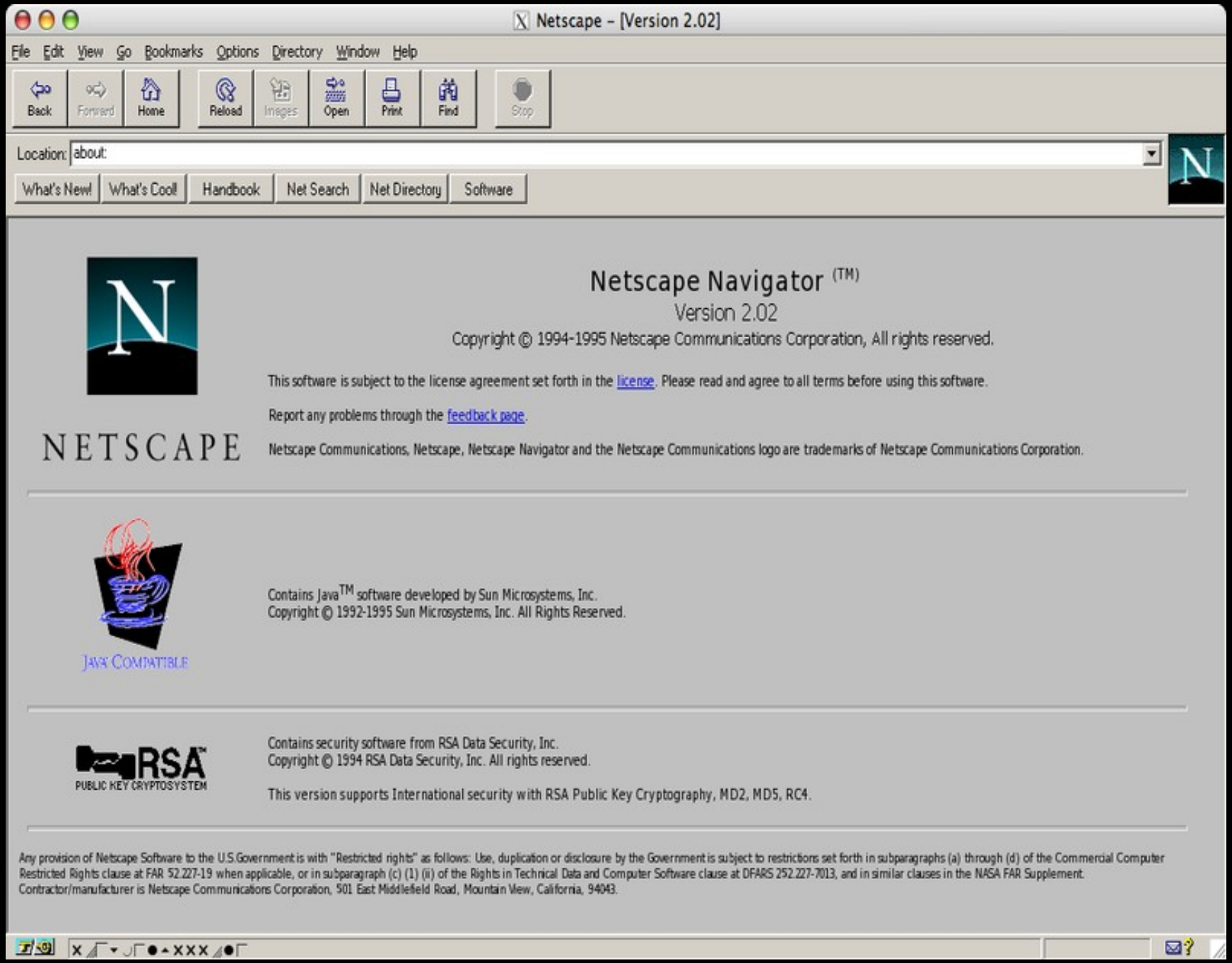
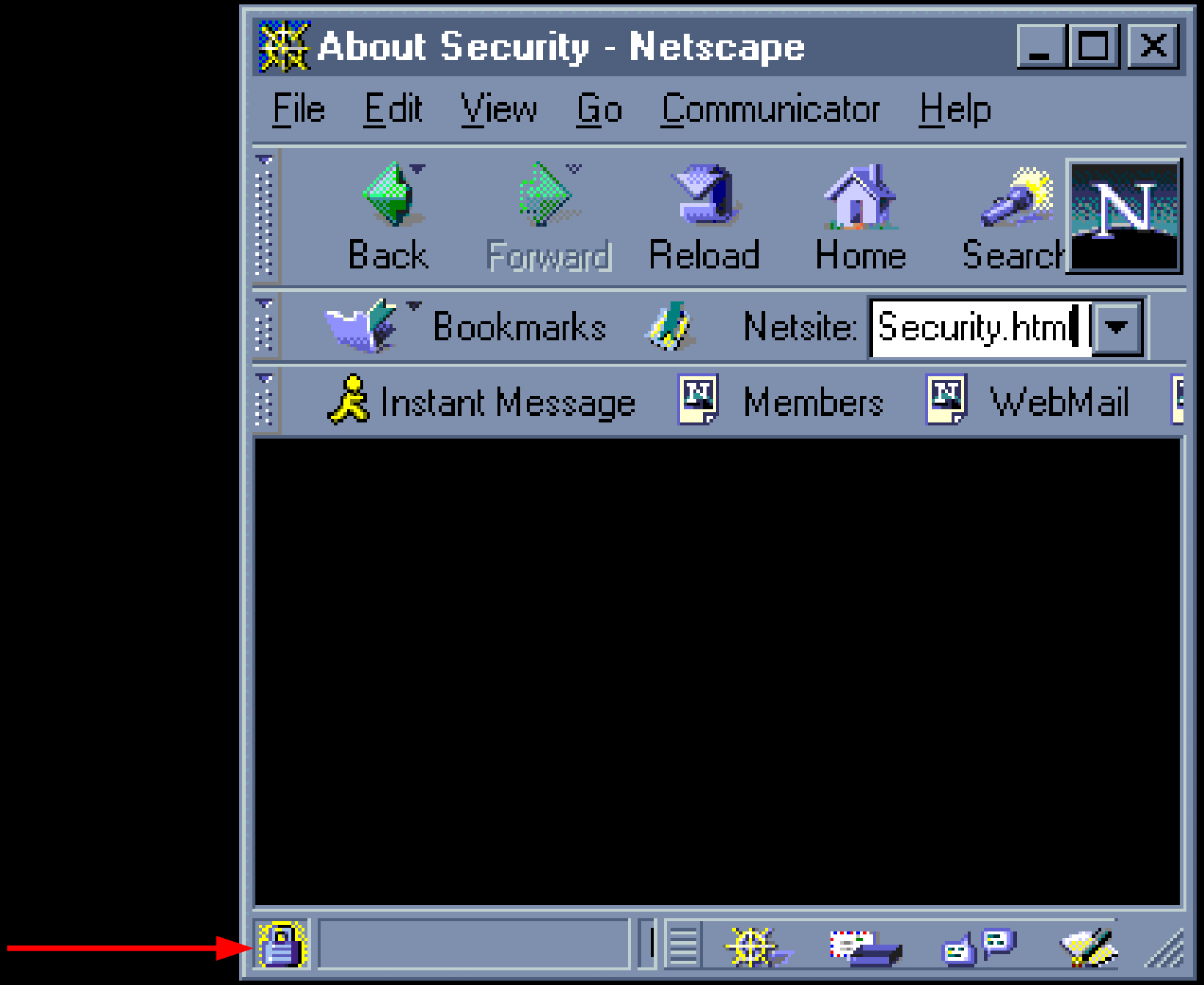
Changing Threats To Privacy

moxie@thoughtcrime.org


Netscape - [Version 2.02]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Location: about:
What's New! What's Cool! Handbook Net Search Net Directory Software
Netscape Navigator (TM)
Version 2.02
Copyright © 1994-1995 Netscape Communications Corporation, All rights reserved.
This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.
Report any problems through the feedback page.
Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.
NETSCAPE
Contains Java™ software developed by Sun Microsystems, Inc.
Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.
JAVA COMPATIBLE
RSA
PUBLIC KEY CRYPTOSYSTEM
Contains security software from RSA Data Security, Inc.
Copyright © 1994 RSA Data Security, Inc. All rights reserved.
This version supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.
Any provision of Netscape Software to the U.S.Government is with "Restricted rights" as follows: Use, duplication or disclosure by the Government is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement.
Contractor/manufacturer is Netscape Communications Corporation, 501 East Middlefield Road, Mountain View, California, 94043.


Microsoft Welcomes You To The Internet!
File Edit View Favorites Help
Address: http://www.msn.net/
New to the Internet?
Click here
msn. Membership
Explore the Internet
Windows95
On-Line Launch Event
Help Index Search Mic
© 1995 Microsoft Corporation
history
File Edit View Help
[atm.geo.nsf.gov]
00index.txt (ftp.seagate.com)
05 (gopher.novell.com)
32 bit Development Kits
About Microsoft Internet Central
About the Microsoft Developer Network
About This Site
ATLAS XP34300S XP32150S XP31070S
252 object(s)
51.0KB


About Security - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search
Bookmarks Netsite: Security.html
Instant Message Members WebMail

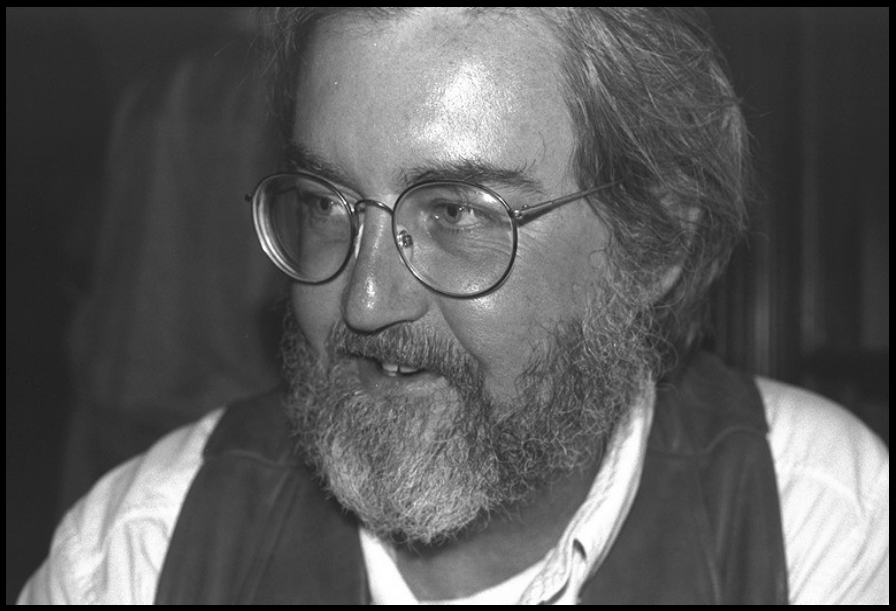

About Security - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search
Bookmarks Netsite: Security.html
Instant Message Members WebMail

Cypherpunks

Moxie Marlinspike
Institute For Disruptive Studies

Government


David Chaum



Dangerous

Scared

The Fuck

Out Of Them

Ultimate Control → No Control

As Dangerous?

=


Mykotronx
MYK78T
22422
200005

Cryptography Is Not A Banana

!=

Cypherpunks Write Code!

Moxie Marlinspike
Institute For Disruptive Studies

"PGP: source code and internals"
MIT Press 1995

2000 == GAME OVER?

THE SPREAD OF INFORMATION IS INEVITABLE

PREDICTIONS

- Anonymous digital cash will flourish.
- Intellectual property will disappear.
- Surveillance will become impossible.
- Governments will be unable to continue collecting taxes.
- Governments will fall.

IO YEARS ON

Moxie Marlinspike
Institute For Disruptive Studies

Is This Victory?

- Everyone's mother has an illegal copy of an mp3 somewhere.
- Cryptography is everywhere.
- There are actual darknets which should make the eradication of information impossible.

SURVEILLANCE > PRIVACY

What Happened?

FUTURE

FACISM

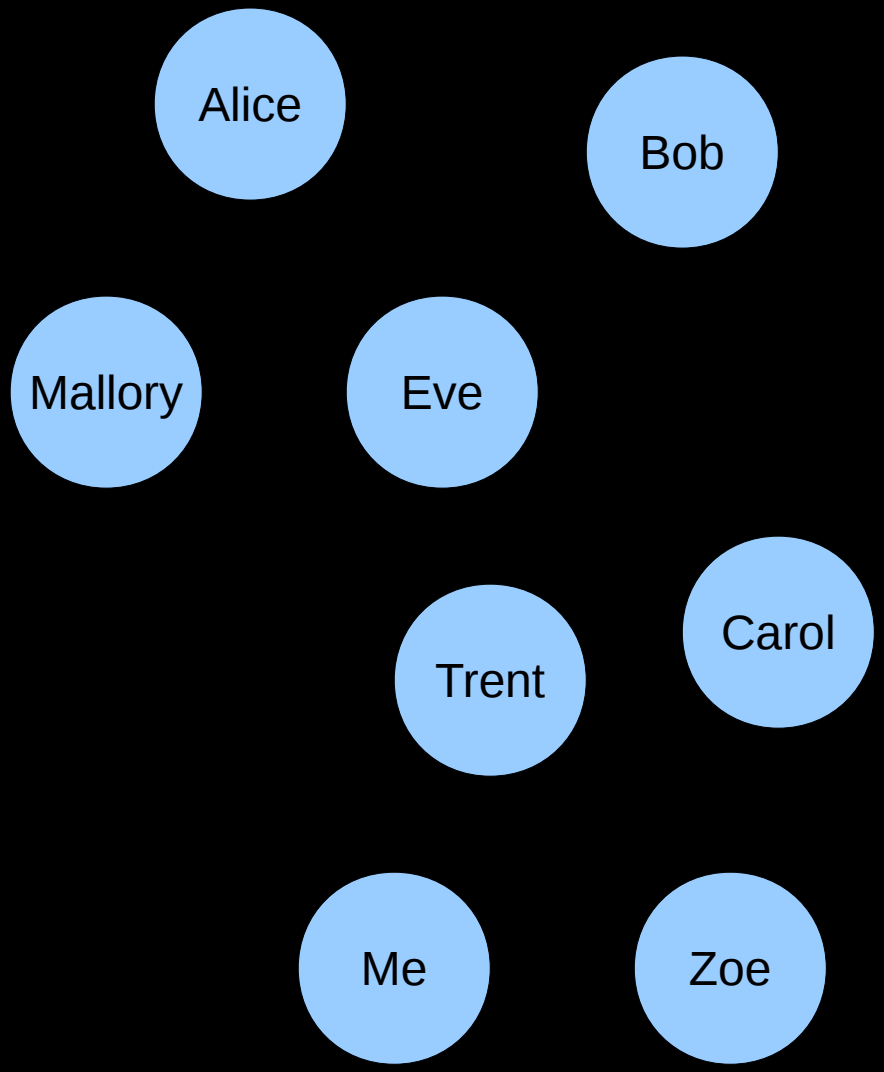
Moxie Marlinspike
Institute For Disruptive Studies

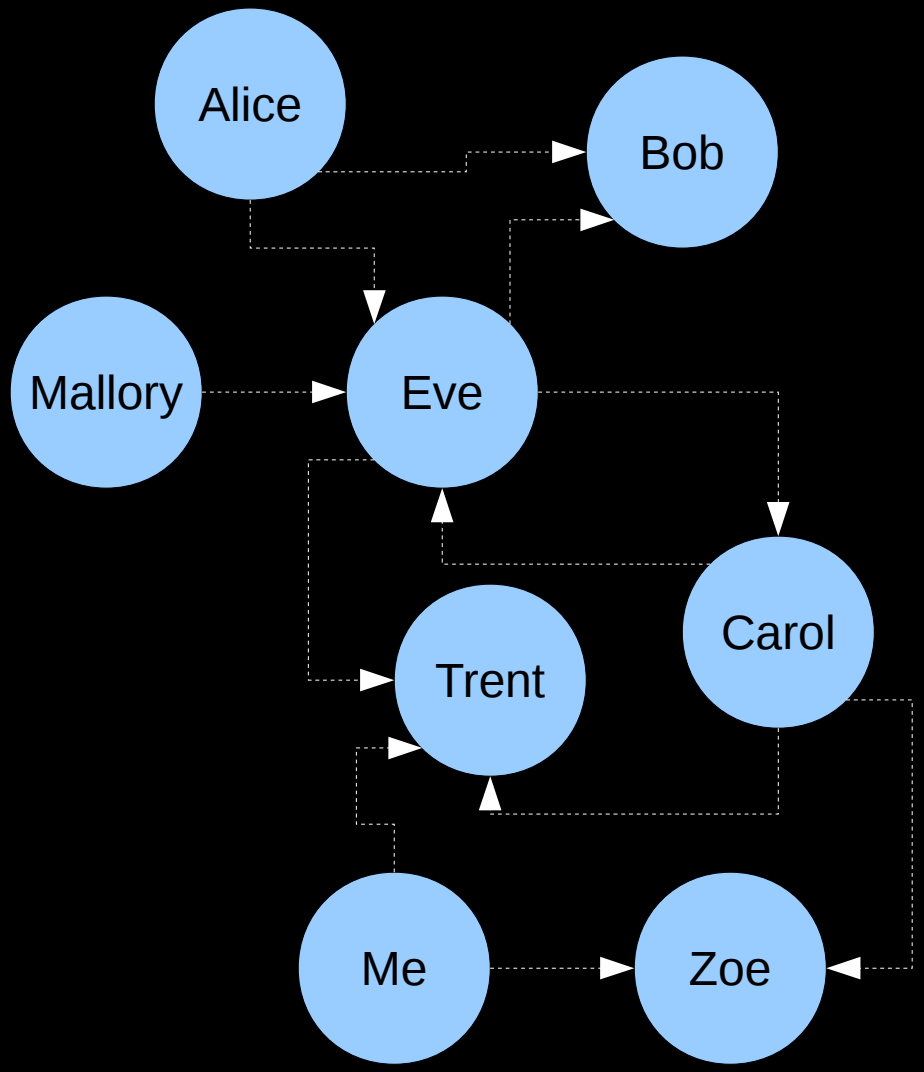
SOCIAL DEMOCRACY

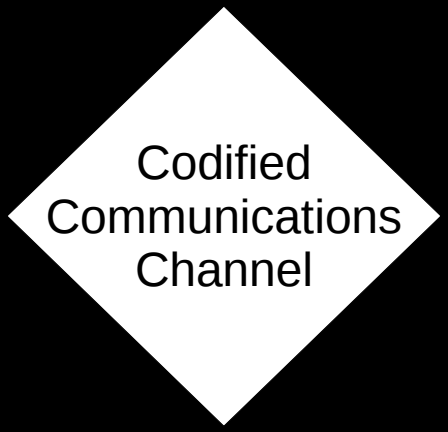
Moxie Marlinspike
Institute For Disruptive Studies

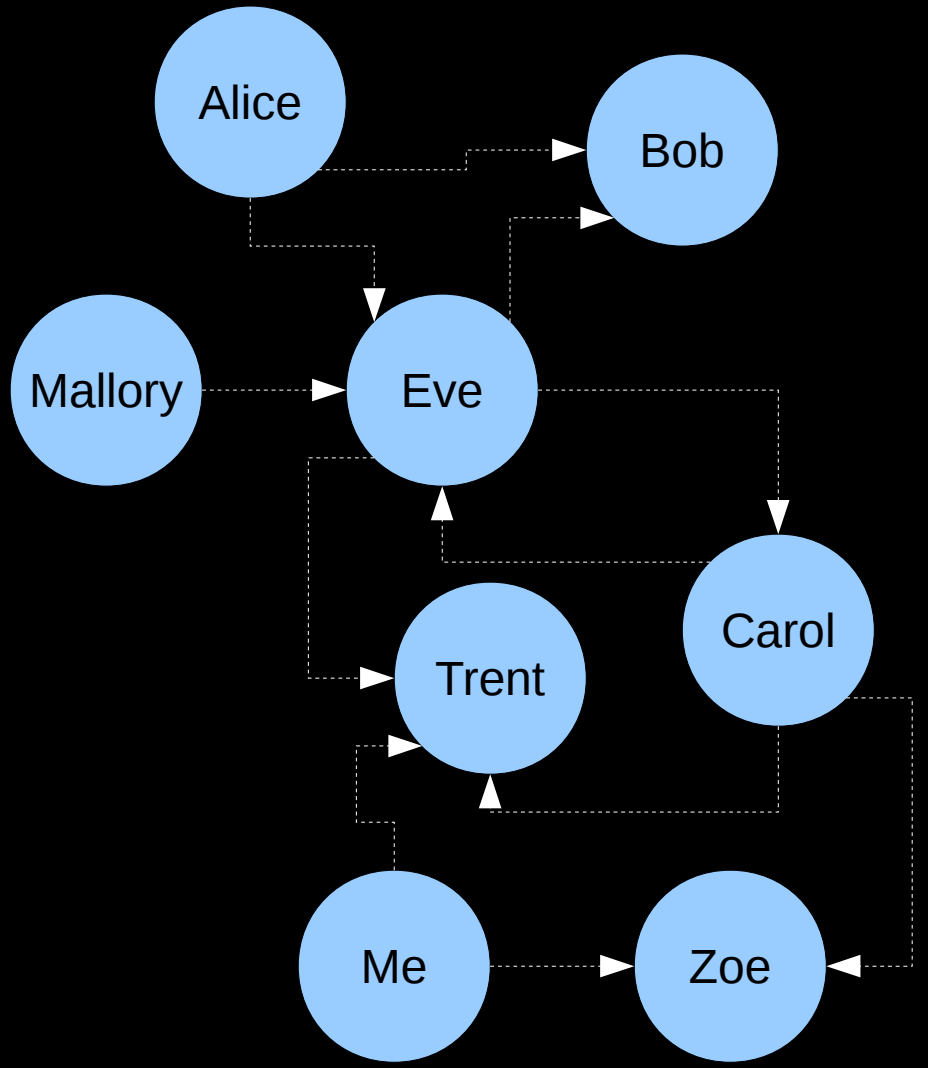
Choice


NOKIA
NOKIA
1 qo
2 abc
def 3
4 ghi
5 jkl
mno 6
7 pqrs
8 tuv
wxyz 9
0
#

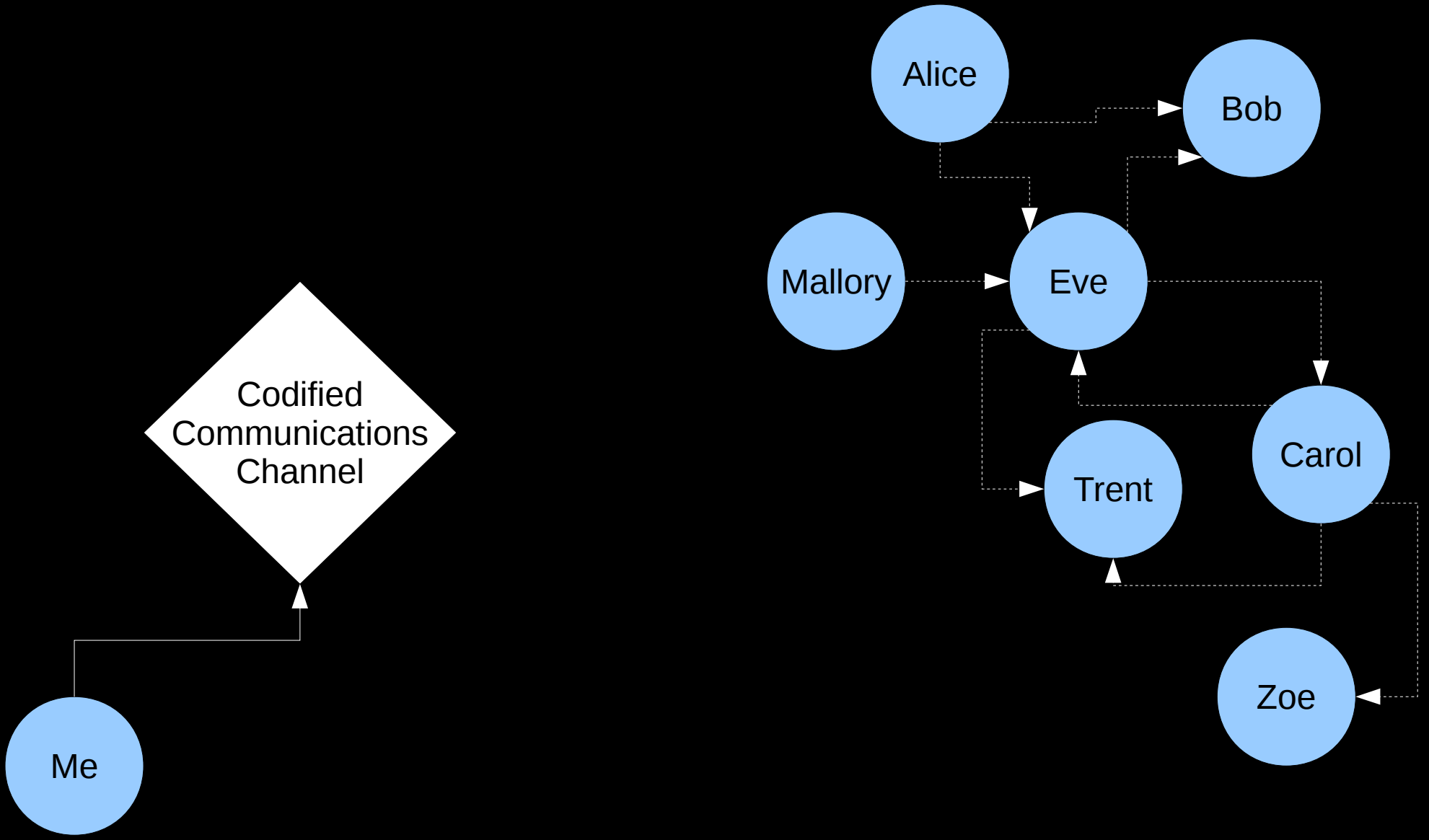

Alice
Bob
Mallory
Eve
Carol
Trent
Me
Zoe

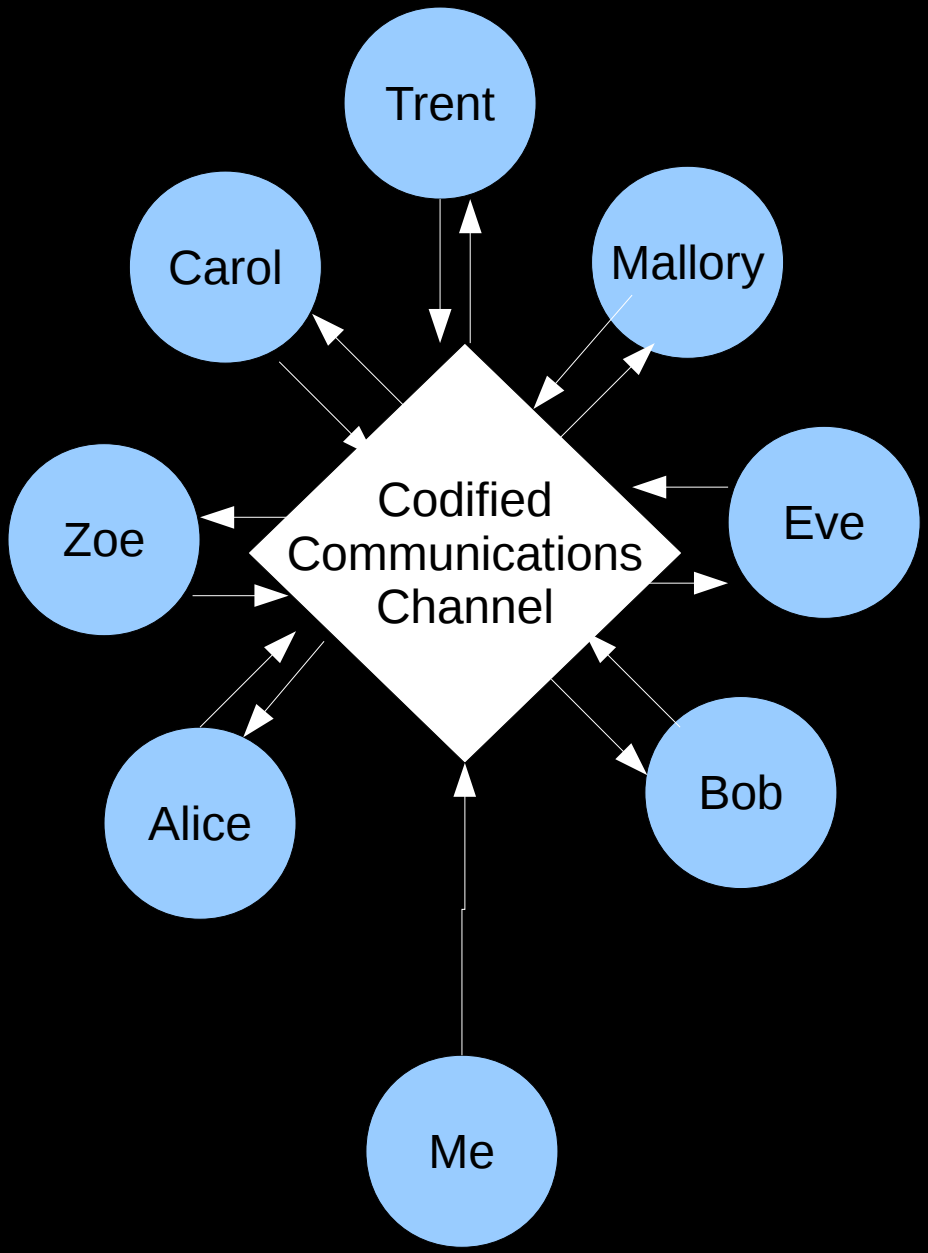

Alice
Bob
Mallory
Eve
Carol
Trent
Me
Zoe

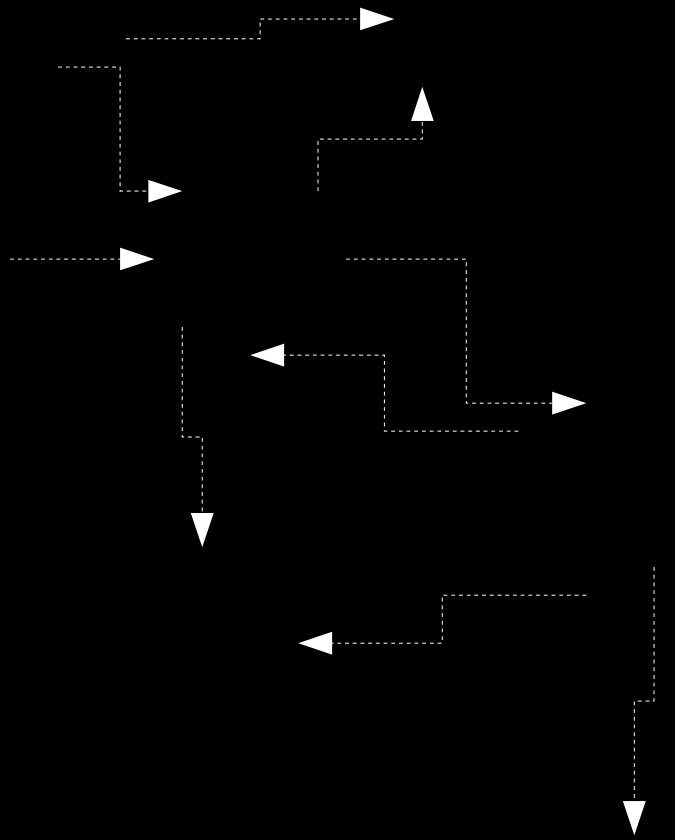

Codified
Communications
Channel

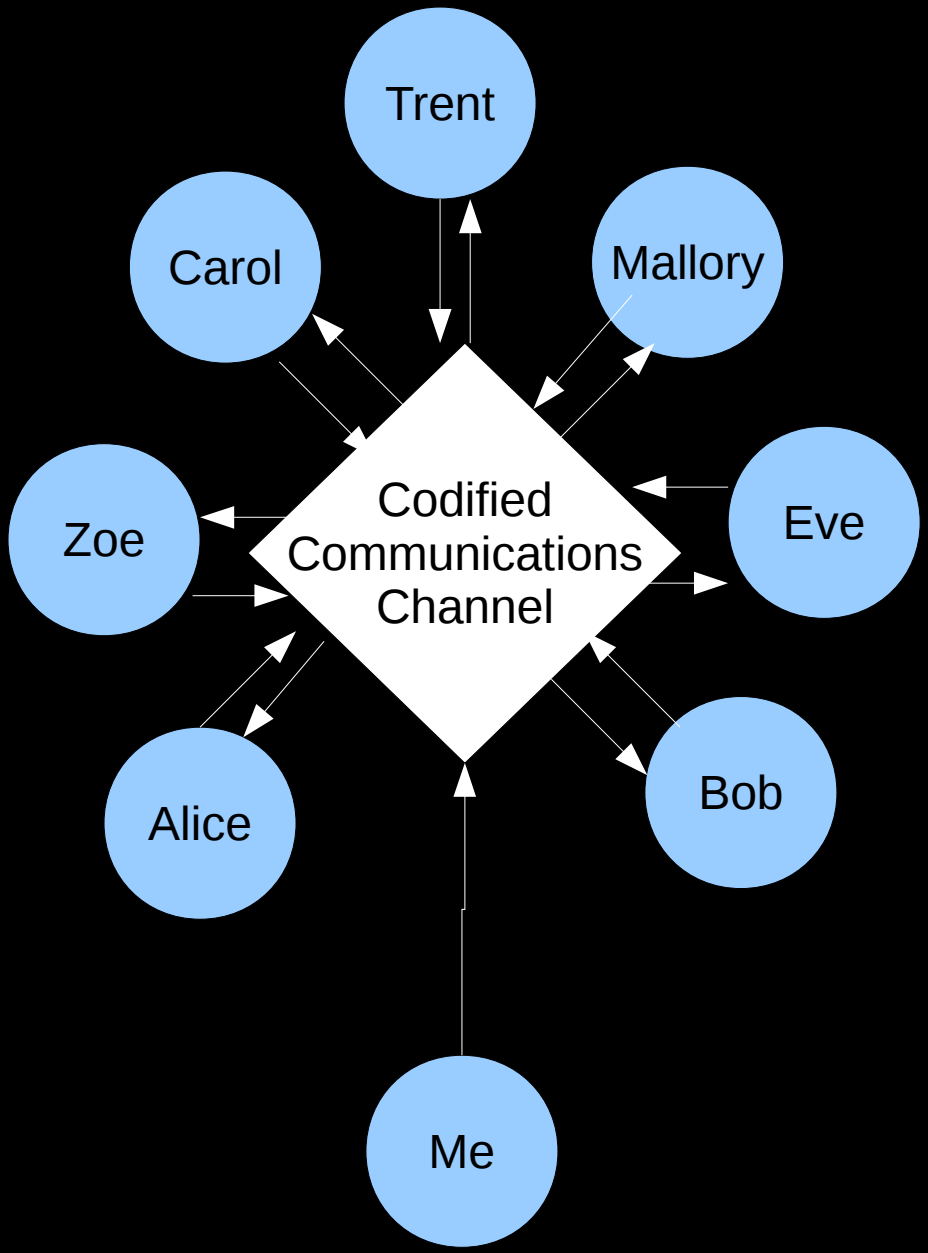

Alice
Bob
Mallory
Eve
Carol
Trent
Me
Zoe

“No Network Effect”

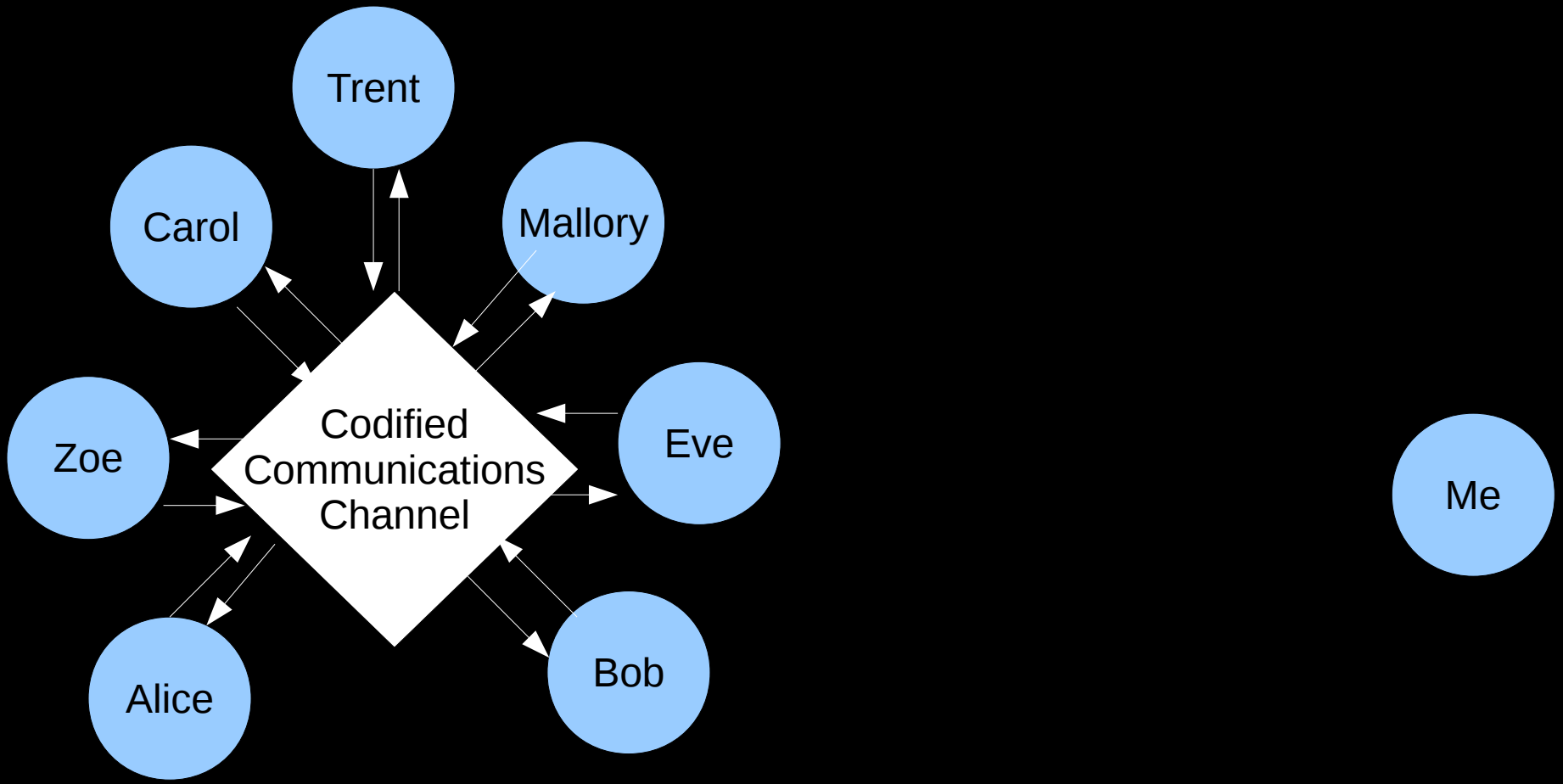



Trent
Carol
Mallory
Zoe
Codified
Communications
Channel
Eve
Alice
Bob
Me



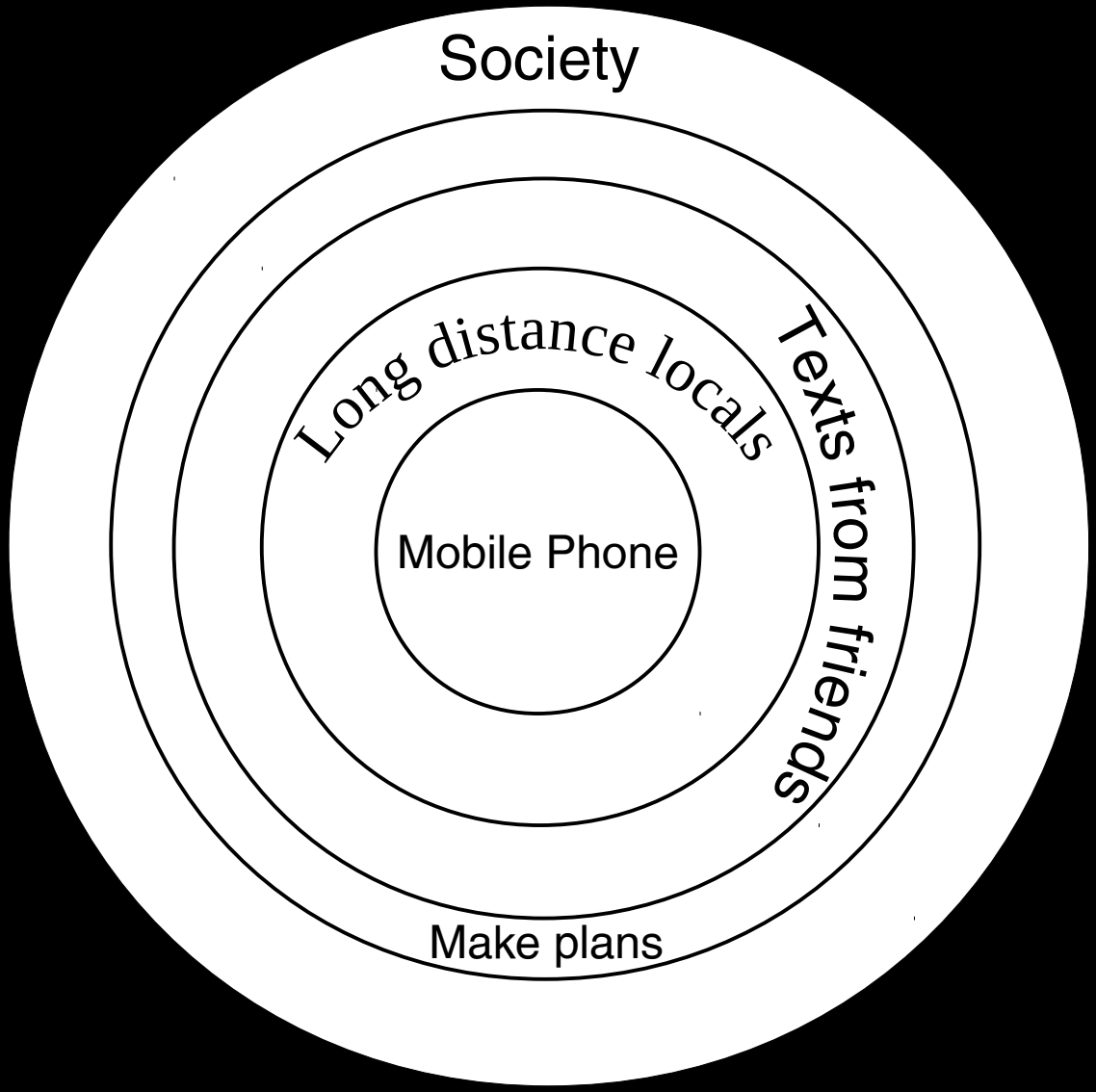

Trent
Carol
Mallory
Zoe
Codified
Communications
Channel
Eve
Alice
Bob
Me

“No Network Effect”

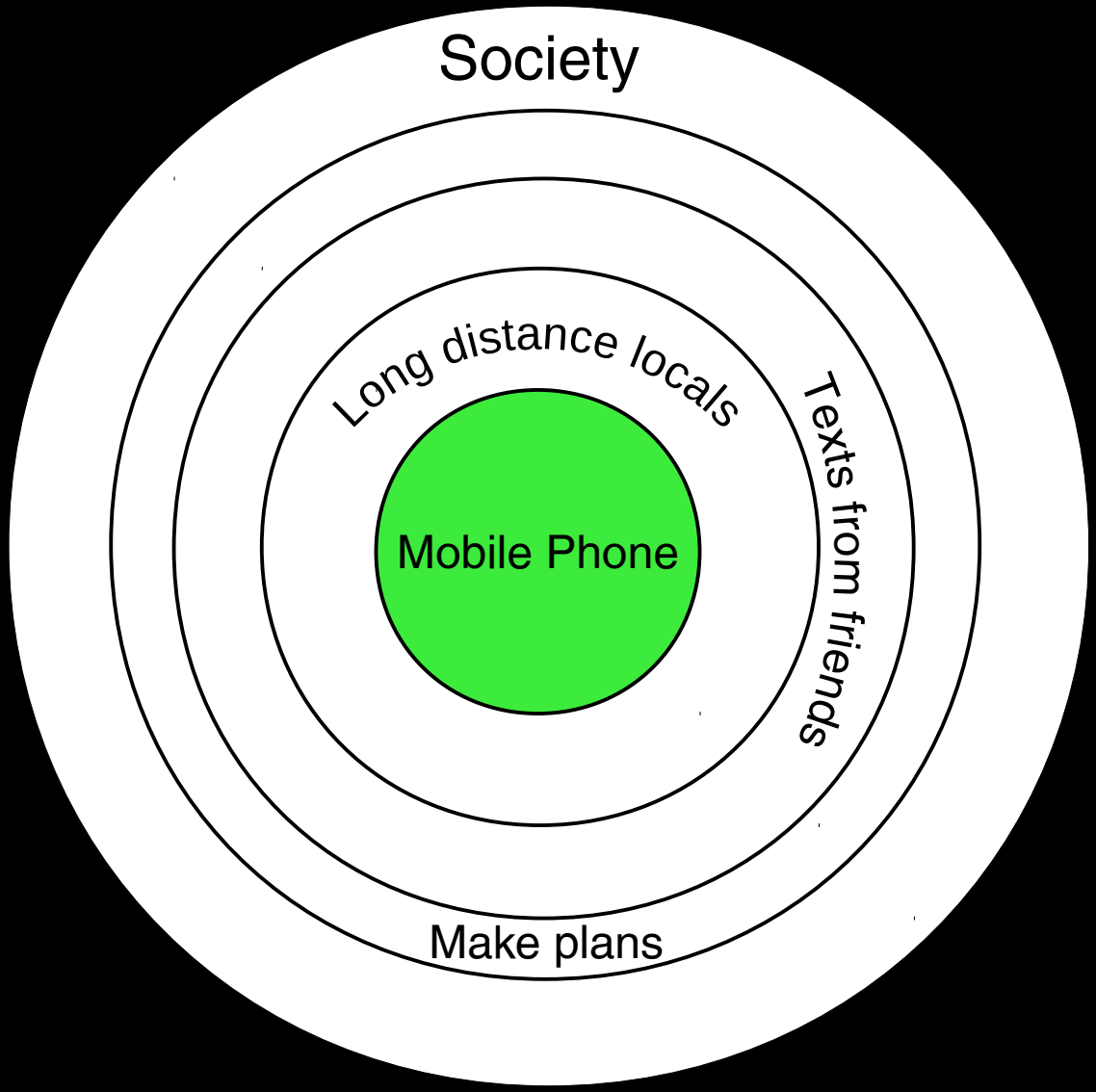


What *kind* of choice?

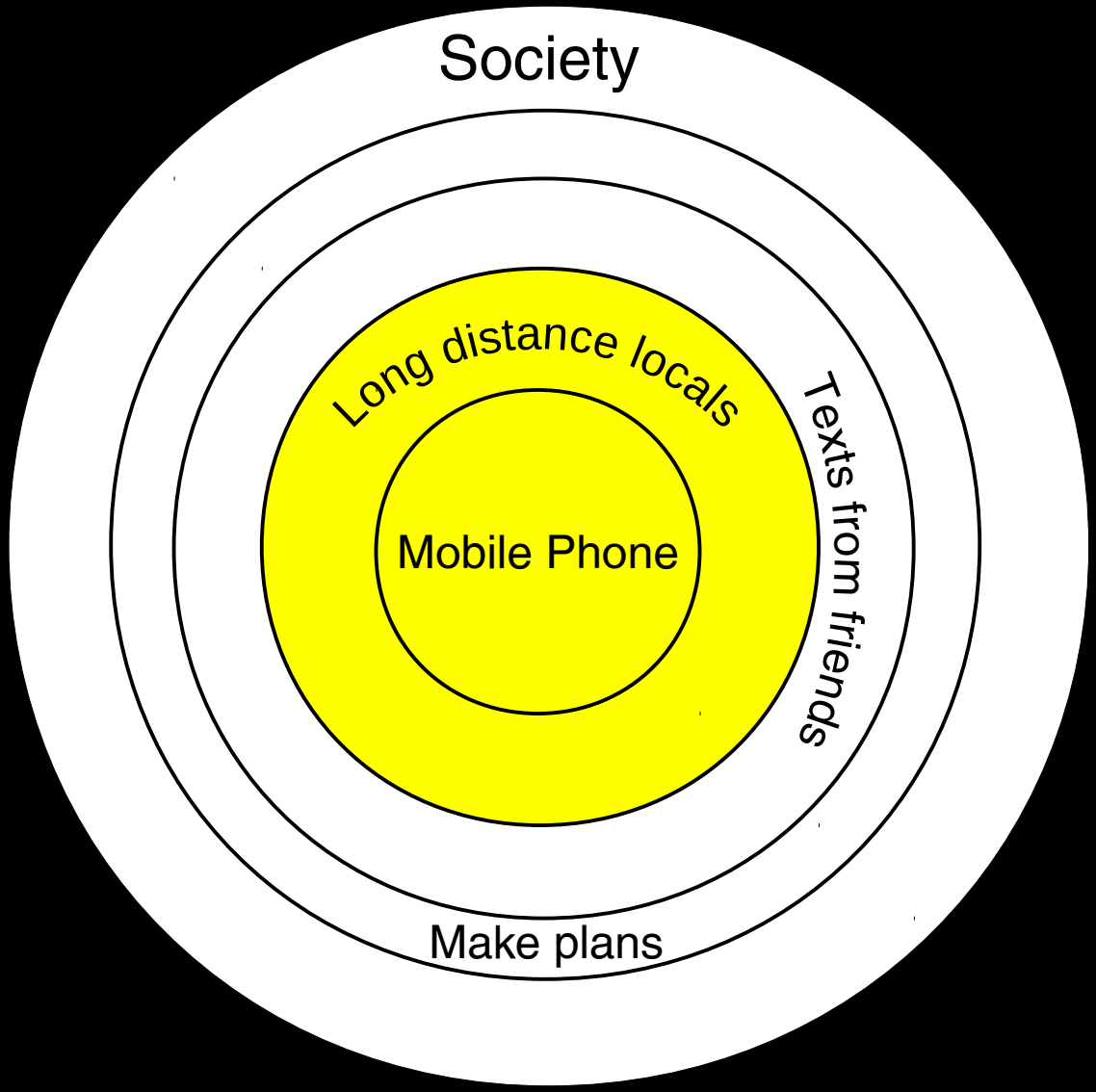
The push to expand choice scope



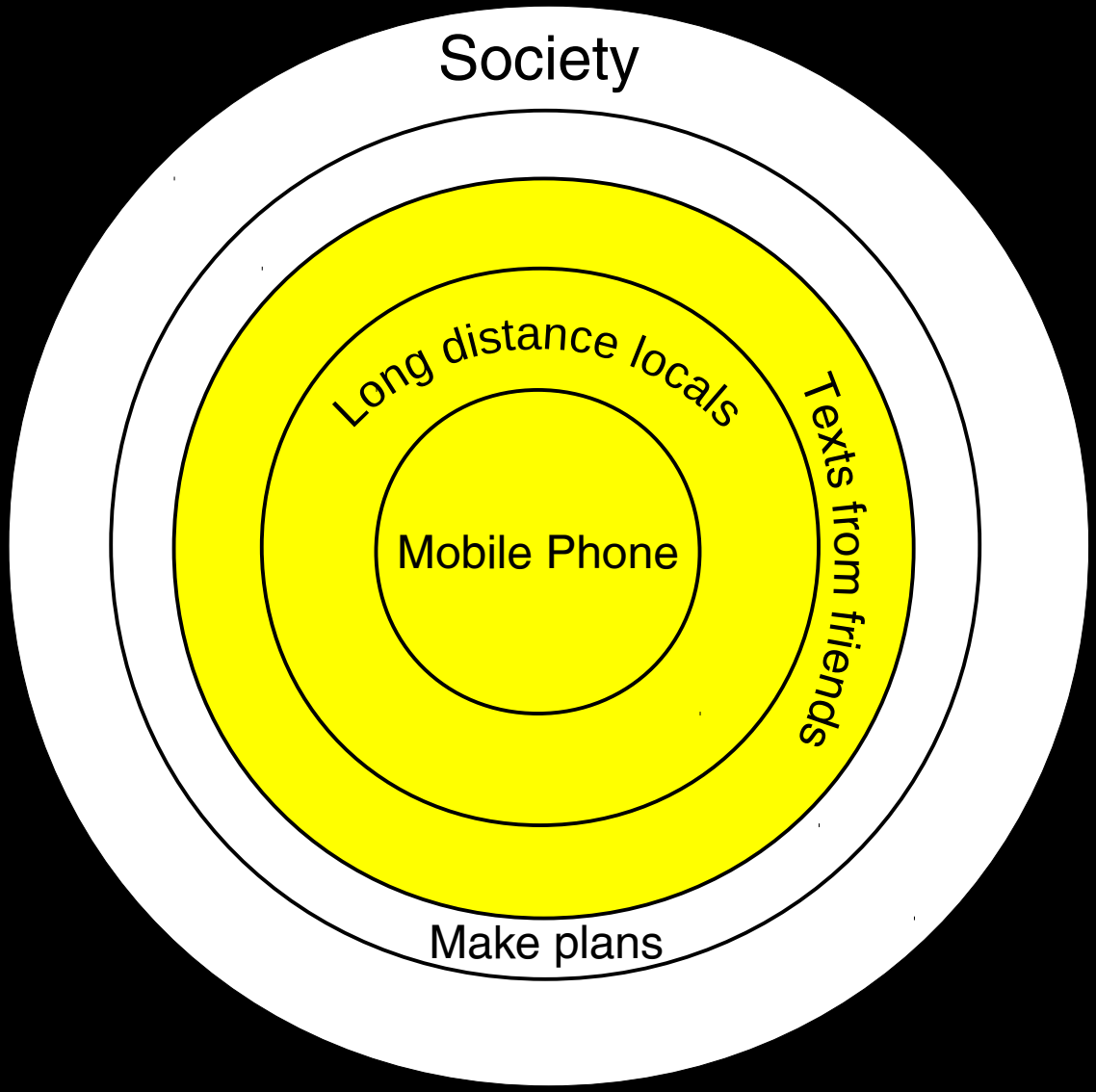
The push to expand choice scope



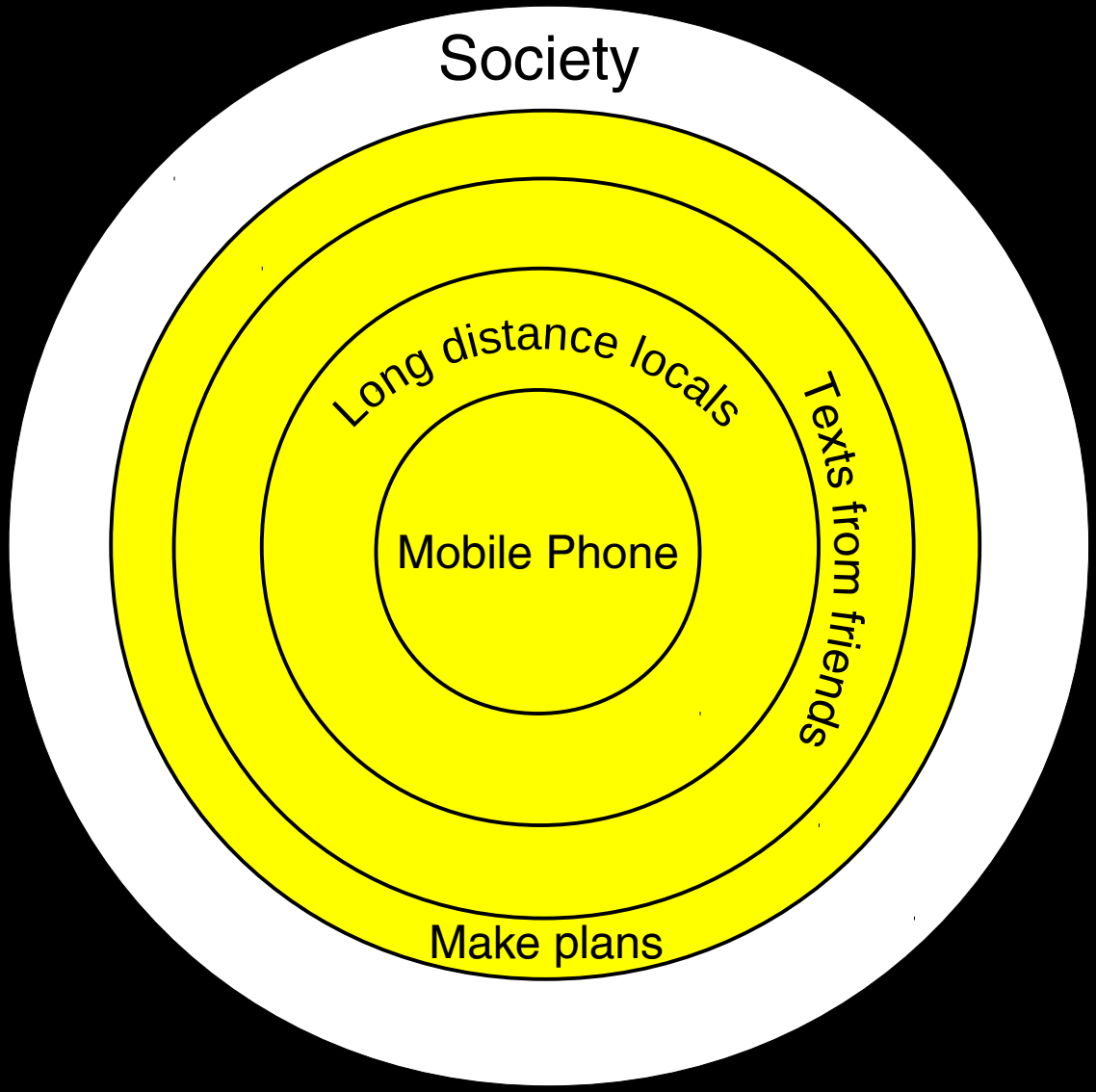
The push to expand choice scope



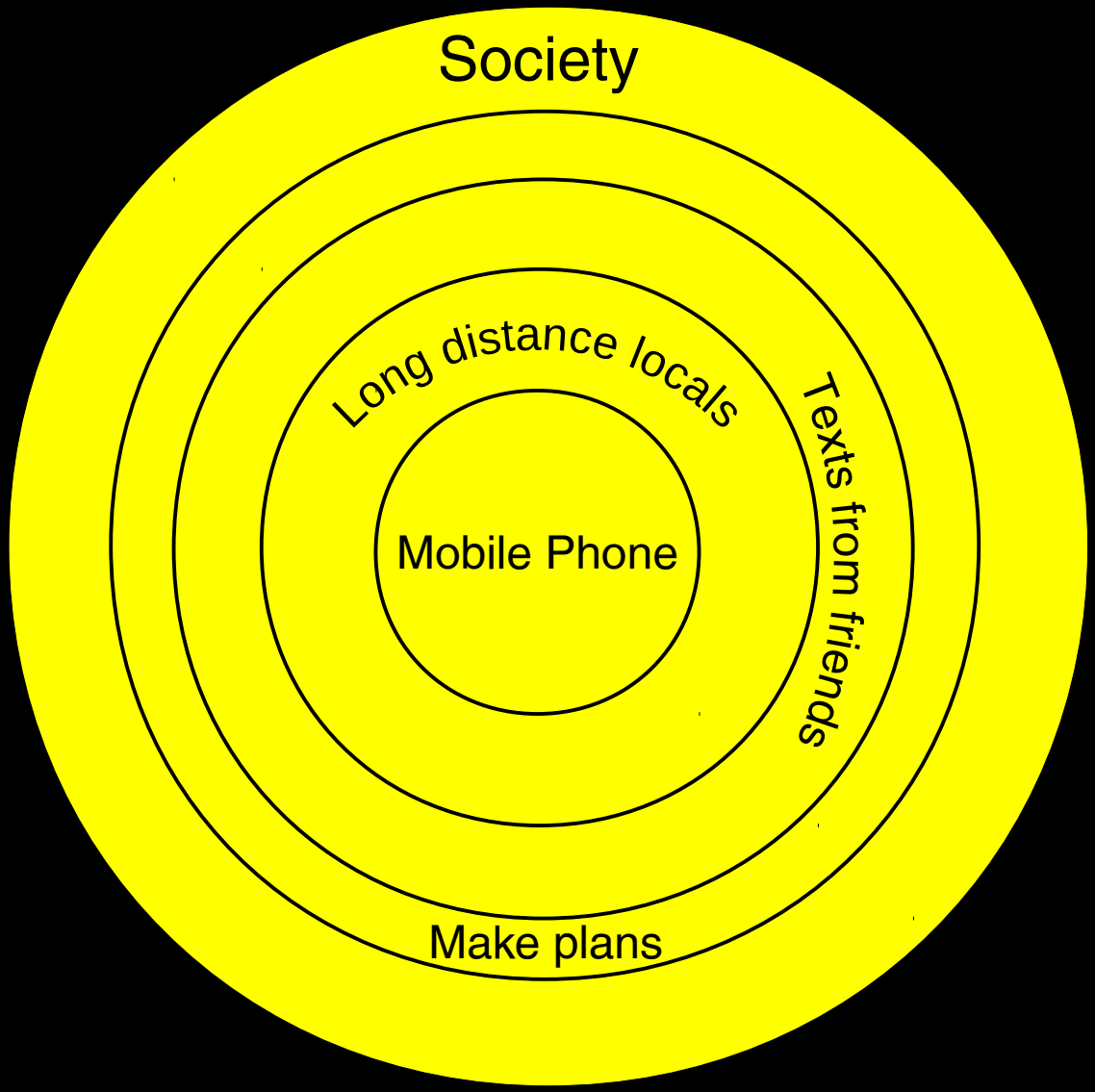
The push to expand choice scope



The push to expand choice scope



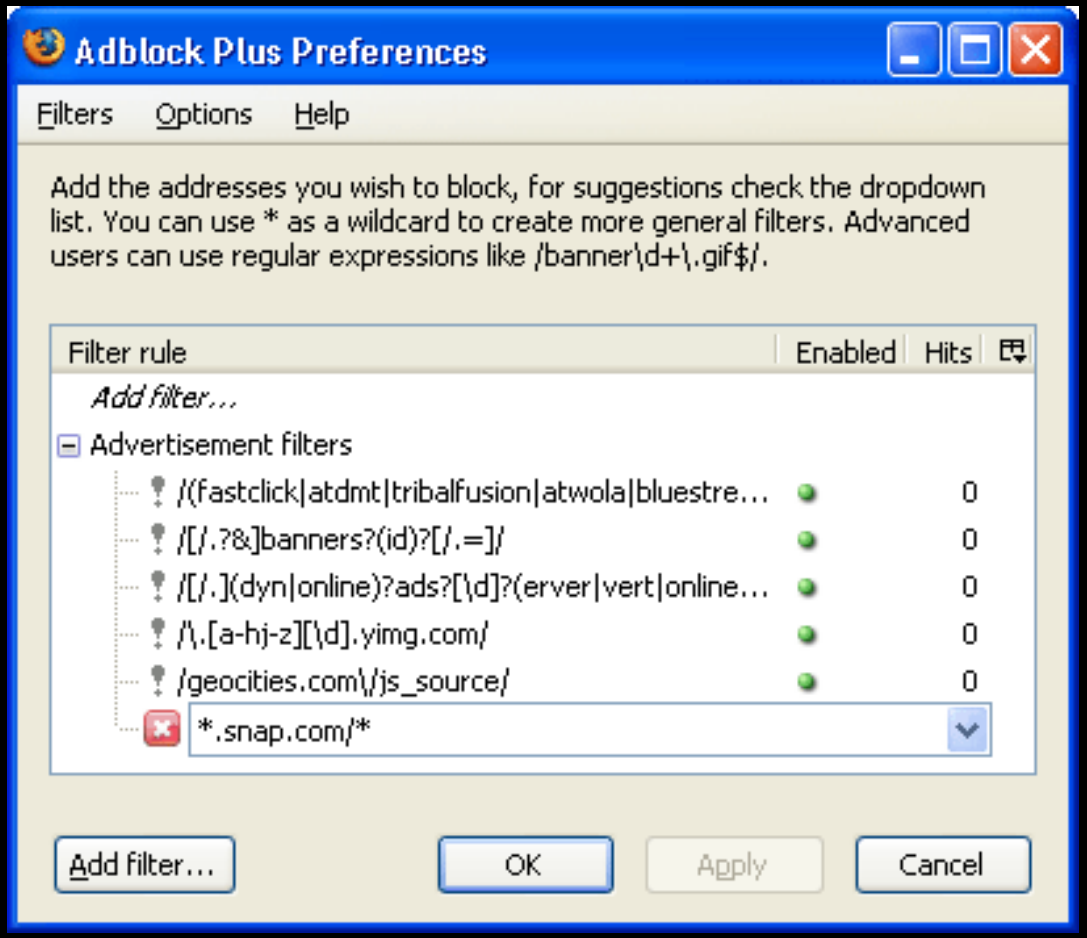
The push to expand choice scope



Small Chocies → Big Choices

EVERYWHERE

Another Example



Another Example

GOOGLE ANALYTICS == NOT EVIL?

Another Example

```
      <!-- BEGIN google analytics -->
  <script type="text/javascript">
    var gaJsHost = (("https:" == document.location.protocol) ?
"https://ssl." : "http://www.");
    document.write(unescape("%3Cscript src='" + gaJsHost +
"google-analytics.com/ga.js' type='text/javascript'%3E%3C
/script%3E"));
  </script>
  <script type="text/javascript">
    var pageTracker = _gat._getTracker("UA-30775-6");
    pageTracker._setDomainName("twitter.com");
          url = '/statuses/rebeccakelley/1207938518';
              pageTracker._setVar('Logged In');
        pageTracker._setVar('lang: en');
        pageTracker._trackPageview(url);
  </script>

  <!-- END google analytics -->
```

Expand the scope of the choice

SIGNIFICANT?

Moxie Marlinspike
Institute For Disruptive Studies


INFORMATION AWARENESS OFFICE
DARPA
SCIENTIA EST POTENTIA

Total Information Awareness

"...data must be made available in large-scale repositories with enhanced semantic content for easy analysis..."

-John Poindexter

A System For Easy Data Mining

- Store all:
  - Email
  - Web Traffic
  - Credit Card History
  - Medical Records
- Develop the technology to easily mine the massive amount of data you collect.

THE TOTALITARIAN FUTURE, THE CYPHERPUNK NIGHTMARE

Moxie Marlinspike
Institute For Disruptive Studies

People Freaked Out

People Freaked Out

People Freaked Out

People Freaked Out

People Freaked Out

Google™

A System For Easy Data Mining

- Store all:
  - Email
  - Web Traffic
  - Credit Card History
  - Medical Records

- Develop the technology to easily mine the massive amount of data you collect.
  - That's Google's jam!

Intent

Surveillance Business

Moxie Marlinspike
Institute For Disruptive Studies

Effect is the same

Who knows more about the citizens in their own country, Kim Jong-Il or Google?

Choice

The choice is expanding

SOCIETY

Trends Have Changed

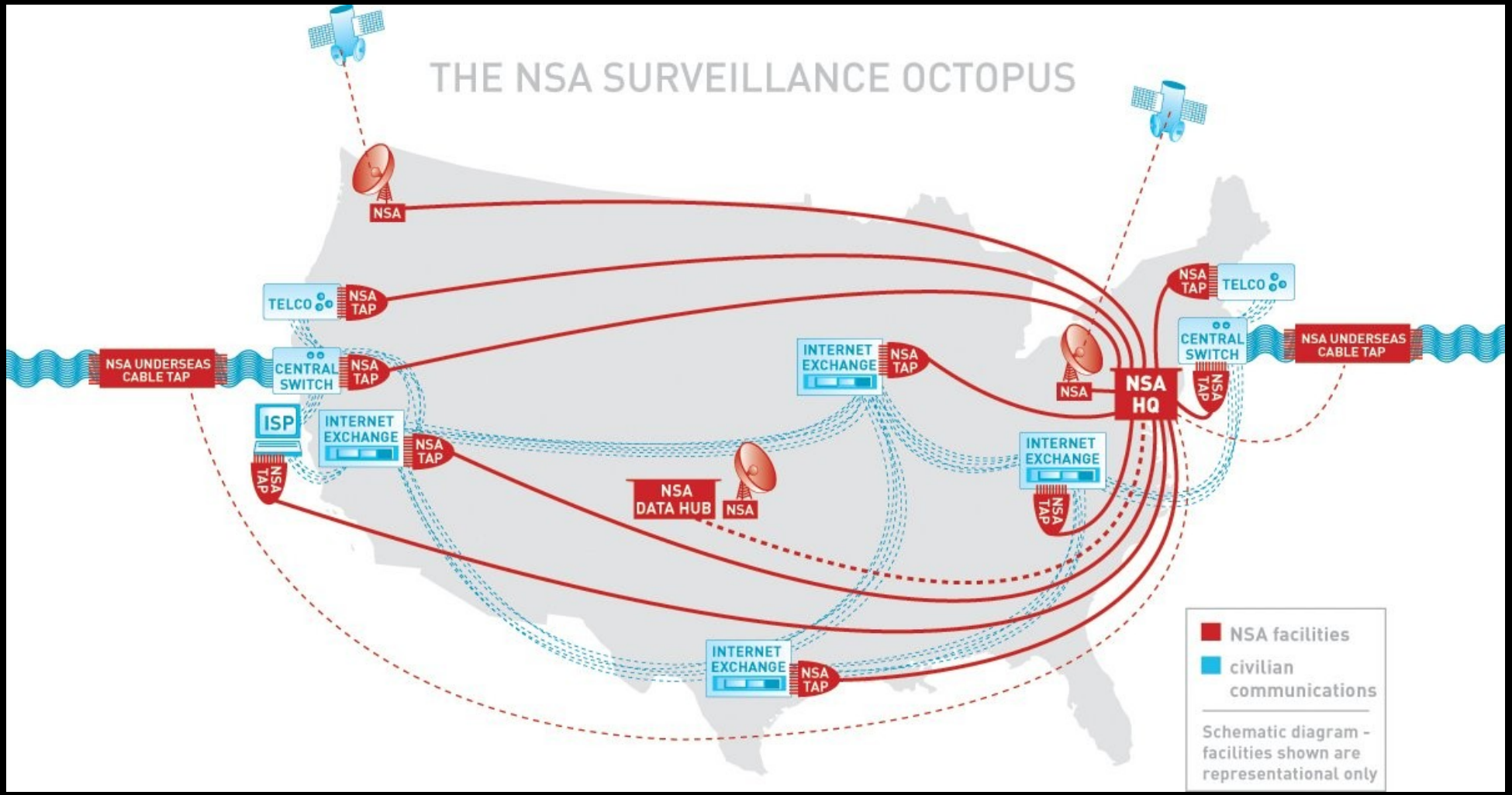
- Technology alters society.
- Information accumulates in distinct places as a result.
- Eavesdroppers move to those points of accumulation.

Past was direct

Past

Present is subtle

Present


THE NSA SURVEILLANCE OCTOPUS
NSA
TELCO
NSA TAP
NSA UNDERSEAS CABLE TAP
CENTRAL SWITCH
ISP
INTERNET EXCHANGE
NSA DATA HUB
NSA HQ
NSA facilities
civilian communications
Schematic diagram - facilities shown are representational only

Present

Past was direct

Present is subtle

Thoughts for the future

1. Deal with the choices that aren't choices.

Acknowledge

Choices → Expanding

Choices → Demands

Some Projects

What's up with Google?

- They have an awful lot of data.
  - They record everything. Your IP address, the cookie they issue, your search requests, the contents of every email you've sent or received, the news you read, the places you go, even your TCP headers. They're even collecting realtime GPS location and DNS lookups.
  - The know who your friends are, where you live, where you work, and where you spend your free time. They know about your health, your love life, and your political leanings.
  - They know not just what you're *doing*, but also a lot about what you're *thinking*.

Control the terms

- “We anonymize your data after nine months.”
  - “Anonymize” means drop the last octet of an IP address. And cookies are simply translated.
- “We take privacy so seriously that we put it under your control.”
  - Only shows you some of the information that they are most obviously capable of connecting to you.
  - Requires that you have an account, be logged in while using services, and maintain a consistent cookie in order to participate.

“If there's something you don't want anyone to know, maybe you shouldn't be doing it in the first place.”

