Mirror Theory and Cryptography

Jacques Patarin

Laboratoire de Mathématiques de Versailles, UVSQ,
CNRS, Université Paris-Saclay, 78035 Versailles, France

Abstract. "Mirror Theory" is the theory that evaluates the number of solutions of affine systems of equalities ($=$) and non equalities ($\neq$) in finite groups. It is deeply related to the security and attacks of many generic cryptographic secret key schemes, for example random Feistel schemes (balanced or unbalanced), Misty schemes, Xor of two pseudo-random bijections to generate a pseudo-random function etc. In this paper we will assume that the groups are abelian. Most of time in cryptography the group is $((\mathbb{Z}/2\mathbb{Z})^n, \oplus)$ and we will concentrate this paper on these cases. We will present here general definitions, some theorems, and many examples and computer simulations.

1 Definitions

Definition 1 (Mirror System T, and $H(T)$). *A "Mirror system" T is a set of affine equations ($=$) or affine non equalities ($\neq$) in a finite group G. In this paper we will assume that the group G is abelian. Very often in cryptography G will be $G = ((\mathbb{Z}/2\mathbb{Z})^n, \oplus)$. Then T is a set of equations (and respectively non equalities) of the form: $X_1 \oplus X_2 \ldots \oplus X_k = c$ (respectively $\neq c$), where c is a constant of G. Let m be the number of equalities in T, and v be the number of variables $X_1, \ldots, X_v$ in T.*
Each equality of G has a linear part and a constant. We denote by $c_1, \ldots, c_m$ these m constants (c_i can be 0 or not). We denote by $H(T)$, or by $H(c_1, \ldots, c_m)$, or simply by H, the number of solutions $(X_1, \ldots, X_v)$ of T.

Remark 1. In more general abelian groups we can have variables X_i or X_i^{-1} in these equalities or non equalities, and the same variable can appear more than one time (for example $X_1 * X_1 * X_1 * X_2 * X_2 = c$), i.e. we can have some coefficients in the affine equations. However in the cryptographic applications if we change $G = ((\mathbb{Z}/2\mathbb{Z})^n, \oplus)$ for another abelian group, we will generally have no coefficient (except 0 or 1) in the variables of the mirror systems that we will want to study. Therefore the definitions, analysis, and results obtained for $G = ((\mathbb{Z}/2\mathbb{Z})^n, \oplus)$ will be generally very similar for other abelian groups in most cryptographic applications.

Definition 2. *First case : when $G = ((\mathbb{Z}/2\mathbb{Z})^n, \oplus)$.*
Let T be a mirror system. We will say that an equation E can be obtained (or deduced) from T "by linearity" when we can obtain E by xoring some equalities of T.
Second case : more general abelian groups $(G, *)$.
Here the definition is more complex since from one equation we also have its inverse equation (for example from $X_1 * X_2 = c$, we can also use $X_1^{-1} * X_2^{-1} = c^{-1}$), and since it is usefull to integrate some simplification rules on the coefficients, but also since we have to be careful about a coefficient making a variable to 0. All these points can be solved, but we will not give details here since in this paper we concentrate only on First Case. (Moreover as said in Remark 1 above for cryptographic applications we generally have mirror systems with no coefficients).

Definition 3. *Let X_1 be a variable of T. A "minimal equation" for X_1 is an equation B such that:*

- *we can deduce B from T by linearity*
- *B has the variable X_1*
- *all the other equations with the variables X_1 that we can deduce by linearity from T have at least more or the same number of variables than B.*

Definition 4 (block of variables, $\xi(A)$, $\xi_{\mathbf{max}}$, depth(A)). *We will say that two variables X_i and X_j are "in the same block" when we can deduce this from these rules:*

- *if $(i = j)$ then X_i and X_j are in the same block.*
- *If there is a minimal equation for X_i with the variable X_j then X_i and X_j are in the same block.*
- *If there is a variable X_k such that (X_i and X_k are in the same block) and (X_j and X_k are in the same block) then X_i and X_j are in the same block.*

When A is a block of variables $\xi(A)$ denotes the number of variables in A. ξ_{max} denotes the maximum value $\xi(A)$ for a block A. depth(A) denotes the minimum number of variables that we have to fix in order to fix by linearity all the variables of A.

For example if T is: $x_1 \oplus x_3 = x_2 \oplus x_4$, then in T we have only one block A, with $\xi(A) = 4$, and depth$(A) = 3$. However, if we add the equation $x_1 = x_2 \oplus a$, then now T has two blocks: $x_1 = x_2 \oplus a$ and $x_3 = x_4 \oplus a$, with $\xi = 2$ and depth $= 1$ in these two blocks.
From Definition 4 we see that "being in the same block" is (as expected) an equivalence relation.

Example 1 ("$\xi = 3$ and $\xi = 2$ system"). Let T be this system of 4 equations on $(\mathbb{Z}/2\mathbb{Z})^n$, with pairwise distinct variables $P_1, P_2, P_3, P_4, P_5, P_6, P_7$:

$$P_2 = P_1 \oplus c_1$$

$$P_4 = P_3 \oplus c_2$$

$$\begin{cases} P_6 = P_5 \oplus c_3 \\ P_7 = P_5 \oplus c_4 \end{cases}$$

c_1, c_2, c_3, c_4 are the constants.
We have here 3 blocks of equations, two blocks with $\xi = 2$ and one block with $\xi = 3$, so $\xi_{\max} = 3$.

Definition 5 (Regular Systems). *We will say that T is a "regular system" if it is a miror system that satisfies these properties S1 and S2:*

S1: By linearity from the equalities of T we cannot obtain X_i = a constant, or $X_i \neq$ a constant (where X_i is one of the variables of T), i.e. we always have by linearity at least two variables in $=$ or $\neq$.
S2: Let $X'_1, \ldots, X'_a$ be the variables of a block B, and $X_1, \ldots, X_q$ the other variables of T (not in B). We say that we have property S2 when: for each block B of T, when $X_1, \ldots, X_q$ are fixed, the number of $X'_1, \ldots, X'_a$ that satisfy the non equalities $(\neq)$ do not depend on $X_1, \ldots, X_q$.

Example. In example 1 above the system T is a "regular system". For example when P_1, P_2, P_3, P_4 are fixed, for (P_5, P_6, P_7) we have exactly $(2^n - 4)(2^n - 5)(2^n - 6)$ solutions that satisfy all the non equalities $(\neq)$.
However with this system T':

$$X_1 \oplus X_2 = c_1,$$

$$X_3 \oplus X_4 = c_2,$$

$$X_5 \oplus X_6 = c_3,$$

$$X_5 \neq X_1,\ X_5 \neq X_3,$$

T' is not a "regular system" since when X_1, X_2, X_3, X_4 are fixed, the number of solutions (X_5, X_6) that satisfy $X_5 \neq X_1$ and $X_5 \neq X_3$ depend on the fact that $X_1 = X_3$ or not.

Definition 6 ("Standard form"). *A system T is in "standard form" when all the non equalities $(\neq)$ of T are of the form $X_i \neq X_j$ (with $i \neq j$). By introducing new variables X_k it is always possible to write a system T in standard form.*

Definition 7 **($\mathrm{Weight}(T)$).** *$\mathrm{Weight}(T)$ is the number of $(X_1, \ldots, X_v)$ that satisfy only the non equalities ($\neq$) of T (i.e. we give up here the equalities). In standard form, $\mathrm{Weight}(T)$ is always easy to compute.*

Example. In example 1 above, $\mathrm{Weight}(T) = 2^n(2^n-1)(2^n-2)(2^n-3)(2^n-4)(2^n-5)(2^n-6)$.

Definition 8 **(Block conditions and $\mathrm{Space}(T)$).** *The "block conditions" are equalities or non equalities on the constants c_i that we can deduce by linearity by using the equalities and non equalities of T (when we consider $c_1, \ldots, c_m$ as variables).*

Example. In example 1 above the "Block conditions" are

$$c_1 \neq 0, c_2 \neq 0, c_3 \neq 0, c_4 \neq 0, c_3 \neq c_4.$$

We say that a constant c_i is "compatible with T by linearity" if c_i satisfies all the block conditions. When T is in standard form, $\mathrm{Space}(T)$ is the number of $(c_1, \ldots, c_m)$ that are compatible with T by linearity. $\mathrm{Space}(T)$ is also easy to compute.

Example. In example 1 above

$$\mathrm{Space}(T) = (2^n-1)^3(2^n-2).$$

Remark 2. As said above, any system can be written in standard form. However the resulting system will generally not have the same weight, or space.

Definition 9 **($\tilde{H}$ and $\tilde{M}$).** *We will denote*

$$\tilde{H} = \frac{\mathrm{Weight}(T)}{\mathrm{Space}(T)}$$

$\tilde{H}$ is the mean value of H when $(c_1, \ldots, c_m)$ are randomly chosen compatible by linearity with T.

$$\tilde{H} = \sum_{c_1,\ldots,c_m \text{ compatible by linearity}} \frac{H(T)}{\text{Number of } c_1,\ldots,c_m \text{ compatible by linearity}}$$

We will denote

$$\tilde{M} = \frac{\mathrm{Weight}(T)}{|G|^m}.$$

$\tilde{M}$ is the mean value of H when $(c_1, \ldots, c_m)$ are randomly chosen in G^m.

$$\tilde{M} = \sum_{(c_1,\ldots c_m)\in G^m} \frac{H(T)}{|G|^m}$$

Definition 10 **(Tame and Wild systems).** *We say that T is "Tame" (on $(c_1, \ldots, c_m)$) when $H \simeq \tilde{H}$ i.e. $H \simeq \frac{\mathrm{Weight}(T)}{\mathrm{Space}(T)}$ (here $c_1, \ldots, c_m$ are fixed).*
We say that T is "Wild" when T is not Tame.
For a system T (now $c_1, \ldots, c_m$ are not fixed), the "wild" coefficient is defined as $\mathrm{W}(T) = \frac{E(|H-\tilde{H}|)}{\tilde{H}}$ where E is the mean value function.
We say that T is "Tame on average" when for randomly chosen $(c_1, \ldots, c_m)$ compatible by linearity with T there is a high probability that T is Tame, i.e. when $\mathrm{W}(T) \ll 1$.
We say that T is "Always Tame" or "Tame in worst case" when for all constants $(c_1, \ldots, c_m)$ compatible with T by linearity

$$H(c_1, \ldots, c_m) \gtrsim \frac{\mathrm{Weight}(T)}{\mathrm{Space}(T)}.$$

Here $a \gtrsim b$ means $a \geq b$ or $a \simeq b$.
We say that H is "homogeneous" when for all constants $(c_1, \ldots, c_m)$ compatible with T by linearity

$$H(c_1, \ldots, c_m) \simeq \frac{\mathrm{Weight}(T)}{\mathrm{Space}(T)}.$$

Remark 3. The use of the fusy term ($\simeq$) in the definition of "Tame" can look at first surprising, but, as we will see, "Tame" will be closely related to "Secure" in most generic cryptographic application, and in the same way that we can use "Advantage" to evaluate precisely the security, we can use the wild coefficient (defined without the fusy term) to evaluate Tame.

