

Implementation of Multi-Signature Scheme Using Elliptic Curve Digital Signature Algorithm

Myint Myint Than, Yee Yee Soe
Computer University, Myeik
hinthr23@gmail.com, yinminhansoe@gmail.com

Abstract

Multi-signature schemes provide data authenticity, integrity, and non-repudiation. The proposed signing and verifying schemes are extensions of standardized algorithms ECDSA (Elliptic Curve Digital Signature Algorithm). These schemes are faster than repeated ECDSA (RECDSA). ECDSA schemes can be directly used in many applications, such as E-Business for a joint signature of a contract between two or more organizations, or E-Government. The final multi-signature of a message can be verified individually for each signer or collectively for a subgroup or entire group as well.

Keywords: Multi-signature, Finite Field, Elliptic Curve, ECDSA, Hashing.

1. Introduction

E-signature are generally divided into, two separate categories: digital signatures and electronic signatures. In contrast with digital signatures, electronic signatures do not rely on cryptographic methods, and are often biometrics, biometrics-based solutions. Digital signatures can be classified into two main categories: single signature and multiple signature (or multi-signature). Single signature refers to the cases where only one party signs a document, while multiple signatures refer to the cases where more than one party signs a single document. A digital signature is a bit pattern that depends on the message being signed, to prove the source of the data and protect against forgery. Digital signatures are dependent on public-key cryptography algorithms for their operation. Methods of implementing digital signature have been developed and are widely used today. For most of

the multi-signature schemes described in the literature, the following observations need to be mentioned: There are no official approved standards defining multi-signature. Most of the schemes are specific for some E-applications [3].

2. Elliptic Curve Cryptography

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was also accepted in 1998 as an ISO standard, and is under consideration for inclusion in some ISO standards. Unlike the ordinary discrete logarithm problem and the integer factorization problem, no sub exponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key-bit is substantially greater in an algorithm that uses elliptic curves [1].

2.1. Hash Function

A hash function H is a transformation that takes an input m and returns a fixed-size string, which is called the hash value h (that is, $h = H(m)$). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography, the hash functions are usually chosen to have some additional properties. The following figure 1 describes the hash function.

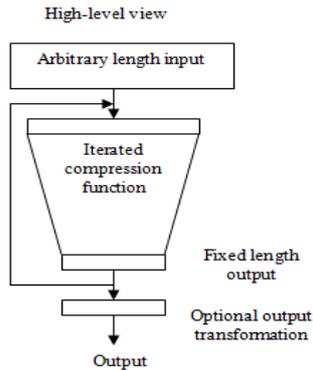


Figure 1. Diagram for an hash function

The basic requirements for a cryptographic hash function are as follows.

- The input can be of any length.
- The output has a fixed length.
- $H(m)$ is relatively easy to compute for any given m .
- $H(m)$ is one-way.
- $H(m)$ is collision-free.

2.2. Digital Signature Scheme

A digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Digital signature has many applications in information security, including authentication, data integrity and non-repudiation. Digital signature is commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering. The following figure 2 shows the classical digital signature.

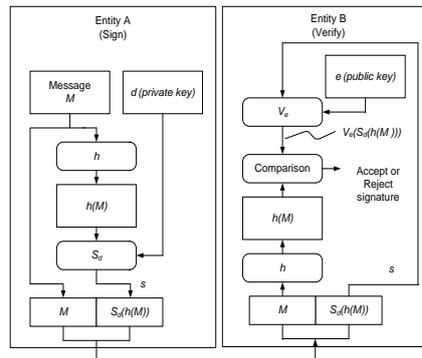


Figure 2. Diagram for Classical Digital Signature

2.3. Multi-Signature Scheme

In everyday life, many legal documents require signatures from more than one party: contracts, decision making processes, petitions, workflow systems. The purposes and uses of multiple signatures are various. A multi-signature scheme enables a group of signers to produce a compact, joint signature on a common document. The multi-signature allows two entities to sign a message which can be validated by another entity [4]. Figure 3 describes the classical multi-signature.

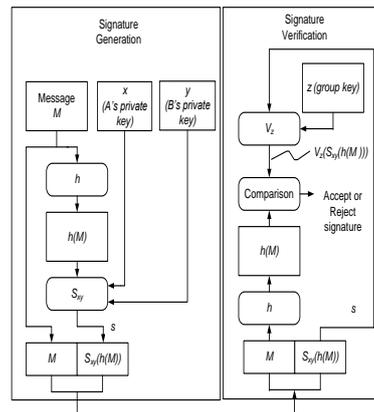


Figure 3. Diagram for Classical multi-signature

3. Finite Field

A field is more than just a set of elements: it is a set of elements under two operations, called addition and multiplication, along with a set of properties governing these operations. The addition and multiplication operations also imply inverse operations called subtraction and division. Several examples of fields are the real field R , the complex field C , the field of rational numbers Q , and the binary field F_2 . Therefore Fields are abstractions of familiar number systems (such as the rational numbers Q , the real numbers R , and the complex numbers C) and their essential properties. They consist of a set of elements F together with two operations, addition (denoted by $+$) and multiplication (denoted by \cdot), that satisfy the usual arithmetic properties:

(1) $(F, +)$ is an abelian group with (additive) identity denoted by 0.

(2) $(F \setminus \{0\}, \cdot)$ is an abelian group with (multiplicative) identity denoted by 1.

(3) The distributive law holds: $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in F$.

If the set F is finite, then the field is said to be finite [5].

4. ECDSA-based Multi-Signature

Scheme

4.1. Common Parameters

The common parameters are similar to those defined for ECDSA standard to which we have added the group dimension. Assuming a group of n signers, the following parameters are defined:

The domain parameter for ECDSA consist of a suitably chosen elliptic curve E defined over a finite field F_p of characteristic p , and a base point $G \in E_p(a, b)$ with order n .

d_1, d_2, \dots, d_n : Group members' secret keys such that $1 \leq d \leq n-1$, is selected randomly and known only by the i th group member.

Q_1, Q_2, \dots, Q_n : Group members' public keys such that is computed [2].

4.2. Signature Generation

As for the DSA-Based approach, this scheme requires *signer1* (the group manager GM) and

other signing group members to carry out an exchange of data during the signature generation process.

1. Computes (M) (is the message to be signed), and make this bit string to an integer.
2. chooses a random integer k , ($1 < k < n$) and computes:
 - o $KG = (x_1, y_1)$ and convert x_1 to an integer $\overline{x_1}$;
 - o $a_1 = x_1 \bmod n$. If $a_1 = 0$ then go to step 2.
 - o $K^{-1} \bmod n$.
3. computes:
 - $b = k^{-1} (m + d_1 a) \bmod n$. If $b = 0$ then go to step 2.
 - $s = b^{-1} \bmod n$.
4. Sends M and $Sign_1(M) = \{a_1, s\}$ to other signers (and keep k secret).

4.3. Signature Verification

Each other *Signer* checks the signature of the manager as follows:

1. Verify that are integers less than n and not equal to zero.
2. Compute $H(M) = m$ and make m an integer less than n .
3. Compute $u = m \cdot s^{-1} \bmod n$ and $v = a_1 \cdot s \bmod n$.
4. Compute $P = u \cdot G + v \cdot Q_1$. If $P = 0$, reject the signature.
5. Convert the x -coordinate of P to an integer x_p of P to an integer x_p and compute $w = x_p \bmod n$.
6. Check if the following equation is true:
 $w = a_1 \dots (3)$

If equation (3) is true, then signature $Sign_1(M) = \{a_1, s\}$ of message M is valid.

4.3.1. Proof that signature verification work

IF a signature (r, s) on a message m was indeed generated by A, then $s=k(e+rd) \pmod n$.

Rearranging gives:

- $s=k^{-1}(e+rd) \pmod n$
- $k=s(e+rd) \pmod n$
- $k=(se \pmod n + srd \pmod n) \pmod n$
- $K=(u_1+u_2d) \pmod n$
- $X=u_1G+u_2Q$
- $=u_1G+u_2dG$
- $=(u_1+u_2d)G$
- $=kG$
- $v=r$

5. Comparing DSA and ECDSA

Conceptually, the ECDSA is simply obtain from the DSA by replacing the subgroup of order q of $(\mathbb{Z}/p\mathbb{Z})^x$ generated by g with the subgroup of points on an elliptic curve that are generated by G. The only significant difference between ECDSA and DSA is in the generation of n. The DSA does this by taking the random element $X=g^k \pmod p$ and reducing it modulo q, thus obtaining an integer in the interval [1, q-1]. The ECDSA generates r in the interval [1, n-1] by taking the x-coordinate of the random point kG and reducing it modulo n.

