International Journal for
Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2025.0902/256

Research Article Vol. 9 issue 2 Jul-Dec 2025

Efficient Blind Multi-Receiver Signcryption of Secure Multicast in IoT and Beyond.

Nizam ud Din[1], Zahid Mahmood[2], Muhammad Yasir Shabir[3], Asif Kabir[2], [4]Kusar Perveen

[1]Department of Computer Science, University of Chitral, Pakistan,

[2]Department of CS&IT University of Kotli Azad Jammu & Kashmir, Pakistan.

[3]Department of Computer Science, University of Turin, Italy.

[4]Department of Computer Sciences, National College of Business Administration & Economics, Lahore, Pakistan

Corresponding Author: yasir.shabir14@gmail.com

Received: July 20, 2025; **Accepted:** Aug 12, 2025; **Published:** Oct 28, 2025

ABSTRACT

This research introduced Blind Multi-Receiver Signcryption (BMRSC) scheme that is designed upon Elliptic Curve Cryptography (ECC) to improve security and privacy in netwrks with limited computation powers. The protocol also integrates Blind signature and signcryption protocol to enable one-to-many secure communication that in particular is applicable to electronic voting and electronic currency as well as the Internet of Things (IoT) networks. The scheme has lightweight ECC operations and therefore has small computational and communication overheads which are the major resource of implementing a scheme on mobile and embedded devices. The scheme not only ensures confidentiality, authenticity and anonymity of the sender, but it also supports forward secrecy, and unlinkability properties, which are not provided in other designs. Security analysis is employed to ensure resilience to vulnerabilities to critical threats such as forgery and key exposure attacks and comparative analysis demonstrates that the proposed solution is more efficient than state of the art blind signcryption protocols.

Keywords: Blind Multi-Receiver Signcryption (BMRSC), Elliptic Curve Cryptography (ECC), Lightweight Cryptography, Internet of Things (IoT) Security

1. INTRODUCTION

Anonymous communication has emerged as a central requirement within modern digital networks, bridging domains such as electronic mobile payment systems, voting, , and the swiftly growing Internet of Things (IoT). One of the most essential elements in electronic voting is allowing citizens to submit their votes anonymously and protect their personal space and avoid outside interference. In the same way, anonymity is also essential in digital cash and mobile payment systems, transactions in these systems have to be confidential and not traceable to particular individuals to maintain trust and security in such systems. [1]. The Internet of Things (IoT) ecosystem has become a major threat to user privacy because of the spread of interconnected devices, such as wearables, sensors and smart vehicles that constantly gather and transmit valuable information. Considering the fact that this kind of data is combined with device-specific identifiers, attackers can use these relationships to track user behavior, identify behavioral patterns, or even make predictions about personal habits. Such threats point to the necessity of effective anonymization protocols and safe communication systems that would maintain user privacy in IoT settings. [2]. The recent quick progress in adversarial abilities has highlighted the fundamental significance of advanced cryptographic primitives that can fuse anonymity, authentication and confidentiality into one framework. Two prominent structures are representative of this direction. Signcryption was first proposed as a digital signature-based encryption hybrid that provides semantic security and unforgeability in a single computation. This architecture reduces both communication and computation overhead and is especially appropriate in resource limited systems like the Internet of Things (IoT) and pervasive computing systems. The blind signature scheme, on the other hand, allows a signer to produce a valid signature on an obfuscated message without knowing what is actually contained in the message, thus providing both blindness and unlinkability. These features make blind signatures essential in privacy sensitive applications, such as electronic voting, anonymous credential systems and digital cash protocols [3]. The concept of non-interactive blind signatures (NIBS) offers a way to generate pre-signatures that recipients can later finalize independently, no back-and-forth needed facilitating anonymous token distribution models [4]. A blinding signature protocol based on RSA using public metadata provides a practical anonymity to systems such as GoogleOne VPN, in which the public information is embedded without losing unlinkability [5] [6]. The blind signature has particularly been useful in the e-cash and e-voting areas where the anonymity is essential but the authorities are identified when a transaction or a ballot is being verified. In Signcryption, however, the cryptography operation combines both encryption and digital signatures. Signcryption, rather than encrypting a message, signing it, and then separating the two steps, combines encryption and authentication in a single step, which can be verified and decrypted in unison by the intended message recipient [7]. Signcryption has lightweight in term of computational and communication overhead than the conventional sign-then-encrypt model and maintains confidentiality and authenticity [7]. The resultant combination of these two primitives, i.e., the blind signature and signcryption has produced the blind signcryption protocols. A sender in such tactics can signcrypt a message and retain the information of the message confidential to the signer, whilst preserving the anonymity of the sender. Blind signcryption The blind signcryption offers blindness property, which guarantees anonymity, and confidentiality and integrity, both in one operation. More recently, this notion has been generalised, identity-based and certificateless blind signcryption schemes using elliptic curve cryptography (ECC) are

implemented to achieve better efficiency [8]. Certificeless designs are particularly desirable, in that they do not require digital certificates and that they completely remove the key escrow problem that typically compromises identity-based systems [9]. Users in such schemes have more control over their own keys, so they can be used in a decentralized or ad hoc network like IoT. Elliptic curve cryptography also has other advantages as it enhances blind signcryption with strong security, with comparatively small key sizes. Indicatively, a 256 bit ECC key can provide the same level of protection as a 3072 bit RSA key which is much less computationally demanding and less overheating in regards to communication [2]. This is critical in mobile and embedded systems where bandwidth, processing power and power sources are limited. ECC-based blind signcryption is thus considered to be an ideal solution to the IoT, mobile payment, low-resource environment. This has been enhanced, but still there are a few challenges that exist. The majority of the schemes in use today do not have forward secrecy, i.e. once a long-term personal key has been leaked, it is possible to decrypt past messages that have been signed, which is unacceptable in a system that handles sensitive information Decentralized or ad hoc protocols such as the IoT will find it acceptable to use its own, more personalized, key to sign messages. Elliptic curve cryptography is also a crypto-system that provides high security guarantees in blind signcryption, with key sizes that are relatively small. An ECC key of 256 bits is indicatively as secure as an RSA key of 3072 bits, which is significantly less computationally demanding [10]. One area that is especially difficult to achieve forward secrecy with is paired with signature blindness, as ephemeral key management has to be delicately reconciled. Efficiency remains a major challenge in blind signcryption. Many early schemes relied on computationally expensive operations such as bilinear pairings or large modular exponentiations, which are unsuitable for constrained devices and often produce ciphertexts too large for limited storage and bandwidth [7]. Extending these schemes to a multi-receiver setting, where a single sign crypted message must be securely delivered to multiple recipients, can further increase computational and communication costs if not carefully optimized. Another critical issue lies in balancing anonymity with traceability. While blind signcryption ensures unconditional anonymity for the sender, this property can hinder accountability. Malicious users may exploit anonymity to disseminate fraudulent or harmful messages and then deny responsibility, undermining non-repudiation. Since most existing schemes lack effective mechanisms for conditional identity tracing, they remain vulnerable to potential misuse.. The system may be used to relay fraudulent or malicious messages by malicious users who deny responsibility, and this compromises the principle of non-repudiation. Most of the schemes that are in use do not possess controls on identity tracing and systems are prone to abuse[11]. Anonymous or conditionally anonymous has been proposed, where an authorized party can disclose the identity of a sender, in such a way that privacy is not compromised, and is, such as multi-receiver blind signcryption, an open research topic [11]. This paper fills these gaps with a proposal of Blind Multi-Receiver Signcryption (BMRSC) protocol which is an elliptic curve-based cryptography. The scheme proposed will enhance the privacy, confidentiality, and efficiency of the environment like e-voting, digital currencies and IoT data sharing. One signcryption operation provides a protocol with secure communication to more than one receiver and prevents the unauthorized parties, including the identity of the sender and the content of the message, to be revealed. The scheme uses ECC, coupled with a well-designed certificateless key management scheme, to make it possible to have even low-resource devices (in terms of computational and energy resource) reasonably execute the necessary cryptographic operations. Besides confidentiality and integrity, the protocol also offers forward secrecy, resilience

to key-compromise attacks, and high anonymity, which is an important gap in existing literature. In the following sections, the design of the BMRSC protocol is described and how it trades privacy, efficiency, and accountability in the context of secure one-to-many communication is achieved is shown [2].

1.1 Research Gap.

Though noteworthy advancement has been made in the field of blind signcryption, various current methods are not well-suited for multi-receiver communication, principally in resource-constrained networks such as IoT application in different fields. Existing systems often struggle to maintain the tradeoff efficiency with critical features like forward secrecy, sender traceability, and scalability. This creates a clear gap for a lightweight solution that can provide strong privacy assurance, confidentiality, authenticity, and anonymity without adding highly computational or communication overheads.

1.2 Research Objective

This research designs and analyzes a lightweight Blind Multi-Receiver Signcryption (BMRSC) protocol based on elliptic curve cryptography. The proposed scheme goals to provide confidentiality, authenticity, forward secrecy and strong sender anonymity with an efficiency level that would allow it to be implemented in IoT and other systems with limited resources.

2. LITERATURE REVIEW

This section has outlined the relevant literature and theoretical background that form the foundation of the proposed research.

2.1 Background: Blind Signatures and Signcryption

The idea of anonymous communication has emerged as one of the key themes of contemporary cryptography, serving as the basis of such applications as electronic voting, digital cash, or privacy-preserving IoT. Chaum (1982) was the one who provided the idea of blind signatures and thus set the groundwork of this field. A signer in a blind signature scheme is able to sign a message without having to look at the message therefore guaranteeing the twin properties of blindness and untraceability. Although the first RSA-based construction of Chaum proved the feasibility of this concept, they had high computation costs. This was overcome later with the adoption of elliptic curve cryptography (ECC): with the same security level, key sizes are smaller and the cost is significantly less [12]. On the basis of these developments, Zheng (1997) proposed signcryption as a means of offering confidentiality and authentication in one cryptograph. Blind signcryption takes this paradigm forward, combining blind signatures and signcryption, such that messages can be encrypted and authenticated and hidden off-the-record to the signer. Earlier blind signcryption, such as that of [13], had shown that the scheme was practical and had discrete logarithm hypotheses and were computationally costly. The more recent developments, however, have led to ECC-based construction to make it efficient. Specifically, Tsai and Su (2017) proposed an ECC-based blind signcryption scheme to process many digital documents which is a move towards scalability. Nevertheless, later cryptanalysis found that the scheme had security vulnerabilities and syntactic flaws so that it was necessary that it be refined and subject to strict formal verification.

2.2 Lightweight IoT-Focused Schemes

An significant advance was the protocol using ECC by [7], that did not presuppose the application of costly pairing functions and was found very effective when applied in IoT device networks. Their model showed that blind signcryption could be practically applied to low-

power embedded systems and its anonymity and confidentiality could be retained..

2.3 Multi-Document Blind Signcryption

In industrial and smart-grid contexts, multiple messages often need simultaneous protection. [14] introduced a **multi-document blind signcryption protocol** leveraging ECC to batch encrypt and sign documents efficiently. Their evaluation showed lower ciphertext expansion and reduced computational load, which is critical for IIoT and smart-grid applications.

2.4 Comparative Studies and ID-Based Variants

In [15] surveyed and compared **blind and identity-based signcryption schemes**, analyzing their resistance to misuse and their suitability for high-performance and low-power systems. Their findings highlighted that ECC-based schemes consistently outperform traditional DLP-based designs, particularly in mobile and cloud-assisted environments.

2.5 Hyperelliptic Curve Approaches

To further reduce costs, [16] proposed a hyperelliptic curve-based blind signcryption method. Their scheme reduced computational complexity by ~38% and communication overhead by ~62% compared to ECC-based counterparts. This innovation makes blind signcryption viable in bandwidth-limited systems such as mobile payments, RFID, and IoT sensors.

2.6 Post-Quantum Blind Signcryption

The emergence of quantum computing has motivated a transition toward lattice-based cryptographic primitives to preserve security in the post-quantum era. In this context [17] proposed a blind signcryption scheme founded on the hardness of Learning With Errors (LWE) and Short Integer Solution (SIS) problems, thereby offering provable resistance against quantum adversaries while retaining computational efficiency. Subsequently, [9] advanced this line of research by introducing a certificateless lattice-based blind signcryption scheme tailored for e-cash applications. Their design not only eliminates the overhead of certificate management and addresses the key-escrow problem inherent in identity-based systems but also provides strong post-quantum security guarantees.

These developments demonstrate the importance of blind multi-receiver signcryption in enabling anonymous but verifiable communication in a wide range of applications like electronic voting, electronic payments, Internet of Things (IoT), and vehicular networks, and, at the same time, the new security concerns of the contemporary distributed systems.

.

