Article can be accessed online at http://www. publishingindia. com

Application of Quaternion Numbers in Identification Scheme

Reza Alimoradi*

Abstract

The goal of an identification procedure is access control. Methods that permit an identification are called identification protocols. In this paper, first we introduced quaternion numbers. In addition we proposed a new identification scheme based on quaternions. Finally, the security of our scheme is analysed.

Keywords: Identification, Quaternion, Challenge-Response, Zero-Knowledge Proof, Defantiuos Equation.

Introduction

We know that public key cryptography is based on difficult problems of mathematics such as integer factorization problem (IFP), discreet logarithm problem (DLP), Bilinear Diffie- Hellman Problem. Many protocols have been based on these problems (Harn & Ren, 2008; Lee, Kim, Kim, Oh, 2005; Lee, Wu, & Wang, 2008; Meshram, Huang, & Meshram, 2012; Meshram, Meshram, & Zhang, 2012). Besides, some researchers are applying new difficult problems (Dehkordi& Alimoradi, 2010; Okamoto & Pointcheval, 2001; Stakhov, 2007; Su, 2012). In this research, a new problem is introduced and an identification scheme based on this is offered. In this identification protocol, the prover, Alice, proves to the verifier, Bob, that it is really Alice who is communicating with Bob. Now, in this section some methods of identification will introduced (Stinson, 2006).

Types of Identification Protocols

a) Identification with password: Access to Unix or Windows NT is typically controlled by a password system. Each user picks his individual and secret password, w. The computer stores the image f(w) of the password w under a one-way function, f. When the user requests access using his name and password, w, the computer determines f(w) and compares the result with the stored value. If the computed value is equal to the stored one, access is granted. Otherwise the user will be rejected.

b) Challenge-Response Identification: Alice wants to introduce herself to Bob in a challenge-response system:

i. Bob asks a question from Alice (the challenge).

ii. Alice computes the response using her secret key and sends it to Bob (the response).

iii. Bob verifies the response using the same secret key or the corresponding public key (the verification).

Types of Systems Used in Identification

1. A simple challenge-response identification system which uses a symmetric cryptosystem.
2. Challenge-Response systems can also be based on public key signature schemes. In a challenge-response protocol, the prover proves that he knows a secret. If a symmetric cryptosystem is used, then the verifier also knows the secret. If public key crypto system is used, then the verifier does not know the secret (Zero-Knowledge Proof). Currently, most of the zero-knowledge identification protocols are based on integer factorization problem (IFP) or discrete logarithm problem (DLP). Fiat-Shamir (Fiat & Shamir, 1987), Feige-Fiat-Shamir (Feige, Fiat, & Shamir, 1988) and Schnorr (Schnorr, 1991) proto-

* Assistant Professor of Computer Science, Qom University, Iran. Email: alimoradi@iust. ac. ir

cols are some examples for such systems. The security is closely related to the difficulty of finding the factorisation of an integer or discrete logarithm, but it is not really known whether these problems will remain difficult in the future or not. Therefore, we look for a new scheme as an alternative to these systems. For more details concerning zero-knowledge systems, we refer the reader to research by Stakhov (2007).

The scheme we describe in this paper is a zero-knowledge identification protocol based on quaternion. This paper is organised into five sections. In the next section, a brief review of the quaternion numbers and background theories related to above subject would be introduced. In third section, a new scheme would be proposed. In fourth section, the security of our scheme is analysed. Finally, a summary will be given in the last section.

Quaternion Overview

A quaternion number is shown as q = (x1, x2, x3, x4) or q = x1+x2i+x3j+x4k in which ji = −k; kj = −i; ik = −j; ij = k; jk = i; ki = j; i2 = j2 = k2 = −1. The conjugate of the quaternion q = (x1, x2, x3, x4) is expressed as ˜q = (x1, −x2, −x3, −x4).

The norm of the quaternion is defined as N (q) = q ˜q = x21+ x22 + x23 + x24.

