Elliptic Curve for Data protection

Wasim A Al-Hamdani, Ph.D.
Kentucky State University
400 East Main, KY 40601 USA
wasim.al-hamdani@kys.edu

ABSTRACT

The cryptography of elliptical curve (ECC) is an approach in cryptography public key based on the algebraic structure of elliptical curves on the finished fields; a smaller group can be used to obtain the same level of security as RSA-based. In this article a simple presentation on cryptography with focus on elliptic curve algorithm, examine its security, benefits and its functions with privacy issues. The last part of this article is “protection and privacy components”, for each component the article look at privacy issue then examine the elliptic curve angle to be used with the component. These work results in using elliptic curve in multipart security (or single party) is more efficient in key size, speed and retrieve encrypted information.

Categories and Subject Descriptors

C.2.0 [Computer Communications Networks]: General – Security and protection
D.4.6 [Security and Protection]: Cryptographic controls, Access controls
D.4.6 [Operating Systems]: Security and Protection - Access controls – Authentication, Cryptographic controls, Information flow controls, Invasive software.

General Terms

Cryptography, Cryptography Algorithms, Elliptic curve cryptography, security, RSA,

1. INTRODUCTION

Cryptography is the science of secret writing and is an ancient art; the first documented use of cryptography when an Egyptian scribe used non-standard hieroglyphs in an inscription. Cryptography has many applications as: from diplomatic missives to war-time battle plans. With using computers and communications the new forms of untrusted medium, which includes just about *any* network, particularly the Internet.

- Privacy *or* Confidentiality: information must be kept from unauthorized parties.
- Integrity: message must not be altered or tampered with.
- Authentication: sender and recipient must prove their identities to each other.
- Non-repudiation: proof is needed that the message was indeed received.

The main classification for cryptography algorithms are Public key algorithms and private keys. The cryptography public key is founded on the intractable character of certain mathematical problems. First public key system is RSA, are sure assumption that it is difficult to put a whole number in mailmen with two big primordial mailmen. One of the public key algorithms is elliptical curve based, which have lower key size and high level of security comparing to other public key algorithms, for this many cryptography based suits start to integrate elliptic curve to substitute RSA as in Elliptic Curve Digital Signature Algorithm (FIPS 186-2 [25])and Key Exchange using elliptic curve Diffie-Hellman**.** There are three mainstream families of public-key algorithms. The most widely used systems are those based on integer factorization; in particular, the RSA cryptographic. Systems based on the discrete logarithm problem and can provide support for both digital signatures (with the Digital Signature Algorithm) and key agreement (with the Diffie-Hellman algorithm). There is a third family of public-key algorithms that is growing in importance as key sizes for the other two families increase. This family is based on arithmetic using elliptic curves. First described in 1985, [1] Elliptic curve cryptography (ECC) is a new family of public-key system that can provide shorter key lengths and, depending upon the applications and the operating platform for which they are used, may provide improved performance over systems based on integer factorization and discrete logarithms. The greatness of the elliptical curve resolves the difficulty of problem. A smaller group can be used to acquire the same level of security as RSA-based systems. The use of the small group reduced by requirements of transmission and a storage requirements. This places onerous requirements, not only on its usability, but also on its integration with applications and its internal and external interfaces. A great deal of effort has been dedicated in recent years to the standardization of elliptic curve cryptography. However, there are still some areas where work remains to be

Information Security Curriculum Development Conference 2011 October 7-9, 2011, Kennesaw, GA, USA.

completed. Even where the standardization work has been completed, the results have not fully flowed through into commercial products. Until these deficiencies have been addressed, it will not be a straightforward matter to deploy a general-purpose ECC infrastructure.

In this article a simple general introduction to cryptography with focus on elliptic curve algorithm, examine its security, benefits and its functions with privacy issues. The last part of this article is "protection and privacy components", for each component the article look at privacy issue then examine the elliptic curve angle to be used with the component.

2. CRYPTOGRAPHY

Cryptography is one of the major topics to secure information, whether electronic information or any other media. The word Cryptography is taken from a Greek word "Krypto" which means "secure" and "Graphy" means "Writing", means secure or "Secret Writing" . Some define "Cryptography" as "The Study of mathematical techniques with related aspects of Information Security such as confidentiality, data integrity, entity authentication and data origin authentication". Cryptography has two parts. The first is to transfer "Plaintext" (Massage M), into "ciphertext" C .

2.1 Classify the algorithms in term of key

There are two major classifications:

Public Key (Asymmetric) Algorithms: three keys: **one public key** and **two private Keys**, one for encryption and one for decryption.

Secret Key (Symmetric) Algorithms: There is only **one key** for encryption and decryption.

The symmetric algorithms (secret key) can be further classified into "conventional algorithms" or "classical algorithms" and "modern algorithms". The classical algorithms are further classified into:

Transposition Algorithms: to reorganize the alphabet organization in different order from the plaintext and

Substitution Algorithms: alternate the alphabet of plaintext into different alphabet. It could be from the same alphabet of the plaintext.

The symmetric algorithms are classified (in most literature) into:

Block Algorithms: using block m of plaintext to produce block c of the ciphertext.

Stream Algorithms: using one bit of plaintext at a time to produce one bit of ciphertext using XOR to combine the two bits. That means treat the plaintext as a sequence of bits to produce a sequence of bits of ciphertext.

Some texts classify Cryptography as "Mechanical Cryptography" and "Electronic Cryptography".

Another type of Cryptography algorithm is called the "Hybrid algorithm". It combines Symmetric and asymmetric algorithms to form hybrid ciphers. Typically an asymmetric algorithm (like RSA) is used to securely transfer a symmetric key (like DES) to the correct recipient and to provide authentication with integrity. When a symmetric algorithm is used to encrypt the actual message, Cryptographic software called "Pretty Good Privacy" is a good example of "hybrid algorithms".A new algorithm of Cryptography tested lately called "Quantum Cryptography" (Quantum cryptography is best known for key distribution) is an effort to allow two users of a common communication channel to create a body of shared and secret information. The elements of quantum information exchange are observations of Quantum States. Typically Photons are put into a particular state by the sender and then observed by the recipient.

Sending a message using photons is straightforward in principle, since one of their quantum properties, namely polarization, can be used to represent a 0 or a 1. Each photon therefore carries one bit of quantum information, which physicists call a *qubit* (A basic unit of quantum information, representing either 0 or 1 but capable of being carried by a particle in both states until measured or resolved) [2] To receive such a qubit, the recipient must determine the photon's polarization, for example by passing it through a filter, a measurement that inevitably alters the photon's properties. This is bad news for eavesdroppers, since the sender and receiver can easily spot the alterations these measurements cause. Cryptographers cannot exploit this idea to send private messages, but they can determine whether its security was compromised in retrospect.

The genius of quantum cryptography is that it solves the problem of key distribution. A user can suggest a key by sending a series of photons with random polarizations. This sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail. The first published paper to describe a cryptographic protocol using these ideas to solve the key distribution problem was written in 1984 by Charles Bennett and Gilles Brassard [3]. In it, Bennett and Brassard described an unconditionally secure quantum key distribution system. The system is called the BB84 system after (Bennett & Brassard, Quantum cryptography: Public key distribution and coin tossing, 1984 [3]) and its operation is as follows Quantum cryptography in 1992[4].

2.2 Public key Cryptography

Public-key cryptosystems have two primary uses, Encryption, and digital signatures. In their system, each person gets a pair of keys, one called the public key, and the other called the private key. The public key is published, while the private key is kept secret. The need for the Sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. In this system, it is no longer necessary to trust the security of some means of communications. The only requirement is that public keys be associated with their users in a trusted (authenticated) manner (for instance, in a trusted directory). Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. Furthermore, public-key cryptography can be used not only for privacy (Encryption), but also for authentication (digital signatures) and other various techniques.

In a public-key cryptosystem, the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public-key system by deriving the private key from the public key. Typically, the defense against this is to make the problem of deriving the private key from the public key as difficult as possible. For instance, some public-key cryptosystems are designed such that deriving the private key from the public key requires the attacker to factor a large number, it this case it is computationally infeasible to perform the derivation. This is the idea behind the RSA public-key cryptosystem. The idea of public key cryptosystem is closely related with the idea of one way function [5,6,7]. Given an argument value x, it is easy to compute the function f(x), where it is difficult (hard) to compute x from f(x). One way function conditions are:

(1) it is easy to compute f(x) from x
(2) Computation of x from f(x) is likely to be intractable

The computation of x from f(x) should be hard for the crypto attacker. The legal receiver should have a trapdoor available (the key to solve the one way function), a trapdoor function[8] is an transformation of the text which is easy to apply, but which cannot be easily reversed Generally speaking Public Key Algorithms are based on *one-way* or *trapdoor* functions

Public key Algorithms are for encrypting messages to be transmitted over an insecure channel, and Digital Signatures algorithms are for authenticating the author of a message transmitted over an insecure channel, are emerging as fundamental tools for conducting business securely over the Internet. These technologies are widely expected to be used to conduct billions of dollars in electronic commerce within the next few years. RSA is a public-key cryptosystem for both Encryption and authentication; it was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It works as follows: take two large primes, p and q, and find their product n = pq; n is called the modulus. Choose a number, e, less than n and relatively prime to (p-1)(q-1), which means that e and (p-1)(q-1) have no common factors except 1. Find another number d such that (ed - 1) is divisible by (p-1)(q-1). The values e and d are called the public and private exponents, respectively. The public key is the pair (n,e); the private key is (n,d). The factors p and q maybe kept with the private key, or destroyed

RSA is patented under U.S. Patent 4,405,829, issued September 20, 1983 and held by RSA Data Security[10], Inc. of Redwood City, California; the patent expires 17 years after issue, in 2000. RSA Data Security has a standard, royalty-based licensing policy which can be modified for special circumstances. The U.S. government can use RSA without a license because it was invented at MIT with partial government funding.

Export of RSA falls under the same U.S. laws as all other cryptographic products. RSA used for authentication is more easily exported than when it is used for privacy. In the former case, export is allowed regardless of key (modulus) size, although the exporter must demonstrate that the product cannot be easily converted to use for encryption. In the case of RSA used for privacy (encryption), the U.S. government generally does not allow export if the key size exceeds 512 bits.

Since that time, the algorithm has been employed in the most widely-used Internet electronic communications Encryption program, Pretty Good Privacy (PGP).It is also employed in both the Netscape Navigator and Microsoft Explorer web browsing programs in their implementations of the Secure Sockets Layer (SSL), and by MasterCard and VISA in the Secure Electronic Transactions (SET) protocol for credit card transactions.

The RSA algorithm based on

Key generation: Primes p and q such that n=pq and ϕ = (p-1) (q-1)

Select e with $1<e<\phi$ and gcd $(e, \phi)=1$ (In other words, e is relatively prime to ϕ)

Then find d with $1<d<\phi$ with $ed \equiv 1 (\text{mod } \phi)$

Encryption: $C_t = P_t^e \bmod n$,

Decryption: $P_t = C_t^d \bmod n$,

The algorithm has three parts the first is the Key Generation, the Encryption and the Decryption

2.2.1 RSA steps

Pick two large primes, p and q.
Find N = p * q. N is the RSA modulus.
Let e be a number relatively prime to (p-1)*(q-1).
Find d, so that d*e = 1 mod (p-1)*(q-1) .
The set (e, N) is the public key. Make it known to everyone.
The set (d, N) is the private key. Keep it private and safe.

To encrypt a message m,

Make sure $M < N$, otherwise chop m in suitably small pieces and perform RSA on each individual piece.

Compute $C = M^e \bmod N$, C is the encrypted message

To decrypt a ciphertext C

Compute $M=C^{d} \bmod N$, M is the original message

To sign message M,

Compute $S=M^{d} \bmod N$, S is the digital signature. Send along with message m.
To verify signed message S,

Compute $M=S^{e} \bmod N$; Check if m from above calculation is the same with message sent.
Other public key algorithms: Rabin cryptosystem Pohlig-Hellman, ElGamal public-key cryptosystem, Knapsack Public-Key

3. ELLIPTIC CURVE SYSTEM [10, 11, 12, 13, 14]

Elliptic curves are mathematical constructions from number theory and algebraic geometry, which in recent years have found numerous applications in cryptography. An elliptic curve can be defined over any field (e.g., real, rational, complex). However, elliptic curves used in cryptography are mainly defined over finite fields. Elliptic curves are simple functions that can be drawn as gently looping lines in the (x, y) plane. It can provide versions of public-key methods that, in some cases, are faster and use smaller keys, with equivalent level of security. Their advantage comes from using a different kind of mathematical group for public-key arithmetic. All practical public-key systems today exploit the properties of arithmetic using large *finite groups*.

3.1 Elliptic Curves over Real Numbers

Elliptic curves are not ellipses. They are so named because they are described by cubic equations; In general, cubic equations for elliptic curves take the form

$$y^2+axy+by=x^3+cx^2+dx+e$$

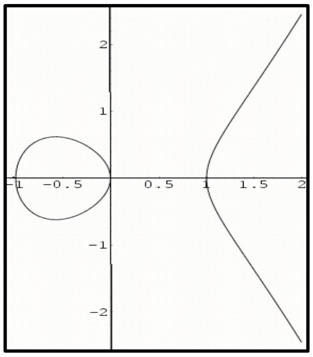
Where a,b,c,d and e are real numbers; x and y take on values in the real numbers. It is sufficient to be limited to equations of the form

$$y^2=x^3+ax+b$$

such equations are said to be *cubic*, or of degree 3, because the highest exponent they contain is a 3. Also included in the definition of an elliptic curve is a single element denoted $\mathbf{O}$ and called the *point at infinity* or the *zero point,*. To plot such a curve, it needs to compute

$$y=\sqrt{x^3+ax+b}$$

For given values of a and b, the plot consists of positive and negative values of y for each value of x. Thus each curve is symmetric about $y=0$. Figure1 shows two examples of elliptic curves.



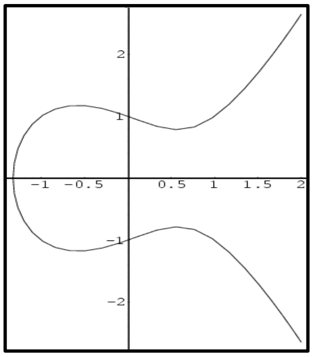
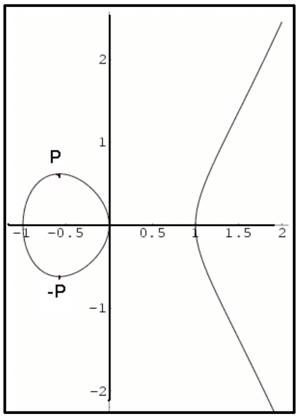


Figure 1a. $y^2=x^3-x$ **Figure 1b.** $y^2=x^3+x+1$

Consider the set of points $E(a, b)$ consisting of all of the points (x, y) that satisfy Equation $y^2=x^3+ax+b$ together with the element $\mathbf{O}$. Figure1 represent the sets $E(-1, 0)$ and $E(1, 1)$, respectively (Using different value of the pair (a, b))

The addition law on E has the following properties:
(a) P + O = O + P = P for all P $\in$ E.
(b) P + (-P) = O for all P $\in$ E.
(c) P + (Q + R) = (P + Q) + R for all P; Q; R $\in$ E.
(d) P + Q = Q + P for all P; Q $\in$ E.
The addition law + makes the points of E into a commutative group and it can be shown that the set E(a, b) is an abelian group. All of the group properties are trivial to check except for the associative law (c). The associative law can be verified by a lengthy computation using explicit formulas, or by using more advanced algebraic or analytic methods



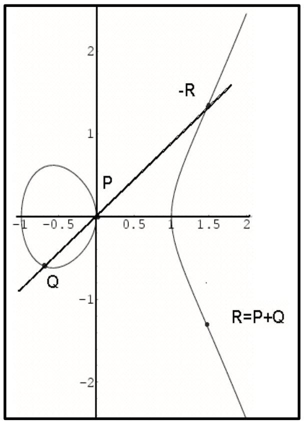


Figure2. Two points P and –P **Figure 3. R=P+Q**

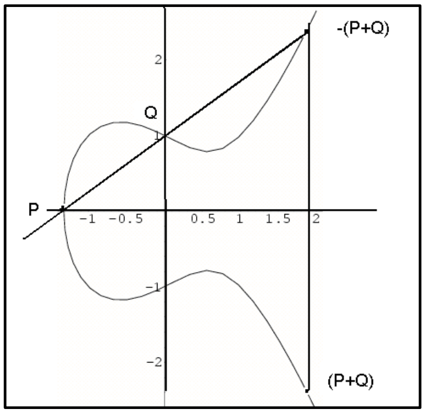


Figure 4. (P+Q)

For two distinct points $P=(x_P,y_P)$ $Q=(x_Q,y_Q)$ that are not negatives of each other, the slope of the line l that joins them is

$$\lambda=(y_Q-y_P)/(x_Q-x_P)$$

There is exactly one other point where $\mathbf{1}$ intersects the elliptic curve, and that is the negative of the sum of P and Q. After some algebraic manipulation, we can express the sum $R=P+Q$ as follows:

$$x_R=\lambda^2-x_P-x_Q \quad ,$$

$$y_R=-y_p+\lambda(x_P-X_R)$$

Need to be able to add a point to itself: P+P =2P =R

When $y_P\neq 0$, the expressions are:

$$x_R=\left(3x_P^2+2x_P/2y_P\right)-2x_P \ ,$$

$$y_R=\left(3x_P^2+a/2y_P\right)\left(x_P-x_R\right)-y_P$$

3.2 Elliptic Curves over Z_p

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: *prime curves* defined over Z_p, and *binary curves* constructed over GF(2). Points out that prime curves are best for software applications, because the extended bit-fiddling operations needed by binary curves are not required; and that binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful, fast cryptosystem. There is no obvious geometric interpretation of elliptic curve arithmetic over finite fields. The algebraic interpretation used for elliptic curve arithmetic over real numbers does readily carry over.

For elliptic curves over Z_p; normally use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p — 1, for some prime number p, and in which calculations are performed modulo p. As with real numbers, limit ourselves to equations of the form $y^2=x^3+ax+b$, but in this case with Coefficients and variables limited to Z_p: "The elliptic curve over Z_p, $p>3$ is a set of all pairs $(x,y)\in Z_p$ which fulfill $y^2 \bmod p=(x^3+ax+b) \bmod p$ where $a,b\in Z_p$ and $(4a^3+27b^2) \bmod p\neq 0 \quad \bmod p$, A primitive element is satisfy $c*P=\mathbf{O}$ where c= b-a "

Example

$a=1, b=1, x=9, y=7, p=23:$

$(4a^3+27b^2) \bmod p\neq 0 \quad \bmod p,$

$7^2 \bmod 23=(9^3+9+1) \bmod 23,$

$49 \bmod 23=739 \bmod 23$, 3=3

Place equations in Z_p will be as :

$$x_R=\lambda^2-x_P-x_Q \ \bmod p$$

$$y_R=\lambda(x_P-x_R)-y_P \ \bmod p$$

$$\text{Where } \lambda=\begin{cases}\dfrac{y_Q-y_P}{x_Q-x_P} \bmod p & \text{if } P\neq Q\\[2ex] \dfrac{3x_p^2+a}{2y_p} \bmod p & \text{if } P=Q\end{cases}$$

- $x_P=x_Q \ \bmod p$ and $y_P=-y_Q \ \bmod p$ then $P+Q=\mathbf{O}$ which is infinity point
- is the neutral element of the group: $P+\mathbf{O}=\mathbf{O}$ for all P
- Additive inverse of any point $P=(x_P,y_P)$ is $P+(-P)=\mathbf{O}$ such that $(x_P,y_P)+(x_P,-y_P)=\mathbf{O}$

The points on an elliptic curve together with **O** have cyclic subgroups.

Example

P=11, a=1,b=6, find all points on elliptic curve of

$E_{11}(1,6):(y^2=x^3+x+6) \bmod 11$

Use P(2,7) as the primitive element., P=(2,7)

2P=P+P= (2,7)+(2,7)= (x_R,y_R)

$\lambda=3x_p^2+a/2y_p \ \bmod p$ because $P=Q$

$\lambda=3*2^2+1/2*7 \bmod 11$,

$\lambda=(2*7)^{-1}(3*2^2+1) \bmod 11$, $\lambda=(14)^{-1}(13) \bmod 11$

$\lambda=(\ (14)^{-1}=3^{-1} \bmod 11)(13) \bmod 11$, $\lambda=4*13 \bmod 11$

$\lambda=8 \ \bmod 11$

$x_R=\lambda^2-x_P-x_Q \ \bmod p$

$x_R=8^2-2-2 \ \bmod 11=(64 \text{ -}4) \bmod 11=60 \bmod 11,$

$x_R=5 \ \bmod 11$

$y_R=\lambda(x_P-x_R)-y_P \ \bmod p,$

$y_R=8(2-5)-7 \ \bmod 11=-31 \bmod 11=2$

2P=P+P= (2,7)+(2,7)= (5,2)

$3P = 2P + P = (8,3)$

$4P = 3P + P = (10,2)$

$5P + P = ..$

....

