The Complexities of Healing in Secure Group Messaging: Why Cross-Group Effects Matter

USENIX 2021

Cas Cremers

CISPA Helmholtz Center for Information Security

Britta Hale*

Naval Postgraduate School (NPS)

Konrad Kohbrok

Aalto University

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

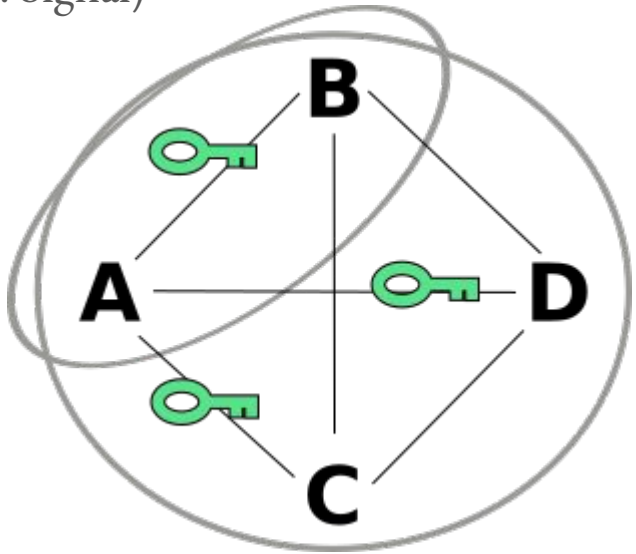
Two Group Messaging Paradigms

Groups are made of 1-to-1 connections
(e.g. Signal)

Group states are independent
(e.g. MLS Draft 11, ART)

Two Group Messaging Paradigms

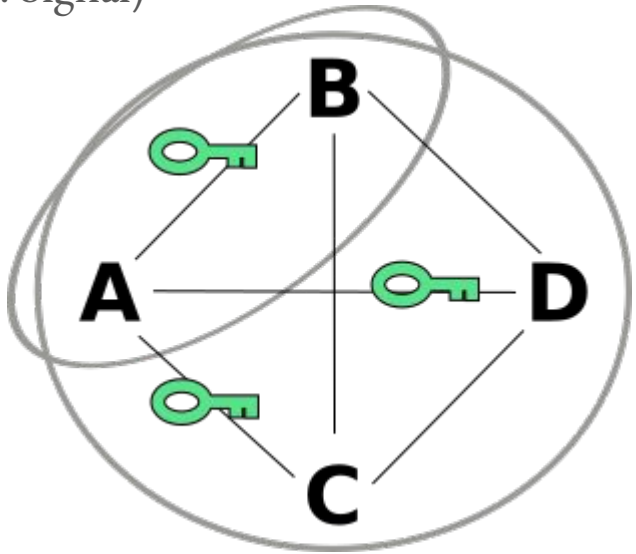
Groups are made of 1-to-1 connections
(e.g. Signal)



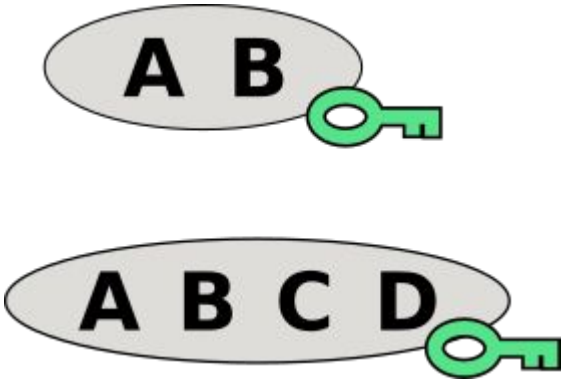
Group states are independent
(e.g. MLS Draft 11, ART)

Two Group Messaging Paradigms

Groups are made of 1-to-1 connections
(e.g. Signal)



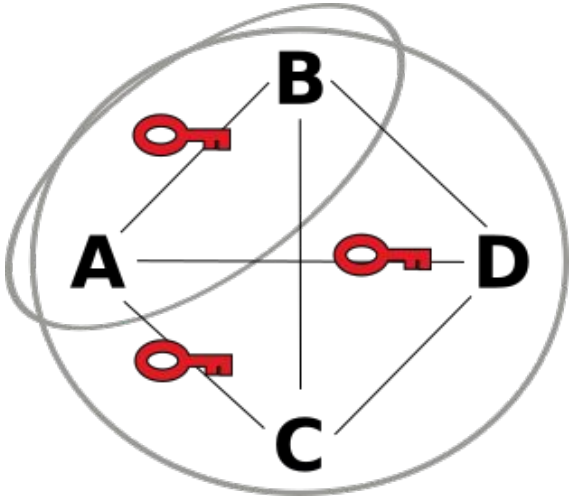
Group states are independent
(e.g. MLS Draft 11, ART)

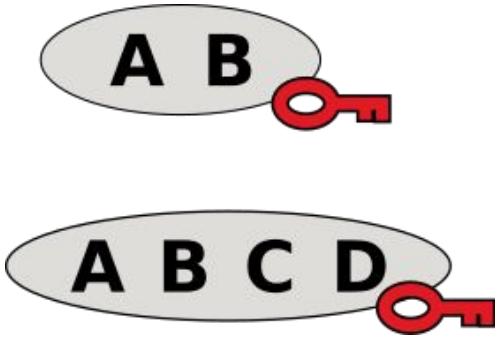


Post-Compromise Security (PCS)

Post-Compromise Security (PCS)

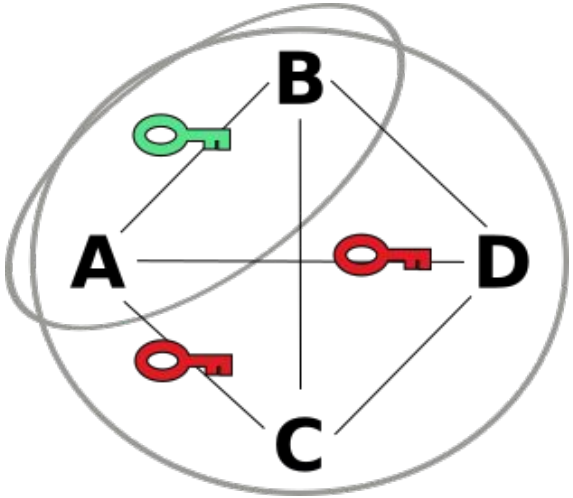
- A is compromised

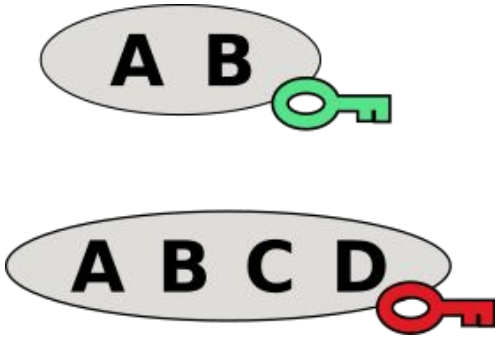




Post-Compromise Security (PCS)

