ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **10** (2021), no.1, 589–595
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.1.58

A KEY EXCHANGE ALGORITHM WITH BINARY QUADRATIC FORMS TO DESIGN COMPLEX SECURITY FRAMEWORK

K. Vijaya Prasamsa[1], P. Anuradha Kameswari, K. Narasimha Raju, T. Surendra, and D. Mrudula Devi

ABSTRACT. A binary quadratic form $f(x, y)$ is a homogeneous polynomial $f(x, y) = ax^2 + bxy + cy^2$ of degree 2 denoted by (a, b, c) where the coefficients a, b and c are fixed integers and the variables x and y are restricted to integers. A binary quadratic form will possess it's equivalent form by the unimodular substitution. Therefore, computing the unimodular matrix used, from the equivalent form is difficult in general for the binary quadratic forms. This difficulty regarding the unimodular substitutions for computing the equivalent binary quadratic forms is another source for trapdoor functions in Public Key Cryptosystem. In this paper, we described how linear transformations of x and y variables can change one binary quadratic form into other form by a unimodular substitution in the key exchange cryptosystem and proposed a method for recovering the secret key in the key exchange system using binary quadratic forms.

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 94A60, 11T71.

Key words and phrases. Binary Quadratic Forms, Equivalent Form, Unimodular Matrix, Key Exchange.

Submitted: 23.12.2020; *Accepted:* 07.01.2021; *Published:* 24.01.2021.

1. Introduction and Preliminaries

The basic concept of cryptographic algorithm works in combination with a key which can be a number, word, or phrase to encrypt the plain text to cipher text. A cryptographic algorithm with all possible public and private keys and all the protocols which make it work comprise a cryptosystem. A number of cryptosystems have been proposed to maintain the security of the message. The security is maintained by using trapdoor or one-way functions in public key cryptography. In this paper, the importance and use of binary quadratic forms by the receiver and sender in establishing a secret shared key is discussed and going in line with Harry Yosh, paper [6], we adapted operators with some parameters and a method for recovering the secret key by the sender and recipient using the binary quadratic forms is proposed. This method is based on the difficulty of computing the unimodular matrices from the equivalent form [3, 4].

Binary Quadratic Forms: A binary quadratic form $f(x, y)$ is a homogeneous polynomial $f(x, y) = ax^2 + bxy + cy^2$ of degree 2 denoted by (a, b, c) where the coefficients a, b and c are fixed integers and the variables x and y are restricted to integers. A binary quadratic form (a, b, c) is said to be primitive if $\gcd(a, b, c) = 1$ otherwise non primitive, [1].

Definition 1.1. *[2] The discriminant of a binary quadratic form $f = (a, b, c)$ denoted as 'd' is defined to be the value $d = b^2 - 4ac$.*

Definition 1.2. *[5] A binary quadratic form $f(x, y) = (a, b, c)$ is said to be equivalent to $g(x, y)$ if there exists a unimodular matrix $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \epsilon SL_2\mathbb{Z}$ such that:*

$$\begin{aligned} g(x, y) &= f \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= f(px + qy, rx + sy) \\ &= \left(ap^2 + bpr + cr^2, 2apq + b(ps + rq) + 2crs, aq^2 + bqs + cs^2\right). \end{aligned}$$

2. Proposed Key Exchange Scheme

In this section we introduce a key exchange protocol using binary quadratic forms as follows [7–9].

a. Recipient sets a random binary quadratic form $f(x,y)$ of a randomdiscriminant 'd' witha random unimodular matrix $S = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \epsilon SL_2\mathbb{Z}$ The binary quadratic form $f(x,y)$ is the public key and S is the private key.

b. The sender sets an equivalent binary quadratic form $g = g(x,y) = (a,b,c)$ of $f(x,y)$ using his choice of unimodular matrix S_1 and constructs a public key using the operator $T_{[p_i,q_i,r_i}$ for $i = 1,2,\ldots,m$ to the polynomials say, F,G,H with n coefficients each, given as:

$$\begin{aligned} T_{[p_i,q_i,ri]}(F,G,H) &= \left(T_{[p_i]}(F), T_{[q_i]}(G), T_{[r_i]}(H)\right) \\ &= \left(T_{[p_1,p_2,p_3,p_4,\ldots,p_m]}(F), T_{[q_1,q_2,q_3,q_4,\ldots,q_m]}(G), T_{[r_1,r_2,r_3,r_4,\ldots,r_m]}(H)\right) \\ &= ((((F+p_1)\,p_2+p_3)\,p_4+\ldots)\,p_m, (((G+q_1)\,q_2+q_3)\,q_4+\ldots)\,q_m \\ &\quad (((H+r_1)\,r_2+r_3)\,r_4+\ldots)\,r_m) \end{aligned}$$

where the choice of ' m ' parameters p_i, sq_i ' s and r_i 's of each polynomial are composite numbers such that $m > n$.

Then the sender applies this operator to $g[S] = (ap^2+bpr+cr^2, 2apq+b(ps+rq) +2crs, aq^2+bqs+cs^2)$ with his choice of any number of parameters, $m > 3$ for some random $S = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2\mathbb{Z}$ and obtains $h(S) = (a_h, b_h, c_h)$ i.e.

$$\begin{aligned} & T_{[p_i,q_i,r_i]}(g[S]) = T_{[p_i,q_i,r_i]}\left(ap^2+bpr+cr^2, 2apq+b(ps+rq)+2crs, aq^2+\right. \\ & \left. bqs+cs^2\right) \\ = \; & \left(T_{[p_i]}\left(ap^2+bpr+cr^2\right), T_{[q_i]}(2apq+b(ps+rq)+2crs), T_{[r_i]}\left(aq^2+\right.\right. \\ & \left.\left. bqs+cs^2\right)\right) \\ = \; & \left(T_{[p_1,p_2,p_3,p_4,\ldots,p_m]}\left(ap^2+bpr+cr^2\right), T_{[q_1,q_2,q_3,q_4,\ldots,q_m]}(2apq+b(ps+rq)+\right. \\ & \left. 2crs), T_{[r_1,r_2,r_3,r_4,\ldots,r_m]}\left(aq^2+bqs+cs^2\right)\right) \\ = \; & \left(\left(\left(\left(ap^2+bpr+cr^2+p_1\right)p_2+p_3\right)p_4+\ldots\right)p_m, (((2apq+b(ps+rq)+\right. \\ & \left. 2crs+q_1)\,q_2+q_3)\,q_4+\ldots)\,q_m, \left(\left(\left(aq^2+bqs+cs^2+r_1\right)r_2+r_3\right)r_4+\ldots\right)r_m\right) \\ = \; & (a_h,b_h,c_h) = h(S) \end{aligned}$$

The sender makes $g = (a,b,c)$ and $h(S)$ public.

a. The Recipient evaluates $g^*[S] = (a^*, b^*, c^*)$ and $h^*(S) = (a_h^*, b_h^*, c_h^*)$ for his choice of $S = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2\mathbb{Z}$ and makes $h^*(S)$ public and $g^*[S]$ as private keys.

b. The sender recovers the binary quadratic form $g^*[S]$ from $h^*(S)$ by applying the inverse operator T^{-1} to $h^*(S)$ given by,

