BLOCK CIPHERS FOCUS ON THE LINEAR LAYER

Introduction

Although the original purpose of the Internet is to serve science, the commercialization integrates its services and technology into all aspects of modern life. However, the Internet represents an insecure channel of information exchange which lead to a high risk of intrusion or fraud, such as phishing, online viruses, trojans, worms and more. Hence, one of the biggest hurdles when it comes to the Internet is that of security. Many methods are used to protect data transfer, including encryption and from-the-ground-up engineering. One of the most widely used ciphers, AES, is usually considered a fast, lightweight block cipher that can be found even on-chip credit cards that protect one's financial transactions. Not only does AES offer robust security, but its structure also inspired many cipher designs ever since. Fast and lightweight are related terms when compared to worn-out passwords such as DES; however, in the case of embedded systems, AES still exists when used on 8-bit or 16-bit microcontrollers, the password is too large and speed slow microprocessor.

On October 5th, 2018, Dr. Yalçin presented his work to everyone in the INF501 course in Northern Arizona University. Dr. Yalçin's research explores the genuinely fast and lightweight cryptographic ciphers that are both secure and efficient for use on embedded systems.

Research Topic Overview

Block ciphers in cryptosystems are one of the most prominently used cryptographic primitives, and the linear layer is a core component in any substitution-permutation network block cipher. The Advanced Encryption Standard (AES) is a significant step forward in the field of block cipher design. Not only does AES offer robust security, but its structure also inspired many cipher designs ever since. Dr.Tolga's research is focused on the methodology to construct functional, sometimes optimal, linear layers allowing for a large variety of trade-offs.

As it stands, there are two general ways for the design of linear layers. The first one is to design it in a somewhat ad-hoc fashion, without following the general layout. This method might result in very secure and efficient algorithms, but it is not very well-pleasing from a scientific point-of-view. Another general design strategy is the wide-trail strategy which the main idea is to link the number of active S-boxes for linear and differential cryptanalysis to the minimal distance of a particular linear code associated with the successive layer of the cipher. However, there are virtually no general constructions or guidelines that would allow a substitution-permutation network (SPN) design to benefit from security vs. efficiency trade-offs. In response to this, Dr.Tolga's research and presentation is centered on the linear layer construction, and top underlines its value by presenting a new block cipher. Using such an approach to uncover alternative methods for 8-bit micro-controllers will significantly enhance the capabilities regarding code size and cycle count.

The application of linear layers is rooted in a simple and powerful applicability concept that a block-interleaving construction which allows combining several strong linear mappings on a few numbers of bits into a robust linear layer for a more significant amount of bits. An optimal trade-off between hardware-efficiency and the number of active S-boxes is the point in which the concept of the most efficient linear layer theory is being incorporated into the algorithm development outlined in Dr.Tolga's presentation. Dr.Tolga also explained that by designing a new block cipher named PRIDE that significantly outperforms all existing block ciphers of similar keysizes. The key points here is that our construction of strong linear layers is nicely in line with a bit-sliced implementation of the S-box layer.

Discussion

I was able to distinguish some critical connections between my INF638 class which is cryptography and cryptosystems with Dr. Bertrand Cambou and that of Dr.Tolga's research. Since a significant portion of my course is focused on the underlying motivation, definition, and application of cryptography and cryptosystems.

In INF638, I know that the cipher algorithm (or cryptographic algorithm) is a means of changing data from a readable form (also known as plaintext) to a protected form (also known as ciphertext) and back into a readable form. There are two main types of a cipher: stream ciphers and block ciphers. In a stream cipher, each plaintext digit is encrypted one with the corresponding number of the keystream to give the ciphertext stream number. A block cipher applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encoding one bit at a time as in stream ciphers. Such as Dr.Tolga said, even there are so many ways to block ciphers, but the modern approach is the substitution-permutation networks (SPNs). However, as it stands, the most method has been placed on the substitution (confusion or non-linear layer) phase, whereas there hasn’t been much in the way of permutation (diffusion or linear layer) phase.

While cybersystems must consider security, there lies another problem: a balance point between safety and efficiency. Understanding linear layer -based algorithms to determine a balance point between safety and efficacy could be of vital importance. More specifically, the evolution of the linear layer could essentially emulate applications of cryptosystem theory in that what is best for a single cryptograph method will likely be the best for all given a specific set (security and efficiency) of minimal sacrifices. The critical point at here is the public-key infrastructure.

In 1976, Whitfield Diffie, Martin Hellman|Hellman, Ron Rivest, Adi Shamir, and Leonard Adleman and others announced the security key exchange and crucial asymmetric algorithm, and the entire communication method changed. A public-key infrastructure (PKI) is a system designed to transmit encryption keys over a secure or insecure channel. These keys can then be used to encrypt messages back and forth, thereby independently acquiring new keys from which to communicate or communicate directly with the keys themselves. With the development of high-speed electronic digital communication, users are increasingly demanding secure connection. The higher the security of the system, the longer it takes to run the algorithm. Therefore, we can focus on creating a system that can adequately generate a public key that balances security and efficiency.

Conclusion

Most research in cryptography and cryptosystems would only focus on the pure strength and security of the algorithms designed. Safety and efficiency have long been trade-offs in the cryptography. The security of cryptosystems, whether it is physical screening or requirements for the transportation of message, requires time, money, and workforce. Efficiency, the ability to transfer the message with the least amount of delay, requires different types of investments of time, money, and manpower. While establishing a balance between security and efficiency has always been a difficult job for the designer, as the number of inefficient systems continues to increase, researchers have to consider new ciphers not only for today but also for further use. By learning from the design principles of PRIDE, I plan to apply them toward my project on INF638.

Reference

1. Albrecht, Martin R., et al. "Block ciphers–focus on the linear layer (feat. PRIDE)." International Cryptology Conference. Springer, Berlin, Heidelberg, 2014.
2. Kavun, Elif Bilge, Gregor Leander, and Tolga Yalcin. "A reconfigurable architecture for searching optimal software code to implement block cipher permutation matrices." Reconfigurable Computing and FPGAs (ReConFig), 2013 International Conference on. IEEE, 2013.