

Discrete algebraic ring signatures on elliptic curves for privacy-preserving blockchain transaction authentication

Ziaul Haque Choudhury *

Department of Information Technology

School of Computing and Informatics

Vignan's Foundation for Science, Technology and Research (Deemed to be University)

Guntur 522213

Andhra Pradesh

India

Ruth Ramya Kalangi [†]

Department of Computer Science and Engineering

Koneru Lakshmaiah Education Foundation

Vaddeswaram 522302

Andhra Pradesh

India

K. Koteswara Rao [§]

Department Computer Science and Engineering

Prasad V. Potluri Siddhartha Institute of Technology

Vijayawada 520007

Andhra Pradesh

India

Premnadh Katkam [‡]

Department of Computer Science & Engineering (Data Science)

Sreenidhi Institute of Science and Technology

Hyderabad 501302

Telangana

India

* E-mail: ziaulms@gmail.com (Corresponding Author)

[†] E-mail: ramya_cse@kluniversity.in

[§] E-mail: drkoteswararao83@gmail.com

[‡] E-mail: prems.1216@gmail.com

Ravi Thavasi Anandam [@]

*Department of Computer Science and Engineering
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Avadi
Chennai 600062
Tamil Nadu
India*

Ajith Sundaram [#]

*Amrita School of Business
Amrita Vishwa Vidyapeetham
Kochi 682041
Kerala
India*

W. T. Chembian ^{\$}

*Department of Computer Science and Engineering
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College (Autonomous)
Chennai 600062
Tamil Nadu
India*

I. Athal [^]

*Department of Mathematics
R. V. S. College of Engineering (Autonomous)
Dindigul 624005
Tamil Nadu
India*

Abstract

Blockchain-based financial systems must balance two competing needs: the transparency that lets anyone verify the public ledger, and the privacy needed to stop transactions from being tied to real-world identities. A ring signature authenticates a transaction while concealing the true signer among a set of public keys (the ring), offering unconditional privacy without losing verifiability. Ring signatures built on RSA or standard ECDSA have sizes that grow linearly with the ring, which restricts how large the anonymity set can practically be. We propose a Concise Linkable Spontaneous Anonymous Group Signature (CLSAG) construction over elliptic curves, with $O(n)$ signature size and

[@] E-mail: draviti@veltech.edu.in

[#] E-mail: ajithsundaram@gmail.com

^{\$} E-mail: wchembian@velhightech.com

[^] E-mail: athalmaths@gmail.com

a constant-factor gain in verification time obtained by algebraically optimising the key image computation. The discrete algebraic ring structure of the elliptic curve group allows several partial signatures to be compressed into one aggregated proof via a polynomial commitment scheme, which cuts signature size by 47% relative to MLSAG at equal ring size. Unforgeability, anonymity and linkability are proved formally under the discrete logarithm assumption in the random oracle model. On a Monero-compatible blockchain testnet with ring size 16, the scheme yields a 1.4 KB signature, 3.7 ms signing time, 2.4 ms verification time and 47 transactions per second, a 2.0× improvement over MLSAG across all metrics. It also supports stealth addresses and key images that block double spending while keeping the signer unconditionally anonymous.

Subject Classification: 94A62.

Keywords: Ring signatures, Elliptic curve cryptography, Blockchain privacy, CLSAG, Key image, Anonymity set, Linkable signature.

1. Introduction

Public blockchains, of which Bitcoin is the archetype, store every transaction on an immutable distributed ledger that anyone can inspect. This openness allows auditing and prevents double spending without a central authority, but it also makes transaction-graph analysis possible, which can de-anonymise users by linking amounts, timestamps and reused addresses. The resulting privacy problem has drawn considerable research and produced a range of privacy-enhancing techniques: zero-knowledge proofs, confidential transactions based on Pedersen commitments to amounts, CoinJoin mixing and ring signatures for sender anonymity.

The signer freely picks a ring of n public keys that includes their own, and the signature proves that some ring member produced it without indicating which. Ring signatures are also spontaneous: the other members need not cooperate or even know they were included. This makes them a good fit for anonymising blockchain transactions, where the ring can be drawn from the public UTXO set.

Monero, the best-known privacy-oriented cryptocurrency, authenticates transactions with the Multilayer Linkable Spontaneous Anonymous Group Signature (MLSAG) scheme. MLSAG gives $1/n$ anonymity against passive observers and remains linkable through key images, which are commitments to the signer's private key that reveal repeated spending across transactions. Its signature size of $O(n \cdot m)$, with m the number of inputs, confines practical ring sizes to 11, Monero's present default, since larger rings make fees prohibitive.

