Construction of Resilient Functions over a Finite Alphabet

Paul Camion, Anne Canteaut

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Construction of resilient functions over a finite alphabet

Paul Camion and Anne Canteaut

N° 2789

Fvrier 1996

PROGRAMME 2

ISSN 0249-6399

INRIA
ROCQUENCOURT

Construction of resilient functions over a finite alphabet

Paul Camion * and Anne Canteaut **

Programme 2 — Calcul symbolique, programmation et génie logiciel
Projet Codes

Rapport de recherche n° 2789 — Février 1996 — 12 pages

Abstract: We extend the notions of correlation-immune functions and resilient functions to functions over any finite alphabet endowed with the structure of an Abelian group. Thus we generalize the results of Gopalakrishnan and Stinson as we give an orthogonal array characterization and a Fourier transform characterization for resilient functions over any finite alphabet. This leads to a generalization of some related cryptographic objects as perfect local randomizers. It also enables us to construct new resilient functions by composition of resilient functions of smaller order.

Key-words: correlation-immune functions, resilient functions, orthogonal arrays, randomizers, cryptographic primitives

(Résumé : tsvp)

to appear in Advances in Cryptology - EUROCRYPT'96

* Centre National de la Recherche Scientifique
** Grant-holder from the DRET, also with École Nationale Supérieure de Techniques Avancées, 32 boulevard Victor, F-75015 Paris.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
Téléphone : (33 1) 39 63 55 11 – Télécopie : (33 1) 39 63 53 30

Construction de fonctions résilientes sur un alphabet fini

Résumé : Nous étendons les notions de fonctions sans corrélation et de fonctions résilientes sur un alphabet fini quelconque muni d'une structure de groupe abélien. Nous généralisons ainsi les résultats de Gopalakrishnan et Stinson en donnant une caractérisation des fonctions résilientes sur un alphabet fini en termes de tableaux orthogonaux, et en termes de transformée de Fourier. Nous en déduisons une généralisation de certains objets cryptographiques apparentés, tels les générateurs aléatoires locaux parfaits. Cela nous permet également de construire de nouvelles fonctions résilientes par composition de fonctions résilientes d'ordre inférieur.

Mots-clé : fonctions sans corrélation, fonctions résilientes, tableaux orthogonaux, générateurs aléatoires, primitives cryptographiques

1 Introduction

Resilient functions were introduced independently by Chor *et al.* [4] and Bennett, Brassard and Robert [1] and were originally applied respectively to the generation of random strings in presence of faulty processors and to key distribution especially for quantum cryptography. Several other applications afterwards emerged and the theory of resilient functions (or the equivalent combinatorial structure of orthogonal arrays) is now almost omnipresent in cryptography.

These functions are first of all used for designing running-keys for stream ciphers; in the common case, the running-key generator is composed of several linear feedback shift registers combined by a non-linear function f; f should then be a correlation-immune function in order to resist Siegenthaler's correlation attack [12]. A resilient function is usually chosen. The output digits are then uniformly distributed. In a more general view, Maurer and Massey [9] showed that an additive stream cipher can be provably-secure under the restriction that the number of plaintext digits that the enemy can obtain is limited: the running-key generator thus should be a perfect local randomizer, what is equivalent to the structure of an orthogonal array.

A second application consists in designing "conventional" cryptographic primitives, *i.e.* primitives based on a network with some gates. Such a network contains both confusion boxes for hiding any structure and diffusion boxes for merging several inputs. Schnorr and Vaudenay [11] recommend that the diffusion boxes should be functions realizing perfect diffusion in order to avoid some cryptanalysis, especially collision attacks. These functions are called multipermutations and they can be deduced from perfect local randomizers of maximal order. These objects are also used in threshold schemes for secret sharing.

In this paper we extend the notions of correlation-immune functions and resilient functions to functions over any finite alphabet endowed with an Abelian group structure. We generalize the characterizations of q-ary resilient functions given by Gopalakrishnan and Stinson [6]: we give in section 2 an orthogonal array characterization and in section 3 a characterization by means of characters (similar to a Fourier transform characterization). Section 4 applies this generalization to perfect local randomizers and it establishes the link with coding theory. These generalizations also enable us to construct new resilient functions by composition of resilient functions of smaller order. This construction can immediately be applied to the combination of linear feedback shift registers.

