Optimizing Diffusion and Confusion in Cryptographic Primitives

M.S. Thesis Proposal

Christopher Wood

March 31, 2012

1 Objectives

The following list enumerates some long-term goals from this research effort.

- (THEORY) Study the mathematical theory behind diffusion and confusion, stemming from Shannon's communication entropy and the use of nonlinear functions in cryptographic primitives.
  - Question: Can discrete-time dynamical system equations be utilized effectively as diffusion layers? [2]
  - Question: To what extent does the study of chaos theory lend itself to constructing effective diffusion layers in cryptographic primitives? [2]
  - Question: Are there any other unpopular or unused discrete mathematical objects that can be used to build (fast and secure) diffusion layers with high nonlinearity properties? [6] [5] [4]
- (THEORY) Analyze and evaluate existing cryptographic algorithm design mechanics that promote high diffusion and confusion through nonlinearity.
  - Substitution-Permutation Network designs (SPN).
    - Skein
  - Add-Rotate-XOR (ARX) designs.
    - Rijndael
  - Question: Can existing sources of nonlinearity (S-boxes, ARX functions, etc) be manipulated to provide higher measures of diffusion without affecting their susceptibility to linear and differential cryptanalysis?
  - Question: What diffusion layer designs provide the best security and performance tradeoffs? Can this be mathematically proved or solved by reduction to an integer optimization problem?

- (THEORY/SOFTWARE) Investigate the application of combinatorial and integer optimization techniques to block cipher designs and internal operations.
  - Question: Can diffusion layers be represented as multivariate polynomial equations, and if so, can we apply common optimization techniques to find the most effective constructions?
  - Question: How can such optimization techniques be extended to the cryptanalysis of block ciphers?
- (THEORY/SOFTWARE) Perform a statistical and randomness analysis on existing diffusion layers in cryptographic primitives.
  - Question: To what extent can the statistical properties of diffusion layers be extrapolated to full-round cryptographic primitives?
- (SOFTWARE/HARDWARE) Investigate the implementation aspects of chosen diffusion layers
  - Explore optimization techniques for different software and hardware implementation mediums (but limit to reconfigurable hardware - FPGAs) [1] [3]

References

[1] *Cryptographic engineering.* Springer, New York, 2009.

[2] *Chaos-based cryptography theory, algorithms and applications.* Springer, Berlin, 2011.

[3] Francisco Henriquez. *Cryptographic algorithms on reconfigurable hardware.* Springer, New York, 2006.

[4] Kaisa Nyberg. Perfect nonlinear s-boxes. In *Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'91, pages 378–386, Berlin, Heidelberg, 1991. Springer-Verlag.

[5] Deng Tang, Weiguo Zhang, and Xiaohu Tang. Construction of balanced boolean functions with high nonlinearity and good autocorrelation properties. Cryptology ePrint Archive, Report 2010/362, 2010. `http://eprint.iacr.org/`.

[6] WeiGuo Zhang and GuoZhen Xiao. Construction of highly nonlinear resilient boolean functions satisfying strict avalanche criterion. Cryptology ePrint Archive, Report 2010/579, 2010. `http://eprint.iacr.org/`.