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

Authentication Schemes Based on Resilient Maps

Juan Carlos Ku-Cauich · Guillermo Morales-Luna

the date of receipt and acceptance should be inserted later

Abstract We introduce four constructions of systematic authentication codes. The first two are built over finite fields using resilient functions and they provide optimal impersonation and substitution probabilities. The 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. For the special case of characteristic p^2, those maps are bent indeed, and this case is subsumed by our general construction of characteristic p^s, with $s \geq 2$.

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

1 Introduction

Authentication codes have been extensively studied in the literature. Let us recall a basic setting [4]: A *systematic authentication code without secrecy* 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* $S \to T$.

A *transmitter* and a *receiver* agree a secret key $k \in K$. Whenever a source $s \in S$ should be sent, the participants proceed according to the following protocol:

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

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

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

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

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

At [4] there are introduced systematic authentication codes using perfect and almost-perfect non-linear functions. Namely, let $q = p^\ell$ be the power of a prime number and let $m \in \mathbb{Z}^+$.

Codes with perfect non-linear functions Let g be a perfect non-linear function. For the first code

$$(S, T, K) = \left(\mathbb{F}_{q^m}^2, \mathbb{F}_q, \mathbb{F}_{q^m} \times \mathbb{F}_q\right)$$

with $\forall k = (k_0, k_1) \in \mathbb{F}_{q^m} \times \mathbb{F}_q$,

$$e_k : s = (s_0, s_1) \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_0\, g(k_0) + s_1 k_0\right) + k_1,$$

the following bounds are obtained:

$$p_I = \frac{1}{q} \quad , \quad p_S \leq \frac{1}{q} + \frac{q-1}{q^{\frac{m+2}{2}}}. \tag{3}$$

For the second code

$$(S, T, K) = \left((\{1\} \times \mathbb{F}_{q^m}) \cup \{(0, 1)\}, \mathbb{F}_q, \mathbb{F}_{q^m}\right)$$

(the set S consists of representatives of the projective space $\mathrm{PG}(1, q^m)$ of dimension 1 over $\mathbb{F}_{q^m}$), with $\forall k \in \mathbb{F}_{q^m}$,

$$e_k : s = (s_0, s_1) \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_0\, g(k) + s_1 k\right),$$

the following bounds are obtained:

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

Codes with almost-perfect non-linear functions Let

$$\mathrm{in} : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \quad , \quad x \mapsto \begin{cases} x^{-1} & \text{if } x \in \mathbb{F}_{q^m}^* \\ 0 & \text{if } x = 0 \end{cases}.$$

For the first code

$$(S, T, K) = \left(\left(\mathbb{F}_{q^m}^* \times \mathbb{F}_{q^m} \times \{0\}\right) \cup \left(\{0\} \times \{0\} \times \mathbb{F}_{q^m}\right), \mathbb{F}_q, \mathbb{F}_{q^m} \times \mathbb{F}_q\right)$$

with $\forall k = (k_0, k_1) \in \mathbb{F}_{q^m} \times \mathbb{F}_q$,

$$e_k : s = (s_0, s_1, s_2) \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_0 \,\mathrm{in}(k_0 + s_1) + s_2 k_0\right) + k_1,$$

the following bounds are obtained:

$$p_I = \frac{1}{q} \quad , \quad p_S \leq \frac{1}{q} + \frac{1 + 2(q-1)(1 + q^{\frac{m}{2}})}{q^{m+1}}. \tag{5}$$

For the second code

$$(S, T, K) = \left(\left(\{1\} \times \mathbb{F}_{q^m}^2\right) \cup \{(0,1\}, \mathbb{F}_q, \mathbb{F}_{q^m}\right)$$

with $\forall k \in \mathbb{F}_{q^m}$,

$$e_k : s = (s_0, s_1) \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_0 \,\mathrm{in}(k) + s_1 k\right),$$

the following bounds are obtained:

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

2 Authentication schemes over finite fields

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

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

– As shown in [1,5]:

$$\zeta_{af}(b) = \sum_{x \in \mathbb{F}_{q^m}^n} e^{\frac{2\pi}{p}\, i\, T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(a\, f(x) + b \cdot x)} = 0. \tag{7}$$

– As a more general result than Corollary 2 at [7] we have that the map

$$\gamma_{abf} : \mathbb{F}_{q^m} \to \mathbb{F}_q \ , \ \gamma_{abf} : x \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\, f(x) + b \cdot x). \tag{8}$$

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* $u \in \mathbb{F}_{q^m}$*:*

$$\operatorname{card}\left(\gamma_{abf}^{-1}(u)\right) = q^{mn-1}. \tag{9}$$

Proof If $a = 0$ then (9) follows immediately.

