mathematics

MDPI

Article

Three Authentication Schemes without Secrecy over Finite Fields and Galois Rings

Juan Carlos Ku-Cauich *,†,‡ **and Miguel Angel Márquez-Hidalgo** †

Computer Science, CINVESTAV-IPN, Mexico City 07360, Mexico; mmarquez@computacion.cs.cinvestav.mx
* Correspondence: jcku@cs.cinvestav.mx
† These authors contributed equally to this work.
‡ Current address: Av. IPN 2508, San Pedro Zacatenco, Mexico City 07300, Mexico.

Abstract: We provide three new authentication schemes without secrecy. The first two on finite fields and Galois rings, using Gray map for this link. The third construction is based on Galois rings. The main achievement in this work is to obtain optimal impersonation and substitution probabilities in the schemes. Additionally, in the first and second scheme, we simplify the source space and obtain a better relationship between the size of the message space and the key space than the one given in a recent paper. Finally, we provide a third scheme on Galois rings.

Keywords: authentication schemes; resilient functions; Gray map

MSC: Primary: 11T71; Secondary: 14G50; 94A60; 94A62

Citation: Ku-Cauich, J.C.; Márquez-Hidalgo, M.A. Three Authentication Schemes without Secrecy over Finite Fields and Galois Rings. *Mathematics* **2021**, *9*, 942. https://doi.org/10.3390/math9090942

Academic Editors: Marian Ioan Munteanu, Michele Elia and Nadir Murru

Received: 29 January 2021
Accepted: 20 April 2021
Published: 23 April 2021

1. Introduction

In an authentication model introduced by Simmons [1], three participants: a transmitter, a receiver, and an intruder. The transmitter wants to send a message to the receiver through a public channel. Since the communication channel is public, there is the possibility that an intruder could deliberately observe or disrupt the ordinary communication. There are two types of authentication schemes: without secrecy and with secrecy [2]. In an authentication code without secrecy, the pieces of information are sent to the receiver in plaintext, and the secret key is used for authentication purposes only. In an authentication code with secrecy, the information pieces are sent to the receiver in an encrypted form.

Different messages can be sent by the receiver through the communication channel using the same secret key in an authentication scheme. The intruder observes the $i \geq 0$ distinct messages and sends a message m' to the receiver, hoping that it will be accepted as authentic. This action is known as the *spoofing attack* [3]. If $i = 0$, it is called impersonation game, and if $i = 1$, it is called the substitution game. We study the cases when $i = 0$ and $i = 1$ (cases considered, for example, in [4–6]).

The authentication schemes without secrecy are considered, for instance, in [4,5]. There are two main problems: the first problem consists of determining optimal minimal attack probabilities. The second is keeping the size of the key spaces as low as possible compared to the size of the message space, namely the product of the dimensions of the source state space and the tag space. These goals are conflicting, and thus a trade-off strategy is required. 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 [6], and Theorem 14 in [7]). In this case, an optimal relationship between the sizes of the spaces can be found.

In this work, we achieve the main objective in the three schemes: to determine the minimum values for the success probabilities of impersonation and substitution attacks (related to impersonation game and substitution game). Furthermore, the spaces' size inequalities are better in construction 1, 2 than the scheme given in [8] because here, we use a source space with more elements (giving less difference between the key space and the message space). Besides, in [8], the source space is impractical, and the proof of injection between the key space and the encoding rules is very long (approximately eight pages) and laborious. In the second scheme, we reduce the first schemes' parameters, thus obtaining an alternative scheme. Construction 3 is a generalization, now on Galois rings, of the scheme given in [9] on finite fields. If the characteristic of the Galois ring is p^s, p prime, s positive integer, then there is one more variable in the scheme, s. If p is kept constant and s increases, then the values for the success probabilities of impersonation and substitution attacks decrease. If $s = 1$, we have the case of [9].

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 balanced functions and distinct properties, for instance, Corollary 1, Theorems 9, 10 and 13.

The current construction scheme 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 [10–12].

