Public Key Identification Scheme Based on Quaternion Properties

Massoud Hadian Dehkordi*
Reza Alimoradi**
Mohammad Sabzinejad***

Abstract

Public key cryptosystems are based on the difficulty of solving complicated problems in mathematics. As examples there are Integer Factorization Problem (IFP), Discrete Logarithm Problem (DLP) in finite multiplicative group and Elliptic Curved Discrete Logarithm Problem (ECDLP). More recently, different algorithms have been introduced in order to solve eth problems. These algorithms are exponential and sub-exponential with regard to their complexities. But according to the new research, in the near future, new hardwares and new methods will come to decrease the complexity of solving the problems. Therefore, new difficult problems and their application in public key cryptosystems are being investigated. Identification protocols are one of the much applicable protocols in cryptography. The identification protocol controls the users' entering a system. In this paper, using quaternion numbers, a difficult problem and based on it a new identification scheme will be introduced.

Keywords : Quaternion, Rotation Matrix, Norm, Identification.

1. Introduction

In 1977, using the difficulty of an Integer Factorization Problem, Rivest- Shamir- Adlemane introduced public key cryptosystem of RSA. Also, in 1980, Koblitze and Miller presented a group resulted from the definition of an elliptic curve on a finite field to use in the cryptography. Today, many researches are done to make these problems more difficult and also to solve them more rapidly. Therefore, it is quite logical to look for new difficult problems to use them when needed. In 1843, Hamilton was the first who introduced quaternion numbers, and from then on these numbers were frequently used in different sciences. Various examples of quaternion numbers used in the cryptography are mentioned in [1-3-12-14]. Nagase et.al [13] used the difficult problem of this article to design a public key cryptosystem. This problem has made use of some characteristics of the quaternion numbers and is based on the difficulty of not finding a quaternion number of its rotation matrix. In this article, using this difficult problem, an identification protocol will be introduced. Identification protocols are one of the most important and much applicable protocols in data security field. In an identification protocol, the user (prover) will prove to the other person in the center (the verifier) that s/he is really the same person s/he claims, that is , s/he proves himself to be an allowed user. There are different

*Department of Mathematical Sciences, Iran University of Science and Technology, Narmak, Tehran, Iran
** & *** Research Center of Intelligent Signal Processing, Tehran, Iran

methods for the identification such as passwords, one-time passwords, and challenge-response identification. Methods based on passwords and one-time passwords are more advantageous than other methods in terms of their speed. But the problem is that in these methods, the intruder finds the password long before the real time of identification. Therefore, they are much less secure than the other methods. Challenge-response identification systems don't have this Achill's heels! Supposing that a user wants to introduce him or herself to the other person (the center) according to the challenge-response system; they will do as follows:

- Commitment: the user sends his/her request to the center.
- Challenge: the center asks the user a question.
- Response: the user answers the question using his/her private (hidden) key.
- Verification: the center verifies the user's reply using the same hidden key or its corresponding public key. The center can accept or reject the user's identity.

To do an identification protocol, one can use symmetrical cryptosystems or asymmetrical cryptosystems which are also called public key systems. In case of using symmetrical cryptosystems, the center must know the user's private key to verify him/her. Knowing the genuine user's private key, it is probable that the verifier (the center) misuse it. To solve this problem, one can use public key systems. Challenge-Response systems are based on signature. If the user wants to introduce himself/herself to the center, s/he receives a random number from the center and signs with his/her private key. The center using the user's public key affirms his/her signature and so verifies his/her identity. In this method, the opposite person or the center is not able to misuse. Because the center can only know the amount of the genuine user's public key while for misusing, the private key is also needed. Using public key challenge – response systems has the advantage that the user can prove himself or herself to the center without revealing his/her private data, disclosing which might lead to forging his/her identity. This quality is called zero - knowledge proof [2-17]. For Further information regarding zero – knowledge proof, see [8-9]. Some identification schemes based on famous hard problems are mentioned in [4-5-6-7-11-15-16].

The coming sections of this article will be as follows: in part 2, we will take a look at quaternion numbers. In part 3, an identification scheme based on the quaternion numbers will be introduced which has the characteristic of zero - knowledge proof and the article will end with the conclusion.

2. Preliminaries

The quaternion number q is defined as $q = w + xi + yj + zk$ in which $w, x, y, z \in R$ and the following equations hold:
$i x i = j x j = k x k = -1, i x j = -j x i = k, j x k, j x k = -k x j = i, k x i = -i x k = j$

Of course q is also shown as a quadratic q = (w, x, y, z) ∈ R4. Addition and subtraction and multiplication of two quaternion numbers $q_1 = (w_1, x_1, y_1, z_1)$ and $q_2 = (w_2, x_2, y_2, z_2)$ are defined as:
$q_2 \pm q_1 = (w_2 \pm w_1, x_2 \pm x_1, y_2 \pm y_1, z_2 \pm z_1)$,
$q_1 q_2 = (w_1 w_2 + x_1 x_2 + y_1 y_2 + z_1 z_2) + (w_1 x_2 + w_2 x_1 + y_1 z_2 - y_2 z_1) i + (w_1 y_2 + w_2 y_1 + x_2 z_1 - x_1 z_2) j + (w_1 z_2 + w_2 z_1 + x_1 y_2 - x_2 y_1) k$

Conjugate, norm, and inverse of the quaternion number q are respectively:

$$\bar{q} = (w, -x, -y, -z),\ N(q) = w^2 + x^2 + y^2 + z^2,\ q^{-1} = \frac{\bar{q}}{N(q)} = \frac{(w, -x, -y, -z)}{w^2 + x^2 + y^2 + z^2}.$$

if $N(q) = 1$, then q will be called unit quaternion. The quaternion number q has a Matrix $\Gamma(q)$ as follows:

$$\begin{pmatrix} w^2 + x^2 - y^2 - z^2 & 2xy - 2wz & 2xz + 2wy \\ 2xy + 2wz & w^2 - x^2 + y^2 - z^2 & 2yz - 2wx \\ 2xz - 2wy & 2yz + 2wx & w^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

which is called Rotation Matrix q.

Theorem 1 : If q_1 and q_2 are two quaternion numbers then:

$$N(q q_2) = N(q_1) N(q_2),$$
$$|\Gamma(q_1 q_2)| = |\Gamma(q_1)| \ |\Gamma(q_2)|.$$

Theorem 2 : Having the Matrix $\Gamma(q)$ of the quaternion number $q = (w, x, y, z)$, we can calculate the amount of $N(q)$.

Proof : There are different methods and one will be explained here. Supposing that the rotation Matrix is equal,

$$\Gamma(q) = \begin{pmatrix} w^2 + x^2 - y^2 - z^2 & 2xy - 2wz & 2xz + 2wy \\ 2xy + 2wz & w^2 - x^2 + y^2 - z^2 & 2yz - 2wx \\ 2xz - 2wy & 2yz + 2wx & w^2 - x^2 - y^2 + z^2 \end{pmatrix} = \begin{pmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{pmatrix}$$

then we have :
$q_{22} + q_{11} = w^2 + x^2 - y^2 - z^2 + w^2 - x^2 + y^2 - z^2 = 2(w^2 - z^2)$,
$q_{223} q = 4y^2 z^2 - 4w^2 x^2$,
$q_{311} q = 4x^2 z^2 - 4w^2 y^2$,
$q_{23} q_{32} + q_{31} q_{13} = 4z^2 (x^2 + y^2) - 4w^2 (x^2 + y^2) = 4 (x^2 + y^2) (z^2 - w^2)$,
$\Rightarrow \frac{q_{23} q_{32} + q_{31} q_{13}}{-(q_{22} + q_{11})} = 2(x^2 + y^2)$
$\Rightarrow q_{33} + 2x^2 + 2y^2 = w^2 - x^2 - y^2 + z^2 + 2x^2 + 2y^2 = w^2 + x^2 + y^2 + z^2 = N(q).$ •

For further information regarding the above concepts see [10-18].

