PLOS ONE

RESEARCH ARTICLE

Efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography

Rui Ma[1], **Linyue Du**[2]*

1 Xingzhi College, Zhejiang Normal University, Jinhua, China, **2** Personnel Department, Zhejiang Normal University, Jinhua, China

* duly@zjnu.edu.cn

OPEN ACCESS

Citation: Ma R, Du L (2024) Efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography. PLoS ONE 19(5): e0300153. https://doi.org/10.1371/journal.pone.0300153

Editor: Hua Wang, Victoria University, AUSTRALIA

Received: November 27, 2023

Accepted: February 22, 2024

Published: May 9, 2024

Data Availability Statement: All relevant data are in the manuscript and its Supporting Information files.

Funding: "Jinhua Public Welfare Technology Application Research Project in 2022" (2022-4-057). The funders play an important role in Conceptualization, Methodology, Formal analysis and Writing—original draft.

Competing interests: The authors have declared that no competing interests exist.

Abstract

In an attribute-based strong designated verifier signature, a signer who satisfies the access structure signs the message and assigns it to a verifier who satisfies the access structure to verify it, which enables fine-grained access control for signers and verifiers. Such signatures are used in scenarios where the identity of the signer needs to be protected, or where the public verifiability of the signature is avoided and only the designated recipient can verify the validity of the signature. To address the problem that the overall overhead of the traditional attribute-based strong designated verifier signature scheme is relatively large, an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography is proposed, as well as a security analysis of the new scheme given in the standard model under the difficulty of the elliptic curve discrete logarithm problem (ECDLP). On the one hand, the proposed scheme is based on elliptic curve cryptography and uses scalar multiplication on elliptic curves, which is computationally lighter, instead of bilinear pairing, which has a higher computational overhead in traditional attribute-based signature schemes. This reduces the computational overhead of signing and verification in the system, improves the efficiency of the system, and makes the scheme more suitable for resource-constrained cloud end-user scenarios. On the other hand, the proposed scheme uses LSSS (Linear Secret Sharing Schemes) access structure with stronger access policy expression, which is more efficient than the "And" gate or access tree access structure, making the computational efficiency of the proposed scheme meet the needs of resource-constrained cloud end-users.

1. Introduction

In the modern information society, digital signature technology has been widely used in various fields, and it is an important tool to ensure data reliability and achieve authentication. Digital signature technology has practical applications in the commercial, financial, and military sectors, especially in e-trade, e-checks, e-shopping, e-publishing, and intellectual property protection.

In traditional standard digital signatures, anyone is able to verify the validity of a signature. However, in many applications where the identity of the signer needs to be protected or the public verifiability of the signature avoided, only the designated recipient of the signature can verify the validity of the signature. For example, in electronic voting, the voter wants to protect the privacy of his or her identity, and only his or her designated verifier can confirm that the signature is valid. But the verifier cannot prove that validity to any third party, and even if the verifier publishes his or her private key, it does not allow the third party to trust that the signature was indeed signed by the voter. To solve this problem, Jakobsson et al. [1] first introduced the concept of Designated Verifier Signature (DVS) in Eurocrypt 1996. However, if a third party intercepts the signature message during message transmission, it can be determined that the recipient did not receive the signed message. It can still be determined that the signature was generated by the signer. Therefore, Saeednia et al. formally proposed the strong designated verifier signature (SDVS) scheme in the literature [2], which requires the participation of the verifier's private key in the verification algorithm to complete the verification, thus ensuring the private nature of the verification. Strong designated verifier signature (SDVS) provides higher security than designated verifier signature (DVS), and at the same time, better protects the privacy of the signer. This traditional strong designated verifier signature (SDVS) is all about a signer generating a signature that is assigned to a verifier for verification. However, in practical application scenarios, multiple signatures that satisfy certain conditions or certain attributes are used, assigned to multiple verifiers who satisfy certain conditions or certain attributes to verify the signature. For example, in electronic bidding, bids are sensitive information and are not expected to be freely disseminated. It is well suited to use a strong designated verifier signature (SDVS) for signing. By designating agents with certain qualifications as validators, these agents can confirm the validity of the bid to the bid evaluation experts and other necessary persons, and the bidder himself can confirm to the agents and other necessary persons that the bid is his. Other than this, no one else can judge the validity of the tender, much less confirm the validity of the tender to third parties.

Attribute-based signature (ABS) has strong anonymity, i.e., the verifier can only know from the signature that the attributes of the signer satisfy the access structure but not the specific information of the signer, which can effectively achieve fine-grained access control. It is of great theoretical and practical importance to study attribute-based strong designated verifier signatures by combining attribute-based signatures with strong designated verifier signatures. Workflow of an attribute-based strong designated verifier signature scheme is shown in Fig 1. There are two forms of ABS: key policy attribute-based signature (KP-ABS) and ciphertext policy attribute-based signature (CP-ABS).

1.1. The research problem

The currently existing attribute-based strong designated verifier signature schemes involves bilinear pairing operations in the construction process. The computational overhead of one bilinear pairing operation is approximately two to three times that of one scalar multiplication operation on the same elliptic curve [3]. Therefore, minimizing the number of calculations of bilinear pairings in the algorithm or cleverly using other operations to achieve the same algorithmic function can improve the efficiency of the attribute-base signature algorithm to some extent. In addition, the access structures of existing attribute-based strong designated verifier signatures are "And" gate or access tree structures, which have many limitations in policy expression and also affect the efficiency of attribute-based strong designated verifier signature schemes.

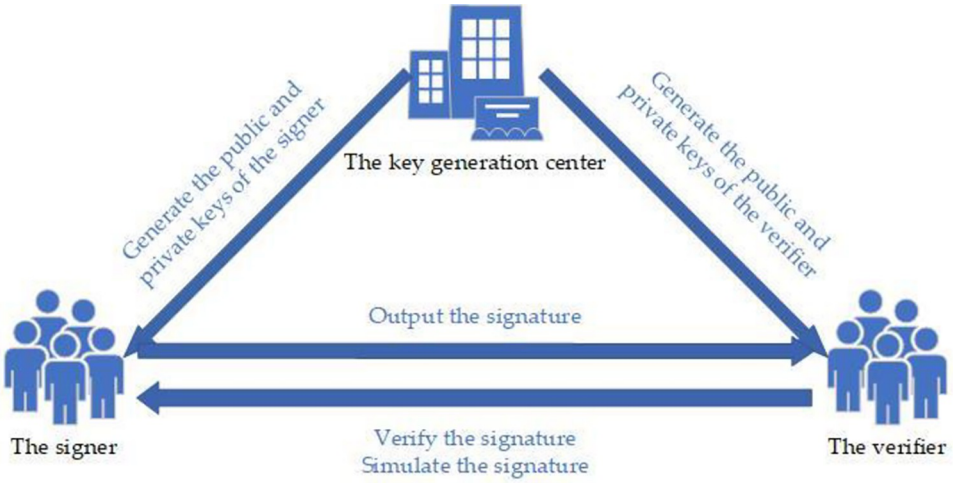

Fig 1. Workflow of an attribute-based strong designated verifier signature scheme.

https://doi.org/10.1371/journal.pone.0300153.g001

This study adopts the access structure of LSSS (Linear Secret Sharing Schemes) with stronger access policy expression. The linear secret sharing schemes are more efficient than the access structures "And" gates or access trees by using the linear secret reconfigurable nature of the secret to reconstruct the secret without recursive operations. Meanwhile, the new scheme is based on the elliptic curve cryptography. The scalar multiplication on elliptic curves, which is computationally lighter, is used instead of the bilinear pairing operation, which is computationally more expensive in traditional attribute-based signature schemes. The computational overhead of signing and verification in the system is reduced and the efficiency of the system is improved. This makes the computational efficiency of the proposed scheme meet the needs of resource-constrained cloud end-users.

1.2. Our contribution

In this paper, we propose an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography, and optimize the security model for an attribute-based strong designated verifier signature scheme. The security of the efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography is analyzed. The advantages of this study are as follows.

1. To reduce the computational overhead of the system, the scheme is based on the elliptic curve cryptography, using the more lightweight scalar multiplication on the elliptic curve instead of the complex bilinear pairing operation, which effectively improves the signature and verification efficiency. The security of the scheme relies on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). To the best of our knowledge, our scheme is the first attribute-based strong designated verifier signature scheme constructed using the elliptic curve cryptography.
2. The traditional "And" gate or tree access structure is less expressive, and too many redundant attributes increase the length of the ciphertext key. In order to reduce the system storage overhead, enrich the expressiveness of the access structure and save the communication overhead, we use the more expressive and computationally efficient LSSS (Linear Secret Sharing Schemes) access structure.

3. The new scheme uses a concatenated summation algorithm in the signature generation process, so that the length of the generated signature is independent of the number of attributes of the signer and does not vary with the number of attributes of the signer.

1.3. Organization

The remainder of this paper is organized as follows. In Section 2, we introduce some related work. In Section 3, we introduce the necessary preliminaries and provide the general form of the attribute-based strong designated verifier signature and its security model. In Section 4, we present an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography. In Section 5, the efficiency of the proposed scheme is analyzed. In Section 6 we summarize the full text.

2. Related work

In privacy-protected cloud computing environments, e-commerce, social networks, e-voting and other web application scenarios, there exists a security requirement that the signer does not want the authenticity of his digital signature to spread arbitrarily among some unauthorized users. In response to this situation, Jakobsson et al. [1] first introduced the concept of designated verifier signatures in 1996 to make the authenticity of signatures more private. In addition, considering the case that a third party can intercept the signature before it reaches the designated verifier, a strong designated verifier signature system with stronger security is proposed in the appendix of [1]. In a strong designated verifier signature scheme, the verifier must use his or her own private key to perform the verification algorithm. In this way, even if the designated verifier signature is intercepted in advance, the third party still has no signature verification capability. In 2003, Saeednia, Kremer and Markowitch [2] gave a formal definition of strong designated verifier signature and gave the first scheme for strong designated verifier signature. This scheme [2] used the Schnorr [4] signature scheme and Zheng [5] signature encryption scheme to propose a strong designated verifier signature scheme, which achieves signer identity privacy by avoiding the use of encryption algorithms and further improves the efficiency of signing and verification. A secure and flexible access control scheme and protocol for M-services based on role based access control (RBAC) [6] in the same year. In 2004, Laguillaumie et al. [7] provided the first formal description of the concept of designated verifier signatures and a formal definition of the signer identity privacy property in strong designated verifier signatures. They also improved the designated verifier signature scheme proposed by Steinfeld et al. [8] at Asiacrypt'03 using bilinear pairs and proposed a new signature scheme that possesses lower computational consumption and proved that the scheme can guarantee the privacy of the signer's identity. Susilo et al. studied strong designated verifier signatures in the context of identity-based cryptosystems and proposed a strong designated verifier signature scheme for IBC [9], which integrates identity-based cryptosystem with strong designated verifier signature to solve the public key certificate management problem. In 2006, a usage control model to protect services and devices in ubiquitous computing environments [10], which allows the access restrictions directly on services and object documents was presented. In 2008, Zhang et al. [11] applied identity cryptography to propose a novel strong designated verifier signature scheme and proved its security to be close to the Bilinear Diffie-Hellman (BDH) hard problem under the random oracle model. Huang et al. [12] proposed a short strong designated verifier signature scheme and one of its identity-based morphing schemes, also noting that this signature is shorter than the signature lengths of all existing schemes, and finally discussing the short strong designated verifier signature under the standard model. In

2009, Kang et al. [13] demonstrated authorization attacks on some existing identity-based strong designated verifiers and proposed new signature schemes that can withstand authorization attacks. A model for privacy preserving access control which is based on variety of purposes [14] was presented in the same year. Yang et al. [15] similarly proposed a certificate-free strong designated verifier signature regime at the International Conference on Intelligence and Security in that year. In 2011, Huang et al. [16] proposed two efficient strong designated verifier signature schemes, the first one is a strong designated verifier signature scheme under the standard model and the second one is a non-authorized strong designated verifier signature scheme, and suggested that the non-authorized designated verifier signature under the standard model is still a difficult problem. Islam et al. [17] constructed provably secure certificate-free strong designated verifier signature regime using elliptic curve bilinear pairs in 2013. In 2014, Wang et al. proposed a strong designated verifier signature scheme that is recognizable by the signer [18]. In [18], if permission is offered, the signatory can acknowledge that the signature is his own. In 2015, Jiang et al. proposed an identity-based online and offline designated verifier signature scheme [19]. In 2015, Zhang proposed a strong designated verifier signature scheme that resists replay attacks [20]. In 2017, Masoumeh et al. [21] proposed a strong designated verifier signature scheme. Ge et al. [22] proposed two SDVS schemes that guarantee the privacy of the signer. In 2019, Han et al. [23] proposed certificateless SDVS, which satisfies the requirements of verifiability, non-authorizability, non-transmissibility, and signer ambiguity. In 2020, Zhang et al. [24] proposed secure and efficient quantum DVS scheme, which is theoretically secure and a distributed memetic algorithm (DMA) is proposed for enhancing database privacy and utility [25]. In 2022, Venkateswaran et al. proposed the use of a neuro Deep learning wireless intrusion detection system that distinguishes the attacks in MANETs [26]. Dharmaraj et al. proposed a feature selection and majority voting based solutions for detecting intrusions [27]. In the same year, a novel three-layer DDE framework with adaptive resource allocation (DDE-ARA) [28] was proposed and a multitasking database fragmentation problem for privacy preservation requirements [29] is formally defined. During the same period, Yin et al. [30] proposed a modality-aware graph convolutional network (MAGCN) module to embed multimodality entity attributes and topological graph connectivity features into a unified lower dimensional feature space to boost link prediction performance. In 2023, Ravinder et al. [31] proposed a proactive approach based on natural language processing and deep learning that can enable online platforms to actively look for the signs of antisocial behaviour and intervene before it gets out of control. Ge et al. proposed a distributed prediction-randomness framework for the evolutionary dynamic multiobjective partitioning optimization of databases [32] and a distributed cooperative coevolutionary genetic algorithm (DCCGA) to optimize the MODP problem [33].

In 2008, Maji [34] et al. first proposed the attribute-based signature (ABS) scheme based on the IBS scheme. The access structure consists of a threshold structure consisting of "And" and "Or" and finally proves its security under a general group model. In 2010 Li et al. [35] et al. proposed three schemes, the first one is an ABS scheme with threshold predicates, the second one is an ABS scheme without random oracle machines, and the third one is an ABS scheme with multi-attribute authorities. In 2011, Maji et al. [36] presented a general framework for constructing attribute-based signatures and gave several concrete examples using bilinear pairs. In 2012, Sun et al. [37] proposed a threshold attribute-based signature scheme without trusted central attribute authority that is not only unforgeable under selective attribute and adaptive selective plaintext attacks, but is also resistant to conspiracy attacks. In 2013, Ma et al. [38] designed a secure and provable threshold-based attribute signature scheme. 2014, Tang et al. [39] constructed an ABS scheme with limited circuit depth using a mathematical tool of multilinear mapping, further enriching the predicate expression capability. In 2015, Nandi et al.

[40] constructed an ABS scheme supporting multiple access methods with control methods including Boolean formulas and conventional languages. In 2016, Sakai et al. [41] proposed an ABS scheme supporting arbitrary circuit depth with good expressiveness via bilinear pairs. In 2017, for application to electronic medical record systems and to reduce the computational overhead, Moro et al. [42] proposed an ABS scheme that can support a tree access structure. Su et al. [43] proposed an attribute-based signature scheme with attribute revocation to protect the privacy of the user's identity. Lu et al. [44] propose an efficient traceable constant-size attribute-based ring signature scheme for electronic health record system, focusing on fine-grained authentication and traceability of file publishers. Ma et al. [45] present an attribute-based blind signature scheme based on elliptic curve cryptography (ECC), and the security of new scheme is proved under the difficulty of the elliptic curve discrete logarithm problem (ECDLP). The access structure of the scheme uses the LSSS matrix. In the same year, an efficient pairing-free attribute-based blind signature scheme based on ordered binary decision diagram [46] is proposed.

Currently, the following works are available on attribute-based strong designated verifier signature. In 2009 and 2012, Shao et al. [47] and Fan et al. [48] proposed attribute-based strong designated verifier signature schemes, respectively, but these two schemes have multiple bilinear pairing operations in the signature and verification process, which makes the overall efficiency of the schemes inefficient. The attribute-based designated verifier signature scheme proposed by Tang et al. [49] in 2014 and the deniable attribute-based designated confirmer signature scheme proposed by Ren et al. [50] in the same year are not true attribute signatures because the secret value y_1 is incorrectly given to the signer in the public-private key extraction algorithm. Based on the paper [50], in 2016, Yan Ren [51] proposed a deniable attribute-based designated confirmer signature scheme under no random prediction model. In 2020 Zhang et al. [52] used a key strategy and then proposed an attribute-based designation confirmer signature scheme with a monotonic Boolean circuit for the access structure using multilinear mapping. The access structure of both schemes is a "And" gate or access tree structure, which involves bilinear pairing operations in the signature and verification process, making the overall system inefficient.

Most existing attribute-based strong designated verifier signature schemes involve complex bilinear pairing operations in the construction process, which are considered to be the most computationally expensive operations in pairing-based cryptographic protocols [53]. This makes these solutions overall inefficient and difficult to apply to cloud terminal scenarios or resource-constrained devices. Therefore, minimizing the number of calculations of bilinear pairings in the algorithm or cleverly using other operations to achieve the same algorithmic function can improve the algorithmic efficiency of the attribute-based strong designated verifier signature scheme to some extent. The design of the access structure is also a fairly important part of the construction of an attribute-based strong designated verifier signature scheme. A better access structure not only improves the efficiency of the system and the expressiveness of the access policy, but also reduces the number of attributes that need to be embedded in the signature to shorten the signature length and reduce the communication and storage overhead.

3. Preliminaries

In this section, we introduce linear secret sharing schemes (LSSS), elliptic curve cryptography, and the necessary security assumption. In addition, the definition and security model of the attribute-based strong designated verifier signature algorithm are provided.

3.1. Linear secret sharing schemes

Definition 1 (Access Structure) [54]. Suppose that the set of n participants is $\{P_1,P_2,\cdots,P_n\}$, and $P = 2^{\{P_1,P_2,\ldots,P_n\}}$. If the set A is a non-empty subset of the set $\{P_1,P_2,\cdots,P_n\}$, then it satisfies $A\subseteq P\backslash\{\Phi\}$. If $\forall B,C$, satisfying $B\in A$ and $B\subseteq C$, has $C\in A$, then A is said to be a monotonic access structure.

Definition 2 (Linear Secret Sharing Schemes Access Structure). Let $\{P_1,P_2,\cdots,P_n\}$ be the set of a series of participants, let M_T be the matrix of $s\times t$, and $\rho:\{1,2,\cdots,s\}\rightarrow P$ be the mapping of each row of the matrix to one of the participants in the set. According to the definition of a linear secret sharing scheme [54], linear secret sharing schemes access structure is defined as the following two algorithms.

1.*Distribute*(M_T,ρ,α). The input matrix M_T with row s and column t, the mapping function ρ and the secret value $\alpha\in Z_p^*$, randomly selected $\alpha_2,\ldots,\alpha_t\in Z_p^*$, forms the vector $v=(\alpha,\alpha_2,\cdots,\alpha_t)$, and then output the s shared values $\{\lambda_i = M_{T_i}\cdot v\}_{i\in[1,s]}$ of attribute $\rho(i)$, where M_{T_i} is the i-th row vector of matrix M_T.

2.*Reconstruct*(M_T,ρ,W). The input matrix M_T with row s and column t, the mapping function ρ and the set of authorized attributes $W\in P$. According to the Gaussian elimination method, the set of reconstruction constants $\{w_i\}_{i\in I}$ can be found in polynomial time, satisfying $\sum_{i\in I} M_{T_i}w_i = (1,0,\ldots,0)$, i.e., $\sum_{i\in I}\lambda_i w_i = \alpha$. Then output $\{w_i\}_{i\in I}$, where $I=\{i\in[1,s]:\rho(i)\in W\}$.

3.2. ECDLP

In the mid-1980s, Koblitz [55] and Miller [56] respectively proposed the elliptic curve cryptography (ECC), whose security relies on the intractability of the discrete logarithm problem (ECDLP) on the elliptic curve group. The elliptic curve discrete logarithm problem can be described as follows:

Let F_p denote a finite field and E be an elliptic curve over F_p. The point G as the base point of this elliptic curve $E(F_P)$, n is the order of G. A point $Q\in E(F_P)$, The elliptic curve discrete logarithm problem (ECDLP) is the search for an integer $l\in[0,n-1]$ such that $Q = lG$. For any algorithm $\mathcal{B}$, the probability of solving the ECDLP is defined as follows,

$$Adv^{ECDLP}(\mathcal{B}) = \Pr[\mathcal{B}(G,lG) = l,\ l\in[0,n]]$$

Definition 3. The elliptic curve discrete logarithm problem (ECDLP) is said to be a hard problem if the probability of any algorithm $\mathcal{B}$ solving the ECDLP is negligible.

3.3. A generic definitions of an attribute-based strong designated verifier signature scheme

An attribute-based strong designated verifier signature scheme generally includes the following five algorithms.

3.3.1. Setup.

$$Setup(k) \longrightarrow \{P_{pub}, MSK, params\}$$

A probabilistic algorithm has as input a security parameter k, outputs a system master key MSK and a master public key P_{pub}, and a system public parameter $params$.

3.3.2. Extract.

$$Extract(params, MSK, T_A, T_B) \longrightarrow \{SK_A, PK_A, SK_B, PK_B\}$$

A probabilistic algorithm with input system parameters $params$, master key MSK,access

structure T_A, and output private key SK_A and public key PK_A of the signer. Similarly, input system parameters *params*, master key *MSK*, access structure T_B, and output private key SK_B and public key PK_B of the signer.

3.3.3. Sign.

$$Sign(M, params, SK_A, PK_A, PK_B)\overrightarrow{\sigma}$$

A probabilistic algorithm with input system parameters *params*, private key SK_A and public key PK_A of the signer, public key PK_B of the verifier, message M, output the signature σ of message M.

3.3.4. Verify.

$$Verify(params, PK_A, PK_B, M, \sigma) \longrightarrow \{1, 0\}$$

A deterministic algorithm with input system parameters *params*, the public key PK_A of the signer, the private key SK_B of the verifier, the message M and its signature σ, and output whether the signature verification passes or not. If the signature σ is valid, output 1, otherwise output 0.

3.3.5. Simulate.

$$Simulate(M, \sigma, PK_A, SK_B, params)\overrightarrow{\sigma'}$$

A deterministic algorithm that takes as input the message M and its signature σ, the public key PK_A of the signer, the private key SK_B of the designated verifier and other public parameters *params*, and outputs a simulated signature σ' of the message M.

3.4. A security model of an attribute-based strong designated verifier signature scheme

A secure attribute-based strong designated verifier signature scheme needs to satisfy correctness, signer identity anonymity, unforgeability, and privacy non-transmissibility.

3.4.1. Correctness. An attribute-based strong designated verifier signature scheme

$$\pi = (Setup, Extract, Sign, Verify, Simulate)$$

assuming that the set W_A of attributes owned by the signer satisfies the access structure T_A, the signer outputs the designated verifier signature $\sigma = Sign(M,params,SK_A,PK_A,PK_B)$ for message M. Assuming that the set W_B of attributes owned by the designated verifier satisfies the access structure T_B, the designated verifier signature σ generated by the signer must be verified by the verifier, there must be

$$Verify(params, PK_A, PK_B, M, \sigma) = 1$$

3.4.2. Signer identity anonymity. An attribute-based strong designated verifier signature scheme

$$\pi = Setup, Extract, Sign, Verify, Simulate)$$

signer identity anonymity without access to the private key of the signer or the designated verifier can be defined as a series of games between adversary and challenger as follows.

1. *Init*: Adversary $\mathcal{A}$ selects the attribute set W_A^* and the set W_B^* of attributes owned by the designated verifier to be challenged, and sends them to challenger $\mathcal{C}$.

2. *Setup*: Challenger $\mathcal{C}$ chooses security parameters k, computes $(params,MSK)\leftarrow Setup(k)$, and sends public parameters *params* to adversary $\mathcal{A}$.
3. *Queries*: Adversary $\mathcal{A}$ is allowed to perform polynomial subadaptive queries.
   - Key extraction queries. Adversary $\mathcal{A}$ sends the LSSS access structure T_A and T_B to challenger $\mathcal{C}$, if $T_A(W_A^*) \neq 1$ and $T_B(W_B^*) \neq 1$, challenger $\mathcal{C}$ runs algorithm *Extract* and returns to adversary $\mathcal{A}$ the public-private key (PK_A,SK_A) of the signer and the public-private key (PK_B,SK_B) of the verifier.
   - Signature queries. Adversary $\mathcal{A}$ sends the attribute set W_A, the message M, and the attribute set of the verifier W_B to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ invokes the *Sign* algorithm to generate signature σ, which is sent to adversary $\mathcal{A}$.
   - Verify queries. Adversary $\mathcal{A}$ sends message M and signature σ to challenger $\mathcal{C}$, requesting challenger $\mathcal{C}$ to verify that signature σ is signed by a signer with attribute W_A and designated verifier attribute W_B. If σ is a signature generated by a legitimate signer with attribute set W_A, then challenger $\mathcal{C}$ returns "1", if not, then returns "0".
4. *Challenge*: Adversary $\mathcal{A}$ submits two plaintexts of equal length M_0 and M_1,to challenger $\mathcal{C}$, the attribute set W_A of the signer and the attribute set W_B of the verifier. Challenger $\mathcal{C}$ performs a random coin flip, set to $b\in\{0,1\}$, and generates a strong designated verifier signature $\sigma_b = Sign(W_A^*, W_B^*, M_b)$, which is sent to adversary $\mathcal{A}$.
5. *Guess*: Adversary $\mathcal{A}$ outputs a guess b' for b. Before giving the guess, adversary $\mathcal{A}$ can make signature queries to challenger $\mathcal{C}$ other than M_0 and M_1 and verify queries other than σ_b. If $b' = b$, output "1", otherwise, output "0".

We define $Adv^{anony}(1^\lambda)$ to be the advantage over 1/2 of $\mathcal{A}$ in the above game.

Definition 4 (Signer identity anonymity). An attribute-based strong designated verifier signature scheme satisfies signer identity anonymity under a choice message attack if there exists no adversary $\mathcal{A}$ can win the above game with non-negligible advantage $Adv^{anony}(1^\lambda)$.

3.4.3. Unforgeability. An attribute-based strong designated verifier signature scheme

$$\pi = (Setup, Extract, Sign, Verify, Simulate)$$

it is computationally infeasible to construct a legitimate attribute-based strong designated verifier signature scheme without obtaining the signer's or designated verifier's private key. Unforgeability under selective attribute set and selective messages attack can be defined as the following game in polynomial time between adversary $\mathcal{A}$ and challenger $\mathcal{C}$.

1. *Init*: Adversary $\mathcal{A}$ selects the attribute set W_A^* and the set W_B^* of attributes owned by the designated verifier to be challenged, and sends them to challenger $\mathcal{C}$.
2. *Setup*: Challenger $\mathcal{C}$ chooses security parameters k, computes $(params,MSK)\leftarrow Setup(k)$, and sends public parameters *params* to adversary $\mathcal{A}$.
3. *Queries*: Adversary $\mathcal{A}$ is allowed to perform polynomial subadaptive queries.
   - Key extraction queries. Adversary $\mathcal{A}$ sends the LSSS access structure T_A and T_B to challenger $\mathcal{C}$, if $T_A(W_A^*) \neq 1$ and $T_B(W_B^*) \neq 1$, challenger $\mathcal{C}$ runs algorithm *Extract* and returns to adversary $\mathcal{A}$ the public-private key (PK_A,SK_A) of the signer and the public-private key (PK_B,SK_B) of the verifier.

- Signature queries. Adversary $\mathcal{A}$ sends the attribute set W_A, the message M, and the attribute set of the verifier W_B to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ invokes the *Sign* algorithm to generate signature σ, which is sent to adversary $\mathcal{A}$.
- Verify queries. Adversary $\mathcal{A}$ sends message M and signature σ to challenger $\mathcal{C}$, requesting challenger $\mathcal{C}$ to verify that signature σ is signed by a signer with attribute W_A and designated verifier attribute W_B. If σ is a signature generated by a legitimate signer with attribute set W_A, then challenger $\mathcal{C}$ returns "1", if not, then returns "0".

4. *Forgery*: Adversary $\mathcal{A}$ outputs the signature σ*of message M^* with the corresponding signer's attribute set $W_A{}^*$, the corresponding verifier's attribute set $W_B{}^*$, and the following three conditions are satisfied

$$Verify(params, W_A{}^*, M^*, \sigma^*, SK_B) = 1. \quad (1)$$

Adversary $\mathcal{A}$ did not conduct a signature queries $(M^*, W_A{}^*, W_B{}^*)$.

The access structures T_A and T_B for conducting either query, both satisfy $T_A(W_A{}^*) \neq 1$ and $T_B(W_B{}^*) \neq 1$.

Definition 5 (Unforgeability). An attribute-based strong designated verifier signature scheme is unforgeable under the selective attributes and selective messages attacks when the probability that adversary $\mathcal{A}$ can successfully win the above game in polynomial time is negligible.