– Eric Schmidt, Google CEO

“AURORA” WAS ABOUT INTERCEPT

GoogleSharing

Moxie Marlinspike
Institute For Disruptive Studies

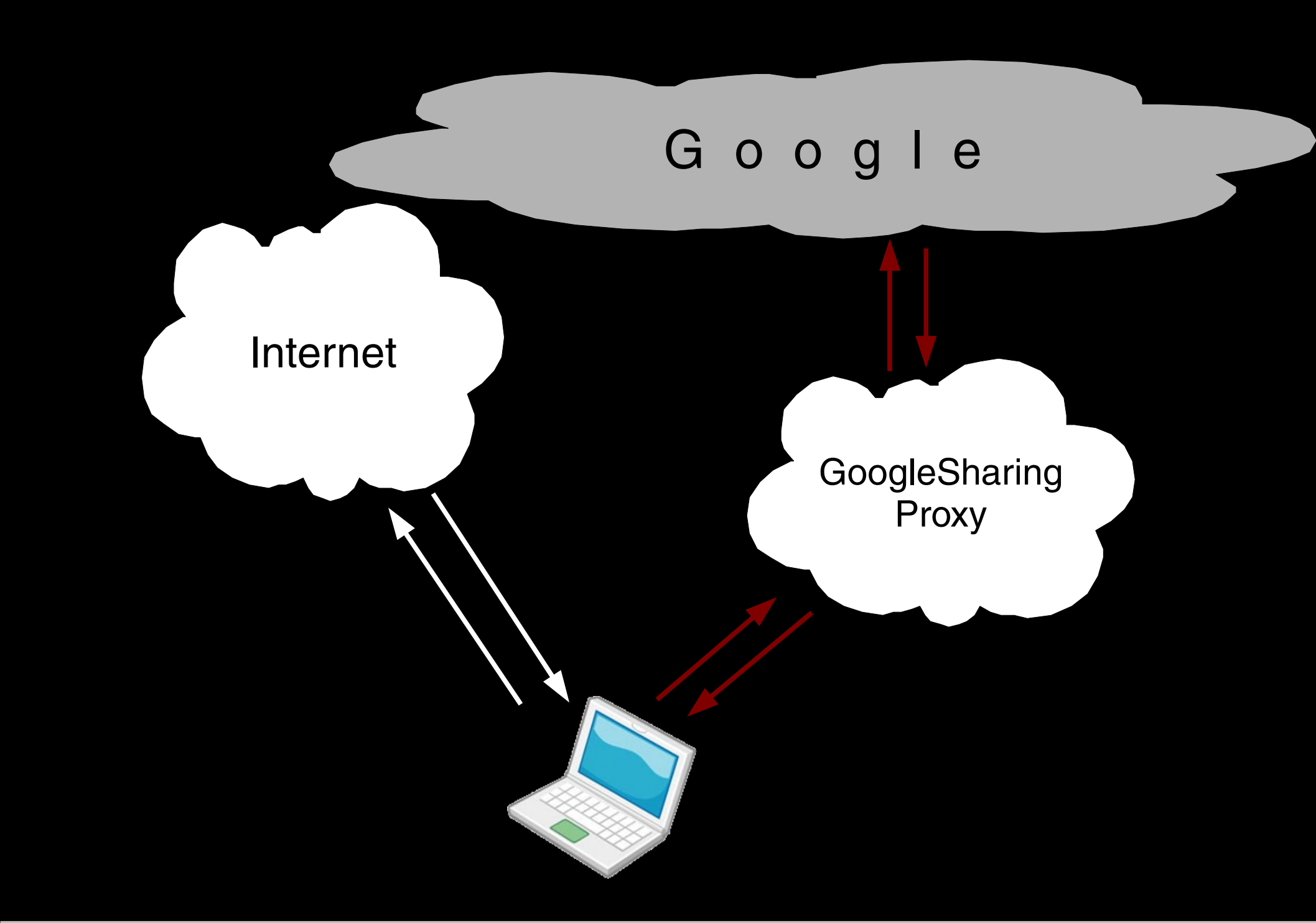
Premise

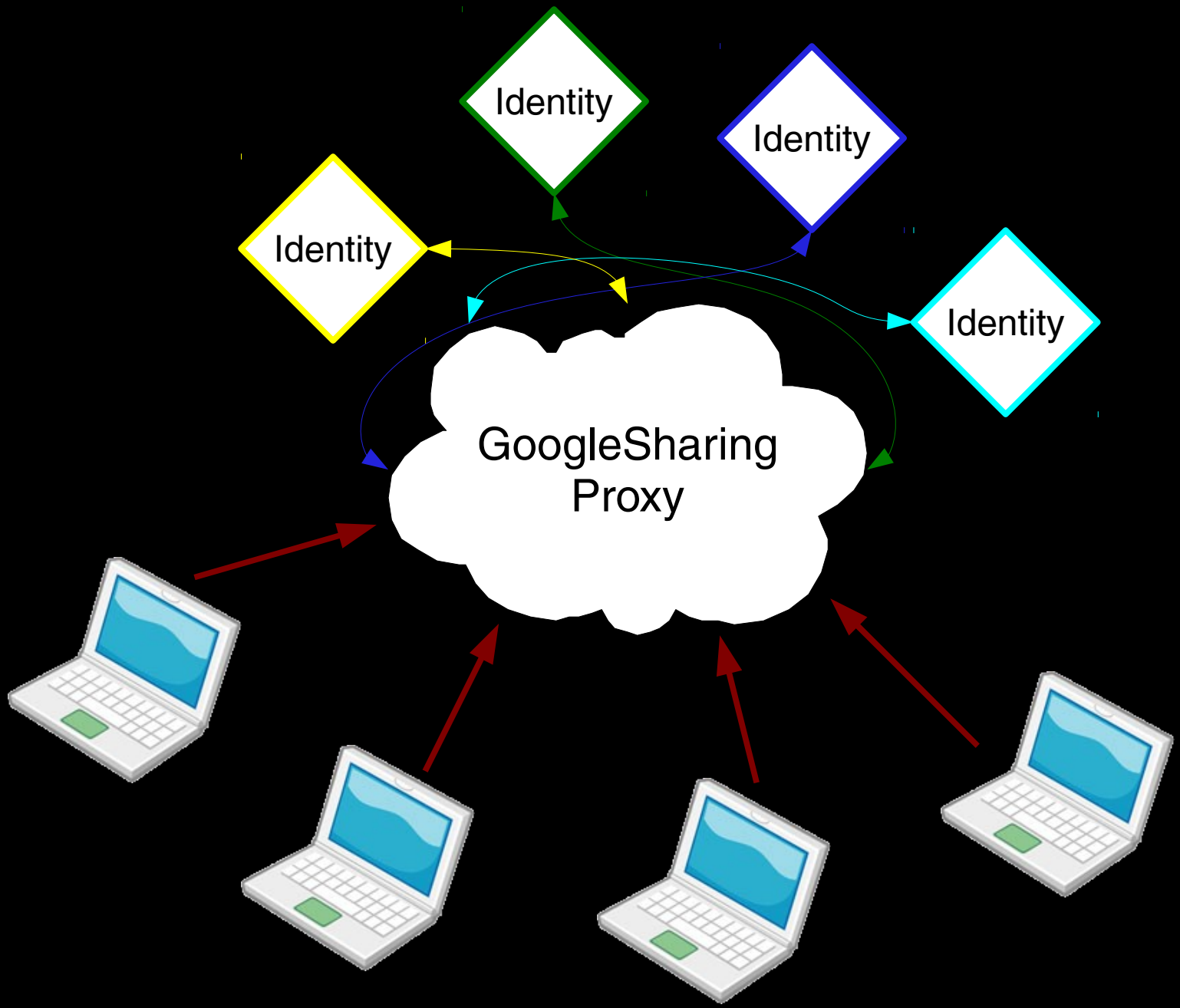
- The scope of the “Google choice” has become quite large.
- We need some innovation that allows us to reject this type of false choice while still maintaining anonymity.
- We need anonymous access to Google services that is fast and reliable.

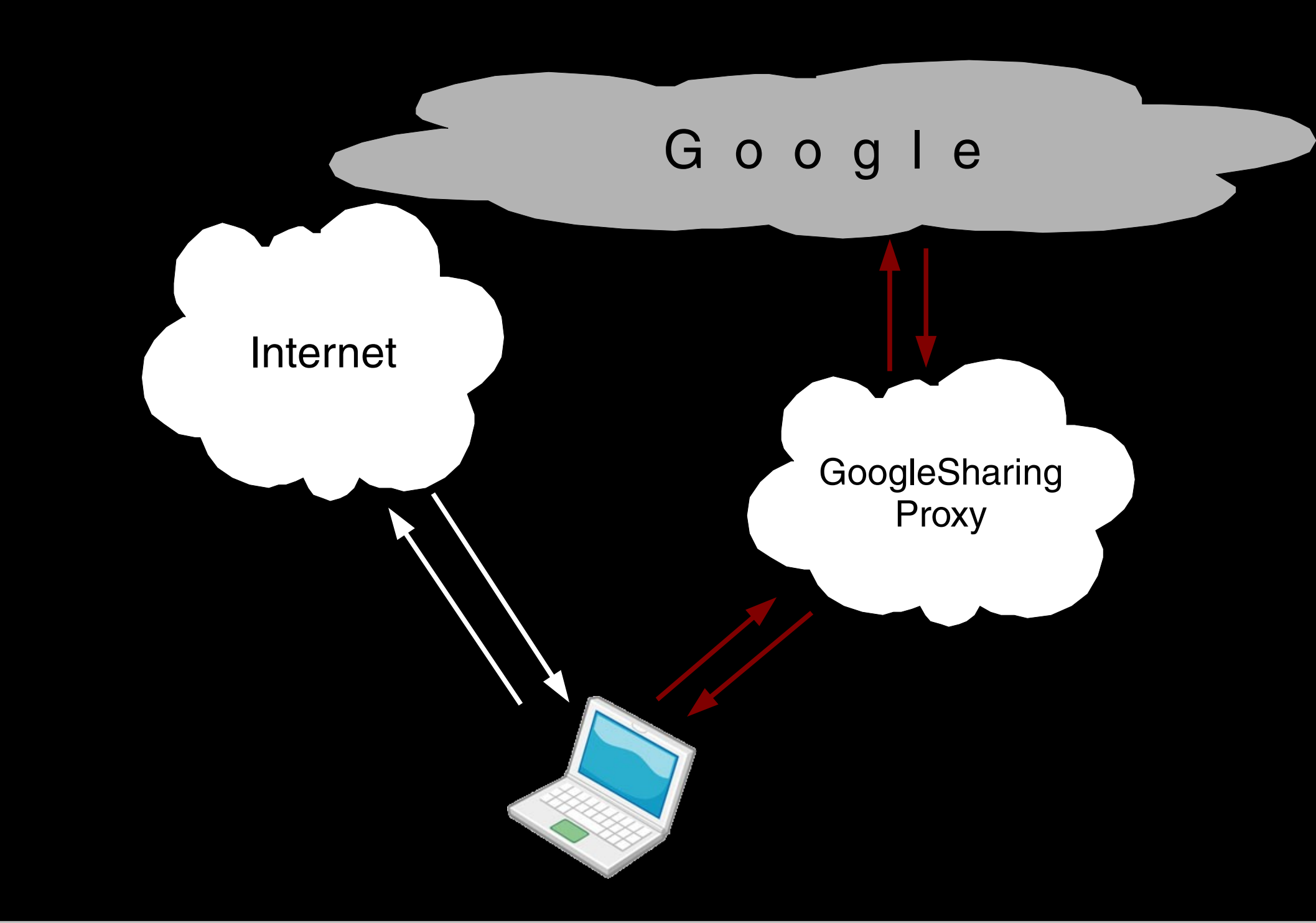
GoogleSharing

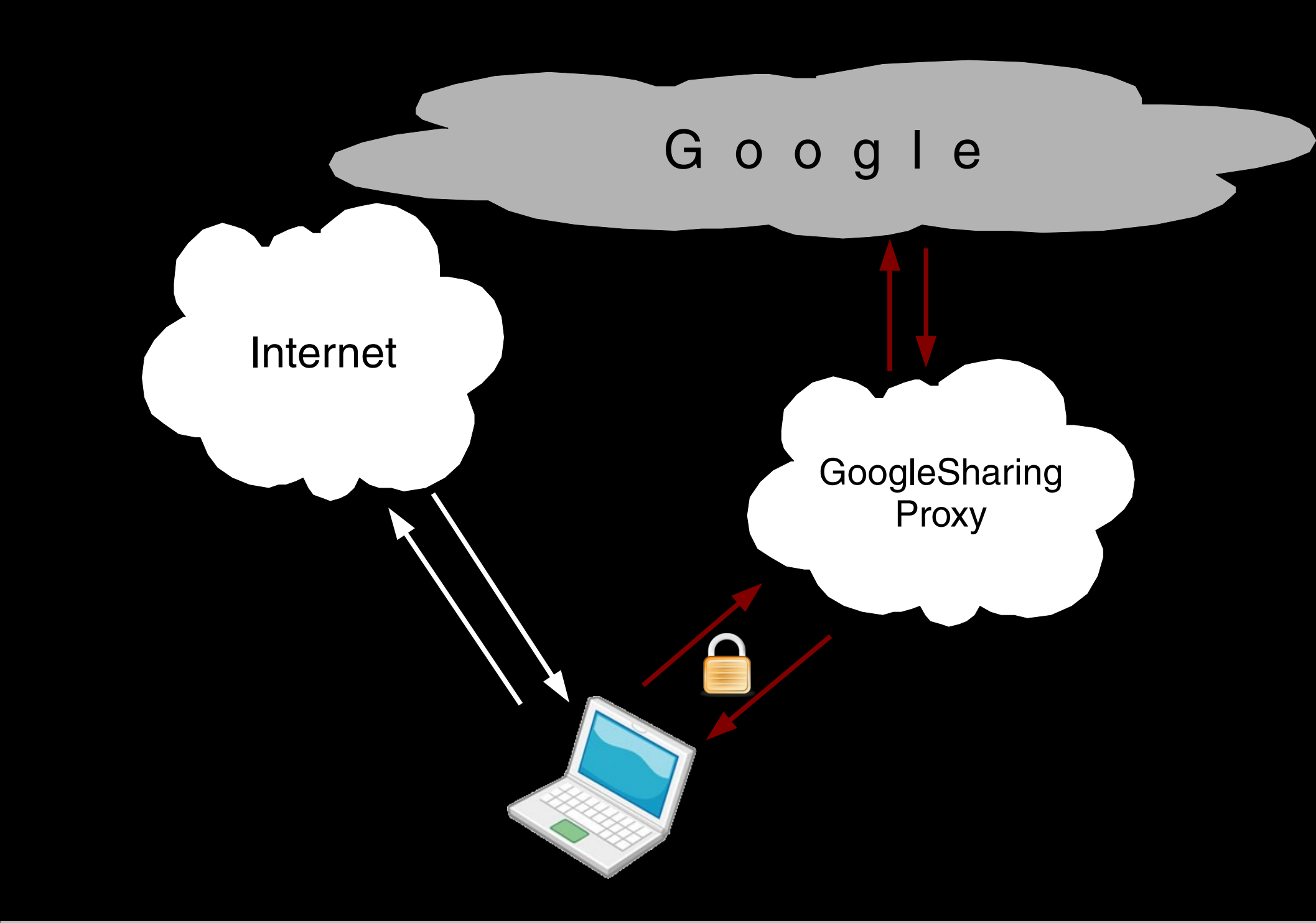
+

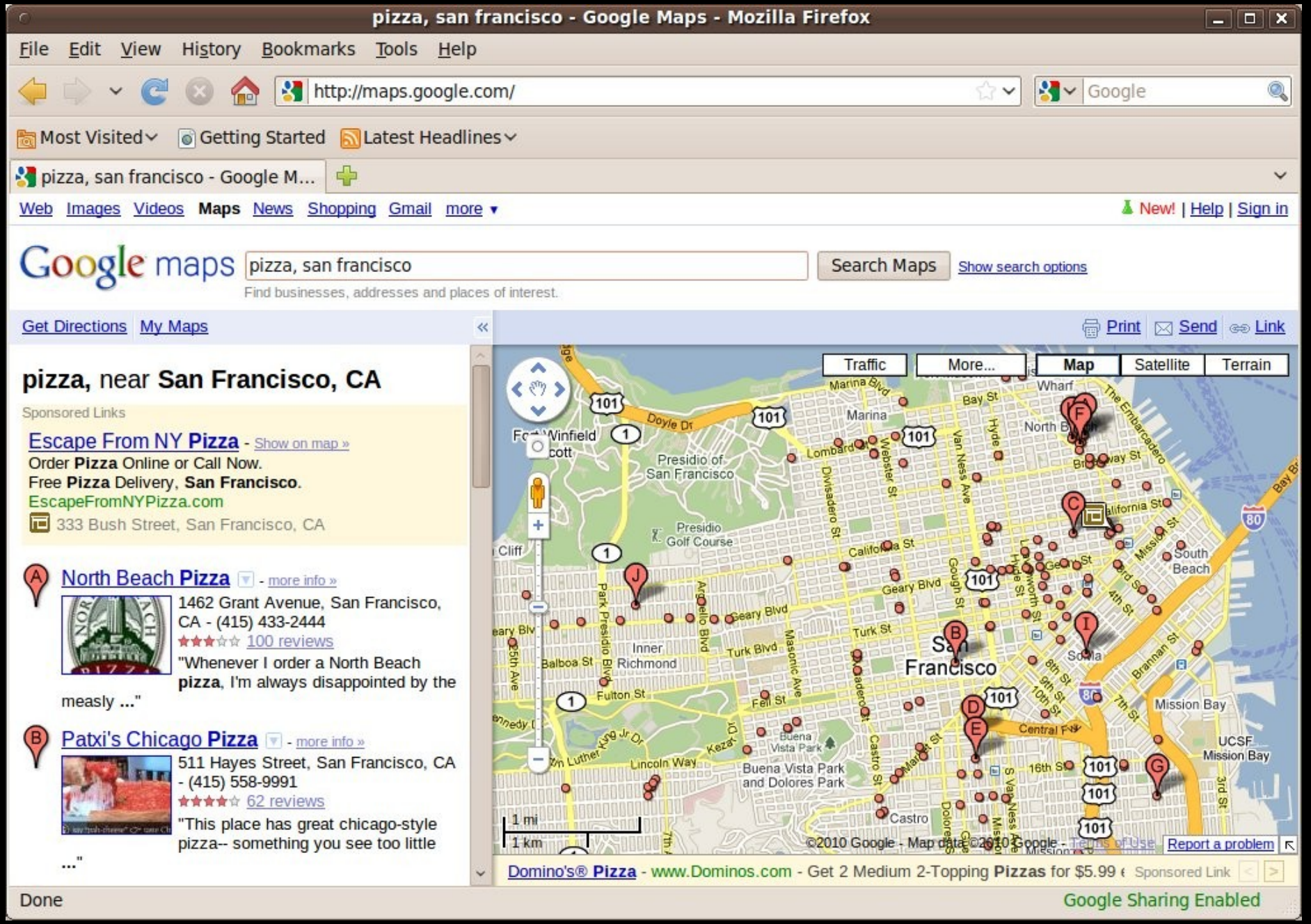
+


G o o g l e
Internet
GoogleSharing
Proxy


Identity
Identity
Identity
Identity
GoogleSharing
Proxy


G o o g l e
Internet
GoogleSharing
Proxy


G o o g l e
Internet
GoogleSharing
Proxy


pizza, san francisco - Google Maps - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://maps.google.com/
Google
Most Visited
Getting Started
Latest Headlines
pizza, san francisco - Google M...
Web Images Videos Maps News Shopping Gmail more
New! | Help | Sign in
Google maps
pizza, san francisco
Search Maps
Show search options
Find businesses, addresses and places of interest.
Get Directions
My Maps
Print
Send
Link
pizza, near San Francisco, CA
Sponsored Links
Escape From NY Pizza - Show on map »
Order Pizza Online or Call Now.
Free Pizza Delivery, San Francisco.
EscapeFromNYPizza.com
333 Bush Street, San Francisco, CA
A
North Beach Pizza - more info »
1462 Grant Avenue, San Francisco, CA - (415) 433-2444
100 reviews
"Whenever I order a North Beach pizza, I'm always disappointed by the measly ..."
B
Patxi's Chicago Pizza - more info »
511 Hayes Street, San Francisco, CA - (415) 558-9991
62 reviews
"This place has great chicago-style pizza-- something you see too little ..."
Traffic
More...
Map
Satellite
Terrain
San Francisco
Marina
Presidio of San Francisco
Presidio Golf Course
Inner Richmond
Buena Vista Park and Dolores Park
South Beach
Mission Bay
UCSF Mission Bay
Castro
1 mi
1 km
©2010 Google - Map data ©2010 Google - Terms of Use
Report a problem
Domino's® Pizza - www.Dominos.com - Get 2 Medium 2-Topping Pizzas for $5.99 ¢
Sponsored Link
Done
Google Sharing Enabled

Business - Google News - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://news.google.com/news/section?pz=1&cf=all&ned=us&topic=b&ict=ln

Most Visited Getting Started Latest Headlines

Business - Google News

Web Images Videos Maps **News** Shopping Gmail more ▾ Sign in

Google news

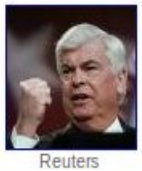
Search News Search the Web Advanced news search Preferences

U.S.

- Top Stories
- Starred
- World
- U.S.
- **Business**
- Sci/Tech
- Entertainment
- Sports
- Health
- Spotlight
- Most Popular

› **All news**
Headlines
Images

Business Updated **5 minutes ago**


Reuters

Fed gets new oversight powers under Dodd bill: sources

Reuters - Jim Young - **15 minutes ago**

Senator Christopher Dodd (D-CT) addresses the AFL-CIO Building and Construction Trades Presidential Candidates Forum in Washingtonn,in this March 28, 2007 file photo.

Dodd's Financial Overhaul Plan Said to Transform Fed Powers BusinessWeek
Dodd seeking middle ground on new financial rules The Associated Press
New York Times - Politico - Financial Times - WBUR
all 144 news articles » Email this story


Times Online

Wen Rebuffing Yuan Calls Risks Retaliation From US Congress

BusinessWeek - **4 hours ago**

March 15 (Bloomberg) -- Chinese Premier Wen Jiabao rebuffed calls for the yuan to appreciate, risking a further downturn in relations with the US where lawmakers and economists say his stance is hampering a global recovery.

Chinese premier slams US 'protectionism,' says yuan is not too low Los Angeles Times
Wen links inflation to Communist party future Financial Times
Wall Street Journal - Economic Times - Washington Post
all 2,185 news articles » GOOG Email this story


ABC News

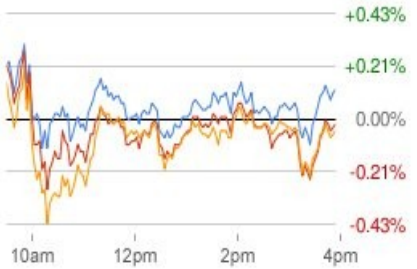
Toyota, US Can't Replicate Prius Acceleration (Correct)

BusinessWeek - Angela Greiling Keane - **58 minutes ago**

March 15 (Bloomberg) -- Tests by Toyota Motor Corp. and US regulators on a Prius hybrid whose driver said it accelerated out of control couldn't replicate his account, according to a report prepared for US lawmakers.

Investigation questions Prius driver's story: report Reuters

Finance Powered by Google Finance



Dow	10,624.69	+12.85	(0.12%)
S&P 500	1,149.99	-0.25	(-0.02%)
Nasdaq	2,367.66	-0.80	(-0.03%)

Quotes

Get quotes
Example: "CSCO" or "Google"

In the news

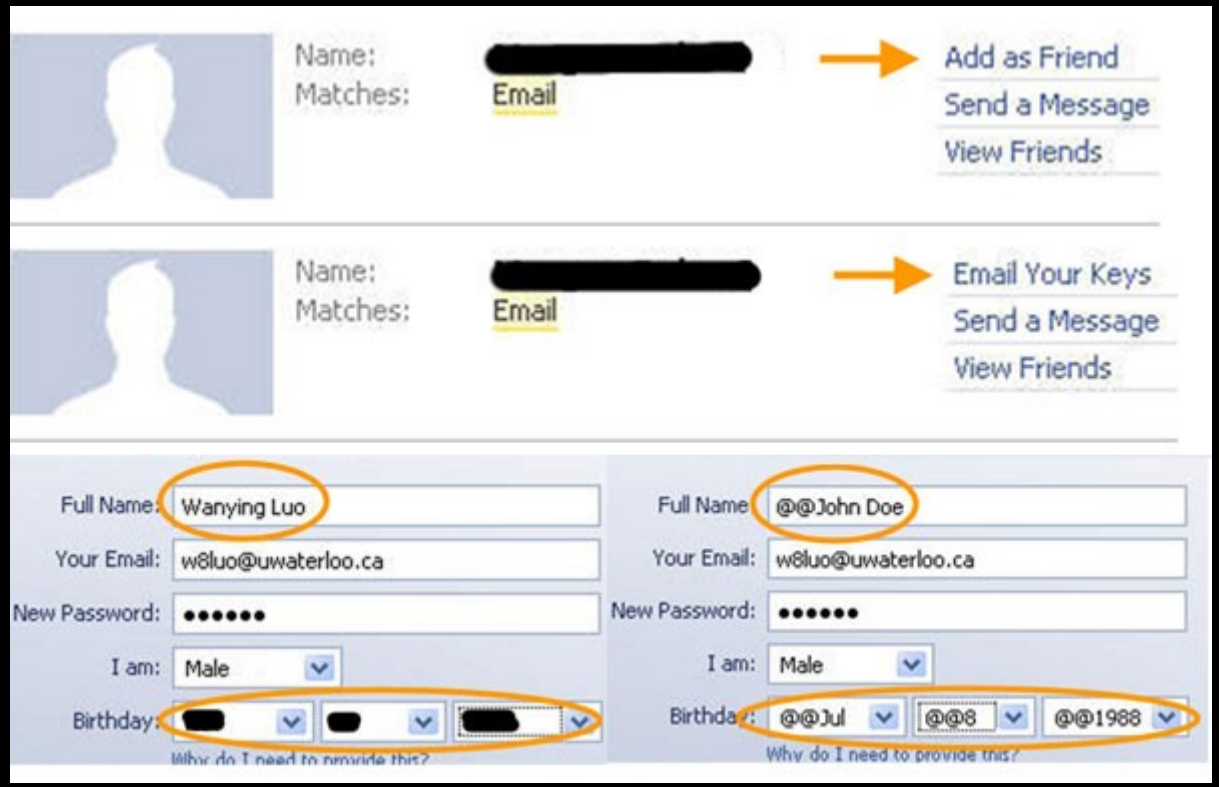
GOOG	579.54	-1.60	(-0.28%)
TM	76.99	+0.05	(0.06%)
TOM	28.19	-0.10	(-0.37%)

Done Google Sharing Enabled

FACECLOAK

Moxie Marlinspike
Institute For Disruptive Studies

Prof. Urs Hengartner


Name:
Matches:
Email
Add as Friend
Send a Message
View Friends
Name:
Matches:
Email
Email Your Keys
Send a Message
View Friends
Full Name:
Wanying Luo
Your Email:
w8luo@uwaterloo.ca
New Password:
I am:
Male
Birthday:
Why do I need to provide this?
Full Name
@@John Doe
Your Email:
w8luo@uwaterloo.ca
New Password:
I am:
Male
Birthday:
@@Jul
@@8
@@1988
Why do I need to provide this?

TWITTER

BROADCAST || CONVERSATION

Second thesis

CRYPTO WAR → DATA FREEDOM

Moxie Marlinspike
Institute For Disruptive Studies

Future of data control

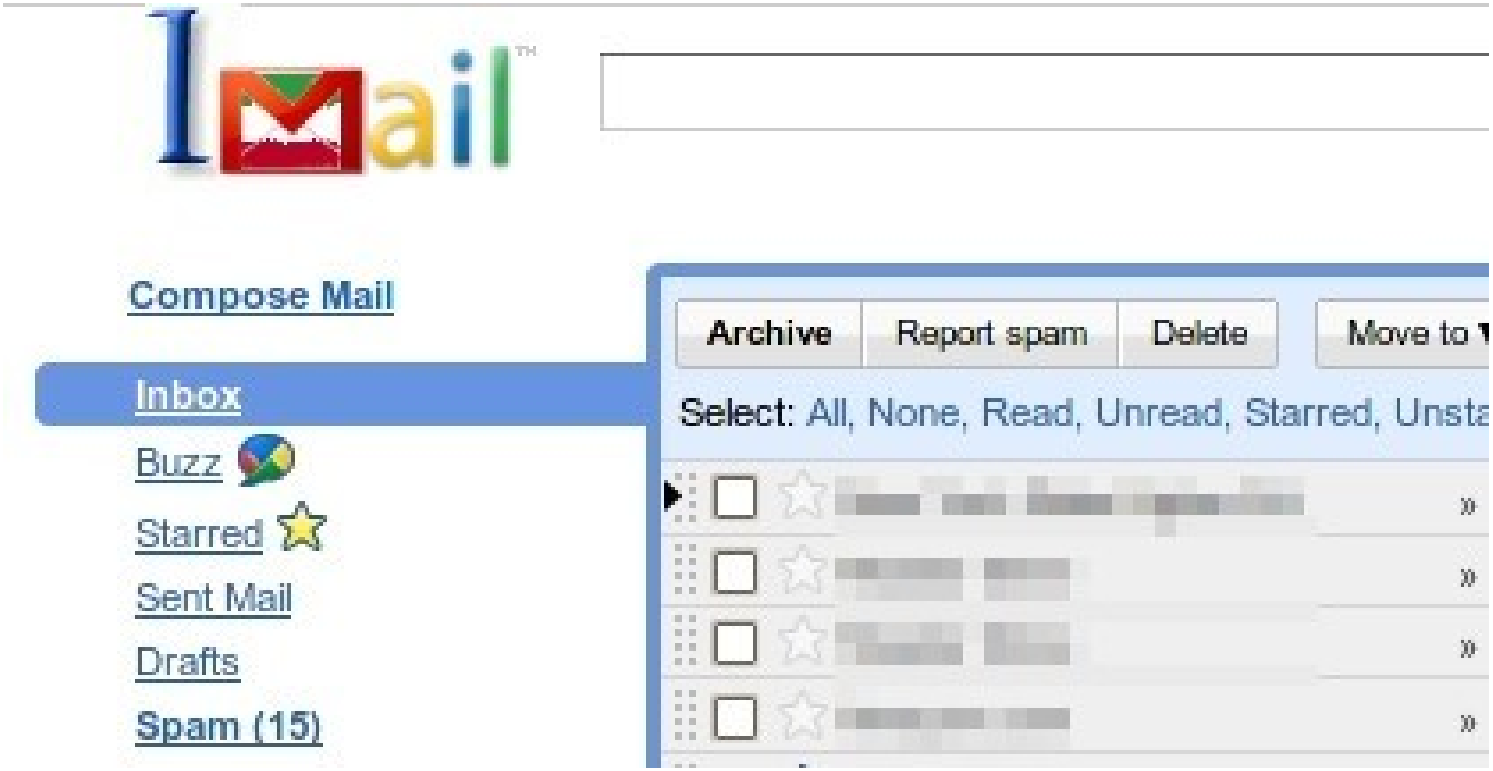
Projects born out of reality

DARKNETS, DATA HAVENS, HIDDEN SERVICES

Not the future we got

Privacy advocates love "the other."

“Iran launches national email service”



LOSS ON CRYPTO

GIVING UP → CHANGING STRATEGIES

Key escrow → Key disclosure

Regulation of Investigatory Powers Act (RIPA)

KEY DISCLOSURE

NO FORWARD SECURITY

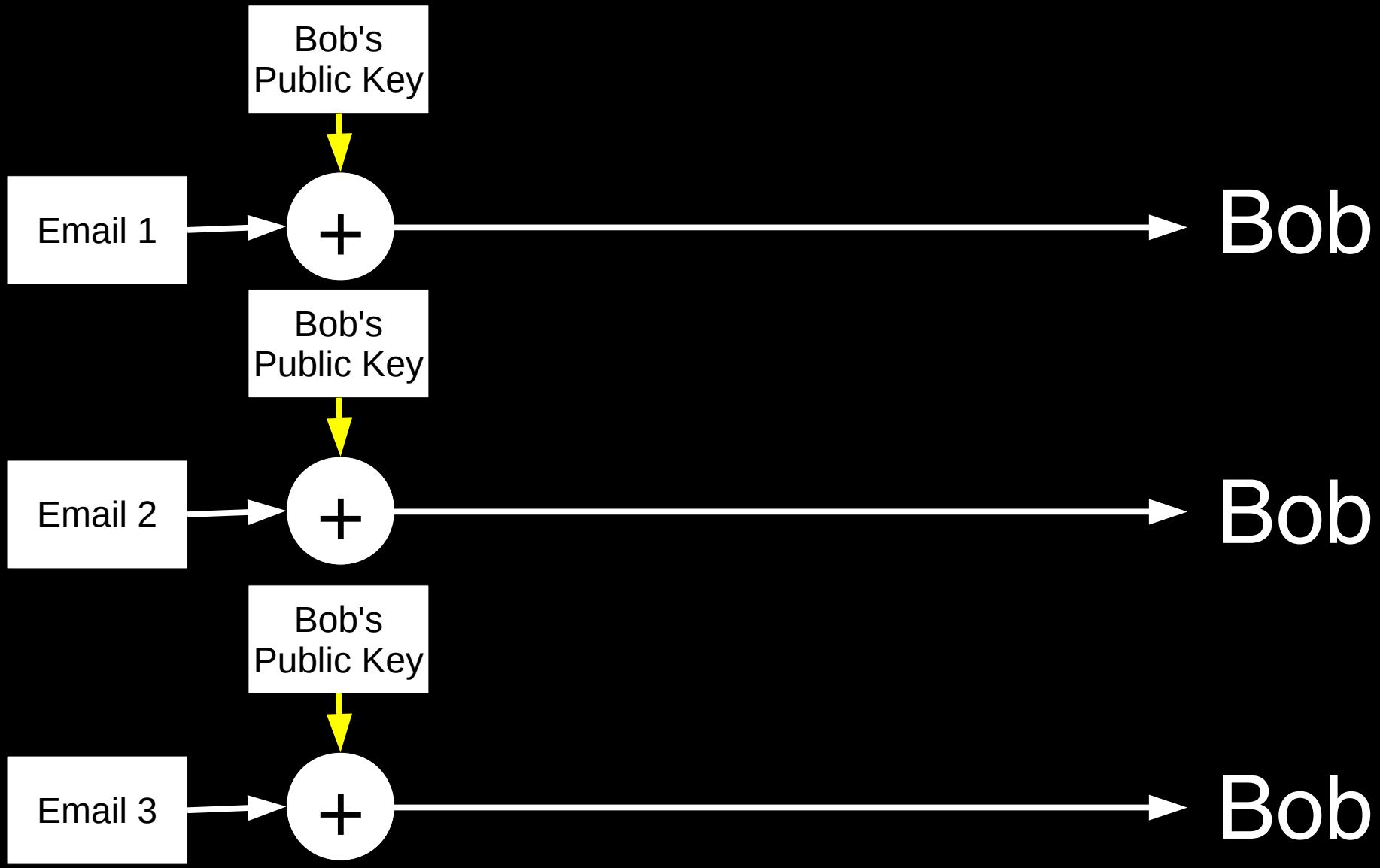
Tasks For The Future

1. Deal with the choices that aren't choices.
2. Worry a little less about information freedom.
3. Worry a lot more about forward security.

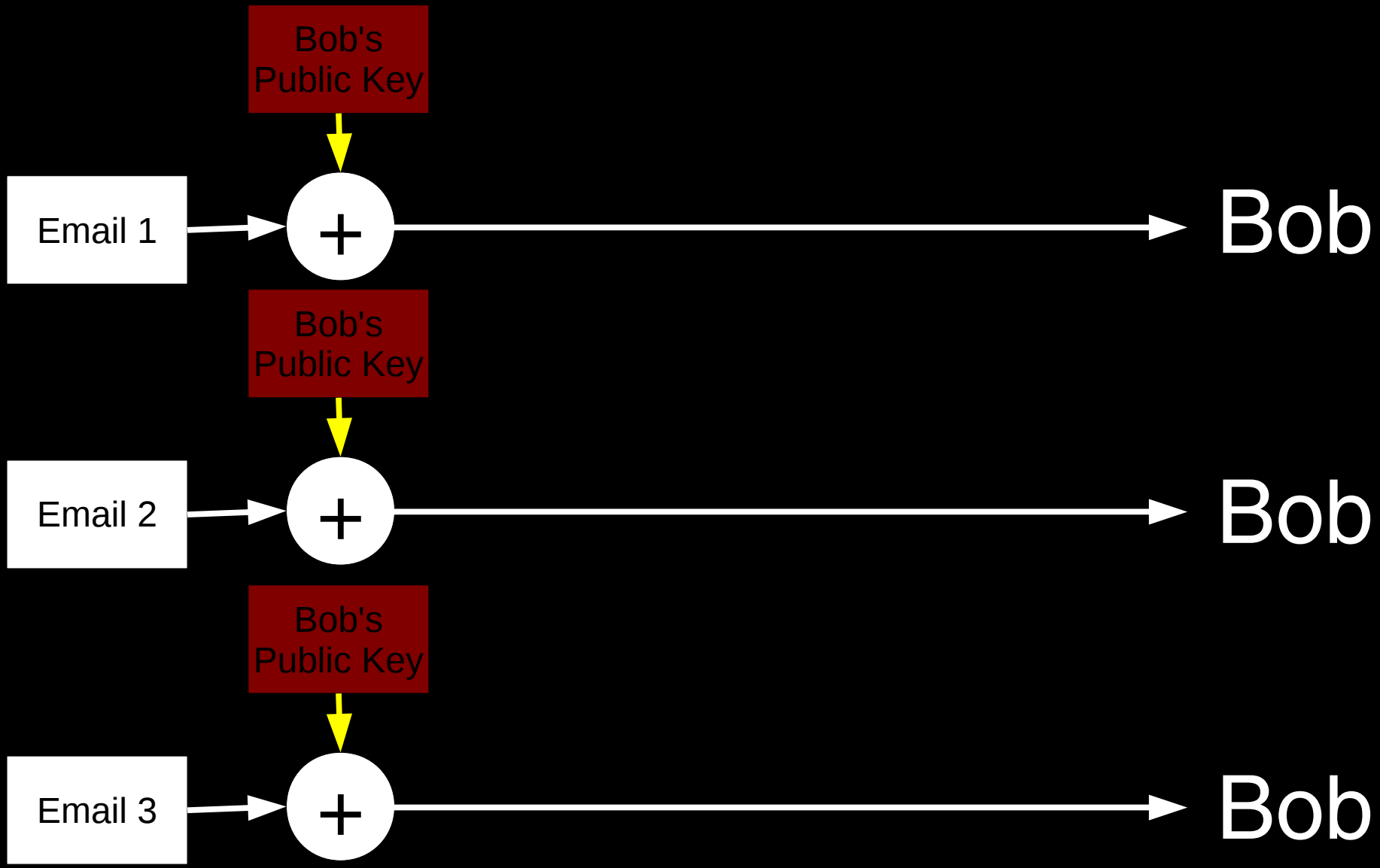
"Off-the-record communication, or, why not to use PGP"

- Nikita Borisov, Ian Goldberg, Eric Brewer

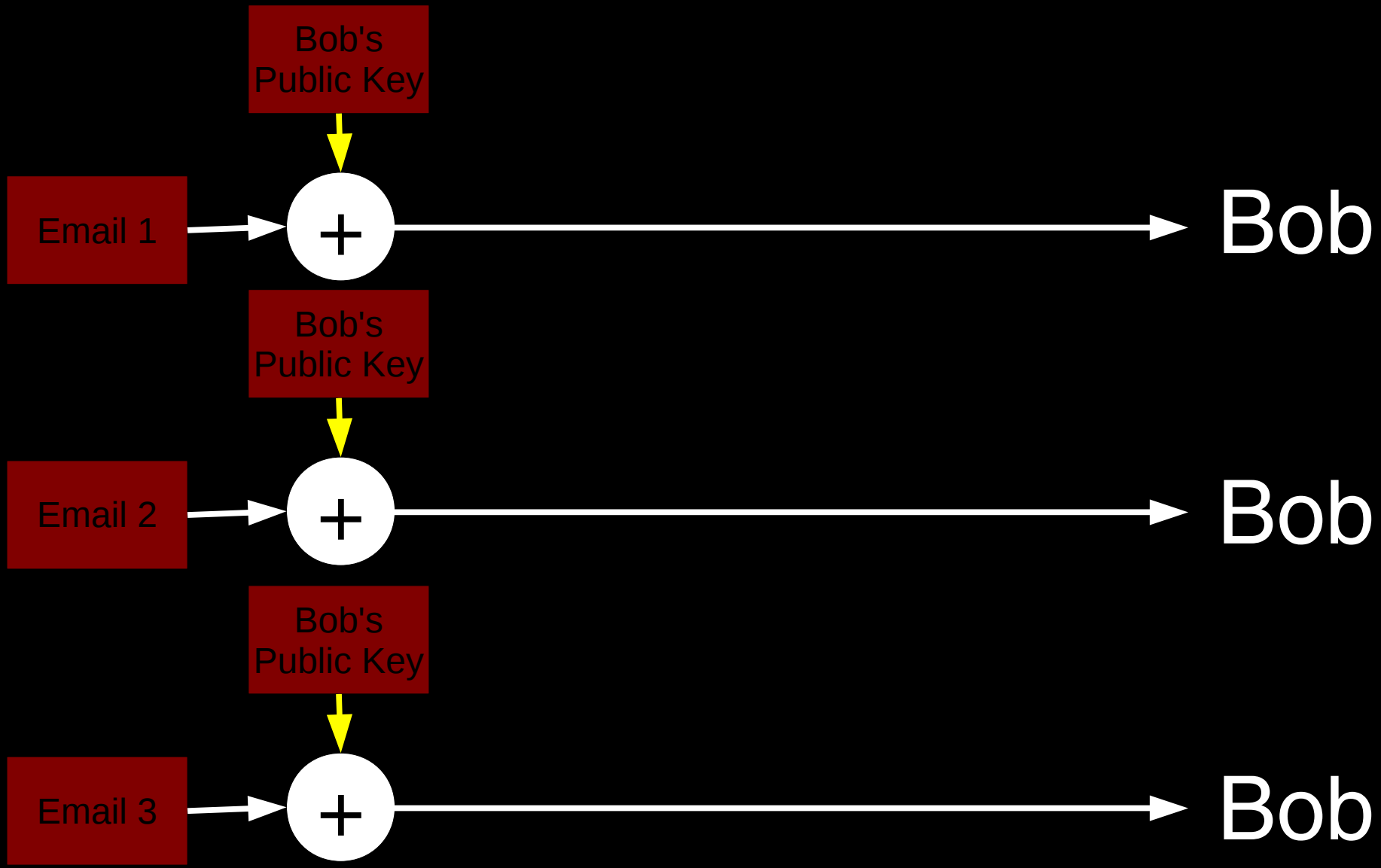
PGP Model


Bob's Public Key
Email 1
+
Bob
Bob's Public Key
Email 2
+
Bob
Bob's Public Key
Email 3
+
Bob

PGP Model


Bob's Public Key
Email 1
+
Bob
Bob's Public Key
Email 2
+
Bob
Bob's Public Key
Email 3
+
Bob

PGP Model


Bob's Public Key
Email 1
+
Bob
Bob's Public Key
Email 2
+
Bob
Bob's Public Key
Email 3
+
Bob

PGP Model

- One key compromise affects all previous correspondence.

PGP Model

- One key compromise affects all previous correspondence.
- The secrecy of what *I* write is function of *your* security practices.

PGP Model

- One key compromise affects all previous correspondence.
- The secrecy of what *I* write is function of *your* security practices.
- There is authenticity, but no deniability.

PGP Model

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hey Bob, today I was thinking that Eve is a real jerk.

-----BEGIN PGP SIGNATURE-----

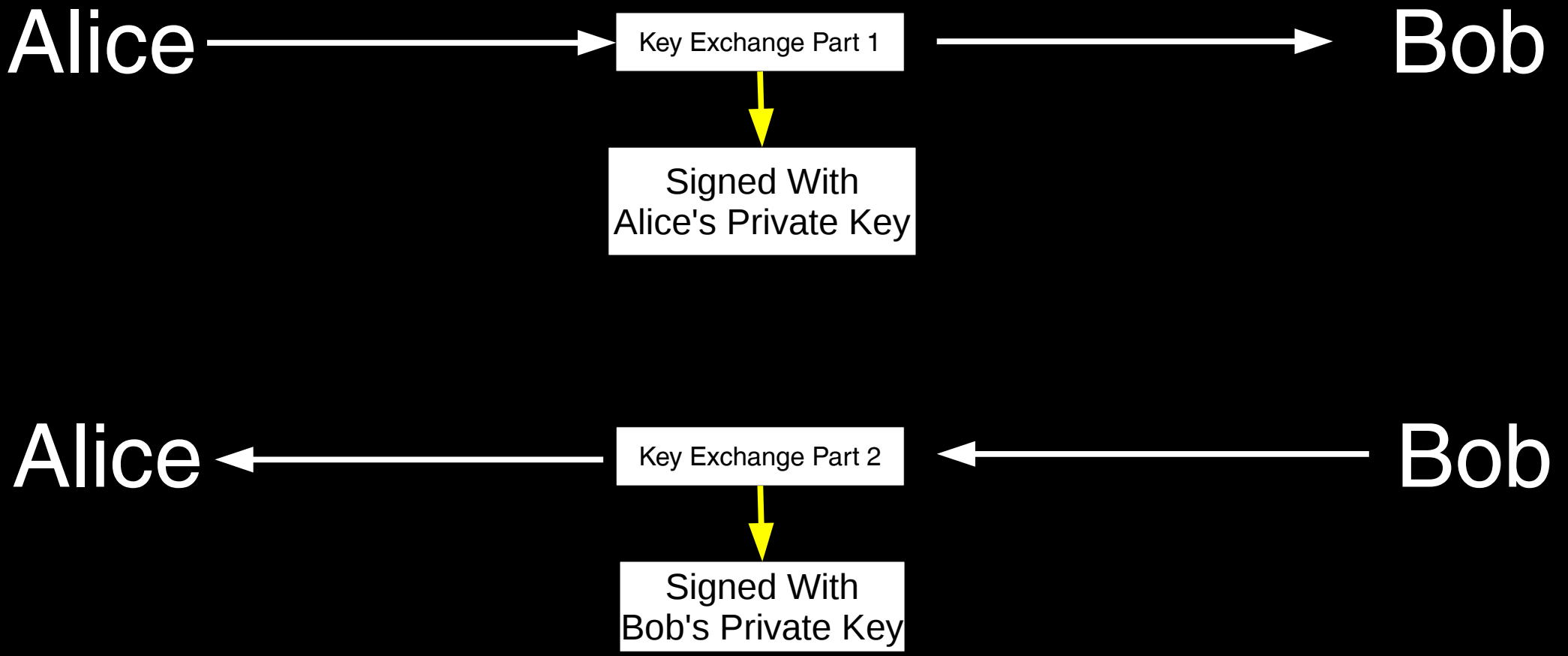
iEYEARECAAYFAkumY0MACgkQ2yS3tG03iIJhAACgiufmacfyU
M/9PYcVS2Mdb9tdmhYAoO4P0pZug2D7BuFEPkLovKpipore=8
rKh

