Research Journal of Applied Sciences, Engineering and Technology 4(18): 3437-3439, 2012
ISSN: 2040-7467

Submitted: April 17, 2012 Accepted: May 06, 2012 Published: September 15, 2012

Improved Digital Signature Scheme Based on Elliptic Curve

[1]Yunpeng Zhang, [1]Tong Chen, [2]Xianwei Zhang and [1]Weidong Zhao
[1]College of Software and Microelectronics, Northwestern Polytechnical University, 710072 Xi'an, China
[2]Department of Computer Science, University of Pittsburgh Pittsburgh, PA 15260 USA

Abstract: Compared with public key cryptography such as RSA, elliptic curve cryptosystem owns features like high security, low computation overload, short key size and less bandwidth and therefore this system has been recognized by the world and has been applied into digital signature field. However, the current elliptical curve signature scheme has the shortage of low defense of birth defects. Accordingly, this study introduces a new scheme based on two random numbers to decrease the possibility of the same random number used in two signatures. After the analysis of security and complexity, it is proved that the scheme can defend birth defects better and thus improves the security of signature. Besides, the signature scheme has the features of automatically recovery, low computational complexity and easy operation.

Keywords: Cryptography, digital signature, elliptic curve

INTRODUCTION

Digital signature is not only one significant authorization but also the focus of current study of cryptography. Digital signature is the equivalent of daily handwritten signature whose main function is to realize the authorization of information stored in digital form. The security of signature depends on the difficulty of calculating discrete logarithm, factorizing and finding the second remains. Although RSA is the typical digital signature scheme, it has a series of disadvantages such as easily being forged, low calculation speed and excessively high length of the signature.

The attraction of elliptic curve cryptography (Youan *et al*., 2006) is that key length can be shortened with the same security when compared with other public-key cryptosystems (Table 1).

In terms of security, Elliptic Curve Cryptosystem with 163-bit key length is equivalent to RSA with 1024 bits. In other words, with the same security, key length used by ECC is 84% shorter than that of RSA and this makes ECC's lower requirements of storage space, bandwidth and processor speed. This advantage is extremely important for mobile user terminals with limited resources. At present, ECC has been widely used and various relevant hardware and software products have emerged. So, it can be estimated that ECC will replace RSA and become the primary public-key system in the future.

According to literature (Shun *et al*., 2004), the process of sign and verification of ECDSA, the current elliptic curve digital signature, can be described in the following flow chart (Fig. 1 and 2):

Table 1: Comparison of security of key length between ECC and RSA

ECC key length	RSA key length	Computer decryption cost (years) 100,00,000 instructions per sec
160	1024	IE+12
320	5120	IE+36
600	21000	IE+78
1200	l20000	IE+168

Similar to birthday problem, the possibility of choosing the same secret key twice is calculated to be $p = 1 - P_{n-1}^{t} / (n-1)^{t}$, t is the times of signature, to ensure p is bigger than 0.5, then t should be about $\sqrt{n-1}$ to break the private key c_A of A. Assuming that the same k is chosen in two signatures, $s_1 = k + r_1 c_A \pmod{n}$, $s_2 = k + r_2 c_A \pmod{n}$, then $c_A = r_{-1}(s_1 - s_2)$.

To enhance security, the improved scheme uses two random numbers to decrease the possibility of choosing the same private key (Gu, 2007).

SCHEME DESIGN

The specific algorithm and the initialization process are as following:

Assuming that user A owns private keys c_{A1} and c_{A2}, public key D_{A1} and D_{A2}, $c_{A1}, c_{A2} \in \{1, 2, 3, ..., n-1\}$ and $c_{A1} \neq c_{A2}$, $D_{A1} = c_{A1}P$, $D_{A2} = c_{A2}P$; user B owns private key c_B, public key D_B and $c_B \in \{1, 2, 3, ..., n-1\}$, $D_B = c_B P$;
The signature process (Fig. 3):

- User A chooses random numbers $k_1, k_2 \in \{1, 2, 3, ..., n-1\}$, k_1, k_2 is called message key.

Corresponding Author: Yunpeng Zhang, College of Software and Microelectronics, Northwestern Polytechnical University 710072 Xi'an, China

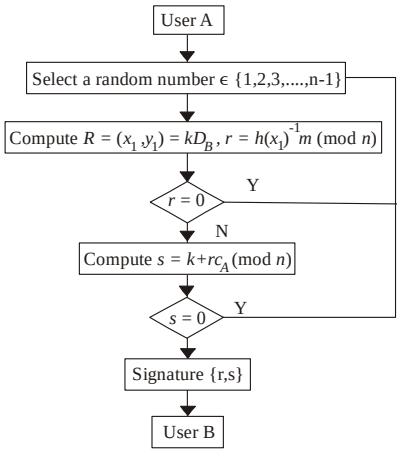

Fig. 1: Sign process of ECDSA

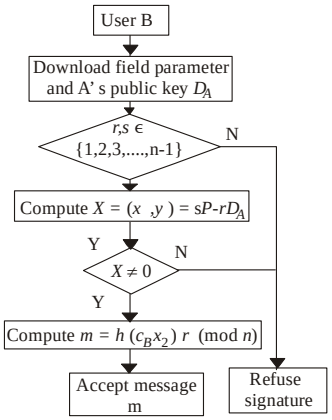

Fig. 2: Message recovery and verification process of ECDSA

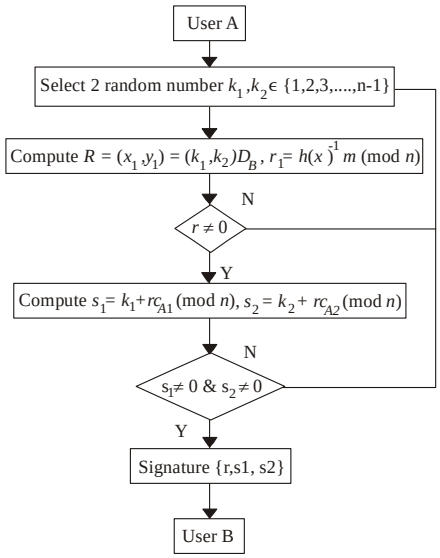

Fig. 3: Signature process of improved elliptic curve digital signature scheme

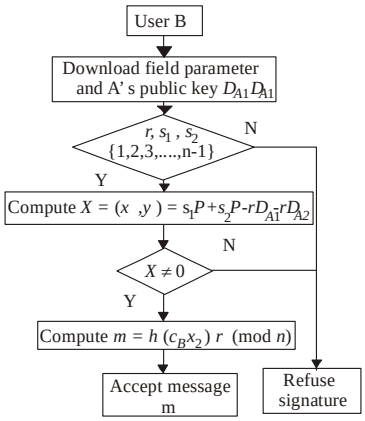

Fig. 4: Message recovery and verification process of improved elliptic curve digital signature scheme

- Compute $R = (x_1, y_1) = (k_1+k_2)D_B$, $r = h(x_1)^{-1}m \pmod n$, if r = 0, then return (1).
- Then compute $s_1 = k_1+rc_{A1} \pmod n$, $s_2 = k_2+rc_{A2} \pmod n$, if $s_1 = 0$ or $s_2 = 0$, then return (1).
- User A sends the signature of message m {r, s1, s2} to user B.

Message recovery and verification process (Fig. 4):

- User B receives signature {r, s1, s2}, he/she will first downloads the domain parameters along with user A's public keys D_{A1} and D_{A2}.
- Check whether r, s1, s2 are in the interval [1, n-1], if not, then user B refuse the signature.
- User B computes $X = (x_2, y_2) = s_1P + s_2P - rD_{A1} - rD_{A1}$ and $m = h(c_B x_2) r \pmod n$.
- If, X = 0 then B refuses the signature, or B computes the original message m and check the end of the message which can identify the redundant bits. If it is correct, the user B accepts the signature, or refuses.

