Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 16, Number 2 (2020), pp. 233-239
©Research India Publications
http://www.ripublication.com/gjpam.htm

Multivariate Polynomial and Exponential Mappings based Password Authentication Protocol

Meher Krishna Duggirala[1], **Ravi Duggirala**[2], **Krishna Subba Rao Pulugurtha**[3]

[1,2,3]*Gayatri Vidya Parishad College of Engineering (Autonomous),*
Madhurawada, Visakhapatnam– 530 048, Andhra Pradesh, India.

[1]*E-mail: duggiralameherkrishna@gmail.com*

[2]*E-mail: ravi@gvpce.ac.in; duggirala.ravi@yahoo.com;*
duggirala.ravi@rediffmail.com; drdravi2000@yahoo.com

[3]*krishnasubbarao@gvpce.ac.in*

Abstract

In this paper, a multivariate polynomial and exponential mappings based password protocol is presented. The method can be utilized in public domains. The key generator generates a vector, intended to be used as a password by the authentication protocol subsequently, such that when the vector is substituted and evaluated in certain fixed multivariate polynomials – that may be listed in a public domain – the value 0 is found as a result of proper authentication. The public domain in this context could be internal to a large, and possibly distributed, system. The key generator can take hints from the owner of the password to generate the particular zero vector to suit the user. It may take into consideration biometric and any other user specific information at the time of key generation. The information collected by the key generator can be saved by the owner of the password for its possible retrieval upon requisition by the user, during the period of its validity, in case it is forgotten by the user.

Keywords: Multivariate polynomials; Exponential mappings; Gröbner basis; Zeros of mappings; User authentication.

1. INTRODUCTION

In this paper, a multivariate polynomial and exponential mappings based password protocol is presented. The method can be utilized in public domains. In recent times, the need to generate and utilize high security passwords has attracted a great deal of attention. The passwords need be resistant to a variety of attacks. The authentication protocol for allowing access to an authorized user of a secure system usually checks only for passwords. The approach of password based authentication can apply also to implementation of access restriction to security critical resources. The authentication method may have to be to be transparent, eliminating entry into the system by any unauthorized means to make the use of the system trustworthy. Other forms of application of this method include – but not limited to – software registry, web access, watermarking, *etc*.

A very common and standard method is to store the password itself in an encrypted form, by a one-to-one or hashing function. The authentication tests for the equality with the stored encrypted password after applying the chosen function on the input password. The difficulty relies on the strength of the encryption file and the resistance of the instances in the password file, for the particular chosen encryption and hashing functions. The space where the decryption keys are stored, when encryption mappings are employed, is the single most point of criticality, whereby necessitating the use of hashing mappings with default padding message applied at the input. The discussion moves on to collision-resistant hashing, even for small sized passwords, with default padding to fit to block length of hashing function input. Some of the articles for related literature are listed in the references.

The mapping that is used in the method proposed in this paper may be thought of some sort of hashing, but varies from user to user. These “hashing” mappings are stored in an authentication space, which may be treated as a public domain. The security does not depend on the difficulty of computing the preimage of a single password file, for a single encryption or hashing mapping. The parameters required for the password strength can be selected for each user, independently. The strength of a password depends on finding a simultaneous zero vector of authentication multivariate polynomial and exponential mappings. Authentication space may occupy considerably large space as compared to the size of the password itself, but when an attack occurs, it may be only one-off on a single user. The rest of the users may remain and carry on unaffected, because any unauthorised attempt to get a password is an independent attack for each user. In a future work by the authors, the need for so much extra space would most likely be overcome by another design.

2. MULTIVARIATE POLYNOMIAL AND EXPONENTIAL MAPPING BASED PASSWORDS

Let $\mathbb{Z}$ be the ring of integers, p be a large prime number, and $\mathbb{Z}_{\mathrm{p}}$ be the finite field of integers $\mathsf{mod}\ \mathrm{p}$. Let $\mathbb{F}$ be a field, which is preferably finite, and intended to be of characteristic p, although this assumption is not explicitly utilized in the discussion.

2.1. Multivariate Polynomial Mappings

In this subsection, $\mathbb{F}$ is not necessarily assumed to be finite, and the discussion holds also for fields of characteristic 0.

