On the Expansion Complexity of Sequences over Finite Fields

Domingo Gómez-Pérez, László Mérai, Harald Niederreiter

Abstract—In 2012, Diem introduced a new figure of merit for cryptographic sequences called expansion complexity. In this paper, we slightly modify this notion to obtain the so-called irreducible-expansion complexity which is more suitable for certain applications. We analyze both, the classical and the modified expansion complexity. Moreover, we also study the expansion complexity of the explicit inversive congruential generator.

Index Terms—pseudorandom sequence, expansion complexity, inversive generator

I. INTRODUCTION

Sequences over finite fields which are generated by a short linear recurrence relation are considered cryptographically weak. This observation leads to the notion of *linear complexity profile* of sequences, which is an infinite sequence of nondecreasing integers such that the Nth term is the length of a shortest linear recurrence relation which generates the first N elements of the sequence. The linear complexity profile is a measure for the unpredictability of a sequence and thus its suitability in cryptography. A sequence with small Nth linear complexity (for a sufficiently large N) is disastrous for cryptographic applications. We recommend the interested reader to consult the survey of Meidl and Winterhof [5] and previous articles by Niederreiter [7] and Winterhof [8].

Xing and Lam [9] gave a general construction of infinite sequences over finite fields with optimal linear complexity. The construction is based on functional expansion into expansion series. Diem [4] showed that this type of sequence can be efficiently computed from a relatively short subsequence. This observation leads to the *expansion complexity*. For the connection between the linear and expansion complexity we refer to the recent paper [6].

In this paper we study the properties of this figure of merit for sequences over finite fields. In Section II we slightly modify the notion of expansion complexity to obtain the so-called i(rreducible)-expansion complexity which is more suitable for certain applications. We analyze the properties of both the classical and the modified expansion complexity.

Then we study the expansion complexity of the explicit inversive congruential generator in Section III. We prove that this sequence has optimal expansion complexity and we give a lower bound on the expansion complexity if the sequence is randomly shifted. We finish the paper with a summary of the results in Section IV.

II. EXPANSION SEQUENCES AND EXPANSION COMPLEXITY

For a sequence $\mathcal{S} = (s_i)_{i=0}^{\infty}$ over the finite field $\mathbb{F}_q$ of q elements, we define the *generating function* $G(x)$ of $\mathcal{S}$ by

$$G(x) = \sum_{i=0}^{\infty} s_i x^i,$$

viewed as a formal power series over $\mathbb{F}_q$.

A sequence $\mathcal{S}$ is called an *expansion sequence* if its generating function satisfies an algebraic equation

$$h(x, G(x)) = 0 \tag{1}$$

for some nonzero $h(x, y) \in \mathbb{F}_q[x, y]$. Clearly, the polynomials $h(x, y) \in \mathbb{F}_q[x, y]$ satisfying (1) form an ideal in $\mathbb{F}_q[x, y]$. This ideal is called the *defining ideal* and it is a principal ideal generated by an irreducible polynomial, see [4, Proposition 4].

An expansion sequence can be efficiently computed from a relatively short subsequence via the generating polynomial of its defining ideal [4, Section 5].

Proposition 1. *Let $\mathcal{S}$ be an expansion sequence and let $h(x, y)$ be the generating polynomial of its defining ideal. The sequence $\mathcal{S}$ is uniquely determined by $h(x, y)$ and its initial sequence of length $(\deg h)^2$. Moreover, $h(x, y)$ can be computed in polynomial time (in $\log q \cdot \deg h$) from an initial sequence of length $(\deg h)^2$.*

Based on Proposition 1, Diem [4] defined the Nth expansion complexity in the following way. For a positive integer N, the *Nth expansion complexity* $E_N = E_N(\mathcal{S})$ is $E_N = 0$ if $s_0 = \ldots = s_{N-1} = 0$ and otherwise the least total degree of a nonzero polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ with

$$h(x, G(x)) \equiv 0 \mod x^N. \tag{2}$$

Note that E_N depends only on the first N terms of $\mathcal{S}$. However, small expansion complexity does not imply high predictability in the sense of Proposition 1.

Example 1. Let $\mathcal{S}$ be a sequence over the finite field $\mathbb{F}_p$ ($p \geq 3$) with initial segment $\mathcal{S} = 000001\ldots$ and generating function $G(x) \equiv x^5 \mod x^6$. Then its 6th expansion complexity is $E_6(\mathcal{S}) = 2$ realized by the polynomial $h(x, y) = x \cdot y$.

