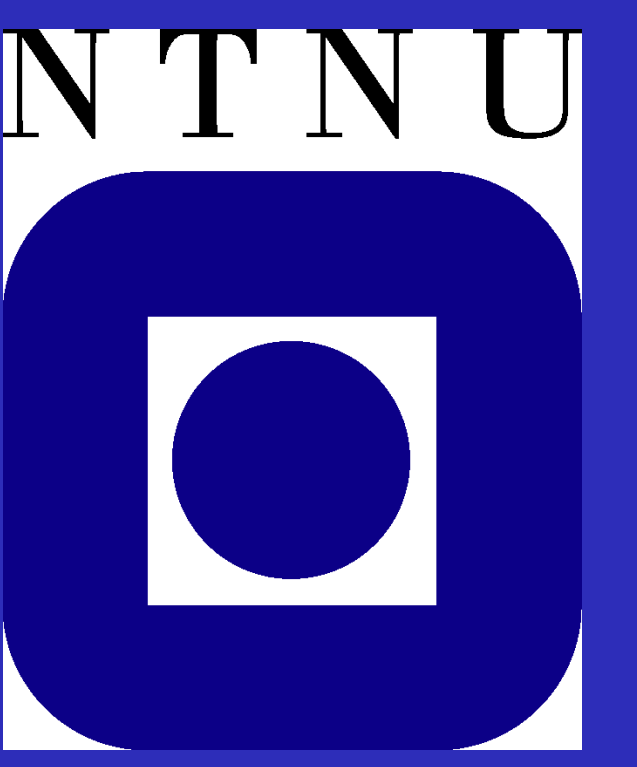




# MUTUAL AUTHENTICATION BASED ON ELLIPTIC CURVE CRYPTOSYSTEM

Trang Tran Thi Thuy

Helsinki University of Technology, Finland  
Norwegian University of Science and Technology, Norway  
ttranthi@cc.hut.fi



## INTRODUCTION

While demand on shopping online grows tremendously, it seems that many users still don't pay enough attention to the security of their online transaction. Due to lack of enough users' carefulness, the number of phishing cases is still increasing. Hence, mutual authentication scheme have been proposed not only as a solution for this problem but also as a increasing need when weak computing power such as smart card system. In this poster, we introduce a mutual authentication based on Elliptic Curve Crypto-system. Our scheme is against forgery attack and replay attack. The scheme was inspired by Identification Scheme based on RSA by Tatsuaki Okamoto

## FUNDAMENTAL THEORY

An elliptic curve  $E$  over a field  $F$  is the set of solutions  $(x;y)$  which satisfy the Weierstrass equation:

$$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

We can construct an Abel group from all points on the elliptic curve by defining the addition operator (+) and scalar multiplication operator (\*).

### ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Given elliptic curve  $E$ , and point  $G$  with order  $n$ , the elliptic curve discrete logarithm problem is to find the unique integer  $k$ ,  $1 \leq k \leq n$  such that

$$Q = k * G$$

if such an integer exists.

## AGAINST REPLAY ATTACK

The adversary cannot perform a replay attack because the authentication server generates different pair of numbers  $(r_1, r_2)$  at the beginning of different authentication process.

## AGAINST FORGERY ATTACK

The adversary have to construct a valid sequence  $\langle x_1', x_2', e' \rangle$ . Therefore, we have:

$$x_1'P_1 + x_2'P_2 + e'Z = X \quad \text{and} \quad e' = H(X_x || X_y)$$

We have:

$$x_1'P_1 + x_2'P_2 + e'(-s_1P_1 - s_2P_2) = X$$

$$(x_1' - e's_1)P_1 - (x_2' - e's_2)P_2 = X$$

Suppose that the user with the secret key chose 2 numbers

$$r_1 = x_1' - e's_1 \text{ mod } h \quad \text{and} \quad r_2 = x_2' - e's_2 \text{ mod } h \quad (1)$$

So  $e = H(X_x || X_y) \neq e' = H(X_x || X_y)$

$$\text{And} \quad x_1 = r_1 + es_1 \text{ mod } h \quad \text{and} \quad x_2 = r_2 + es_2 \text{ mod } h \quad (2)$$

