Dr. Johannes Wolkerstorfer

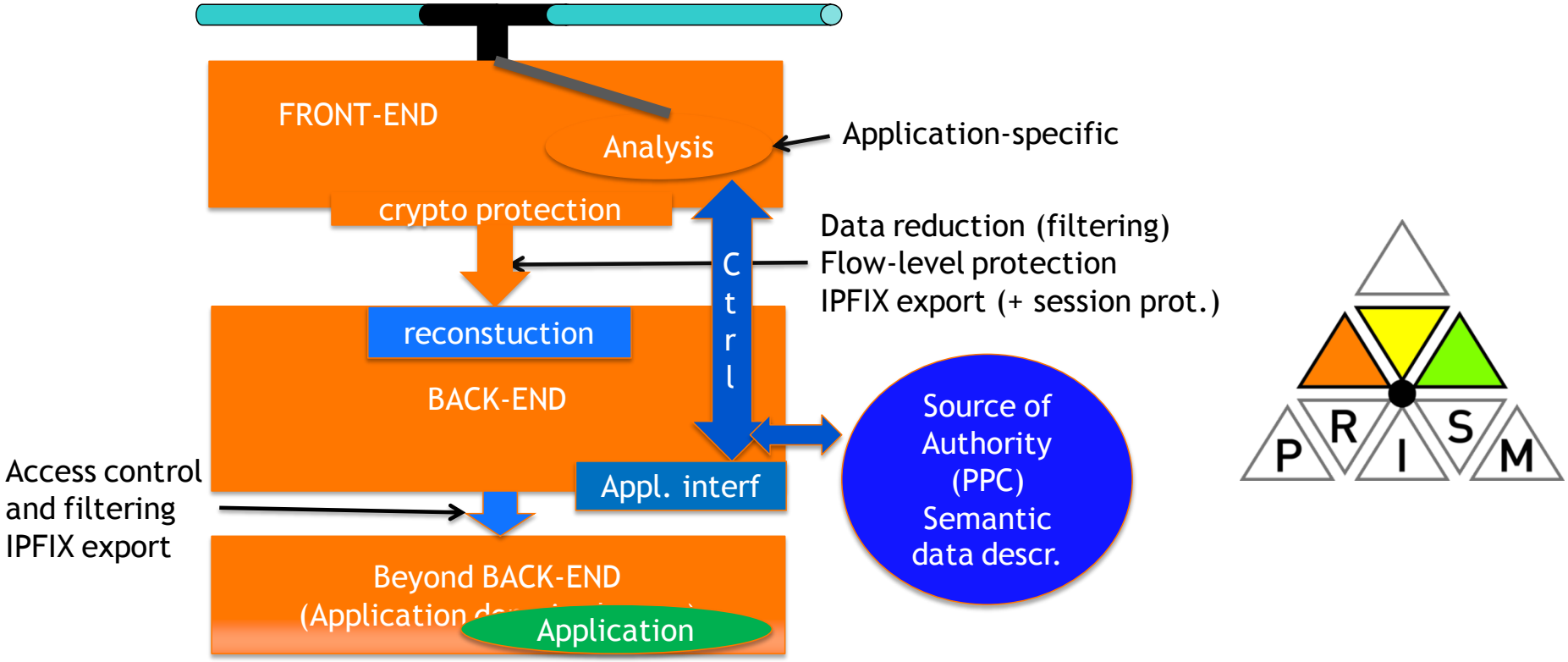
SECRET-SHARING HARDWARE IMPROVES THE PRIVACY OF NETWORK MONITORING

DPM 2010, Athens Vouliagmeni, 23 Sept 2010

Contents

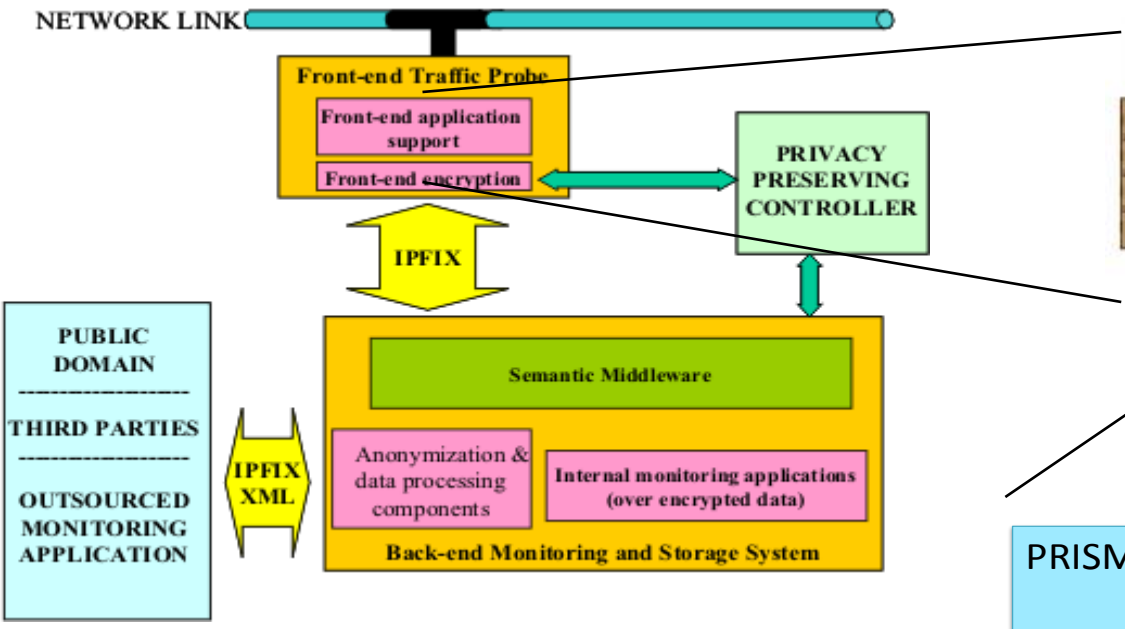
- Functionality and requirements
- Architecture / approach
- Optimizations
- Verification
- Results achieved

Problem: Network monitoring and privacy

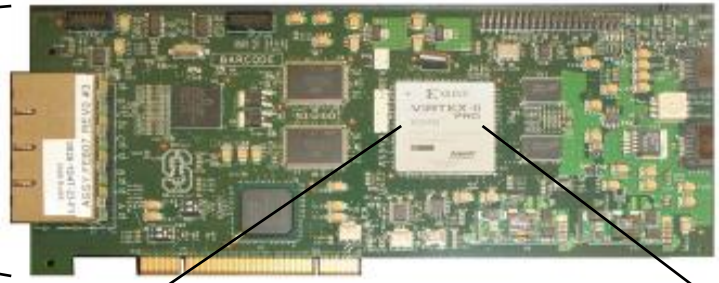


