Noname manuscript No.
(will be inserted by the editor)

Authentication Codes Based on Resilient Boolean Maps

Juan Carlos Ku-Cauich · Guillermo Morales-Luna

Received: February 23, 2015/ Accepted: date

Abstract We introduce new constructions of systematic authentication codes over finite fields and Galois rings. One code is built over finite fields using resilient functions and it provides optimal impersonation and substitution probabilities. Other two proposed codes are defined over Galois rings, one is based on resilient maps and it attains optimal probabilities as well, while the other uses maps whose Fourier transforms get higher values. Being the finite fields special cases of Galois rings, the first code introduced for Galois rings apply also at finite fields. For the special case of characteristic p^2, the maps used at the second case in Galois rings are bent indeed, and this case is subsumed by our current general construction of characteristic p^s, with $s \geq 2$.

Keywords Authentication Schemes · Resilient Maps · Finite Fields · Galois Rings

1 Introduction

Resilient maps were introduced by Chor *et al.* [7] and independently by Bennet *et al.* [1] by describing several applications on key distribution at quantum cryptography protocols. Resilient maps have been applied on random sequences generation for streaming ciphers [15] as well. We introduce new authentication codes with the aim to optimize by minimizing impersonation and substitution probabilities. Similar constructions have been introduced at [3, 4, 9] using bent and almost-bent maps, but now we are using resilient maps and

Both authors acknowledge the support of Mexican Conacyt

Juan Carlos Ku-Cauich
Computer Science, CINVESTAV-IPN, Mexico City, Mexico, E-mail: jckc35@hotmail.com

Guillermo Morales-Luna
Computer Science, CINVESTAV-IPN, Mexico City, Mexico, E-mail: gmorales@cs.cinvestav.mx

another special class of functions able to provide optimal least bounds. In our presentation we compare the introduced codes on Galois rings with previous authentication codes that use rational functions and non-degenerate maps [13] on Galois rings.

The first introduced authentication code is built on finite fields, and the other two codes are built over Galois rings, the first one uses resilient maps, while the second construction uses a class of maps that generalizes the bent maps produced at [4]. In the introduced code for finite fields and in one at Galois rings optimal minimal impersonation and substitution probabilities are got.

2 Systematic authentication codes

Authentication codes have been extensively studied in the literature. Let us recall a basic setting [9]:

A *systematic authentication code* is a structure (S, T, K, E) where S is the *source state space*, T is the *tag space*, K is the *key space* and $E = (e_k)_{k\in K}$ is a sequence of *encoding rules* $S \to T$.

In general terms, a *transmitter* sends to a *receiver* a source element $s \in S$ codified by a tag $t \in T$ through an encoding rule. The communicating channel is public, thus it can be intervened by an *intruder* that is able to perform either *impersonation* or *substitution* attacks through the public channel. The intruder's success probabilities for impersonation and substitution are, respectively

$$p_I = \max_{(s,t)\in S\times T} \frac{\operatorname{card}(\{k \in K |\ e_k(s) = t\})}{\operatorname{card}(K)} \tag{1}$$

$$p_S = \max_{(s,t)\in S\times T} \max_{(s',t')\in(S-\{s\})\times T} \frac{\operatorname{card}(\{k \in K |\ e_k(s) = t \ \&\ e_k(s') = t'\})}{\operatorname{card}(\{k \in K |\ e_k(s) = t\})} \tag{2}$$

Thus a goal in the design of authentication codes is to maintain these probabilities as lower as possible. However, they cannot be zero, because there are positive inferior bounds for these probabilities, namely [9]:

$$p_I \geq \frac{1}{\operatorname{card}(T)} \quad , \quad p_S \geq \frac{1}{\operatorname{card}(T)} \tag{3}$$

An authentication code [14] is *with secrecy* if for any $t \in T$, and any $s \in S$, $p_S(s|T = t) = p_S(s)$. Namely, the knowledge of a tag does not provide any information of the source message that it codifies. The authentication code is *without secrecy* if $p_S(s|T = t) =\in \{0, 1\}$. Namely, the knowledge of a tag is enough to decide for a given message whether it is codified by the tag, independently of the encoding map. If an encoding rule $S \to T$ is one-to-one then $p_S(s|T = t) \neq p_S(s)$, thus it is not with secrecy, while certainly $p_S(s|T = t) =\in \{0, 1\}$ does hold, thus it is without secrecy.

Here, we will assume the following transmission protocol [9], which is without secrecy: A *transmitter* and a *receiver* agree a secret key $k \in K$. Whenever a source $s \in S$ should be sent, the participants proceed as follows:

Transmitter		Receiver
calculates $t = e_k(s) \in T$		
forms the pairing $m = (s, t)$	$\xrightarrow{m}$	receives $m' = (s', t')$, calculates $t'' = e_k(s') \in T$ if $t' = t''$ then she/he accepts s', otherwise the message m' is rejected

At [9] there are introduced systematic authentication codes using perfect and almost-perfect non-linear functions. Two codes are presented using perfect non-linear functions with

$$p_I = \frac{1}{q} \quad , \quad p_S \leq \frac{1}{q} + \frac{q-1}{q^{\frac{m+2}{2}}}. \tag{4}$$

in one case and

$$p_I \leq \frac{1}{q} + \frac{q-1}{q}\frac{1}{q^{\frac{m}{2}}} \quad , \quad p_S \leq \frac{1}{q}\left[1 + \frac{q^2-1}{q^{\frac{m}{2}} - q + 1}\right]. \tag{5}$$

in the second case. Two other codes are presented using almost-perfect non-linear functions with

$$p_I = \frac{1}{q} \quad , \quad p_S \leq \frac{1}{q} + \frac{1 + 2(q-1)(1+q^{\frac{m}{2}})}{q^{m+1}}. \tag{6}$$

for the first case, and

$$p_I \leq \frac{1}{q} + \frac{(q-1)(1+2q^{\frac{m}{2}})}{q^{m+1}} \quad , \quad p_S \leq \frac{1}{q}\left[1 + \frac{2(q^2+q-2)q^{\frac{m}{2}} + q^2}{q^m - 2(q-1)q^{\frac{m}{2}} - 1}\right]. \tag{7}$$

for the second case.