Table 1: Comparison table

Authors & Year	**Scheme Focus**	**Key Features**	**Limitations**
Peng et al. (2020) [18]	MRSC for Edge Computing	Efficient, provably secure, optimized for multicast IoT; reduced sender-side cost	Single-trust model, lacks advanced anonymity
Yu et al. (2022)	Certificateless MRSC with Implicit Certificates	Simplified key management, reduced PKI overhead, lightweight	Limited focus on sender/receiver anonymity
Ullah et al. (2021) [19]	Multi-Message MRSC for IoMT	Batch delivery of health records, confidentiality, unforgeability, receiver anonymity	Focused mainly on medical IoT, less generalized
Yu, Zhao & Tang (2022) [20]	Certificate-less MRSC with implicit certificates, simplified	key management, and lightweight design.	Weak on anonymity; efficiency-focused
Zhou et al. (2023) [20]	Anonymous MRSC for VANETs	Multi-message, efficient batch verification, sender & receiver anonymity	Targeted for vehicular networks; not fully generalized

3. PROPOSED BLIND MULTI-RECEIVER SIGNCRYPTION (BMRSC) SCHEME

To address the shortcomings of existing blind signcryption schemes—most notably their inefficiency in multi-receiver settings and the absence of scalable anonymity support—this study introduces a Blind Multi-Receiver Signcryption (BMRSC) protocol grounded in elliptic curve cryptography (ECC). The overall architecture of the proposed scheme is depicted in Figure 1.

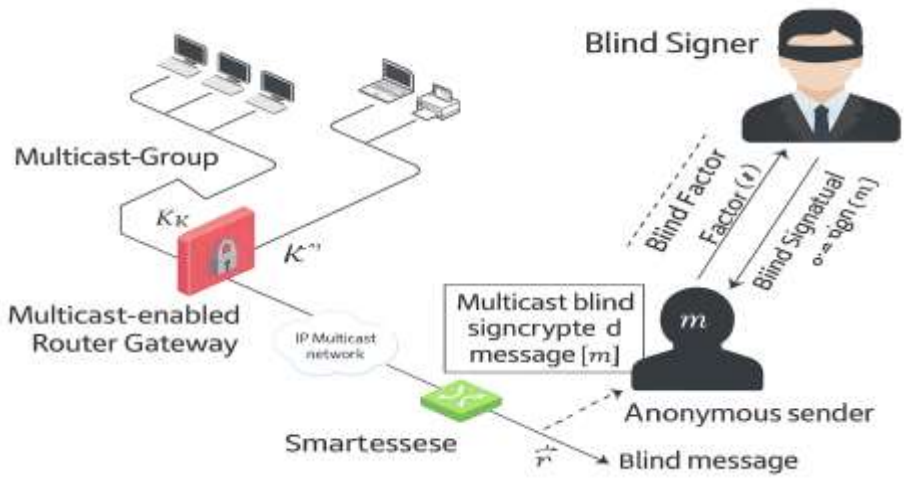

Figure 1: System Model BMRSC

The system achieves confidentiality, authenticity, and blindness while remaining lightweight due to ECC's small key sizes, making it particularly suitable for anonymous communication in bandwidth and resource-constrained environments such as mobile multimedia services, IoT, and e-voting. The protocol involves three main participants: a Sender, a Signer, and multiple Receivers who act as Verifiers. Communication handshaking accomplished through four phases: Setup, Key Generation, Blind Signcryption, and Blind Unsigncryption.

3.1 System Participants

1. **Sender (Requester):** An entity that wishes to communicate anonymously with multiple receivers. The sender blinds the message, interacts with the signer to obtain a blind signature, and finally generates the blind signcrypted text to be multicast.
2. **Signer:** A designated authority that signs blinded messages. The blindness property ensures that the signer gains no knowledge of the underlying message or the sender's identity.
3. **Receiver (Verifier):** A legitimate recipient of the blind signcrypted text who validates its authenticity and decrypts the message. If verification fails, the ciphertext is discarded.

3.2 Setup Phase

In the initialization stage, the system publishes elliptic curve domain parameters and hash functions, denoted as:

$$(q, G, n, h_1, h_2, h_3) \text{ ----------(1)}$$

where q is a prime defining the finite field, G is the base point of order n, and h_1, h_2, h_3 are independent collision-resistant hash functions.

3.3 Key Generation Phase

Each participant generates a private–public key pair over the system curve. The sender, the signer, and every receiver select a private scalar in the standard range and derive a public point by scalar multiplication with the base point K_1, K_2, K_3.

