Symbiosis

www.symbiosisonline.org
www.symbiosisonlinepublishing.com
ISSN Online: 2474-9257

Short Communication | Journal of Computer Science Applications and Information Technology | Open Access

On A Mixed 3-Pass GGH –Quaternion and Braid Group Protocol

Ahmed E*

Mathematics department, Faculty of Science, Mansoura 35516, Egypt

Received: June 07, 2018; Accepted: June 14, 2018; Published: June 25, 2018

***Corresponding author:** Ahmed E, Mathematics department, Faculty of Science, Mansoura 35516, Egypt, E-mail: magd45@yahoo.com*

Abstract

3-pass protocol is generalized to mixed 3-pass GGH Quaternion protocol.

Keywords: 3-pass protocol; Quaternion; GGH cryptography;

Three Pass Protocol [1]

In cryptography, the three-pass protocol for sending messages is a framework which allows one party to securely send a message to a second party without the need to exchange or distribute encryption keys.

It is called the three-pass protocol because the sender and the receiver exchange three encrypted messages. The first three-pass protocol was developed by Adi Shamir circa 1980. The basic concept of the Three-Pass Protocol is that each party has a private encryption key and a private decryption key. The two parties use their keys independently, first to encrypt the message, and then to decrypt the message.

The Three-Pass Protocol works as follows:

i. The sender chooses private encryption key *es* and corresponding decryption key *ds*. The sender encrypts the message m with the key es and sends the encrypted message *E(es,m)* to the receiver.

ii. The receiver chooses a private encryption key er and a corresponding decryption key *dr* and encrypts the first message *E(es,m)* with the key *er* and sends the doubly encrypted message *E(er,E(es,m))* back to the sender.

iii. The sender decrypts the second message with the key *ds.* Because of the commutative property described above *D(ds,E(er,E(es,m)))=E(er,m)* which is the message encrypted with only the receiver's private key. The sender sends this to the receiver.

The receiver can now decrypt the message using the key *dr,* namely *D(dr,E(er,m))=m* the original message.

Notice that all of the operations involving the sender's private keys *es* and *ds* are performed by the sender, and all of the operations involving the receiver's private keys *er* and *dr* are performed by the receiver, so that neither party needs to know the other party's keys.

GGH Cryptography 3-Pass Protocol

GGH cryptography is a part of lattice cryptography which is known to be one of the quantum resistant cryptographies [2]. We propose the following 3-pass GGH algorithm:

A and B agrees on good basis v1, v2,... vn.

A chooses bad basis w1, w2,...,wn and sends the message:

r11w1+r12w2+...+r1nwn+m1v1+m2v2+...+mnvn, (1)

where (m1, m2,...,mn) is the message and (r11, r12,...,r1n) are the perturbation of the message.

B chooses bad basis w'1, w'2,...,w'n and sends back the message:

r11w1+r12w2+...+r1nwn+m1v1+m2v2+...+mnvn+ r'11w'1+r'12w'2+...+r'1nw'n,

A removes her perturbation and send the following message to B:

r'11w'1+r'12w'2+...+r'1nw'n+m1v1+m2v2+...+mnvn,

which B decrypts and gets the correct message.

On a Mixed 3-Pass GGH –Quaternion and Braid Group Protocol

Quaternion [3] can be represented by M=aE+bI+cJ+dK where

$$E = \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$

$$I = \begin{matrix} 0 & -i \\ i & 0 \end{matrix}$$

$$J = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$$

$$K = \begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix}$$

are the Pauli matrices.

 ***Corresponding author email:** magd45@yahoo.com*

The mixed 3-pass GGH Quaternion protocol is to generalize the procedure of the previous sec. as follows:

The message sent is

(m0w0E+m1w1I+m2w2J+m3w3K)+(r0E+r1I+r2J+r3L) (2)

And the rest of the protocol is as above.

Similarly we can propose the mixed 3-pass GGH braid group protocol is to generalize the procedure of the previous sec. as follows:

The message sent is

$\sum\{m(i)w(i)B(i) + r(i)B(i)\}$ (3)

Where {B(i), i=1,2,…,n} are the generators of the braid group [4].

I conclude with the following comment: mixed cryptography may solve the problems of both types included e.g. braid group cryptography may be broken in some cases. This may not be the case when combined with GGH.

References

1. 3-pass protocol. Wikipedia. Available from: https://en.wikipedia.org/wiki/Three-pass_protocol
2. Hoffstein J, Pipher J, Silverman JH. An Introduction to Mathematical Cryptography, Springer. 2014.
3. Pade J. Quantum Mechanics for Pedestrians 2: Applications and Extensions. Springer. 2014.
4. Garber D. Braid Group Cryptography. arXiv:0711.3941. 2008.