An identity authentication solution based on ECC for mobile terminal

Jie Deng1,a, Juan LI2,b
1Office College of Chinese Armed Police,Chengdu,610213 China
2Office College of Chinese Armed Police,Chengdu,610213 China
adjie_2006@126.com, bemail:954949592@qq.com

Abstract

With the development of mobile communication technology, there are more and more concern about the mobile cyber security. However, numerous existing authentication solutions have the issues as encryption and decryption keys long, slow, consuming large storage space and transmission bandwidth. This article presents an approach based on elliptic curve cryptography is suitable for the identity of the mobile terminal lightweight equipment certification program, which improve efficiency, while reducing the bandwidth consumption of transmission. Therefore, the solution has a great potentiality in the application of intelligent terminal.

Keywords: identity authentication

Introduction

With the fast development of mobile communication technology, as well as its own mobile platform openness and flexibility, mobile phone has became indispensable in people's lives and work. Meanwhile, it has also become another target for hackers. Because of the data theft, tampering; unauthorized users of theft, attacks and other malicious programs for mobile platforms the security issues have become increasingly prominent. So what protective measures adopted to protect the safety of mobile phone is the focus of attention [2].

With the development of the theory of the cipher code, the mobile terminal may also need to implement user authentication. In document [3], a bidirectional authentication solution based on ELGamal digital signature was proposed against the flaws of low efficient authentication and complicated process. However the proposed solution also has the flaws as the key has to be exchanged face to face, and the certification process is too cumbersome. As an enhancement, document [4] proposed an bidirectional authentication solution based on ELGamal digital signature which improved the secured transmission over common signal tunnel, with no necessity of face to face password exchange, simplified the authentication process as well for better efficiency. However, the solution can’t prevent the fraud attack, yet the algorithm for public key of ELGamal is too complicated to be applied in a light mobile device to avoid huge heat, slow response and burning of the precision device.

In today's public-key cryptosystem, ECC key system has the highest per-bit security strength, and has a short key, fast speed, high security and low computational complexity [5] as advantage. Therefore, by taking advantage of elliptic curve cryptography system, this paper proposes an identity authentication solution based on ECC for light mobile device with the idea of document [4]. The solution remains the same security of the original solution proposed in document [4], meanwhile it simplify the key negotiation, enhance the efficiency by deducting the complexity of the identity certification. Because of the above advantages the solution is applicable for the mobile communication. Its innovation lies in: (1) A secure channel isn’t compulsory to get the keys, which improves the flexibility of key management. (2) It decreases the calculation burden of key negotiation and authentication processes; improve the efficiency of authentication, applicable for mobile communication; (3) it is easy to implement authentication and digital signatures in a distributed environment.

1.ECC-based Bidirectional Authentication Solution

The authentication solution is divided into three steps: registration, the key acquisition and user authentication. The certification idea is based on digital signature of elliptic curve encryption algorithms.

Symbols specification is used in the solution:

Fq is a selected finite field, $\mathrm{E(Fq)}$ is the elliptic curve on a finite field Fq, G is the $\mathrm{E(Fq)}$ base point of the elliptic curve, n (a large prime number), A and B denotes the two-user, IDA and IDB presents the flag information of A and B, $\mathrm{H()}$ is the hash function.

In this solution, LRA is the advance operation of a trusted local registration authority center:

① Select a unused integer $d \in [1, \mathrm{n}-1]$,Calculate：$Y = d \cdot \mathrm{G} \in \mathrm{E(Fq)}$

② Open the public key information to system:$\mathrm{E(Fq)}$，G，Y，n. Reserve the private key d.

1.1 User Register

（1）user h offline register to the closest LRA, the detail registration procedure is as blow:

① User h selects a random $\mathrm{k} \in [1, n-1]$ as temporary private key.

② Calculate $\mathrm{C1} = \mathrm{k} \cdot \mathrm{G} = (\mathrm{x1}, \mathrm{y1}), \mathrm{C1}$ as the temporary public key.$\mathrm{t1} = \mathrm{x1} \bmod \mathrm{n}, \mathrm{if}\ \mathrm{t1} = 0$,then return to step ①, then send the message $\{ID_h, \mathrm{C1}\}$ to LRA.

（2）When LRA receive the message, then do the following calculation:

① $\mathrm{m1} = \mathrm{ID_h} \oplus \mathrm{ID_{LRA}} \oplus \mathrm{T_h}$，and present $\mathrm{m1}$ as a domain element $\mathrm{P_m^1}$. Above $\mathrm{T_h}$ is the legal duration of temporary public key $\mathrm{C1}$, and save the information$\{\mathrm{ID_h}, \mathrm{C1}, \mathrm{T_h}\}$.

② calculate：$\mathrm{V1} = \mathrm{d_{LRA}} \cdot \mathrm{C1} + \mathrm{P_m^1}$,and send the cipher text｛V1，$\mathrm{T_h}$｝to user h.

1.2 Key Acquisition

（1）After user h receive the information, the following process will be done：

① calculate $\mathrm{C2} = \mathrm{k} \cdot \mathrm{Y}_{LRA}$，$\mathrm{m1} = ID_h \oplus ID_{LRA} \oplus T_h$，and present m1 as a domain element$\mathrm{P_m^1}$.

② Verify the truth of formula $\mathrm{C2} + \mathrm{P_m^1} = \mathrm{V1}$. If the result is false, authentication is failed.

③ If the authentication passed, user h calculates $\mathrm{e} = \mathrm{H}(ID_h)$, $\mathrm{C4} = \mathrm{k} \cdot \mathrm{Y_{LRA}} + \mathrm{e} \cdot \mathrm{G}$; and send the message $\{\mathrm{ID_h}, \mathrm{C4}\}$to LRA.

（2） LRA verify the legality of user h ,the detail procedure is as below:

① Verify the truth of $\mathrm{e} \cdot \mathrm{G} + \mathrm{d} \cdot \mathrm{C1} = \mathrm{C4}$，then decide the legality of user h accordingly.

② If the identity of user h is legal, then select an private key $\mathrm{d_H}$ randomly which is not existed in the database. Calculate $\mathrm{m2} = \mathrm{d_H} \oplus \mathrm{T_h} \oplus \mathrm{ID_h}$, and present m2 as a domain element $\mathrm{P_m^2}$, and select a random r ,calculate $\mathrm{V2} = \mathrm{r} \cdot \mathrm{G} = (\mathrm{x3}, \mathrm{y3})$,if $\mathrm{x3} \bmod \mathrm{n} = 0$，then return to reselect r.

③ Calculate $\mathrm{V3} = \mathrm{r} \cdot \mathrm{C1} = (\mathrm{x4}, \mathrm{y4})$，if $\mathrm{x4} \bmod \mathrm{n} = 0$，then return to step ② to reselect r.

④ Generate the cipher text $S^* = \{\mathrm{V2}, \mathrm{P_m^2} + \mathrm{V3}\}$ and send to user h.

（3）the user h does the following calculation by using temporary private key k of itself：

$$(P_m^2 + V3) - k \cdot V2 = P_m^2 + r \cdot k \cdot G - k \cdot r \cdot G = P_m^2$$

Through P_m^2 get $m2$，and then calculate $d_H = \mathrm{m2} \oplus T_h \oplus ID_h$，and then calculate $\mathrm{V} = (ID_h \oplus d_H) \cdot G$, send message $\{ID_h, V\}$ to LRA..

（4）LRA calculate $\mathrm{V'} = (ID_h \oplus d_H) \cdot G$，verify whether V‘ equal to V,and delete $\{ID_h, \mathrm{C1}, T_h\}$ if the verification result is legal. LRA destroy the temporary public key and temporary private key.