Password Key Generation. The key generation steps are as follows:

1. collects information on the following items from the user: the choice of the field $\mathbb{F}$, the dimension of the password key vector n, and information for retrieval of the password in case it needs to be retried by filling out a questionnaire;

2. the system uses internally defined high security hash and padding information, possibly involving user specific discrete choices, to generate a password vector $\mathbf{c} \in \mathbb{F}^n$; the user specific discrete choices may be based on the place and time of origin and any other information that the user is able to supply discretely; the information required to retrieve the password in case it is requisitioned by the user is saved in encrypted form by the system, but remains inscrutable by unauthorized means; this information may not always directly lead to retrieval of the original password vector $\mathbf{c}$, but may be useful for resetting the former password and choosing another password for subsequent uses;

3. the system randomly chooses sparse multivariate polynomials $q_i(\mathbf{x})$ with coefficients in $\mathbb{F}$, where $\mathbf{x} = (x_1, \ldots, x_n)$, for $i = 1, \ldots, L$, for some large positive integer L, selected as part of security parameter; the product terms in the sum of products form of $q_i(\mathbf{x})$, for $i = 1, \ldots, L$, may be small in number (which are certainly many more than just one), but are very diverse in their appearance; the authentication polynomials are $P_i(\mathbf{x}) = q_i(\mathbf{x}) - q_i(\mathbf{c})$, for $i = 1, \ldots, L$; thus, $P_i(\mathbf{c}) = 0$, for $i = 1, \ldots, L$;

4. the authentication polynomials $P_i(\mathbf{x})$, for $i = 1, \ldots, L$, together with the information concerning $\mathbb{F}$ and n, are saved in an authentication space accessible by the system and user; since the system itself contains users internal to it, who

may be more privileged than the owner of the password and other external users, the authentication space is considered as a public domain by the system.

Authentication Protocol. The authentication steps are as follows:

1. to gain a fresh access by a user, the system requests the user to enter the password vector $\mathbf{w} \in \mathbb{F}^n$, which the user must oblige;
2. the system tests whether the condition $P_i(\mathbf{w}) = 0$, for $1 \leq i \leq L$, is satisfied, for granting access to the user.

The aspect of transparency in this context is that the authentication space may be visible to – but unmodified by – the environment, along with the authentication test process. But once the authentication step is over, the password vector appears nowhere, except as known to the owner of the password. Thus, the password vector is seen by the system only during authentication test, but this part can be treated as a memoryless operation. If any other user having gained access to the authentication polynomials tries to get the password, then the only available option is to solve these polynomials to find a zero vector. Any zero vector can pass the authentication test, but getting a zero vector from the authentication polynomials is hard.

2.2. Multivariate Polynomial and Exponential Mappings

In this subsection, let $\mathbb{F}$ be a finite field of characteristic p, containing three or more elements. Let G be a subgroup of nonzero elements of $\mathbb{F}$, with $\mathsf{n} \geq 2$ elements. It is preferable that n be not too small, and G be the full group of nonzero elements of $\mathbb{F}$. Let $\mathbb{Z}_{\mathsf{n}}$ be the ring of integers with addition and multiplication $\mathsf{mod}\ \mathsf{n}$. The discussion can indeed be extended to fields of characteristic 0 as well, with $\mathbb{Z}$ in place of $\mathbb{Z}_{\mathsf{n}}$. Let α be a primitive element of G, *i.e.*, $\mathsf{G} = \{\alpha^i \ : \ 0 \leq i \leq \mathsf{n} - 1\}$. If $\mathbb{F}$ is of characteristic 0, then G can chosen to be $\{\alpha^i \ : \ i \in \mathbb{Z}\}$, which is a possibly infinite group, for some $\alpha \in \mathbb{F} \backslash \{0,\ 1\}$. For obtaining a finite group, when the field characteristic is 0, it may be convenient choose $\mathbb{F}$ to be the cyclotomic field, with α as a primitive n-th root of unity, to get a finite group G.

With exponential mappings, the components of the password vector $\mathbf{c}$ and the indeterminate vector $\mathbf{x}$ are elements of $\mathbb{Z}_{\mathsf{n}}$ or $\mathbb{Z}$, as appropriate, and $P_i(\mathbf{x}) = Q_i(\mathbf{x}) - Q_i(\mathbf{c})$, in step 3 in the preceding section, where $Q_i(\mathbf{x}) = \sum_{j=1}^{J_i} \beta_{i,\,j}\alpha^{[q_{i,\,j}(\mathbf{x})]}$, for some positive integer $J_i > 1$, sparse multivariate polynomials $q_{i,\,j}(\mathbf{x})$, with coefficients in $\mathbb{Z}_{\mathsf{n}}$ or $\mathbb{Z}$, as appropriate, but with very diverse terms occurring in them, and nonzero scalars

$\beta_{i,j} \in \mathbb{F}\backslash\{0\}$, for $1 \leq j \leq J_i$ and $1 \leq i \leq L$. The elements $Q_i(\mathbf{c})$ are evaluated in $\mathbb{F}$, and substituted in their respective places.

3. SECURITY ANALYSIS

In this section, the main known methods for solving multivariate polynomials are described.