Remark 4. Very often systems T will have a very small number of $(c_1, \ldots, c_m)$ with $H(c_1, \ldots, c_m)$ much larger than $\frac{\text{Weight}(T)}{\text{Space}(T)}$. This will generally not be a problem (as long as this number of $(c_1, \ldots, c_m)$ is small) and this is why in the definition of "Always Tame" we used $\gtrsim$ instead of $\simeq$. Homogeneous systems seldom appear and are at present much less important than Always Tame systems in systems that are used in cryptography.

We say that H is "σ Tame" when, for constants $(c_1, \ldots, c_m)$ randomly chosen compatible by linearity with T the standard deviation $\sigma(H)$ of H satisfies: $\sigma(H) \ll \frac{\text{Weight}(T)}{\text{Space}(T)}$ ($a \ll b$ means as usual that a is small compared with b).
"Mirror Theory" is the theory that evaluates the number of solutions H of mirror systems T. A particularly important aim in Mirror Theory is to evaluate when T is Tame. As we will see this is closely related to the security of many generic cryptographic designs, where "Tame" will be associated with "secure" (with a proof of security).

Remark 5. The nickname "Mirror" comes from the fact that we will have a huge number of induction formulas between these systems, and also with the systems related with $\sigma(H)$.

2 First Properties

Theorem 1. *For all Mirror systems T,*

$$\begin{tikzcd}
 & \text{Always Tame} \arrow[dr, Rightarrow] & \\
\text{homogeneous} \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & & \text{Tame in average} \\
 & \sigma \text{ Tame} \arrow[ur, Rightarrow] &
\end{tikzcd}$$

Proof.

- Homogeneous $\implies$ Always Tame: comes immediately from the definitions.
- Homogeneous $\implies$ σ Tame: if $\forall c_1, \ldots, c_m$, $|H - E(H)| \leq \epsilon$, then $\sigma(H) \leq \epsilon$.
- Always Tame $\implies$ Tame in average: if $\forall c_1, \ldots, c_m$, $H \geq E(H) - \epsilon$, then $E(|H - E(H)|) \leq 2\epsilon$
- σ Tame $\implies$ Tame in average: $E(|H - E(H)|) \leq \sigma(H)$ (see Cauchy-Schwartz or Jensen's inequality since x^2 is a convex function).

However σ Tame $\not\Longrightarrow$ Always Tame (example: a small probability where $H \ll E(H)$), and Always Tame $\not\Longrightarrow$ σ Tame (example: $H \geq E(H) - \epsilon$ and with probability $\frac{\epsilon}{2A}$, $H \geq E(H) + A$ with $A \geq \frac{1}{\epsilon}$).

Theorem 2. *Let T' be a regular system. Let T be a sub-system of T' where some blocks of T' have been removed. Then:*

- *if T' is Tame, T is Tame,*
- *if T' is Always Tame, T is Always Tame,*
- $\mathrm{W}(T) \leq \mathrm{W}(T')$.

Proof. Let $X'_1, X'_2, \ldots, X'_v$ be the variables in T' and not in T. Let $X_1, X_2, \ldots, X_q$ be the variables of T. Let $c'_1, c'_2, \ldots, c'_\mu$ be the constants in T' and not in T. Let $c_1, c_2, \ldots, c_\alpha$ be the constants of T.
Since T' is regular:

$$H(c_1, \ldots, c_\alpha) = \frac{\displaystyle\sum_{c'_1, \ldots, c'_\mu} H(c_1, \ldots, c_\alpha, c'_1, \ldots, c'_\mu)}{[\text{Number of } X'_1, \ldots, X'_v \text{ that satisfy the } \neq \text{ when } X_1, \ldots, X_q \text{ is fixed}]}. \tag{1}$$

Therefore $H(c_1, \dots, c_\alpha)$ of T is proportional (with a fixed constant) to the average value (on $c'_1, \dots, c'_\mu$) of $H(c_1, \dots, c_\alpha, c'_1, \dots, c'_\mu)$ of T'.
By definition,

$$\mathrm{W}(T) = \frac{E(|H - E(H)|)}{E(H)}, \tag{2}$$

$$\text{and } \mathrm{W}(T) = \frac{E(|H' - E(H')|)}{E(H')}, \tag{3}$$

where H' denotes $H(c_1, \dots, c_\alpha, c'_1, \dots, c'_\mu)$. From 1 and 2 we get $\mathrm{W}(T) \leq \mathrm{W}(T')$ as claimed (we regroup some terms of H' in H, and due to the absolute value $\mathrm{W}(T) \leq \mathrm{W}(T')$).

Definition 11 ((P1), (P2) and (P3) properties). *We will denote by (P1), (P2) and (P3) these properties (they can be satisfied or not):*

(P1): For all $(c_1, \dots, c_m)$ compatible by linearity with T we have: $H(c_1, \dots, c_m) \neq 0$

P1 means that if $(c_1, \dots, c_m)$ are compatible by linearity, then $(c_1, \dots, c_m)$ are really compatible.

(P2): For all $(c_1, \dots, c_m)$ compatible by linearity with T we have: $H(c_1, \dots, c_m) \geq \tilde{M}$.

Very often we will see that Tame systems T have property (P1) and (P2).

(P3): When a set A of systems T satisfies: "for all $T \in A$, if T satisfies (P1) then T is Tame" we will say that A satisfies property (P3).

Typical Theorem in Mirror Theory

A typical Theorem in Mirror Theory will be for example: if in all the blocks $\xi \ll$ a value A (or if the average value of ξ is $\leq A$) and the number v of variables is $v \ll |G|$, then the system is Tame. Notice that here for the number of variables we have $|G|$ and not $\sqrt{|G|}$ for example. Moreover we will generally want precise evaluations for how "Tame" the system is, and for $\ll$, and for the value A. This is what is done for some T systems in [**?**], [**?**] or [**?**] for example.

