sensors

MDPI

Article

A Novel Method for Polar Form of Any Degree of Multivariate Polynomials with Applications in IoT

Sedat Akleylek [1], Meryem Soysaldı [1], Djallel Eddine Boubiche [2] and Homero Toral-Cruz [3,*]

[1] Department of Computer Engineering, Ondokuz Mayıs University, Samsun 55139, Turkey; sedat.akleylek@bil.omu.edu.tr (S.A.); meryem.soysaldi@bil.omu.edu.tr (M.S.)
[2] LaSTIC Laboratory, Department of Sciences & Technologies, University of Batna 2, Batna 05000, Algeria; dj.boubiche@gmail.com
[3] Department of Sciences and Engineering, University of Quintana Roo, Chetumal 77019, Mexico
* Correspondence: htoral@uqroo.edu.mx

Received: 23 December 2018; Accepted: 3 February 2019; Published: 21 February 2019

Abstract: Identification schemes based on multivariate polynomials have been receiving attraction in different areas due to the quantum secure property. Identification is one of the most important elements for the IoT to achieve communication between objects, gather and share information with each other. Thus, identification schemes which are post-quantum secure are significant for Internet-of-Things (IoT) devices. Various polar forms of multivariate quadratic and cubic polynomial systems have been proposed for these identification schemes. There is a need to define polar form for multivariate dth degree polynomials, where $d \geq 4$. In this paper, we propose a solution to this need by defining constructions for multivariate polynomials of degree $d \geq 4$. We give a generic framework to construct the identification scheme for IoT and RFID applications. In addition, we compare identification schemes and curve-based cryptoGPS which is currently used in RFID applications.

Keywords: multivariate polynomials; post-quantum cryptography; bilinear functions; identification schemes; IoT; RFID

1. Introduction

Identification schemes are needed to provide identity of the communicating parties [1]. In these schemes, there are two parties: prover and verifier. The prover wants to prove to the verifier that he/she is really the person who is communicating. The verifier asks questions to convince the prover's commitment. The prover tries to convince the verifier without revealing his secret information. Identification schemes are the most important elements for many area, such as devices connected to the Internet. IoT is a popular technology that allows objects to identify and communicate with each other by connecting to Internet [2]. IoT consists of billions of devices that can communicate, gather and share information, make a decision without human interaction. IoT provides the opportunities for devices to see, hear, think and talk with each other via Internet [3]. According to Cisco predictions, there will be approximately 50 billion devices connected to the Internet by 2020 [4]. In this respect, we can say that there is a big demand for IoT applications since IoT has a wide range of applications such as intelligent transportation systems, smart home and building automation, medical and health systems, industrial management, energy systems, environment and infrastructure monitoring [5–8]. For understanding of IoT applications, IoT systems need to be divided into small components in view of tasks [2]. Thus, the first task of IoT systems is

to identify and monitor the objects communicating with. The second task is to collect and process the information. In this structure, we have two main problems: identification and (secure) communication. Therefore, we focus on efficient and secure identification in IoT systems in this paper.

Identification is crucial to communicate among devices securely and properly. Radio-frequency identification technology (RFID) serves to identify objects automatically with electromagnetic frequency waves in IoT [9]. An RFID system consists of two components: the RFID tag which collects the information and transmits the collected data to the application and the RFID reader which stores the information [10]. Identification schemes used in RFID applications have some properties such as scalability, low memory requirement, communication and computational cost. In addition, an identification scheme has zero-knowledge property that does not allow an intruder verifier to hold communication [11]. CryptoGPS protocols which are of standard designed commonly use RFID applications [12,13]. CryptoGPS is a public key identification scheme which uses modular explementation in a multiplication group or a scalar multiplication in an additive group. Recall that after the quantum computer idea had been introduced, a quantum computer with two qubits was build. Then, the number of qubits increased. Nowadays, we know that Google and D-wave have 72-qubit and 2048-qubit quantum computers, respectively [14]. In addition, the systems whose security depends on integer factorization or discrete logarithm problems which are used in the identification schemes are called insecure due to Shor's polynomial time algorithm in quantum computers [15]. For this reason, there is a big demand to construct quantum secure identification schemes. There are many classes since there is no known polynomial time algorithm to solve multivariate polynomial in any computational area. The cryptosystems based on multivariate polynomials are used in quantum secure areas [16–18].

In the literature, identification schemes based on multivariate quadratic polynomials as well as cubic ones have received interest since they are efficient for different platforms [19–21]. In [19], 3 and 5-pass zero-knowledge identification schemes based on multivariate quadratic (MQ) polynomials over a finite field were proposed. They defined bilinear functions as polar form of the MQ polynomial systems. In addition, they indicated whether or not it is able to build an efficient protocol using multivariate polynomials of degrees greater than two. In [20], 3-pass zero-knowledge identification scheme-based multivariate quadratic polynomials over a finite field by using the same bilinear functions were presented. However, they used a different way to divide secret key. Then, in [21], these identification schemes were improved in view of communication complexity by using new dividing techniques with the help of bilinearity of a polar form of the MQ function. Moreover, 3 and 5-pass identification schemes based on multivariate cubic (MC) polynomials over finite field were proposed. A new associated linear-in-one argument form, i.e., polar form of MC functions was defined and can be applied to a cubic version of the problem without changing bilinear form. The main difference between [19] and [21] is the degree of multivariate polynomial systems.

A different polar form is used with the same bilinear property. In [22], identification schemes based on multivariate polynomials over a finite field in the literature were surveyed. 3 and 5-pass identification schemes based on multivariate quadratic and cubic polynomials were given with the dividing technique of the secret key and polar form construction. In addition, all identification schemes based on multivariate polynomials were compared in view of memory requirements, communication length, and computation time. In [23], a new identification scheme based on multivariate quadratic polynomials was presented by using a different dividing technique of the secret key. Then, the proposed identification scheme was transformed to the signature scheme.

1.1. Motivation

In [21], efficient constructions based on multivariate polynomials of degree $d \geq 4$ are given as an open problem (see Section 2.1). The hardness of this problem comes from the nonlinear terms in $f(x+y) - f(x) - f(y)$. In [24], a solution with a different perspective was proposed for the open problem. They denoted a polarization identity for a system of multivariate polynomials of any degree d. The function $G : (\mathbb{F}_q^n)^d \to \mathbb{F}_q^m$ is given as follows:

$$G(r_0, r_1, \ldots, r_{d-1}) = \sum_{i=1}^{d} (-1)^{d-i} \sum_{\substack{S \subset \{0,\ldots,d-1\} \\ |S|=i}} F(\sum_{j \in S} r_j). \tag{1}$$

By Equation (1), polar form of the system of multivariate polynomials in $d-$linear form was obtained. They also generalized identification protocol for multivariate $d-$degree polynomials with this perspective.

Variants of CryptoGPS are used in RFID applications. However, these protocols are not quantum secure. There is a need to construct identification schemes that are secure against quantum attacks.

1.2. Our Contribution

We propose a solution for the open problem with a different perspective. We generalize polar form for any degree of multivariate polynomials using bilinear functions. We define how the polar function will be when any degree of multivariate polynomials is used with Theorem 1. The idea comes from the bilinear functions used in both multivariate quadratic [19,20] and cubic [21] polynomials over a finite field. We present a generic identification scheme based on any degree of multivariate polynomials. In addition, we provide a comparison for the cryptoGPS standard and identification schemes based on multivariate polynomials. The generic identification scheme framework can be used to construct identification scheme for RFID applications due to the zero-knowledge property.

1.3. Organization

The rest of this paper is organized as follows. In Section 2, we give some definitions and then explain our solution proposal for the open problem. Moreover, we express our solution with examples and compare it to the other approach [24] for the open problem. We give a generic scheme for identification construction when using any degree of multivariate polynomials. Then, we compare curve-based cryptoGPS and identification schemes based on multivariate polynomial. The conclusion and future works are stated in Section 3.

2. A Novel Method for Polar Form of Multivariate Polynomials of Any Degree

In this section, we first review some definitions and notations. We recall the open problem given in [24]. Then, we express our method for polar form of multivariate polynomials and give examples. We compare our solution and the other approach [24].

