Criptografia e Cripto-análises Diferencial e Linear

Resumo

1 Criptografia moderna: breve histórico

1.1 1976-77 – criptografia aberta

2 Cripto-análise diferencial

3 Cripto-análise linear

4 Evolução

5 Complexidade de 'PAC learning' e aplicações

Routo Terada 1997

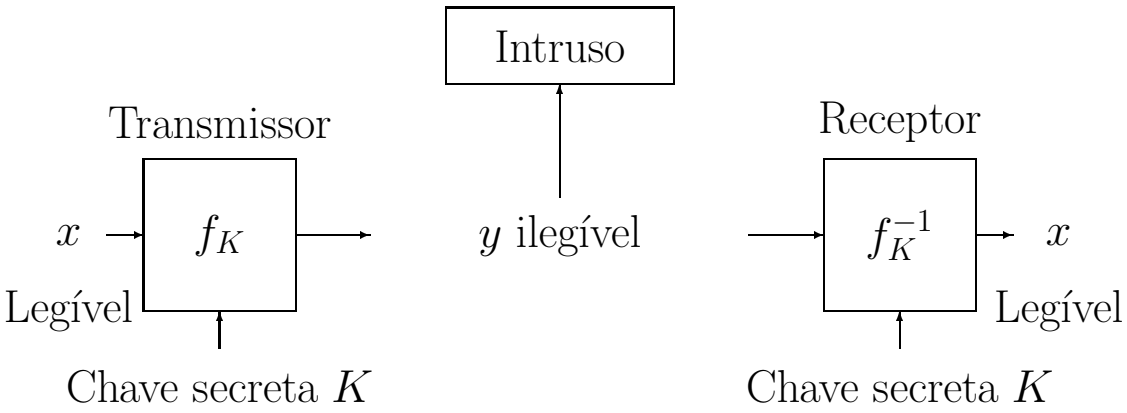
1 CRIPTOGRAFIA MODERNA: breve histórico

Objetivo: projetar famílias de funções:

$$f_K : \{0, ..., 2^n - 1\} \rightarrow \{0, ..., 2^n - 1\}$$

$f_K(x) = y$, x é *legível*, y é *ilegível*, (inversa $f_K^{-1}(y) = x$ deve existir)

- n é um inteiro positivo,
- $K \in \{0, ..., 2^n - 1\}$ é denominada *chave secreta*



Conhecendo-se: $x \in \{0, ..., 2^n - 1\}$ e K,
deve ser *fácil* calcular: $f_K(x) = y$ e a inversa $f_K^{-1}(y)$,
mas *sem* conhecer K, deve ser computacionalmente *impraticável*:

- calcular $f_K^{-1}(y)$, ou
- calcular (i.e., "quebrar") K a partir do conhecimento de pares (x, y).

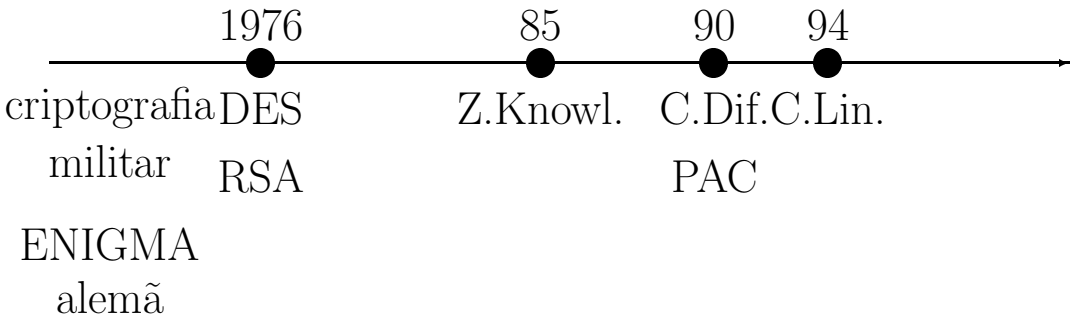
Diz-se então que $f_K()$ é uma função *segura*.

- Dificuldade de "quebra "da chave baseada em complexidade de problemas computacionalmente difíceis:
  - NP-difíceis (tempo polinomial não-determinístico) ou
  - P-espaço-difíceis.

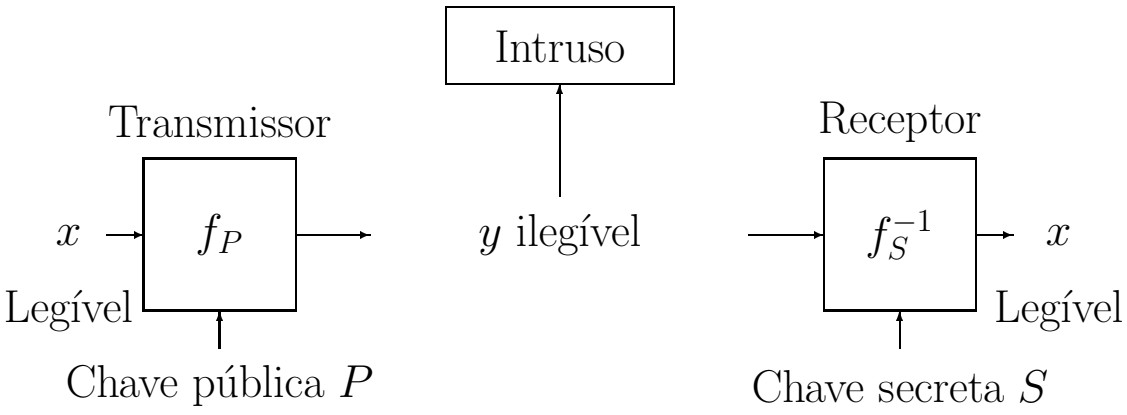
Aplicações diversas das funções criptográficas:

1. sigilo em redes de computador
2. proteção de senhas
3. proteção de cartões magnéticos ou 'smart cards'
4. proteção de bilhetes de metrô, de loteria, de 'ticket-refeição', etc.
5. deteção de 'vírus eletrônico'
6. autenticação de integridade de documentos
7. "assinatura eletrônica", por ex.
   (a) em transf. eletrônica de fundos,
   (b) em EDI,
   (c) em software comercial (Microsoft, Lotus, Borland, etc.),
   (d) etc.
8. perigos e vulnerabilidades estruturais: por ex. senha criptografada na linha ('impersonation')

1.1 1976 - 77: criptografia aberta



- Diffie e Hellman (Stanford) publicam conceito de Chave Pública
- Rivest, Shamir e Adleman (MIT) publicam algoritmo RSA (patente)



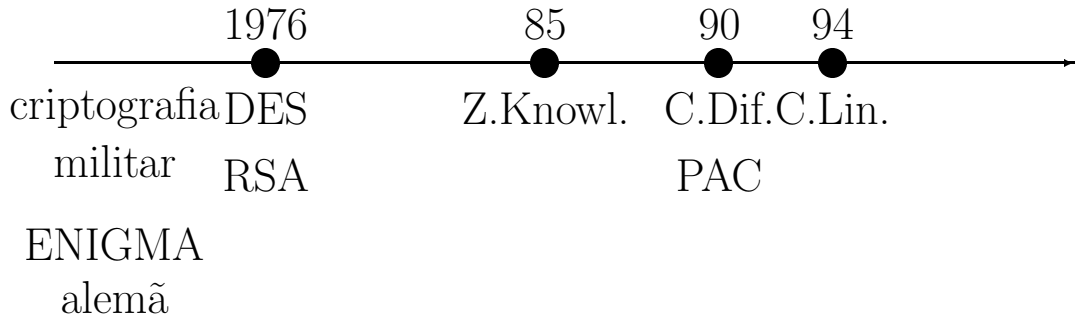
Mesmo sabendo P, é comput. inviável calcular S

- No RSA: dificuldade de "quebra" baseado na dificuldade de fatoração de inteiro em primos:
  - Calculam-se primos c, p e q, e seja $n = p.q$
  - Calcula-se a inversa d de c: $d.c = 1\ mod\ [(p-1)(q-1)]$
  - A chave pública é o par $P = (c, n)$ e a secreta é o par $S = (d, n)$

– A função $f_{(c,n)}(x) = x^c \ mod \ n = y$ e demonstra-se que a sua inversa é $f^{-1}_{(d,n)}(y) = y^d \ mod \ n = x$ (aplicar Teorema de Euler)

- Merkle e Hellman (Stanford): baseado no problema NP-difícil chamado Knapsack (Mochila) – quebrado por Shamir

- o primeiro 'standard': DES – Data Encription Standard (IBM e NSA)



DES é baseado no seguinte problema NP-completo:

Instância:

Polinômios $P_i(x_1, x_2, \cdots, x_n), 1 \leq i \leq m$, sobre corpo de Galois [2], i.e., cada polinômio é uma soma de termos, onde cada termo é um inteiro 1 ou é um produto de x_i distintos.

Problema:

Existe $u_1, u_2, \cdots, u_n \in \{0, 1\}$ tais que, $1 \leq i \leq m$, $P_i(u_1, u_2, \cdots, u_n)$= 0, onde as operações aritméticas são definidas no corpo de Galois [2], com $1 \oplus 1 = 0$, e $1.1 = 1$?

Outros algoritmos com estrutura DES: FEAL (NTT-Japão) [2], LOKI (Australia, J. Seberry), IDEA (Suiça, J. Lai), SAFER (Suiça, J. Massey), Khufu (Xerox-EUA, R. Merkle).

Em 1990 apresentamos na prestigiosa conferência CRYPTO o artigo [1].

Patente concedida em 1991

Exemplo: $C(n, d)$ para $n = 10$ and $d = 3$

Entra	1	0	1	1	0	0	1	0	0	1
K_1	$-$	0	1	$-$	$+$	$+$	1	1	$-$	$+$
Sai	0	0	0	0	0	0	0	1	1	1
K_2	$+$	1	0	1	1	$+$	0	$-$	$+$	$-$
Sai	1	1	0	1	1	1	0	1	0	1
K_3	$-$	0	1	$+$	$+$	0	$-$	$+$	$+$	$-$
Sai	1	1	1	0	0	1	0	0	1	1

Referências

[1] Koyama, K. and R. Terada: "Nonlinear Parity Circuits and Their Cryptographic Applications", *Lecture Notes in Computer Science – CRYPTO'90, Springer-Verlag*, pages 582–599, 1991.

[2] A. Shimizu and S. Miyaguchi. Fast Data Enchipherment Algorithm FEAL. In *Proc. of Eurocrypt'87*, Springer-Verlag Lec. Notes in C.S., v. 304.

********** Figura 1 **********

Claude Shannon: entropia, iteração de funções fracas.

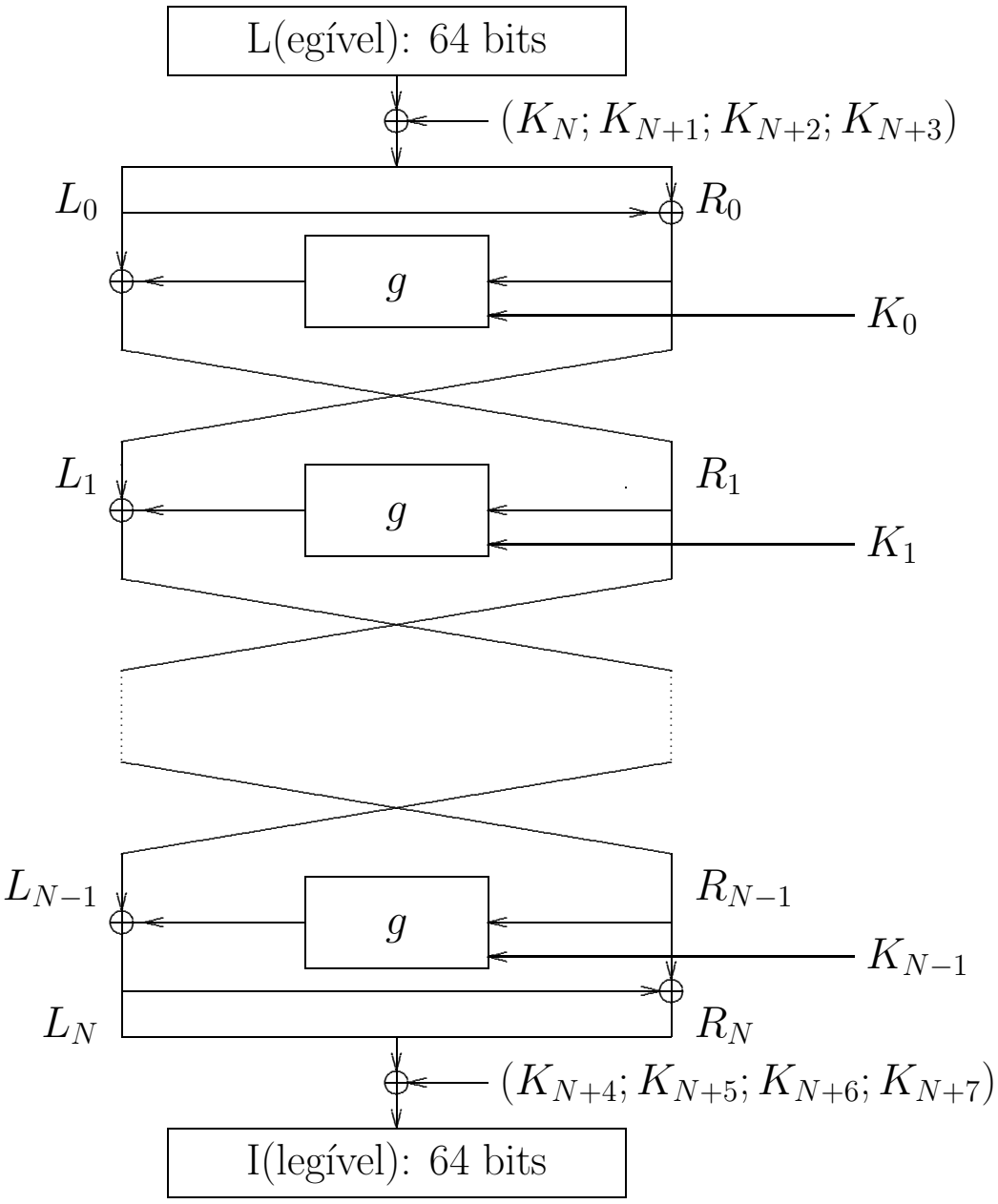


Figura 1: Cálculo da inversa: $R_N = R_{N-1} \oplus L_N \;\Rightarrow\; R_{N-1} = R_N \oplus L_N$

Seja: $\alpha = g_{K_{N-1}}(R_{N-1})$;

Então: $L_{N-1} = L_N \oplus \alpha$, pois $L_N = L_{N-1} \oplus \alpha$ e $\alpha \oplus \alpha = 0$.

2 Pesquisa em cripto-análise (ou 'quebra') diferencial

Cripto-análise Diferencial é constituída de uma forma de se medir a segurança de funções criptográficas.

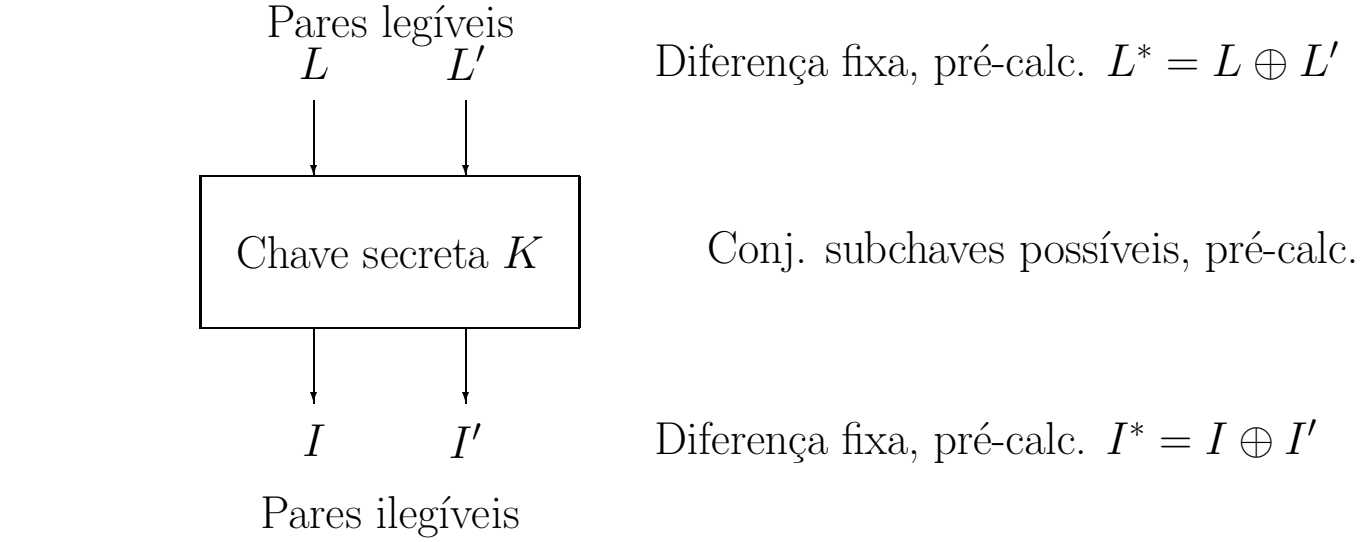
Tipo de cripto-análise criado por E. Biham e A. Shamir [1], [2].

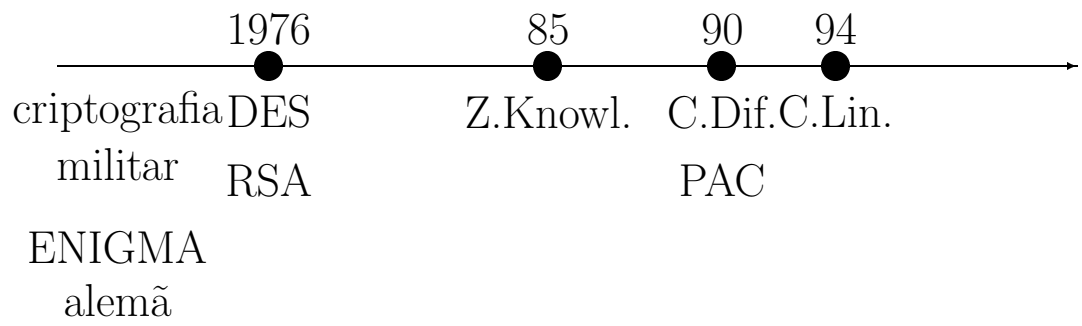
Referências

[1] A. Shamir and E. Biham. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1), 1991.

[2] A. Shamir and E. Biham. Differential cryptanalysis of the Data Encryption Standard. Springer-Verlag, New York, 1993.

- Análise probabilística efetiva para recálculo da chave secreta
- Experimentos com uma amostra relativamente pequena de dados de entrada para uma função como o DES: $2^{47} << 2^{|K|}$





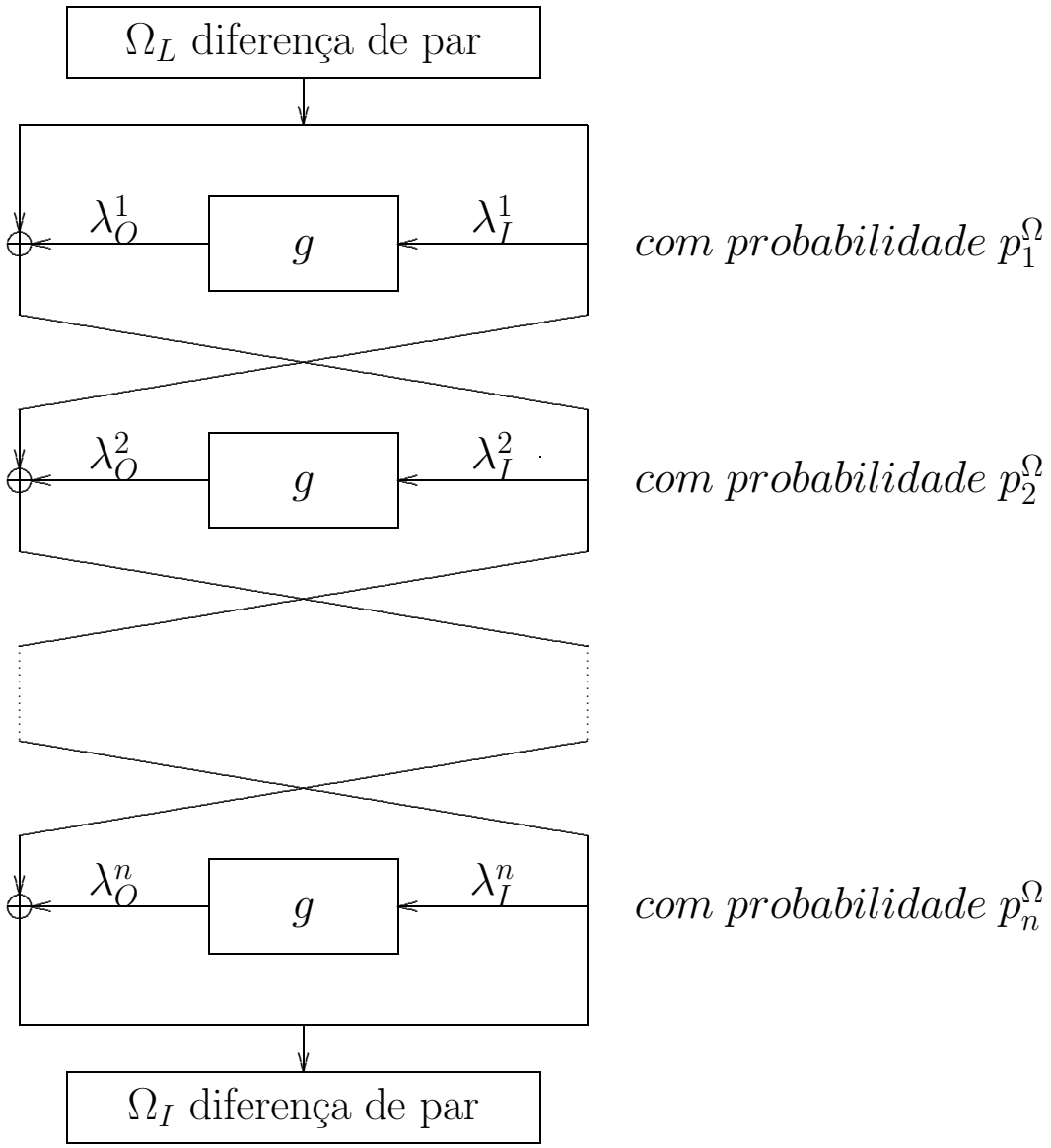
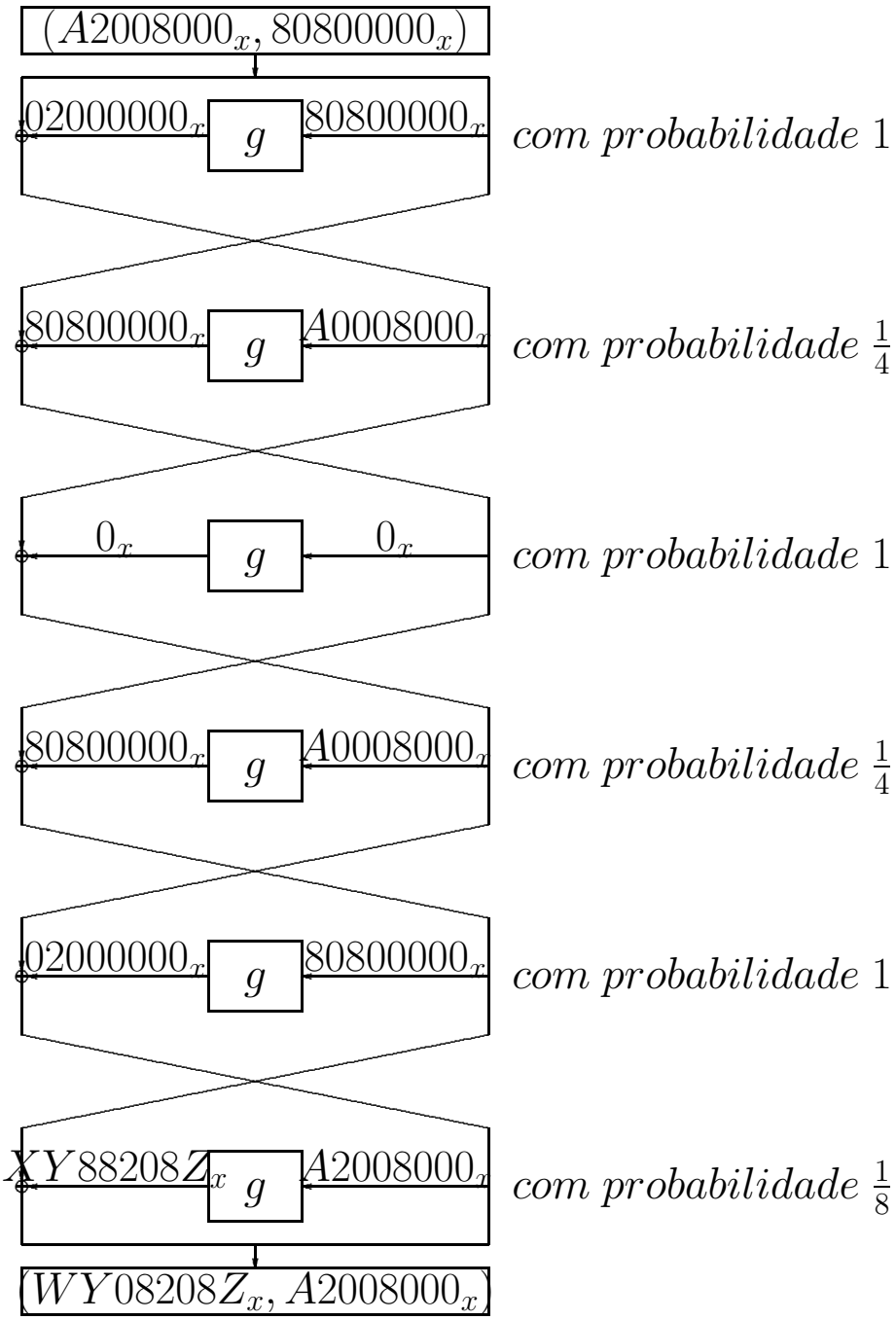


Figura 2: Uma característica diferencial genérica. Shamir provou: Complex. $\simeq$ const. $\frac{1}{p_\Omega}$.

Obs.: $(X \oplus \alpha) \oplus (X' \oplus \alpha) = X \oplus X'$,

- de modo que conhecimento de uma diferença flui
  - do topo até a base, ou da base até o topo.



onde: $X \in \{5, 6, 7, 9, A, B, D, E, F\}$ $Y \in \{9, A, B\}$ $Z \in \{0, 1, 3\}, W = X \oplus 8$

Figura 3: Uma característica por Biham e Shamir

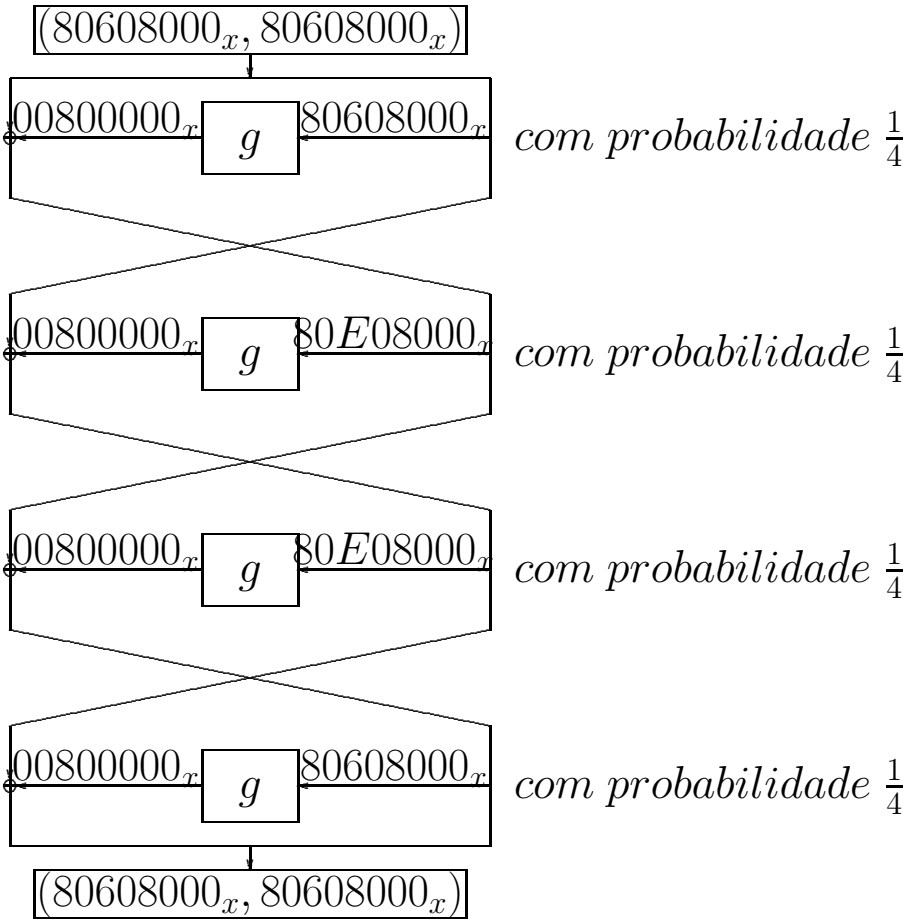


Figura 4: Uma característica diferencial iterativa por Biham e Shamir.

Função $S(x)$: troca metades se Ímpar(x).

Exemplos para $n = 4$ bits.