- A is compromised
- (Adversary is passive)
- A sends an update to B

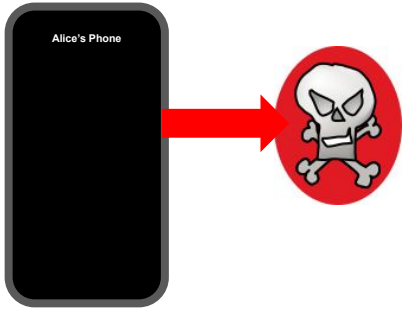




Alice, the CEO, is returning from a business meeting

On the way back, her phone is compromised and all data extracted.

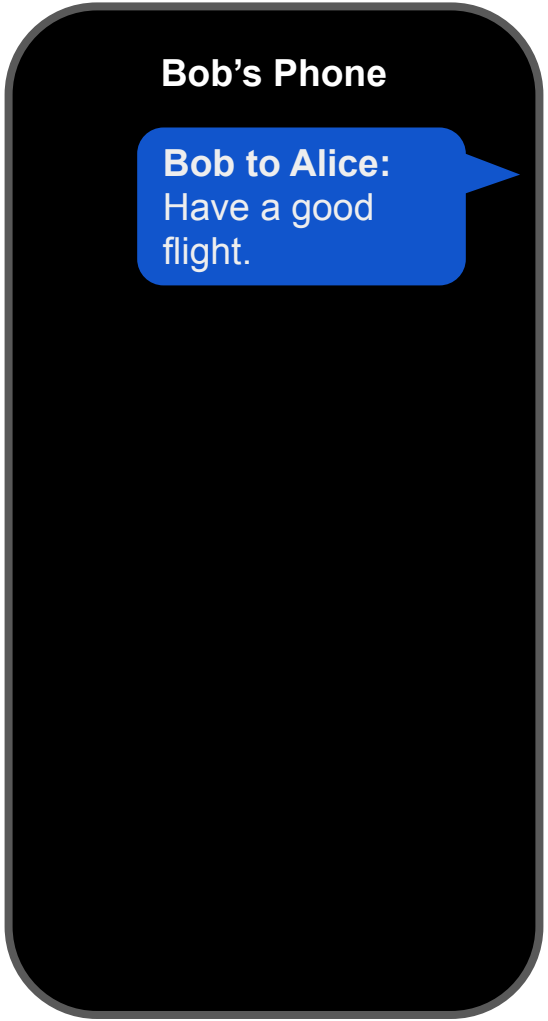
Source:
https://en.wikipedia.org/wiki/File:Heathrow_Terminal_5_ePassport_gates.jpg



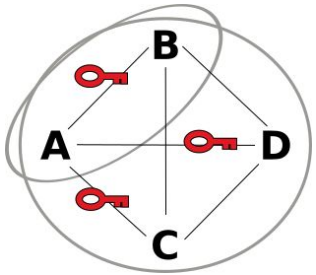
Source:
https://commons.wikimedia.org/wiki/File:011_Aircraft_of_various_airlines_together_at_Narita_Airport,_Japan._Swiss_Air_Lines,_United_Airlines,_Thai_Airways.JPG

