Message Encryption

Trevor Perrin

2 Perspectives

- Key management
- Protocols

Key Management

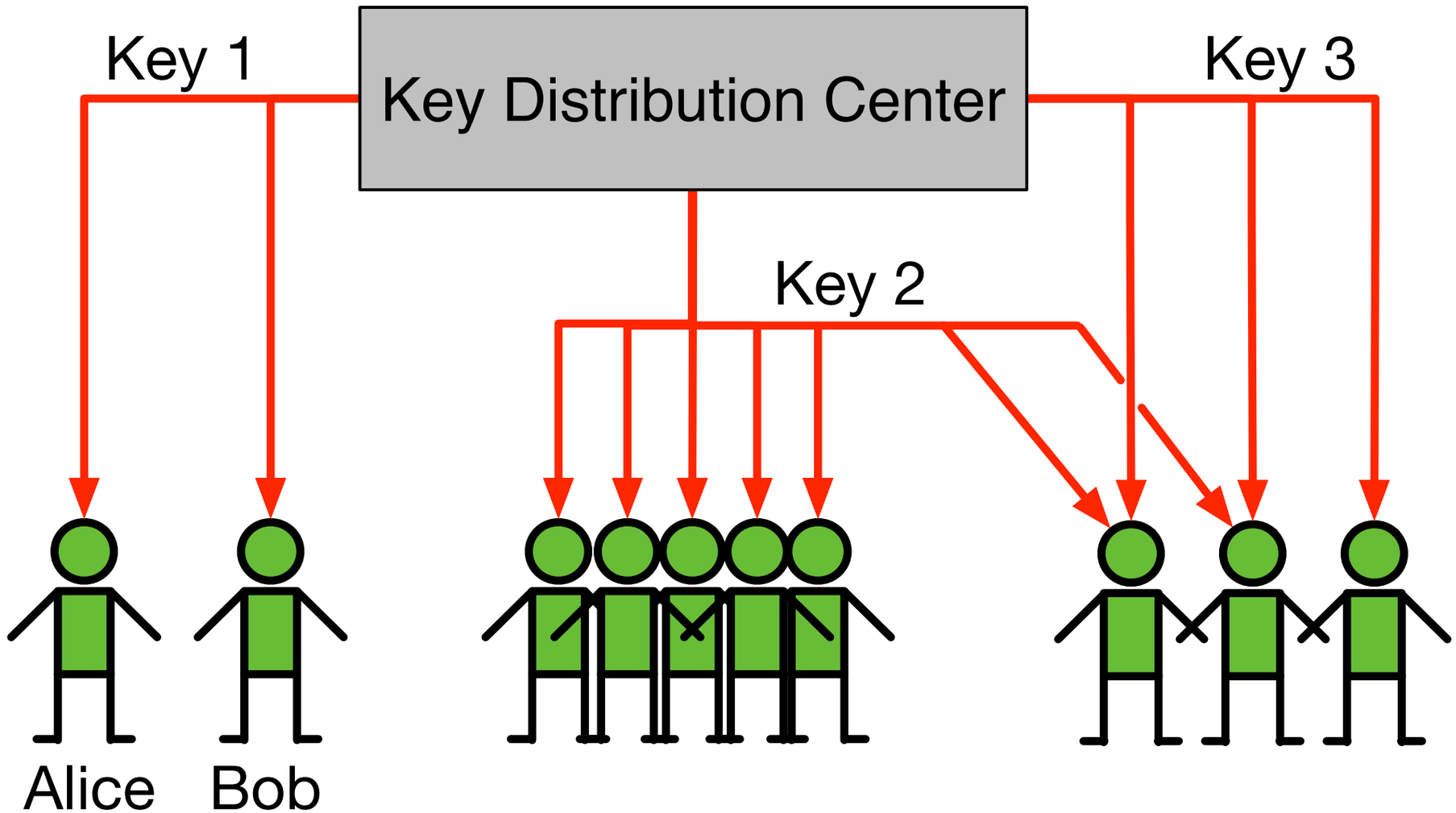
< 20th Century

- Manual ciphers
  - Higher security = harder to use
- Codebooks
  - Expensive to create

1900…1940s

- Radio, World Wars
- WWII
  - One time pads *(high-level, or spies)*
  - Cipher machines *(all levels)*
  - Manual ciphers and codebooks *(low-level)*

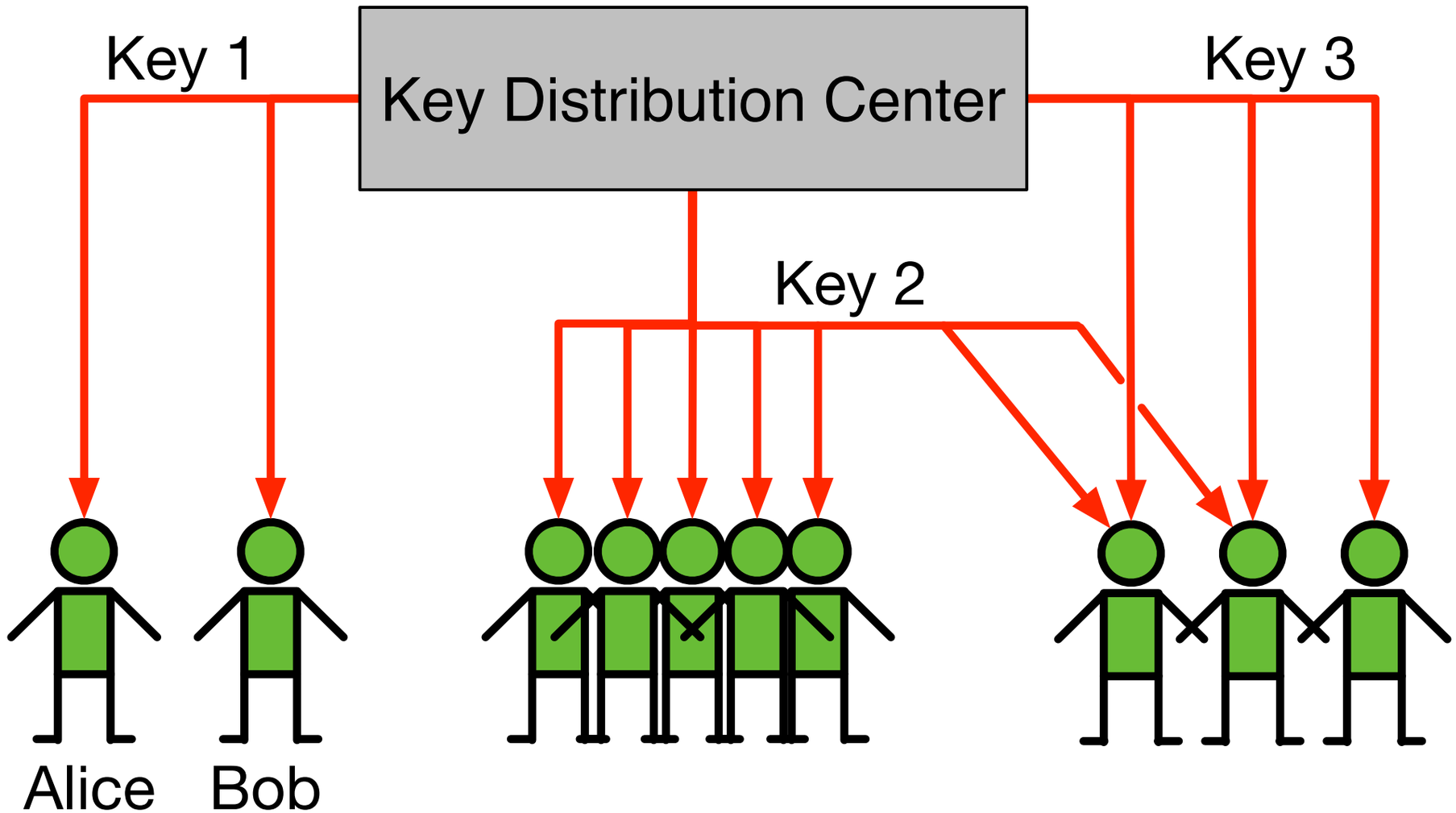
...1940s



1950s…1970s

- Modern symmetric encryption
- Electronic stream ciphers
- Small keys and random nonces
- Strong security models

