MS Thesis Progress Report

Large Substitution Boxes with Efficient Combinational Implementations

Christopher A. Wood

Committee Chair: Professor Stanisław Radziszowski

Department of Computer Science, Rochester Institute of Technology

February 21, 2013

1 Progress

- Implemented two of Nyberg's three *differentially uniform* mappings in software (differential uniformity is an indication of the probability of finding a non-zero output difference $\beta \neq 0$ for all input pairs $(x + \alpha, x)$ - this is critical for differential cryptanalysis to work):

$$F(x) = x^{-1}$$
$$F(x) = x^{2^k+1}$$

- Decided to limit measurement scope to nonlinearity, resiliency, correlation immunity, and differential uniformity.
- Started hardware design for 16-bit S-box using composite fields $GF((2^8)^2), GF(((2^4)^2)^2), GF((((2^2)^2)^2)^2)$.

2 Upcoming Work

- The software and hardware testbeds need to be completed first as they will enable different functions to be analyzed - HARD deadline of week 5 in spring quarter.
- Extend SAC construction techniques to vectorial Boolean functions (functions of the form $GF(2^n) \rightarrow GF(2^m)$ can be defined as $F(x) = (f_1(x), ...f_m(x))$, where $f_i(x) : GF(2^n) \rightarrow GF(2)$).
- Find other Boolean function constructions for experimentation (high nonlinearity, resiliency, satisfaction of propagation criteria, and correlation immunity) that can extend to 16-bits.
- Determine what properties Sage and *boolfun* can measure and write the software for the rest.

3 Questions and Concerns

- How do the cryptographic measurements change when looking at vector Boolean functions as opposed to one-dimensional Boolean functions?
- The isomorphic mapping δ to and from composite field elements is unclear. Is it enough to "split" the elements in half? For example, is $\delta(\{10010110\}_2) = \{1001\}_2 x + \{0110\}_2$ a valid isomorphism? Some papers seem to suggest so [1].
- I need to find an effective way to check all irreducible polynomials for composite field construction. That is, for the field $GF(2^n)$ defined over $GF(2)$ by $P(x)$, I need to find all polynomials $Q(y)$ that can be used to build $GF((2^n)^m)$ over $GF(2^n)$.

References

[1] E. N. Mui. Practical Implementation of Rijndael S-Box using Combinational Logic. *Texco Enterprise Ptd. Ltd,[Online]. Available: http://www. xess. com/projects/Rijndael_SBox. pdf*, 2007.