Three authentication schemes based on finite fields and Galois rings

Juan Carlos Ku-Cauich · Miguel Angel Márquez-Hidalgo

Abstract We give three new systematic authentication schemes, two using Gray map, finite fields and Galois rings, and one using only Galois rings. In the first scheme, we increase the size and simplify the scheme's source space in [9]. In the second scheme, we reduce the key space of the first scheme. Finally, by not considering Gray map, used in the previous schemes, we give a third scheme on Galois rings, which generalizes the scheme over finite fields given in [8]. The introduced schemes obtain optimal impersonation and substitution probabilities.

Kewords: Authentication Schemwes, Galois Rings, Gray map

1 Introduction

The resilient maps were introduced in 1985 at [4] and, independently, at [1], in the context of key distribution and quantum cryptography protocols. Resilient maps have also been used in the generation of random sequences aimed to stream ciphering [11].

The systematic authentication schemes without secrecy are considered, for instance, in [5]. In these schemes, it is desired to obtain minimum probabilities in the impersonation and substitution attacks success. When optimal probabilities are reached, there are then inequalities regarding the size of the key space and the message space (see Theorems 2.3 and 3.1 in [12], and Theorem 14 in [2]).

The authors acknowledge the support of Mexican Conacyt

Juan Carlos Ku-Cauich
Computer Science, CINVESTAV-IPN, Mexico City, Mexico, E-mail: jcku@cs.cinvestav.mx

Miguel Angel Márquez-Hidalgo
Computer Science, CINVESTAV-IPN, Mexico City, Mexico, E-mail: mmarquez@computacion.cs.cinvestav.mx

In this work, in the three schemes, we obtain minimum values for the success probabilities of impersonation and substitution attacks, and the inequalities in the size of the spaces can be appreciated, being better in the construction 1 and 3 than the previous schemes given in [9] and [8] respectively (schemes that allow comparison).

In the first scheme, we simplify the scheme's source space in [9]. In that scheme, the source space is impractical, and the proof of injection between the key space and the encoding rules is very laborious, approximately eight pages. Here we use a source space with more elements (giving less difference between the key space and the message space), and at the same time, we simplify its structure, obtaining in this way a new simplified scheme. In the second scheme, we reduce first scheme's parameters, getting a smaller size of the space key. Finally, by not considering Gray map used in the previous schemes, we give a third scheme, only on Galois rings. This new authentication scheme is a generalization of the one provided, using finite fields, in [8].

In general, we work over two structures, Galois rings and finite fields, using the Gray map to relate these. Additionally, trace function and resilient functions are introduced in these schemes. Using the composition of all these functions we obtain different properties concerning the balanced as the Corollary 1, Theorem 9, Theorem 10 and Theorem 13.

The current code construction is in line with previously constructed codes using rational, non-degenerated and bent functions on Galois rings and compositions of maps and the generalized Gray map on Galois rings [6,7,10].

The paper is organized as follows: In Section 2 the Galois rings are reviewed, and the t-resilient functions and Gray maps definitions over these rings and finite fields are recalled. It also reviews the important properties of these functions. In Section 3, three authentication schemes without secrecy are introduced. Its main characteristics are resolved and compared with other schemes. In Section 3.1, the general authentication scheme without secrecy scheme is recalled. In the Section 3.2 a first authentication scheme using the map Gray is proposed. In Section 3.3 a second scheme using the Gray map also is presented, a modification of the first scheme. In the Section 3.4 a third construction only over Galois rigs is introduced. In the Section 4 the finally conclusion are presented.

2 Background

A monic polynomial $h(x) \in \mathbb{Z}_{p^s}[x]$ is called *monic basic irreducible* (*basic primitive*) if its reduction modulo p is an irreducible polynomial (primitive polynomial) over $\mathbb{F}_p$. The Galois ring of characteristic p^s and degree extension m, respect to $\mathbb{Z}_{p^s}$, can be write as:

$$\mathrm{GR}(p^s, m) = \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle,$$

where $h(x) \in \mathbb{Z}_{p^s}[x]$ is a monic basic irreducible polynomial of degree m and $\langle h(x)\rangle$ is the ideal of $\mathbb{Z}_{p^s}[x]$ generated by $h(x)$.

If $h(x)$ is a monic basic primitive polynomial, then it is possible to define the *Teichmüller set*

$$\mathcal{T}_{GR(p^s,m)} := \{0, 1, \xi, \ldots, \xi^{p^m-1}\}$$

and each element in $GR(p^s, m)$ can be written uniquely in a p-adic form,

$$\sum_{k=0}^{s-1} b_k p^k,$$

with $b_k \in \mathcal{T}_{GR(p^s,m)}$. For details we refer the reader to [14] and [15].

Definition 1 [13] Let $n \in \mathbb{Z}^+$, $J := \{j_0, ..., j_{t-1}\} \subset \{0, ..., n-1\}$. The affine J-variety determined by $a = (a_0, ..., a_{t-1}) \in \mathbb{F}_2^t$ is

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

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a functions, $m \leq n$.

1. The function f is J-resilient if $\forall a \in \mathbb{F}_2^t$, the function $f|_{V_{J,a,n}}$ is balanced.
2. The function f is t-resilient if it is J-resilient for any set J such that $|J| = t$.

The above definition is also given for finite fields of any characteristic and Galois rings [3].

Let m, n, s positive integers, p prime number. Let $S = GR(p^s, mn)$ and $R = GR(p^s, m)$ Galois rings of characteristic p^s, such that S is an extension of R of degree mn, R an extension of $\mathbb{Z}_{p^s}$ of degree m, and $f : S^r \to S$ a t-resilient function. We denote $S^\times = S - pS$, $U(S) = (S - pS) \cup \{0\}$. The following observations can be found in [9].

1. For $a \in S^\times$, the function $S^r \to S, x \mapsto af(x)$, is t-resilient.
2. For $a \in S^\times$, the function $S^r \to \mathbb{Z}_{p^s}, x \mapsto T_{S/R}(af(x))$, where $T_{S/R} : S \to R$ is the trace function, is a balanced function.
3. The function

$$\gamma_{abf} : S^r \to R,\ \gamma_{abf} : x \mapsto T_{S/R}(af(x) + b \cdot x)$$

is balanced whenever $w_H(b) \leq t$, $(a, b) \in U(S) \times (U(S))^r$, $(a, b) \neq (0, \mathbf{0})$.
4. The Fourier transform of the function af is

$$S^r \to \mathbb{C},\ b \mapsto \zeta_{af}(b),\ \zeta_{af}(b) = \sum_{x \in S^r} e^{\frac{2\pi}{p^s} i T_{S/R}(af(x) - b \cdot x)}.$$

Which satisfies that $\zeta_{af}(b) = 0$ because the function $x \mapsto T_{S/R}(af(x) + b \cdot x)$ is balanced under the same conditions as the above assertion.

Consider $q = p^m$. Let us recall neccesary facts [10]:

Lemma 1 [10] *Let $u \in R$. Then,*

$$\sum_{x\in R} e^{2\pi i T_{S/R}(ux)/p^s} = \begin{cases} q^s, & \text{si } u = 0, \\ 0, & \text{si } u \neq 0. \end{cases}$$

Definition 2 [10] Let $u \in R$,

$$s(u) := \sum_{x\in R-pR} e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(ux)/p^s} \text{ y } w_h(u) := -\frac{1}{q}s(u) + (q^{s-1} - q^{s-2}).$$

w_h is called the *homogeneous weight* at the ring R.