The unit quaternion is defined as 1 = (1, 0, 0, 0). The summation and subtraction operations are defined for quaternion numbers q1 = (x1, x2, x3, x4), q2 = (y1, y2, y3, y4) as follows: q1 ± q2 = (x1 ± y1, x2 ± y2, x3 ± y3, x4 ± y4).

The product of q1, q2 is equal to q3 = (z1, z2, z3, z4), in which z1 = x1y1 + x2y2 + x3y3 + x4y4 z2 = x1y2 + x2y1 + x3y4 − x4y3 z3 = x1y3 − x2y4 + x3y1 + x4y2 z4 = x1y4 + x2y3 − x3y2 + x4y1.

Theorem 2. 1: If x and y are quaternion numbers, then we have fx y = ˜y˜x , N (x y) = N (x)N (y).

Proposed Scheme

In this section, we describe a new identification scheme based on quaternion numbers. Some example of public key identification schemes are mentioned in research by Dehkordi and Alimoradi (2009a, 2009b) and Kim and Kim (2002). In key generation stage, Alice generates large random prime number, p.

Alice chooses two quaternion numbers qa, qs such that qs qa mod p _ 1. Alice's public key is {p, qs} and her private key is qa. To obtain the private key, a quaternion congruence equation should be solved, which is very time consuming. In this zero–knowledge scheme, Alice proves to Bob that she knows secret (private key).

1. Commitment: Alice chooses a random quaternion number x = (x1, 0, 0, 0) such that x1 6= 0 and sends x to the verifier, Bob.
2. Challenge: Bob chooses a random number e 2 {0, 1} and sends it to Alice.
3. Response: Alice computes y = qa xe ˜ qa (qa is Alice's private key) and sends it back to Bob. It is noted that since x = (x1 6= 0, 0, 0, 0), hence y = (y1, 0, 0, 0).
4. Verification: Bob accepts Alice's identity if and only if_ qs y ˜ qs mod p _ x, If Bob sent e =1 to Alice. qs y ˜ qs mod p _ 1, If Bob sent e =0 to Alice. Proof:If e = 1 then qs y ˜ qs mod p _ qs qa x ˜ qa ˜ qs mod p _ 1 x (qgsqa) mod p _ x. If e = 0 then y = qa x0 ˜ qa = N (qa), in which x0 = 1.) qs y ˜ qs mod p _ qs N (qa) ˜ qs _ N (qa) qs ˜ qs _ N (qa)N (qs). Since qsqa mod p _ 1 we have: 9k 2 Z 3 qs qa = kp + 1) N (qs qa) = N (kp + 1) N (qs)N (qa) = (kp + 1)2 3 = (kp)2 + 2kp + 1) N (qa)N (qs) mod p = 1 Hence in the case e = 0 , we have qsy ˜ qs mod p _ 1.

Improvement of Scheme

Alice and Bob for increasing security of scheme made some changes in scheme as follows:

1. Commitment: Alice chooses random quaternion numbers xi = (xi1, 0, 0, 0) such that xi1 6= 0 for all 1 _ i _ t then she sends (x1, . . ., xt) to the verifier, Bob.
2. Challenge: Bob chooses random value (e1, . . ., et) 2 {0, 1}t then sends it to Alice.
3. Response: Alice computes yi = qa xi ei ˜ qa mod p for all 1 _ i _ t then sends (y1, . . ., yt) back to Bob. It is noted that since xi = (xi1 6= 0, 0, 0, 0), hence yi = (yi1, 0, 0, 0) for all 1 _ i _ t .
4. Verification: Bob accepts Alice's identity if and only if _ qs yi ˜ qs mod p _ xi, If Bob sent ei = 1 to Alice. qs yi ˜ qs mod p _ 1, If Bob sent ei = 0 to Alice. for all 1 _ i _ t is hold.

Security Analysis

Lemma 4. 1: It is impossible for the verifier, Bob, to obtain the secret, qa (Alice's private key).

