*International Journal of*
*Mathematical Modelling & Computations*
Vol. 01, No. 04, 2011, 245 - 250

# A New Protocol Model for Verification of Payment Order Information Integrity in Online E-Payment System using Elliptic Curve Diffie-Hellman Key Agreement Protocol

A. Zaghian and M. J. Hashemi*

*Faculty of Applied Sciences, Maleke Ashtar University, Isfahan, Iran.*

Received: 26 August 2011; Accepted: 30 November 2011.

**Abstract.** Two parties that conduct a business transaction through the internet do not see each other personally nor do they exchange any document neither any money hand-to-hand currency. Electronic payment is a way by which the two parties transfer the money through the internet. Therefore integrity of payment and order information of online purchase is an important concern. With online purchase the customer and merchant can not be assumed to be completely honest or they can act to change either payment information or the order information. Pateria, Singh and Raghuwanshi proposed a new protocol model based on tree entities customer, merchant and the payment authority that can verify each other. Unfortunately, this protocol is not secure. In this paper, a new protocol is proposed based on elliptic curve Diffie-Hellman key agreement protocol which is secure. The security of our protocol depends on ECDLP and since the ECC is a suitable public key cryptosystem, this protocol can be replaced with another protocol.

**Keywords:** Elliptic Curve, Diffie-Hellman Key exchange protocol, E-Payment, Payment Information, Order Information, Security.

**Index to information contained in this paper**



## 1. Introduction

The use of e-commerce has been connected with a lot of skepticism and apprehension due to some crimes linked with e-commerce and specifically to payment system. When electronic money is transferred from a buyer to a seller over telecommunication networks, accuracy and security is critical. So designing a secure protocol to assure the security of transactions is necessary . Pateria et. al. [5] proposed a new

*Corresponding author. Email: mjhashemi69@yahoo.com

protocol that is not secure. They only say that the protocol can be made secure when it is applied with some cryptographic algorithm. In public key cryptography, Rivest, Shamir and Adelman (RSA), Digital Signature Authentication (DSA), and Diffie-Hellman , protocol are used traditionally. Unfortunately, the use of these schemes imposes significant performance penalty on web servers and has a great impact of web performance on e-commerce transaction while small devices like cell phone are beyond the scope. They conclude that ECC is better for e-payment systems, also ECC would be most suitable public key cryptography scheme for a constraint and open environment like payment systems.

## 2. Elliptic Curve

### 2.1 *Definition*

In this section, we briefly outline the basics of elliptic curves over finite field and the cryptography application related to elliptic curves. Let $p$ to be an odd prime $> 3$. We will consider an elliptic curve E defined over $GF(p)$ by

$$y^2 = x^3 + ax + b \tag{1}$$

with $x, y, a$ and $b \in GF(p)$ and $4a^3 + 27b^2 \neq 0(modp)$. The latter condition ensures that the cubic curve on the right does not have multiple roots. All solutions $(x, y) \in GF(p) \times GF(p)$ of equation (1) together with a special point $\infty$, called the point at infinity, form $E(GF(p))$.It is well-known that $E(GF(p))$ is an (additively written) abelian group with the point $\infty$ serving as its identity element. For more rules of group addition, ready reference [4] is recommanded. We use finite fields, i.e., fields with a finite number of elements. Using elliptic curves in public key cryptography was first suggested in 1985 by N.Koblitz and V.Miller. They believed that the discrete logarithm problem was harder for elliptic curve than for finite fields. Elliptic curve cryptography (ECC) requires the computation of the cardinality of the curves. The elliptic curve key length is shorter than RSA key length. If the key length for ECC is 256 bits, then for RSA, it will be 3072 bits. We conclude that ECC outperforms RSA Algorithm [2].