3 Examples

Example (same example as in section 1)"$\xi = 3$ and $\xi = 2$ system"). Let T be this system of 4 equations on $(\mathbb{Z}/2\mathbb{Z})^n$, with pairwise distinct variables $P_1, P_2, P_3, P_4, P_5, P_6, P_7$:

$$P_2 = P_1 \oplus c_1$$

$$P_4 = P_3 \oplus c_2$$

$$\begin{cases} P_6 = P_5 \oplus c_3 \\ P_7 = P_5 \oplus c_4 \end{cases}$$

c_1, c_2, c_3, c_4 are the constants.
We have here 3 blocks of equations, two blocks with $\xi = 2$ and one block with $\xi = 3$ so $\xi_{\max} = 3$.
The block conditions are $c_1 \neq 0$, $c_2 \neq 0$, $c_3 \neq 0$, $c_4 \neq 0$ and $c_3 \neq c_4$.
In $(\mathbb{Z}/2\mathbb{Z})^3$, i.e. on 3 bits

On 3 bits, we have

$$\tilde{M} = \frac{\text{Weight}(T)}{8^4} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{8^4} = \frac{40320}{4096} = 9.84.$$

$\text{Space}(T) = 7^3 \cdot 6 = 2058$ constants (c_1, c_2, c_3, c_4) satisfy the bloc conditions.

$$\tilde{H} = \frac{\text{Weight}(T)}{\text{Space}(T)} = 19.59.$$

Computer simulations show that here we have:

- 924 values (c_1, c_2, c_3, c_4) satisfy the block conditions but have $H = 0$
- 1008 values have $H = 32$

- 126 values have $H = 64$.

We can check that: $924 + 1008 + 126 = 2058$ (all the constants that satisfy the block conditions) and that: $1008 \cdot 32 + 126 \cdot 64 = 40320$ (all the $(P_1, P_2, \ldots, P_7)$).

We see that here the system T (on 3 bits) is "always wild", i.e. for every constants c_1, c_2, c_3, c_4, H is never $\simeq 9.84$.

In $(\mathbb{Z}/2\mathbb{Z})^4$, i.e. on 4 bits

On 4 bits we have $\tilde{M} = \frac{\text{Weight}(T)}{16^4} = 879.78$.

We have $15^3 \cdot 14 = 47250$ constants that satisfy the block conditions, and $\tilde{H} = \frac{\text{Weight}(T)}{47250} = 1220.26$.

Computer simulations show that here we have:

- 0 values $(c_1, \ldots, c_4)$ that satisfy the bloc conditions with $H = 0$
- 7560 values have $H = 1024$
- 20160 values have $H = 1152$
- 2520 values have $H = 1280$
- 15120 values have $H = 1344$
- 1260 values have $H = 1536$
- 630 values have $H = 1920$.

Let $\sigma'(H) = E(|H - \tilde{H}|)$. Here we have: $\sigma'(H) \simeq 120 \ll 1220$ and therefore here T is "Tame on average". The standard deviation is $\sigma(H) \simeq 152 \ll 1220$ and therefore here T is also "σ Tame". Moreover here the system T (on 4 bits) is "always Tame", i.e. for every constants c_i compatible with the block conditions we have $H \gtrsim \tilde{H}$ since $1024 \simeq 1220$. Here the system is always Tame but not Homogeneous since 1920 is not $\simeq 1220$ but this is classical: very often tame systems have very large H on a very small number of variables. We also have here properties (P1) and (P2). Figure 1 illustrates such systems.

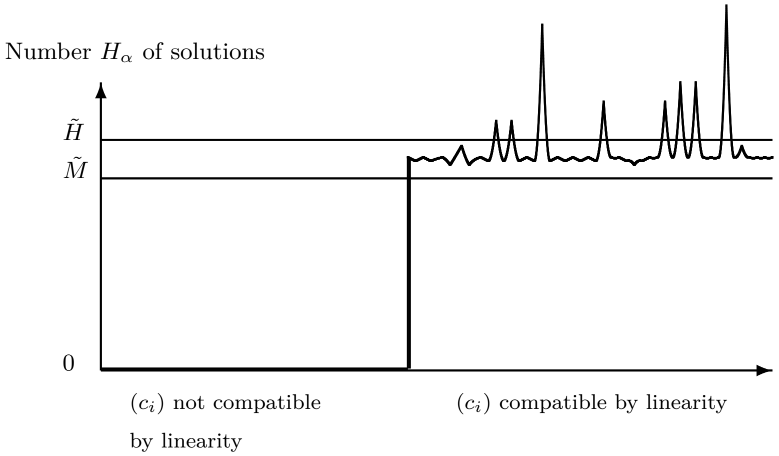

Fig. 1. Typical solution H for always Tame systems but not Homogeneous systems, with property (P2).

Example 2 ("$P_i \oplus Q_j$ with $\xi_{\max} = 2$", or "Xor of Two bijections in H standard"). Let T be this system of 7 equations with pairwise distinct variables P_i, and pairwise distinct variables Q_i:

$$P_1 \oplus Q_1 = c_1$$
$$P_2 \oplus Q_2 = c_2$$
$$P_3 \oplus Q_3 = c_3$$
$$P_4 \oplus Q_4 = c_4$$
$$P_5 \oplus Q_5 = c_5$$
$$P_6 \oplus Q_6 = c_6$$
$$P_7 \oplus Q_7 = c_7.$$

We have here 7 blocks of equations, $\xi = 2$ on each block. Here we have no block conditions on the c_i.
We did our computation on $G = (\mathbb{Z}/2\mathbb{Z})^3$, i.e. on 3 bits. Here Weight$(T) = (8!)^2$, Space$(T) = 8^7$,

$$\tilde{H} = \tilde{M} = \frac{\text{Weight}(T)}{8^7} = 775.19.$$

Computer simulation show that here we have:

- 0 values $(c_1, \ldots, c_7)$ with $H = 0$
- 40320 values have $H = 384$
- 987840 values have $H = 640$
- 752640 values have $H = 768$
- 258720 values have $H = 1152$
- 35280 values have $H = 1408$
- 18816 values have $H = 1920$
- 1960 values have $H = 3456$
- 1568 values have $H = 5760$
- 8 values have $H = 40320$.