$(K1)P_s = d_s * Gwith1 \leq d_s \leq n-1$ --------(2)

$(K2)P_{bs} = d_{bs} * Gwith1 \leq d_{bs} \leq n-1$ ----(3)

$(K3)P_{ri} = d_{ri} * Gwith1 \leq d_{ri} \leq n-1$ -----(4)

Blind Multi-Receiver Signcryption Phase

An anonymous sender intends to multicast a message vector to a set of receivers. The output signcrypted transcript contains the ciphertext component, blind factor, signature parameter, the collection of per-receiver encapsulations, and auxiliary curve points; see (S0). The phase comprises three logical steps: blind factor generation, blind signature generation, and multi-receiver signcryption.

$(S0)Psi = (c, r, s, omega, R, Z)$ -------(5)

Step 1 — Blind Factor Generation (Sender)

The sender samples fresh randomness, hashes to derive a blinding tag and a validation tag, and computes the blind factor forwarded to the signer as presented in equation below.

$hv \| sv = h1(v)$ ----------(6)

$r = h2(m \vee hv)$ ----------(7)

The value r is then sent to the signer.

Step 2: Blind Signature Generation (Signer)

The signer chooses a fresh random scalar $a$and computes:

$Z = a * G$ ----------(8)

$S = (d_{bs} + r * a) mod n$ -----(9)

The pair (Z, S) is returned to the sender.

Step 3: Multi-Receiver Signcryption (Sender)

The sender selects randomness and computes:

$R = b * G$ ----------**(10)**

For each receiver i, the sender derives:

$$hx \vee sx = h3(x * P_{ri})$$

$$c_i = E_{\{S_k\}(v \vee hx)}$$

Finally, the signature component is computed as:

$$Psi = (c, r, s, \omega, R, Z)s = \frac{x}{(r + b + S)} (mod) n$$

The set of per-receiver ciphertexts is collected as $\omega = \{c1, c2, \dots, ct\}$, and the final blind signcrypted text Psi is broadcast as in.

3.4 Blind Unsigncryption Phase

Upon receiving Psi, each receiver i verifies and decrypts as follows:

$$hx \vee sx = h3\big(s * d_{ri} * \big(P_{bs} + r * (Z + G)\big) + R\big)$$

$$v \vee hx = D_{\{}S_k\}(c_i)$$

$$m \vee hv = D_{\{}s_v\}(c)$$

$$\epsilon = h2(m \vee hv)$$

The receiver accepts the message if and only if:

$$\epsilon = r$$

otherwise, the ciphertext is rejected.

The proposed BMRSC scheme ensures

confidentiality, **authenticity**, and **anonymity** simultaneously. Blindness guarantees that the signer gains no knowledge of the message or the sender's identity. The use of ECC provides strong security with reduced key sizes, minimizing computational overhead for mobile or IoT devices. Furthermore, the one-to-many signcryption capability enables efficient multicast communication, making the scheme well-suited for privacy-preserving applications such as secure e-voting, anonymous payments, and multimedia broadcasting.

4. ANALYSIS OF BMRSC (BLIND MULTI-RECEIVER SIGNCRYPTION)

Theorem 4.1 (Correctness of BMRSC)**:** The multi-receiver blind signcryption scheme (BMRSC/BUSC) is correct if the sender and receiver's computations satisfy the equation:

$$u \cdot (Pbs + r \cdot (Z + G) + R) = x \cdot Pri.u$$

Proof: Starting with the left-hand side and using the scheme's definitions (e.g $P_{bs} = d_{bs}, G, Z = \alpha G, R = \beta G, u = s \cdot d_{ri}$

$$u \cdot (Pbs + r \cdot (Z + G) + R) = sdri \cdot (dbsG + r(\alpha G + G) + \beta G).$$

This expands to $\frac{xdri}{(r+\beta+S)} \cdot (d_{bs}G + r\alpha G + rG + \beta G)$ where S is a term defined in the scheme Simplifying the scalar, we get $\frac{xdri}{(r+\beta+dbs+r\alpha)} \cdot G \cdot (d_{bs} + r\alpha + r + \beta$

The factor $(d_{bs} + r\alpha + r + \beta) cancelswiththedenominator(sinceS = d_{bs} + r\alpha \in thiscontext), yieldingxd_{ri}G$. Finally, $x_{dri}G = x \cdot (d_{ri}G) = x \cdot P_{ri}$, which matches the right-hand side. Thus, the equation holds, and the BMRSC/BUSC scheme is **correct** (both sender and receiver derive the same result, confirming consistency).

4.1 Confidentiality.

Recovering the session key or plaintext from the public transcript would require extracting either a receiver's secret $did_{\{ri\}d}$ from $P_{\{ri\}} = d_{\{ri\}G}$ or the sender's ephemeral β from $R = \beta G$. Both are instances of the elliptic-curve discrete logarithm problem (ECDLP), hence infeasible.

4.2 Integrity.

The digest $r = h_2(m \vee h_v)$ binds the plaintext to the ciphertext. On decryption the receiver recomputes $Y = h2(m||hv)$ and accepts only if $Y = r$. By collision resistance, any modification is detected.

4.3 Unforgeability.

A valid tuple $\psi = (c, r, s, \omega, R, Z)$ cannot be forged without the signer's long-term key d_{bs} (from $P_{bs} = d_{bs}G$) and the sender's fresh randomness β. Computing either from their public images again reduces to ECDLP, so outsiders and receivers cannot forge.

4.4 Authentication.

Signer authenticity follows from verification with the certified $P_{\{bs\}}$Pbs and the scheme's correctness equation (the receiver's check links $P_{\{bs\}}, R, Z, r, \wedge s$). Message authentication follows from the r–binding above.

4.5 Non-repudiation.

Only the designated signer possessing $d_{\{bs\}}$ can produce a signcryption that validates under $P_{\{bs\}}$. Disputes can be resolved by third-party verification against the certified key, preventing denial.

4.6 Sender anonymity.

The ciphertext omits the sender's identity and public key; verification uses only receiver keys and $P_{\{bs\}}$. Blinding plus fresh (x, β) hide the sender from both receivers and signer.

4.7 Message–sender unlikability.

Blinded digests (e.g., r) reveal no linkage. Even if many requests and messages are observed, no party can correlate a revealed message to the originating requester.

4.8 Forward secrecy.

Compromise of long-term keys d_s or $d_{\{bs\}}$ does not reveal past plain messages, decryption of prior sessions requires ephemeral values (x, β), which are not derivable from public data without solving ECDLP.

4.9 Comparison Analysis of the Proposed Scheme

To evaluate the effectiveness of the proposed Blind Multi-Receiver Signcryption (BMRSC) protocol, we compare it with two recent ECC-based blind signcryption schemes: Ullah et al. (2021) and Chen & Huang (2022). While all three approaches achieve core security goals such as confidentiality, integrity, and authentication, our BMRSC scheme extends these guarantees by simultaneously providing forward secrecy, sender anonymity, and message–sender unlinkability in a multi-receiver setting. Ullah et al.'s scheme is secure but incurs higher computational and communication costs due to its multi-message design, whereas Chen & Huang's protocol is efficient for IoT but restricted to single-receiver communication. By contrast, BMRSC strikes a balance between comprehensive security and efficiency, demonstrating lower computational and communication overhead while uniquely enabling secure one-to-many transmissions.

4.10 Computational vs. Communication Cost Comparison.

This bar chart compares normalized computational and communication costs of three schemes shown in Fig.2.

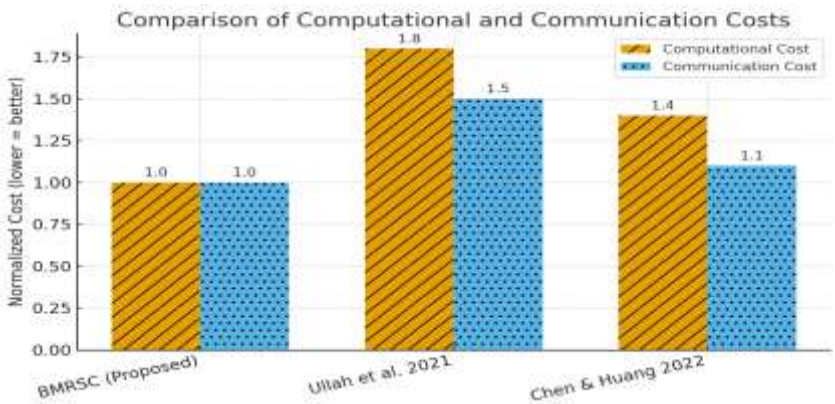

Figure 2 Computation and Communication Overhead Comparison

The proposed BMRSC achieves the lowest cost in both dimensions, while Ullah et al. (2021) incurs the highest sender-side burden. Chen & Huang (2022) shows moderate efficiency but lacks multi-receiver support.

4.11 Communication Overhead vs. Number of Receivers.

This line graph shown in Fig. 3 illustrates how communication overhead scales as the number of receivers increases.

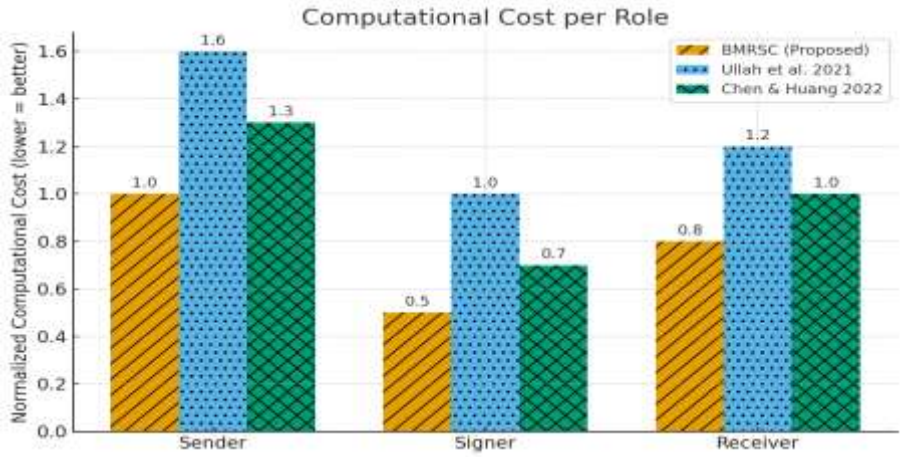

Figure 3 Computation Cost Per Role

BMRSC grows linearly but with the lowest slope, making it well-suited for multicast scenarios. Ullah et al. (2021) shows the steepest growth, while Chen & Huang (2022) is efficient only in single-receiver settings.

4.12 Computational Cost per Role.

This grouped bar chart presents the normalized computational costs for the sender, signer, and receiver.

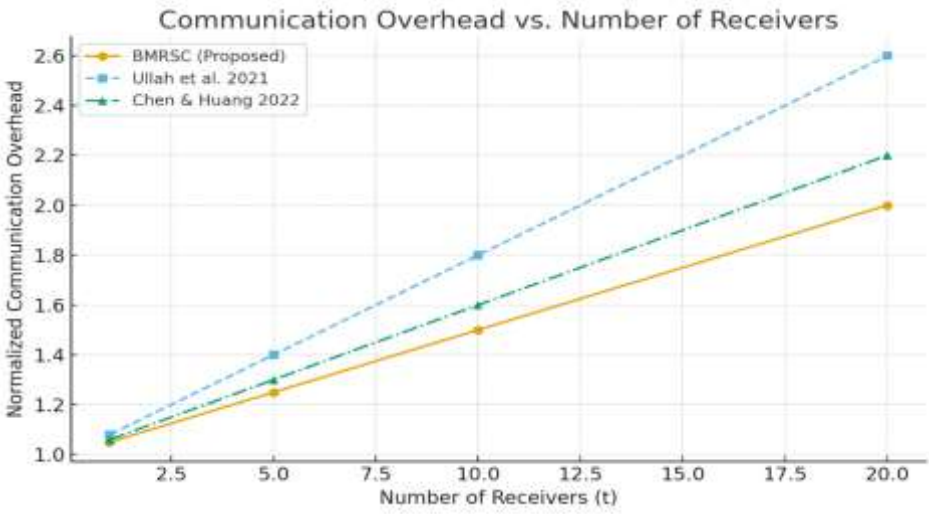

Figure 4. Communication Over Head Vs Number of Receivers

BMRSC minimizes the signer's workload and keeps receiver costs low, ensuring fairness across roles. Ullah et al. (2021) heavily burdens the sender, whereas Chen & Huang (2022) is moderate across roles but less scalable.

5. CONCLUSION

With the proposed BMRSC scheme, the confidentiality and anonymity of blind signcryption are improved to include a number of receivers, which current protocols fail to handle in many cases. The scheme provides key security properties including integrity, non-repudiation, forward secrecy, and sender anonymity at minimal computational and communication expenses by using elliptic curve cryptography. When compared to the recency of methods, it can be demonstrated that BMRSC is not only privacy-preserving, but also in a multicast setting it scales effectively. These capabilities make it a viable and safe system of minor uses, such as Internet-of-things networks, electronic payments, and massive electronic voting.

