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

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

Juan Carlos Ku-Cauich · Guillermo Morales-Luna · Horacio Tapia-Recillas

Received: June 22, 2015/ Accepted: date

Abstract A new systematic authentication scheme based on the Gray map over Galois rings is introduced. The Gray map determines an isometry between the Galois ring and a vector space over a Galois field. The introduced code attains optimal impersonation and substitution probabilities.

keywords Authentication codes; optimality against impersonation and substitution attacks; Gray map; Galois rings.

1 Introduction

Resilient maps were introduced in 1985 by Chor *et al.* [4] and independently by Bennett*et al.* [1], in the context of key distribution and quantum cryptography protocols. Resilient maps have been used also in the generation of random sequences aimed to stream ciphering [10].

We introduce a new authentication systematic code with the purpose to optimally reduce the success probabilities of impersonation and substitution attacks.

In a former construction [7], two codes on Galois rings were introduced based on resilient maps, in a similar manner as in [3].

The authors acknowledge the support of Mexican Conacyt

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

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

Horacio Tapia-Recillas
Departamento de Matemáticas, Universidad Autónoma Metropolitana-I, Mexico City, Mexico, E-mail: htr@xanum.uam.mx

The current code construction is based mainly on the Gray map and it is in line with previously constructed codes using rational, non-degenerated and bent functions on Galois rings and also with other codes that use compositions of maps and the generalized Gray map on Galois rings [6,8,9].

Here, through the generalized Gray map and resilient maps on Galois rings we obtain minimal upper bounds for the attack probabilities, improving in this way former codes. Indeed, the obtained impersonation and substitution are optimal. However, the introduced code diminishes the source sate space with respect to the tag and key spaces. We introduce precise characteristics on Galois rings of the notions of resilient maps and generalized Gray function. The introduced construction over Galois rings is translated into finite fields via the Gray map, providing thus similar codes on Galois fields as those in [7].

The paper is organized as follows: In Section 2 we recall the basic construction of the Gray map. Then in Section 3 we introduce a new systematic authentication code based on the Gray map. At Subsection 3.1 we recall the general construction of a systematic authentication code, at Subsection 3.2 we give a precise definition of the new code and at Subsection 3.3 we show its main properties, in a rather long but exhaustive way we prove that the key space is in a bijective correspondence with the set of encoding maps.

2 The Gray map

Let p be a prime number and $r, \ell, m \in \mathbb{Z}^+$. Let us write $q = p^\ell$. Let $A = \mathrm{GR}(p^r, \ell)$ and $B = \mathrm{GR}(p^r, \ell m)$ be the corresponding Galois rings, A is an extension of $\mathbb{Z}_{p^r}$ and B is an extension of A. Let $T_{B/A} : B \to A$, $T_{B/\mathbb{Z}_{p^r}} : B \to \mathbb{Z}_{p^r}$ and $T_{A/\mathbb{Z}_{p^r}} : A \to \mathbb{Z}_{p^r}$ be the corresponding trace maps, and let pA and pB denote the sets of zero divisors of A and B respectively.

Firstly, let us recall well known facts [9]:

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

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

Let us assume, from now on, that $r \geq 2$. The *homogeneous weight* on the ring A is the map [6]

$$w_h : A \to \mathbb{N} \quad , \quad u \mapsto w_h(u) = \left(q^{r-1} - q^{r-2}\right) - \frac{1}{q} \sum_{x\in A-pA} e^{\frac{2\pi}{p^r} i\, T_{A/\mathbb{Z}_{p^r}}(ux)} \qquad (1)$$

and according to Lemma 1,

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

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

Let us define the *Gray map* which relates Galois rings and Galois fields. Let $\mathbb{F}_q^q$ be the q-dimensional vector space over the Galois field $\mathbb{F}_q$. Let $\otimes$ denote the Kroenecker product

$$\mathbb{F}_q^m \times \mathbb{F}_q^n \to \mathbb{F}_q^{mn}\ ,\ \left((u_i)_i\,, (v_j)_j\right) \mapsto (u_i)_i \otimes (v_j)_j = \left(w_{in+j} = u_i v_j\right)_{i,j}\,,$$

and let us iterate this product "by the right":

$$\bigotimes_{k=0}^{n} v_k = \left(\bigotimes_{k=0}^{n-1} v_k\right) \otimes v_n.$$

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 Kroenecker delta, $\mathbf{1}^{(q)} = (1, \ldots, 1) = \sum_{j=0}^{q-1} e_j \in \mathbb{F}_q^q$, the vector with constant entries equal to 1, and $\rho : A \to \mathbb{F}_p$ the reduction modulus p map. Let

$$T(A) = \{0\} \cup \left(\xi_A^j\right)_{j=0}^{q-2}$$

be a set of Teichmüller representatives at A and let

$$\Xi = (0, \rho(\xi_A), \ldots, \rho(\xi_A^{q-2}), \rho(\xi_A^{q-1})) \in \mathbb{F}_q^q.$$

For each index $i = 0, \ldots, r-2$ let

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

(here, for any $v \in \mathbb{F}_q^q$, $v^{\otimes 0} = [1]$ and $v^{\otimes(k+1)} = v^{\otimes k} \otimes v$).

For each $k \in \mathbb{Z}^+$ let $[y]_k = y\mathbf{1}^{(k)} = (\underbrace{y, \ldots, y}_{k\text{-times}})$.

From relation (3) we see that 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 $j = 0, \ldots, q-1$.

Then, the vector ϕ_i can be efficiently constructed: given an index k, with $0 \le k \le q^{r-1} - 1$, let $k_0 = k \bmod q^{r-1-i}$ and let $k_i = \lfloor \frac{k_0}{q^{r-2-i}} \rfloor$. Then $\phi_i(k)$ is the k_i-th coordinate of Ξ.

