Dear researchers at the Cryptography and Security Group at Aarhus University,

We would like to express our sincere appreciation for your thorough security analysis of our Letter Sealing (end-to-end encryption protocol) and for sharing your findings with us. We take all security-related feedback very seriously.

The replay, message blocking, and message reordering issue; the forging read receipts issue; and the impersonation issue are all limitations inherent in our protocol design, of which we were aware. However, we appreciate your independent validation and additional insights. Our protocol focuses on providing confidentiality and integrity of user communication, but we are actively evaluating ways to provide additional security properties at the protocol level to eliminate the previously mentioned issues. Additionally, we have the following comments to provide regarding these issues:

- Replay, Message Blocking and Message Reordering: We found that relying on client-provided timestamps can cause issues, such as newly received messages being inserted off-screen among past messages due to network issues or an incorrectly configured device. We chose to prioritize user experience, which is why we use the server reception timestamp instead, leading to the cryptographic protocol issues you mentioned.
- Forging read receipt: Read receipt metadata has historically been treated as non-sensitive in our threat model; however, your work shows scenarios where it can be misused. We are updating both our threat model and our encryption report accordingly.
- Impersonation issue: There are checks at the server level preventing impersonated messages from being sent through our infrastructure, but we understand this is not a sufficient countermeasure in the E2EE threat model.

The leakage issue through stickers and URLs is a result of how we chose to balance privacy with usability. We acknowledge that these features degrade privacy, and we have documented this in our public encryption report. Additionally, we have the following comments to provide regarding these issues:

- Leakage through Stickers: This issue is hard to avoid, as there are too many stickers to store on the client; therefore, they have to be loaded dynamically. We are very interested in advances in private information retrieval, but we do not believe the current state-of-the art would work at our scale.

- Leakage through URLs: We decided to create the preview on the server-side because, depending on which side creates the preview, the user on the side creating the preview will have their IP exposed, even if they do not visit the URL. Users can opt-out of this feature in the settings (Settings → Chats → URL previews).

We remain committed to improving our security and are looking into updating our cryptographic protocol. We will consider how to better address some of the issues you reported, as well as other limitations mentioned in our public encryption report. Thank you once again for your valuable research and for responsibly disclosing your findings to us.

Sincerely,