Proof: Assume qa = (q1, q2, q3, q4), then we will have:

y = qa xe ˜ qa = (q1, q2, q3, q4) xe (q1, −q2, −q3, −q4).

If e = 0 then

y = qa ˜ qa = N (qa) = q2

1 + q2

2 + q2

3 + q2

4

) y1 = q2

1 + q2

2 + q2

3 + q2

4,

In this case, it is impossible to obtain qa from Diophantine equation.

If e = 1 then

y = qa xe ˜ qa = (qa x1

e ˜ qa, 0, 0, 0)

) y1 = x1N (qa)) N (qa) = y1

x1

.

Also in this case, it is impossible to obtain qa from Diophantine equation.

Lemma 4. 2: Nobody could introduce him/herself as Alice to Bob without having

Alice's private key. In other words, this protocol is resistant to key forgery.

4

Proof: In the verification process, Bob computes qs y ˜ qs. Since the cheater (Oscar)

has used a key different from qa, the value of qs y ˜ qs cannot be equal to x or 1.

So, Bob will not accept the cheater (Oscar).

Conclusion

In this paper, we have introduced a new scheme for identification (zero–knowledge proof) using quaternion numbers, having enough security, not using hash functions, and not being based on IFP and DLP.

References

Dehkordi, M. H., & Alimoradi, R. (2009a). Zero-knowledge identification scheme based on weil pairing. *Lobachevskii Journal of Mathematics*, 30(3), 203-207.

Dehkordi, M. H., & Alimoradi, R. (2009b). A new batch identification scheme. *Discrete Mathematics, Algorithms and Applications*, 1 (3), 369-376.

Dehkordi, M. H., & Alimoradi, R. (2010). Public Key Identification Scheme Based on Quaternion Properties. *IMS Manthan: The Journal of Management, Computer Science & Journalism*, 5 (1), 1-3.

Feige, U., Fiat, A. & Shamir, A. (1988). Zero- Knowledge proofs of identity. *Journal of Cryptology*, 1(2), 77-94.

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, (pp. 186-194). Santa-Barbara, California, Springer- Verlag.

Harn, L., & Ren, J. (2008). *Efficient identity-based RSA multi-signatures computers security*, Elsevier.

Kim, M., & Kim, K. (2002). *A new identification scheme based on the bi-linear Diffie- Hellman problem*. In the 7th Australian Conference on Information Security and Privacy, ACISP 02, (pp. 362-378). Springer-Verlag.

Lee, H., Kim, D., Kim, S., & Oh, H. (2005). *Identity-based key agreement protocols in a multiple PKG environment*. Proceedings of the International Conference on Computational Science and Its Applications,

ICCSA 2005. Lecture Notes in Computer Science, 3483, pp. 877-886.

Lee, N. Y., Wu, C. N., & Wang, C. C. (2008). Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings. *Journal of Computers and Electrical Engineering*, January, 34 (1), 12-20.

Meshram, C., Huang, X., & Meshram, S. A. (2012). Identity-based cryptographic scheme for IFP and DLP based cryptosystem. *International Journal of Pure and Applied Mathematics*, 81 (1), 65-79.

Meshram, C., Meshram, S. A., & Zhang, M. (2012). *ID-based cryptographic mechanisms based on GDLP and IFP*. Information Processing Letters- Elsevier.

Okamoto, T., & Pointcheval, D. (2001). *The gap-problems: A new class of problems for the security of cryptographic schemes, Public Key Cryptography*, Springer.

Schnorr, C. P. (1991). Efficient signature generation by smartcards. *Journal of Cryptology*, 4(3), 161-174.

Stakhov, A. P. (2007). *The golden matrices and a new kind of cryptography, Chaos, Solitons Fractals*, Elsevier.

Stinson, D. (2006). *Cryptogaphy*, CRC Press, Boca Raton, Florida.

Su, S. (2012). *A public key cryptosystem based on three new provable problems, Theoretical Computer Science*, Elsevier.