Multivariate Cryptography with Mappings of Discrete Logarithms and Polynomials

Duggirala Meher Krishna * and Duggirala Ravi †
Gayatri Vidya Parishad College of Engineering (Autonomous),
Madhurawada, VISAKHAPATNAM – 530 048, Andhra Pradesh, India.

Abstract

In this paper, algorithms for multivariate public key cryptography and digital signature are described. Plain messages and encrypted messages are arrays, consisting of elements from a fixed finite ring or field. The encryption and decryption algorithms are based on multivariate mappings. The security of the private key depends on the difficulty of solving a system of parametric simultaneous multivariate equations involving polynomial or exponential mappings. The method is a general purpose utility for most data encryption, digital certificate or digital signature applications. For security protocols of the application layer level in the OSI model, the methods described in this paper are useful.

Keywords Public key cryptography ; Digital Signature ; and Multivariate parametric analysis

Mathemetics Subject Classification (2010) 03C10, 11C08, 11T71, 12E20, 12Y05, 13A15, 13P10, 81P94, 94A60

Contents

*E-mail : duggiralameherkrishna@gmail.com
†E-mail : ravi@gvpce.ac.in ; duggirala.ravi@yahoo.com ; drdravi2000@yahoo.com ; duggirala.ravi@rediffmail.com

1 Introduction

1.1 Preliminary Discussion

The role of cryptographic algorithms is to provide information security [[9], [28], [42], [44], [45] and [46]]. In general, proper data encryption and authentication mechanisms with access control are preferred for a trusted secure system [[44] and [45]]. The most popular public key cryptosystems are the RSA [[41]], NTRU [[21], [22], [23] and [24]], ECC [[27], [37], [43] and [48]], the algorithms based on diophantine equations [[33]] and discrete logarithms [[15]], and those based on multivariate quadratic polynomials [[6] and [29]].

The RSA, the NTRU and the ECC are assumed to be secure algorithms unless there are new breakthroughs in integer factoring (for RSA), or in lattice reduction (for NTRU), or in elliptic curve discrete logarithm techniques (for ECC) [[11] and [19]].

In this paper, algorithms for public key cryptography as well as digital signature based on multivariate mappings are described, with plain and encrypted message arrays consisting of elements from a fixed commutative and finite ring or field. The keys can be built up starting from independently chosen small degree polynomial or easy exponential mappings, resulting in fast key generation and facilitating easy changes of keys as often as required. The security depends on the difficulty of solving parametric simultaneous multivariate equations involving polynomial or exponential mappings [[8], [10], [16], [17], [35], [36], [12] and [14]] in the case of straightforward attacks, and on the difficulty of finding the private keys in the case of key recovery attacks. For security protocols of the application layer level in the OSI model, the methods described in this paper are useful.

1.2 Notation

In the sequel, let $\mathbb{Z}$ be the set of integers, and let $\mathbb{N}$ be the set of positive integers. For a positive integer $\mathfrak{n} \geq 2$, let $\mathbb{Z}_{\mathfrak{n}}$ be the ring of integers with addition and multiplication $\mathsf{mod}\ \mathfrak{n}$, and $\mathbb{Z}_{\mathfrak{n}}^*$ be the commutative group of invertible elements in $\mathbb{Z}_{\mathfrak{n}}$, with respect to multiplication operation in $\mathbb{Z}_{\mathfrak{n}}$. The representing elements in $\mathbb{Z}_{\mathfrak{n}}$ are taken to be those from the set $\{0, \ldots, \mathfrak{n} - 1\} \subseteq \mathbb{Z}$. Let $\mathbb{F}$ be a finite field, consisting of p^n elements for some positive integer n and prime number p, and let $\mathbb{F}^*$ be the multiplicative group of nonzero elements in $\mathbb{F}$. Let G be a finite cyclic group of order $\mathfrak{n} \geq 2$. Let E be either $\mathbb{F}$ or $\mathbb{Z}_{\mathfrak{n}}$ or G. If $\mathsf{E} = \mathsf{G}$, where G is equipped with only the group operation, then G is isomorphic to $\mathbb{Z}_{\mathfrak{n}}$, where the group operation in G is identified with the addition operation of $\mathbb{Z}_{\mathfrak{n}}$. The addition operation of $\mathbb{Z}$ is a primary operation, and the multiplication operation, that can be treated as a secondary operation [[34]] over the additive group $\mathbb{Z}$, is defined uniquely by the distribution laws, with 1 as the multiplicative identity, rendering $\mathbb{Z}$ as the commutative ring. The same holds for $\mathbb{Z}_{\mathfrak{n}}$, with 1 acting as the multiplicative identity. Let $\mathsf{E}[x_1, \ldots, x_m]$, for $m \in \mathbb{N}$, be the algebra of multivariate polynomials in m formal variables $x_1, \ldots, x_m$ with coefficients in E. Now, if $\mathsf{G} = \mathbb{F}^*$, for a finite field $\mathbb{F}$, then the group operation in G coincides with the multiplication operation in $\mathbb{F}$ and $\mathsf{G}[x_1, \ldots, x_m] = \mathbb{F}[x_1, \ldots, x_m]$. If $m = 1$, then $\mathsf{E}[x_1, \ldots, x_m]$ is denoted by $\mathsf{E}[x]$, with $x = x_1$. A variable with its name expressed in bold face assumes values from a product space, which is a product of finitely many copies of the same set, and each component of the variable, expressed in the corresponding case without boldness and a positive integer subscript, assumes values from the constituent component space, succinctly as, for example, $\mathbf{x} = (x_1, \ldots, x_m) \in \mathsf{E}^m$, for some $m \in \mathbb{N}$.

1.3 Polynomials over $\mathbb{Z}_{\mathfrak{n}}$

Let $\mathfrak{n} = \prod_{i=1}^{r} \mathsf{p}_i^{l_i}$, where r and l_i are positive integers, and p_i are distinct prime numbers, for $1 \le i \le r$. Let $\mathsf{q}_i = \mathsf{p}_i^{-l_i}\mathfrak{n} = \prod^{r}_{\substack{j=1 \\ j \neq i}} \mathsf{p}_j^{l_j}$, and let $m_i \in \mathbb{N}$ be such that $m_i \mathsf{q}_i \equiv 1 \bmod \mathsf{p}_i^{l_i}$, for $1 \le i \le r$. Then, $\mathbb{Z}_{\mathfrak{n}} = \oplus_{i=1}^{r} m_i \mathsf{q}_i \mathbb{Z}_{\mathsf{p}_i^{l_i}}$.

Now, a polynomial $f(x) \in \mathbb{Z}_{\mathfrak{n}}[x]$ can be expressed as $\sum_{i=1}^{r} m_i \mathsf{q}_i f_i(x)$, for some unique polynomials $f_i(x) \in \mathbb{Z}_{\mathsf{p}_i^{l_i}}[x]$, for $1 \le i \le r$. For some $x \in \mathbb{Z}$ and index i, where $1 \le i \le r$, if $\mathsf{p}_i \mid f(x)$, then $\mathsf{gcd}\big(f(x) \bmod \mathsf{p}_i^{l_i}, \mathsf{p}_i\big) = \mathsf{gcd}\big(f_i(x), \mathsf{p}_i\big) = \mathsf{p}_i \neq 1$. Thus, $\mathsf{gcd}(f(x), \mathfrak{n}) = 1$, for every $x \in \mathbb{Z}_{\mathfrak{n}}$, if and only if $\mathsf{gcd}(f_i(x), \mathsf{p}_i) = 1$, for every $x \in \mathbb{Z}_{\mathsf{p}_i^{l_i}}$, for every index i, where $1 \le i \le r$. Similarly, f is a surjective (hence bijective) mapping from $\mathbb{Z}_{\mathfrak{n}}$ onto $\mathbb{Z}_{\mathfrak{n}}$, if and only if f_i is a surjective (hence bijective) mapping from $\mathbb{Z}_{\mathsf{p}_i^{l_i}}$ onto $\mathbb{Z}_{\mathsf{p}_i^{l_i}}$, or equivalently, $f_i(x) \bmod \mathsf{p}_i$ is a bijective mapping from $\mathbb{Z}_{\mathsf{p}_i}$ into itself and, when $l_i \ge 2$, $f_i'(x) \not\equiv 0 \bmod \mathsf{p}_i$, for all $x \in \mathbb{Z}_{\mathsf{p}_i^{l_i}}$, where f_i' is the formal algebraic derivative of f_i, for every index i, where $1 \le i \le r$ [[31]]. Now, if $g(x) \in \mathbb{Z}_{\mathfrak{n}}[x]$, where $g(x) = \sum_{i=1}^{r} m_i \mathsf{q}_i g_i(x)$, for some $g_i(x) \in \mathbb{Z}_{\mathsf{p}_i^{l_i}}[x]$, for $1 \le i \le r$, then $f(x)g(x) = \sum_{i=1}^{r} m_i \mathsf{q}_i f_i(x) g_i(x)$. Thus, (A) $f(x)$ is a unit in $\mathbb{Z}_{\mathfrak{n}}[x]$, if and only if $f_i(x)$ is a unit, *i.e.*, $f_i(x) \bmod \mathsf{p}_i \in \mathbb{Z}^*_{\mathsf{p}_i}$, for every index i, where $1 \le i \le r$, (B) $f(x)$ is reducible in $\mathbb{Z}_{\mathfrak{n}}[x]$, if and only if $f_i(x)$ is reducible in $\mathbb{Z}_{\mathsf{p}_i^{l_i}}[x]$, for some index i, where $1 \le i \le r$, and (C) $f(x)$ is irreducible in $\mathbb{Z}_{\mathfrak{n}}[x]$, if and only if $f_i(x)$ is irreducible in $\mathbb{Z}_{\mathsf{p}_i^{l_i}}[x]$, or equivalently, $f_i(x) \bmod \mathsf{p}_i$ is irreducible in $\mathbb{Z}_{\mathsf{p}_i}[x]$, for every index i, where $1 \le i \le r$. Thus, for any positive integer k, $\mathbb{Z}_{\mathfrak{n}}[x_1, \ldots, x_k]$ can be expressed as $\oplus_{i=1}^{r} m_i \mathsf{q}_i \mathbb{Z}_{\mathsf{p}_i^{l_i}}[x_1, \ldots, x_k]$.

1.4 Modular Exponentiation over $\mathbb{Z}_{\mathfrak{n}}$

The modular exponentiation operation is extensively studied in connection with the RSA cryptosystem [[9], [28], [41], [42], [44], [45] and [46]]. In this section, the modular exponentiation is extended to the situation, wherein the exponents are functions. The security of the RSA system depends on the difficulty of factorization of a positive integer into its prime factors. However, simplification of computations as well as porting of variables from base level to exponentiation level by a homomorphism requires availability of prime factors in advance for both encryption and decryption, while working with multivariate mappings involving functions as exponents. In the sequel, let φ be Euler phi or totient function [[9], [28], [42] and [46]]. Let $\mathfrak{n} = \prod_{i=1}^{r} \mathsf{p}_i^{l_i}$, where $r \in \mathbb{N}$, $l_i \in \mathbb{N}\backslash\{1\}$ and p_i are distinct prime numbers, for $1 \le i \le r$. Let $\mathcal{EXP}(\mathbb{Z}_{\mathfrak{n}}\,;\,[x_1,\,\ldots,\,x_m])$ be the smallest set of expressions, closed with respect to addition and multiplication, and containing expressions of the form $a(x_1,\,\ldots,\,x_m)^{b(x_1,\ldots,x_m)}$, where $a(x_1,\,\ldots,\,x_m) \in \mathbb{Z}_{\mathfrak{n}}[x_1,\,\ldots,\,x_m]$, and either

1. as a formal expression, $b(x_1,\,\ldots,\,x_m)$ does not depend on $(x_1,\,\ldots,\,x_m)$ and evaluates to any fixed positive integer, or

2. $a(x_1,\,\ldots,\,x_m)$ evaluates to elements in $\mathbb{Z}_{\mathfrak{n}}^*$, for all values of $(x_1,\,\ldots,\,x_m)$ in some domain of interest, which is a subset of $\mathbb{Z}_{\mathfrak{n}}^m$, and $b(x_1,\,\ldots,\,x_m)$ is of the form $c(h(x_1),\,\ldots,\,h(x_m))$, for some expression $c(z_1,\,\ldots,\,z_m) \in \mathcal{EXP}(\mathbb{Z}_{\varphi(\mathfrak{n})}\,;\,[z_1,\,\ldots,\,z_m])$ and ring homomorphism h from $\mathbb{Z}_{\mathfrak{n}}$ into $\mathbb{Z}_{\varphi(\mathfrak{n})}$.

The condition in (1) above implies that $\mathbb{Z}_{\mathfrak{n}}[x_1,\,\ldots,\,x_m] \subseteq \mathcal{EXP}(\mathbb{Z}_{\mathfrak{n}}\,;\,[x_1,\,\ldots,\,x_m])$. Thus, the integers in $\mathbb{Z}$ and those in $\mathbb{Z}_{\mathfrak{n}}$, for various modulus positive integers $\mathfrak{n} \ge 2$, need to be distinguished clearly as separate elements. The expressions in $\mathcal{EXP}(\mathbb{Z}_{\mathfrak{n}}\,;\,[x_1,\,\ldots,\,x_m])$ are turned into mappings, by identifying appropriate domains of values and interpretation for variables and operations in the respective domains [[12], [14], [34] and [35]]. For $\mathbf{x} \in \mathbb{Z}_{\mathfrak{n}}^m$ and $s \in \mathbb{N}\backslash\{1\}$, such that $s \mid \mathfrak{n}$, let $\mathbf{x} \bmod s = \big(x_1 \bmod s,\,\ldots,\,x_m \bmod s\big)$. Let $f(\mathbf{x}) \in \mathbb{Z}_{\mathfrak{n}}[x_1,\,\ldots,\,x_m]$ be such that $f(\mathbf{x})$ evaluates to elements in $\mathbb{Z}_{\mathfrak{n}}^*$, for $\mathbf{x} \in X$, for some $X \subseteq \mathbb{Z}_{\mathfrak{n}}^m$, and let $f_i(\mathbf{x}) \in \mathbb{Z}_{\mathsf{p}_i^{l_i}}[x_1,\,\ldots,\,x_m]$, for $1 \le i \le r$, be such that $f(\mathbf{x}) = \sum_{i=1}^r m_i \mathsf{q}_i f_i(\mathbf{x} \bmod \mathsf{p}_i^{l_i})$. Now, for $\mathbf{x} \in X$ and $k \in \mathbb{Z}$, the following holds: $\big(f(\mathbf{x})\big)^k = \big(f(\mathbf{x})\big)^{k \bmod \varphi(\mathfrak{n})} = \sum_{i=1}^r m_i \mathsf{q}_i \big(f_i(\mathbf{x} \bmod \mathsf{p}_i^{l_i})\big)^{k \bmod \varphi(\mathfrak{n})}$ $= \sum_{i=1}^r m_i \mathsf{q}_i \big(f_i(\mathbf{x} \bmod \mathsf{p}_i^{l_i})\big)^{k \bmod \varphi(\mathsf{p}_i^{l_i})}$. Let $g(\mathbf{y}) \in \mathbb{Z}_{\varphi(\mathbb{Z}_{\mathfrak{n}})}[y_1,\,\ldots,\,y_n]$ and $g_i(\mathbf{z}) \in \mathbb{Z}_{\varphi(\mathsf{p}_i^{l_i})}[z_1,\,\ldots,\,z_n]$ be such that the following holds: $g_i\big(\mathbf{y} \bmod \varphi(\mathsf{p}_i^{l_i})\big) = g(\mathbf{y}) \bmod \varphi\big(\mathsf{p}_i^{l_i}\big)$, for $1 \le i \le r$. Thus, $f^{g(\mathbf{y})}(\mathbf{x}) = \sum_{i=1}^r m_i \mathsf{q}_i f_i^{g(\mathbf{y})}(\mathbf{x}) = \sum_{i=1}^r m_i \mathsf{q}_i f_i^{g_i(\mathbf{y} \bmod \varphi(\mathsf{p}_i^{l_i}))}(\mathbf{x} \bmod \mathsf{p}_i^{l_i})$, for independent vectors $\mathbf{x} \in X$ and $\mathbf{y} \in \mathbb{Z}_{\varphi(\mathfrak{n})}^n$. Now, $\varphi(\mathsf{p}_i^{l_i}) = (\mathsf{p}_i - 1)\mathsf{p}_i^{l_i - 1}$, where $l_i \ge 2$, for $1 \le i \le r$. Let $w_i = (\mathsf{p}_i - 1)^{-1} \bmod \mathsf{p}_i^{l_i - 1}$, and let $h_i : \mathbb{Z}_{\mathsf{p}_i^{l_i}} \to \mathbb{Z}_{\varphi(\mathsf{p}_i^{l_i})}$ be the map defined by $h_i(x) = (\mathsf{p}_i - 1)(w_i x \bmod \mathsf{p}_i^{l_i - 1})$, for $1 \le i \le r$. Then, h_i is a ring homomorphism, for $1 \le i \le r$. Now, let $h\big(\sum_{i=1}^r m_i \mathsf{q}_i z_i\big) = \big(h_1(z_1),\,\ldots,\,h_r(z_r)\big)$, for $z_i \in \mathbb{Z}_{\mathsf{p}_i^{l_i}}$ and $1 \le i \le r$. Then, the map h is a ring homomorphism from the ring $\oplus_{i=1}^r m_i \mathsf{q}_i \mathbb{Z}_{\mathsf{p}_i^{l_i}}$ into the ring of direct product $\prod_{i=1}^r \mathbb{Z}_{\varphi(\mathsf{p}_i^{l_i})}$. If the base level and exponentiation level interpretation maps are $\mathcal{I}_{\text{base}}$ and $\mathcal{I}_{\text{exponent}}$, respectively, then $\mathcal{I}_{\text{exponent}}$ can be chosen to be $h \circ \mathcal{I}_{\text{base}}$, applied from right to left in the written order, preserving the respective ring operations in the base level and exponentiation level subexpressions. If $l_i = 1$, for some index i, where $1 \leq i \leq r$, then exponentiation along ith component can be carried by interpreting $\mathbb{Z}_{\mathsf{p}_i}$ to be a finite field, and porting values of base level expressions to exponentiation level expressions by discrete logarithm mapping, as discussed in section 1.5.

1.5 Modular Exponentiation over $\mathbb{F}$

Let $\mathbb{F}$ be a finite field containing p^n elements and $\mathfrak{n} = \mathsf{p}^n - 1$, for some prime number p and positive integer n. Let $\mathcal{EXP}\big(\mathbb{F}\,;\,[x_1,\,\dots,\,x_m]\big)$ be the smallest set of expressions, closed with respect to addition and multiplication, and containing expressions of the form $a(x_1,\,\dots,\,x_m)^{b(x_1,\dots,x_m)}$, where $a(x_1,\,\dots,\,x_m) \in \mathbb{F}[x_1,\,\dots,\,x_m]$, and either

1. as a formal expression, $b(x_1,\,\dots,\,x_m)$ does not depend on $(x_1,\,\dots,\,x_m)$ and evaluates to any fixed positive integer, or

2. $a(x_1,\,\dots,\,x_m)$ evaluates to elements in $\mathbb{F}^*$, for all values of $(x_1,\,\dots,\,x_m)$ in some domain of interest, which is a subset of G^m, where $\mathsf{G} = \mathbb{F}^*$, and $b(x_1,\,\dots,\,x_m)$ is of the form $c(h(x_1),\,\dots,\,h(x_m))$, for some expression $c(z_1,\,\dots,\,z_m) \in \mathcal{EXP}\big(\mathbb{Z}_{\mathfrak{n}}\,;\,[z_1,\,\dots,\,z_m]\big)$ and group isomorphism h from G into $\mathbb{Z}_{\mathfrak{n}}$.

The condition in (1) above implies that $\mathbb{F}[x_1,\,\dots,\,x_m] \subseteq \mathcal{EXP}\big(\mathbb{F}\,;\,[x_1,\,\dots,\,x_m]\big)$. For a primitive element $a \in \mathbb{F}^*$, let $\log_a : \mathbb{F}^* \to \mathbb{Z}_{\mathfrak{n}}$ be the discrete logarithm function defined by $\log_a(g) = x$, exactly when $a^x = g$, for $g \in \mathbb{F}^*$ and $x \in \mathbb{Z}_{\mathfrak{n}}$. Thus, the group homomorphism h can be taken to be $\log_a$. If the base level and exponentiation level interpretation maps are $\mathcal{I}_{\text{base}}$ and $\mathcal{I}_{\text{exponent}}$, respectively, then $\mathcal{I}_{\text{exponent}}$ can be chosen to be $\log_a \circ \mathcal{I}_{\text{base}}$, applied from right to left in the written order. For porting a subexpression involving addition operation in $\mathbb{F}$, such as, for example, $f(\mathbf{x}) \in \mathbb{F}[x_1,\,\dots,\,x_m]$, where $f(\mathbf{x}) \neq 0$, for $\mathbf{x} \in \mathsf{G}^m$, where $\mathsf{G} = \mathbb{F}^*$, occurring in a base level expression to an exponentiation level, the base level subexpression is replaced by a supplementary variable z, which is ported to first exponentiation level by the discrete logarithm mapping. In the subsequent levels of exponentiation, the interpretation is performed by applying ring homomorphisms, as discussed in section 1.4.

2 Main Results

2.1 Parametric Injective Mappings

Let E be either $\mathbb{F}$ or $\mathbb{Z}_{\mathfrak{n}}$. Let $\mathsf{G} \subseteq \mathsf{E}$ be the domain of interpretation for the variables occurring in the mappings. For $l \in \{0\} \cup \mathbb{N}$ and $m \in \mathbb{N}$, a parametric multivariate injective mapping $\eta\big(z_1,\,\dots,\,z_l;\,(x_1,\,\dots,\,x_m)\big)$ from

G^m into E^m is a multivariate injective mapping, which is an expression from either $\mathsf{E}[x_1, \ldots, x_m, z_1, \ldots, z_l]$ or $\mathcal{EXP}(\mathsf{E}; [x_1, \ldots, x_m, z_1, \ldots, z_l])$ with interpretation conventions as discussed in sections 1.4 and 1.5, as appropriate, for $(x_1, \ldots, x_m) \in \mathsf{G}^m$ and $(z_1, \ldots, z_l) \in \mathcal{Z} \subseteq \mathsf{E}^l$, and its parametric inverse $\eta^{-1}(z_1, \ldots, z_l; (y_1, \ldots, y_m))$ is such that, for every fixed $(z_1, \ldots, z_l) \in \mathcal{Z}$, the following holds: if $\eta(z_1, \ldots, z_l; (x_1, \ldots, x_m)) = (y_1, \ldots, y_m)$, then $(x_1, \ldots, x_m) = \eta^{-1}(z_1, \ldots, z_l; (y_1, \ldots, y_m))$, for every $(x_1, \ldots, x_m) \in \mathsf{G}^m$ and $(y_1, \ldots, y_m) \in \mathsf{E}^m$. For example, let $\mathfrak{n}$ be the set cardinality of $\mathsf{G} = \mathbb{F}^*$, $a \in \mathbb{F}^*$ be a fixed primitive element, which is made known in the public key, and $\eta(z_1, \ldots, z_l; x) = f(z_1, \ldots, z_l)x^{g(\log_a(z_1), \ldots, \log_a(z_l))}$, where $f(z_1, \ldots, z_l) \in \mathcal{EXP}(\mathbb{F}; [z_1, \ldots, z_l])$ and $g(t_1, \ldots, t_l) \in \mathcal{EXP}(\mathbb{Z}_{\mathfrak{n}}; [t_1, \ldots, t_l])$ are such that $f(z_1, \ldots, z_l) \neq 0$, for $z_1, \ldots, z_l \in \mathbb{F}^*$, and $\mathsf{gcd}(g(t_1, \ldots, t_l), \mathfrak{n}) = 1$, for $t_1, \ldots, t_l \in \mathbb{Z}_{\mathfrak{n}}$. Then, $\eta(z_1, \ldots, z_l; x)$ is a parametric bijective mapping from $\mathbb{F}^*$ into $\mathbb{F}^*$, with $z_1, \ldots, z_l \in \mathbb{F}^*$ as parameters, and the inverse mapping of η is $\eta^{-1}(z_1, \ldots, z_l; x) = [\ [f(z_1, \ldots, z_l)]^{-1}x\ ]^{[\ [g(\log_a(z_1), \ldots, \log_a(z_l))]^{-1} \bmod \mathfrak{n}\ ]}$.

For the multivariate surjective mappings for digital signature scheme discussed at the end of section 3, mappings $f(z_1, \ldots, z_l) \in \mathcal{EXP}(\mathbb{F}; [z_1, \ldots, z_l])$ and $g(t_1, \ldots, t_l) \in \mathcal{EXP}(\mathbb{Z}_{\mathfrak{n}}; [t_1, \ldots, t_l])$ can be chosen, such that both the conditions $f(z_1, \ldots, z_l) \neq 0$ and $\mathsf{gcd}(g(\log_a(z_1), \ldots, \log_a(z_l)), \mathfrak{n}) = 1$, simultaneously hold for $(z_1, \ldots, z_l) \in \mathcal{Z} \subseteq \mathsf{G}^l$, where the required exact domain $\mathcal{Z} \neq \emptyset$ is a private key and known only to the signer.

2.1.1 Parametrization Methods

Let, for some positive integers k, l and m, $g_i(z_1, \ldots, z_l)$, $1 \leq i \leq k$, be a partition of unity of E^l, *i.e.*, $\sum_{i=1}^{k} g_i(z_1, \ldots, z_l) = 1$ and $g_i(z_1, \ldots, z_l) \cdot g_j(z_1, \ldots, z_l) = 0$, $i \neq j$, $1 \leq i, j \leq k$, for every $(z_1, \ldots, z_l) \in \mathsf{E}^l$. The partition of unity required for the parametric mappings discussed of this section need not necessarily be strict, and it is possible that, for some i, where $1 \leq i \leq k$, $g_i(z_1, \ldots, z_l) = 0$, for every $(z_1, \ldots, z_l) \in \mathsf{E}^l$. Let $\zeta_i(z_1, \ldots, z_l; \mathbf{x})$, $1 \leq i \leq k$, $\mathbf{x} = (x_1, \ldots, x_m)$, be parametric multivariate injective mappings from G^m into E^m, that may or may not depend on the parameters $z_1, \ldots, z_l$. The vectors $\mathbf{x}$ and $\zeta_i(z_1, \ldots, z_l; \mathbf{x})$, $1 \leq i \leq k$, are identified with the corresponding $m \times 1$ column vectors, whose j-th row entry is the j-th element, for $1 \leq j \leq m$, for allowing them to become amenable to matrix operations. Let $\phi_i(z_1, \ldots, z_l)$ be an $m \times m$ matrix, and $\chi_i(z_1, \ldots, z_l)$ be $m \times 1$ vectors, both with multivariate expressions as entries, such that $\phi_i(z_1, \ldots, z_l)$ evaluates to an invertible matrix, for every $(z_1, \ldots, z_l) \in \mathsf{E}^l$ and $1 \leq i \leq k$. Then, the expression $\eta(z_1, \ldots, z_l; \mathbf{x}) = \sum_{i=1}^{k} g_i(z_1, \ldots, z_l) \cdot \phi_i(z_1, \ldots, z_l) \cdot [\zeta_i(z_1, \ldots, z_l; \mathbf{x}) + \chi_i(z_1, \ldots, z_l)]$ is a parametric multivariate injective mapping, with its parametric inverse $\eta^{-1}(z_1, \ldots, z_l; \mathbf{y}) = \sum_{i=1}^{k} g_i(z_1, \ldots, z_l) \cdot \zeta_i^{-1}(z_1, \ldots, z_l; \mathbf{x}_i)$, where $\mathbf{x}_i = \big[[\phi_i(z_1, \ldots, z_l)]^{-1} \cdot \mathbf{y}\big] - \chi_i(z_1, \ldots, z_l)$, $\mathbf{y} = (y_1, \ldots, y_m)$, which is also identified with the corresponding $m \times 1$ column vector, and $[\phi_i(z_1, \ldots, z_l)]^{-1}$ is the matrix inverse of $[\phi_i(z_1, \ldots, z_l)]$, for $1 \le i \le k$.

For the multivariate surjective mappings for digital signature scheme discussed at the end of section 3, it is possible to choose $\zeta_i(z_1, \ldots, z_l; \mathbf{x})$ to be bijective, only for some indexes i, where $1 \le i \le k$, letting it be arbitrary for the remaining indexes. Since the domain information is a private key, as discussed in the last paragraph of the preceding section, the updates mentioned here must be so chosen that the effective domain will become feasible, while maintaining it as a private key.

2.1.2 Partition of Unity of $\mathbb{F}$

Let $f(z) \in \mathcal{EXP}(\mathbb{F}; [z])$, which is called a discriminating function, and let K_f be the codomain of f, *i.e.*, $K_f = \{f(x) : x \in \mathbb{F}\} = \{a_i : 1 \le i \le k\}$, for some positive integer k. Let $\ell_i(x) = \left[\prod_{\substack{j=1 \\ j \ne i}}^{k} (a_i - a_j)\right]^{-1} \cdot \prod_{\substack{j=1 \\ j \ne i}}^{k} (f(x) - a_j)$, $1 \le i \le k$. Then, $\ell_i(x) = 1$, for $x \in E_i = \{z \in \mathbb{F} : f(z) - a_i = 0\}$, and $\ell_i(x) = 0$, for $x \in \mathbb{F} \backslash E_i$, $1 \le i \le k$. Thus, $\{E_i : 1 \le i \le k\}$ is a partition of $\mathbb{F}$, and $\ell_i(x)$ is the characteristic function of the equivalence class E_i, $1 \le i \le k$. Now, the set $\{g_i(z_1, \ldots, z_l) = \ell_i(h(z_1, \ldots, z_l)) : 1 \le i \le k\}$, where $h(z_1, \ldots, z_l) \in \mathcal{EXP}(\mathbb{F}; [z_1, \ldots, z_l])$, is a partition of unity of $\mathbb{F}^l$.

Examples. (A) Let the vector space dimension of $\mathbb{F}$ be n as an extension field of $\mathbb{Z}_{\mathtt{p}}$, and let $f(z) = \sum_{i=1}^{n} a_i z^{\mathtt{p}^{i-1}}$, where $a_i \in \mathbb{F}$, $1 \le i \le n$, be a noninvertible linear operator from $\mathbb{F}$ into $\mathbb{F}$, with $\mathbb{Z}_{\mathtt{p}}$ as the field. For every linear operator T from $\mathbb{F}$ into $\mathbb{F}$ with $\mathbb{Z}_{\mathtt{p}}$ as the field, there exist scalars $c_i \in \mathbb{F}$, $1 \le i \le n$, such that $Tz = \sum_{i=1}^{n} c_i z^{\mathtt{p}^{i-1}}$ [[32]]. Now, each equivalence class is an affine vector subspace of the form $\{y + x : f(x) = 0,\ x \in \mathbb{F}\}$, for some $y \in \mathbb{F}$. Thus, if r is the rank of f as linear operator from $\mathbb{F}$ into $\mathbb{F}$ with $\mathbb{Z}_{\mathtt{p}}$ as the field, then the nullity of f is $n - r$, each equivalence class has $\mathtt{p}^{n-r}$ elements, and there are $k = \mathtt{p}^r$ equivalence classes. For the number of equivalence classes to be small, the rank r of f must be small, such as $r = 1$ or $r = 2$. (B) Let $f(z) = z^r$, where r is a large positive integer dividing $\mathtt{p}^n - 1$. Now, the equivalence classes are $\{0\}$ and the cosets of the congruence relation $x \sim y$ if and only if $(x^{-1}y)^r = 1$, for $x, y \in \mathbb{F}\backslash\{0\}$. Since $K_f = \{0\} \cup \{z^r : z \in \mathbb{F}\backslash\{0\}\}$, there are $k = 1 + (\mathtt{p}^n - 1)/r$ equivalence classes.

2.1.3 Partition of Unity of $\mathbb{Z}_{\mathtt{p}^l}$

Let $s \in \mathbb{N}$ be a divisor of $(\mathtt{p} - 1)$ and $k = 1 + \frac{(\mathtt{p}-1)}{s}$. Now, $\mathtt{p}^{l-1} \ge l$, for any $l \in \mathbb{N}$ and prime number $\mathtt{p}$. Let $h(x) = x^{s\mathtt{p}^{l-1}}$, for $x \in \mathbb{Z}_{\mathtt{p}^l}$. Then, $\left(h(x)\right)^{k-1} = 1$, for $x \in \mathbb{Z}^\star_{\mathtt{p}^l}$, and $h(x) = 0$, for $x \in \mathbb{Z}_{\mathtt{p}^l} \backslash \mathbb{Z}^\star_{\mathtt{p}^l}$. Thus, the set $\{x^{s\mathtt{p}^{l-1}} : x \in \mathbb{Z}_{\mathtt{p}^l}\}$ contains k distinct elements. Let $x, y \in \mathbb{Z}_{\mathtt{p}^l}$ be such that $h(x) \ne h(y)$. If $h(x) = 0$ or $h(y) = 0$, then $(h(y) - h(x)) \in \mathbb{Z}^\star_{\mathtt{p}^l}$. Now, let $x, y \in \mathbb{Z}^\star_{\mathtt{p}^l}$. If $(x^{-1}y)^{s\mathtt{p}^{l-1}} = 1 + b\mathtt{p}^t$, for some $b \in \mathbb{Z}^\star_{\mathtt{p}^l}$ and $t \in \mathbb{N}$, then, since $1+$

$b\mathsf{p}^t\sum_{i=1}^{k-1}\frac{(k-1)!}{i!(k-i-1)!}b^{i-1}\mathsf{p}^{(i-1)t} = (1+b\mathsf{p}^t)^{k-1} = \big((x^{-1}y)^{s\mathsf{p}^{l-1}}\big)^{k-1} = 1 \bmod \mathsf{p}^l$, it follows that either $t \geq l$ or $(k-1)+\sum_{i=2}^{k-1}\frac{(k-1)!}{i!(k-i-1)!}b^{i-1}\mathsf{p}^{(i-1)t} = 0 \bmod \mathsf{p}^{l-t}$. However, since $k = 1+\frac{\mathsf{p}-1}{s}$, and therefore, $1 \leq k-1 \leq \mathsf{p}-1$, it follows that $(k-1)+\sum_{i=2}^{k-1}\frac{(k-1)!}{i!(k-i-1)!}b^{i-1}\mathsf{p}^{(i-1)t} = k-1 \bmod \mathsf{p}$. Thus, if $x, y \in \mathbb{Z}^\star_{\mathsf{p}^l}$ and $h(x) \neq h(y)$, then $(x^{-1}y)^{s\mathsf{p}^{l-1}} - 1 \neq 0 \bmod \mathsf{p}$, and hence if $x, y \in \mathbb{Z}_{\mathsf{p}^l}$ and $h(x) \neq h(y)$, then $(h(y)-h(x)) \in \mathbb{Z}^\star_{\mathsf{p}^l}$. If $a_j \in \mathbb{Z}_{\mathsf{p}^l}$, $1 \leq j \leq k$, are such that $\{x^{s\mathsf{p}^{l-1}} : x \in \mathbb{Z}_{\mathsf{p}^l}\} = \{a_j : 1 \leq j \leq k\}$, then $(a_i - a_j) \in \mathbb{Z}^\star_{\mathsf{p}^l}$, for $i \neq j$, $1 \leq i, j \leq k$, and the Lagrange interpolation polynomials $g_j(x) \in \mathbb{Z}_\mathsf{p}[x]$ can be obtained for the equivalence classes $E_j = \{x^{s\mathsf{p}^{l-1}} = a_j : x \in \mathbb{Z}_{\mathsf{p}^l}\}$. Thus, corresponding to every homomorphism of $\mathbb{Z}^\star_\mathsf{p}$ into $\mathbb{Z}^\star_\mathsf{p}$, a partition of unity of $\mathbb{Z}_{\mathsf{p}^l}$ can be obtained.

2.1.4 Multivariate Mappings that Evaluate to only Invertible Elements

Let $f(z) \in \mathbb{F}[z]$ be a polynomial which is not surjective as a mapping from $\mathbb{F}$ into $\mathbb{F}$. Then, there exists an element $c \in \mathbb{F}$, such that $f(z) - c \neq 0$, for every $z \in \mathbb{F}$. For $a \in \mathbb{F}\backslash\{0\}$ and $g(z_1, \ldots, z_l) \in \mathbb{F}[z_1, \ldots, z_l]$, $a\big(f(g(z_1, \ldots, z_l)) - c\big) \neq 0$, for every $(z_1, \ldots, z_l) \in \mathbb{F}^l$.

Examples. (A) Let $f(z)$ be a product of irreducible polynomials in $\mathbb{F}[z]$ of degree 2 or more each. Then, c can be chosen to be 0. (B) Let the vector space dimension of $\mathbb{F}$ be n as an extension field of $\mathbb{Z}_\mathsf{p}$, and let $f(z) = \sum_{i=1}^n a_i z^{\mathsf{p}^{i-1}}$, where $a_i \in \mathbb{F}$, $1 \leq i \leq n$, be a noninvertible linear operator from $\mathbb{F}$ into $\mathbb{F}$, with $\mathbb{Z}_\mathsf{p}$ as the field. Then, for any basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathbb{F}$, with $\mathbb{Z}_\mathsf{p}$ as the field, there exists an index j, $1 \leq j \leq n$, such that $\sum_{i=1}^n a_i z^{\mathsf{p}^{i-1}} - \alpha_j \neq 0$, for every $z \in \mathbb{F}$, and c can be taken to be α_j. (C) Let $r \geq 2$ be a positive integer divisor of $\mathsf{p}^n - 1$, and let $f(z) = z^r$. Then, there exists an element $c \in \mathbb{F}\backslash\{0\}$, such that $c^{(\mathsf{p}^n-1)/r} \neq 1$. Now, since $c^{(\mathsf{p}^n-1)/r} \neq 0$ and $c^{(\mathsf{p}^n-1)/r} \neq 1$, it follows that $f(z) - c \neq 0$, for every $z \in \mathbb{F}$.

If $f(z) \in \mathbb{F}[z]$ is such that $f(z) \neq 0$, for every $z \in \mathbb{F}$, then $[f(z)]^{-1} = \sum_{i=1}^k a_i^{-1}\ell_i(z)$, where $\{a_i : 1 \leq i \leq k\} = \{f(z) : z \in \mathbb{F}\}$, and $\ell_i(z) = \left[\prod_{\substack{j=1 \\ j \neq i}}^k (a_i - a_j)\right]^{-1} \cdot \prod_{\substack{j=1 \\ j \neq i}}^k \big(f(z) - a_j\big)$, $1 \leq i \leq k$.

Let $\mathfrak{n} = \prod_{i=1}^r \mathsf{p}_i^{l_i}$, where $r, l_i \in \mathbb{N}$ and p_i are distinct prime numbers, for $1 \leq i \leq r$, and $f(z) \in \mathbb{Z}_\mathfrak{n}[z]$. From section 1.3, it can be recalled that, $f(z) \in \mathbb{Z}^*_\mathfrak{n}$, for $z \in \mathbb{Z}_\mathfrak{n}$, if and only if for every i, where $1 \leq i \leq r$, $f(z) \bmod \mathsf{p}_i \in \mathbb{Z}^*_{\mathsf{p}_i}$, for $z \in \mathbb{Z}_\mathfrak{n}$.

It may observed that if $a \in \mathbb{F}^*$, $\mathfrak{n}$ is the number of elements of $\mathbb{F}^*$ and l is a positive integer, then $a^{g(t_1, \ldots, t_l)} \in \mathbb{F}^*$, for every $(t_1, \ldots, t_l) \in \mathbb{Z}^l_\mathfrak{n}$ and any expression mapping $g(t_1, \ldots, t_l) \in \mathcal{EXP}\big(\mathbb{Z}_\mathfrak{n}; [t_1, \ldots, t_l]\big)$.

2.1.5 Invertible Square Matrices with Multivariate Mapping Entries

For a positive integer m, a parametric $m \times m$ invertible square matrix is equivalent to a product of a permutation matrix, followed by a lower triangular matrix with nonzero diagonal entries, an upper triangular matrix with nonzero diagonal entries and finally by another permutation matrix, the four matrices being parametric and written from left to right in the product. Parametric permutation matrices can be constructed from a partition of unity. Let $g_s(z_1, \ldots, z_l)$, for $0 \leq s \leq m-1$, be a partition of unity of $\mathbb{F}^l$, which may not necessarily be strict. Let $\sigma \in \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ be a mapping such that for each fixed $r \in \mathbb{Z}_m$, $\sigma(r, \cdot)$ is a bijective mapping (permutation of indexes) from $\mathbb{Z}_m$ into itself as a mapping of the second argument, and for each fixed $s \in \mathbb{Z}_m$, $\sigma(\cdot, s)$ is a bijective mapping (permutation of indexes) from $\mathbb{Z}_m$ into itself, as a mapping of the first argument. Then, the matrix with entries $g_{\sigma(i-1, j-1)}(z_1, \ldots, z_l)$ in the i-th row and j-th column, for $1 \leq i, j \leq m$, is a parametric permutation matrix. For an example of an index map σ as discussed, let f_i and h be bijective mappings from $\mathbb{Z}_m$ into itself, for $i \in \{1, 2\}$, and $\sigma(r, s) = h\big((f_1(r) + f_2(s)) \bmod m\big)$. It can be easily checked that the mapping σ is as required. Products and transposes of parametric permutation matrices are also parametric permutation matrices.

Caution! This paragraph is concerning an important restriction for parametric surjective mappings onto G^m (and also for verification bijective mappings advertised in public key tables) in digital signature applications, when $\mathsf{G} = \mathbb{F}^*$, for a finite field $\mathbb{F}$, for exponential mappings. The parametric lower and upper triangular matrices need to be chosen to be a parametric diagonal matrix with nonzero diagonal entries, *i.e.*, with entries that are multivariate mappings evaluating to invertible elements, for every assignment of values for the variables in their domains. The parametric permutation matrices are still permitted, in any case. The reason for this caution is the difficulty to deal with test-for-zero conditions. For overcoming this restriction, the exponential mappings need to be extended to mappings that include $0 \in \mathbb{F}$ in their domains and co-domains, mapping 0 to itself, but the test-for-zero conditions must be very carefully considered.

2.2 Univariate Bijective Mappings without Parameters

2.2.1 Single Variable Permutation Mappings without Hashing

Examples in $\mathbb{F}[x]$. Bijective mappings in $\mathbb{F}[x]$, also called permutation polynomials, are extensively studied as Dickson polynomials [[13]] in the literature. A comprehensive survey on Dickson polynomials can be found in [[1], [18], [31], [38] and [39]]. Some recent results are presented in [[2], [3] and [4]]. If $f(z) \in \mathbb{F}[z]$ is a permutation polynomial, then, for every

$a \in \mathbb{F}\backslash\{0\}$, $b \in \mathbb{F}$ and nonnegative integer i, the polynomial $af(z^{\mathsf{p}^i}) - b$ is a permutation polynomial. Some easy examples are described in the following.

Examples. (A) Let $\mathbb{F}$ be a finite dimensional extension field of $\mathbb{Z}_{\mathsf{p}}$ of vector space dimension n. Any polynomial $f(z) = \sum_{i=1}^{n} a_i z^{\mathsf{p}^{i-1}}$, where $a_i \in \mathbb{F}$, $1 \le i \le n$, that is an invertible linear operator from $\mathbb{F}$ onto $\mathbb{F}$, with $\mathbb{Z}_{\mathsf{p}}$ as the field, is a permutation polynomial. (B) Let r be a positive integer divisor of n, and $f(z) = z^{\mathsf{p}^r} - az$, where $a^{(\sum_{i=1}^{n/r} \mathsf{p}^{(i-1)r})} \ne 1$. Then, for every $z \in \mathbb{F}\backslash\{0\}$, $z^{(\mathsf{p}^r-1)} - a \ne 0$, since $z^{\mathsf{p}^n - 1} = z^{(\mathsf{p}^r-1)\sum_{i=1}^{n/r} \mathsf{p}^{(i-1)r}} = 1$, and therefore, the null space of $f(z)$, as a linear operator from $\mathbb{F}$ into $\mathbb{F}$ with $\mathbb{Z}_{\mathsf{p}}$ as the field, is $\{0\}$. Thus, $f(z)$ is a permutation polynomial. (C) Let r be a positive integer relatively prime to $(\mathsf{p}^n - 1)$. Then, the polynomial $f(z) = z^r$ is a permutation polynomial.

Examples in $\mathbb{Z}_{\mathsf{p}^l}[x]$. Let $l \in \mathbb{N}$ and p be a prime number. For any positive integer n, Dickson polynomials that are permutation polynomials, having nonvanishing derivatives over the finite field containing p^n elements, are found in [[1], [2], [3], [4], [18], [31], [38] and [39]]. For a small prime number p, two methods for construction of permutation polynomials $f(x) \in \mathbb{Z}_{\mathsf{p}}[x]$, such that $f'(x) \not\equiv 0 \bmod \mathsf{p}$, are described below. As a set, $\mathbb{Z}_{\mathsf{p}}$ is taken to be the set of integers i, where $0 \le i \le \mathsf{p} - 1$. For $\mathsf{p} = 2$, since $x^{i+1} \equiv x^i \equiv x \bmod 2$, for every $i \in \mathbb{N}$ and $x \in \mathbb{Z}_{2^l}$, the only permutation polynomial mappings in $\mathbb{Z}_{2^l}[x]$ are of the form $b_0 + \sum_{i=1}^{k} b_i x^i$, for some $k \in \mathbb{N}$, $b_i \in \mathbb{Z}_{2^l}$, for $0 \le i \le k$, such that $\sum_{i=1}^{k} b_i \equiv 1 \bmod 2$, and, when $l \ge 2$, $b_1 \equiv 1 \bmod 2$ and $\sum_{i=2}^{k} ib_i \equiv 0 \bmod 2$, or equivalently, $b_1 \equiv 1 \bmod 2$ and the number of indexes j, with $b_{2j+1} \equiv 1$ and $2 \le 2j+1 \le k$, is an even integer, for the condition $f'(x) \equiv 1 \bmod 2$ to hold.

Now, let $\mathsf{p} \ge 3$ be a small prime number, such that the computations below are not difficult for implementation. Let $\ell_i(x) = \left[\prod_{\substack{j=0 \\ j \ne i}}^{\mathsf{p}-1} (i-j)\right]^{-1} \cdot \prod_{\substack{j=0 \\ j \ne i}}^{\mathsf{p}-1} (x-j) = -\prod_{\substack{j=0 \\ j \ne i}}^{\mathsf{p}-1} (x-j)$, since $\mathbb{Z}_{\mathsf{p}}$ is the solution set for x in the polynomial equation $x^{\mathsf{p}-1} - 1 = 0$, and hence, $\left[\prod_{\substack{j=0 \\ j \ne i}}^{\mathsf{p}-1} (i-j)\right]^{-1} = -1$, for $i \in \mathbb{Z}_{\mathsf{p}}$. Now, $\ell_i'(x) = -\sum_{\substack{j=0 \\ j \ne i}}^{\mathsf{p}-1} \prod_{\substack{k=0 \\ k \notin \{i,\, j\}}}^{\mathsf{p}-1} (x-k)$, for $i \in \mathbb{Z}_{\mathsf{p}}$, which implies that $\ell_i'(j) = -\prod_{\substack{k=0 \\ k \notin \{i,\, j\}}}^{\mathsf{p}-1} (j-k) = (j-i)^{-1}$, for $j \ne i$ and $j \in \mathbb{Z}_{\mathsf{p}}$, and $\ell_i'(i) = -\sum_{\substack{j=0 \\ j \ne i}}^{\mathsf{p}-1} \prod_{\substack{k=0 \\ k \notin \{i,\, j\}}}^{\mathsf{p}-1} (i-k) = \sum_{\substack{j=0 \\ j \ne i}}^{\mathsf{p}-1} (i-j)^{-1} = 0$, for $i \in \mathbb{Z}_{\mathsf{p}}$, since $\mathsf{p} \ge 3$. For a fixed permutation sequence $\{a_i \in \mathbb{Z}_{\mathsf{p}} : 0 \le i \le \mathsf{p} - 1\}$ of $\mathbb{Z}_{\mathsf{p}}$, either of the two procedures described below constructs a permutation polynomial $f(x) \in \mathbb{Z}_{\mathsf{p}}[x]$, such that $f(i) = a_i$ and $f'(i) \not\equiv 0 \bmod \mathsf{p}$, for $i \in \mathbb{Z}_{\mathsf{p}}$.

$\boxed{\text{Method 1}}$ Let $\sum_{i=0}^{\mathsf{p}-1} a_i \ell_i(x) = b_0 + \sum_{i=1}^{\mathsf{p}-1} b_i x^i$, for some $b_i \in \mathbb{Z}_{\mathsf{p}}$, for

$0 \le i \le \mathsf{p}-1$, and let $g(x) = c_1 + \sum_{i=2}^{\mathsf{p}-1} c_i x^{i-1}$, for some $c_i \in \mathbb{Z}_\mathsf{p}$, for $1 \le i \le \mathsf{p}-1$, be such that $g(x) \not\equiv 0 \bmod \mathsf{p}$, for every $x \in \mathbb{Z}_\mathsf{p}$. Let $\rho_i = i^{-1}c_i$ and $\sigma_i = b_i - \rho_i$, for $1 \le i \le \mathsf{p}-1$. Let $f(x) = b_0 + \sum_{i=1}^{\mathsf{p}-1}(\rho_i x^i + \sigma_i x^{i\mathsf{p}})$. Then, $f(x) \equiv b_0 + \sum_{i=1}^{\mathsf{p}-1} b_i x^i \bmod \mathsf{p}$, for every $x \in \mathbb{Z}_\mathsf{p}$, and $f'(x) \equiv \rho_1 + \sum_{i=2}^{\mathsf{p}-1} i\rho_i x^{i-1} \equiv c_1 + \sum_{i=2}^{\mathsf{p}-1} c_i x^{i-1} \bmod \mathsf{p}$, for every $x \in \mathbb{Z}_\mathsf{p}$, satisfying the stated requirement. In this method, $\mathsf{deg}\big(f(x)\big)$ can be as high as $(\mathsf{p}-1)\mathsf{p}$. In the next method, $\mathsf{deg}\big(f(x)\big)$ is at most $(2\mathsf{p}-2)$.

Method 2 Let b_i, c_i, $\sigma \in \mathbb{Z}_\mathsf{p}$, for $0 \le i \le \mathsf{p}-1$, be such that $b_0 = a_0$ and $b_j + c_j = a_j$, for $1 \le j \le \mathsf{p}-1$, and let $f(x) = \sum_{i=0}^{\mathsf{p}-1}(b_i + x^{\mathsf{p}-1}c_i - \sigma i)\ell_i(x) + \sigma x^\mathsf{p}$. It can be immediately verified that $f(i) \equiv a_i \bmod \mathsf{p}$, for $0 \le i \le \mathsf{p}-1$, and $f'(x) = \sum_{i=0}^{\mathsf{p}-1}(b_i + x^{\mathsf{p}-1}c_i - \sigma i)\ell_i'(x) + \mathsf{p}\sigma x^{\mathsf{p}-1} + (\mathsf{p}-1)x^{\mathsf{p}-2}\sum_{i=0}^{\mathsf{p}-1} c_i\ell_i(x)$, where $\mathsf{p} \ge 3$. Thus, the parameters c_0, σ, b_j and c_j, for $1 \le j \le \mathsf{p}-1$, need to be chosen such that $f'(x) \not\equiv 0 \bmod \mathsf{p}$, for all $x \in \mathbb{Z}_\mathsf{p}$. Now, $f(x) + \sigma x = \sum_{i=0}^{\mathsf{p}-1}(b_i + c_i x^{\mathsf{p}-1})\ell_i(x) + \sigma x^\mathsf{p}$, and $f'(x) + \sigma = \sum_{i=0}^{\mathsf{p}-1}(b_i + c_i x^{\mathsf{p}-1})\ell_i'(x) + \mathsf{p}\sigma x^{\mathsf{p}-1} + (\mathsf{p}-1)x^{\mathsf{p}-2}\sum_{i=0}^{\mathsf{p}-1} c_i\ell_i(x)$. Thus, $f'(0) + \sigma \equiv -\sum_{i=1}^{\mathsf{p}-1} i^{-1}b_i \bmod \mathsf{p}$ and $f'(j) + \sigma \equiv \sum_{\substack{i=0 \\ i \ne j}}^{\mathsf{p}-1} a_i(j-i)^{-1} + c_0 j^{-1} - j^{-1}c_j \bmod \mathsf{p}$, for $1 \le j \le \mathsf{p}-1$, which implies that every element in the sequence of numbers $(f'(i)+\sigma) \bmod \mathsf{p}$, for $0 \le i \le \mathsf{p}-1$, is independent of the choice of σ, and the condition that $f'(i) \not\equiv 0 \bmod \mathsf{p}$, for $0 \le i \le \mathsf{p}-1$, is equivalent to that $\sigma \notin \{(f'(i)+\sigma) \bmod \mathsf{p} \,:\, 0 \le i \le \mathsf{p}-1\}$. For $\mathsf{p} \ge 3$, $\sum_{i=0}^{\mathsf{p}-1} i \equiv \sum_{i=0}^{\mathsf{p}-1} 1 \equiv 0 \bmod \mathsf{p}$, and since $\mathbb{Z}_\mathsf{p}$ is the splitting field of the polynomial $x^\mathsf{p} - x = \prod_{i=0}^{\mathsf{p}-1}(x-i)$, the elementary symmetric polynomials $s_r(t_1, t_2, \ldots, t_n)$, which are homogeneous of degree r in n variables, for the particular instances of parameters $n = \mathsf{p}$ and $t_i = i-1$, for $1 \le i \le \mathsf{p}$, as defined in [[30]], are all congruent to $0 \bmod \mathsf{p}$, for $1 \le r \le \mathsf{p}-2$. Thus, $\sum_{i=0}^{\mathsf{p}-1} i^r \equiv \sum_{i=0}^{\mathsf{p}-1} 1 \equiv 0 \bmod \mathsf{p}$, for $r \in \mathbb{N}$, $1 \le r \le \mathsf{p}-2$ and $\mathsf{p} \ge 3$, which implies that for a nonzero polynomial $g(x) \in \mathbb{Z}_\mathsf{p}[x]$ of degree at most $\mathsf{p}-2$, $\sum_{i=0}^{\mathsf{p}-1} g(i) \equiv 0 \bmod \mathsf{p}$. Now, $\mathsf{p}\sum_{i=0}^{\mathsf{p}-1} i^{\mathsf{p}-1} \equiv 0 \bmod \mathsf{p}$, and, for $l \in \mathbb{N}$, such that $\mathsf{p}+1 \le l \le 2\mathsf{p}-2$, $l\sum_{i=0}^{\mathsf{p}-1} i^{l-1} \equiv l\sum_{i=0}^{\mathsf{p}-1} i^{l-1-(\mathsf{p}-1)} \equiv l\sum_{i=0}^{\mathsf{p}-1} i^{l-\mathsf{p}} \equiv 0 \bmod \mathsf{p}$, since $1 \le l - \mathsf{p} \le \mathsf{p}-2$. Thus, for a nonzero polynomial $h(x) \in \mathbb{Z}_\mathsf{p}[x]$ of degree at most $2\mathsf{p}-2$, $\sum_{i=0}^{\mathsf{p}-1} h'(i) \equiv 0 \bmod \mathsf{p}$. The coefficients c_i, for $0 \le i \le \mathsf{p}-1$, must be so chosen that the additional requirement that $f(x)+\sigma x$ is a polynomial of degree at most $2\mathsf{p}-2$ can also be fulfilled. Now, let $\lambda_i \in \mathbb{Z}_\mathsf{p}$, for $0 \le i \le \mathsf{p}-1$, be chosen, such that the cardinality of the set $\Lambda = \{\lambda_i \,:\, 0 \le i \le \mathsf{p}-1\}$ is at most $\mathsf{p}-1$ and $\sum_{i=0}^{\mathsf{p}-1} \lambda_i = 0$. Then, $c_j - c_0$ are found from the condition $f'(j)+\sigma = \sum_{\substack{i=0 \\ i \ne j}}^{\mathsf{p}-1} a_i(j-i)^{-1} - j^{-1}(c_j - c_0) = \lambda_j$, for $1 \le j \le \mathsf{p}-1$, and hence, $f'(0)+\sigma = -\sum_{i=1}^{\mathsf{p}-1} i^{-1}b_i = \lambda_0$, for all choices of c_0. Now, let σ be chosen from $\mathbb{Z}_\mathsf{p}\backslash\Lambda$, where the latter set is nonempty, since the cardinality of Λ is at most $\mathsf{p}-1$, by the choices of λ_i, for $0 \le i \le \mathsf{p}-1$.

Finally, c_0 is chosen, and b_j and c_j, for $1 \le j \le \mathsf{p}-1$, are determined by the aforementioned conditions.

For a small prime number p, positive integers l and r, such that $l \ge 2$ and $1 \le r \le l$, a bijective mapping $f(x) \in \mathbb{Z}_{\mathsf{p}^l}[x]$ and $y \in \mathbb{Z}_{\mathsf{p}^l}$, the following procedure computes $x_r \in \mathbb{Z}_{\mathsf{p}^r}$, such that $f_r(x_r) \equiv y \bmod \mathsf{p}^r$, assuming $x_1 \in \mathbb{Z}_{\mathsf{p}}$ is known, such that $f_1(x_1) \equiv y \bmod \mathsf{p}$, where $f_r(x) = f(x) \bmod \mathsf{p}^r$, applying the $\bmod \mathsf{p}^r$ operation only to the coefficients. Let $2 \le r \le l$, where $l \ge 2$, $s \in \mathbb{N}$ be such that $\lceil \frac{r}{2} \rceil \le s \le r-1$ and $y_r = y \bmod \mathsf{p}^r \in \mathbb{Z}_{\mathsf{p}^r}$, and $x_s = f_s^{-1}(y_r \bmod \mathsf{p}^s) \in \mathbb{Z}_{\mathsf{p}^s}$ has been computed. Let $\hat{x}_s \in \mathbb{Z}_{\mathsf{p}^r}$ be such that $\hat{x}_s \equiv x_s \bmod \mathsf{p}^s$. Since $f_r(\hat{x}_s) \equiv y_r \bmod \mathsf{p}^s$, it follows that $f_r(\hat{x}_s) = y_r + \mathsf{p}^s g_{r,\,s}(\hat{x}_s,\, y_r)$, for some mapping $g_{r,\,s}(\hat{x}_s,\, y_r)$, and therefore, $f_r\big(\hat{x}_s + [f_r'(\hat{x}_s)]^{-1} \cdot [y_r - f_r(\hat{x}_s)]\big) \equiv f_r(\hat{x}_s) + f_r'(\hat{x}_s) \cdot \big[f_r'(\hat{x}_s)\big]^{-1} \cdot \big[y_r - f_r(\hat{x}_s)\big] \equiv f_r(\hat{x}_s) + \big[y_r - f_r(\hat{x}_s)\big] \equiv y_r \bmod \mathsf{p}^r$. Thus, $f_r^{-1}(y_r) = \hat{x}_s + \big[f_r'(\hat{x}_s)\big]^{-1} \cdot \big[y_r - f_r(\hat{x}_s)\big] \bmod \mathsf{p}^r$. If $r = l$, then the $f^{-1}(y)$ is just computed for $y \in \mathbb{Z}_{\mathsf{p}^l}$, and the procedure can be stopped; otherwise, the previous steps are repeated, replacing the current value of r by $\min\{2r,\, l\}$.

