A New Directed Digital Signature Scheme

Manoj Kumar  
Department of Mathematics,  
Rashtriya Kishan Postgraduate College Shamli  
Utter Pradesh- India- 247776.  
e-mail- yamu_balyan@yahoo.co.in

Abstract—In this modern age of electronic era, digital signature scheme is a latest and burning platform for researcher. A variety of digital signature schemes are available in the literature of cryptography. Different signature schemes are used according to the peculiar requirement/situations. A plenty of digital signature schemes have been proposed and discussed. This paper presents a directed signature scheme with the property that the signature can be verified only with the help of signer or signature receiver.

Keywords—Cryptography, public key cryptography, public key, private key, digital signature scheme, hash function, discrete logarithm.

I. INTRODUCTION

To ensure confidentiality and to prevent forgery of a signed message, there is a ancient method for centuries for the sender of the message to put an identification sign, the hand written signature at the end of the message and then sealed this letter in an envelope, before handing it over to a open channel/deliverer.

In this modern electronic-era of communication, hand written physical signature is not suitable. For this situation, digital signature is the cryptographic solution to the problems of information security and authenticity of the signed message. W. Diffie and M. Hellman [1] originally defined digital signatures. Practically, digital signature is in some sense similar to hands written signature. A hand written signature is verified by comparing it to others authentic signatures. The hand written signature does not depend upon the content of the message. In contrast to hand written signature, which is independent of message, digital signature depend on the message and must somehow reflect both the content of the message and the signer of the message.

In order to achieve these requirements of digital signature, a signer of the message who holds private/secret key, can generate digital signature by applying those secret information and a publicly known digital signature algorithm. To check the authenticity of the digital signature, the signature receiver uses the public key/information and a publicly known algorithm. In this way, a digital signature scheme allows a user with a public key and a corresponding private key to sign a document in such a way that everyone using his/her (signer) public key can verify the signature of the signed message/document, but no one other than the original signer can forge or copy the signature. This property of digital signature is known as self-authenticity. This property of self authenticity is essentially requirement for practical applications of digital signatures.

Some practical situations are the requirement of digital signature on a certificate or an official announcements issued by any competent/government authority.

On the other hands, there are many situations, where a signed message may be sensitive to the signature receiver. For example signature on sensitive medical records of the signature receiver/patient, tax information of a client and most personal/business transactions are such situations. For these situations, signature is generated in such a way that only the signature receiver can check the authenticity of the message and whenever it required, he/she is able to prove the authenticity of the message to any third party. Such signatures are called as directed signatures [11-14, 17-21]. In directed signature scheme, the signature receiver has full control over the signature verification process. Nobody can check the validity of signature without his cooperation.

The concept of directed signatures was first presented by C. H. Lim and P. J. Lee [6]. Since than, a plenty of such scheme have been proposed. This paper proposes a new directed signature scheme. In the proposed scheme, any third party can check the authenticity of the signature with the help of signature receiver or the signer as well. Both the signer and signature receiver have full control over the signature verification process. In other words, they are independent to prove the validity of the signature to any third party, whenever required and necessary. The paper is organized as follows

The section- II presents some basic tools. Section- III describes a new directed signature scheme. Proposed scheme is illustrated in section IV. The security of the proposed scheme is discussed in section- V. Finally, comes to a conclusion in the section VI.
II. PRELIMINARIES

A. Preliminary Settings
Throughout this paper we use the following system setting.
• A prime modulous \( p \), where \( 2^{11} < p < 2^{12} \);
• A prime modulous \( q \), where \( 2^{159} < q < 2^{160} \) and \( q \) is a divisor of \( p - 1 \);
• A number \( g \), where \( g \equiv k^{(p-1)/q} \mod p \), \( k \) is random integer with \( 1 \leq k \leq p - 1 \) such that \( g > 1 \); \( (g \) is a generator of order \( q \) in \( \mathbb{Z}_p^* \)),
• A collision free one-way hash function \( h \) [10];

The parameters \( p, q, g \) and \( h \) are common to all users. We assume that every user \( A \) chooses a random \( x_A \in \mathbb{Z}_q \) and computes \( y_A = g^{x_A} \mod p \). Here \( x_A \) is the private key of \( A \) and \( y_A \) is the public key of \( A \). For our purpose, we use Schnorr’s signature scheme [8]. These basic tools are briefly described below.

B. Schnorr’s signature scheme
In this scheme, the signature of \( A \) on message \( m \) are given by \((r_A, S_A)\), where,
\[
\begin{align*}
\nonumber r_A &= h(g^{k_A} \mod p, m) \text{ and} \\
\nonumber S_A &= k_A - x_A \cdot r_A \mod p.
\end{align*}
\]
Here random \( k_A \in \mathbb{Z}_q \) is private to \( A \).

The signature are verified by checking the equality
\[
r_A = h(g^{S_A} \cdot y_A \cdot r_A \mod p, m).
\]

III. NEW DIRECTED SIGNATURE SCHEME
Suppose that signer \( A \) wants to generate a signature on message \( m \) so that only signature receiver \( B \) can directed verify the signature. The signature receiver \( B \) as well as signer \( A \) can independently prove the validity of signature to any third party \( C \), whenever required. Our proposed directed signature scheme is based on Schnorr’s signature scheme. The signing and verification processes are as follows.

A. Signature generation by \( A \)
• A picks random \( K_{a_1} \) and \( K_{a_2} \in \mathbb{Z}_q \) and computes
\[
\begin{align*}
W_B &= g - K_{a_1} \mod p \\
V_B &= g^{K_{a_1} \cdot y_B} K_{a_2} \mod p.
\end{align*}
\]
Here \( y_B \) is the public key of the signature receiver \( B \).
• Using a one-way hash function \( h \), \( A \) computes a secret value \( r_A = h(g^{K_{a_1} \cdot y_B} K_{a_2} \mod p, m) \).

B. Signature verification by \( B \)
• Using his private key \( x_B \), \( B \) computes
\[
R = V_B (W_B)^x_B \mod p.
\]
• \( B \) checks the following congruence for a valid signature
\[
g^{S_A} \equiv R \cdot y_A \cdot r_A \mod p.
\]

If hold then \( (S_A, W_B, V_B, m) \) is a valid signature.

C. Proof of validity to \( C \)
In this scheme, both the signer and signature receiver can independently prove the validity of signature to any third party, whenever necessary. This sub-section describes the protocol using which the signer and the signature receiver can prove the validity of signature.

a) Proof of validity by \( A \) to \( C \)
• A computes \( V_C = g^{K_{a_1} \cdot y_C} K_{a_2} \mod p \) and sends to \( C \).
• \( C \) uses \( V_C \) in place \( V_B \) to checks the validity of signature by using his secret key. The signature verification process will remain same as in sub-section B.

b) Proof of validity by \( B \) to \( C \)
• \( B \) picks random \( K \in \mathbb{Z}_q \) and computes
\[
\begin{align*}
W_C &= g - K \mod p, \\
V_C &= R \cdot y_C \cdot K \mod p,
\end{align*}
\]
and sends to \( C \).
• \( C \) uses \((W_C, V_C)\) in place \((W_B, V_B)\) to checks the validity of signature by using his secret key. The signature verification process will remain same as in sub-section B.

IV. ILLUSTRATION
We choose smaller parameters to illustrate the scheme. Taking \( p = 23, q = 11 \) and \( g = 3 \). The secret and public key of users is as follow.
from this equation. Obviously, this is also again computationally infeasible for a forger to collect any information.

.Key: Can one impersonate the signer?

A forger may try to impersonate the signer by randomly selecting two integers \( K_1 \) and \( K_2 \in \mathbb{Z}_q \) and calculate

\[
W_B = g^{-K_1} \mod p,
\]

\[
V_B = g^{K_1 \cdot y_B} K_2 \mod p,
\]

\[
r_A = h(g^{K_1 \cdot m}).
\]

But without knowing the secret key \( x_A \), it is difficult to generate a valid \( S_A \) to satisfy the verification equation

\[
g^{S_A} \equiv [R, y_A \cdot r_A] \mod p.
\]

.Key: Can one forge a signature \( \{ S_A, W_B, V_B, m \} \) by the equation \( g^{S_A} \equiv [R, y_A \cdot r_A] \mod p? \)

A forger may randomly select an integer \( R \) and then computes the hash value \( r_A \) such that

\[
r_A = h(R, m) \mod q.
\]

Obviously, to compute the integer \( S_A \) is equivalent to solving the discrete logarithm problem. On the other hand, the forger can randomly select \( r_A \) and \( S_A \) first, then try to determine a value \( R \), that satisfy the signature verification equation. Thus these attacks will not be successful.

VI. CONCLUSION

The new directed scheme has the following properties:

- This proposed directed scheme is based upon W. Diffie and M. Hellman’s public key cryptosystem and Schnorr’s signature scheme.
- This scheme is applicable, when the message is different documents.
- The signer can use the security parameters and secrets as one-time secrets. There is no need to fix these security parameters.
- The signer can change the secret values to sign different documents.
REFERENCES


About the Author: