# Some Identity Based Strong Bi-Designated Verifier Signature Schemes

***Sunder Lal and Vandani Verma***
***Department of Mathematics, Dr. B.R.A. (Agra), University, Agra-282002 (UP), India.***
**E-mail- sunder_lal2@rediffmail.com, verma_vandani@rediffmail.com**

**Abstract:** The problem of generalization of (single) designated verifier schemes to several designated verifiers was proposed by Desmedt in 2003. The paper proposes eight new Identity Based Strong Bi-Designated Verifier Signature Schemes in which the two designated verifiers may not know each other. The security and the computational efficiency of the schemes are also analyzed.

**Keywords:** ID based cryptography, multi-designated verifier, bilinear pairing, hash functions.

## 1. Introduction

Jakobsson et al [3] introduced the concept of designated verifier signatures (DVS) at Eurocrypt'1996. These signatures unlike the other digital signatures do not provide non-repudiation which is the main property of ordinary digital signatures. Such signatures are intended to a specific and unique designated verifier, who is the only one able to check their validity. The designated verifier is not able to convince the third person that the signatures are valid as he himself is able to produce the indistinguishable signatures. Saeednia, Kreme and Markotwich [7] introduced the concept of Strong Designated Verifier Signatures (SDVS) in 2003, which forces the designated verifier to use his secret key at the time of verification.

Desmedt [2], raised the problem of generalizing the designated verifier scheme to a specific set of different verifiers. This primitive is known as Multi-Designated Verifier Signature (MDVS). The validity of such signatures can only be checked by specified number of designated verifiers. Bi-designated schemes are formed when the number of designated verifiers is limited to two. The first Strong Bi-Designated verifier (SBDVS) scheme based on bilinear maps was proposed by Laguillaumie and Vergnaud in 2004.

In this paper we propose eight new Identity based strong bi-designated verifier signature (ID-SBDVS) schemes. All these schemes are based on [1, 4, 5, 6, 7, 8] but one of the scheme is new. In MDVS, a verifier uses the identity of the other designated verifiers to verify the signatures. In our schemes, the two designated verifiers may be unknown to each other. However, using the information provided with signatures and his own public key, the designated verifier may know the public key of the other verifier.

The rest of the paper is organized as follows: in section 2, we describe background concepts of bilinear parings and some related problems. Section 3 presents the model for our ID-SBDVS schemes. In section 4, we describe the proposed ID-SBDVS schemes. Section 5, presents the computational aspects of the schemes and section 6 gives the security analysis of the schemes. Finally we conclude the paper in section 7.

## 2. Background Concepts

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

### 2.1 Bilinear pairings

Let $G_1$ be a group of order a large prime number q and $G_2$ be a multiplicative subgroup of a finite field F of same order and P be a generator of $G_1$. A map e: $G_1 \times G_1 \rightarrow G_2$ is called a bilinear map if it has 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*:** $\exists$ P, Q $\in$ $G_1$, such that $e(P, Q) \neq 1$, the identity of $G_2$.

***Computability*:** $\forall$ P, Q $\in$ $G_1$ there is an efficient algorithm to compute e (P, Q).

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.

### 2.2 Computational problems

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

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

***Decisional Diffie-Hellman Problem (DDHP)*:** Given P, aP, bP, cP, for (unknown) a, b, c $\in$ $Z_q^*$, decide whether c = ab mod q.

***Computational Diffie-Hellman Problem (CDHP)*:** Given P, aP, bP, for (unknown) a, b $\in$ $Z_q^*$, compute abP

***Bilinear Diffie-Hellman Problem (BDHP):*** Given P, aP, bP, cP, for (unknown) a, b, c $\in$ $Z_q^*$, 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 which can solve CDHP in polynomial time.

## 3. Model for the proposed ID-SBDVS schemes

In this section we define the concept of a strong bi-designated verifier signature and list the various phases through which it is generated and state the properties that such a scheme is expected to have.

An ID-SBDVS has three users Alice (A), Bob (B) and Cindy (C) along with a key generating centre (KGC). KGC generates secret key of the user using user's public key and his own secret key. Using her secret key and public keys of B and C, A generates a signature on a message 'm'. Using her secret key and the public keys of A

and C, the user B can verify the signature. Similarly, C can verify the validity of the signatures.

Each of the proposed identity based strong bi-designated verifier signature scheme (ID-SBDVS) has five phases described as follows:

- **Setup:** Given security parameter k, this algorithm outputs the public parameters.
- **Key generation:** Given a user identity and the public parameters, this algorithm computes secret key of the user.
- **Signature generation:** On receiving the message 'm', the secret key of the signer and the public keys of the designated verifiers, this algorithm computes the bi-designated signature '$\sigma$' on message 'm'.
- **Signature verification:** On receiving the message signature pair (m, $\sigma$) and the secret of the designated verifiers, this algorithm tests whether '$\sigma$' is valid or not.
- **Simulation:** On receiving secret key of the designated verifiers and the public key of the signer, this algorithm simulates the signature designated to the designated verifiers such that it satisfies the verification process.

An ID-SBDVS scheme must satisfy the following properties:

- **Correctness:** A properly formed ID-SBDVS is accepted by the verifying algorithm.
- **Unforgeability:** It is computationally infeasible to construct a valid ID-SBDVS without the knowledge of the secret key of either the signer or those of the two designated verifiers.
- **Source hiding:** Given a message 'm' and ID-SBDVS on 'm', it is infeasible to determine who from the original signer or the designated verifiers performed the signature, even if one knows all the secret keys.
- **Non-delegatability:** Given any derivative of the secret key of the signer it is infeasible to construct a valid ID-SBDVS.

## 4. Identity Based Strong Bi-Designated Verifier Signature Schemes

In this section we propose eight new ID-based strong bi-designated verifier signature (ID-SBDVS) schemes. We also give the reviews of the schemes on which we base our schemes. In our schemes we have assumed A as the original signer and B and C as the two designated verifiers.

### 4.1 ID-SBDVS based on Laguillaumie and Vergnaud's scheme

Laguillaumie and Vergnaud [5] proposed the first strong bi-designated verifier signature scheme based on bilinear pairings. The review of the scheme is as follows:

- **Setup:** (q, $G_1$, $G_2$, e, P, H) is the output of this phase where $G_1$ is an additive group of a prime order q, $G_2$ is a multiplicative group of same order q, e: $G_1 \times G_1 \rightarrow G_2$ is a binear pairing, P is the generator of $G_1$ and H: $\{0, 1\}^* \times G_2 \rightarrow G_1$ is a hash function
- **Key generation:** Each user picks a random member $u \in Z_q^*$ and computes public key $P_u = uP$ and retains 'u' as his secret key.

- **Signature generation:** Given a message m $\in\{0,1\}^*$, A picks two random integers $r_1, r_2 \in Z_q^*$ Computes $U_1 = P_B + P_C$, $U_2 = e(P_B, P_C)^a$, $U_3 = H(m, U_2^{r_2})$, $U_4 = r_1P$, $V = a^{-1}(U_3 - r_1 U_1)$, The signature on message 'm' is the triple $\sigma = (r_2, U_4, V)$.
- **Signature verification:** Given $(m, \sigma)$ and the identity of the other designated verifier C, B computes $U_2 = e(P_A, P_C)^b$, $U_3 = H(m, U_2^{r_2})$ and accepts the signature iff $e(V, P_A)\, e(U_4, U_1) = e(U_3, P)$. Similarly, C can verify the signatures.

Now, we introduce the concept of identity in the above scheme to form our first ID-SBDVS scheme.

***Proposed scheme***

1. **Setup:** Given security parameter $k \in N$, this phase produces public parameters $(q, G_1, G_2, e, P, P_{pub}, H_1, H_2)$ where q, $G_1$, $G_2$, e and P are defined as above, $P_{pub} = sP$ ($s \in Z_q^*$ is a randomly chosen secret key of the KGC), $H_1: \{0,1\}^* \rightarrow Z_q^*$ and $H_2: \{0,1\}^* \times G_2 \rightarrow Z_q^*$ are the hash functions.

2. **Key Generation:** For a user U with identity $ID_U$ this phase generates public key $Q_{IDU} = H_1(ID_U)$ and secret key $S_{IDU} = s^{-1}.Q_{IDU}.P$ and communicates this secret key to the user in a secure manner.

3. **Signature generation:** Given secret key $S_{IDA}$ of the signer A, message 'm' and the public keys $Q_{IDA}$, $Q_{IDB}$ and $Q_{IDC}$ of the signer A, the two designated verifiers B and C and, this phase computes the signature $\sigma$ as follows:
   By choosing random numbers $(r_1, r_2) \in Z_q^*$ the signer A computes
   $U_1 = Q_{IDB} + Q_{IDC}$, $U_2 = e(S_{IDA}, P)^{Q_{IDB} Q_{IDC}}$, $U_3 = H_2(m, U_2^{r_2})$,
   $U_4 = r_1 .Q_{IDA}.P$, $V = S_{IDA}(U_3 - r_1 U_1)$.
   Alice sends $(m, \sigma)$ as the signatures on message 'm' to the designated verifiers Bob and Cindy where $\sigma = (r_2, U_1, U_4, V)$.

