Yet Another Attack on Vest

Pascal Delaunay – Antoine Joux

date / references

- Side-Channel Attacks
  - Models of leakage
  - Side-Channel Attacks on Stream Ciphers
- VEST ciphers
  - Core components
  - Global system
- First Attack – Differential Analysis
  - Differential characteristic of the NLFSR
  - Application in the counter
- Second Attack – Simple Analysis
  - NLFSR-oriented curves to highlight biases
  - Information recovery
  - False prediction

- Attacks introduced in 1998 by *P. Kocher et al*.
  - *Differential Power Analysis*, CRYPTO'99
- Cryptographic algorithms performed on *untrusted* devices
  - Computers, smart cards, FPGA ...
- Attacks applied to many standards
  - Private key algorithms (AES, DES ...)
  - Public key algorithms (RSA, ECDSA ...)
  - ... few attacks on stream ciphers

- *"Affordable"* investment
  - Initial investment from 100 000 $ (equipment)
- Important flaws in cryptographic algorithms performed on embedded devices
  - Independent of the theoretical robustness of the algorithm
  - Based on implementation and operations performed
  - Secret data are subject to recovery
- The leak observed is related to the data handled
  - Models deeply studied
  - Depend on the implementation (software or hardware)

- Hamming weight model
  - The observed leak ω is related to the hamming weight H of the data d (the number of bits equal to 1 in a d-bits long word) handled by the device plus some noise b
  - $\omega = a\, H(d) + b$
- Hamming distance model
  - H is related to the hamming distance H_δ between the previous data p and the current data d handled by the device
  - $\omega = a\, H_\delta + b,\ H_\delta = H(p+d)$
- Validity of these models
  - Software : micro-controller registers, bus values ...
  - Hardware : flip flops (registers) storing values

- Traditional attacks (differential attacks)
  - E0 (bluetooth)
  - A5/1 (GSM communication)
- Refined attacks
  - Galois LFSR (Indocrypt' 06)
  - Traditional LFSR (Indocrypt' 07)
  - TRIVIUM, GRAIN (CT-RSA 07)
  - VEST (this presentation)

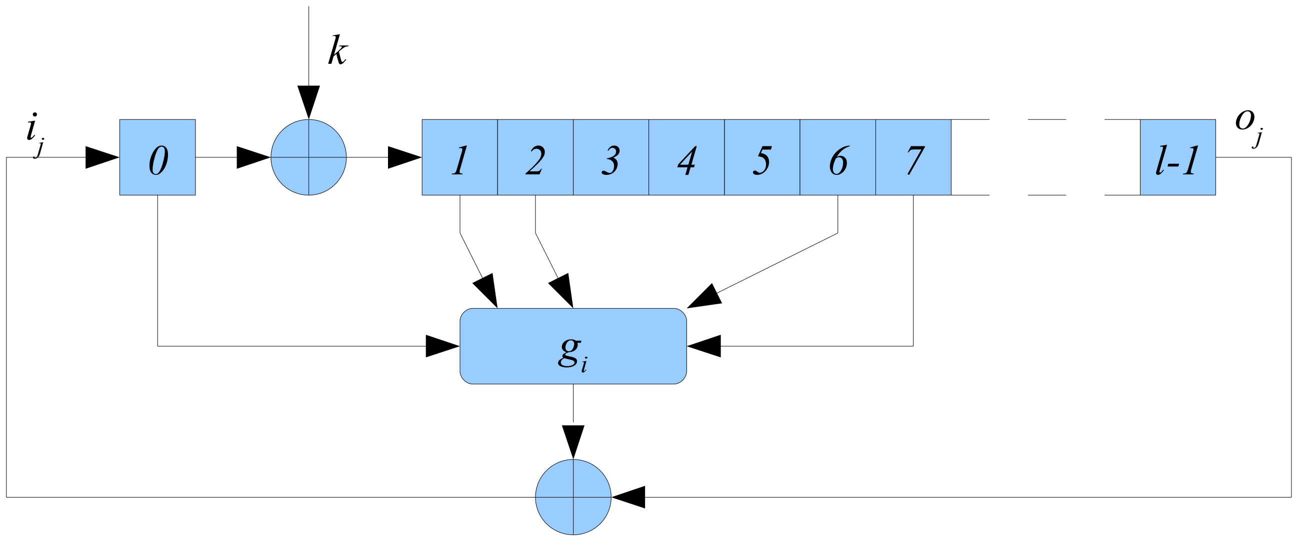
- Four Hardware dedicated stream ciphers

Family tree	***VEST 4***	***VEST 8***	***VEST 16***	***VEST 32***
Expexted security	80	128	160	256
Counter Size	163	163	171	171
Core Size	83	211	331	587
State Size	256	384	512	768
Speed (Gbps)	10	19	32	52
Min Gates	5K	9K	13K	22K

- E-STREAM project
  - Passed phase 1
  - Failed phase 2
    - **Overtaking VEST**, *A. Joux* and *J.R. Reinhard*, FSE 2007

- Facts
  - Minor change to thwart the attack (said it was a typo...)
  - Ciphers not free of use

