Discrete Mathematics Applied to Symmetric Cryptography

Yann Rotella, Anne Canteaut supervisor,
Inria project-team SECRET
yann.rotella@inria.fr

September 2, 2018

Abstract

In this thesis, we study the security of symmetric cryptographic primitives. These systems are based on transformations relying on mathematical objects that can be represented in multiple ways. We then exploit different induced structures to highlight new vulnerabilities. By exploiting various representations, we cryptanalyzed some schemes submitted to the CAESAR competition, and also some dedicated and generic stream ciphers. We exhibited design criteria for lightweight block ciphers in view of the NIST standardization process and in the case of stream ciphers we defined new cryptographic criteria more relevant than the usual ones. This work led to publications in conferences and journals of reference in cryptography (CRYPTO, FSE, IACR TOSC, ASIACRYPT).

Introduction

Cryptography. One of the main goals of cryptography is to allow, thanks to an encryption method, two entities to be able to communicate confidentially on an unsecured communication channel. It is well known - since Shannon's work [Sha49] that inconditional security requires sharing a secret size as long as the message to be exchanged. Hence, perfect encryption systems are therefore unusable in practice. The security of the algorithms we use is then empirical in the sense that it is determined by the cost of the best algorithm to "break" the system. Continuous and extensive cryptanalysis work is therefore essential to determine the level of security of existing algorithms and to identify design criteria to ensure that new ciphers are structurally resistant to known attacks.

There exist two different types of cryptography: symmetric and asymmetric. In symmetric contexts, both users share beforehand a common secret (the key) and they want to communicate without anyone who intercepts the communication can decrypt a message that would not be intended. In asymmetric contexts, each has its own secret key (and a public key associated with it), and anyone can encrypt a message with the public key, but only the holder of the secret key can decrypt the message. The security of asymmetric cryptography relies on algorithmic problems that are supposed to be hard to solve, unlike symmetric ciphers where security is essentially based on cryptanalysis. On the other hand, symmetric encryption algorithms are the only ones that have acceptable performance in terms of throughput, key size, or hardware implementation complexity for most applications.

Over the past ten years, the appearance of new applications and the proliferation of connected objects have imposed new constraints on encryption algorithms, for example on energy consumption or the size of the circuit implementing the algorithm. The design of low-cost ciphers is therefore currently an important research avenue that responds to a pressing industrial demand. The work on lightweight cryptography should lead to a standardization process that will probably be initiated by the National Institute of Standards and Technology (NIST) at the end of 2018.

Problem. By definition, ciphers must be indistinguishable from a bijective application drawn at random according to the uniform distribution in the set of functions having the same parameters. It is far too expensive or impossible to implement transformations that operate on real-size data, for example, on functions operating on 128 bits. The ciphers used in practice must therefore necessarily use structured and non-random transformations to have a low cost of implementation.

However, these structures that facilitate the implementation correspond to very specific mathematical structures, which can be the source of vulnerabilities. Determining whether certain mathematical structures can be exploited in a cryptanalysis is therefore an essential problem, at the heart of symmetric cryptography. It is in this general problem that my thesis works.

In my thesis, I study the security of a vast choice of cryptosystems, both general constructions such as substitution-permutation networks and filtered registers, or specific and concretely instantiated, such as the FLIP family of stream cipher or authenticated ciphers such as KETJE and MORUS. For all these systems, I designed new attacks exploiting the properties of the mathematical objects that are used. In addition, I focused on identifying the structures that gave rise to these attacks, which allowed me to define new design criteria, more relevant than the previous ones, but also to show that several representations of the same object can imply the existence of vulnerabilities, these vulnerabilities being specific to the representation and not to the object itself.

My Publications

[AEL+18] Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, and Benoit Viguier. "Cryptanalysis of Full MORUS". In: *ASIACRYPT 2018* (2018), pp. 1–30.

[BCL+17] Christof Beierle, Anne Canteaut, Gregor Leander, and Yann Rotella. "Proving Resistance Against Invariant Attacks: How to Choose the Round Constants". In: *CRYPTO 2017, Part II*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10402. LNCS. Springer, Heidelberg, Aug. 2017, pp. 647–678.

[CDM+18] Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, and Yann Rotella. "On the Concrete Security of Goldreich's Pseudorandom Generator". In: *ASIACRYPT 2018* (2018), pp. 1–55.

[CMR17] Claude Carlet, Pierrick Méaux, and Yann Rotella. "Boolean functions with restricted input and their robustness; application to the FLIP cipher". In: *IACR Trans. Symm. Cryptol.* 2017.3 (2017), pp. 192–227. ISSN: 2519-173X.

[CR16] Anne Canteaut and Yann Rotella. "Attacks Against Filter Generators Exploiting Monomial Mappings". In: *FSE 2016*. Ed. by Thomas Peyrin. Vol. 9783. LNCS. Springer, Heidelberg, Mar. 2016, pp. 78–98.

[DLR16] Sébastien Duval, Virginie Lallemand, and Yann Rotella. "Cryptanalysis of the FLIP Family of Stream Ciphers". In: *CRYPTO 2016, Part I*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. LNCS. Springer, Heidelberg, Aug. 2016, pp. 457–475.

[FNR18] Thomas Fuhr, María Naya-Plasencia, and Yann Rotella. "State-Recovery Attacks on Modified Ketje Jr". In: *IACR Trans. Symmetric Cryptol.* 2018.1 (2018), pp. 29–56.

1 Preliminaries

Symmetric encryption algorithms are divided into two families: block ciphers and stream ciphers. Most of stream ciphers consist of adding bit-to-bit (XOR) the plaintext with a pseudo-random sequence (the keystream) generated from the secret key in order to replicate the principle of Vernam encryption (one-time pad). Block ciphers consist of encrypting message blocks of a fixed size (typically 64 or 128 bits), the different blocks are eventually chained by means of a mode of operation.

Attacks on symmetric ciphers consist in finding secret information in a faster time than the security provided by the designers. For example, this may be the key used in a block cipher or the initial state of a pseudo-random generator used in a stream cipher. The basic attack is to test all possible secret keys (exhaustive search). The goal of the cryptographer is often to design an encryption on which the best attacks are done in a time equivalent to the exhaustive search. More generally, the keystream or the permutation defined by a block cipher must be indistinguishable from random sequences or permutations.

2 Cryptanalysis of FLIP

FLIP is a family of stream cipher designed by Pierrick Méaux, Anthony Journault, François-Xavier Standaert and Claude Carlet at EUROCRYPT 2016 [MJS+16]. This cipher was designed to be used in an hybrid scenario, in order to be combine with a fully homomorphic encryption asymmetric algorithm. The aim of the authors was therefore to minimize the multiplicative depth of the circuit involving the pseudo-randomness of the generator so that it could be evaluated "homomorphically" at a reasonable cost. As we will explain it now, we proposed an attack on FLIP with Virginie Lallemand and Sébatien Duval that totally "breaks" the original version proposed by the authors [DLR16]. Indeed, the authors claimed that best attacks required at least 2^{80} (respectively 2^{128} for the second version) operations, but our attack has a cost of 2^{54} (respectively 2^{68}) operations.

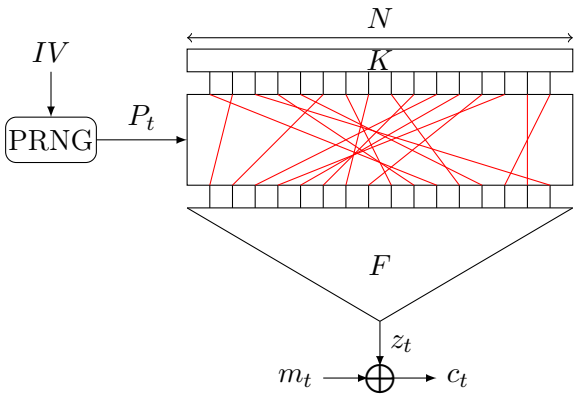

Figure 1 – General structure of the FLIP familiy of stream ciphers.

As in all pseudo-random generators, the internal state of FLIP is stored in a register, to which a non-linear function F (the filtering function) extracts at every time one bit of information from the register. However, FLIP has a very special particularity: the content of the register is fixed (and its value is the secret key) and is never updated (*cf.* figure 1). At each iteration, the bits of the register are permuted by the means of a public permutation drawn using a pseudor-random generator. A Boolean function F is then applied to the "permuted key", producing one bit of keystream. Each bit of the keystream corresponds then to $F(P_t(K))$ where P_t is a known permutation.

The filtering function F has been has been carefully chosen by the designers to satisfy all the classical cryptographic criteria: high algebraic degree, high non-linearity, immunity to correlations,... It is defined by a sum of monomials involving independent variables. Its specificity that

we are going to exploit in our attack is that, while it possesses many monomials of degree 1 and 2, it comprises only one monome of degree i, for all $3 \leq i \leq F$.

Our attack relies on a "Guess and Determine" technique where the idea is to guess few positions of the key where the value of the bits is zero. Hence, this allows us to cancel the monomials of high degree in the equations we get and eventually determine quadratic relations between keystream bits and key bits. We therefore assume at first that ℓ bits of the key have the value 0; the probability that this hypothesis is verified is noted $\mathbb{P}_{rg}$. The attacker therefore retains the equation $z_t = F(P_t(K))$ at all times t for which this equation is of degree at most 2, *i.e.* if the positions assumed to be zero initially are sent by P_t in monomials of degree greater than or equal to 3, so that they cancel each other out. The probability that a random permutation P_t provides an equation of degree 2 is denoted $\mathbb{P}_\ell$. It suffices then to solve a system of degree 2 by linearization, which requires $v_\ell \simeq N^2$ quadratic equations, so $v_\ell \mathbb{P}_\ell^{-1}$ keystream bits.

The total cost of our attack is then $v_\ell^3 \mathbb{P}_{rg}^{-1}$ in time and $v_\ell \mathbb{P}_\ell^{-1}$ in data, which gives us an attack that can be done using only 2^{54} (respectively 2^{68}) elementary operations for the recommended parameters proposed by the authors. A compromise between the time complexity and the number of keystream bits that the attacker needs is possible, by increasing the value of the number of guesses, that is ℓ. Our attack brought

Our attack caused the FLIP designers to modify their encryption in the final version of their article, by increasing the size of the key. The instance of FLIP resulting from this change for an assumed security of 80 bits (resp. 128) requires a key of 530 bit size (resp. 1394).

3 Cryptanalysis of Goldreich's PRG

Goldreich's pseudo-random generator [Gol00] (PRG) is a very famous theoretical construct, allowing to extend a source of entropy (seed) into a larger size sequence. The security is based on the absence of attack operating in polynomial time and raises the question of the existence of PRG, the output bits of which depend only on a small number of input bits. This construction has a structure similar to that of FLIP. We can therefore apply an attack similar to the one we proposed on FLIP. However, the difficulty of solving the equations does not come from their degree, but from the very small number of equations available. However, we can use the technique that allows for a compromise between data complexity and time complexity in the FLIP attack. This then leads to an attack on this PRG, with the complexity of $\mathcal{O}(2^{\sqrt{n}})$, where n is the size of the seed [CDM+18].

In addition, we use another technique that uses particular dependencies in equations to derive a much larger number of linearly independent equations in order to solve a quadratic system under certain conditions.

Combining these two techniques, we show that a minimum security level (eg 80 bits) in the Goldreich generator imposes a very large seed size (at least $10,000$ bit), which makes the use of this PRG very impractical, if not impossible.

Finally, this study severely challenges the security of Goldreich's PRG, which was based on the lack of polynomial attack, since we have proposed a sub-exponential time algorithm that is extremely powerful for "reasonable" sizes. ". Moreover, we conclude that it is impossible to construct a pseudo-random generator with a small locality, that is to say whose output depends only on few bits of the input, which refines the knowledge on this theoretical construction.

4 Analysis of filtered LFSR using monomial equivalence

Many pseudo-random generators use, for their good statistical properties, linear feedback shift registers (LFSRs), which are circuits that generate binary sequences governed by a linear recurrence relation. These LFSR are never used alone: one applies at each moment to their internal state a nonlinear Boolean function as described in the figure 2.

These filtered LFSRs are then used either directly, as in Sfinks [BLM+05], or most often as part of a more sophisticated pseudo-random generator. The analysis of their security is therefore

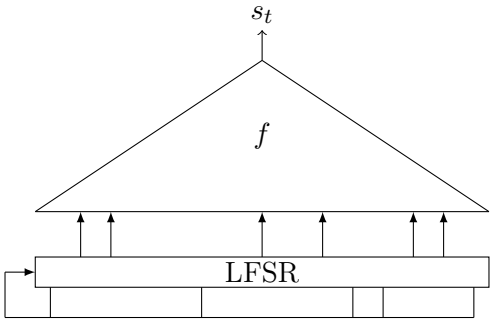

Figure 2 – Filtered register.

essential. The most effective attacks are the algebraic attacks and their variants [CM03; RH07; GRH+11] and fast correlation attacks [MS88]. Linear feedback shift registers have a strong mathematical structure: if we identify the contents of a register of n bits to an element of the finite field to 2^n elements $\mathbb{F}_{2^n}$, the transition function of an LFSR corresponds to the multiplication by a given primitive element α of the finite field.

Nonlinear equivalence. In the following, we define the nonlinear equivalence described in [RC10] as we will use it to mount an attack on filtered register. Let X_0 be the initial state of the register seen as an element of the finite field with 2^n elements. Under these conditions, the pseudo-random bit sequence produced by the LFSR filtered by the function f is defined by

$$\forall t \geq 0, s_t = f(\alpha^t X_0) \ .$$

We consider an integer k such that $\gcd(k, 2^n - 1) = 1$. The register defined by the feedback polynomial whose root is α^k, filtered by the Boolean function $g(X) = f(X^{k^{-1}})$ where k^{-1} is the inverse of $k \mod (2^n - 1)$ and initialized with $Y_0 = X_0^k$, is equivalent to the initial register filtered by f, in the sense that both generators produce exactly the same ciphering sequence, when their initial states are linked by the relation $Y_0 = X_0^k$. Thus, we can create an equivalence relation between filtered registers, which we have called monomial equivalence, and the attacker can choose to attack not the initial filtered register, but the weakest (with regard to the classical attacks) in the equivalence class.

We therefore studied the complexity of the two large classical families, algebraic attacks and correlation attacks, in order to determine how it varied within the same class of monomial equivalence [CR16].

The best known algebraic attack is to solve a linear system of size $\Lambda \times \Lambda$ where Λ is the linear complexity of the sequence, *i.e.* the size of the smallest LFSR that generates it [GRH+11]. We prove that the notion of monomial equivalence between filtered registers preserves linear complexity. In other words, the complexity of the best algebraic attacks can not be improved by the monomial equivalence.

Fast correlation attacks exploit the short distance of the filter function to a function of degree 1 [MS88]. Cryptosystem designers therefore use filtering functions with good nonlinearity, *i.e.* functions that are far from all affine functions. However, the monomial equivalence implies that the relevant criterion for analyzing the security of the filtered LFSR is not the nonlinearity of the filtering function but the generalized nonlinearity, defined as the distance from f to the set of all functions of the form $\mathsf{Tr}(\lambda X^k)$ where k is first with $2^n - 1$ and Tr is the classically defined trace application. Surprisingly, the criterion of generalized nonlinearity was introduced in 2001 by Gong and Youssef [YG01] but without any cryptographic motivation, whereas here, we prove that this quantity directly measures the resistance to a concrete attack.