At [6] a similar approach is assumed within constructed authentication codes without secrecy, using Boolean functions with high nonlinearity, and their optimality, with respect to reduce the number of encoding rules and the impersonation and substitution probabilities.

Our purpose here is the introduction of authentication codes without secrecy with minimal impersonation and substitution probabilities.

3 Authentication codes over finite fields

3.1 Preliminaries on finite fields

Let $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ be the n- and m-dimensional vector spaces over the prime field $\mathbb{F}_2$ of characteristic 2, $1 \leq m \leq n$. For any index t-subset $J \subset \{0, \ldots, n-1\}$,

say $J = \{j_0, \ldots, j_{t-1}\}$, and any $a = (a_0, \ldots, a_{t-1}) \in \mathbb{F}_2^t$, let the *affine J-variety determined by a* be

$$V_{J,a,n} = \{x \in \mathbb{F}_2^n |\ \forall k \in \{0, \ldots, t-1\} :\ x_{j_k} = a_k\}.$$

A map $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is *J-resilient* if $\forall a = (a_0, \ldots, a_{t-1}) \in \mathbb{F}_2^t$, the map $f|_{V_{J,a,n}}$ is balanced, namely, $\forall y \in \mathbb{F}_2^m$, $\mathrm{card}\left(V_{J,a,n} \cap f^{-1}(y)\right) = 2^{n-t-m}$. Map $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is *t-resilient* if it is J-resilient for any set J such that $\mathrm{card}\,(J) = t$.

This characterization, assumed here as a definition, is suitable to be stated in the context of Galois rings [2] as well.

For instance [2], let $S = \mathrm{GR}\,(p^s, \ell m)$ be the Galois ring of characteristic p^s and order ℓm, where p is a prime and $s, \ell, m \in \mathbb{Z}^+$. For the particular case of $s = 1$, the Galois ring is the finite field $S = \mathbb{F}_{p^{\ell m}}$. Let S^n be the n-Cartesian power of S with its structure of S-module, let $t = n - 1$, let $g : S^n \to S$ be an arbitrary map and

$$\phi : S^n \to S^n \quad , \quad \left(\sum_{i=0}^{s-1} a_{i0} p^i, \ldots, \sum_{i=0}^{s-1} a_{i,n-1} p^i\right) \mapsto (a_{00}, \ldots, a_{0,n-1}), \tag{8}$$

then the map

$$f : S^{2n} \to S \quad , \quad (x, y) \mapsto f(x, y) = x \cdot \phi(y) + g(y),$$

where $\cdot$ is the inner product, is t-resilent. □

An equivalent definition will be quoted at section 4.1 below.

Let $q = p^\ell$ be the power of a prime number, $m \in \mathbb{Z}^+$ be a positive integer and $T_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ be the trace map. Clearly, $\forall a \in \mathbb{F}_{q^m}^*$, map $\mathbb{F}_{q^m} \to \mathbb{F}_p$, $x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(ax)$, is balanced. Let $n \in \mathbb{Z}^+$ be a positive integer and $\cdot$ be the inner product map $\mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$. Then $\forall b \in \mathbb{F}_{q^m}^n - \{0\}$ map $\mathbb{F}_{q^m}^n \to \mathbb{F}_p$, $x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b \cdot x)$ is balanced as well. Let $w_H : \mathbb{F}_{q^m}^n \to \mathbb{N}$ be the *Hamming weight* $x \mapsto w_H(x) = \mathrm{card}\,(\{i |\ x_i \neq 0\})$.

We observe that whenever $t \leq n$, $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ is t-resilient, and $a \in \mathbb{F}_{q^m}$, $b \in \mathbb{F}_{q^m}^n$ are such that $w_H(b) \leq t$ and $(a, b) \neq (0, 0)$ then:

– As shown in [2,11]:

$$\zeta_{af}(b) = \sum_{x \in \mathbb{F}_{q^m}^n} e^{\frac{2\pi}{p}\, i\, T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(a\, f(x) + b \cdot x)} = 0. \tag{9}$$

– As a more general result than Corollary 2 at [17] we have that

$$\gamma_{abf} : \mathbb{F}_{q^m} \to \mathbb{F}_q\ ,\ \gamma_{abf} : x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(a\, f(x) + b \cdot x). \tag{10}$$

is balanced.

Proposition 1 *Under the above conditions: $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ t-resilient, $a \in \mathbb{F}_{q^m}$, $b \in \mathbb{F}_{q^m}^n$, $w_H(b) \leq t$ and $(a, b) \neq (0, 0)$, for any $u \in \mathbb{F}_{q^m}$:*

$$\mathrm{card}\left(\gamma_{abf}^{-1}(u)\right) = q^{mn-1}. \tag{11}$$

Proof If $a = 0$ then (11) follows immediately.

If $a \neq 0$ then

$$\begin{aligned} q \operatorname{card}\left(\gamma_{abf}^{-1}(u)\right) &= \sum_{x \in \mathbb{F}_q^n} \left[\sum_{y \in \mathbb{F}_{q^m}} e^{\frac{2\pi}{p} i T_{\mathbb{F}_q/\mathbb{F}_p}(y\,(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\,f(x)+b\cdot x)-u))} \right] \\ &= q^{mn} + \sum_{y \in \mathbb{F}_{q^m}^*} \sum_{x \in \mathbb{F}_{q^m}^n} e^{\frac{2\pi}{p} i T_{\mathbb{F}_q/\mathbb{F}_p}(y\,(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\,f(x)+b\cdot x)-u))} \\ &= q^{mn} + \sum_{y \in \mathbb{F}_{q^m}^*} e^{\frac{2\pi}{p} i T_{\mathbb{F}_q/\mathbb{F}_p}(-y\,u))} \sum_{x \in \mathbb{F}_{q^m}^n} e^{\frac{2\pi}{p} i T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(ya\,f(x)+yb\cdot x)} \\ &= q^{mn} \end{aligned}$$

since, by (9), $\sum_{x \in \mathbb{F}_{q^m}^n} e^{\frac{2\pi}{p} i T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(ya\,f(x)+yb\cdot x)} = 0$. Hence, relation (11) follows. □

3.2 A new construction for an authentication code on finite fields

Let q be the power of a prime number, say $q = p^\ell$, $m \in \mathbb{Z}^+$ a positive integer, $T_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ the trace map, $n \in \mathbb{Z}^+$ another positive integer and $e_i = (\delta_{ij})_{j=0}^{n-1}$ the i-th vector in the canonical basis of $\mathbb{F}_{q^m}^n$. Let $f : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}$ be a t-resilient map, $t \leq n$.

