ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.6, 2799–2806
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.6.8

AN APPLICATION OF LINEAR DIOPHANTINE EQUATIONS TO CRYPTOGRAPHY

P. Anuradha Kameswari[1], S.S. Sriniasarao, and Aweke Belay

ABSTRACT. In this chapter we propose a Key exchange protocol based on a random solution of linear Diophantine equation in n variables, where the considered linear Diophantine equation satisfies the condition for existence of infinitely many solutions. Also the crypt analysis of the protocol is analysed.

1. INTRODUCTION

Public key Cryptography is quite useful in developing key exchange protocol for classical Cryptosystem. These protocols are based on hard computational problems, like factorization, discrete logarithm and evaluating short vector in lattices. A protocol based on Diophantine equation was proposed by Lin Chang, Lie in 1995, which was proved to be insecure in cusick. Hary yosh in [5] proposed a protocol based on solutions of non linear Diophantine equations and certain operators, whose security is based on the hardness to find solution to the equation. This protocol was adapted in paper [9] by using pell equation and elliptic curves. In paper [7] the efficiency of the protocol by Hary yosh was analyzed and suggested for security and efficiency that n, the number of variables in

[1]*corresponding author*

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

Key words and phrases. Diophantine equation, key exchange.

Submitted: 11.05.2021; *Accepted:* 26.05.2021; *Published:* 10.06.2021.

the polynomial are to be such that $n \geq 3$ and noted that the key exchange based on m parameters used for the operators may be evaluated with the knowledge of the $2m$ solutions of the Diophantine equation considered leading to breaking of the protocol. In this paper we propose a key exchange protocol with solutions of linear Diophantine equation with n variables, based on a random solution and controlled by a bijective operator depending on a set of parameters, where evaluation of the parameters is hard.

2. Linear Diophantine equations in n variables for $n > 2$

In [2, 7] the study of solutions of linear Diophantine equations with two variables is extended to n variables for $n > 2$. The existence of solutions is based on a relation between greatest common divisor of all the coefficients and the constant coefficient of the given Linear Diophantine equation. In this section we define Diophantine equation in n variables for $n > 2$ and recall the theorems as in [2, 7] on the conditions for existence of solutions for these equations and the possibility for existence of infinitely solutions for these equations.

Definition 2.1. *Let $n > 2$ a linear Diophantine equations in n variables is an equation of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ where a_i are all integers for all $i = 1, 2, \ldots, n$ and $x_1, x_2, \ldots, x_n$ are unknowns.*

To describe condition for the existence of solutions of the above Diophantine equation in n variables for $n > 2$ we compute the $gcd(a_1, a_2, \ldots, a_n)$ for $n > 2$ from the following theorem.

Theorem 2.1. *Given integers $a_1, a_2, \ldots, a_n$, $n > 2$ we have*

$$gcd(a_1, a_2, \ldots, a_n) = gcd(a_1a_2 \ldots a_{n-2},\ gcd(a_{n-1}, a_n)).$$

Now in the following theorem the solutions of Diophantine equation of n variables are expressed as solutions of system of two equations one in $(n-1)$ variables and other in two variables.

Theorem 2.2. *Let $a_1, a_2, \ldots, a_n$ be n integers for $n > 2$ then for $e = gcd(a_{n-1}, a_n)$, the set of solutions of the equation in n variables $a_1x_1 + a_2x_2 + \ldots a_nx_n = b$ is same*

as the set of solutions of the system of two equations in $n+1$ *variables*

$$\begin{cases} a_1x_1 + a_2x_2 + \dots a_{n-2}x_{n-2} + ex_{n+1} = b \\ a_{n-1}x_{n-1} + a_nx_n - ex_{n+1} = 0 \end{cases}.$$

In the following theorem we have the condition for the existence of solutions of the linear Diophantine equation with n variables for $n \geq 2$ basing on the gcd of the coefficients.

Theorem 2.3. *The equation* $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$ *has integer solutions if and only if* $gcd(a_1, a_2, \dots, a_n)$ *divides* b

Now in the following theorem we have the condition for linear Diophantine equations of n variables with $n > 2$ to have infinitely many solutions.

Theorem 2.4. *Let* $n \geq 2$ *if* $gcd(a_1, a_2, \dots a_n)$ *divides* b *then the Diophantine equation* $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$ *has infinitely many solutions. m*

3. The key exchange protocol with solution of linear Diophantine equation with n variables

In this section we construct a Key Exchange protocol based on solution of linear diophantine equation with n variables.

