Pseudorandom permutation families over abelian groups

Louis Granboulan, Éric Levieil, and Gilles Piret

March 14, 2006

Motivations

- Adding an encryption layer within a system that stores its data in decimal value
- For public-key cryptosystems requiring an ideal permutation of an arbitrary group (cf. for example Abdalla and al., Password-based Group Key Exchange in a constant number of rounds, PKC'2006)
- Build a general theory of pseudorandom permutation families

Previous work

- Black and Rogaway: permuting arbitrary domains by iterating a block cipher(RSA CT'02)
- Our toy-cipher is an adaptation of Rijndael, using the building principles of a key-alternating cipher
- The generalization of differential cryptanalysis appears in the study of ciphers like Twofish, IDEA and Multiswap. It has been etudied by Nyberg(Eurocrypt'93)
- The only example of a generalization of linear cryptanalysis was over $\mathbb{Z}_4$ (Parker and Raddum)

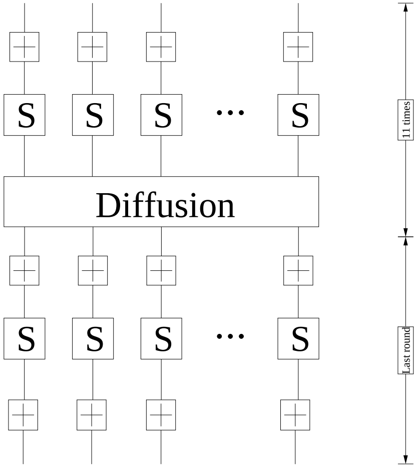
Main results

- Design and analysis of a pseudorandom permutation family over $(\mathbb{Z}_{100})^{32}$: TOY100
- Generalization of piling-up theorems for differential and linear cryptanalysis
- Study of the distribution of $D(f)$ for random f
- Optimal resistance to linear cryptanalysis in the prime case is equivalent to f being a degree 2 polynomial

Outline

1. TOY100
   - Description
   - Analysis
2. Differential cryptanalysis
   - Definition
   - Piling-up lemma
   - Distribution of $D(f)$
3. Linear cryptanalysis
   - Two approaches: L and λ
   - Piling-up lemma
   - Optimal functions

TOY100



S-box

This function has $D(f) = 5$, $L(f) = 5^2$ and $\lambda(f) = 734.122\cdots$

	0	1	2	3	4	5	6	7	8	9
0	0	67	12	32	30	53	34	37	71	38
10	42	94	58	95	78	35	6	22	36	81
20	61	93	43	72	25	27	15	69	90	47
30	1	91	84	86	24	79	66	40	10	33
40	59	8	11	48	28	76	73	82	39	51
50	45	13	97	74	9	7	52	88	62	96
60	23	29	3	4	75	56	5	64	17	49
70	68	77	80	55	85	92	44	21	98	50
80	20	31	65	83	19	57	41	70	18	99
90	89	60	46	26	63	14	87	16	54	2

Diffusion

$$Mix\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} a_4 \boxplus a_1 \boxplus a_2 \\ a_1 \boxplus a_2 \boxplus a_3 \\ a_2 \boxplus a_3 \boxplus a_4 \\ a_3 \boxplus a_4 \boxplus a_1 \end{pmatrix}$$

Mix is inversible. The diffusion layer applies *Mix* to each column, and then to each row.
The function has a branch number of 6(minimum of the sum of non-null S-box inputs and outputs, upon all non-null inputs).
There is a lack of theory for the diffusion layer.

Key-schedule

The first round key K^0 is the key itself. For the following rounds, we iterate as follows:

$$
\begin{aligned}
k_{0,j}^{r+1} &= k_{0,j}^{r} \boxplus S(k_{3,(j+1)\bmod 4}^{r}) \boxplus 3^r && (j \in \{0,1,2,3\}) \\
k_{i,j}^{r+1} &= k_{i,j}^{r} \boxplus k_{i-1,j}^{r+1} && (i \in \{1,2,3\}, j \in \{0,1,2,3\})
\end{aligned}
$$

There are very few theoretical elements about the key-schedule.

Differential attacks

The best differentials we found rely on the following property of the linear layer:

$$\begin{bmatrix} \delta & -\delta & 0 & 0 \\ -\delta & \delta & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{\theta} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & -\delta \\ 0 & 0 & -\delta & \delta \end{bmatrix} \tag{1}$$

It could be used to attack up to seven rounds.

Linear attacks

Table: Estimated bias for the best $(n+1)$-round linear characteristic

# Rounds $n+1$	Best Bias
2	$2.49 \cdot 10^{-6}$
3	$8.78 \cdot 10^{-9}$
4	$3.10 \cdot 10^{-11}$
5	$1.09 \cdot 10^{-13}$
6	$3.86 \cdot 10^{-16}$

Up to 7 rounds of the cipher can be attacked this way.

Structural attacks

- The diffusion layer of our cipher operates on well-aligned blocks, which could make it vulnerable to structural attacks.
- We explored truncated differential, impossible differential, and square attacks.
- The best such attack we found is a square-like attack, which can be used for a practical cryptanalysis of up to 4 rounds of TOY100.

