Introduction to OTR

Alexander Færøy

@ahfaeroey

What is OTR?

End-to-End Encryption for Instant Messaging.

- Encryption.
- Authentication.
- Deniability.
- Perfect Forward Secrecy.

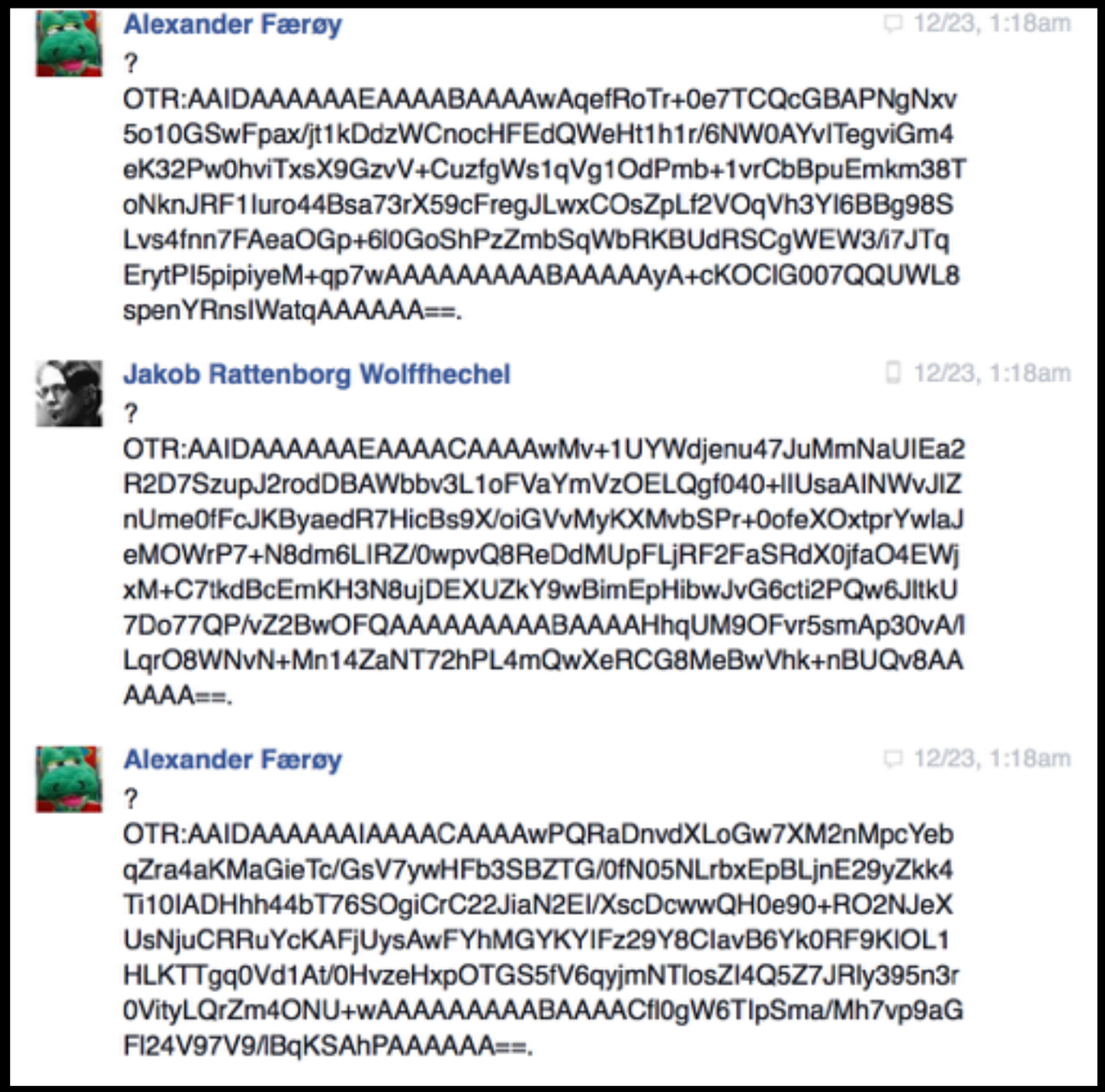
Encryption

- Reference implementation is open source.
- Peer reviewed design.
- Protocol agnostic.

Protocol Agnostic

- Jabber (XMPP).
- Internet Relay Chat.
- Facebook.
- Everything! **:-)**

Protocol Agnostic



Alexander Færøy 12/23, 1:18am

?
OTR:AAIDAAAAAAEAAAABAAAAwAqefRoTr+0e7TCQcGBAPNgNxv
5o10GSwFpax/jt1kDdzWCnocHFEdQWeHt1h1r/6NW0AYvlTegviGm4
eK32Pw0hviTxsX9GzvV+CuzfgWs1qVg1OdPmb+1vrCbBpuEmkm38T
oNknJRF1luro44Bsa73rX59cFregJLwxCOsZpLf2VOqVh3Yl6BBg98S
Lvs4fnn7FAeaOGp+6l0GoShPzZmbSqWbRKBUdRSCgWEW3/i7JTq
ErytPI5pipiyeM+qp7wAAAAAAAABAAAAAyA+cKOCIG007QQUWL8
spenYRnslWatqAAAAAA==.

Jakob Rattenborg Wolffhechel 12/23, 1:18am

?
OTR:AAIDAAAAAAEAAAACAAAAwMv+1UYWdjenu47JuMmNaUIEa2
R2D7SzupJ2rodDBAWbbv3L1oFVaYmVzOELQgf040+lIUsaAINWvJIZ
nUme0fFcJKByaedR7HicBs9X/oiGVvMyKXMvbSPr+0ofeXOxtprYwlaJ
eMOWrP7+N8dm6LIRZ/0wpvQ8ReDdMUpFLjRF2FaSRdX0jfaO4EWj
xM+C7tkdBcEmKH3N8ujDEXUZkY9wBimEpHibwJvG6cti2PQw6JltkU
7Do77QP/vZ2BwOFQAAAAAAAABAAAAHhqUM9OFvr5smAp30vA/l
LqrO8WNvN+Mn14ZaNT72hPL4mQwXeRCG8MeBwVhk+nBUQv8AA
AAAA==.

Alexander Færøy 12/23, 1:18am

?
OTR:AAIDAAAAAAIAAAACAAAAwPQRaDnvdXLoGw7XM2nMpcYeb
qZra4aKMaGieTc/GsV7ywHFb3SBZTG/0fN05NLrbxEpBLjnE29yZkk4
Ti10IADHhh44bT76SOgiCrC22JiaN2EI/XscDcwwQH0e90+RO2NJeX
UsNjuCRRuYcKAFjUysAwFYhMGYKYIFz29Y8CIavB6Yk0RF9KlOL1
HLKTTgq0Vd1At/0HvzeHxpOTGS5fV6qyjmNTlosZl4Q5Z7JRly395n3r
0VityLQrZm4ONU+wAAAAAAAAABAAAACfl0gW6TlpSma/Mh7vp9aG
Fl24V97V9/lBqKSAhPAAAAAA==.