Finally, Siegenthaler's classical correlation attack [Sie85] is a "divide and conquer" attack on systems using multiple LFSR. It does not generalize to filtered LFSR which has a single register

because it is not possible to find a part of the internal state independently of the rest. The main result of my work on filtered registers is to show how one can, against all odds, exploit the monomial equivalence to perform a "divide and conquer" attack in the presence of a single register.

Instead of exploiting a correlation between the target generator and a second generator defined with a primitive element α^k avec $\gcd(k, 2^n - 1) = 1$, we use the fact tha the output of our generator is correlated with the output of a generator (*cf.* figure 3) of feedback polynomial P_{α^k} where k is no longer prime to $(2^n - 1)$. Hence, the number of possible internal states of this second generator is no longer $2^n - 1$ but the multiplicative order τ_k of the element α^k.

In this situation, one can test all possible τ_k internal states of the "small" generator, since it costs less than the exhaustive search. We then find X_0^k, which provides $\log(\tau_k)$ bits of information on the initial state. We can also realize this attack with several k mutually prime, and, using the Chinese remaining theorem, find the complete initial state of the target generator. We thus succeed in breaking down in several parts the content of a single register according to the multiplicative subgroups of $\mathbb{F}_{2^n}$, in order to realize a "divide and conquer" technique.

Figure 3 – Generalized correlation attack with $\gcd(k, 2^n - 1) > 1$.

5 New security criteria for Boolean functions

In existing stream ciphers, the choice of filtering Boolean functions is governed by various security criteria which relate to their entire truth table. For example, a filter function must be balanced, *i.e.* it must produce the values 0 and 1 with the same probability when the input describes the set of words of n bits. This criterion ensures that the output of a filtered LFSR is uniformly distributed. However, this is based on the fact that the set of internal states of an LFSR is uniformly distributed. On the other hand, in FLIP, the function takes as input only permuted versions of the same word of n bits (the key). In particular, all its entries have the same Hamming weight, *i.e.* the same number of ones. Thus, the fact that the Boolean function is balanced does not guarantee that the output of the generator is uniformly distributed. For example, the 5 variable Boolean function defined by $f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 + x_4 + x_5$ is balanced on $\mathbb{F}_2^5$, but is constant when the Hamming weight is fixed as input since $f(x) = \mathsf{w}_H(x) \mod 2$ where $\mathsf{w}_H(x)$ is the Hamming weight of x.

The same goes for the other cryptographic criteria that must be modified to take into account the fact that the input of the filtering function is of constant Hamming weight. Thus, with Pierrick Méaux and Claude Carlet, we analyzed how the classical cryptographic properties of Boolean functions [CMR17] (balancedness, nonlinearity and algebraic immunity) could degrade when the input of functions is restricted to a subset, and more particularly to subsets composed of words of n bits and weight k: $S_{n,k} = \{x \in \mathbb{F}_2^n, \mathsf{w}_H(x) = k\}$.

In particular, we built families of balanced functions on each subset $S_{n,k}$. These functions only exist if all $S_{n,k}$ have an even cardinality, *i.e.* If n is a power of 2. For any number of variables, we constructed almost perfectly balanced functions in the sense that the number of 0 values and the number of 1 values taken by the function on each $E_{n,k}$ differ by at most 1.

As for balancedness, the nonlinearity of a filtering function (*i.e.* its Hamming distance to affine functions) can collapse when focusing on constant weight words. For example, we have pointed out

curved functions (which have the best possible classical nonlinearity) that are linear on the words of weight k. We found bounds on nonlinearity restricted to subsets arbitrarily taken as well as nonlinearity restricted to $S_{n,k}$.