Examples in $\mathcal{EXP}\big(\mathbb{F}\,;\,[z]\big)$. Let $\mathbb{F}$ be a finite field of p^n elements, for some prime number p and $n \in \mathbb{N}$, such that $\mathsf{p}^n \ge 3$, and let $\mathfrak{n} = \mathsf{p}^n - 1$. Let $s,\, t \in \mathbb{N}$ be such that $\mathsf{gcd}(s,\, t) = 1$, $st = \mathfrak{n}$ and $2 \le s,\, t \le \mathfrak{n} - 1$, and let $H_t = \{x^t = 1 \,:\, x \in \mathbb{F}^*\}$. Let $f(x) \in \mathbb{Z}[x]$ be such that $f(x) \bmod t$ yields a polynomial mapping from $\mathbb{Z}_t$ onto itself. It may be recalled that, as a set, $\mathbb{Z}_t$ is assumed to consist of integers i, where $0 \le i \le t-1$. Let a be a primitive element in $\mathbb{F}^*$. Now, for $x \in H_t$, since $x^t = 1$, applying $\log_a$ operation on both sides, $t \log_a x = 0 \bmod \mathfrak{n}$, which implies that $\log_a x$ is an integer multiple of s, for every $x \in H_t$, and, since the cyclic subgroup generated by a^s is H_t, it follows that $\log_a$ is a bijective mapping of H_t onto $s \cdot \mathbb{Z}_{\mathfrak{n}}$. Now, $f(\log_a(x)) \bmod \mathfrak{n}$, for $x \in H_t$, is an injective mapping, when restricted to H_t, which can be modified appropriately, by changing its constant term, if necessary, to obtain a polynomial g, which results in a bijective mapping from $s \cdot \mathbb{Z}_{\mathfrak{n}}$ into itself, with respect to $\bmod \mathfrak{n}$ operation. Then, the mapping $\eta(x) = a^{g(\log_a x)}$, for $x \in \mathbb{F}^*$, is such that its restriction to H_t is a bijective mapping from H_t onto itself.

2.2.2 Hybrid Single Variable Permutation Mappings with Hashing

$\boxed{\text{Method 1}}$ Let $\ell_i(x) \in \mathbb{F}[x]$, $1 \le i \le k$, where $k \in \mathbb{N}$, $k \ge 2$, be indicator functions of a partition $\{S_i \,:\, 1 \le i \le k\}$ of $\mathbb{F}$. Let σ be a permutation on $\{1,\, \ldots,\, k\}$, such that the set cardinalities of S_i and $S_{\sigma(i)}$ are equal, for $1 \le i \le k$. Let g_i be a mapping from $\mathbb{F}$ into $\mathbb{F}$, such that $g_i\big(S_i\big) = S_{\sigma(i)}$, for $1 \le i \le k$. Thus, g_i is one-to-one when restricted to S_i, for $1 \le i \le k$. Let $\eta(x) \in \mathbb{F}[x]$ be a permutation polynomial, and $\chi(x) = \sum_{i=1}^{k} \ell_i(x)\eta(g_i(x))$.

Then, $\chi(\mathbb{F}) = \bigcup_{i=1}^{k} \eta\big(g_i(S_i)\big) = \bigcup_{i=1}^{k} \eta\big(S_{\sigma(i)}\big)$, and since $\{S_{\sigma(i)} : 1 \le i \le k\}$ is a partition of $\mathbb{F}$, $\chi(x)$ is a surjective (hence bijective) polynomial from $\mathbb{F}$ onto $\mathbb{F}$. For inverting $\chi(x) = y$, for fixed $y \in \mathbb{F}$, let $\xi = \eta^{-1}(y)$. Now, there exists exactly one index i, where $1 \le i \le k$, such that $\xi \in S_{\sigma(i)} = g_i\big(S_i\big)$, and therefore, the unique element $x \in S_i$, such that $x = g_i^{-1}(\xi)$, satisfies $\chi(x) = y$. If f_i, for $1 \le i \le k$, are mappings from $\mathbb{F}$ into $\mathbb{F}$, such that $f_i(g_i(x)) = x$, for $x \in S_i$, then $\chi^{-1}(y) = \sum_{i=1}^{k} \ell_{\sigma(i)}\big(\eta^{-1}(y)\big) f_i\big(\eta^{-1}(y)\big)$, for $y \in \mathbb{F}$. The case of bijective mappings in $\mathcal{EXP}\big(\mathbb{F}\,;\,[x]\big)$ can be similarly discussed. In the following examples, the corresponding examples in section 2.1.2 are revisited.

Examples. (A) Let $T(x) = \sum_{i=1}^{n} a_i x^{\mathtt{p}^{i-1}}$, $a_i \in \mathbb{F}$, $1 \le i \le n$, be of rank t, where t is a small positive integer, such as $t \in \{1, 2\}$, as described in the first example in section 2.1.2 and let $V = \{x \in \mathbb{F} : T(x) = 0\}$. Then, there exist $k = \mathtt{p}^t$ representative elements $b_i \in \mathbb{F}$, $1 \le i \le k$, such that $\{T(b_i) : 1 \le i \le k\} = T(\mathbb{F})$, and $S_i = V + b_i = \{x + b_i : x \in V\}$, $1 \le i \le k$. Let $f_i(x) = c_{i,0} + \sum_{i=1}^{n} c_{i,j} x^{\mathtt{p}^{j-1}}$, where $c_{i,j}$, $x \in \mathbb{F}$, $0 \le j \le n$, be such that $V \subseteq f_i(V)$, for $1 \le i \le k$. Thus, in the notation of the above discussion, the permutation polynomial $f_i(x) - b_i + b_{\sigma(i)}$ can be chosen to be $g_i(x)$, for $x \in \mathbb{F}$ and $1 \le i \le k$. (B) Let $f(z) = z^t$, where t is a large positive integer dividing $\mathtt{p}^n - 1$, as described in the second example of section 2.1.2. Let $a_1 = 0$ and $a_i \in \mathbb{F}^*$, for $2 \le i \le k$, where $k = 1 + \frac{(\mathtt{p}^n - 1)}{t}$, be such that $\{f(a_i) : 1 \le i \le k\}$ is the codomain of f. Let σ be a permutation on $\{1, \ldots, k\}$, such that $\sigma(1) = 1$, and let $H_t = \{y \in \mathbb{F} : y^t = 1\}$. Then, $S_i = a_i H_t = \{a_i v : v \in H_t\}$, for $1 \le i \le k$. Let $h_i(x)$, $x \in H_t$, be a bijective mapping discussed in the previous section, for $2 \le i \le k$. Thus, representing elements $c_i \in \mathbb{F}^*$ can be found easily, such that the mapping $g_i(x) = c_i h_i(a_i^{-1} x)$ satisfies $g_i\big(S_i\big) = S_{\sigma(i)}$, for $x \in S_i$ and $2 \le i \le k$.

$\boxed{\text{Method 2}}$ Let G be $\mathbb{F}^*$ or $\mathbb{F}$. Let $k, \rho \in \mathbb{N}$, such that $2 \le k \le \rho$. Let f_i be bijective mappings from G into itself, for $1 \le i \le \rho$, and h be a mapping from G into itself, such that $h\big(f_i(x)\big) = h\big(f_j(x)\big)$, for $x \in \mathsf{G}$ and $1 \le i, j \le \rho$. Let σ be a permutation on $\{1, \ldots, \rho\}$, and $\{S_i : 1 \le i \le k\}$ be a partition of $\mathbb{F}$, and let $\ell_i(x)$, $x \in \mathbb{F}$, be the indicator function of S_i, for $1 \le i \le k$. Let η be a bijective mapping from G into G, and $\zeta(x) = \sum_{i=1}^{k} \ell_i\big(h(x)\big)\eta\big(f_{\sigma(i)}(x)\big)$, for $x \in \mathsf{G}$. Let $x, y \in \mathsf{G}$ be such that $\zeta(x) = \zeta(y)$, and let $i, j \in \{1, \ldots, k\}$ be such that $\ell_i(h(x)) = 1$ and $\ell_j(h(y)) = 1$. Then, $\eta\big(f_{\sigma(i)}(x)\big) = \eta\big(f_{\sigma(j)}(y)\big)$, and since η is bijective, it follows that $f_{\sigma(i)}(x) = f_{\sigma(j)}(y)$. Now, since $h\big(f_i(x)\big) = h\big(f_j(x)\big)$, for $x \in \mathsf{G}$ and $1 \le i, j \le \rho$, and σ is a permutation on the set $\{1, \ldots, \rho\}$, it follows that $h(x) = h(y)$, $\sigma(i) = \sigma(j)$ and $i = j$, and therefore, $x = y$. Thus, $\zeta^{-1}(y) = \sum_{i=1}^{k} \ell_i\big(h(\eta^{-1}(y))\big) f_{\sigma(i)}^{-1}\big(\eta^{-1}(y)\big)$, for $y \in \mathsf{G}$.

Examples. (A) Let (i) f be a bijective mapping from G into itself, such that the cyclic group generated by it, as a subgroup of bijective mappings from G into G, with composition as the group operation, is of small order $\rho \ge 2$, (ii) $g : \mathsf{G}^\rho \to \mathbb{F}$ is a symmetric function, which can be an expression in $\mathcal{EXP}\big(\mathbb{F}\,;\,[z_1,\,\ldots,\,z_\rho]\big)$, symmetric in all the ρ variables, (iii) $f_0(x)=x$ and $f_i(x)=f\big(f_{i-1}(x)\big)$, for $1\le i\le\rho$, and (iv) $h(x)=g\big(x,\,f_1(x),\,\ldots,\,f_{\rho-1}(x)\big)$, for $x\in\mathsf{G}$. Then, $f_\rho(x)=x$ and, since $h\big(f(x)\big)=h(x)$, for $x\in\mathsf{G}$, it follows that $h\big(f_i(x)\big)=h\big(f_j(x)\big)$, for $x\in\mathsf{G}$ and $1\le i,\,j\le\rho$. If $\mathsf{G}=\mathbb{F}^*$, then it is interesting to choose $f(x)=a^{\phi(\log_a x)}$, for $x\in\mathbb{F}^*$ and some primitive element $a\in\mathbb{F}^*$. However, it is important to choose f such that ρ is a small positive integer. (B) Let $\mathsf{G}=\mathbb{F}^*$ and $s,\,t,\,v\in\mathbb{N}$ be such that $\mathsf{gcd}(s,\,t)=1$, $st=\mathfrak{n}$, $2\le s,\,t\le\mathfrak{n}-1$, $sv=1 \bmod t$ and s large. Let $\phi\,:\,\mathbb{Z}_\mathfrak{n}\to\mathbb{Z}_\mathfrak{n}$ be a polynomial mapping such that $sv\phi(y)$ is a bijective mapping from $sv\mathbb{Z}_\mathfrak{n}$ into itself and the order of the cyclic group generated by $sv\phi(y)$ as a subgroup of the group of bijective mappings from $sv\mathbb{Z}_\mathfrak{n}$ into itself is a small positive integer ρ. Now, let $\pi(x)=a^{sv\phi(\log_a x)}$, for $x\in\mathbb{F}^*$, where a is a primitive element in $\mathbb{F}^*$. Then, $\pi\big(\mathbb{F}^*\big)=\pi\big(H_t\big)=H_t$, where $H_t=\{x\in\mathbb{F}^*\,:\,x^t=1\}$. Let $\pi_1=\pi$ and $\pi_{i+1}=\pi_i(\pi)$, for $i\in\mathbb{N}$. Then, $\pi_{\rho+1}(x)=\pi_1(x)$, for $x\in H_t$. Let f_i be bijective mappings from $\mathbb{F}^*$ into itself, such that the restriction of f_i to H_t is π_i, for $1\le i\le\rho$, and g be the symmetric mapping as in the previous example and $h(x)=g\big(\pi_1(x),\,\ldots,\pi_\rho(x)\big)$. It can be easily checked that $h\big(f_i(x)\big)=h\big(f_j(x)\big)$, for $x\in\mathsf{G}$ and $1\le i,\,j\le\rho$.

2.3 Multivariate Injective Mappings without Parameters

2.3.1 Multivariate Injective Mappings from G^m into E^m

In this subsection, an iterative algorithm to construct a multivariate bijective mapping from G^m into E^m, for $m\in\mathbb{N}$, is described. The algorithm utilises parametric univariate bijective mappings discussed in the previous sections. In later subsections, some variations involving hashing are described.

1. Let $f_i\,:\,\mathsf{G}\to\mathsf{G}$ and $g_i\,:\,\mathsf{E}\to\mathsf{E}$, for $1\le i\le m$, be bijective mappings.

2. Let $h_i(z_1,\,\ldots,\,z_{m-1};\,x)$ be parametric injective mappings from G into E, for $1\le i\le m$, $x\in\mathsf{G}$ and $z_1,\,\ldots,\,z_{m-1}\in\mathsf{E}$ being parameters, constructed, for example, as described in section 2.1.1.

3. Let $\zeta_i(\mathbf{x})=h_i\big(\zeta_{i+1}(\mathbf{x}),\,\ldots,\,\zeta_m(\mathbf{x}),\,x_1,\,\ldots,\,x_{i-1}\,;\;f_i(x_i)\big)$ and $\eta_i(\mathbf{x})=g_i\big(\zeta_i(\mathbf{x})\big)$, for $\mathbf{x}=(x_1,\,\ldots,\,x_m)\in\mathsf{G}^m$ and $1\le i\le m$. Let $\eta(\mathbf{x})=(\eta_1(\mathbf{x}),\,\ldots,\,\eta_m(\mathbf{x}))$.

For finding $\mathbf{x}=(x_1,\,\ldots,\,x_m)\in\mathsf{G}^m$, such that $\eta(\mathbf{x})=\mathbf{y}$, for any fixed $\mathbf{y}=(y_1,\,\ldots,\,y_m)\in\mathsf{E}^m$, let $\epsilon_i=g_i^{-1}(y_i)$ and $\delta_i=h_i^{-1}(\epsilon_{i+1},\,\ldots,\,\epsilon_m,\,x_1,\,\ldots,\,x_{i-1};\,\epsilon_i)$, for $1\le i\le m$. Then, $x_i=f_i^{-1}(\delta_i)$, for $1\le i\le m$. Now, for $\mathsf{E}=\mathbb{F}$ and $\mathsf{G}=\mathbb{F}^*$, if g_i and h_i, for $1\le i\le m$, are bijective mappings and parametric bijective mappings, respectively, from $\mathbb{F}^*$ into $\mathbb{F}^*$, then the above procedure can be applied to obtain multivariate bijective mappings from G^m into G^m. These mappings are required in appealing for a security that is immune to threats resulting from Gröbner basis analysis. It can be observed that one level of exponentiation suffices for the purpose.

A one-to-one mapping from G^m into E^n, where m and n are positive integers, with $m \leq n$, and G is a subset of a finite field $\mathbb{F}$, is obtained as follows: for a carefully chosen bijective mapping $P(\mathbf{y})$ from G^n into E^n and hashing keys $f_i(\mathbf{x})$, for $\mathbf{x} = (x_1, \ldots, x_m) \in \mathsf{G}^m$ and $1 \leq i \leq n-m$, the argument vector $(f_1(\mathbf{x}), \ldots, f_{n-m}(\mathbf{x}), x_1, \ldots, x_m)$ is substituted for $\mathbf{y} \in \mathsf{G}^n$ in $P(\mathbf{y})$. Thus, $Q(\mathbf{x}) = P(f_1(\mathbf{x}), \ldots, f_{n-m}(\mathbf{x}), x_1, \ldots, x_m)$ is a generic multivariate one-to-one mapping from G^m into G^n.

2.3.2 Hybrid Multivariate Injective Mappings with Hashing

For Method 1 of the previous subsection, in the first example, in place of $T(x)$, $x \in \mathbb{F}$, $T\big(\alpha(\mathbf{x})\big)$, $\mathbf{x} \in \mathbb{F}^m$, and in the second example, in place of $f(z)$, $z \in \mathbb{F}$, $f\big(\beta(\mathbf{x})\big)$, $\mathbf{x} \in \mathbb{F}^m$, are chosen, where $\alpha : \mathbb{F}^m \to \mathbb{F}$ is a non constant affine mapping in the first example, and $\beta(\mathbf{x}) = c \prod_{i=1}^{m} x_i^{s_i}$, for some nonnegative integers s_i, which, when positive, are relatively prime to $\mathsf{p}^n - 1$, and, when zero, for the corresponding subscript index i, the variable x_i does not occur in the product, for $1 \leq i \leq m$, such that $\beta(\mathbf{x})$ is nonconstant, in the second example. Similarly, Method 2 hashing of the previous subsection can also be extended to multivariate mappings, replacing x with $\mathbf{x}$, and choosing $\Phi(\mathbf{y}) = \big(\phi_1(\mathbf{y}), \ldots, \phi_m(\mathbf{y})\big)$ to be a bijective mapping from $\mathbb{Z}_{\mathsf{n}}^m$ into itself in place of $\phi(y)$. It can be observed that g can also be chosen to depend only on a few scalar components from each vector, while maintaining symmetry in all its vector parameters, with each vector consisting of m scalars components. In the first example of Method 2 hashing of the previous section, if $h(\mathbf{x})$ is a symmetric mapping in its m components, then $f(\mathbf{x})$ can be chosen to be a permutation of components of $\mathbf{x}$, independent of order ρ of the cyclic group generated by f, with respect to composition operation.

3 Public Key Cryptography and Digital Signature

Let the number of elements in the plain message (or plain signature message) be μ, and the number of elements in the encrypted message (or encrypted signature message) be ν, where $\mu, \nu \in \mathbb{N}$ and $\mu \leq \nu$. Let E be $\mathbb{F}$ or $\mathbb{Z}_{\mathsf{n}}$, and $\mathsf{G} \subseteq \mathsf{E}$ be the set from which plain message elements are sampled. If the number of plain and encrypted (or plain and signed) messages are the same, then a multivariate bijective mapping $P : \mathsf{G}^\mu \to \mathsf{G}^\mu$ is chosen and advertised in the public key lookup table T, while P^{-1} is saved in the back substitution table B. Let $\big(\xi_1, \ldots, \xi_\mu\big) \in \mathsf{G}^\mu$ be plain message. For public key cryptography, the encrypted message is $\big(\epsilon_1, \ldots, \epsilon_\mu\big) = P\big(\xi_1, \ldots, \xi_\mu\big)$, and the decryption is $P^{-1}\big(\epsilon_1, \ldots, \epsilon_\mu\big)$. For digital signature, the signed message is $\big(\epsilon_1, \ldots, \epsilon_\mu\big) = P^{-1}\big(\xi_1, \ldots, \xi_\mu\big)$, and recovered message is $P\big(\epsilon_1, \ldots, \epsilon_\mu\big)$.

In the remaining part of the section, it is assumed that $1 \leq \mu \leq \nu - 1$. Let κ be the number of padding message elements in the hashing keys. It is assumed that the key generator ensures that a prospective owner of the pertinent keys is provided with an abundance of options for generating multivariate one-to-one mappings, whose inverse mappings are known only to the owner. Let $\mathbf{x} = (x_1, \ldots, x_\mu) \in \mathsf{G}^\mu$ be the plain message, $\mathbf{y} = (y_1, \ldots, y_\nu) \in \mathsf{E}^\nu$ be the encrypted or signed message, and $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_\kappa) \in \mathsf{G}^\kappa$ be a padding message. For public key encryption, an injective mapping P from G^ν into E^ν is chosen, while for digital signature, a surjective mapping P from G^ν onto G^μ (in addition to two more surjective mappings) is chosen. Thus, for public key cryptography mapping, invertible parametric matrices in the most general form can be utilised, while for digital signature multivariate surjective or bijective mappings, only parametric permutation and diagonal matrices are employed.

For public key cryptography, let $\lambda = \nu - \mu$, and let P be an injective mapping from G^ν into E^ν. Let $\mathbf{y} \in \mathsf{G}^\nu$ be the argument vector of the bijective mapping P. Then, the vector $\big(f_1(\mathbf{x}, \boldsymbol{\omega}), \ldots, f_\lambda(\mathbf{x}, \boldsymbol{\omega}), x_1, \ldots, x_\mu\big)$, for some hidden keys $f_1(\mathbf{x}, \boldsymbol{\omega}), \ldots, f_\lambda(\mathbf{x}, \boldsymbol{\omega})$, is substituted for $\mathbf{y}$ of the public key encryption mapping. Let $F(\mathbf{x}, \boldsymbol{\omega}) = \big(f_1(\mathbf{x}, \boldsymbol{\omega}), \ldots, f_\lambda(\mathbf{x}, \boldsymbol{\omega})\big)$, and it is assumed that $F(\mathbf{x}, \boldsymbol{\omega}) \in \mathsf{G}^\lambda$, for $\mathbf{x} \in \mathsf{G}^\mu$ and $\boldsymbol{\omega} \in \mathsf{G}^\kappa$. The information required to compute $P^{-1}(\boldsymbol{\varepsilon})$, for $\boldsymbol{\varepsilon} \in \mathsf{E}^\nu$, and the hidden hashing keys $F(\mathbf{x}, \boldsymbol{\omega})$, for $\mathbf{x} \in \mathsf{G}^\mu$ and $\boldsymbol{\omega} \in \mathsf{G}^\kappa$, is saved in a private key back-substitution table B, while the mapping $P\big(F(\mathbf{x}, \boldsymbol{\omega}), \mathbf{x}\big)$ is saved in the public key lookup table T. If the sender and receiver agree on $\boldsymbol{\omega}$, and the encrypted message received is $\boldsymbol{\varepsilon} \in \mathsf{G}^\nu$, then, with $(\mathbf{z}, \mathbf{x}) = P^{-1}(\boldsymbol{\varepsilon})$, the receiver can ascertain data integrity by testing whether $F(\mathbf{x}, \boldsymbol{\omega}) = \mathbf{z}$. It is possible to utilise $\boldsymbol{\omega}$ as a session key in handshake protocols for repeated key negotiations.