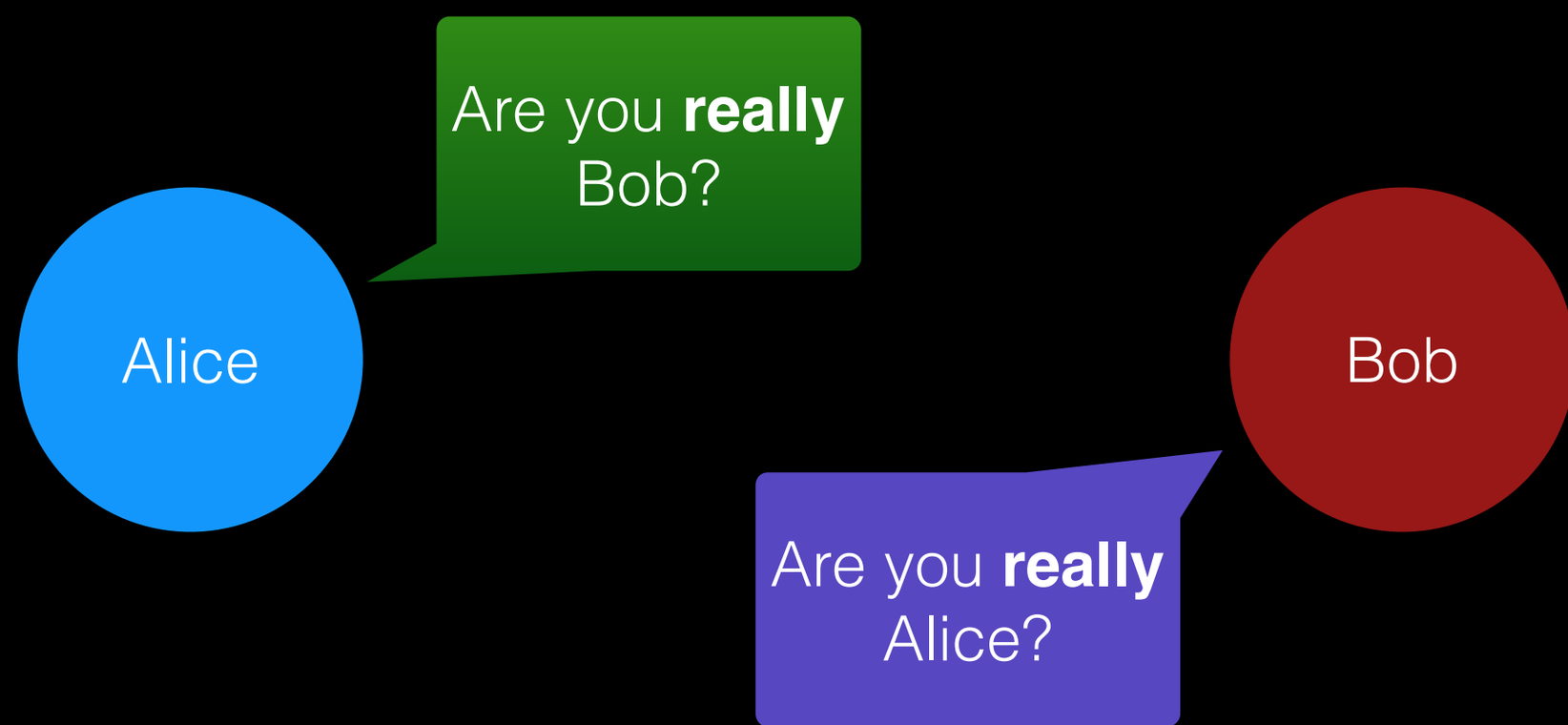
Authentication

- Fingerprint verification, like with PGP.
- Socialist Millionaires Protocol.

Socialist Millionaires Protocol

Ask a question that **only** the person you are communicating with is able to answer.

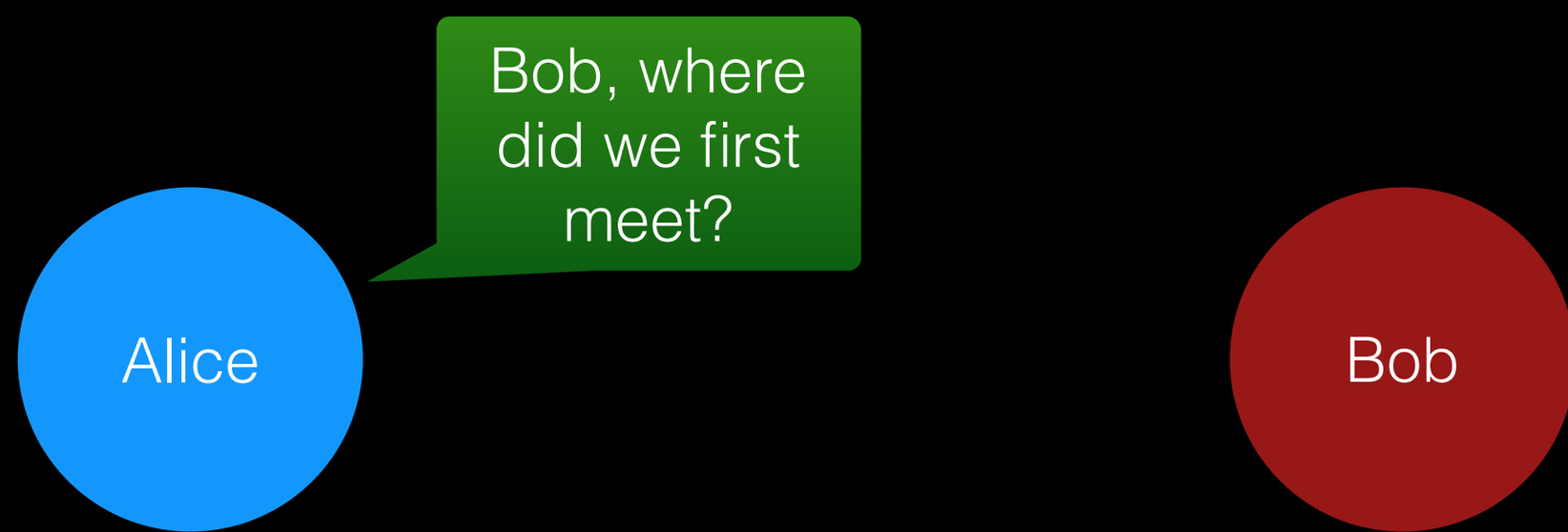
Socialist Millionaires Protocol



Socialist Millionaires Protocol

Alice and Bob have a shared secret that **only** they know.

Socialist Millionaires Protocol



Socialist Millionaires Protocol

Socialist Millionaires Protocol

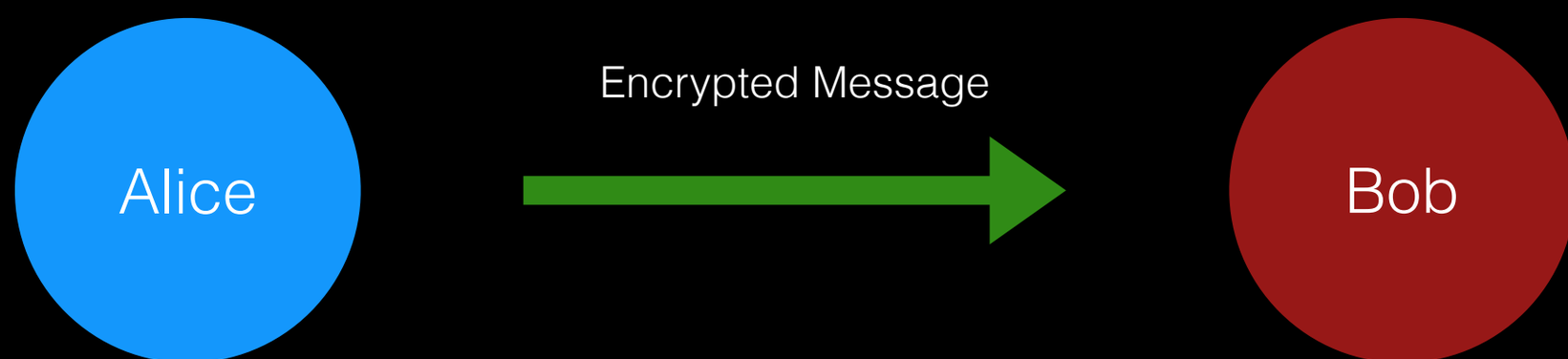
Because Bob knew the answer, Alice and Bob are now **authenticated**.

If Bob had gotten the answer wrong, Alice would have known that she **is not** communicating with the right Bob.

Be creative and careful with your question **:-)**

Deniability

Bob is sure that Alice **sent** the message.

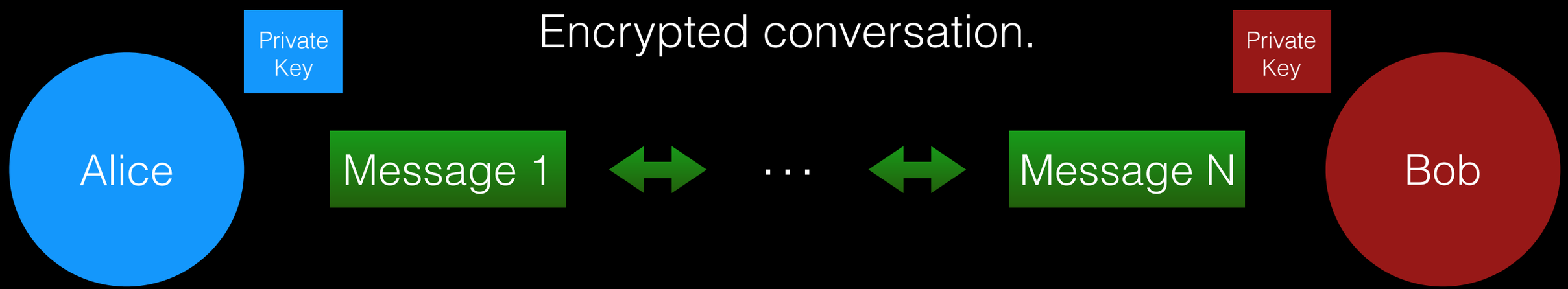


But, Bob cannot prove that Alice **wrote** the message.

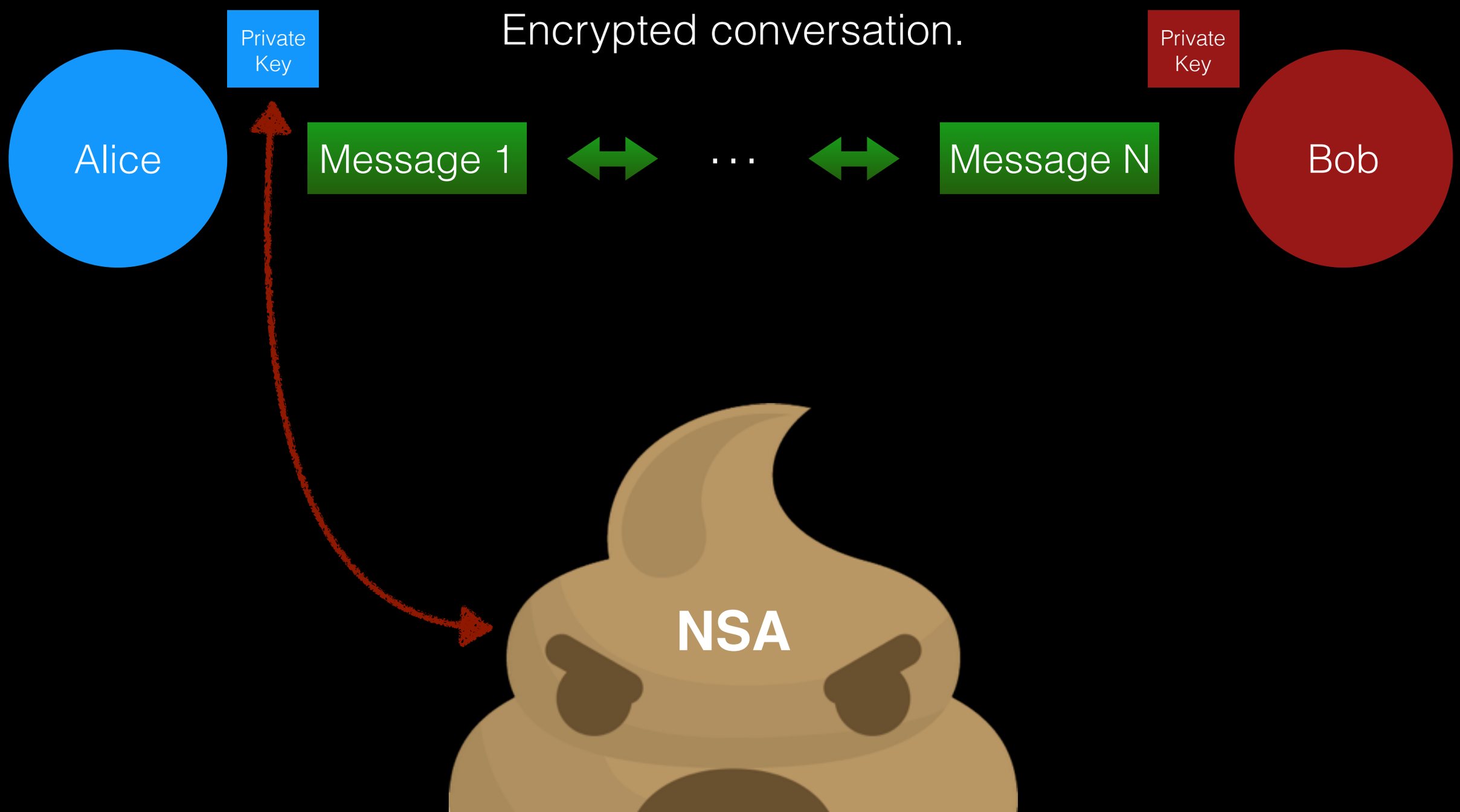
Deniability

Have yet to be tested in court **:-)**

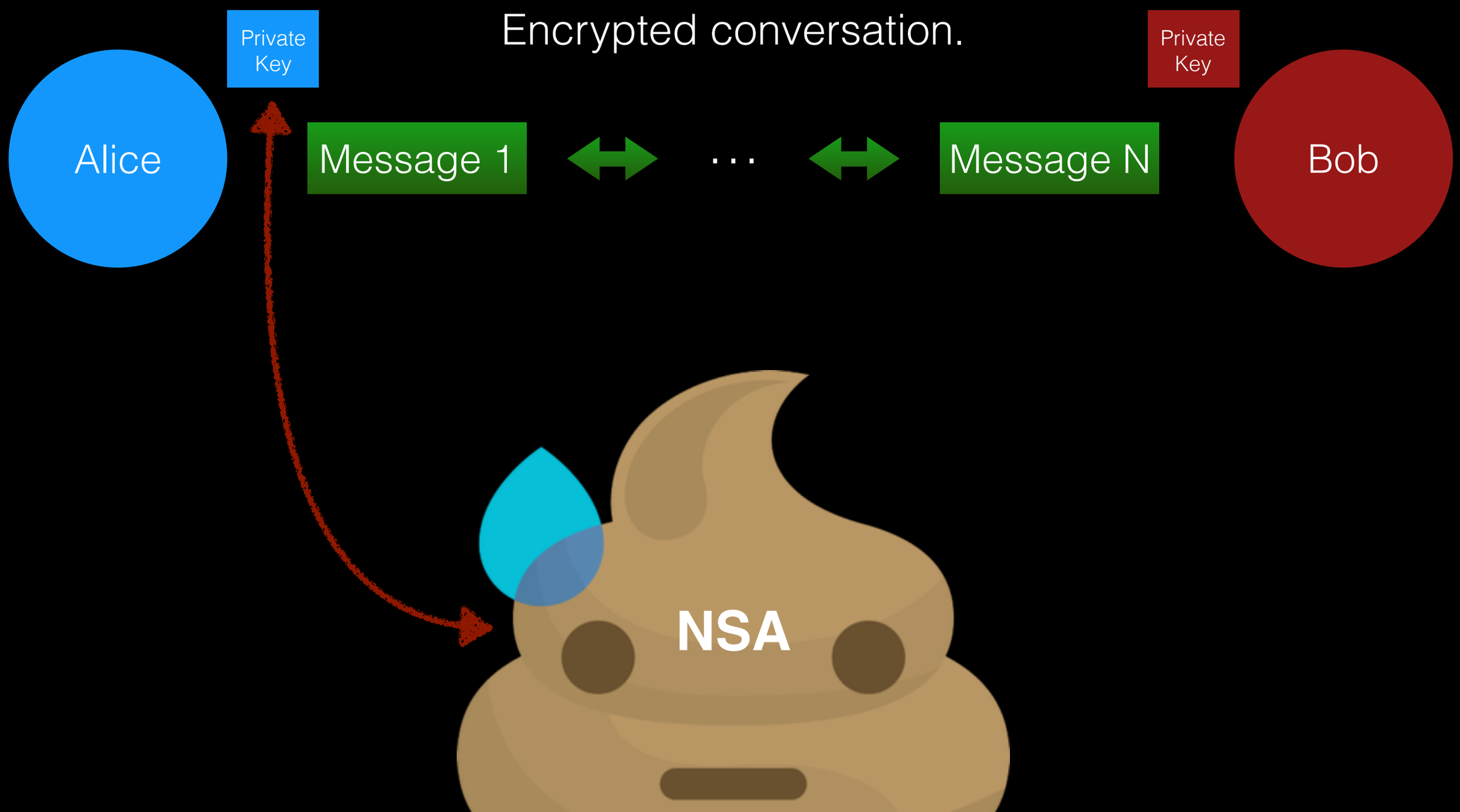
Perfect Forward Secrecy



Perfect Forward Secrecy



Perfect Forward Secrecy



Questions?

Twitter: **@ahfaeroey**

Jabber: **ahf@0x90.dk**

05B4D6F3 C9B88F7C 1A99C3A4 4723D542 3BD3C3F0