2 Correlation immune functions and orthogonal arrays

Let $\mathcal{F}$ denote a finite alphabet with q elements ($q \geq 2$). Let $f : \mathcal{F}^n \rightarrow \mathcal{F}^\ell$ be a function and let $\{X_1, X_2, ..., X_n\}$ be a set of random input variables assuming values from $\mathcal{F}$ with independent equiprobable distributions (*i.e.* every input vector occurs with probability $\frac{1}{q^n}$).

The function f may satisfy the following properties:

- f is *balanced* if each possible output vector occurs with equal probability $\frac{1}{q^\ell}$.

- f is *correlation-immune with respect to the subset* $T \subset \{1, 2, \ldots, n\}$ if the probability distribution of the output vector is unaltered when $\{X_i, i \in T\}$ is fixed and $\{X_i, i \notin T\}$ is a set of independent equiprobable random variables.
- f is *t-th order correlation-immune* if for every T of cardinality at most t, f is correlation-immune with respect to T.
- f is *t-resilient* if f is t-th order correlation-immune and balanced.

Correlation-immune functions are closely related to the combinatorial structures introduced by Rao as orthogonal arrays [10].

Definition 1. An orthogonal array A of size m, n constraints, strength t and index λ over the alphabet $\mathcal{F}$ (or with q levels) is an $m \times n$ array of which rows are the vectors from a subset M of $\mathcal{F}^n$ such that $|M| = m$ which has the property that in any subset of t columns of A, each of the q^t vectors of $\mathcal{F}^t$ appears exactly λ times as a row. Such an array is denoted by (m, n, q, t). Clearly $m = \lambda q^t$.

In [3] it was observed that the characterization by Xiao and Massey [15] of a t-th order correlation immune function $f : \{0,1\}^n \to \{0,1\}$ is equivalent to the following property: the array of which rows are the vectors of $f^{-1}(1)$ is an orthogonal array of strength t. In [6] K. Gopalakrishnan and D.R. Stinson show directly that $f : GF(q)^n \to GF(q)^\ell$ is t-th order correlation immune if and only if $\forall y \in GF(q)^\ell$, $f^{-1}(y)$ consists in the rows of an orthogonal array A_y of strength t.

In fact characterizing the t-th order correlation immune functions in terms of orthogonal arrays is merely translating the probability definition into an enumeration definition. Then this characterization holds for any finite alphabet $\mathcal{F}$. We sum up what is needed as follows:

Proposition 2. *If the independent equiprobable random variables $X_1, \ldots, X_n$ are defined on a finite alphabet $\mathcal{F}$, then $f(X_1, \ldots, X_n)$, which has its values in a finite set E, is a t-order correlation immune function with respect to the alphabet $\mathcal{F}$ if and only if $\forall y \in E$, $f^{-1}(y)$ consists in the rows of an orthogonal array of strength t over $\mathcal{F}$.*

Additionally, f is t-resilient if

$$\forall y, y' \in E, |f^{-1}(y)| = |f^{-1}(y')|$$

3 Characterization by means of characters

In [6] K. Gopalakrishnan and D.R. Stinson give a characterization of correlation immune functions in terms of Fourier transform when the alphabet $\mathcal{F}$ is $GF(q)$. We here give statements which are valid for any finite alphabet $\mathcal{F}$ of order q, $q \geq 2$ endowed with the structure of an Abelian group.

We know that the homomorphisms from the Abelian group $\mathcal{F}$ into the multiplicative group of $\mathbb{C}$ form an Abelian group $\mathcal{F}'$, called the characters group, which is isomorphic with $\mathcal{F}$. For $x \in \mathcal{F}$ and $y \in \mathcal{F}'$ we denote by $< x, y >$ the complex image of x under the character y.

For example if $\mathcal{F}$ is the additive group $(GF(q),+)$ of the Galois field $GF(q)$ where $q=p^s$, p a prime, then $<x,y>=\theta^{Tr_{GF(q)/GF(p)}(xy)}$ where θ is a primitive p-th root of unity in $\mathbb{C}$.