The homogeneous weight at R is given by

$$w_h(u) = \begin{cases} 0 & if\ u = 0 \\ q^{s-1} & if\ u \in p^{s-1}R\backslash\{0\} \\ q^{s-1} - q^{s-2} & if\ u \in R\backslash p^{s-1}R \end{cases}.$$

An essential tool since it provides a relationship between Galois rings and finite fields is the Gray function.

Definition 3 [6] The Gray map at R is

$$\begin{array}{ccc} \Phi : & R & \rightarrow & \mathbb{F}_q^{q^{s-1}} \\ & r_0 + r_1p + \cdots + r_{s-1}p^{s-1} & \rightarrow & \overline{r}_0c_0 + \overline{r}_1c_1 + \cdots + \overline{r}_{s-1}c_{s-1} \end{array},$$

$$c_i := (v + \delta_{i0}(u - v) \otimes \cdots \otimes v + \delta_{is-2}(u - v)), \quad i = 0, \ldots, s - 1,$$

and

$$v := (1, \ldots, 1) \in \mathbb{F}_q^q, u := (0, \overline{\eta}, \overline{\eta}^2, \ldots, \overline{\eta}^{q-1}) \in \mathbb{F}_q^q.$$

$$\mathcal{T}_R := \{0, 1, \eta, \ldots, \eta^{q-1}\},$$

Theorem 1 [6] *Let u, $v \in R$. Then*

$$d_h(u, v) = d_H(\Phi(u), \Phi(v)),$$

where d_H is the Hamming distance and $d_h = (u, v) = w_h(u - v)$.

□

There is an isometry between the Galois rings and the finite fields, considering the homogeneous distance and the Hamming distance.

Lemma 2 [9] *Let Φ be the Gray map at R. Then,*

$$\Phi(a + b) = \Phi(a) + \Phi(b),$$

for all $a \in R$ and $b \in p^{t-1}R$.

3 An authentication scheme without secrecy on Galois rings

3.1 A general scheme without secrecry

An authentication scheme [5] provides a method to ensure the integrity of the information when sent through a p-channel public. A transmitter and receiver share a secret key, which allows the receiver to verify that the message received is authentic. An authentication scheme (without secret) is a quadruple:

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E} = \{E_k : k \in \mathcal{K}\}),$$

where $\mathcal{S}$ is the source space, $\mathcal{T}$ the tag space, $\mathcal{K}$ the space key, and $E_k : \mathcal{S} \to \mathcal{T}$ the encoding rule. The sets $\mathcal{S}$, $\mathcal{T}$, and $\mathcal{K}$ are assumed to be finite and not empty. Additionally, the message space is defined, $\mathcal{M} := \mathcal{S} \times \mathcal{T}$.

A transmitter and the receiver share a secret key $k \in \mathcal{K}$. The transmitter wants to send a piece of information (called source) $s \in \mathcal{S}$ to the receiver, then the transmitter calculates $t = E_k(s) \in \mathcal{T}$ and inserts into the public channel the message m consisting of the ordered pair (s, t). The receiver, when receiving $m' = (s', t')$ calculates $E_k(s')$ and verifies if $E_k(s') = t'$; if so, the receiver accepts the message as authentic, otherwise the message is rejected. Since the communication channel is public, there is a risk that an intruder may deliberately observe, and cause a communication disturbance. It is assumed that the intruder can insert a message into the channel or replace the observed message m with another message m'. The success probabilities in these attacks (impersonation and substitution) denoted by P_I and P_S, are respectively [12].

$$P_I = \max_{s\in\mathcal{S}, t\in\mathcal{T}} \frac{|\{k \in \mathcal{K} : E_k(s) = t\}|}{|\mathcal{K}|} \tag{1}$$

$$p_S = \max_{(s,t)\in\mathcal{S}\times\mathcal{T}} \max_{(s',t')\in(\mathcal{S}-\{s\})\times\mathcal{T}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|} \tag{2}$$

Lower bounds are obtained for P_I y P_S [5]:

$$\frac{1}{|\mathcal{T}|} < P_I, \quad \frac{1}{|\mathcal{T}|} < P_S.$$

Relationships between the sizes of the spaces are given.

Theorem 2 [2] *Let $\mathcal{A}$ an authentication scheme without secrecy, then $|\mathcal{K}| \geq |\mathcal{S}|(|\mathcal{T}| - 1) + 1$ if $|\mathcal{S}| \geq |\mathcal{T}| + 1$. The authentication scheme is optimal if the equality $|\mathcal{K}| = |\mathcal{S}|(|\mathcal{T}| - 1) + 1$ if $|\mathcal{S}| \geq |\mathcal{T}| + 1$.*

3.2 A first construcction using Map Gray

We give an authentication scheme without secret. Encoding rules with domain in a Galois ring and image over a finite field, using Gray map, trace map, and resilient functions are given. We obtain minimum bounds in success probabilities in impersonation and substitution attacks.

In [9] there are a tedious source space and a long injection proof between key space and encoding maps, eight pages approximately. Here we simplify the source space increasing its number of elements, obtaining a better relation between message space and key space. The reader can see the link between the message space and key space in [12]. On the other hand, we reduce the injection proof of [9], mainly due to Theorem 3, Gray map properties, and the way of the new source space.

Let $n > s, p > 2$, and $L := \{l_0+l_1p+\cdots+l_{s-2}p^{s-2} \mid l_0,\ldots,l_{s-2} \in \mathcal{T}_R\}$. We can see that $\langle p^{s-1}\rangle = \{ap^{s-1} \mid a \in \mathcal{T}_R\}$. If $a, b \in L$, then $a-b \in (R\backslash p^{s-1}R) \cup \{0\}$.

Let $f : S^r \longrightarrow S$ a t-resilient function, $r, t \in \mathbb{Z}^+$, $r > t > 1$, $\Phi : R \to \mathbb{F}_q^{q^{s-1}}$ the Gray map. We build the following authentication scheme,

$$\mathcal{A}_1 = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}) : \tag{3}$$

$$\begin{aligned}
&\mathcal{S} := U(S) \times \{(b_1,\ldots,b_{t-1},0\ldots,0),(0,\ldots,0,b_t,0,\ldots,0),\ldots,(0,\ldots,0,b_r)\}\\
&\times L,\ b_i \in U(S), i=1,\ldots,r, \quad \text{if } (a,b,c) \in \mathcal{S}, (a,b) \neq 0,\\
&\mathcal{T} := \mathbb{F}_q,\\
&\mathcal{K} := \mathbb{Z}_{q^{s(nr+1)}},\\
&\mathcal{E} := \{E_k(s) = pr_k(u_s),\ k \in \mathcal{K}, s \in \mathcal{S}\}.
\end{aligned}$$

Where $s = (a, b, c) \in \mathcal{S}$, $\beta \in p^{s-1}R = \{\beta_1, \beta_2, \ldots, \beta_q\}$,

$$\begin{aligned}
v_{s,\beta}(x) &= \beta + T_{S/R}(af(x) + b \cdot x) + c,\\
u_{s,\beta} &= (\Phi(v_{s,\beta}(x)))_{x \in S^r},\\
u_s &= (u_{s,\beta})_{\beta \in p^{s-1}R},
\end{aligned}$$

and pr_k the projection function $\mathbb{Z}_q^{q^{s(nr+1)}}$ to $\mathbb{F}_q$, sending u_s to the k-th coordinate.

