Reconfigurable Hardware Implementations of the Rabbit Stream Cipher

Background and Objective

Reconfigurable hardware implementations of stream ciphers is essential for 1) their evaluation in mobile and embedded devices, and 2) the use of field programmable gate arrays (FPGAs) for many-stream cryptanalysis applications.

The Rabbit stream cipher is among four software-oriented stream ciphers which were selected for the eSTREAM software portfolio in 2008. Its strength against modern attacks and high throughput in software makes it a desirable candidate for hardware applications requiring fast and strong cryptographic primitives.

Rabbit Stream Cipher Design

- Additive synchronous cipher
- Strong security properties
  - 128-bit key support
  - No attacks < exhaustive key-search
- Counter-assisted design
- Minimum period guaranteed
- Chaos-inspired (g function)
  - Highly non-linear state update
- AES (128-bit key support)

Key IV

Counter & State Update

Keystream Extractor

Keystream

Hardware Implementations and Results

We implemented the g function using three DSP48 slices, four 32-bit adders, and one 32-bit XOR.

We further compacted the 8-GFS design by modifying it for variable output rate (denoted by V).

The presented place & route results of various Rabbit designs were implemented using System Generator and Xilinx XST (ISE 11.1). Although we use a new-generation FPGA, for completeness we compare against one of the fastest AES implementations and previous eSTREAM hardware-oriented stream cipher results.

Virtex 5 Results

- First hardware implementation of Rabbit
- Generic hardware framework for Rabbit cipher, supported by various implementations appropriate for
  - Very high-speed applications
  - Resource-constrained environments
- Alternative to hardware-oriented eSTREAM candidates

References: