ISSN 2350 - 0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 1, Issue 1, August 2014

A Digital Signature Scheme Based On Pell Equation

Aditya Mani Mishra

Department of Mathematics, Motilal Nehru National Institute of Technology, Allahabad, India

ABSTRACT: Elliptic curve digital signature algorithm (ECDSA) is well established digital signature scheme based on the discrete logarithms problems. On the other hand, many cryptosystem has been designed using the Pell Equation. We apply the idea of ECDSA on the solution space of Pell equation to design a digital signature scheme. In this paper we compare the security of our signatures scheme to DSA and ECDSA. Our scheme is as secure as conventional DSA. We show that the signatures scheme based on Pell equation is more efficient than its analogue to elliptic curve i.e. ECDSA.

KEYWORDS: DSA, ECDSA, Pell Equation.

I. INTRODUCTION

In 1985, ElGamal [6] proposed a public key cryptosystem and a digital signature scheme based on the difficulty of solving the Discrete Logarithm Problem in the multiplicative group of an appropriate finite field. In 1991, the National Institute of Standards and Technology of USA proposed the Digital Signature Algorithm (DSA) which is an efficient variant of the ElGamal digital signature scheme [MVV97, NIST94]. The security of DSA is based on discrete logarithms problem.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is being proposed as an ANSI standard. Unlike the normal discrete logarithm problem (DLP) and the integer factorization problem (IFP), the elliptic curve discrete logarithm problem (ECDLP) has no sub exponential-time algorithm. For this reason, the strength-per-key-bit is substantially greater in an algorithm that uses elliptic curves. An original ECDSA was proposed in 1992 by Vanstone [18], and its three variants were given in [21, 4]. These signature schemes are basically the analogues of the corresponding ElGamal digital signature schemes [16]. Many variants of ECDSA have been given in [20].

The Pell Equation has existence since a very ancient time in number theory [3]. It has a number of applications in mathematics [7, 19]. In Algebra, it can be used to find regulator of group [2, 11]. Pell Equation has infinite solution and its solution space forms a cyclic group under appropriate group operation. On the basis of this group, many variants of cryptosystem have been designed [19, 5, 15, 8]. In [5] author proposed fast RSA type scheme based on Pell equation in which encryption speed is 1.5 times faster than then standard RSA and the decryption in 2 times faster. In [15] author defined a new operation on the solution space of Pell Equation and proposed three RSA type cryptosystems. In [8] author proposed a PKC whose security is based on DLP. To the best of our knowledge no signature scheme is found in the literature over the Pell's equation. So, our motivation to this article is to construct a digital signature scheme over Pell's equation.

II. PRELIMINARIES

In this section we brief the Pell's equation and Elliptic Curve.

A. Pell Equation:

Suppose $D\epsilon Z^{+}$ is a square free integer. The Diophantine equation

$x^2 - D\,y^2 = 1$... (2.1.1)

is called Pell Equation. The equation has infinite solutions in the real field. The solution of this equation can be found by continued fraction method [19]. By Lagrange theorem [19], once the fundamental solution of Pell Equation is known, one can find its all solutions. Hence, the solution space of (2.1.1) forms a cyclic group, in fact an infinite cyclic group.

Now consider equation (2.1.1) under modulo system. Let p be a positive prime number. Consider

$x^2 - D\,y^2 = 1 \; mod\; p$ … (2.1.2)

The solution space of (2.1.2) forms a finite cyclic group denote as $C\ (D, p) \subset GF\ (p) \times GF\ (p)$
This group has order $p - \left(\frac{D}{p}\right)$ [13]. This group is either isomorphic to the multiplicative group in *GF(p)* or to the multiplicative subgroup of order p+1in *GF*(p^2). Let (x_p, y_p) denotes the generator of this group. We represented it as P.
Suppose $(x_1, y_1), (x_2, y_2) \in C\ (D, p)$ then we define '+' operation as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_1 x_2 + y_1 y_2 D \; mod\; p,\; x_1 y_2 + x_2 y_1 \; mod\; p)$$

... (2.1.3)

It can also be represented as

$$(x_1, y_1) + (x_2, y_2) = (x_1 + \sqrt{D} y_1)(x_2 + \sqrt{D} y_2)$$

In fact, any of (x, y) can be written in the form$\left(x_p + \sqrt{D} y_p\right)^t$ $for\ some\ t \in Z$ and vice versa. This illustration follows by Lagrange Theorem.