From (1) and (2), we have equations

$$x_1' = r_1 + e's_1 \text{ mod } h \quad x_2' = r_2 + e's_2 \text{ mod } h$$

$$x_1 = r_1 + es_1 \text{ mod } h \quad x_2 = r_2 + es_2 \text{ mod } h$$

From this, we can compute  $(s_1, s_2)$ :

$$(s_1, s_2) = ((x_1 - x_1') / (e - e')) \text{ mod } h, (x_2 - x_2') / (e - e') \text{ mod } h \quad (3)$$

We have equation  $Z = -s_1P_1 - s_2P_2$  has  $n$  solutions  $(s_1, s_2)$  if given  $\langle x_1', x_2', e' \rangle$ . We suppose to have two different solutions  $(s_1, s_2)$  and  $(s_1^*, s_2^*)$  both satisfying  $Z = -s_1P_1 - s_2P_2$ . Choose  $r_1^* = r_1 + e(s_1 - s_1^*) \text{ mod } h$  and  $r_2^* = r_2 + e(s_2 - s_2^*) \text{ mod } h$ , we have 3 equations:

$$Z = -s_1P_1 - s_2P_2 = -s_1^*P_1 - s_2^*P_2$$

$$x_1 = r_1 + es_1 = r_1^* + es_1^* \text{ mod } h$$

$$x_2 = r_2 + es_2 = r_2^* + es_2^* \text{ mod } h$$

All three above equations satisfying the given sequence  $\langle x_1, x_2, e \rangle$ . Therefore, we cannot determine which  $(s_1, s_2)$  is the accurate secret pair generating the sequence  $\langle x_1, x_2, e \rangle$  and because  $(r_1, r_2)$  and  $(r_1^*, r_2^*)$  have the same probability of being chosen (because of random choosing), the probability of the solution  $(s_1, s_2)$  of equation (3) different from original  $(s_1, s_2)$  is  $(n-1)/n$ . We call it  $(s_1^*, s_2^*)$ . Then, we have:

$$-s_1P_1 - s_2P_2 = -s_1^*P_1 - s_2^*P_2$$

$$P_1(s_1 - s_1^*) = P_2(s_2 - s_2^*)$$

By this reasoning, in a possible period of time, with the probability of  $(n-1)/n$ , we can solve the ECDLP problem with 2 points  $P_1$  and  $P_2$ . That is illogical and denies the assumptions of ECDLP. That is why the forgery attacks are impossible in our authentication scheme.

## MUTUAL AUTHENTICATION SCHEME

The scheme includes three main phases

### SETUP PHASE

Suppose that the system parameters for an Elliptic curve over finite field  $F_p$  or  $F_{2^m}$  as follows:

$$T = \langle q, FR, a, b, G, n, h \rangle$$

$q$ : prime  $p$  or  $2^m$  decides a finite field

$FR$ : the field representation

$a, b$ : the curve coefficients

$P_1, P_2$ : Two points of order  $n$  on the curve

$n$ : order of  $P_1, P_2$ .  $N = \#E(F_q)$  is divisible by  $n$

$h$ :  $\#E(F_q)/n$

We assume that the ECDLP problem is hard to solve under defined elliptic curve above. We have

$H: \{0,1\}^* \rightarrow Z_q^*$  is a hash function

Registration server **RS** picks up an secret key  $(s_1, s_2)$  with  $s_i \in Z_n$   $i=1,2$  and computes public key  $Z = -s_1P_1 - s_2P_2$  and transfers public key  $Z$  to authentication server **AS**.

Authentication server **AS** chooses a secret key  $(a_1, a_2)$  with  $a_i \in Z_n$   $i=1,2$  and computes public key  $AS_{PUB} = -a_1P_1 - a_2P_2$  and transfers public key  $AS_{PUB}$  to registration server **RS**.

### REGISTRATION PHASE

User authenticate himself with **RS** and **RS** provide user with secret keys  $(s_1, s_2)$ ,  $AS_{PUB}$  in a secure manner.

## MUTUAL AUTHENTICATION

