Study of Undeniable Digital Signatures Schemes

Mohit Kaushik[1], Om Pal[2], Neha Mittal[3]

[1,3]*Student, Department of Information & Technology, CDAC Noida, India*

[2]*Sr. Technical Officer, CDAC Noida, India*

***Abstract*:-In the era of electronic communications, almost all the business and personal transactions are being performed over the internet. Hence it is a necessity to make the transactions or exchange of information absolutely reliable and secure. A cryptographic system, to be complete and secure, requires a cryptographic function, a key parameter and a good management system to manage the cryptographic keys. However, no matter how secure an encryption scheme is, it is worthless if the other party is not convinced of the authenticity of the message/document. The undeniable signatures is a modern authentication technique that helps in proving the genuineness of the message or document. The undeniable schemes not only protect the interests of both the parties, but also secures the signer's ownership over the signature and message even further by requiring the participation of the signer in the verification process of the signature. In addition, it also provides the signer with the ability to deny the forged signature. This paper explores and draws comparison among various schemes on the basis of the security notions, along with performance in terms various operations required during the different phases of signature.**

***Index Terms*:-Undeniable signatures, digital signatures, survey, authentication.**

I. INTRODUCTION

In today's era, generally known as Information Era, information is the most critical resource for every organization. Hence, the security of this information is now-a-days the prime concern for all industries. It has been a major issue since the ancient times, where signs and symbols were used to convey the secret messages and to protect the critical knowledge to go public. The security of the data is particularly crucial in sectors such as defense, banking and stock exchange, etc. Today, most of the information is shared using the internet. While exchanging the information over an insecure channel we must take into account the major aspects of the information security, which are, confidentiality, authenticity, integrity, and non-repudiation.

Information Security, sometimes termed as Info Sec, refers to the practices of defending the information from unauthorized access, modification, disclosure, usage, disruption, or destruction. There are two major aspects of information security, namely, IT security and information assurance. Initially, cryptography was concerned solely with the information confidentiality. It means the message to be transmitted over the network is converted from comprehensible form to some incomprehensible form. This process of rendering the message incomprehensible is called encryption. The encrypted message called cipher text is thus unreadable to the eavesdroppers or interceptors without the secret knowledge (namely, the key required for decryption). The cipher text is then converted back into the comprehensible form at the receiver's end. This process is termed as decryption. This overall methodology was initially applied for defense, diplomat, and government applications to ensure secrecy during the communication. The scope of cryptography, in past few decades, have been expanded to include the concerns for identity authentication, digital signatures, message integrity, interactive proofs and secure computing.

Digital signature schemes [1] provide the cryptographic analogue for the traditional handwritten signatures that in fact, provide stronger security guarantees. They serve as a powerful and sophisticated tool and are now accepted in many nations for legal bindings; they are used widely for authentication of individuals and even corporations, for certifying the business and legal contracts or notarizing the documents, and as components of more complex protocols. In addition, digital signatures enable the secure transmission and distribution of the public parameters and therefore, in very real sense, serve as the foundation for the public-key cryptography.

Undeniable signature schemes [2], first introduced by Chaum and van Antwerpen have various applications in cryptology. Such signatures are characterized by the property that verification can be only achieved by interacting with the legitimate signer through a confirmation protocol, on the other hand, the signer can prove that a forgery is such by engaging in a denial protocol.

If the signer does not succeed in denying (in particular, if it refuses to cooperate) then the signer remains legally bound to the signature. On the other hand the signer is protected by the fact that his signature cannot be verified by unauthorized third parties without his own cooperation.

Since its introduction in 1989, undeniable signature schemes have received a significant attentions in the cryptographic research community. These works have provided a variety of different schemes for undeniable signature schemes with variable degree of security, provability and additional features.

They have two distinctive features:

- The verification process is interactive, so that the signatory can limit who can verify the signature.

ISSN: 2278 – 1323

- A disavowal protocol, which is a cryptographic protocol that allows them to determine whether a given signature is a forgery.

The first means that a signatory can allow only others who are authorized to access the document to verify their signature. If the document were to be leaked to a third party, the third party would be unable to verify that the signature is genuine. This is a designated verifier signature. However, because of this property it means that the signatory may deny a signature which was valid. To prevent this, there is the second property, a method to prove that a given signature is a forgery.

This paper provides an overview of some modern authentication techniques that helps in proving the genuineness of the message or document. The undeniable schemes not only protect the interests of both the parties, but also secures the signer's ownership over the signature and message even further by requiring the participation of the signer in the verification process of the signature. In addition, it also provides the signer with the ability to deny the forged signature. This paper explores and draws a comparison of the various undeniable signature schemes on the basis of security notions. Also the performance comparison is drawn based on the number of different operations performed during each phase of the signature scheme.

This paper is organized as follows: section 2 studies various undeniable signature schemes proposed using various concepts over the time. In section 3 comparisons of the reviewed schemes are drawn based on various notions. Section 4 concludes the survey of the undeniable signature schemes.

II. SURVEY OF UNDENIABLE SIGNATURE SCHEMES

This section reviews various schemes for the undeniable signatures.

A. CVA UNDENIABLE SIGNATURES

Chaum and van Antwerpen gave the first realization of an undeniable signature scheme [2,3]. It is a non-self-authenticating scheme where the signature must be verified with the signer's cooperation. It is based on the intractability of computing discrete logarithms in the group Z^*_p, where, p is a prime number. The notion of undeniability is that the signer of the message cannot prove his own signature is a forgery, and he cannot prove that a false signature is genuine. The signing part of the scheme is very much like any other DLP scheme.

CVA KEY GENERATION

B chooses a large prime p of the form $p=2r+1$, where r is also a prime. B finds a random element $g \in Z^*_p$ of multiplicative order r, selects a random integer $d \in \{2,\ldots,r-1\}$ and compute $y:=g^d \pmod p$. Public key is (p, g, y) and d is kept as private key. The value $d^{-1} \pmod r$ is needed during verification.

CVA SIGNATURE GENERATION

- Calculate digest, $m:=H(M)$
- Compute signature, $s:=m^d \pmod p$

CVA SIGNATURE VERIFICATION PROTOCOL

- A computes $m:=H(M)$
- A chooses two secret random integers $i,j \in \{,\ldots,p-1\}$
- A computes $u:=s^i y^j \pmod p$ and sends to B
- B computes $v:=u^{d^{-1} \pmod r} \pmod p$ and sends to A
- A computes $v' := m^i g^j \pmod p$ and accepts the signature (M,s) if and only if $v=v'$.

CVA SIGNATURE DISAVOWAL PROTOCOL

- A chooses two secret random integers $i1,j1 \in \{1,\ldots,p-1\}$ and computes $u1:=s^{i1} y^{j1} \pmod p$ and sends $u1$ to B
- B computes $v1:=u1^{d-1 \pmod r} \pmod p$ and sends $v1$ to A
- A chooses two secret random integers $i2, j2 \in \{1,\ldots,q-1\}$ and computes $u2:=s^{i2} y^{j2} \pmod p$ and sends $u2$ to B
- B computes $v2:= u2^{d-2 \pmod r} \pmod p$ and sends $v2$ to A
- A computes $w1:= (v1 g^{-j1})^{i2} \pmod p$ and $w2:=(v2 g^{-j2})^{i1} \pmod p$. If $w1 = w2$, then A concludes that the signature s is forged. Otherwise A concludes that B is trying to deny the signature.

B. RSA-BASED UNDENIABLE SIGNATURES

RSA based Undeniable Signatures were realized by Rosario Gennaroy, Hugo Krawczykz and Tal Rabin [5]. It is based on the intractability of prime factorization of the large integers.

NOTATIONS

For a positive integer k, $[k] = \{1,\ldots,k\}$. Z^*_n denotes the multiplicative group of integers modulo n, and $\Phi(n) = (p-1)(q-1)$ the order of this group. For an element $w \in Z^*_n$, ord(w) denotes the order of w in Z^*_n. The subgroup generated by an element $w \in Z^*_n$ is denoted by $\langle w \rangle$.

THE SIGNATURE SCHEME

We start by defining the following set:

$N = \{n \mid n = pq, p < q, p = 2p' + 1, q = 2q' + 1$, and p, q, p', q' are all prime numbers$\}$

The system is set up by the signer in the following manner: chooses a random element $n \in N$; selects elements $e, d \in \Phi(n)$ such that $ed \in 1 \bmod \Phi(n)$; chooses a pair (w, S_w) with $w \in Z^*_n$, $w \neq 1$, $S_w = w^d \bmod n$; sets the public key parameters to the tuple (n, w, S_w); sets the private key to (e, d).

GENERATING A SIGNATURE

To generate a signature on a message m the signer carries out a regular RSA signing operation, i.e. he computes $S_m = m^d \bmod n$, outputting the pair (m, S_m). More precisely, the message m is first processed through a suitable encoding (e.g. via one-way hashing) before applying the exponentiation

such that the resultant signature scheme can be assumed to be unforgeable even against chosen message attacks (plain RSA does not have this property). Given a message m we will denote by m the output of such an encoding of *m*. Thus, the resultant signature of m will *be* $S_m = \bar{} \; m^d \; mod \; n$.

CONFIRMATION PROTOCOL

Input : Prover : Secret key $(d,e) \in [\Phi(n)]^2$

Common : Public key$(n,w,S_w) \in PK$,

$m \in Z^*_n$ and alleged $\hat{S}_m$

Steps:

- *V* chooses $i,j \in_R [n]$ and computes $Q = \hat{S}_m^{\,2i} S_w^{\,j} \; mod \; n$

  $V \rightarrow P: Q$

- *P* computes $A = Q^e \; mod \; n$

  $P \rightarrow V: A$

- *V* verifies that $A == \bar{} \; m^{2i} w^j \; mod \; n$.

  If equality holds then *V* accepts $\hat{S}_m$ as the signature on *m*, otherwise "undetermined".

DENIAL PROTOCOL

Input : Prover : Secret key $(d,e) \in [\Phi(n)]^2$

Common : Public key$(n,w,S_w) \in PK$,

$m \in Z^*_n$ and $\hat{S}_m$

Steps:

- *V* chooses $i = 4b$, $b \in_R [k]$ and $j \in_R [n]$
- Sets $Q_1 = \bar{} \; m^i w^j \; mod \; n$ and $Q_2 = \hat{S}_m^{\,i} S_w^{\,j} \; mod \; n$

  $V \rightarrow P: (Q_1, Q_2)$

- *P* computes $Q_1 / Q_2^{\,e} = (\bar{} \; m / \hat{S}_m^{\,e})^i$ and computes $i = 4b$ by testing all possible values of $b \in [k]$

  If such a value was found then *P* sets $A = i$, Otherwise abort.

  $P \rightarrow V: A$

  V verifies that $A == i$. If equality holds then *V* rejects $\hat{S}_m$ as a signature of *m*, otherwise, undetermined.

C. CONVERTIBLE UNDENIABLE SIGNATURES

Convertible Undeniable Signatures were introduced by Convery Joan Boyar, David Chaum and Ivan Damgard [7]. In these schemes, release of a single bit string by the signer turns all of his signatures, which were originally undeniable signatures, into ordinary digital signatures.

SETUP

One chooses two large primes *p,q* with $q|(p-1)$ and a group generator $\alpha (mod \; p)$ of two integers with order *q*.

KEY GENERATION

The signer performs following calculations:

- Generates secret parameter $x,z \in Z^*_q$.
- Computes $y = \alpha^x \; mod \; p$.
- Computes $u = \alpha^z \; mod \; p$.
- The public key is (y, u) and secret keys are (x, z).

Note : Let $x = K_{s1}$ and $z = K_{s2}$.

SIGNATURE GENERATION

To sign a message *m*, the signer performs the following steps:

- Picks two random numbers $t,k \in Z^*_q$.
- Computes $T = \alpha^t \; mod \; p$.
- Computes $r = \alpha^k \; mod \; p$.
- Computes $s = k^{-1} (m - xr) \; (mod \; q)$.

The signature for message m is the triple (T, r, s).

CONFIRMATION PROTOCOL

Let $w = T^{Tm}$ and $v = y^r r^s$ which can be computed from public information. The signature is valid if the equality $w^z = v$ holds. The signer proves the equality by proving $log_w v = log_\alpha u$ using the zero knowledge protocol.

DISAVOWAL PROTOCOL

The signature is invalid if the equality $w^z = v$ does not hold. The signer needs to prove the inequality that the discrete logarithm $log_w v \neq log_\alpha u$ using the zero knowledge protocol.

SELECTIVE CONVERSION

By releasing the secret value *t*, only the signature that was signed by *t* will be converted into an ordinary signature. The signer can check the signature by checking $u^{tTm} \equiv y^r r^s (mod \; p)$ and $t \equiv \alpha^t (mod \; p)$.

TOTAL CONVERSION

By releasing the secret parameter *z*, every signature that was signed by the signer with *z* can be verified by the verifier by checking $w^z = v$.

D. DISTRIBUTED PROVER UNDENIABLE SIGNATURES

The idea of distributing the power of verifying was first experimented with by Ben-Or, Goldwasser and Wigderson [8] as well as Chaum, Crepeau and Damgard [9]. Pederson made the practical implementation of the method more efficient [10]. This setup is called a distributed prover protocol because at least k out of n agents will be needed during the verification phase.

KEY GENERATION

The signer:

- Selects two large integers *p,q* where *q* divides $(p-1)$.
- Selects a generator α for the subgroup G_q.

- Selects secret elements $x, z \in Z^*_q$.
- Computes $y = \alpha^x$ and $u = \alpha^z$.

The public key is (p, q, α, y, u), the first secret key (K_{s1}) is x and the secondary secret key (K_{s2}) is z.

SIGNATURE GENERATION

To sign a message m, the signer performs the following steps:

- Picks two random numbers $t, k \in Z^*_q$.
- Computes $T = \alpha^t \bmod p$.
- Computes $r = \alpha^k \bmod p$.
- Computes $s = k^{-1} (m - xr) \pmod q$.

The signature for message m is the triple (T, r, s).

SECRET DISTRIBUTION FROM THE SIGNER

The signer distributes his secret with each agent i where $i = 1$ ….. n, as follows:

- He computes shares $z_i = f(x_i)$ for each agent using $f(x) = f_0 + f_1 x + \ldots + f_{k-1} x^{k-1}$, where $f_0 = z, f_i$ where $i = 1 \ldots .k\text{-}1$ are randomly chosen and x_i is the agent's identification code.
- He computes $h_i = \alpha^{z_i}$ and publishes h_i. This is the corresponding public information of the secret share z_i.
- He sends the share z_i to agent i and broadcasts $(\alpha^{f_i})_{i=0,\ldots k-1}$ to all n agents.

VERIFYING SHARES ON THE AGENT'S SIDE

Each agent i, uponreceiving the shares, does the following steps:

- Computes $h_l = \prod_{j=0}^{k-1} (\alpha^{f_j})^{j^l}$ for all $l = 1, \ldots, n$.
- Verifies that $h_i = \alpha^{z_i}$.
- If this is false, then broadcasts z_i and stops; otherwise, accepts the share.

DISTRIBUTED VERIFICATION

Given a message m and its signature (T,r,s), both the signer and the verifier can compute $w = T^{Tm}$ and $v = y^r r^s$. The verifier is required to interact with each and every k agent through the following interactive protocol:

- The verifier chooses $a, b \in Z$, computes the challenge $ch = w^a \alpha^b$ and sends ch to prover i.
- The prover i selects a random number $r_i \in Z$ and computes $h_{i1} = ch^{r_i}$ and $h_{i2} = h_{i1}^{r_i}$. The prover sends h_{i1} and h_{i2} to the verifier.
- The verifier sends a, b to the prover.
- The prover sends r_i to the verifier.
- The verifier collects all k numbers of r_i and computes $h_{i1} = (w^a \alpha^b)^{r_i}$ and $h_{i2}^{a_i r_i^{-1}}$.

If $\prod_{i=1}^{k} h_{i2}^{a_i r_i^{-1}} = v^a T^b$ and $h_{i1} = (w^a \alpha^b)^{r_i}$ for all $i = 1, \ldots, n$, then the verifier accepts the signature.

DISTRIBUTED DISAVOWAL

The disavowal protocol is same as the verification process, except that the prover will need to prove the inequality $\prod_{i=1}^{k} h_{i2}^{a_i r_i^{-1}} \neq v^a T^b$ to the verifier. If the inequality holds then the verifier rejects the signature.

SELECTIVE CONVERSION

By releasing the secret value t, only the signature that was signed by t will be converted into an ordinary signature. The signer can check the signature by checking $u^{tTm} \equiv y^r r^s \pmod p$ and $t \equiv \alpha^t \pmod p$.

TOTAL CONVERSION

By releasing the secret parameter z, every signature that was signed by the signer with z can be verified by the verifier by checking $w^z = v$.

III. COMPARATIVE ANALYSIS

This section draws comparison among the above reviewed schemes on the basis of the security notions proofs presented by their authors, along with performance in terms various operations required during the different phases of signature.

A. SECURITY COMPARISON

Various undeniable signature schemes are compared and the table is drawn based on the security notions for the undeniable signatures. The security notions referred for comparison are unforgeability, invisibility, anonymity and non-transferability.

Scheme	Unforgeable	Invisible	Anonymity	Non-Transferable
CvA Undeniable Signature Scheme	✓	✓		✓
RSA Undeniable Signature Scheme	✓	✓		✓
Convertible Undeniable Signature Scheme	✓	✓	✓	✓
Distributed Prover Undeniable Signature Scheme	✓	✓		

Table 1 Comparison table based on security notions

B. PERFORMANCE COMPARISON

The following table shows the comparison drawn between various signature schemes based on the number of different operations required during various stages of the signature schemes.

Scheme	Phase	Multiplication	Addition/ Subtraction	Exponent	Modular	Other
CvA Undeniable Scheme	Set up	1	1	2	2	
	Sign	0	0	1	1	1H
	Verification	2	0	5	3	1H
	Disavowal	4	0	10	6	
RSA Undeniable Scheme	Set up	4	4	1	1	
	Sign	0	0	1	1	1H
	Verification	4	0	5	3	1H
	Disavowal	4	0	7	2	2D
ConvertibleUndeniable Scheme	Set up	0	1	2	2	1D
	Sign	2	1	3	3	1H
	Verification	7	2	4	0	2L
	Disavowal	2	0	8	0	
Distributed Prover Scheme	Set up	0	1	2	0	1D
	Sign	2	1	3	3	1H
	Verification	7	0	17	0	
	Disavowal	7	0	17	0	

Table 2 Performance comparison table(where D- division, H- hashing & L- logarithm)

IV. CONCLUSION

A cryptographic system, to be complete and secure, requires a cryptographic function, a key parameter and a good management system to manage the cryptographic keys. However, no matter how secure an encryption scheme is, it is worthless if the other party is not convinced of the authenticity of the message/document. The undeniable signatures is a modern authentication technique that helps in proving the genuineness of the message or document. The undeniable schemes not only protect the interests of both the parties, but also secures the signer's ownership over the signature and message even further by requiring the participation of the signer in the verification process of the signature. In addition, it also provides the signer with the ability to deny the forged signature. The paper explored various undeniable schemes and also the comparison is drawn on the basis of the provided security notions proofs. The comparative performance analysis of the undeniable schemes is done to enhance the understanding of the readers. In addition, this paper helps the readers in proper selection of the undeniable signature approaches as per the requirements.

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. In: Comm. of the ACM, volume 21 (2), 1978. Pages 120-126.

[2] David Chaum and Hans van Antwerpen. Undeniable signatures. In Advances in Cryptology–CRYPTO'89, pp.212-216, 1989.

[3] David Chaum. Zero-knowledge undeniable signatures (extended abstract). In Advances in Cryptology – EUROCRYPT '90, pp.458-464, 1990.

[4] Y. Desmedt and M. Yung. Weaknesses of Undeniable Signature Schemes. Advances in Cryptology-EUROCRYPT'91. Springer-Verlag, 547: 205-220, April 1991.

[5] Rosario Gennaro, Hugo Krawczyk and Tal Rabin. RSA-based undeniable signatures. In Advances in Cryptology – CRYPTO '97. Lecture Notes in Computer Science Volume 1294, 1997, pp. 132-149.

[6] T. El-Gamal. A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. IEEE Transactions on Information Theory, 31: 469-472, 1985.

[7] J. Boyar, D. Chaum, I. Damgard, and T. Pedersen. Convertible undeniable signatures. In Advances in Cryptology-CRYPTO '90, pages 189-205, 1990.

[8] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (extended abstract). Proceedings of the 20th Annual ACM Symposium on Theory of Computing, pages 1-10, May 1988.

[9] D. Chaum, Claude Crepeau, and I. Damgard. Multiparty Unconditionally Secure Protocols (extended abstract). In Proceedings of the @0th Annual ACM Symposium on Theory of Computing, pages 11-19, May 1988.

[10] T. P. Pedersen. Distributed Provers with Applications to Undeniable Signatures. Advances in Cryptology-EUROCRYPT'91. Springer-Verlag, 547: 221-242, April 1991.