The correctness of this signature can be proved by the following equations:

$$
\begin{aligned}
R &= (k_1+k_2)D_B \\
&= (k_1+k_2)c_BP \\
&= c_B\,(k_1+k_2)P \\
&= c_B\,(s_1P+s_2P-rD_{A1}-rD_{A2}) \\
&= c_B\,(x_2+y_2) \\
m &= h\,(x_2+y_2)
\end{aligned}
$$

$$
\begin{aligned}
X &= s_1P+s_2P-rD_{A1}-rD_{A2} \\
&= k_1P+rc_{A1}P+k_2P+rc_{A2}P-r(c_{A1}+c_{A2})P \\
&= k_1P+k_2P \\
&= (k_1+k_2)P \\
&= (x_2+y_2)
\end{aligned}
$$

SCHEME ANALYSIS

The main idea of the above improved digital signature scheme is that user owns two secrete keys and uses two random numbers namely two message private keys and thus decreases the possibility of using two same random numbers and increase the difficulty of birthday attacks. If sign t times, then the possibility of choosing both k_1 and k_2 is $p = \left[1 - P_{n-1}^{t}/(n-1)^{t}\right]^2$. So, to make p bigger than 0.5, should be about n-1; here n is a very large prime number which is virtually impossible. If $k_1 = k_2$, then it can be calculated that $c_{A1} - c_{A2} = r^{-1}(s_1 - s_2)$ which is the difference of the two private keys. Since $c_{A1}, c_{A2} \in Z_n^*$, the possibility of cracking c_{A1}, c_{A2} is $p = 1/(n-1)^2$; Here n is very large prime number and p is very small. If certain cracker intercepts a message, he/she still cannot impersonate user A to sign.

If the cracker intends to impersonate user A to sign the message m and he/she chooses k_1, k_2 randomly, then computes $R = (k_1+k_2)P_B = (x_R, y_R)$, $r = h(x_R)^{-1}m(\text{mod } n)$, $s_1 = k_1+rc_{A1}$, $s_2 = k_2+rc_{A2}$. In fact, the method of solving S_1, S_2 is equivalent to getting c_{A1}, c_{A2}, namely solving ECDLP (Cheng *et al*., 2009; Al-Somani *et al*., 2008). So, crackers cannot impersonate user A to generate signature (r, s_1, s_2).

Application: Adopting the above digital signature scheme and at the same time considering the reality of online transactions (Yao *et al*., 2010), we can apply the scheme to e-bank. Assuming online users A and B and user A send message M to user B. A owns a pair of secrete keys (private key c_A, public key D_A and $D_A = c_AP$, P is the point in ellipse E). And B also have a pair of keys (secrete key c_B, public key D_B and $D_B = c_BP$, P is the point in ellipse E). Detailed operation process is as what is listed in the above algorithm. For user A, who owns a pair of secrete keys private key c_A, public key D_A and $D_A = c_AP$, P is the point in ellipse E) and user B, who also has a pair of keys (secrete key c_B, public key D_B and $D_B = c_BP$, P is the point in ellipse E), user A could send message M to user B and the detailed operation process is as above).

CONCLUSION

The improved digital signature scheme in this study uses two random numbers and therefore decreases the possibility of the same random number chosen by two signatures. Compared to the current schemes, it can defense birthday attack more efficiently with higher security level. Considering the advantages, the above scheme can be applied to online bank smoothly.

ACKNOWLEDGMENT

This study is supported by Science and Technology Development Project of Shaanxi Province Project (2010K06-22g), Industrial application technology research and development project of Xi'an (CXY1118 (1), Basic research fund of Northwestern Polytechnical University (GAKY100101) and R Fund of College of Software and Microelectronics of Northwestern Polytechnical University (2010R001).

REFERENCES

Al-Somani, T.F. and A. Alaaeldin, 2008. High performance elliptic curve point operations with pipelined GF(2m) field multiplier [R]. 2008-6th IEEE/ACS International Conference on Computer Systems and Applications, pp: 82-88.

Cheng, H., X. Huang and G. Yang, 2009. Defense against collusion scheme based on elliplic curve cryptography for wireless sensor networks [J]. J. Electr. (China), 26(5).

Gu, D., 2007. Study on Digital Signature Scheme based on Elliptic Curve [D]. M.D Thesis, Guizhou University, Guizhou.

Shun, S., 2004. Application of Cryptography[M]. Tsinghua University Press, Beijing.

Youan, X., 2006. Study on Elliptic Curve Cryptosystem [M]. Huazhong University of Scientice and Technology Press, Wuhan, pp: 10.

Yao, X. and Z. Wei, 2010. Application of ECC in E-cash of multiple-bank [J]. Comput. Eng. Design, 31(7): 1603-1605.