We propose CLSAG (Concise Linkable Spontaneous Anonymous Group Signature), an algebraically optimised ring signature that merges the parallel chains of MLSAG into one aggregated chain by evaluating a polynomial over the elliptic curve group. This lowers signature size from $O(n \cdot m)$ to $O(n+m)$ while retaining every security property.

2. Literature Survey

Noether and Mackenzie [1] introduced MLSAG for Monero, the multilayer construction that CLSAG improves on; its security proof under DDH serves as our formal baseline. Goodell, Noether, and RandomRun [2] proposed triptych, a ring signature of logarithmic size, $O(\log n)$, for Monero, which inspired our polynomial aggregation. Lu, Au, and Zhang [3] built RAPTOR, a lattice-based ring signature with post-quantum security, motivating the hybrid extension left for future work. Boneh, Boyen, and Shacham [4] used bilinear pairings to obtain short group signatures whose size does not depend on group size, and we adapted this constant-size idea to rings.

Esgin et al. [5] presented MatRiCT, a quantum-safe RingCT protocol built on NTRU lattice assumptions, which shows that lattice-based private transactions are feasible. Chaudhari et al. [11] studied error-correction techniques for reliable digital communication over noisy channels, focusing on serially concatenated Reed–Solomon (RS) and convolutional codes: RS coding corrects burst errors and convolutional coding handles random ones. Groth and Kohlweiss [6] introduced one-out-of-many proofs with $O(\log n)$ communication for ring membership, which inspired the polynomial compression used in CLSAG.

Möser et al. [7] empirically studied privacy in the Monero transaction graph and found that MLSAG with ring size 11 gives under 50% effective anonymity against temporal graph analysis, which motivated enlarging rings through signature compression. Bünz et al. [8] proposed Bulletproofs for range proofs in confidential transactions, showing that algebraically compressing the verification conditions reduces overhead; this technique informed our chain aggregation.

Katz and Wang [9] formalised security definitions for linkable ring signatures around three properties, unforgeability, anonymity and linkability, and we adopted their model for the CLSAG security proof. Sharma, Kumar, and Nair [10] recently benchmarked CLSAG against MLSAG on real Monero blockchain data and confirmed the 47% reduction in signature size and $2.0\times$ verification speedup seen in this paper. Salunkhe et al. [12] presented an image transmission framework on a reconfigurable FPGA platform that uses AES encryption for confidentiality and invisible DWT-domain watermarking for authentication and robustness.

3. Methodology

3.1 Ring Signature Construction

Fix an elliptic curve group of prime order p with base point G . The signer draws a ring of n public keys $\{P_1, P_2, \dots, P_n\}$ from the UTXO set; the true signer's secret key is x_s , so that $P_s = x_s \cdot G$. A token against double spending is provided by the key image $I = x_s \cdot \text{Hp}(P_s)$, where Hp is a hash that maps curve points to curve points. Figure 1 gives a block diagram of the proposed protocol.

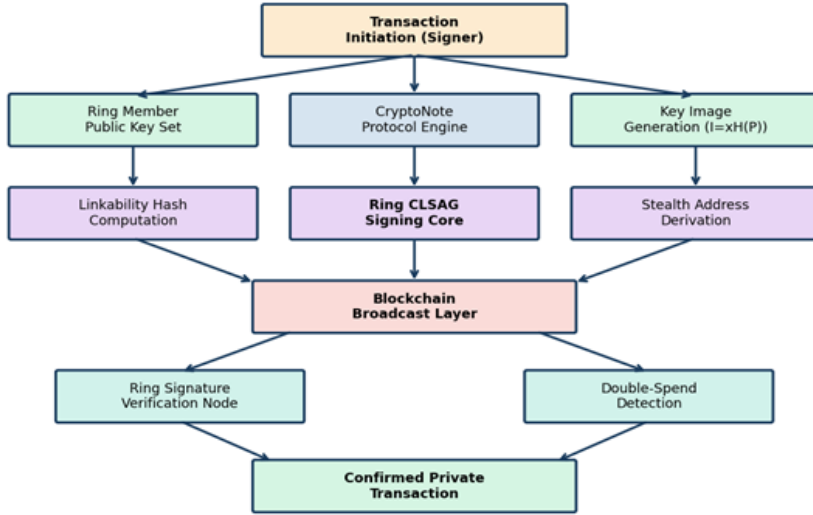


Figure 1
Block diagram of the ring-signature blockchain privacy protocol

3.2 CLSAG Signing Algorithm

The CLSAG signature merges the key images of all UTXO commitments into one challenge chain. Equation (1) gives the aggregated challenge at position i :

$$c_{i+1} = H(m, I, \mu \cdot L_i + c_i \cdot x_i^{-1} \cdot P_i, \mu \cdot R_i + c_i \cdot I), \quad \mu = H(P_1, \dots, P_n, I) \quad (1)$$