4. **Signature verification:** On receiving $(m, \sigma)$, the designated verifier B first computes the public key of the other designated verifier C from $U_1$ and then computes
   $Z_2 = e(S_{IDB}, P)^{Q_{IDA} Q_{IDC}}$, $Z_3 = H_2(m, Z_2^{r_2})$.
   He accepts the signatures iff $e(V, P)^{Q_{IDB}}\, e(U_4, S_{IDB})^{U_1} = e(S_{IDB}, P)^{Z_3 Q_{IDA}}$
   But if the verification procedure fails then either B is not the designated verifier or $\sigma$ is not correct.
   Similarly, on receiving $(m, \sigma)$ the designated verifier C computes the public key of the other designated verifier B with the help of $U_1$ and then computes
   $Z_2'$ = $e(S_{IDC}, P)^{Q_{IDA} Q_{IDB}}$, $Z_3'$ = $H_2(m, Z_2'^{r_2})$ and accepts the signature iff
   $e(V, P)^{Q_{IDC}}\, e(U_4, S_{IDC})^{U_1} = e(S_{IDC}, P)^{Z_3' Q_{IDA}}$

5. **Correctness:** The following equation gives the correctness of the verification for the designated verifier B.

$e(V, P)^{Q_{IDB}}\, e(U_4, S_{IDB})^{U_1}$
$= e(S_{IDA}(U_3 - r_1 U_1), Q_{IDB}.P)\, e(U_1.r_1 Q_{IDA}.P, S_{IDB})$
$= e(U_3 Q_{IDA}P - r_1 U_1 Q_{IDA} P, S_{IDB})\, e(r_1 U_1 Q_{IDA} P, S_{IDB})$
$= e(S_{IDB}, P)^{Z_3 Q_{IDA}}$ .

Similar correctness equation can also be given for the verifier C as follows:

$e(V, P)^{Q_{IDC}}\, e(U_4, S_{IDC})^{U_1}$
$= e(S_{IDA}(U_3 - r_1 U_1), Q_{IDC}.P)\, e(U_1.r_1 Q_{IDA}.P, S_{IDC})$
$= e(U_3 Q_{IDA}P - r_1 U_1 Q_{IDA} P, S_{IDC})\, e(r_1 U_1 Q_{IDA} P, S_{IDC})$
$= e(S_{IDC}, P)^{Z_3 Q_{IDA}}$ .

6. **Simulation:** The designated verifier B (and C) cannot prove to third party that the signature $\sigma$ has been produced by the signer A, as B (and C) can also produce the signature $\sigma'$ in the following way:
Bob chooses random numbers $t_1, t_2 \in Z_q^*$ computes
$U_1' = Q_{IDA} + Q_{IDC}$ , $U_2' = e(S_{IDB}, P)^{Q_{IDA} Q_{IDC}}$ , $U_3' = H_2(m, U_2'^{\,t_2})$,
$U_4' = t_1.Q_{IDB}.P$, $V' = S_{IDB}(U_3' - t_1 U_1')$.
$\sigma' = (t_2, U_1', U_4', V')$ is the simulated signatures produced by B on message 'm' which can be verified by A and C. Similarly, Cindy can simulate the signatures to be verified by A and B.

## 4.2 ID-SBDVS based on Kumar, Saxena and Shailaja's scheme

The review of Kumar's ID based strong designated verifier signature scheme is as follows:

- **Setup:** Except the hash functions $H_1$ and $H_2$ all settings are same as in proposed scheme in section 4.1. The hash functions are defined here into $G_1$ and not in $Z_q^*$.
- **Key generation:** Given an identity $ID_U$ of a user U, this phase generates $Q_{IDU} = H_1(ID_U)$ as the public key of the user. Further, KGC computes $S_{IDU} = sH_1(ID_U)$ as the secret key of the user and communicates through the secure channel.
- **Signature generation:** To generate signature on the message m which can be verified by the user B. The signer A chooses three random numbers $r_1, r_2, r_3 \in Z_q^*$ and computes
$U_1 = r_1 Q_{IDB}$ , $U_2 = r_2 Q_{IDA}$, $U_3 = r_3 U_1$ , $V = r_3 H + r_1^{-1} S_{IDA}$
where $H = H_2(m, e(r_2 Q_{IDB}, S_{IDA}))$.Signer A sends $(U_1, U_2, U_3, V)$ to the designated verifier B.
- **Signature verification:** On receiving $(U_1, U_2, U_3, V)$ the designated verifier B computes $H = H_2(m, e(U_2, S_{IDB}))$. B accepts the signature iff
$e(U_1, V) = e(U_3, H)\, e(S_{IDB}, Q_{IDA})$.

We now, use the above scheme to form our second ID-SBDVS scheme.

***Proposed scheme***

1. **Setup:** Except $H_1$: $\{0, 1\}^* \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \times G_2 \rightarrow G_1$ all the other settings are same as the proposed scheme in section 4.1.

2. **Key Generation:** Same as scheme proposed in section 4.1.

3. **Signature generation:** To generate signature on the message m which can be verified by the designated verifiers B and C, the signer A chooses three random numbers $r_1, r_2, r_3 \in Z_q^*$ and computes
   $X = Q_{IDB}Q_{IDC}$, $U_1 = r_1.X.P$, $U_2 = r_2Q_{IDA}.P$, $U_3 = r_3U_1$,
   $V = r_3H + r_1^{-1}S_{IDA}$, where $H = H_2(m, e(P, S_{IDA})^{r_2X})$.
   A sends $\sigma = (X, U_1, U_2, U_3, V)$ to the designated verifiers B and C as the signature on the message 'm'.

4. **Signature verification:** On receiving $(m, \sigma)$, the designated verifier B computes
   $Q_{IDC} = Q_{IDB}^{-1} X$ and $H = H_2(m, e(U_2, S_{IDB})^{Q_{IDC}})$.
   B accepts the signature iff $e(U_1, V) = e(U_3, H)\, e(S_{IDB}, P)^{Q_{IDA}.Q_{IDC}}$.
   Similarly, C can check the validity of the signatures.

5. **Correctness:** The following equation gives the correctness of the scheme for B.
   $e(U_1, V)$
   $= e(r_1.X.P, r_3H + r_1^{-1}S_{IDA})$
   $= e(r_1r_3 Q_{IDB}.Q_{IDC}.P, H)\, e(s^{-1} Q_{IDB}.Q_{IDC}.P, Q_{IDA}.P)$
   $= e(U_3, H)\, e(S_{IDB}, P)^{Q_{IDA}.Q_{IDC}}$.
   Similar correctness equation can also be given for C.

6. **Simulation:** The designated verifier produces the simulated signature $\sigma'$ in the following way: B chooses $t_1, t_2, t_3 \in Z_q^*$ and computes
   $X' = Q_{IDA}Q_{IDC}$, $U_1' = t_1.X'P$, $U_2' = t_2Q_{IDB}.P$, $U_3' = t_3U_1'$, $V' = t_3H' + t_1^{-1}S_{IDB}$
   where $H' = H_2(m, e(P, S_{IDB})^{t_2X'})$. $\sigma' = (X', U_1', U_2', U_3', V')$ is the simulated signatures produced by B. Similarly, C can simulate the signatures.

**4.3 ID-SBDVS based on Saeednia, Kreme and Markotwich's scheme**

The strong designated verifier signature scheme of Saeednia' et al [7] works as follows:

- **Setup:** A large prime p, a prime factor (p-1), a generator $g \in Z_q^*$ of order q and a one way hash function h are assumed to be some common parameters initially shared between the users.

- **Key generation:** Each user 'i' chooses a secret key $x_i \in Z_q$ and the corresponding public key $y_i = g^{x_i} \bmod p$ is made public.
- **Signature generation:** To sign a message m for B, A selects two random numbers $r_1, r_2 \in Z_q$ and computes $U_1 = y_b^{r_1} \bmod p$, $U_2 = h(m, U_1)$, $V = r_1 r_2^{-1} - U_2 x_a \bmod q$. A sends $(r_2, U_2, V)$ to B as signature on the message m.
- **Signature verification:** B accepts $(r_2, U_2, V)$ as the signature on 'm' iff $h(m, (g^V y_a^{U_2})^{r_2 x_b} \bmod p) = U_2$

Based on the above we propose third ID-SBDVS scheme as follows:

***Proposed scheme:***

1. **Setup:** Except $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : \{0,1\}^* \times G_2 \rightarrow Z_q^*$ rest of the settings are same as the proposed scheme in section 4.1

2. **Key Generation:** Same as review scheme in section 4.2.

3. **Signature generation:** A chooses two random numbers $r_1, r_2 \in Z_q^*$ and computes $X = Q_{IDB} + Q_{IDC}$, $U_1 = r_2.P$, $U_2 = e(U_1, X)$, $U_3 = H_2(m, U_2)$, $V = r_1^{-1} U_1 - U_3.S_{IDA}$ He sends $\sigma = (r_1, X, U_1, U_2, U_3, V)$ as signature on message 'm' to B and C.

4. **Signature verification:** On receiving $(m, \sigma)$, B first computes $Q_{IDC}$ (from X) and $U_3 = H_2(m, U_1)$, then he accepts the signature iff
   $[e(V, Q_{IDB})\, e(Q_{IDA}, S_{IDB})^{U_3}]^{r_1} e(U_1, Q_{IDC}) = U_2$.
   Similarly, C can check the validity of signatures by using his secret key.