Zeros of Multivariate Polynomial Mappings. Almost all the methods for solving multivariate polynomial mappings are formulated based on Hilbert's Nullstellensatz. A slight variation is to apply the Euclidean long division algorithm along one particular independent variable, treating the coefficients as the elements of the integral domain of polynomial functions or the field of rational functions in the remaining variables. Some of the prominent methods are found in [2], [4] and [5]. The terms in the given multivariate polynomials are visualized as points in a lattice, whose components are formed by the exponents of the independent variables. The elements in the lattice are somehow ordered, as in a dictionary, but the particular order relation may be vary from algorithm to algorithm. For two polynomials g_1 and g_2, polynomials f_1 and f_2 are found, such that $f_1 g_1 + f_2 g_2 = g_3$, where the dominant term in g_3 is smaller than that in either of g_1 or g_2. The tuple $(f_1, f_2, -1)$ is called the syzygy of (g_1, g_2, g_3). If $s_1 > 2$ and $s_2 > 2$ are the number of terms in the polynomials g_1 and g_2, respectively, then the number of terms in the polynomial g_3 can be as high as $s_1 + s_2 - 2$, which means that the number of terms can grow exponentially in a sequence of derivation steps. The syzygies are used mainly for succinct representation of the derivation steps in the ideal generation process, which allows a trade-off between space and time, avoiding the resulting polynomials to be explicitly stored in the directed acyclic graph of derivation representation, whose nodes contain information of previous nodes, the syzygy in this step, and the dominant term of the resulting polynomial in the ideal. Hence the polynomial g_3 (and -1) itself need not be stored, and the pointers to nodes from where g_1 and g_2 are found, the corresponding syzygy polynomials f_1 and f_2, together with the lattice point (exponent vector) of the dominant term of g_3, are saved in the information in the node corresponding to g_3. The computation path starting from ancestral nodes where the correspondingly previously computed resulting polynomials are explicitly stored down to the nodes where the derivation step is currently applied must be tracked, and the polynomials must be re-evaluated along the path, for each derivation step, when syzygies are used for space-time trade-off. The lengths of the derivation paths, *i.e.*, the number of nodes in the paths, obviously grow at least linearly with the numbers of terms in the polynomials in the ideal generated thus far.

Zeros of Multivariate Polynomial and Exponential Mappings. It is not directly known how to solve multivariate exponential mappings. As an indirect method, $\gamma_{i,j} \in \mathbb{F}$, $1 \leq j \leq J_i$ and $1 \leq i \leq L$, may be chosen, such that $\sum_{j=1}^{J_i} \beta_{i,j}\gamma_{i,j} - Q_{i,j}(\mathbf{c}) = 0$, for $1 \leq i \leq L$, and the multivariate polynomial equations $q_{i,j}(\mathbf{x}) = \log_\alpha(\gamma_{i,j})$ – where $\log_\alpha$ is the discrete logarithm function defined on G with respect to base α – with the additional conditions that $\gamma_{i,j} \in \mathsf{G}$, $1 \leq j \leq J_i$ and $1 \leq i \leq L$, may be attempted to be solved. If G is the group of nonzero elements of a finite field $\mathbb{F}$, the number of possibilities for the sequences of elements $\gamma_{i,j} \in \mathsf{G}$, $1 \leq j \leq J_i$ and $1 \leq i \leq L$, may remain excessively large, which is the main contributory reason for the choice of $\mathbb{F}$ as a finite field, with G as the group of nonzero elements of $\mathbb{F}$.

REFERENCES

[1] S. Akleylek, M. Soysaldı, D. E. Boubiche, and H. Toral-Cruz, “A Novel Method for Polar Form of Any Degree of Multivariate Polynomials with Applications in IoT”, *Sensors*, Special Issue Internet of Things and Machine-to-Machine Communication, 2019 (4)

[2] 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

[3] Ya-Fen Chang, and Chin-Chen Chang, “A Secure and Efficient Strong-Password Authentication Protocol”, *ACM SIGOPS Operating Systems Review*, July 2004

[4] 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

[5] 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

[6] Lein Harn, and Guang Gong, “Conference Key Establishment Protocol using a Multivariate Polynomial and its Applications”, *Security and Communication Networks*, 2014

[7] Moni Naor, and Benny Pinkas, “Oblivious Polynomial Evaluation”, *SIAM Journal on Computing*, 35(5), pp. 1254—1281, 2006

[8] D. Vikram, "An Optimal Strong Password Authentication Protocol with USB Sticks", *IACR Cryptology ePrint*, 2014

[9] Hsien-Chu Wu, Min-Shiang Hwang, and Chia-Hsin Liu, "A Secure Strong-Password Authentication Protocol", *Fundamenta Informaticae*, XXI (2001), pp. 1001—1008

[10] Yan Zhao, Shiming Li, and Liehui Jiang, "Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment", *Security and Communication Networks*, Vol. 2018