### 2.2 *Elliptic Curve DiffeHellman Key Exchange (ECDH)*

In complete analogy to the conventional Diffe-Hellman key exchange (DHKE) introduced in [3], we can now realize a key exchange using elliptic curves. This is referred to as elliptic curve Diffe-Hellman key exchange, or ECDH. The elliptic curve Diffe-Hellman key exchange protocol is shown in Fig 1.

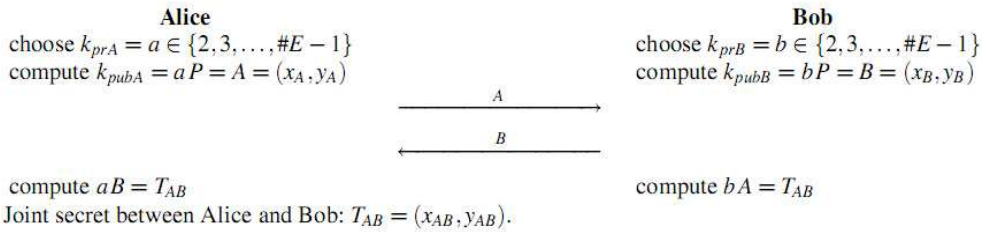


Figure 1. Elliptic Curve Diffe Hellman Key Exchange (ECDH).

## 3. Electronic Payment Systems

An electronic payment is any kind of non-cash payment that does not involve a paper check. Electronic payment lowers cost of businesses. More the payment processed electronically,less cost will be spent on paper and postage. Electronic transaction uses the cryptography for many purposes such as protect the transactions against attack on the network, ensuring the security without prior arrangements between customers and merchants, and to guarantee the transaction.

### 3.1 *Off-Line Electronic Payment Model*

In this model the payees accumulate the digital money, and then deposit it in his account when the network traffics are low. Essential components of this model are [1]: Public Key Certificates, Smart card and Digital Money.

### 3.2 *On-Line Electronic Payment Model*

Major participants [5] of online purchasing system are as below:

**customer:** In the electronic environment, consumers and corporate purchaser interact with the merchant via personal computers over the internet. A customer may be an authorized person having a payment card or account issued by bank.

**Merchant:** A merchant is a person or organization that has goods or services to sell to the customer.Typically these goods and services are offered via a web siteo by electronic mail.

**Financial Institute:** The Financial Institution, such as a bank that provides account for the merchant and possibly a payment card for the customer. These institutes can be act as either aquire from merchant site and issuer from customer site.

**Payment Gateway:** This is the function operated by acquirer or a designated third party. It processes the merchant payment message and authorize it and also authenticate the customer by its digital certificates.

**Certification Authority:** This is the authority that is trusted and issues public key certificates for the customer, merchant and payment gateways.

### 3.3 *Characteristic of E-Payment Systems*

[5] A wide range of systems has been developed for online payment. It is divided into account based and electronic currency systems. Account-based systems allow payment via an existing personalized account(usually a bank account), whereas electronic currency systems allow payment simply if the payer has an appropriate amount of electronic currency. Following are the basic characteristics of different online payment systems.

**Applicability:** Availability (point of sale coverage), payment size(e.g. micro payment, large sums) and destination (e.g. merchant, private persons).

**Ease to obtain:** Ease / complexity of registration.

**Cost:** Distribution of costs between merchants and users cost structure (e.g. fixed transaction charge or proportion of sales value).

**Security:** Customer confidence and economic sustainability, information transmission from buyer to seller, security of information stored on client and seller equipment.

**Anonymity:** Protection of personal information, trade-off between anonymity and traceability for payment support.

With the online purchase payment processing the integrity of payment order information is an important concern. The customers and merchants are not directly in front of each other and entire transaction processes electronically. This leads for a dispute may be produced by either customer or merchant after the transaction. So it is very necessary to verify the integrity of payment and order information on which both customer and merchant are agreed. Following sequence of events occur during the transaction process [5], but in step 5 Payment Authority checks the integrity of payment order information using our new protocol (based on elliptic curve Diffie-Hellman key agreement protocol) and authorize the customer.