In summary, for each $i = 0, \ldots, r-2$, ϕ_i defined by (3) can be expressed as:

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

where we are using the notation introduced immediately after the relation (3). As a last vector, let us define

$$\phi_{r-1} = [1]_{q^{r-1}}$$

The *Gray map* is defined as follows

$$\begin{aligned} \Phi : \mathrm{GR}\left(p^r, \ell\right) = A &\to \mathbb{F}_q^{q^{r-1}} \\ \sum_{i=0}^{r-1} r_i p^i &\mapsto \Phi\left(\sum_{i=0}^{r-1} r_i p^i\right) = \sum_{i=0}^{r-1} \rho(r_i)\, \phi_i \end{aligned} \quad (5)$$

where the elements of A are represented in their p-adic form.

In particular, for the special case of $r = 2$, we have

$$\phi_0 = (0, \rho(\xi_A), \ldots, \rho(\xi_A^{q-2}), \rho(\xi_A^{q-1})) \quad , \quad \phi_1 = (1, 1, \ldots, 1, 1) \in \mathbb{F}_q^q.$$

Then the Gray map, as defined by (5), equals, for any $r_0 + r_1 p \in \mathrm{GR}\left(p^2, \ell\right)$:

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

which coincides with the definition given at [9].

The vector space $\mathbb{F}_q^{q^{r-1}}$ can be endowed of 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 two propositions:

Proposition 1 *The following assertions hold:*

1. **Isometry** *[6]. The Gray map is an isometry between the Galois ring A and the vector space $\mathbb{F}_q^{q^{r-1}}$:*

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

2. *The Gray map preserves addition [8]:*

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

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

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

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 he/she accepts s', otherwise the message m' is rejected

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

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

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

3.2 A new systematic authentication code

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

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

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

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 [2], we have that for any $n \in \mathbb{Z}^+$, if B is a Galois ring and $f_0 : B^n \to B^n$ 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 $f_1 : B^n \to B$ is any map, then the map $f : B^{2n} \to B$, $(x, y) \mapsto x \cdot f_0(y) + f_1(y)$ is a t-resilient map.

Let us build in this section a systematic authentication code using Gray maps.

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

Let us denote by $U(B) = (B - pB) \cup \{0\}$ the set of elements at the Galois ring B that are either units or zero.

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

- For $a \in B - pB$, the map $B^n \to B$, $x \mapsto a\, f(x)$, is t-resilient, hence it is also balanced.
- For $a \in B - pB$, the map $B^n \to B$, $x \mapsto T_{B/\mathbb{Z}_{p^r}}(a\, f(x))$, is balanced (as composition of balanced maps).
- As a more general result than Corollary 2 of [11], we have that the map

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

  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 $(a, b) \in (B - pB) \times B^n$.
- Let us recall that the Fourier transform of af is the map $B \to \mathbb{C}$,

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

  As shown in [2], $\zeta_{af}(b) = 0$ under the same conditions as the above assertion, just because the map $x \mapsto T_{B/\mathbb{Z}_{p^r}}(af(x) + b \cdot x)$ is balanced.

Let $T(A)$ and $T(B)$ be sets of the Teichmüller representatives of A and B respectively. Let us remark that the principal ideal generated by p^{r-1} within A can be expressed as $p^{r-1}A = \{a\, p^{r-1} |\ a \in T(A)\}$.

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 basis of B^n. For any $b \in T(B)^n$, let

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

then $|X_{b,t}| = n - t + 1$. Let

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

thus $|N| = q^{m(t-1)} + (n - (t-1))q^m$. Let

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

Then, $|L| = q^{r-1}$, $L \subset (A - p^{r-1}A) \cup \{0\}$ and also

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

Let $\eta = \{\eta_k\}_{k=0}^{(r-1)n-1}$ be an $(r-1)n$-subset of $T(A) - \{0,1\}$, and let

$$D_\eta = \left\{(\eta_{(i-1)n+j}, p^i e_j) |\ 1 \le i \le r-1\,,\ 0 \le j \le n-1\right\}. \tag{11}$$

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

Let us assume that $T(B) = \{0\} \cup \left(\xi_B^k\right)_{k=0}^{q^m-2}$ and let

$$G(T(B)) = \{\xi_B^k |\ \gcd(k, q^m-1) = 1\}$$

be the set of powers of ξ_B with exponent relatively prime with $q^m - 1$. Let $\theta = \{\theta_j\}_{j=0}^{n-1}$ be an n-sequence of $G(T(B))$ (repetitions are allowed), and let $\zeta \in T(B) - \{0\}$. For each integer index k, with $0 \le k \le q^m - (r-1)n - 2$ let

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

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

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

$$T_{\eta\theta\zeta} = D_\eta \cup \bigcup_{k=0}^{q^m-(r-1)n-2} T_{\theta\zeta_k k}. \tag{12}$$

Then $T_{\eta\theta\zeta} \subset B \times B^n$, and

$$\begin{aligned} |T_{\eta\theta\zeta}| &= (r-1)n + (q^m - 1 - (r-1)n)(q^m-1)n \\ &= \left[(r-1) + \left[(q^m-1) - (r-1)n\right](q^m-1)\right] n \end{aligned}$$

Let

$$\begin{aligned} S = \quad & \{0\} \times (N - \{0\}) \times L \cup \\ & T_{\eta\theta\zeta} \times L \cup \\ & (T(B) - (\{0\} \cup \eta)) \times \{0\} \times L \\ T = {} & \mathbb{F}_q \\ K = {} & \mathbb{Z}_{q^{r(mn+1)}} \end{aligned} \tag{13}$$

Certainly, at this point the definition of the source set S is quite unnatural. However, defined in this way, it guarantees a distance between elements of special form (see Proposition 2 below) leading to optimality results (see Proposition 4 below), while preserving the balancedness of the maps $x \mapsto T_{B/\mathbb{Z}_{p^r}}(af(x) + b \cdot x)$, for a t-resilient map f. The special form of S also allows to prove that the correspondence between keys and encoding maps is one-to-one (see Proposition 3 below).

