

# WhatsUpp with Sender Keys?

## Analysis, Improvements and Security Proofs

David Balbás\*, Daniel Collins†, Phillip Gajland‡

\* IMDEA Software Institute & Universidad Politécnica de Madrid, Spain

† EPFL, Switzerland

‡ Max Planck Institute for Security and Privacy & Ruhr University Bochum, Germany



Work under submission!

### Group Messaging

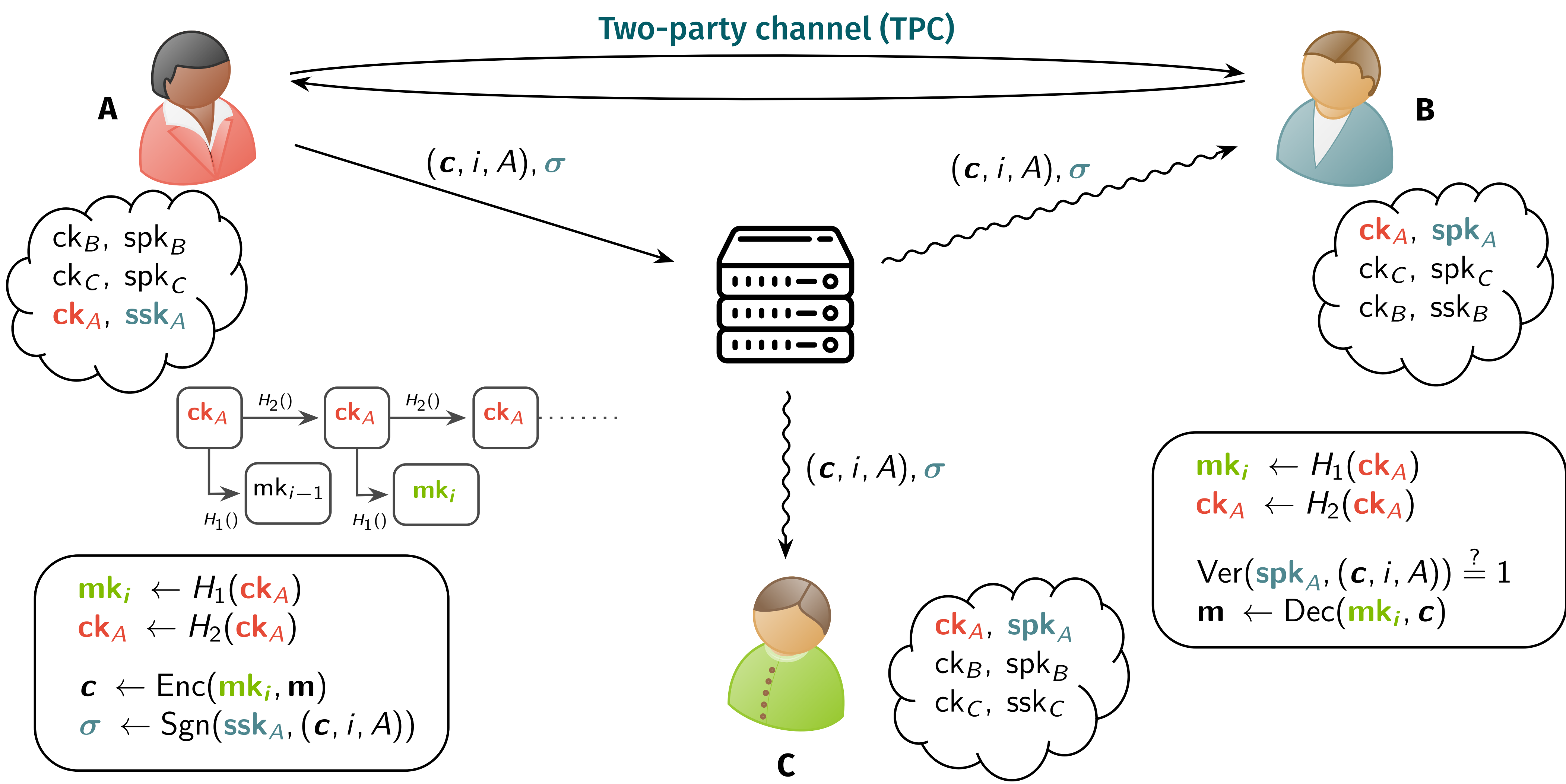
- Widely used messaging protocols claim security and end-to-end encryption. But this is vague and often misleading...
- For example, Telegram has no end-to-end encryption (in groups).
- Sender Keys** is the protocol used in WhatsApp and Signal for groups; surprisingly, **no formal analysis exists!**
- Known group messaging models [1, 2, 3] do not suit Sender Keys.
- Can we formalise Sender Keys in a meaningful security model?**

