ISSN 2706-655X Vol.5, Issue 12: 118-121, DOI: 10.25236/IJFET.2023.051218

# Design of information integrity scheme in smartphone forensics

**Yu Hanbing**

*Leshan Vocational and Technical College, Leshan, Sichuan, China*
*yuhanbing123456@163.com*

***Abstract:*** *The vulnerability of electronic data itself makes the originality of digital forensic information become the key to the process of computer evidence identification. Based on smartphone forensics, using the ECDSA signature mechanism, this paper puts forward an anti-repudiation scheme to prove the integrity of electronic evidence. The scheme can transfer the obtained forensics information in real-time and safely during the operation of the smartphone system, and fix the evidence to ensure its integrity. On the premise of some cryptographic assumptions, the security of the scheme is proved.*

***Keywords:*** *smartphone forensics; Information consistency; ECDSA signature; non-repudiation*

## 1. Introduction

Smartphone forensics is the use of special forensics tools ( including hardware and software devices) to extract digital evidence from mobile phones that may contain evidence based on various systems ( such as Android and IOS), and then filter, recover, and fix relevant evidence through procedures prescribed by law, and present the evidence in a certain way, and it will result in a judicial appraisal report ultimately [1].

Smartphone forensics is mainly carried out around electronic evidence, digital evidence refers to the original data (including documents, logs, etc.) to find electronic evidence used to prove a specific crime. Like any other legitimate evidence, this electronic evidence must be authentic and legal [2]. Different from traditional evidence, electronic evidence has the characteristics of high technology, intangibility and easy destruction, which makes it difficult to protect their security. Any change in the process between the moment it is produced and the time it is presented to legitimate investigators will render it legally invalid. Therefore, how to ensure that the electronic evidence submitted is exactly consistent with the original electronic information, and preventing denial, has become very important.

At present, in this research field, some scholars at home and abroad have carried out corresponding theoretical research. Literature [3] uses encryption technology and MAC verification to realize the integrity verification of forensic information; Literature [4] uses DSA, a mathematical signature mechanism to propose an integrity scheme to prove the integrity of forensic information. These schemes can realize the integrity verification of information, but when the parameters required for verification are also tampered with and deleted, the integrity verification of forensic information cannot be realized, and the denial cannot be prevented.

## 2. Symbol and basic definition

"IMEI" indicates the identification number of the mobile phone device. "||" indicates the string connection operation; "S" represents the fetched phone; "V" stands for the verifier of information record consistency; "mi " in the computer system, some key files such as system logs, network information records and other files contain many information records, by viewing these records, you can check the cause of the error, or the evidence left by the attacker when the system is attacked, in order to facilitate description, We use "mi " to represent the i information record generated by the computer in the key file; "mi ", at present, there is no encryption method to prevent the intruder from deleting or adding the malicious behavior of key files and the information records in the key files. To solve this problem, it is necessary to copy and transfer the information records when they are generated, and store them in a secure place, which can be a secure file or a secure output machine. "mi " is the object that "mi " is used for secure copy and transfer in this process; "ti " represents the moment at which the computer generates

ISSN 2706-655X Vol.5, Issue 12: 118-121, DOI: 10.25236/IJFET.2023.051218

the Article i record in the corresponding critical file;

The information conformance scheme in this paper can be viewed as a set of usage protocols between the forensics machine S (signer) and user V (verifier). The information conformance scheme is defined as follows:

Definition 1 An information consistency scheme is a set of protocols between pairs of sets (S, V). Here S is a binary set (S, M), where M is the security object used to store mi '; V= (V, M) is the protocol between the verifier and M, which states that only the verifier with a secure identity will be able to access the secure object M and verify the signature in M.

## 3. Information conformance Scheme

This section focuses on the specific details of our proposed information consistency scheme. In order to facilitate the understanding of the specific process of the protocol, before proceeding to the specific analysis,

Firstly, the digital signature standard ECDSA algorithm is introduced. ECDSA is a signature algorithm proposed by Jonhson and Menezes in 1999. The algorithm is as follows: E is an elliptic curve over a finite field Fq, P is a rational point on E, called a base point, the Order of P is a prime number n, and the order Order(E) = hn of the rational point group of E. It is usually required that n be a large prime number and h a small positive integer. The user chooses his private key a, 1<a<n, and calculates the corresponding public key Q=aP, where a is the private key and Q is the public key. In addition, a one-way hash function H (m) is used in the algorithm, and the standard specifies the secure hash algorithm SHA[5] . The details of the procedure for signing and validating message musing ECDSA are not covered in this article. In our message conformance scheme, we use the same system parameters as ECDSA.

### *3.1 Signature of the information record*

As mentioned earlier, the information records of critical files that need to be securely transferred in the smartphone forensics system may be evidence of crimes committed by smartphone users. Therefore, the information records in the corresponding key files must be copied and signed as soon as possible after they are generated and transferred securely.

In order to quickly and securely transfer the newly generated information record mi, it must be copied, signed, and securely stored when mi is obtained. This process can be described by the process shown in Figure 1.

The detailed steps of information record signature are discussed below, which are described as follows: Signature results and other information

(1)S generates E satisfying the conditions and the base point P on it, calculates the order n of P, and selects the appropriate h. The user then selects his private key a (1<a<n) and calculates the corresponding public key Q=aP. a is the private key and Q is the public key.

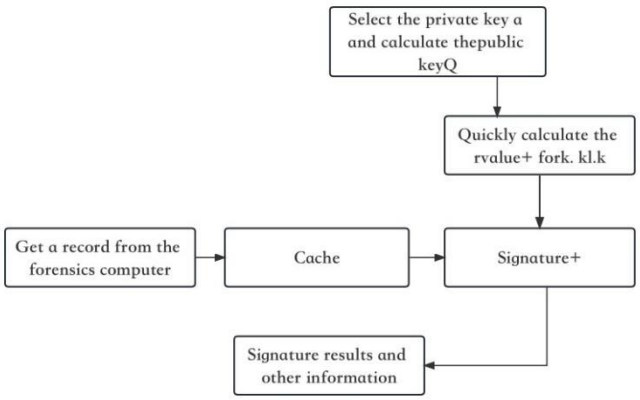


*Figure 1: Information record signature process*

(2) Since the k value used in the signature process has nothing to do with the specific information, a string of random k values less than n can be generated, and the corresponding r value is calculated by

ISSN 2706-655X Vol.5, Issue 12: 118-121, DOI: 10.25236/IJFET.2023.051218

kP=(x,y), r=x mod n. For each k value, k-1 is calculated, where 0<k<n. And take out the corresponding IMEI.

(3) When a new information record mi is generated, a complete copy mi 'will be generated in the cache in Figure 1. At this time, a set of values are extracted from the result of step (2) : (ki, k-1i, ri, IMEI);

(4) Calculate the corresponding si according to the formula s= (k-1 (SHA (m) +ra)) mod n, where m=mi '||i||ti. If time ti is included in mi ', then ti is no longer considered in the expression for m.

(5) The ri and si obtained through the previous steps are the digital signatures of mi recorded in Article i information by the forensics mobile phone system S. When the signature of a new information record is completed, S sends the signature ri, si and information record mi ', the serial number of the record i, and the time ti when the record was generated to the secure storage object M.

(6) When the signature of article i information record and its related information are stored in M, the secure hash SHA algorithm is invoked to digest mi '| |i||ti||SHA(I-1)||IMEI, that is, SHAi=SHA (mi '| |i||ti||SHA(I-1)||IMEI), which is a recursive formula. When the relevant information of the article i information record arrives, SHA(I-1) of the article I- 1 information record has been generated. At this time, it is not difficult to calculate SHAi.

### *3.2 Verification of the signature of the Section I Information Record*

When all signed information records are stored insecure object M, the security of M becomes very important. In order to protect the security of M, the following measures are adopted:

(1) As shown in Figure 1, the information record security transfer process is process hidden, and all the copying, calculation and signing processes are automatically completed by S, and are completely transparent to all users (legal or not). Through process hiding, network malicious intruders will not be able to find that the information records in the system's conventional critical files (such as log files) are transferred;

(2) All files in secure object M are in a custom format and are invisible to any user who has not obtained the legal identity authentication to access M;

And (3) Strict controls are imposed on administrators who have legal identity to access M. This prevents attacks from internal administrators as much as possible. Under the condition of protecting the security of M as much as possible, we aim to make sure that the information stored in Mis is exactly the same as its original state, and any modification, deletion, or addition will be proved. In this way, the integrity of the information record will be able to be used against malicious attackers, with full legal force. In M, every information record has been signed and summarized by the process shown in Figure 1, and the whole process is completed by S. Then, when the signature and information summary are correctly verified, its integrity can be determined. The following is the verification process of the signature and information summary:

(1) The information consistency verifier V proves his legal identity to the secure storage object M through the commonly used Feige-Fiat-Shamir authentication protocol. After obtaining legal identity, the digital signature and information summary of any information record can be verified. The following is an example of verifying a Section i information record signature.