If $a \neq 0$ then

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

since, by (7), $\sum_{x \in \mathbb{F}_{q^m}^n} e^{\frac{2\pi}{p} i T_{\mathbb{F}_{q^m}/\mathbb{F}_p}(ya\,f(x)+yb\cdot x)} = 0$. Hence, relation (9) follows. □

Let us construct two authentication schemes.

2.1 First construction

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

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

$$(S, T, K) = \left(\mathbb{F}_{q^m} \times \bigcup_{b \in \mathbb{F}_{q^m}^n} X_{b,t} \ , \ \mathbb{F}_q \ , \ \mathbb{F}_{q^m}^n \times \mathbb{F}_q \right). \tag{10}$$

From the relation (10) we have

$$\begin{aligned} \operatorname{card}(S) &= q^m \left[q^{m(t-1)} + (n-t)q^m \right] = q^{mt} + (n-t)q^{2m} \\ \operatorname{card}(T) &= q \\ \operatorname{card}(K) &= q^{mn+1} \end{aligned}$$

Let us define the following encoding maps: $\forall k = (k_0, k_1) \in \mathbb{F}_{q^m}^n \times \mathbb{F}_q$,

$$e_k : s = (s_0, s_1) \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0\,f(k_0) + s_1 \cdot k_0) + k_1, \tag{11}$$

namely, $\forall k = (k_0, k_1) \in \mathbb{F}_{q^m}^n \times \mathbb{F}_q$, $\forall s = (s_0, s_1) \in \mathbb{F}_{q^m} \times \bigcup_{b \in \mathbb{F}_{q^m}^n} X_{b,t}$:

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

according to (8).

Proposition 2 *The map $k \mapsto e_k$ defined by the relation (11) is one-to-one.*

Proof Namely, let us assume $e_k = e_{k'}$ for two keys $k = (k_0, k_1), k' = (k'_0, k'_1) \in \mathbb{F}_{q^m}^n \times \mathbb{F}_q$. Evaluation at $s = (0, 0)$ produces, according to (11),

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

consequently, $\forall s = (s_0, s_1) \in \mathbb{F}_{q^m} \times \bigcup_{b \in \mathbb{F}_{q^m}^n} X_{b,t}$:

$$0 = T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_0\left(f(k_0) - f(k'_0)\right) + s_1 \cdot (k_0 - k'_0)\right),$$

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

$$\forall s_1 \in \bigcup_{b \in \mathbb{F}_{q^m}^n} X_{b,t} \ : \ 0 = T_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(s_1 \cdot (k_0 - k'_0)\right),$$

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

Proposition 3 *For the authentication scheme defined by the relations (10)-(11) the following equations hold:*

$$p_I = \frac{1}{q} \quad , \quad p_S = \frac{1}{q}. \tag{12}$$

Proof Let us calculate the impersonation probability p_I according to (1). For any $s \in S = \mathbb{F}_{q^m} \times \bigcup_{b \in \mathbb{F}_{q^m}^n} X_{b,t}$ let us introduce the following equivalence relation on the key space $K = \mathbb{F}_{q^m}^n \times \mathbb{F}_q$: $\left[k \sim_s k' \iff e_k(s) = e_{k'}(s)\right]$. For any $t \in T = \mathbb{F}_q$, 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 $q^{mn} = \frac{1}{q}\,\mathrm{card}\,(K)$. From (1), we obtain $p_I = \frac{1}{q}$.

Now, let us calculate the substitution probability p_S according to (2). For any $(s,t), (s',t') \in S \times T$, 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 $k_0 \mapsto \gamma_{s_0 - s'_0, s_1 - s'_1, f}(k_0)$. Let us observe that $w_H(s_1 - s'_1) \leq t$, thus the conditions of the Proposition 1 are fulfilled. From relation (9), it follows that this numerator has value q^{mn-1}. From (2), we obtain $p_S = \frac{1}{q}$. □

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

$$S = \mathbb{F}_{q^m} \times \{b \in \mathbb{F}_{q^m}^n |\ w_H(b) \leq \frac{t}{2}\}$$

producing the same probability values as in (12).