The paper is organized as follows: In Section 2, Galois rings are reviewed, and 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 constructed and compared with other schemes. Minimum values for the success probabilities of impersonation and substitution attacks are obtained. In Section 3.1, the general authentication scheme without secrecy scheme is recalled. In 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 Section 3.4 a third construction only over Galois rigs is introduced. In Section 4 the final conclusions 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 written 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 [13,14].

Definition 1. [15] *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 $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, $m \leq n$.

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 [16].

Let m, n, s be positive integers, p prime number. Let $S = GR(p^s, mn)$ and $R = GR(p^s, m)$ be 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 [8].

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 $w_H(b) \leq t$, $(a, b) \in U(S) \times (U(S))^r$, $(a, b) \neq (0, 0)$.
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 necessary facts [12]:

Lemma 1. [12] *Let $u \in R$. Then,*
$$\sum_{x \in R} e^{2\pi i T_{S/R}(ux)/p^s} = \begin{cases} q^s & \text{if } u = 0 \\ 0 & \text{if } u \neq 0 \end{cases}.$$

Definition 2. [12] *Let $u \in R$,*
$$s(u) := \sum_{x \in R - pR} e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(ux)/p^s} \quad \text{and} \quad w_h(u) := -\frac{1}{q} s(u) + (q^{s-1} - q^{s-2}).$$

w_h is called the homogeneous weight at the ring R.

The homogeneous weight at R is given by
$$w_h(u) = \begin{cases} 0 & \text{if} \quad u = 0 \\ q^{s-1} & \text{if} \quad u \in p^{s-1}R - \{0\} \\ q^{s-1} - q^{s-2} & \text{if} \quad u \in R - p^{s-1}R \end{cases}.$$

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

Definition 3. [10] *The Gray map on R is*
$$\begin{array}{rccc} \Phi : & R & \to & \mathbb{F}_q^{q^{s-1}} \\ & r_0 + r_1 p + \cdots + r_{s-1} p^{s-1} & \mapsto & \bar{r}_0 c_0 + \bar{r}_1 c_1 + \cdots + \bar{r}_{s-1} c_{s-1} \end{array}$$
$$c_i := (v + \delta_{i0}(u - v) \otimes \cdots \otimes v + \delta_{is-2}(u - v)), \quad i = 0, \ldots, s-1,$$
and
$$v := (1, \ldots, 1) \in \mathbb{F}_q^q,\ u := (0, \bar{\eta}, \bar{\eta}^2, \ldots, \bar{\eta}^{q-1}) \in \mathbb{F}_q^q.$$

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

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

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

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

Lemma 2. [8] *Let Φ be the Gray map on R. Then,*

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

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

3. An Authentication Scheme without Secrecy on Galois Rings

3.1. A General Scheme without Secrecy

An authentication scheme [5] provides a method to ensure the integrity of the information when sent through a 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 secrecy is a quadruple:

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

where $\mathcal{S}$ is the source space, $\mathcal{T}$ is the tag space, $\mathcal{K}$ is the space key, and $E_k : \mathcal{S} \to \mathcal{T}$ is 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 [6].

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

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

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

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

Relationships between the sizes of the spaces are given.

Theorem 2. [7] *Let $\mathcal{A}$ be an authentication scheme without secrecy in which $P_I = P_S = \frac{1}{|\mathcal{T}|}$. Then*

$$|\mathcal{K}| \geq |\mathcal{S}|(|\mathcal{T}| - 1) + 1 \text{ if } |\mathcal{S}| \geq |\mathcal{T}| + 1 \quad \text{and} \quad |\mathcal{K}| \geq |\mathcal{T}|^2 \text{ if } |\mathcal{S}| \leq |\mathcal{T}| + 1.$$

The authentication scheme is optimal if the equality $|\mathcal{K}| = |\mathcal{S}|(|\mathcal{T}| - 1) + 1$ if $|\mathcal{S}| \geq |\mathcal{T}| + 1$.

In this way, the relationship between the cardinality of the source space and the tag space is compromised by obtaining the minimum bounds for P_I and P_S.

