Efficient Identity-Based Universal Designated Verifier Signature Proof Systems

Yifan Yang , Xiaotong Zhou , Binting Su * , Wei Wu

Posted Date: 20 January 2025

doi: 10.20944/preprints202501.1409.v1

Keywords: UDVSP; ID-based SM2 digital signature; non-interactive proof; credential management

Article

Efficient Identity-Based Universal Designated Verifier Signature Proof Systems

Yifan Yang [1], Xiaotong Zhou [2], Binting Su [3,*] and Wei Wu [4]

[1] College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
[2] School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
[3] Network and Data Center, Fujian Normal University, Fuzhou 350117, China
[4] College of Education Sciences, Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511455, China
* Correspondence: bintingsu@fjnu.edu.cn

Abstract: The implementation of Universal Designated Verifier Signatures Proofs (UDVSP) enhances data privacy and security in various digital communication systems. However, practical applications of UDVSP face challenges such as high computational overhead, onerous certificate management, and complex public key initialization. These issues hinder the adoption of UDVSP in daily life. To improve the efficacy of existing UDVSP, Lin et al. in IEEE TSC'23 designed a bilinear pairing-free UDVSP system but their proposal still involves cumbersome certificate management, and inherent interactive operations that can sometimes significantly degrade system efficiency. In this paper, we first utilize the identity-based (ID-based) SM2 digital signature scheme to construct an ID-based UDVSP system which sidesteps the cumbersome certificate management issue. To further remove the interactive requirement, we also employ the OR-proof and Fiat-Shamir technologies to design the other ID-based UDVSP system. Our designs not only own the same bilinear pairing-free advantage as Lin et al.'s proposal, but also achieve the certificate-free or non-interactive goal. Security proofs and performance analysis confirm the viability and efficiency of the systems we have put forward.

Keywords: UDVSP; ID-based SM2 digital signature; non-interactive proof; credential management

1. Introduction

In modern society, with the widespread application of digital signatures, protecting the privacy of signers has become a major concern for researchers. To address this issue, Universal Designated Verifier Signatures (UDVS) was proposed by Steinfeld et al. in Asiacrypt 2003 [1]. UDVS ensures that the designated verifier has the capacity to verify the digital signature, while preventing him/her from conveying the reliability of the signature to anyone else. This characteristic makes it suitable for scenarios where only a few specifically designated verifiers are required for signature verification. As an illustration, within the realm of e-government, government departments can utilize UDVS to provide proof of confidential information to relevant staff members as required for their work. However, these staff members are unable to convince third parties of the authenticity of this confidential information. This is important for preventing the malicious dissemination of confidential information. There are numerous such application scenarios, including electronic voting systems, electronic medical records, and electronic income certificates.

Although innovative, Steinfeld's scheme does have some drawbacks. In Asiacrypt 2005, Baek et al. [2] indicated that in this scheme, the designated verifier is required to create a public/private key pair by using the parameters set by the signer. This is impractical in certain scenarios. In certificate-based (CA-based) public key systems, regenerating public/private key-pairs entails cumbersome public key certificate management and results in significant computational overhead. Even in certificateless-based systems where the overhead of regenerating key pairs is relatively smaller, it still places an additional burden on the verifier. If the verifier has already generated public/private key pairs with public key parameters different from those set by the signer, it is unlikely that they will generate another key pair

 doi:10.20944/preprints202501.1409.v1

just for verifying a signature. Baek et al. [2] proposed the Universal Designated Verifier Signature Proof (UDVSP) to circumvent the issue of key initialization by the verifier. In contrast to UDVS, UDVSP employs interactive protocol with the designated verifier to demonstrate the validity of a signature. So, the verifier's key pairs will play no role in this particular proof, which eliminates the need for the verifier to reinitialize a key.

Beyond the problem of reinitializing the verifier's key pairs, the onerous management of public key certificates is also an issue of widespread concern. The UDVS/UDVSP schemes of Steinfeld et al.[1–3] are all constructed under CA-based system. To be more specific, these schemes involve cumbersome certificate processes, including application, issuance, query, and revocation. As a direct consequence, this gives rise to a significant amount of overhead. In contrast, ID-based systems [4] streamline the key management process while ensuring a moderate level of security. This makes them a favorable substitute to CA-based systems. In light of this, Zhang et al. [5] constructed ID-based UDVS. Subsequently, Chen et al. [6] introduced ID-based UDVSP. These schemes allow UDVS and UDVSP to avoid the complex certificate management process.

Interesting, with the proposition of the UDVSP, a new issue has emerged. The application of the interactive protocol in UDVSP can, on occasion, lead to a substantial decrease in the efficiency of the system. Specifically, interactive proofs necessitate that both parties be online concurrently. If either party is offline or in a network environment with high latency, it will incur additional time spent waiting and more communication overhead due to the need to resend messages.

In addition to the above-mentioned issue, the substantial computation cost associated with UDVS/UDVSP is also not something that can be overlooked. As Lin et al.[7] point out, existing UDVSP schemes [2,6] involve time-consuming bilinear pairing operations (one bilinear pairing operation on a mobile terminal takes about 32 ms, which is approximately 9 times the time demanded by an elliptic curve multiplication operation [8]). In order to reduce the computational overhead of UDVSP, Lin et al. [7] designed a UDVSP scheme based on the Chinese cryptographic SM2 algorithm. This scheme eschews bilinear pairing operations and, conversely, makes use of operations on elliptic curves. This approach serves to enhance the computational efficiency of the scheme. However, it is still constructed under CA-based public key systems. Moreover, it is encumbered with the intricacies and challenges inherent to the interactive protocol.