$12P = 11P + P = (2,4)$

13P=12P+P=O

14P=13P+P=O+P=P

...

All 12 none zero elements together with **O** form the cyclic group are

P=(2,7)	2P=(5,2)	3P=(8,3)
4P=(10,2)	5P=(3,6)	6P=(7,9)
7P=(7,2)	8P=(3,5)	9P=(10,9)
10P=(8,8)	11P=(5,9)	12P=(2,4)

3.2.1 Menezes-Vanstone Algorithm

The first part of this algorithm is to organize the plaintext in sequence of pairs $(x_1, x_2)(x_3, x_3)...$ the Encryption function is

$$C_t = (Y_0, Y_1, Y_3)$$

Where $Y_0 = k.\alpha,\ Y_1 = c_1.x_1 \bmod p,\ Y_2 = c_2.x_2 \bmod p$,

$(x_1, x_2)(x_3, x_3)...$ are plaintext pairs

$(c_1, c_2) = k.\beta$ where $0 < k < \#E$

$\alpha \in E$, and $\alpha = (x_\alpha, y_\alpha)$

And the decryption is $x_1 = Y_1 c_1^{-1} \bmod p$ and

$x_2 = Y_2 c_2^{-1} \bmod p$

Example

Key generation: P=11, a=1,b=6,

$(4a^3 + 27b^2) \bmod p \neq 0 \quad \bmod p$,

$(4.1^3 + 27 * 6^2) \bmod 11 \neq 0 \quad \bmod p$. Compute

$E_{11}(1,6) : (y^2 = x^3 + ax + b) \bmod p$

$E_{11}(1,6)$

$P0 = (2, 4), P1 = (2, 7), P2 = (3, 5)$

$P3 = (3, 6), P4 = (5, 2), P5 = (5, 9)$

$P6 = (7, 2), P7 = (7, 9), P8 = (8, 3)$

$P9 = (8, 8), P10 = (10, 2), P11 = (10, 9)$

Choose $\alpha \in E$ and $\alpha = (x_\alpha, y_\alpha)$, $\alpha = (8,3) \in E_{11}(1,1)$

Choose receiver secrete key integer $a \in \{2,3,4,...\#E-1\}$, $\gamma = 7 < \#E$.

Compute β : $\gamma.\alpha = \beta = (x_\beta, y_\beta) = 7*(8, 3) = (3,5)$

Encryption: plaintext $= (x_1, x_2) = (8,1)$.

Selects a point k, $0 < k < \#E$ let k=

Compute $(c_1, c_2) = k.\beta = 6 * (3, 5) = (10, 9)$.

Compute

$Y_0 = k.\alpha = = 6 * (8, 3) = (3, 6)$

$Y_1 = c_1 * x_1 \pmod p = 10 * 8 \pmod{11} = 3$

$Y_2 = c_2 * x_2 \pmod p = 9 * 1 \pmod{11} = 9$

The ciphertext is $C_t = (Y_0, Y_1, Y_2) = (3,6,3,9)$

Decryption:

$(c1, c2) = \gamma * Y_0 = 7 * (3, 6) = (10, 9)$,

$x_1 = Y_1 c_1^{-1} \bmod p = 3 * 10^{(-1)} \pmod{11}$,

$x_1 = 3 * 10 \pmod{11}$, $x_1 = 8$.

To solve $10^{(-1)} \bmod 11$ use multiplicative inverse Algorithm Chapter 2, 10*x == 1 (mod 11)=10,

$x_2 = Y_2 c_2^{-1} \bmod p = 9 * 9^{(-1)} \pmod{11}$,

$x_2 = 9 * 5 \pmod{11}$, $x_2 = 1$

3.3 Elliptic Curve Efficiency and Security

The majority of public key systems in use today use 1024-bit parameters for RSA and Diffie-Hellman. The US National Institute for Standards and Technology has recommended that these 1024-bit systems are sufficient for use until 2010 [15]. After that, NIST recommends that they be upgraded to something providing more security.

- One option is to simply increase the public key parameter size to a level appropriate for another decade of use.
- Another option is to take advantage of the past 30 years of public key research and analysis and move from first generation public key algorithms and on to elliptic curves.
-

Table 1. NIST Recommended Key Sizes [15]

RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)	Symmetric Key Size (bits)
1024	160	80
2048	224	112
3072	256	128
7680	384	192
15360	521	256

Security is not the only attractive feature of elliptic curve cryptography (nsa.gov, 2009). Elliptic curve cryptosystems also are more computationally efficient than the first generation public key systems, RSA and Diffie-Hellman. Although elliptic curve arithmetic is slightly more complex per bit than either RSA or DH arithmetic, the added strength per bit more than makes up for any extra compute time. The following table shows the ratio of Diffie-Hellman computation versus Elliptic curve computation for each of the key sizes listed in Table 3.

Table 2. Relative Computation Costs of Diffie-Hellman and Elliptic Curves [15]

Security Level (bits)	Ratio of DH Cost : EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

In choosing an elliptic curve as the foundation of a public key system there are a variety of different choices. The National Institute of Standards and Technology (NIST) has standardized on a list of 15 elliptic curves of varying sizes. Ten of these curves are for what are known as binary fields and 5 are for prime fields. Those curves listed provide cryptography equivalent to symmetric encryption algorithms (e.g. AES, DES or SKIPJACK) with keys of length 80, 112, 128, 192, and 256 bits and beyond.

For protecting both classified and unclassified National Security information, the National Security Agency has decided to move to elliptic curve based public key cryptography. Where appropriate, NSA plans to use the elliptic curves over finite fields with large prime moduli (256, 384, and 521 bits) published by NIST.

The United States, the UK, Canada and certain other NATO nations have all adopted some form of elliptic curve cryptography for future systems to protect classified information throughout and between their governments.

Public- and private-key operations vary in efficiency: for RSA, public-key operations are significantly more efficient than private-key ones, whereas for Elliptic curve cryptography, private-key operations are slightly more efficient than public-key (Entrust, 2008). Therefore, the performance of one algorithm relative to another depends on the operations used by the application. Profiles that involve significantly more public-key operations than private-key and key generation operations will favor RSA over ECC. Other mixes will tend to favor ECC

Direct comparison of performance between different cryptographic groups is difficult. However, For application profiles that make heavy use of public-key operations, compared to private-key and key generation operations, the crossover point is around the 128-bit cryptographic strength level (i.e., 3072 bits for RSA and 256 bits for ECC). This profile is the one that shows RSA in the most favorable light. So, the crossover point occurs at a lower strength level for all other profiles.

