Performance Analysis of Hashing Schemes in HDMA

Student: Jesus G. Vega Alejandro, Mentor: Shahab Tayeb PhD.
University of Puerto Rico, Mayaguez Campus, Computer Engineering Department

Abstract

Vehicle communication and networking capabilities are important aspects of Intelligent Transportation Systems as of the last decade. With goals of further providing and maintaining quality for services such as complete automation and platooning, and with aid of recent 5G ultra low latency technology and high bandwidth the focus is on performance. Optimization of information transmission rate is necessary to compensate for relatively high computational procedures during entity link set up and information delivery stages. Although lightweight schemes have been proposed, it is important to not fixate on the prospect of performance while pushing on the threshold of security and efficiency of the scheme itself. In this work, we develop a partial replication of the Zero Evidence Proof based Hybrid D2D Message Authentication Scheme presented by Pen Wang and colleagues. The focus is on exploration of hashing schemes of the SHA2 group for the purpose of analyzing performance of the algorithm and viability of varied size bit block schemes exclusively for V2V authentication. Timing comparison of these schemes is essential to decide whether the execution threshold is significant, and whether it's favorable in regards to the security. Light SHA 1 and SHA2 schemes offer a secured 13% increment in performance, and a potential higher benefit as 5G sidelink efficiency increases, at the cost of vulnerability toward more complex and efficient collision attacks as exploits develop.

Background

Research in optimization of negotiation schemes between vehicles and their surroundings has been a priority as it aids to quality maintenance of time-essential services . Implementation of access technologies such as 5G, and schemes like Edge Computing and SDN further aid in communication stability and minimize computational overhead to essentially increase performance in real life implementations. My focus is centered on the optimization of link stage processes in regards to vehicle to vehicle authentication. Schemes such as LIAU have demonstrated the benefit of exploring performance with lower bit block hashing schemes which would be beneficial to HDMA, which is already efficient while depending on SHA256-512.

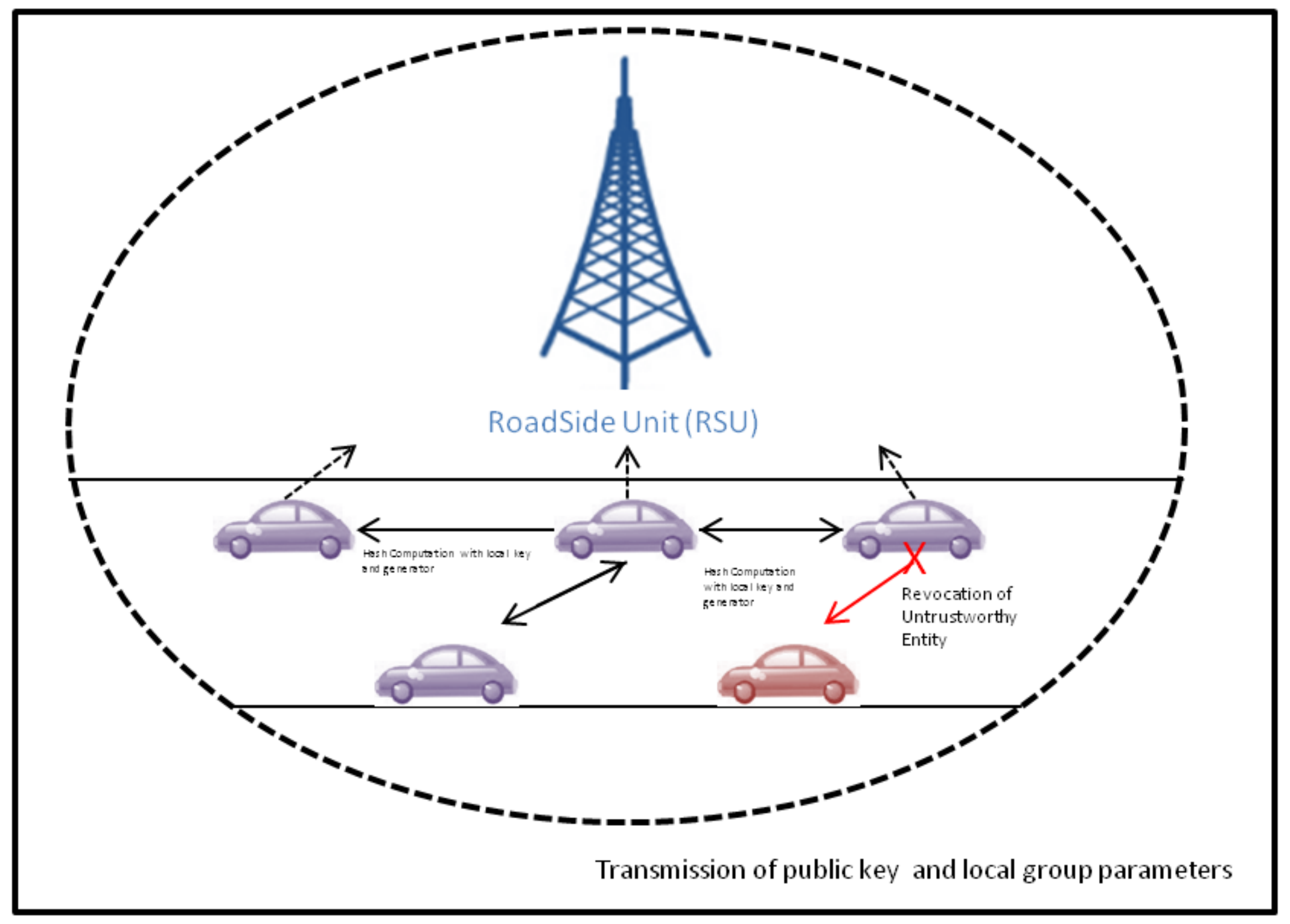
RoadSide Unit (RSU)
Hash Computation with local key and generator
Hash Computation with local key and generator
Revocation of Untrustworthy Entity
Transmission of public key and local group parameters

