Cryptanalysis of LC-MUME: A Lightweight Certificateless Multi-User Matchmaking Encryption for Mobile Devices

Ramprasad Sarkar

***Abstract*—Yang *et al.* proposed a lightweight certificateless multi-user matchmaking encryption (LC-MUME) scheme for mobile devices, published in IEEE Transactions on Information Forensics and Security (TIFS) (DOI: 10.1109/TIFS.2023.3321961). Their construction aims to reduce computational and communication overhead within a one-to-many certificateless cryptographic framework. The authors claim that their scheme satisfies existential unforgeability under chosen-message attacks (EUF-CMA) in the random oracle model. However, our cryptanalytic study demonstrates that the scheme fails to meet this critical security requirement. In particular, we show that a Type-I adversary can successfully forge a valid ciphertext without possessing the complete private key of the sender. Both theoretical analysis and practical implementation confirm that this attack can be mounted with minimal computational cost. To address these weaknesses, we propose a modification strategy to strengthen the security of matchmaking encryption schemes in mobile computing environments.**

***Index Terms*—Cryptanalysis, Identity-based encryption, Match-Making encryption, Chosen-ciphertext attack security, Anonymity**

I. Introduction

Matchmaking Encryption (ME) is an advanced cryptographic primitive that enables bilateral access control between the sender and the receiver. Unlike traditional encryption schemes that enforce access policies unilaterally, ME empowers the sender to define an access policy specifying which receivers may decrypt the message, while simultaneously allowing the receiver to verify whether the ciphertext originates from a legitimate sender. This dual control mechanism improves communication privacy, particularly by protecting the sender's identity.

To address the shortcomings of conventional attribute-based encryption and signature-based mechanisms, Chen *et al.* [1] introduced a certificateless matchmaking encryption (CL-ME) scheme tailored for IoT environments, presenting two efficient constructions based on bilinear pairings and lightweight cryptographic techniques. Building on this line of work, Yang *et al.* [2] proposed a lightweight certificateless multi-user matchmaking encryption (LC-MUME) scheme for mobile platforms. Their construction aims to improve efficiency by avoiding pairings and relying on standard hardness assumptions. They claim that their scheme achieves existential unforgeability under chosen-message attacks (EUF-CMA).

II. Review of Yang *et al.*'s LC-MUME

The original LC-MUME scheme includes five algorithms due to space limitations; here, we omit the detailed description, which can be referred to [2].

III. Our Proposed Attacks

In this section, we identify the security vulnerabilities present in Yang et al.'s scheme [2]. A secure Certificateless Multi-User Matchmaking Encryption scheme should ensure that a sender cannot repudiate sending a valid encrypted message to a receiver. Additionally, it must prevent any adversary from impersonating the sender to create valid encrypted messages without knowing the full private key of the sender. Yang et al. [2] claim that their scheme is existentially unforgeable under a chosen message attack. However, we will demonstrate that a Type-I Adversary $\mathcal{ADV}_I$ can successfully forge a valid encrypted message to the receiver by substituting the sender's public key. The attack comprises the following three stages:

Step-1. In this stage, $\mathcal{ADV}_I$ replaces public key of the sender. For that, $\mathcal{ADV}_I$ randomly selects $a^*, b^* \in \mathbb{Z}_q^*$ and replaces the corresponding public key $\mathsf{PK}_{\mathsf{Id_S}}^{*1} = a^*\mathsf{P}$, $\mathsf{PK}_{\mathsf{Id_S}}^{*2} = b^*\mathsf{P}$, while $\mathcal{ADV}_I$ uses the secret key for the sender as $\mathsf{SK}_{\mathsf{Id_S}}^{*} = (\mathsf{SK}_{\mathsf{Id_S}}^{*1}, \mathsf{SK}_{\mathsf{Id_S}}^{*2}) = (a^*, b^*)$.

Step-2. In this stage, $\mathcal{ADV}_I$ generates a ciphertext under the replaced public key $\mathsf{PK}_{\mathsf{Id_S}}^{*}$. $\mathcal{ADV}_I$ does the following.

(i) $\mathcal{ADV}_I$ chooses $r, s, d_1^*, d_2^* \in \mathbb{Z}_q^*$ and computes $\mathsf{CT}_1^* = r\mathsf{P}$ and $\mathsf{CT}_2^* = s\mathsf{P} - \mathcal{H}_1(\mathsf{Id_S}, \mathsf{PK}_{\mathsf{Id_S}}^{*2})\mathcal{P}'$.

