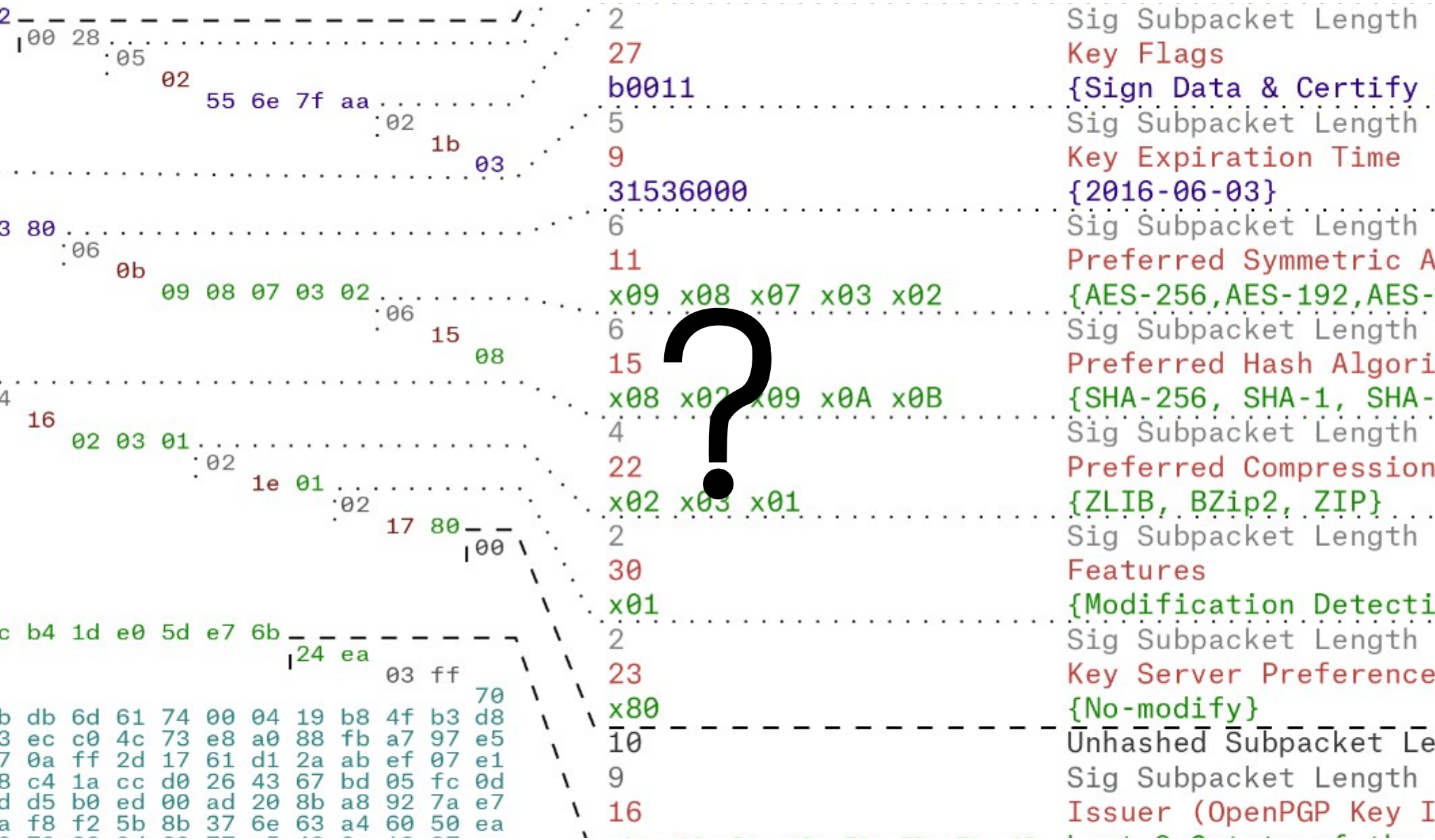
CryptoParty must die.

@shiromarieke

You are needed.