For any $b = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_{q^m}^n$, let

$$X_{b,t} = \{\sum_{j=0}^{t-2} b_j e_j, b_{t-1} e_{t-1}, \ldots, b_{n-1} e_{n-1}\} \subset \mathbb{F}_{q^m}^n,$$

then $\operatorname{card}(X_{b,t}) = n - t + 1$. Let

$$(S, T, K) = \left(\left(\{1\} \times \bigcup_{b \in \mathbb{F}_{q^m}^n} X_{b,t} \right) \cup \left(\{0\} \times (e_j)_{j=0}^{n-1} \right) \;,\; \mathbb{F}_q \;,\; \mathbb{F}_{q^m}^n \right) \tag{12}$$

From relation (12) we have

$$\begin{aligned} \operatorname{card}(S) &= q^{m(t-1)} + (n-t+1)q^m + n \\ \operatorname{card}(T) &= q \\ \operatorname{card}(K) &= q^{mn} \end{aligned}$$

We define the following encoding maps: $\forall k \in \mathbb{F}_{q^m}^n$,

$$e_k : s = (s_0, s_1) \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0\,f(k) + s_1 \cdot k), \tag{13}$$

namely, $\forall k \in \mathbb{F}_{q^m}^n$, $\forall s = (s_0, s_1) \in S$: $e_k(s) = \gamma_{s_0 s_1 f}(k)$, according to (10).

Proposition 2 *Map $k \mapsto e_k$ defined by the relation (13) is one-to-one.*

Proof Namely, let us assume $e_k = e_{k'}$ for two keys $k, k' \in \mathbb{F}_{q^m}^n$. Then, necessarily

$$\forall s = (s_0, s_1) \in S: \; T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_0\left(f(k) - f(k')\right) + s_1 \cdot (k - k')\right) = 0,$$

In particular, for each $j = 0, \ldots, n-1$, by taking $(s_0, s_1) = (0, e_j)$ we get

$$0 = T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(0\left(f(k) - f(k')\right) + e_j \cdot (k - k')\right) = T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(k_j - k'_j\right),$$

by taking now $(s_0, s_1) = (1, e_j)$ we get

$$T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(f(k) - f(k')\right) = -T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(k_j - k'_j\right) = 0,$$

and finally, by taking $(s_0, s_1) = (1, b_j e_j)$, with $b_j \in \mathbb{F}_{q^m}$, we get

$$T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(b_j(k_j - k'_j)\right) = -T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(f(k) - f(k')\right) = 0.$$

Then necessarily, $k_j = k'_j$. Thus, $k = k'$. □

Proposition 3 *Let $s_0 = (s_{00}, s_{10}), s_1 = (s_{01}, s_{11}) \in S$ be two different points at S, $t_0, t_1 \in \mathbb{F}_q$, and*

$$C(f; s_0, s_1; t_0, t_1) = \{k \in \mathbb{F}_{q^m}^n \mid \left(e_k(s_0) = t_0\right) \& \left(e_k(s_1) = t_1\right)\}$$

Then $\mathrm{card}\left(C(f; s_0, s_1; t_0, t_1)\right) = q^{mn-2}$.

Proof Let us write $N(f; s_0, s_1; t_0, t_1) = \mathrm{card}\left(C(f; s_0, s_1; t_0, t_1)\right)$. Through a direct calculation,

$$\begin{aligned}
q^2\, N(f; s_0, s_1; t_0, t_1) &= \sum_{x \in \mathbb{F}_{q^m}^n} \left[\sum_{y_0 \in \mathbb{F}_q} e^{\frac{2\pi}{p}\, i\, T_{\mathbb{F}_q/\mathbb{F}_p}\left(y_0\left(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_{00}\, f(x) + s_{10} \cdot x\right) - t_0\right)\right)}\right] \\
&\qquad \left[\sum_{y_1 \in \mathbb{F}_q} e^{\frac{2\pi}{p}\, i\, T_{\mathbb{F}_q/\mathbb{F}_p}\left(y_1\left(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_{01}\, f(x) + s_{11} \cdot x\right) - t_1\right)\right)}\right] \\
&= \sum_{x \in \mathbb{F}_{q^m}^n} \sum_{(y_0, y_1) \in \mathbb{F}_q^2} \Sigma(y_0, y_1, x)^{(0)} \\
&= q^{mn} + \sum_{x \in \mathbb{F}_{q^m}^n} \sum_{(y_0, y_1) \in \mathbb{F}_q^2 - \{(0,0)\}} \Sigma(y_0, y_1, x)^{(0)} \\
&= q^{mn} + \sum_{(y_0, y_1) \in \mathbb{F}_q^2 - \{(0,0)\}} \sum_{x \in \mathbb{F}_{q^m}^n} \Psi(y_0, y_1, x)^{(1)}\, \Psi(y_0, y_1)^{(2)} \\
&= q^{mn} + \sum_{(y_0, y_1) \in \mathbb{F}_q^2 - \{(0,0)\}} \Psi(y_0, y_1)^{(2)} \sum_{x \in \mathbb{F}_{q^m}^n} \Psi(y_0, y_1, x)^{(1)} \\
&= q^{mn}
\end{aligned}$$

where

$$\Sigma(y_0,y_1,x)^{(0)} = \exp\left[\frac{2\pi}{p}\, i\, T_{\mathbb{F}_q/\mathbb{F}_p}\left(y_0\,(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_{00}\,f(x)+s_{10}\cdot x)-t_0)+ \right.\right.$$
$$\left.\left. y_1\,(T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_{01}\,f(x)+s_{11}\cdot x)-t_1)\right)\right]$$
$$\Psi(y_0,y_1,x)^{(1)} = \exp\left[\frac{2\pi}{p}\, i\, T_{\mathbb{F}_{q^m}/\mathbb{F}_p}\left((y_0\,s_{00}+y_1\,s_{01})\,f(x)+(y_0\,s_{10}+y_1\,s_{11})\cdot x\right)\right]$$
$$\Psi(y_0,y_1)^{(2)} = \exp\left[\frac{2\pi}{p}\, i\, T_{\mathbb{F}_q/\mathbb{F}_p}\left(-y_0t_0-y_1t_1)\right)\right],$$

because, by (9), $\sum_{x\in\mathbb{F}_{q^m}^n}\Psi(y_0,y_1,x)^{(1)}=0$.