2.2 Second construction

Let q be the power of a prime number, say $q = p^\ell$, and let $m \in \mathbb{Z}^+$ be a positive integer. Let $T_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be the trace map. Let $n \in \mathbb{Z}^+$ be another positive integer and let $e_i = (\delta_{ij})_{j=0}^{n-1}$ be 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 $b \in \mathbb{F}_{q^m}^n$, let $X_{b,t} = \{\sum_{j=0}^{t-2} b_j e_j, b_{t-1}e_{t-1}, \ldots, b_{n-1}e_{n-1}\} \subset \mathbb{F}_{q^m}^n$ and

$$(S, T, K) = \left(\left(\{1\} \times \bigcup_{b \in \mathbb{F}_{q^m}^n} X_{b,t} \right) \cup \left(\{0\} \times (e_j)_{j=0}^{n-1} \right) \ , \ \mathbb{F}_q \ , \ \mathbb{F}_{q^m}^n \right) \tag{13}$$

From the relation (13) we have

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

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

$$e_k : s = (s_0, s_1) \mapsto T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0 f(k) + s_1 \cdot k), \tag{14}$$

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 (8).

Proposition 4 *The map $k \mapsto e_k$ defined by the relation (14) 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

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

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

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

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

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

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

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

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

Proposition 5 *Let $s_0 = (s_{00}, s_{10}), s_1 = (s_{01}, s_{11}) \in S$ be two different points at S and let $t_0, t_1 \in \mathbb{F}_q$. Let*

$$\begin{aligned} C(f; s_0, s_1; t_0, t_1) &= \{k \in \mathbb{F}_{q^m}^n \mid (e_k(s_0) = t_0) \,\&\, (e_k(s_1) = t_1)\} \\ N(f; s_0, s_1; t_0, t_1) &= \operatorname{card}(C(f; s_0, s_1; t_0, t_1)). \end{aligned}$$

Then $N(f; s_0, s_1; t_0, t_1) = q^{mn-2}$.

Proof Through a direct calculation,

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

where

$$
\begin{aligned}
\mathrm{smnd}^{(0)}_{y_0 y_1 x} &= \exp\left[\frac{2\pi}{p}\, i\, T_{\mathbb{F}_q/\mathbb{F}_p} \big(y_0\, (T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_{00}\, f(x) + s_{10} \cdot x) - t_0) + \right. \\
&\qquad \left. y_1\, (T_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_{01}\, f(x) + s_{11} \cdot x) - t_1) \big) \right] \\
\mathrm{fctr}^{(1)}_{y_0 y_1 x} &= \exp\left[\frac{2\pi}{p}\, i\, T_{\mathbb{F}_{q^m}/\mathbb{F}_p} \left((y_0\, s_{00} + y_1\, s_{01})\, f(x) + (y_0\, s_{10} + y_1\, s_{11}) \cdot x \right) \right] \\
\mathrm{fctr}^{(2)}_{y_0 y_1} &= \exp\left[\frac{2\pi}{p}\, i\, T_{\mathbb{F}_q/\mathbb{F}_p} \left(-y_0 t_0 - y_1 t_1 \right) \right],
\end{aligned}
$$

because, by (7), $\sum_{x \in \mathbb{F}_{q^m}^n} \mathrm{fctr}^{(1)}_{y_0 y_1 x} = 0$.

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 6 *For the authentication scheme defined by the relations (13)-(14) the following equations hold:*

$$
p_I = \frac{1}{q} \quad , \quad p_S = \frac{1}{q}. \tag{15}
$$

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

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

producing the same probability values as in (15).

3 Authentication schemes over Galois rings

Let p be a prime number, and let $s, \ell, m \in \mathbb{Z}^+$ be positive integers, let $q = p^\ell$. 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. Let $T_{S/R} : S \to R$, $T_{S/\mathbb{Z}_{p^s}} : S \to \mathbb{Z}_{p^s}$ and $T_{R/\mathbb{Z}_{p^s}} : R \to \mathbb{Z}_{p^s}$ be the corresponding trace maps, and let pR and pS denote the sets of zero divisors of R and S. 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 [6]:

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 [1], 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

$$f_0 : \left(\sum_{i=0}^{s-1} a_{i0} p^i, \ldots, \sum_{i=0}^{s-1} a_{i,n-1} p^i \right) \mapsto (a_{00}, \ldots, a_{0,n-1})$$

specified through the p-adic representation of elements at S, produces t-resilient maps, with $t < n$.

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

- For $a \in S - pS$, the map $S^n \to S$, $x \mapsto a\, f(x)$, is t-resilient, hence it is also balanced.