$$\begin{aligned} T^{-1}_{[p_i,q_i,r_i]}\left(h^*(S)\right) &= \left(T^{-1}_{[p_1,p_2,p_3,p_4,\ldots,p_m]}\left(a_h^*\right), T^{-1}_{[q_1,q_2,q_3,q_4,\ldots,q_m]}\left(b_h^*\right) T^{-1}_{[r_1,r_2,r_3,r_4,\ldots,r_m]}\left(c_h^*\right)\right) \\ &= \left(\left(\left((a_h^*)\,\frac{1}{p_m} - \cdots\right)\frac{1}{p_4} - p_3\right)\frac{1}{p_2} - p_1, , \right. \\ &\quad \left(\left((b_h^*)\,\frac{1}{q_m} - \cdots\right)\frac{1}{q_4} - q_3\right)\frac{1}{q_2} - q_1, \\ &\quad \left.\left(\left((c_h^*)\,\frac{1}{r_m} - \ldots\right)\frac{1}{r_4} - r_3\right)\frac{1}{r_2} - r_1\right) \\ &= (a^*, b^*, c^*) = g^*[S] \end{aligned}$$

Thus the sender and the recipient uses the secret key $g^*[S]$ as a key exchange.

Note: Finding the parameters can be made difficult by choosing composite parameters for $T_{[p_1,\ldots,p_n;q_1,\ldots,q_n;r_1,\ldots,r_n]}$ such that $n \geq 4$ As for each public key is of the form $(f(p,r), 2apq + b(ps + rq) + 2crs, f(q,s))$ and the polynomials in p, q, r, s are with only four coefficients each equating to polynomials expressed in terms of p_i, s, q_i, s, r_i, s as variables, hence $p_i, s, q_i s, r_i, s$ cannot be evaluated from this system of four equations for $n \geq 4$

3. Algorithm to compute: $T^{-1}_{[p_i,q_i]}\left(h^*(S)\right)$

Step1: Start

Step2: Input $h^*(S) = (a_h^*, b_h^*, c_h^*)$

Step3: Input $p_1, p_2, ..p_m, q_1, q_2, \ldots q_m, r_1, r_2, \ldots r_m$

Step4: Compute:

$$\begin{aligned} T^{-1}_{[p_1,p_2,\ldots,p_m]}\left(a_h^*\right) &= \left(\left((a_h^*)\,\tfrac{1}{p_m} - \ldots\right)\tfrac{1}{p_4} - p_3\right)\tfrac{1}{p_2} - p_1 = a^* \\ T^{-1}_{[q_1,q_2,\ldots,q_m]}\left(b_h^*\right) &= \left(\left((b_h^*)\,\tfrac{1}{q_m} - \ldots\right)\tfrac{1}{q_4} - q_3\right)\tfrac{1}{q_2} - q_1 = b^* \\ T^{-1}_{[r_1,r_2,\ldots,r_m]}\left(c_h^*\right) &= \left(\left((c_h^*)\,\tfrac{1}{r_m} - \ldots\right)\tfrac{1}{r_4} - r_3\right)\tfrac{1}{r_2} - r_1 = c^* \end{aligned}$$

Step5: Output $T^{-1}_{[p_i,q_i,r_i]}\left(h^*(S)\right) = (a^*, b^*, c^*)$
Step6: Stop.

4. Illustration of Proposed Key Technique

The key exchange protocol begins from the recipient side. The recipient chooses a random binary quadratic form $f = (30, 48, 24)$ and a unimodular matrix $S = \begin{pmatrix} 7 & 5 \\ 11 & 8 \end{pmatrix} \in SL_2\mathbb{Z}$ and makes f as public. Sender receives f and finds $g = f[s_1]$ for his choice of $S_1 = \begin{pmatrix} 3 & 7 \\ -4 & -9 \end{pmatrix} \in SL_2\mathbb{Z}$. Hence, $g = (78, 348, 390)$ say $(\mathrm{a}, \mathrm{b}, \mathrm{c})$. Now for a random $S = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2\mathbb{Z}$ and $\mathrm{m} = 6$, let $p_1 = 6, p_2 = 21$

$$\begin{aligned} p_3 &= 15, p_4 = 12, p_5 = 14, p_6 = 18, q_1 = 8, q_2 = 36, q_3 = 22, q_4 = 35, q_5 = 18, , q_6 \\ &= 10, r_1 = 24, r_2 = 18, r_3 = 28, r_4 = 30, r_5 = 33, r_6 = 16 \end{aligned}$$

