International Journal of Technology and Engineering Studies
volume 7 issue 1 pp. 10-16 doi: https://dx.doi.org/10.20469/ijtes.7.10002-1

An Efficient Strong Designated Multi-Verifier Signature Scheme with Shared Verification

Han-Yu Lin[*]
Department of Computer Science & Engineering,
National Taiwan Ocean University,
Keelung, 202, Taiwan

Tung-Tso Tsai
Department of Computer Science & Engineering,
National Taiwan Ocean University,
Keelung, 202, Taiwan

Pei-Yih Ting
Department of Computer Science & Engineering,
National Taiwan Ocean University,
Keelung, 202, Taiwan

Hsu-Lun Wu
Department of Computer Science & Engineering,
National Taiwan Ocean University,
Keelung, 202, Taiwan

Abstract: This paper proposes an efficient Strong Designated Multi-Verifier Signature (SDMVS) scheme for facilitating the privacy-preserving group-oriented electronic commerce applications. A Designated Verifier Signature (DVS) scheme can support online transactions that must simultaneously guarantee the property of confidentiality and authenticity since the generated signature can only be authenticated by a designated verifier. In this study, we combine the concept of DVS and multi-recipients to propose an SDMVS scheme. In particular, our mechanism further enables a group of intended recipients to examine the signature validity. All members of the designated verifier group must cooperate in carrying out the signature verification procedure. Besides, the property of non-transferability provides the designated verifier group with the ability to create another legitimate transcript that is hard to be differentiated from the original signature. The analysis results of security proof and efficiency show that the construction of our system fulfills essential security requirements, and the expansion of group size will not influence the computational costs of each party.

Keywords: *Strong designated verifier, group-oriented, shared verification, digital signature, public-key system*

Received: 26 August 2020; ***Accepted:*** 19 January 2021; ***Published:*** 27 February 2021

I. INTRODUCTION

In public-key cryptosystems [1, 2, 3], digital signature schemes have been applied in many fields. A digital signature should ensure crucial properties, including authenticity, integrity, along with non-repudiation. Nevertheless, the confidentiality property is not fulfilled in generic digital signature schemes. It is thus obvious that a traditional signature scheme is not well-suited for privacy-aware applications like online auctions, credit card transactions, and copyright protection [4, 5, 6].

The undeniable signature [7] was first introduced in 1990. In such a scheme, a verifier and the signature signer must work together to authenticate a signature. In other words, the original signer has the right to decide who has permission to access his/her signatures. However, this also leads to an evident disadvantage that an original signer must join every verification process.

In 1996, a designated verifier proof system [8] was proposed. This system allows a verifier to perform the verification procedure of signature solely. Meanwhile, the authenticity of the generated signature is only convinced by a specified person due to the property of non-transferability. Specifically, designated verifiers are capable of producing legitimate transcripts at will.

[*] Correspondence concerning this article should be addressed to Han-Yu Lin, Department of Computer Science & Engineering, National Taiwan Ocean University, Keelung, 202, Taiwan. E-mail: lin.hanyu@msa.hinet.net

In 2003, some researchers [9] further addressed a Strong version of DVDs (SDVS for short) which combined the verification key of the specified recipient with the signature inspection procedure. In this way, anyone without knowing the information of the correct private key cannot verify a given signature. Later, Zhang and Wen [10] presented an identity-based SDVS mechanism using the intractable Gap Bilinear Diffie-Hellman Problem (GBDHP).

In 2007, some researchers [11] integrated the functionality of message recovery with SDVS so that a verifier could recover the original message from the received signature. Similarly, in 2008, Lei and Daxing [12] proposed a ring signature variant of SDVS schemes with $O(1)$ computational cost of bilinear pairings and implemented in identity-based cryptosystems.

Without relying on a single PKG, in 2011, Zhang et al. [13] realized a novel ID-based SDVS protocol utilizing two independent PKGs to prevent the impersonation attack. For facilitating the group applications, Tian [14] presented the strong multiple designated verifiers signature (SMDVS) scheme that could be applied in broadcast propagation.

In 2018, Deng et al. [15] considered the many-to-many applications and proposed a multi-signer universal designated multi-verifier signature in identity-based systems. Their system employs the famous Discrete Logarithm Problem (DLP) as the basic security assumption and could be proved secure using random oracle security models. Nevertheless, they fail to discuss the non-delegatability in their mechanism.

In 2019, Rastegari et al. [16] further combined DVS with certificates cryptosystems and achieved a substantial system that was proved to be secure using the standard model. At present, many scholars have paid attention to the development of SDVS systems [17, 18, 19, 20, 21, 22, 23].

This study aims to extend the traditional SDVS scheme to group-oriented applications. Consequently, the authors pay attention to the collaborative system. They will introduce a new SDVS variant called Strong Designated Multi-Verifier Signature (SDVMS), which permits shared verification among a designated verifying group. The importance of this study is obvious, as the proposed SDMVS scheme is suitable for privacy-enabled services in electronic commerce applications.

II. PRELIMINARIES

We first recall some mathematical and computational backgrounds, including some characteristics of the bilinear map, and utilized cryptographic problems.

A. *Definition of Bilinear Pairings*

Let G_1 and G_2 be two groups. The former is additive, and the latter is multiplicative. These two groups have a prime order q. The function of bilinear pairing can be expressed as e: G_1 x $G_1 \rightarrow G_2$ having some characteristics below:

1) Bilinearity:

$$e(P_X + P_y,\, W) = e(P_x, W)\, e(P_y, W)$$
$$e(R, Q_x + Q_y) = e(R, Q_x)\, e(R, Q_y)$$

2) Non-degeneracy: If P is a generator of group G_1, $e(P, P)$ would be a generator of group G_2.

3) Computability: Given two values $P_x, P_y \in G_1^2$, the parameter e(P_x, P_y) could be derived efficiently utilizing a polynomial-time algorithm.

- Bilinear Diffie-Hellman Problem (BDHP): Given a problem input $(P, X, Y, Z) \in G_1$ in which $X = aP$, $Y = bP$ and $Z = cP$ for some $a, b, c \in Z_q^*$, it must derive the correct parameter $e(P,P)^{abc}$.
- Assumption of Bilinear Diffie-Hellman (BDH): It is computationally difficult for any probabilistic algorithm to solve the above BDHP in polynomial-time.

III. THE PROPOSED SCHEME

We introduce the proposed scheme, including joined roles, composed algorithms, and a substantial protocol.

A. *Joined Roles*

The proposed SDMVS system has two main entities, i.e., a signer and a specified verifier group of N members. The signer will produce a designated verifier signature intended for the specified verifier group. There is also a clerk in the group and would be responsible for assisting all members in inspecting the signature and creating an indistinguishable transcript if necessary.

B. *Algorithms*

The proposed SDMVS system has four composing algorithms. We describe each algorithm below:

- Setup: By running the Setup algorithm with a given security parameter, we could initialize the system parameters.
- SDMVS-Gen: The SDMVS-Gen algorithm will generate a designated verifier signature δ for the designated verifier group. The input parameters consist of the public parameter, a message, the signer's private key, and the public keys of all members in the designated verifier group.
- SDMVS-Verify: The goal of this algorithm is to verify the validity of the signature δ. It will output

True if δ is valid. If not, an error flag is returned. The input values consist of public parameters, the signer's public key, the private keys of all members in the designated verifier group, a message along with its SDMVS δ.

- Transcript-Simulation (TS): The specified verifier group can produce another SDMVS transcript δ^* intended for themselves by running the TS algorithm. The necessary input values include public parameters, the signer's public key, the private keys of all members in the specified verifier group, a message, and its corresponding designated verifier signature δ^*.

C. Construction

According to the algorithms described in section 3.2, the authors will present a concrete protocol of the proposed strong designated multi-verifier signature system below:

- Setup: Let the symbol of k be a given security parameter. This algorithm will select two groups (G_1, G_2). The group of G_1 is additive while that of G_2 is multiplicative, and each group has an order of the prime value q. A generator in the group G_1 is denoted as P. Two secure hash functions, i.e., (h_1, h_2), will be employed in the system. A bilinear map e is expressed as e: G_1 x $G_1 \rightarrow G_2$. The public values consist of G_1, G_2, q, P, e, h_1, h_2.
- SDMVS-Gen: Let the symbols U_s be a signer and V_G = V_1, V_2, ..., V_n a designated verifier group of n verifiers. Every user has a private-public key pair of ($x_i \in Z_q$, Y_i = x_i P). For signing a message m designed for the group V_G, U_s randomly selects a salt $t \in Z_q^*$ to derive:

$$R = tP \qquad (1)$$

$$W = t\sum_{i=1}^{n} Y_{v_i} \qquad (2)$$

$$Z = e\left(x_s \sum_{i=1}^{n} Y_{v_i}, h_2(W)\right) \qquad (3)$$

$$\sigma = e\left((x_s + h_1(m,Z,R))R, P\right) \qquad (4)$$

Here, (R,σ) is the SDMVS associated with m.

- SDMVS-Verify: In order to verify the SDMVS (R,σ) with the message m, each verifier V_i of the group V_G will compute

$$R_i = x_{v_i}R \qquad (5)$$

and then sends it to the clerk V_k who obtains all R_i's will compute

$$W' = \sum_{V_i \in VG} R_i \qquad (6)$$

and then broadcasts W' to $V_i \in V_G$. Upon receiving it, each V_i computes

$$Z_i = e\left(x_{v_i}Y_s, h_2\left(W'\right)\right) \qquad (7)$$

and delivers it to the clerk V_k. After receiving all Z_i's, V_k computes

$$Z' = \prod_{V_i \in VG} Z_i \qquad (8)$$

and verifies the validity of it by checking if

$$\sigma = e\left(R, h_1\left(m, Z', R\right)P + Y_s\right) \qquad (9)$$

The authors show that Eq. 9 is correct by the following derivations. Derived from the right side of this equality, we obtain that

$$= e\left(\left(x_s + h_1\left(m, e\left(x_s\sum_{i=1}^{n} Y_{v_i}, h_2\left(\sum_{V_i \in VG} R_i\right)\right), R\right)\right)R, P\right) \qquad \text{(by Eq. 7)}$$

$$= e\left(\left(x_s + h_1\left(m, e\left(x_s\sum_{i=1}^{n} Y_{v_i}, h_2\left(\sum_{V_i \in VG} x_{v_i}R\right)\right), R\right)\right)R, P\right) \qquad \text{(by Eq. 6)}$$

$$= e\left(\left(x_s + h_1\left(m, e\left(x_s\sum_{i=1}^{n} Y_{v_i}, h_2\left(t\sum_{i=1}^{n} Y_{v_i}\right)\right), R\right)\right)R, P\right)$$

$$= e\left(\left(x_s + h_1\left(m, e\left(x_s\sum_{i=1}^{n} Y_{v_i}, h_2(W)\right), R\right)\right)R, P\right) \qquad \text{(by Eq. 5)}$$

$$= e\left((x_s + h_1(m,Z,R))R, P\right)$$

$$= \sigma \qquad \text{(by Eq. 2)}$$

- Transcript-Simulation (TS): For creating a signature transcript associated with the signed message m, the clerk V_k initially selects $R' \in_R G_1$ and broadcasts it to all members of V_G. Every user in the group V_G will derive

  $$R''_i = x_{v_i} R'' \tag{10}$$

  and then sends it back to the clerk V_k who will compute

  $$W'' = \sum_{V_i \in VG} R''_i \tag{11}$$

  and then broadcasts W'' to $V_i \in V_G$. Upon receiving it, each V_i computes

  $$Z''_i = e\left(x_{v_i} Y_s, h_2\left(W''\right)\right) \tag{12}$$

  and delivers it to the clerk V_k who can therefore derive

  $$Z'' = \prod_{V_i \in VG} Z''_i \tag{13}$$

  $$\sigma'' = e\left(Y_s + h_1\left(m, Z'', R'\right) P, R'\right) \tag{14}$$

  The computed δ'' composed of (R'', σ'') would be viewed as a valid transcript of SDVS with the message m.

IV. SECURITY PROOF AND EFFICIENCY

We demonstrate that the proposed mechanism achieves the necessary security characteristics. In addition, some efficiency evaluation will also be made.

A. *Security Proof*

Theorem 1: Provided that there is no probabilistic adversary who could break the assumption of BDH with the non-negligible advantage and run within polynomial-time, the proposed SDMVS protocol is selectively secure against adaptive chosen-message attacks (CMA) in random oracle models.

1) Proof: This theorem is completed by using the technique of reduction. Specifically, suppose there is a probabilistic adversary $\mathscr{A}$ who runs in polynomial-time and has the advantage ε, which is non-negligible to break the proposed system in the adaptive chosen-message attacking scenarios. In that case, we could break the assumption of BDH by generating another algorithm, say $\mathscr{B}$. Let (*P, aP, bP, cP*) be an input of BDHP, and the success output of $\mathscr{B}$ has to be $e(P,P)^{abc}$. $\mathscr{B}$ is also responsible for returning $\mathscr{A}$'s oracle queries below:

- Setup: At the beginning, $\mathscr{B}$ initializes system parameters and sends public parameters $G_1, G_2, q, P, e, Y_s = aP, Y_{v_1}, Y_{v2}, Y_{v3}, \ldots, Y_{v_n} = bP - (Y_{v1} + Y_{v_2} + \ldots Y_{v_n})$ to the adversary $\mathscr{A}$.
- Phase 1: The procedures performed by $\mathscr{B}$ are stated below:
  – h_1 oracle: If adversary $\mathscr{A}$ submits an h_1(*m, Z, R*) oracle, $\mathscr{B}$ searches the maintained h_1-table for a consistent value $V_1 \in_R Z_q$ within the entry (*m, Z, R,* V_1) and then outputs it.
  – h_2 oracle: If adversary $\mathscr{A}$ submits an $h_2(W)$ query, $\mathscr{B}$ looks at the maintained h_2-table for a consistent value $V_2 \in_R G_1$ within the entry (W, v_2, V_2) then return it. Note that when $\mathscr{A}$ makes the j-th query, $\mathscr{B}$ would directly return the value cP and add a new record of (W, null, cP) into the h_2-table.
  – SDMVS-Gen query: Whenever $\mathscr{A}$ queries a strong designated verifier signature associated with the message m, $\mathscr{B}$ will return a derived $\delta = (R, \sigma)$ in which $R = tP$ where $t \in Z_q^*$,

$$W = t \sum_{i=1}^{n} Y_{v_i} = t(bP) \tag{15}$$

$$Z^* = e\left(x_s \sum_{i=1}^{n} Y_{v_i}, h_2(W)\right) = e\left(aP, v_2(bP)\right) \tag{16}$$

$$\sigma = e\left(aP + h_1(m, Z, R)\right) R, P) \tag{17}$$

Note that a fresh record in the form of (*t(bP)*, V_2, V_2) would be added into the h_2-table during this query.

- Forgery: Finally, $\mathscr{A}$ forges an SDMVS signature $\delta^* = (R^*, \sigma^*)$ for its selected data m^*.

2) Analysis: It is evident that during the j-th h_2 oracle, $\mathscr{B}$ takes the given parameter cP as the response to $\mathscr{A}$. We claim that as long as $\mathscr{A}$ finally utilizes the parameter to derive an SDMVS associated with m*, the temporal value Z, which is equivalent to *e(b(aP), cP) = e(P, P)*^{abc} would be stored within a record of h_1-table. Consequently, $\mathscr{B}$ could have the non-negligible advantage to break the given BDHP by randomly picking the meta value Z out from the h_1-table.

Theorem 2: In key-compromise attacks in which an adversary has known the signer's private key, the proposed SDMVS scheme still fulfills the property of signer ambiguity.

1) Proof: Assume that an attacker has obtained the knowledge of a signer's private key. Given a strong designated verifier signature that is intercepted during transmission, the attacker will attempt to tell apart the signer identity by verifying if Eq. 4 holds or not. However, in Eq. 4, there is a meta value Z which could be expressed as

$$Z = e\left(x_s \sum_{i=1}^{n} Y_{v_i}, h_2(W)\right) = e\left(x_s \sum_{i=1}^{n} Y_{v_i}, h_2\left(t \sum_{i=1}^{n} Y_{v_i}\right)\right)$$

It is clear that when the secret integer t selected by the signer is unknown, any attacker cannot compute the value Z to test Eq. 4 successfully. Hence, even under the key-compromise attacks, the proposed scheme achieves strong signer ambiguity.

Theorem 3: The construction of our SDMVS scheme achieves the security requirement of non-transferability.

1) Proof: Following the construction of the proposed TS algorithm presented in the previous section, the verifying group has the power to produce another legitimate transcript associated with the signed message. That is to say, the verifying group cannot transfer received signatures to any third party.