The key exchange protocol is given in the following steps.

Step 1: Public Key Generation by Sender

- The sender considers a linear Diophantine equation $g(x_1x_2 \dots x_n)$ and using the parameters p_i, q_i with $p_i \geq 0$ $q_i > 0$ $\forall i = 1, 2, \dots m$ considers the operator on the Diophantine equation given as for $T_i = T_{[p_i,q_i]}(g) = (g + p_i)q_i$.
- The sender generates the public key by taking key as $T = T_moT_{m-1}o \dots oT_1$ and computes $T(g)$ as

$$\begin{aligned} T(g) &= T_m.T_{m-1} \dots T_1(g(x_1x_2 \dots x_n)) \\ &= (((g(x_1x_2 \dots x_n) + p_1)q_1 + p_2)q_2 \dots + p_m)q_m \\ &= h(x_1x_2 \dots x_n). \end{aligned}$$

- The sender makes the Diophantine equations $h(x_1x_2 \dots x_n)$ and $g(x_1x_2 \dots x_n)$ public.

Step 2: Public Key and Private Key Generation by Recipient

- The recipient considers a linear Diophantine equation $f(x_1x_2\ldots x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ in n variables for $n > 2$ such that $gcd(a_1, a_2, \ldots, a_n)$ divides b and selects a random solution $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of the linear Diophantine equation $f(x_1x_2\ldots x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$.
- The recipient on receiving the public key Diophantine equations evaluates $h(x_1x_2\ldots x_n)$ and $g(x_1x_2\ldots x_n)$ evaluates $h(\alpha_1\alpha_2\ldots\alpha_n) = u$(say), $g(\alpha_1\alpha_2\ldots\alpha_n) = v$(say).
- The recipient keeps the evaluated value v as secret key and makes u public key.

Step 3: Private Key Recovery by the Sender

- The sender recovers the secret key v from public key u by applying the inverse of operators T_i where for T_i we have $T_i^{-1} = T_{[p_i,q_i]}^{-1}$, with $T_{[p_i,q_i]}^{h} = (h)\frac{1}{q_i} - p_i$.
- Sender from T_i^{-1} the inverse of T_i recovers v from u by

$$\begin{aligned}(T_m \circ T_{m-1}\ldots T_1)^1(u) &= T_1^{-1}T_2^{-1}\ldots T_{m-1}^{-1} \circ T_m^{-1} \\ &= ((u)\frac{1}{q_m} - p_m)\ldots\frac{1}{q_1} - p_1.\end{aligned}$$

Step 4: Key Exchange

The secret key evaluated by both sender and receiver $g(\alpha_1\alpha_2\ldots\alpha_n) = v$ can be used as the key for key exchange.

Example 1. *The sender considers a linear Diophantine equation* $g(x_1, x_2, x_3) = 2x_1 + 7x_2 + 5x_3 - 2$ *and constructs the public key* $h(x_1, x_2, x_3)$ *using the operators* $T_1 = T_{[3,2]}, T_2 = T_{[4,5]}$

$$\begin{aligned}h(x_1, x_2, x_3) &= T_2 \circ T_1(g(x_1, x_2, x_3)) \\ &= T_2 \circ T_1(2x_1 + 7x_2 + 5x_3 - 2) \\ &= T_{[4,5]}.T_{[3,2]}(2x_1 + 7x_2 + 5x_3 - 2) \\ &= T_{[4,5]}.((2x_1 + 7x_2 + 5x_3 - 2 + 3).2) \\ &= ((4x_1 + 14x_2 + 10x_3 + 2) + 4)5\end{aligned}$$

i.e. $h(x_1, x_2, x_3) = 20x_1 + 70x_2 + 50x_3 + 30$.

Sender makes

$$\begin{cases} 2x_1 + 7x_2 + 5x_3 - 2 \\ 20x_1 + 70x_2 + 50x_3 + 30 \end{cases}$$

public.

Recipient considers the linear Diophantine equation $f(x_1, x_2, x_3) = 3x_1 + 7x_2 + 4x_3 - 5$ *picks a solution* $(\alpha_1, \alpha_2, \alpha_3) = (-2, 1, 1)$ *and keeps it private.*

Recipient evaluates

$$\begin{aligned} h(\alpha_1, \alpha_2, \alpha_3) &= 20(-2) + 70(1) + 50(1) + 30 \\ &= -40 + 70 + 50 + 30 \\ &= 110 \end{aligned}$$

$$\begin{aligned} g(\alpha_1, \alpha_2, \alpha_3) &= 2(-2) + 7(1) + 5(1) - 2 \\ &= -4 + 7 + 5 - 2 \\ &= 6 \end{aligned}$$

Recipient now keeps $v = g(\alpha_1, \alpha_2, \alpha_3) = 6$ *as secret key, makes* $u = h(\alpha_1, \alpha_2, \alpha_3) = 110$ *as public key.*

Sender recovers secrete key v *from the private key* $h(\alpha_1\alpha_2\alpha_3)$ *by applying*

$$\begin{aligned} (T_2 \circ T_1)^{-1}(h(\alpha_1\alpha_2\alpha_3)) &= T_1^{-1} \circ T_2^{-1}(h(\alpha_1\alpha_2\alpha_3)) \\ &= T_{[3,2]}^{-1} \circ T_{[4,5]}^{-1}(110) \\ &= T_{[3,2]}^{-1}((110)\frac{1}{5} - 4) \\ &= T_{[3,2]}^{-1}(18) \\ &= (18)\frac{1}{2} - 3 \\ &= 6 \\ &= v \end{aligned}$$

Therefore the common secrete key $v = 6$ *can be used as a key exchange.*

Proposition 3.1. *The proposed protocol is a cryptosystem.*

Proof. The proposed protocol is a cryptosystem with the tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ given as $\mathcal{P} = \mathbb{Z}$, $\mathcal{C} = \mathbb{Z}$, $\mathcal{K} = \{f : f = a_1x_1 + a_2x_2 + \cdots + a_nx_n - b, a_i \in \mathbb{Z}$ for all $i =$

$1, 2, \ldots, n\}$, $\mathcal{E} = \{T(g)(\alpha_f) : f, g \in \mathcal{K},\ \alpha_f = (\alpha_1, \alpha_2, \ldots \alpha_n)$ with $f(\alpha_f) = 0\}$ and $\mathcal{D} = \{T^{-1}(h(\alpha_f)) : f, g \in \mathcal{K}, h = T(g), \alpha_f = (\alpha_1, \alpha_2, \ldots \alpha_n)$ with $f(\alpha_f) = 0\}$.

Further note the integer plain texts which are functional values $g(\alpha_f)$ are encrypted and is recovered from public key $h(\alpha_f) = u$ by decryption with operators as follows: $T^{-1}(h(\alpha_f)) = T^{-1}(T(g))(\alpha_f) = T^{-1}oT(g(\alpha_f)) = g(\alpha_f)$. □

3.1. **Cryptanalysis.** To compute the common secret key either α_f or the 2m parameters p_i, q_i for all $i = 1, 2, \ldots, m$ are required. The difficulty of computing these with the public data is discussed in the following propositions.

Proposition 3.2. *Infeasible to compute α_f with the public data for $n > 1$.*

Proof. The considered Diophantine equation has n number of variables n and the solution α_f is to be evaluated only from the two equations available as public data given as $h(\alpha_1\alpha_2 \ldots \alpha_n) = u$, $g(\alpha_1\alpha_2 \ldots \alpha_n)$. Now as α_f is any solution of $f(x_1x_2 \ldots x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ in n variables where $gcd(a_1, a_2, \ldots, a_n)$ divides b, there are infinite possible values for $(x_1x_2 \ldots x_n)$ so finding the choosen value α_f from the equation $h(\alpha_1\alpha_2 \ldots \alpha_n) = u$ is hard for $n > 1$. □

Proposition 3.3. *Infeasible to compute the 2m parameters for $2m > n + 1$.*

Proof. We have

$$\begin{aligned} h(x_1x_2 \ldots x_n) &= T_m.T_{m-1} \ldots T_1(g(x_1x_2 \ldots x_n)) \\ &= (((g(x_1x_2 \ldots x_n) + p_1)q_1 + p_2)q_2 \ldots + p_m)q_m. \end{aligned}$$

Now if $h(x_1x_2 \ldots x_n) = b_1x_1 + b_2x_2 + \ldots + b_nx_n = c$, note each of the n coefficients of the polynomial h gives an equation in the $2m$ parameter variables $p_1 \ldots p_m$ and $q_1 \ldots q_m$, given as

$$C_i(p_1p_2 \ldots p_m, q_1q_2 \ldots q_m) = b_i \text{ for all } i = 1, 2 \ldots n.$$