5. **Correctness:** The following equation gives the correctness of the scheme for B.
   $$\begin{aligned}
   &[e(V, Q_{IDB})\, e(Q_{IDA}, S_{IDB})^{U_3}]^{r_1} e(U_1, Q_{IDC}) \\
   &= [e(r_1^{-1} U_1 - U_3.S_{IDA}, Q_{IDB})\, e(U_3.S_{IDA}, Q_{IDB})]^{r_1} e(U_1, Q_{IDC}) \\
   &= e(r_1^{-1} U_1, Q_{IDB})^{r_1} e(U_1, Q_{IDC}) \\
   &= e(U_1, Q_{IDB} + Q_{IDC}) \\
   &= e(U_1, X) \\
   &= U_2
   \end{aligned}$$
   Similar correctness equation can also be given for C.

6. **Simulation:** The signature $\sigma$ can be simulated by B in the following way:
   B chooses two random numbers $t_1, t_2 \in Z_q^*$ and computes
   $X' = Q_{IDA} + Q_{IDC}$, $U_1' = t_2.P$, $U_2' = e(U_1', X')$,
   $U_3' = H_2(m, U_2')$, $V' = t_1^{-1} U_1' - U_3' S_{IDB}$
   $\sigma' = (t_1, X', U_1', U_2', U_3', V')$ is the simulated signature on the message 'm'. C can also produce the simulated signatures.

**4.4 ID-SBDVS based on K. G. Paterson's scheme**

K.G.Paterson's [6] ID based signatures on elliptic curves works as follows:

- **Setup:** Except the hash functions $H_1:\{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow Z_q$, $H_3: G_1 \rightarrow Z_q$ all the other settings are same as in the proposed scheme in section 4.1.
- **Key generation:** Same as review scheme in section 4.2.
- **Signature generation:** To sign a message user A chooses a random number $r \in Z_q^*$ and computes $U = rP$, $V = r^{-1}[H_2(m).P + H_3(U).S_{IDA}]$. The pair (U, V) is the signature on message 'm'.
- **Signature verification:** On receiving (U, V) the verifier B accepts the signature iff $e(U, V) = e(P, P)^{H_2(m)} e(P_{pub}, Q_{IDA})^{H_3(U)}$

Now, we add the concept of strong bi-designated verifier to the above scheme to form our forth ID-SBDVPS scheme.

***Proposed scheme:***

1. **Setup:** In this phase only two hash functions $H_1 : \{0,1\}^* \rightarrow Z_q$ and $H_2 : G_1 \rightarrow Z_q^*$ are used and rest of the settings are same as in the review scheme.

2. **Key Generation:** Same as proposed scheme in section 4.1.

3. **Signature generation:** A chooses a random number $r \in Z_q^*$ and computes
   $X = Q_{IDB}.Q_{IDC}$ , $U = r.X.P$, $V = r^{-1}[H_1(m).P + H_2(U).S_{IDA}]$.
   A sends $\sigma = (X, U, V)$ to B and C as the signatures on message 'm'.

4. **Signature verification:** On receiving $(m, \sigma)$, B first computes $Q_{IDC} = Q_{IDB}^{-1} X$ and accepts the signature iff $e(U, V) = e(P, P)^{X H_1(m)} e(S_{IDB}, P)^{Q_{IDA} Q_{IDC} H_2(U)}$ .
   Similarly, C can check the trueness of the signatures by using his secret key.

5. **Correctness:** The following equation gives the correctness of the scheme for B .
   $e(U, V)$
   $= e(r.X.P,\ H_1(m) P + H_2(U) S_{IDA})$
   $= e(P, P)^{X H_1(m)} e(S_{IDB}, P)^{Q_{IDA} Q_{IDC} H_2(U)}$
   Similar correctness equation can also be given for C.

6. **Simulation:** The signature $\sigma$, can be simulated by B in the following way:
   B chooses a random numbers $t \in Z_q^*$ and computes
   $X' = Q_{IDA} Q_{IDC}$ , $U' = t.\ X'.P$, $V' = t^{-1}[\ H_1(m).P + H_2(\ U').S_{IDB}]$.
   The simulated signature $\sigma' = (X', U', V')$ satisfies the verification process. C can also produce the simulated signatures satisfying the verification process.

**4.5 ID-SBDVS based on Cha and Cheon's scheme**

Cha and Cheon's [1] ID based signature scheme works as follows:

- **Setup:** Except the hash functions $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \times G_1 \rightarrow Z_q$ all the other system parameters (q, $G_1$, $G_2$, P, $P_{pub}$, e) are same as scheme proposed in section 4.1.
- **Key generation:** Same as review scheme in section 4.2.
- **Signature generation:** To sign a message user A chooses a random number $r \in [2, q-1]$ and computes $U_1 = r\, Q_{IDA}$, $U_2 = H_2(m, U_1)$, $V = (r + U_2)\, S_{IDA}$. $(U_1, V)$ is the signature on message 'm'.
- **Signature verification:** On receiving $(U_1, V)$ the verifier B computes $U_2 = H_2(m, U_1)$, $W = U_1 + U_2\, Q_{IDA}$ and accepts the signature iff $e(P, V) = e(P_{pub}, W)$

***Proposed scheme:***

1. **Setup and Key Generation:** Same as proposed scheme in section 4.1.

