Abstract—The aim of this paper is to provide an overview for the research that has been done so far on elliptic curves cryptography role in information security area. The elliptic curves cryptosystem is the newest public-key cryptographic system and represents a mathematically richer procedure then the traditional cryptosystem based on public-key, like RSA, Diffie-Hellman, ElGamal and Digital Signature Algorithm.

Keywords: elliptic curve, public key, encryption, signature, RSA, ElGamal.

I. INFORMATION SECURITY

Information security is based on cryptography. Cryptography word comes from the two ancient Greek words: “krypto”, which means “hidden” and “grafo”, which means “to write”. Cryptography meaning is how to make what you write obscure, unintelligible to everyone except whom you want to communicate with.

Cryptography provides many sophisticated security tools for a variety of problems, from protecting data secrecy, through authenticating information and parties, to more complex multi-party security implementations. There are two popular kinds of cryptographic protocols: symmetric-key and asymmetric-key protocols. In the symmetric protocols, the common key (the secret-key) is used by both the sender and the received of the communication in order to encrypt and decrypt the message. In public key protocols there are two associated key; one is kept private by the owner and the other is published in the public domain (public key-server). Different public key cryptographic systems are used to provide public-key security. Among these we can mention the RSA, Diffie-Hellman, Digital Signature Algorithm, ElGamal cryptosystem and in recent years the Elliptic Curve Cryptography. These systems provide the information security by relying on the difficulty of different classical mathematical problems.

II. ELLIPTIC CURVE INTRODUCTION

Elliptic curves are mathematical constructions from number theory and algebraic geometry, which in recent years have found numerous applications in cryptography. Elliptic curve cryptosystems do not introduce new cryptographic algorithms, but they implement existing public-key algorithms using elliptic curves.

Three basic choices for public key systems are available for these applications:

• RSA
• Diffie-Hellman (DH) or Digital Signature Algorithm (DSA) modulo a prime p
• Elliptic Curve Diffie-Hellman (ECDH) or Elliptic Curve Digital Signature Algorithm (ECDSA).

RSA is a system that was published in 1978 by Rivest, Shamir, and Adleman, based on the difficulty of factoring large integers.

Whitfield Diffie and Martin Hellman proposed the public key system now called Diffie-Hellman Key Exchange in 1976. DH is key agreement and DSA is signature, and they are not directly interchangeable, although they can be combined to do authenticated key agreement. Both the key exchange and digital signature algorithm are based on the difficulty of solving the discrete logarithm problem in the multiplicative group of integers modulo a prime p.

Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems almost 20 years ago, independently by Victor Miller from IBM [1] and Neal Koblitz from the University of Washington [2].

For the same level of security per best currently known attacks, elliptic curve-based systems can be implemented with much smaller parameters, leading to significant performance advantages. Such performance improvements are particularly important in the wireless arena where computing power, memory, and battery life of devices are more constrained [5].

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. 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. [4].
Therefore, currently, for the same level of resistance against the best known attacks, the system parameters for an elliptic-curve-based system can be chosen to be much smaller than the parameters for RSA or mod p systems. For example, an elliptic curve over a 163-bit field currently gives the same level of security as a 1024-bit RSA modulus or Diffie-Hellman prime. The difference becomes even more dramatic as the desired security level increases. For example, 571-bit ECC is currently equivalent in security to 15,360-bit RSA/DH/DSA. Public key protocols are used in combination with symmetric key algorithms. The overall strength of the system is the strength of the weakest link. Recently the new federal Advanced Encryption Standard (AES) was introduced, providing greater security than its symmetric key predecessor. At key lengths of 128, 192, and 256, AES has made ECC systems even more attractive as a key agreement alternative.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz[1] and Victor S. Miller[2] in 1985.

### III. ELLIPTIC CURVE REPRESENTATION

An elliptic curve can be defined over any field like real, rational, complex. Elliptic curves used in cryptography are mainly defined over finite fields. Finite fields, also named Galois fields, are fields consisting of a finite number of elements. There are usually two finite fields to work on: prime finite field and binary finite field. Abstractly, a finite field consists of a finite set of objects called field elements together with the description of two operations, addition and multiplication, that can be performed on pairs of field elements. The addition operation in an elliptic curve is the counterpart to modular multiplication in common public-key cryptosystems and multiple addition is the counterpart to modular exponentiation.

An elliptic curve can be thought of as being given by an affine equation of the form
\[ y^2 = x^3 + ax + b, \]
where \(a\) and \(b\) are elements of a finite field with \(p^n\) elements, where \(p\) is a prime larger than 3.

The set of points on the curve is the collection of ordered pairs \( (x, y) \) with coordinates in the field and such that \(x\) and \(y\) satisfy the relation given by the equation defining the curve, plus an extra point that is said to be at infinity. The set of points on an elliptic curve with coordinates in a finite field also form a group, and the operation is as follows: to add two points on the curve \(Q_1\) and \(Q_2\) together, pass a straight line through them and look for the third point of intersection with the curve, \(R_1\). Then reflect the point \(R_1\) over the x-axis to get \(-R_1\), the sum of \(Q_1\) and \(Q_2\). Thus, \(Q_1 + Q_2 = -R_1\). The idea behind this group operation is that the three points \(Q_1, Q_2,\) and \(R_1\) lie on a common straight line, and the points that form the intersection of a function with the curve are considered to add up to be zero (Fig. 1).

