Proceedings of the 2007 Winter Simulation Conference
S. G. Henderson, B. Biller, M.-H. Hsieh, J. Shortle, J. D. Tew, and R. R. Barton, eds.

AN ELLIPTICAL CRYPTOGRAPHIC ALGORITHM FOR RF WIRELESS DEVICES

Robert Steven Owor
Khalil Dajani
Zephyrinus Okonkwo

Department of Math and Computer Science
Albany State University
Albany, GA 31705, U.S.A.

John Hamilton

Department of CS and Software Engineering
Auburn University
Auburn, AL 36849, U.S.A.

ABSTRACT

In this paper, we propose a new asymmetric cryptographic algorithm (HOOD CRYPT) based on the Elliptical Curve Cryptographic approach. The algorithm describes how an orthogonal frequency division multiplexing (OFDM) based RF wireless system can be encrypted using planner matrix Elliptical Curve Cryptography (ECC). The newly described asymmetric algorithm can be applied to the OFDM transmission scheme in the design of more robust and secure cryptography in portable wireless devices. An analysis of the proposed algorithm is made using the discrete logarithm approach. Two methods, namely, Pollard's rho Attack and Index Calculus are investigated with respect to the new algorithm. We found that our method makes it even more difficult to break the ECC encryption.

1 INTRODUCTION

Asymmetric cryptography has increasingly become more important as vital military, financial and other sensitive data becomes pervasively transmitted on electronic networks (The case for Elliptical Cryptography 2007). With ever higher increasing demands for speed and efficiency, it is imperative that fast and highly secured algorithms evolve accordingly. This is especially valid for wireless RF devices which are becoming used more intensively in military and commercial applications. It is instructive to begin by examining the properties which make elliptical curves a particularly attractive choice for asymmetric cryptography.

1.1 General Form of the Elliptical Curve

An Elliptical curve may be defined as an equation of the form $ay^2 + bxy = cx^3 + dx^2 + ex + f$, *where a ,b, c, d, e, f, x and y are for cryptographic purposes restricted to each belong to a finite field i.e. a, b, c, d, e, f, x and y are each chosen from a distinct set of integral values* (Gupta et al. 2004).

1.2 Desirable Properties of a Cryptographic Algorithm

The encryption algorithm should provide the highest possible level of encryption security at the lowest possible cost in terms of the size of the encryption key, the number of operations and the unit time of encryption. These conditions are particularly more desirable in small portable devices such as RF wireless systems (Gao et al. 1999). In order to implement these conditions in a processor or sensor device, certain mathematical properties must be present in the encryption equation thereby leading us to finite field theory.

In Complex number theory, $i^2+1=0$, where $i^2=-1$. A complex polynomial can be reduced by factorizing powers of i and substituting each i^2 instance with -1. This approach can be used for real, rational and integer fields as well. For computational efficiency, we will restrict our values to integer field set I, and more particularly to the field set I_p, i.e. Integer Mod P, where P is from the prime field set. Ip has the additive, multiplicative and the converse inverse operations respectively. The integer field I_p will have p^m elements where m is the degree of the reduction rule. Some polynomials functions are not reducible. Certain polynomial functions can be reducible as to provide potential points of weakness in the encryption scheme [3]. We therefore need to restrict reducibility to an acceptable degree in the polynomials we choose.

1.3 Properties of the Elliptical Curve

The Elliptical curve provides desirable properties of simple and straight forward encryption computation. The inverse operation is intractable and very difficult to compute (Hitchcock et al. 2004). We can define a rule for adding two points S_1 and S_2 on the curve to find a third point S_3. These points are all on the curve thus forming an Abelian group (Bailey and Parr 1998). The trivial case of infinity

also needs to be included. The order of the curve is defined as the number of distinct points which satisfy this condition including the infinity point as follows:

$$\prod_{t=1}^{m} S_t = \sum_{t=1}^{m} S_t$$

$S_3=S_1+S_2,\ S_4=S_3+S_2,\ S_3=S_1 x S_2,\ S_4=S_1 x S_2 x S_3.$

If we set b=0 in the equation $ay^2+bxy=cx^3+dx^2+ex+f$ i.e. $ay^2=cx^3+dx^2+ex+f$ with conditions:

(i) $4a^3+27b^2 \neq 0$

(ii) $b \neq 0$

The Discrete Logarithm Problem: At the foundation of every cryptosystem is a hard mathematical problem that is computationally almost infeasible to solve (Hitchcock et al. 2004). The discrete logarithm problem is the basis for the security of many cryptosystems including the Elliptic Curve Cryptosystem (ECC). More specifically, the ECC relies upon the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

There are two geometrically defined operations over certain elliptic curve groups. These two operations are point addition and point doubling. By selecting a point in an elliptic curve group, one can double it to obtain the point 2*S*. After that, one can add the point *S* to the point 2*S* to obtain the point 3*S*. The determination of a point m*S* in this manner is referred to as Scalar Multiplication of a point. The ECDLP is based upon the intractability of scalar multiplication products. In the multiplicative group I_p, the discrete logarithm problem is: Given elements r and q of the group, and a prime p, find a number k such that r = qk mod p.

If the elliptic curve groups is described using multiplicative notation, then the elliptic curve discrete logarithm problem is: Given points S_1 and Q in the group, find a number that S_1 k = Q; k is called the discrete logarithm of Q to the base P.

When the elliptic curve group is described using additive notation, the elliptic curve discrete logarithm problem is: Given points P and Q in the group, find a number k such that S_1 k = Q.

It is widely believed that the elliptic curve discrete logarithm problem is hard to computationally solve when the point P has large prime order. The known methods for solving the ECDLP are (Gupta et al. 2004):

- The Pohlig-Hellman algorithm (which reduces the problem to subgroups of prime order).
- Shanks' baby-step-giant-step method.
- Pollard's methods (especially the parallel Pollard method of van Oorschot and Wiener).
- The Menezes-Okamoto-Vanstone (MOV) attack using the Weil pairing.
- The Frey-Rueck attack using the Tate pairing.
- The attacks on anomalous elliptic curves (i.e., elliptic curves over I_p which have p points) due to Semaev, Satoh-Araki and Smart.
- Weil descent (for some special finite fields).

Of the above methods, only the anomalous curves attack runs in polynomial time. The MOV, Frey-Rueck and Weil descent methods are (at their fastest) sub-exponential in complexity. The Pohlig-Hellman algorithm is restrictive in the case where the point P has large prime order. The only algorithms which are applicable for all elliptic curves are the methods of Shanks and Pollard, and these methods have exponential complexity. The following section describes the special case of Wireless RF devices before proceeding with other specific properties of Elliptical curves.

2 WIRELESS RF DEVICE COMMUNICATIONS

There are several aspects to Wireless RF Device communications. A wireless communications system consists of one or more transmitters and receivers using communications channels to enable them exchange information (audio, video or other signals) using the radio spectrum. Several techniques have been used to send and receive information wirelessly. The following table shows some of the more common frequency band designations (Perrig et al. 2004, El-Gammal 1985).

Table1: Sample frequencies of the Radio Spectrum

Frequency (f)	Wavelength (λ)	Band	Description
300–3000 Hz	10^3–10^2 Km	VF	Voice frequency
3–30 KHz	10–1Km	LF	Low frequency
30-300 MHz	10-1m	VHF	Very High Frequency
30-300 GHz	10–1mm	EHF	Ext. High Frequency

These frequency bands are subdivided by the FCC (Federal communications Commission) for SOS, AM, FM, Aviation, Radar, GPS, Cellular, RFID, Television and Commercial radio, Satellite radio and WIFI LANS among others (Watro et al. 2004).

The proliferation of wireless devices has raised at least three critical issues:

- There is a need for greater control and or elimination of signal interference arising from bandwidth congestion.
- There is increasing demand for higher transmission speeds for audio, video and data. Since all of them are now digitized, modulation techniques are becoming increasingly more complex. This translates into demand for higher frequencies.

- There is increased need for security as sensitive military, commercial and private data increasingly becomes transmitted wirelessly. This translates into more sophisticated encryption algorithms which add to additional hardware, power and time requirements. Since most portable wireless devices are small and rely on battery power, it is imperative that encryption algorithms do not add an overbearing cost in terms of time, power and weight to the design of these systems.