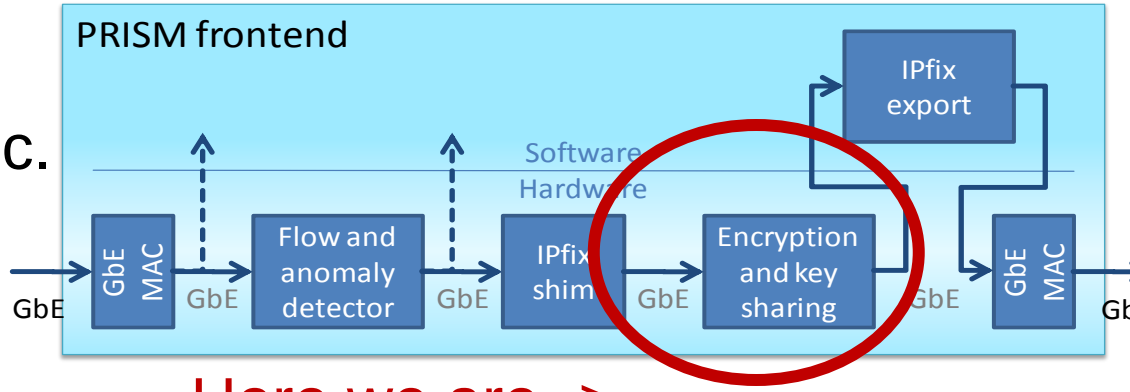
- Network monitoring stores private data (IP adr)
- PRISM approach: encrypt data (@ front-end)
  - Decryption (@ back-end) possible when enough evidence
  - Real analysis of decrypted traffic (@ beyond back-end)

Overview: HW for network monitoring



NetFPGA

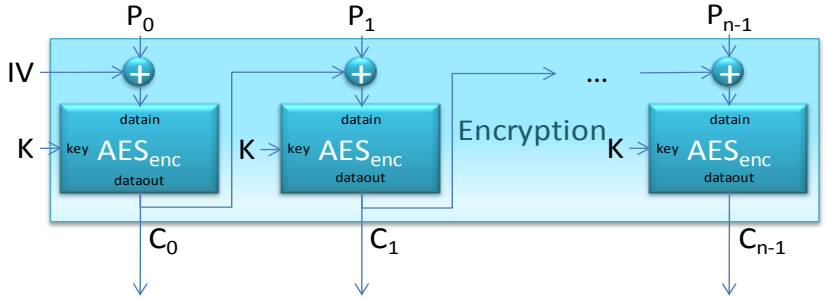




- Frontend: per-packet proc.
  - Flow extraction and anomaly detection
  - Cryptographic protection