It is worth to note that the equations $y_0\,s_{00}+y_1\,s_{01}=0$ and $y_0\,s_{10}+y_1\,s_{11}=0$ cannot hold simultaneously because the points s_0 and s_1 are linearly independent.

The claim follows. □

Proposition 4 *For the authentication code defined by relations (12)-(13):*

$$p_I=\frac{1}{q}\quad,\quad p_S=\frac{1}{q}. \tag{14}$$

Proof The result follows from relations (1) and (2) and the above calculations. □

Observe that also within this construction, the source space can be replaced by the space

$$S=\left(\{1\}\times\{b\in\mathbb{F}_{q^m}^n|\ w_H(b)\le\frac{t}{2}\}\right)\cup\left(\{0\}\times(e_j)_{j=0}^{n-1}\right)$$

producing the same probability values as in (14).

4 Authentication codes over Galois rings

4.1 Preliminaries on Galois rings

Let p be a prime number, $s,\ell,m\in\mathbb{Z}^+$ positive integers, and $q=p^\ell$. Let $R=\mathrm{GR}\,(p^s,\ell)$ and $S=\mathrm{GR}\,(p^s,\ell m)$ be the corresponding Galois rings, R is an extension of $\mathbb{Z}_{p^s}$ and S is an extension of R. The corresponding trace maps are $T_{S/R}:S\to R$, $T_{S/\mathbb{Z}_{p^s}}:S\to\mathbb{Z}_{p^s}$ and $T_{R/\mathbb{Z}_{p^s}}:R\to\mathbb{Z}_{p^s}$, and the sets of zero divisors of R and S are denoted, respectively, pR and pS. Let us denote by $U(S)=(S-pS)\cup\{0\}$ the set of elements at the Galois ring S that are either units or zero.

Firstly, let us recall well known facts [13]:

Lemma 1 *Let $u\in R$. Then the following assertions hold:*

1. $\displaystyle\sum_{x\in R} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(ux)} = \begin{cases} q^s & \text{if } u = 0 \\ 0 & \text{if } u \neq 0 \end{cases}$
2. $\displaystyle\sum_{x\in pR} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(ux)} = \begin{cases} q^{s-1} & \text{if } u \in p^{s-1}R \\ 0 & \text{if } u \notin p^{s-1}R \end{cases}$
3. $\displaystyle\sum_{x\notin pR} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(ux)} = \begin{cases} q^s - q^{s-1} & \text{if } u = 0 \\ -q^{s-1} & \text{if } u \in p^{s-1}R - \{0\} \\ 0 & \text{if } u \notin p^{s-1}R \end{cases}$

The notion of t-resilient maps has been studied by several authors in the context of Galois rings and well known wider classes of t-resilient maps have been provided. For instance, from Theorem 1 in [2], we have that for any $n \in \mathbb{Z}^+$, if $f_0 : S^n \to S^n$ is a map such that any element at its image $f_0(S^n)$ has more than t entries which are units in S and $f_1 : S^n \to S$ is any map, then the map $f : S^{2n} \to S$, $(x, y) \mapsto x \cdot f_0(y) + f_1(y)$ is a t-resilient map. In particular the map $f_0 = \phi : S^n \to S^n$ defined by the relation (8), produces t-resilient maps, with $t < n$.

Let $n \in \mathbb{Z}^+$ be another positive integer, and $f : S^n \to S$ a t-resilient map. The following assertions hold:

- For $a \in S - pS$, map $S^n \to S$, $x \mapsto a\, f(x)$, is t-resilient, hence it is also balanced.
- For $a \in S - pS$, map $S^n \to S$, $x \mapsto T_{S/\mathbb{Z}_{p^s}}(a\, f(x))$, is balanced (as composition of balanced maps).
- Whenever the entries of $b \in S^n - \{0\}$ are units or zero, i.e., $b \in U(S)^n - \{0\}$, $S^n \to S$, $x \mapsto T_{S/\mathbb{Z}_{p^s}}(b \cdot x)$, is balanced.
- As shown in [2]:

$$\zeta_{af}(b) = \sum_{x\in S^n} e^{\frac{2\pi}{p^s} i\, T_{S/\mathbb{Z}_{p^s}}(a\, f(x) + b\cdot x)} = 0.$$

  whenever $a \in U(R)$, $b \in U(S)^n$, with $w_H(b) \leq t$, and $(a, b) \neq (0, 0)$.
- As a more general result than Corollary 2 at [17] we have that

$$\gamma_{abf} : S^n \to R\ ,\ \gamma_{abf} : x \mapsto T_{S/R}(a\, f(x) + b \cdot x). \tag{15}$$

  is balanced whenever $a \in R - pR$, $b \in U(S)^n$, and $w_H(b) \leq t$.

Proposition 5 *Let us assume one of the following conditions:*

1. $a \in U(R)$, $b \in U(S)^n$, $w_H(b) \leq t$ *and* $(a, b) \notin (0, 0)$, *or*
2. $a \in R - pR$, $b \in S^n$ *and* $w_H(b) \leq t$.

Then for any $u \in R$*:*

$$\text{card}\left(\gamma_{abf}^{-1}(u)\right) = q^{s(mn-1)}. \tag{16}$$

Proof Under the stated conditions, γ_{abf} is balanced, hence (16) holds for each $u \in R$. □

Let us recall the important notion of *bent functions* in Galois rings.