Wireless security transmission can be compromised in a number of ways including rogue hopping devices which attach themselves to wireless networks, TCP/IP based intrusion, user/password high-jacks, denial of service attacks, channel connection hijacks, destructive interference attacks, IP spoofing, and breaking of encryption codes (Gupta et al. 2005). Our focus in this paper is on the encryption of wireless RF devices and specifically those using the Orthogonal Frequency Division Multiplexing (OFDM) scheme.

2.1 Orthogonal Frequency Division Multiplexing (OFDM)

OFDM is a subset of frequency division multiplexing in which a single channel uses multiple sub-carriers on adjacent fields. The sub-carriers overlap to maximize spectral efficiency. Overlapping sub-carriers usually results in interference, but orthogonality insures that the overlap occurs without interference (El-Gammal 1985).

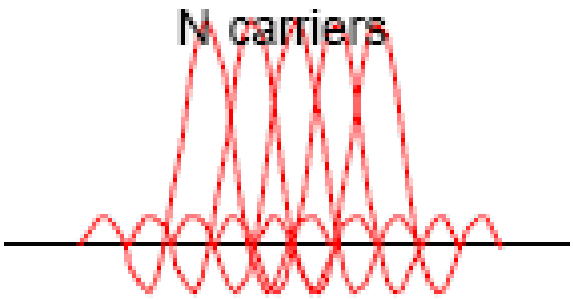

Figure 1: OFDM overlapped orthogonal signal

Below, we illustrate the frequency domain of an OFDM system graphically in Figure 2. Each sub-carrier is represented by a different peak. In addition, the peak of each sub-carrier corresponds directly with the zero crossing of all channels. The x-axis represents frequency in terms of amplitude.

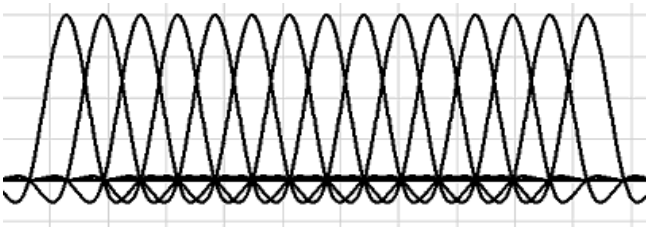

Figure 2: Frequency versus Amplitude in OFDM

Note that OFDM channels are different from band-limited FDM channels in how they apply a pulse-shaping filter. With FDM systems, a sinc-shaped pulse is applied in the time domain to shape each individual symbol and prevent Inter-channel Signal Interference (ISI). With OFDM systems, a sinc-shaped pulse is applied in the frequency domain of each channel. As a result, each sub-carrier remains orthogonal to the other.

Transmitter/Receiver Implementation: In order to use multiple sub-carriers to transmit an individual channel, an OFDM communications system must perform several steps, described in the figure below.

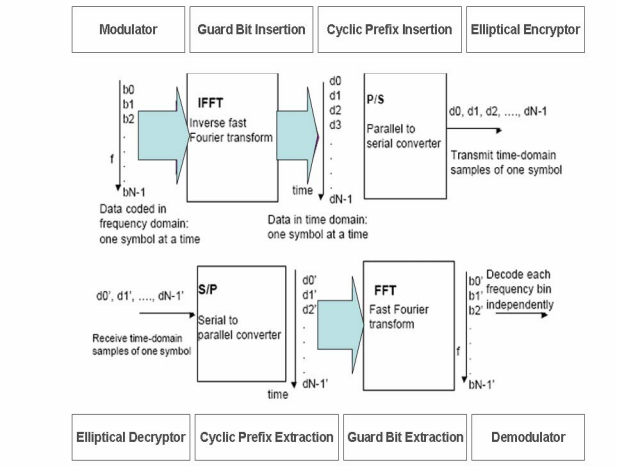

Figure 3: HOOD CRYPT encryption and transmission module

Serial to Parallel Conversion: In an OFDM system, each channel can be broken into various sub-carriers. Sub-carriers make optimal use of the frequency spectrum and also require additional processing by the transmitter and receiver. Additional processing is necessary to convert a serial bit-stream into several parallel bit-streams to be divided among the individual carriers. Once the bit-stream has been divided among the individual sub-carriers, each sub-carrier is modulated as if it was an individual channel before all channels are combined back together and transmitted as a whole. The receiver performs the reverse process to divide the incoming signal into appropriate sub-

carriers and then demodulating these individually before reconstructing the original bit-stream.

