A Secure Money Transaction Scheme (Identification Scheme) using Elliptic Curves

Atul Chaturvedi
Department of Mathematics
PSIT, Kanpur (UP)

Varun Shukla
Department of Electronics and Communication
PSIT, Kanpur (UP)

ABSTRACT
Identification protocols have an important role for building secure communications amongst two or more entities over the internet. In this paper we introduce a new identification scheme (or money transaction protocol) based on the elliptic curve Diffie - Hellman problem. We show that our protocol meets the security attributes under the assumption that the elliptic curve discrete logarithm problem is secure.

Keywords
Identification schemes, elliptic curve Diffie – Hellman problem, secure communication, discrete logarithm problem

1. INTRODUCTION
In recent years several proposals [2, 3] have emerged for secure two party authentication schemes for secure communication using elliptic curves. The idea of using the elliptic curve as a platform for cryptosystems was introduced in [4, 7]. The elliptic curve cryptosystems which are based on the elliptic curve discrete logarithm problem (ECDLP) over a finite field have some advantages over other systems: the key size can be much smaller than those in the other systems as exponential - time attacks have only been known so far if the curve is carefully chosen [5].

Here we propose an entity authentication (or money transaction management) scheme using key agreement protocol on elliptic curves. We also prove security of our scheme.

It is well known fact that an identification scheme is an important and useful cryptographic tool. It is an interactive protocol where a Bank customer Alice (an assuror) tries to convince a verifier (for example Bank), of his identity. Only Alice knows the secret value corresponding to his public one and the use of this secret value allows Alice to convince Bank of its identity.

The rest of the paper is organized as follows: We present a brief introduction of Identification schemes in section 2. In section 3, we define elliptic curve Diffie – Hellman Key Agreement scheme. In section 4, we present our identification schemes, and we give a proof of security and zero - knowledge for our schemes. The paper ends with conclusion.

2. IDENTIFICATION SCHEMES
An identification scheme or entity authentication protocol is used to prevent impersonation. This protocol allows one party to gain assurances that the identity of another is as declared.

It is an interactive protocol which involves an assuror or a Bank customer Alice and a verifier Bank. In general, Alice tries to convince the verifier (Bank) of his identity. The verifier is present with, or presumes beforehand, the purported identity of the assuror. The aim is to corroborate that the identity of the assuror is indeed Alice (a genuine Bank customer). Only Alice knows the secret value corresponding to his public one and it is the proper use of this secret value which allows Alice to convince Bank of the identity of him.

The objective of an identification protocol includes the following.

- In the case of honest parties Alice and Bank, Alice is able to successfully authenticate himself to Bank.
- (Transferability) Bank cannot reuse an identification exchange (communication) with Alice so as to successfully impersonate Alice to a third party say, Eve.
- (Impersonation) The probability that any third party Eve is different from Alice, carrying out the protocol and playing the role of Alice, can cause Bank to accept Alice’s identity is negligible.
- The previous points hold even if a polynomial large number of previous authentication between Alice and Bank have been observed: the adversary Eve has participated in previous protocol executions with either or both Alice and Bank; and multiple instances of the protocol, possibly initiated by Eve, may run simultaneously.

3. ELLIPTIC CURVE DIFFIE-HELLMAN KEY AGREEMENT
Many researchers have examined elliptic curve cryptosystems, which were firstly proposed by Miller [7] and Koblitz [4]. The elliptic curve cryptosystems which are based on the elliptic curve discrete logarithm problem (ECDLP) over a finite field and this problem is defined as follows.

Definition 1: Let E be an elliptic curve defined over a finite field \( F_q \) and let \( P \in E \left( F_q \right) \) be a point of order \( n \). Given \( Q \in E \left( F_q \right) \), the ECDLP is to find the integer \( a \), \( 0 \leq a \leq n -1 \), such that \( Q = aP \).

This paper we use an elliptic curve defined over a finite field \( F_q \) of characteristic \( p \). Firstly, we choose elliptic curves domain parameters [6]:

- A field size \( q \), where \( q \) is a prime power (either \( q = p \), an odd prime, or \( q = 2^m \))
- Two field elements \( r,s \in F_q \), which define the equation of the elliptic curve \( E \) over \( F_q \) (i.e. \( y^2 = x^3 + r \cdot x + s \) in the case \( p > 3 \), where \( 4r^3 + 27s^2 \neq 0 \)).
• Two field elements \( x_p \) and \( y_p \) in \( F_p \) which define a finite point \( P = (x_p, y_p) \) of prime order in \( E(F_p) \). \( P \neq O \), where \( O \) denotes the point at infinity.
• The order \( n \) of the point \( P \).