Let $n, m \in \mathbb{N}$, $n \geq 2m$, n even. A map $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *bent* if

$$\forall b \in \mathbb{F}_2^n,\ a \in \mathbb{F}_2^m - \{0\} :\ |\hat{\zeta}_{a\cdot f}(b)| = 2^{\frac{n}{2}} \tag{17}$$

where

$$\hat{\zeta}_{a\cdot f}(b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a\cdot f(x)+b\cdot x}.$$

This definition is extended to finite fields of odd prime characteristic [8] and to Galois rings [2]. We recall that the *perfectly non-linear maps* are those whose derivatives are balanced, and the *almost-perfectly non-linear* maps are characterized by $\{0, 2\}$-valued derivatives. The perfectly non-linear maps are equivalent to bent maps, however it is not the case in Galois rings. For odd n and $m = n$, the *almost-bent* maps [5] are $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$\forall b \in \mathbb{F}_2^n,\ a \in \mathbb{F}_2^n - \{0\} :\ |\hat{\zeta}_{a\cdot f}(b)| \leq 2^{\frac{n+1}{2}}. \tag{18}$$

Almost-bent maps are almost-perfectly non-linear, although the converse does not hold. At [4] a family of bent maps is produced in Galois rings of characteristic p^2. Although up to now we have failed in providing a bent map in Galois rings with characteristic p^s, with $s > 2$, we are going to introduce now a family of more general maps, useful for the construction of systematic authentication codes.

Let us now introduce an useful class of maps for systematic authentication codes. At [4] there was introduced a class of bent maps over Galois rings of characteristic p^2. Let us introduce a class of maps defined over Galois rings of characteristic p^s, with $s \geq 2$, that, although they are not bent, they preserve some of the bent maps properties quite useful in the context of systematic authentication codes.

Let p be a prime number, $s, \ell \in \mathbb{Z}^+$two positive integers, and $q = p^\ell$. Let us consider the Galois ring $R = \mathrm{GR}\,(p^s, \ell)$. $T(R) = \{0\} \cup \left(\xi^j\right)_{j=0}^{q-2}$ is a set of Teichmüller representatives at R.

For any map $f : R \to R$ and $a \in R - \{0\}$, the Fourier transform of af is

$$b \mapsto \zeta_{af}(b) = \sum_{x \in R} e^{\frac{2\pi}{p^s}\, i\, T_{R/\mathbb{Z}_{p^s}}(a\, f(x) - bx)}.$$

From the p-adic representation,

$$\forall x \in R\ \exists t = (t_0, \ldots, t_{s-1}) \in T(R)^s :\ x = \sum_{j=0}^{s-1} t_j p^j.$$

For any unit $u \in R$ we have:

$$\begin{aligned}
\sum_{t \in T(R)^{s-1}} e^{\frac{2\pi}{p^{s-1}}\, i\, T_{R/\mathbb{Z}_{p^s}}\left(u\left(\sum_{j=0}^{s-2} t_j p^j\right)\right)} &= \sum_{t \in T(R)^{s-1}} e^{\frac{2\pi}{p^s}\, i\, T_{R/\mathbb{Z}_{p^s}}\left(u\left(\sum_{j=1}^{s-1} t_j p^j\right)\right)} \\
&= \sum_{r \in pR} e^{\frac{2\pi}{p^s}\, i\, T_{R/\mathbb{Z}_{p^s}}(u\, r)} \\
&= 0
\end{aligned} \tag{19}$$

In a similar way as for the cyclic multiplicative group of a finite field, we also have:

Remark 1 Let $r \in \mathbb{Z}^+$ be such that $(r, p^\ell - 1) = 1$. Then $\mathbb{F}_{p^\ell} \to \mathbb{F}_{p^\ell}$, $y \mapsto f(y) = y^r$, is a polynomial permutation on $\mathbb{F}_{p^m}$ [12]. Under the same conditions, $T(R) \to T(R)$, $y \mapsto Y^r$, is a permutation on the set $T(R)$ of Teichmüller representatives.

Proposition 6 *Let $R = \mathrm{GR}(p^s, \ell)$ be the Galois ring, extension of order ℓ of $\mathbb{Z}_{p^s}$, with $p \geq s$. Let r be an exponent relative prime with $q-1$, $(r, q-1) = 1$, and $c \in R$. Let us consider*

$$f : R \to R \ , \ x \mapsto f(x) = x^{pr+1} + cx^p. \tag{20}$$

Then, for any $u \in T(R)$, the map uf is such that for any $b \in T(R)$ the absolute value of the Fourier transform of uf at b satisfies:

$$|\zeta_{uf}(b)| = q^{s-1}. \tag{21}$$

Proof Using the p-adic representation, for any $x = \sum_{j=0}^{s-1} t_j p^j \in R$, $t \in T(R)^s$, and any $u, b \in T(R)$:

$$\begin{aligned}
uf(x) - bx &= u\left[\left(\sum_{j=0}^{s-1} t_j p^j\right)^{pr}\left(\sum_{j=0}^{s-1} t_j p^j\right) + c\left(\sum_{j=0}^{s-1} t_j p^j\right)^{p}\right] - b\sum_{j=0}^{s-1} t_j p^j \\
&= u\left[t_0^{pr}\left(\sum_{j=0}^{s-1} t_j p^j\right) + ct_0^p\right] - b\sum_{j=0}^{s-1} t_j p^j \\
&= u\left[t_0^{pr+1} + ct_0^p\right] - bt_0 + ut_0^{pr}\sum_{j=1}^{s-1} t_j p^j - b\sum_{j=1}^{s-1} t_j p^j \\
&= u\left[t_0^{pr+1} + ct_0^p\right] - bt_0 + u\left(t_0^{pr} - d\right)\sum_{j=1}^{s-1} t_j p^j \\
&= \left[uf(t_0) - bt_0\right] + u\left(t_0^{pr} - d\right)\sum_{j=1}^{s-1} t_j p^j
\end{aligned}$$

with $d = u^{-1}b \in T(R)$. Thus,

$$\begin{aligned}
&\sum_{x \in R} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(uf(x) - bx)} \\
&= \sum_{(t_0, t) \in T(R) \times T(R)^{s-1}} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}\left(\left[uf(t_0) - bt_0\right] + u\left(t_0^{pr} - d\right)\sum_{j=1}^{s-1} t_j p^j\right)} \\
&= \sum_{t_0 \in T(R)} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(uf(t_0) - bt_0)}\, \Xi(t_0, t, d)
\end{aligned} \tag{22}$$

where

$$\Xi(t_0,t,d)=\sum_{t\in T(R)^{s-1}} e^{\frac{2\pi}{p^s}\,i\,T_{R/\mathbb{Z}_{p^s}}\left(u\left(t_0^{pr}-d\right)\sum_{j=1}^{s-1}t_j p^j\right)}.$$