- The counter
  - 16 NLFSR running in parallel
  - Traditional LFSR but g_i : non linear function
  - *l* either *10* or *11* bits long
  - *k* : data introduced (keying mode), 1 bit at each clock cycle



- Counter diffusor
  - Extracts 16 bits from the counter
  - Combines them to form 10 output bits
- Accumulator
  - Substitution and permutation of the internal state
  - First 10 bits XORed with the linear counter diffusor output
- Linear memoryless output combiner
  - Linearly combines the state of the accumulator
  - Outputs 4, 8, 16 or 32 bits (depends on the chosen cipher)

- Characteristics of the NLFSR
  - 10 or 11 bits long, unknown initial value
  - Plain text introduction during IV setup
  - NLFSR cells synthesized as flip flops
  - Differential analysis for all the initial values
    - Hamming weight model
    - Selection function : Hamming weight mean
    - After the sealing step (32 clock cycles)

Feedback Function	Length of the NLFSR	Length of IV	Number of IV	Validity of DPA	Closest ghost peak
0xDD1B4B41	11	2	4000	☑	11%
0xDD1B4B41	11	3	4000	☑	11%
0xDD1B4B41	11	2	10000	☑	8%
0x94E74373	10	2	4000	☑	10%
0x94E74373	10	3	4000	☑	9%
0x94E74373	10	2	10000	☑	6%

Validity of DPA : highest peak obtained for the correct initial state

Closest ghost peak : second highest peak proportion

- Whole counter
  - 16 NLFSR running in parralel
  - No cross computation, independent behavior
  - Target 1 NLFSR, others act as noise
  - Require substantially more IV for the same SNR

Number of IV	Length	Mean of closest ghost peaks	Highest ghost peaks
10000	16	12%	14%
10000	24	12%	14%
20000	16	9%	10%
35000	16	6%	7%

- Conclusions
  - 16 bytes of IV (2 for each NLFSR) is sufficient
  - Contribution of the other NLFSR can be tightened (vary only the bytes targeting the attacked NLFSR)
  - 8 NLFSR internal states are recovered (half of the counter)

- Properties of the NLFSR
  - Small and predetermined prime periods
  - Independent computation for each NLFSR

- Retrieve a leak curve $E = (E_0, \ldots E_{N-1})$

- Construct NLFSR oriented curves
  - Construct 16 NLFSR-oriented curves C_i from E and the recovered periods T_i
    - $C_i = (C_{i,0} \ldots C_{i,Ti-1})$, $C_{i,j} = \sum_{k=0}^{\lfloor N/Ti \rfloor} E_{j+k*T_i} = A_{i,j} + B_{i,j}$

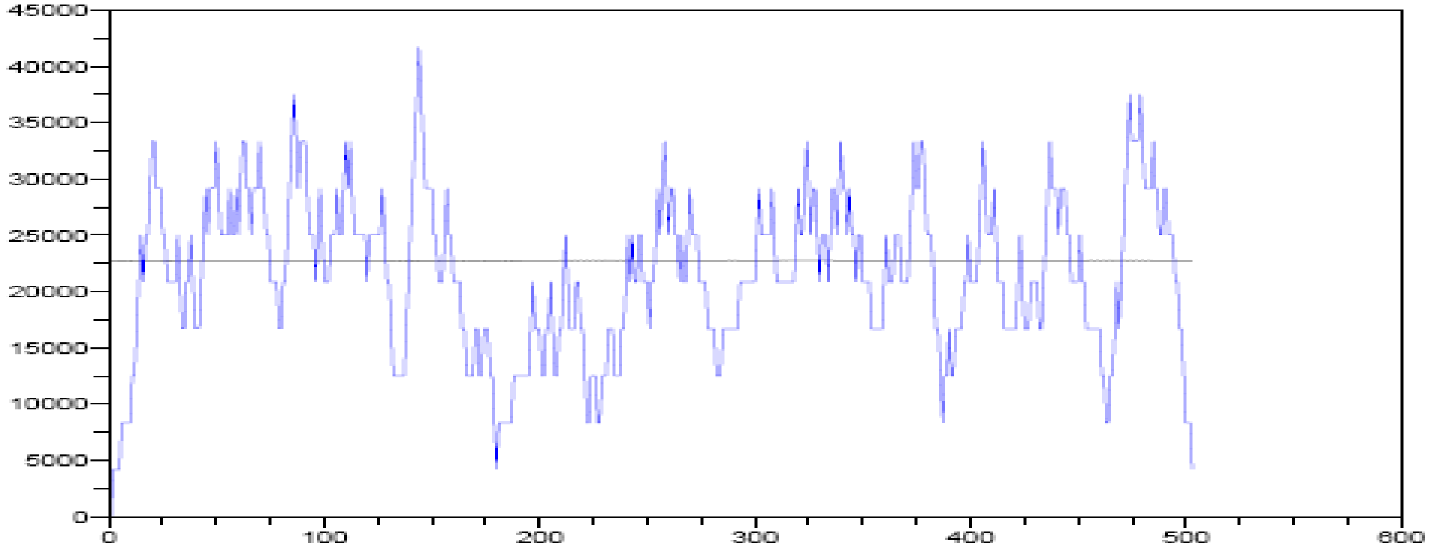
- Each $C_{i,j}$ is made of 2 parts
  - The part from NLFSR N_i, called $\boldsymbol{A_{i,j}}$
  - The part from the other NLFSR, denoted $\boldsymbol{B_{i,j}}$
  - Some noise ***N***