#### What is group messaging?

Secure, correct, asynchronous algorithms for:

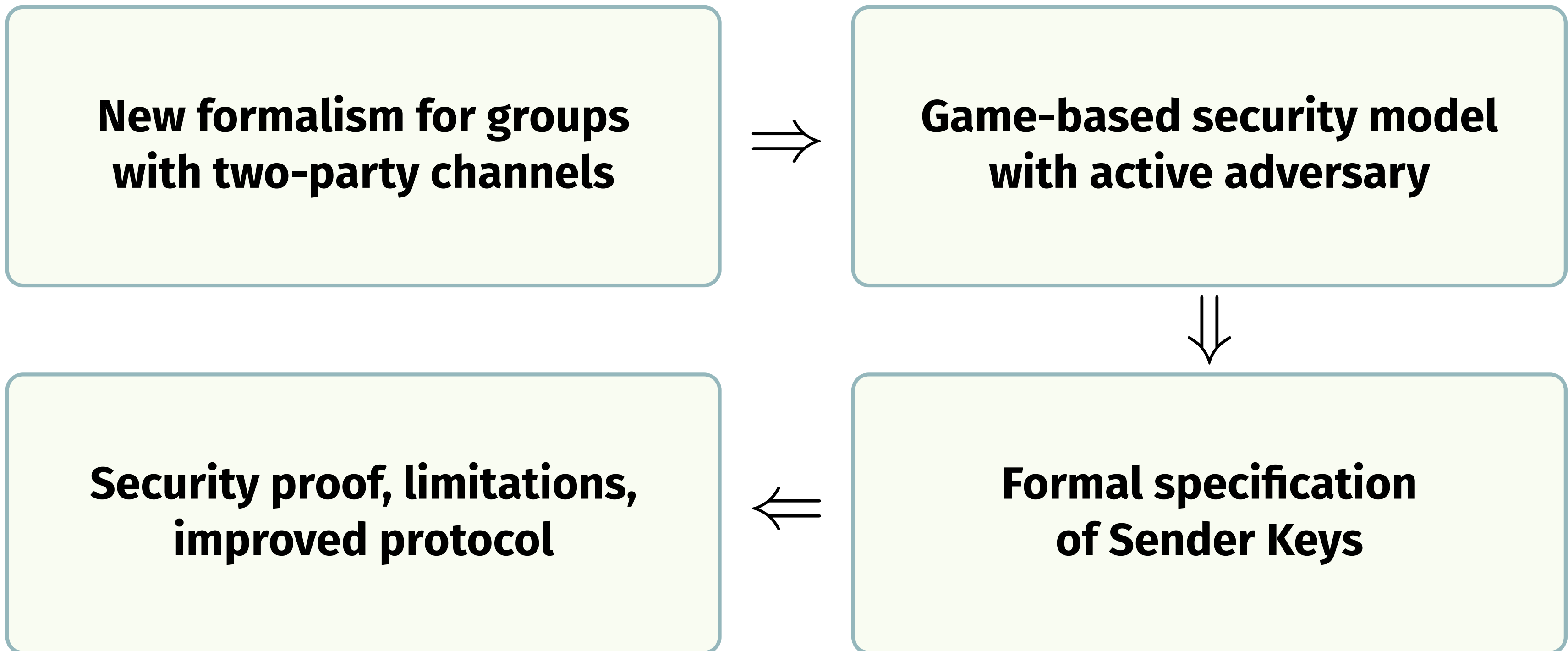
- Send:** message  $m$  encrypted  $\rightarrow C$ .
- Recv:** retrieve ciphertext  $C$ , decrypt it, and obtain the  $ID$  of the sender  $\rightarrow (m, ID)$ .
- Exec:** execute a group change: *create, add, remove or update*  $\rightarrow T$ .
- Proc:** process  $T$  and apply group change.

### Sender Keys



- Members share a **sender key**  $SK = (ck, spk)$  with everyone.
- $spk$  is a public signature key,  $ck$  is a symmetric **chain key**.
- A sends  $m$ :** Encrypts using a **message key**  $mk_i$  deterministically derived from  $ck_A$ . Ciphertext  $c$  signed ( $\sigma$ ) with  $spk_A$ .
- B & C receive:** Server broadcasts. B & C derive  $mk_i$ , check signature  $\sigma$  and decrypt  $c$ .
- Key agreement over “secure” two-party channels** between pairs. New keys sent after updates, adds, and removes.