For digital signature, let κ λ, K, L, μ and ν be positive integers, such that $K \leq \kappa$, $L \leq \lambda$ and $\nu \geq L+\mu$. Let P, Q and R be multivariate surjective mapping from G^ν onto $\mathsf{G}^{L+\mu}$, from G^κ onto G^K and from G^λ onto G^L, respectively. The right inverse mappings of the stated multivariate surjective mappings are known only to the signer. Let $F(\mathbf{x}, \boldsymbol{\omega}) = \big(f_1(\mathbf{x}, \boldsymbol{\omega}), \ldots, f_L(\mathbf{x}, \boldsymbol{\omega})\big)$. The components of the mapping P, corresponding to the plain message, are advertised in a public key signature verification table V, and the information for computing a right inverse of P — and, in general, all the information required by the signing algorithm — is saved in a private key signature table S, for signing plain message. Now, for a plain message $\mathbf{x} \in \mathsf{G}^\mu$ and a padding message $\boldsymbol{\omega} \in \mathsf{G}^\kappa$, the signed message $\boldsymbol{\varepsilon}$ is obtained by applying a right inverse mapping of P on the instance $(\mathbf{z}', \mathbf{x}) \in \mathsf{G}^{L+\mu}$, where $\mathbf{z}' = F(\mathbf{x}, \boldsymbol{\omega})$. The parameter $\mathbf{z} \in \mathsf{G}^\lambda$ is so chosen by the signer that $F(\mathbf{x}, \boldsymbol{\omega}) = R(\mathbf{z})$, by computing a right inverse of the multivariate surjective mapping R. For a plain message $\mathbf{x} \in \mathsf{G}^\mu$, the padding message $\boldsymbol{\omega} \in \mathsf{G}^\kappa$ is obtained by computing a right inverse, which is known only to the signer, of the multivariate surjective mapping Q from G^κ onto G^K, such that $Q(\boldsymbol{\omega}) = \boldsymbol{\omega}'$, where $\boldsymbol{\omega}' \in \mathsf{G}^K$ is agreed upon by the singer with a trusted authentication verifier TAV, for this particular signature transaction, as a first step in the signature generation procedure. The plain message can be found by computing the components of the mapping P, that are advertised in the public key signature verification table V, for a signed message $\boldsymbol{\varepsilon} \in \mathsf{G}^{\nu}$. For claiming the authenticity of the signature, the receiver of the signature needs to produce also $\mathbf{z}$, which must be transmitted to the receiver by the signer. In addition to the signature verification table V, containing plain message components of the mapping P, another table A, called the signature authentication table, containing the full mapping P and additional functions $H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega})$, with several components, *i.e.*, with values in E^{τ}, for some positive integer τ, is employed for signature authentication verification purpose, for which the signer meeds to provide $(\mathbf{z}, \boldsymbol{\delta}, \boldsymbol{\omega})$, where $\boldsymbol{\delta} \in \mathsf{E}^{\tau}$ is such that $\boldsymbol{\delta} = H\big(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega}\big)$, at the signer end, and the signature authentication is verified by testing whether $H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega}) = \boldsymbol{\delta}$ and $R(\mathbf{z}) = F(\mathbf{x}, \boldsymbol{\omega})$, by the verification authority, such that the vector $(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega})$ satisfies additional conditions, such as $Q(\boldsymbol{\omega}) = \boldsymbol{\omega}'$, where $\boldsymbol{\omega}'$ has been consented by the TAV for this signature.

The signature authentication table A is registered with a trusted authentication verifier (TAV), which is a public authority responsible for signature authentication verification purpose. The authentication information shared by the signer with TAV contains the multivariate mappings $P(\boldsymbol{\varepsilon})$, $F(\mathbf{x}, \boldsymbol{\omega})$, $Q(\boldsymbol{\omega})$ and $R(\mathbf{z})$, where P, Q and R are surjective mappings from G^{ν} onto $\mathsf{G}^{L+\mu}$, from G^{κ} onto G^{K} and from G^{λ} onto G^{L}, respectively. The information required to compute any right inverse mappings of P, Q and R is known only to the owner of the signature keys, *i.e.*, the signer. The verification protocol at TAV side checks whether $Q(\boldsymbol{\omega})$ and $\mathbf{x}$ meet certain obligations, and whether $R(\mathbf{z}) = F(\mathbf{x}, \boldsymbol{\omega})$, without knowing right inverse mappings of Q and R. Now, for a particular plain message $\mathbf{x}$ to be signed, the signer obtains an extra padding message $\boldsymbol{\omega}' \in \mathsf{G}^{K}$, with the consent of TAV, conforming to the predefined agreement for a valid padding message with TAV, and computes right inverse of Q with $\boldsymbol{\omega}'$ as the argument, to get the actual padding message $\boldsymbol{\omega} \in \mathsf{G}^{\kappa}$. Finally, with $\mathbf{x}$ and $\boldsymbol{\omega}$ having been chosen or computed, the signer generates $\mathbf{z} \in \mathsf{G}^{\lambda}$ by computing a right inverse of R with $F(\mathbf{x}, \boldsymbol{\omega})$ as the argument, and the signature itself by computing the inverse of the key mapping P, which is a multivariate surjective mapping from G^{ν} into $\mathsf{G}^{L+\mu}$.

It is possible to include $H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega})$ in the signature verification public key table V, in order to facilitate the receiver with a data integrity check, before approaching the TAV. This choice depends on the group of possible receivers and signers besides TAV. If the intended group of possible receivers is very large, such as external world, then it is convenient to reserve $H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega})$ to be present only in the signature authentication table A. In any case, the components of the map P corresponding to $F(\mathbf{x}, \boldsymbol{\omega})$ may be exclusively present only in the signature authentication table A, since disclosing this information to the public may lead to its speculation based on various observed values.

In the proposed model of digital signature scheme, the signer approaches the TAV, with a request for generating a signed message for a specific purpose. The TAV issues consent for a particular extra padding message $\boldsymbol{\omega}'$, for a period of validity along with a transaction number. The extra padding message $\boldsymbol{\omega}'$ may contain a small gist of transaction details, encrypted by the key of TAV. Thus, the signer must request TAV, for the issuance of the extra padding message $\boldsymbol{\omega}'$, by submitting a form containing a gist of transaction or signature details and its intended purpose. The TAV then generates an extra padding message $\boldsymbol{\omega}'$, transaction number and period of validity, and issues them to the signer. The signer is required to transmit the transaction number and period of validity to the intended receiver of the signature, who will have to produce these particulars to TAV for claiming the authenticity of the signed message. It may additionally be required that the claimants of the authenticity of a signed message will be required to furnish their signatures to TAV, with TAV and possibly also the sender bearing the role of the receiver, for a proof of the claim.

Multivariate surjective mappings can be realised as parametric mappings, which are bijective for some choice of parameter component values, and may be arbitrary mappings for some other choice of parameter values. The choice of parameters is known to the signer. For example, for the multivariate surjective mapping Q from G^{κ} onto G^{K}, $\kappa - K$ components of $\boldsymbol{\omega}$ are taken in the argument vector of the partition of unity functions of section 2.1, with $l = \kappa - K$ and $m = K$, in the notation followed there. When combined with the partitioning methods of section 2.1.1, for some partitions, with index i, the mappings $\zeta_i\big(z_1, \ldots, z_l; \mathbf{x}\big)$ are chosen to be bijective, and for the remaining, the mappings are arbitrary.

4 Complexity Analysis of Computing Left Inverse Mappings of Multivariate Injective Mappings and of Computing Right Inverse Mappings of Multivariate Surjective Mappings

Model theory of fields and polynomial algebras is extensively studied in mathematical logic [12, 14, 20, 35, 36]. Let $\mathbb{F}$ be a field, and let $\mathcal{ARITH}\text{-}\mathcal{EXP}(\mathbb{F})$ be the set of arithmetic expressions without quantifiers, obtained by collecting the expressions involving any number of finitely many variables, constructed using parentheses and the binary or unary arithmetic operators of addition $+$, subtraction $-$, multiplication $\cdot$, possibly division $/$, exponentiation ^{k}, where k is a positive integer, and binary valued relational operator $=$ (and possibly other relational operators such as $<$, $>$, $\leq$ and $\geq$). The relational operators allow construction of assertions that evaluate to any-one of the special symbolic constants `false` and `true`, represented by 0 and 1, respectively. In the sequel, the variables assume values from $\mathbb{F}$, the arithmetic expressions evaluate to values in $\mathbb{F}$, as defined by the arithmetic operations in $\mathbb{F}$, and the assertions evaluate to values in $\{0, 1\}$. A variable taking values in $\{0, 1\}$ is a boolean variable. The arithmetic expressions in $\mathcal{ARITH}\text{-}\mathcal{EXP}(\mathbb{Z}_2)$ are boolean expressions. For any field $\mathbb{F}$, a boolean variable x can be obtained from the equation $x^2 - x = 0$. For boolean variables x and y, $\neg x$ can be represented by $1-x$, $x \wedge y$ by $x \cdot y$, $x \vee y$ by $1-(1-x)\cdot(1-y)$, $x \oplus y$ by $(x-y)^2$, $x \rightarrow y$ by $1-x\cdot(1-y)$, and $x \leftrightarrow y$ by $1-(x-y)^2$, where $\neg$ denotes the logical "negation", $\wedge$ the logical "and", $\vee$ the logical "or", $\oplus$ the logical "exclusive or", $\rightarrow$ the logical "implies", and $\leftrightarrow$ the logical "implies and is implied by". The inequality operator, denoted by $\neq$, is a secondary binary operator defined as the logical negation of the equality operator. Let $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$ be the set of arithmetic expressions in which some (none, some or all) variables are constrained by "existential" $\exists$ or "universal" $\forall$ quantifiers. A variable constrained by a quantifier is called a *bound* variable. A variable that is not bound is called a *free* variable. An arithmetic expression in which all the variables are free is a quantifier free arithmetic expression, *i.e.*, an expression in $\mathcal{ARITH}\text{-}\mathcal{EXP}(\mathbb{F})$. A quantified arithmetic expression is in prenex normal form, if all the quantifiers occur before the otherwise quantifier free arithmetic expression, *i.e*, a quantified arithmetic expression of the form $\forall y_1 \ldots \forall y_{k_1} \exists x_1 \ldots \forall y_{k_{i-1}+1} \ldots \forall y_{k_i} \exists x_i \ldots \forall y_{k_{m-1}+1} \ldots \forall y_{k_m} \exists x_m$ $\forall y_{k_m+1} \ldots \forall y_n \quad f(x_1, \ldots, x_m, y_1, \ldots, y_n)$, where m and n are positive integers, and k_i, for $1 \leq i \leq m$, are nonnegative integers such that $k_i \leq k_{i+1}$, for $1 \leq i \leq m-1$, and $k_m \leq n$. The variables y_j, $1 \leq j \leq n$, are *independent* variables, as they are bound to universal quantifiers. The variable x_i depends on the variables y_j, $1 \leq j \leq k_i$, $1 \leq i \leq m$, and is a *dependent* bound variable. A tuple $\left(a_1, \ldots, a_i, b_1, \ldots, b_{k_i}\right) \in \mathbb{F}^{i+k_i}$, $1 \leq i \leq m$, is *feasible* to a quantified arithmetic expression in prenex normal form with no free variables as described before, if either $i = m$ and $f(a_1, \ldots, a_m, b_1, \ldots, b_{k_m}, y_{k_m+1}, \ldots, y_n)$ evaluates to 1, for $y_{k_m+1}, \ldots, y_n \in \mathbb{F}$, or $1 \leq i \leq m-1$ and each tuple $(a_1, \ldots, a_i, x_{i+1}, b_1, \ldots, b_{k_i}, y_{k_i+1}, \ldots, y_{k_{i+1}})$, for $y_{k_i+1}, \ldots, y_{k_{i+1}} \in \mathbb{F}$, and for some $x_{i+1} \in \mathbb{F}$, that may depend on $a_1, \ldots, a_i, b_1, \ldots, b_{k_i}, y_{k_i+1}, \ldots, y_{k_{i+1}} \in \mathbb{F}$ is feasible. If for every $b_1, \ldots, b_{k_1} \in \mathbb{F}$, there exists $a_1 \in \mathbb{F}$, such that the tuple $\left(a_1, b_1, \ldots, b_{k_1}\right)$ is feasible, then the given instance of binary valued quantified arithmetic expression is *satisfiable*. The evaluation problem for quantified boolean expressions in prenex normal form with no free variables in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$ is to find whether the given input instance is satisfiable. Let $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{F}) \subseteq \mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$ be the set of satisfiable binary valued quantified arithmetic expressions (*i.e.*, quantified arithmetic assertions) in prenex normal form with no free variables that evaluate to `true`. Let $\mathcal{B}_{\mathcal{Q}}$ and $\mathcal{B}_{\mathcal{Q}-\mathrm{SAT}}$ be $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(Z_2)$ and $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(Z_2)$, respectively. By the previous discussion, every boolean expression in $\mathcal{B}_{\mathcal{Q}}$, analogously in $\mathcal{B}_{\mathcal{Q}-\mathrm{SAT}}$, can be represented by some arithmetic expression in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$, analogously in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{F})$, with equality binary relation, for any field $\mathbb{F}$. The evaluation problem for quantified boolean expressions in prenex normal form with no free variables in $\mathcal{B}_{\mathcal{Q}}$ is PSPACE-complete, where PSPACE is the set of formal languages acceptable in polynomial space [25].

4.1 Constraint Satisfaction Problem

Let $\forall y_1 \ldots \forall y_{k_1} \exists x_1 \ldots \forall y_{k_{i-1}+1} \ldots \forall y_{k_i} \exists x_i \ldots \forall y_{k_{m-1}+1} \ldots \forall y_{k_m} \exists x_m$ $\forall y_{k_m+1} \ldots \forall y_n \ f(x_1, \ldots, x_m, y_1, \ldots, y_n)$ be an instance in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{F})$, where m and n are positive integers, and k_i, for $1 \leq i \leq m$, are nonnegative integers such that $k_i \leq k_{i+1}$, for $1 \leq i \leq m-1$, and $k_m \leq n$. A tuple $(a_1, \ldots, a_r, b_1, \ldots, b_{k_r}) \in \mathbb{F}^{r+k_r}$, $1 \leq r \leq m$, is *functionally feasible by quantifier free arithmetic expressions* to the given constraint satisfaction problem, if there exist quantifier free arithmetic expressions $g_1(y_1, \ldots, y_{k_1})$ and $g_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, $2 \leq i \leq m$, in $\mathcal{ARITH}\text{-}\mathcal{EXP}\big(\mathbb{F}\big)$, such that the following holds: $\forall y_1 \ldots \forall y_n \ f(x_1, \ldots, x_m, y_1, \ldots, y_n) = \texttt{true}$, where $x_1 = g_1(y_1, \ldots, y_{k_1})$, $x_i = g_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, $2 \leq i \leq m$, $g_1(b_1, \ldots, b_{k_1}) = a_1$ and $g_i(a_1, \ldots, a_{i-1}, b_1, \ldots, b_{k_i}) = a_i$, $2 \leq i \leq r$. It can be observed that for a finite field $\mathbb{F}$, a feasible tuple is also functionally feasible by quantifier free arithmetic expressions. A solution to the constraint satisfaction problem is to find quantifier free arithmetic expressions, if and when they exist, $g_1(y_1, \ldots, y_{k_1})$ for x_1 and $g_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$ for x_i, $2 \leq i \leq m$, such that for all $y_1 \ldots y_n \in \mathbb{F}$, $f(x_1, \ldots, x_m, y_1, \ldots, y_n) = 1$, where $x_1 = g_1(y_1, \ldots, y_{k_1})$ and $x_i = g_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, for $2 \leq i \leq m$. The constraint satisfaction problem is feasible, if it has a solution in quantifier free arithmetic expressions.

Theorem 1 *The constraint satisfaction problem for binary valued instances in prenex normal form with no free variables in* $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{F})$ *is* PSPACE*-hard.*

Proof. Let

$$\forall y_1 \ldots \forall y_{k_1} \exists x_1 \ldots \forall y_{k_{m-1}+1} \ldots \forall y_{k_m} \exists x_m \forall y_{k_m+1} \ldots \forall y_n \ f(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

where m and n are positive integers and k_i, $1 \leq i \leq m$, are integers such that $0 \leq k_i \leq k_{i+1} \leq n$, $1 \leq i \leq m-1$, be a given instance of binary valued quantified boolean expression with no free variables in $\mathcal{B}_{\mathcal{Q}}$ for the evaluation problem. Let

$$\begin{aligned}
&\exists w_1 \quad \forall y_1 \ldots \forall y_{k_1} \exists x_1 \ldots \forall y_{k_{m-1}+1} \ldots \forall y_{k_m} \exists x_m \ \ \forall y_{k_m+1} \ldots \forall y_n \\
&\quad \exists t_1 \ldots \exists t_{k_1} \forall v_1 \ldots \exists t_{k_{m-1}+1} \ldots \exists t_{k_m} \forall v_m \ \ \exists t_{k_m+1} \ldots \exists t_n \\
&[\ w_1 \wedge f(x_1, \ldots, x_m, y_1, \ldots, y_n)\ ] \vee \ [\ (\neg w_1) \wedge (\neg f(v_1, \ldots, v_m, t_1, \ldots, t_n))\ ]
\end{aligned}$$

be an instance to the constraint satisfaction problem with no free variables, which can be easily shown to be in $\mathcal{B}_{\mathcal{Q}-\mathrm{SAT}}$, since feasibility coincides with functional feasibility by arithmetic expressions for $\mathbb{Z}_2$. The input binary valued quantified boolean expression evaluates to 1 if and only if w_1 is 1 in any solution to the constructed instance of the constraint satisfaction problem. Now, as discussed at the beginning of the section, the field $\mathbb{Z}_2$, together with all its arithmetic and logical operations, can be emulated by the arithmetic operations and equality operator with any field $\mathbb{F}$. Thus, the constraint satisfaction problem for $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{F})$, which includes equivalent binary valued quantified arithmetic expressions for those in $\mathcal{B}_{\mathcal{Q}-\mathrm{SAT}}$, is PSPACE-hard. ■

4.2 Quantifier Elimination Problem

Let $\mathfrak{P}(\mathbb{F})$ be a set of parametric subsets of $\mathbb{F}$, parametrized by variables assuming values in $\mathbb{F}$, such that the binary valued characteristic functions of the sets are assertions in $\mathcal{ARITH}\text{-}\mathcal{EXP}(\mathbb{F})$. For an instance in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$, the quantifier elimination problem for a given instance is to compute, for $x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i} \in \mathbb{F}$, sets $G_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$ in $\mathfrak{P}(\mathbb{F})$, $1 \leq i \leq m$, such that $\{x_i \in \mathbb{F} : (x_1, \ldots, x_i, y_1, \ldots, y_{k_i})$ is feasible to the given instance$\}$ $= G_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, $1 \leq i \leq m$. If $\mathbb{F}$ is the field of real numbers, with the set of binary relations $\{=, <, \leq, >, \geq\}$ and the set of constants $\{0, 1\}$, then the emptiness testing of parametric subsets of $\mathbb{F}^n$, for an arbitrary positive integer n, where the characteristic functions of the parametric subsets are binary valued quantified arithmetic expressions, is decidable (or computable), and quantifier elimination is possible, *i.e.*, equivalent quantifier free arithmetic assertions can be computed for the quantified arithmetic assertions as characteristic functions for the parametric subsets of $\mathbb{F}^n$ [12, 14, 35, 47]. Thus, $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$ admits quantifier elimination, and the sets of feasibility tuples for instances in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$ have characteristic functions in $\mathcal{ARITH}\text{-}\mathcal{EXP}(\mathbb{F})$, that can be computed by an algorithm. Set solutions can be enumerated by backtracking method [26]. By the same proof of Theorem 1, the quantifier elimination problem can be shown to be PSPACE-hard.