From relations (13) we have $S \subset B \times B^n \times A$, and

$$\begin{aligned} |S| = {} & \left(\left(q^{m(t-1)} + (n-(t-1))q^m - 1\right) + \right. \\ & \left((r-1) + ((q^m-1) - (r-1)n)\,(q^m-1))\,n + \right. \\ & \left.(q^m - ((r-1)n+1))\right) q^{r-1} \\ = {} & \Big(\quad \left(q^m(q^{m(t-2)} - t) + 2(q^m-1)\right) \\ & + n\ (q^m(q^m-1)+1) \\ & - n^2(q^m-1)(r-1) \quad \Big)\, q^{r-1} \\ |T| = {} & q \\ |K| = {} & q^{r(mn+1)}. \end{aligned} \tag{14}$$

The introduced construction imposes the supplementary condition

$$(r-1)(n+1) < p^m - 1.$$

3.3 Main characteristics of the new code

Let $\Phi : A \to \mathbb{F}_q^{q^{r-1}}$ be the Gray map on A as defined by (5).

We observe that for any $y = \sum_{i=0}^{r-2} a_i p^i \in L$, with $(a_0, \ldots, a_{r-2}) \in T(A)^{r-1}$ (see (10)), the evaluation of Φ at y, according with (5), is

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

We remark also that, since $q-1$ is even, for any ξ generating T_A, either $-\xi \in T_A$ or $-1 \in T_A$, thus the following implication holds:

$$\forall z \in A \, \forall d \in \{1, \ldots, q-1\} : \ \left[z^d \in T_A \implies -z^d \in T_A \right].$$

Hence, if the p-adic form of an element in A is $z = \sum_{k=0}^{s-1} z_k p^k$ then the p-adic form of $-z$ is $-z = \sum_{k=0}^{s-1} (-z_k) p^k$.

Let $f : B^n \to B$ be a t-resilient map. For each $s = (s_0, s_1, s_2) \in S$ and each $w \in p^{r-1}A$ let us consider the map

$$\begin{aligned} v_{s,w} : B^n &\to A \\ x &\mapsto v_{s,w}(x) = T_{B/A}(s_0 f(x) + s_1 \cdot x) + s_2 + w \\ &\qquad = \gamma_{s_0 s_1 f}(x) + s_2 + w \end{aligned} \tag{15}$$

(see relation (8) above). Let us define the following arrays:

$$\begin{aligned} u_{s,w} &= \left(\Phi\left(v_{s,w}(x)\right)\right)_{x \in B^n} \in \left(\mathbb{F}_q^{q^{r-1}}\right)^{q^{rmn}} \\ u_s &= \left(u_{s,w}\right)_{w \in p^{r-1}A} \in \left(\mathbb{F}_q^{q^{r-1}}\right)^{q^{rmn+1}}. \end{aligned} \tag{16}$$

Since $\left|p^{r-1}A\right| = q$, we have $\left(\mathbb{F}_q^{q^{r-1}}\right)^{q^{rmn+1}} \simeq \mathbb{F}_q^{q^{r(mn+1)}}$, 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 $f : B^n \to B$ 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 equation holds:

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

Proof Let $s_2 = s_0 - s_1$ and $w_2 = w_0 - w_1$. Then:

$$\begin{aligned}
d_H(u_{s_0,w_0}, u_{s_1,w_1}) &= \sum_{x\in B^n} d_H\left(\Phi\left(v_{s_0,w_0}(x)\right), \Phi\left(v_{s_1,w_1}(x)\right)\right) \\
&\overset{(i)}{=} \sum_{x\in B^n} d_h\left(v_{s_0,w_0}(x), v_{s_1,w_1}(x)\right) \\
&= \sum_{x\in B^n} w_h\left(v_{s_0,w_0}(x) - v_{s_1,w_1}(x)\right) \\
&= \sum_{x\in B^n} w_h\left(v_{s_2,w_2}(x)\right) \\
&\overset{(ii)}{=} \sum_{x\in B^n} \left(\left(q^{r-1} - q^{r-2}\right) - \frac{1}{q} \sum_{r_0\in A-pA} e^{\frac{2\pi}{p^r} i\, T_{A/\mathbb{Z}_{p^r}}(r_0\, v_{s_2,w_2}(x))} \right) \\
&= q^{rmn}\left(q^{r-1} - q^{r-2}\right) \\
&\quad -\frac{1}{q} \sum_{x\in B^n} \sum_{r_0\in A-pA} e^{\frac{2\pi}{p^r} i\, T_{A/\mathbb{Z}_{p^r}}(r_0\, v_{s_2,w_2}(x))} \\
&\overset{(iii)}{=} q^{rmn}\left(q^{r-1} - q^{r-2}\right) \\
&\quad -\frac{1}{q} \sum_{r_0\in A-pA} e^{\frac{2\pi}{p^r} i\, T_{A/\mathbb{Z}_{p^r}}(r_0\, w_2)} e^{\frac{2\pi}{p^r} i\, T_{A/\mathbb{Z}_{p^r}}(r_0\, s_{22})} \\
&\qquad \sum_{x\in B^n} e^{\frac{2\pi}{p^r} i\, T_{B/\mathbb{Z}_{p^r}}(r_0\, s_{02} f(x) + r_0\, s_{12}\cdot x)}
\end{aligned} \tag{17}$$

(equality (i) holds because Φ is an isometry, equality (ii) follows from the defining relation (1), and equality (iii) is due to relation (15)).

If $(s_{02}, s_{12}) \neq (0,0)$, since f is t-resilient and $x \mapsto T_{B/\mathbb{Z}_{p^r}}(r\, s_{12}\cdot x))$ is a balanced map, from (17) the claim follows:

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

If $(s_{02}, s_{12}) = (0,0)$, also from (17) we obtain

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

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

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

$$s \mapsto e_k(s) = \pi_k(u_s) : \text{ the } k\text{-th entry of the array } u_s. \tag{18}$$

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

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

Proof The proposition is clearly equivalent to the following statement:

$$\forall k_0, k_1 \in K : \ [k_0 \neq k_1 \implies \exists s \in S : \ \pi_{k_0}(u_s) \neq \pi_{k_1}(u_s)] \tag{19}$$

where u_s is given by the relation (16).