"It is worth noting that the experts at the U.S. Government's National Security Agency have determined that beyond the 1024-bit public-key systems in common use today, rather than increase key size, a switch to ECC is necessary" (Entrust, 2008).

For many severely constrained environments the crossover point is also lower than 128 bits. Furthermore, there exist a number of platforms that cannot support the large integer arithmetic required for even moderately sized RSA operations (1024- or 2048-bit). And, in these environments, RSA is not an option.

3.4 Elliptic Curve Intellectual Property [15]

Regardless of the many advantages of elliptic curves and despite the adoption of elliptic curves by many users, many vendors and academics view the intellectual property environment surrounding elliptic curves as a major roadblock to their implementation and use. Various aspects of elliptic curve cryptography have been patented by a variety of people and companies around the world. Notably the Canadian company, Certicom Inc. holds over 130 [15] patents related to elliptic curves and public key cryptography in general.

As a way of clearing the way for the implementation of elliptic curves to protect US and allied government information, the National Security Agency purchased from Certicom a license that covers all of their intellectual property in a restricted field of use. The license would be limited to implementations that were for national security uses and certified under FIPS 140-2 or were approved by NSA. Further, the license would be limited to only prime field curves where the prime was greater than 2255. On the NIST list of curves 3 out of the 15 fit this field of use: the prime field curves with primes of 256 bits, 384 bits and 521 bits. Certicom identified 26 patents that covered this field of use. NSA's license includes a right to sublicense these 26 patents to vendors building products within the restricted field of use. Certicom also retained a right to license vendors both within the field of use and under other terms that they may negotiate with vendors.

Commercial vendors may receive a license from NSA provided their products fit within the field of use of NSA's license. Alternatively, commercial vendors may contact Certicom for a license for the same 26 patents. Certicom is planning on developing and selling software toolkits that implement elliptic curve cryptography in the field of use. With the toolkit a vendor will also receive a license from Certicom to sell the technology licensed by NSA in the general commercial marketplace. Vendors wishing to implement elliptic curves outside the scope of the NSA license will need to work with Certicom if they wish to be licensed.

3.4.1 Elliptic curve and Suite B Cryptography [16]

Suite B is a set of cryptographic algorithms promulgated by the National Security Agency as part of its cryptographic modernization program. It is to serve as an interoperable cryptographic base for both unclassified information and most classified information. Suite B was announced on February 16, 2005 and includes:

E**ncryption**: Advanced Encryption Standard (AES) - FIPS 197(with keys sizes of 128 and 256 bits)

Digital Signature: Elliptic Curve Digital Signature **Algorithm** - FIPS 186-2 (using the curves with 256 and 384-bit prime moduli)

Key Exchange: Elliptic Curve Diffie-Hellman Draft NIST Special Publication 800-56 (using the curves with 256 and 384-bit prime moduli)

Hashing: Secure Hash Algorithm - FIPS 180-2 (using SHA-256 and SHA-384)

4. PROTECTION AND PRIVACY COMPONENTS

4.1 Biometrics

Biometrics is the t used for the many ways that we humans can be identified by single characteristics (Physiological and behavioral) of our bodies. Technologies includes: Palm Print Recognition, Fingerprint Recognition, Hand Geometry ,Dynamic Signature, Vascular Pattern Recognition, Iris Recognition, Face Recognition, Speaker Recognition, retina Recognition, Fingerprints are the most commonly known.

The biometrics industry is booming, after September 11, 2001. [17]

- Several airports in the U.S. and other countries have since installed facial recognition biometrics systems to identify individuals on law enforcement agencies' "most-wanted" lists.
- Various biometrics systems are being employed to provide secure access to computer systems, for example in health care institutions.
- Biometrics technologies are seen by the financial services industries as a way to deter fraud and identify fraudsters.
- Many casinos now use facial recognition biometrics systems to identify known card-counters and cheaters and expel them from their facilities.
- Many national governments, including the U.S., use biometrics to speed border crossings and customs entry for frequent travelers.

Biometrics is now being used deployed in a wide range of public and private sector applications such as: Access control, attendance recording, payment mechanisms, crime prevention, and border security. While biometrics promise many benefits, including stronger user authentication, greater user convenience, and improved security and operational efficiencies, they pose data privacy and security concerns that are significant. Some of these concerns include unauthorized secondary uses (function creep), expanded surveillance and profiling of individuals, data misuse (including identity theft), false matches, no matches, and system errors. Significant data security risks include potential spoofing, tampering, various security attacks, and insufficient accuracy. Some of the key benefits and advantages of biometric encryption technology include: No retention of the original biometric image or template from the same biometric, multiple and unlikable identifiers for different uses can be generated that are cancelable and revocable. Improved authentication security: stronger binding of user biometric and identifier improved security of personal data and communications Greater public confidence, acceptance, and use Suitable for large-scale applications. Biometric encryption is a process that securely binds a PIN or a cryptographic key to a biometric (in another words: Biometric Encryption refers to a process of secure key management), so that neither the key nor the biometric can be retrieved from the stored template. The key is recreated only if the accurate live biometric sample is presented on verification. Some of the key benefits and advantages of biometric encryption technology include:

- No retention of the original biometric image or template
- Greater public confidence, acceptance, and use
- multiple and unlikable identifiers for different uses can be generated that are cancelable and revocable
- Improved security of personal data and communications
- Improved authentication security: stronger binding of user biometric and identifier
- Suitable for large-scale applications

There are various methods that can be deployed to secure a key with a biometric [18]:

- Involves remote template matching and key storage.
- A second method involves hiding the cryptographic key within the enrollment template itself via a trusted (secret) bit-replacement algorithm.
- A third method is to use data derived directly from a biometric image.
- The key is linked with the biometric at a more fundamental level during enrollment, and is later retrieved using the biometric during verification.

4.1.1 Elliptic Curve Comments

Using with one biometric device elliptic curve will provide speed of encryption, conditionality of key management and high accrue; however with more one biometric device connected in a network to provide high level of authentication, access control it would be very useful and high retune of investment using PKI infra-structure with elliptic curve

Through using elliptic curve would be very useful in multiparty management system to access biometric data. It will be advantage to Elliptic curve to sign data communication with multi-party access

Using biometric with integration of elliptic curve would be very useful for Kerberos Version 5 extension that provides for the use of public key cryptography, this has been highlight in RFC5349 - Elliptic Curve Cryptography (ECC) Support for Public [19].

Holding integrity of data storage for biometrics devices would be through elliptic curve with SHA-256/384

4.2 E-Commerce

Commonly known as (electronic marketing) e-commerce or e-Commerce, consists of the buying and selling of products or services over electronic systems such as the Internet (was designed as an inherently insecure communications) and other computer networks. E-commerce threats could include:

- Computer hackers trying to penetrate into a system to read or change sensitive data
- Burglars stealing a server or laptop that has unprotected sensitive data on its disk
- Imposters posing as legitimate users and even creating a website similar to yours

- Users allowed webpage or accepting an electronic mail with the hidden active contents which attacks your systems or sends information sensitive to
- People made without approval Internet companies have designed numerous ways to track web users as they travel and shop throughout cyberspace. "Cookie" is no longer a word associated solely with sweets. It now refers to cyber-snooping.
- Identity thieves are able to shop online anonymously using the credit-identities of others.
- Web-based information brokers sell sensitive personal data, including Social Security numbers, relatively cheaply.

