International Journal of Theoretical & Applied Sciences, **2**(2): 61-64(2010) **ISSN : 0975-1718**

An efficient non-delegatable identity based strong designated verifier signature scheme

Sunder Lal and Vandani Verma

Department of Mathematics, Dr. B.R.A. (Agra), University, Agra-282002 (UP),India.

Amity School of Engineering and Technology (ASET), Amity University, Sector-125, Noida.

ABSTRACT : Designated verifier signatures are intended to a specific and unique designated verifier, who is the only one person to check their validity. This paper proposes a new efficient non-delegatable strong designated verifier signature scheme based on identity based cryptography. We analyze the security of the scheme and compare its computational aspects with the other ID-SDVS schemes existing in literature and the result shows that our scheme is more efficient as compared to others.

Keywords : ID based cryptography, designated verifier, bilinear pairing, delegatability

I. INTRODUCTION

A designated verifier signature proposed by Jakobsson et al [2] is a special type of digital signature that provides message authentication without non-repudiation. Such signatures are intended to a specific and unique designated verifier, who is the only person to check the validity of these signatures. When a chosen unique designated verifier is given designated verifier signatures, he can have either of following two conclusions:

1. The signatures are produced by the signer or
2. His private key is known to the signer.

The verifier knows that only he himself and the signer can sign the message and that he has not produced the signature. Moreover, he has not revealed his private key to the signer. So with high probability he is convinced that the signatures are produced by the signer and not by him. However, the designated verifier cannot convince any third party about the validity of the signatures, even if he agrees to disclose his private key as he himself is able to produce the same indistinguishable signatures i.e. he can simulate the signature using his private key. So, DVS provides signers anonymity to the rest of the world and only the original signer and the designated verifier knows who has signed the message.

Saeednia et al [5] in 2003 introduced the new concept of strongness in the DVS schemes that forces the specified recipient to use his secret key for verifying the signatures. The comparison of the two schemes in terms of communication and computation results that the Saeednia's [5] scheme is more efficient as compared to first DVS proposed by Jakobsson et al [2]. Kumar et al [3] in 2006 proposed an ID based SDVS based on Saeednia's [5] scheme that overcomes the '***Delegatability Attack***' (*in this attack signer can delegate her signing ability with respect to a fixed designated verifier, to a third party without disclosing the secret key*) proposed by Lipmaa et al [3] on Saeednia's [5] scheme. Recently, several ID-SDVS schemes [1, 6, 7] have been proposed In this paper we propose a new non-delegatable identity based strong designated verifier signature (ID-SDVS) scheme that is more efficient than [1, 3, 6, 7] and that does not suffer with the delegatability attack proposed by Lipmaa et al [4].

Rest of the paper is organized as follows: Section 2 gives the background concepts, section 3 gives the model of the proposed scheme, section 4 proposes the non-delegatable identity based strong designated verifier signature scheme. In section 5, we analyze the security aspects of our scheme and compare the computational aspects in section 6. Finally section 7 and 8 are devoted to applications and conclusion respectively.

II. BACKGROUND CONCEPTS

In this section, we briefly review the concepts of bilinear pairings and some related mathematical problems.

A. Bilinear pairings

Let G_1 be a cyclic additive group generated by P, whose order is a large prime number q and G_2 be a cyclic multiplicative group with the same order q. Let e: $G_1 \times G_1 \rightarrow G_2$ be a map with the following properties :

Bilinearity **:** $e(aP, bQ) = e(P, Q)^{ab}$ $\forall$ P, Q $\in G_1$ and a, b $\in Z_q^*$.

Non-degeneracy**:** $ P, Q $\in G_1$, such that e (P, Q) $\neq$ 1, the identity of G_2.

Computability**:** There is an efficient algorithm to compute e (P, Q) P, Q G_1.

Such pairings may be obtained by suitable modification in the Weil-pairing or the Tate-pairing on an elliptic curve defined over a finite field.

B. Computational problems

Here we present some computational hard problems, which form the basic security of our schemes.

***Discrete Logarithm Problem (DLP)*:** Given QG_1, find an integer aZ_q^*, such that $Q = aP$, P is a generator of G_1.

***Decisional Diffie-Hellman Problem (DDHP)*:** a, b, cZ_q^* and given P, aP, bP, cP, decide whether $c = ab \bmod q$

***Computational Diffie-Hellman Problem (CDHP)*:** a, b Z_q^* and given P, aP, bP, compute abP

Bilinear Diffie-Hellman Problem (BDHP): a, b, c Z_q^* and given P, aP, bP, cP compute $e(P, P)^{abc}$.

***Gap Diffie-Hellman Problem (GDHP)*:** A class of problems, where DDHP can be solved in polynomial time but no probabilistic algorithm exists that can solve CDHP in polynomial time.

III. MODEL OF THE PROPOSED ID-SDVS SCHEME

A SDVS scheme consists of four phases like an ordinary digital signature scheme. However, it differs from the digital signature scheme when we talk about the signature generation phase and the signature verification phase. In SDVS, during signature generation phase signer uses the public key of designated verifier and the designated verifier uses his secret key in the signature verification phase for verifying the signatures. The model of the SDVS scheme is as follows:

- **Setup:** Given security parameters, this probabilistic algorithm outputs the public parameters.
- **Key generation**: This probabilistic algorithm takes input the public parameters of users and outputs the public key and secret key of the users.
- **Signature generation**: It inputs a message *'m'*, random numbers, secret key of the signer and public key of the verifier and outputs the signature on message *'m'*.
- **Signature verification**: This deterministic algorithm takes input the message signature pair, secret key of the designated verifier and pubic key of the signer and outputs whether the signature are accepted or rejected.

IV. PROPOSED ID-SDVS SCHEME

The security of this scheme is based on the discrete logarithmic problem.

- **Setup:** In this phase, KGC chooses a generator P_1, a random number sZ_q^* and computes $P_{pub} = sP$. KGC also chooses two cryptographic hash functions H_1: $\{0, 1\}^*$ G_1 and $H_2 : \{0,1\}^*$ G_2 Z_q. The system parameters $(G_1, G_2, e, P, P_{pub}, H_1, H_2)$ (as defined earlier) are made public and *'s'* is kept secret with KGC.
- **Key Generation**: Given a user's identity ID_U, this phase generates $Q_{IDU} = H_1(ID\text{-}_U)$ as the public key, and $S_{IDU} = sH_1(ID_U)$ as the secret key of the user.
- **Signature Generation**: Alice chooses rZ_q^* and computes

  $U = r^{-1}Q_{IDB},\ h = H_2(m, e(P_{pub}, Q_{IDB})),\ V = rhS_{IDA}$

  Alice sends $s = (U, V)$ as the signature on message '*m*' to the verifier Bob.
- **Signature Verification**: On receiving (m, s) Bob computes

  $h = H_2(m, e(P, S_{IDB}))$ and accepts the signature iff $e(U,V) = e(S_{IDB}, Q_{IDA})^h$

V. SECURITY ANALYSIS

- **Correctness**: The following equation gives the correctness of the equation:

  $$\begin{aligned} & e(U,V) \\ & = e(r^{-1}Q_{IDB}, rhS_{IDA})^h \\ & = e(Q_{IDB}, sQ_{IDA})^h \\ & = e(S_{IDB}, Q_{IDA})^h \end{aligned}$$
- **Strongness:** The designated verifier Bob uses his secret key S_{IDC} to verify the signatures in the signature generation phase. So, our scheme provides the property of Strongness
- **Unforgeability:** It is not possible to construct V without the knowledge of the random numbers and the secret key of Alice. So, the signatures are unforgeable.
- **Non-Delegatability:** The signature generation phase involves the secret key of Alice and the signature verification phase uses the secret key of Bob to verify the signatures. So, neither Alice nor Bob can delegate their signing/verifying powers. Moreover, if any intruder gets the pairing $e(S_{IDC}, Q_{IDA})$ even then he cannot verify the signatures as the verification process involves the construction of '*h*' that uses S_{IDC}.

VI. EFFICIENCY ANALYSIS

Here we discuss the efficiency of our scheme and give a performance comparison of our scheme with the ID-SDVS scheme [1, 3, 6, 7] based on the length of signatures and the required signing and the verification cost. Here we have assumed that the bit length of elements in G_1 is $|G_1|$ and the bit length of elements in Z_q is $|Z_q|$

Table 1 : Performance Comparison with other ID-SDVS schemes

Schemes	**Signature Length**	**Signing Cost**	**Verification Cost**
Proposed	$2|G_1|$	$3M(G_1)+1H+1P$	$1H+1E+3P$
Huang et al [1]	$1\ |G_1|+4|Z_q|$	$1H+3E+3P$	$2M(G_2)+1H+4E+4P$
Kumar et al [3]	$4\ |G_1|$	$6M(G_1)+1H+1I+1P$	$1M(G_2)+1H+4P$
Bin Wang [6]	$3|G_1|+1|Z_q|$	$6M(G_1)+1H+2P$	$2M(G_1)+1M(G_2)+1H+3P$
Zhang et al [7]	$3\ |G_1|$	$4M(G_1)+1H+1I$	$1M(G_2)+1H+3P$

H = Hash, **M** = Multiplication, **E** = Exponential, **P** = Pairing, **I** = Inverse

Table 2 : Total number of computations used in each ID-SDVS scheme

Schemes/Operations	**Proposed**	**Huang et al [1]**	**Kumar et al [3]**	**Bin Wang [6]**	**Zhang et al [7]**
Hash	2	2	2	2	2
Multiplication	3	2	7	9	5
Pairing	4	7	5	5	3
Exponential	1	7	0	0	0
Inverse	0	0	1	0	1

From the above tables we get this result that our proposed scheme is more efficient in signing phase as it requires only one pairing and three multiplications and the signature size is only $2G_1$ in our proposed scheme which is smallest as compared to rest of the schemes. Moreover, no multiplication operations are required in signature verification phase. Thus, our scheme is efficient as compared to these schemes.

VII. APPLICATIONS

Strong Designated Verifier Signature scheme proposed in this paper have several practical applications in the situations where the signer wishes to convince only one person about the validity of the signatures. Consider, for example a situation where a private organization ‘O’ (Education Institute or a Software Company), invites the tender for equipments required to setup a new laboratory. The willing company ‘C’ is required to quote their prices for the tender requested by ‘O’, here the company quoting the lesser price will hold this financial contract.

Now following two important scenarios arise:

- Organization ‘O’ requires properly (preferably digitally) signed quotations by intending companies so that these quotations can actually be checked for their authenticity and originality, from whom they claimed to be. This is a valid requirement by the ‘O’.
- Company ‘C’, which is submitting their quotations, does not want their tenders to be affected by the decisions of other quoting companies. As there is a possibility that a company may capture the signed price proposal of another company (while in transfer to the organization ‘O’) and modify their own proposal so to increase their chances for gaining the tender.

To prevent their quotations from leaking, every company encrypts its signed quotations so that they can only be decrypted and read by the organization. However, once the proposal is decrypted, organization may use it to influence the other companies to quote a lesser price and in this way organization can obtain his requirements at a good price i.e. as low as possible.

Using ‘***Designated Verifier Signature***’ companies can sign their priced proposals and send them to the institutions. Now, if anyone captures these signed proposals (online, before arriving at the institution) one can only be convinced that they are produced by the company and not by the organization. Moreover, the organization can not show these proposals to any third party for getting their requirements at a lower price as the third party will not believe that they are signed by the company because the organization ‘O’ is also able to produce the same signed proposals.

Another application of SDVS is in software licensing. Software companies’ use digitally signed keys as there software license so that these keys can only be used by the person who buys the product. Use of SDVS to produce digitally signed keys/licenses protects illegal distribution of the software.

VIII. CONCLUSION

This paper proposes a new Efficient Non-Delegatable Identity Based Strong Designated Verifier Signature scheme. The proposed ID based SDVS scheme is more efficient as compared to the ID-SDVS scheme [1, 3, 6, 7] existing in literature. The signature length in our scheme is only $2|G_1|$ and also it requires only one pairing for signing algorithm and overall four pairing is required in our proposed ID-SDVS scheme.

REFERENCES

[1] Q.Huang, W.Susilo, D.S.Wong. Non-delegatable Identity based designated verifier signature scheme. Cryptography eprint Archive Report 2009/367. Available at http://eprint.iacr.org/2009/367.pdf

[2] M.Jakobsson, K.Sako, K.R.Impaliazzo. Designated verifier proofs and their applications. Eurocrypt 1996, LNCS #1070, Springer-Verlag, 1996, 142-154.

[3] K.P Kumar, G.Shailaja, Ashutosh Saxena. Identity based strong designated verifier signature scheme. Cryptography eprint Archive Report 2006/134. Available at http://eprint.iacr.org/2006/134.pdf

[4] H.Lipmaa, G.Wang, F.Bao. Designated verifier signatures schemes: Attacks, New security Notions and a new construction, 32nd International Colloquim on Automata, Languages and Programming, ICALP 2005, LNCS #3580, Springer-Verlag, 2005, 459-471.

[5] S.Saeednia, S.Kreme, O.Markotwich. An efficient strong designated verifier signature scheme. ICICS 2003, LNCS #2971, Springer-Verlag, 2003, 40-54.

[6] Bin Wang. A non-delegatable identity based strong designated verifier signature scheme. Cryptography eprint Archive Report 2008/507. Available at http://eprint.iacr.org/2008/507.pdf

[7] J.Zhang, J.Mao. A novel ID-based designated verifier signature scheme. Information Sciences, **178**(3)**:** 2008, 766-773.