3.4.4. Privacy non-transmissibility. An attribute-based strong designated verifier signature scheme

$$\pi = (Setup, Extract, Sign, Verify, Simulate)$$

satisfies privacy non-transmissibility means that given a message M and a strong designated verifier signature σ, the probability that a third party can determine in polynomial time whether the signature σ was generated by the signer or the verifier is negligible. Privacy non-transmissibility can be defined as the following game in polynomial time between adversary $\mathcal{A}$ and challenger $\mathcal{C}$.

1. *Init*: Adversary $\mathcal{A}$ selects the attribute set $W_A{}^*$ and the set $W_B{}^*$ of attributes owned by the designated verifier to be challenged, and sends them to challenger $\mathcal{C}$.
2. *Setup*: Challenger $\mathcal{C}$ chooses security parameters k, computes (*params*,*MSK*)←*Setup*(k), and sends public parameters *params* to adversary $\mathcal{A}$.
3. *Queries*: Adversary $\mathcal{A}$ is allowed to perform polynomial subadaptive queries.

- Key extraction queries. Adversary $\mathcal{A}$ sends the LSSS access structure T_A and T_B to challenger $\mathcal{C}$, if $T_A(W_A{}^*) \neq 1$ and $T_B(W_B{}^*) \neq 1$, challenger $\mathcal{C}$ runs algorithm *Extract* and returns to adversary $\mathcal{A}$ the public-private key (PK_A,SK_A) of the signer and the public-private key (PK_B,SK_B) of the verifier.
- Signature queries. Adversary $\mathcal{A}$ sends the attribute set W_A, the message M, and the attribute set of the verifier W_B to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ invokes the *Sign* algorithm to generate signature σ, which is sent to adversary $\mathcal{A}$.
- Verify queries. Adversary $\mathcal{A}$ sends message M and signature σ to challenger $\mathcal{C}$, requesting challenger $\mathcal{C}$ to verify that signature σ is signed by a signer with attribute W_A and designated verifier attribute W_B. If σ is a signature generated by a legitimate signer with attribute set W_A, then challenger $\mathcal{C}$ returns "1", if not, then returns "0".

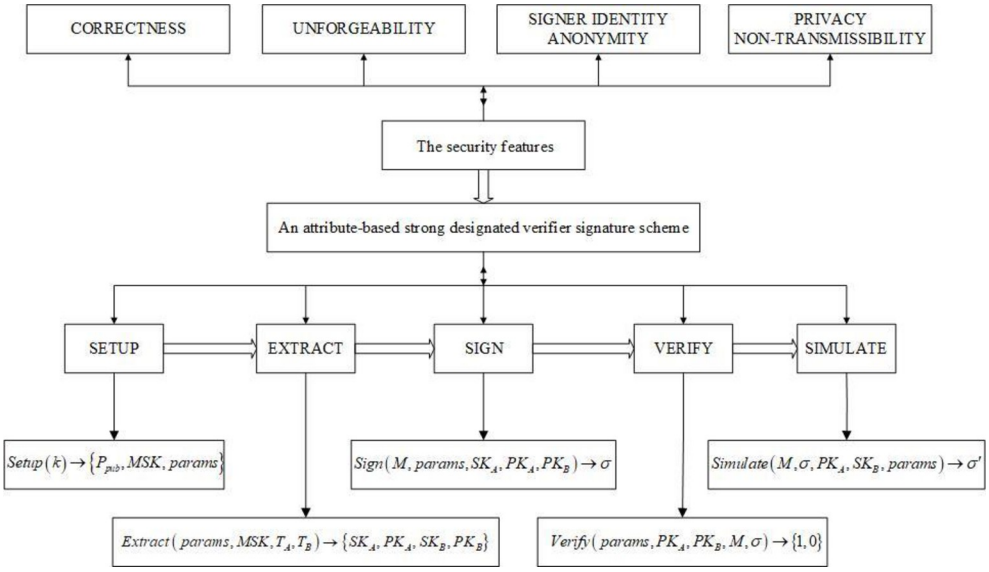

Fig 2. System model of an attribute-based strong designated verifier signature scheme.

https://doi.org/10.1371/journal.pone.0300153.g002

4. *Challenge*: Challenger $\mathcal{C}$ runs *Simulate* algorithm and generates a signature σ', which is sent to challenger $\mathcal{A}$. The signature verification equation still holds. If adversary $\mathcal{A}$ can distinguish between the signature σ generated by the signer and signature σ' generated by the challenger $\mathcal{C}$ in polynomial time, then adversary $\mathcal{A}$ wins.

Definition 6 (Privacy non-transmissibility). An attribute-based strong designated verifier signature scheme satisfies privacy non-transmissibility when the probability that adversary $\mathcal{A}$ can successfully win the above game in polynomial time is negligible.

System model of an attribute-based strong designated verifier signature scheme is shown in Fig 2.

4. An efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography

Most of the existing attribute-based strong designated verifier signature schemes involve complex bilinear pairing operations and the "And" gate or access tree access structure used in the scheme construction has many limitations in policy expression, which makes the signing and verification process computationally inefficient. To address this issue, an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography is proposed and its security is analyzed in this section.

4.1. Our construction

In this section we propose an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography including the following five algorithms.

4.1.1. Setup. The finite field $GF(p)$ of order p is chosen, E is an elliptic curve defined on $GF(p)$, and the system chooses the point G as the base point of this elliptic curve. Assume that the set of attributes in the system is $U = \{1,2,\cdots,n\}$ and i is one of the attributes. $H : \{0,1\}^* \longrightarrow Z_p^*$ is a cryptographically secure hash function. Randomly select $\alpha \in Z_p^*$ and compute $P_{pub} = \alpha G$. For each attribute $i \in U$, randomly select the secret value $z_i \in Z_p^*$ and compute $h_i = z_i G$.

Output public parameters $params = \{p,G,H,h_1,h_2,\cdots,h_n,P_{pub}\}$. The master key is $MSK = \{\alpha, z_1,z_2,\cdots,Z_n\}$.

4.1.2. Extract. Assume that the access structure T_A of the signer is (L_A,ρ_A), L_A is a matrix of rows and columns S_A and t_A. The function ρ_A is a mapping of rows to attributes about L_A. Each row L_{A_j} of L_A corresponds to an attribute ρ_{A_j}.

The key generation center randomly selects $r_{A_2}, r_{A_3}, \ldots, r_{A_t} \in Z_p^*$, constructs the vector $\overrightarrow{v}_A = (\alpha, r_{A_2}, r_{A_3}, \ldots, r_{A_t})$, calculates the secret value $\lambda_{A_i} = \overrightarrow{L}_{A_i} \cdot \overrightarrow{v}_A$ for each row $i \in [1,S_A]$ of the LSSS matrix L_A, and then calculates $d_{A_i} = \lambda_{A_i} + z_{\rho_A(i)}$.

Output the private key of the signer as $SK_A = \{d_{A_i}\}_{i\in[1,s_A]}$. Compute $D_{A_i} = d_{A_i}G$ and the public key of the signer as $PK_A = \{D_{A_i}\}_{i\in[1,s_A]}$.

Assume that the access structure T_B of the verifier is (L_B,ρ_B), L_B is a matrix of rows and columns S_B and t_B. The function ρ_B is a mapping of rows to attributes about L_B. Each row L_{B_j} of L_B corresponds to an attribute ρ_{B_j}.

The key generation center randomly selects $r_{B_2}, r_{B_3}, \ldots, r_{B_t} \in Z_p^*$, constructs the vector $\overrightarrow{v}_B = (\alpha, r_{B_2}, r_{B_3}, \ldots, r_{B_{t_B}})$, calculates the secret value $\lambda_{B_i} = \overrightarrow{L}_{B_i} \cdot \overrightarrow{v}_B$ for each row $i \in [1,S_B]$ of the LSSS matrix L_B, and then calculates $d_{B_i} = \lambda_{B_i} + z_{\rho_B(i)}$.

Output the private key of the signer as $SK_B = \{d_{B_i}\}_{i\in[1,s_B]}$. Compute $D_{A_i} = d_{B_i}G$ and the public key of the signer as $PK_B = \{D_{B_i}\}_{i\in[1,s_B]}$.

4.1.3. Sign. If the attribute set W_A of the signer satisfies the access structure T_A, it must be possible to find a set of constant $\{\omega_{A_i} \in Z_p^*, i \in \varpi_A\}$ in polynomial time such that $\sum_{i\in\varpi_A} \omega_{A_i} L_{A_i} = (1,0,\ldots,0)$, where $\varpi_A = \{i \in [1,s_A] : \rho_A(i) \in W_A\}$.

The signer signs the message as follows.

Randomly select $e \in Z_p^*$ and compute $R = eM$, $r = H(R)$. Randomly select $k_1 \in Z_p^*$ and compute $s = k_1 - r\sum_{i\in\varpi_A} d_{A_i}\omega_{A_i}$.

If the attribute set W_B of the verifier satisfies the access structure T_B, it must be possible to find a set of constant $\{\omega_{B_i} \in Z_p^*, i \in \varpi_B\}$ in polynomial time such that $\sum_{i\in\varpi_B} \omega_{B_i} L_{B_i} = (1,0,\ldots,0)$, where $\varpi_B = \{i \in [1,s_B] : \rho_B(i) \in W_B\}$.

The signer picks $k_2 \in Z_p^*$ randomly and computes $V = k_2 \cdot \sum_{i\in\varpi_B} D_{B_i}$ and $Z = k_1 \sum_{i\in\varpi_B} D_{B_i} + k_2 G$.

The signer sends the signature $\sigma = (R,s,V,Z)$ to the verifier.

4.1.4. Verify. After the verifier receives the signature σ, calculate $r = H(R)$.

Verify that the equation $Z = \sum_{i\in\varpi_B} d_{B_i}[sG + r(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i})] + (\sum_{i\in\varpi_B} d_{B_i})^{-1} V$ Whether it holds. If it holds, accept the signature, if not, reject it.

4.1.5. Simulate. The verifier randomly selects $k \in Z_p^*$ and computes $Z = k\sum_{i\in\varpi_B} D_{B_i}$.

The verifier computes $r = H(R)$, $s = k$, $V = -r(\sum_{i\in\varpi_B} d_{B_i})^2 (P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i})$, generating a simulated signature $\sigma' = (R,s,V,Z)$ such that the verification equation

$$Z = \sum_{i\in\varpi_B} d_{B_i}[sG + r(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i})] + (\sum_{i\in\varpi_B} d_{B_i})^{-1} V \quad (2)$$

also holds.

4.2. Security analysis

In this section we analyze the security of an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography. The security features mainly include correctness, signer identity anonymity, unforgeability, and privacy non-transmissibility.

4.2.1. Correctness. The efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography proposed by us satisfies the correctness.

Proof: When the attribute set W_A of the signer satisfies the access structure T_A, the same set of reconstruction constants $\{\omega_{A_i} \in Z_p^*, i \in \varpi_A\}$ as the signer can be found, where $\varpi_A = \{i \in [1, s_A] : \rho_A(i) \in W_A\}$. According to the properties of the LSSS matrix, $\sum_{i\in\varpi_A} \lambda_{A_i}\omega_{A_i} = \alpha$ and the system parameters *params*, the correctness of the signature σ is verified as follows.

$$Z = k_1 \sum_{i\in\varpi_B} D_{B_i} + k_2 G$$

$$= k_1 \sum_{i\in\varpi_B} d_{B_i} G + k_2 G$$

$$= \left(s + r\sum_{i\in\varpi_A} d_{A_i}\omega_{A_i}\right)\sum_{i\in\varpi_B} d_{B_i} G + k_2 G$$

$$= s\sum_{i\in\varpi_B} d_{B_i} G + r\sum_{i\in\varpi_A} d_{A_i}\omega_{A_i}\sum_{i\in\varpi_B} d_{B_i} G + k_2 G$$

$$= \sum_{i\in\varpi_B} d_{B_i}\left(sG + r\sum_{i\in\varpi_A} d_{A_i}\omega_{A_i} G\right) + k_2 G$$

$$= \sum_{i\in\varpi_B} d_{B_i}\left[sG + r\sum_{i\in\varpi_A}\left(\lambda_{A_i} + z_{\rho_A(i)}\right)\omega_{A_i} G\right] + k_2 G$$

$$= \sum_{i\in\varpi_B} d_{B_i}\left[sG + r\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)\right] + \left(\sum_{i\in\varpi_B} d_{B_i}\right)^{-1} V$$

4.2.2. Signer identity anonymity. If the probability that an adversary $\mathcal{A}$ can distinguish a legitimate attribute-based strong designated verifier signature in polynomial time without obtaining a signer or designated verifier private key is no greater than 1/2, the efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography proposed by us satisfies the signer identity anonymity.

Proof: The game between adversary $\mathcal{A}$ and challenger $\mathcal{C}$ is as follows.

1. *Init*. Adversary $\mathcal{A}$ selects the attribute set W_A^* of the signer and the attribute set W_B^* owned by the designated verifier to be challenged, and sends them to challenger $\mathcal{C}$.
2. *Setup*. challenger $\mathcal{C}$ selects a security parameter k and simulates the generation of public parameters as follows.

Randomly selects $x \in Z_p^*$, calculate $P_{pub} = xG$. For each attribute $i \in U$, randomly select the secret value $z_i \in Z_p^*$ and compute $h_i = z_i G$. Let $H : \{0,1\}^* \longrightarrow Z_p^*$ be a secure cryptographic hash function. Challenger $\mathcal{C}$ generates the public parameter $params = \{p, G, H, h_1, h_2, \cdots, h_n, P_{pub}\}$ and the master key $MSK = \{x, z_1, z_2, \cdots, z_n\}$ to adversary $\mathcal{A}$.

3. *Queries*. Adversary $\mathcal{A}$ can perform polynomial times of key extraction queries, signature queries, and verify queries to challenger $\mathcal{C}$.

- Key extraction queries. Adversary $\mathcal{A}$ sends the access structure T_A satisfying $T_A(W_A^*) \neq 1$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ randomly selects $r_{A_1}, r_{A_2}, \ldots, r_{A_t} \in Z_p^*$, constructs vector $\overrightarrow{v}_A = (x, r_{A_2}, r_{A_3}, \ldots, r_{A_t})$, computes $\lambda_{A_i} = \overrightarrow{L}_{A_i} \cdot \overrightarrow{v}_A$ for each row $i \in [1, S_A]$ of the LSSS matrix L_A, and then computes the private key of the signer as $d_{A_i} = \lambda_{A_i} + z_{\rho_A(i)}$ and the public key of the signer as $PK_A = \{D_{A_i}\}_{i \in [1, s_A]}$.

Adversary $\mathcal{A}$ sends the access structure T_B satisfying $T_B(W_B^*) \neq 1$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ randomly selects $r_{B_1}, r_{B_2}, \ldots, r_{B_t} \in Z_p^*$ and constructs the vector $\overrightarrow{v}_B = (x, r_{B_2}, r_{B_3}, \ldots, r_{B_t})$. For each row $i \in [1, S_B]$ of the LSSS matrix L_A, compute $\lambda_{B_i} = \overrightarrow{L}_{B_i} \cdot \overrightarrow{v}_B$. Compute the private key of the verifier as $d_{B_i} = \lambda_{B_i} + z_{\rho_B(i)}$ and the public key of the verifier as $PK_B = \{D_{B_i}\}_{i \in [1, s_B]}$.

- Signature queries. Adversary $\mathcal{A}$ sends the attribute set W_A of the signer, message M, and verifier attribute set W_B of the verifier to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ signs message M according to the signature step.

If the attribute set W_A satisfies the access structure T_A, then one can obtain a set of constants $\{\omega_{A_i} \in Z_p^*, i \in \varpi_A\}$ such that $\sum_{i \in \varpi_A} \omega_{A_i} L_{A_i} = (1, 0, \ldots, 0)$, where $\varpi_A = \{i \in [1, s_A] : \rho_A(i) \in W_A\}$. Randomly select $e \in Z_p^*$ and calculate $R = eM$, $r = H(R)$, randomly select $k_1 \in Z_p^*$ and calculate $s = k_1 - r \sum_{i \in \varpi_A} d_{A_i} \omega_{A_i}$.

If the attribute set W_B of the verifier satisfies the access structure T_B, then a set of constants $\{\omega_{B_i} \in Z_p^*, i \in \varpi_B\}$ can be found in polynomial time such that $\sum_{i \in \varpi_B} \omega_{B_i} L_{B_i} = (1, 0, \ldots, 0)$, where $\varpi_B = \{i \in [1, s_B] : \rho_B(i) \in W_B\}$.

Challenger $\mathcal{C}$ picks $k_2 \in Z_p^*$ randomly and computes $V = k_2 \sum_{i \in \varpi_B} D_{B_i}$ and $Z = k_1 \sum_{i \in \varpi_B} D_{B_i} + k_2 G$.

Challenger $\mathcal{C}$ sends the signature $\sigma = (R, s, V, Z)$ to adversary $\mathcal{A}$.

- Verify queries. Adversary $\mathcal{A}$ sends signature $\sigma = (R, s, V, Z)$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ verifies the signature according to the verification algorithm as follows.

Challenger $\mathcal{C}$ computes $r = H(R)$ and verifies that equation

$$Z = \sum_{i \in \varpi_B} d_{B_i} [sG + r(P_{pub} + \sum_{i \in \varpi_A} h_{A_i} \omega_{A_i})] + (\sum_{i \in \varpi_B} d_{B_i})^{-1} V. \tag{3}$$

If it holds, then challenger $\mathcal{C}$ returns "1" to adversary $\mathcal{A}$. Otherwise, it returns "0".

4. *Challenge*.Adversary $\mathcal{A}$ submits to challenger $\mathcal{C}$ two plaintexts of equal length M_0 and M_1, the attribute set W_A of the signer and the attribute set W_B of the designated verifier.

Challenger $\mathcal{C}$ performs a random coin flip, set to $b\in\{0,1\}$. Invoke signature algorithm *Sign*, randomly select $e \in Z_p^*$, compute $R = eM_b$ and $r = H(R)$. Randomly select $k_1 \in Z_p^*$, compute $s = k_1 - r\sum_{i\in\varpi_A} d_{A_i}\omega_{A_i}$. Randomly select $k_2 \in Z_p^*$, compute $V = k_2\sum_{i\in\varpi_B} D_{B_i}$ and $Z = k_1\sum_{i\in\varpi_B} D_{B_i} + k_2 G$.

Generate the designated verifier signature $\sigma_b = Sign(W_A, W_B, M_b) = (R,s,V,Z)$ to send to adversary $\mathcal{A}$.

5. *Output*. Adversary $\mathcal{A}$ outputs a guess b' for b. Before giving the guess, adversary $\mathcal{A}$ can make signature queries other than M_0 and M_1 and verify queries other than σ_b to challenger $\mathcal{C}$.

In order to obtain the value of M_b, e must be derived from $R = eM_b$. Since e is randomly selected, the probability that adversary $\mathcal{A}$ determines the true value of M_b in polynomial time does not exceed 1/2. Therefore, the proposed scheme satisfies signer identity anonymity.

4.2.3. Unforgeability. If there exists a polynomial-time adversary $\mathcal{A}$ that can crack the proposed attribute-based strong designated verifier signature scheme based on elliptic curve cryptography with a non-negligible advantage ε, then challenger $\mathcal{C}$ can solve the problem of the elliptic curve discrete logarithm problem (ECDLP) with a non-negligible probability.

Proof: The finite field $GF(p)$ of order p is chosen, E is an elliptic curve defined on $GF(p)$, and the system chooses the point G as the base point of this elliptic curve.

1. Init. Adversary $\mathcal{A}$ selects the attribute set W_A^* of the signer and the attribute set W_B^* owned by the designated verifier to be challenged, and sends them to challenger $\mathcal{C}$.

2. Setup. challenger $\mathcal{C}$ selects a security parameter k and simulates the generation of public parameters as follows.

Randomly selects $x \in Z_p^*$, calculate $P_{pub} = xG$. For each attribute $i\in U$, randomly select the secret value $z_i \in Z_p^*$ and compute $h_i = z_iG$. Let $H : \{0,1\}^* \longrightarrow Z_p^*$ be a secure cryptographic hash function. Challenger $\mathcal{C}$ generates the public parameter $params = \{p,G,H,h_1,h_2,\cdots,h_n,P_{pub}\}$ and the master key $MSK = \{x_1,z_1,z_2,\cdots z_n\}$ to adversary $\mathcal{A}$.

3. Queries. Adversary $\mathcal{A}$ can perform polynomial times of key extraction queries, signature queries, and verify queries to challenger $\mathcal{C}$.

- Key extraction queries. Adversary $\mathcal{A}$ sends the access structure T_A satisfying $T_A(W_A^*) \neq 1$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ randomly selects $r_{A_1}, r_{A_2}, \ldots, r_{A_t} \in Z_p^*$, constructs vector $\overrightarrow{v}_A = (x, r_{A_2}, r_{A_3}, \ldots, r_{A_t})$, computes $\lambda_{A_i} = \overrightarrow{L}_{A_i}\cdot\overrightarrow{v}_A$ for each row $i\in[1,S_A]$ of the LSSS matrix L_A, and then computes the private key of the signer as $d_{A_i} = \lambda_{A_i} + z_{\rho_A(i)}$ and the public key of the signer as $PK_A = \{D_{A_i}\}_{i\in[1,s_A]}$.

Adversary $\mathcal{A}$ sends the access structure T_B satisfying $T_B(W_B^*) \neq 1$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ randomly selects $r_{B_1}, r_{B_2}, \ldots, r_{B_t} \in Z_p^*$ and constructs the vector $\overrightarrow{v}_B = (x, r_{B_2}, r_{B_3}, \ldots, r_{B_t})$. For each row $i\in[1,S_B]$ of the LSSS matrix L_A, compute $\lambda_{B_i} = \overrightarrow{L}_{B_i}\cdot\overrightarrow{v}_B$. Compute the private key of the verifier as $d_{B_i} = \lambda_{B_i} + z_{\rho_B(i)}$ and the public key of the verifier as $PK_B = \{D_{B_i}\}_{i\in[1,s_B]}$.

- Signature queries. Adversary $\mathcal{A}$ sends the attribute set W_A of the signer, message M, and verifier attribute set W_B of the verifier to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ signs message M according to the signature step.

If the attribute set W_A satisfies the access structure T_A, then one can obtain a set of constants $\{\omega_{A_i} \in Z_p^*, i \in \varpi_A\}$ such that $\sum_{i\in\varpi_A} \omega_{A_i} L_{A_i} = (1, 0, \ldots, 0)$, where $\varpi_A = \{i \in [1, s_A] : \rho_A(i) \in W_A\}$. Randomly select $e \in Z_p^*$ and calculate $R = eM$, $r = H(R)$, randomly select $k_1 \in Z_p^*$ and calculate $s = k_1 - r\sum_{i\in\varpi_A} d_{A_i}\omega_{A_i}$.

If the attribute set W_B of the verifier satisfies the access structure T_B, then a set of constants $\{\omega_{B_i} \in Z_p^*, i \in \varpi_B\}$ can be found in polynomial time such that $\sum_{i\in\varpi_B} \omega_{B_i} L_{B_i} = (1, 0, \ldots, 0)$, where $\varpi_B = \{i \in [1, s_B] : \rho_B(i) \in W_B\}$.

Challenger $\mathcal{C}$ picks $k_2 \in Z_p^*$ randomly and computes $V = k_2\sum_{i\in\varpi_B} D_{B_i}$ and $Z = k_1\sum_{i\in\varpi_B} D_{B_i} + k_2 G$.

Challenger $\mathcal{C}$ sends the signature $\sigma = (R,s,V,Z)$ to adversary $\mathcal{A}$.

- Verify queries. Adversary $\mathcal{A}$ sends signature $\sigma = (R,s,V,Z)$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ verifies the signature according to the verification algorithm as follows.

  Challenger $\mathcal{C}$ computes $r = H(R)$ and verifies that equation

$$Z = \sum_{i\in\varpi_B} d_{B_i}[sG + r(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i})] + (\sum_{i\in\varpi_B} d_{B_i})^{-1} V. \tag{4}$$

  If it holds, then challenger $\mathcal{C}$ returns "1" to adversary $\mathcal{A}$. Otherwise, it returns "0".

4. *Forgery*. Adversary $\mathcal{A}$ forges the signature σ^* of message M^*, corresponding to the attribute set of the signer as W_A^*, and specifies the attribute set of the verifier as W_B^* to send to challenger $\mathcal{C}$.

Challenger $\mathcal{C}$ first finds the reconstructed constant sets $\{\omega_{A_i} \in Z_p^*, i \in \varpi_A\}$ and $\{\omega_{B_i} \in Z_p^*, i \in \varpi_B\}$ based on the attribute sets W_A^* and W_B^* provided by adversary $\mathcal{A}$. The constant sets satisfy the reconstruction of $\sum_{i\in\varpi_A} \omega_{A_i} L_{A_i} = (1, 0, \ldots, 0)$ and $\sum_{i\in\varpi_B} \omega_{B_i} L_{B_i} = (1, 0, \ldots, 0)$.

Then replaying with the same parameters and choosing a different hash function $H_1(\cdot)$, challenger $\mathcal{C}$ obtains another legal signature $\sigma^{*\prime}$ for M^* according to the forking lemma. Thus both σ^* and $\sigma^{*\prime}$ satisfy the verification equation, then there are the following equations

$$Z = \sum_{i\in\varpi_{B_i}} d_{B_i}\left[s^*G + r^*\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)\right] + \left(\sum_{i\in\varpi_B} d_{B_i}\right)^{-1} V \tag{5}$$

$$Z = \sum_{i\in\varpi_{B_i}} d_{B_i}\left[s^{*\prime}G + r^{*\prime}\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)\right] + \left(\sum_{i\in\varpi_B} d_{B_i}\right)^{-1} V \tag{6}$$

Subtract the two formulas to get:

$$0 = \sum_{i\in\varpi_B} d_{B_i}\left[(s^* - s^{*\prime})G + \left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)(r^* - r^{*\prime})\right]$$

$$(s^* - s^{*\prime})G + (r^* - r^{*\prime})P_{pub} + (r^* - r^{*\prime})\sum_{i\in\varpi_A} h_{A_i}\omega_{A_i} = 0(r^{*\prime} - r^*)P_{pub}$$
$$= (s^* - s^{*\prime})G + (r^* - r^{*\prime})\sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}$$

$$(r^{*\prime} - r^*)xG = (s^* - s^{*\prime})G + (r^* - r^{*\prime})\sum_{i\in\varpi_A} z_i G\omega_{A_i}$$

Since challenger $\mathcal{C}$ knows the process of signature generation and verification, it can calculate $x = [(s^* - s^{*\prime}) + (r^* - r^{*\prime})\sum_{i\in\varpi_A} z_i\omega_{A_i}](r^{*\prime} - r^*)^{-1}$.

Thus challenger $\mathcal{C}$ outputs x as a solution to the discrete logarithm problem, that is, if adversary $\mathcal{A}$ can successfully forge the attribute-based strongly designated verifier signature equal to cracking the elliptic curve discrete logarithm problem (ECDLP). Due to the fact that the elliptic curve discrete logarithm problem is a challenge based on the elliptic curve public key cryptosystem, no adversary $\mathcal{A}$ wins this game by a non-negligible advantage in polynomial time. The scheme satisfies unforgeability.

4.2.4. Privacy non-transmissibility. Our efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography satisfies privacy non-transmissibility.

Proof: The game between adversary $\mathcal{A}$ and challenger $\mathcal{C}$ is as follows.

1. *Init*. Adversary $\mathcal{A}$ selects the attribute set $W_A{}^*$ of the signer and the attribute set $W_B{}^*$ owned by the designated verifier to be challenged, and sends them to challenger $\mathcal{C}$.
2. *Setup*. challenger $\mathcal{C}$ selects a security parameter k and simulates the generation of public parameters as follows.
   Randomly selects $x \in Z_p{}^*$, calculate $P_{pub} = xG$. For each attribute $i\in U$, randomly select the secret value $z_i \in Z_p{}^*$ and compute $h_i = Z_iG$. Let $H : \{0,1\}^* \longrightarrow Z_p{}^*$ be a secure cryptographic hash function. Challenger $\mathcal{C}$ generates the public parameter $params = \{p,G,H,h_1,h_2, \cdots h_n,P_{pub}\}$ and the master key $MSK = \{x,z_1,z_2,\cdots,z_n\}$ to adversary $\mathcal{A}$.
3. *Queries*. Adversary $\mathcal{A}$ can perform polynomial times of key extraction queries, signature queries, and verify queries to challenger $\mathcal{C}$.
   - Key extraction queries. Adversary $\mathcal{A}$ sends the access structure T_A satisfying $T_A(W_A{}^*) \neq 1$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ randomly selects $r_{A_1}, r_{A_2}, \ldots, r_{A_t} \in Z_p{}^*$, constructs vector $\overrightarrow{v}_A = (x, r_{A_2}, r_{A_3}, \ldots, r_{A_t})$, computes $\lambda_{A_i} = \overrightarrow{L}_{A_i} \cdot \overrightarrow{\mathrm{v}}_{\mathrm{A}}$ for each row $i\in[1,S_A]$ of the LSSS matrix L_A, and then computes the private key of the signer as $d_{A_i} = \lambda_{A_i} + z_{\rho_A(i)}$ and the public key of the signer as $PK_A = \{D_{A_i}\}_{i\in[1,s_A]}$.