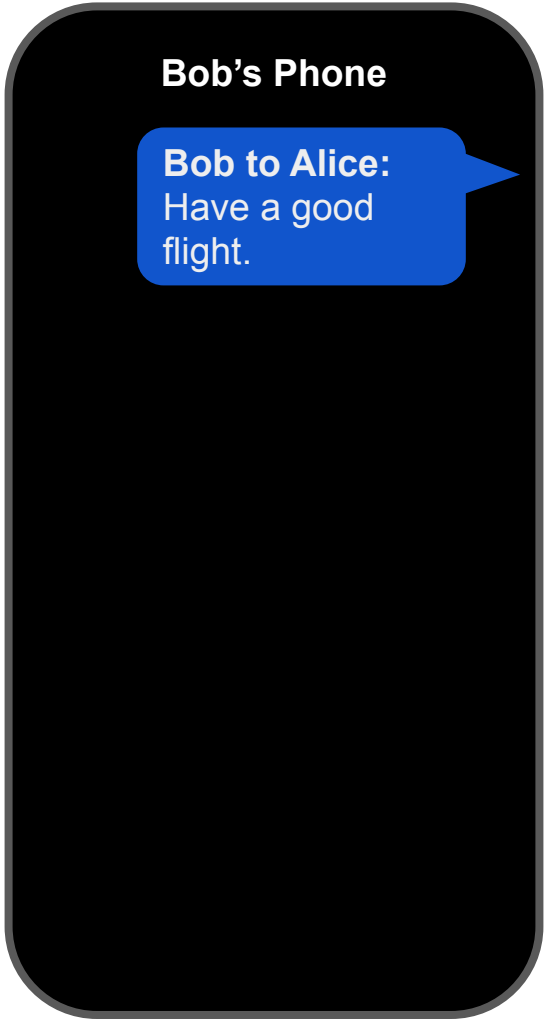
Groups using 1-1 keys

Groups using group keys

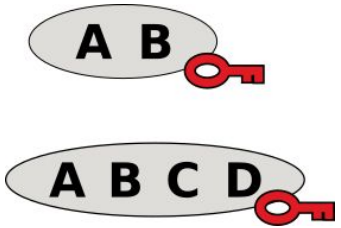


Groups using 1-1 keys

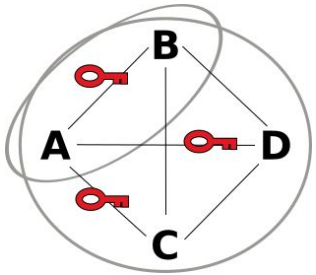




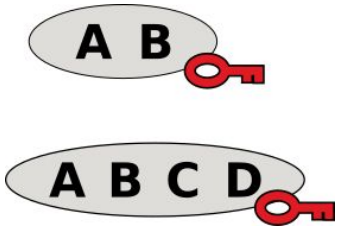
Groups using group keys



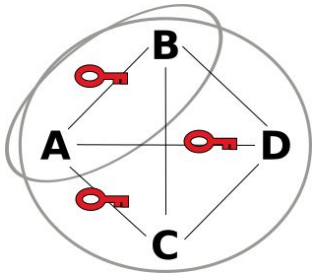
Groups using 1-1 keys



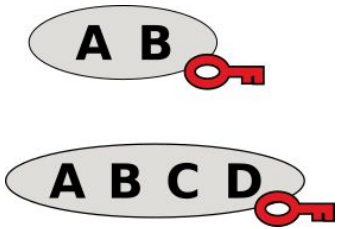
Groups using group keys



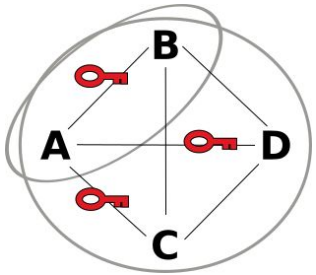
Groups using 1-1 keys

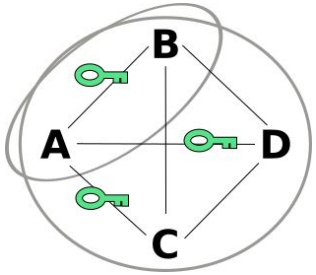


Groups using group keys

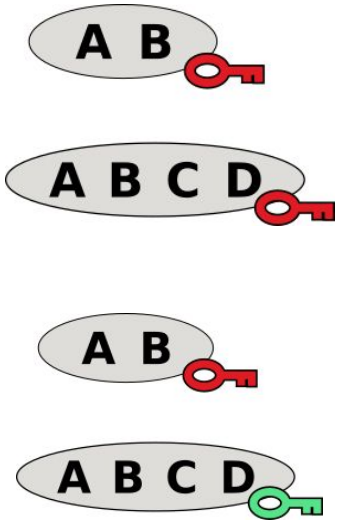


Groups using 1-1 keys

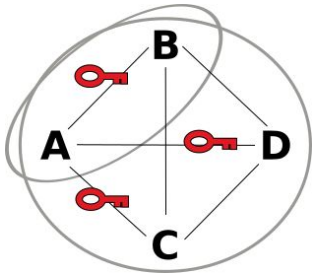


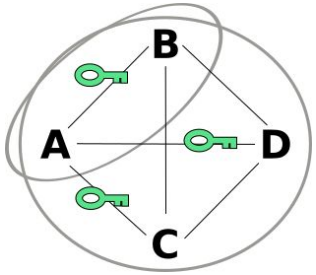


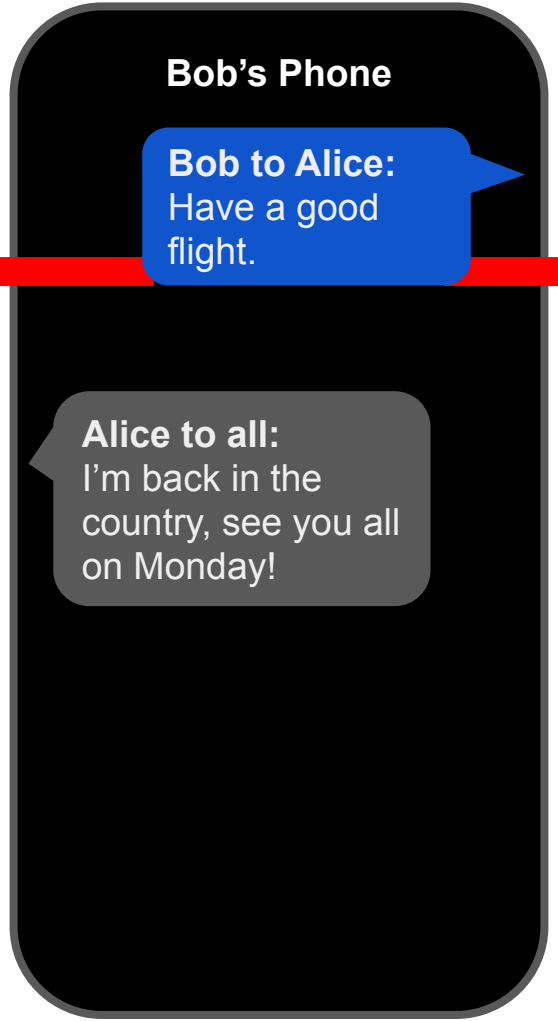
Groups using group keys



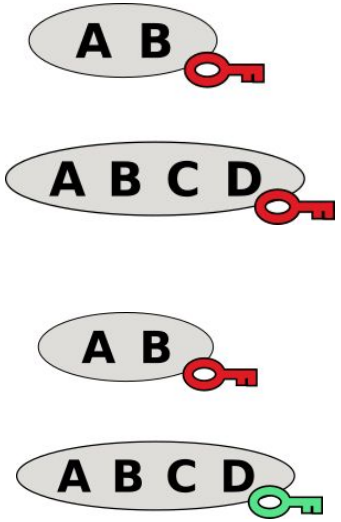
Groups using 1-1 keys



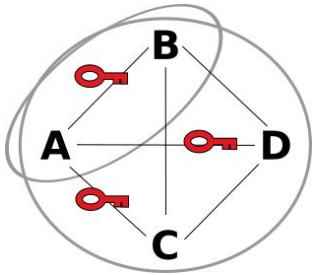


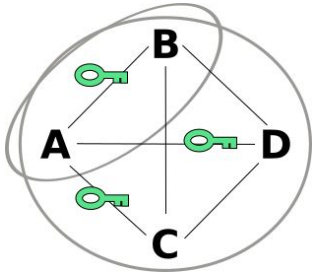


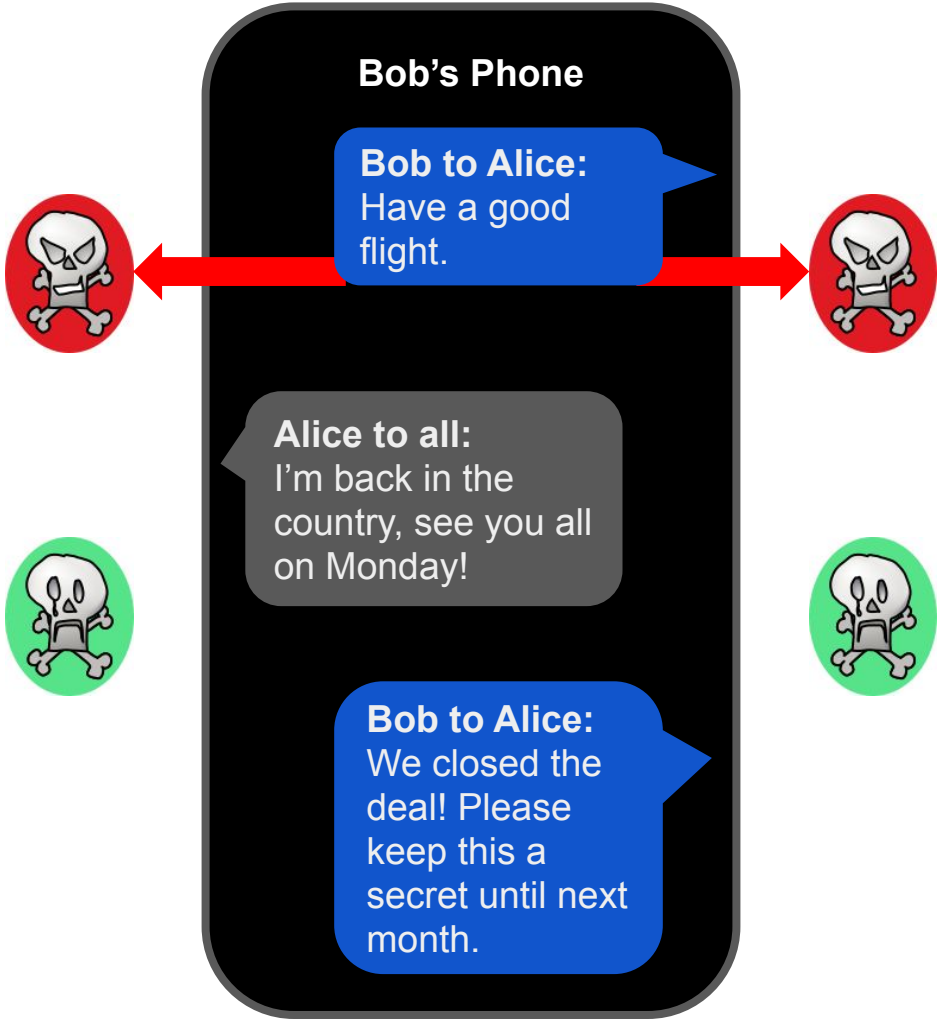
Groups using group keys



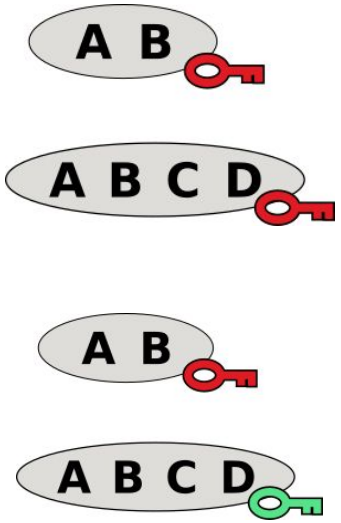
Groups using 1-1 keys



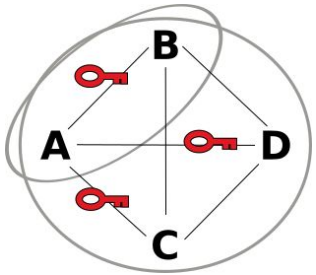


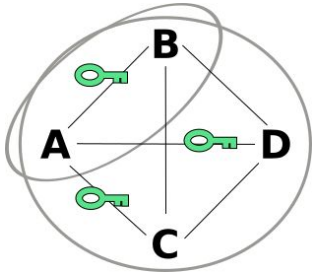


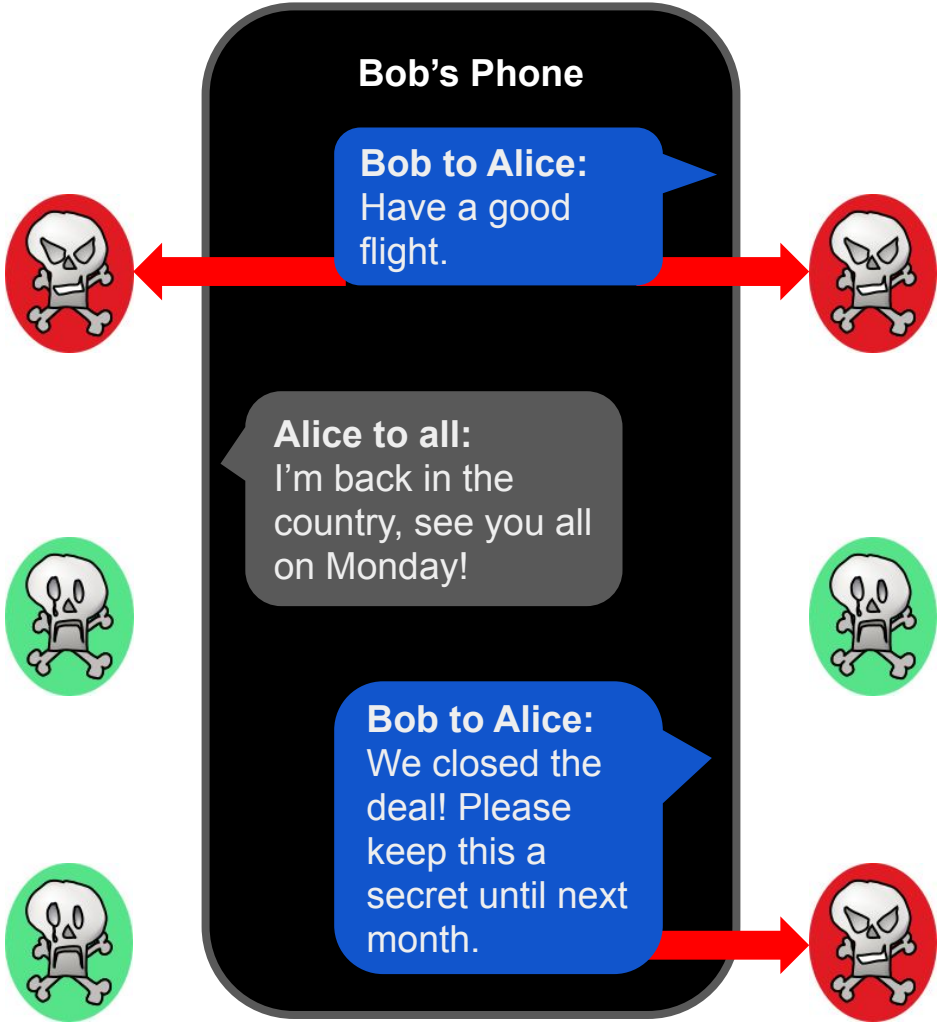
