


Article

An Authentication Code over Galois Rings with Optimal Impersonation and Substitution Probabilities

Juan Carlos Ku-Cauich ^{1,†,‡}, Guillermo Morales-Luna ^{1,*,‡}  and Horacio Tapia-Recillas ²¹ Computer Science, CINVESTAV-IPN, Mexico City 07360, Mexico; jcku@cs.cinvestav.mx² Departamento de Matemáticas, Universidad Autónoma Metropolitana-I, Mexico City 14387, Mexico; htr@xanum.uam.mx

* Correspondence: gmorales@cs.cinvestav.mx

† Current address: Av. IPN 2508, San Pedro Zacatenco, Mexico City 07300, Mexico

‡ These authors contributed equally to this work.

Received: 27 July 2018; Accepted: 2 September 2018; Published: 6 September 2018



Abstract: Two new systematic authentication codes based on the Gray map over a Galois ring are introduced. The first introduced code attains optimal impersonation and substitution probabilities. The second code improves space sizes, but it does not attain optimal probabilities. Additionally, it is conditioned to the existence of a special class of bent maps on Galois rings.

Keywords: authentication schemes; resilient maps; gray map

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

1. Introduction

Resilient maps were introduced in 1985 by Chor et al. [1] and independently by Bennett et al. [2], 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 [3].

The current paper deals with the notion of systematic authentication codes without secrecy as defined in [4] and considered in [5,6]. Within the systematic authentication codes, two main problems arise: the first problem consists of getting optimal minimal attack probabilities, the second problem consists of keeping the size of the key spaces as low as possible in comparison with the size of the message space—namely, the product of the sizes of the source state space and the tag space. These two goals are conflicting, and thus a trade-off strategy is required. Theorems 2.3 and 3.1 in [7] state that when optimal values for the *impersonation* and the *substitution* probabilities p_I , p_S are reached, then some relations among the sizes of the spaces arise (see also Theorem 14 in [8]).

In this paper, two new systematic authentication codes based on the Gray map on a Galois ring are introduced with the purpose of optimally reducing the impersonation and substitution probabilities. In the context of authentication codes, the substitution and impersonation probabilities are important characteristics. We build a first code with optimal values for these probabilities but at the cost of huge key and source spaces. A second code is introduced with convenient spaces sizes, but the corresponding substitution probability is not optimal.

The first code presented here is another example of a previously constructed code using the Gray map on Galois rings and modules over these rings [9]. The construction in [9] is based on rational non-degenerated maps. Here, through the generalized Gray map and resilient maps on Galois rings we obtain minimal upper bounds for the attack probabilities, thus improving former codes. Indeed, the obtained impersonation and substitution probabilities are optimal. However, the introduced code

has a smaller source state space in comparison with the key space. We introduce precise definitions over Galois rings of the notions of resilient maps and the generalized Gray map. The introduced construction over Galois rings is translated into finite fields via the Gray map, thus providing similar codes on Galois fields.

In [10] a family of bent maps is introduced over Galois rings of characteristic p^2 , with p a prime number. The class of these maps is closed under multiplication by units in the Galois ring, under the assumption that there exists a similar class of bent functions in Galois rings of characteristic p^r , with $r > 2$. For this hypothetical code we obtain spaces of acceptable size, similar to sizes in former constructions but with improved impersonation and substitution probabilities. In fact, the probabilities are lower than those in other authentication codes with no optimal probabilities.

The paper is organized as follows: In Section 2 the basic construction of the Gray map is recalled. In Section 3 a new systematic authentication code based on the Gray map is introduced and its main properties are determined. In Section 3.1 the general construction of a systematic authentication code is recalled, and the new code is treated in Sections 3.2 and 3.3. In Section 3.4 we introduce the second code on the assumption of the existence of an appropriate class of bent functions. In Section 4 we make a succinct comparison with formerly introduced systematic authentication codes, and in Section 5 we state some conclusions. The existence of the required bijection between the key space and the set of encoding maps is proved exhaustively and the current proof is rather long (hence, tedious). However, the reader can find it in [11].

2. The Gray Map over Galois Rings

Let \mathbb{Z}_{p^r} be the ring of integers modulo p^r , where p is a prime and r a positive integer. A monic polynomial $f(x) \in \mathbb{Z}_{p^r}[x]$ is called *monic basic irreducible (primitive)* if its reduction modulo p is an irreducible (primitive) polynomial over \mathbb{F}_p . The Galois ring of characteristic p^r is defined as

$$\text{GR}(p^r, l) = \mathbb{Z}_{p^r}[x] / \langle f(x) \rangle,$$

where $f(x) \in \mathbb{Z}_{p^r}[x]$ is a monic basic irreducible polynomial of degree l and $\langle f(x) \rangle$ is the ideal of $\mathbb{Z}_{p^r}[x]$ generated by $f(x)$. The polynomial $f(x)$ can be taken such that it is a divisor of $x^{p^l-1} - 1$.

The Galois ring $R = \text{GR}(p^r, l)$ is local with maximal ideal $M = \langle p \rangle = pR$ and residue field isomorphic to \mathbb{F}_q where $q = p^l$. This ring has characteristic p^r , is a chain ring, and $|R| = p^{rl}$. The group of units of R is $U(R) = C \times G$, where G is a group of order $p^{(r-1)l}$, $C = \langle \omega \rangle$ has order $(p^l - 1)$, and $f(\omega) = 0$. The Teichmüller set of representatives of R is $T(R) = \{0\} \cup C$. Any $\beta \in R$ has a unique p -adic (multiplicative) representation: $\beta = \beta_0 + \beta_1 p + \dots + \beta_{r-1} p^{r-1}$, where $\beta_i \in T(R)$ for $0 \leq i \leq r - 1$. The ring R has the structure of a \mathbb{Z}_{p^r} -module: $R = \mathbb{Z}_{p^r}[\omega] = \mathbb{Z}_{p^r} + \omega \mathbb{Z}_{p^r} + \dots + \omega^{l-1} \mathbb{Z}_{p^r}$. For details and further properties we refer the reader to ([12], [Chapter XVI]) and [13].