If $\mathcal{F}$ is the additive group $(\mathbb{Z}_q,+)$, *i.e.* a cyclic group of order q, then $<x,y>=\theta^{xy}$ where θ is a primitive q-th root of unity in $\mathbb{C}$ and where the product xy is performed in the ring $\mathbb{Z}_q$. We will need the following classical lemma:

Lemma 3. *Let F and G be two Abelian groups with respective characters groups F' and G'. Then the characters group of $H=F\times G$ is $F'\times G'$.*
For $h=(f,g)\in F\times G$ and $h'=(f',g')\in F'\times G'$, we have $<h,h'>=<f,f'><g,g'>$.

We now show how the Fourier transform characterization of K. Gopalakrishnan and D.R. Stinson can be stated for a general Abelian group and is then a straightforward corollary of theorem 4.4 of Delsarte ([5] page 43).

Let $\mathcal{F}$ be an Abelian group. The n-th Cartesian power $G=\mathcal{F}^n$ is then an Abelian group in its turn. The Hamming weight of an element x of G is the number $w_H(x)$ of components of x in $\mathcal{F}$ which are distinct from zero. Theorem 4.4 of Delsarte can be written as follows.

Theorem 4. *The array consisting of a set $M\subset G$ of λq^t rows is orthogonal with n constraints, q levels, strength t and index λ if and only if*

$$\forall y\in G', 1\le w_H(y)\le t, \sum_{x\in M}<x,y>=0$$

We now deduce a general characterization of correlation immune functions in terms of Fourier transform.

Theorem 5. *The function $f:\mathcal{F}^n\to\mathcal{F}^\ell$ is t-th order correlation immune if and only if:*

$$\forall v\in\mathcal{F}^\ell,\ \forall u\in\mathcal{F}^n, 1\le w_H(u)\le t, \sum_{x\in\mathcal{F}^n}<x,u><f(x),v>=0$$

Proof. This condition is sufficient: we write $\hat{a}_{y,u}$ for $\sum_{x\in f^{-1}(y)}<x,u>$, with the convention $\hat{a}_{y,u}=0$ when $f^{-1}(y)=\emptyset$.
Then the above relations can be written as:

$$\forall v\in\mathcal{F}^\ell,\ \forall u\in\mathcal{F}^n, 1\le w_H(u)\le t, \sum_{y\in\mathcal{F}^\ell}\hat{a}_{y,u}<y,v>=0$$

Since the matrix of group characters of the Abelian group $\mathcal{F}^\ell$ is invertible then we have: $\forall u\in\mathcal{F}^n, 1\le w_H(u)\le t, \hat{a}_{y,u}=0$.
Then Theorem 3 applies: $\forall y\in\mathcal{F}^\ell$, $f^{-1}(y)$ is a $(|f^{-1}(y)|,n,q,t)$ orthogonal array over $\mathcal{F}$.
The converse also results from Theorem 3.

4 Perfect local randomizers over any finite alphabet

As pointed out by Maurer and Massey [9] one of the most important cryptographic applications of orthogonal arrays consists in designing running-key generators for additive stream ciphers. The problem is then to transform a k-component secret sequence into a longer one of n components which will be added to the plaintext. Since such a running-key can obviously not be completely random, the associate stream cipher can not be provably secure. However the running-key generator can be designed such that if the k input components are uniformly random, then any subset of t or less components of the output sequence is a set of uniformly random digits. Such a generator is called a (k, n) *perfect local randomizer of order* t. The use of a perfect local randomizer then leads to a provably-secure stream cipher under the assumption that the enemy is able to obtain only a limited number of plaintext digits.

This concept exactly corresponds to the combinatorial structure of orthogonal arrays. Furthermore Massey showed in [8] that it can be relied, even in non-linear case, to the dual distance of a code, *i.e.* the smallest positive weight of the MacWilliams' transform of the distance distribution of the code, as defined by Delsarte [5].

We can now generalize the concept of perfect local randomizer over any finite alphabet $\mathcal{F}$ of size q since Delsarte proved the previous property about the dual distance for a code over a finite alphabet endowed with the structure of an Abelian group.