Fig1. Demonstration of Vehicle to Vehicle Connectivity in a Local Group under HDMA

Introduction

Implementation of Vehicle Ad-Hoc Networks (VANETS) in Internet of Vehicle (IoT) services have been a point of interest for research as of recent. VANETS aim to allow for efficient incorporation and management of large scale, time sensitive operation for intelligent vehicles, while keeping their data secure. Operations revolve around creating an ambience dependent on data transfer from roadside units to the vehicles (V2I) and further extend the communication scheme by relaying requests through the vehicles themselves, through vehicle to vehicle communication (V2V). This involves implementation of tactics for data integrity preservation, device authentication and confidentiality. Authentication schemes provide a means of security against malicious entities with the objective of collecting or manipulating data in the system through attack vectors such as man in the middle or message injection. Ensuring authentication is overall a collective of processes which potentially involve a large overhead in the system, creating a complicated issue of balancing security with performance. Considering this, the focus is on the partial replication of a secure authentication algorithm, the Hybrid Device-to-Device (D2D) Message Authentication (HDMA) scheme, and its execution under various hashing schemes. The Hybrid D2D message Authentication Scheme introduced by Peng Wan and colleagues, utilizes a zero knowledge proof of a logarithmic equation. Zero knowledge proofs allow for an indirect corroboration of knowledge of some piece of data between entities. In this case the common hidden element would involve a common secure key for vehicles and a hash value; a secondary message digest is calculated and along with certain additional parameters, is transmitted to a secondary vehicle, if both vehicles compute the same result the authentication is complete. This type of scheme is protected against message injections as any alteration to the transmitted data would interfere with the corroboration of the hash value. There are various ways to explore performance variations in this scheme; exploration of symmetric encryption schemes for lighter key exchange within a local group could be a potential angle. for pre authentication procedure. In this case, we analyze the variations on the SHA hashing scheme. The original work presented its findings utilizing 256/512 secure bit block SHA2 scheme. The goal is to observe the gap in execution time of messages depending on the hashing utilized in the modular equation.

Motivation

Acknowledgement of possible optimization of time essential segments of the vehicle communication scheme are necessary for the future of VANET. Dependency on lower bit block scheme will reduce latency which considering the computational overhead already present from key creation and sharing scheme its a favorable turnout.

Future Work

Utilization of RSA cryptography for key sharing pre-authentication creates a large overhead for system communication that's managed by road side units. Solution may rely on of incorporation of lightweight symmetric cryptographic schemes for utilization of keys generated with lower bit ranges for higher performance. This would mean favoring less secure and traditional schemes in comparison to **RSA, AES, and ECC**. A possible path to take would be incorporation of light way cryptographic scheme pre-authentication with observations centered around vulnerabilities such as MITM and exploitation through small key attacks.

Results

The results of the HDMA scheme comparison under SHA2 hashing schemes is presented on Table 1. A computational overhead of 1024 bit RSA for a 256 bit local group key must be considered in pre authentication execution. The average time for RSA is Rt = 37.3ms. Timing of message signing and verification stages consists of the timing of the Secure Hash Algorithm and the modular exponential function. Modular exponential function consists of factors such as multiple 128 bit prime factors, a 256 bit local area key and the hash digest, and its execution time is considered for the total timing in Table1. Optimization of the scheme could be achieved by incorporation of SHA 284 as it offers a 13% increase in performance without compromising security, as is the case with SHAQ 160 bits. SHA1, although significantly lighter to implement, will continuously become less dependable as the HDMA message signature could be compromised by efficient collision attacks and lead to the authentication of non-trusted entities. Demonstration of performance data was done with MATLAB and Excel through a spreadsheet link.