The operation '+' is called "addition of points on *C(D,p)*". The identity element of the group is (1, 0). The inverse of *(x, y)* is *(x, -y)*. So

$$(x_1, y_1) - (x_2, y_2) = (x_1, y_1) + (x_2, -y_2)$$

Again, for any integer, $k \,\epsilon\, Z$. A denotes k times addition of A to itself where A=*(x, y)* is any point in *C(D,p), i.e.* $k.A = (x + \sqrt{D}\ y)^k$.

B. Elliptic Curve

An elliptic curve E over *is* defined by an equation of the form

$y^2 = x^3 + ax + b,$ …….(2.2.1)

where $a, b \in Z_p^*$ and $4a^3 + 27b^2 \neq 0\ (mod\ p)$, together with a special point *O* called the *point at infinity*. The set *E*(Z_p) consists of all points $(x, y) \in Z_p \times Z_p$, which satisfy the defining equation (2.2.1), together with *O***.**
Let P, Q be in *E*, let *l* be the line connecting P and Q (tangent line if P = Q), and let T be the third point of intersection of *l* with *E*. If *l*` is the line connecting T and *O*, then P +Q is the point such that *l* intersects *E* at T and P+Q. This composition law makes *E* into an Abelian group with identity element *O*. The addition operation is defined as below.

C. Addition law of Elliptic Curve E(a, b) over F_p

The elliptic curve $E_p(a, b)$ forms an Abelian group under the certain conditions.

(a) O is the identity element with respect to addition,
(b) If $(x_1, y_1) \in E_p(a, b)$ then -(x, y) = $(x, -y)$.
(c) If and Q= $(x_2, y_2) \in E_p(a, b)$ and Q^{1} -P, then

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

Where $x_3 = \lambda^2 - x_1 - x_2$and

$$y_3 = \lambda(x_1 - x_2) - y_1$$

and$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ if Q ≠P

$\lambda = \frac{3x_1^2 + a}{2\, y_1}$if Q=P

III. DIGITAL SIGNATURE ALGORITHM

The DSA was proposed in August 1991 by the U.S. National Institute of Standards and Technology (NIST) and became a U.S. Federal Information Processing Standard (FIPS 186) in 1993. It was the first digital signature scheme accepted as legally binding by a government [17]. The protocol of DSA is as below.

A. Key Generation:
Let p be a L- bit prime such that the discrete log problem in$\mathbb{Z}_p$is intractable, where $L \equiv 0$mod 64 and$512 \leq L \leq 1024$and let q be a 160 bit prime that divides p-1. Let$\alpha \in \mathbb{Z}_p^*$be a q^{th}root of 1 modulo p. Let $\wp = \{0,1\}^*$and$A = \mathbb{Z}_q^* \times \mathbb{Z}_q^*$and define

$$K = \{(p, q, \alpha, a, \beta) : \beta \equiv \alpha^a modp\},$$

where$0 \leq a \leq q - 1$.The values$p, q, \alpha, \beta$are the *public key* and α is *private key*.

B. Signature Generation:
For K=$(p, q, \alpha, \beta)$and for (secret) random number k, $1 \leq k \leq q - 1$, define

$$sig_k(x, k) = (\gamma, \delta)$$

where

$$\gamma = (\alpha^k modp)modq \text{and}$$
$$\delta = (SHA - 1(x) + \alpha\gamma)k^{-1} modq.$$

(If$\gamma = 0$or$\delta = 0$,a new random value of k should be chosen.)