According to (16), each array u_s, $s \in S$, is the concatenation of q arrays $u_{s,w}$, each of length q^{rmn}. The index range $\{0, \ldots, q^{r(mn+1)} - 1\}$ of the array u_s can be split as the concatenation of q^{rmn+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

$$\left|B^n \times p^{r-1}A\right| = q^{rmn}q = q^{rmn+1}.$$

Let $\alpha_b : B^n \to \{0, \ldots, q^{rmn} - 1\}$, $\alpha_a : p^{r-1}A \to \{0, \ldots, q-1\}$ be corresponding natural bijections. Then, up to these enumerations and the representation sketched at relation (4), we may identify

$$K_{x,w} \approx \{k \in K |\ k_{x,w}q^{r-1} \leq k \leq k_{x,w}q^{r-1} + (q^{r-1} - 1)\},$$

where

$$k_{x,w} = \alpha_b(x)q + \alpha_a(w) \quad , \quad \forall (x, w) \in B^n \times p^{r-1}A. \tag{20}$$

Let $k_0, k_1 \in K \approx \{0, \ldots, q^{r(mn+1)} - 1\}$ be two keys such that $k_0 \neq k_1$. Depending on the intervals $K_{x,w}$ in which these keys fall, we may consider four 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, providing a full proof of the proposition, is rather extensive, thus we postpone it to the appendix. □

Proposition 4 *For the authentication scheme defined by the relations (13) and (18) the following equations hold:*

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

Proof Let $s = (s_0, s_1, s_2) \in S$ and $x \in B^n$ be fixed, then the map

$$p^{r-1}A \to \mathbb{F}_q^{q^{r-1}} \ , \ w \mapsto \Phi\left(T_{B/A}(s_0 f(x) + s_1 \cdot x) + s_2 + w\right)$$

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

$$|\{k \in K |\ \pi_k(u_s) = t\}| = q^{r(mn+1)-1}. \tag{22}$$

where u_s is defined by relation (16). Since $|K| = q^{r(mn+1)}$, we have, from (6), $p_I = \frac{1}{q}$.

Now, we 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,

$$\left.\begin{array}{l} e_k(s_0) = t_0 \\ e_k(s_1) = t_1 \end{array}\right\} \iff \left\{\begin{array}{l} \pi_k(u_{s_0}) = t_0 \ \ \& \\ \pi_k(u_{s_1}) = t_1 \end{array}\right.$$

$$\iff \left\{\begin{array}{rl} \pi_k \circ \Phi(v_{s_0,w}(x)) = t_0 & \& \\ \pi_k \circ \Phi(v_{s_1,w}(x)) - \pi_k \circ \Phi(v_{s_0,w}(x)) = t_1 - t_0 & \end{array}\right.$$

$$\iff \left\{\begin{array}{rl} \pi_k \circ \Phi(v_{s_0,w}(x)) = t_0 & \& \\ \pi_k \circ \Phi(v_{s_1,w}(x)) - \pi_k \circ \Phi(v_{s_0,w}(x)) = t_1 - t_0 & \end{array}\right.$$

$$\overset{\text{Prop. 1}}{\iff} \left\{\begin{array}{rl} \pi_k \circ \Phi(T_{B/A}(s_{00}\, f(x) + s_{10} \cdot x) + s_{20} + w) = t_0 & \& \\ \pi_k \circ \Phi(T_{B/A}(s_{01}\, f(x) + s_{11} \cdot x) + s_{21}) & \\ \quad -\pi_k(T_{B/A}(s_{00}\, f(x) + s_{10} \cdot x) + s_{20}) = t_1 - t_0 & \end{array}\right.$$

From here, it can be seen that

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

Now, from (7), (22), we have:

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

□

Observe at this point that it is possible to take, instead of N at (13), the set $N' = \{b \in B^n |\ w_h(b) \leq \frac{t}{2}\}$ in order to produce a new systematic authenticatication code with the same impersonation and substitution probabilities as in (21).

4 Conclusions

We have constructed an authentication code using the trace and the Gray maps. In this regard, the current construction is similar to former constructions [8,9]. In order to diminish the substitution and impersonation probabilities, we used here resilient maps on Galois rings of general characteristic p^r, with p a prime number and r an integer greater or equal than 2, in contrast with the former approach based either on non-degenerate and rational maps on Galois rings of general characteristic [9], or on bent maps at Galois rings of characteristic p^2 [8]. The current construction provides optimal substitution and impersonation probabilities, at the cost of cardinalities growth and an elaborated space structure.

References

1. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210–229 (1988)
2. Carlet, C.: More correlation-immune and resilient functions over Galois fields and Galois rings. In: W. Fumy (ed.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 1233, pp. 422–433. Springer (1997)
3. Carlet, C., Ku-Cauich, J.C., Tapia-Recillas, H.: Bent functions on a Galois ring and systematic authentication codes. Adv. in Math. of Comm. **6**(2), 249–258 (2012)
4. 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., Morales-Luna, G.: Authentication schemes based on resilient maps. IACR Cryptology ePrint Archive **2014**, 547 (2014). URL http://eprint.iacr.org/2014/547
8. 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)
9. Özbudak, F., Saygi, Z.: Some constructions of systematic authentication codes using Galois rings. Des. Codes Cryptography **41**(3), 343–357 (2006)
10. Rueppel, R.: Analysis and design of stream ciphers. Communications and control engineering series. Springer (1986)
11. Zhang, X.M., Zheng, Y.: Cryptographically resilient functions. IEEE Transactions on Information Theory **43**(5), 1740–1747 (1997)

A Proof of Proposition 3

Let us present in full detail the proof of Proposition 3. The plan of the proof is sketched as Plan 1. The referenced lemmas appear immediately after.