The third important criterion to consider when designing a new cryptographic system is the algebraic immunity of the f filtering function. This is the minimal degree of a boolean function h that cancels f, *i.e.* such that $h(x)f(x) = 0$ for all $x \in \mathbb{F}_2^n$. We found bounds on algebraic immunity when the function is restricted to entries in a fixed subspace S, using Reed and Muller codes. We deduce, for example, that the algebraic immunity of the restriction of f to $S_{n,k}$ is at least equal to the smallest integer e which satisfies $2\binom{n}{e} > \binom{n}{k}$.

More generally, this study has shown that conventional security criteria are absolutely irrelevant in the context of FLIP and that they must be replaced by other properties. In particular, we have built several families of appropriate filtering functions that provide an excellent level of security in this type of situation.

6 Invariant attacks on block ciphers

The previously mentioned works exploit mathematical structures in the components of some stream ciphers. Another part of my thesis deals with the second large family of symmetric ciphers: block ciphers.

Many lightweight block ciphers have been proposed in recent years and most of them follow an iterative construction: they iterate a relatively simple permutation, inserting after each iteration a secret quantity, called subkey, derived from the master key of the algorithm as described in the figure 4.

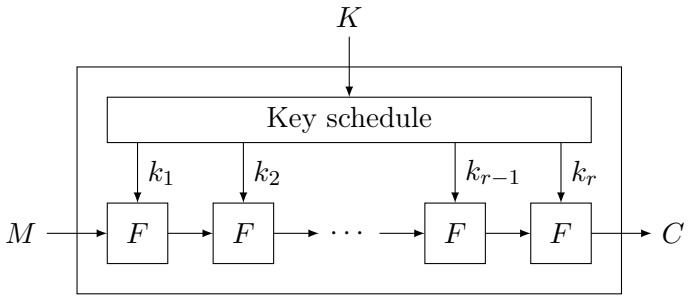

Figure 4 – Bock cipher scheme E_K using iterative construction.

One of the specificities of lightweight algorithms is to derive each round key by adding the master key to a constant. This simplicity in the calculation of subkeys, however, opened the way to new attacks, including invariant attacks [LAA+11] and their generalization [TLS16].

The principle of these attacks is to find a subset of the encryption entries, $\mathcal{S} \subset \mathbb{F}_2^n$, such that the partition of the entries in $(\mathcal{S}, \mathbb{F}_2^n \backslash \mathcal{S})$ is preserved, *i.e.*

$$E_K(\mathcal{S}) = \mathcal{S} \text{or} E_K(\mathcal{S}) = \mathbb{F}_2^n \backslash \mathcal{S}$$

The keys K checking this property are called weak keys. The special case where $\mathcal{S}$ is a vectorial subspace corresponds to the invariant subspace attack [LAA+11]. If the subset is an invariant subset of the nonlinear part and the linear part of the iterated function, and invariant by the addition of each key of a round, then it will be invariant for the block cipher.

The work I conducted with Anne Canteaut and Christof Beierle and Gregor Leander from the University of Bochum (Germany) [BCL+17] on the subject allowed me to characterize the mathematical properties of the linear part of the iterated function and round constants that prevent this attack. We have shown that the existence of an invariant attack is closely related to the dimension of the space $W_L(c_1, \ldots, c_t)$ defined as the smallest invariant vector space by L which

contains all differences $c_1, \ldots, c_t$ between the round constants. In particular, if this space covers $\mathbb{F}_2^n$, then we can conclude to the absence of invariant, a conclusion that we were able to reach for a large number of block ciphers.