Theorem 2 *The constraint satisfaction problem for binary valued instances in prenex normal form with no free variables in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{F})$, that have unique solutions, is* PSPACE-*hard.*

Proof. Let

$$\forall y_1 \ldots \forall y_{k_1} \exists x_1 \ldots \forall y_{k_{m-1}+1} \ldots \forall y_{k_m} \exists x_m \forall y_{k_m+1} \ldots \forall y_n \; f(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

be an instance in $\mathcal{B}_{\mathcal{Q}}$ for the quantifier elimination problem in prenex normal form with no free variables. Let $X_i(x_1, \ldots, x_i, y_1, \ldots, y_{k_i})$ be the characteristic function of the set $G_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, for $x_1, \ldots, x_i, y_1, \ldots, y_{k_i} \in$

$\mathbb{Z}_2$, $1 \le i \le m$. Let $X_{i,\,b}(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i}) = X_i(x_1, \ldots, x_{i-1}, b, y_1, \ldots, y_{k_i})$, for $x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i} \in \mathbb{Z}_2$, $b \in \mathbb{Z}_2$, $1 \le i \le m$. In the remaining part of the proof, the sets $G_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$ are represented by the pair of boolean functions $X_{i,\,b}(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, for $x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i} \in \mathbb{Z}_2$, $b \in \mathbb{Z}_2$, $1 \le i \le m$. Let the following instance to the constraint satisfaction problem be considered:

$$\begin{aligned}
&\forall y_1 \ldots \forall y_{k_1} \;\; \exists v_{1,\,0} \;\; \exists v_{1,\,1} \;\; \forall x_1 \ldots \forall y_{k_{i-1}+1} \ldots \forall y_{k_i} \;\; \exists v_{i,\,0} \;\; \exists v_{i,\,1} \;\; \forall x_i \, \forall y_{k_i+1} \ldots \forall y_{k_{i+1}} \\
&\quad \ldots \forall y_{k_{m-1}+1} \ldots \forall y_{k_m} \;\; \exists v_{m,\,0} \;\; \exists v_{m,\,1} \;\; \forall x_m \, \forall y_{k_m+1} \ldots \forall y_n \\
&\bigwedge_{i=1}^{m-1} \{ \;\; [\; (x_i = 0) \;\rightarrow\; [\; v_{i,\,0} \;\leftrightarrow\; (v_{i+1,\,0} \vee v_{i+1,\,1}) \;]\;] \;\; \wedge \\
&\qquad [\; (x_i = 1) \;\rightarrow\; [\; v_{i,\,1} \;\leftrightarrow\; (v_{i+1,\,0} \vee v_{i+1,\,1}) \;]\;] \;\; \} \;\; \bigwedge \\
&\{ \;\; [\; (x_m = 0) \;\rightarrow\; [\; v_{m,\,0} \;\leftrightarrow\; f(x_1, \ldots, x_m, y_1, \ldots, y_n) \;]\;] \;\; \wedge \\
&\qquad [\; (x_m = 1) \;\rightarrow\; [\; v_{m,\,1} \;\leftrightarrow\; f(x_1, \ldots, x_m, y_1, \ldots, y_n) \;]\;] \;\; \}
\end{aligned} \tag{1}$$

The boolean functions $X_{m,\,b}(x_1, \ldots, x_{m-1}, y_1, \ldots, y_{k_m})$, that encode the indicator function of the set $G_m(x_1, \ldots, x_{m-1}, y_1, \ldots, y_{k_m})$, are the solutions to the boolean variables $v_{m,\,b}$, $b \in \mathbb{Z}_2$, respectively, for $x_1, \ldots, x_{m-1}, y_1, \ldots, y_{k_m} \in \mathbb{Z}_2$, for the following instance of constraint satisfaction problem:

$$\begin{aligned}
&\forall y_1 \ldots \forall y_{k_1} \, \forall x_1 \ldots \forall y_{k_{m-1}+1} \ldots \forall y_{k_m} \;\; \exists v_{m,\,0} \;\; \exists v_{m,\,1} \;\; \forall x_m \, \forall y_{k_m+1} \ldots \forall y_n \\
&\{ \;\; [\; (x_m = 0) \;\rightarrow\; [\; v_{m,\,0} \;\leftrightarrow\; f(x_1, \ldots, x_m, y_1, \ldots, y_n) \;]\;] \;\; \wedge \\
&\qquad [\; (x_m = 1) \;\rightarrow\; [\; v_{m,\,1} \;\leftrightarrow\; f(x_1, \ldots, x_m, y_1, \ldots, y_n) \;]\;] \;\; \}
\end{aligned}$$

After obtaining the boolean functions $X_{i+1,\,b}(x_1, \ldots, x_i, y_1, \ldots, y_{k_{i+1}})$, $b \in \mathbb{Z}_2$, of $G_{i+1}(x_1, \ldots, x_i, y_1, \ldots, y_{k_{i+1}})$, the boolean functions $X_{i,\,b}(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, $b \in \mathbb{Z}_2$, of $G_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, for $x_1, \ldots, x_i, y_1, \ldots, y_{k_{i+1}} \in \mathbb{F}$, are the solutions to the boolean variables $v_{i,\,b}$, $1 \le i \le m-1$, $b \in \mathbb{Z}_2$, respectively, for the following instance of constraint satisfaction problem:

$$\begin{aligned}
&\forall y_1 \ldots \forall y_{k_1} \, \forall x_1 \ldots \forall y_{k_{i-1}+1} \ldots \forall y_{k_i} \;\; \exists v_{i,\,0} \;\; \exists v_{i,\,1} \;\; \forall x_i \, \forall y_{k_i+1} \ldots \forall y_{k_{i+1}} \\
&\{ \;\; [\; (x_i = 0) \;\rightarrow\; [\; v_{i,\,0} \;\leftrightarrow \\
&\quad (X_{i+1,\,0}(x_1, \ldots, x_i,\, y_1, \ldots, y_{k_{i+1}}) \;\vee\; X_{i+1,\,1}(x_1, \ldots, x_i,\, y_1, \ldots, y_{k_{i+1}})) \;]\;] \;\; \wedge \\
&\quad [\; (x_i = 1) \;\rightarrow\; [\; v_{i,\,1} \;\leftrightarrow \\
&\qquad (X_{i+1,\,0}(x_1, \ldots, x_i,\, y_1, \ldots, y_{k_{i+1}}) \;\vee\; X_{i+1,\,1}(x_1, \ldots, x_i,\, y_1, \ldots, y_{k_{i+1}})) \;]\;] \;\; \}
\end{aligned}$$

In summary, the boolean functions $X_{i,\,b}(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, that encode the indicator function of the set $G_i(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$, are the solutions to the boolean variables $v_{i,\,b}$, $b \in \mathbb{Z}_2$, respectively, for $x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i} \in \mathbb{Z}_2$ and $1 \le i \le m$, in the proposed instance of constraint satisfaction problem. The actual solutions for $v_{i,\,b}$ can also depend on $v_{j,\,c}$, for $b, c \in \mathbb{Z}_2$, $1 \le j \le i-1$ and $2 \le i \le m$, in the proposed instance of the constraint satisfaction problem. Nonetheless, the boolean formulas $X_{i,\,b}(x_1, \ldots, x_{i-1}, y_1, \ldots, y_{k_i})$

are assumed to be the main solutions for $v_{i,,b}$, for $b \in \mathbb{Z}_2$ and $1 \leq i \leq m$, as these are the solutions of the instance for the quantifier elimination problem, which is reduced to the instance of the constraint satisfaction problem. ■

In the proof of Theorem 2, for avoiding the possibility of dependence of a solution for $v_{i,1}$ on $v_{i,0}$, the formulas in the above are encoded treating the variables in pairs, representing $v_{i,b}$, $b \in \mathbb{Z}_2$, by a single variable $v_i = (v_{i,0}, v_{i,1})$, performing the required computations in $\mathbb{Z}_2^2$, for $1 \leq i \leq m$. Thus, the encoding contains only a single dependent variable v_i, $1 \leq i \leq m$, and either component of it depends only on the variables constrained by quantifiers occurring before the lone existential quantifier. The components v_{i,x_i} are replaced by a projection $T(x_i, v_i)$, which can further be chosen to be linear in v_i for each fixed x_i, for $1 \leq i \leq m$, to avoid duplication. There is a unique solution separately for each component $T(x_i, v_i)$ of the dependent variable v_i, for $1 \leq i \leq m$. Now, as discussed in the beginning of the section, the field $\mathbb{Z}_2$, together with all its arithmetic and logical operations, can be emulated by the arithmetic operations and equality operator with any field $\mathbb{F}$. The characteristic functions of set solutions to the quantifier elimination problem for binary valued instances in prenex normal form with no free variables in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{F})$, which includes $\mathcal{B}_{\mathcal{Q}}$, are unique. Thus, the constraint satisfaction problem for instances in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{F})$, that admit unique solutions, is PSPACE-hard, since the stated set of instances also contains those instances encoding the characteristic functions for quantifier elimination problem for instances in $\mathcal{B}_{\mathcal{Q}}$.

4.3 Simultaneous Multivariate Polynomial Equations over $\mathbb{F}$

Let $l, m, m \in \mathbb{N}$ and$f_i\big(x_1, \ldots, x_m, y_1, \ldots, y_n\big) \in \mathcal{ARITH}\text{-}\mathcal{EXP}(\mathbb{F})$, for $1 \leq i \leq l$, be arithmetic expressions. A system of (multivariate) polynomial equations is the following:

$$f_i\big(x_1, \ldots, x_m, y_1, \ldots, y_n\big) \quad = \quad 0\,, \qquad 1 \leq i \leq l\,, \tag{2}$$

where y_j, $1 \leq j \leq n$, are independent variables and x_i, $1 \leq i \leq m$, are dependent variables, assuming values from $\mathbb{F}$, both specified as part of an instance. A tuple $\big(a_1, \ldots, a_i, b_1, \ldots, b_n\big)$ is feasible to (2), if either (1) $i = m$ and (2) holds with $x_r = a_r$, for $1 \leq r \leq m$, and $y_j = b_j$, for $1 \leq j \leq n$, or (2) $1 \leq i \leq m-1$, and $\big(a_1, \ldots, a_i, a_{i+1}, b_1, \ldots, b_n\big)$ is feasible for some a_{i+1} depending on $\big(a_1, \ldots, a_i, \ldots, b_1, \ldots, b_n\big)$. Let $\mathfrak{P}\big(\mathbb{F}\big)$ be the collection of admissible subsets of $\mathbb{F}$, whose indicator functions are in $\mathcal{ARITH}\text{-}\mathcal{EXP}\big(\mathbb{F}\big)$. A complete solution to (2) are parametric maximal sets $G_i\big(a_1, \ldots, a_{i-1}, y_1, \ldots, y_n\big) \in \mathfrak{P}(\mathbb{F})$, such that $G_i\big(a_1, \ldots, a_{i-1}, y_1, \ldots, y_n\big) = \big\{\, a_i \in \mathbb{F} : \big(a_1, \ldots, a_{i-1}, a_i, y_1, \ldots, y_n\big) \text{ is feasible } \big\}$, for $1 \leq i \leq m$.

In the above system, the ordering of the variables $x_1, \ldots, x_m$ appears specified. However, this ordering can be made innocuous by additional constraints as follows:

$$
\begin{array}{rclcrcl}
w_{i,j}^2 & = & w_{i,j}\,, & & 1 \le i,\, j \le m & & \\
\displaystyle\sum_{j=1}^{m} w_{i,j} & = & 1 & \text{and} & \displaystyle\sum_{j=1}^{m} \prod_{\substack{k=1 \\ k \neq j}}^{m} (1 - w_{i,k}) & = & 1, \quad 1 \le i \le m \\
\displaystyle\sum_{i=1}^{m} w_{i,j} & = & 1 & \text{and} & \displaystyle\sum_{i=1}^{m} \prod_{\substack{k=1 \\ k \neq i}}^{m} (1 - w_{k,j}) & = & 1, \quad 1 \le j \le m
\end{array}
$$

$$
\begin{bmatrix} w_{1,1} & w_{1,2} & \dots & w_{1,m} \\ w_{2,1} & w_{2,2} & \dots & w_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ w_{m,1} & w_{m,2} & \dots & w_{m,m} \end{bmatrix}
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}
-
\begin{bmatrix} x_{m+1} \\ x_{m+2} \\ \vdots \\ x_{2m} \end{bmatrix}
=
\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \text{and}
$$

$$
f_i\left(x_{m+1}, \dots, x_{2m}, y_1, \dots, y_n\right) = 0, \qquad 1 \le i \le l
$$

where y_j, $1 \le j \le n$, are independent variables, and all the remaining variables are dependent variables. The ordering is concealed by allowing the system to choose an appropriate ordering of the variables $x_{m+1}, \dots, x_{2m}$, while allowing $x_1, \dots, x_m$ to appear in the specified order. In the above set of constraints, for each row of the matrix $\left[w_{i,j}\right]_{1 \le i,\, j \le m}$, for the constraints on i, $1 \le i \le m$, and for each column of the matrix $\left[w_{i,j}\right]_{1 \le i,\, j \le m}$, for the constraints on j, $1 \le j \le m$, the first constraint requires at least one entry of 1, and the second constraint requires $(m-1)$ entries of 0, in the respective row or column, and the matrix $\left[w_{i,j}\right]_{1 \le i,\, j \le m}$ is a permutation matrix.

Theorem 3 *The quantifier elimination problem for instances in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}}(\mathbb{Z}_2)$ is polynomial time subroutine equivalent to the problem of solving systems of multivariate polynomial equations, for the field $\mathbb{Z}_2$.*

Proof. Let

$$
\forall y_1 \dots \forall y_{k_1}\, \exists x_1 \dots \forall y_{k_{m-1}+1} \dots \forall y_{k_m}\, \exists x_m\, \forall y_{k_m+1} \dots \forall y_n\;\; f(x_1, \dots, x_m, y_1, \dots, y_n)
$$

be an instance in $\mathcal{B}_{\mathcal{Q}}$ in prenex normal form with no free variables, for some positive integers m and n, and nonnegative integers k_i, such that $k_{i-1} \le k_i \le n$, for $1 \le i \le n$, where $k_0 = 0$. Let $\chi_{m-i+1,\,a}(x_1, \dots, x_{m-i}, y_1, \dots, y_{k_{m-i+1}}) \in \mathcal{ARITH}\text{-}\mathcal{EXP}(\mathbb{Z}_2)$ be the solution for $v_{m-i+1,\,a}$, for $a \in \mathbb{Z}_2$ and $1 \le i \le m$, such that the following holds:

$$\left.\begin{array}{r} v_{m,\,a} \;\leftrightarrow\; \forall y_{k_m+1} \ldots \forall y_n \;\; f(x_1, \ldots, x_{m-1}, a, y_1, \ldots, y_n), \;\text{ and} \\ v_{m-i+1,\,a} \;\leftrightarrow\; \forall y_{k_{m-i+1}+1} \ldots \forall y_{k_{m-i+2}} \;\; [\\ \chi_{m-i+2,\,0}(x_1, \ldots, x_{m-i}, a, y_1, \ldots, y_{k_{m-i+2}}) \;\vee \\ \chi_{m-i+2,\,1}(x_1, \ldots, x_{m-i}, a, y_1, \ldots, y_{k_{m-i+2}}) \;\;] \\ \text{for } \; a \in \mathbb{Z}_2 \;\text{ and }\; 2 \le i \le m \end{array}\right\} \qquad (3)$$

The above equations can also be expressed as follows:

$$\begin{array}{l} \neg v_{m,\,a} \;\leftrightarrow\; \exists u_{k_m+1} \ldots \exists u_n \;\; \neg f(x_1, \ldots, x_{m-1}, a, y_1, \ldots, y_{k_m}, u_{k_m+1}, \ldots, u_n), \;\text{ and} \\ \neg v_{m-i+1,\,a} \;\leftrightarrow\; \exists u_{k_{m-i+1}+1} \ldots \exists u_{k_{m-i+2}} \;\; [\\ \quad \neg\chi_{m-i+2,\,0}(x_1, \ldots, x_{m-i}, a, y_1, \ldots, y_{k_{m-i+1}}, u_{k_{m-i+1}+1}, \ldots, u_{k_{m-i+2}}) \;\wedge \\ \quad\quad \neg\chi_{m-i+2,\,1}(x_1, \ldots, x_{m-i}, a, y_1, \ldots, y_{k_{m-i+1}}, u_{k_{m-i+1}+1}, \ldots, u_{k_{m-i+2}}) \;\;] \\ \qquad\qquad \text{for } \; a \in \mathbb{Z}_2 \;\text{ and }\; 2 \le i \le m \end{array}$$

Let $G_{m,\,a,\,j,\,b}(x_1, \ldots, x_{m-1}, y_1, \ldots, y_{k_m}, u_{k_m+1}, \ldots, u_{j-1})$, for the ground case $x_m = a$ and $u_j = b$, for $a, b \in \mathbb{Z}_2$ and $k_m + 1 \le j \le n$, be indicator functions of complete solutions in the following system of simultaneous multivariate equations:

$$f(x_1, \ldots, x_{m-1}, a, y_1, \ldots, y_{k_m}, u_{k_m+1}, \ldots, u_n) \;=\; 0$$

Then, the indicator function, $\chi_{m,\,a}(x_1, \ldots, x_{m-1}, y_1, \ldots, y_{k_m})$, which is the solution for $v_{m,\,a}$, for $a \in \mathbb{Z}_2$, is given by

$$\neg[G_{m,\,a,\,k_m+1,\,0}(x_1, \ldots, x_{m-1}, y_1, \ldots, y_{k_m}) \;\vee\; G_{m,\,a,\,k_m+1,\,1}(x_1, \ldots, x_{m-1}, y_1, \ldots, y_{k_m})]$$

Now, for $1 \le i \le m-1$, after obtaining $\chi_{m-i+1,\,a}(x_1, \ldots, x_{m-i}, y_1, \ldots, y_{k_{m-i+1}})$, let $G_{m-i,\,a,\,j,\,b}(x_1, \ldots, x_{m-i-1}, y_1, \ldots, y_{k_{m-i}}, u_{k_{m-i}+1}, \ldots, u_{j-1})$, for the ground case $x_{m-i} = a$ and $u_j = b$, for $a, b \in \mathbb{Z}_2$ and $k_{m-i} + 1 \le j \le k_{m-i+1}$, be indicator functions of complete solutions in the following system of simultaneous multivariate equations:

$$\begin{array}{lcl} \chi_{m-i+1,\,0}(x_1, \ldots, x_{m-i}, y_1, \ldots, y_{k_{m-i}}, u_{k_{m-i}+1}, \ldots, u_{k_{m-i+1}}) & = & 0, \quad \text{and} \\ \chi_{m-i+1,\,1}(x_1, \ldots, x_{m-i}, y_1, \ldots, y_{k_{m-i}}, u_{k_{m-i}+1}, \ldots, u_{k_{m-i+1}}) & = & 0 \\ \text{where } \; x_{m-i} \; \text{ is set to the ground value } \; a\,. & & \end{array}$$

Then, the indicator function, $\chi_{m-i,\,a}(x_1, \ldots, x_{m-i-1}, y_1, \ldots, y_{k_{m-i}})$, which is the solution for $v_{m-i,\,a}$, for the ground instance $x_{m-i} = a$ and $a \in \mathbb{Z}_2$, is given by

$$\begin{array}{l} [\neg G_{m-i,\,a,\,k_{m-i}+1,\,0}(x_1, \ldots, x_{m-i-1}, y_1, \ldots, y_{k_{m-i}})] \;\;\wedge \\ \quad [\neg G_{m-i,\,a,\,k_{m-i}+1,\,1}(x_1, \ldots, x_{m-i-1}, y_1, \ldots, y_{k_{m-i}})] \end{array}$$

for $1 \le i \le m-1$. Thus, finding complete solutions for systems of simultaneous multivariate equations over $\mathbb{Z}_2$ is PSPACE-hard, as it is logically equivalent to the quantifier elimination problem. ■