1. The customer open an account and get its digital certificates.

2. The merchant acquires his/her digital certificates.

3. Customer opens the web of merchant and places the order to the merchant.

4. Merchant verifies the customer with its digital signature through payment authority.

5. Payment Authority checks the integrity of payment order information using our new protocol and authorizes the customer.

6. Merchant verifies the purchase and confirm the order.

## NEW PROTOCOL EXECUTION:

Let the customer and merchant share common information which are the payment and order information. Let m denotes the payment order information ($m = PI + OI$). But how elliptic curve Diffie-Hellman key agreement could bee used in this protocol? First payment order information ($m = PI + OI$) must be transformed to the point on the elliptic curve. This work (e.g. transform a plaintext into the point on elliptic curve) is presented in [6]. The process flow for transforming the message is given in Fig 2.

On the elliptic curve and the probability of failure is about $\frac{1}{2^k}$. In order to recover the message (m) from the point $P_m = (x, y)$,we calculate m, defined by $m = \lfloor \frac{x}{k} \rfloor$, where $\lfloor \frac{x}{k} \rfloor$ is the grates integer less than or equal to $\frac{x}{k}$.

So we can transform payment order information to a point on the elliptic curve in form of (1). Choose an elliptic curve in form of (1). Suppose $m \to (x_m, y_m) = P_m$.Following sequences are used to verify the integrity of payment order information.

