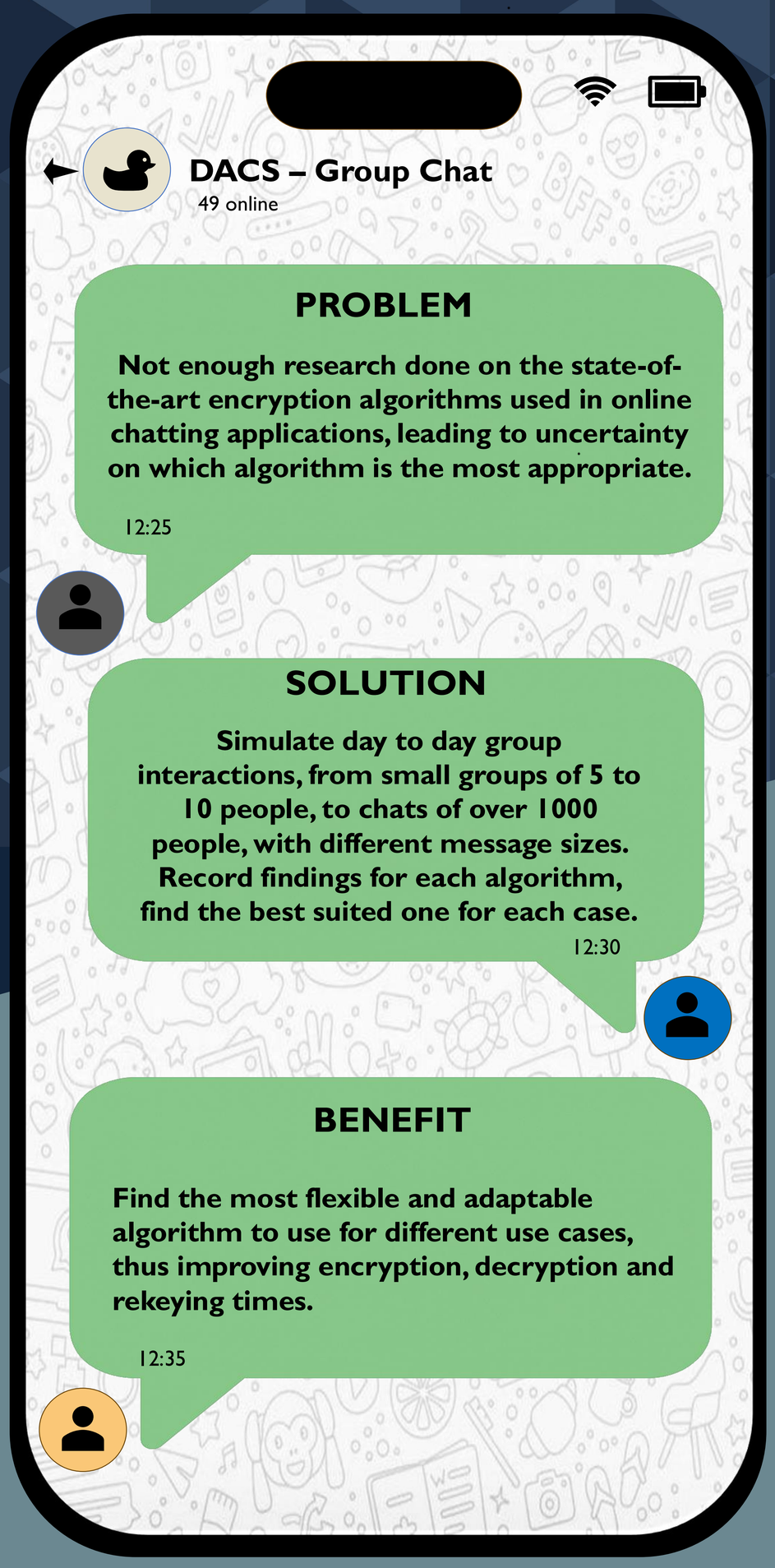
Maastricht University

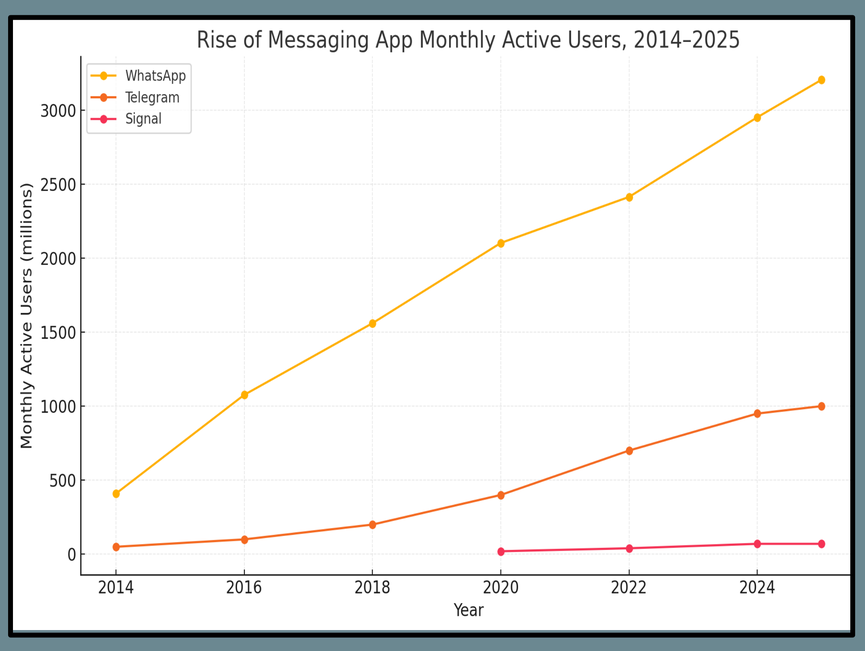
Faculty of Science and Engineering
Computer Science

Your Group Chat is Secure… But Will it Scale?

Encrypted at Scale: How Encryption Holds Up as Group Chats Grow



IMPORTANCE



Communication is essential in today's digital world. Group chat applications are becoming increasingly popular, with user numbers growing rapidly.

HOW?

Develop a tool that implements these algorithms, records and visualizes their performance under certain conditions.

Alexandru Lazarina, Vlad Manolescu, Amir Kalantarzadeh, Bati Gozen, Karol Plandowski, Aukje Heijthuijzen, Vilmos Udvari

METHODOLOGY

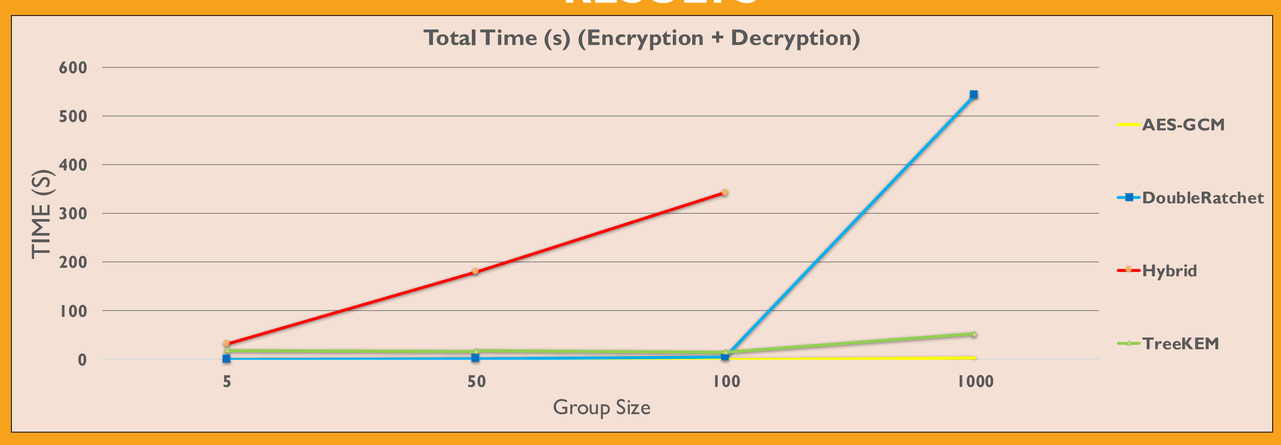
We focus on comparing four encryption algorithms: AES-GCM, Double Ratchet, TreeKEM and a Hybrid method combining AES with RSA/ECIES.

Each has different strengths in terms of performance, scalability, and security. We test their performance with regards to:

MEASURED METRICS

- Encryption/Decryption time
- CPU and memory usage
- Rekeying time during user join/leave events

RESULTS



- **TreeKEM** proved to be the **most scalable** algorithm for **rekeying**, thanks to its tree structure.
- **Hybrid** was the **slowest** with regards to total time and rekeying because it encrypts the session key individually for every user.
- **AES-GCM** was the **fastest** in both encryption and rekeying, but lacks secure key distribution, making it less ideal for large or dynamic groups.
- **Double Ratchet** offers excellent security (used in Signal/WhatsApp), but rekeying and setup becomes expensive due to constant DH key exchanges and state syncing.