We can see that
$|\mathcal{S}| = \left[\left[(q^n-1)q^{n(s-1)}+1\right]\left[\left((q^n-1)q^{n(s-1)}+1\right)^{t-1}+W\right]-1\right] \cdot q^{s-1}$,
$|\mathcal{T}| = q$, $|\mathcal{K}| = |\mathcal{E}| = q^{s(nr+1)}$,
where,
$W = (r-t+1) \cdot \left[(q^n-1)q^{n(s-1)}+1\right]$.

The size of $\mathcal{S}$ is greater than the respective space in the first scheme given in [9] and the tag space is similar. Therefore, in this work $|\mathcal{K}|$ and $|\mathcal{S}|(|\mathcal{T}| - |)+1$ are closer, obtaining then, following the Theorem 2, a better relationship between the spaces.

Note that the source space can be considered as

$\mathcal{S} := \{a \in U(S)\} \times \{b \in S^r \mid b = (b_1, \ldots, b_r), b_i \in U(S), w_H(b) \leq \frac{t}{2} \times L,$
$(a, b) \neq 0,$

In this case $|\mathcal{S}| = \left[\left[\left((q^n - 1)q^{n(s-1)} + 1\right) \cdot W\right] - 1\right] \cdot q^{s-1}$,
where,
$W = C(r, 1)W_0 + C(r, 2)W_0^2 + \cdots + C(r, t/2)W_0^{t/2} + 1$.
$W_0 = (q^n - 1)q^{n(s-1)}$.

Before resolving the injection problem, we give the next results.

Theorem 3 *Let $n > s$, $a \in S$, $a \neq 0$, and $b \in p^{s-1}R$. Then exists an element $a_0 \in S^\times$ such that $T_{S/R}(a_0 a) = b$.*

Proof We know that $q^{n(s-1)}$ is the divisor's zero numbers of S. Given $b \in p^{s-1}R$, there are $(q^{sn}/q^s) = q^{sn-s}$ elements a in S such that $T_{S/R}(a) = b$. As $n > s$, then

$$q^{sn-s} = \frac{q^{sn}}{q^s} > \frac{q^{sn}}{q^n} = q^{sn-n} = q^{n(s-1)}.$$

Let $a \in S^\times$. Hence there is at least an element a_0 in $S^\times$ such that $T_{S/R}(a_0 a) = b$ if $b \in S$.

Let $a \in pS$, in particular $a = p^i a', 1 \leq i \leq s - 1$, $a' \in S^\times$. There is a_0 in $S^\times$ such that $T_{S/R}(a_0 a') = b_0$, $b_0 \in p^{s-i-1}R$.

$$T_{S/R}(a_0 a) = p^i T_{S/R}(a_0 a') = p^i b_0 = b \in p^{s-1}R.$$

□

We will consider Φ_w the value in the w coordinate of Φ, $1 \leq w \leq q^{s-1}$.

Remark 1 [9] Let $c = r_0 + r_1 p + \cdots + r_{s-2}p^{s-2} \in L$. Then

$$\Phi(c) = \overline{r}_0 c_0 + \overline{r}_1 c_1 + \cdots + \overline{r}_{s-2} c_{s-2}.$$

Consider two coordinates k, j of $\Phi(c)$.

If $k - j$ is not a multiple of q, then take c such that only $r_{s-2} \neq 0$. In this case $\Phi_k(c)$ and $\Phi_j(c)$ values are different.

If $k - j$ is multiple of q such that $q^i \leq k - j < q^{i+1}$, $i = 0, 1, \ldots, s - 2$ and $i + 1 + l = s - 1$, then take $c \in L$ such that only $r_l \neq 0$. In this case the two coordinates k and j of $\Phi(c)$ are different.

If $k - j$ is a multiple of q such that $k - j = q^{s-1}$, then take $c \in L$ such that only $r_0 \neq 0$. In this case $\Phi_k(c)$ and $\Phi_j(c)$ values are different.

Remark 2 If $q - 1$ be an even number and $\xi \in T_R$ be a generator, then $-\xi \in T_R$ or $-1 \in T_R$. In any case, if $x^d \in T_R$, $d \in \{1, \ldots, q - 1\}$, hence $-x^d \in T_R$, and then, if $a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} \in R$ in p-adic form, then $-a_0 - a_1 p - \cdots - a_{s-2}p^{s-2} \in R$ its a p-adic form too.

Theorem 4 *Let the function* $H : \mathcal{K} \longrightarrow \mathcal{E}$ *given by* $H(k) = E_k$. *Then* H *is a bijective function.*

Proof Note we need to prove the following:

Let $k_1 \neq k_2$ coordinates of u_s. If $pr_{k_1}(u_s) \neq pr_{k_2}(u_s)$ for an element $s \in \mathcal{S}$, then H is a bijective function.

We compare all the possibles coordinate pairs of u_s considering its length by parts. Let us consider 3 cases.

Caso 1: Two coordinates of $\Phi(v_{s,\beta}(x))$, $x \in S^r$, $\beta \in p^{s-1}R$.

Case 2: A coordinate of $\Phi(v_{s,\beta}(x))$ and a coordinate of $\Phi(v_{s,\beta}(y))$, $x \neq y$, $x, y \in S^r$, $\beta \in p^{s-1}R$.

Case 3: A coordinate of $\Phi(v_{s,\beta_i}(x))$ and a coordinate of $\Phi(v_{s,\beta_j}(y))$, $\beta_i \neq \beta_j$, $\beta_i, \beta_j \in p^{s-1}R$: two cases, $x = y$ and $x \neq y$.

Case 1:

Let $x \in S^r$ and the first two coordinates (a, b) of $\mathcal{S}$. If $T_{S/R}(af(x)+b\cdot x) = a_0 + \cdots + a_k p^k + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1}$, then for Remark 2 we can take $c = -a_0 + \cdots + c_k p^k + \cdots + (-a_{s-2}p^{s-2}) \in L$ such that,
if $a_k \neq 0$, then $c_k = 0$, therefore $T_{S/R}(af(x) + b \cdot x) + c = a_k p^k + a_{s-1}p^{s-1}$,
if $a_k = 0$, then $c_k \neq 0$, therefore $T_{S/R}(af(x) + b \cdot x) + c = c_k p^k + a_{s-1}p^{s-1}$.

Now, considering $s = (a, b, c) \in \mathcal{S}$. Since c is an arbitrary element, by Remark 1 and the Lemma 3.1, given two coordinates of $\Phi(v_{s,\beta}(x))$, $\beta \in p^{s-1}R$, these are distinct.

Case 2: In this case let us pick a coordinate of $\Phi(v_{s,\beta}(x))$ and a coordinate of $\Phi(v_{s,\beta}(y))$, $x \neq y$.

In a first place we consider the same coordinate w in $\Phi(v_{s,\beta}(x))$ and in $\Phi(v_{s,\beta}(y))$, that mean $\Phi_w(v_{s,\beta}(x))$ and $\Phi_w(v_{s,\beta}(y))$.