Groups using group keys



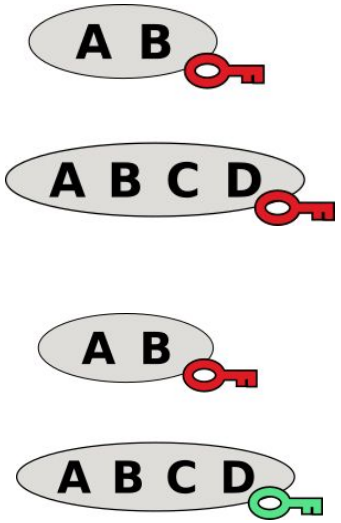
Groups using 1-1 keys



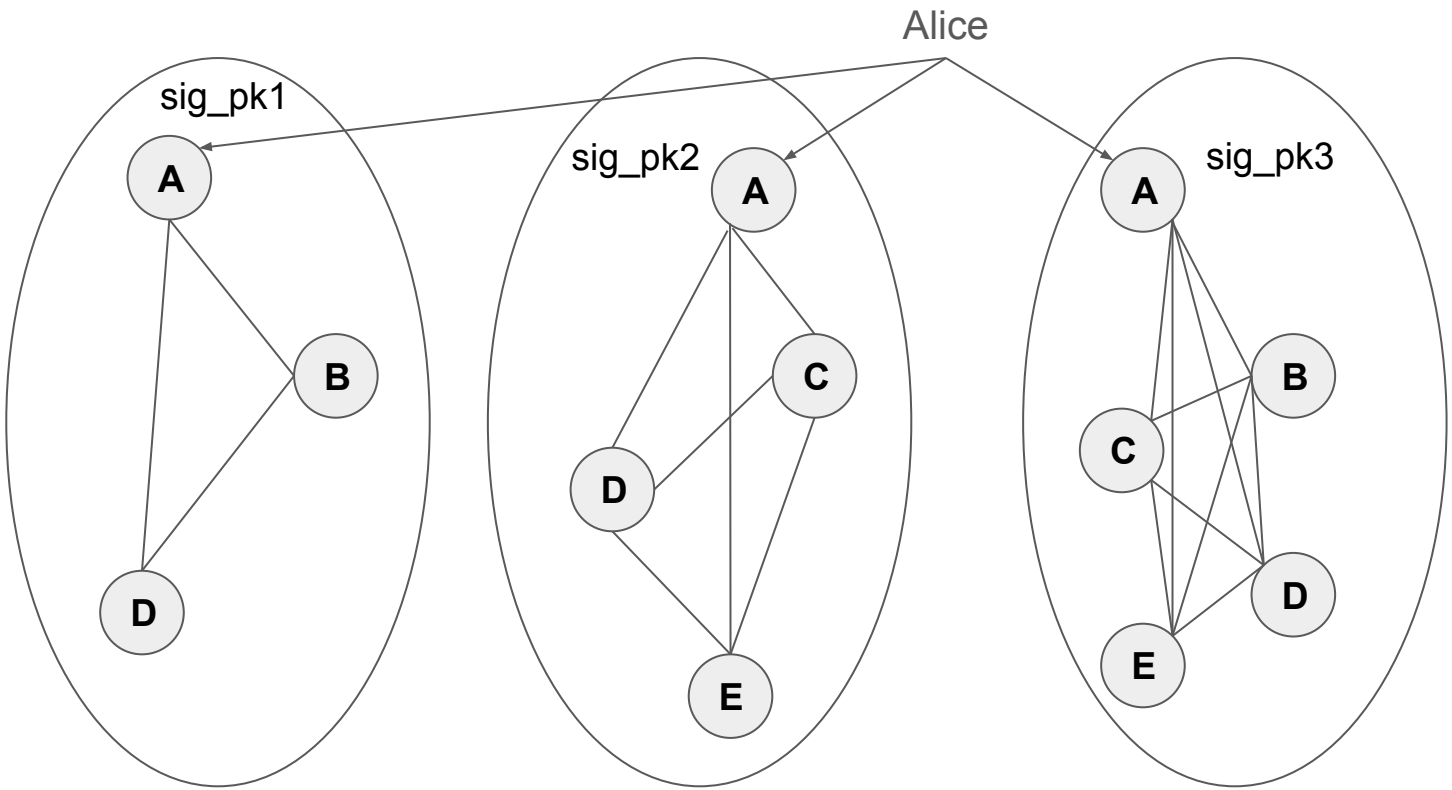


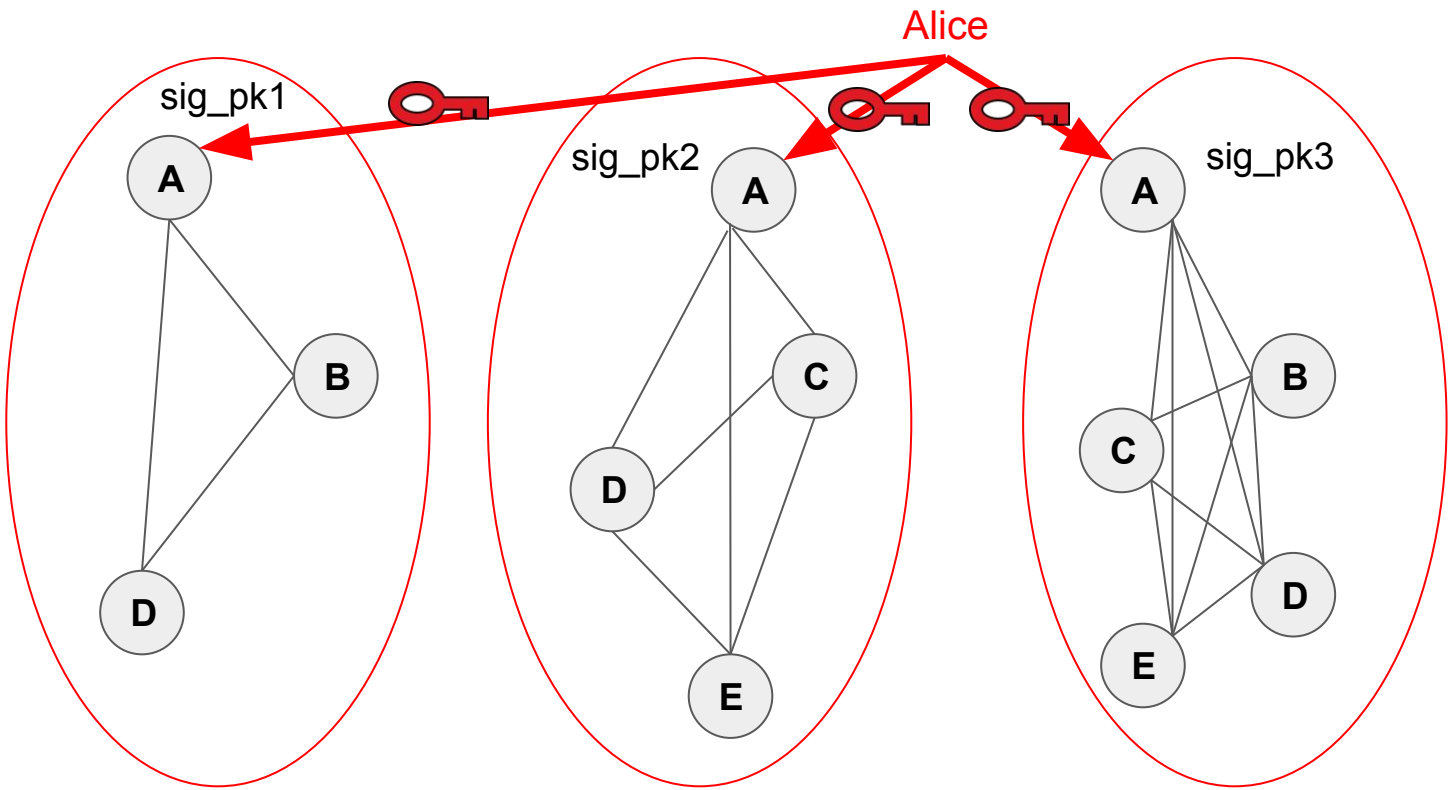


Groups using group keys

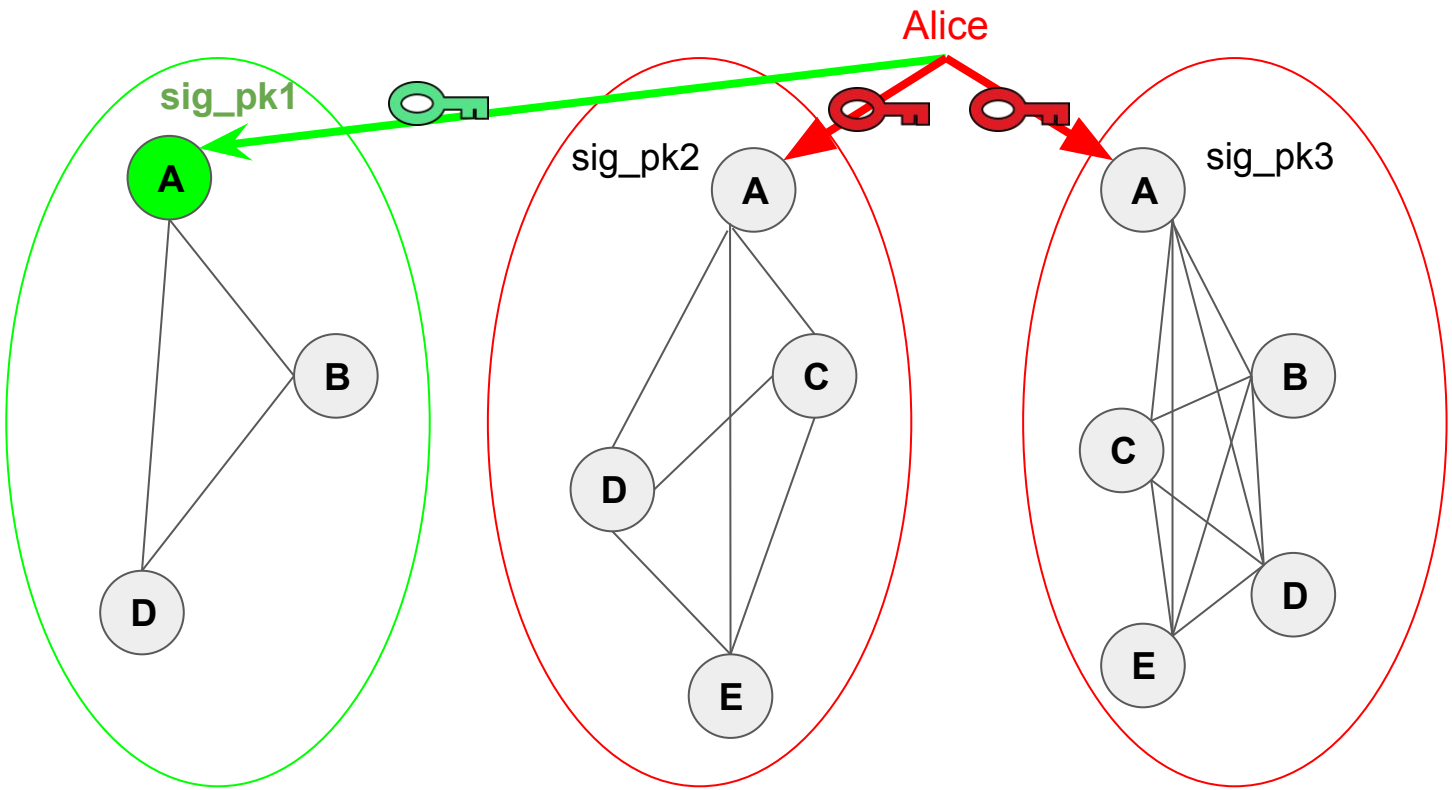


Design Space

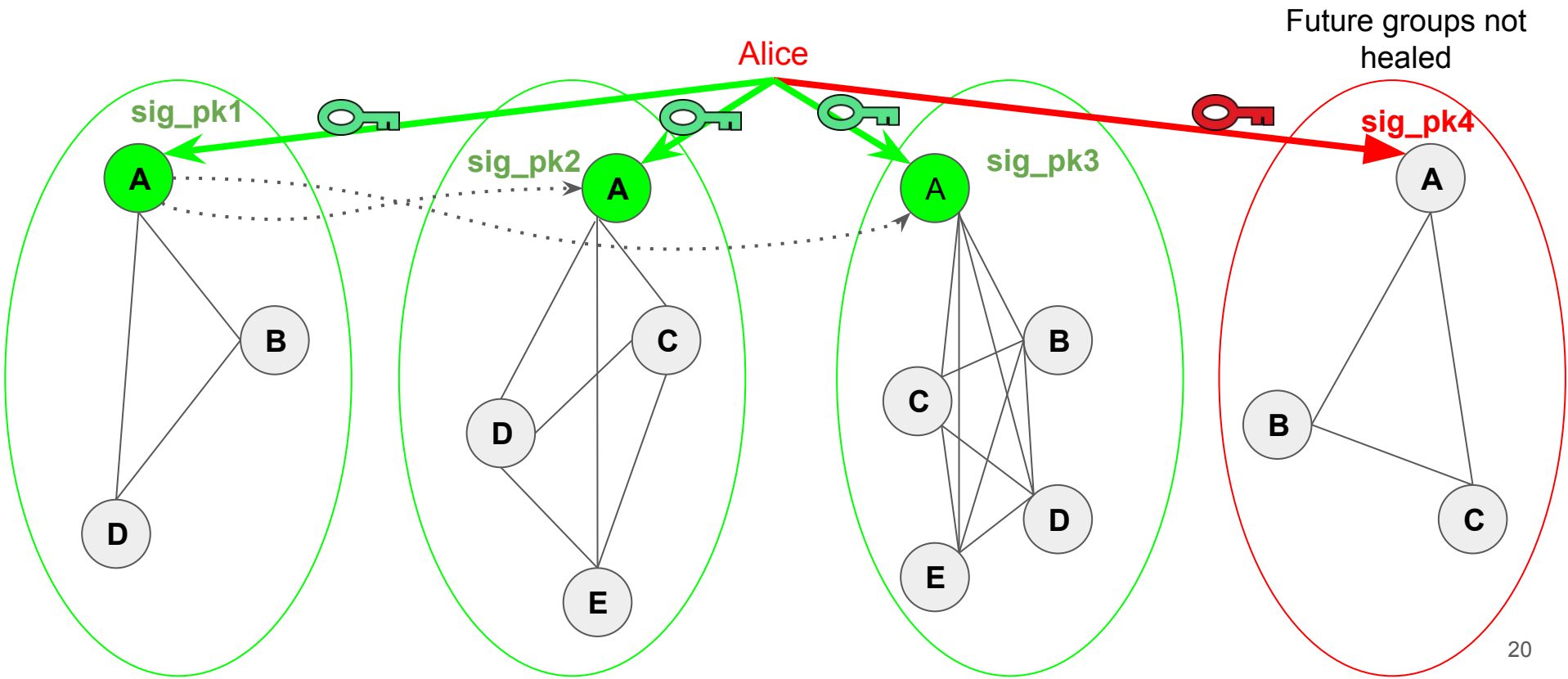



Alice
sig_pk1
A
B
D
sig_pk2
A
C
D
E
sig_pk3
A
B
C
D
E

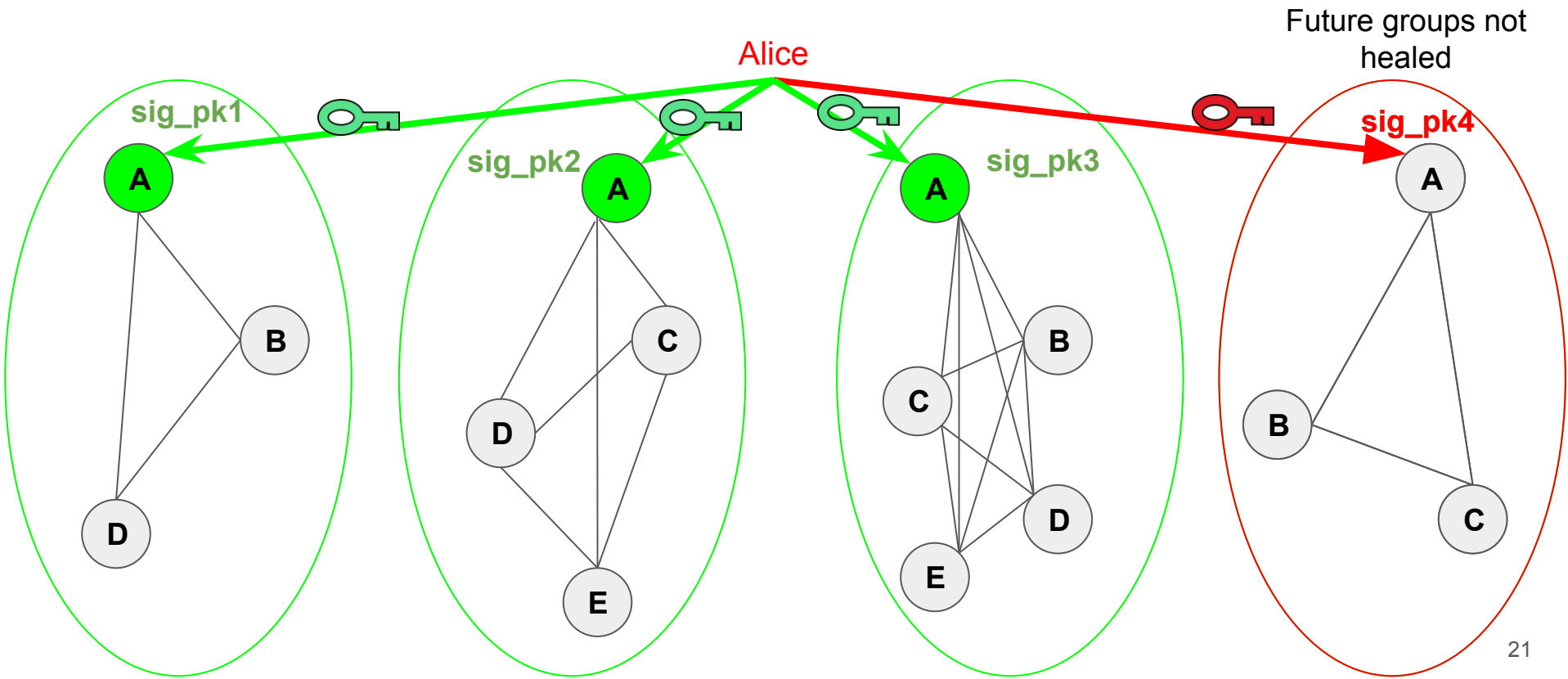
Heal per group



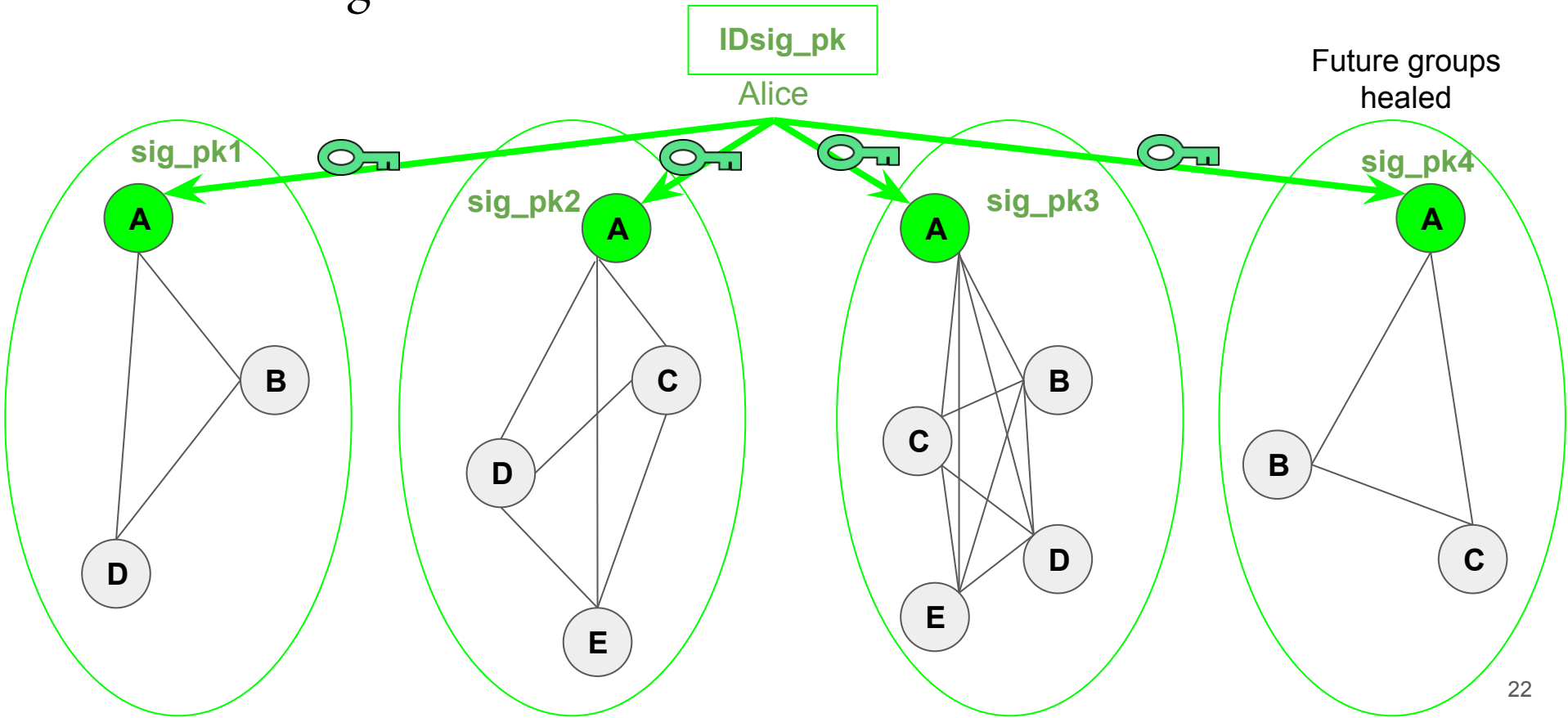
Healing in one group prompts healing in others



Periodic healing in all groups



Global healing



Design Space