2.1. Mathematical Background

Multivariate cryptography depends on solving systems of multivariate polynomials of degree d over a finite field. For $d = 2$ or $d = 3$, then it is called MQ or MC, respectively. The system of multivariate polynomials of degree d with n variables and m equations can be given as follows:

$$\begin{aligned}
f^{(1)}(x_1,\ldots,x_n) &= \sum_{i}^{n}\cdots\sum_{j}^{n} f^{(1)}_{i\cdots j}\overbrace{x_i\cdot\ldots\cdot x_j}^{d}+\ldots+\sum_{i=1}^{n} f_i^{(1)}\cdot x_i + f_0^{(1)}\\
f^{(2)}(x_1,\ldots,x_n) &= \sum_{i}^{n}\cdots\sum_{j}^{n} f^{(2)}_{i\cdots j}\overbrace{x_i\cdot\ldots\cdot x_j}^{d}+\ldots+\sum_{i=1}^{n} f_i^{(2)}\cdot x_i + f_0^{(2)}\\
&\vdots\\
f^{(m)}(x_1,\ldots,x_n) &= \sum_{i}^{n}\cdots\sum_{j}^{n} f^{(m)}_{i\cdots j}\overbrace{x_i\cdot\ldots\cdot x_j}^{d}+\ldots+\sum_{i=1}^{n} f_i^{(m)}\cdot x_i + f_0^{(m)}.
\end{aligned} \tag{2}$$

where the coefficients ($f^{(k)}_{i\ldots j}$ and $f_i^{(k)}$ for $1 \leq k \leq m$) are in a finite field. Note that the MQ problem, which is NP-complete, can be defined as follows:

Definition 1. *[15] Given m multivariate quadratic polynomials $f^{(1)}(\mathbf{x}),\ldots,f^{(m)}(\mathbf{x})$ as shown in Equation (2), find a vector $\bar{\mathbf{x}} = (\bar{x}_1,\ldots,\bar{x}_n)$ such that $f^{(1)}(\bar{\mathbf{x}}) = \ldots = f^{(m)}(\bar{\mathbf{x}}) = 0$.*

The hardness of MQ problem depends on the hardness of solving nonlinear equations over finite field [15]. In Definition 2, the polar form of the MQ function is given.

Definition 2. *[19] Let $x \in \mathbb{F}_q^n$, $f_\ell(x)$ be multivariate quadratic function for $1 \leq \ell \leq m$ and $F(x) = (f_1(x), f_2(x),\ldots,f_m(x)) \in MQ(n,m,\mathbb{F}_q)$. Then polar form of the MQ function is $G(x,y) = F(x+y) - F(x) - F(y)$.*

Definition 3. *Let $G : A \times A \to B$ be a bilinear function. Then, G satisfies the following properties:*

- $G(x+y,z) = G(x,z) + G(y,z)$ *and* $G(ax+y,z) = aG(x,z) + G(y,z)$
- $G(x,y+z) = G(x,y) + G(x,z)$ *and* $G(x,ay+z) = G(x,z) + aG(y,z)$

where $x,y \in A$, $z \in B$ and a is a constant.

Remark 1. *The function G in Definition 2 is bilinear since $G(x,y) = \sum_{ij} a_{\ell,i,j}(x_iy_j + y_ix_j)$, where x,y are $n-$dimension vectors. Because of the bilinearity of $G : A \times A \to B$, $G(x+y,z) = G(x,z) + G(y,z)$, where $x,y \in A$ and $z \in B$. Note that this is only valid for MQ systems. It is difficult to control the terms in $d-$degree of elements because the number of terms increases when higher-order functions are used.*

In Definition 4, polar form of MC function which is a natural extension of MQ ones is given.

Definition 4. *[21] Let $x \in \mathbb{F}_q^n$, $F(x) = (f_1(x), f_2(x),...,f_m(x)) \in MC(n,m,\mathbb{F}_q)$ and $f_\ell(x) = \sum_{i,j,k} a_{\ell,i,j,k}x_ix_jx_k + \sum_{i,j} b_{\ell,i,j}x_ix_j + \sum_i c_{\ell,i}x_i$. $G = (g_1,\cdots,g_m)$ is the polar form of F for $\ell = 1,\cdots,m$, $g_\ell(x,y) = \sum_{i,j,k} a_{\ell,i,j,k}(x_ix_jy_k + x_iy_jx_k + y_ix_jx_k) + \sum_{i,j} b_{\ell,i,j}x_iy_j$ and $g_\ell(y,x) = \sum_{i,j,k} a_{\ell,i,j,k}(y_iy_jx_k + y_ix_jy_k + x_iy_jy_k) + \sum_{i,j} b_{\ell,i,j}y_ix_j$ where x,y are $n-$dimension vectors over $\mathbb{F}_q^n$. Moreover, G is a bilinear function and is obtained from $F(x+y) = F(x) + G(x,y) + G(y,x) + F(y)$.*

Now, we recall the open problem given in [21].

Open Problem. *In [19–21], identification schemes based on multivariate quadratic and cubic polynomials were given. In [21], an open problem was defined: Is there any general method to construct polar form of multivariate polynomials of degree $d \geq 4$ in an efficient way?*

By considering [19–21], we have polar forms of multivariate quadratic and cubic polynomials. By using bilinear functions, polar forms of multivariate polynomials of degree of $d \geq 4$ can be obtained.

2.2. Another Look At Open Problem

Our aim is to generalize polar form for multivariate d-degree polynomials over a finite field. In Theorem 1, we introduce the generalization of linear-in-one-argument for the function of degree $d \geq 4$ which is a modified construction derived from the MQ and MC. Note that by recursive approach, one can obtain the linear form.

Theorem 1. *Let $\mathbb{F}_q$ be a finite field, $x, y \in \mathbb{F}_q^n$ and $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$, $f_\ell(x)$ be any degree of multivariate polynomial. Let $P(x^j, y^{i-j})$ be a permutation with $\binom{i}{j}$ elements which contains j times x and $i-j$ times y in any positions for a vector with i elements. Then, the generalization of linear-in-one-argument form for the function of degree $d \geq 4$ is defined as $F(x+y) = F(x) + G(x,y) + G(y,x) + F(y)$, where*

$$G(x,y) = xy + \sum_{i=3}^{d} \begin{cases} \sum_{j=1}^{\frac{(i-1)}{2}} P(x^{i-j}, y^j) & \text{if } i \text{ is odd}, \\ \sum_{j=1}^{(\frac{i}{2}-1)} P(x^{i-j}, y^j) + \frac{P(x^{i/2}, y^{i/2})}{2} & \text{if } i \text{ is even}. \end{cases}$$

and

$$G(y,x) = yx + \sum_{i=3}^{d} \begin{cases} \sum_{j=1}^{\frac{(i-1)}{2}} P(x^{j}, y^{i-j}) & \text{if } i \text{ is odd}, \\ \sum_{j=1}^{(\frac{i}{2}-1)} P(x^{j}, y^{i-j}) + \frac{P(x^{i/2}, y^{i/2})}{2} & \text{if } i \text{ is even}. \end{cases}$$

Proof. Both Definition 2 and Definition 4 have the same structure in terms of the usage of the functions. In other words, $G(x,y)$ is complement of $G(y,x)$ in view of commutativity.

Our observation is that the polar form defined for the quadratic and cubic versions can be generalized for any degree of multivariate polynomial systems since $G(x,y)$ and $G(y,x)$ can be obtained by using this idea. We combine this observation with the complementary property of the function. The formula can be classified for any z by considering even or odd case. In this step, we have two cases:

1. When i is odd, it is obvious to compute $G(x,y)$ and $G(y,x)$ since the number of the outputs of the P permutation is odd and the number of x and y in the output of the P permutation is not equal.
2. When i is even, we need to consider whether the number of x vectors equals the number of y vectors. In this case, we need to take half of the existing terms to be complementary. For this reason, the even case is different from the odd case.

Then, the number of distinct elements in $G(x,y)$ or $G(y,x)$ is $2^d - d - 1$ due to the Pascal triangle. To compute each part of $G(x,y)$ or $G(y,x)$, $2^d - d - 1$ distinct elements having two vectors (only x and y) up to d vectors ($i-j$ times x and j times y) are computed. For $d = 2$ case, the permutation P permutes the positions of x and y in the element. Note that some terms are complement the other, i.e., $G(x,y)$ is complement of $G(y,x)$. This completes the proof. □

Now, we look at the following examples to compare our solution with the other approach [24]. In Example 1, we apply Theorem 1 to multivariate cubic polynomials ($d = 3$ case) and show that this is the same in Definition 4.

Example 1 (bilinear polar form of degree 3)**.** *For $d = 3$, we have*

$$F(x+y) = F(x) + G(x,y) + G(y,x) + F(y)$$

By using Theorem 1, $g_\ell(x,y) = \sum_{i,j,k} a_{\ell,i,j,k}(x_i x_j y_k + x_i y_j x_k + y_i x_j x_k) + \sum_{i,j} b_{\ell,i,j} x_i y_j$ and $g_\ell(y,x) = \sum_{i,j,k} a_{\ell,i,j,k}(y_i y_j x_k + y_i x_j y_k + x_i y_j y_k) + \sum_{i,j} b_{\ell,i,j} y_i x_j$. These $g_\ell(x,y)$ and $g_\ell(y,x)$ polynomials are same in [21] and in Definition 4.