However, the first 4 elements do not determine the whole initial segment with length 6.

In order to achieve the predictability of sequences in terms of Proposition 1, one needs to require that the polynomial $h(x, y)$ satisfying (2) is *irreducible*. This observation leads to the *i(rreducible)-expansion complexity* of a sequence. Accordingly, for a positive integer N, the Nth *i-expansion complexity* $E_N^* = E_N^*(\mathcal{S})$ is $E_N^* = 0$ if $s_0 = \ldots = s_{N-1} = 0$ and otherwise the least total degree of an irreducible polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ with (2).

Example 2. Let $\mathcal{S}$ be the sequence in Example 1. Then its 6th i-expansion complexity is $E_6^*(\mathcal{S}) = 5$ realized by the polynomial $h(x, y) = y - x^5$.

Clearly, for any sequence $\mathcal{S}$ we have

$$E_N^*(\mathcal{S}) \leq E_{N+1}^*(\mathcal{S})$$

and

$$E_N(\mathcal{S}) \leq E_N^*(\mathcal{S}) \leq \max\{1, N-1\}. \tag{3}$$

The second inequality immediately gives a bound on the expansion complexity. In the following theorem we give a stronger bound.

Theorem 1. *For any sequence $\mathcal{S}$, the expansion complexity $E_N(\mathcal{S})$ satisfies the following inequality:*

$$\binom{E_N(\mathcal{S}) + 1}{2} \leq N. \tag{4}$$

Proof:
With an integer d, consider the set of monomials

$$M(d) = \{x^i y^j | i + j \leq d\}$$

of size $\#M(d) = \binom{d+2}{2}$. For each monomial in that set, $x^i y^j \in M(d)$, we substitute $y = G(x)$ and reduce it modulo x^N to obtain a polynomial of degree at most $N-1$. The set of all polynomials of degree less than N is a vector space over $\mathbb{F}_q$ of dimension N. Each of the evaluations of the monomials in $M(d)$ gives a polynomial in that space and there are $\binom{d+2}{2}$ of these monomials, which means that they are linearly dependent if there are more than N. Now we put $d = E_N(\mathcal{S}) - 1$. If (4) were not satisfied, then the argument just presented leads to a contradiction. ∎

It follows from (4) that $E_N(\mathcal{S}) \leq \sqrt{2N}$. On the other hand, for the i-expansion complexity, we have $E_N^*(\mathcal{S}) \geq \sqrt{2N}$ for almost all sequences, as will be shown in Theorem 2 below.

Let μ_q be the uniform probability measure on $\mathbb{F}_q$ which assigns the measure $1/q$ to each element of $\mathbb{F}_q$. Let $\mathbb{F}_q^\infty$ be the sequence space over $\mathbb{F}_q$ and let μ_q^∞ be the complete product probability measure on $\mathbb{F}_q^\infty$ induced by μ_q. We say that a property of sequences $\mathcal{S} \in \mathbb{F}_q^\infty$ holds μ_q^∞-*almost everywhere* if it holds for a set of sequences $\mathcal{S}$ of μ_q^∞-measure 1. We may view such a property as a typical property of a random sequence over $\mathbb{F}_q$.

Theorem 2. *We have*

$$\liminf_{N \to \infty} \frac{E_N^*(\mathcal{S})}{\sqrt{2N}} \geq 1 \qquad \mu_q^\infty\text{-almost everywhere.}$$

We remark, that Theorem 2 is the corrected form of [6, Theorem 4].

Proof:
First we fix ε with $0 < \varepsilon < 1$ and we put

$$b_N = \lfloor (1-\varepsilon)\sqrt{2N} \rfloor \qquad \text{for } N = 1, 2, \ldots.$$

Then $b_N \geq 1$ for all sufficiently large N. For such N put

$$A_N = \{\mathcal{S} \in \mathbb{F}_q^\infty : E_N^*(\mathcal{S}) \leq b_N\}.$$

Since $E_N^*(\mathcal{S})$ depends only on the first N terms of $\mathcal{S}$, the measure $\mu_q^\infty(A_N)$ is given by

$$\mu_q^\infty(A_N) = q^{-N} \cdot \#\{\mathcal{S} \in \mathbb{F}_q^N : E_N^*(\mathcal{S}) \leq b_N\}. \tag{5}$$

An irreducible polynomial with degree d can define at most d expansion sequences (see [4, p. 332]). Moreover, if two irreducible polynomials are constant multiples of each other, they define the same sequences.

Let a polynomial $f(x, y)$ of degree d be called *normalized* if in the coefficient vector $(a_0, a_1, \ldots, a_d)$ of the homogeneous part with degree d of f, i.e.,

$$a_0 x^d + a_1 x^{d-1} y + \cdots + a_d y^d,$$

the first nonzero element is 1.

Let $I_2(d)$ be the number of *normalized* irreducible polynomials (with two variables) in $\mathbb{F}_q[x, y]$ of total degree d. Then by [2] (see equation (11) there) we have

$$I_2(d) = \frac{1}{q-1} q^{\binom{d+2}{2}} + O\left(q^{\binom{d+1}{2}}\right).$$

Thus

$$\{\mathcal{S} \in \mathbb{F}_q^N : E_N^*(\mathcal{S}) \leq b_N\} \leq \sum_{d=1}^{b_N} d \cdot I_2(d) \ll \sum_{d=1}^{b_N} d \cdot q^{\binom{d+2}{2}-1}$$

$$\ll b_N^2 q^{\binom{b_N+2}{2}-1}. \tag{6}$$

Thus it follows from (5) and (6) that $\mu_q^\infty(A_N) \leq q^{-\delta N}$ for some positive δ and for all sufficiently large N. Therefore $\sum_{N=1}^\infty \mu_q^\infty(A_N) < \infty$. Then the Borel-Cantelli lemma (see [1, Lemma 3.14]) shows that the set of all $\mathcal{S} \in \mathbb{F}_q^\infty$ for which $\mathcal{S} \in A_N$ for infinitely many N has μ_q^∞-measure 0. In other words, μ_q^∞-almost everywhere we have $\mathcal{S} \in A_N$ for at most finitely many N. It follows then from the definition of A_N that μ_q^∞-almost everywhere we have

$$E_N^*(\mathcal{S}) > b_N > (1-\varepsilon)\sqrt{2N} - 1$$

for all sufficiently large N. Therefore μ_q^∞-almost everywhere,

$$\liminf_{N \to \infty} \frac{E_N^*(\mathcal{S})}{\sqrt{2N}} \geq 1 - \varepsilon.$$

By applying this for $\varepsilon = 1/r$ with $r = 1, 2, \ldots$ and noting that the intersection of countably many sets of μ_q^∞-measure 1 has again μ_q^∞-measure 1, we obtain the result of the theorem. ∎

We finish this section showing that, for sequences having maximal expansion complexity, we have $E_N^*(\mathcal{S}) = E_N(\mathcal{S})$.

Theorem 3. *If the sequence $\mathcal{S}$ has maximal expansion complexity, i.e. if for $d \geq 1$, we have*

$$E_N(\mathcal{S}) = d \quad \text{whenever} \quad \binom{d+1}{2} \leq N < \binom{d+2}{2},$$

then

$$E_N^*(\mathcal{S}) = d' \quad \text{whenever} \quad \binom{d'+1}{2} + 2 \leq N < \binom{d'+2}{2},$$

for $d' \geq 6$.

Proof:

Let $d \geq 6$ and assume that $\binom{d+1}{2} + 2 \leq N$. We will show that if a polynomial $h(x, y)$ satisfies the congruence (2) with total degree equal to $d = E_N(\mathcal{S})$, then it must be irreducible. We proceed proving the result by assuming the opposite, that is $h(x, y) = h_1(x, y) h_2(x, y)$ and $d_1 = \deg h_1(x, y)$ and $d_2 = \deg h_2(x, y)$ positive. Then $h(x, y)$ satisfies (2) if and only if for nonnegative integers N_1, N_2 with $N = N_1 + N_2$,

$$h_1(x, G(x)) \equiv 0 \mod x^{N_1}, \quad h_2(x, G(x)) \equiv 0 \mod x^{N_2}.$$

Without loss of generality, we may suppose that N_1 and N_2 are positive integers. We also suppose that $E_{N_1}(\mathcal{S}) = d_1$ and $E_{N_2}(\mathcal{S}) = d_2$. Applying Theorem 1, we obtain

$$\binom{d_1 + d_2 + 1}{2} \leq N_1 + N_2 < \binom{d_1 + 2}{2} + \binom{d_2 + 2}{2}.$$

This implies by simple manipulation that

$$(d_1 - 1)(d_2 - 1) \leq 2.$$

If the last inequality holds, then either $d_1 = 1$, or $d_2 = 1$ by the assumption $d_1 + d_2 = d \geq 6$. If $d_1 = 1$, then $N_1 \leq 2$ and, applying again Theorem 1, implies

$$\binom{d_2 + 2}{2} - 2 \leq N_2 < \binom{d_2 + 2}{2}$$

i.e.

$$\binom{d+1}{2} \leq N < \binom{d+1}{2} + 2,$$

a contradiction. We proceed similarly in the case $d_2 = 1$. ∎

Remark 4. For a sequence $\mathcal{S}$ over $\mathbb{F}_q$, we have $E_N(\mathcal{S}) = O(1)$ if and only if $\mathcal{S}$ is a q-automatic sequence, i.e., $\mathcal{S}$ can be generated by a finite automaton over an alphabet of size q. First of all, since there are only finitely many polynomials over $\mathbb{F}_q[x, y]$ of a fixed total degree, it follows from $E_N(\mathcal{S}) = O(1)$ that there exists a nonzero polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ for which (2) holds for infinitely many N. This implies that $h(x, G(x)) = 0$, and so the generating function $G(x)$ of $\mathcal{S}$ is an algebraic function over $\mathbb{F}_q$. Then [3, Théorème 1] shows that $\mathcal{S}$ is a q-automatic sequence. Conversely, if $\mathcal{S}$ is a q-automatic sequence, then by the same criterion $G(x)$ is an algebraic function over $\mathbb{F}_q$, and so $E_N(\mathcal{S}) = O(1)$. The same remark applies to the i-expansion complexity.

III. Expansion Complexity of the Explicit Inversive Congruential Generator

The *explicit inversive congruential generator* is defined in a prime field $\mathbb{F}_p$ $(p \geq 3)$ by

$$s_n = n^{p-2} \mod p \quad \text{for } n = 0, 1 \ldots. \tag{7}$$

Clearly, this is a purely periodic sequence with least period length p. We show that its expansion complexity is maximal in terms of Theorem 1.

Theorem 5. *The explicit inversive generator $\mathcal{S} = (s_n)$ defined in (7) has maximal expansion complexity for all $N = 2, \ldots, p - 1$, i.e. we have*

$$E_N(\mathcal{S}) = d \quad \text{whenever} \quad \binom{d+1}{2} \leq N < \binom{d+2}{2}. \tag{8}$$

By (3) and Theorem 3, this result gives a lower bound for $E_N^*(\mathcal{S})$ for $N \leq p - 1$ which is in line with the asymptotic regime in Theorem 2.

Proof:

By Theorem 1, we have $E_N(\mathcal{S}) \leq d$ if N is in the range (8). Thus it suffices to prove the lower bound $E_N(\mathcal{S}) \geq d$ for such N. As the Nth expansion complexity $E_N(\mathcal{S})$ is a nondecreasing function of N, it is enough to prove the result for integers N having the form $N = \binom{d+1}{2}$ with some positive integer d.

We remark that the derivative $G'(x)$ of the generating function $G(x)$ of $\mathcal{S}$ satisfies

$$G'(x) = \left(\sum_{n=0}^{\infty} n^{p-2} x^n \right)' = \sum_{\substack{0 \leq n < \infty \\ p \nmid n+1}} x^n$$

$$= \frac{1}{1-x} - x^{p-1} \frac{1}{1 - x^p}. \tag{9}$$

Now we prove the theorem by induction on d. For $d = 2$ ($N = 3$) the assertion follows from straightforward computation. Next, we prove the theorem by contradiction. Assume that there is a $d > 2$ that does not satisfy the assertion. Let d be the smallest such integer. Then $E_{N-d}(\mathcal{S}) = \ldots = E_N(\mathcal{S}) = d - 1$ with $N = \binom{d+1}{2}$.

By recursion, we construct nonzero polynomials $f_i(x, y) \in \mathbb{F}_p[x, y]$ $(i = 0, 1 \ldots, d - 1)$ of total degree $d - 1$ such that

$$f_i(x, G(x)) \equiv 0 \mod x^{N-i} \tag{10}$$

and

$f_i(x, y)$ does not contain the terms $x^{d-1-\ell} y^\ell$, $0 \leq \ell < i$. (11)

By assumption $E_N(\mathcal{S}) = d - 1$, thus there is a nonzero polynomial $f(x, y) \in \mathbb{F}_p[x, y]$ of total degree $d - 1$ such that

$$f(x, G(x)) \equiv 0 \mod x^N. \tag{12}$$

Put $f_0(x, y) = f(x, y)$. Now suppose that $f_i(x, y)$ has been constructed for some $0 \leq i \leq d - 2$. To construct the polynomial $f_{i+1}(x, y)$, we take the derivative of (10) with respect to x:

$$\frac{\partial f_i}{\partial x}(x, G(x)) + \frac{\partial f_i}{\partial y}(x, G(x)) G'(x) \equiv 0 \mod x^{N-i-1}. \tag{13}$$

As

$$G'(x) \equiv \frac{1}{1-x} \quad \mod x^{p-1}$$

by (9), we obtain

$$(1-x)\left(\frac{\partial f_i}{\partial x}(x, G(x)) + \frac{\partial f_i}{\partial y}(x, G(x))G'(x)\right) \equiv$$
$$(1-x)\frac{\partial f_i}{\partial x}(x, G(x)) + \frac{\partial f_i}{\partial y}(x, G(x)) \equiv 0 \mod x^{N-i-1}.$$

Put

$$g_i(x, y) = (1-x)\frac{\partial f_i}{\partial x}(x, y) + \frac{\partial f_i}{\partial y}(x, y) \in \mathbb{F}_p[x, y].$$

Observe, that $g_i(x, y)$ and $f_i(x, y)$ have the same total degree. Indeed, if the total degree of $g_i(x, y)$ were strictly less than the total degree of $f_i(x, y)$, then we get a polynomial of total degree at most $d-2$ satisfying (10) (with i replaced by $i+1$), hence $E_{N-i-1}(\mathcal{S}) \leq d-2$, a contradiction. Moreover, the monomials of degree $d-1$ that appear in $g_i(x, y)$ must involve x and appear in $f_i(x, y)$. If $f_i(x, y) = cg_i(x, y)$ for some nonzero $c \in \mathbb{F}_p$, then

$$f_i(x, y) \equiv c^\ell \frac{\partial^\ell f_i}{\partial^\ell y}(x, y) \quad \mod 1-x \quad \text{for all } \ell \geq 0.$$

In particular, $(1-x)$ divides $f_i(x, y)$, so taking $f_i(x, y)/(1-x)$, we get a polynomial with total degree $d-2$ satisfying (10), thus $E_{N-i}(\mathcal{S}) \leq d-2$, a contradiction.

So, there must exist a nonzero linear combination $f_{i+1}(x, y)$ of $f_i(x, y)$ and $g_i(x, y)$ satisfying (10) (with i replaced by $i+1$) and (11). If the total degree of $f_{i+1}(x, y)$ were less than or equal to $d-2$, then $E_{N-i-1}(\mathcal{S}) \leq d-2$, a contradiction.

Finally, observe that if we construct $g_{d-1}(x, y)$ as above, then it does not contain the terms $x^{d-1-\ell}y^\ell$, $\ell = 0, \ldots d-2$, by construction, and also that it does not contain the term y^{d-1}. Thus, the total degree of $g_{d-1}(x, y)$ is at most $d-2$. Moreover, it follows from (10) for $i = d-1$, by the same argument as above, that

$$g_{d-1}(x, G(x)) \equiv 0 \mod x^{N-d},$$

thus $E_{N-d}(\mathcal{S}) \leq d-2$, a contradiction. ∎

As a corollary, we obtain, for many different shifts of the explicit inversive generator, a good lower bound on the expansion complexity.

Corollary 2. *For any $d > 0$ and all values of $1 \leq m < p$ but for $(d-1)^2 \cdot \binom{d}{2}$ choices, the shifted explicit inversive generator $\mathcal{S}' = (s_{n+m})$ satisfies,*

$$E_N(\mathcal{S}') = d \quad if \quad \binom{d+1}{2} \leq N < \min\left\{\binom{d+2}{2}, p\right\}.$$

Proof:

We fix the value $N = \binom{d+1}{2}$ and take again the set of monomials

$$M(d-1) = \{x^i y^j | i+j \leq d-1\}.$$

Then we define the polynomial $G(x, m) = \sum_{i=0}^{p-1} (i+m)^{p-2} x^i$ in the variables m and x. For each monomial in $M(d)$, we can substitute $y = G(x, m)$ and reduce it modulo x^N to obtain a polynomial of degree at most $N-1$ in the variable x. The set of all polynomials of degree in the variable x less than N is a vector space over the field of rational functions in the variable m of dimension N. Each of the evaluations of the monomials gives a polynomial in that space, which can be seen as a vector of length N.

All of the vectors can be written as rows of a matrix and $E_N(\mathcal{S}') = d$ if and only if the determinant of this matrix is different from 0. Multiply all the elements of this matrix by $\prod_{i=0}^{d-1}(m+i)^{d-1}$ and reduce them using that $(m+i)^p = (m+i)$, so the result is a matrix whose entries are polynomials in the variable m and of degree less than $(d-1)^2$. The determinant is a polynomial of degree at most $(d-1)^2 \cdot \#M(d-1)$, which is not the zero polynomial because the determinant is different from zero for $m = 0$. The number of roots of the determinant is at most $(d-1)^2 \cdot \#M(d-1)$, and this remark finishes the proof. ∎

IV. CONCLUSIONS

In this paper, we have studied the expansion complexity and a slight modification of this measure called i-expansion complexity. For the expansion complexity, we have found an upper bound which answers positively to a conjecture posed by Mérai, Niederreiter, and Winterhof [6].

Regarding the i-expansion complexity, Theorem 2 shows that its behavior is different and it is expected that the i-expansion is a stronger measure than the expansion complexity. However, if the expansion complexity of the sequence is maximal, then by Theorem 3, the i-expansion complexity is essentially equal to the expansion complexity.

For the explicit inversive generator, we have shown that the expansion complexity and the i-expansion complexity are maximal. Even if the sequence is shifted randomly, it is expected that the expansion complexity is quite large.

REFERENCES

[1] L. Breiman, *Probability*. SIAM, PA: Philadelphia, 1992.
[2] L. Carlitz, "The distribution of irreducible polynomials in several indeterminates," *Illinois J. Math.* vol. 7 pp. 371–375. 1963.
[3] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, "Suites algèbriques, automates et substitutions," *Bull. Soc. Math. France* vol. 108, pp. 401 – 419, 1980.
[4] C. Diem, "On the use of expansion series for stream ciphers," *LMS J. Comput. Math.*, vol. 15, pp. 326–340, 2012.
[5] W. Meidl, A. Winterhof, "Linear complexity of sequences and multisequences," in: *Handbook of finite fields,*, G.L. Mullen, D. Panario, Ed. CRC Press, FL: Boca Raton, 2013, pp. 324–336.
[6] L. Mérai, H. Niederreiter, A. Winterhof, "Expansion complexity and linear complexity of sequences over finite fields," Cryptogr. Commun. (2016) doi: 10.1007/s12095-016-0189-2
[7] H. Niederreiter, "Linear complexity and related complexity measures for sequences," Progress in cryptology–INDOCRYPT 2003, Lecture Notes in Comput. Sci., 2904, Springer, Berlin, pp. 1–17, 2003.
[8] A. Winterhof, "Linear complexity and related complexity measures," in: Selected topics in information and coding theory, Ser. Coding Theory Cryptol., 7, World Sci. Publ., NJ: Hackensack, pp. 3–40, 2010.
[9] C. P. Xing, K.Y. Lam, "Sequences with almost perfect linear complexity profiles and curves over finite fields," *IEEE Trans. Inform. Theory* vol: 45, no. 4, pp. 1267–1270, 1999.

Domingo Gomez-Perez received his Ph.D. in Mathematics and Computer Sciences in 2006, from the University of Cantabria, Santander, Spain. He has been a visiting academic in different research centers, including the Johann Radon Institute for Computational and Applied Mathematics (RI-CAM), Macquarie University, University of New South Wales and Royal Holloway, University of London. Currently, he is associate professor in the University of Cantabria and his research interests include cryptography, sequences, finite fields and quasi-monte carlo methods.

László Mérai received the Ph.D. from Eötvös Loránd University, Budapest, Hungary in 2011. From 2009 to 2012 he held a junior researcher position at Rényi Institute of Mathematics, Budapest, Hungary. From 2012 to 2014 he was assistant professor at Eötvös Loránd University. Since 2014 he is a postdoctoral researcher at Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Linz, Austria. In 2012, he awarded the Géza Grünwald Prize of the János Bolyai Mathematical Society. His research interests include finite fields and their applications, and number theoretic questions motivated by cryptography.

Harald Niederreiter received his Ph.D. from the University of Vienna in 1969. His research interests in information theory include algebraic coding theory, cryptography and complexity of sequences. His most recent books are "Algebraic Geometry in Coding Theory and Cryptography" (Princeton University Press, 2009) with Chaoping Xing and "Applied Number Theory" (Springer, 2015) with Arne Winterhof. He is a member of the Austrian Academy of Sciences and the German Academy of Sciences.