Requirements: Functionality, …

- Bulk encryption
  - AES-128
  - CBC mode
  - PKCS padding
  - 1 Gbit/s



- Anomaly detection preamble
  - scramble flow identifier

- Secret sharing
  - Shamir's algorithm
  - over finite field GF(2191)
  - threshold ≤ 8

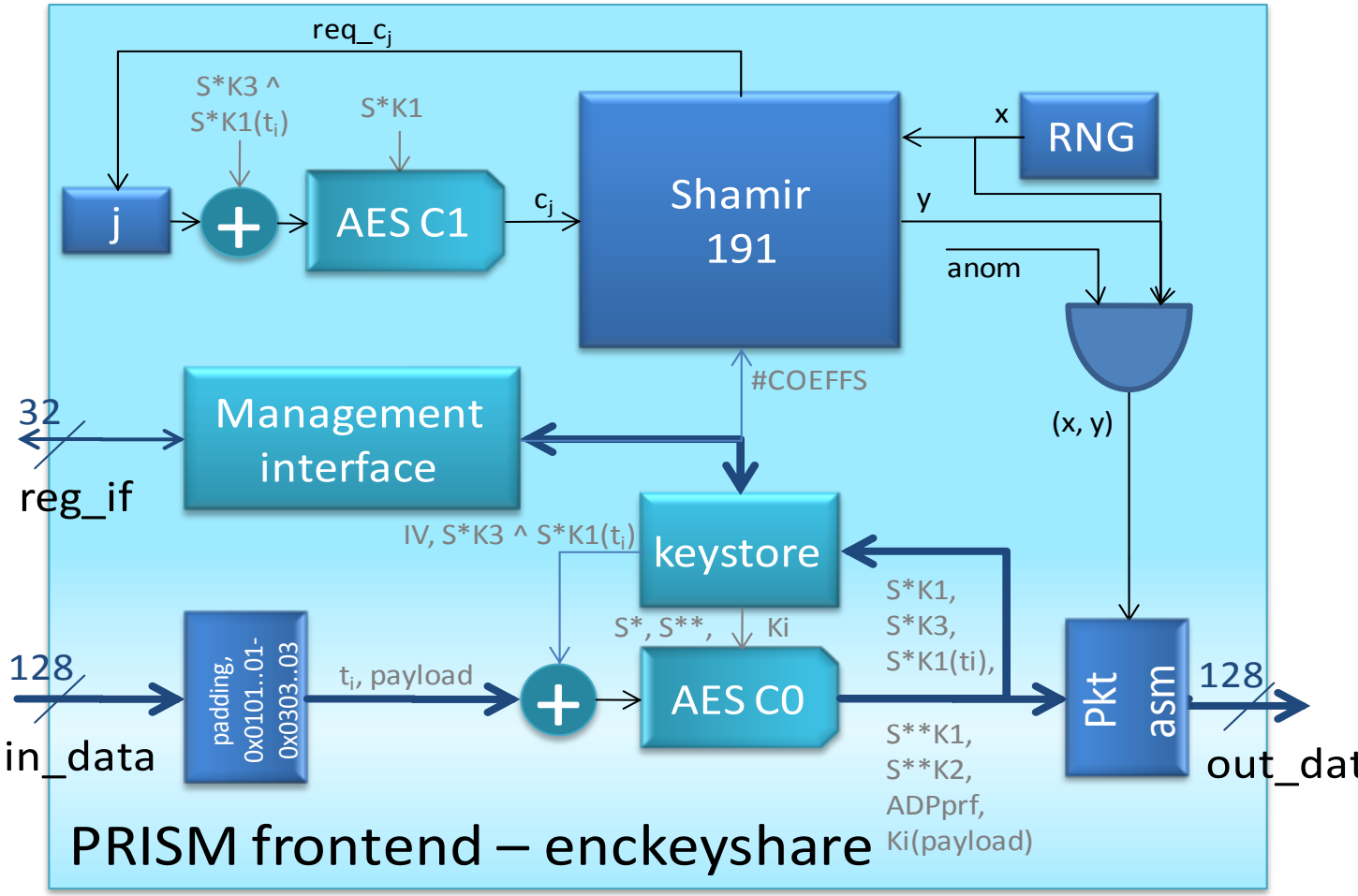
$$(x_i, y_i) = (x_i, P_f(x_i))$$

$$y_i = P_f(x_i) = a_{m-1}x_i^{m-1} + a_{m-2}x_i^{m-2} + \cdots + a_2x_i^2 + a_1x_i + a_0$$

