A Method for Recovering a Key in the Key Exchange Cryptosystem by Diophantine Equations

P. Anuradha Kameswari
Department of Mathematics
Andhra University
Visakhapatnam-530003
Andhra Pradesh

L. Praveen Kumar
Department of Mathematics
Andhra University
Visakhapatnam-530003
Andhra Pradesh

ABSTRACT
The Diophantine equations define an algebraic curve or an algebraic surface and ask about lattice points on it. A Diophantine equation may either possess no non trivial solution or finite number of solutions or infinite number of solutions. Therefore, computing lattice points is difficult in general for Diophantine equations of order greater than one. This ambiguity regarding the solutions of a Diophantine equation is another source for trapdoor functions in Public key cryptography.

In this paper we analyze the potentiality of Diophantine equations in the key exchange cryptosystem and propose a method for recovering a key in the key exchange cryptosystem by Diophantine equations.

Keywords
Key exchange, Diophantine equations

1. INTRODUCTION
The basic idea of cryptography is to communicate securely over an insecured channel. Several cryptosystems are proposed to maintain the security of the message by the communicating parties. In public key cryptography [1,7] the security is maintained by using trapdoor or one-way functions.[4] In this paper the potentiality and use of Diophantine equations [3,5] by the communicating parties in establishing a secret shared key is discussed and a method for recovering the key by sender and recipient using the Diophantine equations is proposed. This method is based on the difficulty of computing solutions of higher order Diophantine equations which are with large solution space [4].

The paper is motivated by the work of Harry Yosh in [5]. A generalization of the operator used in the construction of a cryptosystem using Diophantine equations is given in this paper.

2. KEY EXCHANGE SCHME
- Recipient sets the integer values for variables $X_1, X_2, ..., X_n$ as $X_1 = K_1, X_2 = K_2, ...X_n = K_n$ where $K_1, K_2, ...K_n$ are integers that are the solutions of a Diophantine equation $f(X_1, X_2, ...X_n) = 0$. The Diophantine equation $f(X_1, X_2, ..., X_n) = 0$ is the public key and the values $(K_1, K_2, ...K_n)$ are private key for the recipient.
- The sender sets an element $g(X_1, X_2, ..., X_n)$ in the quotient ring $Z[X_1, X_2, ...X_n] / f(X_1, X_2, ...X_n)$ and constructs a public key using the operator $T_{[a_1,a_2,...a_i;b_1,b_2,...b_i]}$ for i = 1,2,...n given as

$$T_{[a_1,a_2,...a_i;b_1,b_2,...b_i]}(g) = [(((g + a_1)^{b_1} + a_2)^{b_2} + ...)^{b_{i-1}} + a_i]^{b_i}$$

Where the parameters $a_i's$ are integers and $b_i's$ are odd positive integers. Then sender applies this operator to $g(X_1, X_2, ...X_n)$ and obtains a polynomial $h(X_1, X_2, ...X_n) \in Z[X_1, X_2, ...X_n] / f(X_1, X_2, ...X_n)$ i.e

$$T_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(g(X_1, X_2, ...X_n)) = h(X_1, X_2, ...X_n)$$

- As the above polynomial generally has various representations, the sender fixes one of the representations and takes $h(X_1, X_2, ...X_n)$ and $g(X_1, X_2, ...X_n)$ as public key.
- Recipient calculates $h(K_1, K_2, ...K_n) = p$, $g(K_1, K_2, ...K_n) = s$ where $p, s \in Z$ and recipient sends back the value 'p' to the sender with keeping the value's' secret.
- The sender recovers the value's' of $g(X_1, X_2, ...X_n)$ as $s = T^{-1}_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(p) = .$

$$[((p^{\frac{1}{b_n}} - a_n)^{\frac{1}{b_{n-1}}} - a_{n-1})^{\frac{1}{b_{n-2}}} - ...]^{\frac{1}{b_1}} - a_1$$

Thus sender and recipient could share the secret's' as the exchanged key. [1][4]

Example 1:

The key exchange scheme begins from the recipient side. The recipient chooses the integer values of variables say, X, Y as $X=11, Y=2$ a solution of the Diophantine equation as $X^2-30Y^2=1$.. Which is the Pell's equation [3, 5] $X^2-dY^2=1$ for $d=30$ and has infinitely solutions if \$d\$ is not a perfect square, there are infinitely many choices for the X and Y as above.