### Results



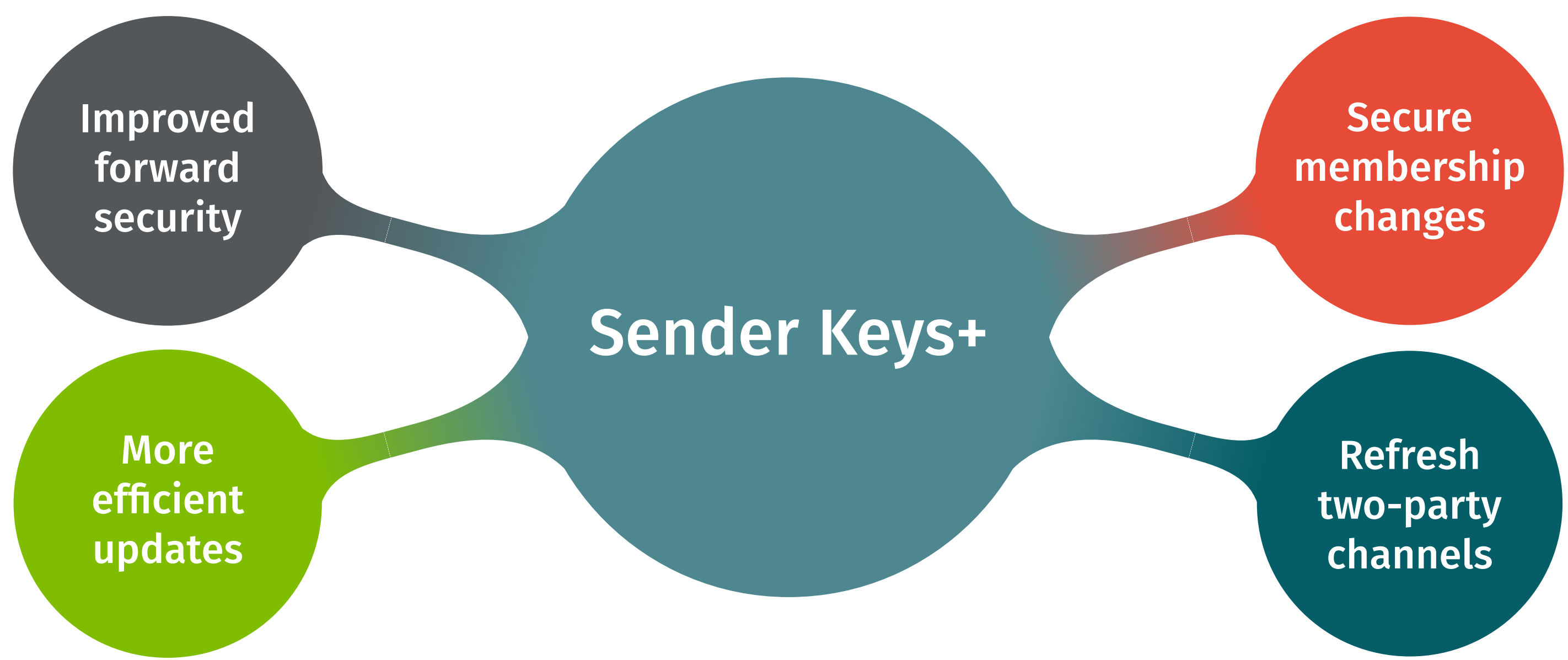
**Theorem 1:** Sender Keys is **secure** in our model - but with respect to a heavily **restricted adversary**.

#### Observations:

- Central server can fully control group membership.
- Stale two-party channels may leak sent keys.
- Forward security is sub-optimal.

**Theorem 2:** Our proposed Sender Keys+ is **more efficient** and secure w.r.t. a **stronger adversary!**

### Our Improved Protocol



### References

- [1] Joël Alwen, Sandro Coretti, Yevgeniy Dodis, and Yiannis Tselekounis. *Security analysis and improvements for the IETF MLS standard for group messaging*. CRYPTO, 2020.
- [2] Joël Alwen, Sandro Coretti, Yevgeniy Dodis, and Yiannis Tselekounis. *Modular Design of Secure Group Messaging Protocols and the Security of MLS*. CCS, 2021.
- [3] David Balbás, Daniel Collins, and Serge Vaudenay. *Cryptographic administration for secure group messaging*. USENIX Security, 2023.