In Example 2, we compare bilinear polar form by using Theorem 1 with trilinear polar form given in [24]. Since the idea is totally different, we have distinct polar forms.

Example 2 (trilinear polar form)**.** *When we use trilinear functions for $d = 3$, we have*

$$F(x+y+z) \quad = \quad G(x,y,z) + F(x+y) + F(x+z) + F(y+z) - F(x) - F(y) - F(z)$$

According to [24], $g_\ell(x,y,z) = \sum_{i,j,k} a_{\ell,i,j,k}(x_i y_j z_k + x_i y_k z_j + x_j y_i z_k + x_j y_k z_i)$ where x, y and z are $n-$dimension vectors over a finite field and $\ell \in \{1, \ldots, m\}$.

From Examples 1 and 2, we see that fewer terms are needed to in the use of bilinear functions than trilinear ones. To compute $F(s)$, by using bilinear function four functions are needed to be computed. However, by using trilinear function one needs seven functions. Note that the bilinear polar form is simpler and more controllable.

In Example 3, we apply Theorem 1 to multivariate quartic polynomials ($d = 4$ case).

Example 3. *Let $d = 4$. Then, multivariate quartic polynomials system F is in the following form:*
$\mathbb{F}(x+y) = \sum_{i,j,k,t} a_{\ell,i,j,k,t}(x_i x_j x_k x_t + y_i y_j y_k y_t + x_i x_j x_k y_t + x_i x_j y_k x_t + x_i y_j x_k x_t + y_i x_j x_k x_t + x_i x_j y_k y_t + x_i y_j x_k y_t + x_i y_j y_k x_t + y_i y_j y_k x_t + y_i y_j x_k y_t + y_i x_j y_k y_t + x_i y_j y_k y_t + y_i y_j x_k x_t + y_i x_j y_k x_t + y_i x_j x_k y_t) + \sum_{i,j,k,t} b_{\ell,i,j,k}(x_i x_j x_k + y_i y_j y_k + x_i y_j x_k + y_i x_j x_k + x_i x_j y_k + y_i x_j y_k + x_i y_j y_k + y_i y_j x_k) + \sum_{i,j} c_{\ell,i,j}(x_i x_j + y_i y_j + x_i y_j + x_j y_i) + \sum_i d_{\ell,i}(x_i + y_i)$.

By using Theorem 1, the linear-in-one-argument form of F is:

$$G(x,y) = xy + P(x^2, y) + P(x^3, y) + \frac{P(x^2, y^2)}{2}. \tag{3}$$

$$G(y,x) = yx + P(x, y^2) + P(x, y^3) + \frac{P(x^2, y^2)}{2}. \tag{4}$$

$P(x^2, y)$ computed in Equation (3) is the complement of $P(x, y^2)$ in view of variables given in Equation (4), i.e., $P(x^2, y) = \overline{P(x, y^2)}$. In a similar manner, all permutation used in $G(x, y)$ are selected as a complement of those used in $G(y, x)$.

2.3. Comparison

Now, we compare the proposed solution with $d-$linear form in terms of the required number of the functions in Table 1.

Table 1. Comparison of the proposed solution and $d-$linear functions

	Partitions	**The Number of Functions**	**Memory Requirements**
This paper	2	$2(r+1)$	$2m(r+1)$
d-linear [24]	d	$2^d - 1$	$(2^d - 1)m$

The number of partitions of s secret key is constant in the proposed method because of the bilinearity. However, in [24] it depends on the degree d. The number of F and G functions to compute $F(s)$ in bilinear polar form is $2(r+1)$, where r is recursion number, whereas it is $2^d - 1$ $\left(\left(\begin{array}{c} d \\ d \end{array}\right) + \left(\begin{array}{c} d \\ d-1 \end{array}\right) + \cdots + \left(\begin{array}{c} d \\ 1 \end{array}\right)\right)$ for $d-$linear form [24]. When $F(s)$ is computed, one needs to calculate two F functions. In addition, one must compute two G polar form according to the proposed generalization form given in Theorem 1. Note that r is the loop number required to obtain each G polar form. For example, the secret key is divided into two parts as x and y. Then, we compute $F(x+y)$ by using polar form given in Definition 4. According to the proposed solution, the recursive construction is used for the calculation of $G(x, y)$. Let $d = 4$ be the degree of multivariate polynomials. The recursion number is $r = 2$ since we run $G(x, y)$ function for $d = 4$ and $d = 3$. Then, $G(x, y)$ function is obtained by adding quadratic terms. $G(y, x)$ is computed similarly. Actually, we use a divide-and-conquer approach for computing $G(x, y)$ and $G(y, x)$ function. The number of F and G functions is $2(r+1)$ by adding the number of F functions. The number of F and G functions is the main factor to determine the computation time in the identification scheme based multivariate polynomial systems (for more details, see [20]). Note that for efficiency reasons, the number of F and G functions should be as small as possible due to the arithmetic operations. Memory requirements in bilinear form and $d-$linear form are $2m(r+1)$ or $(2^d - 1)m$, respectively, where m is bit size of the output of F and G functions.