Let $a = 0$ and $c = 0$. We know that exists a k entry such that $x_k - y_x \neq 0$ (of $x - y$). By Theorem 3 we can choose an element $b \in (S - pS)^r$, $b_k \neq 0$, and $b_j = 0, j \neq k$ such that $T_{S/R}(b(x_k - y_k)) \in p^{s-1}R - \{0\}$. Hence, if $T_{S/R}(bx_k) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b_{s-1}p^{s-1}$ and $T_{S/R}(by_k) = b'_0 + b'_1 p + \cdots + b'_{s-2}p^{s-2} + b'_{s-1}p^{s-1}$, that implies $b_0 = b'_0, b_1 = b'_1, \ldots, b_{s-2} = b'_{s-2}$, $b_{s-1} \neq b'_{s-1}$, so that $\Phi_w(T_{S/R}(bx_k)) \neq \Phi_w(T_{S/R}(by_k))$. Thus $\Phi_w(v_{s,\beta}(x)) \neq \Phi_w(v_{s,\beta}(y))$, with $s = (0, b, 0)$.

Now, we consider distinct coordinates w_1, w_2. That mean, $\Phi_{w_1}(v_{s,\beta}(x))$ and $\Phi_{w_2}(v_{s,\beta}(y))$. In similar way to before, $T_{S/R}(bx_k) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b_{s-1}p^{s-1}$ and $T_{S/R}(by_k) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b'_{s-1}p^{s-1}$, $b_{s-1} \neq b'_{s-1}$. If $a = 0$ and $c = -b_0 - b_1 p - \cdots - b_{s-2}p^{s-2}$ (p-adic form by the Remark 2), then $\Phi_{w_1}(v_{s,\beta}(x)) = \Phi_{w_1}(\beta + b_{s-1}p^{s-1}) \neq \Phi_{w_2}(\beta + b'_{s-1}p^{s-1}) = \Phi_{w_2}(v_{s,\beta}(y))$.

Caso 3:

Let $\beta_i \neq \beta_j$, $\beta_i, \beta_j \in pR$, $(a, b, c) \in \mathcal{S}$. If $x = y$, $x, y \in S^r$, then, $\Phi_w(v_{s,\beta_i}(x)) \neq \Phi_w(v_{s,\beta_j}(y))$. In otherwise we would have $\beta_i = \beta_j$.

Les us consider two distinct elements w_1, w_2. Let an entry k of x, $x_k \neq 0$. Using the Theorem 3, there is a b such that $T_{S/R}(b_k x_k) \in p^{s-1}R$ (b_k, k-th coordinate of $b \in (S - pS)^r$) y $b_j = 0, j \neq k$; from here $\phi_{w_1}(b \cdot x) = \phi_{w_2}(b \cdot y)$. On the other side, $\phi_{w_1}(\beta_i) \neq \phi_{w_2}(\beta_j)$. Therefore $a = 0$ and $c = 0$, and using the Lemma 3.1, $\Phi_{w_1}(v_{s,\beta_i}(x)) \neq \Phi_w(v_{s,\beta_j}(y))$.

Consider now $x \neq y$, $a = 0$ and $c = 0$. Using Theorem 3, we know exists $b \in (S \backslash pS)^r$, such that $T_{S/R}(b_k(x_k - y_k)) = 0$, where $b_k \in S \backslash pS$ and $b_j = 0, j \neq k$. Then, by Lemma 3.1, $\Phi_w(v_{s,\beta_i}(x)) \neq \Phi_w(v_{s,\beta_j}(y))$.

Finally, the case $x \neq y$ and distinct coordinates. Let $a = 0$, and similar to above, we find $b_k \in S \backslash pS$ such that $T_{S/R}(b_k(x_k - y_k)) = 0$. Hence $T_{S/R}(b \cdot x) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b_{s-1}p^{s-1}$ and $T_{S/R}(b \cdot y) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b_{s-1}p^{s-1}$. Then, we consider, $c = -b_0 - b_1 p - \cdots - b_{s-2}p^{s-2}$. Therefore, using Lemma 3.1, $\Phi_{w_1}(v_{s,\beta_i}(x)) \neq \Phi_{w_2}(v_{s,\beta_j}(y))$.

The distinct before cases resolve the affirmation.

□

The procedure to obtain bound for P_I and P_S is similar to the Proposition 4 of [9]. We give this result for granted.

Theorem 5 *The scheme $\mathcal{A}_1$ satisfy,*

$$P_I = \frac{1}{q} \quad \textit{and} \quad P_S = \frac{1}{q}.$$

3.3 A second construction using Map Gray

In this authentication scheme, we remove a parameter from the first scheme, thus reducing the key space's size; however, is necessary reduce the size of the source space. We obtain minimum bounds in success probabilities in impersonation and substitution attacks.

To show that the minimum values for P_I y P_S are obtained, we find balanced properties of the Gray function and balance in the composition of the trace and resilient functions on Galois rings.

Let us recall that $S = GR(p^s, mn)$, $R = GR(p^s, m)$ and L as the scheme $\mathcal{A}_1$.

Let $f : S^r \longrightarrow S$ a t-resilient function, $p > 2$, $n > s$, $r, t \in \mathbb{Z}^+$, $r > t > 1$, $\Phi : R \rightarrow \mathbb{F}_q^{q^{s-1}}$ the Gray map. We build the following authentication scheme,

$$\mathcal{A}_2 = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}) : \tag{4}$$

$$\begin{aligned}
&\mathcal{S} := (\{1\} \times \{(b_1, \ldots, b_{t-1}, 0, \ldots, 0), (0, \ldots, 0, b_t, 0, \ldots, 0), \ldots, (0, \ldots, 0, b_r)\} \times L) \\
&\cup (\{0\} \times \{(b'_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, b'_r)\} \times L), \quad b_i \in U(S), b'_i \in S \backslash pS, \\
&i = 1, \ldots, r, \\
&\mathcal{T} := \mathbb{F}_q, \\
&\mathcal{K} = \mathbb{Z}_{q^{s(nr+1)-1}}, \\
&\mathcal{E} := \{E_k(s) = pr_k(u_s),\ k \in \mathcal{K}, s \in \mathcal{S}\}.
\end{aligned}$$

Where $s = (a, b, c) \in \mathcal{S}$,

$$\begin{aligned}
v_s(x) &= T_{S/R}(af(x) + b \cdot x) + c, \\
u_s &= (\Phi(v_s(x)))_{x \in S^r},
\end{aligned}$$

and pr_k the projection function $\mathbb{Z}_q^{q^{s(nr+1)-1}}$ to $\mathbb{F}_q$, sending u_s to the k-th coordinate.

We can see that $|\mathcal{S}| = \left[\left((q^n-1)q^{n(s-1)}+1\right)^{t-1} + W\right] \cdot q^{s-1}$, $|\mathcal{T}| = q$, $|\mathcal{K}| = |\mathcal{E}| = q^{s(nr+1)-1}$, where,

$W = (r-t+1)\cdot\left[(q^n-1)q^{n(s-1)}+1\right] + r(q^n-1)q^{n(s-1)}$.

Theorem 6 *Let the function $H : \mathcal{K} \longrightarrow \mathcal{E}$ given by $H(k) = E_k$. Then H is a bijective function.*

Proof Note we need to prove the following:

Let $k_1 \neq k_2$ coordinates of u_s. If $pr_{k_1}(u_s) \neq pr_{k_2}(u_s)$ for an element $s \in \mathcal{S}$, then H is a bijective function.

We compare all the possibles coordinate pairs of u_s considering its length by parts. Let us consider 2 cases.

Caso 1: Two coordinates of $\Phi(v_s(x))$, $x \in S^r$.