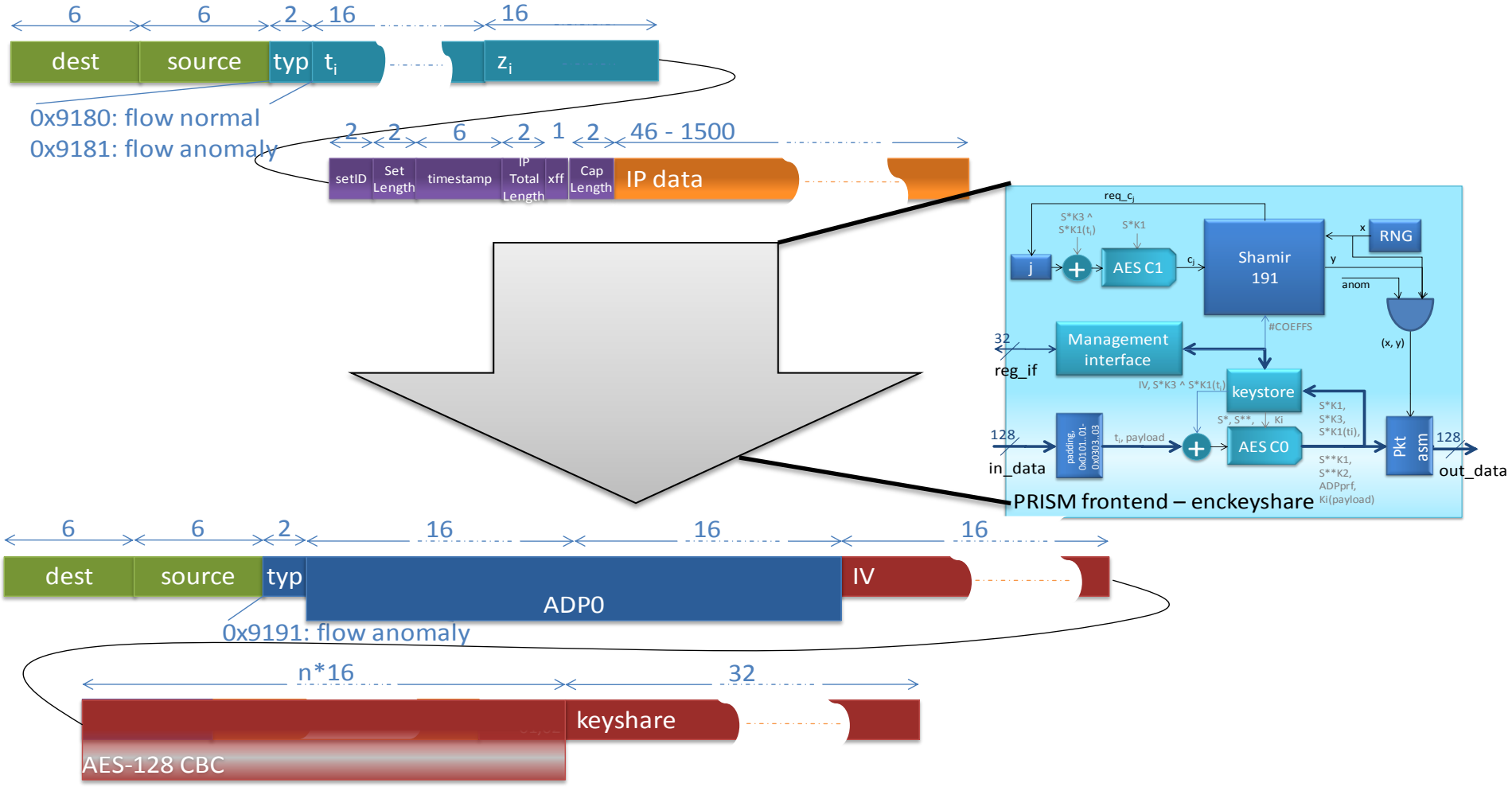
- Key / coeff generation
  - Derive key from flow identifier
  - Derive Shamir coefficients

Approach: Architecture

- AES units
  - AES C0
    - Key Ki
    - ADP
    - Bulk enc
  - AES C1
    - Shamir coeffs
- Shamir unit
- Mgmt interf.
- Reuse of AES C0