Driven by the problem of the UDVS/UDVSP schemes mentioned above, we would like to obtain ID-based UDVSP systems. The main goal is to solve the certificate management issue via leveraging only elliptic curve operations without any bilinear pairing ones to achieve faster calculations. Furthermore, we would like to construct a non-interactive protocol to circumvent the drawbacks associated with interactive protocols, all the while maintaining the advantages inherent in UDVSP.

Our Contribution. In this paper, we construct ID-based UDVSP systems that are engineered to simultaneously resolve the four aforementioned issues. Firstly, by using the ID-based SM2 digital signature scheme, we build the ID-based UDVSP system which avoids the complex issue of certificate management. To further dispense with the need for interactivity, we make use of the OR-proof and Fiat-Shamir methodologies to design an alternative ID-based UDVSP system. These schemes possess not only the same bilinear pairing-free advantage as the proposal by Lin et al., but also attain the certificate-free or non-interactive objective. Moreover, a analysis of the security and performance aspects of the two schemes has been carried out by us.

The subsequent content presents the layout of the remaining part of this paper: Some preliminaries are introduced in Section 2. Section 3 provides our interactive ID-based UDVSP system along with its security analysis. In Section 4, our non-interactive ID-based UDVSP system and its corresponding security analysis are detailed. Section 5 is dedicated to conducting a performance analysis of the two schemes. Finally, Section 6 reaches conclusions.

 doi:10.20944/preprints202501.1409.v1

2. Preliminaries

2.1. Symbols and Definitions

Table 1 mainly presents the involved symbols and definitions.

Table 1. Symbols and definitions.

Symbol	Definition
ID_a	User's identity.
ENTLA	Two bytes converted from the bit length of ID_a.
q	A big prime number.
F_q	A finite field consisting of q elements.
a, b	Elements in F_q that define an elliptic curve E over F_q.
$E(F_q)$	The collection of all rational points on the elliptic curve E over F_q (where the zero point O is also included).
O	A special point on the elliptic curve, referred to as the point at infinity or zero point.
G	The cyclic group containing every point on the elliptic curve E along with the point at infinity.
P	The generator of the group G.
n	The order of the generator P (where n is a prime factor of $\#E(F_q)$).
$H(\cdot), H_o(\cdot), H_n(\cdot), H_v(\cdot)$	A secure cryptographic hash function.

2.2. The ID-Based Digital Signature Based on SM2

The SM2 digital signature algorithm is a component of the key cryptography algorithms based on elliptic curves. This algorithm was was carried out by the Chinese National Cryptography Administration (refer to " SM2 Public Key Cryptographic Algorithms Based on Elliptic Curves ", China's State Cryptography Administration, December 2010 [9]).

The ID-based digital signature based on SM2 [10] is an improved algorithm derived from the SM2 digital signature. Compared with the SM2 digital signature, the ID-based digital signature based on SM2 utilizes identity information to create the user's private key. The application and management of it do not revolve around digital certificates. Consequently, this obviates the necessity of managing and maintaining public-key certificates and circumvents the time-consuming procedures. The ID-based digital signature based on SM2 consists of four steps: Setup, Extraction, Sign, and Verify.

1) Setup: With the security parameter λ provided, the algorithm randomly select a large prime number q, and determine a non-singular elliptic curve $E : y^2 = x^3 + ax + b \mod q$ (where $a, b \in Z_q^*$). From all the points on E (including the point at infinity), select a cyclic group G of prime order n and a generator $P \in G$. Choose three secure hash functions $H : \{0,1\}^* \times \{0,1\}^* \to Zn^*$, $H_v : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^v$, and $H_o : \{0,1\}^* \to \{0,1\}^{256}$. Randomly select $x \in Zn^*$ and generate the partial system public key $Ppub = xP$. The algorithm outputs the system public key $mpk = (E, a, b, q, G, n, P, Ppub, H, H_v, H_o)$ and the master private key $msk = x$.
2) Extract: Given mpk, msk, and user information ID_a. It randomly selects $l \in Z_n^*$, computes the partial user private key $L = lP$, and the intermediate variable $h = H(ID_a \parallel L)$. The partial user private key d is calculated as $d = l + xh \mod n$. The algorithm gives out the user's private key $sk = (L, d)$.
3) Sign: Given mpk , $sk = (L, d)$, and the message m. It computes the user's distinguishable identifier $Z_a = H_o(ENTLA \parallel ID_a \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_L \parallel y_L)$ and its hash value $e = H_v(Z_a \parallel m)$, where $ENTLA$ is the bit length of ID_a, and (x_p, y_p) and (x_L, y_L) are the coordinates of Pr and L, respectively. Select a random number $k \in Z_n^*$, then compute the elliptic curve point $K = kP =$

 doi:10.20944/preprints202501.1409.v1

(x_K, y_K) and the partial signature $r = (e + x_K) \mod n$. If $r = 0$ or $r + k = n$, select a new k and repeat the calculations. Otherwise, compute the partial signature $s = (1 + d)^{-1}(k - rd) \mod n$. If $s \neq 0$, the algorithm outputs the message-signature pair m and $\sigma = (L, r, s)$.

4) Verify: Given mpk, ID_a, m, and the signature to be verified $\sigma = (L, r, s)$. If $r, s \notin Z_n^*$, it outputs 0. Otherwise, it computes $t = r + s \mod n$. If $t = 0$, outputs 0. If $t \neq 0$, the following series of computations are carried out. First, compute $Z_a = H_o(ENTLA \parallel ID_a \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_L \parallel y_L)$. Then, calculate $h' = H(ID_a \parallel L)$. Next, determine $e' = H_v(Z_a \parallel m)$. After that, obtain $K' = sP + t(L + h'P_{pub}) = (x'_K, y'_K)$. Finally, calculate $r' = (e' + x'_K) \mod n$. If $r' = r$, the algorithm outputs 1 to denote the validity of the signature; in contrast, it outputs 0 to denote the invalidity of the signature.