Cryptography is a major enabler of E-Commerce that is so effective, it sometimes goes unnoticed. The key to cryptography is it allows the integrity of E-Commerce transactions and safeguards information for many levels of business including the government and the military. Cryptography been used for secure ecommerce and to provide: privacy, integrity, authentication and non-repudiation.

4.2.1 Elliptic Curve Comments

The use of different techniques of cryptography application as in digital signature, key exchange and encryption seems with many evidence is moving towards elliptic curves and with PKI as infrastructure. This eliminate the use many Public key accelerator for bottle neck problem at the server sides, in addition to high speed , less bits, high security. Using elliptic curve with ecommerce is essential with Cryptographic Message Syntax (CMS). The Cryptographic Message Syntax (CMS) is cryptographic algorithm independent. This specification defines a profile for the use of Elliptic Curve Cryptography (ECC) public key algorithms in the CMS.

The ECC algorithms are incorporated into the following CMS content types:

- 'SignedData' to support ECC-based digital signature methods (ECDSA) to sign content
- 'EnvelopedData' to support ECC-based public-key agreement methods (ECDH and ECMQV) to generate pairwise key-encryption keys to encrypt content-encryption keys used for content encryption –
- 'AuthenticatedData' to support ECC-based public-key agreement methods (ECMQV) to generate pairwise key-encryption keys to encrypt MAC keys used for content authentication and integrity

The Request for Comments: 3278[20] specified the Cryptographic Message Syntax as:

EnvelopedData using ECDH

- Fields of KeyAgreeRecipientInfo
- Actions of the sending agent
- Actions of the receiving agent

EnvelopedData using 1-Pass ECMQV

- Fields of KeyAgreeRecipientInfo
- Actions of the sending agent
- Actions of the receiving agent

AuthenticatedData using ECC

AuthenticatedData using 1-pass ECMQV

- Fields of KeyAgreeRecipientInfo
- Actions of the sending agent
- Actions of the receiving agent

In addition to this, the document supports the Elliptic Curve certification issue with public key.

4.3 Wireless Communications and Local Tracking

The Products and services using wireless technology are advance to a step of extreme. The Digital cell telephones become smaller, cheaper and smarter. The users of mobile phone can send and accept the e-mail and the messages of receiver of call and surfer on Internet. The personal digital helpers of report, PDAs, are also equipped for wireless communications. Blackberry or wireless laptop broadcasts its location whenever the power is on, whether or not a call is in progress. This has led to the ability to automatically identify somebody's location. This took to the capacity automatically to someone to identify the location. This could be used to stalk you or to stalk you your children, check the activities of employee, furnish the true assistance of mapping of time, or book the recommendations of restaurant or aimed fact of the advertising for the content Location tracking combines several technologies. Three basic techniques can be used to determine the location of a wireless phone or laptop [17]:

- GPS compares the timing of radio signals from satellites in space
- Triangulation collects directional signals from cell phone towers
- Wi-Fi local area networks track high-frequency radio signals from transmitters

The wireless industry is well conscious that the consumers do not want that their communication devices for doubled as the supervision technologies. Some industry representatives take steps to develop the intimacy indications. They know that the industry without wire will not prosper unless the intimacy clientele can be protected. The legal standards of intimacy for the usage of your data of location are inconsistent, depending on that holds the data. The telecommunications carriers cannot unveil generally your data of location without one chooses in of consumer. The other entities with the access to your location information cannot be liable to this norm.

In August 2002, the Federal Communications Order refused the request of the industry of telecommunications to adopt the rules of intimacy of information of location without wire that would cover the notification, consent, the security and integrity clientele.

4.3.1 Elliptic Curve Comments

Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem, in particular for mobile (i.e., wireless) environments. Compared to currently prevalent cryptosystems such as RSA, ECC offers equivalent security with smaller key sizes

The security of wireless has two aspects: data security, most wireless based on RC4 encryption which not secure; the other parts is the location tracking. Both issues are based on secure access point , the current technology a user authenticate itself to the access point but the access point does not authenticate itself to the user (portable devices)as the first phase followed by using RC4 for data encryptions.

Elliptic curve can create strong secure communication and key exchange stronger for two parties (user and Access point) allows then to key exchange and encrypted communication (possible using AES).

The major scenario is when a user authenticate him/herself to the access point the access point has to identify itself as tracking free or non-tracking free. At this case the user has the power to use this access point or move to another one

A possible use of key exchange algorithms for transport layer specified in RFC 4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) [21]

- ECDH_ECDSA Fixed ECDH with ECDSA-signed certificates.
- ECDHE_ECDSA Ephemeral ECDH with ECDSA signatures.
- ECDH_RSA Fixed ECDH with RSA-signed certificates.
- ECDHE_RSA Ephemeral ECDH with RSA signatures.
- ECDH_anon Anonymous ECDH, no signatures.

4.4 Identity Theft

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain personal data especially Social Security number, your bank account or credit card number, telephone calling card number, and other valuable identifying data can be used, if they fall into the wrong hands. In the United States and Canada, for example, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts, or, in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victim's names. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his reputation in the community and correcting erroneous information for which the criminal is responsible.

Criminal identity theft occurs when the imposter uses the innocent person's identification when arrested, say, for a traffic violation, shoplifting, marijuana possession, or another misdemeanor. When that individual fails to appear in court on the appointed day, a warrant is issued for the arrest of the innocent person.

4.4.1 Elliptic Curve Comments

Public-key cryptography has achieved massive success in protecting users from identity theft resulting from transactions on the Web, e-mail correspondence and VPN sessions. "But, it is well accepted in information security circles that cryptographic algorithm strength erodes with time, as the computing power available to cryptanalysts increases and the cryptanalytic techniques they use improve. Security architects respond to this trend by specifying larger key sizes, and since the computing power available to the legitimate user also increases with time, the attendant performance degradation is - at least partially – offset" [22]. As soon the required elliptic curve standards achieved and tested (list of standards for elliptic curve can be found in [22], the elliptic curve infrastructure will be usable and such infra-structure will provide lower key size, faster access, high performance to accomplish identity theft

4.5 Information Profiling

It is the process of investigative the data available in an existing information source (e.g. a database or a file) and assembles statistics and information about that data. The purpose of these statistics may be to:

- Assess whether metadata accurately describes the actual values in the source database
- Assess the risk involved in integrating data for new applications, including the challenges of joins
- Find out whether existing data can easily be used for other purposes
- Improve the ability to search the data by tagging it with keywords, descriptions, or assigning it to a category
- Give metrics on data quality, including whether the data conforms to particular standards or patterns
- Understanding data challenges early in any data intensive project, so that late project surprises are avoided. Finding data problems late in the project can lead to delays and cost overruns.
- Have an enterprise view of all data, for uses such as Master Data Management where key data is needed, or Data governance for improving data quality.