Adversary $\mathcal{A}$ sends the access structure T_B satisfying $T_B(W_B{}^*) \neq 1$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ randomly selects $r_{B_1}, r_{B_2}, \ldots, r_{B_t} \in Z_p{}^*$ and constructs the vector $\overrightarrow{v}_B = (x, r_{B_2}, r_{B_3}, \ldots, r_{B_t})$. For each row $i\in[1,S_B]$ of the LSSS matrix L_A, compute $\lambda_{B_i} = \overrightarrow{L}_{B_i} \cdot \overrightarrow{\mathrm{v}}_{\mathrm{B}}$. Compute the private key of the verifier as $d_{B_i} = \lambda_{B_i} + z_{\rho_B(i)}$ and the public key of the verifier as $PK_B = \{D_{B_i}\}_{i\in[1,s_B]}$.

- Signature queries. Adversary $\mathcal{A}$ sends the attribute set W_A of the signer, message M, and verifier attribute set W_B of the verifier to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ signs message M according to the signature step.

If the attribute set W_A satisfies the access structure T_A, then one can obtain a set of constants $\{\omega_{A_i} \in Z_p^*, i \in \varpi_A\}$ such that $\sum_{i\in\varpi_A} \omega_{A_i} L_{A_i} = (1, 0, \ldots, 0)$, where $\varpi_A = \{i \in [1, s_A] : \rho_A(i) \in W_A\}$. Randomly select $e \in Z_p^*$ and calculate $R = eM$, $r = H(R)$, randomly select $k_1 \in Z_p^*$ and calculate $s = k_1 - r\sum_{i\in\varpi_A} d_{A_i}\omega_{A_i}$.

If the attribute set W_B of the verifier satisfies the access structure T_B, then a set of constants $\{\omega_{B_i} \in Z_p^*, i \in \varpi_B\}$ can be found in polynomial time such that $\sum_{i\in\varpi_B} \omega_{B_i} L_{B_i} = (1, 0, \ldots, 0)$, where $\varpi_B = \{i \in [1, s_B] : \rho_B(i) \in W_B\}$.

Challenger $\mathcal{C}$ picks $k_2 \in z_p^*$ randomly and computes $V = k_2\sum_{i\in\varpi_B} D_{B_i}$ and $Z = k_1\sum_{i\in\varpi_B} D_{B_i} + k_2 G$.

Challenger $\mathcal{C}$ sends the signature $\sigma = (R,s,V,Z)$ to adversary $\mathcal{A}$.

- Verify queries. Adversary $\mathcal{A}$ sends signature $\sigma = (R,s,V,Z)$ to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ verifies the signature according to the verification algorithm as follows.

Challenger $\mathcal{C}$ computes $r = H(R)$ and verifies that equation

$$Z = \sum_{i\in\varpi_B} d_{B_i}\left[sG + r\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)\right] + \left(\sum_{i\in\varpi_B} d_{B_i}\right)^{-1} V. \tag{7}$$

If it holds, then challenger $\mathcal{C}$ returns "1" to adversary $\mathcal{A}$. Otherwise, it returns "0".

4. *Challenge*. For any message $M' \in \{0,1\}^*$, challenger $\mathcal{C}$ randomly selects $k \in Z_p^*$, computes $Z = k\sum_{i\in\varpi_B} D_{B_i}$, and compute

$$r = H(R),\ s = k,\ V = -r\left(\sum_{i\in\varpi_B} d_{B_i}\right)^2\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right), \tag{8}$$

to generate the simulated signature $\sigma' = (R,s,V,Z)$.

$$\sum_{i\in\varpi_B} d_{B_i}\left[sG + r\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)\right] + \left(\sum_{i\in\varpi_B} d_{B_i}\right)^{-1} V$$

$$= s\left(\sum_{i\in\varpi_B} d_{B_i} G\right) + r\sum_{i\in\varpi_B} d_{B_i}\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right) - \left(\sum_{i\in\varpi_B} d_{B_i}\right)^{-1}\left[r\left(\sum_{i\in\varpi_B} d_{B_i}\right)^2\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)\right]$$

$$= s\left(\sum_{i\in\varpi_B} d_{B_i} G\right) + r\sum_{i\in\varpi_B} d_{B_i}\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right) - r\sum_{i\in\varpi_B} d_{B_i}\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)$$

$$= s\left(\sum_{i\in\varpi_B} d_{B_i} G\right)$$

$$= k\sum_{i\in\varpi_B} D_{B_i}$$

$$= Z$$

This signature also enables the verification equation

$$Z = \sum_{i\in\varpi_B} d_{B_i}\left[sG + r\left(P_{pub} + \sum_{i\in\varpi_A} h_{A_i}\omega_{A_i}\right)\right] + \left(\sum_{i\in\varpi_B} d_{B_i}\right)^{-1} V \text{ to hold.}$$

The signature σ' simulated by challenger $\mathcal{C}$ is indistinguishable from the signature σ generated by the signer. The probability that adversary $\mathcal{A}$ can determine in polynomial time whether signature σ was generated by the signer or challenger $\mathcal{C}$ is negligible.

5. Efficiency analysis

This section analyses the efficiency of an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography. Table 1 compares our scheme with several other typical attribute-based strong designated verifier signature schemes in terms of access structure, access policy, private key and signature size, signature computation and verification efficiency. Here we have selected four typical attribute-based strong designated verifier signature schemes *SABSDVS* [47], *FABSDVS* [48], *ZABDCS* [52] and *TABSDVS* [49].

In Table 1, the meaning of each symbol is as follows: w denotes the number of attributes, n is the overall number of attributes, s denotes the number of attributes of the visitor, $|G|$ denotes the length of the group G element, T_{exp} denotes the time of modulo power operation, T_{bp} denotes the time required for bilinear pairwise operation, q_1 is the number of monotonic Boolean circuits or gates, and q_2 is the number of monotonic Boolean circuits and gates. See S1 File.

We analyze the efficiency of the above schemes in terms of the access structure, the number of operations, and the length of the secret key and signature. The algorithm execution time consumption is mainly distributed in exponential (T_{exp}) and bilinear pairing (T_{bp}) operations, so the table mainly analyzes these two operations.

As can be seen in Table 1, the scheme has no bilinear pairing operations for both signature and verification calculations compared to other comparison schemes. One bilinear pairing

Table 1. Comparision of schemes.

Scheme	Access structure	Access policy	Private key sizes (|G|)	Signature sizes (|G|)	Signature computation (T_{exp})	Verification computation (T_{bp})
SABSDVS	Threshold access structure	*SP*	w	1	3	2
FABSDVS	Access tree	*SP*	$3w$	$2w$	5	5
ZABDCS	Monotonic boolean circuit	*KP*	$w+2q_1+3q_2+1$	$w+1$	$n+2$	2
TABSDVS	Lagrangian interpolation method	*SP*	w	4	2	4
Our scheme	LSSS matrix	*KP*	w	4	0	0

https://doi.org/10.1371/journal.pone.0300153.t001

operation on the same curve is 2–3 times more than the scalar multiplication [3]. Therefore, it is more efficient to use scalar multiplication on elliptic curves instead of bilinear pairing operations to construct attribute-based strong designated verifier signature schemes in the signing and verification process. In addition, most of the access structures relied on by the existing attribute-based strong designated verifier signature schemes are threshold access structures or access tree structures, which have many limitations in policy expression. The LSSS matrix is stronger in access policy expression and can express any access policy, including "And" gate, "Or" gate and threshold, with flexible access structure [57]. The new scheme uses the LSSS access structure to construct an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography, which is more efficient in both signature generation and verification. It is more efficient than the existing attribute-based strongly designated verifier signature schemes. Also, the signature generation process uses concatenated summation operations to make the signature length fixed. Of course, the limitations of the breadth of the literature search may have led to omissions in the comparison scheme, and we will try to improve this in future research work.

6. Conclusions

It is a hot research topic in the field of cryptography to improve the efficiency and security of attribute-based strongly designated verifier signature schemes as much as possible. Most of the existing attribute-based strong designated verifier signature schemes involve complex bilinear pairing operations, which makes the overall scheme inefficient. To address this problem, in this paper, an efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography is proposed and analyzed for its security. In Section 3, we present some background knowledge and optimize the security model of an attribute-based strong designated verifier signature scheme to facilitate better understanding of the newly proposed scheme. In Section 4, we give our construction of a new efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography. The security of the proposed scheme is analyzed under the difficulty of the elliptic curve discrete logarithm problem (ECDLP) on which the elliptic curve cryptography is based. The new scheme uses scalar multiplication on elliptic curves, which is more lightweight, instead of bilinear pairing operations, which have a higher computational overhead [58, 59]. This reduces the computational overhead in the signature and verification process, making the scheme more suitable for cloud endpoint scenarios and resource-constrained devices. The new scheme replaces the bilinear pairing operation with scalar multiplication on elliptic curves providing a new idea for the study of attribute-based strong designated verifier signature schemes. Meanwhile, our scheme uses LSSS matrix to represent the access structure. LSSS takes advantage of the linear secret sharing scheme's secret reconfigurable nature to reconstruct the secret without recursive operations, improves the signature and efficiency of attribute-based signature schemes, and makes the policy expression more flexible. Compared with several attribute-based strong designated verifier signature schemes in Section 5, the new scheme designed in this paper not only improves the efficiency of access policy expression, but also achieves the signature length independent of the number of signer attributes. The new scheme has greater advantages in terms of computational efficiency and storage space.

Supporting information

S1 File.
(DOCX)

Author Contributions

Conceptualization: Rui Ma, Linyue Du.

Formal analysis: Rui Ma.

Funding acquisition: Rui Ma.

Methodology: Rui Ma.

Writing – original draft: Rui Ma.

Writing – review & editing: Linyue Du.

