send the document and other parties cannot modify it. It is widely used to add authentication, integrity and non-repudiation for digital document.

Several digital schemes have been proven to provide valid authentication for signed paper, among them, we choose three (RSA, ECC and Lamport signature) to evaluate and compare for the research project. Our aim is to observe characteristic and performance of each scheme based on our evaluation metrics and, discuss suitable application domain for each of them.

1.1 Members

Our team member information are as follows.
Group Leader: San Kho Lin

Name	**Student ID**	**Email**
San Kho Lin	829463	sanl1@student.unimelb.edu.au
Yiru Pan	889832	yirup@student.unimelb.edu.au
Tenglun Tan	876792	tenglunt@student.unimelb.edu.au
Zhuohan Xie	871089	zhuohanx@student.unimelb.edu.au

2 Background

RSA[1] is the well-known implementation of public key cryptography and digital signature scheme. It is based on the factorization of two large prime numbers so that it is not computationally feasible for anyone to factor n in such that $n = p \cdot q$ – also known as RSA problem. We will use RSA as our baseline for formulating evaluation metrics.

Elliptic Curve Cryptography (ECC) is another efficient public key cryptography technique. Particularly, we will focus on ECDSA[2] which is based on the difficulty of solving discrete logarithm problem in Elliptic Curve group – also known as elliptic curve discrete logarithm problem. We will also investigate EdDSA[3], the popular variant implementation that has used twisted Edwards curves modifications and parameter tuning for top performance. ECC is well-known for providing greater security with smaller key sizes. This feature is desirable for saving computation resources and bandwidth in securing mobile devices and sensor networks traffic. It is a trending digital signature scheme such that cryptocurrencies like Bitcoin have made use of it. However, ECC discrete logarithms computation is known to be broken by Shor's algorithm[4] on a hypothetical quantum computer.

Lamport one-time signature scheme[5] is an efficient method for constructing a digital signature. One time means that a signature can be used only once due to the algorithm design. When verifying the signature, it reveals a part of the private key. Lamport signatures can be built from any cryptographically secure one-way hash function. It has

been the subject of increased attention recently because it has characteristics like fast verification and resistant to quantum computing. The digital signature schemes like RSA, ECC rely on the computation and algorithmic complexity which is expected to be broken when a quantum computer is practically implemented.

3 Proposal

In this project, we propose to explore three digital signature schemes: RSA, ECC, and Lamport signature scheme. The main idea of choosing these three schemes is their uniqueness in technique and mathematical approaches. We will study their mathematical foundations for generation of keys and verification of digital signatures. We will perform experiments to measure their performance such as timing private/public keys generation, signing and verifying the data packet. We will also discuss their security trade-offs, complexity and the domain it can apply.

For the purpose of evaluation and quality implementation, we aim to utilize the following tools and library:

Name	**Link**
OpenSSL	https://www.openssl.org
NaCl	https://nacl.cr.yp.to
Botan	https://botan.randombit.net
CrypTool	https://www.cryptool.org/en/jcryptool
Bouncy Castle	https://www.bouncycastle.org
SageMath	http://www.sagemath.org
Magma	http://magma.maths.usyd.edu.au/magma/

References

[1] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: http://doi.acm.org/10.1145/359340.359342.

[2] Cameron F. Kerry, Acting Secretary, and Charles Romine Director. *FIPS PUB 186-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS)*. 2013.

[3] Daniel J. Bernstein et al. "High-speed high-security signatures". In: *Journal of Cryptographic Engineering* 2.2 (2012), pp. 77–89. ISSN: 2190-8516. DOI: 10.1007/s13389-012-0027-1. URL: https://doi.org/10.1007/s13389-012-0027-1.

[4] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM J. Comput.* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 0097-5397. DOI: 10.1137/S0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172.

[5] Leslie Lamport. *Constructing Digital Signatures from a One Way Function*. Tech. rep. 1979. URL: https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/.