Consistent and Private Group Communication

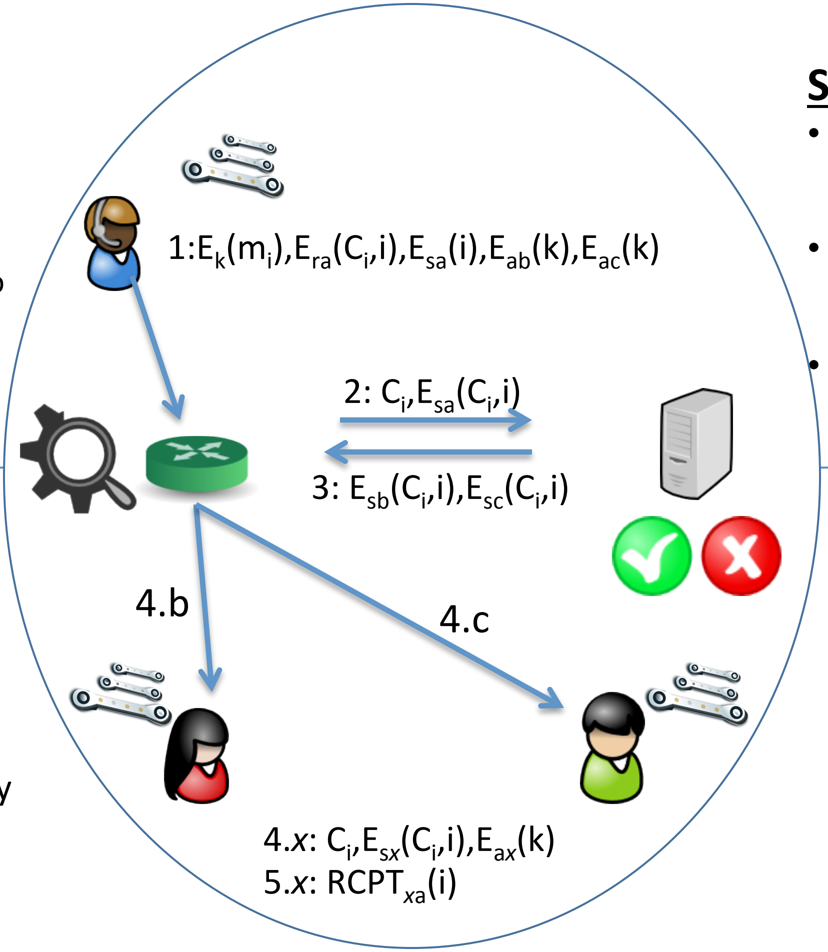
Challenge:

- Provide *conversational integrity, deniability, and authentication* in end-to-end encrypted group messaging
- Provide useable support for group messaging
- Scale to other group settings, e.g. video, online forums, mailing lists

Solution:

- "Mobile messaging" model with synchronous server-client setting
- Non-colluding servers for conversational integrity
- Relaxed notions of deniability required for scaling

1814753: University of Minnesota,
PI: Nicholas Hopper;
hoppernj@umn.edu



1:$E_k(m_i),E_{ra}(C_i,i),E_{sa}(i),E_{ab}(k),E_{ac}(k)$

2: $C_i,E_{sa}(C_i,i)$

3: $E_{sb}(C_i,i),E_{sc}(C_i,i)$

4.b

4.c

4.x: $C_i,E_{sx}(C_i,i),E_{ax}(k)$
5.x: $RCPT_{xa}(i)$

Scientific Impact:

- New security notions, lower bounds for group communication schemes
- New methods for assessing, modeling security of existing protocols
- Provably secure protocols for private group communication

Broader Impact:

- Open-source protocol and system implementations
- Identification and mitigation of vulnerabilities in existing tools
- Contribution to developing standards, e.g. Messaging Layer Security (MLS)