References

1. Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications. Lecture Notes in Computer Science. 1996; 1070: 142–154.
2. Saeednia S, Kremer S, Markowitch O. An efficient strong designated verifier signature scheme," Lecture Notes in Computer Science. 2004; 2971: 40–54.
3. Ding S, Li C, Li H. A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT. IEEE Access. 2018; 6: 27336–27345.
4. Schnor C. Efficient signature generation by smart cards. Journal of Cryptology. 1991; 4: 161–174.
5. Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+ cost (encryption). Advances in Cryptology, Crypto'97, Lecture Notes in Computer Science. 1997; 1294: 165–179.
6. Wang H, Zhang Y, Cao J, Varadharajan V. Achieving secure and flexible M-services through tickets. IEEE transactions on systems, man, and cybernetics. Part A, Systems and humans. 2003; 33(6): 697–708. https://doi.org/10.1109/TSMCA.2003.819917
7. Laguillaumie F, Vergnaud D. Designated verifiers signature: anonymity and efficient construction from any bilinear map. Security in Communication Network. 2004; 3352: 107–121.
8. Steinfeld R, Bull L, Wang H. Universal designated verifier signatures. Advances in Cryptology-ASIACRYPT. 2003; 2894: 523–542.
9. Susilo W, Zheng F, Mu Y. Identity-based strong designated verifier signature schemes. Lecture Notes in Computer Science.2004; 3108: 313–324, 2004.
10. Wang H, Zhang Y, Cao J. Ubiquitous computing environments and its usage access control. Proceedings of the 1st International Conference on Scalable Information Systems, INFOSCALE 2006, ACM Press, Hong Kong (2006). https://doi.org/10.1145/1146847.1146853
11. Zhang J, Mao J. A novel ID-based designated verifier signature scheme. Information Sciences. 2008; 178(3): 766–773,.
12. Huang X, Susilo W, Mu Y. Short designated verifier signature scheme and its identity-based variant. International Journal of Network Security. 2008; 6(1): 82–93.
13. Kang B, Boyd C, Dawson E. Identity-based strong designated verifier signature schemes: attacks and new construction. Computers & Electrical Engineering. 2009; 35: 49–53.
14. Kabir ME, Wang H. Conditional Purpose Based Access Control Model for Privacy Protection. Twentieth Australasian Database Conference (ADC 2009).2009;137–144.
15. Yang B, Hu Z, Xiao Z. Efficient certificateless strong designated verifier signature scheme. International Conference on Computational Intelligence and Security. 2009; 432–436. https://doi.org/10.1109/CIS.2009.191
16. Huang Q, Yang G, Wong DS. Efficient strong designated verifier signature schemes without random oracle or with non delegatability. International Journal of Information Security. 2011; 10(6):373–385.
17. Islam SKH, Biswas GP. Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings. Journal of King Saud University Computer and Information Sciences. 2013; 25:51–61. https://doi.org/10.1016/j.jksuci.2012.06.003
18. Wang H. Signer-admissible strong designated verifier signature from bilinear pairings. Security Comm Networks. 2014; 7: 422–428.
19. Jiang Y. Identity based on-line/off-line signature with designated verifier. Intellgigent Autoimation and Soft Computing. 2015; 21: 433–443.

20. Zhang YL. Strong designated verifier signature scheme resisting replay attack. Information Technology and Control.2015; 44: 165–171.
21. Masoumeh KS, Mahmoud AA, Mahmoud RZ. Provably secure strong designated verifier signature scheme based on coding theory. International Journal of Communication Systems. 2017; 30(7): 1–12.
22. Ge LX. Research on strong designated verifier signature. Ph.D. dissertation, Dept. Comp. Eng., Xihua University, Sichuan, China, 2017.
23. Han S, Xie M, Yang BL. A Certificateless verifiable strong designated verifier signature scheme. IEEE Access. 2019; 7: 126391–126408.
24. Zhang Y, Xin XJ, Li F. Secure and efficient quantum designated verifier signature scheme. Modern Physics Letters A. 2020; 35(18): 1–15.
25. Ge YF, Yu WJ, Cao J, Wang H, Zhan ZH, Zhang Y, et al. Distributed Memetic Algorithm for Outsourced Database Fragmentation. IEEE Transactions on Cybernetics. 2020; 51: 4808–4821.
26. Venkateswaran N, Prabaharan S. An efficient neuro deep learning intrusion detection system for mobile Adhoc networks. (2022) EAI Endorsed Transactions on Scalable Information Systems. 22 (6), art. no. e7. https://doi.org/10.4108/eai.4-4-2022.173781
27. Dharmaraj RP, Tareek MP. Majority Voting and Feature Selection Based Network Intrusion Detection System. EAI Endorsed Transactions on Scalable Information Systems. Volume 9, Issue 6, 2022. https://doi.org/10.4108/eai.4-4-2022.173780
28. Li JY, Du KJ, Zhan ZH, Wang H, Zhang J. Distributed differential evolution with adaptive resource allocation. IEEE Transactions on Cybernetics. 2022; 53: 2791–2804.
29. Ge YF, Orlowska M, Cao J, Wang H, Zhang Y. MDDE: multitasking distributed differential evolution for privacy-preserving database fragmentation. VLDB journal: The international journal of very large data bases. 2022; 31: 957–975 (2022).
30. Yin J, Tang M, Cao J, You M, Wang H, Alazab M. Knowledge-Driven Cybersecurity Intelligence: Software Vulnerability Coexploitation Behavior Discovery. IEEE Transactions on Industrial Informatics. 2023; 19: 5593–5601.
31. Singh R, Subramani S, Du J, Zhang Y, Wang H, Miao Y, et al. Antisocial Behavior Identification from Twitter Feeds Using Traditional Machine Learning Algorithms and Deep Learning. EAI Endorsed Transactions on Scalable Information Systems. 2023; 10(4):1–17. https://doi.org/10.4108/eetsis.v10i3.3184
32. Ge Y. -F et al., "Evolutionary Dynamic Database Partitioning Optimization for Privacy and Utility," in IEEE Transactions on Dependable and Secure Computing, https://doi.org/10.1109/TDSC.2023.3302284
33. Ge YF, Bertino E, Wang H, Cao J, Zhang Y. Distributed Cooperative Coevolution of Data Publishing Privacy and Transparency. ACM Transactions on Knowledge Discovery from Data. 2023; 18: 1–23.
34. Maji H, Prabhakaran M, Prosulek M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance. 2008. [Online]. Available: https://eprint.iacr.org/2008/328.pdf.
35. Li J, Au MH, Susilo W. Attribute-based signature and its applications. Computer and Communications Security.2010; pp. 60–69.
36. Maji H. K, Prabjalaram M, Posulek M. Attribute based signatures. Lecture Notes in Computer Science. 2011; 6558: 376–392.
37. Sun C, Ma W. Secure attribute-based threshold signature without a trusted central authority. Journal of Computers. 2012; 7: 2899–2905.
38. Ma CG, Shi L, Zhou CL. Research on attribute-based threshold signature scheme and its security. Electronic Journal. 2013; 41: 1012–1015.
39. Tang F, Li H, Liang B. Attribute-based signatures for circuits from multilinear maps. Lecture Notes in Computer Science. 2014; 8783: 54–71.
40. Nandi M, Pandit T. On the power of pair encodings: Frameworks for predicate cryptographic primitives. 2015; [Online]. Available: https://eprint.iacr.org/2015/955.pdf.
41. Sakai Y, Attrapadung N, Hanaoka G. Attribute-based signatures for circuits from bilinear map. Lecture Notes in Computer Science. 2016; 9614: 283–300.
42. Mo R, Ma JF, Liu XM. An attribute-based purgeable signature scheme supporting tree access structure. Electronic Journal. 2017; 45:2715–2720.
43. Su Q, Zhang R, Xue R, Li P. Revocable attribute-based signature for blockchain-based healthcare system. IEEE Access. 2020; 8: 127884–127896.
44. Lu A, Li W, Yao Y, Yu N. TCABRS: An efficient traceable constant-size attribute-based ring signature scheme for electronic health record system. 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). 2021; pp. 106–113.

45. Ma R, Du LY. Attribute-based blind signature scheme based on elliptic curve cryptography. IEEE Access. 2022; 10:34221–34227.

46. Ma R, Du LY. Efficient pairing-free attribute-based blind signature scheme based on ordered binary decision diagram. IEEE Access. 2022; 10: 114393–114401.

47. Shao J. Research on strong designated verifier signature based on attributes. Ph.D. dissertation, Dept. Comp. Eng., Shanghai Jiaotong University, Shanghai, China, 2010.

48. Fan CI, Wu CN, Chen WK. Attribute-based strong designated verifier signature scheme. Journal of Systems and Software. 2012, 85: 944–959.

49. Tang CM, Ren Y. Attribute-based designated verifier signature scheme. Journal of Guangzhou University. 2014; 13: 13–16.

50. Ren Y., Tang CM. Deniable attribute-based designated confirmer signature scheme. Computer Application Research. 2014; 31:213–216.

51. Ren Y. Deniable attribute-based designated confirmer signature scheme without random oracles. Computer Science. 2016; 43:162–165.

52. Zhang J. Research on specifying verifier signature based on attributes. Ph.D. dissertation, Dept. Comp. Eng., Minnan Normal University, Zhangzhou, China, 2020.

53. Chen X, Susilo W, Li J. Efficient algorithms for secure outsourcing of bilinear pairings. Theoretical Computer Science. 2015; 562: 112–121.

54. Beimel A. Secure schemes for secret sharing and key distribution. Ph.D. dissertation, Israel Institute of Technology Technion, Haifa, Israel, 1996.

55. Koblitz N. Elliptic curve cryptographys. Mathematics of Compution. 1987; 48: 203–209.

56. Miller V. Use of elliptic curves in cryptography. Lecture Notes in Computer Science. 1986; 218: 417–426.

57. Chen DW, Tang B. LSSS-based hidden policy attribute-based encryption scheme. Computer Technology and Development. 2018; 28:119–124.

58. Barreto PS, Libert B, Mccullagh N. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. International Conference on the Theory and Application of Cryptology and Information Security. 2005; 3788: 515–532.

59. Ding S. Research on data security and efficient sharing control mechanism in the Internet of Things. Ph. D. dissertation, Xidian University. Xi'an, China, 2019.