If we take the point of view of the designer, we try to build a non-invariant cipher and thus find a function L and elements $c_1, \ldots, c_t$ (corresponding to the differences between the round constants) that maximize the dimension of $W_L(c_1, \ldots, c_t)$. We have shown that this dimension is conditioned by the rational canonical form of the matrix representing L where L is the linear layer of the iterated function. Indeed, for any linear function L of $\mathbb{F}_2^n$, there exists a basis of $\mathbb{F}_2^n$ in which L has the following form:

$$\begin{pmatrix} C(Q_r) & & & \\ & C(Q_{r-1}) & & \\ & & \ddots & \\ & & & C(Q_1) \end{pmatrix}$$

where the $C(Q_i)$ are companion matrices of polynomial Q_i, with $Q_r \mid Q_{r-1} \mid \cdots \mid Q_1$ and Q_1 the minimal polynomial of L. The Q_i polynomials are called invariant factors of L. We have indeed proved that the largest dimension reachable for $W_L(c_1, \ldots, c_t)$, with $(t+1)$ round constants equals the sum of the degrees of the first t invariant factors of L:

$$\max_{c_1,\ldots,c_t \in \mathbb{F}_2^n} \dim W_L(c_1, \ldots, c_t) = \sum_{i=1}^{t} \deg Q_i \ .$$

It follows that the degree of the minimal polynomial of the linear function L and the number of invariant factors are essential parameters for security when the subkeys are obtained by adding the master key with a round constant. This is the first time that this mathematical property of the linear function appears in a security analysis: our work is therefore at the origin of a new criterion now used for all new lightweight block ciphers.

7 Cryptanalysis of authenticated ciphers

The interest in authenticated encryption (which ensures the authenticity of messages) has grown in the cryptographic community in recent years, resulting in the CAESAR competition, which aims to select the best authenticated encryption algorithms proposed by the the entire international cryptographic community and is supposed to end with the announcement of the winners at the end of the year.

KETJE [BDP+14] is an authenticated cipher proposed by the authors of the hash function standard SHA-3 [BDP+13] and inspired by this specific construction. Without going into details, KETJE follows an iterative construction called "sponge" that absorbs some of the plaintext and produces some of the ciphertext at each round. For a secret internal state of 200 bits, we have access to a part of the information about this state after each application of the round function. The attack consists in recovering the information coming from the internal state at different times and combining this information in an elegant way so the complete value of the state at a given instant is deduced. In the case of KETJE, we first succeed in exploiting information on two consecutive rounds and in a second step, we use non-trivial techniques of merging lists algorithms, by seeving with non-linear equations to exploit information on 3 consecutive rounds.

Our cryptanalysis [FNR18] applies to a weakened version of KETJE in which the *rate* (critical parameter of the sponge construction) is increased (32 or 40 bits instead of 16). If it does not contradict the security claimed by the designers, our attack sheds new light on KETJE because it highlights a weakness not yet exploited, resulting from the possibility of obtaining sparse equations.

MORUS [WH14] is also an authenticated cipher and is a finalist in the CAESAR competition. We have described a distinction on the single ciphertexts produced by this [AEL+18] encryption

algorithm. Specifically, we have found a linear combination of ciphers that admits a bias of 2^{-76}, independently of the key, which is an attack in a multi-user model.

8 Conclusion and perspectives

All of my work shows that a structural vision of mathematical objects involved in cryptographic systems can have a significant contribution to cryptanalysis. This vision allows to discover new attacks and to highlight new design criteria. It is therefore necessary to go back and forth between the design of ciphers, the cryptanalysis and the fundamental mathematical concepts used in the attacks to precisely determine the level of practical security of the encryption algorithms.

In particular, the various studies conducted during my thesis highlight the fragility of systems using mathematical objects with a very structured representation. For example, we attacked pseudo-random generators such as FLIP or Goldreich's PRG by taking advantage of spars multivariate equations, while our attacks on filtered LFSR exploit the sparsity of the univariate representation of the polynomial employed. The multivariate representation looks at the input space as a vector space, while the univariate representation identifies it as a finite field. These representations are naturally linked, but the equations can be sparse in one case, and dense in the other, which shows that the two approaches do not capture the same phenomenon. This multiplicity of possible representations opens up a vast potential for research. For example, one may question the relevance of any intermediate representations based on subfields of $\mathbb{F}_2^n$, for example the use of bivariate polynomials with coefficients in $\mathbb{F}_2^{n/2}$ when n is even, rather than univariate polynomials with coefficients in $\mathbb{F}_2^n$.