Since $(r,q-1)=1$, we have also $(pr,q-1)=1$, hence $\tau\mapsto\tau^{pr}$ determines a permutation on $T(R)$ according to the remark 1.

Since $d\in T(R)$, then there is exactly one index t_0 such that $t_0^{pr}=d$, namely $t_0=d^{\frac{1}{pr}}$, and for this one we have $\Xi(t_0,t,d)=(q)^{s-1}$. For any other values of t_0, we have that $u\,(t_0^{pr}-d)$ is an unit in R, thus, from (19) we have $\Xi(t_0,t,d)=0$. Consequently, from (22) we have:

$$\sum_{x\in R} e^{\frac{2\pi}{p^s}\,i\,T_{R/\mathbb{Z}_{p^s}}(uf(x)-bx)}=q^{s-1}\left[e^{\frac{2\pi}{p^s}\,i\,T_{R/\mathbb{Z}_{p^s}}\left(u\left[d^{\frac{pr+1}{pr}}+cd^{\frac{p}{pr}}\right]-bd^{\frac{1}{pr}}\right)}\right].$$

By taking absolute value we have $|\zeta_{uf}(b)|=q^{s-1}$. □

4.2 A first authentication code on Galois rings

Let p be a prime number, $s,\ell,m\in\mathbb{Z}^+$ positive integers, and $q=p^\ell$. Let $R=\mathrm{GR}\,(p^s,\ell)$ and $S=\mathrm{GR}\,(p^s,\ell m)$ be the corresponding Galois rings, $T_{S/R}:S\to R$ the trace map and $U(S)=(S-pS)\cup\{0\}$ the set of elements at S that are either units or zero. Let $T(S)$ be a set of Teichmüller representatives at S.

Let $n\in\mathbb{Z}^+$ be another positive integer and for each $i<n$ let $e_i=(\delta_{ij})_{j=0}^{n-1}\in S^n$, where δ_{ij} is Kroenecker's delta. Let $f:S^n\to S$ be a t-resilient map, $t\le n$.

For any $b=(b_0,\ldots,b_{m-1})\in U(S)^n$, let

$$X_{b,t}=\{\sum_{j=0}^{t-2}b_je_j,b_{t-1}e_{t-1},\ldots,b_{n-1}e_{n-1}\}\subset S^n,$$

then $\mathrm{card}\,(X_{b,t})=n-t+1$. Let

$$(Src,T,K)=\left(T(S)\times\bigcup_{b\in T(S)^n}X_{b,t}\ ,\ R\ ,\ S^n\times R\right)\tag{23}$$

From relation (23) we have

$$\begin{aligned}\mathrm{card}\,(Src)&=q^m\left[q^{m(t-1)}+(n-t+1)q^m\right]\\ \mathrm{card}\,(T)&=q^s\\ \mathrm{card}\,(K)&=q^{s(mn+1)},\end{aligned}\tag{24}$$

here, the cardinality of the source space Src, expressed by eq. (24), does not depend on the exponent s at the characteristic p^s of the Galois ring S. We define the following encoding maps: $\forall k=(k_0,k_1)\in S^n\times R$,

$$e_k:s=(s_0,s_1)\mapsto T_{S/R}\,(s_0\,f(k_0)+s_1\cdot k_0)+k_1,\tag{25}$$

namely, $\forall k = (k_0, k_1) \in S^n \times R\,,\ \forall s = (s_0, s_1) \in T(S) \times \bigcup_{b \in T(S)^n} X_{b,t}$:

$$e_k(s) = \gamma_{s_0 s_1 f}(k_0) + k_1,$$

according to (15).

Proposition 7 *Map $k \mapsto e_k$ defined by the relation (25) is one-to-one.*

Proof Namely, let us assume $e_k = e_{k'}$ for two keys $k = (k_0, k_1), k' = (k'_0, k'_1) \in S^n \times R$. Evaluation at $s = (0, 0)$ produces, according to (25),

$$k_1 = e_k(0,0) = e_{k'}(0,0) = k'_1$$

consequently, $\forall s = (s_0, s_1) \in T(S) \times \bigcup_{b \in T(S)^n} X_{b,t}$:

$$0 = T_{S/R}\left(s_0\left(f(k_0) - f(k'_0)\right) + s_1 \cdot (k_0 - k'_0)\right),$$

hence, in particular, for $s_0 = 0$,

$$\forall s_1 \in \bigcup_{b \in T(S)^n} X_{b,t}\ :\ 0 = T_{S/R}\left(s_1 \cdot (k_0 - k'_0)\right),$$

thus necessarily $k_0 = k'_0$, and $k = k'$. □

Proposition 8 *For the authentication code defined by relations (23) and (25) the following equations hold:*

$$p_I = \frac{1}{q^s} \quad , \quad p_S = \frac{1}{q^s}. \tag{26}$$

Proof Let us determine the impersonation probability p_I according to (1). For any $s \in Src = T(S) \times \bigcup_{b \in T(S)^n} X_{b,t}$ consider the equivalence relation on the key space $K = S^n \times R$: $[k \sim_s k' \iff e_k(s) = e_{k'}(s)]$. For any $t \in T = R$, the map $(k_0, k_1) \mapsto (k_0, k_1 + t)$ determines a bijection among two equivalence classes, thus all equivalence classes have the same cardinality, namely $q^{smn} = \frac{1}{q^s}\,\mathrm{card}\,(K)$. From (1), we obtain $p_I = \frac{1}{q^s}$.