Some example of source date used for data profiling are:

- Pay bills with credit cards (leave data trail consisting of purchase amount, purchase type, date, and time)
- Information is collected when we pay by check.
- Supermarket discount cards create a comprehensive database.

- When car, equipped with a radio transponder, passes through an electronic toll booth, our account is debited and a record is created of the location, date, time, and account identification.
- When surf the Internet and visit websites.
- When subscribe to a magazine, sign up for a book or music club, join a professional association, fill out a warranty card, give money to charities, donate to a political candidate, tithe to our church or synagogue, invest in mutual funds, when we make a telephone call, when we interact with a government agency

Here is a story to illustrate the potential harm of untrammeled data collection and profiling.

> "In 1998 the *Salt Lake Tribune* reported that the supermarket chain Smith's Foods was subpoenaed by the U.S. Drug Enforcement Agency (DEA) for its discount card data on several named suspects. Was the DEA looking for high-volume purchases of non-prescription medicines that make up the chemical formula for "speed," like Sudafed? No. They were interested in finding out if these individuals had purchased a lot of plastic "baggies," the presumption being that if you're manufacturing and selling "meth," you will need plastic bags to package it in "[17].

The main issue in creating potential harm "Information that has been gathered for one purpose should not be used for other purposes without the consent of the individual" (paraphrased from the "use limitation principle,"

4.5.1 Elliptic Curve Comments

Cryptography in general cannot stop data profiling without collaboration efforts from different organization, implementing and enforcing cryptography in general and elliptic curve can minimize the large harm of data profiling; this can be achieved through different controls such as:

- Each credit card (or supermarket discount cards)are encrypted and the transaction has two key first to authenticate the transaction and the second to authenticate the use of customer data
- All single customer cards are connected in elliptic key exchange managements protocols, in which a customer can create a good financial control and information profiling control through central keys
- Encryption for each cookies and will be a key to allowed access the cookies
- Paying using check should collaborated with enforcing personal information control (to be used or not in information profiling)

4.6 Video Surveillance

There are dramatic growth of video monitoring throughout the public and private sectors, both in the U.S. and other countries. United Kingdom is the most developing perhaps in its use of video watching by the government in the public places. A risk furthermore is that "tech-low" video surveillance can be converted into recognition of the face biometrics systems with the growth of numerical technologies. As the price of reductions of systems biometrics, temptation to convert units of surveillance tech-low videos into systems of recognition of the face will augment. Widespread implementation of video surveillance is harmful for several reasons; We are becoming used to being watched, and at earlier and earlier ages. Many schools have installed video monitoring throughout their campuses. The main elements in video surveillance is the matching algorithms and its speed "two images match, if a certain percentage of their interest points match, and we say that a pair of interest points match if a certain percentage of their SIFT attributes match" (Senior, 2009) the matching
Could be perform before encryption procedure (normal procedure) and it is possible to be perform after encryption assume that booth videos have encrypted with the same algorithm.

4.6.1 Encryption Angle

the backup of the actual videos or disks or tapes , which contains all the monitoring actions if there is no illegal activities or regulation valuation should be retain for certain period of time and MUST be encrypted . The encryption will protect the personal issues, and personal activities. To retrieve these monitoring videos must apply "need to know "principles. This action will support integrity, preventing altering, unauthorized disclosure, confidentiality.

Encryption could be achieved through different level depending on the security level required, such as:

(a) Immediate after each shot
(b) Before storage (before and after create meta database)
(c) Before set a signal on communication line

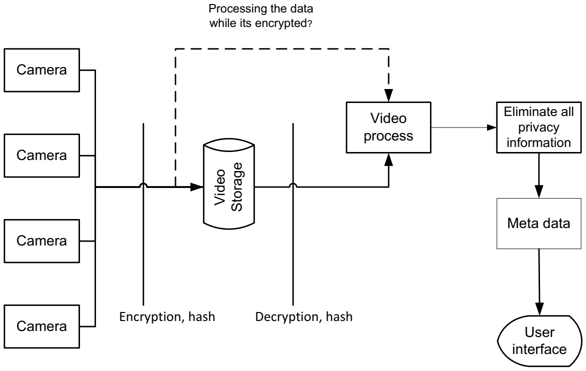


Figure 4. Shows the cryptography process position with video surveillance

The main question which arises in figure one is: is it possible to process data while it is encrypted, this procedure is well known and well used still many problem in processing data while it is in confidential state. There is no clear guideline how to do this or standard procedure.

4.6.2 Elliptic Curve Comments

Elliptic curve will provide faster cheaper and support public key infrastructure for save and secure access to monitoring storage, and possible the use of Elliptic curve digital signature with hashing to verify the person how store the videos. In addition to the possibilities of using smart cards or an devices. Elliptic curve encryption will be very useful for less than 1024 bit encryption which gives high power for encrypting pixel by pixel.

In addition to the general advantage of using elliptic curve, building infra-structure based on public key will give multi personal to access the storage based on access control. However cryptography access control will be most suitable to build such infrastructure [24]

In case of multi part accessing the Video surveillance it would be advantage to use elliptic curve and adopt the Patent "Authentication Method Employing Elliptic Curve Cryptography" [24]. "Disclosed is an authentication method employing elliptic curve cryptography (ECC), applicable to a mobile broadcast TV system having one or more head end systems, at least a transmitter, and at least a mobile set. The authentication method comprises at least one request message from mobile sets simultaneously or in a short period of time arriving at a head end system for authentication; manipulating each broadcast authentication message by ECC; manipulating each service request message by ECC and pairing operation; performing a mutual authentication between the head end system and mobile sets by ECC and pairing operation; and broadcasting one group of authentication messages to all the mobile sets of many requests arrived at the head end system simultaneously or in a short period of time for the same service"

4.7 Public Records on the Internet

Most government agency and court records are considered "public" records. In recent years, however, a growing number of government agencies and court systems have made these records available on the Internet.

4.7.1 Security and Elliptic Curve

Security and Elliptic curve use the need for regulation to secure these records and encrypted them and to read them a person has to decrypt the required record and the key should be granted free. The key use must be recorded in log file to keep tracing the used (and especially the illegal use of the data). ECC provide good solution since these record has different size and some of them could be less than 512 bits Cryptography

4.8 Background Checks

It can uncover illegal criminal records and other inaccurate data. Unless the employer notifies the job applicant of the contents of the investigation, that individual may not learn why he or she was rejected. Federal law requires such disclosure (Fair Credit Reporting Act) "But the law contains loopholes that the employer can use to avoid notifying the applicant that negative information in the background investigation resulted in their not being hired"[17]. Business like Lexis-Nexis and Choice point assemble records from thousands of foundations and recourses to make them available to their subscribers, usually law enforcement agencies, private investigators, attorneys, debt collectors, skip-tracers; insurance claims investigators, and media outlets, among others. A set of voluntary guidelines was accepted by the information broker industry in combination with the Federal Trade Commission in 1997; "But the guidelines are weak and have resulted in no meaningful privacy protections for U.S. consumers" [17].