(ii) For $\mathsf{Id_i} \in \mathsf{Rcvr}$, it computes

$$\tau_i^* = \mathsf{SK}_{\mathsf{Id_S}}^{*1} \cdot \mathsf{PK}_{\mathsf{Id_i}}^{1}$$
$$\mathcal{V}_{\mathsf{Id_i}}^{*} = \mathcal{H}\left(r \cdot \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_i^*)\left(\mathsf{PK}_{\mathsf{Id_i}}^{2} + \mathcal{H}_1(\mathsf{Id_i}, \mathsf{PK}_{\mathsf{Id_i}}^{2})\mathcal{P}'\right)\right)$$
$$\mathcal{Z}_{\mathsf{Id_i}}^{*} = \left(s + \mathsf{SK}_{\mathsf{Id_S}}^{*2} + \mathsf{SK}_{\mathsf{Id_S}}^{*1} \cdot \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_i^*)\right)\mathsf{PK}_{\mathsf{Id_i}}^{1}.$$

(iii) Then the adversary sets two n-degree polynomials as follows.

$$f^*(x) = \prod_{\mathsf{Id_k} \in \mathsf{Rcvr}} (x - \mathcal{V}_{\mathsf{Id_k}}^{*}) + d_1^* = \sum_{\mathsf{k}=0}^{n-1} a_{\mathsf{k}}^* x^{\mathsf{k}} + x^n (\text{mod } q)$$

$$g^*(y) = \prod_{\mathsf{Id_k} \in \mathsf{Rcvr}} (y - \mathcal{Z}_{\mathsf{Id_k}}^{*}) + d_2^* = \sum_{\mathsf{k}=0}^{n-1} b_{\mathsf{k}}^* y^{\mathsf{k}} + y^n (\text{mod } q)$$

(iv) Then, it computes the following ciphertext components as follows.

$$\mathsf{CT}_3^* = [\mathcal{H}_2(\mathsf{CT}_1^*, \mathsf{CT}_2^*, d_1^*, d_2^*)]_{l-l_1} \parallel ([\mathcal{H}_2(\mathsf{CT}_1^*, \mathsf{CT}_2^*, d_1^*, d_2^*)]^{l_1} \bigoplus m)$$
$$\mathsf{CT}_4^* = \mathcal{H}_3(\mathsf{CT}_1^*, \mathsf{CT}_2^*, \mathsf{CT}_3^*, a_0^*, a_1^*, \ldots, a_{n-1}^*, b_0^*, b_1^*, \ldots, b_{n-1}^*).$$

(v) Finally, it returns a corresponding ciphertext $\mathsf{CT}^* = (\mathsf{CT}_1^*, \mathsf{CT}_2^*, \mathsf{CT}_3^*, \mathsf{CT}_4^*, a_0^*, a_1^*, \ldots, a_{n-1}^*, b_0^*, b_1^*, \ldots, b_{n-1}^*)$.

Step-3. We notice that, since there's no binding between a user's identity and his public key, the receiver cannot detect that the sender's public key is replaced by the adversary. In this stage, upon receiving the ciphertext, the receiver $\mathsf{Id_i}$ invokes the decryption algorithm as follows.

1) It parses the ciphertext $\mathsf{CT}^* = (\mathsf{CT}_1^*, \mathsf{CT}_2^*, \mathsf{CT}_3^*, \mathsf{CT}_4^*, a_0^*, a_1^*, \ldots, a_{n-1}^*, b_0^*, b_1^*, \ldots, b_{n-1}^*)$ and check whether the equation $\mathsf{CT}_4^* = \mathcal{H}_3(\mathsf{CT}_1^*, \mathsf{CT}_2^*, \mathsf{CT}_3^*, a_0^*, a_1^*, \ldots, a_{n-1}^*, b_0^*, b_1^*, \ldots, b_{n-1}^*)$.
2) If not, returns $\perp$. Otherwise, it calculates

$$\tau_{\mathsf{i}}^* = \mathsf{SK}_{\mathsf{Id_i}}^{1} \cdot \mathsf{PK}_{\mathsf{Id_S}}^{*1},\ \mathcal{V}_{\mathsf{Id_i}}^{*} = \mathcal{H}(\mathsf{SK}_{\mathsf{Id_i}}^{2} \cdot \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_{\mathsf{i}}^*) \cdot \mathsf{CT}_1^*)$$
$$\mathcal{Z}_{\mathsf{Id_i}}^{*} = \mathsf{SK}_{\mathsf{Id_i}}^{1}\left(\mathsf{CT}_2^* + \mathsf{PK}_{\mathsf{Id_S}}^{*2} + \mathcal{H}_1(\mathsf{Id_S}, \mathsf{PK}_{\mathsf{Id_S}}^{*2})\mathcal{P}' + \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_i^*)\mathsf{PK}_{\mathsf{Id_i}}^{1}\right).$$

3) It then recovers d_1^* and d_2^* by computing $d_1^* = f(\mathcal{V}_{\mathsf{Id_i}}^{*}), d_2^* = g(\mathcal{Z}_{\mathsf{Id_i}}^{*})$. Then it finally returns the message as follows $m = [\mathcal{H}_2(\mathsf{CT}_1^*, \mathsf{CT}_2^*, d_1^*, d_2^*)]^{l_1} \bigoplus [\mathsf{CT}_3^*]^{l_1}$ if

Ramprasad Sarkar is with the Cryptology and Security Research Unit, Indian Statistical Institute Kolkata, 203 B T Road, Kolkata, India-700108 *(e-mail: rpsarkar123@gmail.com).*

$[\mathcal{H}_2(\mathsf{CT}_1^*, \mathsf{CT}_2^*, d_1, d_2)]_{l-l_1} = [\mathsf{CT}_3^*]_{l-l_1}$, otherwise it return $\perp$.

The adversary generated a forged ciphertext that is well-defined and correct due to the following calculations.

$$\begin{aligned}
\tau_i^* &= \mathsf{SK}_{\mathsf{Id_S}}^{*1} \cdot \mathsf{PK}_{\mathsf{Id_i}}^1 = a^* x_{\mathsf{i}} \mathsf{P} \\
\mathcal{V}_{\mathsf{Id_i}}^* &= \mathcal{H}(\mathsf{SK}_{\mathsf{Id_i}}^2 \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_{\mathsf{i}}^*) \mathsf{CT}_1^*) \\
&= \mathcal{H}(r \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_{\mathsf{i}}^*) d_{\mathsf{i}} \mathsf{P}) \\
&= \mathcal{H}(r \cdot \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_{\mathsf{i}}^*)(\mathsf{PK}_{\mathsf{Id_i}}^2 + \mathcal{H}_1(\mathsf{Id_i}, \mathsf{PK}_{\mathsf{Id_i}}^2) \mathcal{P}^{'})) \\
\mathcal{Z}_{\mathsf{Id_i}}^* &= \mathsf{SK}_{\mathsf{Id_i}}^1 \Big(\mathsf{CT}_2^* + \mathsf{PK}_{\mathsf{Id_S}}^{*2} + \mathcal{H}_1(\mathsf{Id_S}, \mathsf{PK}_{\mathsf{Id_S}}^{*2}) \mathcal{P}^{'} \\
&\quad + \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_i^*) \mathsf{PK}_{\mathsf{Id_S}}^{*1} \Big) \\
&= x_{\mathsf{i}} \left(s \mathsf{P} + b^* \mathsf{P} + \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_i^*) a^* \mathsf{P} \right) \\
&= x_{\mathsf{i}} \mathsf{P} \left(s + b^* + \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_i^*) a^* \right) \\
&= \left(s + \mathsf{SK}_{\mathsf{Id_S}}^{*2} + \mathsf{SK}_{\mathsf{Id_S}}^{*1} \cdot \mathcal{H}_4(\mathsf{Id_S}, \mathsf{Id_i}, \tau_i^*) \right) \mathsf{PK}_{\mathsf{Id_i}}^1
\end{aligned}$$

Since the receiver $\mathsf{Id_i}$ is from the set Rcvr, therefore, it can recover the d_1 and d_2 by computing $d_1^* = f(\mathcal{V}_{\mathsf{Id_i}}^*), d_2^* = g(\mathcal{Z}_{\mathsf{Id_i}}^*)$. This follows that the forged ciphertext $\mathsf{CT}^* = (\mathsf{CT}_1^*, \mathsf{CT}_2^*, \mathsf{CT}_3^*, \mathsf{CT}_4^*, a_0^*, a_1^*, \ldots, a_{n-1}^*, b_0^*, b_1^*, \ldots, b_{n-1}^*)$ is valid. Therefore, the scheme is subject to universal forgery with respect to a Type-I adversary $\mathcal{ADV}_I$ who replaces the sender's public key.

IV. Performance Analysis and Implementation

This section presents a performance evaluation and practical implementation of the proposed forgery attacks against the certificateless matchmaking encryption scheme of Yang *et al.* [2], under the EUF-CMA security model. In this setting, a Type-I adversary $\mathcal{ADV}_I$ attacks in two main stages: Step 1 and Step 2, ultimately generating a valid forged ciphertext. In Step 3, the forged ciphertext can be verified and correctly decrypted by an authorized user or the challenger, thus violating the EUF-CMA security notion.

The total cost incurred by $\mathcal{ADV}_I$ is the sum of all operations performed during Steps 1 through 3. Table I summarizes the computational complexity per operation step, as well as the total execution time (in milliseconds) required to complete the forgery for various values of the target user set size n.

Our attack technique was implemented on a Dell laptop equipped with an AMD A9-9400 Radeon processor, 12 GB RAM, running Ubuntu 22.04.4 LTS (64-bit) with GNOME 42.9. We used the Pairing-Based Cryptography (PBC) library, version 0.5.14 [3], utilizing a Type A bilinear pairing over the supersingular curve defined by $y = x^3 + x$.

The attack strategy was executed for different sizes of the user groups: $n \in \{8, 16, 32, 64, 128, 256, 512, 1024\}$. The timing results (in milliseconds) are reported in Table I, along with the detailed breakdown of the cryptographic operations involved. The findings indicate that the proposed attack is highly efficient and scales linearly with the number of target user sets.

TABLE I: Computation Cost and Execution Time of EUF-CMA Attack

Step	#Z	#SM	#SS	#Hash	Attack Time (ms) for Varying User Sizes (n)					
					8	32	128	256	512	1024
Step-1	2	2	–	–	11.20	39.04	150.40	298.88	595.84	1189.76
Step-2	$2n+4$	$3n+1$	$7n+3$	$n+4$						
Step-3	–	–	7	6						

#Z: element generation in $\mathbb{Z}_p^*$, #SM: scalar multiplication in the source or target group, #SS: group addition/multiplication, #Hash: hash function evaluation. n: number of users.

V. Countermeasures Against the Proposed Attacks

As shown in Section III, Yang *et al.*'s scheme [2] is vulnerable to forgery attacks launched by a Type-I adversary. The root cause of this vulnerability lies in unaccounted algebraic dependencies within the underlying group structure, which the security proof fails to capture. In particular, these attacks do not imply that the adversary solves the underlying hard problems in a general or random instance.

Attacks on certificateless encryption systems can broadly be classified into two categories:

- **Passive Attacks:** These involve eavesdropping or traffic analysis, where the adversary observes the system's communication without altering its operation, aiming to extract useful information.
- **Active Attacks:** These are more intrusive, wherein the adversary interferes with system operations, e.g., by injecting, modifying, or replacing cryptographic elements, to breach security properties such as integrity or authenticity.

Our forgery attacks presented in this work fall into the category of active attacks. Specifically, the adversary replaces a user's public key to craft a valid forgery. These attacks are not only feasible but also practical, and thus must be addressed correctly in real-world deployments.

Eliminating the IB Setup. A viable countermeasure is to eliminate the identity-based (IB) setup from the protocol. In an IB setting, the adversary can query key-generation oracles for arbitrary identities. This flexibility allows manipulation of public/private key relationships, which is exploited in the forgery attack.

In contrast, certificateless matchmaking encryption schemes designed without an IB setup restrict the adversary's access: key-generation and hash queries must reference opaque indices mapped to hidden identities. As a result, the adversary cannot associate public keys with real identities, rendering the attack ineffective.

However, the main trade-off is the loss of operational simplicity that IB setups provide, such as reduced certificate management and simplified trust models. Thus, while removing the IB setup offers better resistance to active forgeries, it may require careful design adjustments to preserve usability and scalability.

VI. Conclusion

We have performed a comprehensive cryptanalysis of the Lightweight Certificateless Multi-User Matchmaking Encryption scheme proposed by Yang *et al.*, revealing critical security weaknesses. Specifically, our analysis shows that the scheme does not achieve unforgeability in a multi-user environment. To substantiate our findings, we present explicit attack scenarios that exploit these vulnerabilities, accompanied by a detailed evaluation of the associated computational costs. Furthermore, we propose a potential design strategy aimed at constructing secure and efficient matchmaking encryption protocols suitable for mobile computing framework.

Acknowledgment

This study was funded by the Information Security Education and Awareness (ISEA) Project Phase-III initiatives of the Ministry of Electronics and Information Technology (MeitY) under Grant No. F.No. L-14017/1/2022-HRD.

References

[1] B. Chen, T. Xiang, M. Ma, D. He, and X. Liao, "Cl-me: Efficient certificateless matchmaking encryption for internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 15 010–15 023, 2021.

[2] N. Yang, C. Tang, and D. He, "A lightweight certificateless multi-user matchmaking encryption for mobile devices: Enhancing security and performance," *IEEE Transactions on Information Forensics and Security*, 2023.

[3] B. Lynn *et al.*, "The pairing-based cryptography library," 2006.