Modulation with the Inverse FFT: The modulation of data into a complex waveform occurs at the Inverse Fast Fourier Transform (IFFT) stage of the transmitter. Here, the modulation scheme can be chosen completely independently of the specific channel being used and can be chosen based on the channel requirements. In fact, it is possible for each individual sub-carrier to use a different modulation scheme. The role of the IFFT is to modulate each sub-channel onto the appropriate carrier.

Cyclic Prefix Insertion: Wireless communications systems are susceptible to multi-path channel reflections; a cyclic prefix is added to reduce ISI. A cyclic prefix is a repetition of the first section of a symbol that is appended to the end of the symbol. In addition, it is important because it enables multi-path representations of the original signal to fade so that they do not interfere with the subsequent symbol.

Parallel to Serial Conversion: Once the cyclic prefix has been added to the sub-carrier channels, they must be transmitted as one signal. Thus, the parallel to serial conversion stage is the process of summing all sub-carriers and combining them into one signal. All sub-carriers are generated simultaneously.

2.2 Advantages of HOOD CRYPT Based OFDM Approach

Our orthogonal frequency division multiplexing has been commonly implemented in many emerging communications protocols because it provides several advantages over the traditional FDM approach to communications channels. More specifically, OFDM systems allow for greater spectral efficiency, reduced interference and more resilience to multi-path distortion.

In wireless systems, ISI creates difficulty because the received signal can be slightly distorted. The direct path signal arrives as expected, but slightly attenuated reflections arrive later in time. These reflections create a challenge because they interfere with subsequent symbols transmitted along the direct path. Signal reflections are typically mitigated through a pulse-shaping filter, which attenuates both the starting and ending sections of the symbol period. However, the problem becomes much more significant at high symbol rates. When the reflections make up a significant percentage of the symbol period, ISI is substantial.

Several common commercial protocols [11], such as digital video broadcast (DVB), asymmetric digital subscriber line (ADSL), and wireless Ethernet (WiFI) implement OFDM. With WiFI, the IEEE 802.11a and IEEE 802.11g implementations specifically use OFDM techniques. With IEEE 802.11g, each channel occupies 16.25 MHz of bandwidth at the 2.4GHz frequency range. In addition, each channel is divided into 52 sub-carriers of 312.5 kHz. Together, these sub-carriers overlap to fully utilize the 16.25 MHz channel bandwidth dedicated per channel. In addition, each sub-carrier can use a unique modulation scheme. More specifically, WiFI can use BPS, QPSK, 16-QAM, or 64-QAM depending on the characteristics of the physical channel being used. One of the newest wireless internet protocols, WiMAX, also used OFDM technology. The WiMAX, or IEEE 802.16, is an internet communications protocol specifically designed to provide internet access across long wireless communications links. WiMAX boasts data throughputs of up to 75 Mbps and operates in the 2.5 GHz, 3.5GHz, and 5.8 GHz bands. In addition, it fully utilizes the OFDM approach to a communications channel. For this reason, it is more resilient to multi-path symbol interference and can be used to transmit data distances of up to 30 miles.

3 ENCRYPTION AND DECRYPTION OF HOOD CRYPT ALGORITHM

A description of the cryptographic algorithm implemented in the OFDM based RF wireless system is shown below:

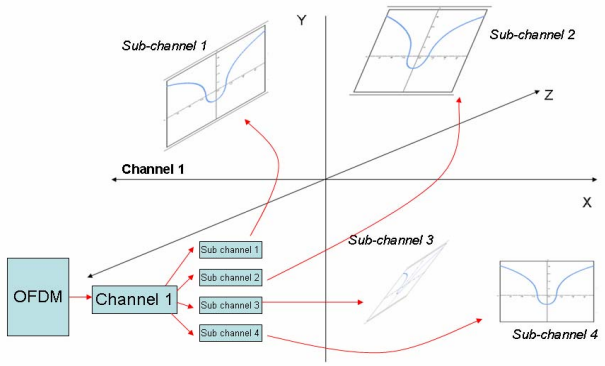

Figure 4: HOOD CRYPT communications channels

The HOOD CRYPT system consists of several channels of communication; branched into several sub-channels. Using r channels with n sub-carriers, the elliptical curve equations for the first channel can be expressed by the following matrix:

It follows that the elliptical curve equations for r channels can be written as:

$$a_{11}y^2_{11}=b_{11}x^3_{11} + c_{11}x^2_{11} + d_{11}x_{11} + e_{11}$$
$$a_{21}y^2_{21}=b_{21}x^3_{21} + c_{21}x^2_{21} + d_{21}x_{21} + e_{21}$$
$$\vdots$$
$$a_{n1}y^2_{n1}=b_{n1}x^3_{n1} + c_{n1}x^2_{n1} + d_{n1}x_{n1} + e_{n1}$$

$$\begin{bmatrix} a_{11}y^2_{11} \\ a_{21}y^2_{21} \\ \vdots \\ a_{nr}y^2_{nr} \end{bmatrix} = \begin{bmatrix} b_{11} & c_{11} & d_{11} & e_{11} \\ b_{21} & c_{21} & d_{21} & e_{21} \\ & \vdots & & \\ B_{nr} & c_{nr} & d_{nr} & e_{nr} \end{bmatrix} X \begin{bmatrix} X3_{11} & x^3_{21} & \cdots & x^3_{n1} \\ x^2_{11} & x^2_{21} & \cdots & x^2_{n1} \\ x_{11} & x_{21} & \cdots & x_{n1} \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

Figure 5: Elliptical Curve encryption matrix for *r* x *n* subcarriers.

Let a unit arithmetic operation take time *t* (largest of multiplication, division, modulo, n-shift, addition, subtraction). The computation time of the equation for channel 1, sub carrier 1 would be approximately 13*t*. Since there are *r* x *n* such computations, the total computation time would be approximately 13*rnt*. If *r* = *n*, this gives us a computation time of $13n^2t$. The running time of this algorithm is there $O(n^2)$.

3.1 Analysis of the Inverse Operation

The elliptic curve discrete logarithm problem describes the inverse operation in the cryptosystem. It is used to effectively perform getting the plaintext back from the cipher text, given only the public key. To find k, we perform repeated addition operations stepping through P, 2P, 3P, until kP is found. The process starts by doubling P, then adding P to 2P finding 3P, then 3P to P finding 4P and so on. This is the brute force method. The drawback of this process is if a large enough prime field to be found, the number of possible values for k becomes inconveniently large. It's quite practical to create a sufficiently large prime field that searching through the possible values of k would take all the processor time currently available.

The National Institute of Standards and Technology (NIST) has defined P192 curve to be used as an example (Watro et al. 2004). On average, a doubling followed by on the order of $3x10^{57}$ additions is required to solve the P192 inverse problem. In the worst case, one has to do twice as many additions. It is probably unnecessary at this point to point out that $3x10^{57}$ is really a very large number which is greater than the few hundreds of operations needed to do the multiplication in the first place.

3.2 Pollard's rho Attack Versus Index Calculus

There is a profound difference in the difficulty of the forward and inverse operations at the centre of all popular asymmetric schemes. In RSA, it's integer multiplication (forward) and factorization (inverse) that make the system work. In Diffie Hellman it's discrete exponentiation (forward) and log (inverse). In ECC its point multiplication (forward) and the elliptic curve discrete logarithm problem (inverse) (Karlof et al. 2004).

In all of these cases, it is easy to see that the difficulty of the brute force approach to the inverse operation increases exponentially with the size of the key. The number of values that must be tried; it doubles with each bit added to the key length. In all of these cryptosystems, the brute force method is not quite the best to be applied. In fact, for Diffie Hellman and for RSA, the process requires retrieving the private key from the public (or the plaintext from the public key and the cipher text) via the index calculus method. It's difficulty grows subexpotentially with the key length. There are shortcuts for doing the inverse operations, but even this poses a major challenge with ECC (Hitchcock et al. 2004, Bailey and Parr 1998).