Here the system is not always Tame since $384 \leq \frac{\tilde{H}}{2}$, but it is Tame on average.
Here we have property (P1) (i.e. 0 values block compatible with $H = 0$) and not property (P2). In fact property (P2) was impossible here since $\tilde{H} = \tilde{M}$ and H is not a constant.
Moreover it is interesting to notice that it was possible to see that property (P1) was true without doing any computation. We just have to use a Theorem of 1952 of Marshall Hall Jr: see [**?**]. We will give more details about this section 5 of this paper.

Remark 6. Let us now consider the system T' such that T' is T plus one more equation: $P_8 \oplus Q_8 = c_8$. In $(\mathbb{Z}/2\mathbb{Z})^3$ we will have: $\bigoplus_{i=1}^{8} P_i = 0$ and $\bigoplus_{i=1}^{8} Q_i = 0$. Therefore if $\bigoplus_{i=1}^{8} c_i \neq 0$, we will have no solution. And if $\bigoplus_{i=1}^{8} c_i = 0$ then $P_8 \oplus Q_8 = c_8$ can be removed since it is just a consequence of T, and T and T' have the same solutions.

Example 3 ("$P_i \oplus P_j$ with $\xi_{\max} = 2$").
7 equations

Let T be this system of 7 equations with pairwise distinct variables P_i:

$$\begin{aligned} P_1 \oplus P_2 &= c_1 \\ P_3 \oplus P_4 &= c_2 \\ P_5 \oplus P_6 &= c_3 \\ P_7 \oplus P_8 &= c_4 \\ P_9 \oplus P_{10} &= c_5 \\ P_{11} \oplus P_{12} &= c_6 \\ P_{13} \oplus P_{14} &= c_7 \end{aligned}$$

We have here 7 blocks of equations, $\xi = 2$ on each block. Here the block conditions are: $\forall i, 1 \leq i \leq 7, c_i \neq 0$.
We did our computation on $G = (\mathbb{Z}/2\mathbb{Z})^4$, i.e. on 4 bits. Here

$$\begin{array}{ll} \text{Weight}(T) = \frac{16!}{2}, & \text{Space}(T) = 15^7, \\ \tilde{H} = \frac{\text{Weight}(T)}{15^7} = 61228.10, & \tilde{M} = \frac{16!}{2 \cdot 16^7} = 38971.73. \end{array}$$

Computer simulations show that here we have (13 cases here):

- 10678710 values $(c_1, \ldots, c_7)$ block compatible give $H = 0$ solutions.
- 40294800 values have $H = 49152$
- 50803200 values have $H = 57344$

- 25401600 values have $H = 65536$
- 11289600 values have $H = 73728$
- 17992800 values have $H = 81920$
- 11289600 values have $H = 98304$
- 2690100 values have $H = 147456$
- 264600 values have $H = 180224$
- 141120 values have $H = 245760$
- 7350 values have $H = 442368$
- 5880 values have $H = 737280$
- 15 values have $H = 5160960$.

Here the system T is Tame but not always Tame. The fact that it is Tame is a very good stability property since here the number of variables (14) is almost the number of elements in G (since here $|G| = 16$) and we have a lot of equations (7). (This result is also compatible with the general analysis of such systems done in [**?**, **?**], i.e. "Theorem $P_i \oplus P_j$").

8 equations

Let us now consider the system T' such that T' is T plus one more equation: $P_{15} \oplus P_{16} = c_8$. In $(\mathbb{Z}/2\mathbb{Z})^4$ we will have $\bigoplus_{i=1}^{16} P_i = 0$. Therefore if $\bigoplus_{i=1}^{8} c_i \neq 0$, we will have no solution. And if $\bigoplus_{i=1}^{8} c_i = 0$ then $P_{15} \oplus P_{16} = c_8$ can be removed since it is just a consequence of T, and T' has exactly 2 times the number of solutions of T (since (P_{15}, P_{16}) and (P_{16}, P_{15}) give the same solution).

6 equations

Let us now consider the system T'' such that T'' is T without the equation $P_{13} \oplus P_{14} = c_7$. On $(\mathbb{Z}/2\mathbb{Z})^4$ computer simulations show that here we have 0 values $(c_1, \ldots, c_6)$ block compatible with $H = 0$ (i.e. we have property (P1)). We have 19 different values H when $(c_1, \ldots, c_6)$ are block compatible, with $H_{\min} = 57344$ and $H_{\max} = 1290240$, $\tilde{M} = 51962$, and $\tilde{H} = 76535$. If we assume $57344 \simeq 76535$ we can say that the system is always Tame (but not Homogeneous, as usual).

4 equations

$$T : \begin{cases} P_2 = P_1 \oplus c_1 \\ P_4 = P_3 \oplus c_2 \\ P_6 = P_5 \oplus c_3 \\ P_8 = P_7 \oplus c_4 \end{cases}$$

We want solutions with pairwise distinct $P_i, 1 \leq i \leq 8$. On $(\mathbb{Z}/2\mathbb{Z})^4$, computer simulations show that we have 0 values $(c_1, \ldots, c_4)$ block compatible with $H = 0$. We have 7 different values H when $(c_1, \ldots, c_4)$ are block compatible, with $H_{\min} = 9216$, $H_{\max} = 26880$, $\tilde{M} = 7918$ and $\tilde{H} = 10250$.