2. **Signature generation:** A chooses a random number $r \in Z_q^*$ and computes
   $X = Q_{IDB}\, Q_{IDC}$, $U_1 = r.Q_{IDA}\, P$, $U_2 = H_2(m, e(P, S_{IDA})^{rX})$, $V = (r + U_2)\, S_{IDA}$
   A sends $\sigma = (X, U_1, V)$ as the signature on message 'm' to B and C.

3. **Signature verification:** On receiving $(m, \sigma)$, B first computes $Q_{IDC} = Q_{IDB}^{-1}\, X$
   $U_2 = H_2(m, e(S_{IDB}, U_1)^{Q_{IDC}})$, and accepts the signature iff
   $e(P, V)^{Q_{IDB}} = e(S_{IDB}, U_1 + U_2\, Q_{IDA}.P)$.
   Similarly, C can check the trueness of the signatures by using his secret key.

4. **Correctness:** The following equation gives the correctness of the scheme for B.
   $e(P, V)^{Q_{IDB}}$
   $= e(P, (r + U_2)\, S_{IDA})^{Q_{IDB}}$
   $= e(s^{-1}\, Q_{IDB}\, P,\ r\, Q_{IDA}\, P + U_2 Q_{IDA} P)$
   $= e(S_{IDB}, U_1 + U_2\, Q_{IDA}.P)$
   Similar correctness equation can also be given for C.

5. **Simulation:** The signature $\sigma$ can be simulated by B in the following way: B chooses a random numbers $t \in Z_q^*$ and computes
   $X' = Q_{IDA}\, Q_{IDC}$, $U_1' = t.Q_{IDB}P$, $U_2' = H_2(m, e(P, S_{IDB})^{tX'})$, $V' = (t + U_2')\, S_{IDB}$
   $\sigma' = (X', U_1', V')$ is the simulated signature on message 'm' satisfying the verification process. C can also produce the simulated signatures satisfying the verification process in the similar way.

**4.6 ID-SBDVS based on Y. Zheng's Short Signature scheme I**

The review of Zheng's [8] shortened form I of digital signature standard (DSS) is as follows:

- **Setup:** A large prime p, a prime factor p-1 , a generator $g \in Z_q^*$ of order q and a one way hash function h are assumed to be some common parameters initially shared between the users.
- **Key generation:** Each user i chooses a secret key $x_i \in Z_q$ and the corresponding public key $y_i = g^{x_i} \bmod p$ is made public.
- **Signature generation:** The signer A chooses $r \in [1,\ldots.p-1]$**.** Computes
  $U_1 = g^r \bmod p$, $U_2 = h(m, U_1)$, $V = r\,(1 + x_a.U_2)^{-1} \bmod q$.
  $(U_2, V)$ is the signature on message 'm'
- **Signature verification:** On receiving $(U_2, V)$ the verifier B computes
  $U_1' = (y_a{}^{U_2}\, g)^V \bmod p$, $U_2' = h(m, U_1')$ and accepts the signature iff $U_2' = U_2$

Now, we add the concept of identity and strong bi-designated verifier to the above scheme to form our sixth ID-SBDVPS scheme.

***Proposed scheme:***

1. **Setup and key generation:** Same as proposed scheme in section 4.1.

2. **Signature generation:** A chooses a random number $r \in Z_q^*$ and computes
   $X = Q_{IDB}\, Q_{IDC}$, $U_1 = e(P, P)^{-r X}$ , $U_2 = H_2(m, U_1)$ ,
   $U_3 = r.Q_{IDA}.P$, $V = -r\,(P + U_2.\, S_{IDA})$ ,
   A sends $\sigma = (X, U_1, U_2, U_3, V)$ as the signature on message 'm' to B and C.

3. **Signature verification:** On receiving $(m, \sigma)$, B first computes $Q_{IDC} = Q_{IDB}^{-1}\, X$ accepts the signature as valid signature on message 'm' iff
   $e(V, P)^X\, e(U_3, S_{IDB})^{U_2 Q_{IDC}} = U_1$

4. **Correctness:** The following equation gives the correctness of the scheme for B.
   $e(V, P)^X\, e(U_3, S_{IDB})^{U_2 Q_{IDC}}$
   $= e(-rP - rU_2\, S_{IDA}, X.P)\, e(r\, U_2\, Q_{IDA}\, P, S_{IDB}\, Q_{IDC})$
   $= e(-rP - rU_2\, S_{IDA}, X.P)\, e(r\, U_2\, S_{IDA}, X.P)$
   $= e(P, P)^{-r X}$
   $= U_1$
   Similar correctness equation can also be given for C.

5. **Simulation:** To simulate the signatures B chooses $t \in Z_q^*$ and computes
   $X' = Q_{IDA}\, Q_{IDC}$ , $U_1' = e(P, P)^{-t X'}$ , $U_2' = H_2(m, U_1')$ ,
   $U_3' = t\, Q_{IDB}.P$, $V' = -t\,(P + U_1'\, S_{IDB})$

$\sigma' = (X', U_1', U_2', U_3', V')$ is the simulated signature on message 'm' satisfying the verification process. C can also produce the simulated signatures satisfying the verification process in the similar way.

**4.7 ID-SBDVS based on Y. Zheng's Short Signature scheme II**

Zheng's[8] shortened form II of digital signature standard (DSS) works as follows:

- **Setup:** A large prime p, a prime factor p-1 , a generator $g \in Z_q^*$ of order q and a one way hash function h are assumed to be some common parameters initially shared between the users.
- **Key generation:** Each user i chooses a secret key $x_i \in Z_q$ and the corresponding public key $y_i = g^{x_i} \bmod p$ is made public.
- **Signature generation:** The signer A chooses $r \in [1,\ldots p-1]$**.** Computes
  $U_1 = g^r \bmod p$, $U_2 = h(m, U_1)$, $V = r (U_2 + x_a)^{-1} \bmod q$.
  $(U_2, V)$ is the signature on message 'm'.
- **Signature verification:** On receiving (r, s) the verifier B computes
  $U_1' = (y_a g^{U_2})^V \bmod p$, $U_2' = h(m, U_1')$ and accepts the signature iff $U_2' = U_2$

Now, we add the concept of identity and strong bi-designated verifier to the above scheme to form our sixth ID-SBDVPS scheme.

***Proposed scheme:***

1. **Setup and key generation:** Same as proposed scheme in section 4.1.

2. **Signature generation:** A chooses a random number $r \in Z_q^*$ and computes
   $X = Q_{IDB} Q_{IDC}$, $U_1 = e(P, P)^{-r X}$, $U_2 = H_2(m, U_1)$ , $U_3 = U_1^{U_2}$ ,
   $U_4 = r.Q_{IDA}.P$, $V = -r (U_2.P + S_{IDA})$ ,
   A sends $\sigma = (X, U_3, U_4, V)$ as the signature on message 'm' to B and C.

3. **Signature verification:** On receiving $(m, \sigma)$, B first computes $Q_{IDC} = Q_{IDB}^{-1} X$ and accepts the signature iff $e(V, P)^X e(U_4, S_{IDB})^{Q_{IDC}} = U_3$.
   Similarly, C checks the validity of the signatures by using his secret key.

4. **Correctness:** The following equation gives the correctness of the scheme for B.
   $e(V, P)^X e(U_4, S_{IDB})^{Q_{IDC}}$
   $= e(-r U_2 P - r S_{IDA}, X P) e(r Q_{IDA} P, S_{IDB} Q_{IDC})$
   $= e(-rU_2 P - r S_{IDA}, Q_{IDB} Q_{IDC} P) e(r S_{IDA}, Q_{IDB} Q_{IDC} P)$
   $= [e(P, P)^{-r X}]^{U_2}$
   $= U_3$
   Similar correctness equation can also be given for C.

5. **Simulation:** To simulate the signatures B chooses $t \in Z_q^*$ and computes $X' = Q_{IDA} Q_{IDC}$, $U_1' = e(P, P)^{-t X'}$, $U_2' = H_2(m, U_1')$, $U_3' = U_1'^{U_2'}$, $U_4' = t\, Q_{IDB}.P$, $V' = -t(U_2'.P + S_{IDB})$.
$\sigma' = (X', U_3', U_4', V')$ is the simulated signature on message 'm' produced by B. C can also produce the simulated signatures

**4.8 A new ID-SBDVS scheme**

In this section we propose a new ID-SBDVS scheme, which is independent of any of the above schemes.

***Proposed scheme:***

1. **Setup:** Except the hash functions $H_1 : \{0,1\}^* \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \times G_2 \rightarrow Z_q^*$ the rest of the settings are same as proposed scheme 4.1.
2. **Key Generation:** Same as proposed scheme in section 4.1

3. **Signature generation:** A chooses a random number $r \in Z_q^*$ and computes $X = Q_{IDB} Q_{IDC}$, $U = r^{-1}.X.P$, $V = r.\, H_2(m, U).\, S_{IDA}$.
Alice sends $\sigma = (X, U, V)$ as the signature on message 'm' to B and C.

4. **Signature verification:** On receiving $(m, \sigma)$, B first computes $Q_{IDC} = Q_{IDB}^{-1} X$ and accepts the signature as valid signature on message 'm' iff
$e(U, V) = e(P, S_{IDB})^{X H_2(m,U)}$.
Similarly, C can check the validity of the signatures.

5. **Correctness:** The following equation gives the correctness of the scheme for B.
$e(U, V)$
$= e(r^{-1}X P, r.\, H_2(m, U).\, S_{IDA})$
$= e(r^{-1}Q_{IDB}\, Q_{IDC}\, P, r.\, H_2(m, U).\, S_{IDA})$
$= e(P, S_{IDB})^{Q_{IDA} Q_{IDC} H_2(m,U)}$.
Similar correctness equation can also be given for C.

6. **Simulation:** To simulate the signatures B chooses $t \in Z_q^*$ and computes
$X' = Q_{IDA} Q_{IDC}$, $U' = t^{-1} X' P$, $V' = t\, H_2(m, U').\, S_{IDB}$.
$\sigma' = (X', U', V')$ is the simulated signature on message 'm' satisfying the verification process. C can also produce the simulated signatures satisfying the verification process in the similar way.

## 5. Computational aspects:

We observe that the formation of the proposed schemes require the operations of the hashing, multiplication, pairing evaluation, exponentiation and taking the inverse. In this section, we compare the proposed eight schemes discussed above by counting the

number of the hash, multiplication, exponentiation, pairing and inverse required in signature generation and signature verification in each scheme. The following table gives the computational complexity of the schemes at a glance:

| Proposed Schemes | Signature Generation | | | | | Signature Verification | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **H** | **M** | **E** | **P** | **I** | **H** | **M** | **E** | **P** | **I** |
| 4.1 | 1 | 5 | 2 | 1 | - | 1 | 2 | 5 | 4 | - |
| 4.2 | 1 | 9 | 1 | 1 | 1 | 1 | 2 | 2 | 4 | 1 |
| 4.3 | 1 | 3 | - | 1 | 1 | - | - | 2 | 3 | - |
| 4.4 | 2 | 6 | - | - | 1 | 2 | 4 | 2 | 3 | 1 |
| 4.5 | 1 | 5 | 1 | 1 | - | 1 | 3 | 2 | 3 | 1 |
| 4.6 | 1 | 6 | 1 | 1 | - | - | 2 | 2 | 2 | 1 |
| 4.7 | 1 | 6 | 2 | 1 | - | - | - | 2 | 2 | 1 |
| 4.8 | 1 | 5 | - | - | 1 | 1 | 2 | 1 | 2 | 1 |

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

Our new proposed scheme 4.8 requires least number of hashing and least numbers of pairing evaluation. However, the scheme based on Saeednia et al (4.3) requires least number of multiplications. The schemes 4.1, 4.2 require maximum number of pairing evaluation (one for signature generation and four for signature verification).

## 6. Security analysis

In this section, we analyze the security of the proposed scheme.

### 6.1 Strongness

In each scheme the designated verifiers B (and C) has to use his secret key during verification. Therefore, no one else except the designated verifiers can check the validity of the signatures. Thus, our proposed schemes are strong bi-designated verifier signature scheme.

### 6.2 Unforgeability

It is not possible to construct certain terms in the signature generation process without the knowledge of either the secret key of the signer A or the two designated verifiers B and C. Thus, the signature is unforgeable.

### 6.3 Non-delegatability

The construction of signature involves the secret key of the signer A. So, A cannot delegate his signing capability to any third party without disclosing her secret. Thus, our schemes are non- delegatable.

### 6.4 Source hiding

Even knowing the secrets of the original signer A and the two designated verifiers B and C, third party cannot identify whose secret key is used in the signing process as the third party does not have any information about the random number used during the signing process.

### 6.5 Non-transferability privacy

The designated verifiers B and C cannot prove to a third party that the signature on message is produced by A as they are also able to simulate the signature.

## 7. Conclusion

In this paper we proposed eight new Identity based strong bi-designated verifier signature schemes in which no one except the two designated verifiers can check the validity of the signatures. The schemes are useful in the situations where the designated signatures are to verifiable by two verifiers only. Out of the eight scheme described here the scheme 4.8 is computationally most efficient.

## Refrences:


1. **J.C.Cha, J.H Cheon.** An identity based signature from gap Diffie-Hellman groups. Public key cryptography PKC 2003, LNCS #2567, Springer-Verlag, 1990, 18-30.
2. **Y.Desmedt.** Verifier-Designated Signatures, Rump Session, Crypto'03 (2003).
3. **M.Jakobsson, K.Sako, K.R.Impaliazzo.** Designated verifier proofs and their applications. Eurocrypt 1996, LNCS #1070, Springer-Verlag, 1996, 142-154.
4. **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