1. Diferença é ímpar mas assimétrica; diferença é alterada:

	x	paridade	ação	$S(x)$	paridade
	01 10	par	não trocada	*01* 10	
	11 01	ímpar	trocada	01 *11*	
$\oplus$	10 11	ímpar(diferença)		00 01	ímpar, mas $\neq$

2. Diferença é par mas assimétrica; diferença não é alterada:

	x	paridade	ação	$S(x)$	paridade
	11 00	par	não trocada	*11* 00	
	11 11	par	não trocada	*11* 11	
$\oplus$	00 11	par(diferença)		00 11	par e =

3. Diferença é par mas assimétrica; diferença é alterada:

	x	paridade	ação	$S(x)$	paridade
	11 10	ímpar	trocada	10 *11*	
	11 01	ímpar	trocada	01 *11*	
$\oplus$	00 11	par(diferença)		11 00	par, mas $\neq$

4. Diferença é par e simétrica; diferença não é alterada:

	x	paridade	ação	$S(x)$	paridade
	10 01	par	não trocada	*10* 01	
	00 11	par	não trocada	*00* 11	
$\oplus$	10 10	par(diferença)		10 10	par e =

5. Diferença é par e simétrica; diferença não é alterada:

	x	paridade	ação	$S(x)$	paridade
	10 00	ímpar	trocada	00 *10*	
	00 10	ímpar	trocada	10 *00*	
$\oplus$	10 10	par(diferença)		10 10	par e =

Obs: Lemas básicos sobre $S(.)$, independentes da definição de $g()$:

Lema 1 Se $X = (X_E; X_D)$ é uma sequência aleatória de 32 bits com distribuição uniforme então:

$$P[S(X) = X] = \frac{1}{2} \ \ and \ \ P[S(X) \neq X] = \frac{1}{2}.$$

Lema 2 Sejam Z, X, Y sequências aleatórias de 32 bits tais que X possui distribuição uniforme Z é fixo e $Z = X \oplus Y$. Então:

$$P[S(X) \oplus S(Y) = Z] = \begin{cases} 1, & \text{se } Sim(Z) \\ \frac{1}{2}, & \text{se } Par(Z) \wedge \overline{Sim(Z)} \\ 0, & \text{c. contrário} \end{cases}$$

********** Figuras 5, 6, 7 **********

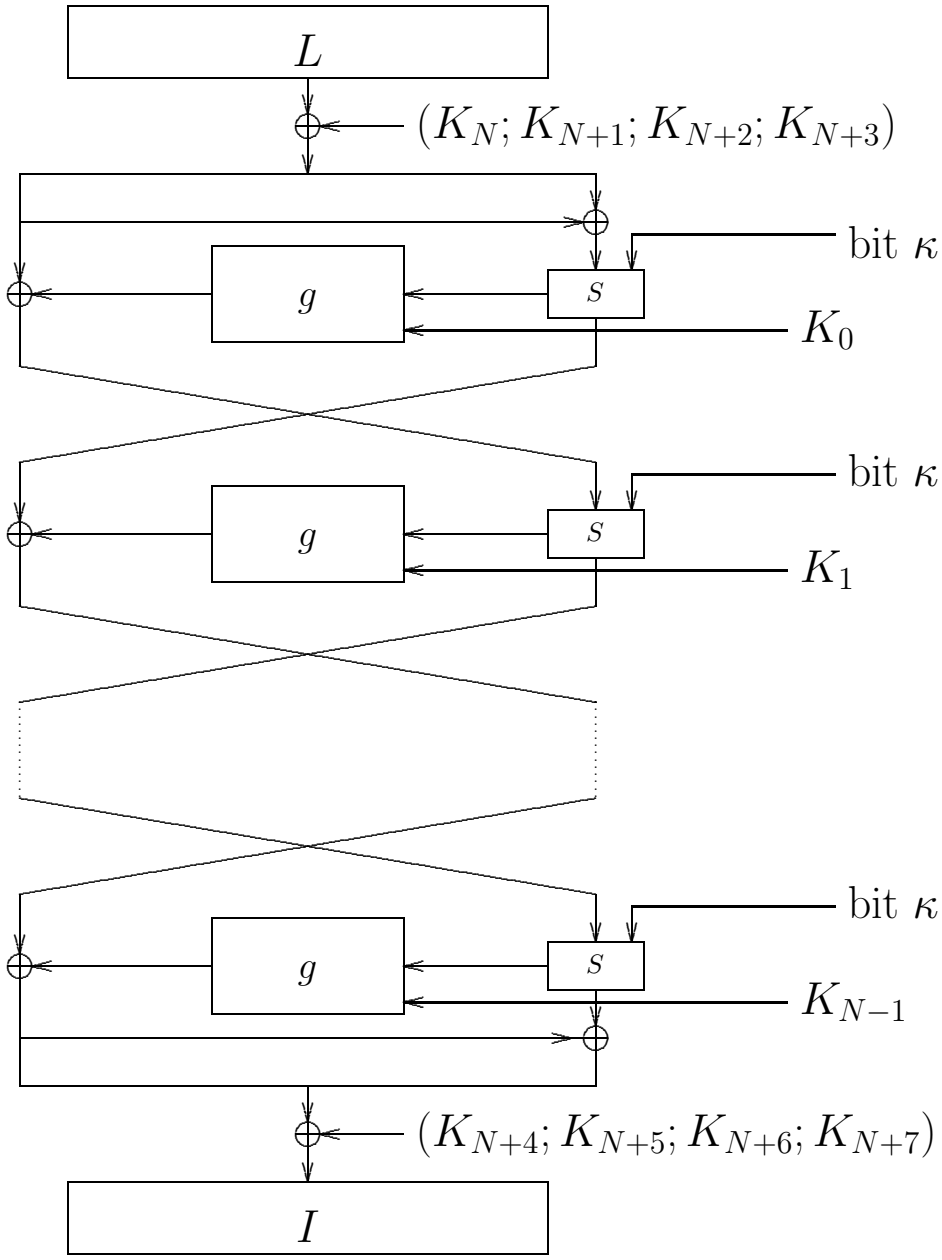
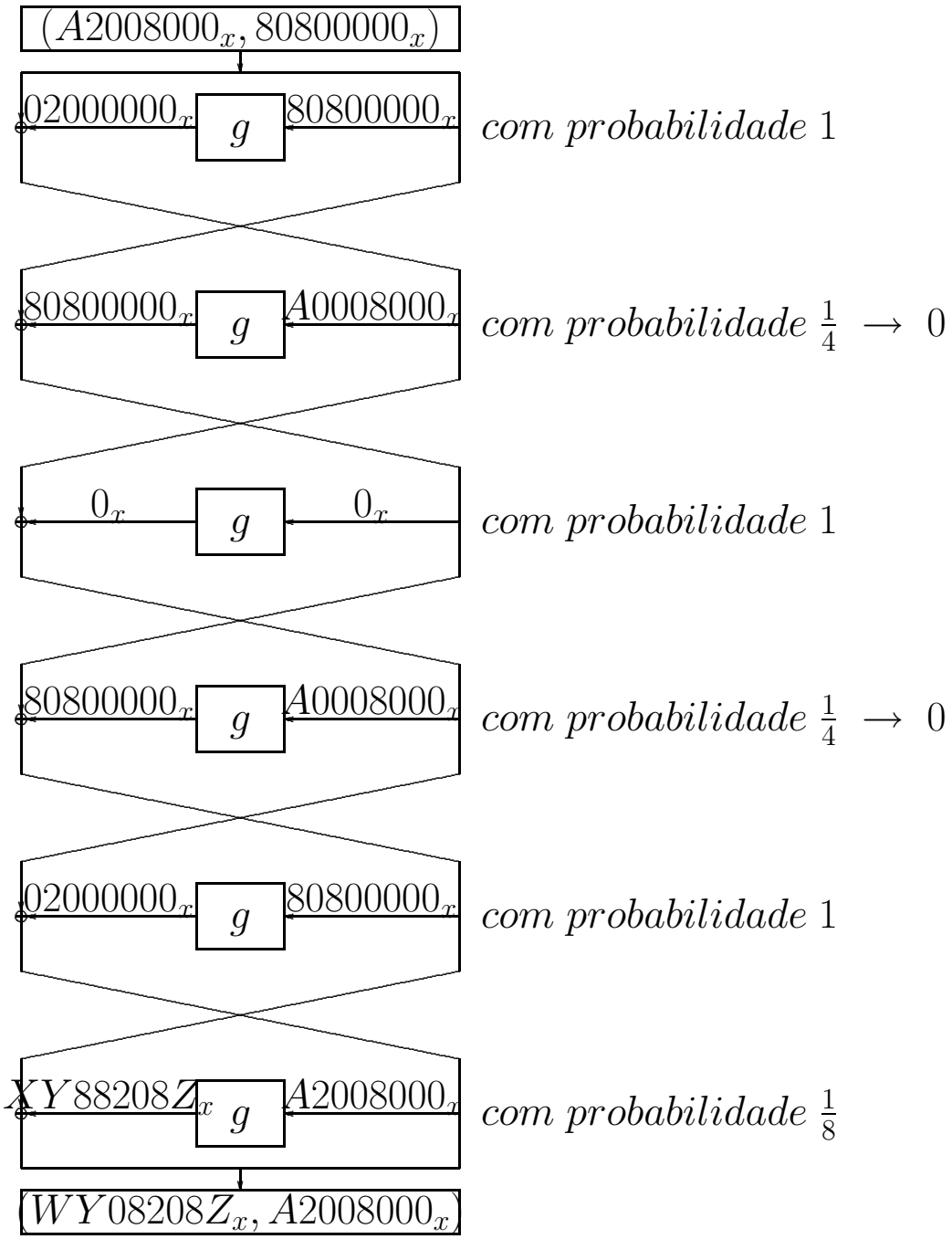


Figura 5: FEAL-N(X)S: inversível.



onde:

$X \in \{5, 6, 7, 9, A, B, D, E, F\} Y \in \{9, A, B\} Z \in \{0, 1, 3\}, W = X \oplus 8$

Figura 6: Uso de uma característica por Biham e Shamir em FEAL-N(X)S

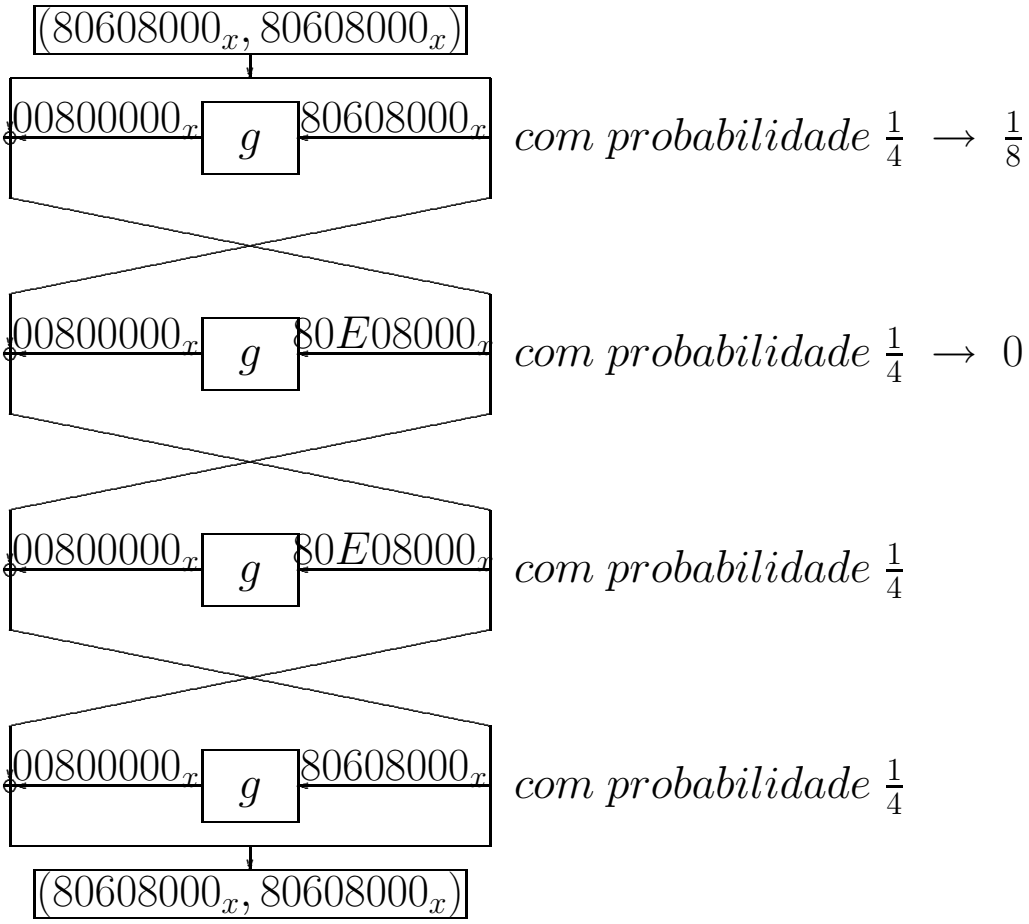


Figura 7: Uso de uma característica iterativa por Biham e Shamir em FEAL-N(X)S.

- FEAL com $S(x)$: complexidade $> 2^{|K|}$ (original/: 2^{29})
- DES com $S(x)$: complexidade $> 2^{|K|}$ (original/: 2^{47})

- Aplicamos $S(x)$ em dois níveis também.
- Mais rápido que 'Triple DES'.

- Importância do DES: usado em grande escala no Brasil.
- Linha de pesquisa iniciada nos artigos [1], [2], [3]

Nesta linha de pesquisa foram publicados os artigos:

Referências

[1] K. Koyama and R. Terada. How to strengthen DES-like cryptosystems against differential cryptanalysis. *Transactions of the Inst of Electr. Info. and Communic. Eng., Japão*, E76-A(1), January 1993.

[2] K. Koyama and R. Terada. Probabilistic swapping schemes to strengthen DES against differential cryptanalysis. In *Proc. of the Symp. of Cryptography and Information Security, Jan. 28-30 1993, Japão*. Institute of Electronics, Information, and Communication Engineers – Japão, 1993.

[3] T. Kaneko, K. Koyama, and R. Terada. Dynamic swapping schemes and differential cryptanalysis. In *Proc. of the 1993 Korea-Japan Joint Workshop on Information Security and Cryptology (Oct. 24-26, 1993)*, pages 292–301. Institute of Electronics, Information, and Communication Engineers – Japão, 1993.

[4] T. Kaneko, K. Koyama, and R. Terada. Dynamic swapping schemes and differential cryptanalysis. *Transactions of the Inst of Electr. Info. and Communic. Eng.*, E77-A(8), August 1994.

[5] R. Terada and P. G. Pinheiro. How to strengthen FEAL against differential cryptanalysis. In *Proc. of the 1995 Japan-Korea Joint Workshop on Information Security and Cryptology (Jan. 24-27, 1995)*. Institute of Electronics, Information, and Communication Engineers – Japão, 1995. Complexidade: $> 2^{|K|}$

3 Pesquisa em cripto-análise linear

Recentemente foi criada a Cripto-análise Linear por Matsui e outros [1] [2] [3].

Referências

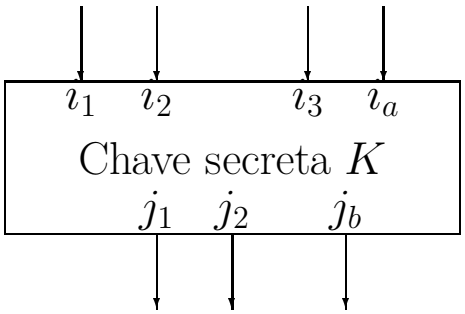
[1] M. Matsui and A. Yamagishi. A new method for known plaintext attack of FEAL cipher. In *Proc. of Eurocrypt'92*, Springer-Verlag Lec. Notes in C.S., v. 658, pp 81-91.

[2] M. Matsui. Linear cryptanalysis method for DES cipher. In *Proc. of EUROCRYPT'93, Lec. Notes in CS 765*, pages 386–397. Springer-Verlag, 1993.

[3] M. Matsui. The first experimental cryptanalysis of the DES. In *Proc. of the Advances of Cryptology – CRYPTO'94*, pages 1–11. Springer-Verlag, 1994.

- Tipo de análise também probabilística
- *Mais* efetiva do que Cripto-análise Diferencial contra o DES: complexidade 2^{43}.
- Matsui descobriu relações lineares entre certas posições dos 64 bits de entrada, de saída, e de chave, para o DES
- $L[i_1, i_2, \cdots, i_a] \oplus I[j_1, j_2, \cdots, j_b] = K[k_1, k_2, \cdots, k_c]$ com certa probabilidade

Posições fixas, pré-determ.



Posições fixas da chave, pré-determ.

Posições fixas, pré-determ.

- Matsui tem aplicado o mesmo tipo de análise para outras funções como o FEAL: complexidade 2^{15} para FEAL com 8 iterações.

- Conjectura de existência de 'dualidade'.

Em cripto-análise linear, temos desenvolvido a linha de pesquisa iniciada no artigo [1].

Referências

[1] Y. Nakao and T. Kaneko and K. Koyama and R. Terada. A study on the security of RDES cryptosystem against Linear Cryptanalysis. In *Proc. of the 1995 Korea-Japan Joint Workshop on Information Security and Cryptology (January 24-27, 1995)*, pages V–2.1– V2.10. Institute of Electronics, Information, and Communication Engineers – Japão, 1995.

Estamos também pesquisando e analisando famílias de funções criptográficas que sejam mais seguras contra as cripto-análises diferencial e linear, *simultaneamente* [1]

Referências

[1] S. Langford and M. E. Hellman. Differential-linear cryptanalysis. In *Proc. of CRYPTO'94*, Springer-Verlag Lec. Notes in C.S., v. 839, pp 17-25.

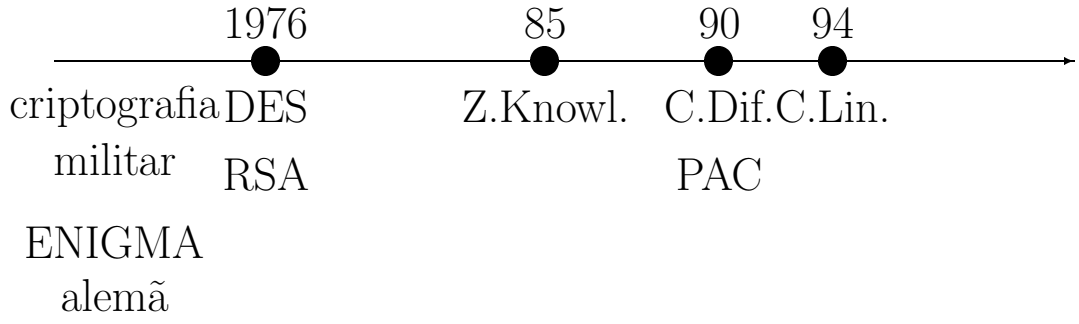
- Disciplina de doutorado em 1994.

Foram publicados em 1996 os seguintes artigos:

Referências

[1] R. Terada and P. G. Pinheiro and Kenji Koyama. A New FEAL, stronger against differential cryptanalysis. Transactions of the Institute of Electronics, Information, and Communication Engineers – E79-A(1):28–34, January 1996.

[2] Y. Nakao and T. Kaneko and K. Koyama and R. Terada. The security of RDES cryptosystem against Linear Cryptanalysis. Transactions of the Institute of Electronics, Information, and Communication Engineers, E79-A(1):12–19, January 1996. (complexidade $> 2^{|K|}$)



3.1 Em 1997:

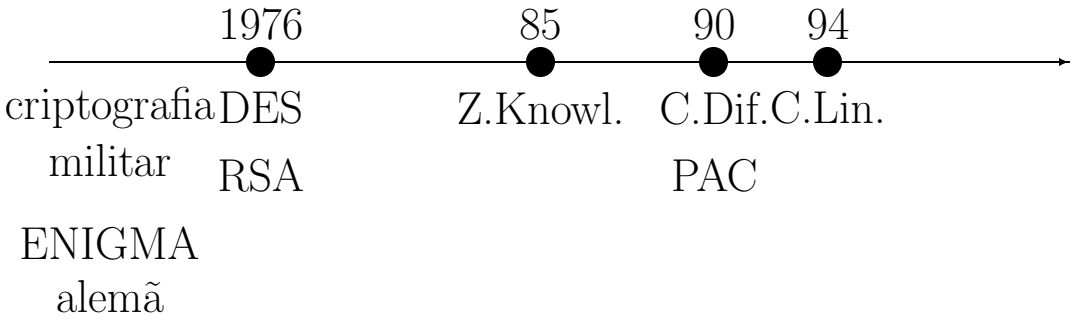
- Em fevereiro de 1997 apresentamos o artigo [1]: maior segurança contra cripto-análise linear.
- Em setembro de 1997 apresentamos o artigo [2]: é um aprimoramento do artigo apresentado na CRYPTO'90, introduzimos uma maior não-linearidade no circuito. Este workshop contou com um comitê internacional de pesquisadores do Japão, Europa, e América do Norte.

Referências

[1] R. Terada and Jorge Nakahara Jr. Linear and differential cryptanalysis of FEAL-N with swapping. 1997 Internat'l Symposium on Computer and Information Security, Fukuoka, Jan 29-Feb 1, Japan.

[2] K. Koyama and R. Terada. An augmented family of Cryptographic Parity Circuits. 1997 Information Security Worshop, Ishikawa, Sep 17-19, 1997, Japan. "Procedings em livro da série Lec. Notes in Comp. Sci., pela Springer-Verlag".

4 Evolução



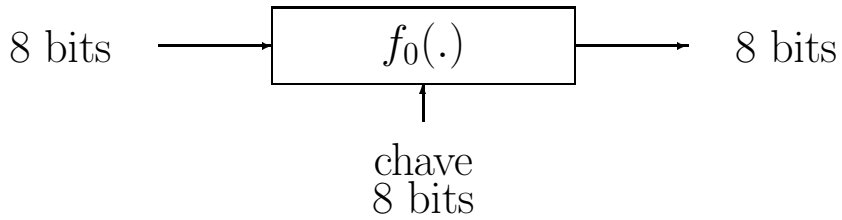
Para fortalecer contra cripto-análise diferencial e linear:

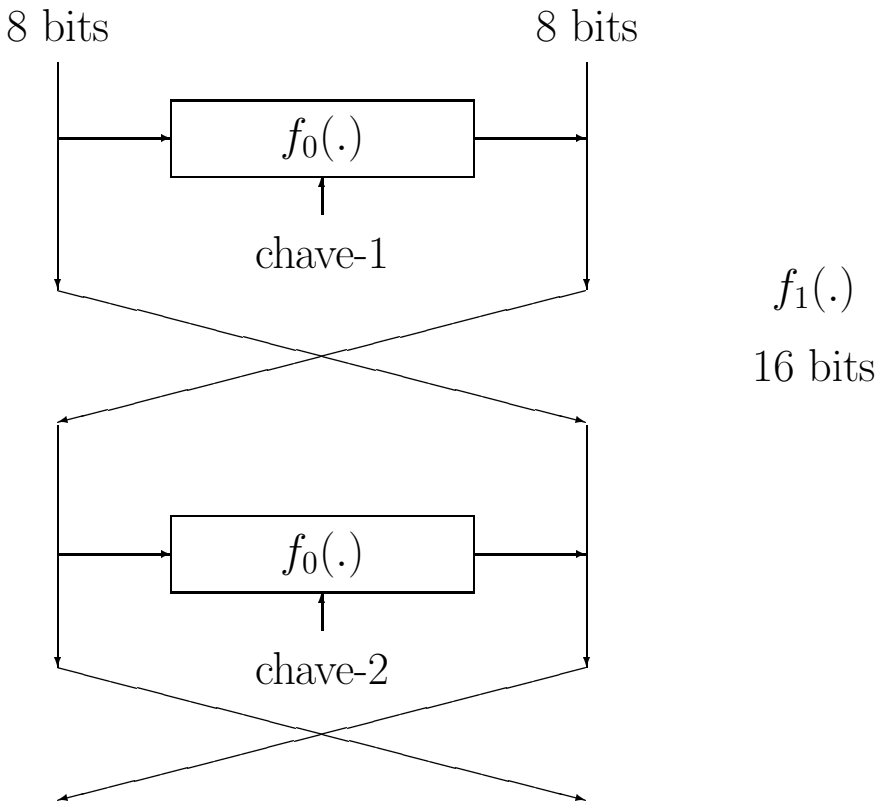
- Alterar projeto da função g: J. Seberry (Australia), L. Knudsen (Dinamarca), S. Tavares (Canadá), etc..
- Combinar RSA com funções 'DES-like': sistema PGP, CYLINK, etc.
- 'Quantum cryptography' - Gilles Brassard, Canadá
- 'Subliminal communication' - Gus Simmons, EUA

- Demonstrar segurança de funções de substituição relativamente simples, e utilizá-las como "building blocks" de funções mais complexas – tema de doutoramento corrente.

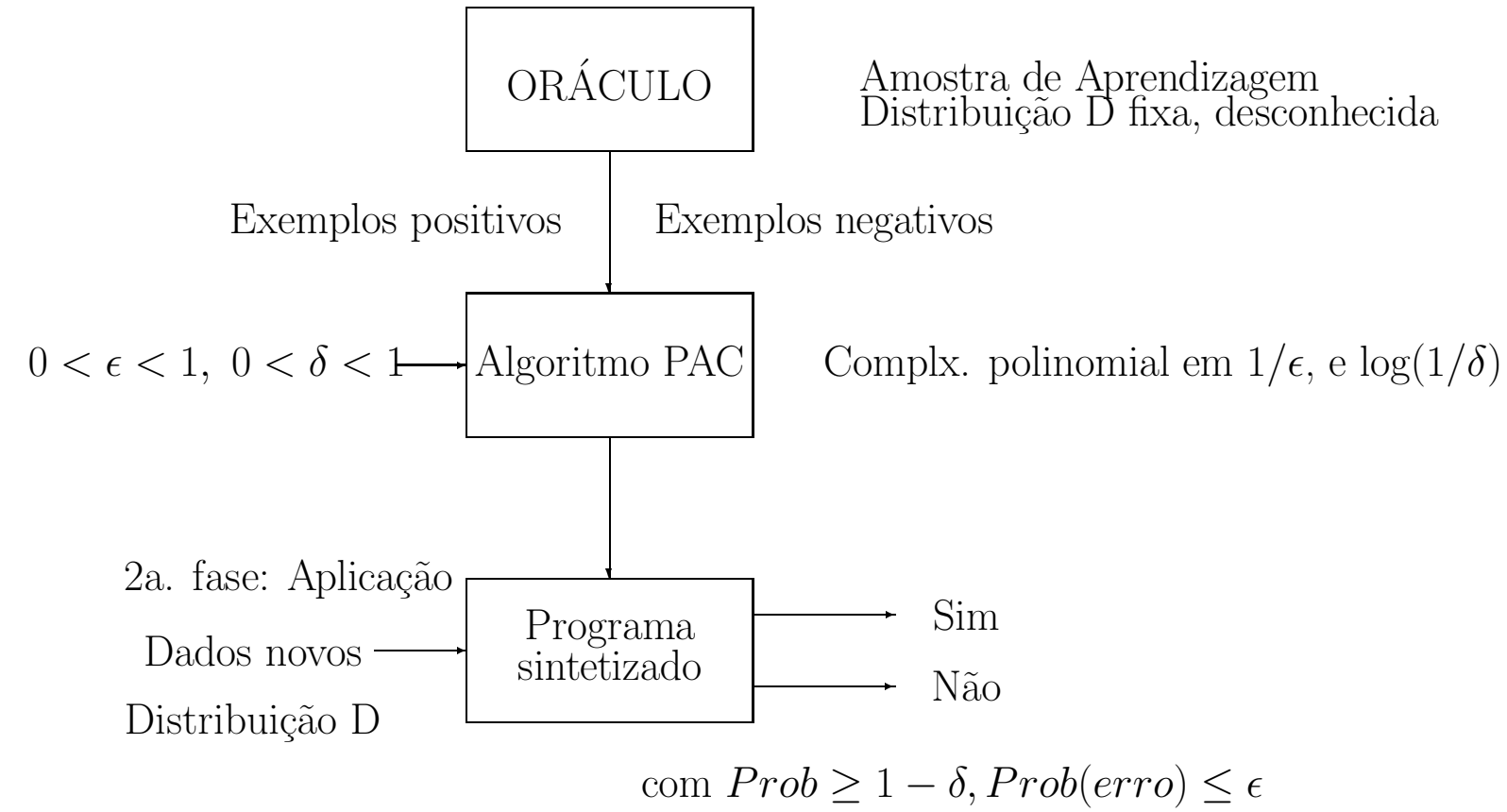
Construção "bottom-up"

- nível de segurança de f_0 incorporado ao nível de f_1,
- e o de f_1 incorporado ao de f_2, ...





5 Pesquisa em PAC Learning e aplicações



PAC – Probably Aproximately Correct

Recentemente estão sendo descobertas conexões interessantes entre

- a teoria de criptografia,
- complexidade de computação, e

- complexidade de aprendizagem ("machine learning"), segundo o modelo PAC, formulado por Leslie Valiant [1, 4] da Universidade de Harvard, e desenvolvido no MIT por Ronald Rivest [2] [3] [5] e seu grupo.

Referências

[1] Leslie G. Valiant. A theory of the learnable. *Communications of the ACM*, 27(11):1134-1142, 1991.

[2] Ron Rivest. Learning decision lists. *Machine Learning*, 2(3):229-246, 1987.

[3] Ron Rivest. Cryptography and machine learning, In *Proc. of Asiacrypt'91*, Springer-Verlag Lec. Notes in C. S., v.739, 1992.

[4] M. Anthony and N. Biggs. COMPUTATIONAL LEARNING THEORY. *Cambridge University Press*, 1992.

[5] M. Kearns and U. Vazirani. COMPUTATIONAL LEARNING THEORY. *MIT Press*, 1994.

Tais conexões são apresentadas no simpósio anual COLT – "COmputational Learning Theory".