Tables

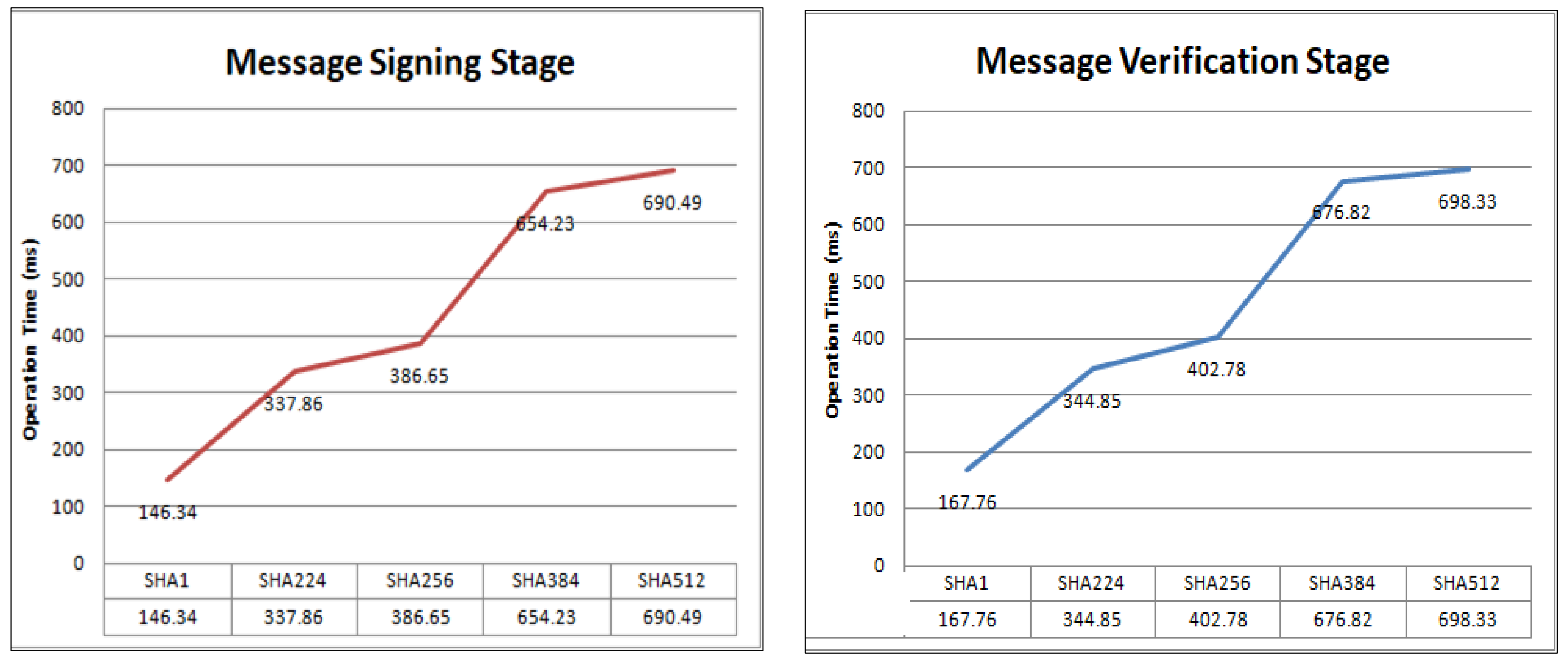

Fig2. Operation time of SHA2 hashing schemes on HDMA Authentication.

Total Time with RSA $T_t = T_{RSA} + T_{HDMA\text{-}SHA}$				
SHA1	SHA224	SHA256	SHA384	SHA512
351.1	720.01	826.53	1449.3	1525.92

Table1. Total Execution Time of Scheme with each Hashing considering overhead and modular expression.

Conclusions

Optimization of processes in reference to the data link layer of device to device communication is an ideal focus to increase quality of service. In this work, a recent implementation of a secure authentication scheme is partially replicated and tested under various size hashes for performance analysis of vehicle to vehicle authentication. Results point to a potential 13%-49% increase in vehicle identification and authentication stages while maintaining a relatively secure scheme in regards to hash collisions of the message signing stage at the bare minimum. Performance can potentially increase as well depending on the factors such as the testing technology utilized, though regardless, modulating the scheme for operation variants on SHA254 and SHA256 would be optimal. Potential alterations to the schemes would be the reduction of overhead through the substitution of RSA in favor of light way symmetric cryptographic schemes.

Reference

References and Works Cited are available through the following QR code .

This material is based upon work supported by the National Science Foundation under Grant No. 2034030 and 1834620. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

September, 2020