

Review of:

Experimental Testing of the Gigabit IPsec-Compliant
Implementations of Rijndael and 3-DES Using SLAAC-1V
FPGA Accelerator Board

- Paper by:
 - Pawel Chodowiec (George Mason) Kris Gaj (George Mason), Peter Bellows (USC) and Brian Schott (USC)
- Published in:
 - Information Security Conference
 - October 2001
- Original copy on-line as:
 - <http://ece.gmu.edu/crypto/publications.htm> (theoretically)
- Survey by:
 - Carlos Macián

The Challenge

- Implement a full suite of IPsec cryptographic transformations using the SLAAC-1V FPGA board

Style of the Paper

- A rationale on hw-implementation of cryptoalgorithms
- Description of their platform
- Implementation of both Rijndael and 3-DES
- Testing procedure
- Results

- It barely mentions related work
- The “further work” section is also very short

Rationale / Scenario

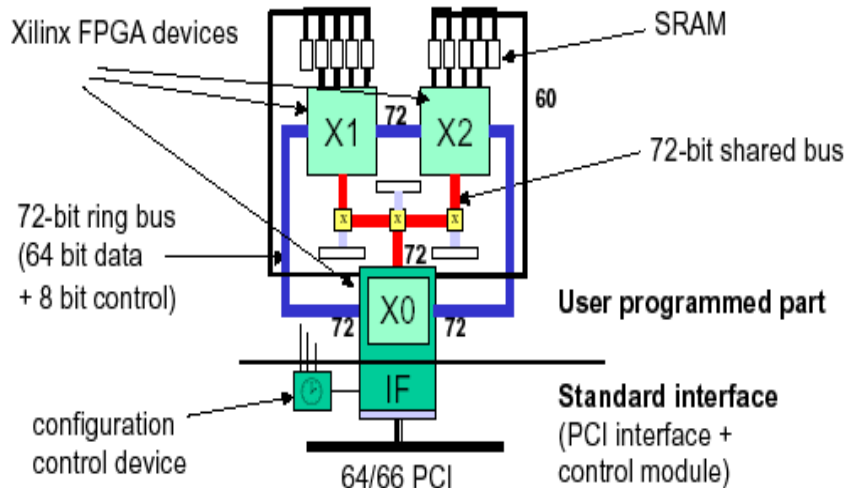
- Security Gateways for IPsec
 - Potentially very high number of simultaneous security associations
 - Cryptoalgorithms evolve rapidly
 - Line-speed necessary
 - Adaptability to changing conditions on-the-fly

- Well-suited to hw virtues!!
 - Typical number-crunching app.

SLAAC-1V Board (I)

- SLAAC project rationale: *Cluster computing*
 - Take PCs, add hw-accelerator cards and interconnect them with a high-speed LAN
 - Also usable in multi-processor systems
 - Also developed the management software
 - <http://www.isi.edu/licensed-sw/slaac/>
- SLAAC completely irrelevant for their work
 - Merely used as convenient programmable platform

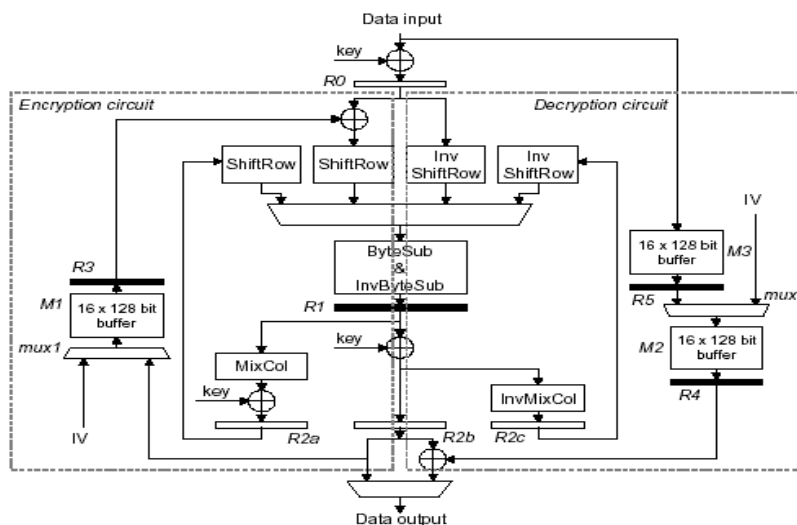
SLAAC-1V Board (II)



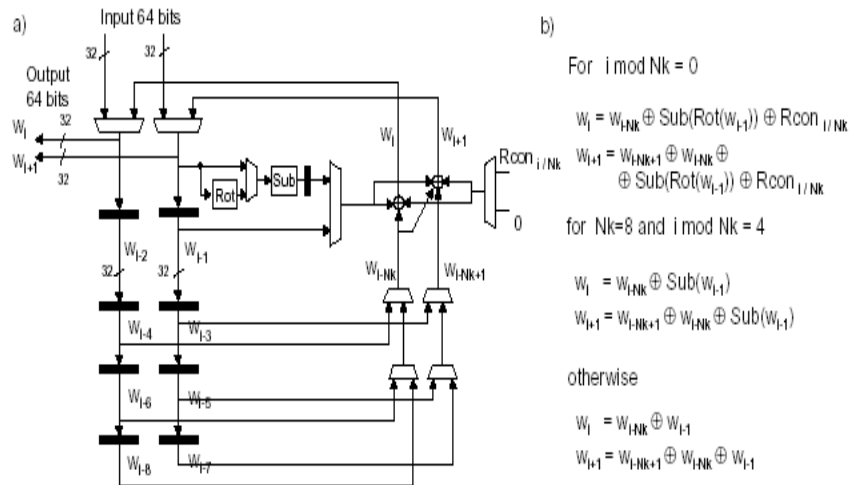
Rijndael Implementation

- Rijndael is the new IPsec cipher standard
 - Symmetric key
 - block cipher (several rounds per block)
 - variable key and block sizes
 - 4 component operations:
 - Byte Substitution (S-Boxes): Implemented using on-chip dual-port RAM
 - Shift Row: Routing only, no logic necessary
 - Mix Column: Express block as matrix and multiply on Galois Field by a known coefficient matrix.
 - Only XOR gates necessary!!!!
 - Add Round Key: XOR

Rijndael Circuit



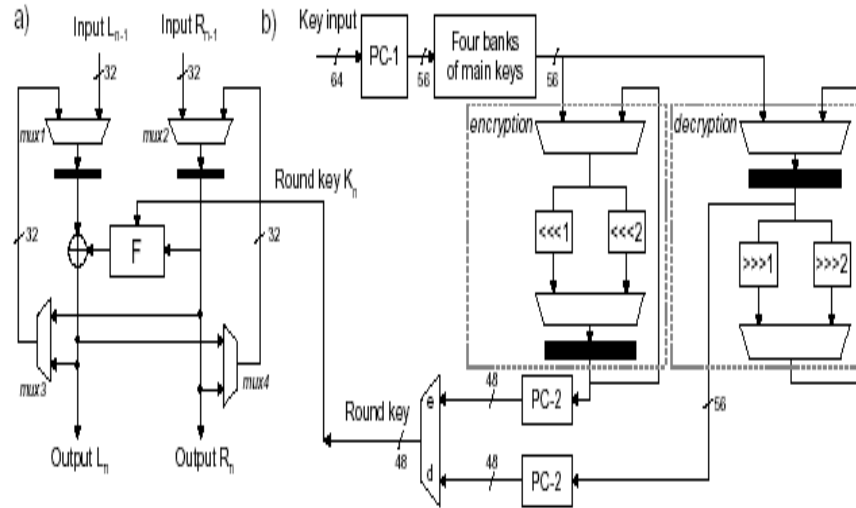
Key Generation Circuit



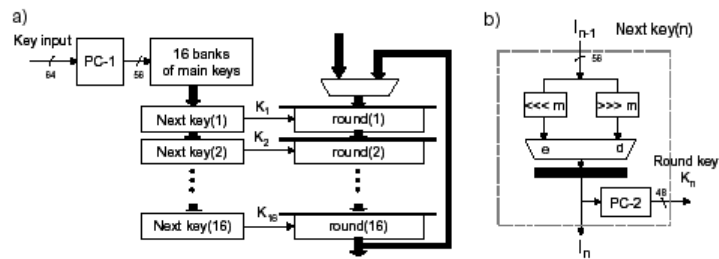
3-DES Implementation

- Same kind of cipher as Rijndael, but:
 - Fixed block and key sizes
 - Overall operations are simpler
 - Perfectly symmetric: Same operation repeated N times
 - Only one round needs to be implemented
 - Extended version: Loop-unrolling (16-stage pipeline)
 - S-Box implemented as logic, not memory
 - Key generation done on-the-fly

3-DES Circuit



3-DES Pipelined Circuit

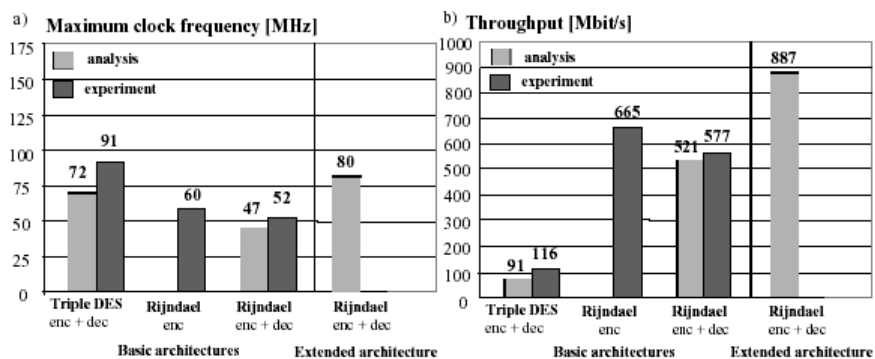


Testing Procedure

- 3 groups of tests:
 - Circuit functionality
 - Known Answer Tests and Monte Carlo tests
 - Maximum working frequency
 - Encrypt 1 GB of data at increasing speed until wrong behaviour
 - Throughput
 - Encrypt 4 GB of data at the maximum speed
 - PCI bandwidth limitation makes measurement somewhat “curious”

Results

- Expanded 1 Gbps circuits fit in a Virtex 1000
- Only basic architectures measured
- Curiously enough, the best possible results were not even extrapolated!!



Literature

- Literature to HW implementations of Rijndael is very concentrated
- References cover the (very specific) topic well
- Since no mention to further-going related work, no references, either

My View of the Paper

- Clear, focused and precise
- Meets its goals well: Explain their implementation of Rijndael and 3-DES in HW
- Solid construction: Architecture + Simulation + Implementation
- If you know the literature, this paper is not very relevant
- Why target 1 Gbps? Why not exhaust the possibilities of the architecture?