The cost of background checks has decreased dramatically in recent years due to cheap electronic resources and storage. Investigations are going beyond a simple reference verification or credit report to include unlawful background checks. Since the terrorist attacks of 9-11, an increasing number of employers are conducting background checks of new hires as well as existing employees. "It's fair to say that a significant percent of background checks are retrieving information that is either incorrect or misleading"[17] . As discussed in the "data profiling" section above, there is no such thing as a perfect database. Because of loopholes in the law, the subjects of background checks might never know the contents of their investigations and the reasons they are not able to land a job.

4.8.1 Security and Elliptic curve

It use the need for strong act to enforce the encryption of these data and not to be sold to support their annual budget (as some court system offers these service) , elliptic curve would be very useful because of the records sizes. And extra regulation are required to enforce strong "need to know" before the release of the information. Elliptic curve could play strong role in this case, as the public record owner would hold the authentication key and has the privilege to delegate the read only for the recodes to who satisfy security required. Whatever the case on encryption using data processing on encrypted data is a strong approach to access data with valuation its confidentiality

4.9 Financial Privacy

Banks, insurance companies, and brokerage firms are now able to associate with one another under one corporate law, known as Gramm-Leach-Bliley (GLB) was implemented in 2001. The Act includes laws that govern the collection and disclosure of customers' personal financial information by financial institutions and requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information.

The Gramm-Leach Bliley Act requires IT attention because they need to account for the security procedures in place regarding protecting consumer data

The act focuses on strategy and specifies to include all four of these components:

- Protection of the data itself through encryption
- Controlled Access to data with strong authentication and authorization systems
- Detection of data at risk to prevent data leakage
- Comprehensive Management of data throughout its lifecycle from its creation through archive

The act emphasize on “Encryption can be used as a preventive control, a detective control, or both. As a prevention control, encryption acts to protect data from disclosure to unauthorized parties.”

The act does not specify the algorithm but emphasize on Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk

- Effective key management practices
- Robust reliability
- Appropriate protection of the encrypted communication’s endpoints

4.9.1 Elliptic Curve Comments

Cryptography in general has great achievement to provide privacy issue through the use of authentication process, however digital signature with hybrid system (combination of public key and private key algorithms) could be great deal to ensure the confidentiality; and in this condense Elliptic curve will be great deal in term of speed, keysize and process time.

5. CONCLUSION

In this article we examine the possibilities of using elliptic curve as a promising cryptogram system since it public key with efficient keysize and high speed with the right operation platform. In this article the introduction of cryptography especially public key and elliptic curve , then follows with privacy components in surveillance ; for each component a general privacy issue been discussed follows with the benefits of using elliptic curve cryptography system. The elliptical curve can be used to obtain the same level of security as RSA-based systems. The use of the small group reduced by requirements of process time, transmission and a storage requirements. This provide not only on usability, but also the integration with applications and its internal and external interfaces.

With all the efforts in recent year for elliptic curve standardization, this covers: Message-based ECC encryption algorithms, PKI Standards, S/MIME, SSL/TLS and XML Signatures and Encryption, IPSec, PKCS#11. However, there are still some works to be completed. Until these deficiencies have been addressed, it will not be a straightforward matter to deploy a general-purpose ECC infrastructure.

6. REFERENCES

[1] Entrust.com 2008. Elliptic Curve PKI: An exploration of the benefits and challenges of a PKI based on elliptic curve cryptography.

[2] Vittorio, S. 2002 . Quantum Cryptography: Privacy Through Uncertainty. Retrieved from CSA information company: http://www.csa.com

[3] Bennett, C. H., & Brassard, G. 1984. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, (pp. 175 – 179). Bangalore, India: IEEE.

[4] Bennett, C. H., Brassard, G., & Ekert, A. K. 1992. Quantum cryptography. Scientific American, pp. 50 - 57.

[5] Goldreich, O. 2001. Foundations of Cryptography: Volume 1, Basic Tools. Cambridge University Press.

[6] Katz, J., & Lindell, Y. 2007. Introduction to Modern Cryptography. Chapman and Hall/CRC Press.

[7] Al-Hamdani, W.A. 1999"Cipher Systems "Iraqi National Library No. 135 in 29-05-1997

[8] Menezes, A. J. 1996. Handbook of Applied Cryptography. CRC Press.

[9] RSALab. 1992. Cryptography FAQ Chapter 2 and Chapter 2. Retrieved from Rsa Lab: http://www.rsa.com/rsalabs/node.asp?id=2213

[10] Koblitz, N. 1987. Elliptic curve cryptosystems. Mathematics of Computation , 48 , 203-209.

[11] Miller, V. 1985. Use of elliptic curves in cryptography. CRYPTO 85.

[12] Lay, G.-J., & Zimmer, H. G. 1998. Constructing elliptic curves with given group order over large finite fields. Proceedings of the First International Symposium on Algorithmic Number Theory. Springer Lecture Notes In Computer Science; Vol. 877.

[13] Rosing, M. 1999. Implementation Elliptic Curve Cryptography. Manning Pub.

[14] Blake, I. F. 2005 . Advances in Elliptic Curve Cryptography. Cambridge University Press Series: London Mathematical Society Lecture Note Series (No. 317).

[15] nsa.gov. 2009. The Case for Elliptic Curve Cryptography. Retrieved from The National Security Agency Central Security Service : can be retrieved from http://www.nsa.gov/business/programs/elliptic_curve.shtml

[16] nsa.gov. (n.d.). NSA Suite B Cryptography. Retrieved from The National Security Agency Central Security Service: can be retrieved from http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[17] Givens, B. (2009). Privacy Today: A Review of Current Issues. Retrieved from Privacy Rights Clearinghouse (PRC): http://www.privacyrights.org/

[18] Soutar, C., Roberge, D., Stoianov, A., Gilro, R., & Kumar, B. V. 1999. Biometric Encryption. In R. K. (ed), ICSA Guide to Cryptography (p. chapter 22 in). McGraw-Hill .

[19] Zhu, L., Jaganathan, K., & Lauter, K. (2008). RFC5349 - Elliptic Curve Cryptography (ECC) Support for Public. faqs.org.

[20] Beth, G. (retrived 20009). privacyrights.org. Retrieved from Privacy Today: A Review of Current Issues: http://www.privacyrights.org/ar/Privacy-IssuesList.htm#u

[21] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., & Moeller, B. 2006. RFC4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for T. faqs.org.

[22] entrust.com. 2008. Elliptic Curve PKI: An exploration of the benefits and challenges of a PKI based on elliptic curve cryptography. Retrieved from www.entrust.com: www.entrust.com

[23] Wasim Al-Hamdani.2010. Cryptography Based Access Control in Healthcare Web Systems. InfoSec CD 2010, Proceedings of the 7th annual conference on Information security curriculum development http://infosec.kennesaw.edu/InfoSecCD/

[24] Leu, M.-C., & Sun, H.-M. (2009). Authentication method employing elliptic curve cryptography. Retrieved from faqs.org: http://www.faqs.org/patents/

[25] FIPS PUB 186-2, 2000. Digital Signature Standard, (DSS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology