Advances in Computational Design, *Vol. 11, No. 3 (2026) 229-247*
https://doi.org/10.12989/acd.2026.11.3.229

Privacy-preserving enhanced ring signature with Paillier based on batch verification for secure e-bidding

T. S. Vasughi[a], P. Muthulakshmi*

Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu 603203, India

(Received May 6, 2026, Revised June 16, 2026, Accepted June 22, 2026)

Abstract. Blockchain is a promising technology that allows transactions to access the data in a decentralized and secure environment among participants on the open ledger network. Each bidder can access the copy of data in the blockchain network. On-chain data privacy for the permissionless blockchain e-bidding systems is the major issue of ensuring bid confidentiality, and bidder anonymity and privacy-preserving verification remains open challenge. To address this issue, the proposed Privacy-Preserving Enhanced Ring signature with Paillier based on Batch Verification for secure E-bidding (ERSPBV) that integrates ring-signed bid submission with Paillier Homomorphic Encryption (PHE) and batch verification smart contract to realize secure bidding, anonymity, and fine-grained access control. Ring signature ensures unlikability and anonymity of bidders during bid submission providing strong bidder privacy, this ensure untrace ability but prevent double signing. PHE supports secure aggregation and computation on ciphertexts without revealing individual values. The auctioneer checks bidder authorization using bidder authentication smart contract. Only those registered and permitted bidders to participate in the auction. Batch verification allows the auctioneer to verify multiple signatures submitted by multiple bidders at once to reduce total verification time. The bidders and auctioneer are interacting with each other through the smart contracts to achieve privacy and fairness and tamper-resistance. Emulated the cryptographic primitives and smart contract of this proposed e-bidding scheme on the Ethereum platform and the performance evaluation shows that high computational efficiency and secure bid processing is feasible in the Sepolia test network.

Keywords: blockchain technology; data privacy; e-bidding; homomorphic encryption; smart contract

1. Introduction

Blockchain technology is integrated into several applications like smart cities, e-health, e-Government, voting, financial transactions, e-bidding etc. These use cases are strategically crafted to harness the inherent advantages of blockchain technology, making the most of its decentralized control, immutability, cryptographic security, fault tolerance, and capability to execute smart contracts. This strategic utilization aims to enhance various aspects of applications, including transparency, security, and operational efficiency by leveraging the distinctive features that blockchain offers.

E-bidding has become an important area of researcher to focusing on rapid digital transformation,

*Corresponding author, Professor., E-mail: muthulap@srmist.edu.in
[a]Assistant Professor, E-mail: vt7068@srmist.edu.in

ISSN: 2383-8477 (Print), 2466-0523 (Online)

fraud prevention, transparency, privacy, confidentiality. Traditional auctions are sealed-bid and open-bid. In sealed-bid auctions, bids are submitted privately, whereas open-bid auction reveal the bids publicly during the auction process. E-bidding can use sealed bids and also support open-bid or real time auction formats depending on the system design [17]. Although there is no unified standard for the E-bidding system which leads to poor real-time collaboration with different systems. Traditional e-bidding systems suffer lack of bidder anonymity, premature leakage of bid values, tamper with submitted bids. An Adoption of blockchain technology has opened new opportunities for decentralization, tamper-proof and trust less e-bidding architectures where participants do not need to trust auctioneer or any other party.

Author combined e-voting and e-bidding systems to function without third party. Participants securely obtain ballot or bidding information directly from the smart contract and independently verify results during the opening phase [1]. A web-based platform to manage the major phrases of the tendering workflow like tender announcements, bid submission, bid opening, evaluation, approval and final awarding. The system enhances the efficiency of the existing manual tendering procedures used by public procurement bodies in Nigeria [6].

In [13] addresses the barriers to E-Tendering implementation in the construction industry to create policies that promote the long-term reform of procurement processes and also support sustainable development goals. Beneficiary-level competitive bidding helps to reduce risk selection issues in health care entitlement programs. Two-sided health insurance market and compares three beneficiary allocation methods are risk-adjusted prospective payments, pure competitive bidding and hybrid of both approaches.

This paper presents a secure and privacy-preserving ERSPBV model that enhances bid confidentiality, anonymity and fairness in decentralized auction environments. The main contributions of this work can be summarized as follows:

1. The proposed two-layer cryptographic model allows a bidder signs a timestamped auction message using ECC ring signature ensuring anonymous and unlikable authentication.
2. HE enforces honest bid processing and bids confidentiality and preventing double bidding.
3. Batch verification ensures authenticate multiple bidder signature while confirming that no bidder has submitted multiple unauthorized signatures. It also reduces total verification time and ensures that signature have not been tampered with or forged, demonstrate the complete workflow of a privacy-preserving e-bidding process.
4. Security and performance evaluation includes tamper-resilience check, signature verification test and the result shows that the achieves high computational efficiency and secure bid processing for decentralized e-bidding applications.

2. Related works

Blockchain has emerged as a foundational technology for building decentralized, immutable and tamper-resistance that remove single points of trust and increase auditability. The immutable ledgers and smart contracts can automate auction logic and enforce transparent bidding rules but blockchain auctions expose sensitive bid information. To protect confidentiality, anonymity, many privacy-preserving techniques are designed with blockchain [5]. Timed Anonymous Ring Signature is applied to decentralized bidding system that is anti-collusion between the auctioneer and bidders. This system ensures anonymous bidding system disclose the winner's identity after the bid announcement, maintaining a transparent, fairness and decentralized bidding process [24].

A spontaneous privacy-preserving auction protocol allows a bidder to authenticate bid by generating a revocable ring signature. The auction manager by verifying this validity of the signature without knowing the bidder's identity [3].

During data sharing in the blockchain network, data could be accessed by intruders and the data could be misused by anyone. Using smart contracts to protect privacy during data sharing is very important. Ensuring security across all levels of the Ethereum blockchain poses a significant challenge. To address this, the implementation of public-private key cryptography can be employed to enhance privacy within Ethereum networks.

A blockchain-based data-sharing framework for a smart city environment that guarantees the confidentiality and secure processing of personal or critical user data. It operates user-defined Access Control List (ACL) rules embedded in smart contracts. Additionally, data owners are incentivized to share their data with stakeholders or third parties. The Privy Sharing approach aligns with key principles of the EU General Data Protection Regulation (GDPR), addressing aspects such as data asset sharing, accessibility, and purging in accordance with the data owner's explicit consent [12].

A secure and decentralized data sharing scheme built on blockchain is introduced to prioritize privacy, particularly in scenarios involving multiple entities interacting with smart contracts [16]. The scheme incorporates proxy re-encryption technology, ensuring that research institutions can decrypt shared intermediary ciphertext. This decryption process is facilitated by the use of semi-trusted proxy cloud servers, enhancing the privacy preserving capabilities of the system [23].

A data sharing framework effectively tackles the access control challenges associated with sensitive data stored in the cloud. A permissioned blockchain is employed, and the design encompasses to grant access to electronic medical records from a shared repository only after verifying the identities and cryptographic keys of data users/owners.

In the protocol, a data requester has the ability to search for specific keywords from a data provider, aiming to locate relevant EHRs on the consortium blockchain. Following data owner authorization, the requester obtains re-encryption ciphertext from the cloud server. The scheme primarily relies on searchable encryption and conditional proxy re-encryption to achieve a balance between data security, privacy preservation, and access control. Additionally, a proof of authorization is structured as the consensus mechanism for the consortium blockchain.

In large scale distributed systems like crowd-sensing, IoT and blockchain. It allows to verify large number of signatures to validate individually which leads inefficiency and computational overhead. Batch verification addresses the inefficiency and computational overhead allows multiple signatures to be verified simultaneously. The proposed linkable signature scheme addresses key challenges in mobile crowd-sensing by balancing identity anonymity with efficient verification. It introduces linkage tags and batch verification to significantly reduce verification overhead while preserving strong privacy guarantees.

The traditional single-sided spectrum action is no longer sufficient to meet the actual needs. So double spectrum auction where participants are composed of multiple sellers and buyers. The spectrum buyers and sellers, semi-honest agents are introduced to calculate the process bit information to determine the winning bidder and difficult to ensure the security and privacy of spectrum actions. Some of the double spectrum auction protocols address these concerns by providing secure bid submission, privacy-preserving winner determination and protection against collusion in e-bidding systems [19].

A secure double spectrum auction protocol is designed using Software Guard Extension (SGX) technology and paillier homomorphic encryption use encrypted bids combined with Pedersen

commitments and zero knowledge proofs to ensures public verifiability, confidentiality and protection against collusion in e-bidding systems [18]. A double spectrum auction server with SGX component and paillier cryptosystem, one-time ring signatures and stealth address technology to protect the private information of spectrum auctions. Multi-stage frameworks structure the process into registration, bidding, clearing and payment phases and double auction enable efficient matching of buyers and sellers for energy trading and resource allocation [14].

This scheme enhances e-auction security and privacy, an adaptive clustering and reputation-based validator selection improves scalability in clustered blockchain consensus mechanism and secure auction execution through encrypted bid submission, quorum-based winner determination and timestamp-driven integrity checks [7]. IoT data sharing through the distributed consensus-based approach designed to work among bidders in the auction context which enforces privacy preserving, incentive compatibility and collusion resistance with improved data sharing efficiency and scalability [4].

The proposed sealed-bid auction protocol that executes sensitive bidding on a Trusted Execution Environment (TEE) backed confidential blockchain. Bidders commit funds to secure enclave generated escrow address, ensuring confidentiality and binding commitments. The confidential chain computes the winner through verifiable off-chain computation. Bulletproof zero-knowledge proofs and Pedersen commitments protect the bid information leakage and improve the efficiency of bid transactions without trusted third party. A Big Data System (BDS) is designed to collect, manage and analyse bidding related data to ensure fair transaction and improve bidding efficiency of the bidding process [26].

[11, 24] Replace traditional databases and process bidding logic replaced by a decentralized e-bidding system where graph-isomorphism based zero-knowledge proofs strengthen privacy by ensuring participant anonymity and secure data transmission and verifiable records

Existing batch verification schemes that generating proofs only after collecting valid signature. This Batch ECDSA transaction verification scheme verified all the signature at the beginning of the protocol to balance between the verification time and proof size, and optimizing proof generation efficiency using incremental verifiable computations and it reduces the overall block validation time [15].

In Traditional verification methods must handle each proof individually to make them computationally expensive and inefficient when verifying large numbers of statement. The key challenge is to securely combine verifiable delay function of multiple PoE statements into fewer testaments while preserving cryptographic security and improving efficiency for both prover and verifier [16]

The problem of the high transaction costs associated with executing smart contracts on the Ethereum blockchain were addressed by iBatch system operates by combining multiple user requests into batches that are processed together and distributing the fixed transaction overhead costs across invocations. The iBatch achieves substantial cost reductions to save 14.6% to 59.1% of gas cost per invocation with a 2-minute delay and 19.06% to 31.52% ether cost per invocation with a delay of 0.26 to 1.66 blocks [17].

The proposed system addresses the batch generation of message-independent PR signatures that support fully non-interactive online signing. The PR signatures are generated offline at about 1.3ms each and final signatures are generated under 100 ms. By relying on an honest-majority settings the protocol preserves strong active security and optimizes cryptographic operations for scalability. This solution provides low latency and high throughput making it practical for deployment in key management networks [18].

The two-parameter elliptic curve digital signature algorithm and KGLP algorithm optimizations and batch verification combining to achieves over 50% performance improvement in security and cryptographic integrity. This scheme enhances transaction processing capacity without compromising security properties of decentralized ledger systems [13]. P2BA a privacy-preserving protocol with batch authentication designed to efficiently authenticate messages against semi trusted road units (RSUs) while significantly enhancing privacy and reducing computational overhead in vehicular Ad-Hoc networks. This approach based on bilinear and non-interactive zero-knowledge proofs mechanism allows the RSU to verify the legitimacy of this blinded certificate without need it to be unblinded.

3. Preliminaries

3.1 Elliptic Curve Cryptography (ECC)

An elliptic curve over a prime field F_q where p is a large prime number. F_q is defined by the equation

$y^2 = x^3 + ax + b(modq)$

$4a^3 + 27b^2 \ \# 0 \ (mod\ q)$

where a and b are constants $a, b, x, y \in F_q. Point\ P(x_1, y_1)$ and $Q(x_2, y_2) \in E_q(a, b)$ on this curve satisfy the elliptic curve equation. The negative of a point $P(x, y)$ is $Q(x, -y)$. A line passing through P and Q intersects the elliptic curve at a third point $R'(x_3, y_3)$ symmetric about the x-axis. The sum $P + Q = R(x_3, y_3)$. The point ∞ called the point of infinity forms an additive cyclic group. The Security of ECC-based cryptographic protocol based on Elliptic Curve Discrete Logarithm Problem (ECDLP). ECDLP involves finding a scalar k such that $Q = kP$, where P and Q are generator points on an elliptic curve. This problem is challenging and forms the foundation for the security of ECC due to its computational complexity.

3.2 Paillier homomorphic encryption

Key Generation

1. Compute the security parameter $n = p.q$. Randomly choose two large prime numbers p and q by selecting the least common multiple of each minus 1.

$\lambda = lcm(p-1)(q-1)$ where$p, q \in 1$

2. Randomly Choose integer i. where$i \in Z^*_{n^2}$. Ensure an order that can be divided by i.

$gcd\left(i^{\lambda} mod n^2, n\right) = 1,$

3. Compute $\mu = \left(L\left(i^{\lambda} mod\ n^2\right)\right)^{-1}$ mod n.

4. Public and private key are $pk = (n, i), sk = (\lambda, \mu)$ respectively.

Encryption

1. Let *m* be message to be encrypted such that $m \in Z^*_n$

2. Choose random integer r such that $1 \leq r < n$ and $gcd(r, n) = 1$.

3. Compute Cipher text$C = i^m . r^n mod n^2$

Decryption

1. Compute $L(u) = u - 1/n$ where $u = i^{\lambda} mod n^2$.

2. Compute message $m = L\ (C^{\lambda}\ mod\ n^2)\ \mu\ mod\ n.$

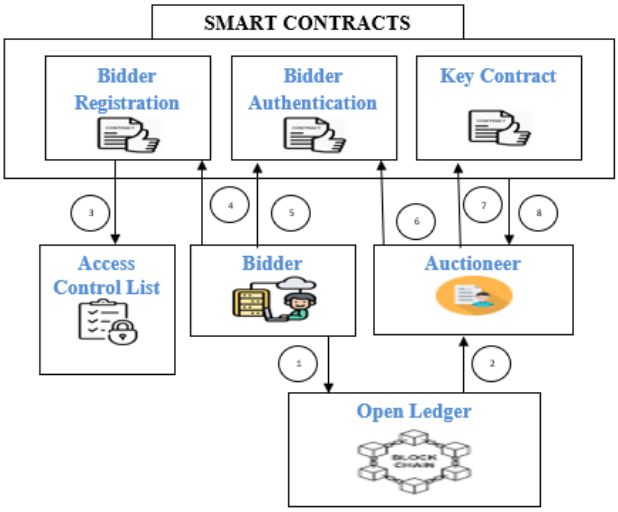

Figure 1. Architecture diagram for ERSPBV model

4. Proposed methodology

The proposed model Privacy-Preserving Enhanced Ring signature with Paillier based on Batch Verification for secure E-bidding (ERSPBV) mainly focuses on e-bidding privacy and anonymous bid submission in the permissionless blockchain. In this model, all auction transactions on the open ledger remains transparent but sensitive bidding information is encrypted data and anonymized before being shared. The bids uploaded by bidders are protected using ECC combined with ring signatures to guarantee bidder anonymity and strong, while Paillier Homomorphic Encryption enables privacy-preserving comparison and secure aggregation of encrypted bid values. The encrypted data is accessible only to authorized auctioneers through smart contracts can access or compute on the encrypted bids. Smart contracts that eliminate manual intervention and prevent tampering, unauthorized access, and bid manipulation. During the batch verification, random coefficients are derived from a publicly verifiable randomness beacon to eliminate any adversarial bias in batch aggregation. This model contains four main entities are Open Ledger, Bidder, Auctioneer, and Access Control List which are managed through three smart contracts namely Bidder Authentication, Bidder Registration and Key contract. The bidder and auctioneer interact with each other through the smart contracts to achieve privacy and fairness fine-grained access control during the bidding process.

Bidder (BD) – The bidder encrypts private data using ECC ring signature based Paillier homomorphic encryption algorithm and shared encrypted bid to open ledge in the permissionless blockchain network. Bidder has full control over the private bidding information, preventing unauthorized bidders, no third party cannot access or tamper with the bid. Ring signature ensures bidder anonymity and preventing any third party or auctioneer linking the bid from its origin.

Auctioneer (AC) – A smart contract to provide data for authorized auctioneer to secure access and process encrypted bids. Auctioneer performs computations such as finding the higher bid or verifying minimum bid requirements without revealing any individual bid values through Homomorphic encryption.

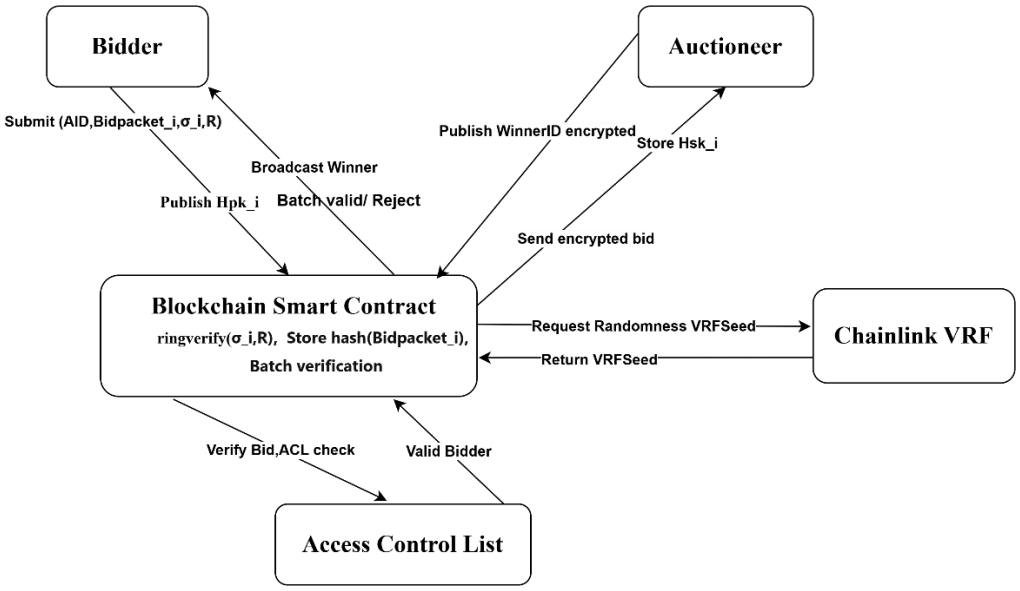

Figure 2. Workflow diagram for enhanced ring signature with paillier based on batch verification for secure e-bidding model

Access Control List (ACL) – The data bidder includes the addresses of authorized auctioneers in a list within a smart contract. Only those bidders whose addresses are on the list are permitted to request access computation on the encrypted bids. Access to the data is restricted for bidders whose addresses are not included in this list.

Bidder Registration smart contract – This contract is executed by the bidder is used to add, delete and check authorized auctioneer addresses from the ACL.

Bidder Authentication smart contract – This contract between the bidders and auctioneers itself. Auctioneers use this contract to request access computation only for authorized auctioneer.

Key Contract - This contract is executed between the bidder itself and auctioneer. Bidder uses this contract to issue a computational output to the authorized auctioneer securely.

The corresponding description for each step number in figure1 is provided below.

1. Bidder encrypted private bid value using ECC and PHE and signs the upload with a ring signature before embedded into an Ethereum transaction.
2. Auctioneer wants to access the encrypted bids shared by the bidders.
3. Bidder Registration smart contract is used to add, delete and check authorized auctioneer addresses from the ACL.
4. Bidder deploys a bidder registration smart contract.
5. Bidder deploys a bidder authentication smart contract.
6. Auctioneer checks their address in the ACL using bidder authentication smart contract.
7. Auctioneer uses this smart contract to request for an aggregated computation from the bidder.
8. Bidder uses this key contract to issue an encrypted computation output to the authorized auctioneer. Fig. 2 shows the step-by-step process of workflow for Enhanced Ring Signature with Paillier based on Batch Verification E-bidding Model.