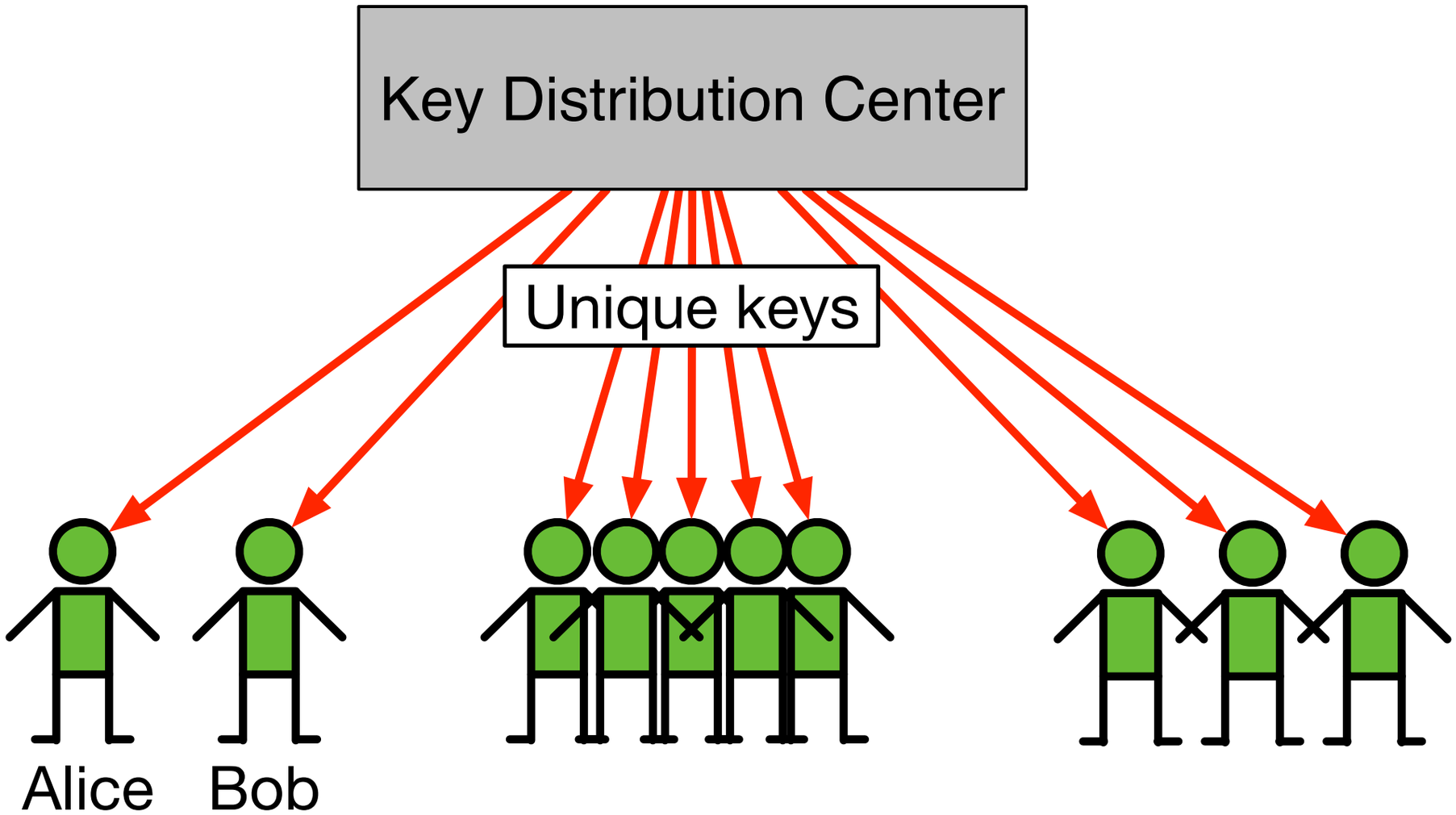
1950s…1970s



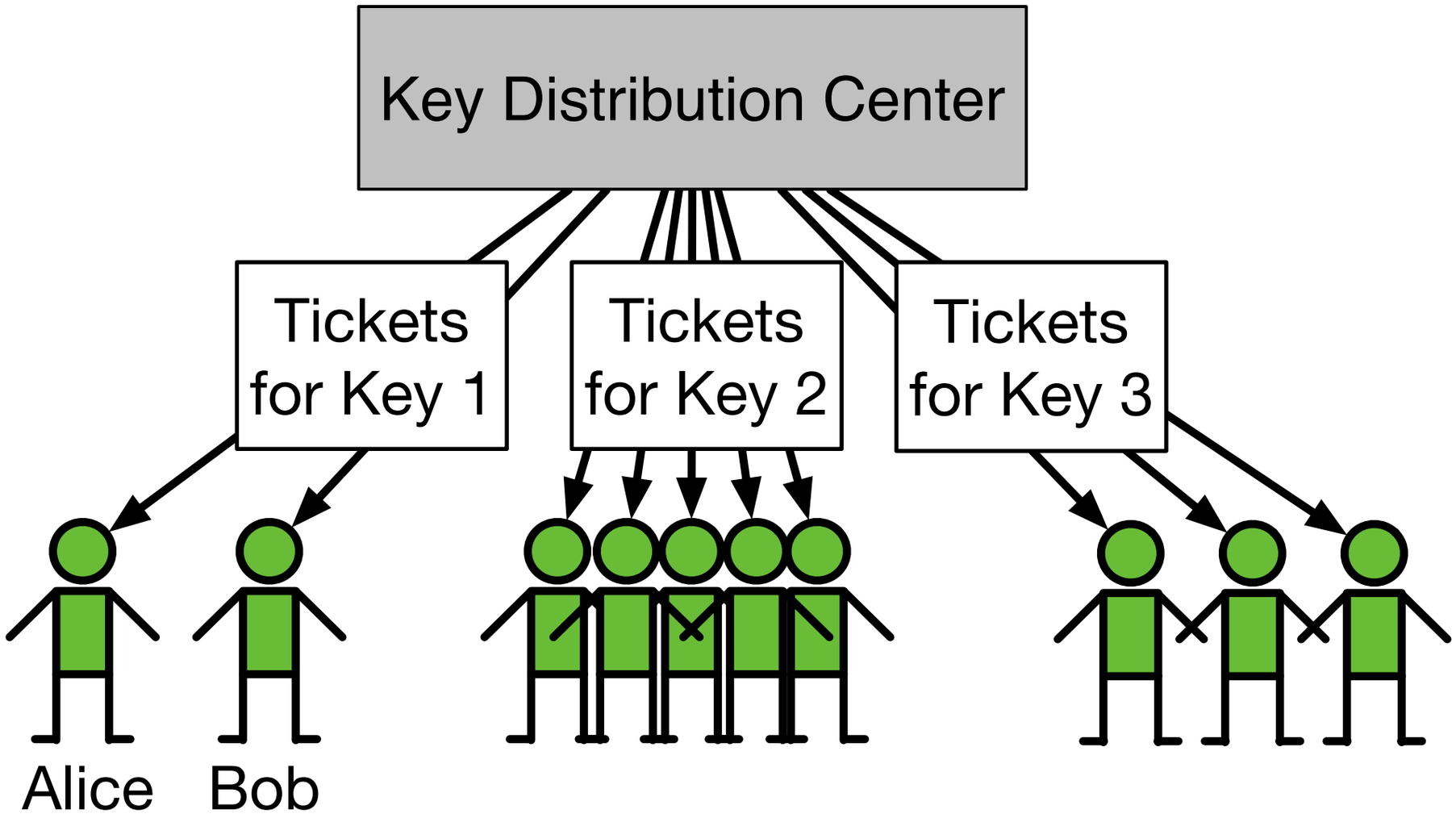
1980s

Symmetric Key Infrastructure (SKI)

1980s (SKI 1/2)



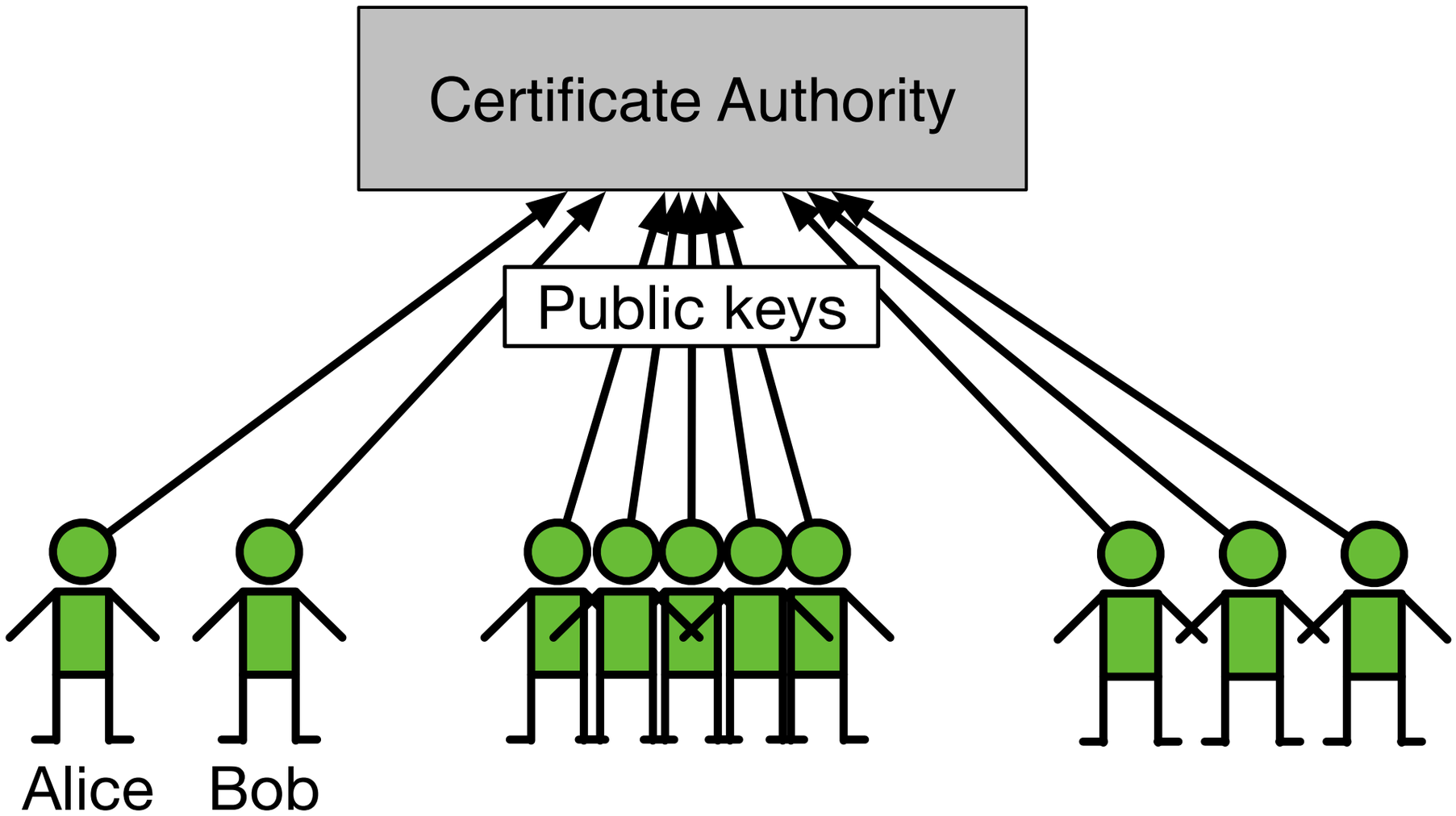
1980s (SKI 2/2)