1. Payment authority PA select two integer randomly such as a and b.

2. PA send the integer a to customer and integer b to the merchant.

3. Customer receives the a and compute the value $P_1 = a.(x_m, y_m)$ and send it to the merchant.

4. Similarly merchant receives the b and compute the value $P_2 = b.(x_m, y_m)$

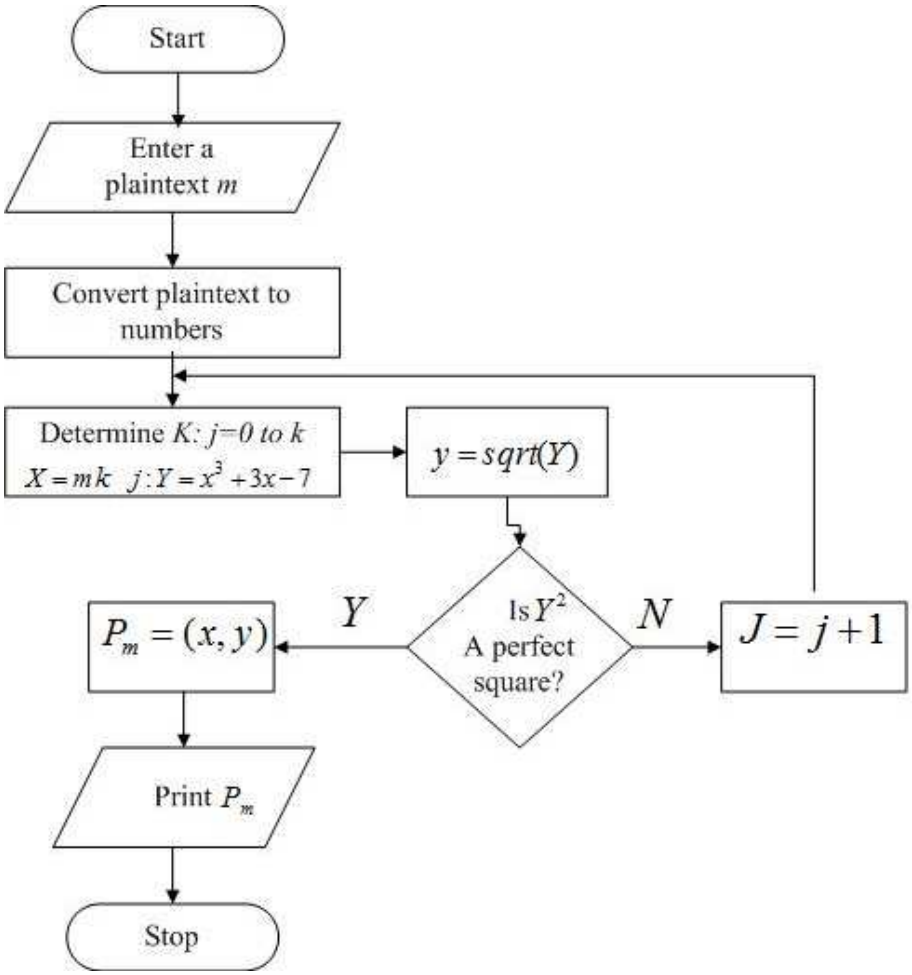


Figure 2. Elliptic Curve Diffe Hellman Key Exchange (ECDH).

and sends it to the customer.

5. Now customer gets $P_2$ from merchant, evaluates $a.P_2$ and sends it to the PA.

6. Similarly merchant gets $P_1$ from customer, evaluates $b.P_1$ and sends it to the PA.

7. Now the PA can verify the m by comparing the values $a.P_2$ and $b.P_1$. Such as

$$a.P_2 = a.b.(x_m, y_m)$$
$$b.P_1 = b.a.(x_m, y_m)$$

At the end of the protocol execution, the Payment Authority can verify the integrity of message by comparing the two values received from customer and merchant by the following two values.

$$a.P_2 = ab.(x_m, y_m)$$
$$b.P_1 = ba.(x_m, y_m)$$

**ANALYSIS**
In this protocol PA can verify the payment order integrity. neither customer nor merchant can be assumed honest. Customer may claim different order or payment information. If he/she tries, it (m) will be changed to $m'$ then

$$(x_m, y_m) \rightarrow (x_{m'}, y_{m'})$$

which shows that

$$a.P_2 = a.b.(x_m, y_m)$$
$$b.P_1 = b.a.(x_{m'}, y_{m'})$$

Therefore the above equation will not be the same and transaction fails. Similarly merchant perhaps claim with different payment order information. Again the two unit will not be same and payment authority can check the wrong payment order message.

$$a.P_2 = a.b.(x_{m'}, y_{m'})$$
$$b.P_1 = b.a.(x_m, y_m)$$

## 4. Conclusions

The model proposed in this paper is best suitable for low and large payment transaction.With this model that is based on elliptic curve cryptography, the online e-payment system security is prepared.In this protocol the integrity of message and payment order information is verified more easely. The properties of ECC such as equivalent security in e-commerce payment system with much smaller key size, low power consumption, low memory usage could enhance e-commerce security on the internet and hence, make electronic transaction and other e-business to be carried out with little or no fear of hackers.

## References

[1] Al-Daoud E., Al-Tahat Kh., Al-Fawareh H. Efficient Electronic Payment System Using Sparse Elliptic Curve Cryptography. International journal of computing & Information sciences (2004) 92-97.
[2] Gura N., Patel A., Wander A., Eberle H., Shantz S. C..Comparing Elliptic Curve Cryptography and rsa on 8-bit CPUs. Cryptographic Hardware and Embeded Systems- CHES (2004), 119-132.
[3] Paar C., Pelzl J., Understanding Cryptography. Springer-Verlag Berlin Heidelberg (2010).
[4] Qingxian W. The Application of Elliptic Curves Cryptography in Embeded Systems. ICESS Proceedings of the Second International Conference on Embedded Software and Systems, pages: , (2005), 527-530.
[5] Raghuwanshi S., Pateria R. K., Singh R. P. A New Protocol Model for Verification of Payment Order Information Integrity in Online E payment System. World Congress on Nature & Biologically Inspired Computing (NaBIC 2009).
[6] Vincent O. R., Folorunso O., Akinde A. D. Improving e-payment security using Elliptic Curve Cryptosystem. Electron Commerce Res, Springer Science, **10** (2010) 27-41.