Algorithm 1: Enhanced Ring Signature with Paillier based on Batch Verification for secure E-bidding (ERSPBV)

Input: a security parameter λ
global par = (q, G, H_0, H_1, H_2)

1. Number of ring members = n
2. for all $_{generate}$ the public key and private key do
3. calculate $keyGen(par) \rightarrow (pk_i, sk_i)$
4. end for
5. for all generate the public key and private key do
6. calculate $keyGen(\lambda) \rightarrow (Hpk_i, Hsk_i)$
7. Publish Hpk_i on-chain
8. Store Hsk_i off-chain with auctioneer
9. End for
10. Bidder B_i chooses bid value b_i
11. ECC encrypt the bid: select random r $\in Z_q$

$C_1 = r * G \quad C_2 = b_i + r * pk_i \quad cECC = (C_1, C_2)$

12. HE encrypts the bid for on-chain aggregation $cHE = HE.Encrypt(Hpk, b_i)$
13. Bidder selects ring $R = \{pk_1, pk_2 \dots \dots . pk_n\}$
14. Call chain-link VRF grt VRF ()→VRFseed

$a_i = H_0(VRFseed||\text{a}||i)$
$b_i = H_0(VRFseed||\text{b}||i)$
$c_i = H_0(VRFseed||\text{c}||i)$

15. Generate a ring signature, s be actual bidder index
    Transaction initiator starts signing and then calculate
16. if i # s $L_i = a_i * G + (b_i + c_i)pk_i$
    $R_i = a_i * H_0(pk_i) + (b_i + c_i)I_s$
17. if i = s $L_i = (a_i + b_i)G$
    $R_i = (a_i + c_i) * H_0(pk_i)$
18. Randomly select r$\in Z_q$*and then calculate challenge hash as follows
19. $h = H_2(AID||VRFseed||Bidpacket_i||r)$
20. Compute final challenge values
21. $C_i = \text{H}_1(\text{AID}\ ||VRFseed||\ \text{h}, \text{L}_1, \dots, \text{L}_\text{n}, \text{R}_1, \dots, \text{R}_\text{n}) - \sum_{i=1}^{n} c_j$
22. Compute response values $d_i = \left(\frac{a_i}{a_i + b_i}\right) - C_i * sk_i$
23. Ring signature output $\sigma_i = \{C_1, \dots . C_n, d_1, \dots d_n\}$

//Bid submittion to smart contract

24. $Submit(AID, Bidpaccket_i, \sigma_i, R)$
25. $UAC\ verifies\ B_i \in ACL$
26. Smart contract executes ring verify $((\sigma_i, R)$
27. Smart contract collects all submitted ring signatures $\Sigma = \{\sigma_1, \sigma_2, \dots \dots \dots \sigma_m\}$
28. VRFseed_onchain=ChainlinkVRF.getRandomness()
29. For each $\sigma_j \in \Sigma$

$$\sigma_j = uint256(Keccak256\left(abi.encode\left(VRFseed||\text{"alpha"}||\ \text{uuint32(j)}||bidhash_j\right)\right))\%q$$

30. End for
31. For each $\sigma_j \in \Sigma$
32. Check $\gamma_\text{i} = d_i * G + C_i * pk_i$
33. Chek $\delta_\text{i} = d_i * H_0(pk_i) + C_i * I_s$

34. Aggregate using random coefficients $\alpha_j \in Z_q^*$
35. U= $\Sigma\alpha_j * \Sigma\gamma_i$
36. V= $\Sigma\alpha_j * \Sigma\delta_i$
37. Csum= $\Sigma\alpha_j * \Sigma C_i$
38. If Ccheck==Csum:
39. Batch valid
40. Else: reject batch
41. Store hash ($Bidpacket_i$) on blockchain
42. Auctioneer aggregates encrypted bids $total = \Sigma CHE_i$
43. Auctioneer decrypts sum using $Hsk\ totalbid = HE.Decrypt(Hsk, total)$
44. Compare encrypted bids using PHE operators
45. Auctioneer determines winner w securely

Publish winner ID, winner encrypted bid, proof of correctness

46. End for

Algorithm 2: Bidder Registration Smart contract

```
Input: Bidder Address u
Output: True or False
// Function to Register a new bidder
1.  function register bidder(u):
2.  if msg. sender! =auctioneer then
3.  reject ("Only auctioneer can register bidders")
4.  end
5.  if u not in ACL, then
6.  ACL[u]. status=active
7.  emit bidder registered(u)
8.  else
9.  emit bidderalreadyexists(u)
10. end
// Function to Deactivate a bidder
11. function deactivate bidder(u):
12. if msg. sender!= auctioneer then
13. reject("unauthorized")
14. end
15. ACL[u]. status=inactive
16. emit bidder deactivated(u)
// Function to check registration status
17.   function is Registered(u)
18.   if ACL[u]. status==active then
19.   return true
20.   else
21.   return false
22.   end
```

In our work, the proposed model consists of three smart contract algorithms given below.

Algorithm 2 smart contract provide a secure bidder registration process by validating eligibility that preventing unauthorized registration and double registration in the bidder list. All actions such

Algorithm 3: Bidder Authentication Smart contract

```
Input: bidder Address u, signature σ
Output: True or False
// Function to Verify bidder Authentication
1. function authenticate (u, σ):
2. if ACL[u]. status! =active then
 return false
3. end
4. if verify signature (u, σ) == true then
5. emit bidder authenticated(u)
6. return true
7. else
8. return false
9. end
```

Algorithm 4: Key Contract

```
Input: auctioneer address a, bidder address b
Output: keyrequesttoken
// Function for Autioneer requests computation output
1. function request key(b):
2. if authentication contract. is Authenticated(a) == false then
3. reject ("Autioneer not authorized")
4. end
5. keyrequesttoken = hash (a, b, timestamp)
6. emit key request (a, b, keyrequesttoken)
7. return keyrequesttoken
// Function: Bidder submits encrypted result
8. function submitencryptedoutput (A, keyrequesttoken, encrypted output):
9. if authentication contract. is Authenticated(a) == false then
10. reject ("Bidder not authorized")
11. end
12. store encrypted output under kdyrequesttoken
13. emit encrypted output submitted (b, a)
```

as adding a bidder, updating their status and verifying their identity is automatically recorded through transparent event logs throughout the e-bidding process.

Algorithm 3 authentication smart contract relies on secure digital signature verification to ensure the request is genuine. The process returns only the result without reveal any keys, thereby maintaining confidentiality and also check the bidder's active status in the ACL before granting access. Maintaining stronger security while preserving bidder anonymity throughout the e-bidding process.

Algorithm 4 Key smart contract issues a key request token, the bidder can respond securely through off-chain encryption mechanism, private keys never exposed on-chain. Since no keys are stored or shared on the blockchain that remains secure and resistant to key exposure threats.