For a positive integer k and bit sequences $(u_1, \ldots, u_k),\ (t_1, \ldots, t_k) \in \mathbb{Z}_2^k$ let "$\succeq$" be the "successor or equal to" relation with respect to the dictionary ordering of finite binary sequences, such that the comparison of corresponding bits is performed starting from least subscript index and up towards higher subscript indexes, as follows:

$$(u_1, \ldots, u_k) \succeq (t_1, \ldots, t_k) \quad \text{exactly when the following holds :}$$
$$(\ (u_1 = 1) \wedge (t_1 = 0)\ ) \ \vee \ \bigvee_{i=2}^{k} (\ \bigwedge_{j=1}^{i-1} (u_j = t_j) \wedge (u_i = 1) \wedge (t_i = 0)\ ) \ \vee \ \bigwedge_{j=1}^{k} (u_j = t_j)$$

Now, the prenex normal form equivalent formula for (3) is the following:

$$\begin{aligned}
&\forall y_1 \ldots \forall y_{k_m} \quad \exists v_{m,a} \exists u_{k_m+1,a} \ldots \exists u_{n,a} \quad \forall z_{k_m+1} \ldots \forall z_n \qquad \underbrace{[}_{0} \\
&\underbrace{(}_{1} [\ v_{m,a} \wedge \bigwedge_{j=k_m+1}^{n} (u_{j,a} = 0)\ ] \quad \wedge \\
&\qquad [\ G_m(x_1, \ldots, x_{m-1}, a, y_1, \ldots, y_{k_m}, z_{k_m+1}, \ldots, z_n)\ ]\ \underbrace{)}_{1} \\
&\bigvee \underbrace{(}_{2} \quad [\ \neg v_{m,a}\ ] \ \wedge \ [\ \neg G_m(x_1, \ldots, x_{m-1}, a, y_1, \ldots, y_{k_m}, u_{k_m+1,a}, \ldots, u_{n,a})\ ] \quad \wedge \\
&\qquad\qquad [\quad (n = k_m) \ \vee \ [\ (z_{k_m+1}, \ldots, z_n) \ \succeq \ (u_{k_m+1,a}, \ldots, u_{n,a})\ ] \ \vee \\
&\qquad [\ G_m(x_1, \ldots, x_{m-1}, a, y_1, \ldots, y_{k_m}, z_{k_m+1}, \ldots, z_n)\ ] \quad] \ \underbrace{)}_{2} \quad \underbrace{]}_{0}
\end{aligned} \tag{4}$$

where

$$\begin{aligned}
G_m(x_1, \ldots, x_{m-1}, x_m, y_1, \ldots, y_{k_m}, y_{k_m+1}, \ldots, y_n) \quad = \\
f(x_1, \ldots, x_{m-1}, x_m, y_1, \ldots, y_{k_m}, y_{k_m+1}, \ldots, y_n)
\end{aligned}$$

The solutions for the dependent variables bound by the existential quantifiers are unique. Let $\chi_{m-i+2,a}(x_1, \ldots, x_{m-i+1}, y_1, \ldots, y_{k_{m-i+1}}, y_{k_{m-i+1}+1}, \ldots, y_{k_{m-i+2}})$ be the solution for the variable $v_{m-i+2,a}$, for $2 \le i \le m$ and $a \in \mathbb{Z}_2$, and let

$$\begin{aligned}
&G_{m-i+1}(x_1, \ldots, x_{m-i}, x_{m-i+1}, y_1, \ldots, y_{k_{m-i+1}}, y_{k_{m-i+1}+1}, \ldots, y_{k_{m-i+2}}) \quad = \\
&\qquad (\quad \chi_{m-i+2,0}(x_1, \ldots, x_{m-i+1}, y_1, \ldots, y_{k_{m-i+1}}, y_{k_{m-i+1}+1}, \ldots, y_{k_{m-i+2}}) \ \vee \\
&\qquad\qquad \chi_{m-i+2,1}(x_1, \ldots, x_{m-i+1}, y_1, \ldots, y_{k_{m-i+1}}, y_{k_{m-i+1}+1}, \ldots, y_{k_{m-i+2}}) \quad)
\end{aligned}$$

and

$$
\begin{aligned}
&\forall y_1 \ldots \forall y_{k_{m-i+1}} \quad \exists v_{m-i+1,\,a} \exists u_{k_{m-i+1}+1,\,a} \ldots \exists u_{k_{m-i+2},\,a} \quad \forall z_{k_{m-i+1}+1} \ldots \forall z_{k_{m-i+2}} \\
&\underbrace{[}_{0} \quad \underbrace{(}_{1} \quad [\, v_{m-i+1,\,a} \wedge \bigwedge_{j=k_{m-i+1}+1}^{k_{m-i+2}} (u_{j,\,a} = 0) \,] \quad \wedge \\
&\qquad [\, G_{m-i+1}(x_1, \ldots, x_{m-i}, a, y_1, \ldots, y_{k_{m-i+1}}, z_{k_{m-i+1}+1}, \ldots, z_{k_{m-i+2}}) \,] \quad \underbrace{)}_{1} \\
&\bigvee \quad \underbrace{(}_{2} \quad [\, \neg v_{m-i+1,\,a} \,] \wedge \\
&\qquad [\, \neg G_{m-i+1}(x_1, \ldots, x_{m-i}, a, y_1, \ldots, y_{k_{m-i+1}}, u_{k_{m-i+1}+1,\,a}, \ldots, u_{k_{m-i+2},\,a}) \,] \wedge \\
&[\quad (k_{m-i+2} = k_{m-i+1}) \quad \vee \quad [\, (z_{k_{m-i+1}+1}, \ldots, z_{k_{m-i+2}}) \succeq (u_{k_{m-i+1}+1,\,a}, \ldots, u_{k_{m-i+2},\,a}) \,] \\
&\quad \vee \; [\, G_{m-i+1}(x_1, \ldots, x_{m-i}, a, y_1, \ldots, y_{k_{m-i+1}}, z_{k_{m-i+1}+1}, \ldots, z_{k_{m-i+2}}) \,] \quad] \\
&\qquad\qquad \underbrace{)}_{2} \quad \underbrace{]}_{0}
\end{aligned} \tag{5}
$$

for $2 \leq i \leq m$ and $a \in \mathbb{Z}_2$. Again, the solutions for the dependent variables bound by the existential quantifiers are unique. This discussion is summarized in the following:

Corollary 3.1 *The constraint satisfaction problem for instances of the form*

$$\forall y_1 \ldots \forall y_k \quad \exists x_1 \ldots \exists x_m \quad \forall y_{k+1} \ldots \forall y_n \quad f(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

that are in $\mathcal{ARITH}\text{-}\mathcal{EXP}_{\mathcal{Q}-\mathrm{SAT}}(\mathbb{Z}_2)$*, where* k*,* m *and* n *are positive integers, such that* $1 \leq k \leq n$ *and* x_i*, for* $1 \leq i \leq m$*, admit unique solutions, is* PSPACE*-hard.*

Proof. Follows from the discussion preceding the statement. ■

4.4 Parametric Multivariate Polynomial Mappings and their Nonparametric Inverses

In this subsection, let $\mathbb{F}$ be a finite field. For integers $l \geq 0$, $m \geq 1$ and $n \geq 1$, a parametric multivariate polynomial mapping, with $z_1, \ldots, z_l$ as parameters, is $\eta(\mathbf{z}; \mathbf{x}) = \big(\eta_1(\mathbf{z}; \mathbf{x}), \ldots, \eta_n(\mathbf{z}; \mathbf{x})\big)$, where $\mathbf{z} = (z_1, \ldots, z_l)$, $\mathbf{x} = (x_1, \ldots, x_m)$, and $\eta_i(\mathbf{z}; \mathbf{x}) \in \mathbb{F}[z_1, \ldots, z_l, x_1, \ldots, x_m]$, for $1 \leq i \leq n$. A parametric left inverse $\eta^{(\text{-L})}(\mathbf{z}; \mathbf{y})$, $\mathbf{y} = (y_1, \ldots, y_n)$, of a parametric multivariate polynomial mapping $\eta(\mathbf{z}; \mathbf{x})$ on $X \subseteq \mathbb{F}^l \times \mathbb{F}^m$ is as follows: for every $\mathbf{z} \in \mathbb{F}^l$, $\mathbf{x} \in \mathbb{F}^m$ and $\mathbf{y} \in \mathbb{F}^n$, such that $(z_1, \ldots, z_l, x_1, \ldots, x_m) \in X$, if $\eta(\mathbf{z}; \mathbf{x}) = \mathbf{y}$, then $\eta^{(\text{-L})}(\mathbf{z}; \mathbf{y}) = \mathbf{x}$. A parametric right inverse $\eta^{(\text{-R})}(\mathbf{z}; \mathbf{y})$ on $Y \subseteq \mathbb{F}^l \times \mathbb{F}^n$ of a parametric multivariate polynomial mapping $\eta(\mathbf{z}; \mathbf{x})$ is as follows: for every $\mathbf{z} \in \mathbb{F}^l$, $\mathbf{x} \in \mathbb{F}^m$ and $\mathbf{y} \in \mathbb{F}^n$, such that $(z_1, \ldots, z_l, y_1, \ldots, y_n) \in Y$, if $\eta^{(\text{-R})}(\mathbf{z}; \mathbf{y}) = \mathbf{x}$, then $\eta(\mathbf{z}; \mathbf{x}) = \mathbf{y}$.

For $\mathbf{z} \in \mathbb{F}^l$, let $S_\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{x})$, $\mathbf{x} \in \mathbb{F}^m$, and $S_\eta^{(\text{-R})}(\mathbf{z};\, \mathbf{y})$, $\mathbf{y} \in \mathbb{F}^n$, be as follows: $S_\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{x}) = \big\{(z_1, \ldots, z_l, y_1, \ldots, y_n) \in \mathbb{F}^l \times \mathbb{F}^n \,:\, \eta(\mathbf{z};\, \mathbf{x}) = \mathbf{y}\big\}$, and $S_\eta^{(\text{-R})}(\mathbf{z};\, \mathbf{y}) = \big\{(z_1, \ldots, z_l, x_1, \ldots, x_m) \in \mathbb{F}^l \times \mathbb{F}^m \,:\, \eta(\mathbf{z};\, \mathbf{x}) = \mathbf{y}\big\}$. Now, the following statements hold: (1) for $\mathbf{z} \in \mathbb{F}^l$ and $\mathbf{x} \in \mathbb{F}^m$, the set $S_\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{x})$ contains exactly one element; (2) for $\mathbf{z} \in \mathbb{F}^l$ and $\mathbf{y} \in \mathbb{F}^n$, the set $S_\eta^{(\text{-R})}(\mathbf{z};\, \mathbf{y})$ may be empty or nonempty; (3) a parametric left inverse $\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{y})$ can be defined on the set $\bigcup_{(z_1, \ldots, z_l, x_1, \ldots, x_m) \in X} S_\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{x})$ if and only if $S_\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{x}) \cap S_\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{x}') = \emptyset$, for $(z_1, \ldots, z_l, x_1, \ldots, x_m) \in X$ and $(z_1, \ldots, z_l, x_1', \ldots, x_m') \in X$, whenever $\mathbf{x} \neq \mathbf{x}'$; and (4) a parametric right inverse $\eta^{(\text{-R})}(\mathbf{z};\, \mathbf{y})$ can be defined on the set Y if and only if $S_\eta^{(\text{-R})}(\mathbf{z};\, \mathbf{y}) \neq \emptyset$, for every $(z_1, \ldots, z_l, y_1, \ldots, y_n) \in Y$. If a parametric left inverse (similarly, a parametric right inverse) of a parametric multivariate polynomial mapping does not depend on the parameters, then it is nonparametric. Let

$$
\begin{aligned}
T_\eta^{(\text{-L})}(\mathbf{x}) \quad &= \bigcup_{(z_1, \ldots, z_l,\, x_1, \ldots, x_m) \in X} \big\{\mathbf{y} \in \mathbb{F}^n \,:\, \eta(\mathbf{z};\, \mathbf{x}) = \mathbf{y}\big\} \\
&\qquad \text{for fixed } \ \mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}^m\,, \quad \text{and} \\
T_\eta^{(\text{-R})}(\mathbf{y}) \quad &= \bigcap_{(z_1, \ldots, z_l,\, y_1, \ldots, y_n) \in Y} \big\{\mathbf{x} \in \mathbb{F}^m \,:\, \eta(\mathbf{z};\, \mathbf{x}) = \mathbf{y}\big\} \\
&\qquad \text{for fixed } \ \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}^n
\end{aligned}
$$

Then, on the set $\bigcup_{(z_1, \ldots, z_l,\, x_1, \ldots, x_m) \in X} S_\eta^{(\text{-L})}(\mathbf{z};\, \mathbf{x})$, a nonparametric left inverse $\eta^{(\text{-L})}(\mathbf{y})$ can be defined if and only if $T_\eta^{(\text{-L})}(\mathbf{x}) \cap T_\eta^{(\text{-L})}(\mathbf{x}') = \emptyset$, for $\mathbf{x}, \mathbf{x}' \in \mathbb{F}^m$, $\mathbf{x} \neq \mathbf{x}'$, and on the set Y, a nonparametric right inverse $\eta^{(\text{-R})}(\mathbf{y})$ can be defined if and only if $T_\eta^{(\text{-R})}(\mathbf{y}) \neq \emptyset$, for $(z_1, \ldots, z_l, y_1, \ldots, y_n) \in Y$ and $\mathbf{y} \in \mathbb{F}^n$. A parametric inverse is simultaneously a parametric left inverse and a parametric right inverse. If a parametric inverse does not depend on the parameters, then it is nonparametric.

Theorem 4 *The computational problems of* (1) *finding nonparametric left inverses as quantifier free arithmetic expressions of parametric multivariate polynomial mappings, and* (2) *nonparametric right inverses as quantifier free arithmetic expressions of parametric multivariate polynomial mappings, with specified conditions on the domains of validity, for the instances for which the stated inverses exist, are both* PSPACE*-hard.*

Proof. Let $\forall t_1 \ldots \forall t_k \;\; \exists w_1 \ldots \exists w_m \;\; \forall t_{k+1} \ldots \forall t_n \;\; f(w_1, \ldots, w_m, t_1, \ldots, t_n) \in \mathcal{B}_{\mathrm{Q-SAT}}$, for some positive integers k, m and n, such that $k \leq n$, be an instance for the constraint satisfaction problem, admitting unique solutions for each of the dependent variables w_i separately as quantifier free boolean expressions $g_i(t_1, \ldots, t_k) \in \mathcal{ARITH\text{-}EXP}(\mathbb{Z}_2)$, for $1 \leq i \leq m$.

Part (1) The proof is given by subroutine reduction taking one variable at a time, starting from m down to 1. For $w_i,\, t_j \in \mathbb{Z}_2$, $1 \leq i \leq m$ and

$1 \leq j \leq n$, let

$$\begin{aligned}
\phi_m(w_1, \ldots, w_m, t_1, \ldots, t_n) &= f(w_1, \ldots w_m, t_1, \ldots, t_n), \quad \text{and} \\
h_m(w_1, \ldots, w_{m-1}, t_1, \ldots, t_n) &= f(w_1, \ldots w_{m-1}, 0, t_1, \ldots, t_n) \oplus \\
&\qquad f(w_1, \ldots w_{m-1}, 1, t_1, \ldots, t_n)
\end{aligned}$$

Let $\zeta_{(m)}(\mathbf{z}; \mathbf{x})$, $\mathbf{z} = (z_1, \ldots, z_{n-k})$ and $\mathbf{x} = (x_1, \ldots, x_{m+k})$, be a parametric multivariate polynomial mapping from $\mathbb{Z}_2^{m+k}$ into $\mathbb{Z}_2^{m+k+1}$, with parameters $z_1, \ldots, z_l$, where $l = n - k$, as follows:

$$\zeta_{(m,\, j)}(\mathbf{z};\, \mathbf{x}) \;=\; \begin{cases} x_j\,, \quad \text{for } \; 1 \leq j \leq m-1\,, \\ x_{j+1}\,, \quad \text{for } \; m \leq j \leq m+k-1\,, \\ h_m(x_1, \ldots, x_{m-1}, x_{m+1}, \ldots, x_{m+k}, z_1, \ldots, z_l)\,, \quad \text{for } \; j = m+k\,, \\ (\, \zeta_{(m,\, m+k)}(\mathbf{z};\, \mathbf{x}) \;\wedge\; \phi_m(x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+k}, z_1, \ldots, z_l)\,) \\ \vee \;\; (\, (\, \neg\, \zeta_{(m,\, m+k)}(\mathbf{z};\, \mathbf{x})\,) \;\wedge\; x_{j-k-1}\,)\,, \quad \text{for } \; j = m+k+1\,, \end{cases}$$

The variables occurring in the above, in comparison with the given instance of constraint satisfaction problem, are as follows: $x_j = w_j$, for $1 \leq j \leq m$, $t_j = x_{m+j}$, for $1 \leq j \leq k$, and $t_j = z_{j-k}$, for $k+1 \leq j \leq n$. Let $\mathbf{x}, \mathbf{x}' \in \mathbb{Z}_2^{m+k}$ and $\mathbf{z} \in \mathbb{Z}_2^{n-k}$ be such that $\zeta_{(m)}(\mathbf{z}; \mathbf{x}) = \zeta_{(m)}(\mathbf{z}; \mathbf{x}')$. If $\mathbf{x} \neq \mathbf{x}'$, then it can only be the case that $x_m \neq x'_m$. Since $\zeta_{(m,\, m+k)}(\mathbf{z}; \mathbf{x}) = \zeta_{(m,\, m+k)}(\mathbf{z}; \mathbf{x}')$, it follows that $h_m(x_1, \ldots, x_{m-1}, x_{m+1}, \ldots, x_{m+k}, z_1, \ldots, z_l) = h_m(x'_1, \ldots, x'_{m-1}, x'_{m+1}, \ldots, x'_{m+k}, z_1, \ldots, z_l)$, and since $\zeta_{(m,\, m+k+1)}(\mathbf{z}; \mathbf{x}) = \zeta_{(m,\, m+k+1)}(\mathbf{z}; \mathbf{x}')$, it follows that $x_m = x'_m$. Now, a nonparametric left inverse of $\zeta_{(m)}$ is sought, which is valid on a maximal domain $X_m \subseteq \mathbb{Z}_2^{m+n}$, subject to the following conditions :

1. if $(x_1, \ldots, x_{m+k}, z_1, \ldots, z_l) \in X_m$, then $(x_1, \ldots, x_{m+k}, z'_1, \ldots, z'_l) \in X_m$, for every $(z'_1, \ldots, z'_l) \in \mathbb{Z}_2^l$;
2. for each fixed $(x_{m+1}, \ldots, x_{m+k}) \in \mathbb{Z}_2^k$, there exists $(x_1, \ldots, x_m) \in \mathbb{Z}_2^m$, such that $(x_1, \ldots, x_{m+k}, z_1, \ldots, z_l) \in X_m$, for every $(z_1, \ldots, z_l) \in \mathbb{Z}_2^l$, where $l = n - k$; and
3. a nonparametric left inverse of $\zeta_{(m)}$ can be defined on $\zeta_{(m)}(X_m)$.