The ID-based digital signature algorithm based on SM2 satisfies correctness and existential unforgeability under adaptively chosen message attacks (EUF-CMA) [11].

2.3. Zero-Knowledge Proof, Σ-Protocol with Its OR Construction

Suppose the interactive protocol Π consists of two entities, a prover Pr and a verifier Vr. Pr can convince Vr about the binary relation $R = (x, w) : \{0,1\}^* \times \{0,1\}^*$ (where x and w refer to the instance and the witness, respectively). If the protocol Π meets the requirements of Completeness and Soundness, it is called as a Proof of Knowledge system. Additionally, if Π further satisfies Honest-Verifier Zero-Knowledge (HVZK), then it is known as an Interactive Honest-Verifier Zero-Knowledge Proof system [12] [13].

The Σ-protocol is an interactive three-move zero-knowledge proof system. Assume Pr and Vr execute the OR proof [14] and obtain the result $(a_0, a_1, c, c_0, c_1, z_0, z_1)$, P chooses a challenge c_{1-b} , where $b = 0$ or 1 . Another challenge $c_b = c \oplus c_{1-b}$ is determined by Vr's random challenge c. The commitment and response (a_0, a_1, z_0, z_1) is generated by Pr using the private witness w based on c_0, c_1. The completeness of the Σ-protocol means that if there exists a valid function $\phi(\alpha, a_1, c, c_0, c_1, z_0, z_1) = 1$, then Vr accepts $(a_0, a_1, c, c_0, c_1, z_0, z_1)$. Special soundness means that given two valid tuples (a, c, z) and (a, c', z') with $c \neq c'$, one can recover Pr's witness w. Special HVZK means that given Vr's random challenge c, there are a probabilistic polynomial-time (PPT) simulator SI that can interact with Vr to output a valid tuple $(a_0, a_1, c, c_0, c_1, z_0, z_1)$. Assume the real interaction between Pr and Vr outputs $(a_0, a_1, c', c'_0, c'_1, z'_0, z'_1)$, then $(a_0, a_1, c, c_0, c_1, z_0, z_1)$ and $(a_0, a_1, c', c'_0, c'_1, z'_0, z'_1)$ are indistinguishable.

The OR proof [14] is a fundamental construction of the Σ-protocol. It allows Pr to prove that for two computational problems x_0 and x_1, Pr knows the witness w for one of the problems, such that either $(x_0, w) \in R$ or $(x_1, w) \in R$, without disclosing which one.

The last property of OR proof is known as witness indistinguishable (WI). This property sets it apart from other Σ-protocols. To elaborate, Pr might be aware of which one in several distinct values of w would enable them to successfully complete the protocol. However, for arbitrary Vr, it is impossible to determine which of these possible values the Pr actually knows merely from the conversations.

The Σ-protocol is capable of being changed into a non-interactive instance through the utilization of the Fiat-Shamir methodologies [15]. Using the normal Σ-protocol to construct a non-interactive scheme will, however, undermine the non-transferability privacy property of UDVS. Therefore, we utilize the OR proof to construct our scheme, leveraging the WI property of the OR proof. In the non-interactive form of OR proof, Pr computes (a_0, a_1) and c_{1-b}. Then directly calls $c = H(x, a)$ to obtain the challenge value c, and determine c_b. Using the private witness w, Pr then computes $z_0, z_1)$ and finally sends $(a_0, a_1, c, c_0, c_1, z_0, z_1)$ to Vr. The non-interactive protocol obtained through the Fiat-Shamir transformation still satisfies the properties of interactive form [15].

3. Interactive ID-Based UDVSP Based on SM2 Digital Signature

3.1. The Proposed System

The interactive ID-based UDVSP scheme was constructed by ID-based SM2 signatures and Σ-protocol. Specifically, it is formed by five algorithms and one protocol.

 doi:10.20944/preprints202501.1409.v1

- Setup: Provided the security parameter λ , randomly picks a big prime number q, and determines a non-singular elliptic curve $E : y^2 = x^3 + ax + b \mod q$ (where $a, b \in \mathbb{Z}_q^*$). Among all points on E (including the zero point), a cyclic group G of prime order n and a generator $P \in G$ are selected. Secure hash functions are chosen as follows: $H : \{0,1\}^* \times \{0,1\}^* \to \mathbb{Z}n^*$, $H_v : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^v$, and $H_o : \{0,1\}^* \to \{0,1\}^{256}$. Here, $H_v(\cdot)$ and $H_o(\cdot)$ are secure cryptographic hash function. A random $x \in \mathbb{Z}q^*$ is selected, and the partial system public key is computed as $P\text{pub} = xP$. The algorithm outputs the system public key $\text{mpk} = (E, a, b, q, G, n, P, P\text{pub}, H, H_v, H_o)$ and the master private key $\text{msk} = x$.This invention is based on the SM2 digital identity signature design, so it uses the same system parameters as the identity-based SM2 digital signature. For specific parameter symbols and definitions, refer to the detailed implementation section (2.1 Symbols and Definitions).
- Extract: Given the system's master public key mpk, master private key msk, and user information ID_a. It randomly selects $l \in Z_n^*$, computes the partial user private key $L = lP$, and the intermediate variable $h = H(ID_a \parallel L)$. The partial user private key d is calculated as $d = l + xh \mod n$. The user's private key $sk = (L, d)$ is output.
- Sign: Given the system's master public key mpk , the user's private key $sk = (L, d)$, and the message m. It computes the user's distinguishable identifier $Z_a = H_o(\text{ENTLA} \parallel ID_a \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_L \parallel y_L)$ and the hash value $e = H_v(Z_a \parallel m)$, where $ENTLA$ is the bit length of ID_a, and (x_p, y_p) and (x_L, y_L) are the coordinates of Pr and L, respectively. A random $k \in Z_n^*$ is selected, then the elliptic curve point $K = kP = (x_K, y_K)$ and the partial signature $r = (e + x_K) \mod n$ are computed. If $r = 0$ or $r + k = n$, a new k is selected and the calculations are repeated. Otherwise, the partial signature $s = (1 + d)^{-1}(k - rd) \mod n$ is computed. If $s \neq 0$, the algorithm outputs the message m and the signature $\sigma = (L, r, s)$.
- Verify: Given the system's master public key mpk, user information ID_a, message m, and the signature to be verified $\sigma = (L, r, s)$. If $r, s \notin Z_n^*$, it outputs 0. Otherwise, it computes $t = r + s \mod n$. If $t = 0$, it outputs 0. Otherwise, it computes $Z_a = H_o(\text{ENTLA} \parallel ID_a \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_L \parallel y_L)$, $h' = H(ID_a \parallel L)$, $e' = H_v(Z_a \parallel m)$, $K' = sP + t(L + h'P_{pub}) = (x'_K, y'_K)$, and $r' = (e' + x'_K) \mod n$. If $r' = r$, the algorithm outputs 1 to denote the validity of the signature; in contrast, it outputs 0 to denote the invalidity of the signature.
- Tran: Given the system public key mpk, user information ID_a, message m, and the signature to be verified $\sigma = (L, r, s)$. It randomly selects $a_r, b_r \in \mathbb{Z}_n^*$ and computes $Z_a = H_o(\text{ENTLA} \parallel \text{ID}_a \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_L \parallel y_L)$, $e = H_v(Z_a \parallel m)$, $\hat{r} = r + a_r - e \mod n$, $\hat{s} = s + b_r \mod n$. The algorithm outputs the transformed signature $\hat{\sigma} = (L, \hat{r}, \hat{s})$ and the transformation key $tk = (a_r, b_r)$.
- IVerf: Provided the system public key mpk, user information ID_a, and the transformed signature $\hat{\sigma}$. The signature owner Pr additionally takes the transformation key tk and the signature σ as input. The signature owner Pr and the designated verifier Vr perform the following interaction:

1. Pr first computes $h = H(\text{ID}a \parallel L)$, $T = hP\text{pub}$, $K = sP + (r + s)(L + T)$. Then Pr randomly selects $\alpha, \beta \in \mathbb{Z}n^*$ and $R \in G$, and computes the commitment value $D = R + \beta P + \alpha(L + hP\text{pub}) + \beta(L + hP_{\text{pub}})$. Finally, Pr sends D to Vr.
2. Vr randomly selects a challenge value $c \in \mathbb{Z}_n^*$ and returns c to Pr.
3. Pr calculates the response to the challenge $Z_K = R - cK$, $z_a = \alpha - c \cdot a_r \mod n$, $z_b = \beta - c \cdot b_r \mod n$, and sends (Z_K, z_a, z_b) to Vr.
4. Vr calculates $e' = H_v(Z_a \parallel m)$, $h' = H(\text{ID}a \parallel L)$, $T = (L + h'P\text{pub})$, and $D' = Z_K + z_bP + z_aT + z_bT + c(\hat{s}P + \hat{r}T + e'T + \hat{s}T)$. If $D' = D$, Vr outputs 1 indicating acceptance; otherwise, Vr outputs 0.

3.2. Security Analysis

This section will show that the constructed interactive ID-based UDVSP system constructed from SM2 can achieve the anticipated security properties. Since the SM2 ID-based digital signature has been proven to be existentially unforgettable under adaptively chosen message and identity attacks (EUF-CM-GID-A) [11], this paper only analyzes the security of the UDVSP system against impersonation

 doi:10.20944/preprints202501.1409.v1

attacks, which are divided into resistance against type 1 impersonation attacks (R-IM-TYPE-1) and resistance against type 2 impersonation attacks (R-IM-TYPE-2).

Theorem 1: If the IVerf protocol of UDVSP satisfies Honest-Verifier Zero-Knowledge (HVZK), then UDVSP satisfies R-IM-TYPE-1.

Proof: First, we construct a simulator SI (Algorithm 1) to prove that the IVerf protocol of UDVSP satisfies HVZK. SI first generate a valid message-signature pair $(m, \sigma = (L, r, s))$ and replicates all interactions with the honest verifier Vr. On account of the random numbers $a_r, b_r \in \mathbb{Z}_n^*$ in steps 1) and 2), the first two steps of SI are completely blind. The point L is a random point derived from the user's private key, and the verifier cannot recover the original signature (L, r, s) from the transformed signature $(L, \hat{r}, \hat{s})$. Additionally, steps 3) to 5) form a σ-protocol, which satisfies special HVZK, effectively preventing the leakage of the transformation key (a_r, b_r). Therefore, the IVerf protocol of UDVSP satisfies HVZK.

Algorithm 1: Simulator SI for the IVerf protocol.

1. SI requests a signature $(m, \sigma = (L, r, s))$ from the signer.
2. SI selects $a_r, b_r \in \mathbb{Z}_n^*$ at random and computes $e = H_v(Z_a \parallel m)$, $\hat{r} = r + a_r - e \mod n$, $\hat{s} = s + b_r \mod n$, and sends $(L, \hat{r}, \hat{s})$ to Vr.
3. SI randomly selects $\alpha, \beta \in \mathbb{Z}n^*$ and $R \in G$, computes the commitment value $D = R + \beta P + \alpha(L + hP\text{pub}) + \beta(L + hP_{\text{pub}})$, and sends D to Vr.
4. SI receives the challenge value $c \in \mathbb{Z}_n^*$ sent by Vr.
5. SI computes the response to the challenge $Z_K = R - cK$, $z_a = \alpha - c \cdot a_r \mod n$, $z_b = \beta - c \cdot b_r \mod n$, and sends (Z_K, z_a, z_b) to Vr

If there exists a PPT adversary $A = (V', P')$ that successfully breaks the R-IM-TYPE-1 security of UDVSP, it implies that A can obtain information about (a_r, b_r) to successfully interact with other designated verifiers. This would violate the HVZK property of the IVerf protocol in UDVSP. Therefore, UDVSP satisfies R-IM-TYPE-1.

Theorem 2: If the SM2 identity-based digital signature has the property of EUF-CM-GID-A, then UDVSP has the property of R-IM-TYPE-2.

Proof: Suppose there exists an algorithm A that successfully breaks the R-IM-TYPE-2 property of UDVSP. Then, there exists an algorithm B that can use the capability of A to successfully break the EUF-CM-GID-A property of the SM2 identity-based digital signature. Algorithm B is given the system public key $\text{mpk} = (E, a, b, q, G, n, P, P_{\text{pub}}, H, H_v, H_o)$ ($P_{\text{pub}} = xP$, $H : 0, 1^* \times \{0,1\}^* \to \mathbb{Z}_n^*$, $H_v : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^v$, $H_o : \{0,1\}^* \to \{0,1\}^{256}$). The goal is to output a valid message-signature pair.

First, B sends $(E, a, b, q, G, n, P, P_{\text{pub}}, H, H_v, H_o)$ to A and calls A to obtain the transformed signature $\hat{\sigma} = (L, \hat{r}, \hat{s})$ for m. Then, B and A execute step 1 of the IVerf protocol to obtain $D = R + \beta P + \alpha(L + hP_{\text{pub}}) + \beta(L + hP_{\text{pub}})$, and D is returned to B. B computes $e' = H_v(Z_a \parallel m)$, $h' = H(\text{ID}_a \parallel L)$, $T = (L + h'P_{\text{pub}})$, and verifies $D = Z_K + z_b P + z_a T + z_b T + c(\hat{s}P + \hat{r}T + e'T + \hat{s}T)$. If this does not hold, B terminates the current interaction; otherwise, B calls A again with a new challenge value $c' \in \mathbb{Z}_n^*$ to obtain new proof values (Z'_K, z'_a, z'_b). If $D' = Z'_K + z'_b P + z'_a T + z'_b T + c(\hat{s}P + \hat{r}T + e'T + \hat{s}T)$, then B can compute $a_r = (z_a - z'_a) \cdot \tau \mod n$, $b_r = (z_b - z'_b) \cdot \tau \mod n$, $K = \tau(Z_K - Z'_K)$, where $\tau = (c - c')^{-1}$ can be solved using the extended Euclidean algorithm. B uses (a_r, b_r) to recover $\sigma = (L, r, s)$, and finally outputs the forged message-signature pair $(m, \sigma = (L, r, s))$. This contradicts the EUF-CM-GID-A property of the SM2 identity-based digital signature, thus UDVSP satisfies R-IM-TYPE-2.

4. Non-Interactive ID-Based UDVSP Based on SM2 Digital Signature

4.1. The Proposed System

The non-interactive ID-based UDVSP scheme is also relies on ID-based SM2 signatures. But different from the previous scheme, it uses OR form of Σ-protocol for protocol design. Although the designated verifier still needs to have a pair of public and private keys, these required key pairs do not have to be generated based on the signer's public key parameters. Instead, the designated verifier can

 doi:10.20944/preprints202501.1409.v1

make use of an existing public-private key pairs. The scheme specifically comprises five algorithms and one protocol.

- Setup: Given the security parameter λ, randomly picks a large prime number q, and determines a non-singular elliptic curve $E : y^2 = x^3 + ax + b \mod q$ (where $a, b \in \mathbb{Z}_q^*$). Among all points on E (including the zero point), a cyclic group G of prime order n and a generator $P \in G$ are selected. Secure hash functions are chosen as follows: $H : \{0,1\}^* \times \{0,1\}^* \to \mathbb{Z}n^*$, $H_v : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^v$, and $H_o : \{0,1\}^* \to \{0,1\}^{256}$. Here, $H_v(\cdot)$ is a cryptographic hash function with a message digest length of v bits, and $H_o(\cdot)$ is a secure cryptographic hash function. A random $x \in \mathbb{Z}q^*$ is selected, and the partial system public key is computed as $P\text{pub} = xP$. The algorithm outputs the system public key $\text{mpk} = (E, a, b, q, G, n, P, P\text{pub}, H, H_v, H_o)$ and the master private key $\text{msk} = x$.This invention is based on the SM2 digital identity signature design, so it uses the same system parameters as the identity-based SM2 digital signature. For specific parameter symbols and definitions, refer to the detailed implementation section (2.1 Symbols and Definitions).
- Extract: Given the system's master public key mpk, master private key msk, and user information ID_a. It randomly selects $l \in Z_n^*$, computes the partial user private key $L = lP$, and the intermediate variable $h = H(ID_a \parallel L)$. The partial user private key d is calculated as $d = l + xh \mod n$. The algorithm outputs the user's private key $sk = (L, d)$.
- Sign: Given the system's master public key mpk , the user's private key $sk = (L, d)$, and the message m. It computes the user's distinguishable identifier $Z_a = H_o(\text{ENTLA} \parallel ID_a \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_L \parallel y_L)$ and the hash value $e = H_v(Z_a \parallel m)$, where $ENTLA$ is the bit length of ID_a, and (x_p, y_p) and (x_L, y_L) are the coordinates of Pr and L, respectively. A random $k \in Z_n^*$ is selected, and the elliptic curve point $K = kP = (x_K, y_K)$ and the partial signature $r = (e + x_K) \mod n$ are computed. If $r = 0$ or $r + k = n$, a new k is selected and the calculations are repeated. Otherwise, the partial signature $s = (1 + d)^{-1}(k - rd) \mod n$ is computed. If $s \neq 0$, the algorithm outputs the message m and the signature $\sigma = (L, r, s)$.
- Verify: Given the system's master public key mpk, user information ID_a, message m, and the signature to be verified $\sigma = (L, r, s)$. If $r, s \notin Z_n^*$, it outputs 0. Otherwise, it computes $t = r + s \mod n$. If $t = 0$, it outputs 0. Otherwise, it computes $Z_a = H_o(\text{ENTLA} \parallel ID_a \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_L \parallel y_L)$, $h' = H(ID_a \parallel L)$, $e' = H_v(Z_a \parallel m)$, $K' = sP + t(L + h'P_{pub}) = (x'_K, y'_K)$, and $r' = (e' + x'_K) \mod n$. If $r' = r$, the algorithm outputs 1 to denote the validity of the signature; in contrast, it outputs 0 to denote the invalidity of the signature.
- DGenr: Given the system public key mpk. It randomly selects $\text{sk}_v \in \mathbb{Z}_n'^*$ and computes $\text{pk}_v = \text{sk}_v P$. The algorithm outputs the designated verifier Vr's private key and public key $(\text{sk}_v, \text{pk}_v)$. The public key parameters of the designated verifier and pk_v are published, while sk_v is kept by Vr.
- DVerf: In this protocol, the signature owner Pr proves to the designated verifier Vr that they possess a signature σ that can be verified or that they possess Vr's private key sk_v. If Vr has not leaked sk_v, they will believe that Pr has a valid σ, but cannot disclose this fact to a third party (because Vr, who possesses sk_v, can forge the related proof). First, Pr selects a hash function $H_n : Z_n^* \to Z_n'^*$ based on Vr's public key parameters. Pr and Vr then execute the following protocol:

1. Pr computes $h = H(\text{ID}a \parallel L)$,$T = L + hP_{\text{pub}}$ and $K = sP + (r + s)T$. Then, Pr randomly selects $\alpha \in Z_n^*$, $\beta, w \in Z_{n'}^*$, and $R \in G$, and computes $D_1 = R - \alpha P - \alpha T$ and $D_2 = \beta P + wpk_v$
2. Pr obtains $c = H_c(D_1, D_2, ID_a, pk_v)$.
3. Pr designates $c_1 = c - H_n(w)$ and $c_2 = w$, then computes $Z_K = R - c_1 K$, $z_a = \alpha - c_1 s$, and $z_b = \beta$. The proof $\hat{s} = (c_1, c_2, Z_K, z_a, z_b)$ is then formed. Subsequently, Pr sends $(L, r, \hat{s})$ and the hash function H_n to Vr.
4. V computes:$h' = H(IDa \parallel L)$,$T' = L + hP_{\text{pub}}$ then $D'_1 = Z_K - z_a P - z_a T' + c_1 r T'$,$D'_2 = z_b P + c_2 pk_v$,$c = H_c(D_1, D_2, ID_a, pk_v)$.If $D'_1 = D_1$, $D'_2 = D_2$, and $c_1 + H_n(c_2) = c$, then output 1 to indicate acceptance; otherwise, output 0.

 doi:10.20944/preprints202501.1409.v1

4.2. Security Analysis

Theorem 3: If the identity - based digital signature based on SM2 has the property of EUF - CM - GID - A, and the Elliptic Curve Discrete Logarithm Problem (ECDLP) is intractable, then UDVSP has the property of R-IM-TYPE-2.

Proof: This section will illustrate that the constructed non - interactive identity - based UDVSP system based on SM2 can hold the anticipated security properties. Since the ID - based digital signature EUF-CM-GID- A based on SM2 has been verified by Lin et al [11]., and Chen et al. [6] have demonstrated that without signature conversion (Tran), due to the zero - knowledge property of the Σ protocol, Type 1 impersonation attacks are tantamount to Type 2 impersonation attacks. Hence, this paper only needs to prove that the UDVSP system complies with R-IM-TYPE- 2.

First, B sends cp, pk_v and mpk to A, and calls A to obtain the hash functions $H_n = Z_n'^* \to Z_n^*$ and $H_c : (D, D, \{0,1\}^*, D) \to Z_n^*$. Then, B and A execute the DVerf protocol to obtain the commitment value, challenge value, and proof values $(D_1, D_2, c_1, c_2, Z_K, z_a, z_b)$. B computes $h = H(ID_a \parallel L)$ and verifies $D_1 = Z_K - z_a P - z_a(L + hP_{pub}) + c_1 r(L + hP_{pub})$, $D_2 = z_b P + c_2 pk_v$, $H_n(D_1, D_2, ID_a, pk_v) = c = c_1 + H_n(c_2)$. If this does not hold, B terminates the current interaction. Otherwise, B calls A again, and B obtains the challenge value and proof values $(D_1, D_2, c_1', c_2', Z_K', z_a', z_b')$. If $D_1 = Z_K' - z_a' P - z_a'(L + hP_{pub}) + c_1' r(L + hP_{pub})$, $D_2 = z_b' P + c_2' pk_v$, $H_c(D_1, D_2, ID_a, pk_v) = c_1' = c_1' + H_n(c_2')$ holds, then B can compute $s = (z_a - z_a') \cdot \tau \mod n$, $K = \tau(Z_K - Z_K')$ or $sk_v = (z_b - z_b') \cdot \tau \mod n$. Here, $\tau = (c - c')^{-1}$, which can be solved using the extended Euclidean algorithm. B can recover $\sigma = (L, r, s)$, and finally output the forged message-signature pair $(m, \sigma = (L, r, s))$ or obtain the discrete logarithm sk_v of the ECDLP instance $pk_v = sk_v P'$. This contradicts the EUF-CM-GID-A property of the identity-based digital signature based on SM2 and the computational hardness of ECDLP, thus UDVSP has the property of R-IM-TYPE-2.

5. Performance Evaluation

Firstly, a analytical study of the calculation and communication consumptions of our scheme is presented in this section, along with a comparison to prevalent existing solutions such as UDVSP [2,7] and UDVS [16,17]. In this context, the two key-producing procedures within UDVS systems are equally accounted for in KGen, and the focus regarding communication overheads lies primarily on the IVerf interactive protocol. As illustrated in Table 2, compared to existing UDVSP/UDVS schemes, our schemes exhibit optimized computational consumptions and communication overheads. This advantage stems from the elimination of the laborious bilinear map operation and hash function for mapping to a point in our scheme.

Lin et al. [7] developed a prototype for each operation within these comparable schemes to acquire the empirical effectiveness. The execution was carried out on a laptop computer equipped with an i7-9750H 2.59 GHz processor, 16 GB of memory, and the Windows 10 operating system. The cryptographic library used was the miracl library (a widely used cryptographic library, version 7.0). In particular, they utilized the BLS (Boneh-Lynn-Shacham) curve with an ate pairing embedding degree of 24, which is highly suitable for the security level AES-256.6. As a result, the sizes of the elements in Zq, G1, G2, and GT are 64 bytes, 160 bytes, 640 bytes, and 1920 bytes respectively. The corresponding notations and execution times are presented in Table 3.

Through theoretical analysis, it is concluded that compared to other existing schemes except UDVSP-3, the two schemes proposed in this paper reduce the computational overhead by at least 82.66%. The computational overhead is approximately 1.38 times that of the UDVSP-3 scheme. However, since the schemes proposed in this paper avoid the cumbersome public key certificate management compared to the UDVSP-3 scheme, the slightly higher computational overhead is acceptable.

 doi:10.20944/preprints202501.1409.v1

Table 2. Theoretical performance comparison results.

Scheme	Computation					Communication
	UKGen	USign	UVerf	UTran	UIVerf	UIVerf
UDVSP-1 [2]	T_{g1sm}	$T_{h2p} + T_{g1sm}$	$2T_{bp} + T_{h2p}$	T_{g1sm}	$2T_{bp} + T_{mm} + T_{ma} + 2T_{ebp} + T_{mbp} + T_{h2p}$	$\|G_T\| + 2\|Z_n\|$
UDVSP-2 [2]	$2T_{g2sm}$	$T_{g1sm} + T_{mi} + T_{mm} + 2T_{ma}$	$2T_{bp} + 2T_{g2sm} + T_{g2pa}$	T_{g1sm}	$2T_{bp} + 2T_{g2sm} + 2T_{g2pa} + T_{ebp} + T_{mm} + T_{ma} + T_{ebp} + T_{mbp}$	$\|G_T\| + 2\|Z_n\|$
UDVS-1 [16]	$4T_{g1sm}$	$3T_{g1sm} + 2T_{g1pa} + T_{mm}$	$T_{g1sm} + T_{g1pa} + 3T_{bp} + T_{mbp}$	$2T_{g1sm} + T_{mm} + 3T_{g1pa} + T_{bp}$	$2\,T_{g1sm} + T_{g1pa} + 2T_{bp} + T_{mbp} + 2T_{ebp}$	$\|G_T\| + \|G_1\|$
UDVS-2 [17]	$2T_{g1sm}$	$5T_{g1sm} + 3T_{g1pa}$	$2T_{g1sm} + 3T_{g1pa} + 3T_{bp} + T_{mbp}$	T_{bp}	$2T_{g1sm} + 3T_{g1pa} + 2T_{bp} + T_{mbp} T_{mbp} + 2T_{ebp}$	$\|G_T\| + \|G_1\|$
UDVSP-3 [7]	T_{g1sm}	$T_{g1sm} + T_{mi} + T_h + 2T_{mm} + 2T_{ma}$	$2T_{g1sm} + T_{g1pa} + 2T_{ma}$ + Th	$3T_{ma} + T_h$	$14T_{g1sm} + 13T_{g1pa} + 7T_{mm} + 3T_{ma} + T_h$	$2\|G_1\| + 3\|Zn\|$
Our UDVSP-1	T_{g1sm}+T_h+ T_{ma}+T_{mm}	T_{g1sm}+T_{mi}+2T_h+ 2T_{ma}+2T_{mm}	$3T_{g1sm}$+ $2T_{g1pa}$+ 2T_{ma}+3T_h	3T_{ma}+2T_h	$16T_{g1sm} + 15T_{g1pa} + 7T_{mm} + 3T_{ma} + 3T_h$	$2\|G_1\| + 3\|Zn\|$
Our UDVSP-2	T_{g1sm}+T_h+ T_{ma}+T_{mm}	T_{g1sm}+T_{mi}+2T_h+ 2T_{ma}+2T_{mm}	$3T_{g1sm}$+ $2T_{g1pa}$+ 2T_{ma}+3T_h	T_{ma}	$15T_{g1sm} + 10T_{g1pa} + 7T_{mm} + 4T_{ma} + 6T_h$	$4\|G_1\| + 5\|Zn\|$

Table 3. Symbol definition and time cost.