5. Correctness analysis

The proposed privacy preserving Enhanced ring signature with Paillier based on Batch Verification E-bidding using Chain link VRF-derived randomness correctness analysis of bid encryption and correctness of ring signature formation and correctness of single verification and correctness of batch verification.

Bid Encryption correctness

ECC encryption is computed as

$$C_1 = r * G \qquad C_2 = b_i + r * pk_i \tag{1}$$

Decryption by the auctioneer retrieves

$$\begin{aligned} C_2 - sk_i C_1 &= (b_i + r * pk_i) - sk_i(rG) \\ &= (b_i + r * sk_i G) - sk_i(rG) \\ &= b_i + sk_i rG - sk_i rG \\ &= b_i \end{aligned} \tag{2}$$

This proves that ECC decryption correctly recovers the original bid value b_i.

Ring signature Correctness

Ring signature correctness ensures that the actual bidder s is hidden inside the ring $R = \{pk_1, pk_2 \dots \dots . pk_n\}$ but verification still succeeds. For each ring member i generates

$$\begin{aligned} a_i &= H_0(VRFseed||\mathrm{a}||i) \\ b_i &= H_0(VRFseed||\mathrm{b}||i) \\ c_i &= H_0(VRFseed||\mathrm{c}||i) \end{aligned} \tag{3}$$

For non-signer i # s $L_i = a_i * G + (b_i + c_i)pk_i$

$$R_i = a_i * H_0(pk_i) + (b_i + c_i)I_s \tag{4}$$

For the actual bidder $L_i = (a_s + b_s)G$

$$R_i = (a_s + c_s) * H_0(pk_s) \tag{5}$$

The challenge value is constructed as $h = H_2(AID||VRFseed||Bidpacket_i||r)$

$$C_i = \mathrm{H_1(AID}\,||VRFseed||\,\mathrm{h, L_1, \dots, L_n, R_1, \dots, R_n}) - \sum_{i=1}^{n} c_j \tag{6}$$

$$\text{Compute response values } d_i = \left(\frac{a_i}{a_i + b_i}\right) - C_i * sk_i \tag{7}$$

Correctness holds because substituting d_i reconstructs $L_i$and R_i during verification

Correctness of single verification

The smart contract recomputes

$$\gamma_{\mathrm{i}} = d_i * G + C_i * pk_i \tag{8}$$

$$\delta_{\mathrm{i}} = d_i * H_0(pk_i) + C_i * I_s \tag{9}$$

Substitute d_i in Eq. (8)

$$\gamma_{\mathrm{i}} = \left(\frac{a_i}{a_i + b_i} - C_i * sk_i\right) G + C_i * sk_i * G \tag{10}$$

$$\gamma_{\mathrm{i}} = \left(\frac{a_i}{a_i + b_i}\right) G$$

Substitute d_i in Eq. (9)

$$\begin{gathered}
\delta_{\mathrm{i}} = \left(\frac{a_i}{a_i+b_i} - C_i * sk_i\right) * H_0(pk_i) + C_i * I_s \\
\delta_{\mathrm{i}} = \left(\frac{a_i}{a_i+b_i} H_0(pk_i)\right) - C_i * sk_i * H_0(pk_i) + C_i * I_s \\
I_s = sk_i * H_0(pk_i) \\
\delta_{\mathrm{i}} = \left(\frac{a_i}{a_i+b_i} H_0(pk_i)\right) - C_i * sk_i * H_0(pk_i) + C_i * sk_i * H_0(pk_i) \\
\delta_{\mathrm{i}} = \left(\frac{a_i}{a_i+b_i} H_0(pk_i)\right)
\end{gathered} \tag{11}$$

Thus, the single verification is always correct for honest signatures.

d) Correctness of Batch Verification

Batch verification aggregates multiple signatures $\Sigma = \{\sigma_1, \sigma_2, \ldots\ldots\sigma_m\}$ to reduce on-chain computation

$$\gamma_{j,i} = d_{j,i} * G + C_{j,i} * pk_i \tag{12}$$

$$\delta_{j,i} = d_{j,i} * H_0(pk_i) + C_{j,i} * I_s \tag{13}$$

Aggregate using random coefficients $\alpha_j \in \mathrm{Z}_{\mathrm{q}}^*$

$$U = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} \gamma_{j,i} \tag{14}$$

Substitute $\gamma_{j,i}$ in Eq. (14)

$$U = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} d_{j,i} * G + C_{j,i} * pk_i = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} d_{j,i} * G + \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} C_{j,i} * pk_i \tag{15}$$

$$V = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} \delta_{j,i} \tag{16}$$

Substitute $\delta_{j,i}$ in Eq. (16)

$$\begin{gathered}
V = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} d_{j,i} * H_0(pk_i) + C_{j,i} * I_s \\
= \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} d_{j,i} * H_0(pk_i) + \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} C_{j,i} * I_s \quad (n-1)
\end{gathered} \tag{17}$$

```
Bids: [408, 257, 35, 309, 382, 491, 98, 481, 97, 73]
Batch Verify OK: True
HE total: 2631
Winner: 5  Bid: 491
```

Figure 3. Output for ERSPBV

Table 1. Copper parameters and their values

Ring Size	No. of Bidders	Sign Generation	Single Verification	Batch
Verification		Time (ms)	Time (ms)	Time (ms)
10	10	12.4	1.3	0.7
30	30	37.5	3.9	1.5
50	50	63.1	6.5	3.8
100	100	124.9	13	6.7
500	500	624	65	27.4

Table 2. Ring Size > No. of Bidders

Ring Size	No. of Bidders	Sign Generation	Single Verification	Batch
Verification		Time (ms)	Time (ms)	Time (ms)
10	5	5.2	7.8	4.0
30	10	15.6	22.4	10.2
50	20	26.1	37.8	16.9
100	30	52.4	75.1	32.5
500	100	262.0	375.4	148.7

Aggregate challenges

$$Ccheck = Csum = \sum_{j=1}^{m} \alpha_j \sum_{i=1}^{n} C_{j,i} \tag{18}$$

Therefor the batch verification is valid

6. Performance analysis

6.1 Experimental setup

The experimental evaluation of the proposed a secure and privacy-preserving ERSPBV for cryptographic operations the secp256k1 elliptic curve for ring signature generation and verification while Paillier Homomorphic Encryption with a 2048-bit key size for secure bid aggregation and comparison. Chain link VRF ensuring unbiased and tamper-proof randomness for batch verification. All experiments were executed on a system equipped with an intel core i5 processor and 16GB of RAM, providing sufficient computational power to accurately measure signature generation and verification time. The evaluation focus on computational cost, Communication overhead, On-chain gas usage and verification accuracy. Fig. 3 shows that all submitted signatures verifies in a

Table 3. Ring Size < No. of Bidders

Ring Size	No. of Bidders	Sign Generation	Single Verification	Batch
Verification		Time (ms)	Time (ms)	Time (ms)
10	20	4.8	6.4	4.1
30	40	14.5	18.2	10.7
50	55	23.9	31.3	16.1
100	120	43.8	62.5	29.4
500	550	238.4	310.2	147.8

Table 4. Smart contract cost test

Smar Contract	Gas used	Actual Cost (ether)	USD
Bidder Registration	85,000	0.00000255	0.00817
Bidder Authentication	70,000	0.00000205	0.00672
Key Contract	90,000	0.00000210	0.00867
Submit Batch Verification ()	140,000	0.0000042	0.0013
Challenge index ()	50,000	0.0000015	0.005
Submit Bid ()	80,000	0.0000024	0.0085
Request VRF for Batch ()	110,000	0.0000033	0.00105

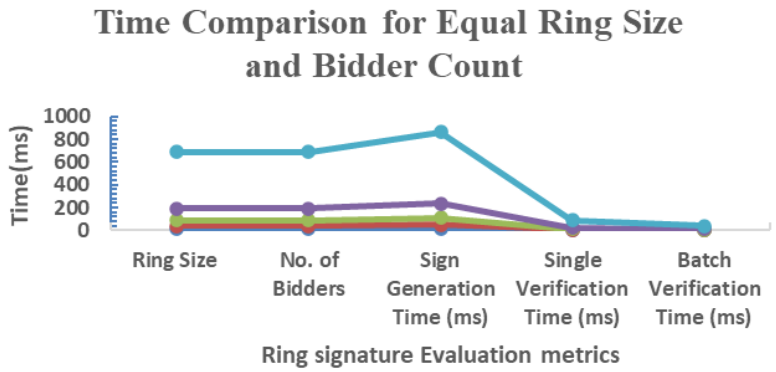

Figure 4. Time comparison for equal ring size and bidder count

single batch and confirming the integrity and authentication of all bids. PHE aggregation computes the encrypted total of all bids as 2631 without revealing the individual bits. The accurate winner selection of highest bid is calculated as 491 to bidder 5 under privacy-preserving and verifiable e-bidding.

6.2 Performance comparison for ring signature e-bidding operations

The comparative evaluation contains three metrics sign Generation time, single verification time, Batch verification which shows that the ring size is equals to the bidder count (Table 1) achieves optimal verification efficiency with moderate signing cost. Fig. 3 shows that sign generation time increases linearly with ring size to offers strong anonymity. The ring size greater

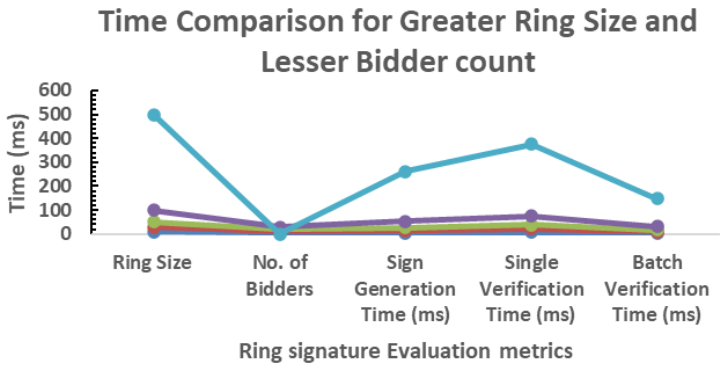

Figure 5. Time comparison for greater ring size and lesser bidder count

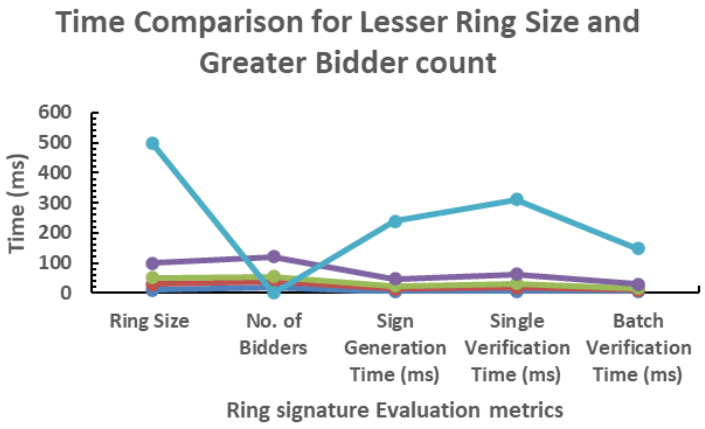

Figure 6. Time comparison for lesser ring size and greater bidder count

than the bidder count (Table 2) strengthen anonymity but significantly increasing verification overhead. Fig. 4 shows that single verification time also increases with ring size and shows a higher computational cost compared to equal-size scenario. The ring size lesser than the bidder count (Table 3) reduce verification but weaker anonymity guarantees but scalable. Fig. 5 shows that providing high performance and it is suitable for large-scale bidding where efficiency is prioritized. Table 4 show the smart contract test cost of Calculation used gas price =0.03gwei ETH= $3200.

Fig. 6 indicates signature generation and single verification time is moderate but batch verification is very efficient compared to Fig. 7,8. Fig. 8 indicates maximum anonymity but poor performance and batch verification cost is heavy compared to Fig. 6-8 shows that signature generation time increases as then number of bidders grows moderately, single verification time rises sharply over 300ms for 550 bidders, batch verification remains faster that single verification even at the highest bidder count 550 but lower anonymity when the ring size is small. Therefore, selecting a ring size requires balancing anonymity requirements with computational efficiency depending on the auction scale and security threshold. Batch verification remains the most efficient among the three metrics significantly reduces overall verification cost by aggregating multiple signature verifications into a single batch process.