Now, let us determine the substitution probability p_S according to (2). For any $(s,t),(s',t') \in Src \times T$, with $s' = (s'_0, s'_1) \neq (s_0, s_1) = s$, we have $\forall k = (k_0, k_1) \in K$:

$$\left.\begin{array}{l}(e_k(s) = t)\ \&\\ (e_k(s') = t')\end{array}\right\} \iff \left\{\begin{array}{l}(\gamma_{s_0 s_1 f}(k_0) + k_1 = t)\ \&\\ \left(\gamma_{s_0 - s'_0, s_1 - s'_1, f}(k_0) = t - t'\right)\end{array}\right.$$

Thus, the numerator at the right side of (2) consists of the cardinality of inverse images of points under the map $k_0 \mapsto \gamma_{s_0 - s'_0, s_1 - s'_1, f}(k_0)$. Let us observe that $w_H(s_1 - s'_1) \leq t$, and $s_1 - s'_1 \in U(S)^n$ because $s_1, s'_1 \in T(S)^n$. Thus the conditions of the Proposition 5 are fulfilled. From relation (16), it follows that this numerator equals $q^{s(mn-1)}$. From (2), we obtain $p_S = \frac{1}{q^s}$. □

Observe that within this construction, the source space can be replaced by the space

$$S_b = T(S) \times \{b \in T(S)^n |\ w_H(b) \leq \frac{t}{2}\}$$

producing the same probability values as in (26).

4.3 A second authentication code on Galois rings

Let us introduce now a second systematic authentication code over Galois rings.

Let p be a prime number, $s, \ell, m \in \mathbb{Z}^+$ positive integers, $R = \mathrm{GR}(p^s, \ell)$ and $S = \mathrm{GR}(p^s, \ell m)$ the corresponding Galois rings. Let $f : S \to S$ be a map as in Proposition 6, defined by (20) but over the ring S.

Proposition 9 *Under the above conditions, for* $(a, b) \in T(S)^2 - \{(0, 0)\}$ *and* $u \in R$ *let*

$$C(a, b; u) = \{x \in S |\ T_{S/R}(af(x) + bx) = u\}$$
$$N(a, b; u) = \mathrm{card}\,(C(a, b; u))\,.$$

Then

$$N(a, b; u) \leq \frac{q^{(s+1)m} + q^{sm+1} - q^{sm}}{q^{m+1}}. \tag{27}$$

Proof Let us estimate

$$V := \mathrm{card}\,(R - pR)\ N(a, b; u) + (\mathrm{card}\,(S) - N(a, b; u))(-q^{s-1}).$$

We have,

$$\begin{aligned} V &\leq \sum_{x \in S} \sum_{y \in R - pR} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(y\,(T_{S/R}(af(x)+bx)-u))} \\ &= \sum_{y \in R - pR} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(-yu)} \sum_{x \in S} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(y\, T_{S/R}(af(x)+bx))} \\ &= \sum_{y \in R - pR} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(-yu)} \sum_{x \in S} e^{\frac{2\pi}{p^s} i\, T_{S/\mathbb{Z}_{p^s}}(y\,(af(x)+bx))}. \end{aligned}$$

Thus, taking absolute value at the last term in the above relations,

$$V \leq \sum_{y \in R - pR} \left| e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(-yu)} \right| \left| \sum_{x \in S} e^{\frac{2\pi}{p^s} i\, T_{S/\mathbb{Z}_{p^s}}(y\,(af(x)+bx))} \right|.$$

and from Proposition 6,

$$V \leq (q^s - q^{s-1}) q^{(s-1)m}.$$

Hence,

$$N(a, b; u) q^s - q^{s(m+1)-1} \leq (q^s - q^{s-1}) q^{(s-1)m}.$$

The result follows. □

After this digression, let us introduce the new systematic authentication code:

$$(Src, T, K) = \big(T(S)^2\ ,\ R\ ,\ S \times R\big) \tag{28}$$

From relation (28) we have

$$\begin{aligned} \operatorname{card}(Src) &= q^{2m} \\ \operatorname{card}(T) &= q^{s} \\ \operatorname{card}(K) &= q^{s(m+1)} \end{aligned} \tag{29}$$

also in this case we have that according to (29), the cardinality of the source space does not depend on the exponent s of the characteristic p^s of S. We observe also that in case $s = 2$, we have $\operatorname{card}(K) = \operatorname{card}(Src) \cdot \operatorname{card}(T)$. Let us define the following encoding maps: $\forall k = (k_0, k_1) \in S \times R$,

$$e_k : s = (s_0, s_1) \mapsto T_{S/R}\left(s_0\, f(k_0) + s_1 k_0\right) + k_1. \tag{30}$$

Proposition 10 *Map $k \mapsto e_k$ defined by the relation (30) is one-to-one.*

Proof Namely, let us suppose that for $k = (k_0, k_1), k' = (k'_0, k'_1) \in K$ we have $e_k = e_{k'}$. Then, evaluation at $s = (0, 0)$ gives $k_1 = k'_1$. Thus $\forall s = (s_0, s_1) \in Src$,

$$0 = T_{S/R}\left(s_0\left(f(k_0) - f(k'_0)\right) + s_1(k_0 - k'_0)\right)$$

in particular, for $s_0 = 0$,

$$\forall s_1 :\ 0 = T_{S/R}\left(s_1(k_0 - k'_0)\right).$$

Necessarily, $k_0 = k'_0$. □

Proposition 11 *For the authentication code defined by the relations (28) and (30) the following equations hold:*

$$p_I = \frac{1}{q^s} \quad , \quad p_S = \frac{1}{q} + \frac{q-1}{q^{m+1}}. \tag{31}$$

Proof Let us determine the impersonation probability p_I according to (1). For any $s \in Src$ consider the equivalence relation on the key space $K = S \times R$: $\left[k \sim_s k' \iff e_k(s) = e_{k'}(s)\right]$. For any $t \in T = R$, the map $(k_0, k_1) \mapsto (k_0, k_1 + t)$ determines a bijection between two equivalence classes, thus all equivalence classes have the same cardinality, namely q^{sm}. From (1), we obtain $p_I = \frac{1}{q^s}$.