6. Design and Implementation of the System

6.1 System Design

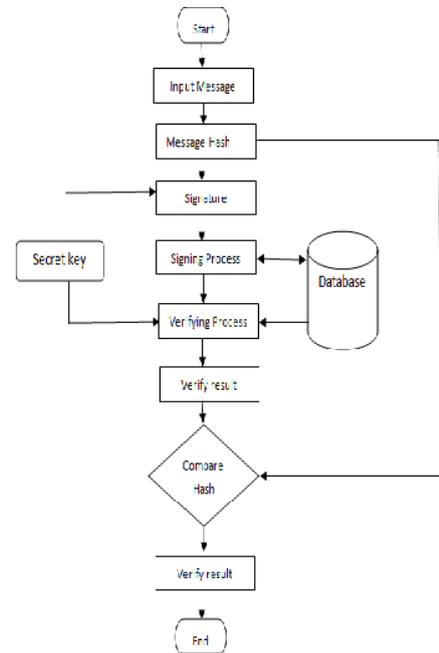


Figure 4. System flow diagram

Figure 4 represents the system design of implementation multi-signature scheme. This system includes two main parts. They are signing and verifying process. Text message is used as an input in this system.

Initially, the system must create key generation. User inputs a message and makes message hashing and sign and then stores in the knowledge base. In this state, signing process has finished.

Verifying process is used to proof signing process. Firstly, retrieve the sign message from the knowledge base. After that verify result message are compared with hash message in this system.

6.2 Implementation of the system

For implementation of the multi-signature scheme, hashing is used 256-bits. Compare the hash's result messages are displayed in figure 5 and figure 6.

If the message hashing and verify result messages' result message are not equal, it can display "reject". If their result message is equal, it can display "successful".

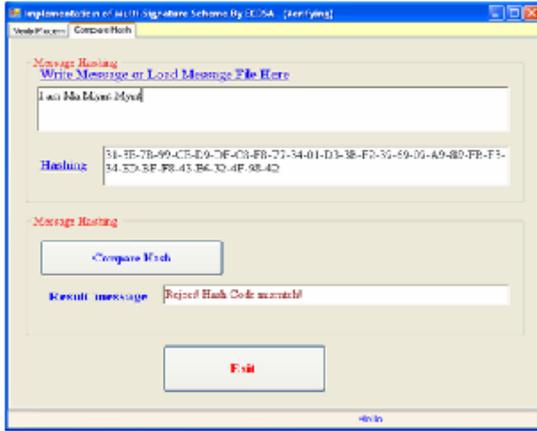


Figure 5. Result of "Fail"

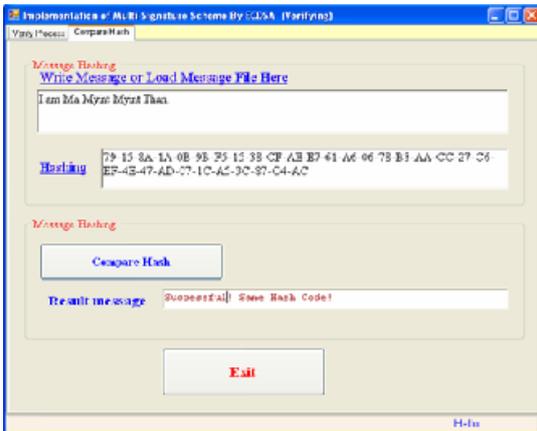


Figure 6. Result of "Successful"

7. Conclusion

The system is presented practical implementation of ECDSA signature generation and verification algorithms. ECDSA can provide very high speed signature generation and verification because it creates faster computations. The signature security is based on the security of DSA and ECDSA. The signature is verified individually for one signer (or

group membership authentication), for a subgroup of signers (or subgroup authentication), or for all signers of the group (group authentication). The system is developed the importance of digital signatures: single and multiple. Although digital signatures schemes that provide (non-repudiation, authentication, and integrity) have been successfully implemented by public key cryptography, those schemes are not sufficient to satisfy different purposes of the traditional signatures, especially multiple signatures. The system is presented a classification of different administrative purposes of multiple signatures.

8. References

- [1] Araki, Kiyomichi, Takakazu Satoh, and Shinji Miura, "Overview of Elliptic Curve Cryptography," Public Key Cryptography, pp. 2948. Springer-Verlag, 1998.
- [2] Hasegawa, J, Nakajima and M, Matsui, "A practical implementation of elliptic curve cryptosystems over GF(p) on a 16-bit microcomputer", Public Key Cryptography – Proceedings of PKC 98, Lecture Notes in Computer Science, 1431 (1998), 182-194.
- [3] N, Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, (48), (1987), 203-209.
- [4] <http://en.wikipedia.org/wiki/ElGamal-signature-scheme>.
- [5] <http://en.wikipedia.org/wiki/Finite-field>.