The recipient sends the information of that Diophantine equation to sender with keeping the values of X and Y are secret. The above equation $X^2-30Y^2=1$ is the public key [4] and X, Y are the private keys for recipient.

The sender constructs a Diophantine equation usingthe Quotient ring $Z[X,Y]/(X^2-30Y^2-1)$

and the operator \$T\$ on that quotient ring given as $T_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(g)=$

$[((((g+a_1)^{b_1}+a_2)^{b_2}+...)^{b_{n-1}}+a_n]^{b_n}$ for some parameters $a_1,a_2,...a_n$ are integers and $b_1,b_2,...b_n$ are odd positive integers,with the inverse operator T^{-1} given as $T^{-1}_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(h)=$

$$[((h^{\frac{1}{b_n}}-a_n)^{\frac{1}{b_{n-1}}}-a_{n-1})^{\frac{1}{b_{n-2}}}-...]^{\frac{1}{b_1}}-a_1$$

Now the operator is applied on any fixed element $g(X,Y)$ in the Quotient ring, applying the operator on the $g(X,Y)=XY\in Z[X,Y]/(X^2-30Y^2-1)$.We have ,

$$T_{[0,3,1,2;1,1,3,1]}(XY)=[(((XY+0)^1+3)^1+1)^3+2]^1$$

$$=(XY+4)^3+2$$

$$=X^3Y^3+12X^2Y^2+48XY+66$$

$$=h(X,Y)$$

$h(X,Y)$ has different expressions in the quotient ring $Z[X,Y]/(X^2-30Y^2-1)$ and one of the representations say $h(X,Y)$ is fixed and is made public. Now the above polynomial can be also represented as,

$$30XY^5+XY^3+360Y^4+12Y^2+48XY+66 = h(X,Y)$$

Selecting this representation as the sender makes $h(X,Y)$ and fixed element $g(X,Y)$ public and keeping the parameters of the operator secret. The recipient calculates $h(11,2), g(11,2)$ and makes the value $h(11,2)=17578$ public, keeping $g(11,2)=22$ secret. Using inverse operator the sender computes value of $g(X,Y)$ as follows:

$$T^{-1}_{[o,3,1,2;1,1,3,1]}(h(11,2))=$$

$$[((17578^{\frac{1}{1}}-2)^{\frac{1}{3}}-1)^{\frac{1}{1}}-3]^{\frac{1}{1}}-0$$

$$=(17576)^{\frac{1}{3}}-4$$

$$=22$$

$$=g(11,2)$$

The sender could recover the value of \$g(11,2)\$ which can be taken as the secret key and the attackers who have the public keys of both sender and recipient to recover the secret key must solve the following system of equations:

$$X^2-30Y^2=1$$

$$30XY^5+XY^3+48XY+360Y^4+12Y^2+66=17578$$

Since the above system of equations contains two variables it can be solved numerically. But when the numbers of variables are greater than two, solving it is difficult in general.

Now consider another example for an elliptic curve.

Example 2:

The recipient chooses the integer values of variables say, X,Y as $X=2, Y=5$ a solution of the Diophantine equation as $Y^2=X^3+17$, which is known as an elliptic curve and infinitely solutions over $E(\square)$.There are infinitely many choices for the X and Y as above.

The recipient sends the information of that Diophantine equation to sender with keeping the values of X and Y aresecret. The above equation $Y^2=X^3+17$ is the public key and X,Y are the private keys for recipient.The sender constructs a Diophantine equation using the Quotient ring $Z[X,Y]/(Y^2-X^3-17)$ and the operator \$T\$ on that quotient ring given as

$$T_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(g)=$$

$$[((((g+a_1)^{b_1}+a_2)^{b_2}+...)^{b_{n-1}}+a_n]^{b_n}$$

For some parameters $a_1,a_2,...a_n$ are integers and $b_1,b_2,...b_n$ are odd positive integers,with the inverse operator T^{-1} given as $T^{-1}_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(h)=$

$$[((h^{\frac{1}{b_n}}-a_n)^{\frac{1}{b_{n-1}}}-a_{n-1})^{\frac{1}{b_{n-2}}}-...]^{\frac{1}{b_1}}-a_1$$

Now the operator is applied on any fixed element $g(X,Y)$ in the Quotient ring, applying the operator on the $g(X,Y)=X^2Y\in Z[X,Y]/(Y^2-X^3-17)$ .We has,

$$T_{[1,-2,3,4;1,3,1,1]}(X^2Y)=[(((X^2Y+1)^1-2)^3+3)^1+4]^1$$
$$=(X^2Y-1)^3+7$$
$$=X^6Y^3-3X^4Y^2+3X^2Y+6$$
$$=h(X,Y)$$

$h(X,Y)$ has different expressions in the quotient ring $Z[X,Y]/(Y^2-X^3-17)$ and one of the representations say $h(X,Y)$ is fixed and is made public. Now the above polynomial can be also represented as,

$$X^9Y+17X^6Y-3X^7-51X^4+3X^2Y+6=h(X,Y)$$

Selecting this representation as the sender makes $h(X,Y)$ and fixed element $g(X,Y)$ public and keeping the parameters of the operator secret. The recipient calculates $h(2,5),g(2,5)$ and makes the value $h(2,5)=6866$ public, keeping $g(2,5)=20$ secret. Using inverse operator the sender computes value of $g(X,Y)$ as follows:

$$T^{-1}_{[1,-2,3,4;1,3,1,1]}(h(2,5))=$$
$$[((6866^{\frac{1}{1}}-4)^{\frac{1}{1}}-3)^{\frac{1}{3}}+2]^{\frac{1}{1}}-1$$
$$=(6859)^{\frac{1}{3}}+1$$
$$=20$$
$$=g(2,5)$$

The sender could recover the value of $g(2,5)$ which can be taken as the secret key and the attackers who have the public keys of both sender and recipient to recover the secret key must solve the following system of equations:

$$Y^2=X^3+17,$$
$$X^9Y+17X^6Y-3X^7-51X^4+3X^2Y+6=6866$$

Since the above system of equations contains two variables it can be solved numerically. But when the number of variables is greater than two, solving it is difficult in general.

Remark

The parameters $b_{i'}s$ of the operator $T_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}$ should be odd, otherwise the image of inverse operator $T^{-1}_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(h)=$ $[((h^{\frac{1}{b_n}}-a_n)^{\frac{1}{b_{n-1}}}-a_{n-1})^{\frac{1}{b_{n-2}}}-...]^{\frac{1}{b_1}}-a_1$ may not be determined uniquely giving raise to different values for `s' and causing ambiguity on the shared secret key `s'.

3. CONCLUSION

An attacker with the public key information $f(X_1,X_2,...X_n)=0$ and $h(X_1,X_2,...X_n)=p$ finds it difficult to recover the key for the Diophantine equation with large number of variables and large solution space. Deciphering can be made still more difficult by increasing the number of parameters in the operator used, this relatively increases the degree and number of equivalent expressions for the polynomial $T_{[a_1,a_2,...a_n;b_1,b_2,...b_n]}(g(X_1,X,...X_n))$ in $Z[X_1,X_2,...X_n]/f(X_1,X_2,...X_n)$.

4. REFERENCES

[1] J. Buchmann “Introduction to cryptography” , Springer-Verlag 2001

[2] D. Burton, “Elementary Number Theory” Sixth ed, Mc Graw Hill, New York, 2007.

[3] H. Davenport's, “The Higher Arithmetic”, Eighth edition, Cambridge University Press, ISBN-13 978-1-107-68854-4.

[4] G. H. Hardy, E. M. Wright, D. R. Heath-Brown and J. H. Silverman, “An Introduction to the Theory of Numbers”, Oxford University Press, 1965.

[5] Harry Yosh, Heco Ltd, Canberra, Australia “The Key Exchange Cryptosystem Used With Higher Order Diophantine Equations” , IJNSA journal Vol.3, No 2, March 2011}

[6] Jacobson. M and W. Hugh, “Solving the Pell equation”, CMS books in Mathematics, Canadian Mathematical society, 2009.

[7] Neal Koblitz “A course in number theory and cryptography ISBN 3-578071-8,SPIN 10893308 “

[8] Lawrence C. Washington, Wade Trappe “Introduction to Cryptography with Coding Theory” 2nd edition, Pearson.

[9] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone., “Handbook of Applied Cryptography,” CRC Press Series on Discrete Mathematics and its Applications. Boca Raton, FL, 1997.

[10] I. Niven, H. S. Zuckerman, and H. L. Montgomery, “An Introduction to the Theory of Numbers”, Fifth edition, John Wiley $\&$ Sons, New York, 1991.

[11] K. H. Rosen”Elementary Numbertheory and Its Applications” 3rd ed., Addison-Wesley,1993

[12] D. R. Stinson, “Cryptography Theory and Practice”, Second Edition, Chapman Hall/CRC, 2002.