B. *Efficiency and Comparison*

To analyze the performance of our SDMVS system, we consider the SDMVS length and the computational costs of every participated party concerning various group sizes. The utilized notations are first stated as follows:

|m|: the bit-length of m;
B: required time to carry out a bilinear map;
PM: required time to carry out a point multiplication in the group G_1;
M: required time to carry out a multiplication in the group G_2;
H: required time to carry out a secure one-way hash function;

The detailed efficiency analyses are demonstrated in Table 1. We can observe that the signature length in our system is a constant size, i.e., |G_1| + |G_2|. A significant characteristic of the proposed scheme is that the computational costs of each participated party remain the same no matter how the group size changes. More precisely, the costs of signer are (2B + 4PM + 2H) while that of each verifier and the clerk are (B + 2PM + H) and (B + PM + H), respectively. Table 2 summarizes the proposed and previous schemes [13, 15, 17].

TABLE 1
PERFORMANCE ANALYSIS OF THE PROPOSED SDMVS SYSTEM VERIFIER

Item/Verifier	$n = 1$	$n = 5$	$n = 10$	$n = 20$
SDMVS Length	|G_1| + |G_2|	|G_1| + |G_2|	|G_1| + |G_2|	|G_1| + |G_2|
Cost of signer U_s	2B + 4PM + 2H	2B + 4PM + 2H	2B + 4PM + 2H	2B + 4PM + 2H
Cost of clerk V_k	B + PM + H	B + PM + H	B + PM + H	B + PM + H
Cost of each verifier U_{vi}	B + 2PM + H	B + 2PM + H	B + 2PM + H	B + 2PM + H

TABLE 2
FUNCTIONALITY COMPARISON AMONG THE PROPOSED AND PREVIOUS SCHEMES

Item/Scheme	[13]	[17]	[15]	Ours
Suitable for Group-Oriented Applications	X	X	√	√
Without Trusted Authority	X	X	X	√
No Key Escrow	X	X	X	√
Support Shard Verification	X	X	X	√
Constant-Size Signature Length	√	√	√	√
Provable Security	X	X	√	√

V. DISCUSSION

In the proposed SDMVS scheme, which integrated the traditional SDVS mechanisms and the multi-signature schemes, the requirement of unforgeability is viewed as crucial security. Therefore, we proved that our system is secure against adaptive chosen message attacks in Theorem 1. As for a variant of SDVS protocols, the other two security properties, i.e., signer ambiguity and non-transferability, are also important. We hence demonstrated that our work satisfies these two characteristics in Theorems 2 and 3, too. In the efficiency and functionality comparison results, we could observe that our scheme has a constant-size signature length.

Additionally, the computational complexity of each party is independent of the group size. Nevertheless, the signer still has to perform two bilinear pairing computations. Since the proposed scheme is not implemented in identity-based systems, our mechanism has no trusted authority and key escrow issues. The other superior properties, such as shared verification, constant-size signature length, and provable security, all make our protocol suitable for privacy-preserving group-oriented electronic commerce applications. In the future, further reduce the computational costs of each party is a potential research direction.

VI. CONCLUSION AND RECOMMENDATIONS

A strong designated multi-verifier signature (SDMVS) mechanism is an important technique in the modern era, which could be applied to privacy-preserving applications in the collaborative system like online auction, copyright protection, etc. The authors presented an efficient SDMVS system employing the intractability of the famous bilinear Diffie-Hellman problem (BDHP) in this literature. Specifically, the computational efforts of each joined entity in our system will not be affected by the size of the verifying group. We also demonstrated that the proposed SDMVS scheme achieves the essential security requirements of strong signer ambiguity, unforgeability, and non-transferability.

Declaration of Conflicting Interests

The authors declare no conflict of interest.

Acknowledgment

This work was supported in part by the Ministry of Science and Technology of the Republic of China under the contract number MOST 109-2221-E-019-052.

REFERENCES

[1] A. Nandanavanam, I. Upasana, and N. Nandanavanam, “NTRU and RSA cryptosystems for data security in IoT environment,” in *International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE),* Bengaluru, India. IEEE, 2020, pp. 371–376.

[2] K. Pavani and P. Sriramya, “Enhancing public key cryptography using RSA, RSA-CRT and N-prime RSA with multiple keys,” in *Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV),* Tirunelveli, India, 2021.

[3] A. H. Alhussain *et al.*, “Using deterministic genetic algorithm to provide secured cryptographic pseudorandom number generators,” *International Journal of Technology and Engineering Studies*, vol. 1, no. 4, pp. 107–116, 2015. doi: https://doi.org/10.20469/ijtes.40001-4

[4] L. Zhong and Z. Dai, “The copyright protection and fair use of commercial data collections based on big data,” in *2nd International Conference on Education, Knowledge and Information Management (ICEKIM),* Xiamen, China, 2021.

[5] L. Liu, W. Shang, W. Lin, and W. Huang, “A decentralized copyright protection, transaction and content distribution system based on blockchain 3.0,” in *21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter),* Ho Chi Minh City, Vietnam. IEEE, 2021, pp. 45–50.

[6] X. Peng, K. Ota, M. Dong, and H. Zhou, “Online resource auction for eavn with non-price attributes,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7127–7137, 2021. doi: https://doi.org/10.1109/TVT.2021.3086179

[7] P. Kale, P. Hazarika, and B. Chandavarkar, “Undeniable signature scheme: A survey,” in *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT),* Kharagpur, India, 2020.

[8] M. Jakobsson, K. Sako, and R. Impagliazzo, “Designated verifier proofs and their applications,” in *International Conference on the Theory and Applications of Cryptographic Techniques,* Berlin Germany, 1996.

[9] S. Saeednia, S. Kremer, and O. Markowitch, “An efficient strong designated verifier signature scheme,” in *International Conference on Information Security and Cryptology,* Berlin, Germany, 2003.

[10] N. Zhang and Q. Wen, “Provably secure blind id-based strong designated verifier signature scheme,” in *Second International Conference on Communications and Networking in China,* Shanghai, China, 2007.

[11] J.-S. Lee and J. H. Chang, “Strong designated verifier signature scheme with message recovery,” in *The 9th International Conference on Advanced Communication Technology,* Gangwon, Korea, 2007.

[12] W. Lei and L. Daxing, “Strong designated verifier

ID-based ring signature scheme," in *International Symposium on Information Science and Engineering,* Shanghai, China, 2008.

[13] L. Zhang, S. He, and S. Liu, "A new identity-based strong designated verifier signature scheme," in *International Conference on Computer Science and Service System (CSSS),* Nanjing, China. IEEE, 2011.

[14] H. Tian, "A new strong multiple designated verifiers signature for broadcast propagation," in *Third International Conference on Intelligent Networking and Collaborative Systems,* Fukuoka, Japan, 2011.

[15] L. Deng, J. Zeng, and H. Huang, "ID-based multisigner universal designated multi-verifier signature based on discrete logarithm," *Chiang Mai Journal of Science*, vol. 45, no. 1, pp. 617–624, 2018.

[16] P. Rastegari, W. Susilo, and M. Dakhilalian, "Certificateless designated verifier signature revisited: Achieving a concrete scheme in the standard model," *International Journal of Information Security*, vol. 18, no. 5, pp. 619–635, 2019. doi: https://doi.org/10.1007/s10207-019-00430-5

[17] M. Beheshti-Atashgah, M. R. Aref, M. Bayat, and M. Barari, "ID-based strong designated verifier signature scheme and its applications in internet of things," in *27th Iranian Conference on Electrical Engineering (ICEE),* Yazd, Iran, 2019.

[18] B. Gong, M. H. Au, and H. Xue, "Constructing strong designated verifier signatures from key encapsulation mechanisms," in *18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)/* Rotorua, New Zealand, 2019.

[19] S. Han, M. Xie, B. Yang, R. Lu, H. Bao, J. Lin, H.-B. Hong, M.-X. Gu, and S. Han, "A certificateless verifiable strong designated verifier signature scheme," *IEEE Access*, vol. 7, pp. 126 391–126 408, 2019. doi: https://doi.org/10.1109/ACCESS.2019.2938898

[20] X. Hu, C. Ma, J. Wang, H. Xu, and W. Tan, "An undeniable strong dsvs scheme with no bilinear pairings," in *9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI),* Datong, China, 2016.

[21] M. Li and T. Fang, "Provably secure and efficient ID-based strong designated verifier signature scheme with message recovery," in *17th International Conference on Network-Based Information Systems,* Salerno, Italy, 2014.

[22] S. Shan, "On the security of a certificateless strong designated verifier signature scheme with non-delegatability," in *International Conference on Internet of Things and Intelligent Applications (ITIA),* Zhenjiang, China, 2020.

[23] M. Ushida, K. Ohta, Y. Kawai, and K. Yoneyama, "Proxiable designated verifier signature," in *International Conference on Security and Cryptography (SECRYPT),* Athens, Greece, 2010.