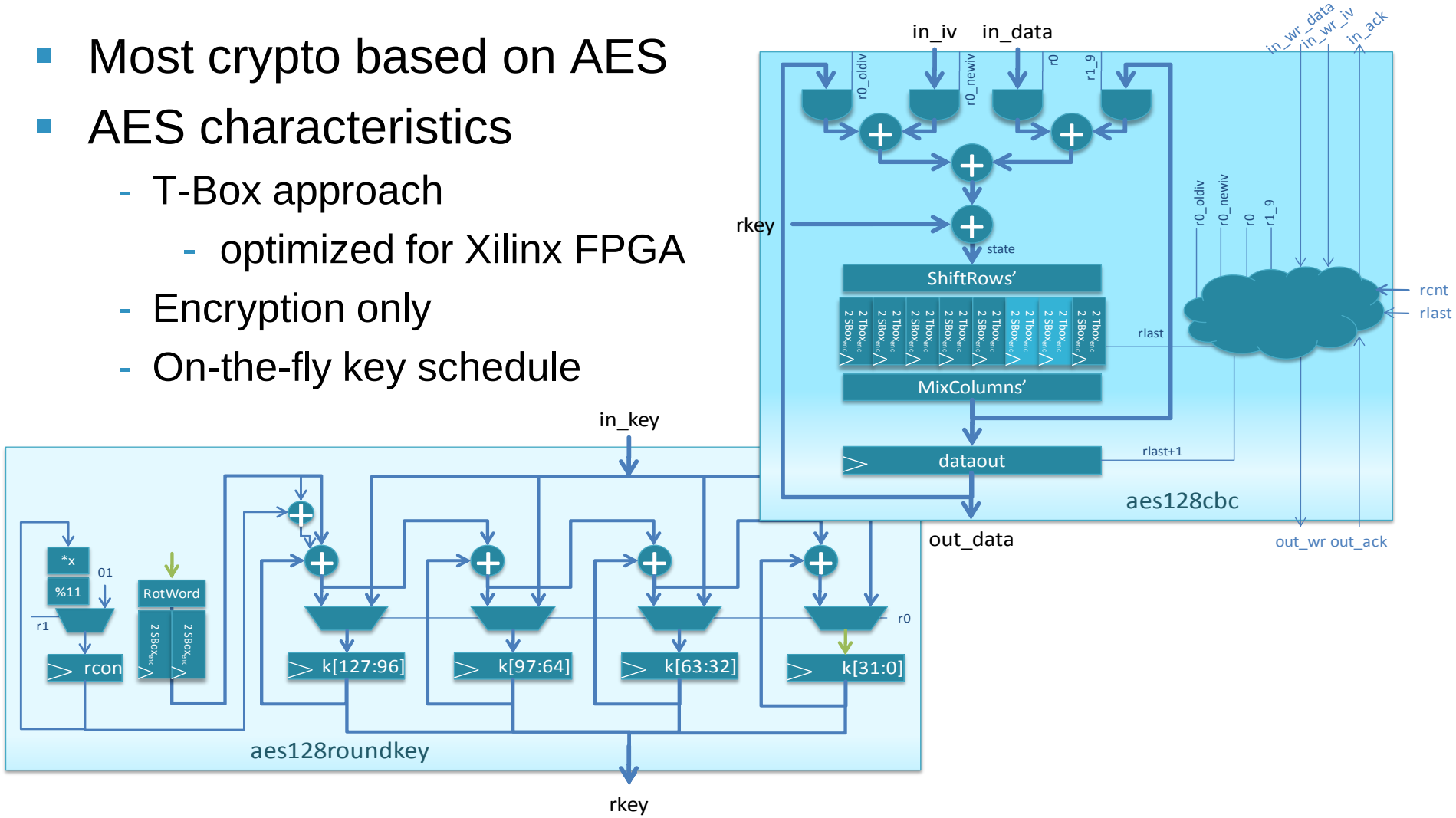


Example: Anomaly packet



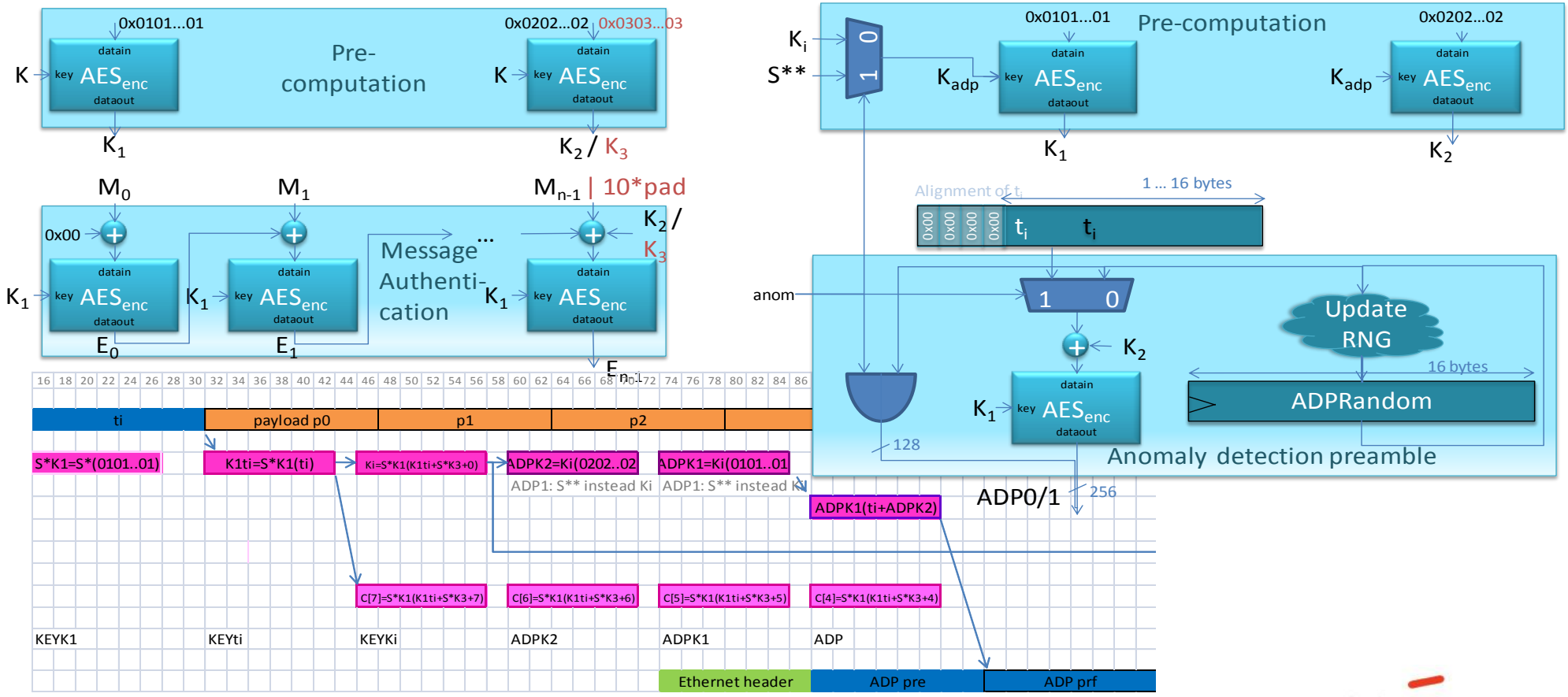
Details: Symmetric encryption

- Most crypto based on AES
- AES characteristics
  - T-Box approach
    - optimized for Xilinx FPGA
  - Encryption only
  - On-the-fly key schedule