C. Signature Verification:
For$x \in \{0.1\}^*$and$\gamma, \delta \in \mathbb{Z}_q^*$,verification is done by performing the following computations:

$$e_1 = SHA - 1(x)\delta^{-1}\ mod\ q$$
$$e_2 = \gamma\delta^{-1} mod\ \ q$$
$$ver_k(x, (\gamma, \delta)) = true \Leftrightarrow$$
$$(\alpha^{e_1}\beta^{e_2}\ mod\ p)\ mod\ q = \gamma$$

Sinceγ and δ are each integers is less than q, DSA signatures are 320 bits in length. The security of the DSA relies on two distinct but related discrete logarithm problems. This algorithm has a sub exponential running time. More precisely, the running time of the algorithm is $O\left(\exp\left((c + o(1))(\ln p) 1/3\, (1\text{n}\ln p) 2/3\right)\right)$.

IV. PROPOSED SCHEME

A.Key Generation:

Domain parameter of our scheme consists of a suitably chosen Pell equation for appropriate D. Let p () be an odd prime such that DLP in Pell's equation is intractable, q such that $q|$ p-1 and P be the generator of solution space of Pell equation. We chose $d \in \mathbb{Z}_p$ Then, D, p, P, d.P is public key and d is private key.

B.Signature Generation

Suppose we have massage m to be sign. Firstly we use a collision resistant hash function, let it be H. We also choose$k \in \mathbb{Z}_q^*$.

The signature of m is (r, s)
where

$$k.P = (u,v)$$
$$r = umodq$$
$$s = k^{-1}(H(m) + dr)modq$$

C. Signature Verification:

To verify signature (r, s) on m, receiver Computes:

$$w = s^{-1} \ mod\ q$$
$$i = wH(m) \ mod\ q$$
$$j = wr \ mod\ q$$
$$\text{and}(u,v) = i.P + j.(d.P)$$
$$\text{if}\ u\ mod\ q = r,$$

Then signature is verified.

D.Correctness:

From above;

$$i = s^{-1}H(m) \ mod \ q$$
$$j = s^{-1}r \quad mod \ q$$

if$P = (x_p, y_p)$ then

$$i.P + j.(d.P) = \left(x_p + \sqrt{D}y_p\right)^i \left(x_p + \sqrt{(D)}y^p\right)^{jd}$$
$$= \left(x_p + \sqrt{D}y_p\right)^{i+jd}$$
$$= \left(x_p + \sqrt{D}y_p\right)^{s^{-1}H(m)+s^{-1}rd}$$
$$= \left(x_p + \sqrt{D}y_p\right)^{s^{-1}(H(m)+dr)}$$
$$= \left(x_p + \sqrt{D}y_p\right)^k = k.P$$

This implies that

$$u \ mod\ q = r$$

Hence correctness proved.

E.Security

Security of proposed signature scheme depends on the problem to find the integer *d* for given *d.P*, where P is a point on Pell's equation. We call this problem the Discrete Logarithm Problem for Pell's equation. That is the security of this system depends on the Discrete Logarithm Problem for Pell's Equation. If P = (*x*, *y*) and $d.P = (x_d, y_d)$then by the addition operation defined in Pell's equation we have, $(x + \sqrt{D}y)^d = (x_d + \sqrt{D}y_d)$. Hence, determining *d* from (*x*, *y*) and(x_d, y_d) is the Discrete Logarithm Problem in *GF*(*p*) or $GF(P^2)$. The best known algorithm for solving DLP in *GF(p)* or $GF(P^2)$have a sub-exponential running time [8], and hence, the DLP for Pell's equation has same order of difficulty as conventional DLP.

F.Efficiency

First we note that for any *d.P* can be computed in O(log *d*) time by square and multiply techniques. Since solving the DLP for Pell's equation has the same order of difficulty as the conventional DLP, the key-length can be chosen as in the original DSA. The only difference is, that we have to encrypt two message blocks at once since the message m is in . Due to this we can sign 2log *p* message at a time. If we want to sign a message of length 2 log *p* bits, then our scheme become two time faster then the standard DSA. Otherwise, the overall efficiency (time to perform operations, key-lengths) has the same order as the original DSA.