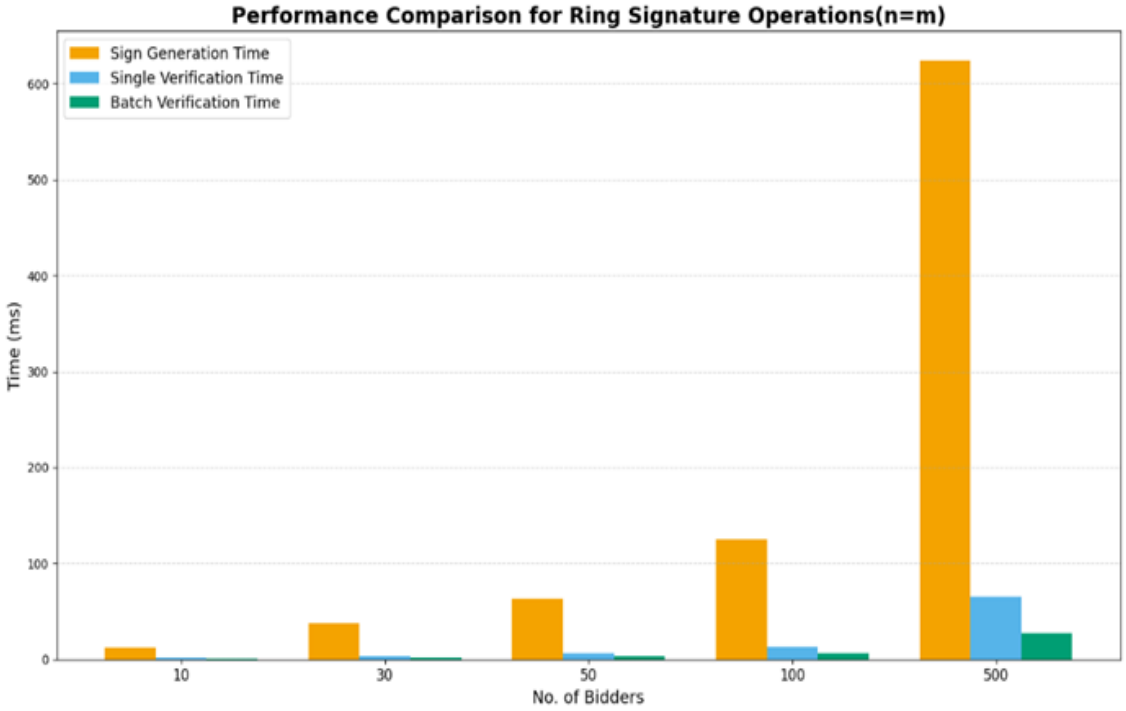

Figure 7. Performance comparison for ring signature operation (n=m)

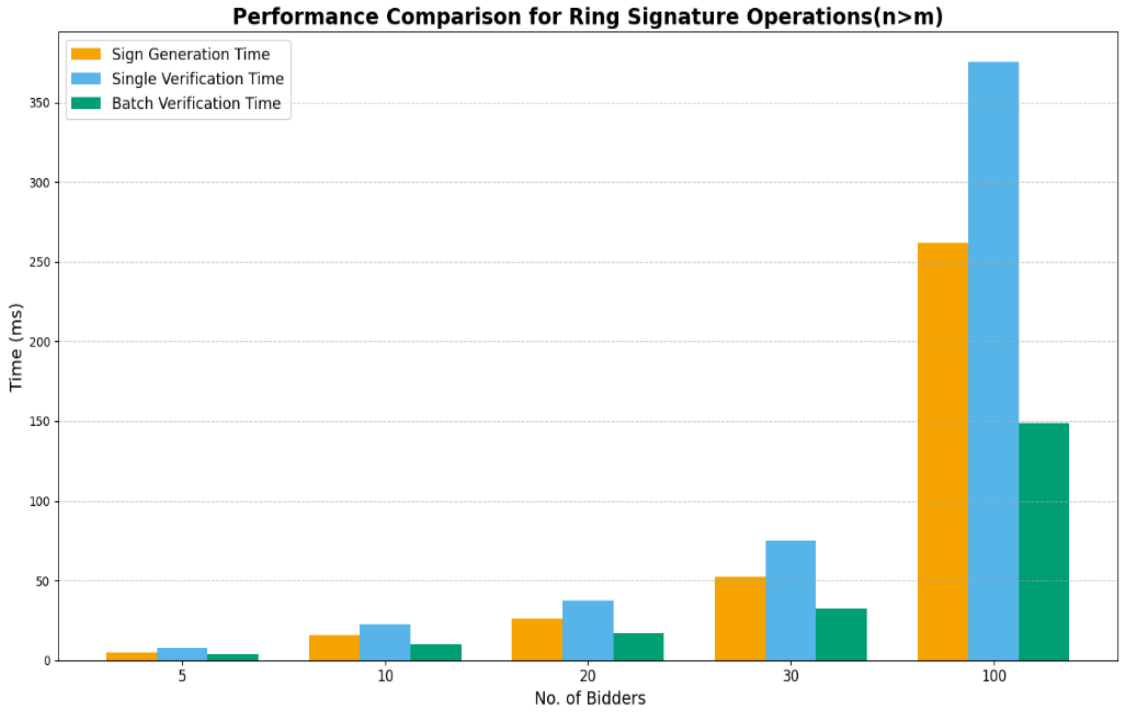

Figure 8. Performance comparison for ring signature operation (n>m)

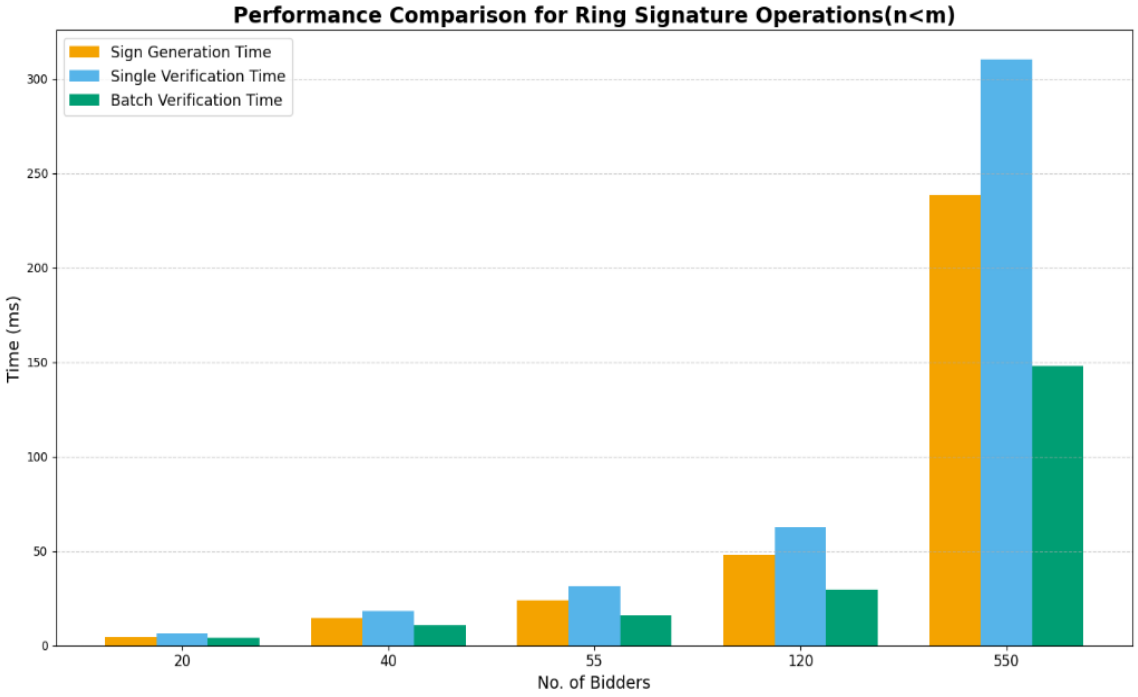

Figure 9. Performance comparison for ring signature operation (n<m)

7. Conclusions

Privacy-Preserving Enhanced Ring signature with Paillier based on Batch Verification for secure E-bidding (ERSPBV) which addresses the challenges of confidentiality, anonymity and secure verification in permissionless blockchain environment. The proposed system guarantees that bid values remain confidential while still allowing authorized auctioneers to verify and process them. Bidders encrypt and sign bids and auctioneers retrieve authorized computation output through dedicated and trustworthy mechanism of smart contracts that eliminates manual intervention and prevents tampering, unauthorized access, and bid manipulation. Experimental deployment on the Ethereum Sepolia test network demonstrates the integrated cryptographic mechanisms and smart contract operates with minimal overhead and high efficiency confirming the feasibility of the system and more suitable for decentralized e-bidding privacy-preserving blockchain applications.

