Improvements over GGH Using Commutative and Non-Commutative Algebra

Massoud Sokouti
Shahid Beheshti University, Iran

Ali Zakerolhosseini
Shahid Beheshti University, Iran

Babak Sokouti
Biotechnology Research Center, Tabriz University of Medical Sciences, Iran

INTRODUCTION

The Internet, a channel of communication for exchanging data between sender and receiver, is a public place which needs to be protected against intruders, spammers, and malicious attacks. This virtual place is a basis for many applications such as e-/m- commerce (Tan, 2014), e-voting (Chamberlain, 2011), e-banking (Pravettoni, Leotta, Lucchiari, & Misuraca, 2007; Rezai-Rad, Vaezi, & Nattagh, 2012), tele-communications such as tele-EEG (Coates, Clarke, Davison, & Patterson, 2012), wireless networking (Johnson, Green, & Leeson, 2013; Tan, Lee, Lam, & Yoo, 2013; Zakerolhosseini, Sokouti, & Pezeshkian, 2013), and security for smart phones/tablets messaging (Aktas et al., 2013; Black, 2006; Curioso et al., 2005; McCreadie & McGregory, 2005). By growth of networking technology and the number of spies and hackers on the Internet, the insecure channel becomes unsafe for transmitting private data. The encryption, the best way for exchanging data safely and securely, is a security service for providing confidentiality. However, there are two general methods for encryption and decryption of transmitting data which are symmetric and asymmetric cipher algorithms. In the symmetric cipher algorithm, the encryption and decryption processes are done by only one shared key between sender and receiver while in the asymmetric cipher algorithm, the encryption is performed by a public key and the decryption is done by its corresponding private key. Lattice based cryptographies are in the group of public key ciphers which are faster than other versions of public key ciphers. The first lattice based cryptography was invented by Ajtai (Ajtai, 1996). The other two known lattice based ciphers are GGH (Goldreich, Goldwasser, & Halevi, 1997) and NTRU (Hoffstein, Pipher, & Silverman, 1998). This article focuses on major attacks and issues of GGH based on arithmetic matrices and proposes two methods (i.e., C-GGH based on complex number algebra and Q-GGH based on quaternion algebra) for improving the original GGH to encounter the existing attacks and increases the security of this cipher against lattice attacks in low dimensions. GGH is known to consume more memory and performs equally as fast as NTRU while it is implemented, and the interesting topic of this article is focused on improving its memory usage, its speed and strength of the security.

DOI: 10.4018/978-1-4666-5888-2.ch334

BACKGROUND

Lattice based cryptographies, a group of public key ciphers, are faster than other versions of public key ciphers. In 1997, Goldreich, Goldwasser, and Halevi presented a lattice based cryptography based on CVP (Closest vector problem). The security of this cryptosystem is based on the complexity of lattice. The authors of GGH, published challenges for the security parameters of $n = 200, 250, 300, 350, 400$. Nguyen attacked all the challenges except $n = 400$, since the key size was too large (Nguyen, 1999). The public and private keys are $n \times n$ matrices where a vector message with size n can be encrypted. In 1999, Fischlin

and Seifert improved the parameters of GGH (Fischlin & Seifert, 1999). In 2001, Micciancio used Hermite Normal Form (HNF) for improving public key generation to reduce the size of the key (Micciancio, 1999, 2001). In 2003, Paeng et al. represented the polynomial implementation of GGH (Paeng, Jung, & Ha, 2003). In 2009, Pan et al. improved the basic GGH by mixing it with knapsack (Pan, Deng, Jiang, & Tu, 2011). In 2012, Xu et al. presented the cryptanalysis of the proposed GGH by Pan et al (Xu, Hu, Sun, & Wang, 2012). In 2010, Portland et al. improved the basic GGH using Chinese remainder theorem (Plantard, Rose, & Susilo, 2009).

GGH is also more efficient when it is compared to the RSA (Rivest, Shamir, & Adleman, 1978) and ElGamal (ElGamal, 1985) cipher systems, since it uses arithmetic algebra over matrices.

MAIN FOCUS OF THE ARTICLE

Goldreich Goldwasser Halevi (GGH)

The GGH cryptosystem similar to McEliece (Galbrith, 2012), based on CVP and randomized encryption, is one of the NP-hard problems presented in 1997 by Goldreich Goldwasser Halevi (Goldreich et al., 1997) and was crypt-analyzed by Nguyen, P.Q. in 1999 (Nguyen, 1999). The GGH relies on the lattice dimension n ($n > 400$) and the security parameter σ (presenting the difficulty of the CVP) The private key is a secret matrix R and its columns are from a basis of Lattice $L \subset \mathbb{Z}^n$. The parameters of GGH are shown in Table 1. For generating a good basis r one may choose a random matrix r with entries in

$$\left\{-4,-3,-2,-1,0,1,2,3,4\right\}$$

or choose $r = k.I_n + E$ where I_n is $n \times n$ identity matrix, $k > 1$ is a medium sized integer and E is a random matrix with small entries. The public matrix B represents another basis for L .

For generating the public key B from the private key r , a random unimodular matrix U is required

$$B = U.r \tag{1}$$

Table 1. GGH parameters

Parameter	Description	Knowledge
n	Dimension	Public
σ	Security Parameter	Public
r	Integral matrix $n \times n$	Private
B	Integral matric $n \times n$	Public

Now, assuming the message vector as $m \in \mathbb{Z}^n$ and short error vector as e randomly chosen, the cipher matrix c is calculated as follows:

$$c = m.B + e \tag{2}$$

The message space is a set of vectors of length n with entries in

$$\left\{-M,-(M-1),\cdots,-1,0,1,\cdots,M-1,M\right\}$$
$$M \in \mathbb{N}\,.$$

Note that this computation is done over $\mathbb{Z}$. The error vector is chosen to be a random vector of length n with entries in $\left\{-\sigma,\sigma\right\}$ for some $\sigma \in \mathbb{N}$ (typically $\sigma = 3$).

To decrypt this cipher, the CVP should be solved by using a good basis r , to obtain the lattice point $m.B$ close to c .

$$\begin{aligned} &c.r^{-1} = (m.B + e)r^{-1} = m.U.r.r^{-1} + \\ &e.r^{-1} = m.U + e.r^{-1} \in \mathbb{Q}^n \end{aligned} \tag{3}$$

For omitting the term $e.\mathrm{r}^{-1}$, the Babai rounding technique (Babai, 1986) is used to deduce the message matrix m

$$m = m.U.U^{-1} \tag{4}$$

The complexity times related to key generation, encryption and decryption in GGH cryptosystem are shown in Table 2.