The left inverse formula is as follows: let $\zeta_{(m)}(\mathbf{z};\; \mathbf{x}) = \mathbf{y}$, for some fixed $\mathbf{y} = (y_1, \ldots, y_{m+k+1}) \in \mathbb{Z}_2^{m+k+1}$; then $x_j = y_j$, for $1 \leq j \leq m-1$, $x_{j+1} = y_j$, for $m \leq j \leq m+k-1$, $x_m = (y_{m+k} \wedge \rho_m(\mathbf{y})) \vee ((\neg y_{m+k}) \wedge y_{m+k+1})$, for some function ρ_m from $\mathbb{Z}_2^{m+k+1}$ into $\mathbb{Z}_2$. The domain X_m of validity of the left inverse satisfies the following inclusion:

$$\begin{aligned}
X_m \quad \supseteq \quad \{\, (x_1, \ldots, x_{m+k}, z_1, \ldots, z_{n-k}) \in \mathbb{Z}_2^{m+n} \;: \\
x_j = g_j(x_{m+1}, \ldots, x_{m+k})\,, \quad \text{for } 1 \leq j \leq m \,\}
\end{aligned}$$

and the function ρ_m satisfies the following:

$$\begin{aligned}
\rho_m\big(g_1(y_m, \ldots, y_{m+k-1}), \ldots, g_{m-1}(y_m, \ldots, y_{m+k-1}), y_m, \ldots, y_{m+k-1}, 1, 0\big) &= \\
\neg g_m(y_m, \ldots, y_{m+k-1})\,, \quad \text{and} & \\
\rho_m\big(g_1(y_m, \ldots, y_{m+k-1}), \ldots, g_{m-1}(y_m, \ldots, y_{m+k-1}), y_m, \ldots, y_{m+k-1}, 1, 1\big) &= \\
g_m(y_m, \ldots, y_{m+k-1}) &
\end{aligned}$$

Specification of the conditions on the domain of validity is part of the left inverse function computational problem, as required by the proof.

Now, after obtaining left inverses of $\zeta_{(i+1)}, \ldots, \zeta_{(m)}$, together with the hidden functions $\rho_{i+1}, \ldots, \rho_m$, for some index i, where $1 \le i \le m-1$, the above procedure is repeated with the following

$$\begin{aligned} \phi_i(w_1, \ldots, w_i, t_1, \ldots, t_n) &= \phi_{i+1}\big(w_1, \ldots w_i\,,\ \rho_{i+1}(w_1, \ldots w_i, t_1, \ldots, t_k, 1, 1)\,, \\ &\qquad\qquad t_1, \ldots, t_k, t_{k+1}, \ldots, t_n\big)\,, \quad \text{and} \\ h_i(w_1, \ldots, w_{i-1}, t_1, \ldots, t_n) &= \phi_i(w_1, \ldots w_{i-1}, 0, t_1, \ldots, t_n) \ \oplus \\ &\qquad\qquad \phi_i(w_1, \ldots w_{i-1}, 1, t_1, \ldots, t_n) \end{aligned}$$

Thus, in the following instance of the constraint satisfaction problem :

$$\forall t_1 \ldots \forall t_k \ \ \exists w_1 \ldots \exists w_i \ \ \forall t_{k+1} \ldots \forall t_n \ \ \phi_i(w_1, \ldots, w_i, t_1, \ldots, t_n)$$

the function $g_j(y_1, \ldots, y_k)$ is the unique solution for the variable w_j, for $1 \le j \le i$. Let $\zeta_{(i)}(\mathbf{z}; \mathbf{x})$, $\mathbf{z} = (z_1, \ldots, z_{n-k})$ and $\mathbf{x} = (x_1, \ldots, x_{i+k})$, be a parametric multivariate polynomial mapping from $\mathbb{Z}_2^{i+k}$ into $\mathbb{Z}_2^{i+k+1}$, with parameters $z_1, \ldots, z_l$, where $l = n-k$, as follows:

$$\zeta_{(i,\,j)}(\mathbf{z};\ \mathbf{x}) \ = \begin{cases} x_j\,, \quad \text{for } \ 1 \le j \le i-1\,, \\ x_{j+1}\,, \quad \text{for } \ i \le j \le i+k-1\,, \\ h_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{i+k}, z_1, \ldots, z_l)\,, \ \ \text{for } \ j = i+k\,, \\ \big(\ \zeta_{(i,i+k)}(\mathbf{z};\ \mathbf{x}) \ \wedge \ \phi_i(x_1, \ldots, x_i, x_{i+1}, \ldots, x_{i+k}, z_1, \ldots, z_l)\ \big) \\ \vee \ \big(\ \big(\neg\, \zeta_{(i,\,i+k)}(\mathbf{z};\ \mathbf{x})\ \big) \ \wedge \ x_{j-k-1}\ \big)\,, \quad \text{for } \ j = i+k+1\,, \end{cases}$$

It may be observed that

$$\begin{aligned} \rho_1\big(y_1, \ldots, y_k, 1, 0\big) &= \neg g_1(y_1, \ldots, y_k)\,, \quad \text{and} \\ \rho_1\big(y_1, \ldots, y_k, 1, 1\big) &= g_1(y_1, \ldots, y_k) \end{aligned}$$

Thus, computing nonparametric left inverses of parametric multivariate polynomial mappings is PSPACE-hard.

Part (2) Let $\eta(\mathbf{z};\ \mathbf{x})$, $\mathbf{z} = (z_1, \ldots, z_{n-k})$ and $\mathbf{x} = (x_1, \ldots, x_{m+k})$, be a parametric multivariate polynomial mapping from $\mathbb{Z}_2^{m+k}$ into $\mathbb{Z}_2^{k+1}$, with parameters $z_1, \ldots, z_{n-k}$ as follows: $\eta_i(\mathbf{z};\ \mathbf{x}) = x_{m+i}$, for $1 \le i \le k$, and $\eta_{k+1}(\mathbf{z};\ \mathbf{x}) = f(x_1, \ldots, x_{m+k}, z_1, \ldots, z_{n-k})$. Now, if $\eta(\mathbf{z};\ \mathbf{x}) = \mathbf{y}$, where $\mathbf{y} = (y_1, \ldots, y_k, 1) \in \mathbb{Z}_2^k \times \{1\}$, with $y_{k+1} = 1$, then $x_i = y_i$, for $1 \le i \le k$, $x_{k+i} = g_i(y_1, \ldots, y_k)$, for $1 \le i \le m$, by the uniqueness of the solution for the given instance of constraint satisfaction problem, and hence, computing nonparametric right inverses of parametric multivariate polynomial mappings is PSPACE-hard. ∎

The construction of parametric injective mappings described in Theorem 4 shows how a general one-to-one mapping from G^m into G^n, where m and n are positive integers, with $m \le n$, and G is a nonempty subset of a finite field $\mathbb{F}$, can be obtained: for a carefully chosen bijective mapping $P(\mathbf{y})$ from G^n into itself and hashing keys $f_i(\mathbf{x})$, for $\mathbf{x} = (x_1, \ldots, x_m) \in \mathsf{G}^m$ and $1 \le i \le n-m$, the argument vector $(f_1(\mathbf{x}), \ldots, f_{n-m}(\mathbf{x}), x_1, \ldots, x_m)$ is substituted for $\mathbf{y} \in \mathsf{G}^n$ in $P(\mathbf{y})$. Thus, $Q(\mathbf{x}) = P(f_1(\mathbf{x}), \ldots, f_{n-m}(\mathbf{x}), x_1, \ldots, x_m)$ is a generic multivariate one-to-one mapping from G^m into G^n.

5 Security Analysis

The classical analysis of multivariate simultaneous equations can be applied only to polynomial equations [[12], [14], [34], [35], [36] and [47]], and the Gröbner basis analysis [[8], [16] and [17]] is employed as the main practical tool. A general purpose method for solving multivariate mappings involving functions as exponents is not known as yet. For a security that is immune to threats from Gröbner basis analysis, parametric injective mappings from G^{μ} into E^{ν}, with κ parameters, for $\mathsf{G} = \mathbb{F}^{*}$, $\mathsf{E} = \mathbb{F}$ and $\mu, \nu, \kappa \in \mathbb{N}$, where $1 \leq \mu \leq \nu$ and $\mathbb{F}$ is a finite field, with component mappings taken as expressions from $\mathcal{EXP}\big(\mathbb{F}\,;\,[x_1, \ldots, x_\mu, \omega_1, \ldots, \omega_\kappa]\big)$, restricting values of x_i and ω_j to $\mathbb{F}^{*}$, for $1 \leq i \leq \mu$ and $1 \leq j \leq \kappa$, with at least one level of exponentiation as described in section 1.5, are required. It is also assumed that the key generator ensures that a prospective owner of the pertinent keys is provided with an abundance of options for generating multivariate one-to-one mappings, whose inverse mappings are known only to the owner.

In public key cryptography, the size of the set $\{F(\mathbf{x}, \boldsymbol{\omega}) : \boldsymbol{\omega} \in \mathbb{F}^{\kappa}\}$ must be large, such as perhaps exponential in ν^{c}, for some fixed $c > 0$, for each $\mathbf{x} \in \mathbb{F}^{\mu}$, while maintaining $F(\mathbf{x}, \boldsymbol{\omega})$ as a secret to the public, for IND-CCA and IND-CPA security, whichever is relevant. Under the assumption of no mistrust, the padding message $\boldsymbol{\omega}$ can be negotiated for mutual agreement by sender and receiver, for ascertaining data integrity, in public key cryptography.

For digital signature, the main security issue is the anonymity of the secret keys $F(\mathbf{x}, \boldsymbol{\omega}) = \big(f_1(\mathbf{x}, \boldsymbol{\omega}), \ldots, f_L(\mathbf{x}, \boldsymbol{\omega})\big)$, which are registered with a trusted authentication verifier (TAV). The size of the set $\{\boldsymbol{\omega} \in \mathsf{G}^{\kappa} : H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega}) = \boldsymbol{\delta}\}$, where $\mathbf{z} \in \mathsf{G}^{\lambda}$, $\mathbf{x} \in \mathsf{G}^{\mu}$ and $\boldsymbol{\delta} \in \mathsf{E}^{\tau}$, must be large, such as perhaps exponential in ν^{c}, for some fixed $c > 0$, whenever the set in the discussion is nonempty, and the ratio of the number of elements in $\{(\boldsymbol{\omega}, \mathbf{z}) \in \mathsf{G}^{\kappa+\lambda} : H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega}) = \boldsymbol{\delta}\}$ to that in $\{(\boldsymbol{\omega}, \mathbf{z}) \in \mathsf{G}^{\kappa+\lambda} : H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega}) = \boldsymbol{\delta}\} \cap \{(\boldsymbol{\omega}, \mathbf{z}) \in \mathsf{G}^{\kappa+\lambda} : R(\mathbf{z}) = F(\mathbf{x}, \boldsymbol{\omega})\}$ must be large, if $H(\mathbf{z}, \mathbf{x}, \boldsymbol{\omega})$ occur in the public key signature verification table V, whenever the stated sets are nonempty, such as perhaps exponential in ν^{c}, for some fixed $c > 0$ and any fixed $\boldsymbol{\delta} \in \mathsf{E}^{\tau}$, admissible plain message $\mathbf{x} \in \mathsf{G}^{\mu}$ and admissible padding message $\boldsymbol{\omega} \in \mathsf{G}^{\kappa}$. The admissibility of the padding message $\boldsymbol{\omega} \in \mathsf{G}^{\kappa}$ is that $R(\boldsymbol{\omega}) = \boldsymbol{\omega}'$, where $\boldsymbol{\omega}' \in \mathsf{G}^{K}$ is the extra padding message agreed upon by the signer with TAV, for the particular reserved transaction, as a first step in the process of generating the signature. The hidden or secret keys $F(\mathbf{x}, \boldsymbol{\omega})$ must not be made known to the public, but, in the digital signature scheme, are shared with the TAV, besides the signer, in order to ensure existential unforgeability. For claiming the authenticity of a signature, the claimant needs to produce $\boldsymbol{\epsilon}$, $\boldsymbol{\delta}$, $\mathbf{x}$, $\mathbf{z}$ and $\boldsymbol{\omega}$, for passing the tests of TAV, without knowing the information in the signature authentication verification table A, which is registered with TAV. The signer must assert with TAV, by means of $\boldsymbol{\omega}'$ and other protocol agreements, regarding authorization of a signature. Thus, the signer is protected by the prudence and unbiasedness of TAV.

6 Conclusion and Summary

In this paper, a new public key data encryption method is proposed, where the plain and encrypted messages are arrays. The method can also be used for digital certificate or digital signature applications. For security protocols of the application layer level in the OSI model, the methods described in this paper are useful. In the regular protocols like TLS and IPSec [[44] and [45]], the traditional methods, requiring only small space for the keys and algorithms, are employed. The key generation algorithm is particularly simple, easy and fast, facilitating changes of keys as frequently as required, and fast algorithms for polynomial multiplication and modular arithmetic [[7] and [40]], whenever appropriate, can be adapted in the encryption and decryption algorithms.

References

[1] María T. Acosta-de-Orozco, and Javier Gómez-Calderón, "The Factorization of the Derivative of Dickson Polynomials", *Extracta Mathematicae*, Vol. 6(1), 1991, pp. 42–43

[2] A. Akbary, S. Alaric, and Q. Wang, "On Some Classes of Permutation Polynomials", *International Journal of Number Theory*, Vol. 4(1), 2008, pp. 121–133

[3] A. Akbary, D. Ghioca, and Q. Wang, "On Permutation Polynomials of Prescribed Shape", *Finite Fields and Their Applications*, Vol. 15, 2009, pp. 195–206

[4] A. Akbary, and Q. Wang, "On Some Permutation Polynomials over Finite Fields", *International Journal of Mathematics and Mathematical Sciences*, Vol. 16, 2005, pp. 2631–2640

[5] Olivier Billet and Jintai Ding, "Overview of Cryptanalysis Techniques in Multivariate Public Key Cryptography", in *Gröbner Bases, Coding, and Cryptography*, M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso (Eds.), Part 1, 2009, pp. 263–283

[6] D. J. Bernstein, J. Buchmann, and E. Dahmen, "Post-Quantum Cryptography", Springer-Verlag, 2009

[7] Richard P. Brent, and Paul Zimmermann, "Modern Computer Arithmetic", Cambridge Monographs on Applied and Computational Mathematics (No. 18) Cambridge University Press, 2010

[8] Bruno Buchberger, "An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal", Ph. D. Thesis, University of Innsbruck (1965), English translation by M. Abramson in *Journal of Symbolic Computation*, Special Issue on Logic, Mathematics, and Computer Science: Interactions, Vol. 41(3), 2006, pp. 475–511

[9] Johannes Buchmann, "Introduction to Cryptography", Second Edition, Springer-Verlag, Heidelberg, 2004

[10] D. Castro, M. Giusti, J. Heintz, G. Matera, and L. M. Pardo, "The Hardness of Polynomial Equation Solving", *Foundations of Computational Mathematics*, Vol. 3(4), 2003, pp. 347–420

[11] D. Coppersmith, and A. Shamir, "Lattice attacks on NTRU", *Advances in Cryptology -Eurocrypt '97*, LNCS Vol. 1233, Springer Verlag, 1997, pp. 52–61

[12] D. van Dalen, "Logic and Structure", Springer-Verlag, 1994

[13] L. E. Dickson, "The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group", *The Annals of Mathematics*, Vol. 11(1), 1896, pp. 65–120 and 161–183

[14] L. van den Dries, "Classical Model Theory of Fields", in *Model Theory, Algebra and Geometry*, MSRI Publications, Vol. 39, 2000, pp. 37–52

[15] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *Advances in Cryptology – Crypto' 84*, LNCS Vol. 196, Springer-Verlag, 1985, pp. 10–18; Journal version in *IEEE Trans. Information Theory*, Vol. 31(4), 1985, pp. 469–472

[16] J.-C. Faugère, "A New Efficient Algorithm for Computing Gröbner Bases (F4)", *Journal of Pure and Applied Algebra*, Vol. 139(1), 1999, pp. 61–88

[17] J.-C. Faugère, "A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5)", *Proc. International Symposium on Symbolic and Algebraic Computation*, ACM Press, 2002, pp. 75–83

[18] S. H. Gao, and G. L. Mullen, "Dickson Polynomials and Irreducible Polynomials over Finite Fields", *Journal of Number Theory*, Vol. 49(1), 1994, pp. 118–132

[19] C. Gentry, "Key Recovery and Message Attacks on NTRU-Composite", *Advances in Cryptology - Eurocrypt 2001*, LNCS Vol. 2045, Springer-Verlag, 2001, pp. 182 - 194

[20] W. Hodges, "Model Theory", Cambridge University Press, 1993

[21] J. Hoffstein, D. Lieman, and J. H. Silverman, "Polynomial Rings and Efficient Public Key Authentication", *Proc. International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99)*, Ed. M. Blum and C.H. Lee, City University of Hong Kong Press, 1999

[22] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A Ring Based Public Key Cryptosystem", *Algorithmic Number Theory (ANTS III)*, LNCS Vol. 1423, Springer-Verlag, 1998, pp. 267–288

[23] J. Hoffstein, J. Pipher, and J. Silverman, "NSS: An NTRU Lattice-based Signature Scheme", *Advances in Cryptology - Eurocrypt 2001*, LNCS Vol. 2045, Springer-Verlag, 2001, pp. 211–228

[24] J. Hoffstein, and J. Silverman, "Polynomial Rings and Efficient Public Key Authentication II", *Proc. Conference on Cryptography and Computational Number Theory (CCNT '99)*, Birkhäuser, 2001, pp. 269–286

[25] J. E. Hopcroft, R. Motwani, and J. D. Ullman, "Introduction to Automata Theory, Languages and Computation", Pearson Education, 2007

[26] E. Horowitz, S. Sahni, and S. Rajasekaran, "Fundamentals of Computer Algorithms", Universities Press, 2007

[27] N. Koblitz, "Elliptic Curve Cryptosystems", *Mathematics of Computation*, Vol. 48(177), 1987, pp. 203–209

[28] N. Koblitz, "A Course in Number Theory and Cryptography", Second Edition, Springer-Verlag, 1994

[29] N. Koblitz, "Algebraic Aspects of Cryptography", *Algorithms and Computation in Mathematics*, Vol. 3, Second Printing, Springer-Verlag, 1994

[30] Serge Lang, "Algebra", Springer-Verlag, 2002 (previously published by Addison-Wesley, 1993)

[31] R. Lidl, G. L. Mullen, and G. Turnwald, "Dickson Polynomials", Pitman Monographs and Surveys in Pure & Applied Mathematics, 65, Longman Scientific & Technical, 1993

[32] R. Lidl, and H. Niederreiter, "Introduction to Finite Fields and Their Applications", Cambridge University Press, 1986

[33] C. H. Lin, C. C. Chang, and R. C. T. Lee, "A New Public Key Cipher System Based upon Diophantine Equations", *IEEE Trans. Computers*, Vol. 44(1), 1995, pp. 13–19

[34] Yu. I. Manin, "A Course in Mathematical Logic for Mathematicians", Second Edition, Translated from Russian by N. Koblitz, Springer-Verlag, 2010

[35] D. Marker, "Introduction to Model Theory", in *Model Theory, Algebra and Geometry*, MSRI Publications, Vol. 39, 2000, pp. 15–35

[36] D. Marker, M. Messmer, and A. Pillay, "Model Theory of Fields", Lecture Notes in Logic, Vol. 5, Springer-Verlag, 1996

[37] V. S. Miller, "Use of Elliptic Curves in Cryptography", *Advances in Cryptology – Crypto' 85*, LNCS Vol. 218, Springer-Verlag, 1986, pp. 417–426

[38] G. L. Mullen, "Dickson Polynomials", *Encyclopedia of Mathematics, Supplement II*, Kluwer Academic Publishers, 2000, pp. 154–156

[39] G. L. Mullen, and H. Niederreiter, "Dickson Polynomials over Finite Fields and Complete Mappings", *Canadian Mathematical Bulletin*, Vol. 30(1), 1987, pp. 19–27

[40] V. Pan, "Complexity of Computations with Matrices and Polynomials", *SIAM Review*, Vol. 34(2), 1992, pp. 225-262

[41] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Vol. 21(2), 1978, pp. 120–126

[42] B. Schneier, "Applied Cryptography", John Wiley & Sons, 1996

[43] N. P. Smart, "The Discrete Logarithm Problem on Elliptic Curves of Trace One", *Journal of Cryptology*, Vol. 12(3), 1999, pp. 193–196

[44] W. Stallings, "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall, 2011

[45] W. Stallings, "Network Security Essentials", Fourth Edition, Prentice Hall, 2011

[46] D. R. Stinson, "Cryptography: Theory and Practice", Chapman & Hall Press, 2005

[47] A. Tarski, "A Decision Method for Elementary Algebra and Geometry", University of California Press, 1951

[48] L. C. Washington, "Elliptic Curves: Number Theory and Cryptography", Chapman & Hall Press, London, 2008