- For $a \in S - pS$, the 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. $b \in U(S)^n - \{0\}$, the map $S^n \to S$, $x \mapsto T_{S/\mathbb{Z}_{p^s}}(b \cdot x)$, is balanced.
- As shown in [1]:

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

  whenever $a \in U(S)$ and $b \in U(S)^n$ with $w_H(b) \leq t$ and $(a, b) \neq (0, 0)$.
- As a more general result than Corollary 2 at [7] we have that the map

$$\gamma_{abf} : S^n \to R\ ,\ \gamma_{abf} : x \mapsto T_{S/R}(a\, f(x) + b \cdot x). \tag{16}$$

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

Proposition 7 *Let us assume one of the following conditions:*

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

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

$$\text{card}\left(\gamma_{abf}^{-1}(u)\right) = q^{s(mn-1)}. \tag{17}$$

Proof Under the sated conditions, the map γ_{abf} is balanced, hence (17) holds for each $u \in R$. □

3.1 A first authentication scheme

Let us proceed in an analogous way as in Section 2.1. Let p be a prime number, and let $s, \ell, m \in \mathbb{Z}^+$ be positive integers, and let $q = p^\ell$. Let $R = \text{GR}\,(p^s, \ell)$ and $S = \text{GR}\,(p^s, \ell m)$ be the corresponding Galois rings. Let $T_{S/R} : S \to R$ be the trace map. Let $U(S) = (S - pS) \cup \{0\}$ be the set of elements at S that are either units or zero and let $T(S)$ be a set of Teichmüller representatives at S.

Let $n \in \mathbb{Z}^+$ be another positive integer and let $e_i = (\delta_{ij})_{j=0}^{n-1}$ be the i-th vector in the canonical basis of S^n. Let $f : S^n \to S$ be a t-resilient map, $t \leq n$.

For any $b \in U(S)^n$, let $X_{b,t} = \{\sum_{j=0}^{t-2} b_j e_j, b_{t-1} e_{t-1}, \ldots, b_{n-1} e_{n-1}\} \subset S^n$ and

$$(S_a, T, K) = \left(T(S) \times \bigcup_{b \in T(S)^n} X_{b,t}\ ,\ R\ ,\ S^n \times R \right) \tag{18}$$

From the relation (18) we have

$$\begin{aligned} \text{card}\,(S_a) &= q^m \left[q^{m(t-1)} + (n-t) q^m \right] \\ \text{card}\,(T) &= q^s \\ \text{card}\,(K) &= q^{s(mn+1)}, \end{aligned} \tag{19}$$

here, the cardinality of the source space S_a, expressed by eq. (19), does not depend on the exponent s at the characteristic p^s of the Galois ring S. Let us define the following encoding maps: $\forall k = (k_0, k_1) \in S^n \times R$,

$$e_k : s = (s_0, s_1) \mapsto T_{S/R}\left(s_0\, f(k_0) + s_1 \cdot k_0\right) + k_1, \tag{20}$$

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 (16).

Proposition 8 *The map $k \mapsto e_k$ defined by the relation (20) is one-to-one.*

Proof The proof follows the same argumentation lines as the proof of Proposition 2. □

Proposition 9 *For the authentication scheme defined by the relations (18) and (20) the following equations hold:*

$$p_I = \frac{1}{q^s} \quad , \quad p_S = \frac{1}{q^s}. \tag{21}$$

Proof Also in this proof we may follow the same argumentation lines as in Proposition 3.

Let us calculate the impersonation probability p_I according to (1). For any $s \in S_a = T(S) \times \bigcup_{b \in T(S)^n} X_{b,t}$ 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 calculate the substitution probability p_S according to (2). For any $(s,t), (s',t') \in S_a \times T$, 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 $k_0 \mapsto \gamma_{s_0 - s'_0, s_1 - s'_1, f}(k_0)$. 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 1 are fulfilled. From relation (17), it follows that this numerator has value $q^{s(mn-1)}$. 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 (21).

3.2 A second authentication scheme

Let us begin this section by introducing an useful class of maps for systematic authentication codes. At [3] 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 and let $s, \ell \in \mathbb{Z}^+$ be two positive integers, let $q = p^\ell$. Let us consider the Galois ring $R = \mathrm{GR}(p^s, \ell)$. Let $T(R) = \{0\} \cup \left(\xi^j\right)_{j=0}^{q-2}$ be a set of Teichmüller representatives at R. 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:

$$\begin{aligned} \sum_{t \in T(R)^{s-1}} e^{\frac{2\pi}{p^{s-1}} i \, T_{R/\mathbb{Z}_{p^s}}\left(u \left(\sum_{j=0}^{s-2} t_j p^j\right)\right)} &= \sum_{t \in T(R)^{s-1}} e^{\frac{2\pi}{p^s} i \, T_{R/\mathbb{Z}_{p^s}}\left(u \left(\sum_{j=1}^{s-1} t_j p^j\right)\right)} \\ &= \sum_{r \in pR} e^{\frac{2\pi}{p^s} i \, T_{R/\mathbb{Z}_{p^s}}(u\, r)} \\ &= 0 \end{aligned} \tag{22}$$