References

1. Abdullahi, B., Ibrahim, Y.M., Ibrahim, A.D., Bala, K. (2022). Development of web-based e-tendering system for Nigerian public procuring entities. International Journal of Construction Management, 22(2), 278-291. https://doi.org/10.1080/15623599.2019.1620492
2. Diallo, N., Shi, W., Xu, L., Gao, Z., Chen, L., Lu, Y., Shah, N., Carranco, L., Le, T.C., Surez, A.B., Turner, G. (2018). EGov-DAO: A better government using blockchain based decentralized autonomous

organization. 2018 5th International Conference on eDemocracy and eGovernment (ICEDEG), 166-171. https://doi.org/10.1109/ICEDEG.2018.8372356
3. Feng, X., Shi, Q., Xie, Q., Wang, L. (2021). P2BA: A privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 16, 3888-3899. https://doi.org/10.1109/TIFS.2021.3098971
4. Gebele, J., Mutzel, T., Oez, B., Matthes, F. (2025). Cross-chain sealed-bid auctions using confidential compute blockchains. arXiv. https://doi.org/10.48550/arXiv.2510.19491
5. Huang, X., Zuo, C., Shao, J., Duan, J., Wang, W., Meng, Y., Wang, L. (2025). Timed anonymous ring signature with application to bidding systems. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2025.3581001
6. Inusah, Y., Kazaz, A., Ulubeyli, S. (2025). Barriers to e-tendering implementation in the construction industry: A comprehensive review and analysis of a decade and beyond. Sustainability, 17(5), Article 2052. https://doi.org/10.3390/su17052052
7. Jia, X., Song, X., Sohail, M. (2022). Effective consensus-based distributed auction scheme for secure data sharing in internet of things. Symmetry, 14(8), Article 1664. https://doi.org/10.3390/sym14081664
8. Katz, J., Urban, A. (2024). Honest-majority threshold ECDSA with batch generation of key-independent presignatures. Cryptology ePrint Archive. https://ia.cr/2024/2011
9. Li, H., Xue, W. (2021). A blockchain-based sealed-bid e-auction scheme with smart contract and zero-knowledge proof. Security and Communication Networks, 2021, Article 5523394. https://doi.org/10.1155/2021/5523394
10. Li, X., Jeon, G., Wang, W., Zhao, J. (2024). A linkable signature scheme supporting batch verification for privacy protection in crowd-sensing. Digital Communications and Networks, 10(3), 645-654. https://doi.org/10.1016/j.dcan.2023.02.015
11. Liu, L., Wei, P., Liu, S., Wang, Z., Hu, D., Kou, Z. (2026). Scalable batch verification of ECDSA for blockchain using IVC. Frontiers of Computer Science, 20(4), Article 2004803. https://doi.org/10.1007/s11704-025-41269-5
12. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, Article 101653. https://doi.org/10.1016/j.cose.2019.101653
13. Montanera, D., Mishra, A.N., Raghu, T.S. (2022). Mitigating risk selection in healthcare entitlement programs: A beneficiary-level competitive bidding approach. Information Systems Research, 33(4), 1221-1247. https://doi.org/10.1287/isre.2021.1062
14. Omar, I.A., Hasan, H.R., Jayaraman, R., Salah, K., Omar, M. (2021). Implementing decentralized auctions using blockchain smart contracts. Technological Forecasting and Social Change, 168, Article 120786. https://doi.org/10.1016/j.techfore.2021.120786
15. Rotem, L. (2021). Simple and efficient batch verification techniques for verifiable delay functions. In Theory of Cryptography Conference (pp. 382-414). Springer, Cham. https://doi.org/10.1007/978-3-030-90456-2_13
16. Shen, B., Guo, J., Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. Applied Sciences, 9(6), Article 1207. https://doi.org/10.3390/app9061207
17. Tso, R., Liu, Z.Y., Hsiao, J.H. (2019). Distributed e-voting and e-bidding systems based on smart contract. Electronics, 8(4), Article 422. https://doi.org/10.3390/electronics8040422
18. Vangujar, A.K., Umrani, A., Chin, J.J., Palmieri, P. (2025). Secure e-auctions: A blockchain-based cluster consensus. 2024 International Conference on Blockchain Computing and Applications (BCCA). https://doi.org/10.1109/BCCA62388.2024.10844472
19. Wang, D., Zhao, J., Mu, C. (2021). Research on blockchain-based e-bidding system. Applied Sciences, 11(9), Article 4011. https://doi.org/10.3390/app11094011
20. Wang, J., Lu, N., Cheng, Q., Zhou, L., Shi, W. (2021). A secure spectrum auction scheme without the trusted party based on the smart contract. Digital Communications and Networks, 7(2), 223-234. https://doi.org/10.1016/j.dcan.2020.06.004
21. Wang, Y., Zhang, Q., Li, K., Tang, Y., Chen, J., Luo, X., Chen, T. (2021). iBatch: Saving Ethereum

fees via secure and cost-effective batching of smart-contract invocations. Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 566-577. https://doi.org/10.1145/3468264.3468568

22. Wu, G., Zhou, J., Fu, X. (2025). Improved blockchain-based ECDSA batch verification scheme. Frontiers in Blockchain, 8, Article 1495984. https://doi.org/10.3389/fbloc.2025.1495984
23. Xia, Q., Sifah, E.B., Asamoah, J.K.O., Du, X., Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers. IEEE Access, 5, 14757-14767. https://doi.org/10.1109/ACCESS.2017.2730843
24. Xiong, H., Chen, Z., Li, F. (2012). Bidder-anonymous English auction protocol based on revocable ring signature. Expert Systems with Applications, 39(8), 7062-7066. https://doi.org/10.1016/j.eswa.2012.01.034
25. Xiong, H., Jin, C., Alazab, M., Yeh, K.H., Wang, H., Gadekallu, T.R., Su, C. (2021). On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT. IEEE Journal of Biomedical and Health Informatics, 26(5), 1977-1986. https://doi.org/10.1109/JBHI.2021.3112693
26. Xu, D., Yang, Q. (2022). The systems approach and design path of electronic bidding systems based on blockchain technology. Electronics, 11(21), Article 3501. https://doi.org/10.3390/electronics11213501