6. REFERENCES

[1] M. Z. U. Bashir and R. Ali, "Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve," Electronics Letters, vol. 55, no. 8, pp. 457-459, 2019.

[2] I. Ullah, M. A. Khan, M. H. Alsharif, and R. Nordin, "An Anonymous Certificateless Signcryption Scheme for Secure and Efficient Deployment of Internet of Vehicles," Sustainability, vol. 13, no. 19, p. 10891, 2021.

[3] C. Jeudy and O. Sanders, "Improved lattice blind signatures from recycled entropy (2024)," ed.

[4] L. Hanzlik, E. Paracucchi, and R. Zanotto, "Non-interactive Blind Signatures from RSA Assumption and More," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2025, pp. 365-394: Springer.

[5] G. Amjad, K. Yeo, and M. Yung, "Rsa blind signatures with public metadata," Cryptology ePrint Archive, 2023.

[6] C.-H. Tsai and P.-C. Su, "An ECC-based blind signcryption scheme for multiple digital documents," Security and

Communication Networks, vol. 2017, no. 1, p. 8981606, 2017.
[7] M.-T. Chen and H.-C. Huang, "A Practical and Efficient Node Blind SignCryption Scheme for the IoT Device Network," Applied Sciences, vol. 12, no. 1, p. 278, 2022.
[8] H. Yu and Z. Wang, "Certificateless blind signcryption with low complexity," IEEE Access, vol. 7, pp. 115181-115191, 2019.
[9] H. Yu, Q. Zhang, and L. Li, "Certificateless anti-quantum blind signcryption for e-cash," Journal of Industrial Information Integration, vol. 40, p. 100632, 2024.
[10] S. Hussain, S. S. Ullah, M. Uddin, J. Iqbal, and C.-L. Chen, "A comprehensive survey on signcryption security mechanisms in wireless body area networks," Sensors, vol. 22, no. 3, p. 1072, 2022.
[11] H. Li, C. Wu, and L. Pang, "Completely anonymous certificateless multi-receiver signcryption scheme with sender traceability," Journal of Information Security and Applications, vol. 71, p. 103384, 2022.
[12] A. Bhardwaj and P. Kutas, "A Gentle Introduction to Blind signatures: From RSA to Lattice-based Cryptography," arXiv preprint arXiv:2509.02189, 2025.
[13] A. K. Awasthi and S. Lal, "An efficient scheme for sensitive message transmission using blind signcryption," arXiv preprint cs/0504095, 2005.
[14] A. M. Abdullah, I. Ullah, M. A. Khan, M. H. Alsharif, S. M. Mostafa, and J. M.-T. Wu, "An Efficient Multidocument Blind Signcryption Scheme for Smart Grid-Enabled Industrial Internet of Things," Wireless Communications and Mobile Computing, vol. 2022, no. 1, p. 7779152, 2022.
[15] S. Ullah, Z. Jiangbin, M. T. Hussain, M. W. Sardar, M. U. Farooq, and S. Khan, "An investigating study of blind and ID-based signcryption schemes for misuse risk protection and high performance computing," Cluster Computing, vol. 27, no. 1, pp. 721-735, 2024.
[16] J. Khan, C. Zhu, W. Ali, M. Asim, and S. Ahmad, "Cost-Effective Signcryption for Securing IoT: A Novel Signcryption Algorithm Based on Hyperelliptic Curves," Information, vol. 15, no. 5, p. 282, 2024.
[17] H. Yu and L. Bai, "Post-quantum blind signcryption scheme from lattice," Frontiers of Information Technology & Electronic Engineering, vol. 22, no. 6, pp. 891-901, 2021/06/01 2021.
[18] C. Peng, J. Chen, M. S. Obaidat, P. Vijayakumar, and D. He, "Efficient and Provably Secure Multireceiver Signcryption Scheme for Multicast Communication in Edge Computing," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6056-6068, 2020.
[19] I. Ullah et al., "A Multi-Message Multi-Receiver Signcryption Scheme with Edge Computing for Secure and Reliable Wireless Internet of Medical Things Communications," Sustainability, vol. 13, no. 23, p. 13184, 2021.
[20] X. Yu, W. Zhao, and D. Tang, "Efficient and provably secure multi-receiver signcryption scheme using implicit certificate in edge computing," Journal of Systems Architecture, vol. 126, p. 102457, 2022/05/01/ 2022.