3. Our Scheme

In this scheme we require an f function such as a hash function, only all numbers A, B must hold in $f(AB) = F(A) f(B)$. First, we will explain the key production stage. The user chooses the quaternion number q. His private key is the quaternion number q and his public key is matrix $\Gamma(q)$. Finding the user's private key means the amount of q from Matrix $\Gamma(q)$ which is impossible, because the components of q have the desired length. In addition, obviously, finding the amount of the quaternion number q of $N(q)$ $f(|\Gamma(q)|)$ is impossible, because there will be infinite possible amounts. Now the user and the center follow these stages:

1. Commitment: the user randomly chooses the quaternion number X and sends it to the center.
2. Challenge: the center randomly chooses the amounts of d ∈ {1, L, 2^t} and sends them to the user.
3. Response: the user calculates the amount of $Y = X^d q$ and sends the amount of its rotation matrix, i.e. $\Gamma(Y)$, to the center.
4. Verification: the center accepts the user's identity if and only if:

$$N(Y) = N(X^d) N(q) \qquad (1),$$
$$f(|\Gamma(Y)|) = f(|\Gamma(X^d)|) f(|\Gamma(q)|) \qquad (2).$$

Now, we compute necessary computations in our scheme.

Response : d exponentiation and 1 multiplication in quaternion numbers, computing rotation matrix: $\Gamma(Y)$.
Verification: d exponentiation in quaternion numbers, 2 multiplication, computing $N(Y)$ of rotation matrix $\Gamma(Y)$, 3 times computations of $N()$ and $f()$.

Theorem 3 : The represented scheme has the quality of completeness, i.e., the true user at the end of the protocol proves himself/herself to the honest center.

Proof : If the legal user sends the amount of $Y = X^d q$ to the center, then based on the theorem 1 and definition of f, we have :

$$N(Y) = N(X^d q) = \mathrm{N}(X^d) N(q) ,$$

$$f(|\Gamma(Y)|) = f(|\Gamma(X^d q)|) = f(|\Gamma(X^d)||\Gamma(q)|) = f(|\Gamma(X^d)|) f(|\Gamma(q)|) .$$

Consequently the verification will happen.

Theorem 4 : This scheme has the quality of zero-knowledge proof.

Proof: The opposite person (the center) has the information of $\Gamma(q)$ $\Gamma(Y)$, Because finding q, y from $\Gamma(q)$ $\Gamma(Y)$ is impossible. Therefore, the center cannot get the user's private key and consequently, the scheme has the quality of zero-knowledge proof. Pay attention to the fact that if the amount of Y becomes known, then the opposite person (the center) solving the equation $Y = X^d q$ finds the amount of q (the user's private key) and so the protocol's zero – knowledge proof quality will be vanished.

Theorem 5 : Using the equation (2) is necessary in the verification stage.

Proof: Supposing that the cheater knows the amounts of $\Gamma(Y), \Gamma(q), d, X$ and so $N(q)$, $N(X^d)$ then Y' if she can find the quaternion number Y' in a way that its norm be true in the relation $N(Y') = N(X^d) N(q)$ now she can cheat the center in the relation (1) through sending the center the amount of $\Gamma(Y')$ and through the way of choosing Y'. But the center with the equation (2) can prevent the success of this forger. Because this amount will not be true in equation (2). Therefore, because the forger doesn't know the real amount of the quaternion number q, s/he cannot generat the exact amount $Y = X^d q$.

Theorem 6 : The number d sent by the center in challenge stage of the protocols must not be constant.

Proof : If d is stable, the cheater can get the exact amount of $\Gamma(Y)$ which is sent by a legal user and then the cheater can cheat the user when again doing the protocol with the center. Therefore, the random choosing of d can easily prevent this intrusion.

If the intruder can guess the exact amount of d challenge beforehand, then in the identification scheme of Fiat–Shamir [6], the intruder's probability to forge the prover's identity)the legal user) is 1/2. This probability in the identification scheme of Feige – Fiat–Shamir [7], with the security parameter t, and the identification scheme of Schnorr [15] with the security parameter of t is 1/2. This problem is solved in the scheme represented in this article.