Differential cryptanalysis

Let us define a $q \times q'$ matrix Δ that describes the action of f over differences by $\Delta(f)_{a,b} = \#\{x | f(x+a) - f(x) = b\}$.
The complexity of an attack by differential cryptanalysis is of order $1/DP(f)$ where the differential probability $DP(f) = D(f)/q$ is defined by:

$$D(f) = \max_{(a,b) \in G \times G' \setminus \{(0,0)\}} \Delta(f)_{a,b}.$$

Composition

$$h_K = g \circ \mathrm{ADD\_KEY}(K) \circ f.$$

Theorem

$$DP(h_K) \approx DP(f)DP(g)$$

if the following hypothesis hold:

- *Stochastic equivalence.* $\Delta(h_K)$ *does not depend heavily on* K*;*
- *Dominant characteristic for* (a, c)*.* $\sum \Delta(f)_{a,b}\Delta(g)_{b,c} \approx \max \Delta(f)_{a,b}\Delta(g)_{b,c}.$
- *Independence.* $\max \Delta(f)_{a,b}\Delta(g)_{b,c} \approx \max \Delta(f)_{a,b_f}\Delta(g)_{b_g,c}.$

Prime case

- Conjecture: If $D(f) = 1$, then the degree of f is 2.
- A way to prove the conjecture: the following lemma
  If $\varphi : \mathbb{F}_p \to \mathbb{Z}$ satisfies $\sum_{y \in \mathbb{F}_p} \varphi(y)^2 = p - 1$, and
  $\forall x \neq 0,\ \sum_{y \in \mathbb{F}_p} \varphi(y)\varphi(x + y) = -1$ then $\forall x,\ \varphi(x) \in \{0, \pm 1\}$.

Average value

Theorem

Let us define $z(p) = \lfloor \Gamma^{-1}(p/(6 \log p)) \rfloor - 1$ *where as usual* $\Gamma(z+1) = z!$, *then*

$$\lim_{p \to \infty} Pr[z(p) \leq D(f) \leq 3z(p)] = 1$$

The case $\mathbb{Z}/q\mathbb{Z}$

- Only a few functions could be interpolated by polynomials.
- Over $\mathbb{Z}/100\mathbb{Z}$: 2.10^{12} polynomials versus 10^{200} functions
- For those polynomials, we could use our study of the prime case.

Linear cryptanalysis: first approach

For any pair $(a, b) \in (G, G')$, let us define the distribution vector $\Lambda_0(f)_{a,b} = (\#\{x \in G \mid \langle a, b|x, f(x)\rangle = u\})_{u\in\mathbb{Z}/\ell\mathbb{Z}}$.
Therefore, if we define the bias $\Lambda_S(f)_{a,b;u} = \Lambda_0(f)_{a,b;u} - S_{a,b;u}$ ($S_{a,b;u}$ is the value for the random behavior), then its greatest term is a measure of non-linearity.

$$L(f) = \max_{a,b\neq 0,u} (\Lambda_S(f)_{a,b;u})^2$$

The complexity of the attack is expected to be of order $1/LP(f)$, where the linear potential $LP(f) = L(f)/q^2$.

Second approach

The other approach generalizes the duality between differential and linear cryptanalysis, as it has been done for example by Chabaud and Vaudenay(Eurocrypt'94).

- Characteristic function of f: $\theta_f : G \times G' \to \{0,1\}$ such that $\theta_f(x,y) = 1$ iff $y = f(x)$
- Convolution: $(f * g)(a) = \sum_x f(x)g(a+x)$
- $(\theta_f * \theta_f)(a,b) = \Delta_{a,b}$
- Transform: $\hat{\phi}(a) = \sum_x \phi(x)\xi^{\langle a|x\rangle}$
  $\lambda(f)_{a,b} = \widehat{(\theta_f * \theta_f)}(a,b)$
  $\lambda(f) = \max_{(a,b)\neq(0,0)} \lambda(f)_{a,b}$.

Comparison between the two approaches

In characteristic 2, we have $\lambda(f) = 4L(f)$. When $\ell \neq 2$, no such simple relation exists. For example, in $\mathbb{Z}/7\mathbb{Z}$, let us take $f(x) = x^6 + x^3$ and $g(x) = x^6 + x^3 + x^2$. Then $L(f) = L(g) = 9$ but $\lambda(f) = 39.96\cdots$ while $\lambda(g) = 26.19\cdots$.

Using high $L(f)$ for an attack is a direct generalization of Matsui's linear cryptanalysis. Using high $\lambda(f)$ is more tricky.

Piling-up lemma

Theorem

$$LP(h_K) \approx LP(f)LP(g)$$

if the following hypothesis hold:

- *Stochastic equivalence.* $\Lambda_S(h_K)_{a,c;u+\langle b|K\rangle}$ *does not depend heavily on* K*;*
- *Dominant trail and independence.*

$$\max_{\substack{a,b,c,u \\ T_{a,b}=T_{b,c}}} \left| \sum_v \Lambda_S(f)_{a,b;u-v} \Lambda_S(g)_{b,c;v} \right| \approx$$

$$\max_{a,b_f,b_g,c,u,v} \left| \Lambda_S(f)_{a,b_f;u-v} \Lambda_S(g)_{b_g,c;v} \right|$$

There is also a piling-up lemma for λ.

Optimal functions

Functions over $\mathbb{F}_p$ that have optimal resistance against linear cryptanalysis have degree 2.

Theorem

Let G be a group of cardinality p, with p prime. If $L(f) = 1$, then f can be interpolated by a polynomial of degree 2.

Open problems

- Explain the differences between the two linear parameters $L(f)$ and $\lambda(f)$
- Generate functions with good such parameters, without using some kind of random search
- Formalize the “special role” of elements of small characteristic
- Is our toy cipher resistant?

Conclusion

- Extension of usual block cipher theory over $\mathbb{Z}_2^n$ to a more general framework in which the input and output spaces are arbitrary abelian groups
- Generalized differential and linear cryptanalysis
- Design and analysis of a new block cipher(using the classical key-alternating structure)