Proposition 6. *An injective function $f : \mathcal{F}^k \to \mathcal{F}^n$, where $k < n$, is a (k, n) perfect local randomizer of order t*
if and only if the $q^k \times n$ array whose rows are the vectors of $f(\mathcal{F}^k)$ is a (q^k, n, q, t) orthogonal array
if and only if f is the encoder for an (n, k) systematic code $\mathcal{C}$ over $\mathcal{F}$ (not necessarily linear) with dual distance $d^\perp < t$.
$d^\perp$ is here the smallest index $i > 0$ such that $b_i > 0$ where $(b_0, \ldots, b_n)$ is given by the generalized MacWilliams' identity :

$$\sum_{i=0}^{n} b_i X^{n-i} Y^i = H_{\mathcal{C}}^{\perp}(X, Y) = \frac{1}{|\mathcal{C}|} H_{\mathcal{C}}(X + qY, X - Y)$$

if $H_{\mathcal{C}}(X, Y) = \sum_{i=0}^{n} a_i X^{n-i} Y^i$ is the Hamming-weight enumerator of $\mathcal{C}$.

[9] and [2] give some bounds stemming from coding theory on the order of binary (k, n) perfect local randomizers. But we can now wonder whether, for fixed k and n, there exists (k, n) perfect local randomizers over some other alphabets whose order exceeds these bounds. In the following example, we use a construction suggested in [14] and we obtain $(2, 4)$ perfect local randomizers of order 2 over some cyclic groups whereas they do not exist in binary case.

Example 1. Let $\mathcal{F}$ be the cyclic group $(\mathbb{Z}_q, +)$ and $\mathcal{A}$ be the orthogonal array whose rows are the 4-tuples $(x_1, x_2, x_1 + ax_2, x_1 + bx_2)$ where $a, b \in \mathbb{Z}_q$.

Theorem 3 says that $\mathcal{A}$ is an orthogonal array of strength t over $\mathbb{Z}_q$ if and only if its dual in the characters group contains no element of Hamming weight less than or equal to t.
In this case it means that

$$\forall x \in \mathcal{A}, \forall y, 1 \leq w_H(y) \leq t, \sum_{i=1}^{n} x_i y_i \neq 0$$

where the product $x_i y_i$ is performed in the ring $\mathbb{Z}_q$, because $< x, y >= \theta^{xy}$ where θ is a primitive q-th root of unity.
If we write this condition for all y of weight 2, we clearly obtain, as a corollary of Theorem 3, that $\mathcal{A}$ is an orthogonal array of strength 2 if and only if a, b and $(a-b)$ are not zero divisors.
For instance the array formed by the 4-tuples $(x_1, x_2, x_1 + 4x_2, x_1 + 11x_2)$ is an orthogonal array of strength 2 over $\mathbb{Z}_{15}$.
Then, as pointed out in [14], $\mathcal{A}$ cannot be an orthogonal array of strength 2 when q is even.

Perfect local randomizers of maximal order can also be used for designing conventional cryptographic primitives because they realize perfect diffusion. Schnorr and Vaudenay [11] formalized this idea through the equivalent concept of multipermutation:

Definition 7. A (r, n) multipermutation over a finite alphabet $\mathcal{F}$ is a function f from $\mathcal{F}^r$ to $\mathcal{F}^n$ such that 2 different $(r+n)$-tuples of the form $(x, f(x))$ cannot collide in any r positions $\Leftrightarrow$ f is a $(r, r+n)$ perfect local randomizer of order r over $\mathcal{F}$.

They claim that all diffusion boxes of the network representing a cryptographic primitive should be multipermutations: if the network contains a gate which does not realize perfect diffusion, it is then possible to find some values such that both inputs and outputs of the gate are close according to the Hamming distance. For example S. Vaudenay constructed some collisions on the first 2 rounds of MD4 using the fact that the diffusion boxes in these rounds are not multipermutations [13].

The design of cryptographic primitives then leads to the search of multipermutations over a given alphabet $\mathcal{F}$. Proposition 5 enables us to construct such functions from codes over $\mathcal{F}$. In particular MDS codes provide multipermutations [13].

5 Construction of new correlation immune functions by composition

The characterizations given in sections 2 and 3 are now used for constructing t-th order correlation immune functions over a finite alphabet by composition of correlation immune functions of smaller order. As above $\mathcal{F}$ is a finite alphabet of size q endowed with the structure of some Abelian group.