With these notations the elliptic curve Diffie – Hellman key agreement [ECDHKA] [6] is describes as follows:

**Definition 2:** In ECDHKA, two communicating parties \( Alice \) and \( Bank \) agree to use the same curve parameters. They generate their private keys \( a \) and \( b \) and corresponding public keys \( Q_a = a.P \) and \( Q_b = b.P \). The parties exchange their public keys. Finally each party can share the secret key \( K = aQ_b = bQ_a \).

4. THE PROPOSED SCHEME

4.1 Objective

To save the hard earned money of the customers being misappropriated, stolen or withdrawn by cheat is the main purpose of authentication.

The growth of identity theft (Bank fraud, credit card fraud etc.) appears to be tied to technology, particularly the internet and the identity theft is becoming an increasing threat to consumer confidence in the internet as a means to conduct business.

Sophisticated theft, hacking, fraud is being committed by the professional criminal who are able to get personal details of the customers through various sources. Thus to save the customers valuables from fraudster’s path the solution is authentication.

It is a process by which the Bank customer determines that the customer is who he/she says that they are. The main purpose of this paper is to verify the person’s information through an electronic transmission to the Bank that he/she is a genuine customer and they have the right to access their accounts digitally. For example there can be digital signatures (an encrypted segment of software) which is also known as digital certificate. This paper gives an insight into how a Bank authenticates their customers and grant the permission for further transaction.

4.2 Step Process

Here we proposed an authentication scheme i.e., the initial setup known to both the parties \( Alice \) (a Bank customer) and \( Bank \) as follows. Let \( E \) be an elliptic curve defined over a finite field \( F_p \) and let \( P \in E(F_p) \) be a point of order \( n \). We assume that the ECDLP is hard in \( E \). We also take \( h \) as a fixed collision-free hash function. The scheme runs as the following steps

1. User \( Alice \), a Bank customer wishes to withdraw some money out of his account from any Bank digitally (for example a ATM). For the safe play \( Alice \) chooses a secret number “a” between 1 and \( n – 1 \) (or in other words we can say he assigns a password to himself). He gives the own created identity \( X_A = aP \) to Bank. This identity is different for different customers and this code is saved with the Bank as an exclusive identity of customer \( Alice \).

2. For the purpose carrying on a transaction, say \( Alice \) desires to withdraw $1000 from the Bank. For this, the code generated by \( Alice \), i.e. \( X_A \) is submitted to Bank for authentication.

3. After receiving the code \( X_A \) of Alice, the part of Bank comes in play. Bank randomly choose a number “h” between 1 and \( n – 1 \) and send \( X = h(\text{bP}) \) as a challenge to the customer \( Alice \) to verify that he is a genuine customer of the Bank.

4. On receiving the code \( X \) from the Bank, Alice sends the response \( Y = h(aX) \) to the Bank.

5. The response so send by Alice to the Bank is cross checked with the \( X_A \) (code which is already available with the Bank as an original identity proof of the customer Alice) by computing \( h(bX_A) \). If \( h(bX_A) = Y \), then Bank verifies that \( Alice \) is a genuine customer and should be permitted for further transaction.

6. Bank will repeat this protocol \( k \) times till the Bank gets satisfied that \( Alice \) is a genuine customer. If any condition is not satisfied from step 1 to 6, \( Alice \) can be denied access to the system.

4.3 Security Analysis

**COMPLETENESS:** Assume that, at step 4, \( Alice \) send \( Z \), then Bank accepts \( Alice \)’s proof if and only if we have \( Z = h(bX_A) \) or if and only if \( Z = h(b(a.X) \) or if and only if \( Z = h(aX) \) or if and only if \( Z = h(a.a.X) \) or if and only if \( Z = h(a.x) \) or if and only if \( Z = Y \)

**SOUNDNESS:** Assume a cheater \( Eve \) is accepted with non-negligible probability. This means that \( Eve \) can compute \( h(bX_A) \) with non-negligible probability. As \( h \) is supposed to be an ideal hash function, this means that \( Eve \) can compute \( x \) satisfying \( h(x) = h(bX_A) \) with non-negligible probability. There are two possibilities: either \( we have x = bX_A \) which contradicts the hypothesis that the ECDLP is hard or \( x \neq b. X_A \) which means that \( Eve \) and Bank are able to find a collision for \( h \), contradicting the hypothesis that \( h \) is collision free.

**HONEST-VERIFIER ZERO-KNOWLEDGE:** After the completion of the protocol an honest verifier gets no knowledge of the secret key of \( Alice \). More formally, if a probabilistic turning machine chooses random \( b \) using the same drawing as the honest verifier, and outputs the instances \( (b.h(bX_A)) \), then the instance generated follows the same probability distribution as the ones generated by \( Alice \) and Bank.

5. CONCLUSION

In present scenario security in each sector including banking transactions is very important and there is lacking of significant work towards the banking security. This paper initiated a secure identification scheme for transactions in banking sectors. The security of our scheme is based on the security of Elliptic curve Diffie – Hellman problem.
6. REFERENCES