Now note as there are n variables and a constant in h, we have a system of $n+1$ equations in the parameter variables $p_1 \ldots p_m$ and $q_1 \ldots q_m$ and for $2m > n + 1$, there are infinitely many solutions, therefore finding the chosen 2m parameters from these solutions is difficult. □

Proposition 3.4. *The protocol may be used with same $f(x_1x_2 \ldots x_n)$ and α_f for at most n-2 times.*

Proof. The protocol if used with same $f(x_1x_2\dots x_n)$ and α_f then for each usage with different parameters the middle man gets a new equation $h_i(\alpha_1\alpha_2\dots\alpha_n) = u_i$ for each turn i from the public data $h(\alpha_1\alpha_2\dots\alpha_n) = u$, so after n-1 turns, there is a n system of equations in $(x_1x_2\dots x_n)$, which may be solved for the common solution $(\alpha_1,\alpha_2\dots\alpha_n) = \alpha_f$, therefore the protocol may be used with same $f(x_1x_2\dots x_n)$ and α_f for at most $n-2$ times. □

4. Conclusion

In this paper we studied the condition for existence of solutions of Linear Diophantine equations and proposed a key exchange. We proposed the Key exchange using a linear Diophantine equation $g(x_1,x_2\dots,x_n)$ and generated a public key $h(x_1,x_2\dots,x_n)$ applying some bijective operators on $g(x_1,x_2\dots,x_n)$, then a linear Diophantine equation $f(x_1,x_2\dots,x_n)$ with gcd of its coefficients dividing the constant coefficient is considered and a random solution α_f is taken, then the g evaluated at this α_f is taken as the common private key and with the public key $h(\alpha_1\alpha_2\dots\alpha_n) = u$ the private key is recovered using the bijective operators.

From the cryptanalysis aspect of the protocol the advantage of this protocol over Harry yosh is that the Diophantine equation $f(x_1x_2\dots x_n)$ whose solution is considered for the private key is not made public and as for the 2m operators involved in the public key construction the 2m parameters p_i, q_i can be chosen to form the public key Diophantine equation $h(x_1x_2\dots x_n)$ such that $2m > n+1$ then as it is infeasible to evaluate the chosen 2m parameters, to evaluate the key exchange from public key is infeasible.

References

[1] Brain Osserman: *LU*-Diophantine equations, (1998).

[2] B.S.S. Srinivasarao: *A key Exchange with Linear Diophantine equations*, M. Phil., Dissertation, 2020.

[3] G.H. Hardy, E.M. Wright, D.R. Heath-Brown, J.H. Silverman: *An Introduction to Theory of Numbers*, Oxford University Press, 1965.

[4] H. Davenports: *The Higher Arithmetic*, Eighth Edition, Cambridge University press.

[5] H. YOSH: *The key exchange cryptosystem used with higher order Diophantine equations*, International Journal of Network Security & Its Applications **3**(2) (2011), 43-50.

[6] M. JACOBSON, W. HUGH: *Solving the Pell equations*, CMS book in Mathematics, Canadian Mathematical Society, 2019.

[7] N. HIRATA-KOHNO, A. PETHO: *A Key Exchange protocol based on Diophantine equation and S-integers*, JSIAM Letters, **6**(0) (2014), 85-88.

[8] N. KOBLITZ: *A course in number theory and cryptography*, Springer Science & Business Media, **114**, 1994.

[9] P. ANURADHA KAMESWARI, L. PRAVEEN KUMAR: LU-*A method for recovering a key in the key exchange cryptosystem by Diophantine equations*, Third Edition, Addison-Wesley, (1998).

[10] T.M. APOSTOL: *Introduction to analytic number theory*, Springer Science & Business Media, 2013.

[11] W. DIFFIE, M. HELLMAN: *New directions in cryptography*, IEEE Transactions on Information Theory, **22**(6) (1976), 644-654.

DEPARTMENT OF MATHEMATICS
ANDHRA UNIVERSITY
VISAKHAPATNAM-530003
INDIA.
Email address: panuradhakameswari@yahoo.in

DEPARTMENT OF MATHEMATICS
ANDHRA UNIVERSITY
VISAKHAPATNAM-530003
INDIA.
Email address: srinivasbhavarajumsc@gmail,com

DEPARTMENT OF MATHEMATICS
ANDHRA UNIVERSITY
VISAKHAPATNAM-530003
INDIA.
Email address: aweke$_b$@$yahoo.com$