Case 2: A coordinate of $\Phi(v_s(x))$ and a coordinate of $\Phi(v_s(y))$, $x \neq y$, $x, y \in S^r$.

Case 1:

Let $x \in S^r$ and a fixed pair (a,b), first coordinates of $\mathcal{S}$.

If $T_{S/R}(af(x)+b\cdot x) = a_0 + \cdots + a_k p^k + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1}$, then for Remark 2, we can take $c = -a_0 + \cdots + c_k p^k + \cdots + (-a_{s-2}p^{s-2}) \in L$, such that,

if $a_k \neq 0$, then $c_k = 0$, therefore $T_{S/R}(af(x)+b\cdot x)+c = a_k p^k + a_{s-1}p^{s-1}$,

if $a_k = 0$, then $c_k \neq 0$, therefore $T_{S/R}(af(x)+b\cdot x)+c = c_k p^k + a_{s-1}p^{s-1}$.

Now, considering $s = (a,b,c) \in \mathcal{S}$. Since c is an arbitrary element, by Remark 1 and the Lemma 3.1, if we give two coordinates of $\Phi(v_s(x))$, these are distinct.

Case 2: In this case let us pick a coordinate of $\Phi(v_s(x))$ and a coordinate of $\Phi(v_s(y))$, $x \neq y$.

In a first place, we consider the same coordinate w in $\Phi(v_s(x))$ and in $\Phi(v_s(y))$, that mean $\Phi_w(v_s(x))$ and $\Phi_w(v_s(y))$.

Let $a = 0$ and $c = 0$. We know that exists a k entry such that $x_k - y_x \neq 0$ (of $x-y$). By Theorem 3, we can choose an element $b \in S^r$, $b_k \neq 0$, and $b_j = 0, j \neq k$ such that $T_{S/R}(b(x_k - y_k)) \in p^{s-1}R\backslash\{0\}$. Hence, if $T_{S/R}(bx_k) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b_{s-1}p^{s-1}$ and $T_{S/R}(by_k) = b'_0 + b'_1 p + \cdots + b'_{s-2}p^{s-2} + b'_{s-1}p^{s-1}$, that implies $b_0 = b'_0, b_1 = b'_1, \ldots, b_{s-2} = b'_{s-2}$, $b_{s-1} \neq b'_{s-1}$, so that $\Phi_w(T_{S/R}(bx_k)) \neq \Phi_w(T_{S/R}(by_k))$. Thus $\Phi_w(v_s(x)) \neq \Phi_w(v_s(y))$, with $s = (0,b,0)$ like before.

Now, we consider distinct coordinates w_1, w_2, that mean, $\Phi_{w_1}(v_s(x))$ and $\Phi_{w_2}(v_s(y))$. In similar way to above, $T_{S/R}(bx_k) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b_{s-1}p^{s-1}$ and $T_{S/R}(by_k) = b_0 + b_1 p + \cdots + b_{s-2}p^{s-2} + b'_{s-1}p^{s-1}$, $b_{s-1} \neq b'_{s-1}$. If $a = 0$ and $c = -b_0 - b_1 p - \cdots - b_{s-2}p^{s-2}$ (p-adic form by Remark 2), then $\Phi_{w_1}(v_s(x)) = \Phi_{w_1}(b_{s-1}p^{s-1}) \neq \Phi_{w_2}(b'_{s-1}p^{s-1}) = \Phi_{w_2}(v_s(y))$.

The two above cases resolve the afirmation.

□

In order to find P_I and P_S, we give the following results.

Let $c_i \in \mathbb{F}_q^{q-1}$ the vectors of Gray map given in Definition 3, $i = 0, \ldots, s-1$.

Theorem 7 *The sum of two or more elements of the vector set* $\{c_0, c_1, \ldots, c_{s-2}\}$ *as above has the form*

$$\left[[P_0(c_l')]_{q^{l-r-1}}, [P_1(c_l')]_{q^{l-r-1}}, \ldots, [P_{q-1}(c_l')]_{q^{l-r-1}}\right]_{q^r},$$

where,

$$c_l' = \left[[0]_{q^{s-l-2}}, [\xi]_{q^{s-l-2}}, \ldots, [\xi^{q-1}]_{q^{s-l-2}}\right],$$

P_i, $i = 0, 1, \ldots, q-1$ *are arbitrary permutations of the vectors* $[\zeta]_{q^{s-l-2}}$ *in* c_l', $\zeta \in \mathbb{F}_q$, *and* c_l *and* c_r *are the last and penultimate terms of the sum, respectively, in increasing order of the indices.*

Proof The claim is proved by mathematical induction.

Basis step:

If there are two summands, c_j and c_i, $j < i$, $j \in \{0, \ldots, s-3\}$, $i \in \{1, \ldots, s-2\}$. We know that,

$$c_j = \left[[0]_{q^{s-j-2}}, [\xi]_{q^{s-j-2}}, \ldots, [\xi^{q-1}]_{q^{s-j-2}}\right]_{q^j}$$

and

$$c_i = \left[[0]_{q^{s-i-2}}, [\xi]_{q^{s-i-2}}, \ldots, [\xi^{q-1}]_{q^{s-i-2}}\right]_{q^i}.$$

Note that,

$$c_i = \left[\left[\left[[0]_{q^{s-i-2}}, [\xi]_{q^{s-i-2}}, \ldots, [\xi^{q-1}]_{q^{s-i-2}}\right]_{q^{i-j-1}}\right]_q\right]_{q^j}.$$

Which indicates that each vector $[\zeta]_{q^{s-j-2}}$ of c_j has exactly q^{i-j-1} times the length of the vector c_i'. Then,

$$c_j + c_i = \left[[P0(c_i')]_{q^{i-j-1}}, [P\xi(c_i')]_{q^{i-j-1}}, \ldots, [P\xi^{q-1}(c_i')]_{q^{i-j-1}}\right]_{q^j},$$

$$P\zeta(c_i') = [\zeta]_{q^{s-j-2}} + [c_i']_{q^{i-j-1}} = \left[[\zeta+0]_{q^{s-i-2}}, [\zeta+\xi]_{q^{s-i-2}}, \ldots, [\zeta+\xi^{q-1}]_{q^{s-i-2}}\right],$$

$\zeta \in \{0, \xi, \ldots, \xi^{q-1}\}$.

Inductive step:

Suppose that we have the sum of $k-1$ vectors (the sum in increasing order with respect to indexes) of the set $\{c_0, c_1, \ldots, c_{s-2}\}$ of vectors of the Gray function, where the penultimate vector is r and the last is l:

$$\left[[P_0(c_l')]_{q^{l-r-1}}, [P_1(c_l')]_{q^{l-r-1}}, \ldots, [P_{q-1}(c_l')]_{q^{l-r-1}}\right]_{q^r}.$$

Now, a k-th vector, c_v, is added to the resulting sum above:

$$\left[[P_0(c_l')]_{q^{l-r-1}}, [P_1(c_l')]_{q^{l-r-1}}, \ldots, [P_{q-1}(c_l')]_{q^{l-r-1}}\right]_{q^r} + \left[\left[[c_v']_{q^{v-l}}\right]_{q^{l-r-1}q}\right]_{q^r}$$

$$= \left[[P0(P_0(c_l'))]_{q^{v-l-1}}, [P\xi(P_1(c_l'))]_{q^{v-l-1}}, \ldots, [P\xi^{q-1}(P_{q-1}(c_l'))]_{q^{v-l-1}}\right]_{q^l},$$

where

$$c_v = \left[\left[[c_v']_{q^{v-l-1}}\right]_q\right]_{q^l} = \left[\left[[c_v']_{q^{v-l}}\right]_{q^{l-r-1}q}\right]_{q^r}.$$

Observe that $[c_v']_{q^{v-l}}$ has length q^{s-l-1}. This completes the inductive step.

So by mathematical induction we prove the statement of the theorem.

□

Let $c_i \in \mathbb{F}_q^{q-1}$ the vectors of Gray map given in Definition 3, $i = 0, \ldots, s-1$.

Corollary 1 *Let $c_0, c_1, \ldots, c_{s-2}$, $s-1$ vectors of the Gray map as above. Then, in the sum of at most $s-1$ of those terms, every element $t \in \mathbb{F}_q$ is in q^{s-2} entries.*

Proof Consider a finite sum, such that the vectors c_v and c_l are the last and penultimate terms of the sum, respectively, in increasing order of the indices.

By the previous theorem, since the resulting vector is conformed by the permutations of the vectors $[\zeta]_{q^{s-l-2}}$ de c_v', and c_v is equal to

$$c_v = \left[\left[[c_v']_{q^{v-l-1}}\right]_q\right]_{q^l}$$

$$c_v' = \left[[0]_{q^{s-v-2}}, [\xi]_{q^{s-v-2}}, \ldots, [\xi^{q-1}]_{q^{s-v-2}}\right].$$

Then, the number of entries equal to a value $t \in \mathbb{F}_q$ is equal to q^{s-2}, being that each element $[\zeta]_{q^{s-v-2}}$ of c_v' is repeated $q^{v-l-1}qq^l = q^v$ times in c_v.

□

Corollary 2 *Let $c, c^\circ \in \{a_0c_0 + a_1c_1 + \cdots + a_{s-2}c_{s-2} \mid a_0, a_1, \ldots, a_{s-2} \in \mathcal{T}_R\}$, $c \neq c^\circ$. Then $\{k \in \mathbb{Z}_{q^{s-1}} \mid \Phi_k(c) = t, \Phi_k(c^\circ) = t'\} = q^{s-3}$.*

Proof By the proof of the Theorem 7, c y c° can be obtained from vectors c_j and c_i, $i, j \in \{0, 1, \ldots, s-2\}$, $j < i$, giving the respective permutations of vectors $[\zeta]_{q^{s-j-2}}$ of these, where

$$c_j = \left[[0]_{q^{s-j-2}}, [\xi]_{q^{s-j-2}}, \ldots, [\xi^{q-1}]_{q^{s-j-2}}\right]_{q^j}$$

and

$$c_i = \left[\left[\left[[0]_{q^{s-i-2}}, [\xi]_{q^{s-i-2}}, \ldots, [\xi^{q-1}]_{q^{s-i-2}}\right]_{q^{i-j-1}}\right]_q\right]_{q^j}.$$

We can see that any element in $\mathbb{F}_q$ is repeated in the same coordinates of c_i y c_j, $q^{s-i-2}q^{i-j-1}q^j = q^{s-j-3}$ times.

Note that unlike the Corollary 3, here the sum of the elements $c_0, c_1, \ldots, c_{s-2}$ have coefficients, but this does not represent a problem, since we would only have additionally permutations of elements of c and c°.

□

The following theorem is a generalization of Proposition 3 of [8], now on Galois rings.

Theorem 8 *Let $f : S^r \to S$ a t-resilient function and let $(a_1, b_1, c_1), (a_2, b_2, c_2) \in \mathcal{S}$ such that $(a_1, b_1) \neq (a_2, b_2)$, $u_1, u_2 \in R$ and*

$$\begin{aligned} &N(f; a_1, b_1, c_1, a_2, b_2, c_2; u_1, u_2) \\ &= |\{x \in S^r : T_{S/R}(a_1 f(x) + b_1 \cdot x) + c_1 = u_1, T_{S/R}(a_2 f(x) + b_2 \cdot x) + c_2 = u_2\}|. \end{aligned}$$

Then,

$$N(f; a_1, b_1, c_1, a_2, b_2, c_2; u_1, u_2) = q^{snr-2s}.$$

Proof There are the following equalities

$$\begin{aligned} &q^{2s} N(f; a_1, b_1, a_2, b_2; u_1, u_2) \\ &= \sum_{x \in S^r} \left[\sum_{y_1 \in R} e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(y_1(T_{S/R}(a_1 f(x)+b_1 \cdot x)+c_1-u_1))/p^s} \right] \\ &\left[\sum_{y_2 \in R} e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(y_2(T_{S/R}(a_2 f(x)+b_2 \cdot x)+c_2-u_2))/p^s} \right] \\ &= \sum_{x \in S^r} \sum_{y_1 \in R} \sum_{y_2 \in R} e^{2\pi i T_{R/\mathbb{Z}_{p^s}}\left(y_1(T_{S/R}(a_1 f(x)+b_1 \cdot x)+c_1-u_1)+y_2(T_{S/R}(a_2 f(x)+b_2 \cdot x)+c_2-u_2)\right)/p^s} \\ &= q^{snr} + \sum_{\substack{y_1, y_2 \in R \\ (y_1, y_2) \neq (0,0)}} \\ &e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(-y_1 u_1 - y_2 u_2 + y_1 c_1 + y_2 c_2)/p^s} \sum_{x \in S^r} e^{2\pi i T_{S/\mathbb{Z}_{p^s}}((y_1 a_1 + y_2 a_2) f(x) + (y_1 b_1 + y_2 b_2) \cdot x)/p^s} \\ &= q^{snr} + \sum_{\substack{y_1, y_2 \in R \\ (y_1, y_2) \neq (0,0)}} e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(-y_1 u_1 - y_2 u_2 + y_1 c_1 + y_2 c_2)/p^s} \sum_{(d_1, d_2, \ldots, d_t) \in S^t} \\ &\sum_{x \in S^r|_{x_1 = d_1, \ldots, x_t = d_t}} e^{2\pi i T_{S/\mathbb{Z}_{p^s}}((y_1 a_1 + y_2 a_2) f(x) + (y_1 b_1 + y_2 b_2) \cdot x)/p^s} \\ &= q^{snr} + \underset{q^{snt} \text{ times}}{0 + \cdots + 0} = q^{snr} \end{aligned}$$

The last equality is justified as follows:

Note that $y_1 b_1 + y_2 b_2$ y $y_1 a_1 + y_2 a_2$ cannot both be zero, unless $y_1 = y_2 = 0$, by the shape of the source space.

If $y_1 a_1 + y_2 a_2 = 0$ and $y_1 b_1 + y_2 b_2 \neq \mathbf{0}$, exists $z \in S^r$ such that $T_{S/\mathbb{Z}_{p^s}}((y_1 b_1 + y_2 b_2) \cdot z) \neq 0$. Then, similarly to the proof of Lemma 2.1 of [10].

$$\sum_{x \in S^r} e^{2\pi i T_{S/\mathbb{Z}_{p^s}}((y_1 b_1 + y_2 b_2) \cdot x)/p^s} = 0.$$

If $y_1a_1 + y_2a_2 \neq 0$ and $y_1b_1 + y_2b_2 = \mathbf{0}$, then, since $f(x)$ is balanced and by the Lemma 1,

$$\sum_{x \in S^r} e^{2\pi i T_{S/\mathbb{Z}_{p^s}}((y_1a_1+y_2a_2)f(x))/p^s} = 0.$$

Finally, if $y_1a_1 + y_2a_2 \neq 0$ y $y_1b_1 + y_2b_2 \neq \mathbf{0}$, assume, without loss of generality, that the nonzero entries of $y_1b_1 + y_2b_2$ are in the entries $x_1, \ldots, x_t$. Since, f is t-resilient, these t entries of S^r are kept constant, then,

$$f(x)_{|x_1=d_1,\ldots,x_t=d_t}$$

is balanced; even more, $(y_1b_1 + y_2b_2) \cdot x_{|x_1=a_1,\ldots,x_t=a_t}$ is constant, and also by Lemma 1 we have the last equality.

From here,

$$q^{2s}N(f; a_1, b_1, a_2, b_2; u_1, u_2) - q^{snr} = 0,$$

so that,

$$N(f; a_1, b_1, a_2, b_2; u_1, u_2) = q^{snr-2s}.$$

□

Theorem 9 *Let $\mathcal{S}, \mathcal{T}, \mathcal{K}$ be as in scheme $\mathcal{A}_2$, y $t \in \mathbb{F}_q$. Then, the vector of length $q^{snr+s-1}$, $(\Phi(v_s(x)))_{x\in S^r}$, where, $v_s(x) = T_{S/R}(af(x) + b \cdot x) + c$, $s = (a, b, c) \in \mathcal{S}$, has $q^{snr+s-2}$ coordinates equal to t, namely, the value of the distinct coordinates are balanced.*

Proof By the Corollary 1, in the sum of at most $s-2$ vectors of $c = c_0, c_1, \ldots, c_{s-2}$ of the Gray map, every element $t \in \mathbb{F}_q$ is in q^{s-2} entries. On the other hand, if an element $a = a_0 + a_1p + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1} \in R$, then $\Phi(a) = \overline{a}_0c_0 + \overline{a}_1c_1 + \cdots + \overline{a}_{s-2}c_{s-2} + \overline{a}_{s-1}c_{s-1} \in \mathbb{F}_q^{q^{s-1}}$.

To have the number of images $\Phi(a)$ equal to a value $t \in \mathbb{F}_q$ for every element a in R, it is necessary to consider the possible values that can have the coefficients $a_0, a_1, \ldots, a_{s-2}, a_{s-1}$:

If we consider the possible combinations for the sum of $s-1$ terms without the case when $a_0 = a_1 = \cdots = a_{s-2} = 0$, and without considering the last term, $(q^{s-1} - 1) \cdot q^{s-2}$ entries are equal t.

Now, if the term $\overline{a}_{s-1}c_{s-1}$ is considered, the following observations are obtained:

1. If the sum of the first $s - 1$ terms is non zero, then the number of combinations increases to $(q^{s-1} - 1) \cdot q^{s-2} \cdot q = (q^{s-1} - 1) \cdot q^{s-1}$, since there are q distinct elements $\overline{a}_{s-1}$.
2. If the sum of the first $s - 1$ terms is zero, then we only have the term $\overline{a}_{s-1}c_{s-1}$. Since there is only one element $\overline{a}_{s-1} \in \mathbb{F}_q$, such that, $\overline{a}_{s-1} = t$, then we have a vector with q^{s-1} entries equal to t. So the possible combinations are $(q^{s-1} - 1) \cdot q^{s-1} + q^{s-1} = q^{2s-2}$.

The above is valid for all elements in R repeated only once. Because in u_s each element of R is repeated q^{snr-s} times, then there are $q^{snr+s-2}$ elements in $\mathcal{K}$ that send the projection of $\Phi(v_s)$ to the element t.

□

Theorem 10 *Let* $\mathcal{S}, \mathcal{T}$, $\mathcal{K}$ *be as in the scheme* $\mathcal{A}_2$, $t_1, t_2 \in \mathbb{F}_q$, $t_1 \neq t_2$. *Then* $|\{x \in \mathcal{S}^r |\, \Phi(v_{s_1}(x)) = t_1, \Phi(v_{s_2}(x)) = t_2\}| = q^{snr-2}$, *where,* $v_{s_1}(x) = T_{S/R}(a_1 f(x) + b_1 \cdot x) + c_1$ *y* $v_{s_2}(x) = T_{S/R}(a_2 f(x) + b_2 \cdot x) + c_2$, $s_1 = (a_1, b_1, c_1) \in \mathcal{S}$, $s_2 = (a_2, b_2, c_2) \in \mathcal{S}$, $(a_1, b_1) \neq (a_2, b_2)$.

Proof Let us find $s_1 = (a_1, b_1, c_1)$ y $s_2 = (a_2, b_2, c_2)$ such that $(a_1, b_1) \neq (a_2.b_2)$. Then, by Theorem 8 and proceeding as in the proof of Theorem 9, $|\{k \in \mathcal{K}|\, e_k(s_1) = t_1, e_k(s_2) = t_2\}| = (q^{s-1} - 1)q^{s-1}q^{snr-2s} + q^{s-1}q^{snr-2s} = q^{2s-2}q^{snr-2s} = q^{snr-2}$.

□

Theorem 11 *In the scheme* $\mathcal{A}_2$,

$$P_I = \frac{1}{q} \;\; y \;\; P_S = \frac{1}{q}.$$

Proof Let us find P_I:

By Theorem 9, $|\{k \in \mathcal{K}|\, e_k(s) = t\}| = q^{snr+s-2}$. Thus, the probability of impersonation is

$$P_I = \frac{|\{k \in \mathcal{K}|\, e_k(s) = t\}|}{|\mathcal{K}|} = \frac{q^{snr+s-2}}{q^{srn+s-1}} = \frac{1}{q}.$$

Let us fin P_S:

Let $(a_1, b_1, c_1) \neq (a_2, b_2, c_2)$ and $t_1 \neq t_2$. By Theorem 10, if $(a_1, b_1) \neq (a_2, b_2)$, then

$$|\{k \in \mathcal{K}|\, e_k(s_1) = t_1, e_k(s_2) = t_2\}| = q^{snr-2}.$$

If $(a_1, b_1) = (a_2, b_2)$, then $c_1 \neq c_2$. Thus, by Corollary 2, $\{k \in \mathbb{Z}_{q^{s-1}} \mid \Phi_k(c) = t, \Phi_k(c') = t'\} = q^{s-3}$. So, in this case

$$|\{k \in \mathcal{K}|\, e_k(s_1) = t_1, e_k(s_2) = t_2\}| = q^{s-3}q^{snr} = q^{snr+s-3}.$$

Therefore, $P_S = \frac{\max\{q^{snr-2},\; q^{snr+s-3}\}}{q^{snr+s-2}} = \frac{1}{q}$.

□

3.4 Third construction: Without Map Gray, over Galois rings

This authentication scheme is on Galois rings, considering the resilient functions and the trace function over these ring. We get a generalization over Galois rings of the scheme given over finite fields of [8]. If $s = 1$, then we obtain the scheme presented in [8], with the difference that the source space of the scheme constructed here has a greater cardinality; this results in a better relationship between the message space and the key space for our schema (see Theorems 2.3 y 3.1 in [12] and Theorem 14 in [2]).