Theorem 7 : Even knowing the challenge amount of d, the intruder will not be able to cheat the opposite person (the center).

Proof : With regard to the protocol's structure, in case the intruder knows the challenge amount of d beforehand, s/he must find Y in a way that it equals $X^d q$. But because the intruder doesn't know the amount of q, s/he cannot send the exact amount of $Y = X^d q$

4. Conclusion

The purpose of this article is investigating the probability of designing important public key cryptography protocols using new difficult problems. In this paper a new identification scheme based on the difficult problem of not extracting a quaternion number from rotation matrix is introduced. Of course the difficulty of this new problem must be compared with those of the other previously existing problems such as the discrete logarithm problem. This scheme is of the challenge-response kind and has the quality of zero-knowledge proof.

5. Reference

1. *Anand. R. P. M, Bajpai. G, Bhaskar. V, Real-Time Symmetric Cryptography using Quaternion Julia Set, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.*
2. *Buchmann. J. A, Introduction to Cryptography, Springer-verlag, 2001.*
3. *Coppersmith. D, "Weakness in quaternion signatures", Crypto '99, LNCS 1666, 1999.*
4. *M. H. Dehkordi, , R. Alimoradi, Zero-Knowledge Identification Scheme Based on Weil Pairing, Lobachevskii Journal of Mathematics, Vol. 30, No. 3, 203–207. 2009.*
5. *M. H. Dehkordi, , R. Alimoradi, A NEW BATCH IDENTIFICATION SCHEME, Discrete Mathematics, Algorithms and Applications, Vol. 1, No. 3, 369–376, 2009.*
6. *Feige. U, Fiat. A, Shamir. A, Zero- Knowledge Proofs of Identity, Journal of Cryptology, vol.1, 77-94, 1988.*
7. *Fiat. A, Shamir. A. 1987: How To Prove Yourself: practical solutions of identification and signature problems. In Odlyzko A. M, editor, Advances in Cryptology - Proceedings of CRYPTO' 86, volume 263 of Lecture Notes in Computer Science, pages 186-194, Santa- Barbara, California, Springer- verlag.*
8. *Goldreich. O, 1999: Modern Cryptography, Probabilistic Proofs and Pseudorandomness, Springer-verlag.*
9. *Goldwasser. S, 1989: Micali. S, and Rackoff. C. The Knowledge Complexity of Interactive Proof Systems, SIAM J. Comput., 18 (1):186208.*
10. *Hamilton. W, 1847: On Quaternions Proceedings of the Royal Irish Academy, Nov 11, Vol .3, 1-16.*
11. *M. Kim and K. Kim. A New Identification Scheme Based on the Bilinear Diffie- Hellman Problem. In The 7th Australian Conference on Information Security and Privacy, ACISP 02, pages 362378. Springer-Verlag, 2002.*
12. *Ong. H. , Schnorr. C.P, Shamir. A, "An efficient scheme based on quadratic equations", Proc. 16th ACM Symp. Theory of Computation, 1984.*
13. *Nagase. T, Koide R., Araki. T and Hasegawa. Y. 2004: A new Quadripartite Public Key Cryptosystem. International Saposium on Comonications and Information Technologies 2004, Sapporo, Japan, Octobere 26 - 29, 74 -79.*
14. *Ruseva.D, Security Analysis of Quaternion Signatures, Bachelor Thesis, University of Technology Darmstadt Department of Mathematics, September 2008.*
15. *Schnorr. C. P, 1991: Efficient signature generation by smart cards. Journal of Cryptology, 4, 161-174.*
16. *Shao. J, Lu. R, and Cao. Z, A New Efficient Identification Scheme Based on the Strong Diffie-Hellman Assumption. In International Symposium on Future Software Technology, 2004.*
17. *Stinson. D, Cryptography, CRC Press, Boca Raton, Florida, 2006.*
18. *Zhang F., "Quaternions and Matrices of Quaternions", Linear Algebra and Its Applications, Vol. 251, Issue 1-3, January 1997.*