-----END PGP SIGNATURE-----

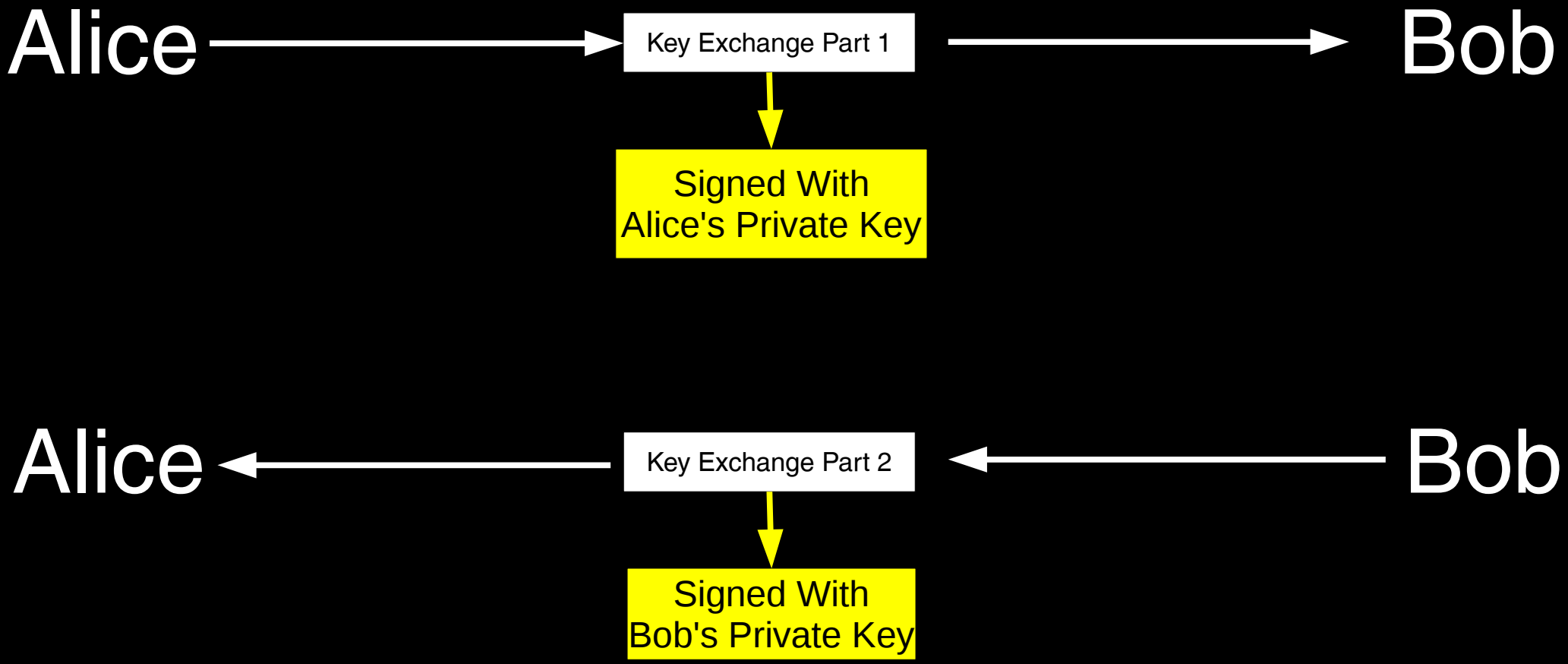
UNDENIABLE

Moxie Marlinspike
Institute For Disruptive Studies

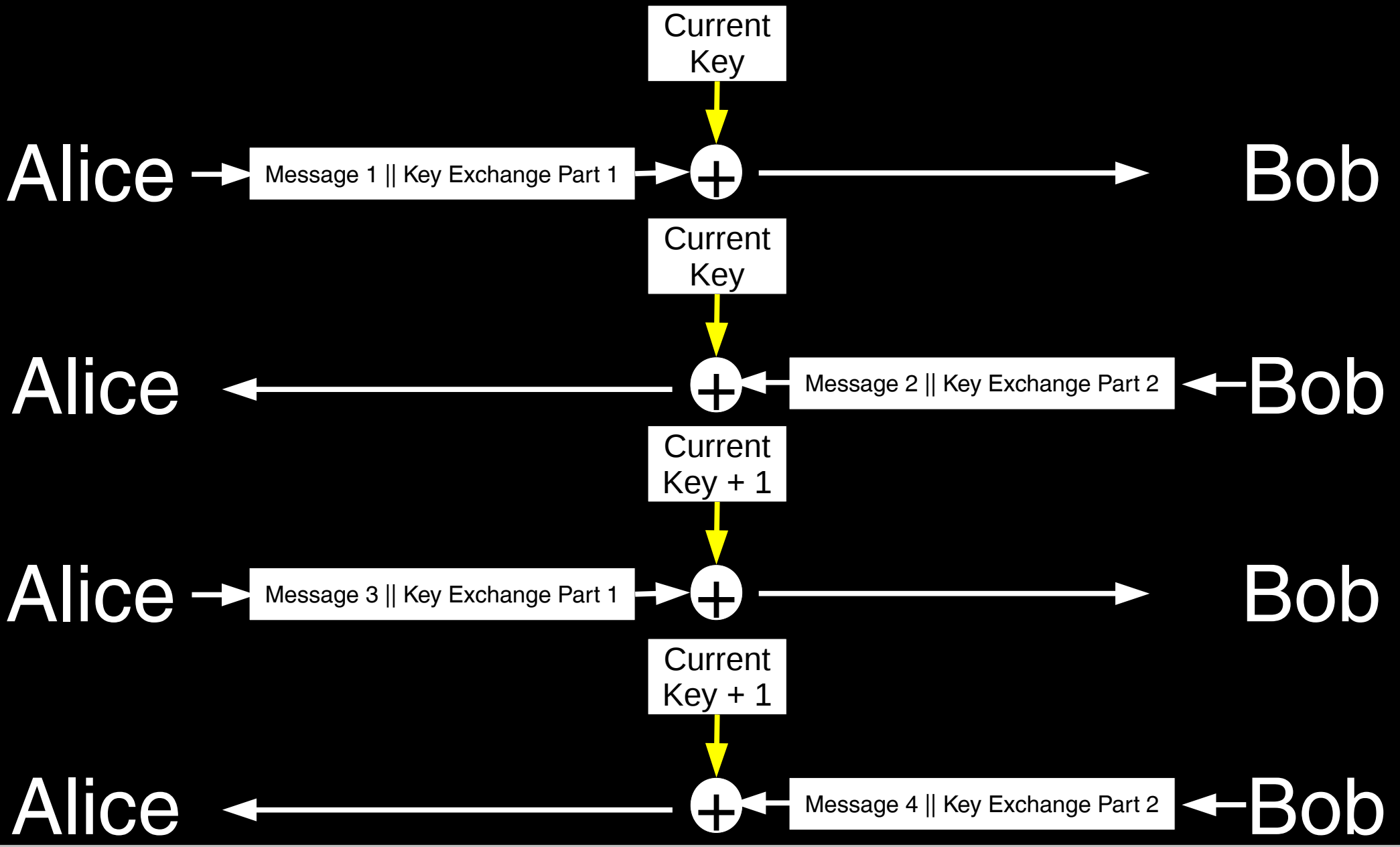
OTR Model


Alice
Key Exchange Part 1
Bob
Signed With
Alice's Private Key
Alice
Key Exchange Part 2
Bob
Signed With
Bob's Private Key

OTR Model

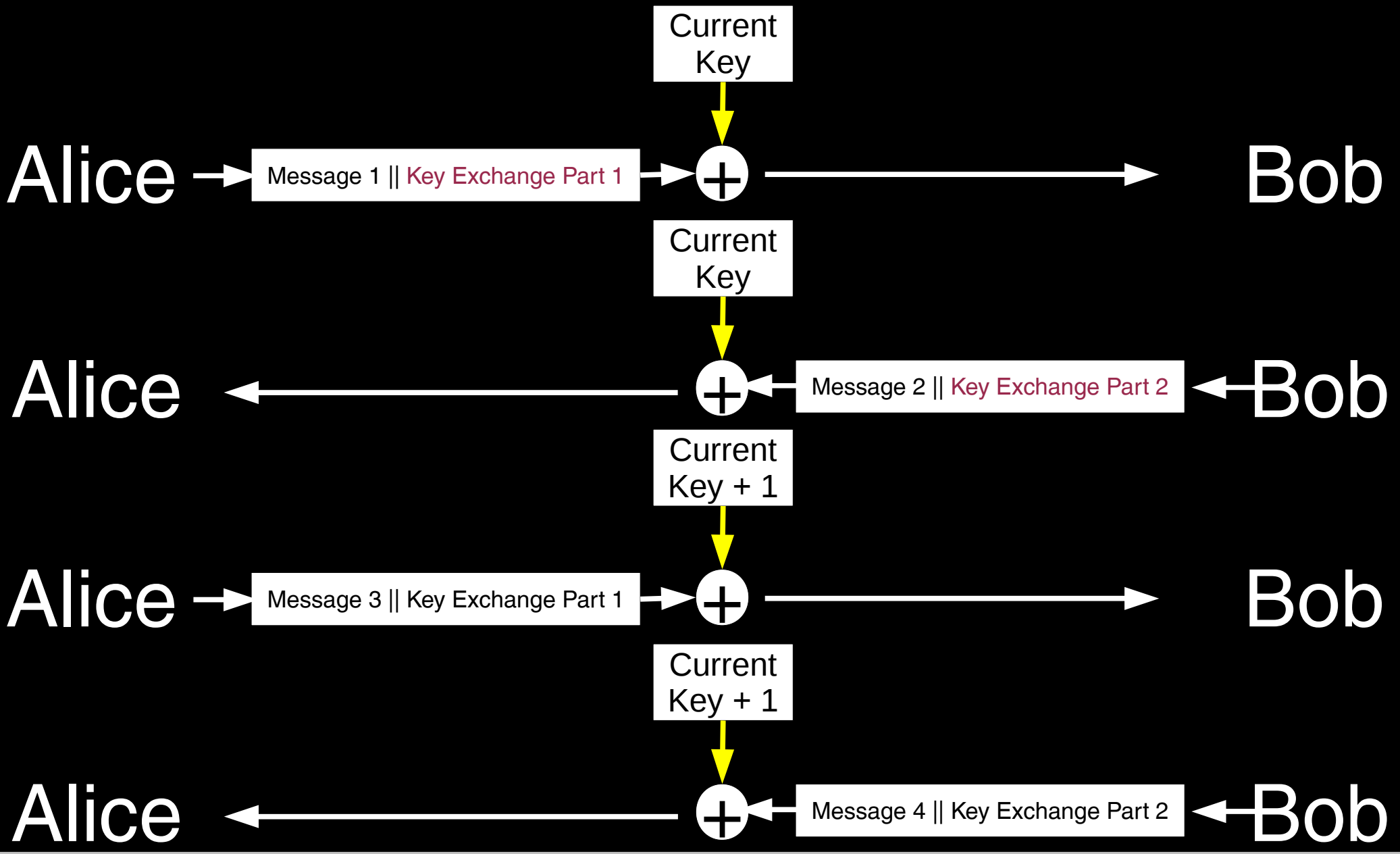

Alice
Key Exchange Part 1
Bob
Signed With
Alice's Private Key
Alice
Key Exchange Part 2
Bob
Signed With
Bob's Private Key

OTR Model

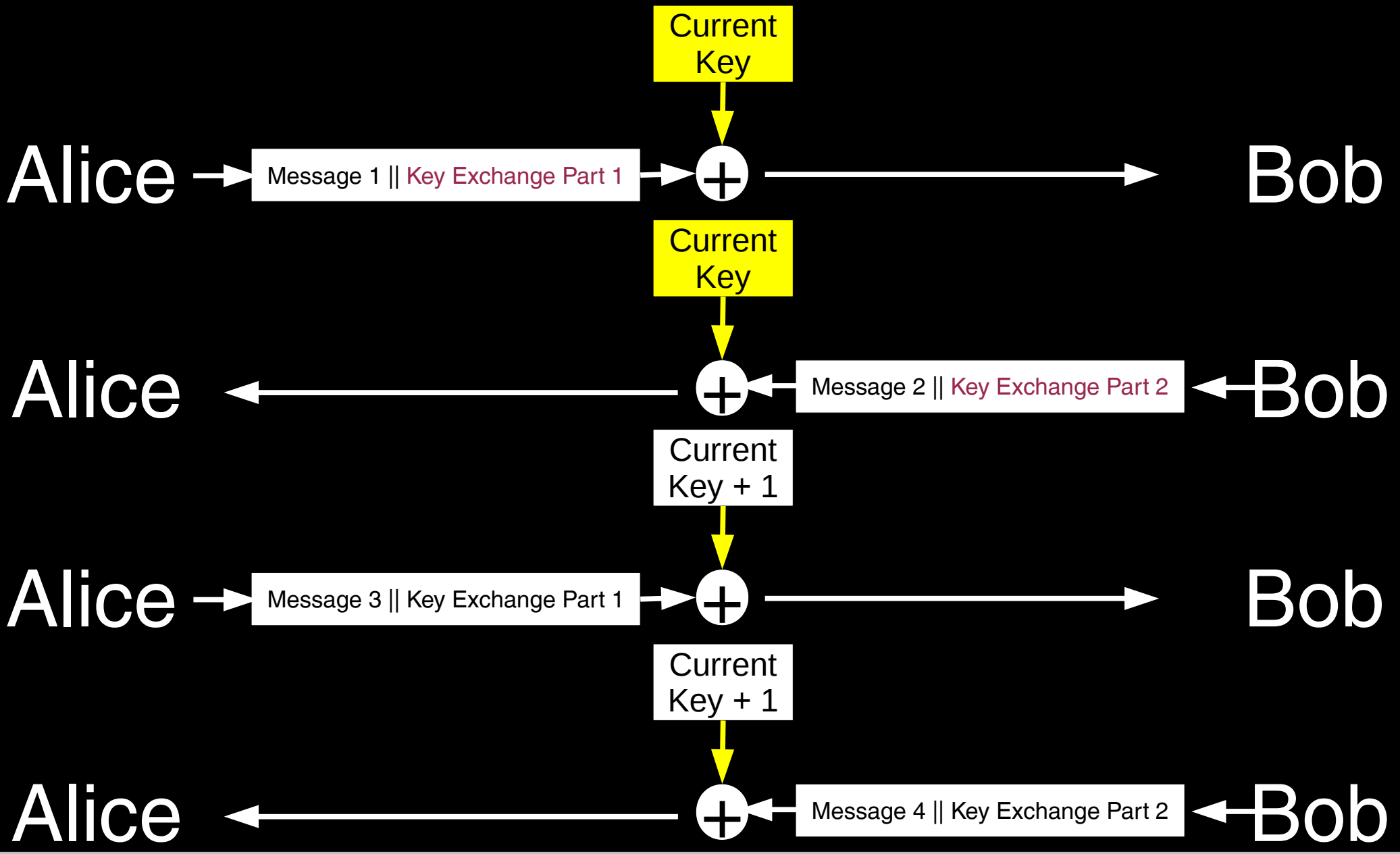


Moxie Marlinspike
Institute For Disruptive Studies

OTR Model

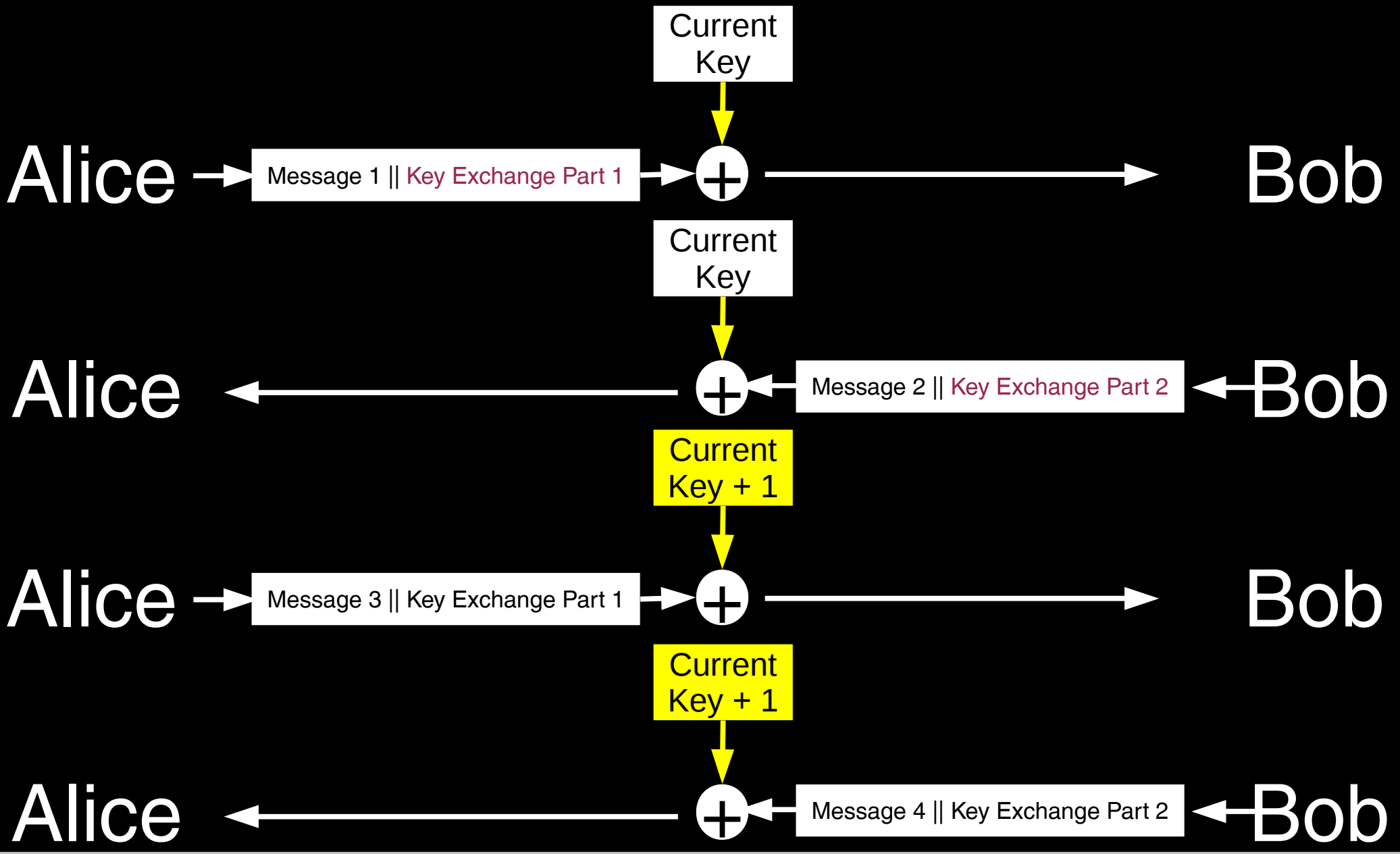

Current Key
Alice
Message 1 || Key Exchange Part 1
Bob
Current Key
Alice
Message 2 || Key Exchange Part 2
Bob
Current Key + 1
Alice
Message 3 || Key Exchange Part 1
Bob
Current Key + 1
Alice
Message 4 || Key Exchange Part 2
Bob

OTR Model

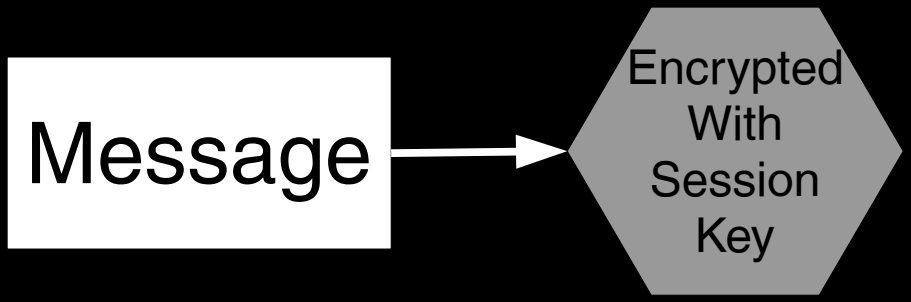


Moxie Marlinspike
Institute For Disruptive Studies

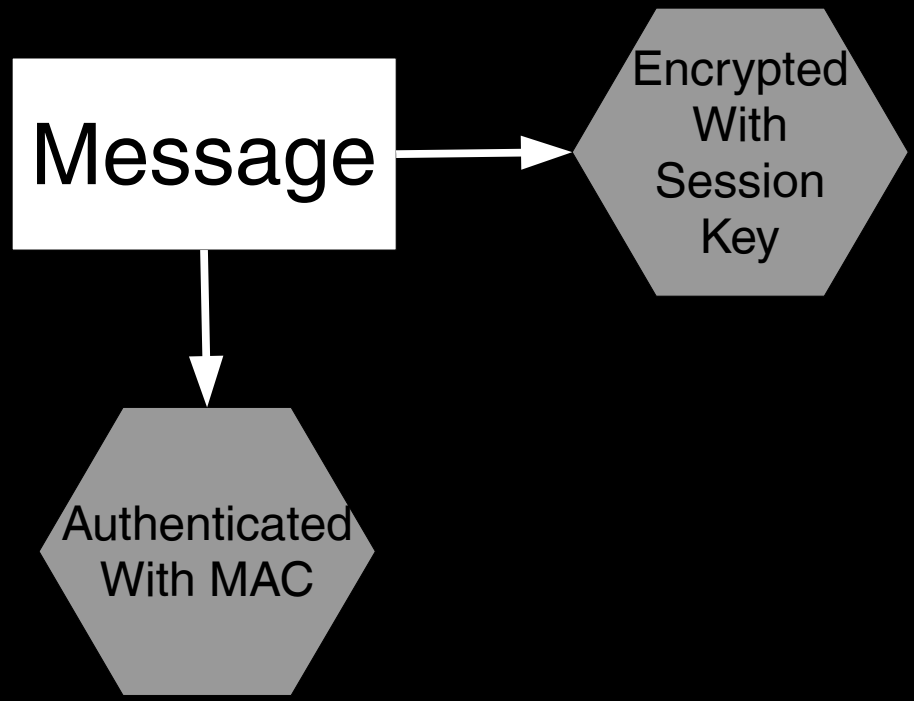
OTR Model


Current Key
Alice
Message 1 || Key Exchange Part 1
Bob
Current Key
Alice
Message 2 || Key Exchange Part 2
Bob
Current Key + 1
Alice
Message 3 || Key Exchange Part 1
Bob
Current Key + 1
Alice
Message 4 || Key Exchange Part 2
Bob

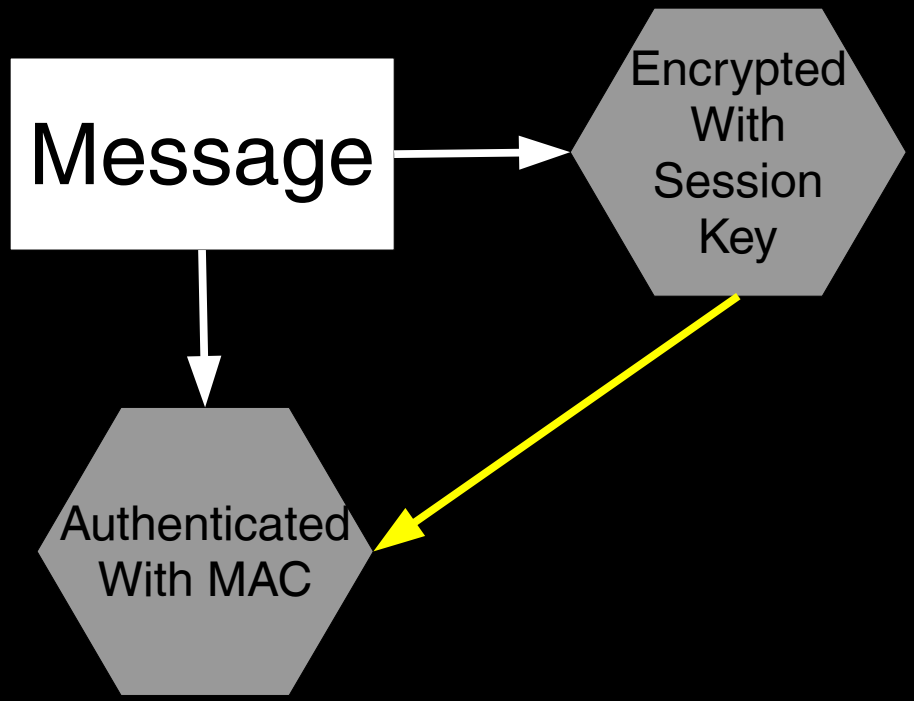
OTR Model



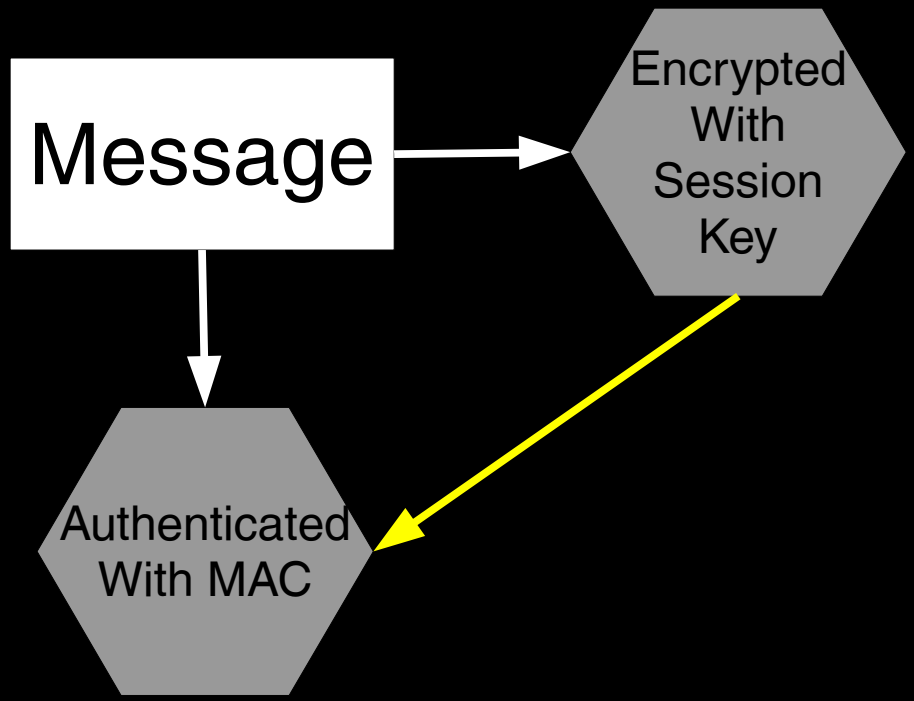
OTR Model


Message
Encrypted With Session Key
Authenticated With MAC

OTR Model

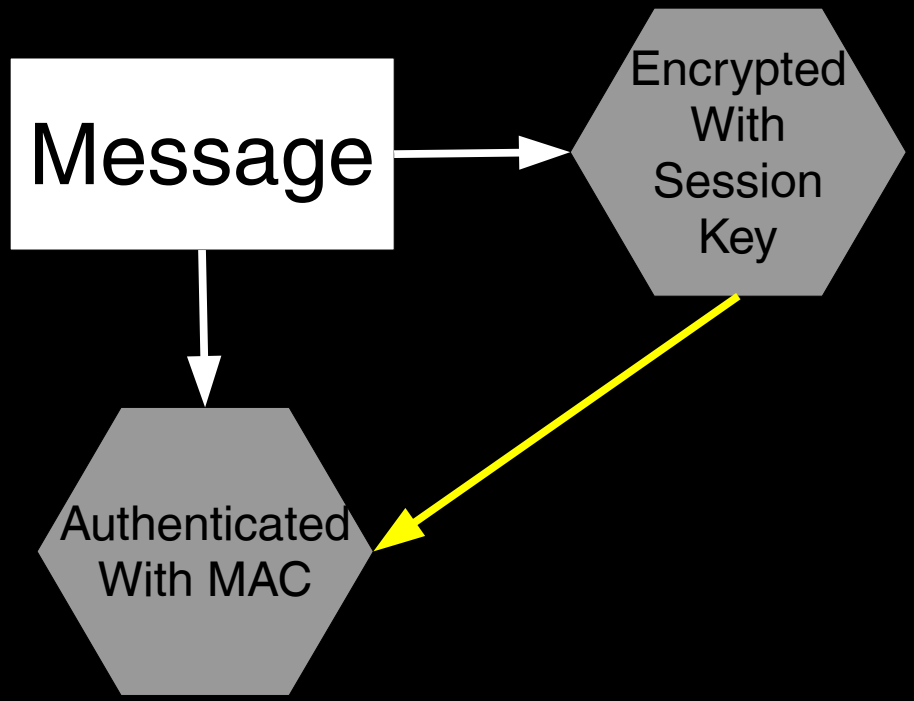

Message
Encrypted With Session Key
Authenticated With MAC

OTR Model



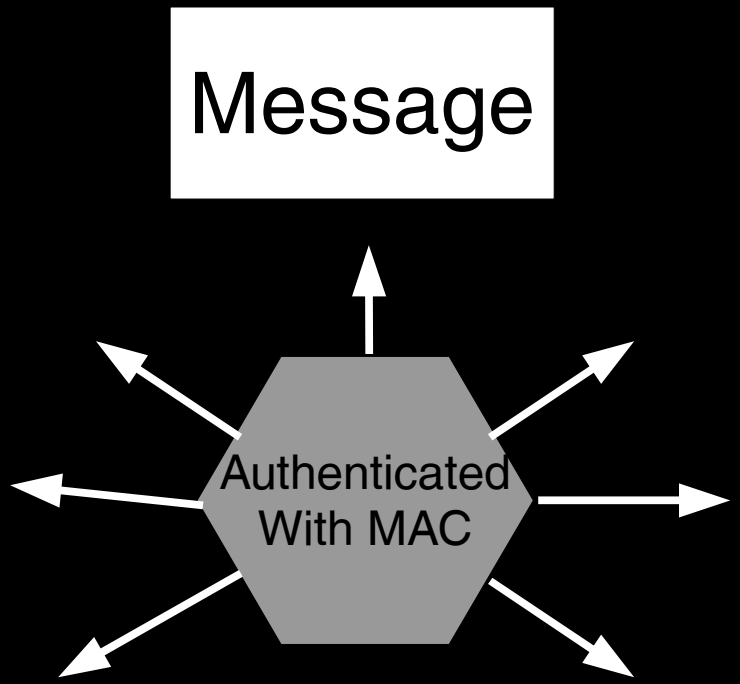
Signatures are undeniable because they have only one possible author.

OTR Model



MACs have *two* possible authors.

OTR Model



After a broadcast, *anyone* can forge an old message.

OTR Model

- A key compromise does not affect previous messages.
- You get authenticity, but also deniability.

Future

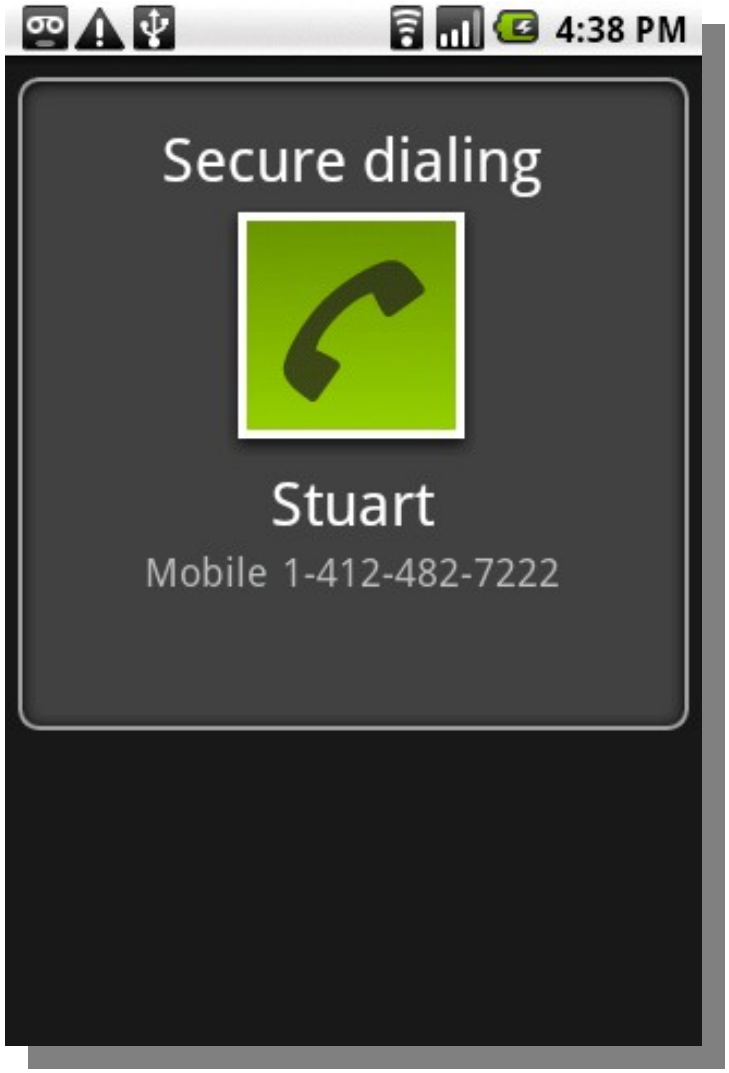
Whisper Systems

Moxie Marlinspike
Institute For Disruptive Studies

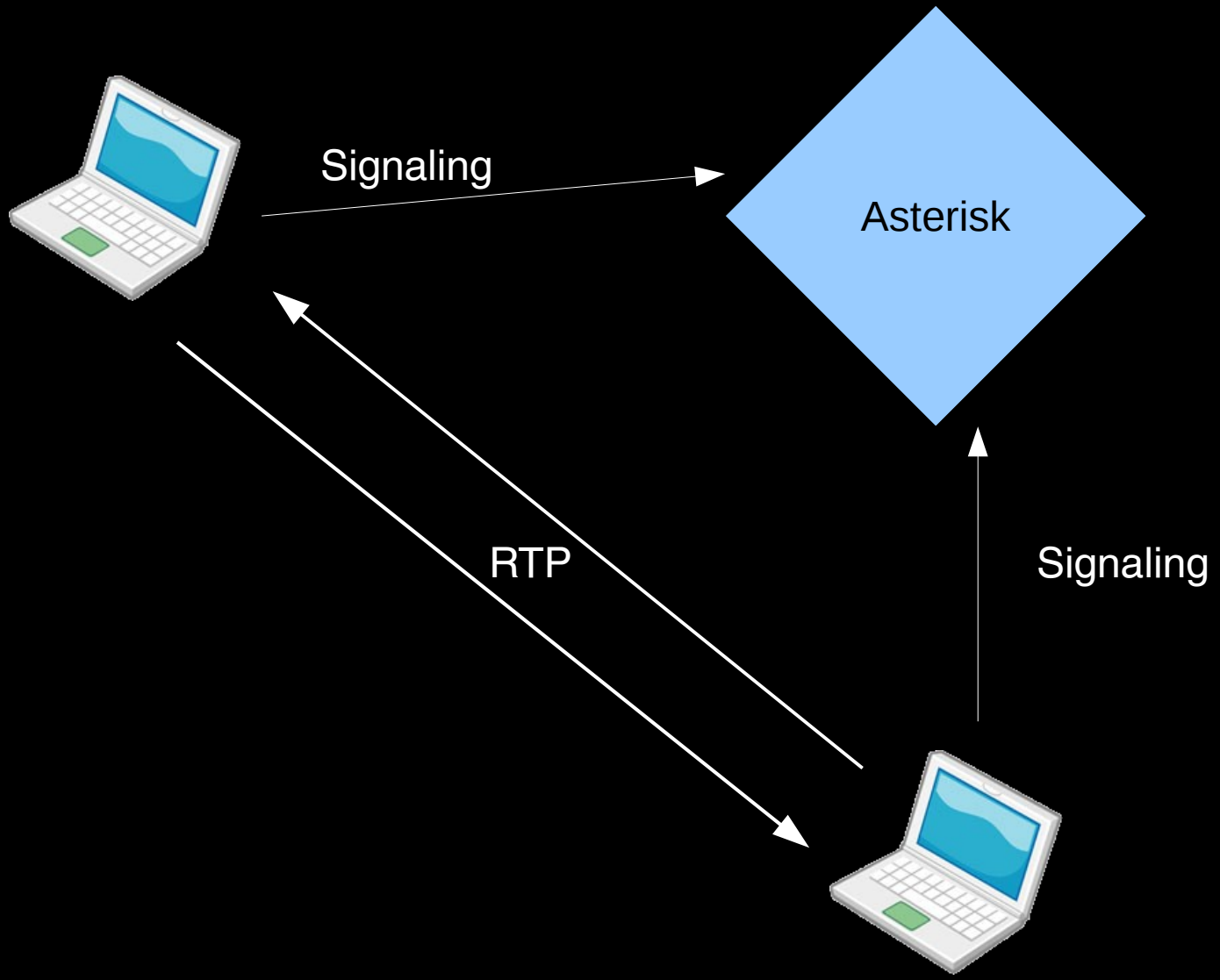
Bring forward secure protocols into mobile phones

Moxie Marlinspike
Institute For Disruptive Studies

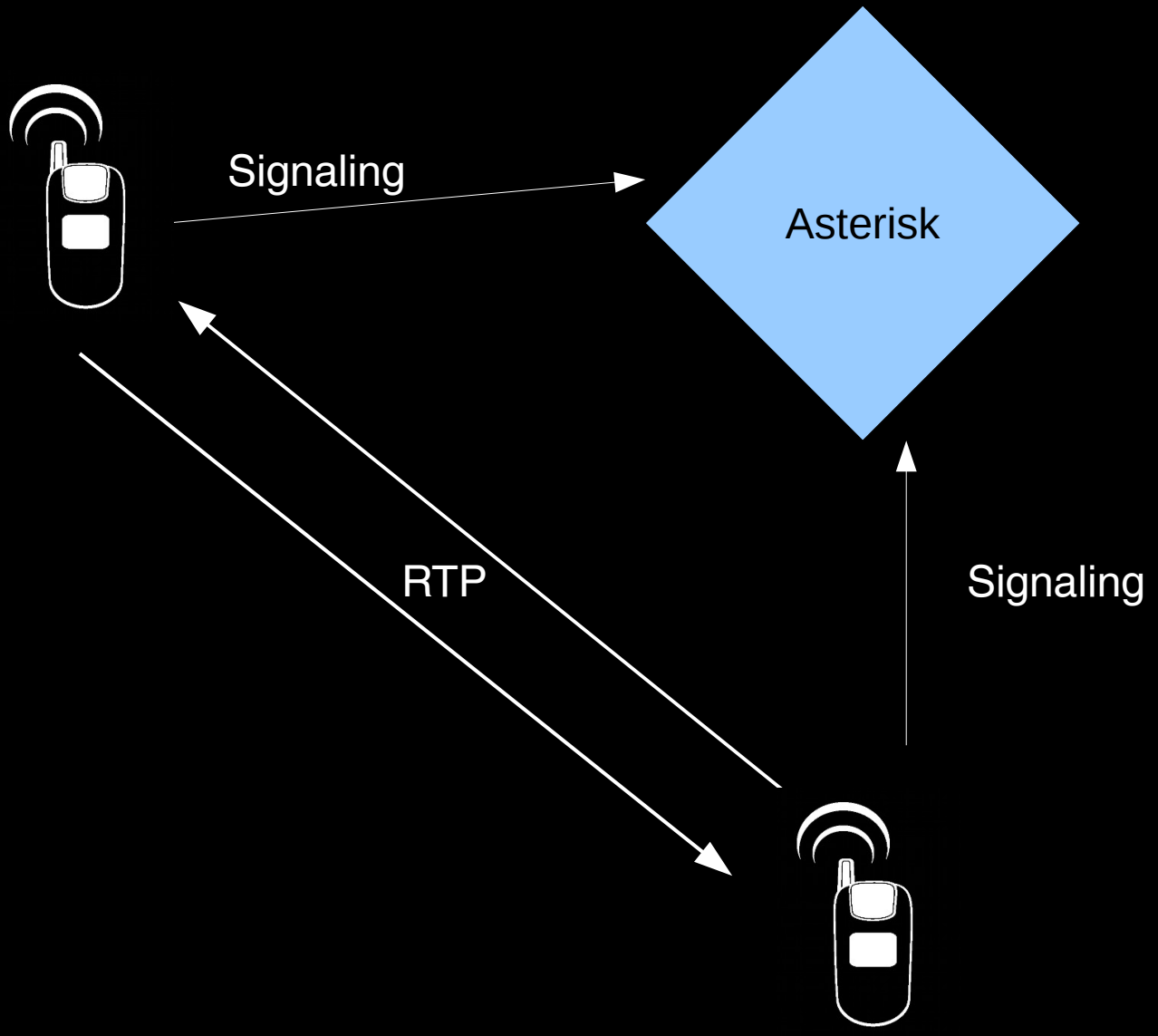
Whisper Systems



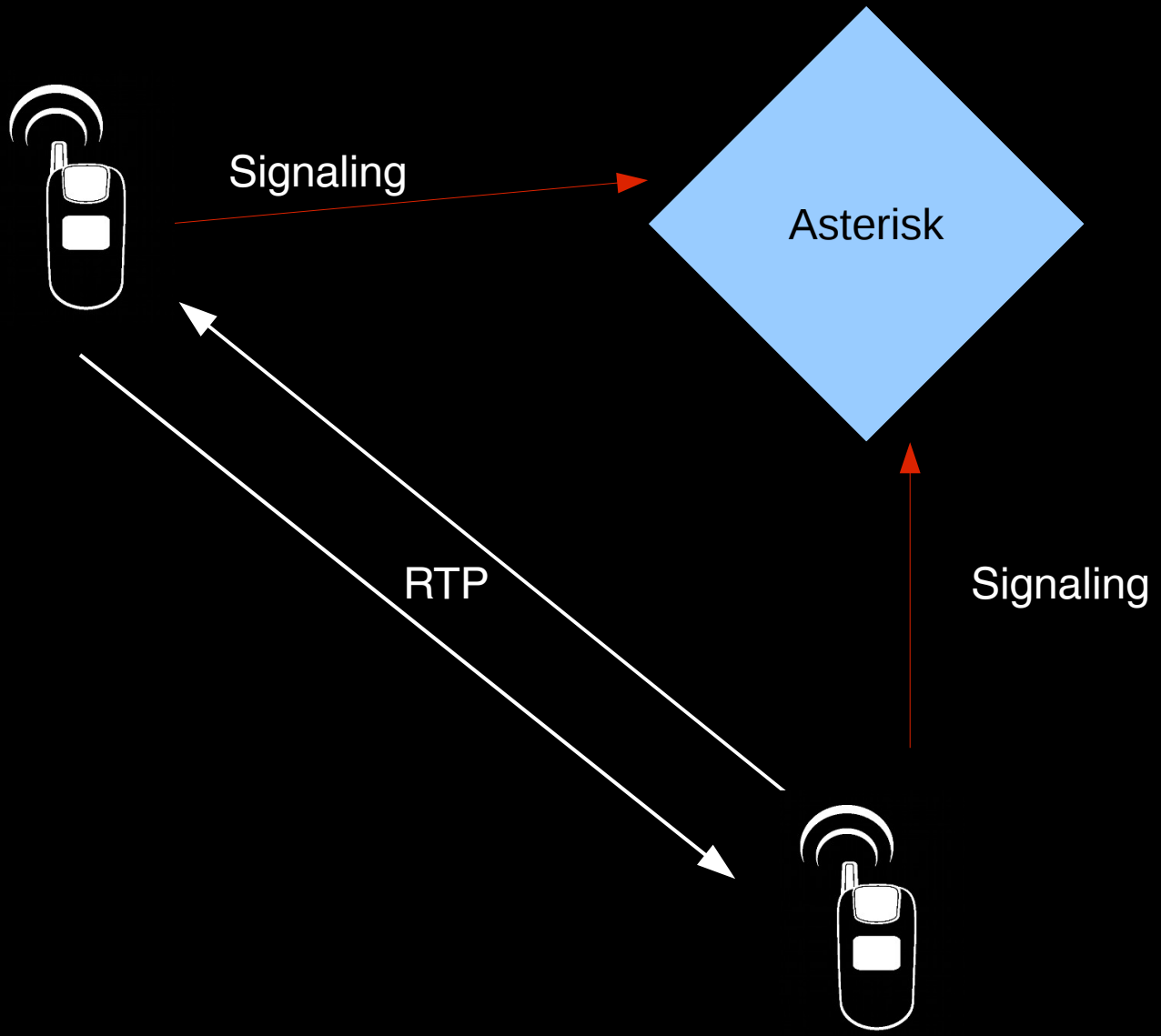
Whisper Systems
But doesn't voip Suck?



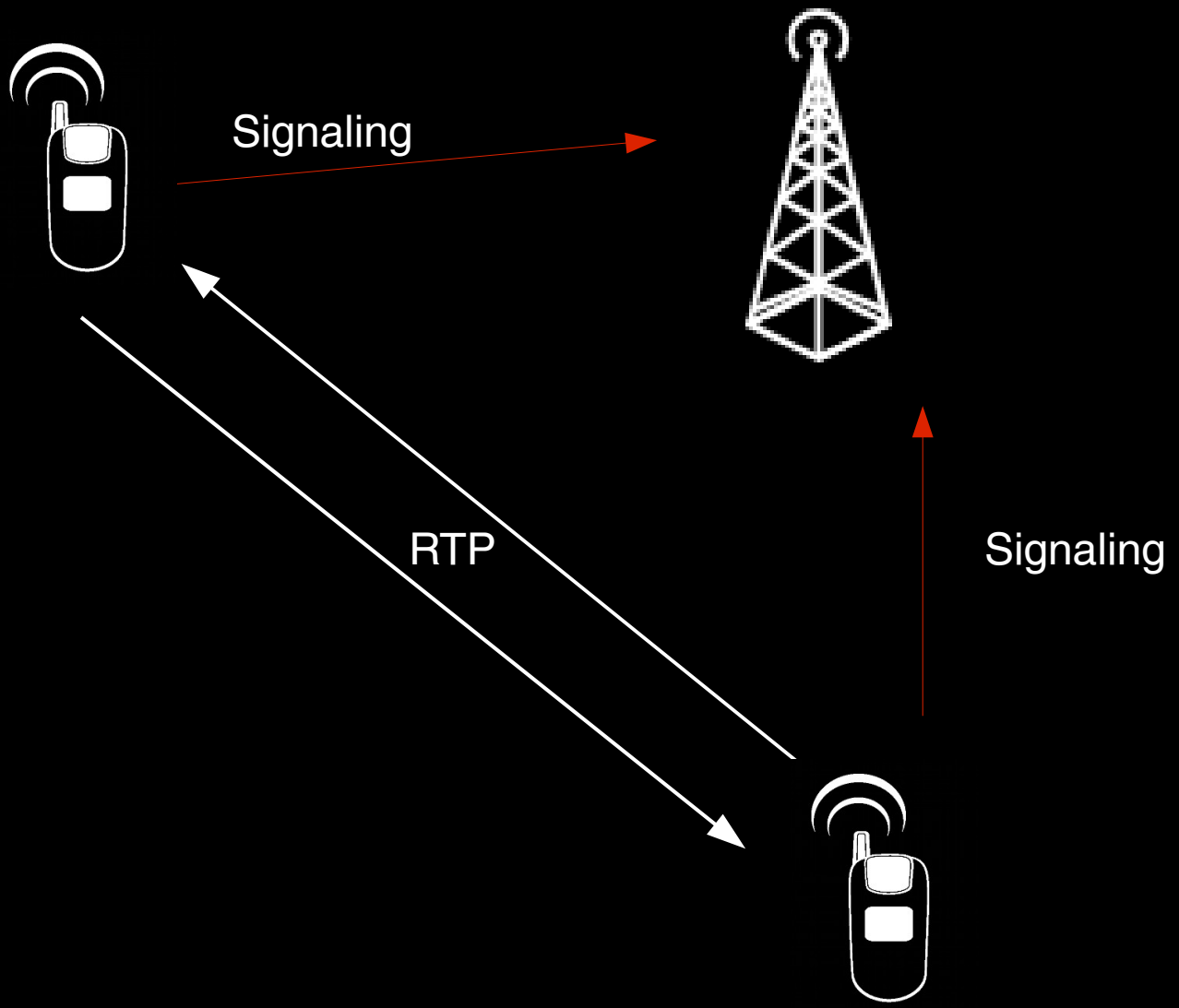
Whisper Systems
But doesn't *mobile* voip Suck?



Whisper Systems
But doesn't *mobile* voip Suck?

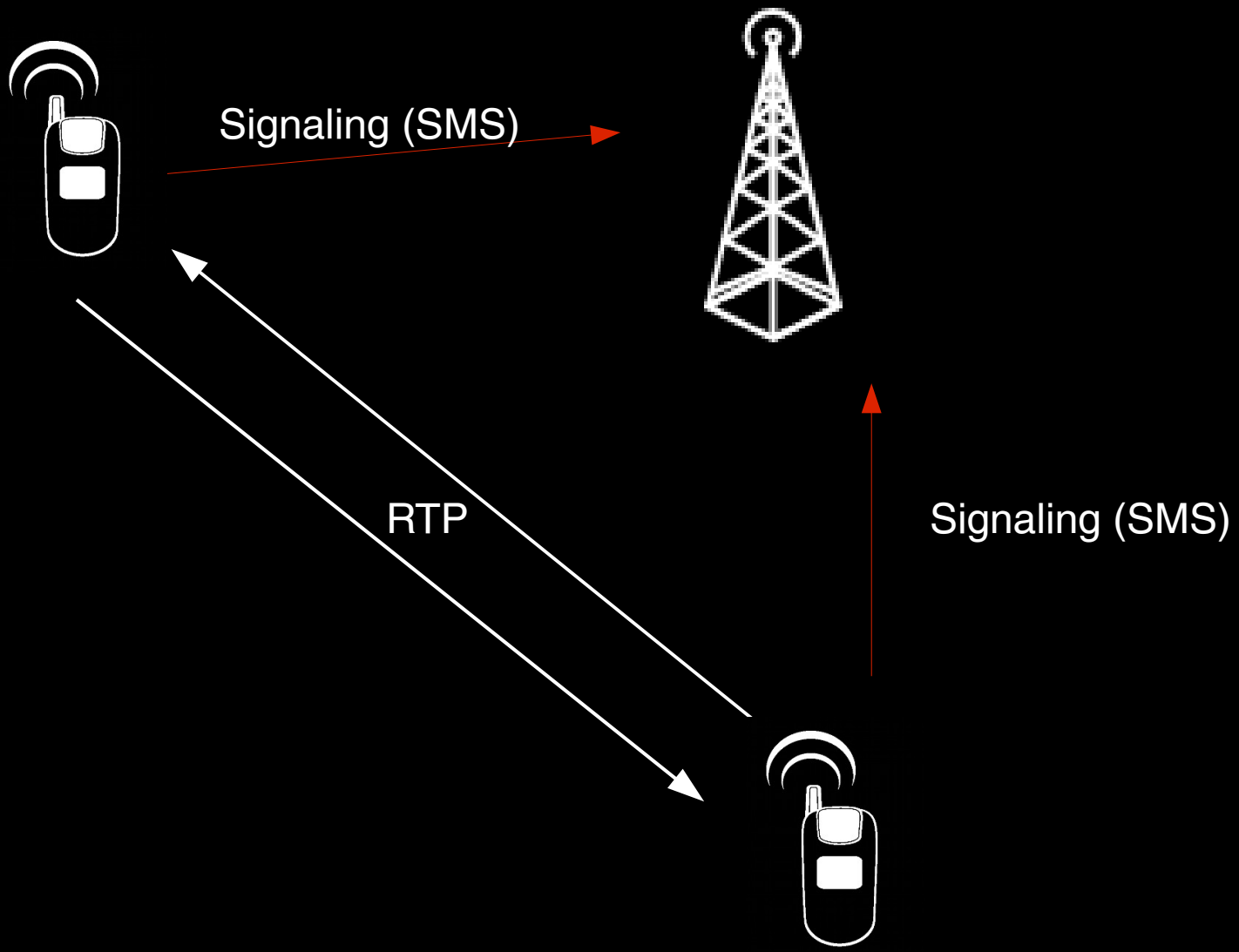


Whisper Systems
But doesn't *mobile* voip Suck?



Moxie Marlinspike
Institute For Disruptive Studies

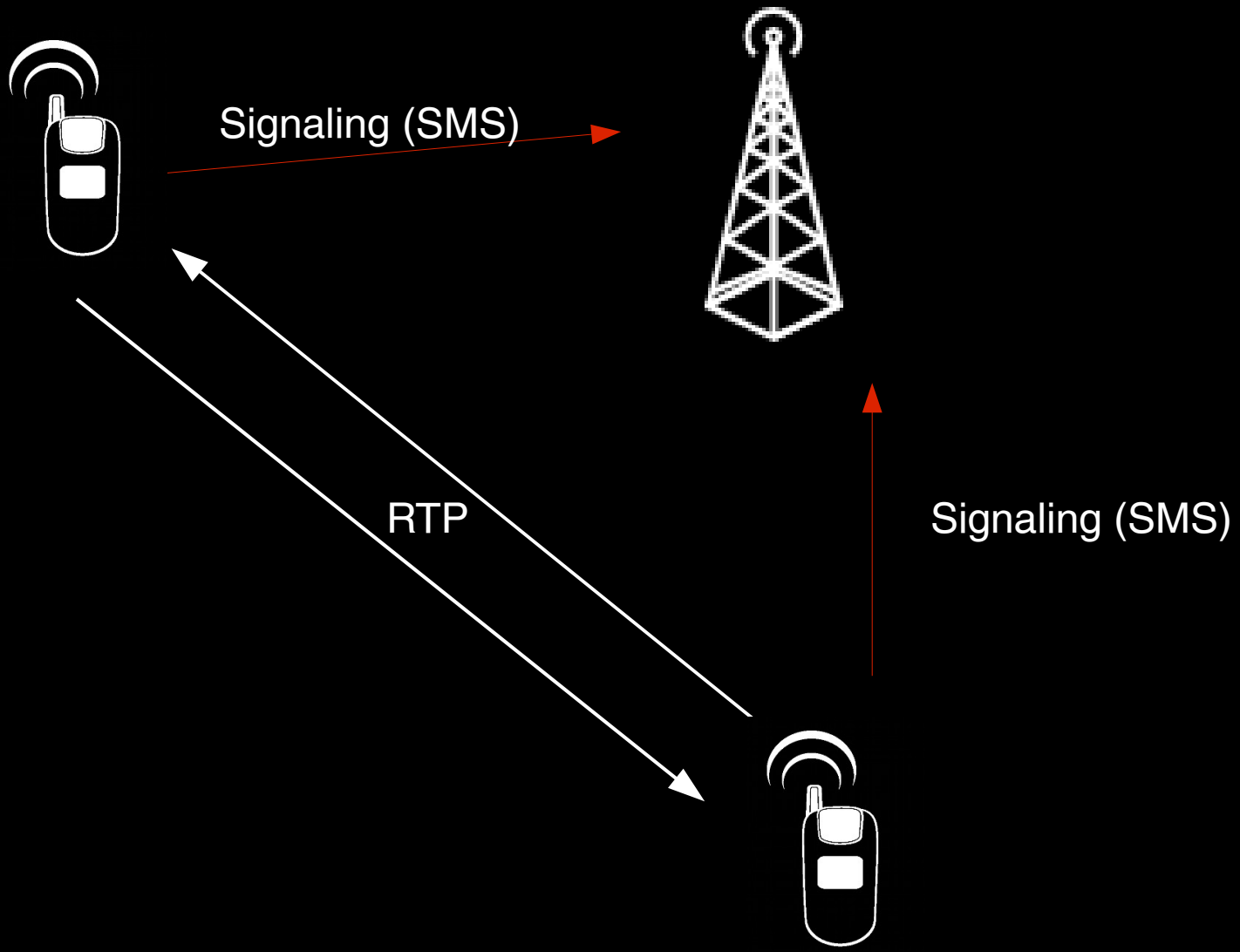
Whisper Systems
But doesn't *mobile* voip Suck?



Whisper Systems

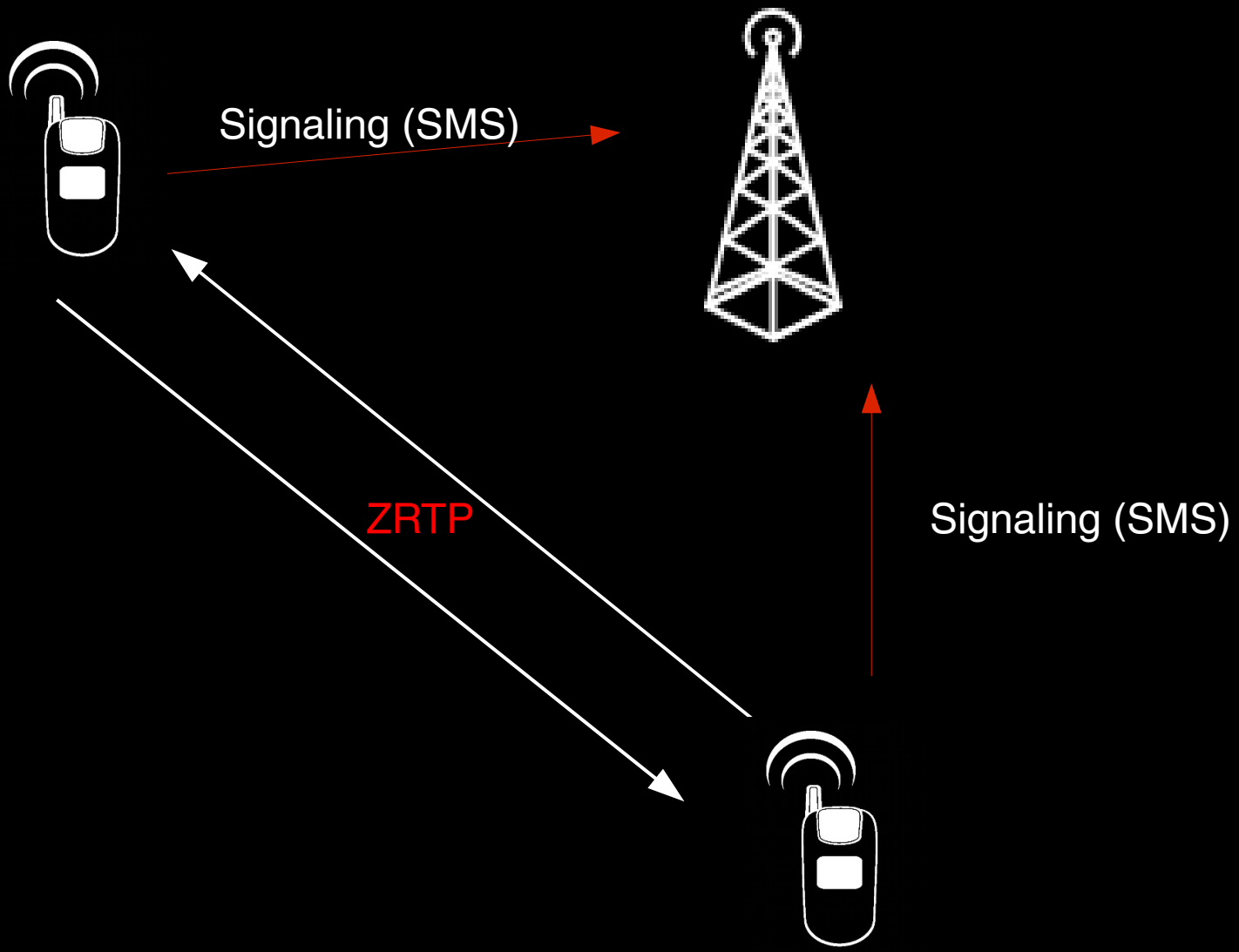
- Your phone doesn't need to maintain a constant network connection to a SIP server.
  - (Your phone can go to sleep!)
- You don't need the equivalent of a Skype ID.
  - (Addressing is based on existing phone numbers!)
- You don't need to run a VOIP server.
  - (Just install the app and you're ready!)

Whisper Systems
But doesn't *mobile* voip Suck?



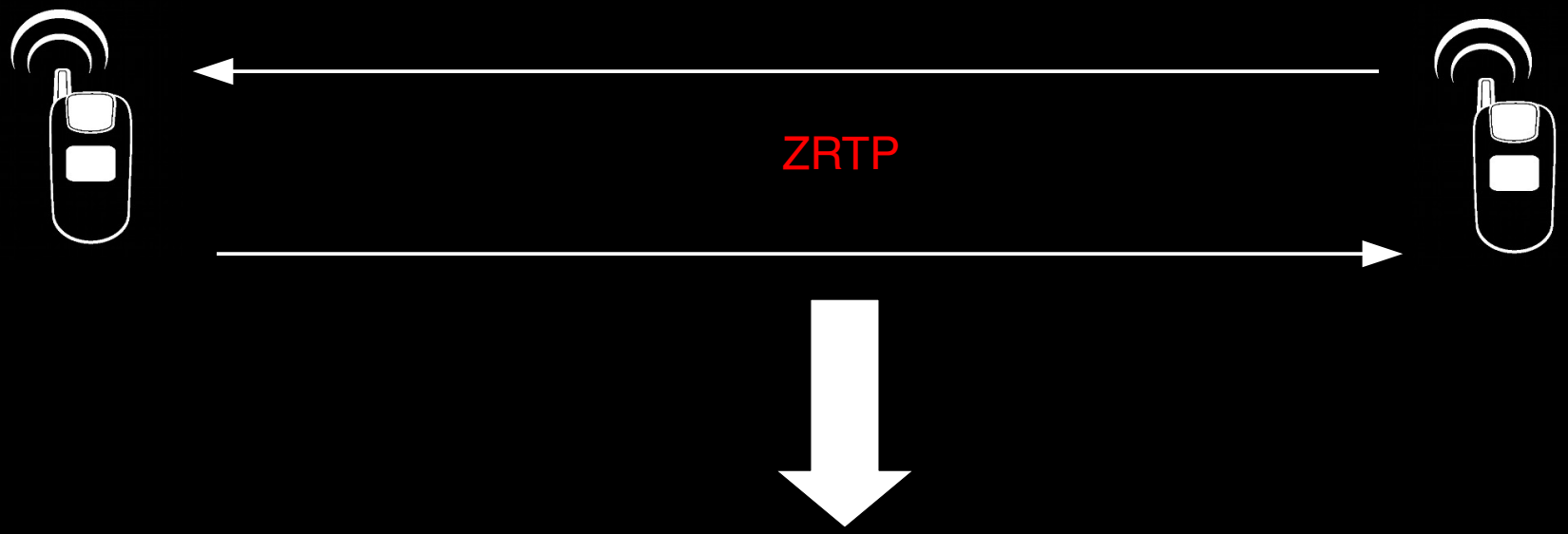
Moxie Marlinspike
Institute For Disruptive Studies

Whisper Systems
But doesn't *mobile* voip Suck?



ZRTP

ZRTP



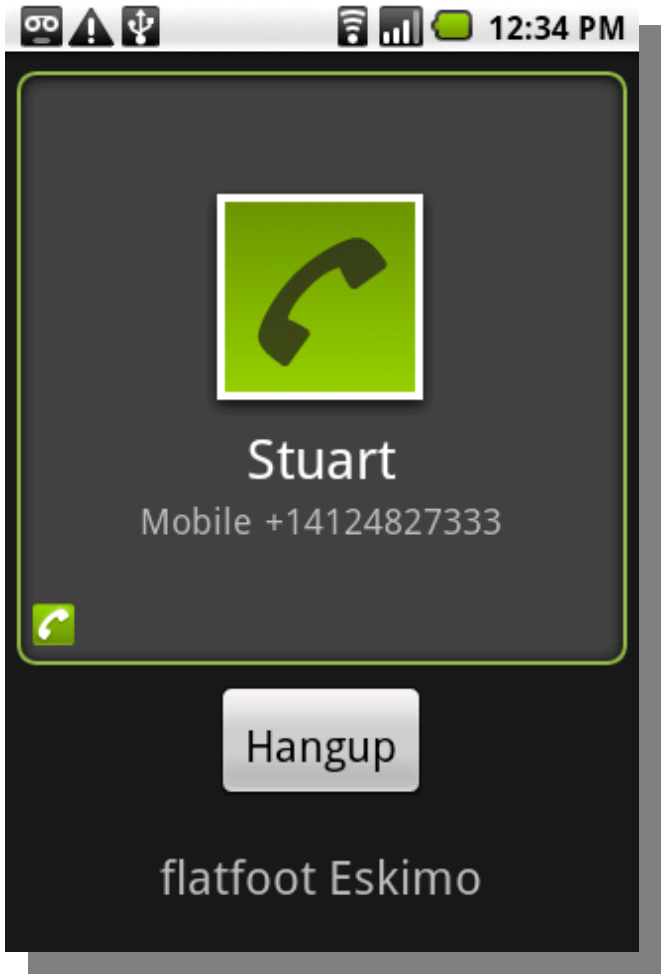
Negotiate ephemeral session key.

ZRTP

Negotiate ephemeral session key.

Derive “Short Authentication String”.

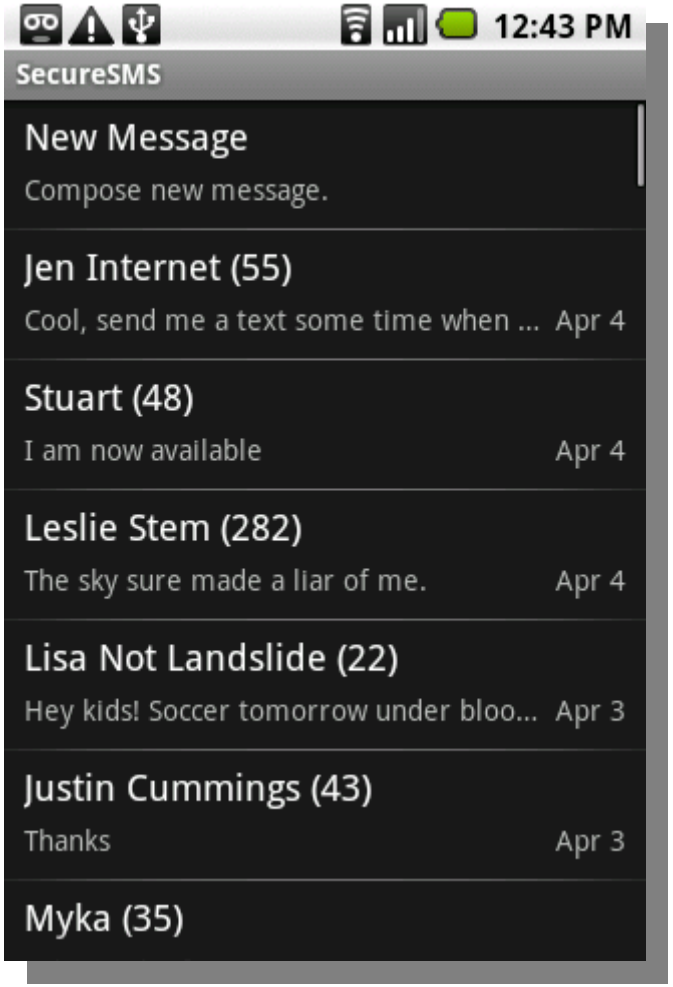
ZRTP



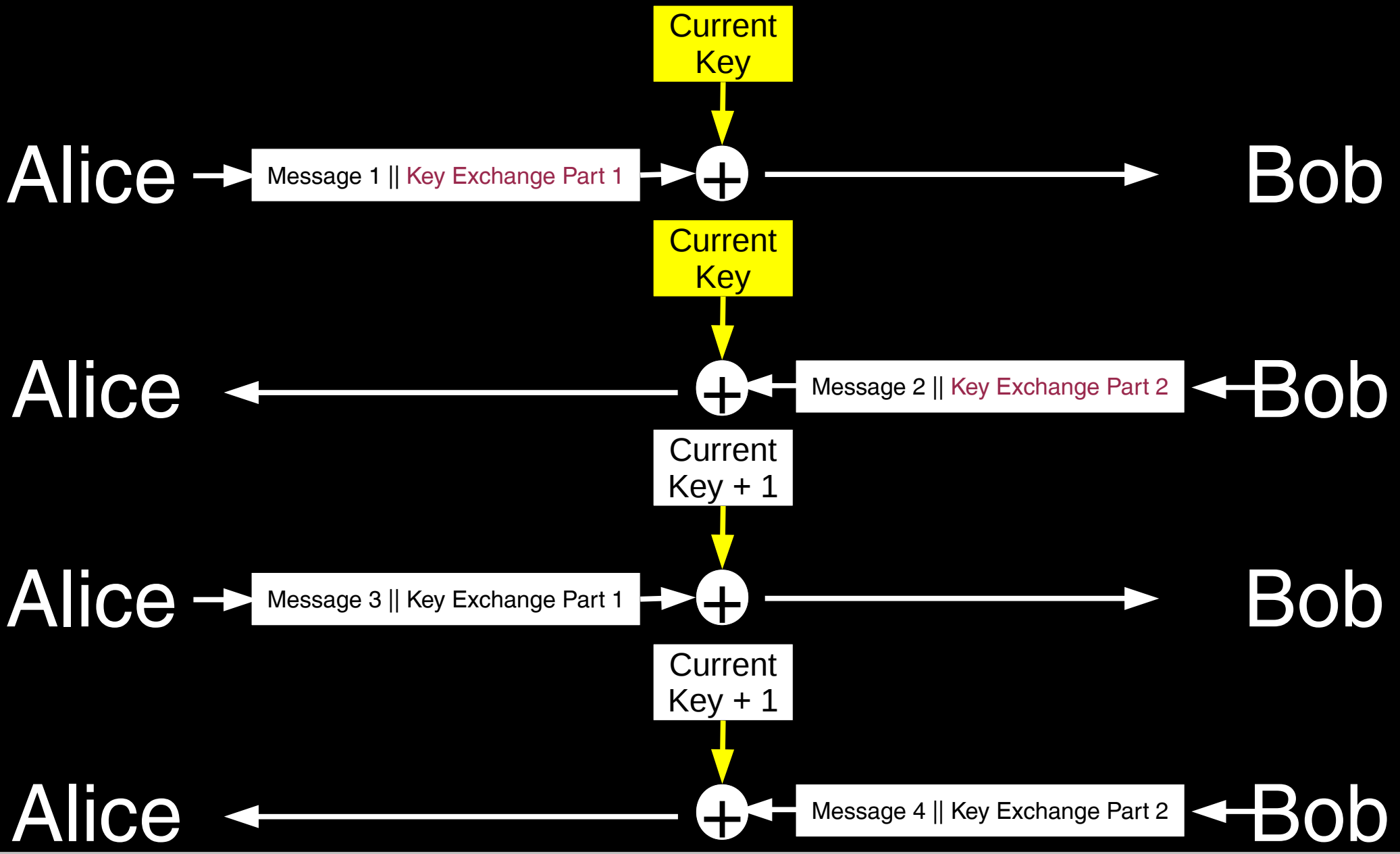
Whisper Systems
OTR-Derived SMS

Moxie Marlinspike
Institute For Disruptive Studies

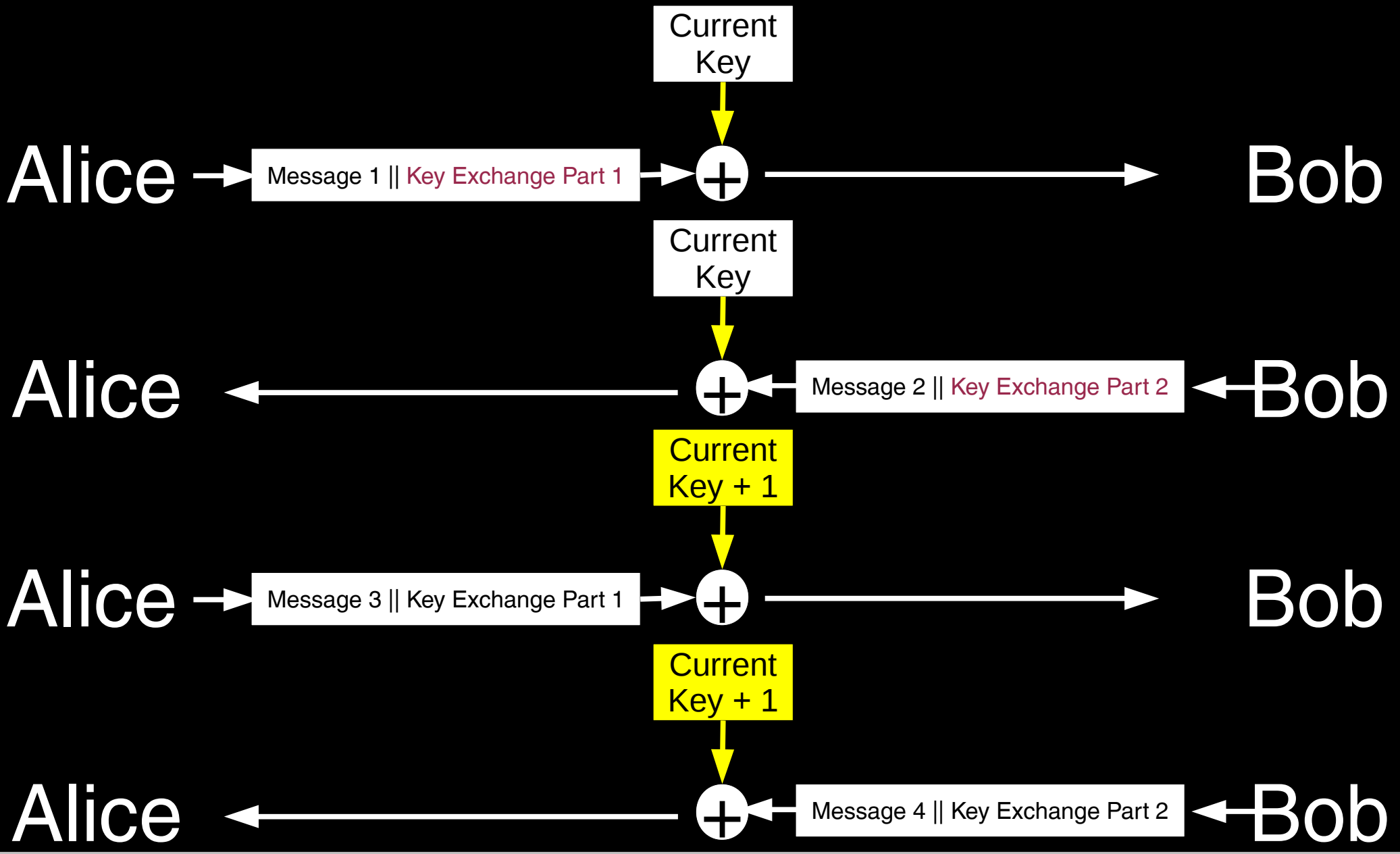
Whisper Systems



OTR Model


Current Key
Alice
Message 1 || Key Exchange Part 1
Bob
Current Key
Alice
Message 2 || Key Exchange Part 2
Bob
Current Key + 1
Alice
Message 3 || Key Exchange Part 1
Bob
Current Key + 1
Alice
Message 4 || Key Exchange Part 2
Bob

OTR Model


Current Key
Alice
Message 1 || Key Exchange Part 1
Bob
Current Key
Alice
Message 2 || Key Exchange Part 2
Bob
Current Key + 1
Alice
Message 3 || Key Exchange Part 1
Bob
Current Key + 1
Alice
Message 4 || Key Exchange Part 2
Bob

Small hope to reduce choice scope

www.thoughtcrime.org
moxie@thoughtcrime.org