Key Distribution Center
Tickets for Key 1
Tickets for Key 2
Tickets for Key 3
Alice
Bob

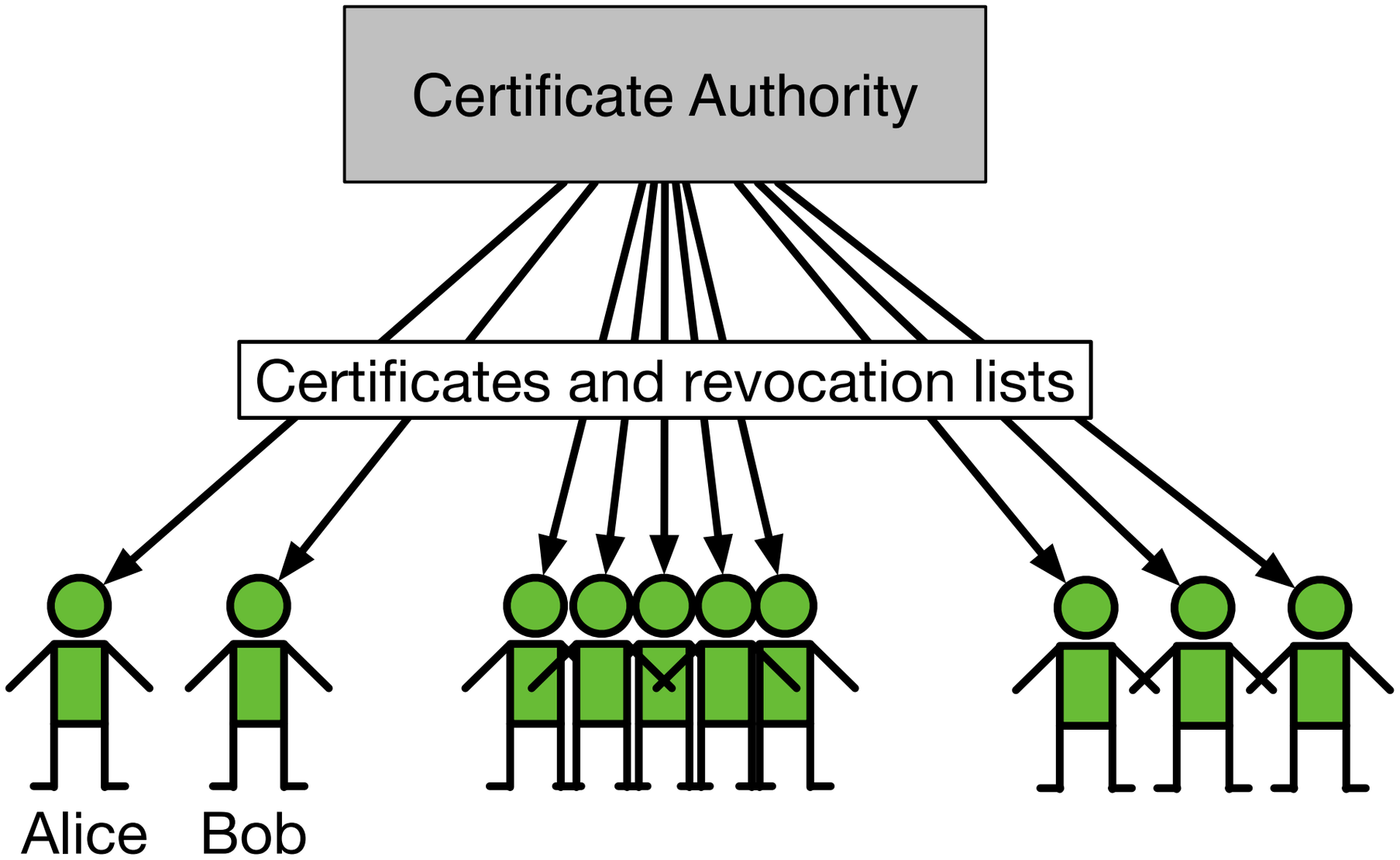
1990s

Public Key Infrastructure (PKI)

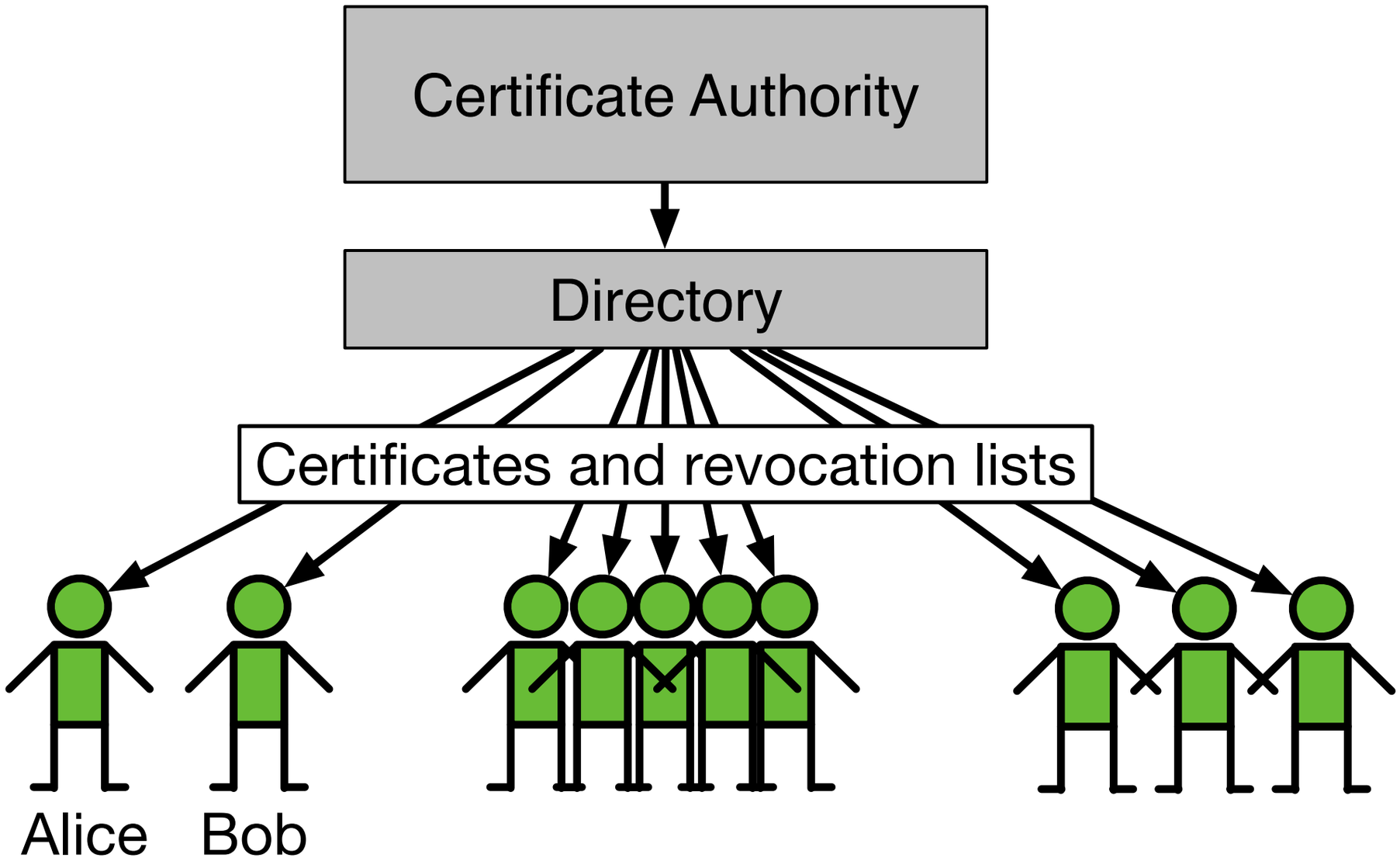
1990s (PKI 1/2)



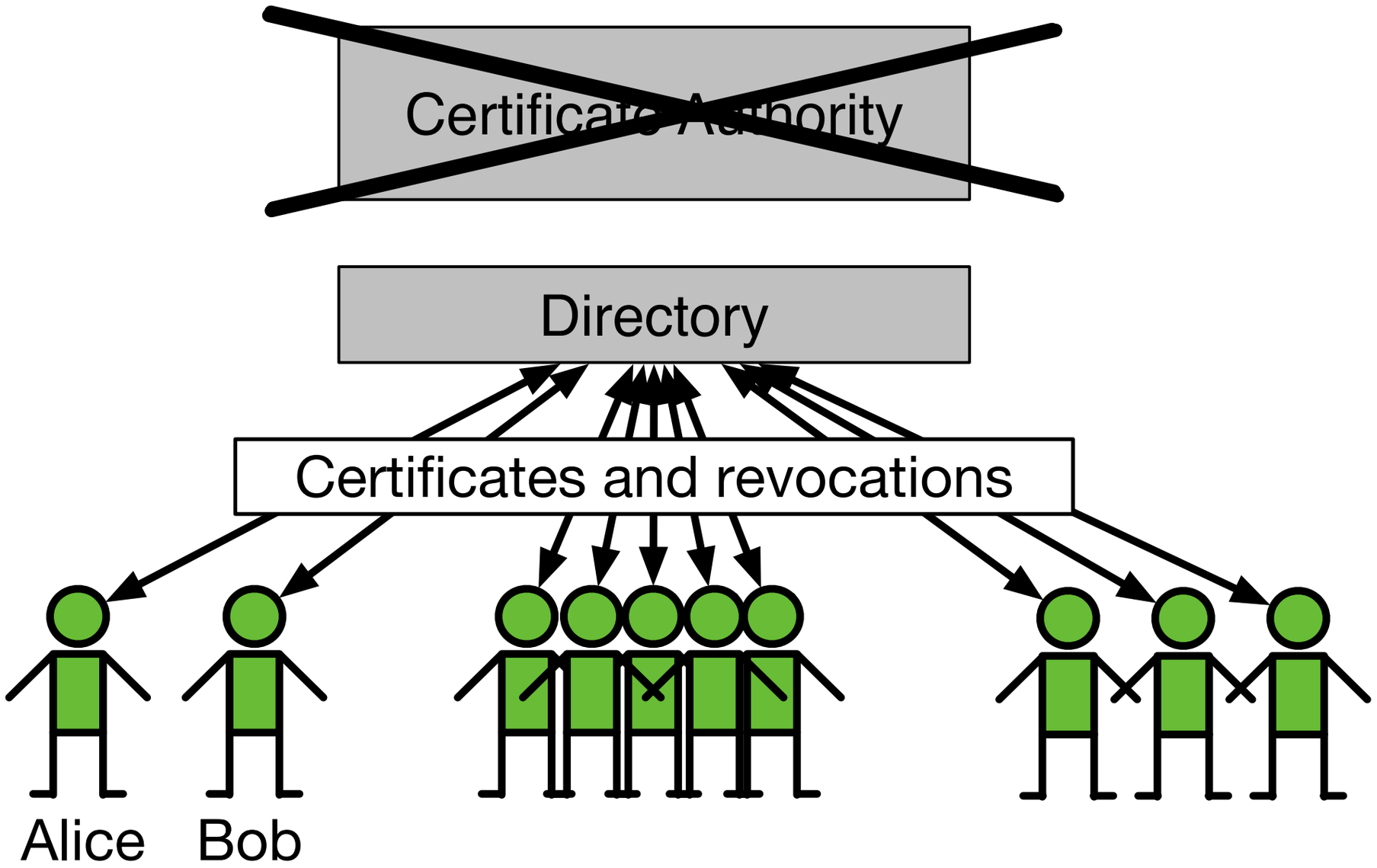
1990s (PKI 2/2)


Certificate Authority
Certificates and revocation lists
Alice
Bob

1990s (PKI 2/2)


Certificate Authority
Directory
Certificates and revocation lists
Alice
Bob

1990s (PGP)


Certificate Authority
Directory
Certificates and revocations
Alice
Bob

2000s

Disillusionment

2010s

Resurgence

2010s

- Awareness of massive breaches and mass surveillance
- Mobile messaging apps

2010s

Encrypted Messaging Apps

●●○○○ AT&T LTE 11:00 PM

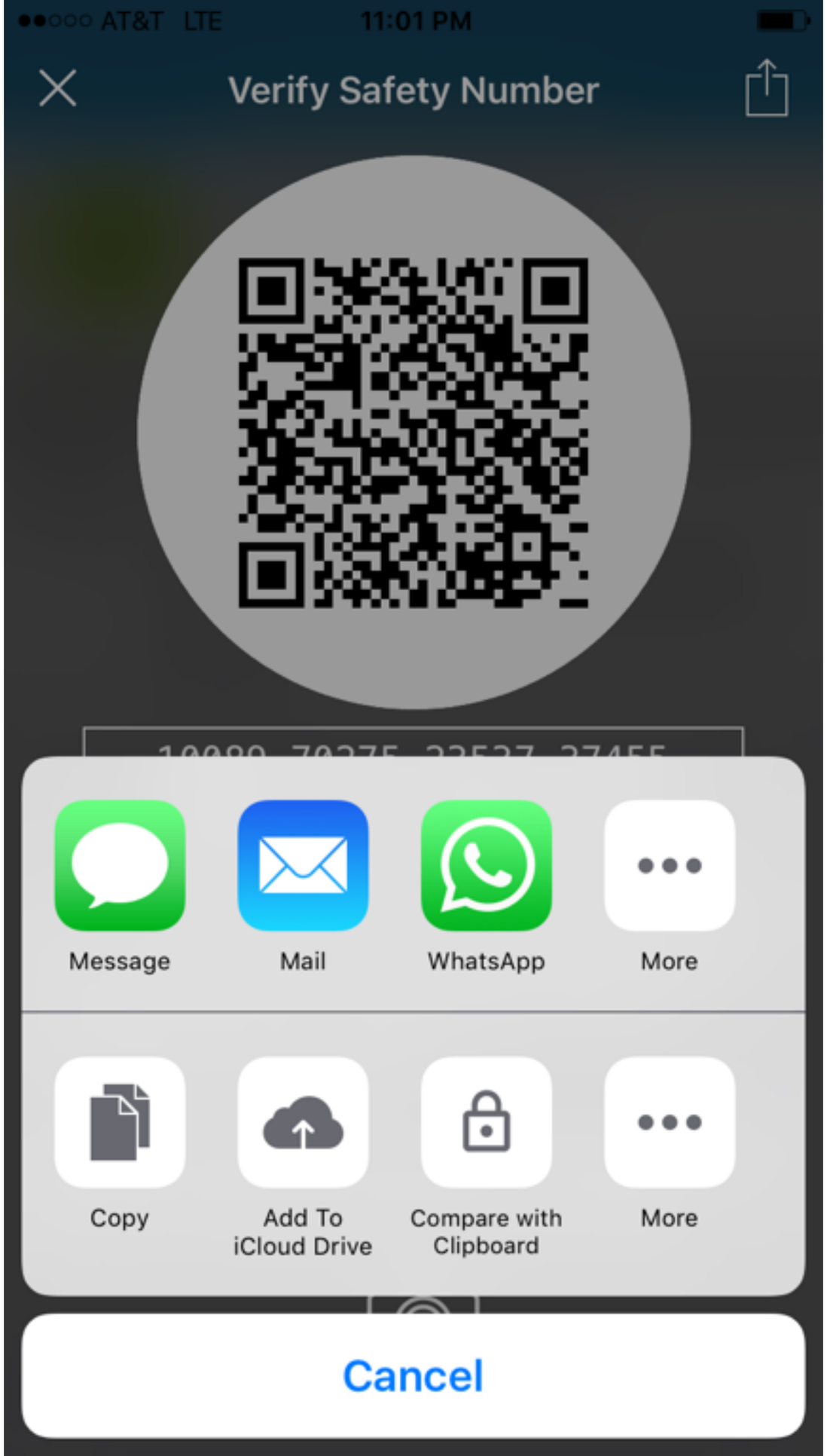
Verify Safety Number

10089 70275 23537 37455
44067 93753 39797 83110
44285 31305 09892 48377

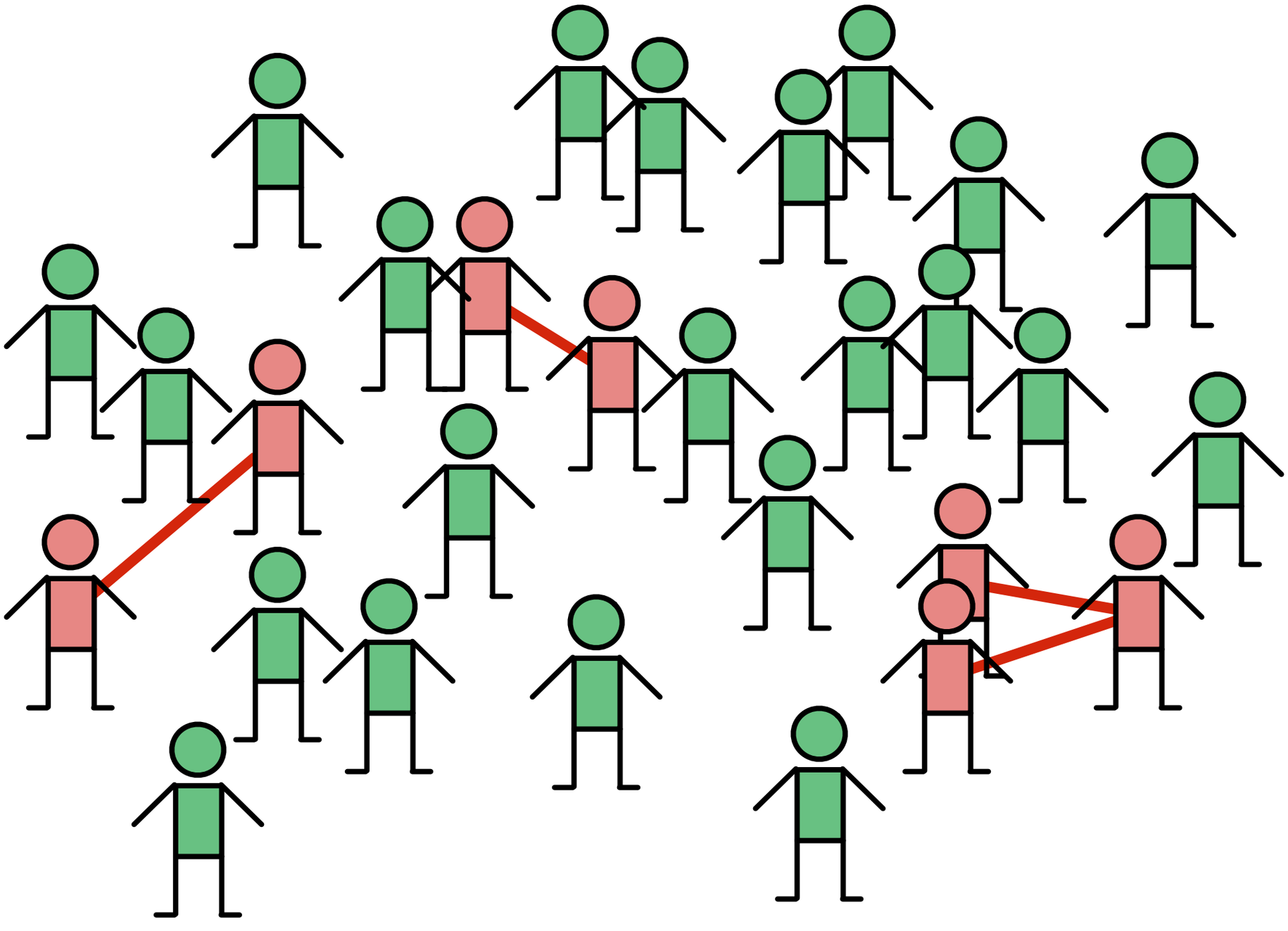
If you wish to verify the security of your end-to-end encryption with Moxie Marlinspike, compare the numbers above with the numbers on their device.

Alternatively, you can scan the code on their phone, or ask them to scan your code.

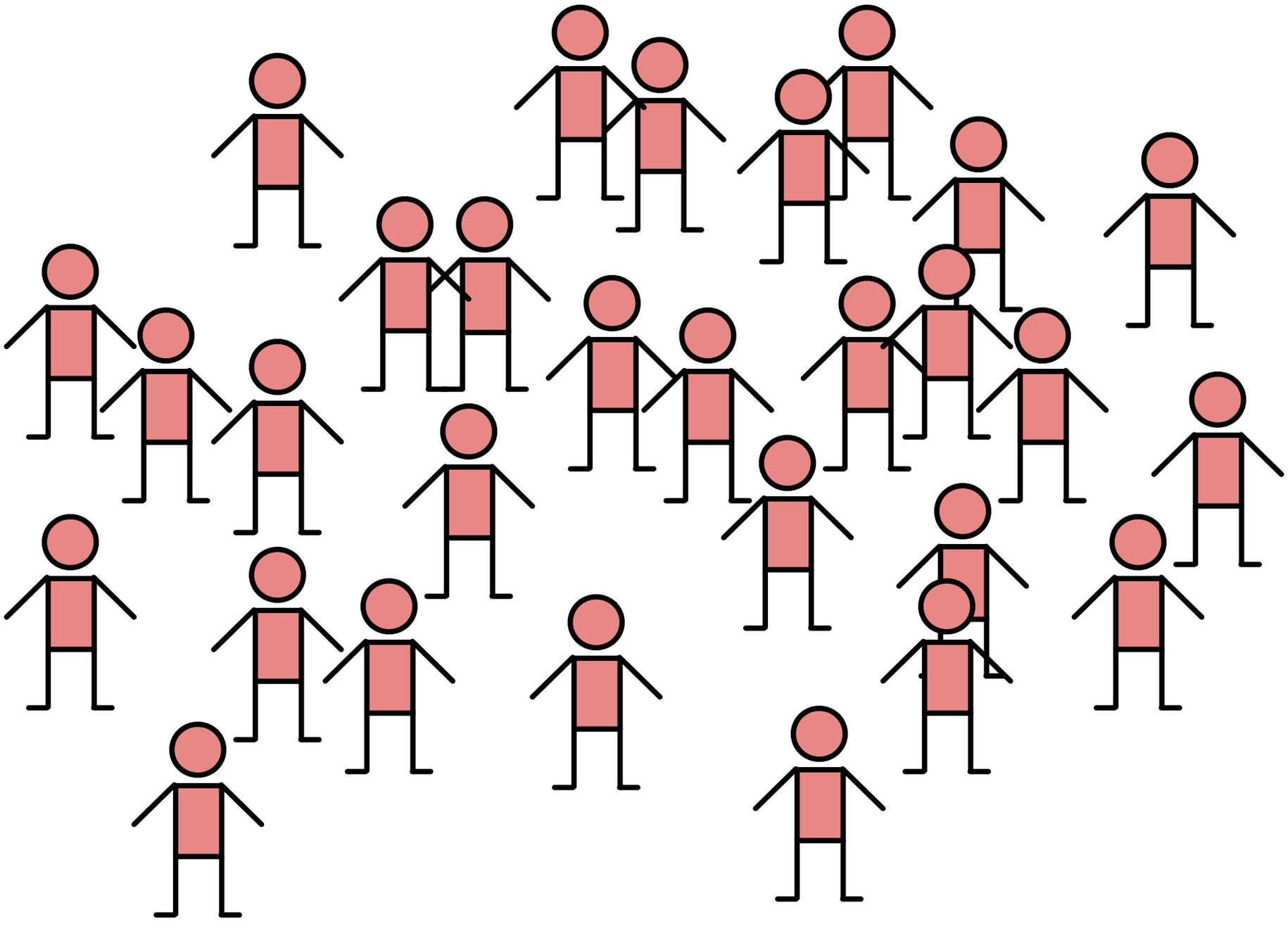
Scan Code


AT&T LTE
11:01 PM
Verify Safety Number
Message
Mail
WhatsApp
More
Copy
Add To iCloud Drive
Compare with Clipboard
More
Cancel

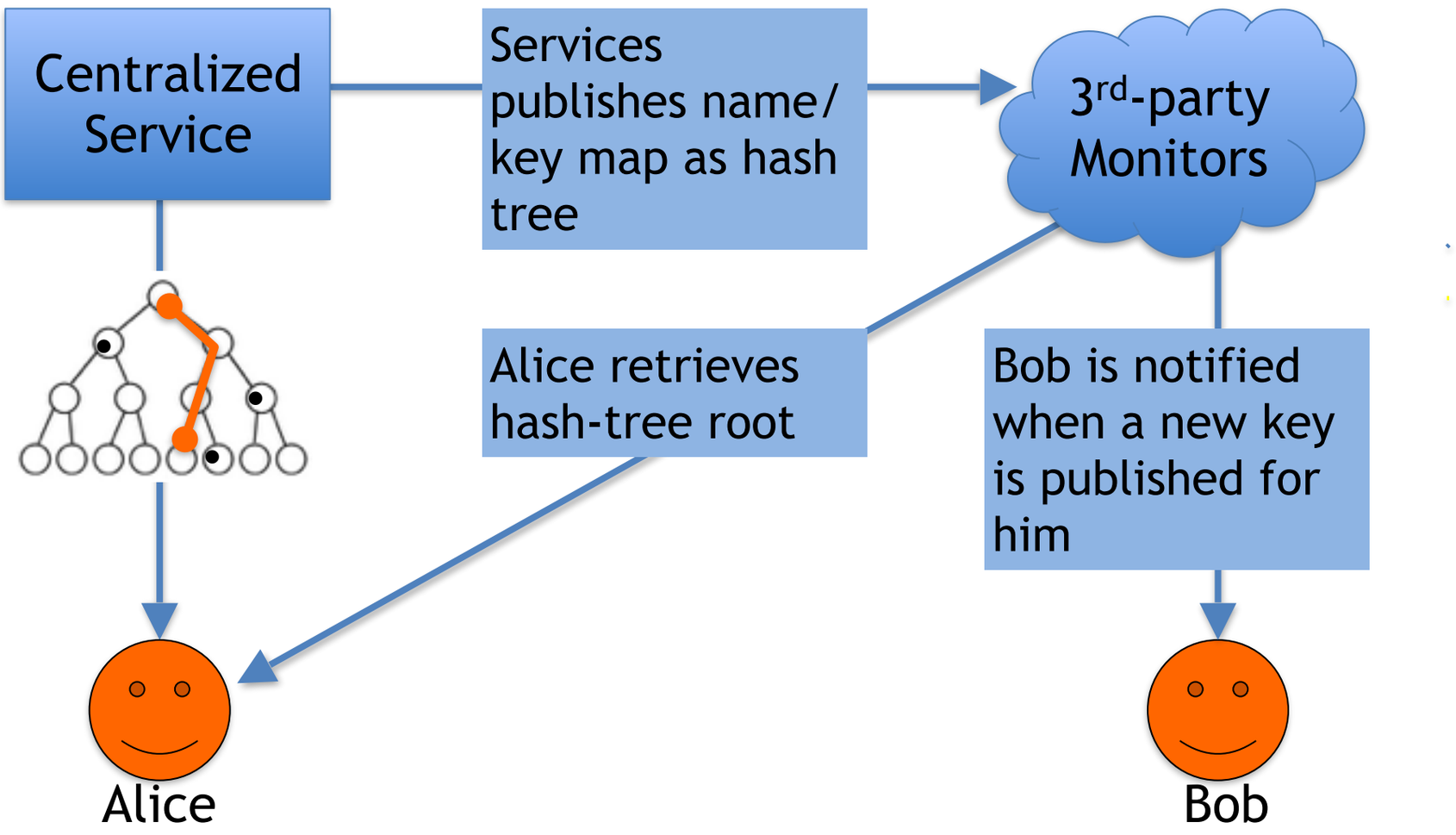
Optional auth checks



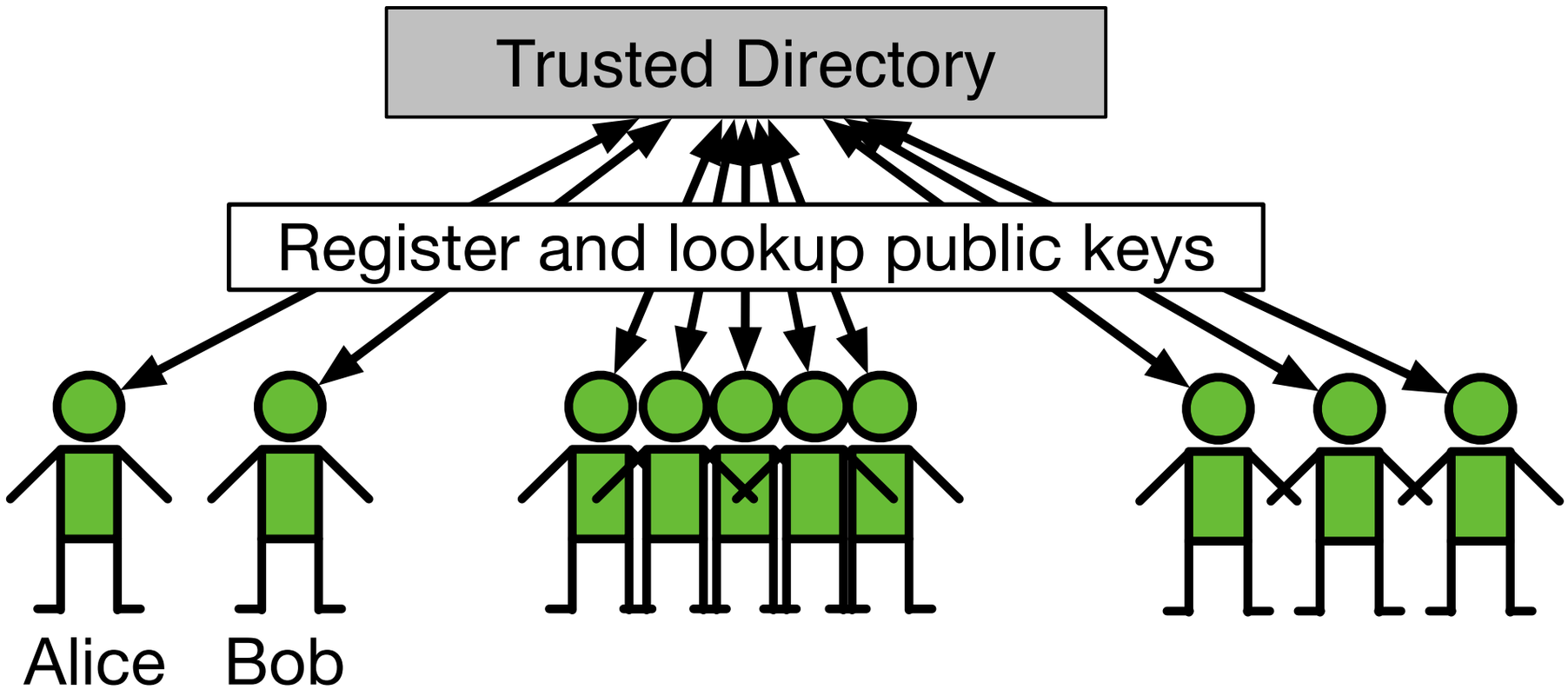
But who?



Certificate Transparency / CONIKS



Trusted Directory



Encrypt-then-Authenticate

- User experience
- Engineering

AtE vs EtA

- Military / Consumer
- Single root of trust / Diverse trust
- Symmetric crypto / Public key crypto
- Radio / Servers

Protocols

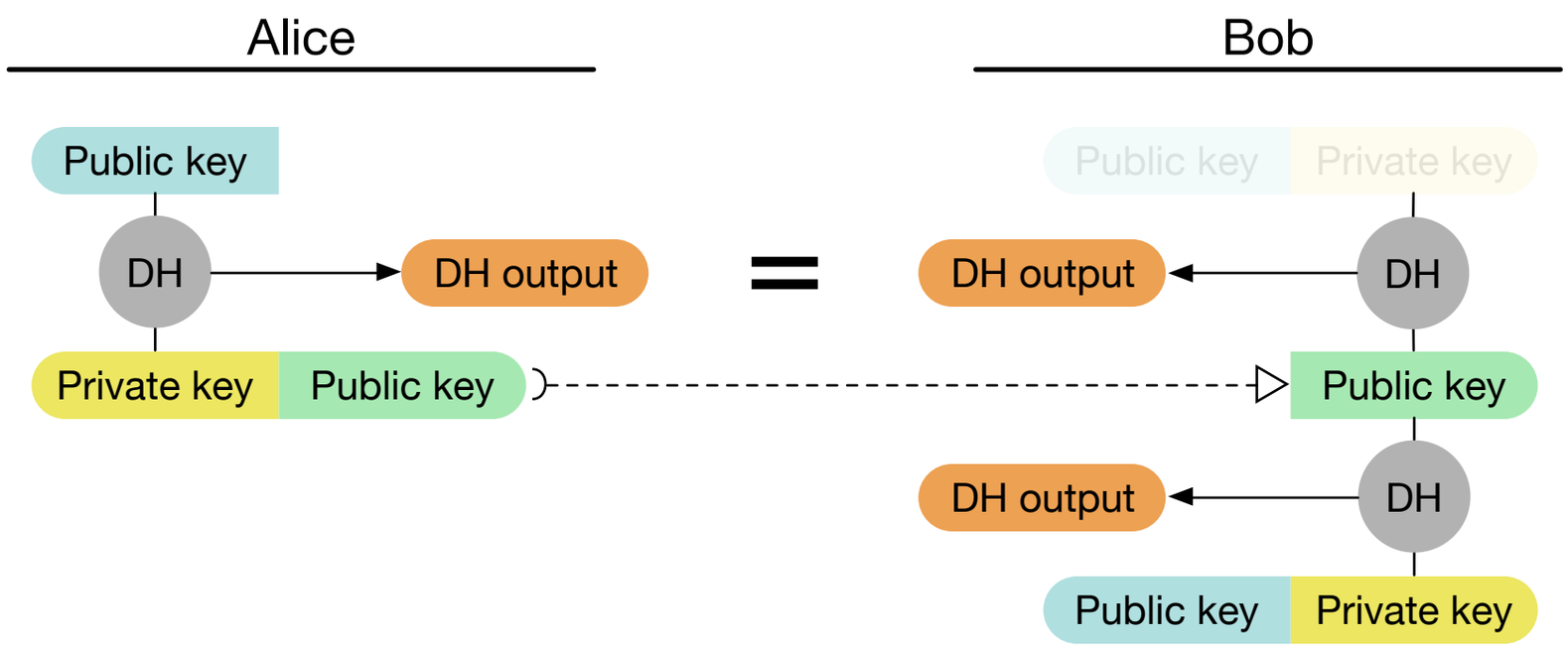
1990s

- Message protocols (S/MIME, PGP)
  - Sign and encrypt
- Session protocols (TLS, SSH, IPsec)
  - Authenticated key exchange
  - Allows forward secrecy

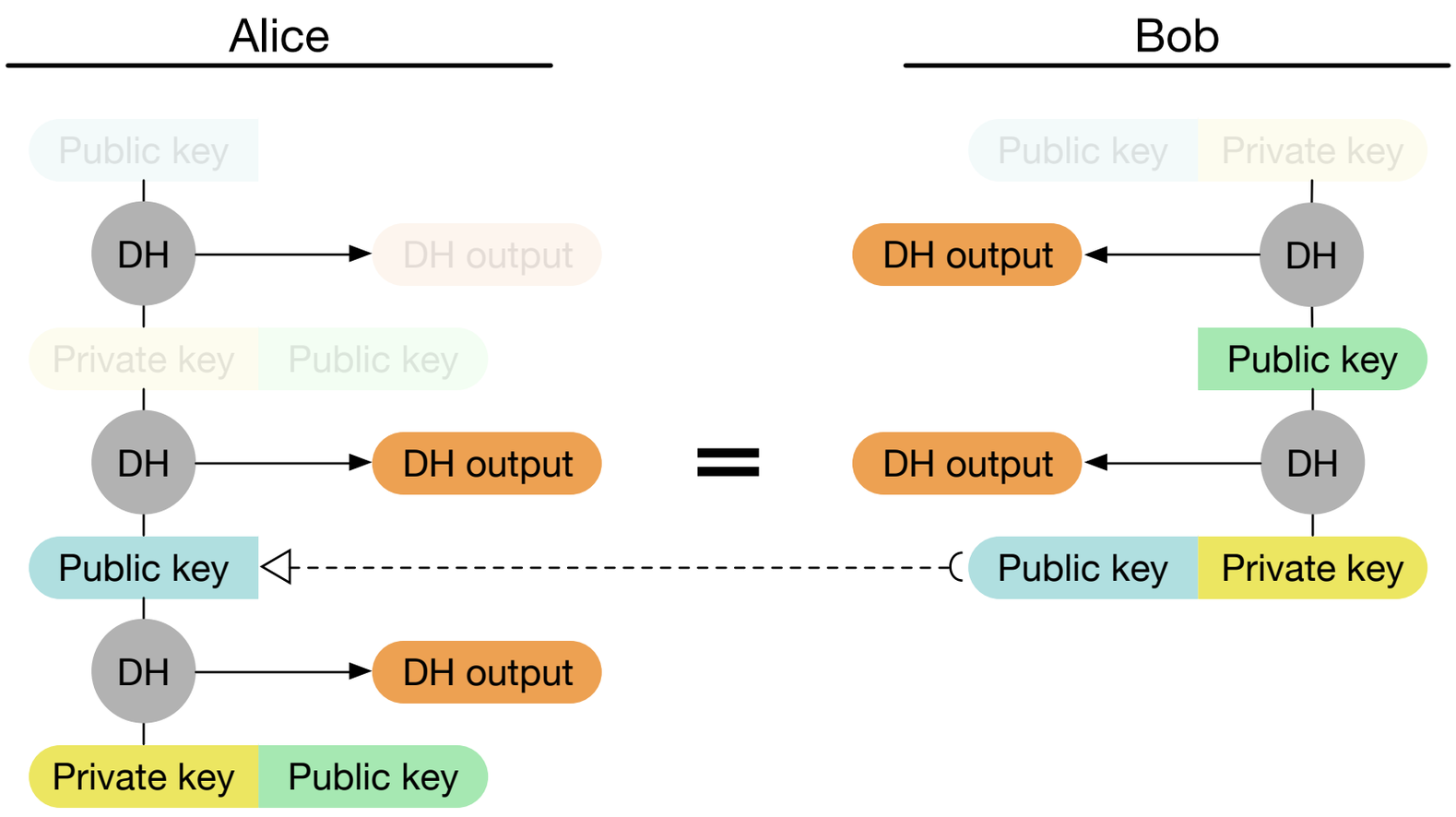
2000s

- OTR
- Deniable key agreement
- “Ratcheting”
  - Update forward secrecy after AKE

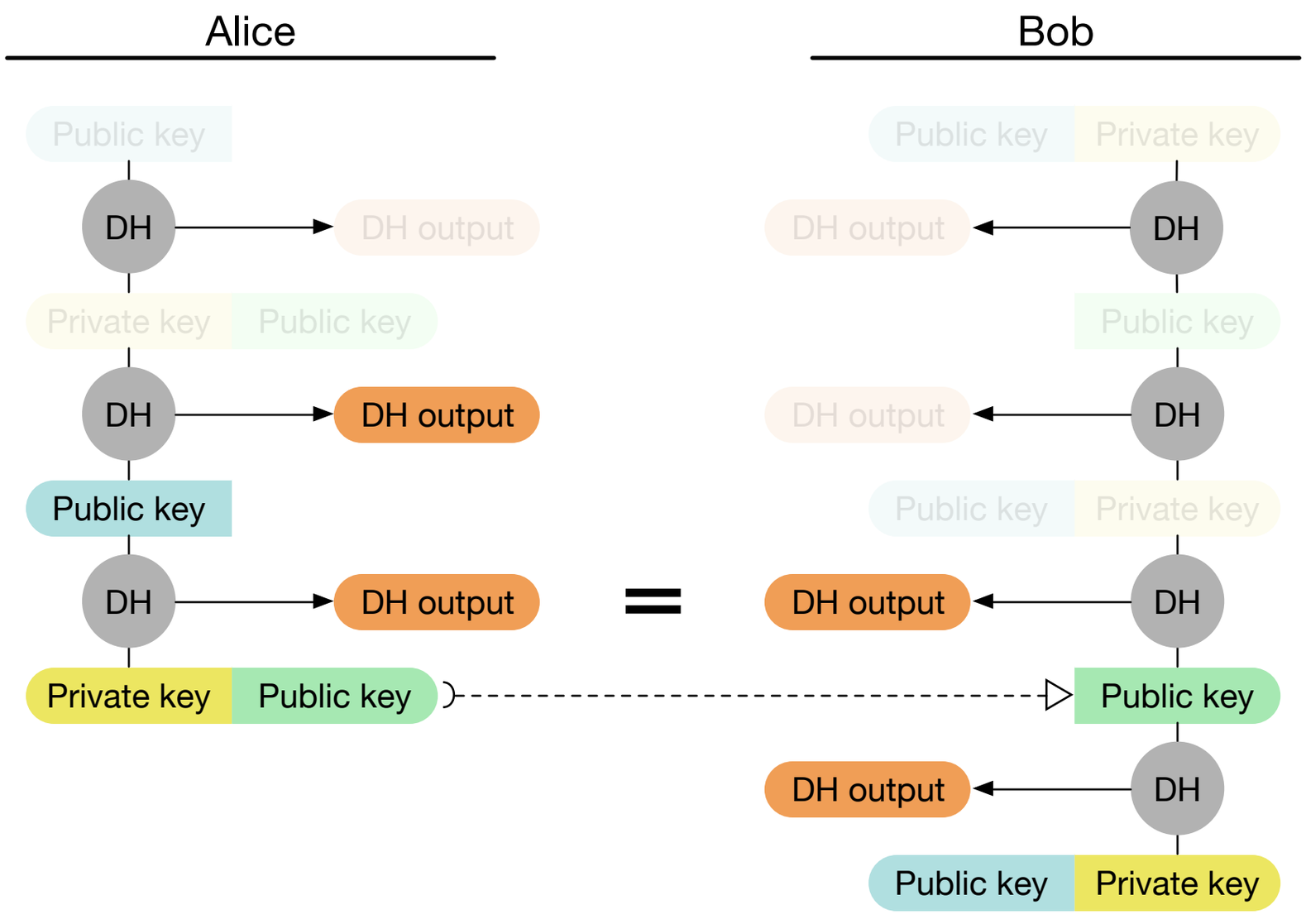
DH ratchet


Alice
Bob
Public key
DH
DH output
=
Private key
Public key
Public key
Private key
DH output
DH
DH output
DH
Public key
Private key

DH ratchet


Alice
Bob
Public key
Private key
DH
DH output
Public key
Private key
DH
DH output
=
DH output
DH
Public key
Public key
Private key
DH
DH output
Private key
Public key

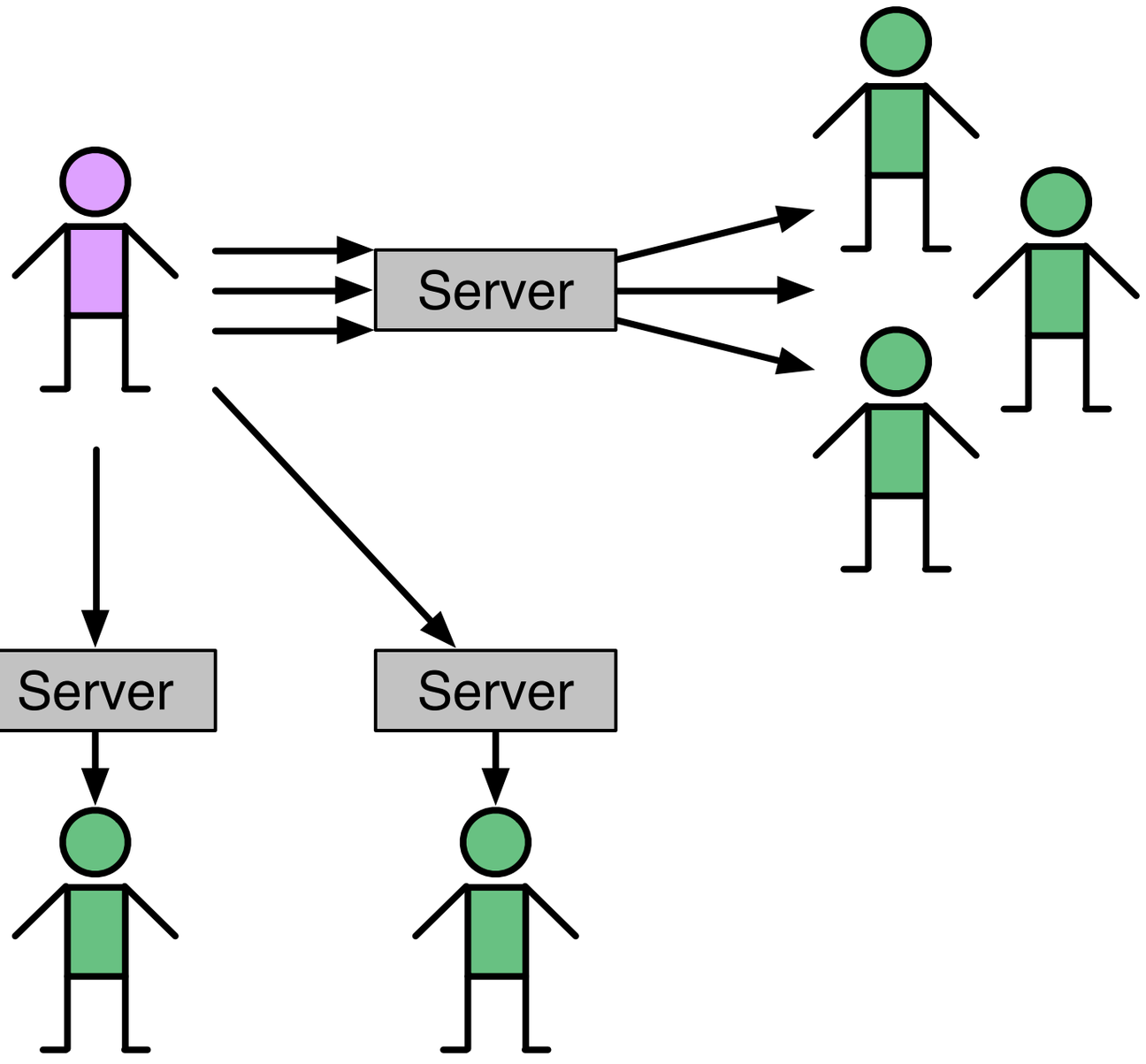
DH ratchet


Alice
Bob
Public key
Private key
DH
DH output
Public key
Private key
DH output
DH
Public key
Private key
DH
DH output
=
DH output
DH
Private key
Public key
Public key
DH output
DH
Public key
Private key

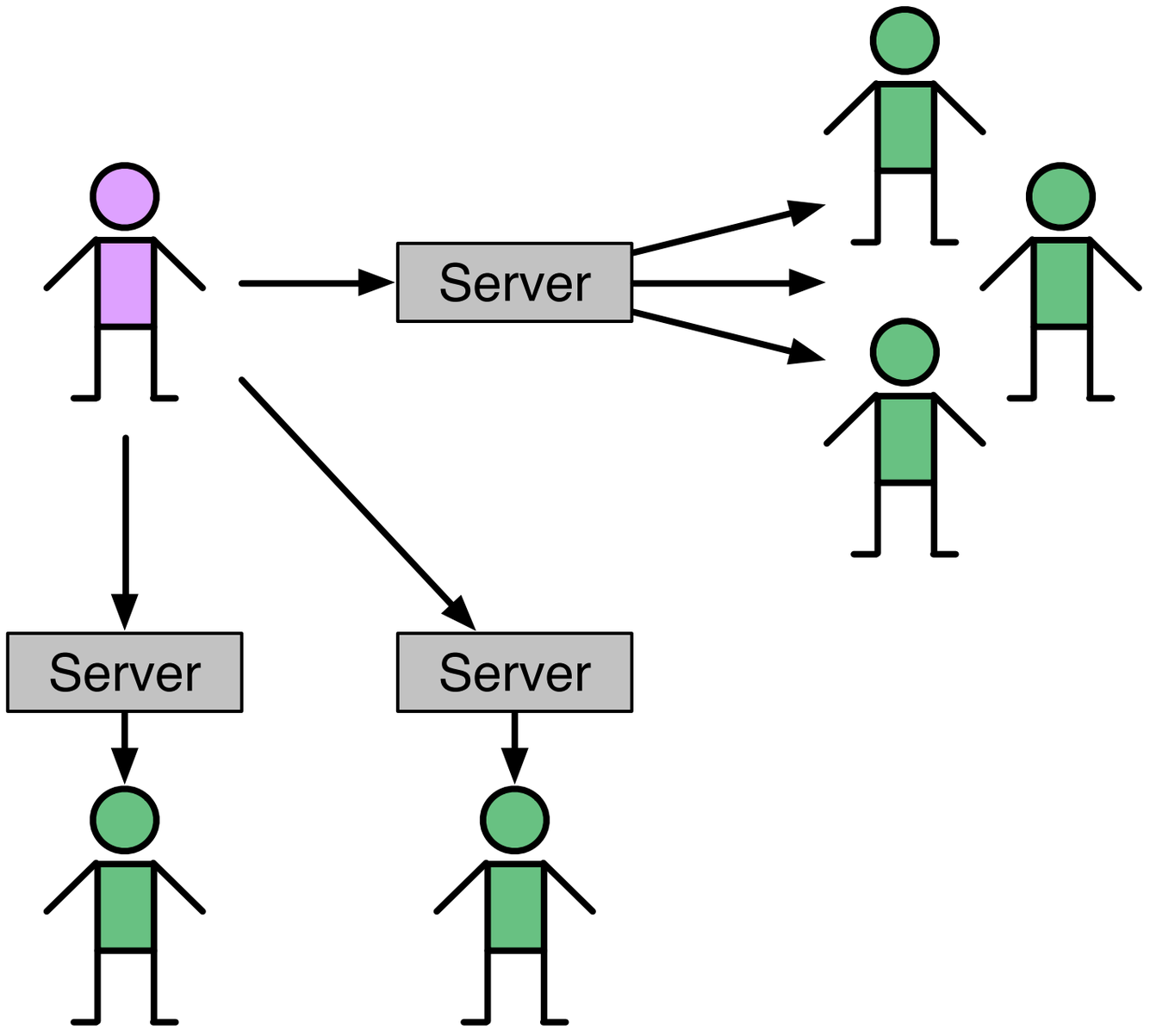
2010s

- TextSecure / Signal
  - Key agreement
    - Added **pre-keys** and a DH-based key agreement
- Ratcheting
  - Added **symmetric-key ratcheting**

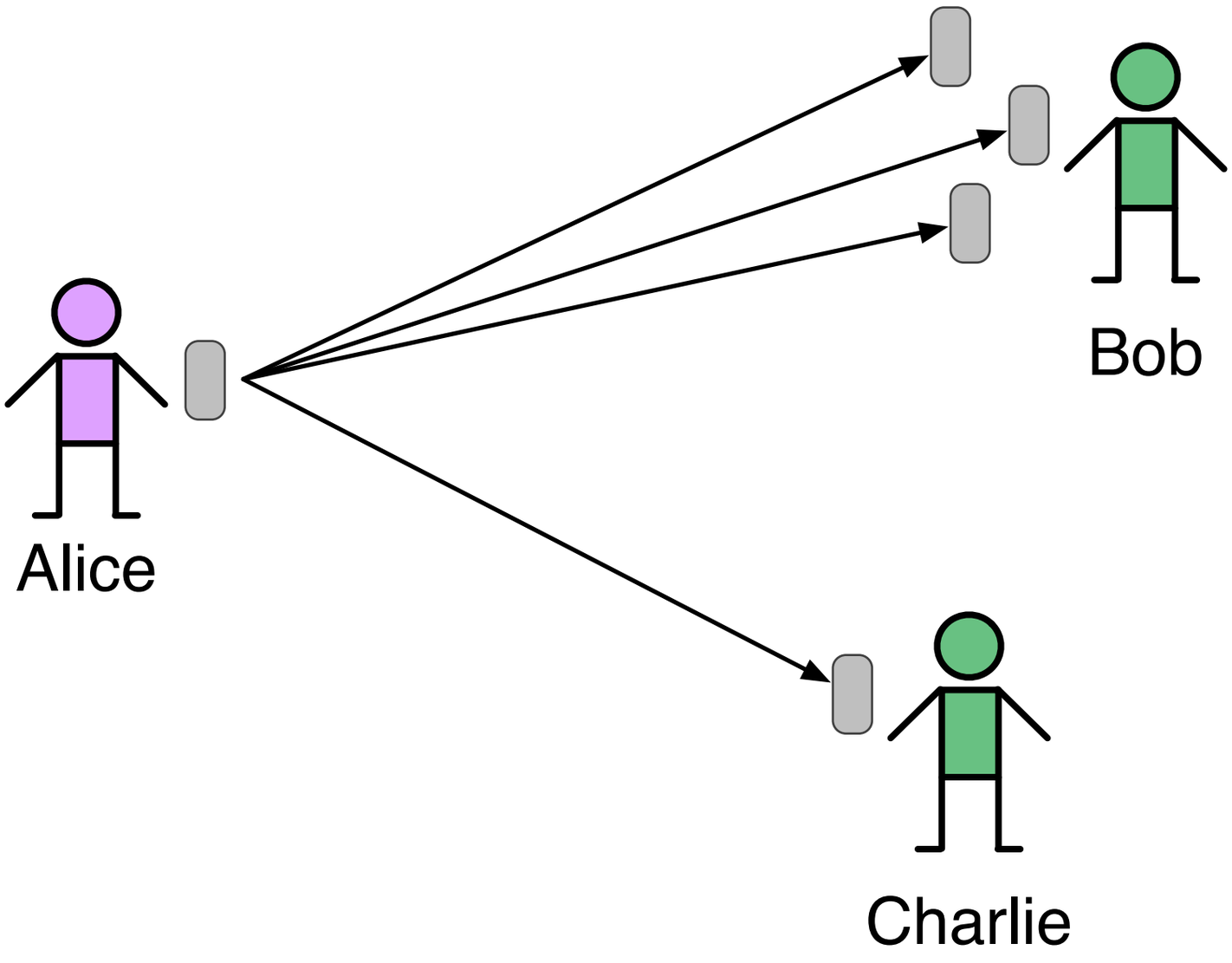
Multi-party



Sender Keys



Multi-device



Protocol Stack

- Multi-device
- Multi-party
- 2-party

Thanks!

- trevp@trevp.net
- Messaging mailing list
- https://moderncrypto.org)