- The constant part $A_{i,j}$
  - $H(N_i^{j+kxTi}) = H(N_i^j)$ (period of the NLFSR)
  - $A_{i,j} = \frac{N}{T_i} * H(N_i^j)$
  - Hamming weight **linearly amplified** with N/T_i

- The random part $B_{i,j}$
  - Hamming weight between 2 states not independent
    - $H(N_i^{t+1}) = H(N_i^t) \pm \{0,1\}$
  - NLFSR are independent
    - No cross-computation
    - Unique and predetermined prime period
    - Global leakage : sum of the leakages of the 15 remaining NLFSR

$$B_{i,j} = \sum_{k=0;k\neq i}^{15} B_{k,j}$$

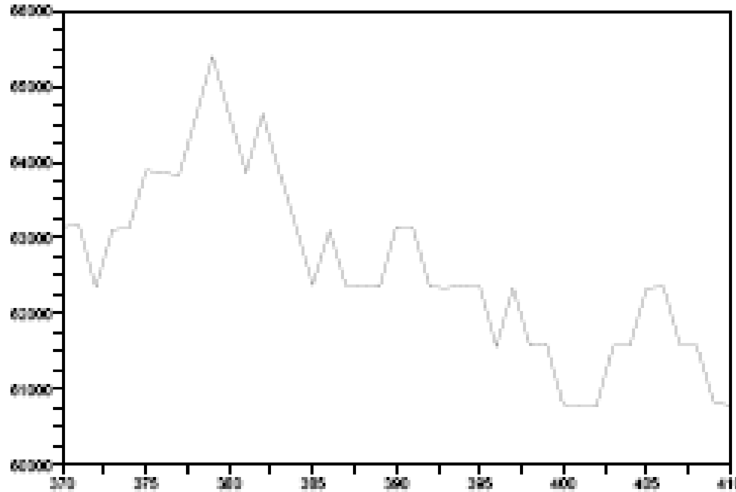
- Leakage model of the random part
  - Short length, Hamming weight model
  - Exhaustive overview of one NLFSR
  - Others will act the very same way
- NLFSR chosen N_{17} with respect to T_1 = 503
  - T_{17} = 1009, close to $2T_1$
  - Theoretical leakages of N_1 and N_{17} with respect to T_1



- The other NLFSR add a constant value to $C_{i,j}$
- Considering the Hamming weight model
  - $C_{i,j+1} - C_{i,j} \approx (A_{i,j+1} - A_{i,j})$
  - $A_{i,j+1} - A_{i,j} = \left[\frac{N}{T_i}\right](H(N_{i,j+1}) - H(N_{i,j}))$
- In other words
  - The difference between two successive states of C_i leaks information on the evolution of $H(N_i)$
  - if $C_{i,j+1} - C_{i,j} > t$
    - Hamming weight increases, $o_{j-1} = 1$ and $i_j = 0$ thus $g_{i-1} = 1$
  - If $C_{i,j+1} - C_{i,j} < -t$
    - Hamming weight decreases, $o_{j-1} = 1$ and $i_j = 0$ thus $g_{i-1} = 1$
  - If $C_{i,j+1} - C_{i,j} \in [-t, t]$
    - Hamming weight does not change, $i_j = o_{j-1}$ and $g_{j-1} = 0$

- Construct 3 sequences
  - The input bit sequence $\{0, 1, x\}^{T_i}$
  - The output bit sequence $\{0, 1, x\}^{T_i}$
  - The non linear function sequence $\{0, 1\}^{T_i}$

- Unpredicted bits x
  - $i_j = o_{j-1} \oplus f_{j-1}$
  - $f_{j-1} = 0$
  - $o_j = i_{j-|N_i|+1}$
  - Thus $i_j = i_{j-|N_i|}$



  - Some unpredicted bits are recovered
- Correlation attack on the remaining unknown bits
- Recover the initial state at t = 0

- Two drawbacks arise from the attack
  - False prediction in I or O
  - An incorrect initial state can match the sequences I and O

- First drawback
  - Tighten the level t
  - Create a new population of discarded bits
  - Differentiate unpredicted bits x and discarded bits
  - Global complexity slightly increases

- Second drawback
  - If n consecutive output bits coincide, so do the initial states
  - Two different initial states can not generate the same output sequence
  - An incorrect internal state can match only the t predicted bits, observe a longer output sequence to decrease the error probability

- Typical implementation of VEST is subject to two attacks
  - Old fashioned Differential Analysis
    - 16 bytes long IV
    - Known/chosen plain text attack
    - Recovery of 8 registers out of 16
  - Refined Simple Analysis
    - Single trace
    - No data knowledge
    - Recovery of the whole counter part at a precise time
- Counter measures
  - Hardware : masked logic
  - Sotfware : open problem