Now, let us determine the substitution probability p_S according to (2). For any $(s, t), (s', t') \in Src \times T$, with $s' \neq s$, we have $\forall k = (k_0, k_1) \in K$:

$$\left.\begin{array}{l} (e_k(s) = t)\ \& \\ (e_k(s') = t') \end{array}\right\} \iff \left\{\begin{array}{l} (\gamma_{s_0 s_1 f}(k_0) + k_1 = t)\ \& \\ \left(\gamma_{s_0 - s'_0, s_1 - s'_1, f}(k_0) = t - t'\right) \end{array}\right.$$

Thus, the numerator at the right side of (2) consists of the cardinality of inverse images of points under the map $k_0 \mapsto T_{S/R}\left((s_0 - s'_0)\, f(k_0) + (s_1 - s'_1)k_0\right)$. By recalling Proposition 9 and the relation (27).

$$p_S = \frac{N(s_0 - s'_0, s_1 - s'_1; e_k(s) - e_k(s'))}{q^{sm}} \leq \frac{q^{(s+1)m} + q^{sm+1} - q^{sm}}{q^{m+1}} \cdot \frac{1}{q^{sm}}.$$

The result follows. □

5 Conclusions

Most of former authentication codes using bent maps over finite fields or almost-bent maps over finite fields or Galois rings show impersonation and substitution probabilities of successful attacks of the form

$$p_I = \frac{1}{q} + o\left(\frac{1}{q^{\varepsilon+\frac{m}{2}}}\right) \quad , \quad p_S = \frac{1}{q} + o\left(\frac{1}{q^{\varepsilon+\frac{m}{2}}}\right)$$

for some $\varepsilon > 0$, as in the above estimations (4), (5), (6), (7) quoted from [9] or as in the estimations appearing at [3,13]. The systematic authentication code using resilient maps over finite fields proposed here is improving these probabilities. The calculated probabilities at (14) are optimal, according with (3). Besides, in this case, within the authentication code proposed here, the resulting source spaces can be made much larger by a variation of the parameter n, the dimension of the involved vector arrays.

On the other hand, in the context of Galois rings, we also propose two systematic authentication codes, the first one based on t-resilient maps and the second code on a particular class of maps with "large curvature". The impersonation and substitution probabilities for the first code, calculated at (26) are optimal, according with (3), and they are indeed improving the corresponding values for the authentication codes formerly proposed at [4]. The bounds calculated at (31) for the second systematic authentication code do not improve the bounds at [4], however they coincide with these bounds for the special case $s = 2$. Also, the source spaces can be enlarged by a variation of the extension degree of the ring S with respect to R.

Since there are no known or reported bent maps for $s > 2$ and the codes defined by the relations (28)-(30) coincide with those built at [4], the construction presented here can be regarded as a generalization of the former construction at [4].

We do not consider optimality with respect to the size of the source space, the tagging space and the key space, with the criteria stated at [16]. Our optimality criteria are those at [6], where the introduced authentication codes use perfectly non-linear maps. At [10], a subcode of the Reed-Muller code generalized to first order is employed to build an authentication code such that the key space size is bounded by the product of the sizes of the source and tagging spaces. Our optimality criteria is in line with those at [6].

References

1. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210–229 (1988)
2. Carlet, C.: More correlation-immune and resilient functions over Galois fields and Galois rings. In: W. Fumy (ed.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 1233, pp. 422–433. Springer (1997)
3. Carlet, C., Ding, C., Niederreiter, H.: Authentication schemes from highly nonlinear functions. Des. Codes Cryptography **40**(1), 71–79 (2006)

4. Carlet, C., Ku-Cauich, J.C., Tapia-Recillas, H.: Bent functions on a Galois ring and systematic authentication codes. Adv. in Math. of Comm. **6**(2), 249–258 (2012)
5. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: Advances in Cryptology, EuroCrypt'94, pp. 356–365. Springer Berlin Heidelberg (1995)
6. Chanson, S.T., Ding, C., Salomaa, A.: Cartesian authentication codes from functions with optimal nonlinearity. Theor. Comput. Sci. **290**(3), 1737–1752 (2003). DOI 10.1016/S0304-3975(02)00077-4. URL http://dx.doi.org/10.1016/S0304-3975(02)00077-4
7. Chor, B., Goldreich, O., Håstad, J., Friedman, J., Rudich, S., Smolensky, R.: The bit extraction problem of t-resilient functions (preliminary version). In: FOCS, pp. 396–407. IEEE Computer Society (1985)
8. Coulter, R.S., Matthews, R.W.: Bent polynomials over finite fields. Bulletin of the Australian Mathematical Society **56**(03), 429–437 (1997)
9. Ding, C., Niederreiter, H.: Systematic authentication codes from highly nonlinear functions. IEEE Transactions on Information Theory **50**(10), 2421–2428 (2004)
10. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theoretical Computer Science **330**(1), 81 – 99 (2005). Insightful Theory
11. Hou, X.D.: p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields and Their Applications **10**(4), 566 – 582 (2004)
12. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics. Springer (1990)
13. Özbudak, F., Saygi, Z.: Some constructions of systematic authentication codes using Galois rings. Des. Codes Cryptography **41**(3), 343–357 (2006)
14. Rees Rolf S., S.D.R.: Combinatorial characterizations of authentication codes II. Designs, Codes and Cryptography **7**(3), 239–259 (1996). DOI 10.1023/A:1018094824862
15. Rueppel, R.: Analysis and design of stream ciphers. Communications and control engineering series. Springer (1986)
16. Stinson, D.R.: Combinatorial characterizations of authentication codes. Des. Codes Cryptography **2**(2), 175–187 (1992)
17. Zhang, X.M., Zheng, Y.: Cryptographically resilient functions. IEEE Transactions on Information Theory **43**(5), 1740–1747 (1997)