Let p be a prime number, $r, \ell, m \in \mathbb{Z}^+$, and $q = p^\ell$. Let $A = \text{GR}(p^r, \ell)$ and $B = \text{GR}(p^r, \ell m)$ be the corresponding Galois rings of degrees ℓ and ℓm . The ring A is an extension of \mathbb{Z}_{p^r} , and B is an extension of A . Let $\text{Tr}_{B/A} : B \rightarrow A$, $\text{Tr}_{B/\mathbb{Z}_{p^r}} : B \rightarrow \mathbb{Z}_{p^r}$ and $\text{Tr}_{A/\mathbb{Z}_{p^r}} : A \rightarrow \mathbb{Z}_{p^r}$ be the corresponding trace maps, and let pA and pB denote the maximal ideals of zero divisors of A and B , respectively.

Firstly, let us recall some well-known facts [9], as follows.

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

1.
$$\sum_{x \in A} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(ux)} = \begin{cases} q^r & \text{if } u = 0 \\ 0 & \text{if } u \neq 0 \end{cases}$$
2.
$$\sum_{x \in pA} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(ux)} = \begin{cases} q^{r-1} & \text{if } u \in p^{r-1}A \\ 0 & \text{if } u \notin p^{r-1}A \end{cases}$$

$$3. \quad \sum_{x \in A-pA} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(ux)} = \begin{cases} q^r - q^{r-1} & \text{if } u = 0 \\ -q^{r-1} & \text{if } u \in p^{r-1}A - \{0\} \\ 0 & \text{if } u \notin p^{r-1}A \end{cases}$$

From this point forward we assume that $r \geq 2$. The *homogeneous weight* on the ring A is the map [14] $w_h : A \rightarrow \mathbb{N}, u \mapsto w_h(u)$, where

$$w_h(u) = \left(q^{r-1} - q^{r-2} \right) - \frac{1}{q} \sum_{x \in A-pA} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(ux)}, \tag{1}$$

and, according to Lemma 1, $\forall u \in A :$

$$w_h(u) = \begin{cases} 0 & \text{if } u = 0 \\ q^{r-1} & \text{if } u \in p^{r-1}A - \{0\} \\ q^{r-1} - q^{r-2} & \text{if } u \in A - p^{r-1}A \end{cases} . \tag{2}$$

Indeed, the map $d_h : A \times A \rightarrow \mathbb{Z}^+, (u, v) \mapsto d_h(u, v) = w_h(u - v)$, is a metric on A . The ring A can also be considered as the metric space (A, d_h) .

Let \mathbb{F}_q^q be the q -dimensional vector space over the Galois field \mathbb{F}_q , and “ \otimes ” denote the Kronecker product $\mathbb{F}_q^m \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{mn}, ((u_i)_i, (v_j)_j) \mapsto (u_i)_i \otimes (v_j)_j = (w_{in+j} = u_i v_j)_{i,j}$. We iterate this product “on the right” as: $\otimes_{k=0}^n v_k = \left(\otimes_{k=0}^{n-1} v_k \right) \otimes v_n$. Let $e_j = (\delta_{ij})_{i=0}^{q-1}$ be the j -th vector in the canonical basis of \mathbb{F}_q^q , where δ_{ij} is the Kronecker delta, $\mathbf{1}^{(q)} = (1, \dots, 1) = \sum_{j=0}^{q-1} e_j \in \mathbb{F}_q^q$ is the vector with constant entries equal to 1, and $\rho : A \rightarrow \mathbb{F}_q$ the reduction modulus p map. Let $T(A) = \{0\} \cup \left(\zeta_A^j \right)_{j=0}^{q-2}$ be the set of Teichmüller representatives of \mathbb{F}_q in A and let $\Xi = (0, \rho(\zeta_A), \dots, \rho(\zeta_A^{q-2}), \rho(\zeta_A^{q-1})) \in \mathbb{F}_q^q$. For each index $i = 0, \dots, r - 2$ let

$$\phi_i = \bigotimes_{k=0}^{r-2} \left(\mathbf{1}^{(q)} + \delta_{ik}(\Xi - \mathbf{1}^{(q)}) \right) = \left(\mathbf{1}^{(q)} \right)^{\otimes i} \otimes \Xi \otimes \left(\mathbf{1}^{(q)} \right)^{\otimes (r-2-i)} \in \mathbb{F}_q^{q^{r-1}} \tag{3}$$

(here, for any $v \in \mathbb{F}_q^q, v^{\otimes 0} = [1]$ and $v^{\otimes(k+1)} = v^{\otimes k} \otimes v$). For $k \in \mathbb{Z}^+$ let $[y]_k = y \mathbf{1}^{(k)} = \underbrace{(y, \dots, y)}_{k\text{-times}}$.

The vector ϕ_i is the concatenation of q^i blocks, each one consisting of the concatenation of blocks of the form $[\rho_j]_{q^{r-2-i}}$, where ρ_j is the j -th coordinate of Ξ , for $j = 0, \dots, q - 1$ (see Relation (3)).

Then, the vector ϕ_i can be efficiently constructed: given an index k , with $0 \leq k \leq q^{r-1} - 1$, let $k_0 = k \bmod q^{r-1-i}$ and $k_i = \lfloor \frac{k_0}{q^{r-2-i}} \rfloor$. Then, $\phi_i(k)$ is the k_i -th coordinate of Ξ . In summary, for each $i = 0, \dots, r - 2$, the vector ϕ_i defined by (3) can be expressed as:

$$\phi_i = \left[[0]_{q^{r-2-i}}, [\rho(\zeta_A)]_{q^{r-2-i}}, \dots, [\rho(\zeta_A^{q-2})]_{q^{r-2-i}}, [\rho(\zeta_A^{q-1})]_{q^{r-2-i}} \right]_{q^i}, \tag{4}$$

where we are using the notation introduced immediately after the relation (3). As a final vector, let us define $\phi_{r-1} = [1]_{q^{r-1}}$. The *Gray map* is defined as follows:

$$\Phi : \text{GR}(p^r, \ell) = A \rightarrow \mathbb{F}_q^{q^{r-1}} \\ \sum_{i=0}^{r-1} a_i p^i \mapsto \Phi \left(\sum_{i=0}^{r-1} a_i p^i \right) = \sum_{i=0}^{r-1} \rho(a_i) \phi_i, \tag{5}$$

where the elements of A are represented in their p -adic form (i.e., $a_i \in T(A)$).

In particular, if $r = 2$, we have

$$\begin{aligned} \phi_0 &= (0, \rho(\xi_A), \dots, \rho(\xi_A^{q-2}), \rho(\xi_A^{q-1})) , \\ \phi_1 &= (1, 1, \dots, 1, 1) \in \mathbb{F}_q^q. \end{aligned}$$

Then the Gray map, as defined by (5), equals, for any element of the form $r_0 + r_1p \in \text{GR}(p^2, \ell)$:

$$\begin{aligned} \Phi(r_0 + r_1p) &= \rho(r_0)\phi_0 + \rho(r_1)\phi_1 \\ &= \rho(r_0)(0, \rho(\xi_A), \dots, \rho(\xi_A^{q-2}), \rho(\xi_A^{q-1})) + \rho(r_1)(1, 1, \dots, 1, 1) \\ &= \left((\rho(r_1), \rho(r_1 + r_0\xi_A), \dots, \rho(r_1 + r_0\xi_A^{q-2}), \rho(r_1 + r_0\xi_A^{q-1})) \right), \end{aligned}$$

which coincides with the definition given in [9].

The vector space $\mathbb{F}_q^{q^{r-1}}$ can be endowed with a structure of metric space with the Hamming distance d_H : the distance between two vectors is the number of entries at which they differ.

Two important properties of the Gray map are stated by the following proposition:

Proposition 1. *The following assertions hold:*

1. **Isometry [14].** *The Gray map is an isometry between the Galois ring A and the vector space $\mathbb{F}_q^{q^{r-1}}$:*

$$\forall u, v \in A : d_h(u, v) = d_H(\Phi(u), \Phi(v)).$$

2. *The Gray map preserves addition:*

$$\forall (u, v) \in A \times p^{r-1}A : \Phi(u + v) = \Phi(u) + \Phi(v).$$

3. A Systematic Authentication Code Based on the Gray Map

3.1. General Systematic Authentication Codes

We recall that a *systematic authentication code without secrecy* [4] 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 $S \rightarrow T$.

A transmitter and a receiver agree to a secret key $k \in K$. Whenever a source $s \in S$ must be sent, the participants proceed according to the protocol depicted in Table 1.

Table 1. Protocol of the transmission of a source $s \in S$.

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

The communicating channel is public, thus it can be eavesdropped upon by an *intruder* able to perform either *impersonation* or *substitution* attacks through the public channel. The intruder's success probabilities for impersonation and substitution are, respectively [7]:

$$p_I = \max_{(s,t) \in S \times T} \frac{|\{k \in K \mid e_k(s) = t\}|}{|K|}, \tag{6}$$

$$p_S = \max_{(s,t) \in S \times T} \max_{(s',t') \in (S - \{s\}) \times T} \frac{|\{k \in K \mid e_k(s) = t \ \& \ e_k(s') = t'\}|}{|\{k \in K \mid e_k(s) = t\}|}. \tag{7}$$

For systematic authentication codes, lower bounds are known for p_I and p_S [5]:

$$\frac{1}{|T|} \leq p_I \text{ and } \frac{1}{|T|} \leq p_S,$$

and in order to be acceptable, both p_I and p_S must be as small as possible.

3.2. A New Systematic Authentication Code

In the context of finite fields of characteristic 2, for $n \in \mathbb{Z}^+$ and $1 \leq t \leq n$, let $J = \{j_0, \dots, j_{t-1}\} \subset \{0, \dots, n-1\}$ be an index t -subset. The affine J -variety determined by $a = (a_0, \dots, a_{t-1}) \in \mathbb{F}_2^t$ is

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

A map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, $m \leq n$, is J -resilient if $\forall a \in \mathbb{F}_2^t$, the map $f|_{V_{J,a,n}}$ is balanced, namely, $\forall y \in \mathbb{F}_2^m$, $|V_{J,a,n} \cap f^{-1}(y)| = 2^{n-t-m}$. The map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is t -resilient if it is J -resilient for any set J such that $|J| = t$. The notion of t -resilient maps has been studied by several authors in the context of Galois rings, assumed as the last property of the above paragraph, and well-known wider classes of t -resilient maps have been provided. For instance, from Theorem 1 in [15], for any $n \in \mathbb{Z}^+$, if B is a Galois ring and $f_0 : B^n \rightarrow B^n$ is a map such that any element at its image $f_0(B^n)$ has more than t entries which are units in B and $f_1 : B^n \rightarrow B$ is any map, then the map $f : B^{2n} \rightarrow B$, $(x, y) \mapsto x \cdot f_0(y) + f_1(y)$ is a t -resilient map, $1 \leq t \leq n$.

In this section, a systematic authentication code is constructed using a resilient function on a Galois ring and the Gray map on this ring.

Let $p > 2$ be a prime number, $r, \ell, m \in \mathbb{Z}^+$, and $q = p^\ell$. Assume the same setting as in the beginning of Section 2.

Let $U(B) = (B - pB) \cup \{0\}$ be the set of elements of the Galois ring B that are either units or zero. Let $n \in \mathbb{Z}^+$ be another positive integer, and $f : B^n \rightarrow B$ be a t -resilient map. The following assertions hold:

- For $a \in B - pB$, the map $B^n \rightarrow B$, $x \mapsto a f(x)$, is t -resilient, hence it is also balanced.
- For $a \in B - pB$, the map $B^n \rightarrow \mathbb{Z}_{p^r}$, $x \mapsto \text{Tr}_{B/\mathbb{Z}_{p^r}}(a f(x))$, is balanced (as composition of balanced maps).
- As a more general result than Corollary 2 of [16], we have that the map

$$\gamma_{abf} : B^n \rightarrow A, \gamma_{abf} : x \mapsto \text{Tr}_{B/A}(a f(x) + b \cdot x). \tag{8}$$

is balanced whenever $w_h(b) \leq t$ and either $(a, b) \in U(B) \times (U(B))^n$, with $(a, b) \neq (0, 0)$, or $(a, b) \in (B - pB) \times B^n$.

- Recall that the Fourier transform of the map $a f$ is the function

$$B^n \rightarrow \mathbb{C}, b \mapsto \zeta_{af}(b) = \sum_{x \in B^n} e^{\frac{2\pi}{p^r} i \text{Tr}_{B/\mathbb{Z}_{p^r}}(a f(x) - b \cdot x)}.$$

As shown in [15], $\zeta_{af}(b) = 0$ under the same conditions as the above assertion, just because the map $x \mapsto \text{Tr}_{B/\mathbb{Z}_{p^r}}(a f(x) + b \cdot x)$ is balanced.

Let $T(A)$ be the set of the Teichmüller representatives of \mathbb{F}_q in A . Then, $p^{r-1}A = \{a p^{r-1} \mid a \in T(A)\}$. Similarly, $T(B)$ is the set of the Teichmüller representatives of \mathbb{F}_q in B .

Let $n \in \mathbb{Z}^+$ and $t \leq n$. For any $i < n$, let $e_i = (\delta_{ij})_{j=0}^{n-1}$ be the i -th vector in the canonical set of generators of B^n . For any $b \in T(B)^n$, let

$$X_{b,t} = \left\{ \sum_{j=0}^{t-2} b_j e_j, b_{t-1} e_{t-1}, \dots, b_{n-1} e_{n-1} \right\} \subset B^n,$$

$$N = \bigcup_{b \in T(B)^n} X_{b,t}, \tag{9}$$

$$L = \left\{ \sum_{i=0}^{r-2} r_i p^i \mid (r_0, \dots, r_{r-2}) \in T(A)^{r-1} \right\}. \tag{10}$$

Then, $|X_{b,t}| = n - t + 1$, $|N| = q^{m(t-1)} + (n - (t - 1))q^m$, $|L| = q^{r-1}$, $L \subset (A - p^{r-1}A) \cup \{0\}$, and also

$$\forall u, v \in L : (u - v) \in (A - p^{r-1}A) \cup \{0\}.$$

Let us consider an $(r - 1)n$ -subset of $T(A) - \{0, 1\}$,

$$\eta = \{\eta_k\}_{k=0}^{(r-1)n-1}, \tag{11}$$

and

$$D_\eta = \{(\eta_{(i-1)n+j}, p^i e_j) \mid 1 \leq i \leq r - 1, 0 \leq j \leq n - 1\}. \tag{12}$$

Then, $D_\eta \subset A \times B^n$ and $|D_\eta| = (r - 1)n$.

Let $T(B) = \{0\} \cup \left(\zeta_B^k\right)_{k=0}^{q^m-2}$, $G(T(B)) = \{\zeta_B^k \mid \gcd(k, q^m - 1) = 1\}$, let $\theta = \{\theta_j\}_{j=0}^{n-1}$ be an n -sequence of $G(T(B))$ (repetitions are allowed), and $\zeta \in T(B) - \{0\}$. For each integer k , with $0 \leq k \leq q^m - (r - 1)n - 2$, let

$$T_{\theta\zeta k} = \left\{ (\theta_j^i, (\zeta + \theta_j p^{1+(k \bmod (r-1))}) e_j) \right\}_{\substack{0 \leq j \leq n-1 \\ 0 \leq i \leq q^m-2}}.$$

Then, $T_{\theta\zeta k} \subset B \times B^n$ and $|T_{\theta\zeta k}| = (q^m - 1)n$.

Now, let $Z = \{\zeta_k\}_{k=0}^{q^m-(r-1)n-2}$ be a subset of $T(B) - \{0\}$, with $(q^m - 1 - (r - 1)n - 1)$ elements, such that $Z \cap \eta = \emptyset$, and

$$\mathbf{T}_{\eta\theta Z} = D_\eta \cup \bigcup_{k=0}^{q^m-(r-1)n-2} T_{\theta\zeta k}. \tag{13}$$

Then, $\mathbf{T}_{\eta\theta Z} \subset B \times B^n$ and

$$\begin{aligned} |\mathbf{T}_{\eta\theta Z}| &= (r - 1)n + (q^m - 1 - (r - 1)n)(q^m - 1)n \\ &= [(r - 1) + [(q^m - 1) - (r - 1)n] (q^m - 1)] n. \end{aligned}$$

Let $S_0 = \{0\} \times (N - \{0\}) \times L$, $S_1 = \mathbf{T}_{\eta\theta Z} \times L$, $S_2 = (T(B) - (\{0\} \cup \eta)) \times \{0\} \times L$ and

$$S = S_0 \cup S_1 \cup S_2, \quad T = \mathbb{F}_q, \quad K = \mathbb{Z}_{q^{r(mn+1)}}. \tag{14}$$

Certainly, at this point the definition of the source set S is quite unnatural. However, defined in this way, it guarantees an appropriate distance between elements (Proposition 2), leading to optimal results (Proposition 4) while keeping balanced the maps $x \mapsto \text{Tr}_{B/\mathbb{Z}_p}(af(x) + b \cdot x)$, for a t -resilient map f . This particular structure of the source space S will allow a one-to-one correspondence between keys and encoding maps (Proposition 3). From Relation (14), $S \subset B \times B^n \times A$, and

$$\begin{aligned}
 |S| &= \left((q^{m(t-1)} + (n - (t - 1))q^m - 1) + \right. \\
 &\quad \left. ((r - 1) + ((q^m - 1) - (r - 1)n) (q^m - 1)) n + (q^m - ((r - 1)n + 1)) \right) q^{r-1} \\
 &= (c_0 + c_1n - c_2n^2) q^{r-1} \\
 |T| &= q \\
 |K| &= q^{r(mn+1)},
 \end{aligned}
 \tag{15}$$

where $c_0 = q^m(q^{m(t-2)} - t) + 2(q^m - 1)$, $c_1 = q^m(q^m - 1) + 1$, $c_2 = (q^m - 1)(r - 1)$. The introduced construction imposes the supplementary condition $(r - 1)(n + 1) < p^m - 1$.

3.3. Main Characteristics of the New Code

Let $\Phi : A \rightarrow \mathbb{F}_q^{q^{r-1}}$ be the Gray map on A as defined in (5). We observe that for any element $y = \sum_{i=0}^{r-2} a_i p^i \in L$, with $(a_0, \dots, a_{r-2}) \in T(A)^{r-1}$ (see (10)), the evaluation of Φ at y , according to (5), is

$$\Phi(y) = \sum_{i=0}^{r-2} \rho(a_i) \phi_i.$$

Also, since $q - 1$ is even, for any ζ generating T_A , either $-\zeta \in T_A$ or $-1 \in T_A$. The following implication holds: $\forall z \in A \forall d \in \{1, \dots, q - 1\} [z^d \in T_A \implies -z^d \in T_A]$. Hence, if the p -adic form of an element in A is $z = \sum_{k=0}^{s-1} z_k p^k$, the p -adic form of $-z$ is $-z = \sum_{k=0}^{s-1} (-z_k) p^k$. Let $f : B^n \rightarrow B$ be a t -resilient map. For each $s = (s_0, s_1, s_2) \in S$ and each $w \in p^{r-1}A$, consider the map $v_{s,w} : B^n \rightarrow A$, $x \mapsto v_{s,w}(x)$, where

$$v_{s,w}(x) = \text{Tr}_{B/A}(s_0 f(x) + s_1 \cdot x) + s_2 + w = \gamma_{s_0 s_1} f(x) + s_2 + w
 \tag{16}$$

(see relation (8) above). Let

$$u_{s,w} = (\Phi(v_{s,w}(x)))_{x \in B^n} \in \left(\mathbb{F}_q^{q^{r-1}} \right)^{q^{rnm}}, \quad u_s = (u_{s,w})_{w \in p^{r-1}A} \in \left(\mathbb{F}_q^{q^{r-1}} \right)^{q^{rnm+1}}.
 \tag{17}$$

Since $|p^{r-1}A| = q$, we have $\left(\mathbb{F}_q^{q^{r-1}} \right)^{q^{rnm+1}} \simeq \mathbb{F}_q^{q^{r(mn+1)}}$, thus we may assume $u_s \in \mathbb{F}_q^{q^{r(mn+1)}}$.

Proposition 2. Let d_H be the Hamming distance on the vector space $\mathbb{F}_q^{q^{r(mn+1)}}$ and let $f : B^n \rightarrow B$ be a t -resilient map. For any two points $s_0 = (s_{00}, s_{10}, s_{20})$, $s_1 = (s_{01}, s_{11}, s_{21}) \in S$, with $s_0 \neq s_1$, and any two $w_0, w_1 \in p^{r-1}A$, the following relation holds:

$$d_H(u_{s_0, w_0}, u_{s_1, w_1}) = q^{rnm} (q^{r-1} - q^{r-2}).$$

Proof. Let $s_2 = s_0 - s_1$ and $w_2 = w_0 - w_1$. Then, the calculation of the Hamming distance of the points $u_{s_0, w_0}, u_{s_1, w_1}$ is displayed in (18), there equality (i) holds because Φ is an isometry, equality (ii) follows from the defining Relation (1), and equality (iii) is due to Relation (16).

$$\begin{aligned}
 d_H(u_{s_0,w_0}, u_{s_1,w_1}) &= \sum_{x \in B^n} d_H(\Phi(v_{s_0,w_0}(x)), \Phi(v_{s_1,w_1}(x))) \\
 &\stackrel{(i)}{=} \sum_{x \in B^n} d_h(v_{s_0,w_0}(x), v_{s_1,w_1}(x)) \\
 &= \sum_{x \in B^n} w_h(v_{s_0,w_0}(x) - v_{s_1,w_1}(x)) \\
 &= \sum_{x \in B^n} w_h(v_{s_2,w_2}(x)) \\
 &\stackrel{(ii)}{=} \sum_{x \in B^n} \left((q^{r-1} - q^{r-2}) - \frac{1}{q} \sum_{r_0 \in A-pA} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(r_0 v_{s_2,w_2}(x))} \right) \\
 &= q^{r mn} (q^{r-1} - q^{r-2}) - \frac{1}{q} \sum_{x \in B^n} \sum_{r_0 \in A-pA} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(r_0 v_{s_2,w_2}(x))} \\
 &\stackrel{(iii)}{=} q^{r mn} (q^{r-1} - q^{r-2}) \\
 &\quad - \frac{1}{q} \sum_{r_0 \in A-pA} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(r_0 w_2)} e^{\frac{2\pi}{p^r} i \text{Tr}_{A/\mathbb{Z}_{p^r}}(r_0 s_{22})} \sum_{x \in B^n} e^{\frac{2\pi}{p^r} i \text{Tr}_{B/\mathbb{Z}_{p^r}}(r_0 s_{02} f(x) + r_0 s_{12} \cdot x)}
 \end{aligned} \tag{18}$$

If $(s_{02}, s_{12}) \neq (0, 0)$, since f is t -resilient and $x \mapsto \text{Tr}_{B/\mathbb{Z}_{p^r}}(r s_{12} \cdot x)$ is a balanced map, from (18) the claim follows:

$$d_H(u_{s_0,w_0}, u_{s_1,w_1}) = q^{r mn} (q^{r-1} - q^{r-2}).$$

If $(s_{02}, s_{12}) = (0, 0)$, also from (18) we obtain

$$d_H(u_{s_0,w_0}, u_{s_1,w_1}) = \sum_{x \in B^n} w_h(v_{s_2,w_2}(x)) = \sum_{x \in B^n} w_h(s_{22} + w_2) = q^{r mn} (q^{r-1} - q^{r-2})$$

because $s_{22} + w_2 \in A - p^{r-1}A$. \square

For each $k \in K = \mathbb{Z}_{q^{r(mn+1)}}$, let $e_k : S \rightarrow T$ be the map

$$s \mapsto e_k(s) = \pi_k(u_s) : k\text{-th entry of element } u_s. \tag{19}$$

The set of encoding rules in the proposed systematic authentication code is thus $E = (e_k)_{k \in K}$.

Proposition 3. The map $K \rightarrow E, k \mapsto e_k$, is one-to-one.

Proof. The proposition is clearly equivalent to the following statement: $\forall k_0, k_1 \in K$,

$$k_0 \neq k_1 \implies \exists s \in S : \pi_{k_0}(u_s) \neq \pi_{k_1}(u_s), \tag{20}$$

where u_s is given by Relation (17).

According to (17), each element $u_s, s \in S$, is the concatenation of q arrays $u_{s,w}$, each of length $q^{r mn}$. The index range $\{0, \dots, q^{r(mn+1)} - 1\}$ of the element u_s can be split as the concatenation of $q^{r mn+1}$ integer intervals

$$K_{x,w} = \{\text{indexes of entries with the value } \Phi(v_{s,w}(x))\},$$

with $(x, w) \in B^n \times p^{r-1}A$, and each integer interval $K_{x,w}$ has length q^{r-1} .

We recall at this point that $|B^n \times p^{r-1}A| = q^{r mn} q = q^{r mn+1}$. Let $\alpha_b : B^n \rightarrow \{0, \dots, q^{r mn} - 1\}$, $\alpha_a : p^{r-1}A \rightarrow \{0, \dots, q - 1\}$ be the corresponding natural bijections. Then, up to these enumerations and relation (4), we can identify $K_{x,w} \approx \{k \in K \mid k_{x,w} q^{r-1} \leq k \leq k_{x,w} q^{r-1} + (q^{r-1} - 1)\}$, where

$$\forall (x, w) \in B^n \times p^{r-1}A : k_{x,w} = \alpha_b(x)q + \alpha_a(w). \tag{21}$$

Let $k_0, k_1 \in K \approx \{0, \dots, q^{r(mn+1)} - 1\}$ be two keys such that $k_0 \neq k_1$. Depending on the intervals $K_{x,w}$ in which these keys fall, we can consider four mutually disjoint and exhaustive cases:

- Case I: $\exists w \in p^{r-1}A, \exists x \in B^n : k_0 \in K_{x,w} \ \& \ k_1 \in K_{x,w}$.
- Case II: $\exists w \in p^{r-1}A, \exists x, y \in B^n : x \neq y \ \& \ k_0 \in K_{x,w} \ \& \ k_1 \in K_{y,w}$.
- Case III: $\exists w_0, w_1 \in p^{r-1}A, \exists x \in B^n : w_0 \neq w_1 \ \& \ k_0 \in K_{x,w_0} \ \& \ k_1 \in K_{x,w_1}$.
- Case IV: $\exists w_0, w_1 \in p^{r-1}A, \exists x, y \in B^n : w_0 \neq w_1 \ \& \ x \neq y \ \& \ k_0 \in K_{x,w_0} \ \& \ k_1 \in K_{y,w_1}$.

The analysis of these cases, giving a full proof of the proposition, is rather extensive and certainly tedious. It is provided in full detail in [11]. \square

Proposition 4. For the authentication code defined by the relations (14) and (19), the following relations hold:

$$p_I = \frac{1}{q}, \quad p_S = \frac{1}{q}. \tag{22}$$

Proof. Let $s = (s_0, s_1, s_2) \in S$ and $x \in B^n$ be fixed. Then, the map $p^{r-1}A \rightarrow \mathbb{F}_q^{q^{r-1}}$,

$$w \mapsto \Phi(\text{Tr}_{B/A}(s_0 f(x) + s_1 \cdot x) + s_2 + w)$$

is one-to-one. For any $t \in T = \mathbb{F}_q$, we have

$$|\{k \in K \mid \pi_k(u_s) = t\}| = q^{r(mn+1)-1}, \tag{23}$$

where u_s is defined by relation (17). Since $|K| = q^{r(mn+1)}$, then, from (6), $p_I = \frac{1}{q}$.

Now, consider $s_0 = (s_{00}, s_{10}, s_{20}), s_1 = (s_{01}, s_{11}, s_{21}) \in S$ such that $s_0 \neq s_1$. For each $t_0, t_1 \in T$, and each $k \in K$, let $w \in p^{r-1}A$ and $x \in B^n$ be such that $k \in K_{x,w}$. Then, equivalent conditions for a pair of encoding sources are shown in the following:

$$\begin{aligned} \left. \begin{aligned} e_k(s_0) &= t_0 \\ e_k(s_1) &= t_1 \end{aligned} \right\} &\iff \left\{ \begin{aligned} \pi_k(u_{s_0}) &= t_0 && \& \\ \pi_k(u_{s_1}) &= t_1 \end{aligned} \right. \\ &\iff \left\{ \begin{aligned} \pi_k \circ \Phi(v_{s_0,w}(x)) &= t_0 && \& \\ \pi_k \circ \Phi(v_{s_1,w}(x)) - \pi_k \circ \Phi(v_{s_0,w}(x)) &= t_1 - t_0 \end{aligned} \right. \\ &\iff \left\{ \begin{aligned} \pi_k \circ \Phi(v_{s_0,w}(x)) &= t_0 && \& \\ \pi_k \circ \Phi(v_{s_1,w}(x)) - \pi_k \circ \Phi(v_{s_0,w}(x)) &= t_1 - t_0 \end{aligned} \right. \\ \text{Prop. 1} &\iff \left\{ \begin{aligned} \pi_k \circ \Phi(\text{Tr}_{B/A}(s_{00} f(x) + s_{10} \cdot x) + s_{20} + w) &= t_0 && \& \\ \pi_k \circ \Phi(\text{Tr}_{B/A}(s_{01} f(x) + s_{11} \cdot x) + s_{21}) &&& \\ -\pi_k(\text{Tr}_{B/A}(s_{00} f(x) + s_{10} \cdot x) + s_{20}) &= t_1 - t_0 \end{aligned} \right. \end{aligned}$$

From there, it can be seen that

$$|\{k \in K \mid (e_k(s_0) = t_0) \& (e_k(s_1) = t_1)\}| = q^{r(mn+1)-1} - d_H(u_{s_0,w}, u_{s_1,w}).$$

Now, from (7) and (23):

$$p_S = \frac{q^{r(mn+1)-1} - d_H(u_{s_0,w}, u_{s_1,w})}{q^{r(mn+1)-1}} \leq \frac{q^{r(mn+1)-1} - q^{r mn} (q^{r-1} - q^{r-2})}{q^{r(mn+1)-1}} = \frac{q^{r mn+r-2}}{q^{r mn+r-1}} = \frac{1}{q}.$$

\square

Observe at this point that instead of N in (14), it is possible to take the set $N' = \{b \in B^n \mid w_h(b) \leq \frac{t}{2}\}$ in order to produce a new systematic authentication code with the same impersonation and substitution probabilities as in (22).

3.4. A Second Systematic Authentication Code

Let p be a prime number, $r, \ell, n \in \mathbb{Z}^+$ and $q = p^\ell$. Let $A = \text{GR}(p^r, \ell)$ and $B = \text{GR}(p^r, \ell n)$ be the corresponding Galois rings of degrees ℓ and ℓn . Let

$$L = \{r_0 + r_1p + \dots + r_{r-2}p^{r-2} \mid r_0, \dots, r_{r-2} \in T(A)\} \subset A \setminus p^{r-1}A \cup \{0\}.$$

Observe that since $\langle p^{r-1} \rangle = \{ap^{r-1} \mid a \in T(A)\}$, if $a, b \in L$ then $a - b \in A \setminus p^{r-1}A$.

Let f be a bent function on B such that uf is a bent function for any unit $u \in S$ and let Φ be the Gray map on A . The proposed systematic authentication code, $\mathcal{A} = (S, T, K, E)$, is the following:

$$\begin{aligned} S &:= (T(B) \times B - \{(0,0)\}) \times L, \\ T &:= \mathbb{F}_q, \\ K &:= \mathbb{Z}_{q^{r(n+1)}}, \\ E &:= \{E_k(s) = pr_k(u_s), k \in K, s \in B\}, \end{aligned}$$

where for $s = (a, b, c) \in S$, $\beta \in p^{r-1}A = \{\beta_1, \beta_2, \dots, \beta_q\}$, $v_{s,\beta}(x) = \beta + \text{Tr}_{B/A}(af(x) + bx) + c$, $u_{s,\beta} = (\Phi(v_{s,\beta}(x)))_{x \in B}$, $u_s = (u_{s,\beta})_{\beta \in p^{r-1}A}$, and pr_k is the k -th projection map from $\mathbb{F}_q^{q^{r(n+1)}}$ onto \mathbb{F}_q , mapping u_s to its k -th coordinate.

Let L be as above and let $V = \{c \in B \mid \text{Tr}_{(B/A)}(c) \in L\}$. With the notation as above, a second systematic authentication code, $\mathcal{A}' = (S', T', K', E')$ is also proposed:

$$\begin{aligned} S' &:= \{(a, b, c) \in T(S) \times S \times V \mid (a, b) \neq (0,0)\}, \\ T' &:= \mathbb{F}_q, \\ K' &:= \mathbb{Z}_{q^{r(n+1)}}, \\ E' &:= \{E_k(s) = pr_k(u_s), k \in K', s \in S'\}. \end{aligned}$$

Note that the code \mathcal{A}' is a slight modification of the code \mathcal{A} : in the definition of the source space S for \mathcal{A} , the set L is taken while in the definition of the source space S' for \mathcal{A}' the set V is used.

The impersonation and substitution probabilities p_I and p_S can be upper-bounded.

Lemma 2. Let d_H be the Hamming distance on $\mathbb{F}_q^{q^{r(n+1)}}$. With the notation as above, for any $s_1 = (a_1, b_1, c_1), s_2 = (a_2, b_2, c_2) \in S, s_1 \neq s_2$, and any elements $\beta_1, \beta_2 \in p^{r-1}R$, we have

$$(q^{r-1} - q^{r-2})(q^{rn} - q^{rn/2}) \leq d_H(u_{s_1, \beta_1}, u_{s_2, \beta_2}) \leq (q^{r-1} - q^{r-2})(q^{rn} + q^{rn/2}).$$

Theorem 1. With the notation as above, the function $H : K \rightarrow E$ given by $H(k) = E_k$ is bijective.

Theorem 2. Let \mathcal{A} be the systematic authentication code as defined above. Then,

$$p_I = \frac{1}{q} \text{ and } p_S \leq \frac{1}{q} + \frac{q-1}{q^{\frac{rn+2}{2}}}.$$

4. Parameter Comparison with Other Codes

We summarize quite succinctly in Table 2 a parameter comparison of our codes with other codes based on the Gray map. There, as in Relation (15),

$$c_0 = q^m(q^{m(t-2)} - t) + 2(q^m - 1), \quad c_1 = q^m(q^m - 1) + 1, \quad c_2 = (q^m - 1)(r - 1).$$

D is an integer in the interval $[1, q^{\frac{n}{2}}]$, and, as stated in [9] Prop. 3.5, N is a positive integer such that $q^n - N > q^{\frac{n}{2}}((p + 1)(N + 1) - 2)$.

Table 2. Parameter comparison of the introduced code with other previously published codes.

Code	Sizes			Bound for p_I	Bound for p_S
	$ S $	$ K $	$ T $		
(1)	$c_0 + c_1n - c_2n^2q^{r-1}$	$q^{r(mn+1)}$	q	q^{-1}	q^{-1}
(2)	q^{2n}	$q^{r(n+1)}$	q^r	q^{-r}	$q^{-1} + (q - 1)q^{-(n+1)}$
(3)	q^{3n+1}	$q^{2(n+1)}$	q	q^{-1}	$q^{-1} + (q - 1)q^{-(n+1)}$
(4)	$q^n \binom{D - \lfloor \frac{D}{p^2} \rfloor}{\lfloor \frac{D}{p^2} \rfloor}$	q^{n+2}	q	q^{-1}	$q^{-1} + \frac{q-1}{q} \frac{D-1}{q^{\frac{n}{2}}}$
(5)	$q^{2n(N+1)}$	$q^2(q^n - N)$	q	q^{-1}	$q^{-1} + \frac{q-1}{q} \frac{q^{\frac{n}{2}}}{q^{n-N}}$ $((p + 1)(N + 1) - 2)$
(6)	$q^n \binom{D - \lfloor \frac{D}{p^2} \rfloor}{\lfloor \frac{D}{p^2} \rfloor} p^{-1}$	p^{n+1}	p	$\frac{p^{-1} + \frac{p-1}{p} \frac{D-1}{p^{\frac{n}{2}}}}{p}$	$\frac{p^{-1} + \frac{p^2+p-2}{p} \frac{D-1}{p^{\frac{n}{2}} - (p-1)(D-1)}}{p}$
(7)	$q^n \binom{D - \lfloor \frac{D}{p^\ell} \rfloor}{\lfloor \frac{D}{p^\ell} \rfloor}$	$q^{n+\ell}$	q	q^{-1}	$q^{-1} + \frac{q-1}{q} \frac{D-1}{q^{\frac{n}{2}}}$

The codes are the following: (1) Our code. (2) [17] Prop. 11 (3) [18] Thm. 4.3. (4) [9] Prop. 3.2. (5) [9] Prop. 3.5 (6). [9] Prop. 4.5. (7) [9] Thm. 5.1.

Our first code provides optimal values for p_I and p_S for all parameters q, m, n, r in which the code exists. For the codes in [9] the optimal values are obtained only if $D = 1$. However, in our code, the cardinality of the key space is greater than the product of the cardinalities of the source and tag spaces.

In [10], it is stated that a map $f : A^n \rightarrow A$ valued on a Galois ring $A = \text{GR}(p^r, \ell)$ is a bent function if

$$\left| \sum_{x \in A^n} e^{\frac{2\pi i}{p^r} \text{Tr}_{A/\mathbb{Z}_p}(f(x) - \langle u, x \rangle)} \right| = |A|^{\frac{n}{2}},$$

and it was shown that, for the special case of $r = 2$, whenever k and $q - 1 = p^\ell - 1$ are relatively prime, then for any $\alpha \in A$ and any unit $u \in A - pA$ in A , the map $A \rightarrow A, x \mapsto u(x^{kp+1} + \alpha x^p)$, is a bent function ($n = 1$).

Namely, for the special case of $r = 2$, a class of bent maps, closed by the multiplication of units in the Galois ring, can be used to build a systematic authentication code (SAC).

Later, the Gray map and the above-mentioned class of bent maps were used to build a new SAC, improving the impersonation and substitution probabilities. In fact, these constructions can be extended to any characteristic p^r , with $r > 1$, under the assumption that there exists a similar class of bent maps, closed by the multiplication of units in the Galois ring. In this case, the obtained SAC \mathcal{A} would have the parameters displayed in Table 3.

Table 3. Parameters of the obtained systematic authentication code (SAC) \mathcal{A} .

Code	Sizes			Bound for p_I	Bound for p_S
	$ S $	$ K $	$ T $		
\mathcal{A}	$(q^{n(t+1)} - 1)q^{(t-1)}$	$q^{t(n+1)}$	q	q^{-1}	$q^{-1} + (q - 1)q^{-\frac{tn+2}{2}}$
\mathcal{A}'	$(q^{n(t+1)} - 1)q^{(nt-1)}$	$q^{t(n+1)}$	q	q^{-1}	$q^{-1} + (q - 1)q^{-\frac{tn+2}{2}}$

In comparison with the values displayed at Table 2, we have that this last hypothetical construction would have more convenient parameters for the spaces: the source space is greater than the key space, and the tag space is rather small. Even more, it has a greater difference on the cardinality of the cardinality of the key space and the product of the cardinalities of the source and tag spaces. This is an advantage even when comparing with other SACs with no optimal impersonation and substitution probabilities. For instance, this last hypothetical construction would improve the probabilities and the space sizes of the codes in [4,8], although the code in [8] does not attain the optimal values for these probabilities.

Similar constructions were performed through resilient maps and functions generalizing bent maps, for any characteristic p^r , with $r > 1$.

5. Conclusions

An authentication code using the trace, the Gray maps, and the resilient functions on Galois rings were constructed. In this regard, the current construction is similar to the constructions in [9]. In order to diminish the substitution and impersonation probabilities, here we used resilient maps on Galois rings of general characteristic p^r , with p a prime number and r an integer greater or equal to 2, in contrast to the former approach based either on non-degenerate and rational maps on Galois rings of general characteristic [9], or on bent maps on Galois rings of characteristic p^2 . The current construction provides optimal substitution and impersonation probabilities, at the expense of growth of cardinalities and an elaborated space structure. In contrast with [9], the key space in our code is of greater cardinality than the source space. Our code attains optimal probability values, but it has a key space greater than the corresponding source space.

A second authentication code was built, and this code has convenient space sizes with a significant difference between the key space and the source space, and a small cardinality in the tag space. The probabilities are rather small, but the substitution probability is not optimal. However, this second construction is conditioned to the existence of a class of bent functions closed under the multiplication by units in the corresponding Galois ring. We look towards the proof of the existence of this necessary class of bent functions.

Author Contributions: The three authors contributed equally to conceptualization and formal analysis of this paper.

Funding: This research received no external funding.

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

References

1. Chor, B.; Goldreich, O.; Håstad, J.; Friedman, J.; Rudich, S.; Smolensky, R. The Bit Extraction Problem of t -Resilient Functions (Preliminary Version). In Proceedings of the 26th Annual Symposium on Foundations of Computer Science (FOCS), Portland, OR, USA, 21–23 October 1985; pp. 396–407.
2. Bennett, C.H.; Brassard, G.; Robert, J.M. Privacy Amplification by Public Discussion. *SIAM J. Comput.* **1988**, *17*, 210–229.

3. Rueppel, R. *Analysis and Design of Stream Ciphers*; Communications and Control Engineering; Springer: Berlin, Germany, 1986.
4. Ding, C.; Niederreiter, H. Systematic authentication codes from highly nonlinear functions. *IEEE Trans. Inf. Theory* **2004**, *50*, 2421–2428.
5. Carlet, C.; Ding, C.; Niederreiter, H. Authentication Schemes from Highly Nonlinear Functions. *Des. Codes Cryptogr.* **2006**, *40*, 71–79.
6. Ding, C.; Helleseht, T.; Kløve, T.; Wang, X. A Generic Construction of Cartesian Authentication Codes. *IEEE Trans. Inf. Theory* **2007**, *53*, 2229–2235.
7. Stinson, D.R. Combinatorial characterizations of authentication codes. *Des. Codes Cryptogr.* **1992**, *2*, 175–187.
8. Chanson, S.; Ding, C.; Salomaa, A. Cartesian authentication codes from functions with optimal nonlinearity. *Theor. Comput. Sci.* **2003**, *290*, 1737–1752.
9. Özbudak, F.; Saygi, Z. Some constructions of systematic authentication codes using Galois rings. *Des. Codes Cryptogr.* **2006**, *41*, 343–357.
10. Carlet, C.; Ku-Cauich, J.C.; Tapia-Recillas, H. Bent functions on a Galois ring and systematic authentication codes. *Adv. Math. Commun.* **2012**, *6*, 249–258.
11. Ku-Cauich, J.C.; Morales-Luna, G.; Tapia-Recillas, H. Proof of Correspondence between Keys and Encoding Maps in an Authentication Code. Technical Report. *arXiv* **2017**, arXiv:1703.08147.
12. McDonald, B. *Finite Rings with Identity*; Pure and Applied Mathematics Series; Marcel Dekker Incorporated: New York, NY, USA, 1974.
13. Wan, Z. *Lectures on Finite Fields and Galois Rings*; World Scientific: Singapore, 2003.
14. 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.
15. Carlet, C. *More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings*; EUROCRYPT; Fumy, W., Ed.; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1233, pp. 422–433.
16. Zhang, X.M.; Zheng, Y. Cryptographically resilient functions. *IEEE Trans. Inf. Theory* **1997**, *43*, 1740–1747.
17. Ku-Cauich, J.C.; Morales-Luna, G. Authentication codes based on resilient Boolean maps. *Des. Codes Cryptogr.* **2015**, 1–15, doi:10.1007/s10623-015-0121-3.
18. 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. Discret. Math.* **2013**, *27*, 1159–1170.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).