Lemma 2 *Under the condition arriving at statement* **I** *in Plan 2, the implication 19 holds.*

if *Case I holds* **then**
  I. See Lemma 2
else
  if *Case II holds* **then**
    let $k_{00} = k_0 - k_{x,w}$ and $k_{10} = k_1 - k_{y,w}$;
    if $k_{00} = k_{10}$ **then**
      proceed as in Plan 2
    else
      proceed as in Plan 3
    end
  else
    if *Case III holds* **then**
      let $k_{00} = k_0 - k_{x,w_0}$ and $k_{10} = k_1 - k_{x,w_1}$, according to (20) ;
      if $k_{00} = k_{10}$ **then**
        III.0 See Lemma 12
      else
        pick $(s_0, s_1) \in \{0\} \times (N - \{0\})$ arbitrarily ;
        if $\pi_{k_{00}} \circ \Phi \left(T_{B/A}(s_0\, f(x) + s_1 \cdot x) + w_0\right) =$
        $\pi_{k_{10}} \circ \Phi \left(T_{B/A}(s_0\, f(x) + s_1 \cdot x) + w_1\right)$ **then**
          III.1.0 See Lemma 13
        else
          III.1.1 See Lemma 14
        end
      end
    else
      (at this point, *Case IV* necessarily does hold)
      let $k_{00} = k_0 - k_{x,w_0}$ and $k_{10} = k_1 - k_{x,w_1}$, according to (20) ;
      if $\pi_{k_{00}} \circ \Phi \left(T_{B/A}(f(x))\right) = \pi_{k_{10}} \circ \Phi \left(T_{B/A}(f(y))\right)$ **then**
        IV.0 See Lemma 15
      else
        IV.1 See Lemma 16
      end
    end
  end
end

Plan 1 Plan of the proof of Proposition 3.

Proof Let $(s_0, s_1) \in \{0\} \times (N - \{0\})$ (see relation (13)). Let us write in p-adic form

$$T_{B/A}(s_0 f(x) + s_1 \cdot x) = \sum_{i=0}^{r-2} a_i p^i + a_{r-1} p^{r-1}.$$

For each $k \in \{0, \ldots, r-2\}$, there exists $y^{(k)} = \sum_{i=0}^{r-2} y_{ik} p^i \in L$ such that

$$T_{B/A}(s_0 f(x) + s_1 \cdot x) + y^{(k)} = \begin{cases} a_k p^k + a_{r-1} p^{r-1} & \text{if } a_k \neq 0 \\ y_{kk} p^k + a_{r-1} p^{r-1} & \text{if } a_k = 0 \ \&\ y_{kk} \neq 0 \end{cases}$$

Thus,

$$\Phi \left(T_{B/A}(s_0 f(x) + s_1 \cdot x) + y^{(k)} + w\right)$$

$$= \begin{cases} \Phi \left(a_k p^k\right) + \Phi \left(a_{r-1} p^{r-1} + w\right) & \text{if } a_k \neq 0 \\ \Phi \left(y_{kk} p^k\right) + \Phi \left(a_{r-1} p^{r-1} + w\right) & \text{if } a_k = 0 \ \&\ y_{kk} \neq 0 \end{cases}$$

choose $j \in \{0, \ldots, n-1\}$ such that the j-th entry of $x - y$ is not zero, namely $x_j - y_j \neq 0$;
if $x_j - y_j \in p^{r-1}B - \{0\}$ **then**
  II.0.0 See Lemma 3
else
  there are $\theta \in T_B - T_A$, and $t \leq r-1$ such that $T_{B/A}(\theta p^t(x_j - y_j)) \in p^{r-1}A - \{0\}$;
  if $T_{B/A}(x_j) = T_{B/A}(y_j)$ **then**
    let $\zeta \in T_A - \{0\}$ be such that $(\theta, (\zeta + \theta p^t)e_j) \in \bigcup_{k=0}^{q^m-(r-1)n-2} T_{\theta\zeta_k k}$ as defined at (12) ;
    we have

$$T_{B/A}(\zeta x_j) = \sum_{k=0}^{r-1} d_k p^k = T_{B/A}(\zeta y_j)$$

$$T_{B/A}(\theta p^t x_j) = \sum_{k=0}^{r-2} a_k p^k + a_{r-1}p^{r-1}$$

$$T_{B/A}(\theta p^t y_j) = \sum_{k=0}^{r-2} a_k p^k + b_{r-1}p^{r-1}$$

    with $a_{r-1} \neq b_{r-1}$;
    let $(s_0, s_1) = (\theta, (\zeta + \theta p^t)e_j)$;
    if $\pi_{k_{00}} \circ \Phi\left(T_{B/A}(\theta f(x))\right) = \pi_{k_{10}} \circ \Phi\left(T_{B/A}(\theta f(y))\right)$ **then**
      II.0.1.0.0 See Lemma 4
    else
      II.0.1.0.1 See Lemma 5
    end
  else
    II.0.1.1 **if** $\pi_{k_{00}} \circ \Phi\left(T_{B/A}(f(x))\right) = \pi_{k_{10}} \circ \Phi\left(T_{B/A}(f(y))\right)$ **then**
      There is a t, $0 \leq t \leq r-1$, such that $T_{B/A}(p^t(x_j - y_j)) \in p^{r-1}A - \{0\}$ (here the hypothesis $T_{B/A}(x_j) \neq T_{B/A}(y_j)$ is very important) ;
      if $t = 0$ **then**
        II.0.1.1.0.0 See Lemma 6
      else
        II.0.1.1.0.1 See Lemma 7
      end
    else
      II.0.1.1.1 See Lemma 8
    end
  end
end

Plan 2 First branch of Case II.

Last expressions can be evaluated by relation (5). We have that $(s_0, s_1, y^{(k)}) \in S$ and $w \in p^{r-1}A$.