(2) Verify that the signature of S is valid

1) Calculate e=H (m);

2) u=s- 1 emodn, v= s- 1r mod n, (x, y)=uP + vQ, then vi=x mod n. After calculation, if vi=ri, then the signature of S is valid, i.e. mi '≡mi. If vi≠riis found during the verification process, the signature is invalid, it indicates that m'i has been modified and the information recorded in m'i is no longer valid and has no legal effect.

(3) Verify that the summary of information corresponding to the Article i signature is valid

The mi ', i, ti value corresponding to the Article i signature and the information summary value SHAii(i- 1)(i- 1) corresponding to the Article I- 1 signature are substituted into the formula SHA (mi '||i||ti ||SHA) to obtain SHA'. If SHA '=SHAi, the information summary value corresponding to the Article i signature is valid. This indicates that no records have been deleted or added between the Section i signature and the Section I- 1 signature.

ISSN 2706-655X Vol.5, Issue 12: 118-121, DOI: 10.25236/IJFET.2023.051218

### *3.3 Proof of Security*

The information consistency scheme proposed in this paper is secure under the following assumptions:

(1) The ECDSA digital signature algorithm is secure;

And (2) the standard Secure Hash SHA algorithm is secure.

Under the above premise, it is proved that our consistency scheme can meet the following security:

(1) Unforgeability

Unforgeability means that any information record in M is unforgeable, and any modification will be proven. Anyone who obtains legal identity to access M can get the values of h,n, Q, ri, si, and mi ' .

Since each signature is based on a unique, randomly generated value of ki, an attacker can't recover S 'private key A from the values already in place to generate S' signature, and any change to ri, si, and mi 'would invalidate the equation vi=ri. Therefore, they cannot produce signatures from S, and any modification to ri, si, and mi' will prevent the equation vi = ri from being satisfied. Therefore, a legitimate verifier can prove the originality of the information record mi 'by verifying the signature.

(2) unerasability

Unerasability means that the deletion of any information record will be proven. For the sake of description, let all records between information record i and j be deleted in bad faith (i<j), and its signature has been verified to be valid before the information digest article j is verified, i.e. the expression mj '| |j||tj is original. Based on the previous assumption, the article i signature is followed not by the article i+1 signature, but by the article j signature. Then, when verifying the information digest of the article j signature, the verification expression is changed from SHAji(j- 1) (mj '| |j||tj| |SHA) to SHA (mj '| |j||tj ||SHA), and the equation SHA '=SHAj is no longer valid.

(3) Non-additionality

Non-additivity means that any addition of information records will prove to be invalid. As mentioned in Security (1), it is impossible for the attacker to recover S's private key based on the existing value, and thus cannot generate any signature of S, so all the added information signatures cannot be verified.

(4) Non-repudiation

Since IMEI is unique and unmodifiable, adding a smartphone to the forensic information that uniquely identifies the criminal is non-repudiation.

## 4. Conclusions

The computer evidence with legal effect must be true, reliable, complete, following the law, and completely consistent with the original information. The information consistency algorithm proposed in this paper can achieve these goals. The security proof shows that the algorithm in this paper is effective, which is of great significance for the identification of smartphone digital evidence.

## References

*[1] Chen Long, Mai Yonghao, Huang Chuanhe. Computer Forensic Technology [M]. Wuhan: Wuhan University Press, 2007*

*[2] Ding Liping, Wang Yongji. Research on legal and Technical Issues related to computer forensics [J]. Journal of Software, 2005, 16(2): 260-275.*

*[3] Liu Jiqiang, Han Zhen, Lan Zengwei. Secure Audit Logs Server to Support Computer Forensics in Criminal Investigations[C]// 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering Proceedings. Beijing: People's Posts and Telecommunications Publishing House, 2002: 220-223*

*[4] Sham Ira. How to share a secret[J]. Communication of the ACM, 1979,22(11):612-613.*

*[5] National Institute of Standards and Technology (NIST). FIPS PUB 180 Secure Hash Standard[S]. 1993.*