Definition 8. Let $(g_i)_{1 \leq i \leq k}$ be a family of functions:

$$g_i : \mathcal{F}^m \rightarrow \mathcal{F}^d = \mathcal{A}, \text{ where } d \leq m$$

We define the function g from $\mathcal{F}^{mk}$ to $\mathcal{A}^k$ by $g(x_1,\ldots,x_k)=(g_1(x_1),\ldots,g_k(x_k))$.
Let h be a function:

$$h:(\mathcal{A})^k \to \mathcal{F}^\ell, \text{ where } \ell \leq kd$$

The composed function $f=h\circ g$ is defined by:

$$\begin{array}{rccc} f: & \mathcal{F}^{mk} & \to & \mathcal{F}^\ell \\ & (x_1,\ldots,x_k) & \mapsto & h(g_1(x_1),\ldots,g_k(x_k)) \end{array}$$

Proposition 9. *If every g_i is balanced and if h is r-th order correlation immune with respect to $\mathcal{A}$, then $h\circ g$ is r-th order correlation immune with respect to $\mathcal{F}^m$.*

Proof. Let $v\in\mathcal{F}^\ell$ and let $R=\{i_1,\ldots,i_r\}$ be a r-element subset of $\{1,\ldots,k\}$ and $\bar{R}=\{j_1,\ldots,j_{k-r}\}$ be the complementary set.
Since h is r-th order correlation immune with respect to $\mathcal{A}$, $h^{-1}(v)$ is an orthogonal array with k constraints, strength r and index λ_v over the alphabet $\mathcal{A}$. Given a vector $a=(a_{i_1},\ldots,a_{i_r})\in\mathcal{A}^r$, the number of elements $z=(z_1,\ldots,z_k)\in\mathcal{A}^k$ in $h^{-1}(v)$ such that $(z_{i_1},\ldots,z_{i_r})=a$ is then equal to λ_v.
We denote by g_R the function $(x_{i_1},\ldots,x_{i_r})\mapsto(g_{i_1}(x_{i_1}),\ldots,g_{i_r}(x_{i_r})$ and by $g_{\bar{R}}$ the function $(x_{j_1},\ldots,x_{j_r})\mapsto(g_{j_1}(x_{j_1}),\ldots,g_{j_{k-r}}(x_{j_{k-r}}))$.
By assumption, every g_i is balanced; this entails that $|g_i^{-1}(a_i)|=|\mathcal{F}|^{m-d}$.
Then $\forall b=(b_{j_1},\ldots,b_{j_{k-r}})$, $g_{\bar{R}}^{-1}(b)$ is a subset of $\mathcal{F}^{m(k-r)}$ of size $|\mathcal{F}|^{(m-d)(k-r)}$. In the same way $|g_R^{-1}(a)|=|\mathcal{F}|^{(m-d)r}$ and $(g_R^{-1}(a))_{a\in\mathcal{A}^r}$ is a partition of $(\mathcal{F}^m)^r$.

Hence every r-tuple of $(\mathcal{F}^m)^r$ appears as the projection on R of exactly $\lambda_v|\mathcal{F}|^{(m-d)(k-r)}$ elements in $(h\circ g)^{-1}(v)$. It means that$(h\circ g)^{-1}(v)$ is an orthogonal array with k constraints, strength r, index $\lambda_v q^{(m-d)(k-r)}$ over the alphabet $\mathcal{F}^m$.

Proposition 10. *If $f=h\circ g$ is r-th order correlation immune with respect to $\mathcal{F}^m$ and if $\forall 1\leq i\leq k$, g_i is t-th order correlation immune with respect to $\mathcal{F}$, then f is t'-th order correlation immune with respect to $\mathcal{F}$ where $t'=(t+1)(r+1)-1$.*

Proof. Let $\mathcal{B}=\mathcal{F}^m$ and $u\in\mathcal{B}^k$. We write $u=(u_1,\ldots,u_k), u_i\in\mathcal{B}$. The Hamming weight of u in $\mathcal{B}^k$, *i.e.* $|\{i/u_i\neq 0\}|$, is denoted by $W_H(u)$ while the Hamming weight of u in $\mathcal{F}^{mk}$, *i.e.* the number of non-zero components of u in $\mathcal{F}$ is denoted by $w_H(u)$.
f is r-th order correlation immune with respect to $\mathcal{B}$ means that $\forall v\in\mathcal{F}^\ell$, $f^{-1}(v)$ is an orthogonal array of strength r over $\mathcal{B}$. By theorem 3 we have

$$\forall u\in\mathcal{B}^k,\ 1\leq W_H(u)\leq r,\quad \sum_{x\in f^{-1}(v),x\in\mathcal{B}^k} < x,u >=0$$