Here the system is always Tame ($9216 \simeq 10250$), but not Homogeneous (as usual).

We see in these examples with 5,6,7 and 8 equations that when we have less blocks the systems are more Tame (as for any system T, see Theorem 2).

Example 4 ("σ for the Xor of two bijections").

Let H be the number of $(f_i, g_i, h_i), 1 \leq i \leq m,\ f_i, g_i, h_i \in (\mathbb{Z}/2\mathbb{Z})^n$ such that:

1. All the f_i are pairwise distinct.
2. All the g_i are pairwise distinct.
3. All the h_i are pairwise distinct.
4. All the $f_i \oplus g_i \oplus h_i$ are pairwise distinct.

This system T is associated with the standard deviation of a value in relation with the Xor of two bijections (see [**?**, **?**]).

In "standard form" H is also the number of $(f_i, g_i, h_i, t_i), 1 \leq i \leq m$, such that:

1. All the f_i are pairwise distinct.
2. All the g_i are pairwise distinct.
3. All the h_i are pairwise distinct.
4. All the t_i are pairwise distinct.
5. $\forall i, 1 \leq i \leq m, f_i \oplus g_i \oplus h_i \oplus t_i = 0$.

Here $\text{Weight}(T) = [2^n(2^n-1)\cdots(2^n-m+1)]^4$ and $\text{Space}(T) = 2^{nm}$. Here the minimal equations have 4 variables.

Example 5 ("large ξ"). Let T be this system of 6 equations with pairwise distinct variables P_i:

$$\begin{cases} P_2 = P_1 \oplus c_1 \\ P_3 = P_1 \oplus c_2 \\ P_4 = P_1 \oplus c_3 \end{cases}$$

$$\text{and} \begin{cases} P_6 = P_5 \oplus c_4 \\ P_7 = P_5 \oplus c_5 \\ P_8 = P_5 \oplus c_6. \end{cases}$$

We have here 2 blocks of equations, $\xi = 4$ on each block.
Here the block conditions are:

$$c_1 \neq 0, c_2 \neq 0, c_3 \neq 0, c_1 \neq c_2, c_1 \neq c_3, c_2 \neq c_3,$$
$$c_4 \neq 0, c_5 \neq 0, c_6 \neq 0, c_4 \neq c_5, c_4 \neq c_6, c_5 \neq c_6.$$

We did our computation on $G = (\mathbb{Z}/2\mathbb{Z})^4$, i.e. on 4 bits. Here

$$\text{Weight}(T) = 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9,$$
$$\text{Space}(T) = (15 \cdot 14 \cdot 13)^2$$
$$\tilde{H} = \frac{\text{Weight}(T)}{\text{Space}(T)} = 69.62$$
$$\tilde{M} = \frac{\text{Weight}(T)}{16^6} = 30.93.$$

Computer simulations show that here we have:

- 141120 values $(c_1, \ldots, c_6)$ block compatible give $H = 0$ solutions
- 725760 values have $H = 32$
- 3991680 values have $H = 64$
- 1935360 values have $H = 80$
- 597240 values have $H = 128$
- 60480 values have $H = 144$
- 1260 values have $H = 192$.

Here 11% of the values $(c_1, \ldots, c_6)$ block compatible have $H < \frac{\tilde{H}}{2}$, and moreover 1.89% have $H = 0$ (however, as often, when $H \neq 0$, then $H \geq \tilde{M}$). The system is not Tame. More generally, let $G = (\mathbb{Z}/2\mathbb{Z})^n$ and let us consider the number h' of $(P_1, \ldots, P_\alpha)$ such that the P_i are pairwise distinct and:

$$\begin{cases} P_2 = P_1 \oplus c_1 \\ P_3 = P_1 \oplus c_2 \\ \vdots \\ P_{\alpha/2} = P_1 \oplus c_{\alpha/2-1} \end{cases} \quad \textit{and} \begin{cases} P_{\alpha/2+2} = P_{\alpha/2+1} \oplus c_{\alpha/2} \\ \vdots \\ P_\alpha = P_{\alpha/2+1} \oplus c_{\alpha-2}. \end{cases}$$

We have here 2 blocks of equations and $\xi = \frac{\alpha}{2}$ on these blocks.
For $(P_1, \ldots, P_{\alpha/2})$ we have 2^n possibilities: just fix P_1 to any value.
For $P_{\alpha/2+1}$ we want this value to be different from all the following values (by convention $c_0 = 0$ and $c_{\alpha-1} = 0$):

$$P_1 \oplus c_i \oplus c_j \qquad \text{for all } 0 \leq i \leq \frac{\alpha}{2} - 1, \frac{\alpha}{2} \leq j \leq \alpha - 1 \qquad \text{(because we want } P_i \neq P_j\text{)}$$

Now when $\alpha^2 \gg 2^n$ with $\alpha \ll 2^n$, it can occur that the $c_i \oplus c_j$ cover all the values of $(\mathbb{Z}/2\mathbb{Z})^n$. Then we will have here $H = 0$ despite the fact that the constants c_i are block compatible.

4 About the computer simulations

When G is very small, we can often perform exhaustive search of the solutions on a computer in reasonable time.
However, there are many ways to accelerate the computations (or do them on larger G, or with more variables or equations). Here are some of these ideas (many more exist).

1. In our examples, we can assume $P_1 = 0$.

   Proof. If we change all the X_i variables by $X_i \oplus c$, where c is a constant, and since in our example we always have an even number of variables in our equations, then if $(X_1, \ldots, X_m)$ is a solution, $(X_1 \oplus c, \ldots, X_m \oplus c)$ is also a solution. Therefore $H = (H \text{ with } P_1 = 0) \cdot 2^n$ when $G = (\mathbb{Z}/2\mathbb{Z})^n$ in our examples. □

2. In our examples 2, 4, 5 we can assume $c_1 = 1$

   Proof. $c_1 \neq 0$ (from the block conditions). Now in GF(2^n) the value c_1 has an inverse $\beta = \frac{1}{c_1}$. If $(X_1, \ldots, X_m)$ is a solution for $(c_1, \ldots, c_m)$, then $(\beta X_1, \ldots, \beta X_m)$ is a solution for $(1, \beta c_2, \ldots, \beta c_m)$. Therefore $(c_1, \ldots, c_m)$ and $(1, \beta c_2, \ldots, \beta c_m)$ have the same number H of solution. So we can assume $c_1 = 1$ (in examples 2, 4, 5) and multiply by $2^n - 1$ the number of $(c_1, \ldots, c_m)$ that give H solutions. □

   Similarly, in example 3 we can compute only for $c_1 = 0$ and for $c_1 = 1$ (all $c_1 \neq 0$ will have the same property as $c_1 = 1$).

3. In example 4 we can assume $P_3 < P_4, P_5 < P_6, \ldots, P_{13} < P_{14}$

   Proof. This is obvious by symmetry of the hypothesis. Then we will just multiply H by 2^6 (since P_1 was fixed, from idea 1 above, we did not use $P_1 < P_2$ here). □

   Similarly in all the other examples we have also many symmetries.

4. We can use symmetries on the c_i
   Here we will separate the case where all the c_i are pairwise distinct, then the case where we have exactly one equality, then 2 cases where we have 2 equalities (like $c_1 = c_2$ and $c_3 = c_4$ or like $c_1 = c_2 = c_3$) etc.

5. In [**?**, **?**] some "Orange", "Purple" and "Red" induction equations have been introduced for a theoretical analysis. We will not present these equations in this paper but it is also possible to use them to accelerate the computations on many systems.

5 Marshall Hall Jr Theorem and my conjecture of 2008

Let F_n be the set of all applications $\{0,1\}^n \longrightarrow \{0,1\}^n$. Let B_n be the set of all bijections $\{0,1\}^n \longrightarrow \{0,1\}^n$.
In 1952, Marshall Hall Jr has proved (see [**?**]) that:

$$\forall f \in F_n, \text{ if } \bigoplus_{x \in \{0,1\}^n} f(x) = 0, \text{ then } \exists (g,h) \in B_n^2 \text{ such that } f = g \oplus h.$$

This theorem was proved again in 1979 in [**?**].
Moreover this result was proved on any abelian group, not only for $((\mathbb{Z}/2\mathbb{Z})^n, \oplus)$.
However in [**?**, **?**] we just have that $\exists (g,h) \in B_n^2$, but we have no information about the number H of such (g,h) (except that $H \neq 0$).

Remark 7. Example 2 of section 3 (or, more precisely the system T' given after example 2 of section 3) is just a special case on $((\mathbb{Z}/2\mathbb{Z})^3, \oplus)$. Marshall Hall Theorem says $H > 0$, and our simulations shows $H \geq 384$.

My conjectures of 2008

Conjecture 1. $\forall f \in F_n$, if $\bigoplus\limits_{x\in\{0,1\}^n} f(x) = 0$, then the number H of $(g,h) \in B_n^2$ such that $f = g\oplus h$ satisfies

$$H \geq \frac{|B_n|^2}{2^{n2^n}}.$$

I made this conjecture on any abelian group, not only for $((\mathbb{Z}/2\mathbb{Z})^n, \oplus)$.

Conjecture 2. The minimum value for H is obtained when f is a bijection.

As far as I know these two conjectures are still open problems.

Remark 8. It is however easy to see that the maximum value for H is obtained when f is a constant function. Then $H = |B_n|$ since then for all $g \in B_n$, $f \oplus h$ is a bijection.
For constant functions f the value H is much larger than the average value for H.

Computer simulations

Example 3 of section 2 shows that my conjecture 1 is true on $(\mathbb{Z}/2\mathbb{Z})^3$ since $384 \geq \frac{775.19}{8} = 96.89$. Emmanuel Volte (of University of Cergy-Pontoise) has done many more computer simulations to test my conjecture 1 on various groups. Let $H^* = \frac{|B_n|^2}{2^{n2^n}}$. Here are the result he found (where the conjecture means $H_{\min} \geq H^*$):

- $(\mathbb{Z}/2\mathbb{Z})^2 : H_{\min} = 8,\ H^* = 2$
- $\mathbb{Z}/4\mathbb{Z} : H_{\min} = 8,\ H^* = 2$
- $\mathbb{Z}/6\mathbb{Z} : H_{\min} = 48,\ H^* = 11$
- $(\mathbb{Z}/2\mathbb{Z})^3 : H_{\min} = 384,\ H^* = 96$ (same result as my example 2)
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} : H_{\min} = 384,\ H^* = 96$
- $\mathbb{Z}/8\mathbb{Z} : H_{\min} = 512,\ H^* = 96$
- $\mathbb{Z}/9\mathbb{Z} : H_{\min} = 2025,\ H^* = 340$
- $\mathbb{Z}/10\mathbb{Z} : H_{\min} = 9280,\ H^* = 1320$
- $\mathbb{Z}/12\mathbb{Z} : H_{\min} = 210432,\ H^* = 25700$
- $(\mathbb{Z}/2\mathbb{Z})^4 : H_{\min} = 244744192,\ H^* = 23700000.$

In each case computed we see that conjecture 1 was true.

6 Examples of Connections between Mirror Systems and Cryptographic Security of Generic Schemes

I_n denotes $\{0,1\}^n$.

Xor of 2 bijections, *H* standard technique

Let f and g be two random bijections from $I_n \to I_n$. We want to distinguish $f\oplus g$ from a random application from $I_n \to I_n$. For this problem, the security in KPA and CPA-2 are equivalent (see [**?**] p. 5).
With m queries we have an exact value for the Advantage (see [**?**] p. 4):

$$\mathrm{Adv}_m = \frac{1}{2\cdot 2^{nm}} \sum_{b_1,\ldots,b_m\in I_n} \left| \frac{h_m}{\tilde{h}_m} - 1 \right| = \frac{1}{2^{nm}} \sum_{b_1,\ldots,b_m\in F} \left(\frac{h_m}{\tilde{h}_m} - 1 \right)$$

where

- h_m is the number of $(P_1,\ldots,P_m,Q_1,\ldots,Q_m) \in I_n^{2m}$ such that
  1. The P_i are pairwise distinct.
  2. The Q_i are pairwise distinct.
  3. $\forall i, 1 \leq i \leq m, P_i \oplus Q_i = b_i$.

- $\tilde{h}_m$ is the average value of h_m when $(b_1, \ldots, b_m) \in_R I_n^m$. We have

$$E(h_m) = \tilde{h}_m = \frac{(2^n(2^n-1)\ldots(2^n-m+1))^2}{2^{nm}}.$$

- $F = \{(b_1, \ldots, b_m) \in I_n^m \text{ such that } h(b_1, \ldots, b_m) \geq \tilde{h}_m\}$.

Therefore, we see that the security for this problem is exactly the fact that the system T: $P_i \oplus Q_i = b_i$ for pairwise distinct P_i, and pairwise distinct Q_i is Tame on average, and $\mathrm{Adv}_m = \frac{\mathrm{W}(T)}{2}$, where $\mathrm{W}(T)$ is the "wild coefficient" of the system T.
From this in [?] security for this problem is proved when $q \ll 2^n$.

Xor of 2 bijections, H_σ technique

With the same notations as above, we have:

$$\mathrm{Adv}_m \leq 2\left(\frac{\sigma(h_m)}{E(h_m)}\right)^{2/3} \qquad \text{(see [?]).}$$

Let λ_m be the number of $(f_i, g_i, h_i) \in I_n^{3m}$ such that:

1. The f_i are pairwise distinct.
2. The g_i are pairwise distinct.
3. The h_i are pairwise distinct.
4. The $f_i \oplus g_i \oplus h_i$ are pairwise distinct.

Let T' be these sets of equalities and non equalities. Let

$$U_m = \frac{(2^n(2^n-1)\cdots(2^n-m+1))^4}{2^{nm}} = \tilde{H}(T').$$

Then

$$\mathrm{Adv}_m \leq 2\left(\frac{\lambda_m}{U_m} - 1\right)^{1/3} \qquad [?]$$

Here we have no more c_i values (only the constant 0), and we introduce $z_i = f_i \oplus g_i \oplus h_i$, we have equations involving 4 variables. The security is directly related to the mirror system T': we have security if $\lambda_m \simeq U_m$, i.e. $H(T') \simeq \tilde{H}(T')$, i.e. if T' is Tame (for the constants 0).
From this security for this problem is proved in [?] when $q \ll 2^n$ (as with classical H technique).

Security of classical(=balanced) Feistel Schemes

As shown in [?, ?], the security (for 4 rounds in KPA, 5 or 6 rounds in CPA-2) is related to this system T of Mirror Theory (called "problem $P_i \oplus P_j$"):
T: The P_i variables are pairwise distinct variables of I_n, and we have some equalities $P_i \oplus P_j = c_{ij}$.
The number of variables P_i is smaller than the number of queries q (it is about $\frac{q^2}{2^n}$), the average value of the number $\xi(A)$ for a block A is about 2.
The security in KPA is related to the fact that T is tame on average, and a sufficient condition for CPA-2 security is for T to be always Tame.
From this security when $q \ll 2^n$ is given in [?].

Security of $f(x||0) \oplus f(x||1)$ when f is a bijection

This problem can be seen as a variant of the Xor of two bijections, but here the two bijections are not independent: we use only one bijections f, and the last bit of the input is fixed to be 0 in the first term, and 1 in the second term. Again, the problem is to distinguish the Xor of these two bijections from a random function from $I_n \to I_n$. In fact, this problem is exactly equivalent to the "problem $P_i \oplus P_j$" (seen above) when $\xi_{\max} = 2$, i.e. for this mirror system T:
T: the P_i variables are pairwise distinct variables of I_n, (we write them $P_{j,1}$ or $P_{j,2}$) and we have some equalities: $P_{i,1} \oplus P_{i,2} = c_i$ $(c_i \neq 0)$.
The security of $f(x||0) \oplus f(x||1)$ is directly related to the analysis if T is Tame on average.
This problem is slightly more difficult than the Xor of two random permutions (we have $P_i \oplus P_j$ instead of $P_i \oplus Q_j$ but we can proceed similarly) and simpler than the general $P_i \oplus P_j$ problem related with the security of classical Feistel schemes (since here ξ is always 2).

Other schemes

We can also get similar connections for generic Benes schemes, Misty L schemes, unbalanced Feistel schemes, Feistel schemes with internal bijections (instead of internal functions) etc.

7 Conclusion

In this paper we have defined the mirror systems, and given some of their properties. We also have shown many examples, some computer simulations, and the connections between these systems and some generic cryptographic constructions. It is interesting to notice how complexity and order quickly appears even on very small examples. This area of research is still in progress. The fact that we have often an equivalence between the security of some generic cryptographic schemes and the property "Tame" or not of the related system is a strong motivation to study the property of these systems.

Acknowledgement I would like to give many thanks to an anonymous referee of AAECC. Thanks to his/her remarks, I was able to improve this paper on many points.