Notation	Description	Time	Notation	Description	Time
T_{g1pa}	A point addition in G_1	0.165954	T_{bp}	A bilinear pairing G_T	820.32
T_{g1sm}	A scale multiplication in G_1	35.3111	T_{ebp}	A exponentiation in G_T	689.273
T_{g2pa}	A point addition in G_2	0.63289	T_{mbp}	A multiplication in G_T	2.05855
T_{g2sm}	A scale multiplication in G_2	206.575	T_{mi}	A modular inversion in Z_{n^*}	0.05023
T_h	A general hash function	0.00576	T_{mm}	A modular multiplication in Z_{n^*}	0.01231
T_{h2p}	A map-to-point hash function	17.1464	T_{ma}	A modular add in Z_{n^*} ,	0.00271

6. Conclusions

Although Lin et al.'s scheme addresses the issue that existing UDVSP schemes all involve highly time-consuming bilinear pairings operation, their scheme still suffers from the cumbersome certificate management problem and the drawbacks brought about by the interactive protocol. To address these issues, we first propose the ID-based UDVSP system constructed from the ID-based SM2 digital signature scheme to eschew the intricate certificate management procedures. Moreover, we construct non-interactive ID-based UDVSP by using the OR-proof and Fiat-Shamir technologies. Our work not merely exhibit the same bilinear pairing-free merit as the proposition of Lin et al., but also fulfills the free or non-interactive ambition of the certificate.

7. Patents

Author Contributions: Conceptualization, Y.Y. and X.Z.; methodology, W.W.; software, Y.Y.; validation, B.S., Y.Y. and X.Z.; formal analysis, B.S.; investigation, W.W.; resources, W.W.; data curation, Y.Y.; writing—original draft preparation, Y.Y.; writing—review and editing, X.Z.; visualization, B.S.; supervision, W.W.; project administration, B.S.; funding acquisition, X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant U21A20466, and Grant 62372108.

References

1. Steinfeld, R.; Bull, L.; Wang, H.; Pieprzyk, J. Universal Designated-Verifier Signatures. *IACR Cryptol. ePrint Arch.* **2003**, p. 192.

2. Baek, J.; Safavi-Naini, R.; Susilo, W. Universal designated verifier signature proof (or how to efficiently prove knowledge of a signature). In Proceedings of the Advances in Cryptology-ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005. Proceedings 11. Springer, 2005, pp. 644–661.
3. Steinfeld, R.; Wang, H.; Pieprzyk, J. Efficient extension of standard Schnorr/RSA signatures into universal designated-verifier signatures. In Proceedings of the Public Key Cryptography–PKC 2004: 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004. Proceedings 7. Springer, 2004, pp. 86–100.
4. Shamir, A. Identity-based cryptosystems and signature schemes. In Proceedings of the Advances in Cryptology: Proceedings of CRYPTO 84 4. Springer, 1985, pp. 47–53.
5. Zhang, F.; Susilo, W.; Mu, Y.; Chen, X. Identity-based universal designated verifier signatures. In Proceedings of the International Conference on Embedded and Ubiquitous Computing. Springer, 2005, pp. 825–834.
6. Chen, X.; Chen, G.; Zhang, F.; Wei, B.; Mu, Y. Identity-based universal designated verifier signature proof system **2009**.
7. LIN, C.; HE, D.; HUANG, X. Blockchain-based electronic medical record secure sharing. *Journal of Computer Applications* **2022**, *42*, 3465.
8. Abbasinezhad-Mood, D.; Nikooghadam, M. An anonymous ECC-based self-certified key distribution scheme for the smart grid. *IEEE Transactions on Industrial Electronics* **2018**, *65*, 7996–8004.
9. Zhang, Z.; Yang, K.; Zhang, J.; Chen, C. Security of the SM2 signature scheme against generalized key substitution attacks. In Proceedings of the International Conference on Research in Security Standardisation. Springer, 2015, pp. 140–153.
10. HE, D.; Zhang, J.; Chen, B.; Zhang, Y. *An identity-based digital signature method and system based on SM2*. 430072 299 Bayi Road, Wuchang District, Wuhan, Hubei Province, China, cn108809658b(in chinese) ed., 2021.
11. LIN, C.; HUANG, X.; HE, D. Efficient Range Proof Protocols Based on Chinese Cryptographic SM2. *Chinese Journal of Computers* **2022**, *45*, 148–159.
12. Bellare, M.; Goldreich, O. On Defining Proofs of Knowledge. In Proceedings of the Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings; Brickell, E.F., Ed. Springer, 1992, Vol. 740, *Lecture Notes in Computer Science*, pp. 390–420. https://doi.org/10.1007/3-540-48071-4_28.
13. Cramer, R.; Damgård, I.; MacKenzie, P.D. Efficient Zero-Knowledge Proofs of Knowledge Without Intractability Assumptions. In Proceedings of the Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000, Proceedings; Imai, H.; Zheng, Y., Eds. Springer, 2000, Vol. 1751, *Lecture Notes in Computer Science*, pp. 354–373. https://doi.org/10.1007/978-3-540-46588-1_24.
14. Ivan, D. On Σ-protocols. LectureNote,University of Aarhus,Department for Computer Science,2002.
15. Faust, S.; Kohlweiss, M.; Marson, G.A.; Venturi, D. On the non-malleability of the Fiat-Shamir transform. In Proceedings of the Progress in Cryptology-INDOCRYPT 2012: 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings 13. Springer, 2012, pp. 60–79.
16. Huang, X.; Susilo, W.; Mu, Y.; Wu, W. Secure universal designated verifier signature without random oracles. *Int. J. Inf. Sec.* **2008**, *7*, 171–183. https://doi.org/10.1007/S10207-007-0021-2.
17. Rastegari, P.; Berenjkoub, M.; Dakhilalian, M.; Susilo, W. Universal designated verifier signature scheme with non-delegatability in the standard model. *Inf. Sci.* **2019**, *479*, 321–334. https://doi.org/10.1016/J.INS.2018.12.020.