1.3 User authentication

The authentication solution is specified as below by with the example of user IDA and user IDB, and detail specification of the authentication flow:

① User IDA send message {IDA，IDB} to LRA.

② LRA inquires private key d_B of IDB, then calculate the public key of IDB $Y_B = d_B \cdot G$ and send Y_B to IDA.

③ IDA calculate $\mathrm{m} = \mathrm{IDA} \oplus \mathrm{IDB}$, and represent m as a domain element Pm, select a random k，calculate： $\mathrm{R} = \mathrm{k} \cdot \mathrm{G}$，$\mathrm{S} = \mathrm{Pm} + \mathrm{k} \cdot Y_B$，$\mathrm{T} = \mathrm{k} \cdot Y_A$，Then send information {R,S,T} to user IDB.

④ IDB uses own private key and calculate $\mathrm{S} - \mathrm{d_B} \cdot \mathrm{R} = \mathrm{Pm} + \mathrm{k} \cdot \mathrm{d_B} \cdot$

$\mathrm{G}-\mathrm{d_B}\cdot\mathrm{k}\cdot\mathrm{G}=Pm$,through Pm get m ,then calculation $\mathrm{m}'=\mathrm{m}\oplus\mathrm{IDB}$, Then user IDB calculate $V^*=\mathrm{d_B}\cdot\mathrm{T}+\mathrm{Pm}'$,Pm′is the domain element of m' and send message ｛V^*｝ to IDA.

⑤ After IDA decrypt message with its own private key $\mathrm{d_A}$and k，get $\mathrm{Pm}'=\mathrm{V}^*-\mathrm{k}\cdot\mathrm{d_A}\cdot\mathrm{Y_B}$， through Pm' get m' ,and compare the equality of m' and IDA .if m' equal to IDA means the authentication is successful, otherwise means the authentication failed.

2.Security analyses

The security of this solution includes two parts: 1）It is secure during the key acquisition. 2）the procedure of identity realization is logical and correct.

2.1 Security during the key acquisition

The procedure of key acquisition is secure, which can demonstrate as below three situations.

（1）if the attacker IDC pretend to be the identity of ID_h, the authentication will failed.

Proof：

②Attacker IDC select k' randomly，send $\{ID_C,\mathrm{C3}\}$ to LRA , $\mathrm{C3}=\mathrm{H}(ID_C)\cdot\mathrm{G}+\mathrm{k}'\cdot Y_{LRA}$.

③ LRA verify $\mathrm{C3}=d_{LRA}\cdot C1+\mathrm{H}(ID_C)\cdot G$ is true by using d_{LRA}. It is equal to verify $k'\cdot d_{LRA}\cdot G=d_{LRA}\cdot C1$，

IDC to be able to guess k' to make the LRA verification to be passed, that is solving the elliptic curve discrete logarithm problem. So validation bound to fail.

（2）If the attacker IDC counterfeit identity of LRA, authentication will fail.

Proof：

① Attacker IDC counterfeit LRA to calculate $\mathrm{m1}'=ID_h\oplus ID_C\oplus T_h$‘，and represent m1‘ as a domain element $\mathrm{P_m^{1'}}$； Calculate $\mathrm{V1}‘=d_C\cdot C1+P_m^{1'}$, and send ｛V1‘，$T_h$‘｝ to user h;

② User h calculate $\mathrm{m1}'=ID_h\oplus ID_C\oplus T_h‘,C2=k\cdot Y_{LRA}$,and then verify the truth of $\mathrm{C2}+\mathrm{P_m^{1'}}=\mathrm{V1}$ to confirm the message is from LRA. It is equal to verify $k\cdot d_{LRA}\cdot G=d_C\cdot k\cdot G$；

If the verification pass, except attacker can get the private key d_{LRA} of LRA, it is impossible, so verification is bound to fail.

（3）if the attacker do the intermediate attack, key can’t acquired yet.

If the attacker attack $S^*=\{V2,P_m^2+V3\}$，however the attacker can’t acquire k of user h, thus it can’t solve S^* to acquire P_m^2，which means attacker is impossible to acquire private key d_H of user h assigned by LRA.

2.2 Logicality and correction of the identity authentication procedure

（1）logicality of the authentication procedure

The message of {R, S, T} can only be decrypted by IDB because only IDB knows d_B to get the identity of IDA. Only IDA can decrypt V^* because only IDA knows d_{A} and fresh digit k to get the legal identity of IDB.

（2）Correct of authentication procedure

If the attacker attacks {R,S,T}, user IDB can use its own private key to pass the authentication, however it cannot decrypt{R,S,T} to get m' ,so IDB unable to get the identity of IDA, so the attacker will fail to counterfeit identity of IDA. If the attacker counterfeit identity of IDB and send V^* message to IDA, however the attacker cannot get $\mathrm{d_B}$. Thus user IDA can't pass the signature of message V^* by public key authentication of IDB. As the result, counterfeit of IDB fails as well.

3.Efficiency Analyses

The solution select SQL Serve2008 database in VC # .NET integrated environment to realize ECC encryption and ELGamal decryption and transmission. The system efficiency can be evaluated from Computational overhead, Key Length and required bandwidth.

（1）Computational overhead analysis

Computational overhead and computational load is the amount of computation required to complete the encryption and decryption (The number of time units required). From the analysis of table1 ECC computation overload is smaller than ECC computation overload and has the advantage of faster processing.

Table1 comparison of ECC & ELGamal computation overload

Cryptography	ECC	ELGamal(n=1024bit)
Encryption/ authentication	120	480
Decryption/ signature	60	240

（2）Key length analysis

Key length determines the number of bits of the storage key and system parameters needed. As can be seen from Table 2, in the condition of the same security level, ECC ELGamal key needed is much smaller than as shown in Table 1.

Table2 comparison of ELGamal and ECC key length

ECC/bit	ELGamal/bit	Length
128	512	1:4
256	3072	1:12

（3）Bandwidth analysis

Bandwidth refers to the required bits for transmission of encrypted information or signature. When the public key cryptography used for encryption or digital signature, a similar bandwidth is required. From Table 3, for the signature of 2000bit and encryption of 100bit short message, ECC can provide a greater bandwidth savings than ELGamal.

Table3 bandwidth comparison for signature and encryption

Algorithm	Signature length/bit	Cipher text size/bit
ELGamal	1024	1024
ECC	320	321

Conclusions

Based on the full analysis of the various deficiencies of the prior existence of identity authentication technology, based on the research results for reference, this paper propose a suitable authentication solution for lightweight mobile device. The solution has a high data security, fast data processing capabilities and lower data transfer bandwidth, suitable for mobile terminal authentication and digital signatures wireless network environment.

References

[1]ZHANG Deyu,XU Lian.Research on an Improved Two-way Dynamic Password Authentication Method[J]. Journal of Shenyang Ligong University,2013,32(5):23-26.

[2]WANG Juan,TANG Ximing,WANG Yong. An Identity Authentication System Based on Mobile-Token and NFC Technology[J]. Journal of Wuhan University(Natural Science Edition),2013,59(5):403-410.

[3]HU Jianjun,WANG Wei,PEI Dong-lin. Double-way Authentication Scheme Based on ELGamal Digital Signature[J]. Computer Engineering,2010,36(6):173-174.

[4]HONG Xiaofen,HU Jian-jun. An Improved Double-Way Authentication Scheme Based on ELGamal’s Digital Signature[J]. Journal of Gansu Lianhe University(Natural Science Edition),2011,25(3):49-54.

[5]XU Dewu,CHEN Wei. Digital Signature and Encrypt Algorithm Based on Elliptic Curve[J]. Computer Engineering, 2011, 37(4):168-169.