Now, let $k_{00} = k_0 - k_{x,w}$ and $k_{10} = k_1 - k_{x,w}$. Let us consider several possibilities:

- $q \not| (k_{10} - k_{00})$: By taking $a_{r-2} \neq 0$, all other coefficients zero, and $s = (s_0, s_1, s_2)$, we have that the k_{00}-projection of $u_{s,w}$ (see (16)) differs to its k_{10}-projection, thus $\pi_{k_0}(u_s) \neq \pi_{k_1}(u_s)$.

let $j \in \{0, \ldots, n-1\}$ be such that $x_j - y_j \neq 0$;
if $x_j - y_j \in p^{r-1}B - \{0\}$ **then**
  II.1.0 See Lemma 9
else
  there exist $\theta \in (T_B - T_A) \cup \{1\}$ and $t \in \{1, \cdots, r-1\}$ such that $T_{B/A}(\theta p^t(x_j - y_j)) \in p^{r-1}A - \{0\}$;
  if $T_{B/A}(x_j) = T_{B/A}(y_j)$ **then**
    let $\zeta \in T_A - \{0\}$ be such that the pair $(s_0, s_1) = (\theta, (\zeta + \theta p^t)e_j)$ is included in the set $\bigcup_{k=0}^{q^m-(r-1)n-2} T_{\theta\zeta_k k}$ as defined at (12) ;
    if $\Phi\left(T_{B/A}(\theta f(x))\right) = \Phi\left(T_{B/A}(\theta f(y))\right)$ **then**
      II.1.1.0.0 See Lemma 10
    else
      II.1.1.0.1 See Lemma 11
    end
  else
    proceed as in statement **II.0.1.1** of Plan 2
  end
end

Plan 3 Second branch of Case II.

– $q|(k_{10} - k_{00})$ and ($\exists d$: $1 \leq d \leq r-1$ & $q^{d-1} \leq k_{10} - k_{00} < q^d$): By taking $a_{r-2-d} \neq 0$ and all other coefficients zero, and $s = (s_0, s_1, s_2)$, we have that the k_{00}-projection of $u_{s,w}$ differs to its k_{10}-projection, thus $\pi_{k_0}(u_s) \neq \pi_{k_1}(u_s)$.

□

Lemma 3 *Under the condition arriving at statement* **II.0.0** *in Plan 2, the implication 19 holds.*

Proof There is a $\theta \in T_B$ such that $T_{B/A}(\theta(x_j - y_j)) \in p^{r-1}B - \{0\}$. We express in their p-adic forms $T_{B/A}(\theta x_j)$ and $T_{B/A}(\theta y_j)$, namely

$$T_{B/A}(\theta x_j) = \sum_{k=0}^{r-1} a_k p^k \quad , \quad T_{B/A}(\theta y_j) = \sum_{k=0}^{r-1} b_k p^k. \tag{23}$$

Thus

$$\sum_{k=0}^{r-1}(a_k - b_k)p^k = (a_0 - b_0) + \sum_{k=1}^{r-1}(a_k - b_k)p^k \in p^{r-1}A - \{0\}$$

and consequently $a_0 - b_0 = 0$. Also

$$\sum_{k=1}^{r-1}(a_k - b_k)p^{k-1} = (a_1 - b_1) + \sum_{k=2}^{r-1}(a_k - b_k)p^k \in p^{r-2}A - \{0\}$$

and consequently $a_1 - b_1 = 0$. Successively, we get $\forall k \leq r-2$, $a_k = b_k$, and $(a_{r-1} - b_{r-1})p \in pA - \{0\}$. Hence $a_{r-1} \neq b_{r-1}$. And consequently:

$$\Phi\left(T_{B/A}(\theta x_j)\right) \neq \Phi\left(T_{B/A}(\theta y_j)\right).$$

Let $s_0 = 0$, $s_1 = \theta e_j$, $s_2 = 0$ and $s = (s_0, s_1, s_2) \in S$. Then, according to (15),

$$\begin{aligned}
\Phi\left(v_{s,w}(x)\right) &= \Phi\left(T_{B/A}(s_0\, f(x) + s_1 \cdot x) + s_2 + w\right) \\
&= \Phi\left(T_{B/A}(\theta x_j)\right) + \Phi\left(w\right) \\
&\neq \Phi\left(T_{B/A}(\theta y_j)\right) + \Phi\left(w\right) \\
&= \Phi\left(T_{B/A}(s_0\, f(y) + s_1 \cdot y) + s_2 + w\right) \\
&= \Phi\left(v_{s,w}(y)\right)
\end{aligned}$$

And, in particular,

$$\pi_{k_{00}} \circ \Phi\left(v_{s,w}(x)\right) \neq \pi_{k_{10}} \circ \Phi\left(v_{s,w}(x)\right).$$

Thus, implication (19) holds on these conditions. □

Lemma 4 *Under the condition arriving at statement* **II.0.1.0.0** *in Plan 2, the implication 19 holds.*

Proof Choose

$$\begin{aligned} s_2 &= d_{r-1}p^{r-1} + a_{r-1}p^{r-1} - T_{B/A}((\zeta + \theta p^t)x_j) \\ &= d_{r-1}p^{r-1} + b_{r-1}p^{r-1} - T_{B/A}((\zeta + \theta p^t)y_j). \end{aligned}$$

Then,

$$\begin{aligned} \Phi\left(v_{s,w}(x)\right) &= \Phi\left(T_{B/A}(s_0\, f(x) + s_1 \cdot x) + s_2 + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x) + (\zeta + \theta p^t)x_j) + s_2 + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x)) + d_{r-1}p^{r-1} + a_{r-1}p^{r-1} + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x))\right) + \Phi\left(d_{r-1}p^{r-1}\right) + \Phi\left(a_{r-1}p^{r-1}\right) + \Phi\left(w\right) \end{aligned}$$

Mutatis mutandis we get

$$\Phi\left(v_{s,w}(y)\right) = \Phi\left(T_{B/A}(\theta f(y))\right) + \Phi\left(d_{r-1}p^{r-1}\right) + \Phi\left(b_{r-1}p^{r-1}\right) + \Phi\left(w\right),$$

hence $\Phi\left(v_{s,w}(x)\right) \neq \Phi\left(v_{s,w}(y)\right)$. And, in particular,

$$\pi_{k_{00}} \circ \Phi\left(v_{s,w}(x)\right) \neq \pi_{k_{10}} \circ \Phi\left(v_{s,w}(x)\right).$$

Thus, implication (19) holds on these conditions. □

Lemma 5 *Under the condition arriving at statement* **II.0.1.0.1** *in Plan 2, the implication 19 holds.*