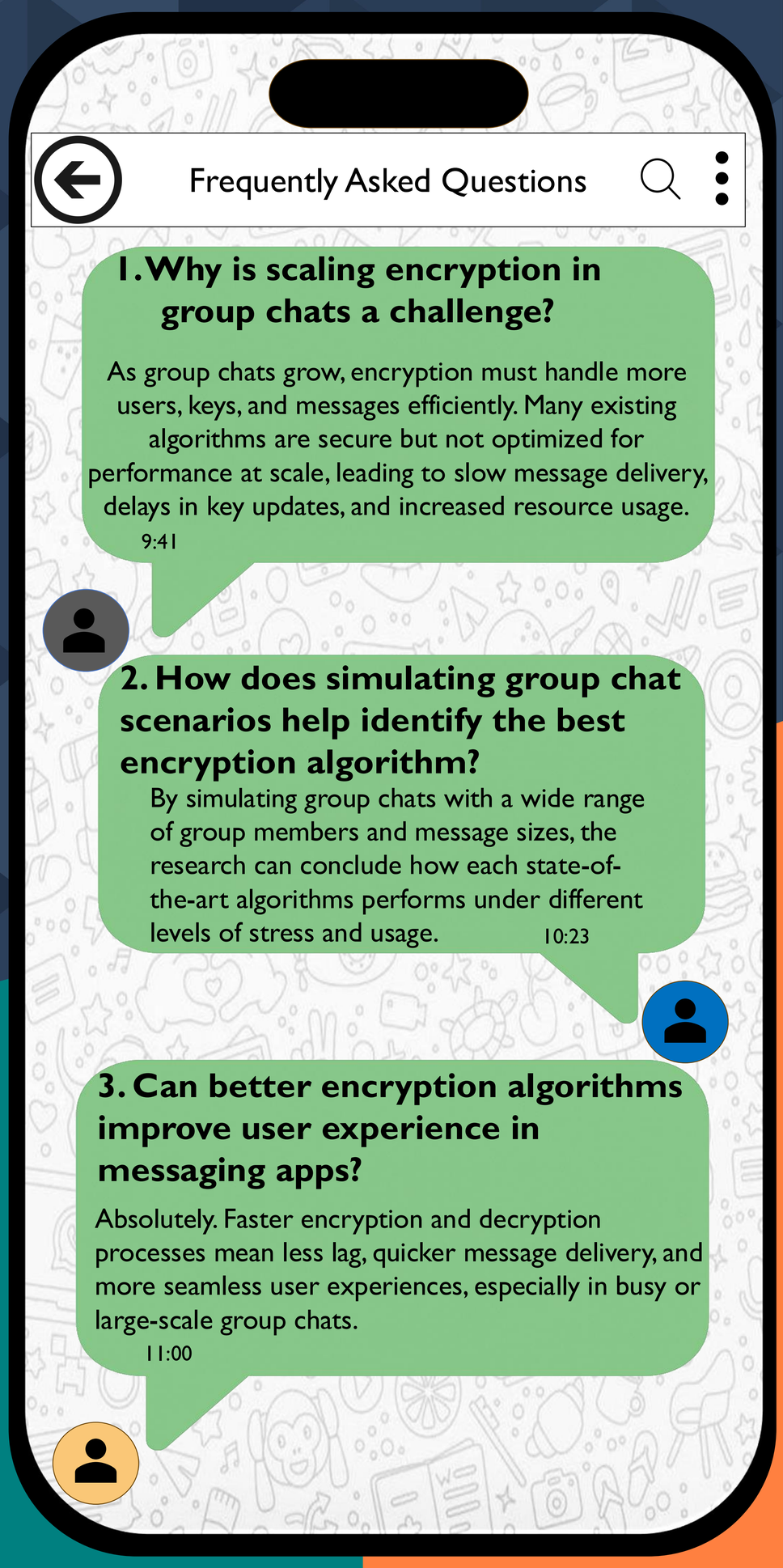
Conclusion: Our results show that there is no one-size-fits-all solution, trade-offs exist between **speed, scalability, and security**.

More results and information here

Information Security – Group 3

Maastricht University

Faculty of Science and Engineering
Computer Science



RESOURCES

1. K. Bhargavan, R. Barnes, and E. Rescorla, "Treekem: Asynchronous decentralized key management for large dynamic groups—a protocol proposal for messaging layer security (mls)," 2018, unpublished manuscript.
2. K. Klein et al., "Keep the dirt: Tainted treekem, adaptively and actively secure continuous group key agreement," in IEEE Symposium on Security and Privacy (SP), 2021.
3. B. Hamouda, "Comparative study of different cryptographic algorithms," Journal of Information Security, vol. 11, pp. 138–148, 2020.
4. S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for iot devices," in 2018 Long Island Systems, Applications and Technology Conference (LISAT), 2018.
5. A. Ghosh, "Comparison of encryption algorithms: Aes, blowfish and twofish for security of wireless net-works," ResearchGate, 2020.
6. Y. Shin, J. Hur, and H. Yoon, "Scalable and efficient approach for secure group communication," in International Symposium on Communications and Information Technologies, 2009.

Alexandru Lazarina, Vlad Manolescu, Amir Kalantarzadeh, Bati Gozen, Karol Plandowski, Aukje Heijthuijzen, Vilmos Udvari

Information Security – Group 3