Now if $W_H(u)>r$ and $w_H(u)<(r+1)(t+1)$, then there is an index $i\in\{1,\ldots,k\}$ such that $1\leq w_H(u_i)\leq t$. Then we get by lemma 2:

$$\sum_{x\in f^{-1}(v),x\in\mathcal{F}^{mk}} < x,u >= \sum_{y\in h^{-1}(v)}\ \sum_{x\in g^{-1}(y)} < x,u >$$

$$= \sum_{y \in h^{-1}(v)} \prod_{i=1}^{k} \sum_{x_i \in g_i^{-1}(y_i)} < x_i, u_i >$$

Since g_i is t-th order correlation immune, at least one of the factors $\sum_{x_i \in g_i^{-1}(y_i)} < x_i, u_i >$ is zero. Thus we obtain:

$$\forall u \in \mathcal{F}^{mk},\ 1 \leq w_H(u) \leq t', \quad \sum_{x \in f^{-1}(v), x \in \mathcal{F}^{mk}} < x, u >= 0$$

As a consequence of these two propositions we obtain the following theorem.

Theorem 11. *If every g_i is t-resilient with respect to $\mathcal{F}$ and if h is r-th order correlation immune with respect to $\mathcal{A}$, then $h \circ g$ is t'-th order correlation immune with respect to $\mathcal{F}$, where $t' = (t+1)(r+1) - 1$.*

Corollary 12. *If every g_i is t-resilient with respect to $\mathcal{F}$ and if h is r-resilient with respect to $\mathcal{A}$, then $h \circ g$ is t'-resilient with respect to $\mathcal{F}$, where $t' = (t+1)(r+1) - 1$.*

The parameters of the orthogonal arrays $g_i^{-1}(z), z \in \mathcal{A}$ are (q^{m-d}, m, q, t), $\lambda_g = q^{m-d-t}$. Those of $h^{-1}(z), z \in \mathcal{F}^\ell$ are $(q^{dk-\ell}, k, q^d, r)$, $\lambda_h = q^{dk-\ell-r}$. This results in orthogonal arrays $f^{-1}(z), z \in \mathcal{F}^\ell$ with parameters $(q^{km-\ell}, km, q, (t+1)(r+1)-1)$, $\lambda_f = q^{km-\ell-tr-t-r}$.

Zhang and Zheng presented at Eurocrypt'95 some results about the construction of new binary resilient functions from old ones by addition (section 3 in [16]) and by composition with a permutation (section 4 in [16]). These results are immediate corollaries of the previous theorem and they can be generalized for functions over any finite alphabet.

Corollary 13. *Let $g_i : \mathcal{F}^m \to \mathcal{F}^d,\ \ i = 1, \ldots, k$ be k t-resilient functions with respect to $\mathcal{F}$ and $h : (\mathcal{F}^d)^k \to \mathcal{F}^d$ be the addition over $\mathcal{F}^d$. Then the composed function f is a t'-resilient function with respect to $\mathcal{F}$ where $t' = k(t+1) - 1$.*

$$\begin{array}{rccc} f: & \mathcal{F}^{mk} & \to & \mathcal{F}^d \\ & (x_1, \ldots, x_k) & \mapsto & g_1(x_1) + \ldots + g_k(x_k) \end{array}$$

Corollary 14. *Let $g : \mathcal{F}^m \to \mathcal{F}^d$ be a t-resilient function with respect to $\mathcal{F}$ and h be a permutation of $\mathcal{F}^d$. Then $h \circ g$ is still a t-resilient function with respect to $\mathcal{F}$.*

6 Combining LFSRs for designing running-key generators

A common type of running-key generator used in stream ciphers consists of several binary Linear Feedback Shift Registers (LFSRs) whose outputs are combined by a boolean function f. This function has to be nonlinear in order to avoid an attack by the Berlekamp-Massey shift register synthesis algorithm. Furthermore Siegenthaler [12] has shown that f has to be correlation-immune, otherwise the generator structure is not resistant to a correlation attack.

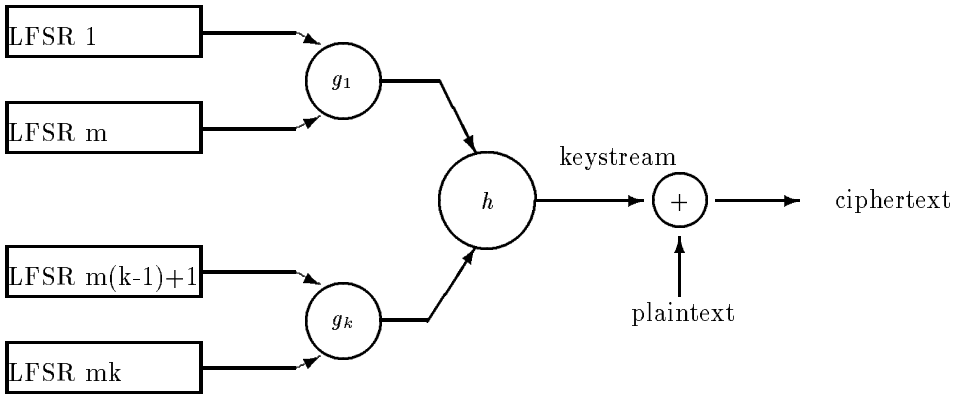

Fig. 1. Combining LFSRs with a composed function $f = h \circ g$

The problem is now to find some nonlinear and correlation-immune combining functions. The previous study enables us to construct such functions and in particular to combine a great number of different LFSRs.

Thanks to Theorem 10 we obtain the order of correlation-immunity of f without writing its truth table which is usually very large. In the following examples we construct a 3-resilient boolean function of degree 2 and a 5-resilient boolean function of degree 4 for combining respectively 6 and 12 LFSRs. We here denote $GF(q)$ by $\mathbb{F}_q$.

Example 2.
Let $g_1 = g_2 : \quad \mathbb{F}_2^3 \quad \rightarrow \quad \mathbb{F}_2^2$
$(x_1; x_2; x_3) \mapsto (x_1 + x_2; x_1 + x_3)$
This function is 1-resilient with respect to $\mathbb{F}_2$.
Let $h : (\mathbb{F}_2^2)^2 \rightarrow \mathbb{F}_2$. The transposed of its truth table T_h is given by:

$$T_h^t = \left[\begin{array}{cccccccc} 0&0&0&0&1&1&1&1 \\ 0&0&1&1&1&1&0&0 \\ \hline 0&1&1&1&0&0&0&1 \\ 1&1&1&0&0&1&0&0 \end{array}\right] \begin{array}{c} x_1 \\ x_2 \\ \\ x_3 \\ x_4 \end{array}$$

h is 1-resilient with respect to $\mathbb{F}_2^2$ and it is nonlinear as a function from $(\mathbb{F}_2)^4$ onto $\mathbb{F}_2$ since $h(x_1; x_2; x_3; x_4) = x_1 + x_4 + x_2x_3 + x_2x_4$.
The composed function $f : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2$
$f(x_1; x_2; x_3; x_4; x_5; x_6) = x_1 + x_2 + x_4 + x_6 + x_1x_5 + x_1x_6 + x_3x_5 + x_3x_6$ is then 3-resilient with respect to $\mathbb{F}_2$.

Its truth table T_f is then a binary orthogonal array of size 32, 6 constraints, index 4 and strength 3:

$$\begin{bmatrix} 0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0 \\ 1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1 \end{bmatrix} \begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{matrix}$$

Example 3.
Let $g_1 = g_2 : \mathbb{F}_2^6 \to \mathbb{F}_2^3$
$x \mapsto xH^t$
where H is the parity-check matrix of the code $\mathcal{C}$,

$$H = \begin{bmatrix} 1\,0\,0\,1\,1\,0 \\ 0\,1\,0\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1 \end{bmatrix}$$

Since $d^\perp = 3$, the corresponding function g_1 is a 2-resilient function with respect to $\mathbb{F}_2$.