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

> Whenever $(r, q-1) = 1$, the map $y \mapsto y^r$ determines a permutation on $T(R)$. (23)

Proposition 10 *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 $q-1$, $(r, q-1) = 1$, let $c \in R$ and let us consider the map*

$$f : R \to R \; , \; x \mapsto f(x) = x^{pr+1} + cx^p. \tag{24}$$

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

$$|\zeta_{af}(b)| \in \{0, q^{s-1}\}. \tag{25}$$

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 $b \in R$ and unit $u \in R$:

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

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

$$\begin{aligned}
&\sum_{x\in R} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(uf(x)-bx)} \\
&= \sum_{(t_0,t)\in T(R)\times T(R)^{s-1}} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}\left([uf(t_0)-bt_0]+u\left(t_0^{pr}-d\right)\sum_{j=1}^{s-1} t_j p^j\right)} \\
&= \sum_{t_0\in T(R)} e^{\frac{2\pi}{p^s} i\, T_{R/\mathbb{Z}_{p^s}}(uf(t_0)-bt_0)}\mathrm{smtn}_{t_0,t,d} \qquad (26)
\end{aligned}$$

where

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

Since $(r, q-1) = 1$, we have also $(pr, q-1) = 1$, hence the map $\tau \mapsto \tau^{pr}$ determines a permutation on $T(R)$ according to the remark (23).

Thus two cases appear.

If $d \in T(R)$, 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 $\mathrm{smtn}_{t_0,t,d} = (q)^{s-1}$. For any other values of t_0, we have that $u\left(t_0^{pr} - d\right)$ is an unit in R, thus, from (22) we have $\mathrm{smtn}_{t_0,t,d} = 0$. Consequently, from (26) 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 $|\zeta_{af}(b)| = q^{s-1}$.

If $d \notin T(R)$, then by (22), $|\zeta_{af}(b)| = 0$. □

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

Let p be a prime number, and let $s, \ell, m \in \mathbb{Z}^+$ be positive integers. Let $R = \mathrm{GR}(p^s, \ell)$ and $S = \mathrm{GR}(p^s, \ell m)$ be the corresponding Galois rings. Let $f : S \to S$ be a map as in Proposition 10, defined by (24) but over the ring S.

Proposition 11 *Under the above conditions, for $(a, b) \in U(S)^2 - \{(0, 0)\}$ 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 the Proposition 10,

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

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:

$$(S_a, T, K) = \left(T(S)^2\ ,\ R\ ,\ S \times R\right) \tag{28}$$

From the relation (28) we have

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

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. 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 12 *The 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 $\forall s = (s_0, s_1) \in S_a$,

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

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 13 *For the authentication scheme 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 Also in this proof we may follow the same argumentation lines as in Proposition 3.

Let us calculate the impersonation probability p_I according to (1). For any $s \in S_a$ 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 among 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 calculate the substitution probability p_S according to (2). For any $(s, t), (s', t') \in S_a \times T$, 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 the Proposition 11 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. □

4 Conclusions

Most of former authentication schemes using resilient maps over finite fields 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 (3), (4), (5), (6) quoted from [4] or as in the estimations appearing at [2,6]. The two systematic authentication codes using resilient maps over finite fields proposed here are improving these probabilities. The calculated probabilities at (12) and (15) are optimal. Besides, in this case, within the authentication codes 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 (21) are optimal, and they are indeed improving the corresponding values for the authentication schemes formerly proposed at [3]. The bounds calculated at (31) for the second systematic authentication code do not improve the bounds at [3], 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 bent maps for $s > 2$ and the codes defined by the relations (28)-(30) coincide with those built at [3], the construction presented here can be regarded as a generalization of the former construction at [3].

References

1. 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)
2. Carlet, C., Ding, C., Niederreiter, H.: Authentication schemes from highly nonlinear functions. Des. Codes Cryptography **40**(1), 71–79 (2006)
3. 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)
4. Ding, C., Niederreiter, H.: Systematic authentication codes from highly nonlinear functions. IEEE Transactions on Information Theory **50**(10), 2421–2428 (2004)
5. 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)
6. Özbudak, F., Saygi, Z.: Some constructions of systematic authentication codes using Galois rings. Des. Codes Cryptography **41**(3), 343–357 (2006)
7. Zhang, X.M., Zheng, Y.: Cryptographically resilient functions. IEEE Transactions on Information Theory **43**(5), 1740–1747 (1997)