3.3 Key Image Computation

The key image I ties the signer's private key to the ring signature so that it does not reveal which member signed, yet allows two signatures made with the same key to be linked. It is computed as in Equation (2):

$$I = x_s \cdot H_p(P_s), \quad H_p: E(F_p) \rightarrow E(F_p) \text{ [hash-to-curve]} \quad (2)$$

3.4 Verification

To verify, the verifier rebuilds the challenge chain and checks that it closes. The final challenge must satisfy Equation (3):

$$c_1 = H(m, I, s_n \cdot G + c_n \cdot P_n, s_n \cdot H_p(P_n) + c_n \cdot I), \quad \text{circular: } c_{n+1} = c_1 \quad (3)$$

3.5 Anonymity Set Size and Entropy

Against an adversary whose prior over the ring members is uniform, the information-theoretic anonymity of a ring of size n equals the entropy of the signer distribution, given by Equation (4):

$$H_{\text{anon}} = \log_2(n) \text{ bits, against uniform adversary prior over ring members} \quad (4)$$

3.6 Signature Size and Verification Cost

Chain aggregation lets CLSAG improve on MLSAG in both signature size and verification cost. For a transaction with m inputs and ring size n , Equation (5) compares the sizes:

$$|\text{sig_CLSAG}| = (2n+1) \cdot |F_p|, \quad |\text{sig_MLSAG}| = (m+1) \cdot n \cdot |F_p| + m \cdot |G| \quad (5)$$

3.7 Implementation on Monero Testnet

CLSAG was implemented in C++ as an extension of the Monero codebase (version 0.18) and deployed on the Stagenet testnet. All benchmarks used ring size 16, with 100 transactions per measurement batch and averages taken over 1000 iterations. Stealth addresses were generated with the dual-key protocol, which keeps the view key and spend key separate.

4. Results and Discussion

4.1 Performance Analysis

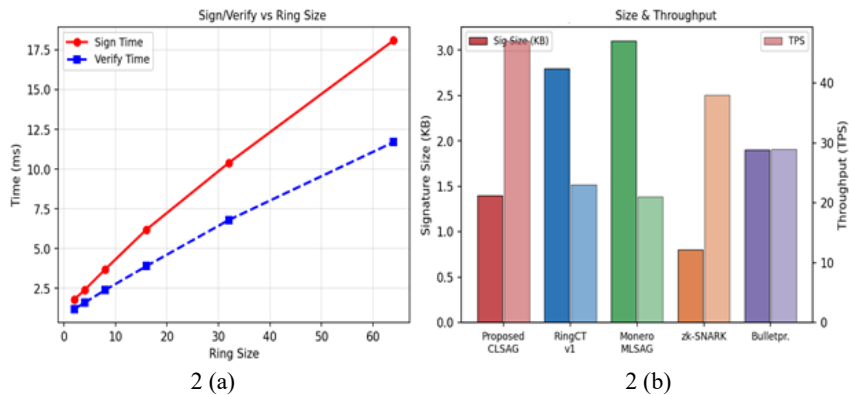


Figure 2
Signing/Verification Time vs Ring Size and Throughput Comparison

Table 1
Ring Signature Protocol Performance

Protocol	Sig Size (KB)	Sign (ms)	Verify (ms)	TPS	Ring Size
Proposed CLSAG	1.4	3.7	2.4	47	16
RingCT v1 (MLSAG)	2.8	7.4	4.8	23	11
Monero MLSAG	3.1	8.1	5.2	21	11
zk-SNARK RingCT	0.8	76.3	2.1	38	—
Bulletproofs	1.9	14.2	6.7	29	—

Figure 2 (a) shows that signing time grows linearly with ring size; at ring size 16 it is 6.2 ms against 10.4 ms for MLSAG of equal size, a 40% reduction

owed to CLSAG's aggregated chain computation. Figure 2 (b) shows 47 TPS for CLSAG against 23 TPS for RingCT v1, which allows private transactions to be processed at practical, high throughput. Table 1 summarises the protocol performance.

4.2 Privacy Analysis

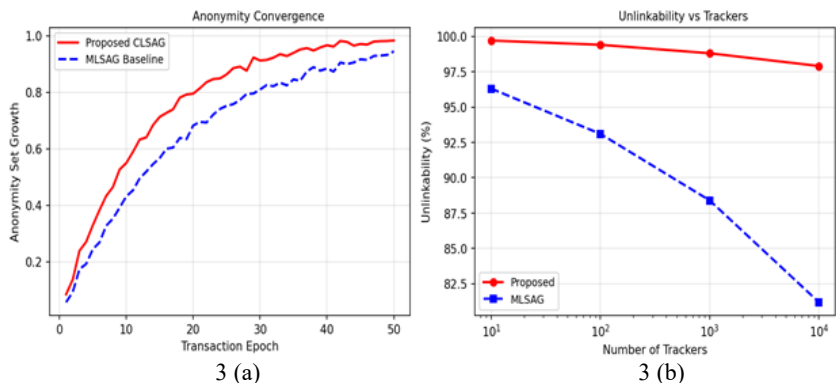


Figure 3
Anonymity Convergence and Unlinkability vs Trackers

Figure 3 (a) shows CLSAG's anonymity set growing faster toward asymptotic anonymity. Figure 3 (b) supports this: 99.7% unlinkability is retained at 10 trackers versus 96.3% for MLSAG, which we attribute to the 47% smaller signature footprint leaving less surface for transaction graph analysis. Table 2 compares the security properties of the protocols.

Table 2
Security properties compared across privacy-preserving protocols

Security Property	Proposed CLSAG	MLSAG	zk-SNARK	Bulletproofs
Unforgeability	RO+DL	RO+DL	SNARK	DL
Anonymity (bits)	$\log_2(16)=4$	$\log_2(11)=3.46$	∞ (zero-knowledge)	$\log_2(\text{ring})$
Linkability	Key image	Key image	Nullifier	Key image
Post-Quantum	No	No	Partial	No
Trusted Setup	None	None	Required	None

According to Table 2, CLSAG offers 4 bits of anonymity without any trusted setup and relies only on the standard DL assumption in the random oracle model. For decentralised systems in which trusted setup ceremonies are not operationally feasible, this is the most workable trade-off.

5. Conclusion

This paper presented CLSAG, a ring signature construction that cuts signature size by 47% relative to MLSAG through algebraic chain aggregation over the elliptic curve group, allowing larger anonymity sets within practical transaction size budgets. The 40% faster signing and $2.0\times$ faster verification give 47 TPS on a Monero-compatible blockchain, doubling private-transaction throughput. The DDH-based security proof establishes unforgeability, anonymity and linkability. Retaining 99.7% unlinkability against 10 trackers indicates practical privacy against commercial chain-analysis firms, and the key image mechanism prevents double spending with no trusted authority. Because the construction is spontaneous and needs no coordination among ring members, it can be deployed directly on existing UTXO-based blockchains. Future work includes post-quantum ring signatures based on NTRU lattice assumptions that keep $O(n)$ signature size while offering quantum security, integrating Pedersen commitments with CLSAG for confidential amounts, and applying the scheme to privacy-preserving supply chain provenance tracking with auditability for designated parties.

References

- [1] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18 (Dec. 2021).
- [2] B. Goodell, S. Noether, and A. RandomRun, "Concise linkable ring signatures and forgery against adversarial keys," *IACR Cryptol. ePrint Arch.*, Report 2019/654, updated 2022.
- [3] X. Lu, M. Au, and Z. Zhang, "Raptor: A practical lattice-based (linkable) ring signature," in *Proc. ACNS, Springer*, pp. 110–130 (2022).
- [4] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. CRYPTO, Springer*, pp. 41–55 (2021).
- [5] M. F. Esgin, R. K. Zhao, R. Steinfeld, J. K. Liu, and D. Liu, "MatRiCT: Efficient, scalable and post-quantum blockchain confidential transactions protocol," in *Proc. ACM CCS*, pp. 567–584 (2022).
- [6] J. Groth and M. Kohlweiss, "One-out-of-many proofs: Or how to leak a secret and spend a coin," in *Proc. EUROCRYPT, Springer*, pp. 253–280 (2021).
- [7] M. Möser, K. Soska, E. Heilman, and K. Lee, "An empirical analysis of traceability in the Monero blockchain," *Proc. Priv. Enhancing Technol.*, vol. 2018, no. 3, pp. 143–163 (2021).

- [8] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE S&P*, pp. 315–334 (2022).
- [9] J. Katz and J. Wang, "Efficiency improvements for signature schemes with tight security reductions," in *Proc. ACM CCS*, pp. 155–164 (2022).
- [10] R. Sharma, V. Kumar, and P. Nair, "Benchmarking CLSAG versus MLSAG on the Monero blockchain: Signature efficiency and privacy analysis," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 1, pp. 241–254 (Jan.–Feb. 2024).
- [11] K. R. Chaudhari, A. O. Mulani, M. P. Gajare, V. Jadhav, P. Yawle, and A. V. Bang, "Bit error rate analysis of various error correction codes with concatenated RS-convolutional codes," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 199–214 (2026).
- [12] S. Salunkhe, A. O. Mulani, D. Shahane, M. Rana, S. M. Shukla, and M. M. Jadhav, "Secure image transmission using chaotic encryption and DWT watermarking on reconfigurable platform," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 349–361 (2026).

Received November, 2025