3.2. *A First Construction Using Gray Map*

We give an authentication scheme without secrecy. 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 [8] 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 [6]. On the other hand, we reduce the injection proof of [8] mainly due to Gray map properties, the new source space, and Theorem 3.

Let $n > s, p > 2$, and $L := \{l_0 + l_1 p + \cdots + l_{s-2}p^{s-2} \mid l_0, \ldots, l_{s-2} \in \mathcal{T}_R\}$. We can see that $\langle p^{s-1} \rangle = \{ap^{s-1} \mid a \in \mathcal{T}_R\}$. If $a, b \in L$, then $a - b \in (R - p^{s-1}R) \cup \{0\}$.

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

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

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

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

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

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 [8], and the tag space is similar. Therefore, in this work $|\mathcal{K}|$ and $|\mathcal{S}|(|\mathcal{T}| - 1) + 1$ are closer, obtaining then (following the Theorem 2) a better relationship between the spaces.

Please note that the source space can be considered to be

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

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 there are $q^{n(s-1)}$ zero divisors in 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. [8] *Let $c = r_0 + r_1 p + \cdots + r_{s-2}p^{s-2} \in L$. Then*

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

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 $q - 1$ is an even number and $\xi \in T_R$ 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 $-x^d \in T_R$. Therefore, if*

$$a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} \in R$$

is in p-adic form, then

$$-a_0 - a_1 p - \cdots - a_{s-2}p^{s-2} \in R$$

is also in its p-adic form.

Theorem 4. *Let the function $H : \mathcal{K} \longrightarrow \mathcal{E}$ be 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 three cases.

Case 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

$$T_{S/R}(af(x) + b \cdot x) = a_0 + \cdots + a_k p^k + \cdots + a_{s-2}p^{s-2} + a_{s-1}p^{s-1},$$

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

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

Therefore if $s = (a, b, c) \in \mathcal{S}$ as above, given two coordinates of $\Phi(v_{s,\beta}(x))$, $\beta \in p^{s-1}R$, these are distinct. It follows from Remark 1 and Lemma 2.

Case 2:

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 means $\Phi_w(v_{s,\beta}(x))$ and $\Phi_w(v_{s,\beta}(y))$.

Let $a = 0$ and $c = 0$. We know that exists a k entry such that $x_k - y_k \neq 0$ (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

$$T_{S/R}(by_k) = b'_0 + b'_1 p + \cdots + b'_{s-2}p^{s-2} + b'_{s-1}p^{s-1},$$

then $b_0 = b'_0, b_1 = b'_1, \ldots, b_{s-2} = b'_{s-2}, b_{s-1} \neq b'_{s-1}$.

So that $\Phi_w(T_{S/R}(bx_k)) \neq \Phi_w(T_{S/R}(by_k))$. Therefore $\Phi_w(v_{s,\beta}(x)) \neq \Phi_w(v_{s,\beta}(y))$ with $s = (0, b, 0)$.

We now consider distinct coordinates w_1, w_2 in $\Phi(v_{s,\beta}(x))$ and in $\Phi(v_{s,\beta}(y))$. Similarly as 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 $\Phi_{w_1}(v_{s,\beta}(x)) = \Phi_{w_1}(\beta + b_{s-1}p^{s-1}) \neq \Phi_{w_2}(\beta + b'_{s-1}p^{s-1}) = \Phi_{w_2}(v_{s,\beta}(y))$.

Case 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 $\beta_i = \beta_j$.

Let two distinct elements w_1, w_2. Let an entry k of x, $x_k \neq 0$. By 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 $b \in (S - pS)^r$) and $b_j = 0, j \neq k$; from here $\phi_{w_1}(b \cdot x) = \phi_{w_2}(b \cdot y)$. On the other hand, $\phi_{w_1}(\beta_i) \neq \phi_{w_2}(\beta_j)$. Therefore $a = 0$ and $c = 0$, and by Lemma 2, $\Phi_{w_1}(v_{s,\beta_i}(x)) \neq \Phi_w(v_{s,\beta_j}(y))$.

Let $x \neq y$, $a = 0$ and $c = 0$. Using Theorem 3, we know exists $b \in (S - pS)^r$, such that $T_{S/R}(b_k(x_k - y_k)) = 0$, where $b_k \in S - pS$ and $b_j = 0, j \neq k$. Then,

$$\Phi_w(v_{s,\beta_i}(x)) \neq \Phi_w(v_{s,\beta_j}(y))$$

follows from Lemma 2.

Finally, the case $x \neq y$ and distinct coordinates. Let $a = 0$, and similar to above we find $b_k \in S - pS$ 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,

$$\Phi_{w_1}(v_{s,\beta_i}(x)) \neq \Phi_{w_2}(v_{s,\beta_j}(y))$$

follows from Lemma 2.

The distinct above cases conclude the proof. □

The procedure to obtain bound for P_I and P_S is similar to Proposition 4 of [8]. We give this result for granted.

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

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

3.3. A Second Construction Using Map Gray

In this authentication scheme, we remove a parameter from the first scheme, thus reducing the key spaces' size; however, it is necessary to 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 and P_S are obtained, we find balanced functions in the composition of the Gray map, the trace and the 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 $f : S^r \longrightarrow S$ be a t-resilient function, $p > 2$, $n > s, r, t \in \mathbb{Z}^+$, $r > t > 1$, and $\Phi : R \to \mathbb{F}_q^{q^{s-1}}$ be the Gray map. We build the following authentication scheme,

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

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

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 $H : \mathcal{K} \longrightarrow \mathcal{E}$ be 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.

Case 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 $\Phi(v_s(y))$, $x \neq y$, $x, y \in S^r$.

We can see that the proof of these two cases is similar to the first two cases of the demonstration of Theorem 4, since in this proof only $\beta = 0$ is considered. Additionally, we know that the image of an element $\beta \in p^{s-1}R$ under the Gray map is a vector with all equal entries. □

To find P_I and P_S, we give the following results.

Let $c_i \in \mathbb{F}_q^{q-1}$ be the vectors in the image of the 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*

$$\Big[[P_0(c'_l)]_{q^{l-r-1}}, [P_1(c'_l)]_{q^{l-r-1}}, \ldots, [P_{q-1}(c'_l)]_{q^{l-r-1}}\Big]_{q^r},$$

where

$$c'_l = \Big[[0]_{q^{s-l-2}}, [\xi]_{q^{s-l-2}}, \ldots, [\xi^{q-1}]_{q^{s-l-2}}\Big],$$

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 second last terms of the sum, respectively, in increasing order of the indexes.*

Proof. The claim is proved by mathematical induction.

Basis step:

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

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

and

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

Please note that

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

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,

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

$$P\zeta(c'_i) := [\zeta]_{q^{s-j-2}} + [c'_i]_{q^{i-j-1}} = \Big[[\zeta + 0]_{q^{s-i-2}}, [\zeta + \xi]_{q^{s-i-2}}, \ldots, [\zeta + \xi^{q-1}]_{q^{s-i-2}}\Big],$$

$\zeta \in \mathbb{F}_q$.

Inductive step:

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

$$\Big[[P_0(c'_l)]_{q^{l-r-1}}, [P_1(c'_l)]_{q^{l-r-1}}, \ldots, [P_{q-1}(c'_l)]_{q^{l-r-1}}\Big]_{q^r}.$$

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

$$\left[[P_0(c'_l)]_{q^{l-r-1}}, [P_1(c'_l)]_{q^{l-r-1}}, \dots, [P_{q-1}(c'_l)]_{q^{l-r-1}}\right]_{q^r} + \left[\left[[c'_v]_{q^{v-l}}\right]_{q^{l-r-1}q}\right]_{q^r}$$

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

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

Corollary 1. *Let $c_0, c_1, \dots, c_{s-2}$, be $s-1$ vectors 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 second last terms of the sum, respectively, in increasing order of the indexes. The resulting vector is conformed by a permutation of the vectors $[\zeta]_{q^{s-l-2}}$ in c'_v, where

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

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

It follows from Theorem 7.

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

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

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

and

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

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

Please note that different from Corollary 3, here the sum of the elements $c_0, c_1, \dots, c_{s-2}$ 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 [9], now on Galois rings.

Theorem 8. *Let $f : S^r \to S$ be 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

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

The last equality is justified as follows:

Please note that $y_1 b_1 + y_2 b_2$ and $y_1 a_1 + y_2 a_2$ cannot both be zero, unless $y_1 = y_2 = 0$, because of the shape of source space.

If $y_1 a_1 + y_2 a_2 = 0$ and $y_1 b_1 + y_2 b_2 \neq 0$, 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, similar to Lemma 2.1 proof of [12],

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

If $y_1 a_1 + y_2 a_2 \neq 0$ and $y_1 b_1 + y_2 b_2 = 0$, then, since $f(x)$ is balanced and by Lemma 1,

$$\sum_{x \in S^r} e^{2\pi i T_{S/\mathbb{Z}_{p^s}}((y_1 a_1 + y_2 a_2) f(x))/p^s} = 0.$$

Finally, if $y_1 a_1 + y_2 a_2 \neq 0$ and $y_1 b_1 + y_2 b_2 \neq 0$, suppose without loss of generality that the nonzero entries of $y_1 b_1 + y_2 b_2$ 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,

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

Therefore,

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

□

Theorem 9. *Let $\mathcal{S},\mathcal{T}$, $\mathcal{K}$ be as in scheme $\mathcal{A}_2$, and $t \in \mathbb{F}_q$. 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 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

$$\Phi(a) = \bar{a}_0c_0 + \bar{a}_1c_1 + \cdots + \bar{a}_{s-2}c_{s-2} + \bar{a}_{s-1}c_{s-1} \in \mathbb{F}_q^{q^{s-1}}.$$

To have the number of images $\Phi(a)$ equal to a value $t \in \mathbb{F}_q$ for any 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 $a_0 = a_1 = \cdots = a_{s-2} = 0$ and without considering the last term, then $(q^{s-1}-1) \cdot q^{s-2}$ entries are equal to t.

If the term $\bar{a}_{s-1}c_{s-1}$ is considered:

1. If the sum of the first $s-1$ terms is nonzero, 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 $\bar{a}_{s-1}$.
2. If the sum of the first $s-1$ terms is zero, then we only have the term $\bar{a}_{s-1}c_{s-1}$. Since there is only one element $\bar{a}_{s-1} \in \mathbb{F}_q$ such that $\bar{a}_{s-1} = t$, then we have a vector with q^{s-1} entries equal to t. Hence, 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. Therefore, there are $q^{snr+s-2}$ elements in $\mathcal{K}$ that corresponding to coordinates of u_s equal to 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 $v_{s_1}(x) = T_{S/R}(a_1f(x) + b_1 \cdot x) + c_1$ and $v_{s_2}(x) = T_{S/R}(a_2f(x) + b_2 \cdot x) + c_2$, $s_1 = (a_1,b_1,c_1) \in \mathcal{S}, s_2 = (a_2,b_2,c_2) \in \mathcal{S}$, $(a_1,b_1) \neq (a_2,b_2)$.

Proof. Let $s_1 = (a_1,b_1,c_1)$ and $s_2 = (a_2,b_2,c_2)$ 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 $\mathcal{A}_2$,*

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

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 find 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, $\{k \in \mathbb{Z}_{q^{s-1}} \mid \Phi_k(c) = t, \Phi_k(c') = t'\} = q^{s-3}$ (follows from Corollary 2). Hence,

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

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

In this scheme, the composition of resilient functions and trace function on Galois rings are provided. We get a generalization on Galois rings of the authentication scheme given on finite fields in [9]. If $s = 1$, then we obtain the scheme presented in [9], with the difference that the source space of the scheme constructed here has a greater cardinality; this result brings a better relationship between the message space and the key space for our scheme (see Theorems 2.3 and 3.1 in [6] and Theorem 14 in [7]).