$$\begin{aligned} h(S) &= T_{[p_i,q_i,r_i]}(g[S]) \\ &= T_{[p_i,q_i,r_i]}\left(ap^2 + bpr + cr^2, 2apq + b(ps + rq) + 2crs\right. \\ &= \left(T_{[p_i]}\left(ap^2 + bpr + cr^2\right), T_{[q_i]}(2apq + b(ps + rq) + 2crs), T_{[r_i]}\left(aq^2+\right.\right. \\ &= \left(T_{[p_1,p_2,p_3,p_4,p_5,p_6]}\left(ap^2 + bpr + cr^2\right), T_{[q_1,q_2,q_3,q_4,q_5,q_6]}(2apq + b(ps + rq)+\right. \\ &\quad \left.\left. bqs + cs^2\right)\right) 2crs), T_{[r_1,r_2,r_3,r_4,r_5,r_6]}\left(aq^2 + bqs + cs^2\right)\Big) \\ &= \Big(\Big(\Big(\Big(ap^2 + bpr + cr^2 + p_1\Big) p_2 + p_3\Big) p_4 + p_5\Big) p_6, (((2apq + b(ps + rq)+ \\ &\quad 2crs + q_1) q_2 + q_3) q_4 + q_5) q_6, \Big(\Big(aq^2 + bqs + cs^2 + r_1\Big) r_2 + r_3\Big) r_4 + r_5\Big) r_6\Big) \\ &= \Big(\Big(\Big(\Big(78p^2 + 348pr + 390r^2 + 6\Big) 21 + 15\Big) 12 + 14\Big) 18, (((156pq+ \\ &\quad 348(ps + rq) + 780rs + 8)36 + 22)35 + 18)10, \\ &\quad \Big(\Big(\Big(78q^2 + 348qs + 390s^2 + 24\Big) 18 + 28\Big)30 + 33)16\Big) \\ &= \left(353808p^2 + 1578528pr + 1769040r^2 + 30708, 1965600pq + 4384800(ps + rq)\right. \\ &\quad \left.+9828000rsrs + 108680, 673920q^2 + 3006720qs + 3369600s^2 + 221328\right) \\ &= (a_h, b_h, c_h), \text{ say} \end{aligned}$$

The sender makes $g = (78, 348, 390)$ and $h(S)$ public, keeping the parameters $p_i's$ and $q_i's$ of the operator secret. The Recipient evaluates $g^*[S] = (a^*, b^*, c^*)$ and $h^*(S) = (a_h^*, b_h^*, c_h^*)$ for his choice of $S = \begin{pmatrix} 7 & 5 \\ 11 & 8 \end{pmatrix} \epsilon SL_2\mathbb{Z}$ as follows: $g^*[S] = (77808, 112728, 40830) = (a^*, b^*, c^*)$ and

$$h^*(S) = (352967796, 1420481480, 352992528) = (a_h^*, b_h^*, c_h^*) \text{ and makes}$$
$$h^*(S) = (352967796, 1420481480, 352992528)$$

public keeping $g^*[S] = (77808, 112728, 40830)$ as secret key.

Using the inverse operator T^{-1}, the sender computes the value of $g^*[S]$ as follows:

$$\begin{aligned}
T^{-1}_{[p_i,q_i,r_i]}(h^*(S)) &= \left(T_{[p_1,p_2,p_3,p_4,p_5,p_6]}(a_h^*), T^{-1}_{[q_1,q_2,q_3,q_4,q_5,q_6]}(b_h^*), T^{-1}_{[r_1,r_2,r_3,r_4,r_5,r_6]}(c_h^*)\right) \\
&= \left(\left(\left((a_h^*)\frac{1}{p_6} - p_5\right)\frac{1}{p_4} - p_3\right)\frac{1}{p_2} - p_1,\right. \\
&\quad \left(\left((b_h^*)\frac{1}{q_6} - q_5\right)\frac{1}{q_4} - q_3\right)\frac{1}{q_2} - q_1, \\
&\quad \left.\left(\left((c_h^*)\frac{1}{r_6} - \ r_5\right)\frac{1}{r_4} - r_3\right)\frac{1}{r_2} - r_1\right) \\
&= \left(\left(\left((352967796)\frac{1}{18} - 14\right)\frac{1}{12} - 15\right)\frac{1}{21} - 6,\right. \\
&\quad \left(\left((1420481480)\frac{1}{10} - 18\right)\frac{1}{35} - \ 22)\ \frac{1}{36} - 8, \right. \\
&\quad \left.\left(\left((352992528)\frac{1}{16} - 33\right)\frac{1}{30} - 28\right)\frac{1}{18} - 24\right) \\
&= (77808, 112728, 40830) = (a^*, b^*, c^*) = g^*[S]
\end{aligned}$$

Thus, the sender could recover the value of $g^*\left[\begin{pmatrix} 7 & 5 \\ 11 & 8 \end{pmatrix}\right]$ which can be used as the secret key.

5. Conclusion

In this key exchange protocol based on binary quadratic forms proposed by us, the key exchange is an equivalent form of a binary quadratic form which is a public key. The equivalent form computation involves finding the unimodular

matrix from an infinitely many possibilities. The equivalent form is computed by both the parties through the operators based on some parameters and finding the parameters also can be made difficult by choosing the number of parameters $'n'$ such that $n \geq 4$. An Algorithm for applying the parameters on binary quadratic forms is also given.

REFERENCES

[1] I. NIVEN, H. S. ZUCKERMAN, H. L. MONTGOMERY: *An Introduction to The Theory of Numbers*, Fifth Edition, John Wiley and Sons, Inc., 2008.

[2] A. BAKER: *A Coprehensive Course in Number Theory*, Cambridge university press, 2012.

[3] K. H. ROSEN: *Elementary Number Theory and Its Applictions*, Addison Wesley, 1993.

[4] N. KOBLITZ: *A course in Number Theory and Cryptography*, Springer-Verlag, 1994.

[5] R. L. SHEPHERD: *Binary Quadratic Forms and Genus Theory*, The University of North Caarolina, 2013.

[6] H. YOSH: *The Key exchange cryptosytem used with higher order Diophantine equations*, 2011, DOI:10.5121/IJNSA.2011.3204, Corpus ID:7736536.

[7] P. ANURADHA KAMESWARI, L. PRAVEEN KUMAR: *A Method for Recovering a Key in the Key Exchange Cryptosystem by Diophantine Equations*, International Journal of Computer Applications, **100**(14) (2014), 4pages.

[8] P. SMITH: *LUC Public Key Encryptiona Secure Alternative to RSA*, DR. Dobbs Journal, **18**(1) (1993), 44-49.

[9] W. STALLINGS: *Cryptography and Network security*, Principles and practices, pearson Education india, 2006.

DEPARTMENT OF MATHEMATICS, VIGNAN'S INSTITUTE OF INFORMATION TECHNOLOGY
VISAKHAPATNAM, A.P, INDIA

DEPARTMENT OF MATHEMATICS, ANDHRA UNIVERSITY, A.P, INDIA

DEPARTMENT OF CSE, LENDIR INSTITUTE OF INFORMATION TECHNOLOGY
VIZIANAGRAM, A.P INDIA

DEPARTMENT OF MATHEMATICS, GITAM UNIVERSITY
VISAKHAPATNAM, AP, INDIA

DEPARTMENT OF MATHEMATICS, VIGNAN'S INSTITUTE OF INFORMATION TECHNOLOGY
VISAKHAPATNAM, A.P, INDIA