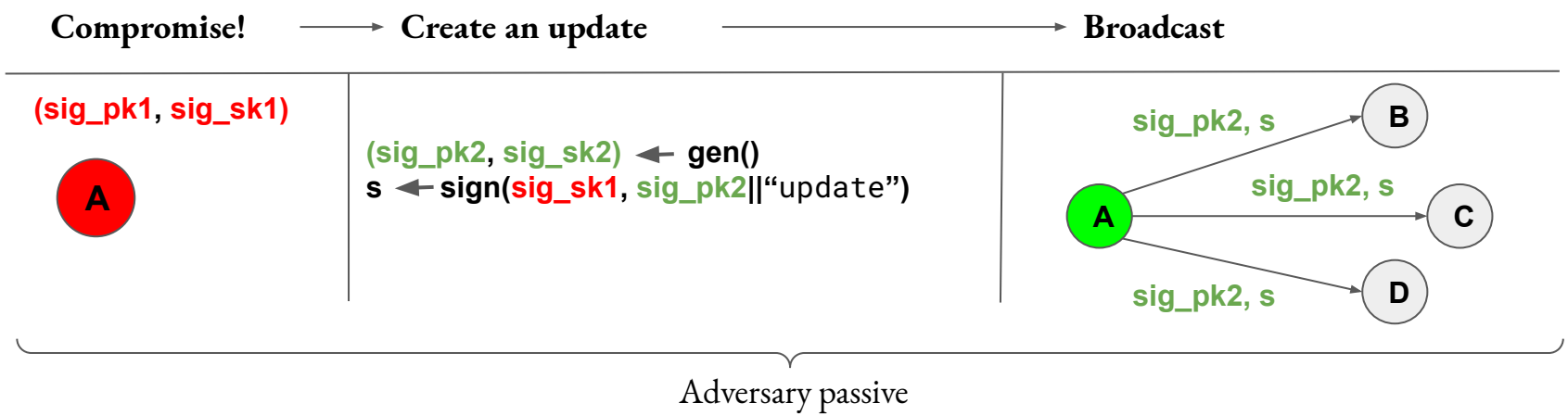
	Scheduling Updates for Confidentiality Keys		
	Communication Activity Related		Periodic
Keys updated	Within group i	Within any group	Epoch-based
Sym. group key: gk^i	Heal conf: group i 2nd Group Attack/NF $O(1)$ Sym. Updates	Heal conf: all groups InfoLeak/NF $O(N)$ Sym. Updates	Heal conf: all groups NF $O(N)$ Sym. Updates

	Scheduling Updates for Authentication Keys		
	Communication Activity Related		Periodic
Keys updated	Within group i	Within any group	Epoch-based
Asym. group key pair: (sk_A^i, pk_A^i)	Heal auth: group i 2nd Group Attack/NF $O(1)$ Asym. Updates	Heal auth: all groups InfoLeak/NF $O(N)$ Asym. Updates	Heal auth: all groups NF $O(N)$ Asym. Updates
Asym. global key pair: (sk_A, pk_A)		Heal auth: all groups + F InfoLeak $O(1)$ Asym. Updates	Heal auth: all groups + F $O(1)$ Asym. Updates

Post-Compromise Secure Signatures

- PCS is an accepted confidentiality security guarantee → can also be applied to *authenticity*!
- Captures forgeries following a successful key update during an passive adversarial phase

Simple scheme: Rotating Signatures: New signature keys signed by old signature keys



The Complexities of Healing in Secure Group Messaging: Why Cross-Group Effects Matter

Check out the paper for more!

- Further attack scenarios and distinctions between the security of pairwise and group approaches
- Exploration of impacts of authentication and confidentiality, update distinctions and impacts
- PCS-SIG security experiment, realizable under further constructions
- How PCS-SIG security fits with existing messaging protocols
- Instantiation and proof of PCS-SIG

Contact:

Cas Cremers
cremers@cispa.de

Britta Hale
britta.hale@nps.edu

Konrad Kohbrok
konrad.kohbrok@datashrine.de