Let $f : S^r \longrightarrow S$ be 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 [9], where the scheme is considered on finite fields. In our scheme if we consider $s = 1$, then we obtain the same scheme, except the size of the source space; here, this is greater than the size of the source space given in [9]. Therefore, in this work $\mathcal{K}$ and $|\mathcal{S}|(|\mathcal{T}| - 1) + 1$ are closer, following the Theorem 2. Then, we have a better relationship 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,

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

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

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

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

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

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 $(a, b) \in \mathcal{S}$, $(a, b) \neq (0, \mathbf{0})$. 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 obtain minimum values for the success probabilities of impersonation and substitution attacks in the distinct schemes. In the first and second scheme, compared to the first scheme in [8], a better relationship between the parameters' size is obtained, simplifying the source space. 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 more in-depth analysis of the Gray map and also of the composition with the resilient functions and the trace function. In the third scheme, a generalization is obtained on Galois rings, of the first scheme on finite fields given in [9], improving the relationship between their spaces' size, based on Theorem 2.

Author Contributions: The two authors contributed equally to conceptualization and formal analysis of this paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Simmons, G.J. Authentication theory/coding theory. In *Advances in Cryptology, Proceedings of Crypto 84 Lecture Notes in Computer Science*; Springer: Berlin, Germany, 1985; Volume 196, pp. 411–432.
2. Ding, C.; Tian, X. Three Constructions of Authentication Codes with Perfect Secrecy. *Des. Codes Cryptogr.* **2004**, *33*, 227–239.
3. Stinson, D.R.; Teirlinck, L. A Construction for Authentication/secrecy Codes from 3-homogeneous Permutation Groups. *Europ. J. Comb.* **1990**, *11*, 73–79.
4. Carlet, C.; Ding, C.; Niederreiter, H. Authentication schemes from highly nonlinear functions. *Des. Codes Cryptogr.* **2006**, *40*, 71–79.
5. Ding, C.; Niederreiter, H. Systematic authentication codes from highly nonlinear functions. *IEEE Trans. Inf. Theory* **2004**, *50*, 2421–2428.
6. Stinson, D.R. Combinatorial characterization of authentication codes. *Des. Codes Cryptogr.* **1992**, *2*, 175–187.
7. Chanson, S.; Ding, C.; Salomaa, A. Cartesian Authentication codes from functions with optimal nonlinearity. *Theor. Comput. Sci.* **2003**, *290*, 1737–1752.
8. Ku-Cauich, J.C.; Morales-Luna G.; Tapia-Recillas, H. An Authentication Code over Galois Rings with Optimal Impersonation and Substitution Probabilities. *Math. Comput. Appl.* **2018**, *23*, 46.
9. Ku-Cauich, J.C.; Morales-Luna G. Authentication Codes based on resilient Boolean maps. *Des. Codes Cryptogr.* **2016**, *80*, 619–623.
10. Greferath, M.; Schmidt, S.E. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Trans. Inf. Theory* **1999**, *45*, 2522–2524.
11. 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.* **2013**, *27*, 1159–1170.
12. Özbudak, F.; Saygi, Z. Some constructions of systematic authentication codes using Galois rings. *Des. Codes Cryptogr.* **2006**, *41*, 343–357.
13. McDonald, B. *Finite Rings with Identity*; Pure and Applied Mathematics Series; Marcel Dekker Incorporated: New York, NY, USA, 1974.
14. Wan, Z. *Lectures on Finite Fields and Galois Rings*; World Scientific: Singapore, 2003.
15. Zhang, X.M.; Zheng, Y. Cryptographically resilient functions. *IEEE Trans. Inf. Theory* **1997**, *43*, 1740–1747.
16. Carlet, C. *More Correlation-Immune and Resilient Functions Over Galois Fields and Galois Rings*; EUROCRYPT; Fumy, W., Ed.; Springer: Berlin/Heidelberg, Germany, 1997; pp. 422–433.