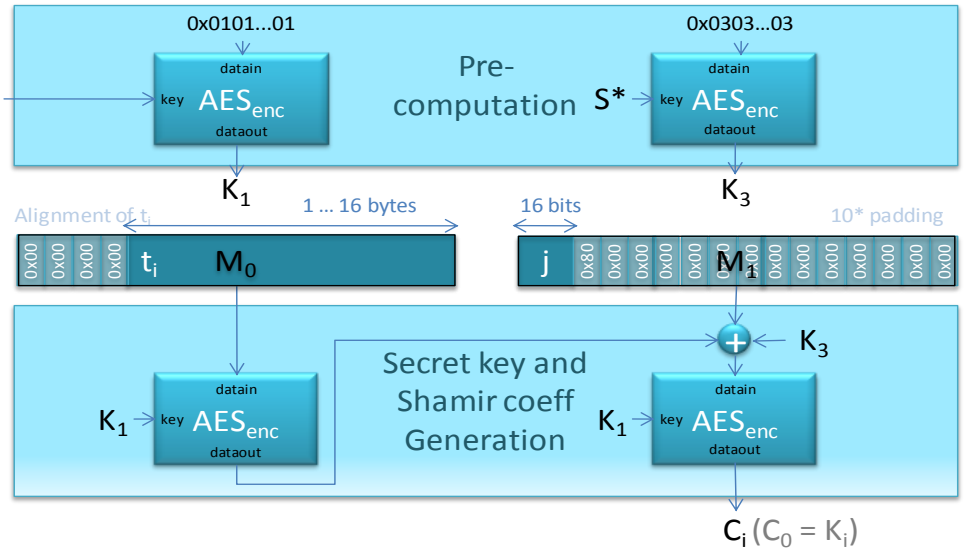
Details: Anomaly preamble

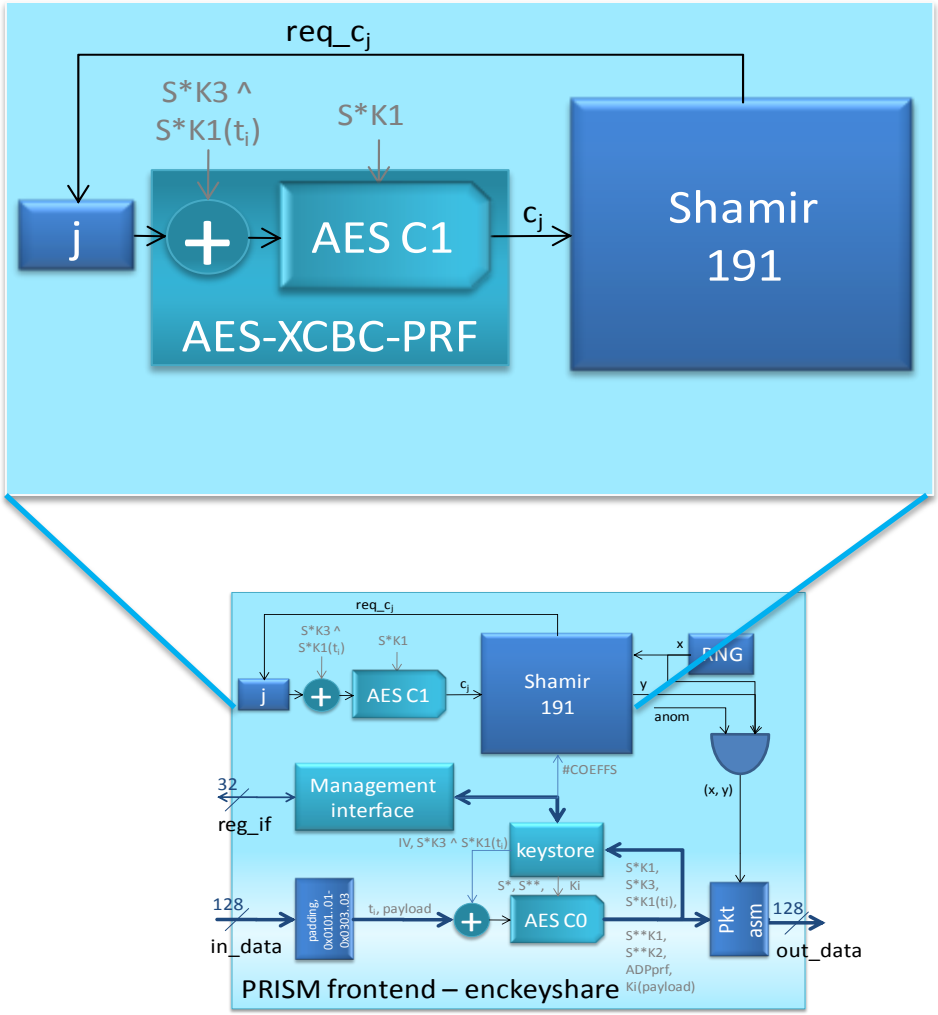
- AES-XCBC-PRF-128
  - as pseudo-random function



