MS Thesis Preproposal

Nonlinear Construction Criteria for Symmetric-Key Cryptographic Algorithms

Christopher A. Wood
Committee Chair: Professor Stanisław Radziszowski
Department of Computer Science, Rochester Institute of Technology
June 16, 2012

1 Background and Motivation

The cryptographic security of symmetric-key cryptographic algorithms is based upon Shannon's principles of confusion and diffusion [3]. Confusion can be defined as the complexity of the relationship between the secret-key and ciphertext, and diffusion is commonly referred to as the degree to which the influence of a single input plaintext bit is spread throughout the resulting ciphertext. When designing new cryptographic algorithms, it is important to optimize these characteristics to make the algorithms less susceptible to common attacks, such as linear and differential cryptanalysis.

Collectively, linear and differential cryptanalysis become less effective as the levels of confusion and diffusion within a symmetric-key cryptographic algorithms are increased. Combinations of linear and nonlinear operations are the standard means by which high measures of confusion and diffusion are realized in symmetric-key cryptosystems, with the S(ubstitution)-box being the most popular nonlinear component used by cryptographers [2].

An S-box is a well-defined function that maps elements in the domain $\mathbb{F}_2^n$ to elements in the range $\mathbb{F}_2^m$. There are, however, other discrete nonlinear functions that are commonly utilized in cryptographic algorithms in place of S-boxes due to their susceptibility to cache-timing attacks. The Addition-Rotation-XOR (ARX) class of functions is one such example that relies on traditional addition with a carry bit, bitwise rotation, and the bitwise XOR operation to attain appropriate measures of nonlinearity after many iterations through the function [4].

In addition to the theoretical correctness and security of these nonlinear operations inside cryptographic algorithms, cryptographers must also consider implementation techniques in both hardware and software that will execute them with high measures of performance. As the sophistication and complexity of modern side-channel attacks increases, such practical issues place constraints on the theoretical construction of cryptographic algorithms and how they are realized in practice. For example, the high-performance T-box implementation of the Advanced Encryption Standard (AES), along with most other lookup-table implementations of cryptographic algorithms, have been proven to be susceptible to cache timing attacks in software. While the algorithm is theoretically secure, this simple side-channel attack indicates that perhaps S-boxes are not the best approach to achieve nonlinearity in cryptographic algorithms and that other functions should be considered.

2 Research Objectives

The mathematical design and cryptographic strength of nonlinear functions used in cryptographic algorithms, which are commonly referred to as the nonlinear layer in such algorithms, has been the focus of extensive research in recent decades. The result of this research has been a very thorough set of design criteria and guidelines for cryptographic algorithm designers that can be followed when formulating a new algorithm, where these design criteria and guidelines are the direct result of cryptanalysis attacks on existing cryptographic algorithm designs. Naturally, with this reactive approach to the security design criteria for nonlinear functions used in cryptography, we can see that there are still elements in the design space left to explore.

Furthermore, with the many theoretical and practical constraints placed on cryptographic algorithms in mind, it has become increasingly difficult to not only construct, analyze, and prove the security of strong cryptographic algorithms with high measures of confusion and diffusion. Therefore, the major objective of

this thesis is to advance the nonlinear construction criteria, design space, and implementation techniques for use in cryptographic algorithms. This work involves the following action items:

- Study the construction criteria for S-boxes (with a focus on the Rijndael S-box)
- Attempt to formulate new security requirements for S-boxes
- Conduct an in-depth literature survey of the number theoretical and combinatorial design criteria for general nonlinear functions used in cryptographic algorithms
- Study and experiment with alternative discrete nonlinear functions for the Rijndael nonlinearity requirement
- Formulate the construction of S-boxes as MINLP problems and solve for optimal designs that can be replicated with fast and efficient discrete mathematical operations
- Implement various nonlinear functions in software and hardware and analyze the corresponding performance and cost

The Rijndael algorithm will play a crucial role in the completion of this work, as its bed of extensive theoretical and practical research has been extensively developed since its standardization as the AES in 2001 [1].

3 Research Plan

Throughout the course of this work I plan to produce an extensive set of documentation that details the results of my literature survey surrounding the design criteria and security requirements for nonlinear functions used in cryptographic algorithms, as well as the practical implementation techniques and successful attacks that have exploited weaknesses in the chosen nonlinear function designs.

In addition, I will develop a large software test-bed that will streamline the experimentation of various nonlinear functions within common cryptographic algorithms, with the primary target being Rijndael. This will include, time permitting, a cryptanalysis attack framework that can be used to replicate published attacks on the selected cryptographic algorithms in order to test the security strength of the various nonlinear functions that will be studied. In addition, since hardware designs for cryptographic algorithms will be another significant portion of the project, I plan to work develop custom hardware designs for these nonlinear operations that easily integrate with existing algorithms designs and test their performance. Unfortunately, due to time constraints, I will not be performing an in-depth study or analysis of published side-channel attacks against these modified algorithms.

References

[1] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.

[2] J. Daemen and V. Rijmen. *The Design of Rijndael*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2002.

[3] K. Kim. A Study on the Construction and Analysis of Substitution Boxes for Symmetric Cryptosystems, 1990.

[4] V. Velichkov, N. Mouha, C. D. Cannière, and B. Preneel. The additive differential probability of arx. In *FSE*, pages 342–358, 2011.