2.4. A Generic Identification Scheme Based on Multivariate Polynomials

In this section, we present a generic scheme for identification construction based on any degree of multivariate polynomials. The identification schemes are compared with the cryptoGPS standard. A 3-pass identification scheme is given in Figure 1.

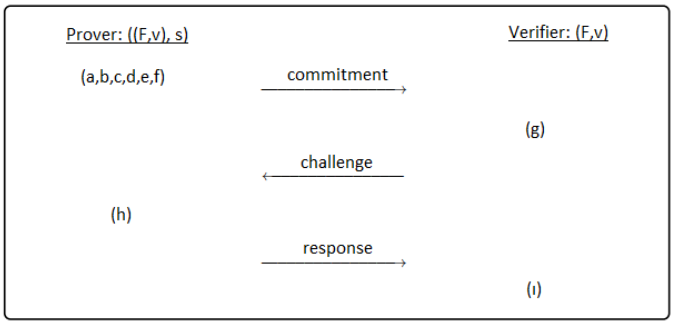

Figure 1. A 3-pass identification scheme.

A generic 3-pass identification scheme between prover and verifier has the following passes:

1. Commitment: The prover performs this pass.

   (a) The multivariate polynomial system F is constructed with n variables and m equations.
   (b) Choose randomly secret key $s \in \mathbb{F}_q$ and generate public key $v = F(s)$.
   (c) Divide secret key s into parts and sub-parts. Generate randomly the parts of s, not all of them. For example; let s be divided into k parts. According to dividing technique, the sub-parts of the secret key like $(r_1, r_2, \ldots, r_{k-1}) \in \mathbb{F}_q$ are generated randomly. Note that the secret key parts must be evaluated in F polynomial system. $v = F(s)$ is satisfied with the help of polar form.
   (d) Compute the parts of the secret key, not chosen randomly at step c. Thus, all parts of the secret key are obtained before the commitment phase.
   (e) According to dividing technique and polar form, the commitment values $c_1, c_2, \ldots, c_i$ are computed, where $i \in N$. The number of the commitment values is changeable according to the constructed scheme.
   (f) In this step, the prover sends the commitment values. Thus, the prover commits the verifier. At the end of this step, the first pass of the identification scheme is completed.

2. Challenge: At the second phase, all operations are performed by the verifier.

   (g) The verifier makes a challenge to the prover. For example; the verifier chooses a challenge value $Ch \in \{0, 1, \ldots, n-1\}$ and sends to the prover.

3. Response: This phase is performed by the prover.

   (h) The prover sends the responses which belong to each challenge in order that the verifier computes the commitment values.

   At the end of the this step, the verifier carries out the following step and terminates the identification scheme as accepted or rejected.

   (ı) The verifier computes the commitment values after the verifier receives the responses. Then the verifier compares these commitment values with the values which sent as commitment by the prover. If they are equal, the verifier accepts the prover's commitment. Otherwise, the verifier rejects. When the verifier computes the commitment values, the verifier can compute the same commitment value with different parts of the secret key unlike the prover. Note that the same values are obtained by using polar form.

Remark 2. *A zero-knowledge identification scheme provides us to restrict information which is sent from the prover to the verifier. When the verifier has any limited and any useless information, he/she can prove the prover's commitments. An identification scheme has to satisfy soundness and completeness properties for security and zero-knowledge. If an identification scheme is completed, i.e., the verifier accepts the prover's commitment, the*

identification scheme has completeness property [25]. If the verifier can not be deceived by the intruding prover (except negligible probability $\epsilon > 0$) , the identification scheme has soundness property [25]. One of the important criteria for identification scheme is impersonation probability. It is defined as the probability that an adversary would impersonate the prover without knowing the secret key.

The proposed generic scheme depends on the dth degree multivariate polynomials. The key pair and communication length are calculated easily with only basic polynomial operations. However, curve-based cryptoGPS identification schemes, which commonly use IoT applications, require scalar-point multiplications. Note that we prove a generic identification scheme framework in Section 2.4. Thus, we do not have numeric parameters for any security level. However, the comparison is provided by identification schemes based on multivariate quadratic or cubic polynomials presented in [19,21,23] with curve-based cryptoGPS [26]. In Table 2, for 80-bit security level, the comparison is given by considering security attacks against quantum attacks, impersonation probability and parameter set including secret key, challenge and response sizes.

Table 2. Comparison of the identification schemes and cryptoGPS.

	cryptoGPS [26]	**MQ-IDS [19]**	**MQ-IDS [23]**	**MC-IDS [21]**
Secret key	160 bits	84 bits	84 bits	84 bits
Challenge	848 bits	104 bits	60 bits	146 bits
Response	1088 bits	248 bits	896 bits	248 bits
Impersonation probability	2^{-32}	2^{-30}	2^{-30}	2^{-30}
Quantum secure	No	Yes	Yes	Yes

In Table 2, challenge indicates the bit size of challenge which is determined so that the verifier can obtain all commitment values for identification schemes based on multivariate polynomials. When we compare the identification schemes for the size of response, identification schemes given in [19,21] have small values. The main reason of small key sizes is the bilinear polar form of multivariate polynomials of degree $d > 1$. If the identification scheme based on multivariate polynomials is well-organized, it has lower cost than cryptoGPS. Thus, it can be used IoT applications efficiently.

3. Conclusions

In this paper, we propose the generalization of linear in one argument form for the function of degree $d \geq 4$ and provide a solution for the open problem given in [21]. When the system of multivariate $d-$degree polynomials is used, we show how to construct the polar form by using a bilinear function. We present a generic framework to construct the identification scheme based on multivariate (cubic) polynomials. Then, we compare curve-based cryptoGPS and the identification schemes based on multivariate polynomials. We explain that the identification scheme based on multivariate polynomials can be used in quantum secure RFID applications. As a future work, new identification schemes based on multivariate dth polynomial systems can be constructed. Then, one can construct a signature scheme based on these identification schemes.

Author Contributions: Methodology & Conceptualization, S.A. and M.S.; error corrections, D.E.B. and H.T.-C.; writing-draft version, S.A. and M.S.; review & editing, S.A., M.S., D.E.B. and H.T.-C.

Funding: Sedat Akleylek and Meryem Soysaldı were partially supported by TÜBİTAK (Scientific and Technical Research Council of Turkey) under grant no. EEEAG-116E279. Homero Toral-Cruz thanks PRODEP and UQROO for partial financial support of this project.

Acknowledgments: The authors would like to express their gratitude to the anonymous reviewers for their invaluable suggestions in putting the present study into its final form. A preliminary version of this study was presented at the Third International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering (AMINSE), Tbilisi, Georgia, December 6-9, 2017.