Proof Let $\theta \in T_B$ be as in Lemma 3 above and $(s_0, s_1, s_2) = (\theta, 0, 0)$. Then,

$$\begin{aligned} \Phi\left(v_{s,w}(x)\right) &= \Phi\left(T_{B/A}(\theta f(x)\right) + \Phi\left(w\right) \text{ and} \\ \Phi\left(v_{s,w}(y)\right) &= \Phi\left(T_{B/A}(\theta f(y)\right) + \Phi\left(w\right) \end{aligned}$$

hence $\pi_{k_{00}} \circ \Phi\left(v_{s,w}(x)\right) \neq \pi_{k_{10}} \circ \Phi\left(v_{s,w}(y)\right)$. □

Lemma 6 *Under the condition arriving at statement* **II.0.1.1.0.0** *in Plan 2, the implication 19 holds.*

Proof Let $s_0 = 0$, $s_1 = e_j$, $s_2 = 0$ and $s = (s_0, s_1, s_2) \in S$. Then as in Lemma 3 we conclude that $\pi_{k_{00}} \circ \Phi\left(v_{s,w}(x)\right) \neq \pi_{k_{10}} \circ \Phi\left(v_{s,w}(y)\right)$. □

Lemma 7 *Under the condition arriving at statement* **II.0.1.1.0.1** *in Plan 2, the implication 19 holds.*

Proof There is a pair $(s_0, s_1) = (\theta, p^t\, e_j)$ in the set D_η, as defined at (11), such that

$$\Phi\left(T_{B/A}(\theta f(x))\right) = \Phi\left(T_{B/A}(\theta f(y))\right)$$

since $\theta \in T_A - \{0\}$. We write in p-adic form

$$T_{B/A}(p^t x_j) = \sum_{i=0}^{r-2} a_i p^i + a_{r-1}p^{r-1} \;\&\; T_{B/A}(p^t y_j) = \sum_{i=0}^{r-2} a_i p^i + b_{r-1}p^{r-1}$$

with $a_{r-1} \neq b_{r-1}$. An adequate selection of s_2 gives

$$\begin{aligned}\Phi\left(v_{s,w}(x)\right) &= \Phi\left(T_{B/A}(\theta f(x) + T_{B/A}(p^t x_j) + s_2 + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x) + a_{r-1}p^{r-1} + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x)\right) + \Phi\left(a_{r-1}p^{r-1}\right) + \Phi\left(w\right).\end{aligned}$$

Similarly,

$$\Phi\left(v_{s,w}(y)\right) = \Phi\left(T_{B/A}(\theta f(y)\right) + \Phi\left(b_{r-1}p^{r-1}\right) + \Phi\left(w\right),$$

and the right sides of the above identities are different, thus the implication (19) holds on this case. □

Lemma 8 *Under the condition arriving at statement* **II.0.1.1.1** *in Plan 2, the implication 19 holds.*

Proof In this case, $\pi_{k_{00}} \circ \Phi\left(T_{B/A}(\eta_{(r-1)n} f(x))\right) \neq \pi_{k_{10}} \circ \Phi\left(\eta_{(r-1)n} T_{B/A}(f(y))\right)$ and there exists a value $\eta_{(r-1)n} \in T(A) - \{0\}$ such that $\eta_{(r-1)n}$ does not appear at η, just because $(r-1)(n+1) < p^m - 1$. Now, we choose $s_1 = 0 \in B^n$, $s_2 = 0$ and $s = (\eta_{(r-1)n}, 0, 0)$. Then,

$$\begin{aligned}\pi_{k_{00}} \circ \Phi\left(v_{s,w}(x)\right) &= \pi_{k_{00}} \circ \Phi\left(T_{B/A}(s_0\, f(x) + s_1 \cdot x) + s_2 + w\right) \\ &= \pi_{k_{00}} \circ \Phi\left(T_{B/A}(\eta_{(r-1)n} f(x)) + w\right) \\ &\neq \pi_{k_{10}} \circ \Phi\left(T_{B/A}(\eta_{(r-1)n} f(y)) + w\right) \\ &= \pi_{k_{10}} \circ \Phi\left(v_{s,w}(y)\right)\end{aligned}$$

and, consequently, the implication (19) holds. □

Lemma 9 *Under the condition arriving at statement* **II.1.0** *in Plan 3, the implication 19 holds.*

Proof There is a $\theta \in T_B$ such that $T_{B/A}(\theta(x_j - y_j))j \in p^{r-1}A - \{0\}$. By writing $T_{B/A}(\theta x_j)$ and $T_{B/A}(\theta y_j)$ in p-adic form as in (23) we have that, as in Lemma 3, for any $i \leq r-2$, $a_i = b_i$ and $a_{r-1} - b_{r-1} \in p^{r-1}B - \{0\}$. Let $(s_0, s_1, s_2) = \left(0, \theta e_j, -\sum_{i=0}^{r-2} a_i p^i\right)$. Then

$$\begin{aligned}\Phi\left(v_{s,w}(x)\right) &= \Phi\left(T_{B/A}(a_{r-1}p^{r-1}\right) + \Phi\left(w\right) \text{ and} \\ \Phi\left(v_{s,w}(y)\right) &= \Phi\left(T_{B/A}(b_{r-1}p^{r-1}\right) + \Phi\left(w\right)\end{aligned}$$

hence $\pi_{k_{00}} \circ \Phi\left(v_{s,w}(x)\right) \neq \pi_{k_{10}} \circ \Phi\left(v_{s,w}(y)\right)$. □

Lemma 10 *Under the condition arriving at statement* **II.1.1.0.0** *in Plan 3, the implication 19 holds.*

Proof There is a s_2 such that

$$\begin{aligned}\Phi\left(v_{s,w}(x)\right) &= \Phi\left(T_{B/A}(s_0\, f(x) + s_1 \cdot x) + s_2 + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x) + (\zeta + \theta p^t)x_j) + s_2 + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x)) + T_{B/A}(\zeta x_j) + s_2 + T_{B/A}(\theta p^t x_j) + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x)) + c_{r-1}p^{r-1} + a_{r-1}p^{r-1} + w\right) \\ &= \Phi\left(T_{B/A}(\theta f(x))\right) + \Phi\left(c_{r-1}p^{r-1}\right) + \Phi\left(a_{r-1}p^{r-1}\right) + \Phi\left(w\right)\end{aligned}$$

where we have used the p-adic forms displayed at Plan 2.