Moreover, the link between the different representations of Boolean functions is not well understood and is a difficult subject, especially since the cardinality of sets (the number of Boolean functions at n variables is 2^{2^n}) forbids any exhaustive search beyond 6 variables.

Références

[BDP+13] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. "Keccak". In: *EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. LNCS. Springer, Heidelberg, May 2013, pp. 313–314.

[BDP+14] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. "Ketje v1". In: *Soumission à la compétition CAESAR* (2014).

[BLM+05] A. Braeken, J. Lano, N. Mentens, B. Preneel, and I. Verbauwhede. *SFINKS: a synchronous stream cipher for restricted hardware environments*. Soumission au projet eSTREAM. `http://www.ecrypt.eu.org/stream/`. 2005.

[CM03] Nicolas Courtois and Willi Meier. "Algebraic Attacks on Stream Ciphers with Linear Feedback". In: *EUROCRYPT 2003*. Ed. by Eli Biham. Vol. 2656. LNCS. Springer, Heidelberg, May 2003, pp. 345–359.

[Gol00] Oded Goldreich. *Candidate One-Way Functions Based on Expander Graphs*. Cryptology ePrint Archive, Report 2000/063. `http://eprint.iacr.org/2000/063`. 2000.

[GRH+11] Guang Gong, Sondre Rønjom, Tor Helleseth, and Honggang Hu. "Fast Discrete Fourier Spectra Attacks on Stream Ciphers". In: *IEEE Trans. Information Theory* 57.8 (2011), pp. 5555–5565.

[LAA+11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. "A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack". In: *CRYPTO 2011*. Ed. by Phillip Rogaway. Vol. 6841. LNCS. Springer, Heidelberg, Aug. 2011, pp. 206–221.

[MJS+16] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. "Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts". In: *EUROCRYPT 2016, Part I*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9665. LNCS. Springer, Heidelberg, May 2016, pp. 311–343.

[MS88] Willi Meier and Othmar Staffelbach. "Fast Correlation Attacks on Stream Ciphers (Extended Abstract)". In: *EUROCRYPT'88*. Ed. by C. G. Günther. Vol. 330. LNCS. Springer, Heidelberg, May 1988, pp. 301–314.

[RC10] Sondre Rønjom and Carlos Cid. "Nonlinear Equivalence of Stream Ciphers". In: *FSE 2010*. Ed. by Seokhie Hong and Tetsu Iwata. Vol. 6147. LNCS. Springer, Heidelberg, Feb. 2010, pp. 40–54.

[RH07] Sondre Rønjom and Tor Helleseth. "A New Attack on the Filter Generator". In: *IEEE Trans. Information Theory* 53.5 (2007), pp. 1752–1758.

[Sha49] C. Shannon. "Communication Theory of Secrecy Systems". In: *Bell System Technical Journal, Vol 28, pp. 656715* (1949).

[Sie85] Thomas Siegenthaler. "Decrypting a class of stream ciphers using ciphertext only". In: *IEEE Trans. Computers* C-34.1 (1985), pp. 81–84.

[TLS16] Yosuke Todo, Gregor Leander, and Yu Sasaki. "Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64". In: *ASIACRYPT 2016, Part II*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10032. LNCS. Springer, Heidelberg, Dec. 2016, pp. 3–33.

[WH14] Hongjun Wu and Tao Huang. "MORUS". In: *Soumission à la compétition CAESAR* (2014).

[YG01] Amr M. Youssef and Guang Gong. "Hyper-bent Functions". In: *EUROCRYPT 2001*. Ed. by Birgit Pfitzmann. Vol. 2045. LNCS. Springer, Heidelberg, May 2001, pp. 406–419.