Let α be a root of $X^3 + X + 1$ and let ϕ be the bijection from $\mathbb{F}_{2^3}$ onto $\mathbb{Z}_8$ defined by $\forall i,\ \phi(\alpha^i) = i$ and $\phi(0) = 0$.
Then we define h as:
$h : \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} \to \mathbb{F}_2$
$(x, y) \mapsto \phi_0^{-1}(\phi(x) + \phi(y))$
where the addition is performed in $\mathbb{Z}_8$ and $\phi_0^{-1}(x)$ denotes the low-weight bit of $\phi^{-1}(x)$.
By construction, h is 1-resilient with respect to $\mathbb{F}_2^3$. If h is considered as a function over $(\mathbb{F}_2)^6$, we obtain the boolean form:
$h(x_1; x_2; x_3; y_1; y_2; y_3) = x_1 + y_1 + x_1y_1 + x_1y_2 + x_1y_3 + x_2y_1 + x_2y_3 + x_3y_1 + x_3y_2 + x_1x_3y_1 + x_1y_1y_3 + x_1x_2y_1y_3 + x_1x_2y_2y_3 + x_1x_3y_1y_2 + x_1x_3y_1y_3 + x_2x_3y_1y_2$
Since h is a boolean function of degree 4, the composed function $f = h \circ g$ is a boolean function with 12 variables of degree 4 and 5-resilient.

One of the advantages of using a composed combining function is that the computation can be parallelized in a natural way.

In some applications, the combining function is used as a secret key. This function is then transmitted as the sequence of its outputs, *i.e.* $\ell 2^m$ bits for $f : \mathbb{F}_2^m \to \mathbb{F}_2^\ell$. If a composed function is used, we only have to send the small functions (g_i) and h, *i.e.* $k2^m d + 2^{kd}$ bits, while transmitting any function for combining km LFSRs requires 2^{km} bits.

References

[1] C.H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Computing*, 17(2):210–229, april 1988.

[2] J. Bierbrauer, K. Gopalakrishnan, and D.R. Stinson. Bounds for resilient functions and orthogonal arrays. In Y.G. Desmedt, editor, *Advances in Cryptology - CRYPTO'94*, number 839 in Lecture Notes in Computer Science, pages 247–256, 1994.

[3] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO'91*, number 576 in Lecture Notes in Computer Science, pages 86–100. Springer-Verlag, 1992.

[4] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich, and R. Smolensky. The bit extraction problem or t-resilient functions. In *Proc. 26th IEEE Symposium on Foundations of Computer Science*, pages 396–407, 1985.

[5] P. Delsarte. An algebraic approach to the association schemes of coding theory. Thesis, Université catholique de Louvain, 1973.

[6] K. Gopalakrishnan and D.R. Stinson. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography*, 5:241–251, 1995.

[7] F.J. MacWilliams and N.J.A. Sloane. The Theory of Error-correcting Codes. North-Holland, 1983.

[8] J.L. Massey. Some applications of coding theory in cryptography. In *IMA Conference Proceedings on Cryptography and Coding IV*, 1993.

[9] U.M. Maurer and J.L. Massey. Perfect local randomness in pseudo-random sequences. In G. Brassard, editor, *Advances in Cryptology - CRYPTO'89*, number 435 in Lecture Notes in Computer Science, pages 100–112. Springer-Verlag, 1990.

[10] C.R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *J. Roy. Statist.*, 9:128–139, 1947.

[11] C.-P. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT'94*, number 950 in Lecture Notes in Computer Science, pages 47–57. Springer-Verlag, 1995.

[12] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory*, IT-30(5):776–780, 1984.

[13] S. Vaudenay. On the need for multipermutations: cryptanalysis of MD4 and SAFER. In *Fast Software Encryption*, Lecture Notes in Computer Science. Springer-Verlag. to appear.

[14] S. Vaudenay. *La sécurité des primitives cryptographiques*. PhD thesis, Université Paris 7, 1995. in french.

[15] G. Xiao and J.L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inform. Theory*, IT-34(3):569–571, 1988.

[16] X. Zhang and Y. Zheng. On nonlinear resilient functions. In L. Guillou and J.J. Quisquater, editors, *Advances in Cryptology - EUROCRYPT'95*, number 921 in Lecture Notes in Computer Science, pages 274–288. Springer-Verlag, 1995.

Unité de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unité de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unité de recherche INRIA Rhône-Alpes, 46 avenue Félix Viallet, 38031 GRENOBLE Cedex 1
Unité de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unité de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
ISSN 0249-6399