If we compare the addition operation defined in Elliptic curve and Pell's equation, we see that, the addition operation defined in Elliptic curve is more complicated then the operation defined in Pell's equation. One addition in Elliptic curve requires one inversion and two multiplication where as in Pell's equation requires five multiplication. Since one inversion is computationally equivalent to six multiplication. Due to this point of view we can see that proposed scheme over Pell Equation is more efficient then ECDSA.

V.CONCLUSION

In this article we proposed a digital signatures scheme based on Pell's equation. The proposed scheme is as secure as standard DSA. We have shown that the proposed scheme is two times faster then standard DSA it 2 log *p* bits are signed at a times and the proposed shcmee is more efficient then the standard ECDSA.

REFERENCES

[1]ANSI X9.62. Public key cryptography for the Financial Services Industry: The elliptic curve digital signature algorithm (ECDSA), 1999.

[2]J Buchmann, A sub exponential algorithm for the determination of class groups and regulators of algebraic number fields, S´eminaire de Th´eorie des Nombres, Paris 1988–1989, Progress in Mathematics Vol. 91,

[3]Devid M. Burton ,Elementry Number Theory: TMH book 2006.

[4]W.J. Caelli, E.P. Dawson and S.A. Rea.PKI, Elliptic curve cryptography, and digital signature. Computer and Security, 18:47–66, 1999.

[5]Chen C. Y., Chang C.C., Yang W P., Fast RSA type schemes Based on Pell Equations over ZN*: , Proceeding of International Conference on Cryptology and Information Security, Taiwan Dec. 1-5, 1996.

[6]ElGamal T.: A public key cryptosystem and a signature scheme based on discrete logarithm. IEEE Trans. Inform. Theory 31, 469–472 (1985).

[7]Edward J. Barbeau, Pell's Equation: Springer ISBN: 0-387-95529-1.1999.

[8]Marc Gysin and Jennifer Seberry, How to use Pell's Equation in cryptography, Preprint 1999.

[9]D Johnson and Alfred Menezes, The Elliptic Curve Digital Signature Algorithm (ECDSA): An Enhanced DSA (Preprint).

[10] Hung Zih Liao, Yuan Yuan Shen, On the Elliptic Curve Digital Signature Algorithm.Tunghai Science, Vol. 8 pp. 109-126, 2006.

[11] Lenstra H W, On the calculation of regulators and class numbers of quadratic fields, London Math. Soc. Lecture Note Series 56 (1982), 123–150. Birkh¨auser, Boston, 1990, pp. 27–41.

[12] Menezes A.J., Van Oorschot P.C., Vanstone S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida (1997).

[13] Menezes A., Elliptic curve pubic key cryptosystem . Kluwer Acad. Pub. 1993.

[14] National Institute of Standards and Technology (NIST). FIPS Publication 186: Digital Signature Standard. May 1994

[15] SahadeoPadhye ,A public Key Cryptosystem based on Pell Equation:Eprint Archive-2005/109, http://eprint.iacr.org/2006/191.pdf.

[16] D. R. Stinson ,Cryptography Theory and Practice:: Chapman & Hall/ CRC 2000.

[17] Serge Vaudenay, The Security of DSA and ECDSA Bypassing the Standard Elliptic Curve Certification Scheme, reprint(2006).

[18] S. Vanstone. Responses to NIST's Proposal. Communications of the ACM, 35:50–52, 1992.

[19] Michael J. Jacobson, Jr.; Hugh C. Williams, Solving The Pell Equation;springer:ISBN 978-0-387-84922-5 e-ISBN 978-0-387-84923-2

[20] Lin You1,2, Yi Xian Yang3, and Chun Qi Zhang, Generalization of Elliptic Curve Digital Signature Schemes, ICICS 2001, LNCS Vol.2229 pp. 246-250.

[21]. Y. Zhang and H. Imai. How to construct efficient signcryption schemes on elliptic curves. Information Processing Letters, 68:227–233, 1998.