Building Secure Block Ciphers on Generic Attacks Assumptions

Jacques Patarin and Yannick Seurin
University of Versailles and Orange Labs

SAC 2008 – August 14-15, 2008

the context

- security of symmetric primitives is mainly heuristic, *e.g.*
  - lack of attacks whose complexity is less than brute-force attacks
  - partial provable security
    (*e.g.* against linear and differential cryptanalysis for AES)
  - provable security when some components are "idealized"
    (*e.g.* for DES in the Luby-Rackoff model where internal functions are pseudorandom)
- very few examples of symmetric primitives with reductionist security proofs: VSH [ContiniLS06], QUAD [BerbainGP06]
- **our work:** we propose to build *efficient* symmetric primitives (mostly block ciphers here) whose security can be reduced to the problem of *generic attacks* on simple schemes

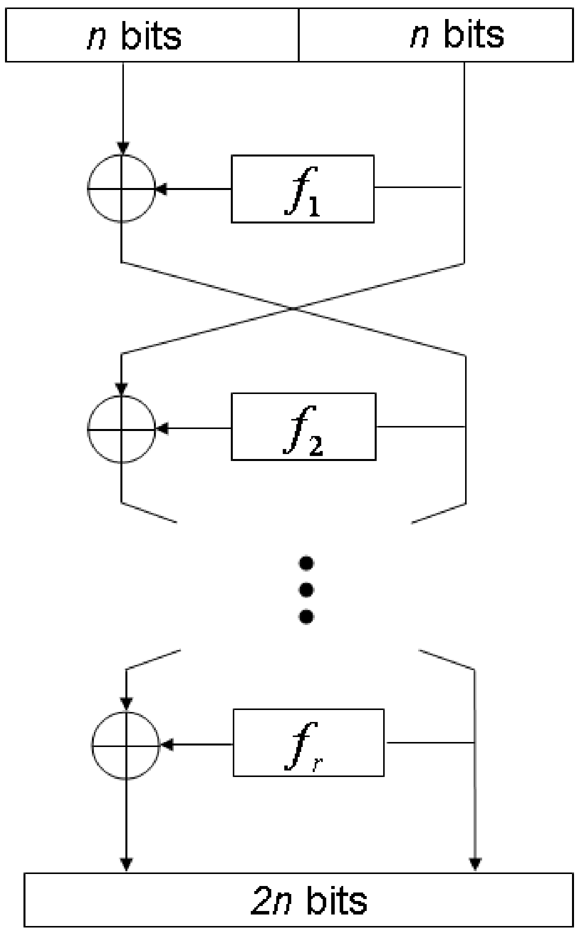
outline

- the general idea of the Russian Dolls construction
- generic attacks on Feistel schemes
- example of construction with Feistel schemes
- practical instantiations
- conclusion and further work

the Russian Dolls construction

- aims at using the results on “generic attacks” to build secure symmetric primitives
- “generic attack“ means any attack performed on a scheme where components are “idealized”: *e.g.* on a Feistel scheme with perfectly random internal functions

$$f_i \xleftarrow{\$} \mathsf{Func}(\{0,1\}^n, \{0,1\}^n), i \in [1..r]$$



the Russian Dolls construction

- the design strategy is as follows:
- starting from a Feistel scheme with r rounds and perfectly inner random functions from n bits to n bits, we evaluate its security in view of the best generic attacks
- we decrease the size of the key $r \times n2^n$ by instantiating each inner random function by a Feistel scheme with r' rounds and inner random functions from $n/2$ bits to $n/2$ bits, again evaluating the security in view of the best generic attacks
- we iterate the process until the size of the key (made of the innermost random functions) reaches a practical size . . .

IT-secure block ciphers

- previously proposed provably secure block-ciphers such as C and KFC [BaignèresF06] are *information-theoretically* secure against limited adversaries
- however information-theoretic results give a security in $\Omega(2^n)$ queries for a number of rounds $r \geqslant 5$; it decreases with the size of blocks and are useless in the Russian Dolls construction
- on the contrary, we start from complexity assumptions on generic attacks and obtain primitives with a reductionist security proof

security of the Russian Dolls construction

- the security of the construction is characterized by the following theorem:
- if E is an (ϵ, T) -secure PRP with key space $\mathrm{Perm}(D_1) \times \cdots \times \mathrm{Perm}(D_l)$, and $E^{(i)}$, $i = 1..l$, are (ϵ_i, T) -secure PRPs on D_i with key space $\mathcal{K}_i$, then E' defined on key space $\mathcal{K}_1 \times \cdots \times \mathcal{K}_l$ by

$$E'_{K_1,\ldots,K_l}(\cdot) = E_{E^{(1)}_{K_1},\ldots,E^{(l)}_{K_l}}(\cdot)$$

is an $(\epsilon + \sum_{i=1}^{l} \epsilon_i, T)$ -secure PRP.

generic attacks on Feistel schemes

- brute-force attacks: exhaustive search on the key space, $q = \mathcal{O}(r2^n)$ queries, $T = \mathcal{O}(2^{2rn2^n})$ computations
- on 3 and 4 rounds, best attacks match the information-theoretic bound:
  - on $\Psi^{(3)}$, CPA attack with $q, T = \mathcal{O}(2^{n/2})$, CPCA attack with $q, T = 3$
  - on $\Psi^{(4)}$, CPA attack with $q, T = \mathcal{O}(2^{n/2})$
- "signature" attacks: a Feistel permutation has always an even signature; this leads to a distinguisher with $q = \mathcal{O}(2^{2n})$, $T = \mathcal{O}(2^{2n})$; this is independent of the number of rounds!...
- but once this "global" property is suppressed (*i.e.* one tries to distinguish a Feistel scheme from an *even* random permutation), complexity of best generic attacks grows exponentially with the number of rounds

generic attacks on Feistel schemes

- best known attacks against r-round Feistel schemes, $r \geqslant 5$ have been described in [Patarin04]
- these are iterated attacks of order 2, and are based on the computation of the transition probabilities (a.k.a. "H coefficients") for couples of plaintexts/ciphertexts pairs $(x_1, y_1), (x_2, y_2)$:

$$\Pr\left[f_1, \ldots, f_r \xleftarrow{\$} \mathsf{Func}(\{0,1\}^n, \{0,1\}^n) \;:\; \Psi^{(r)}_{f_1,\ldots,f_r}(x_1) = y_1, \Psi^{(r)}_{f_1,\ldots,f_r}(x_2) = y_2\right]$$

- closed formula have been given for these transitions probabilities in [Patarin01], and enable to compare them to the transition probability for a random permutation:

$$\Pr^* = \Pr\left[P \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^{2n}) \;:\; P(x_1) = y_1, P(x_2) = y_2\right] = \frac{1}{2^{2n}(2^{2n}-1)}$$

generic attacks on Feistel schemes

- the attack proceeds as follows (for r even):
- one asks for the encryption of random pairs (x_1, x_2), $y_1 = E(x_1)$, $y_2 = E(x_2)$, such that $x_{1R} = x_{2R}$
- the probability that $x_{1L} \oplus x_{2L} = y_{1L} \oplus y_{2L}$ is slightly higher in the case of $\Psi^{(r)}$ than for a random permutation:

$$\Pr\left[(x_1, x_2) \xrightarrow{\Psi^{(r)}} (y_1, y_2)\right] = \Pr^* \left(1 + \frac{1}{2^{(r/2-2)n}}\right)$$

- this is detectable when one does $\simeq 2^{(r-3)n}$ tests
- the total complexity of the attack is $\mathcal{O}(2^{(r-4)n})$
(note: for $r \geqslant 7$ one needs > 1 permutation)

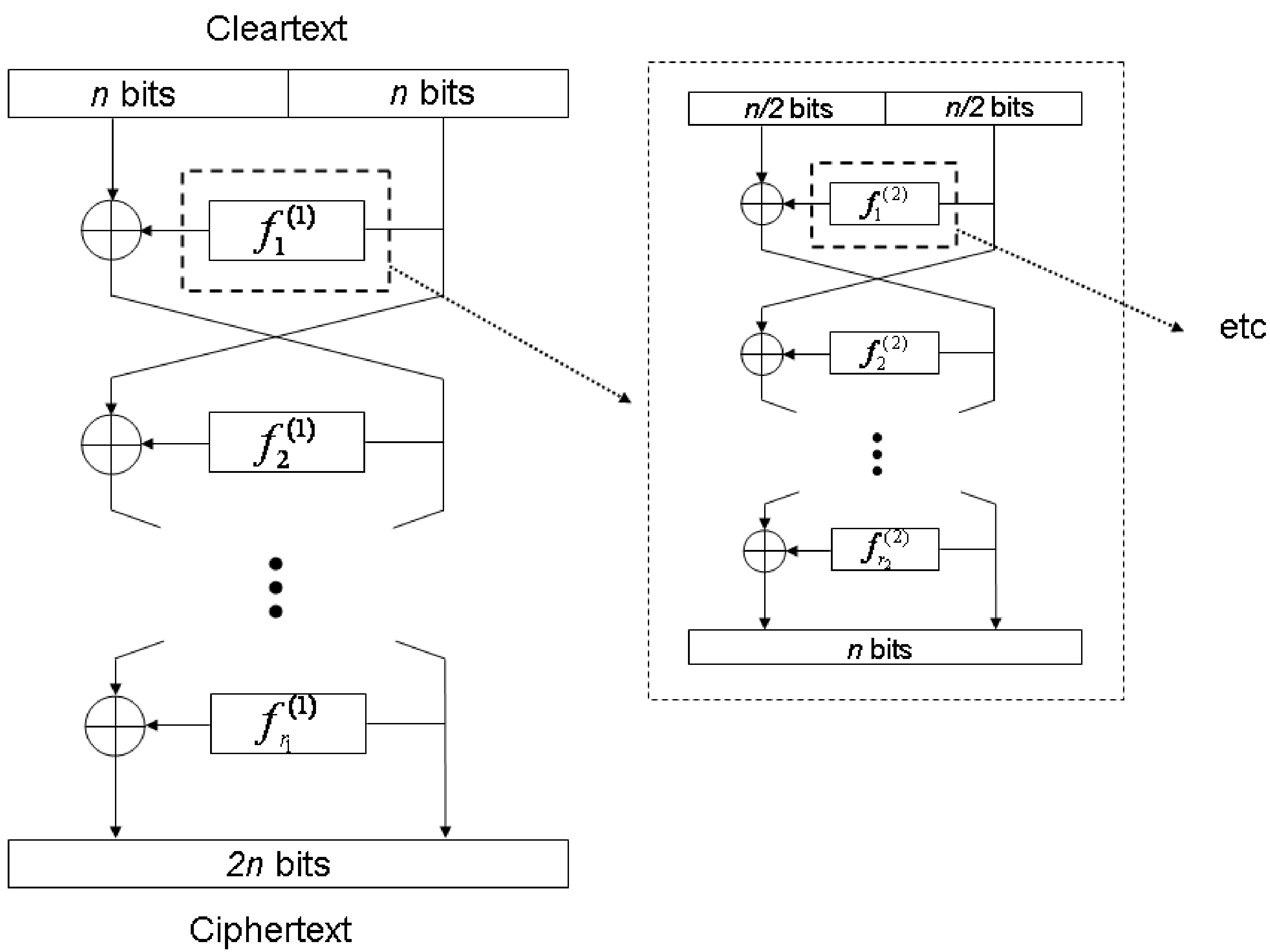
conjecture on the best generic attacks

- we conjecture that the previously described attacks are the best possible ones

> Let $n \geqslant 2$ and $r \geqslant 5$ be two integers. Then the best advantage of any adversary trying to distinguish $\Psi^{(r)}$ from an even random permutation with less than T computations is $\frac{T}{2^{(r-4)n}}$.

- arguments in favor of this conjecture:
  - best attacks on $\Psi^{(3)}$ and $\Psi^{(4)}$ are iterated attacks of order 2: this conjecture is a generalization of the cases $r = 3, 4$
  - the computation of transition probabilities for t-uples, $t \geqslant 3$ becomes very involved: best attacks are probably iterated attacks of order 2

construction with balanced Feistel schemes



construction with balanced Feistel schemes

- we want to build a block cipher from $2n$ bits to $2n$ bits, with security 2^{α}, using balanced Feistel schemes
- we denote s the number of iterations of the Russian Dolls construction and $r_1, \ldots, r_s$ the number of rounds of the Feistel schemes at the i-th iteration of the construction
- at iteration i, the internal functions of the Feistel scheme are from $\frac{n}{2^{i-1}}$ bits to $\frac{n}{2^{i-1}}$ bits; hence we choose the number of rounds such that

$$2^{(r_i-4)\frac{n}{2^{i-1}}} > 2^{\alpha}$$

- we stop the process when the number of bits to store r_{s+1} functions from $\frac{n}{2^s}$ bits to $\frac{n}{2^s}$ bits is greater then the number of bits to store one function of $\frac{n}{2^{s-1}}$ bits to $\frac{n}{2^{s-1}}$ bits

construction with balanced Feistel schemes

- the key is constituted by the $r_1 \times r_2 \cdots \times r_s$ innermost random functions; the length of the key is

$$r_1 \cdot r_2 \cdots r_s \cdot \frac{n}{2^{s-1}} \cdot 2^{\frac{n}{2^{s-1}}}$$

  and encryption/decryption requires $r_1 \times r_2 \cdots \times r_s$ table look-ups

- asymptotically, for $s = \log(n) - c$ (*i.e.* the key is constituted from functions from 2^{c+1} bits to 2^{c+1} bits):
  - the number of rounds at each iteration is $r_i = \text{poly}(n)$
  - the length of the key is $\text{poly}(n)^{\log(n)}$
  - the security, according to our conjecture, is

$$\text{Adv} \leqslant \frac{T}{2^{\text{poly}(n) - \mathcal{O}(\log^2 n)}}$$

practical instantiations

- we want to build a block cipher from $2n = 128$ bits to $2n = 128$ bits, with security $2^\alpha = 2^{80}$
- optimal number of iterations $s = 5$ with:
  - number of rounds: $r_1 = 6$, $r_2 = 7$, $r_3 = 10$, $r_4 = 16$, $r_5 = 28$
  - key constituted of functions from 4 bits to 4 bits
    key size $= 6 \times 7 \times 10 \times 16 \times 28 \times 4 \cdot 2^4 \simeq 1.5$ MB
  - encryption/decryption requires $6 \times 7 \times 10 \times 16 \times 28 = 188\,160$ TLU
- alternative with only $s = 4$ iterations
  - number of rounds: $r_1 = 6$, $r_2 = 7$, $r_3 = 10$, $r_4 = 16$
  - key constituted of functions from 8 bits to 8 bits
    key size $= 6 \times 7 \times 10 \times 16 \times 8 \cdot 2^8 \simeq 1.7$ MB
  - encryption/decryption requires $6 \times 7 \times 10 \times 16 = 6\,720$ TLU

conclusion and further work

- the Russian Dolls design strategy enables to build symmetric primitives quite efficient (implementable) and with a security reduction to the (conceptually simple) problem of generic attacks
- a lot of possible construction remain to explore, mainly based on *unbalanced Feistel schemes*, with contracting or expanding functions (generic attacks studied in [PatarinNB06,07])
- one may also explore the construction of PRFs or PRNGs based on this design principle
- other direction for further work: obtain security results pointing in the direction of our conjecture (proving it will reveal hard since it is linked to the P vs. NP problem)

thanks for your attention!

questions?