Let $f : S^r \longrightarrow S$ a t-resilient function, $r, t \in \mathbb{Z}^+$, $r > t > 1$. We build the following authentication scheme,

$$\mathcal{A}_3 = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}) : \tag{5}$$

$$\begin{aligned}
&\mathcal{S} = (\{1\} \times \{(b_1, \ldots, b_{t-1}, 0 \ldots, 0), (0, \ldots, 0, b_t, 0, \ldots, 0), \ldots, (0, \ldots, 0, b_r)\}) \\
&\cup (\{0\} \times \{(b'_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, b'_r)\}) \subset S \times U(S)^r, \\
&b_1, \ldots, b_{t-1} \in U(S), b'_1, \ldots, b'_r \in S^{\times}. \\
&\mathcal{T} = R, \\
&\mathcal{K} = S^r, \\
&\mathcal{E} = \{E_k : k \in \mathcal{K}\},
\end{aligned}$$

and

$$E_k(s) = T_{S/R}(af(x) + b \cdot x),$$

$x \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

We can see that $|\mathcal{S}| = \left[\left((q^n - 1)q^{n(s-1)} + 1\right)^{t-1} + W'\right]$, $|\mathcal{T}| = q^s$, $|\mathcal{K}| = |\mathcal{E}| = q^{snr}$,

where,

$W' = (r - t + 1) \cdot \left[(q^n - 1)q^{n(s-1)} + 1\right] + r(q^n - 1)q^{n(s-1)}$

This authentication scheme is a generalization of the first authentication scheme given in [8], where the scheme is considered on finite fields. In our scheme if we consider $s = 1$, then we obtain the same scheme, exception the size of the source space; here, this is is greater than the size of the source space given in [8]. Therefore, in this work $\mathcal{K}$ and $|\mathcal{S}|(|\mathcal{T}| - |) + 1$ are closer, following the Theorem 2. Then, we have a better relation between the spaces.

The following result ensures that the encoding rules are equally likely to be chosen.

Theorem 12 *The function $H : \mathcal{K} \to \mathcal{E}$ defined by $H : k \to E_k$ is a bijection.*

Proof Suppose $E_x = E_{x'}$, $x, x' \in S^r$. Then,

$$T_{S/R}(af(x) + bx) = Tr_{S/R}(af(x') + bx'), \quad \forall\ (a, b) \in \mathcal{S}.$$

Let $x - x'$ be nonzero in its i-th entry, i.e., $(x - x')_i$. Consider $a = 0$ and $b = (0, \ldots, 0, b_i, 0, \ldots, 0)$. Then $T_{S/R}(b_i(x - x')_i) = 0 \ \ \forall b_i \in U(S) \backslash \{0\}$. Thus, $x - x' = 0$, namely, $x = x'$.

□

Solving similarly to the proof of Theorem 8, the following result is granted.

Theorem 13 *Let $f : S^r \to S$ a t-resilient function and let $(a_1, b_1) \neq (a_2, b_2)$ elements of $\mathcal{S}$, $u_1, u_2 \in R$ and*

$$N(f; a_1, b_1, a_2, b_2; u_1, u_2) \\ = |\{x \in \mathbb{F}_{q^n}^r : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_1 f(x) + b_1 \cdot x) = u_1, Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_2 f(x) + b_2 \cdot x) = u_2\}|.$$

Then,

$$N(f; a_1, b_1, a_2, b_2; u_1, u_2) = q^{snr-2s}.$$

In the following result, minimum values for P_I and P_S are obtained.

Theorem 14 *Let the authentication scheme $\mathcal{A}_3$. Then,*

$$P_I = \frac{1}{q^s}, \ P_S = \frac{1}{q^s}.$$

Proof Let $(a, b) \in \mathcal{S}$, $(a, b) \neq 0$. We know that the function

$$k \mapsto T_{S/R}(af(k) + bk)$$

is balanced. Then,

$$\begin{aligned} P_I &= \max_{s \in \mathcal{S}, t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : T_{S/R}(af(k) + bk) = t\}}{|\mathcal{K}|} \\ &= \frac{q^{snr-s}}{q^{snr}} \\ &= \frac{1}{q^s}. \end{aligned}$$

Now by Theorem 13,

$$N(f; a_1, b_1, a_2, b_2; u_1, u_2) = q^{snr-2s}.$$

Also,

$$|\{k \in \mathcal{K} : T_{S/R}(af(k) + bk) = t\}| = q^{snr-s}.$$

Thus,

$$\begin{aligned} P_S &= \max_{\substack{s \in \mathcal{S} \\ t \in \mathcal{T}}} \max_{\substack{s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|} \\ &= \frac{q^{snr-2s}}{q^{snr-s}} \\ &= \frac{1}{q^s}. \end{aligned}$$

□

4 Conclusions

We build three authentication schemes, obtaining minimum values for the success probabilities of impersonation and substitution attacks. In the firs scheme, a better relationship between the parameters' size is obtained simplifying the form and increasing the source space's size. On the other hand, the injectivity proof between the key space and the encoding rules is substantially reduced. In the second scheme, a parameter is removed from the first scheme, leading to a deeper analysis of the Gray map, and its composition with the resilient functions and the trace function. In the third scheme, a generalization is obtained, now on Galois rings, of a scheme on finite fields, improving the relationship between the size of their spaces.

References

1. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), pp. 210–229 (1988)
2. Chanson, S., Ding, C., Salomaa, A.: Cartesian Authentication codes from functions with optimal nonlinearity. Theor. Comput. Sci. **290**, pp. 1737–1752 (2003)
3. 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)
4. 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)
5. Ding, C., Niederreiter, H.: Systematic authentication codes from highly nonlinear functions. IEEE Transactions on Information Theory **50**(10), 2421–2428 (2004)
6. Greferath, M., Schmidt, S.E.: Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. IEEE Transactions on Information Theory **45**(7), 2522–2524 (1999). URL http://dblp.uni-trier.de/db/journals/tit/tit45.html#GreferathS99
7. Ku-Cauich, J.C., Tapia-Recillas, H.: Systematic authentication codes based on a class of bent functions and the Gray map on a Galois ring. SIAM J. Discrete Math. **27**(2), 1159–1170 (2013)
8. Ku-Cauich, J.C., Morales-Luna G.: Authentication Codes based on resilient Boolean maps. Des. Codes Cryptogr. **80**, 619-633 (2016)
9. Ku-Cauich, J.C., Morales-Luna G., Tapia-Recillas, H.: An Authentication Code over Galois Rings with Optimal Impersonation and Substitution Probabilities. Mathematical and Computational Applications **23**(46), (2018)
10. Özbudak, F., Saygi, Z.: Some constructions of systematic authentication codes using Galois rings. Des. Codes Cryptography **41**(3), 343–357 (2006)
11. Rueppel, R.: Analysis and design of stream ciphers. Communications and control engineering series. Springer (1986)
12. Stinson, D.R.: Combinatorial characterization of authentication codes. Des. Codes Cryptogr **2**, 175–187 (1992)
13. Zhang, X.M., Zheng, Y.: Cryptographically resilient functions. IEEE Transactions on Information Theory **43**(5), 1740–1747 (1997)
14. McDonald, B.: Finite Rings with Identity. Pure and Applied Mathematics Series Marcel Dekker Incorporated: New York, NY, USA, (1974)
15. Wan, Z.: Lectures on Finite Fields and Galois Rings. World Scientific: Singapore, (2003)