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

References

1. Feige, U.; Fiat, A.; Shamir, A. Zero-knowledge Proofs of Identity. *J. Cryptol.* **1988**, *1*, 77–94. [CrossRef]
2. Rghioui, A.; Sendra, S.; Lloret, J.; Oumnad A. Internet of things for measuring human activities in ambient assisted living and e-health. *Netw. Protoc. Algorithms* **2016**, *8*, 15–28. [CrossRef]
3. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari M.; Ayyash M. Internet-of-Things: A Survey on Enabling Technologies, Protocols and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
4. Evans, D. *The Internet-of-Things: How the Next Evolution of the Internet is Changing Everything*; CISCO White Paper; CISCO: San Jose, CA, USA, 2011; pp. 1–11.
5. Gupta, B.B.; Quamara, M. An overview of Internet-of-Things (IoT): Architectural aspects, challenges, and protocols. *Concurr. Comput. Pract. Exp.* **2018**, e4946. [CrossRef]
6. ITU-T. *Overview of the Internet-of-Things (Y. 2060)*; ITU-T Recommendations: Geneva, Switzerland, 2012.
7. Yi, H.; Nie, Z. On the security of MQ cryptographic systems for constructing secure Internet of medical things. *Pers. Ubiquitous Comput.* **2018**, *22*, 1075–1081. [CrossRef]
8. Kang, M.S.; Im, H.; Jun, H.J.; Kim, T.S. Necessity and Expectation for an Identification Scheme in IoT Service: Cases in South Korea. *Indian J. Sci. Technol.* **2016**, *9*, 1–10. [CrossRef]
9. Dong, Q.; Ding, W.; Wei, L. Improvement and optimized implementation of cryptoGPS protocol for low-cost radio-frequency identification authentication. *Secur. Commun. Netw.* **2014**, *8*, 1474–1484. [CrossRef]
10. Mcloone, M.; Robshaw, M.J.B. Low-cost digital signature architecture suitable for radio frequency identification tags. *Comput. Digit. Tech. IET* **2010**, *4*, 14–26. [CrossRef]
11. Ethmane, E.M. *Authentication Issues in Low-Cost RFID*; Institut National des Télécommunications: Évry, Essonne, France, 2013.
12. Poschmann, A.; Robshaw, M.; Vater, F.; Paar, C. Lightweight cryptography and RFID: tackling the hidden overheads. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Korea, 2–4 December 2009; pp. 129–145.
13. ISO, ISO/IEC 29167-17:2015. *Information Technology—Automatic Identification and Data Capture Techniques—Part 17: Crypto Suite cryptoGPS Security Services for Air Interface Communications*; ISO: Geneva, Switzerland, 2015.
14. Quantum Computing Report. Available online: https://quantumcomputingreport.com/scorecards/qubit-count/ (accessed on 25 January 2019)
15. Bernstein, D.J.; Buchmann, J.; Dahmen, E. *Post-Quantum Cryptography*; Springer Science and Business Media: Berlin, Germany, 2009.
16. Chen, L.; Jordan, S.; Liu, Y.K.; Moody, D.; Peralta, R.C.; Perlner, R.A.; Smith-Tone, D.C. *Report on Post-Quantum Cryptography*; Internal Report 8105; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
17. Cheng, C.; Lu, R.; Petzoldt, A.; Takagi, T. Securing the Internet-of-Things in a quantum world. *IEEE Commun. Mag.* **2017**, *55*, 116–120. [CrossRef]
18. Ding, J.; Petzoldt, A. Current state of multivariate cryptography. *IEEE Secur. Priv.* **2017**, *15*, 28–36. [CrossRef]
19. Sakumoto, K.; Shirai, T.; Hiwatari H. Public-key Identification Schemes Based On Multivariate Quadratic Polynomials. In Proceedings of the Annual Cryptology Conference-CRYPTO 2011, Santa Barbara, CA, USA, 14–18 August 2011; pp. 706–723.
20. Monteiro, F.S.; Terada, R.; Goya, D.H. Improved Identification Protocol Based on the MQ Problem. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2015**, *98*, 1255–1265. [CrossRef]

21. Sakumoto, K. Public-Key Identification Schemes Based on Multivariate Cubic Polynomials. In Proceedings of the International Conference on Practice and Theory in Public Key Cryptography-PKC 2012, Darmstadt, Germany , 21–23 May 2012; Volume 7293, pp. 172–192.
22. Akleylek, S.; Soysaldı, M. Identification schemes in the post-quantum area based on multivariate polynomials with applications in cloud and IoT. In *Authentication Technologies for Cloud Technology, IoT and Big Data*; The Institution of Engineering and Technology (The IET): Stevenage, UK, 2019; pp. 181–207.
23. Akleylek, S.; Soysaldı, M. A Novel 3-pass Identification Scheme and Signature Scheme Based On Multivariate Quadratic Polynomials. *Turk. J. Math.* **2019**, *43*, 241–257. [CrossRef]
24. Nachef, V.; Patarin, J.; Volte, E. Zero Knowledge for Multivariate Polynomials. In Proceedings of the 2nd International Conference on Cryptology and Information Security in Latin America-LATINCRYPT 2012, Santiago, Chile, 10–12 October 2012; Volume 7533, pp. 194–213.
25. Goldreich, O. *Foundations of Cryptography*; Cambridge University Press: Cambridge, UK, 2009.
26. Poschmann, A. Lightweight Cryptography—Cryptographic Engineering for a Pervasive World. Ph.D. Thesis, Faculty of Electrical Engineering and Information Technology, Ruhr-University Bochum, Bochum, Germany, 2009.