Cryptography in Hardware

Terence O'Brien, Ian Perry

***Abstract*—Since the beginning of recorded history, the act of procuring accurate information and utilizing it has marked the difference between those organizations which fail, and those which succeed. Nowhere is this more evident than in adverserial situations. The side which is able to learn the disposition of an enemy force while concealing their own is at a great advantage [1]. As history has progressed, the simple act of hiding information has ceased to be an effective option, and methods of obfuscating, or encrypting, that information has given birth to the field of cryptography. In the modern age, cryptography is used daily by the majority of the population through the usage of ecommerce, email, or any number of secured web sites. This ubiquitous usage has created a situation where quickly processing many crypotraphic requests at once is necessary, but by its nature, these requests are computationally expensive. This is where hardware extensions which implement cryptography come into play. This paper will explore the current state of cryptographic hardware, it's role in modern usage, and the required background information to understand it.**

***Keywords*—IEEE, Cryptography, Information Theory.**

I. Introduction

THIS is the intro blahblah blahblahblahblah blahblahblah-blah blahblah blahblah blahblahblahblah blahblahblah-blah blahblahblahblah blahblahblahblah blahblah I wish you the best of success.

II. History of Cryptography

III. Cryptography Basics

A review of the basics of cryptography as a whole is beyond the scope of this paper. To do that topic justice would require an entire paper in itself. Thus, the basics of modern cryptography as it applies to an understanding of its implementation in hardware will be presented.

Modern cryptography hinges on the use of four main functions, symetric encryption, asymetric encryption, hashing, and random number generation. Symetric encryption is method most often thought of when encryption is mentioned. It is the use of a single key to both encrypt and decrypt a message. Both user's must have the same key, and it must be shared in some fashion. This has classically been a limiting factor in the adoption and usage of cryptography.

In order to ensure a key as not been lost to the adversary, key sets must be periodically changed, which entails distributing entire new sets of keys, or having large tomes with predetermined keys available. This is an enormous burden which grows roughly exponentially

M. Shell was with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332 USA e-mail: (see http://www.michaelshell.org/contact.html).

J. Doe and J. Doe are with Anonymous University.

Manuscript received April 19, 2005; revised August 26, 2015.

A. Symmetric Key Encryption

B. Asymetric Key Encryption

C. Hashing Functions

D. Random Number Generation

IV. Standalone Cryptographic Hardware

A. Secure Cryptoprocessors

B. SSL Acceleration

C. Hardware Security Modules

V. Instruction Set Extensions

VI. Conclusion

The conclusion goes here.

References

[1] S. Tzu, "A quote from the art of war," in Good Reads, Goodreads, 2015. [Online]. Available: http://www.goodreads.com/quotes/744436-conceal-your-dispositions-and-your-condition-will-remain-secret-which. Accessed: Dec. 13, 2016.