A typical number field sieve variant of the index calculus method which can be applied to Diffie Hellman; gets subexponentially more difficult as the field size increases; technically at a rate of $e^{1.9(lnn)1/3(lnlnn)2/3}$ where *n* is the field size which is itself, exponential to the key length. It's not as steep an increase as 2^k, where *k* is the key length, but a graph of the number of steps that must be performed (on average) to find a key via the index calculus method versus the key size is still pretty steep (Szewczyk et al. 2004; Karlof, Sastry, and Wagner 2004).

The fastest known algorithms for finding a solution to the elliptical curve problem are the Index calculus Method and the Pollard's Rho Attack. Pollard's Rho attack is an O (√p) algorithm where p is a prime number. The index calculus method has a running time O(p√p). In each case the running time for these algorithms could increase to at least O(n(√p) and O(np√p) respectively for the proposed implementation based on the current state of the art. For a large p, the algorithm becomes even more intractable since the difficulty increases exponentially or sub-exponentially in the best case as p increases.

4 CONCLUSION

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use. We presented a new algorithm; HOOD CRYPT using asymmetric cryptographic approach. Potential advantages of our proposed algorithm include fast and efficient implementation of prime number factoring, logarithmic transformation and increased difficulty of finding inverse solutions. ECC

is a stronger option than the RSA and is the discrete logarithm systems for the future. ECC is such an excellent choice for doing asymmetric cryptography in portable, necessarily constrained devices at present. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security. We hope to conduct further simulation tests to optimize the HOOD CRYPT algorithm in the near future.

REFERENCES

The case for Elliptical Cryptography. 2007. <http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm>.

Gao, S., J. Howell, and D. Panario. 1999. Irreducible polynomials of given forms. In Finite fields: theory, applications and algorithms, ed. R.C. Mullin and G.L. Mullen, 225:45-54. *Contemporary Mathematics, Amer. Math. Soc.*

Szewczyk, R. et al. 2004. Habitat monitoring with sensor networks. *Communications of the ACM* 47(6): 34–40.

Hitchcock, Y., E. Dawson, A. Clark, and P. Montague. 2003. Implementing an efficient elliptic curve cryptosystem over GF(p) on a smart card. *ANZIAM Journal* 44(E):354-377.

Bailey, D. V. and C. Paar. 1998. Optimal extension fields for fast arithmetic in public-key algorithms. In *Advances in Cryptography CRYPTO '98* 1462: 472-485. Lecture Notes in Computer Science, Springer-Verlag.

Gupta, V., D. Stebila, S. Fung, S. Chang Shantz, N. Gura, and H. Eberle. 2004. Speeding up secure web transactions using elliptic curve cryptography. In *11th Network and Distributed System Security Symposium*, 231-239. February 5-6, 2004, San Diego, CA.

Perrig, A. J. Stankovic and D. Wagner. 2004. Security in wireless sensor networks. *Communications of the ACM* 47(6).

El-Gamal, T. 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Info. Theory* 31:469-472.

R. Watro et al. 2004. TinyPK: Securing sensor networks with public key technology. In *Proc. 2nd ACM Workshop on Security of adhoc and Sensor Networks*, 59–64. ACM Press.

Gupta, V. et al. 2005. Sizzle: A standards-based end-to-end security architecture for the embedded internet. In: *Proc. PerCom 2005*.

National Institute of Standards and Technology. 1999. Recommended elliptic curves for federal government use, August 1999.

Karlof, C., N. Sastry, and D. Wagner. 2004. TinySec: link layer security architecture for wireless sensor networks. ACM SenSys, November 2004.

AUTHOR BIOGRAPHIES

Dr. ROBERT STEVEN OWOR is from the department of Math and Computer Science at Albany State University. His email address is <Robert.Owor@asurams.edu>.

Dr. KHALIL DAJANI is from the department of Math and Computer Science at Albany State University. His email address is <Khalil.Dajani@asurams.edu>.

Dr. ZEPHYRINUS OKONKWO is from the department of Math and Computer Science at Albany State University. His email address is <Zephyrinus.Okonkwo@asurams.edu>.

Dr. JOHN HAMILTON is from the department of Computer Science and Software Engineering at Auburn University. His email address is <Hamilton@eng.auburn.edu>.