Mutatis mutandis we get

$$\Phi\left(v_{s,w}(y)\right) = \Phi\left(T_{B/A}(\theta f(y))\right) + \Phi\left(c_{r-1}p^{r-1}\right) + \Phi\left(b_{r-1}p^{r-1}\right) + \Phi\left(w\right),$$

hence $\Phi\left(v_{s,w}(x)\right) \neq \Phi\left(v_{s,w}(y)\right)$. And, in particular,

$$\pi_{k_{00}} \circ \Phi\left(v_{s,w}(x)\right) \neq \pi_{k_{10}} \circ \Phi\left(v_{s,w}(x)\right).$$

Thus, implication (19) holds on these conditions. □

Lemma 11 *Under the condition arriving at statement* **II.1.1.0.1** *in Plan 3, the implication 19 holds.*

Proof We may proceed as in Lemma 5 to show that implication (19) holds on these conditions. □

Lemma 12 *Under the condition arriving at statement* **III.0** *in Plan 1, the implication 19 holds.*

Proof For any $s = (s_0, s_1, s_2) \in S$ we have

$$\begin{aligned}\Phi(v_{s,w_0}(x)) - \Phi(v_{s,w_1}(x)) = &\ \Phi\left(T_{B/A}(s_0 f(x) + s_1 \cdot x) + s_2 + w_0\right)\\ &-\Phi\left(T_{B/A}(s_0 f(x) + s_1 \cdot x) + s_2 + w_1\right)\\ &= \Phi(w_0) - \Phi(w_1)\\ &\neq 0\end{aligned}$$

In particular,

$$\pi_{k_{00}} \circ \Phi(v_{s,w_0}(x)) \neq \pi_{k_{00}} \circ \Phi(v_{s,w_1}(x)).$$

Thus, implication (19) holds in this case as well. □

Lemma 13 *Under the condition arriving at statement* **III.1.0** *in Plan 1, the implication 19 holds.*

Proof If, written in its p-adic form, $T_{B/A}(s_0\, f(x) + s_1 \cdot x) = \sum_{i=0}^{r-1} a_i p^i$, then let $s_2 = -\sum_{i=0}^{r-2} a_i p^i$. As in Lemma 9, we will have

$$\pi_{k_{00}} \circ \Phi(v_{s,w_0}(x)) \neq \pi_{k_{10}} \circ \Phi(v_{s,w_1}(x)).$$

□

Lemma 14 *Under the condition arriving at statement* **III.1.1** *in Plan 1, the implication 19 holds.*

Proof Let $s_2 = 0$. We will have $\pi_{k_{00}} \circ \Phi(v_{s,w_0}(x)) \neq \pi_{k_{10}} \circ \Phi(v_{s,w_1}(x))$. □

Lemma 15 *Under the condition arriving at statement* **IV.0** *in Plan 1, the implication 19 holds.*

Proof In this case, $\pi_{k_{00}} \circ \Phi\left(T_{B/A}(\eta_{(r-1)n} f(x))\right) = \pi_{k_{10}} \circ \Phi\left(T_{B/A}(\eta_{(r-1)n} f(y))\right)$ with $\eta_{(r-1)n} \in T(A) - \{0\}$ such that $\eta_{(r-1)n} \notin \eta$.

Let $(s_0, s_1, s_2) = (\eta_{(r-1)n}, 0, 0)$. Then $\pi_{k_{00}} \circ \Phi(v_{s,w_0}(x)) \neq \pi_{k_{10}} \circ \Phi(v_{s,w_1}(x))$. □

Lemma 16 *Under the condition arriving at statement* **IV.1** *in Plan 1, the implication 19 holds.*

Proof Let $\eta \in T(A)$. Then,

$$\begin{aligned}\pi_{k_{00}} \circ \Phi\left(\eta T_{B/A}(f(x))\right) &= \eta \pi_{k_{10}} \circ \Phi\left(T_{B/A}(f(x))\right) \quad \text{and}\\ \pi_{k_{00}} \circ \Phi\left(\eta T_{B/A}(f(y))\right) &= \eta \pi_{k_{10}} \circ \Phi\left(T_{B/A}(f(y))\right),\end{aligned}$$

and then if there is $\eta \in T(A)$ such that

$$\pi_{k_{00}} \circ \Phi(w_0) + \pi_{k_{00}} \circ \Phi\left(\eta T_{B/A}(f(x))\right) = \pi_{k_{10}} \circ \Phi(w_1) + \pi_{k_{10}} \circ \Phi\left(\eta T_{B/A}(f(y))\right)$$

then this element is unique.

Let us choose $\zeta = \{\zeta_k\}_{k=0}^{q^m-(r-1)n-2}$, as was done in the relation (12). Thus, either

$$\pi_{k_{00}} \circ \Phi(w_0) + \pi_{k_{00}} \circ \Phi\left(\zeta_k T_{B/A}(f(x))\right) \neq \pi_{k_{10}} \circ \Phi(w_1) + \pi_{k_{10}} \circ \Phi\left(\zeta_k T_{B/A}(f(y))\right)$$

or

$$\pi_{k_{00}} \circ \Phi(w_0) + \pi_{k_{00}} \circ \Phi\left(\zeta_{k'} T_{B/A}(f(x))\right) \neq \pi_{k_{10}} \circ \Phi(w_1) + \pi_{k_{10}} \circ \Phi\left(\zeta_{k'} T_{B/A}(f(y))\right),$$

where $\zeta_k, \zeta_{k'} \in T(A) \cap \zeta$, $k \neq k'$. Let j be an index witnessing the relations above. Let $(s_0, s_1, s_2) = (\eta_j, 0, 0)$. Then $\pi_{k_{00}} \circ \Phi(v_{s,w_0}(x)) \neq \pi_{k_{10}} \circ \Phi(v_{s,w_1}(x))$. □