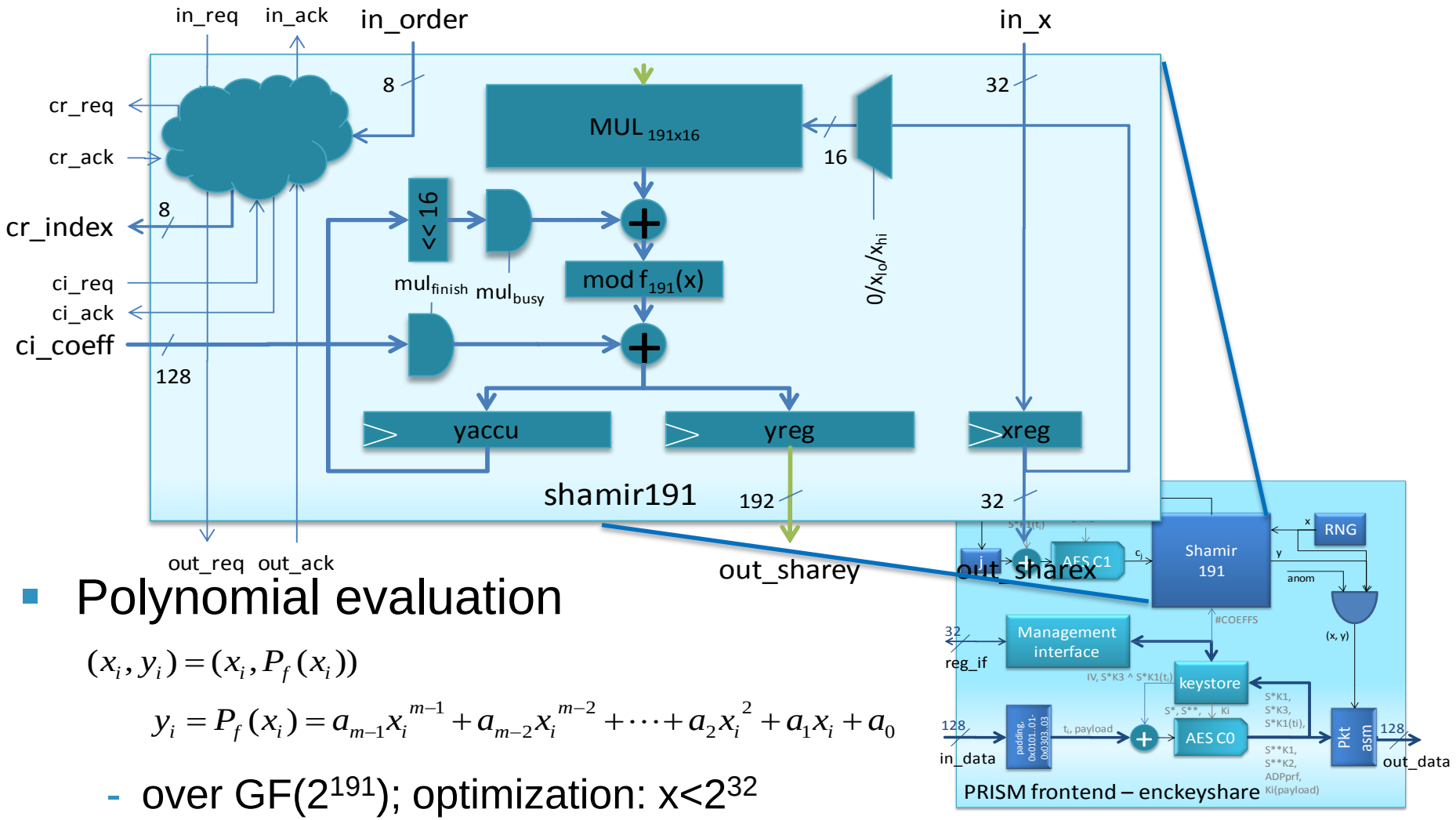
Details: Shamir coefficients

- Threshold: 0 … 8++
  - 1 … 9++ coeffs necessary
- Pipelined interface
- $c_i = PRF(S^*, t_i \mid j)$
  - AES-XCBC-PRF as PRF





Details: Keyshare generation



- Polynomial evaluation

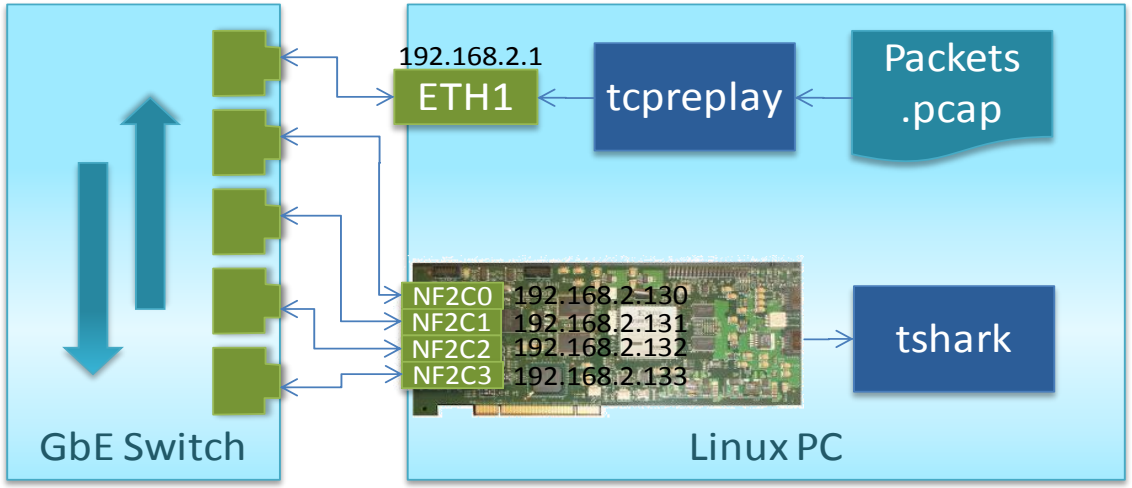
$$(x_i, y_i) = (x_i, P_f(x_i))$$

$$y_i = P_f(x_i) = a_{m-1}x_i^{m-1} + a_{m-2}x_i^{m-2} + \cdots + a_2x_i^2 + a_1x_i + a_0$$

  - over GF(2^{191}); optimization: x<2^{32}
  - Single-cycle 191x16 multiplier

Results: Size and performance

- Circuit size
  - achieved: 15% Virtex-II Pro 50 FPGA
- Performance
  - encryption: 1 Gbit/s
  - sh. secrets: 1.3 M / s (th=8)
- Conclusion
  - Feasible approach for monitoring Gigabit networks



Feature	Value enckeyshare	Val total	Remark
BRAM	18 (of 232: 7%)	18 (7%)	two AES cores (c0, c1) and one round-key generator
slices	3687 (of 23616: 15%)	7330 (31%)	mostly caused by Shamir unit (191*16 multiplier)
f_max	163.5 MHz	129.7 MHz	XST synthesis result
Throughput	1 GBit/s	1 GBit/s	maximum throughput @ f_clk=125 MHz
Latency	75 cycles (600 ns)		delay caused by enckeyshare; required inter-frame gap

Table. Results achieved by the enckeyshare unit on a Xilinx Virtex-II Pro 50