Security is not the only attractive feature of elliptic curve cryptography. 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 DH computation versus EC computation for different values of the key size.

<table>
<thead>
<tr>
<th>Security Level (bits)</th>
<th>Ratio of DH Cost : EC Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>3:1</td>
</tr>
<tr>
<td>128</td>
<td>6:1</td>
</tr>
<tr>
<td>192</td>
<td>10:1</td>
</tr>
<tr>
<td>256</td>
<td>32:1</td>
</tr>
</tbody>
</table>

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.
Elliptic curve cryptography has moved from being an interesting theoretical alternative to being a cutting edge technology adopted by an increasing number of companies. There are two reasons for this new development: one is that ECC is no longer new, and has withstood a generation of attacks; second, in the growing wireless industry, its advantages over RSA have made it an attractive security alternative. Wireless Internet mail industry leaders such as Qualcomm have embraced ECC, as well as other major companies in the wireless industry such as Motorola, Docomo, and RIM. Major computer companies such as IBM, Sun Microsystems, Microsoft, and Hewlett-Packard are all investing in ECC. The U.S. government is backing the use of ECC as well, with NSA creating the security requirements for wireless devices connecting to the military, and NIST providing standardized curves for use in a range of applications of ECC. Smartcard companies such as Gemplus are also using ECC to improve their products’ security. Wireless devices are rapidly becoming more dependent on security features such as the ability to do secure email, secure Web browsing, and virtual private networking to corporate networks, and ECC allows more efficient implementation of all of these features [5].

III APPLICATIONS FOR ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curves are important in number theory, and constitute a major area of current research. They were used in the proof of Fermat’s Last Theorem, they find applications in cryptography and integer factorization.

ElGamal elliptic curve cryptosystems

ElGamal was the first mathematician to propose a public key cryptosystem based on the Discrete Logarithm Problem. He proposed two distinct cryptosystems: one for encryption and the other one for digital signature.

1) ElGamal encryption system based on elliptic curves

The ElGamal encryption protocol based on elliptic curves does not create a common key, but it is used a message represented by a point on the elliptic curve M = (M1, M2).

Here is the algorithm:

- **Key generation** (A)
  1. Select a random integer k, from [1, n-1].
  2. Compute: A = kQ
  3. A’s public key is kQ or (E, P, A), A’s private key is k

- **Encryption** (B)
  1. Select a random integer k, from [1, n-1].
  2. Compute B = kQ such that SK = kQkQ = kQ = (x, y)
  3. If x = 0 (mod p) and y = 0 (mod p) then go to step 2.
  4. Compute: C = xM1 and C = yM2
     (Note the calculation are done, mod p)
  5. Send (B, C, C) to A

- **Decryption** (A)
  A receives (B, C, C) and does the following
  1. Compute S = kQ = (x, y)
  2. Compute M = C/M and M = C/M
     (Note the calculation are done, mod p)
  3. Recover the message M = (M1, M2)

2) ElGamal digital signature based on elliptic curves

A digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

The ElGamal signature algorithm was introduced in 1984. It is based on the discrete logarithm problem, and was originally defined for the multiplicative group of the integers modulo a large prime number. It is straightforward to extend it to use other finite groups, such as the multiplicative group of the finite field GF(2^w) or an elliptic curve group. ElGamal signatures must use a collision-resistant hash function, so
that it can sign messages of arbitrary length and can avoid existential forgery attacks.

**Key generation:** Entity A (Alice) selects a random integer $k_A$ from the interval $[1, n-1]$ as her private key and computes $A = k_A G$ as her public key, which she places in the public-key server.

**Signing scheme**
1. Selects random integer $k$ from the interval $[1, n-1]$.
2. Computes $R = kG = (x_R, y_R)$, where $r = x_k \mod n$; if $r = 0$ then goto step 1;
3. Compute $e = h(M)$, where $h$ is a hash function $\{0,1\}^* \rightarrow F$.
4. Compute $s = k^{-1}(e+rk_A) \mod n$; if then goto step 1. $(R, s)$ is the signature message $M$.

**Verifying scheme**
1. Verify that $s$ is an integer in $[1, n-1]$ and $R = (x_R, y_R) \in E(F_p)$.
2. Compute $V_1 = sR$.
3. Compute $V_2 = h(M)G + rA$, where $r = x_R$.
4. Accept if and only if $V_1 = V_2$.

**Consistency**

$V_1 = sR = skG \{h(M)+k_o+r\} \mod nG, V_2 = h(M)G + rA = [h(M)+rK_A]G.$ And because $G$’s order is $n$, $kG = jG$ where, $j = k \mod n$. Hence, $V_1 = V_2$.

The Digital Signature Standard is on the base of many current research topics today, like signcryption which was introduced by Yuliang Zheng [6].

**ACKNOWLEDGMENT**

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques, RSA and Diffie-Hellman. Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA and DH, ECC offers equivalent security with smaller key sizes, which results in faster computations, lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity. Elliptic Curve Cryptography (ECC) has recently been endorsed by the US government.

**REFERENCES**