2
00 28
05
02
55 6e 7f aa
02
1b
03
3 80
06
0b
09 08 07 03 02
06
15
08
4
16
02 03 01
02
1e 01
02
17 80
00
c b4 1d e0 5d e7 6b
24 ea
03 ff
70
b db 6d 61 74 00 04 19 b8 4f b3 d8
3 ec c0 4c 73 e8 a0 88 fb a7 97 e5
7 0a ff 2d 17 61 d1 2a ab ef 07 e1
8 c4 1a cc d0 26 43 67 bd 05 fc 0d
d d5 b0 ed 00 ad 20 8b a8 92 7a e7
a f8 f2 5b 8b 37 6e 63 a4 60 50 ea
2 Sig Subpacket Length
27 Key Flags
b0011 {Sign Data & Certify
5 Sig Subpacket Length
9 Key Expiration Time
31536000 {2016-06-03}
6 Sig Subpacket Length
11 Preferred Symmetric A
x09 x08 x07 x03 x02 {AES-256,AES-192,AES-
6 Sig Subpacket Length
15 Preferred Hash Algori
x08 x02 x09 x0A x0B {SHA-256, SHA-1, SHA-
4 Sig Subpacket Length
22 Preferred Compression
x02 x03 x01 {ZLIB, BZip2, ZIP}
2 Sig Subpacket Length
30 Features
x01 {Modification Detecti
2 Sig Subpacket Length
23 Key Server Preference
x80 {No-modify}
10 Unhashed Subpacket Le
9 Sig Subpacket Length
16 Issuer (OpenPGP Key I
?

Communicate with people.

Communicate with people.
Share your tools.

Leave the hackerspace.


WX210

We need you.

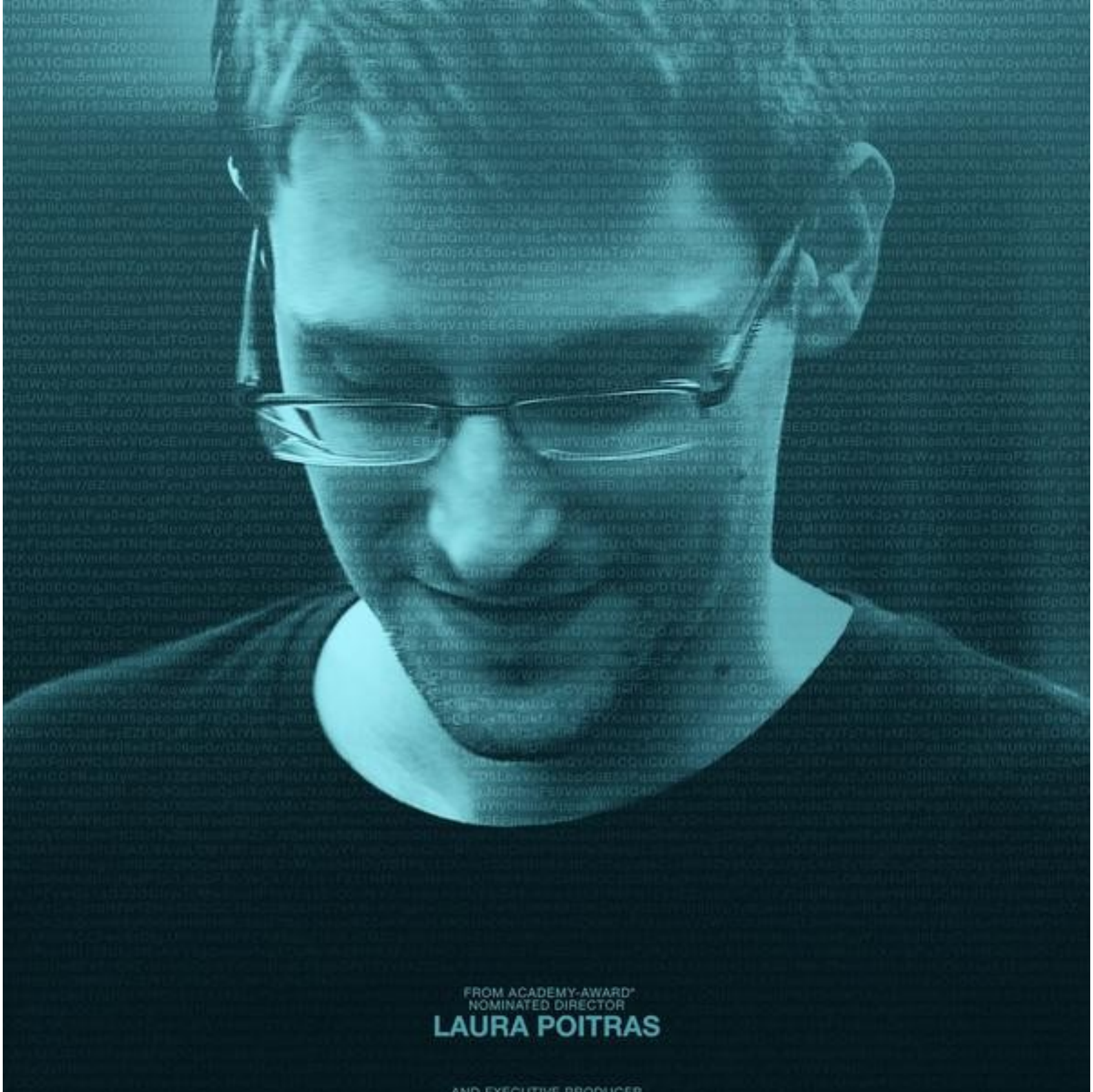
CHATTING IN SECRET WHILE WE'RE ALL BEING WATCHED

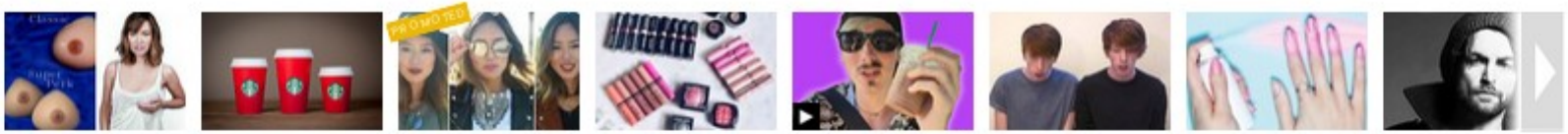
Micah Lee

July 14 2015, 7:08 p.m.

When you pick up the phone and call someone, or send a text message, or write an email, or send a Facebook message, or chat using Google Hangouts, other people find out what you're saying, who you're talking to, and where you're located. Such private data might only be available to the service provider brokering your conversation, but it might also be visible to the telecom companies carrying your Internet packets, to spy and law enforcement agencies, and even to some nearby teenagers monitoring your Wi-Fi network with Wireshark.

But if you take careful steps to protect yourself, it's possible to communicate online in a way that's private, secret and anonymous. Today I'm going to explain in precise terms how to do that. I'll take techniques NSA


FROM ACADEMY-AWARD®
NOMINATED DIRECTOR
LAURA POITRAS



TECH

You Probably Can't Encrypt Anything, Can You?

A new study shows that even the simplest encryption tools are lost on the public.

posted on Nov. 4 2015 at 8:32 p.m.

Joseph Bernstein
BuzzFeed News Reporter


GPG
TOR
OTR
WTF
Landesverräter
CRYPTOPARTY <3 NETZPOLITIK
FCK
NSA

Raise awareness.

SCHLAGWORTE

gesellschaft, überwachung, debatte, snowden, holly herndon, home, künstler, nsa, geheimdienste, privatsphäre

Zur Startseite

FUNKTIONEN

Kommentieren

DRUCKANSICHT

Read: NOW

SOCIAL MEDIA

TRINKGELD

Unterstütze **den Freitag**

MARIE GUTBUB

AUSGABE 1815 | 05.05.2015 | 06:00 4

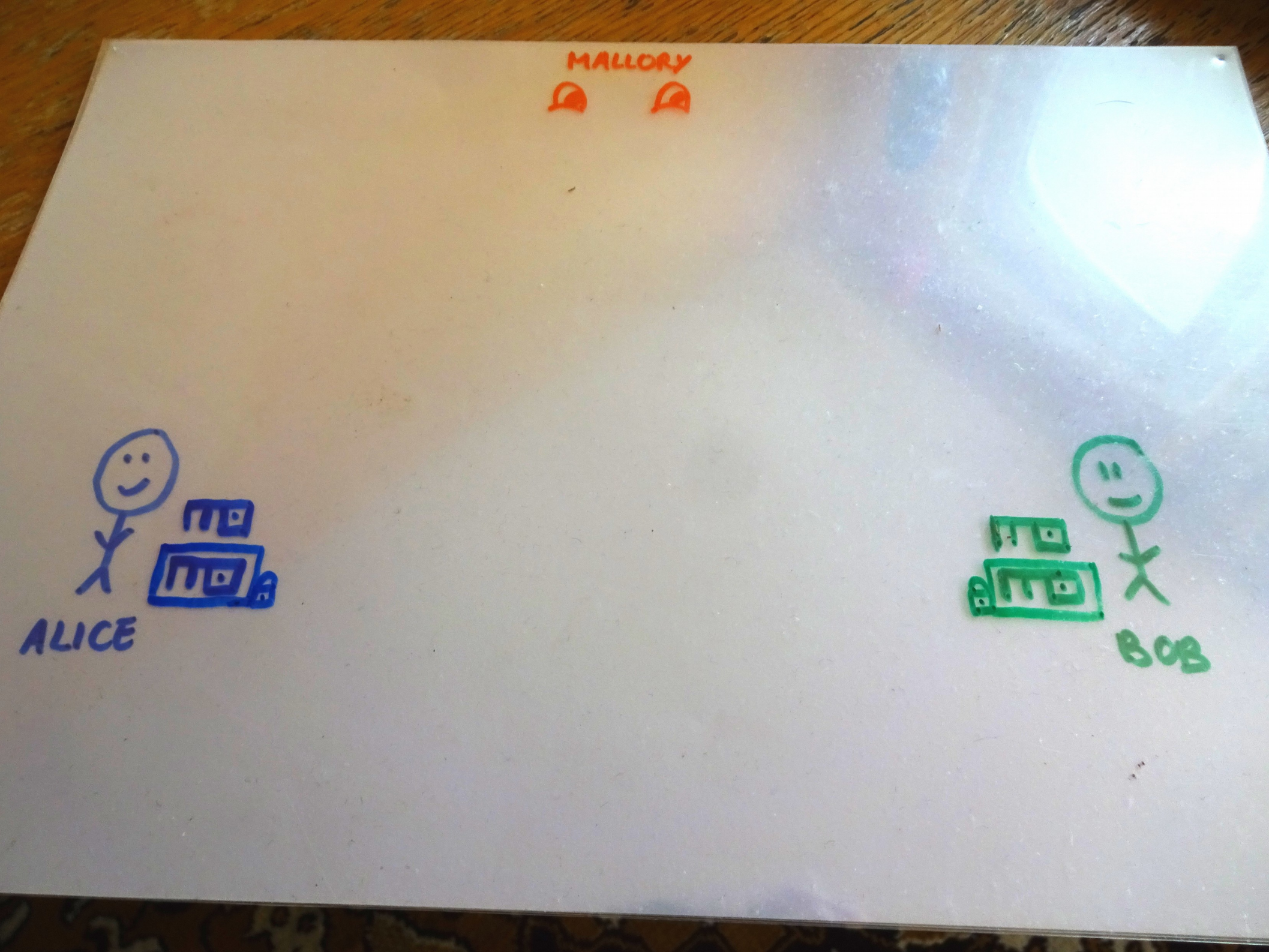
Guten Morgen, NSA

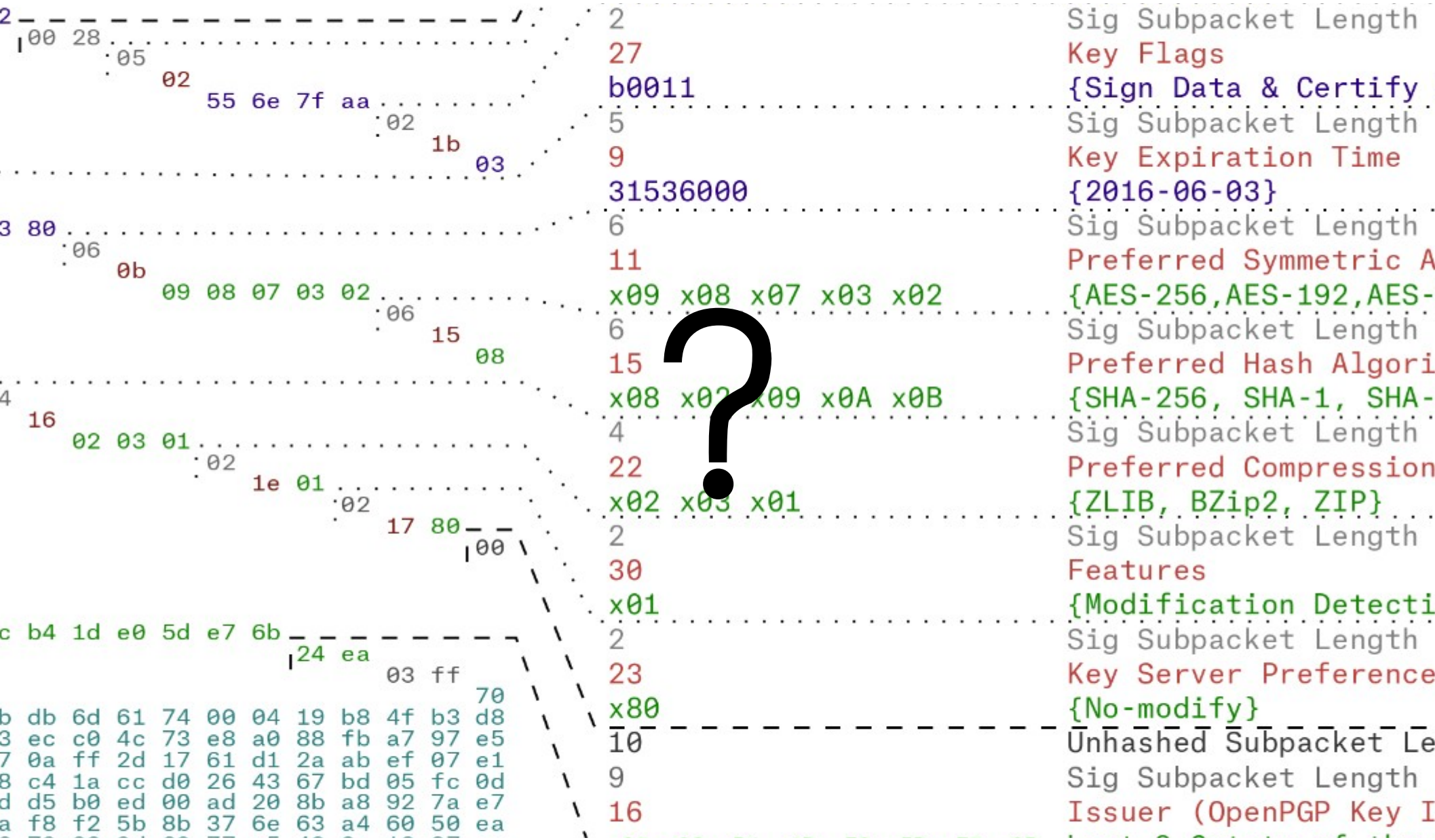
Snowden Zum Start der 9. re:publica ein Weckruf an die Künstler, das Thema Überwachung nicht länger zu ignorieren

„Ich kann euch in meinem Zimmer spüren. Warum wurde ich euch zugewiesen? Ich weiß, dass ihr mich besser kennt, als ich mich selbst kenne“: Holly Herndon steht aufrecht, schaut in die Kamera. Ihr Lied *Home* singt sie für die unsichtbare Person, von der sie in ihrem Videoclip gefilmt und im realen Leben ausspioniert wird. Es geht um eines der Lieblingsthemen der jungen US-amerikanischen Künstlerin sowie der Designerstudios Metahaven, die den Clip produziert haben: die Überwachung.

Von ihrem Spion wird Holly Herndon durch Piktogramme getrennt. Sie fallen in dichter Zahl von dem oberen Rand des Videos herunter und bilden eine Art farbige Regenwand. Es sind Piktogramme aus den NSA-Dokumenten, die Edward Snowden im Sommer 2013 an die Öffentlichkeit gebracht hat. Selbstverständlich habe ich diese Piktogramme sofort erkannt,

Drop the Charges !
Protect the Free Press !


MALLORY
ALICE
BOB


2
00 28
05
02
55 6e 7f aa
02
1b
03
3 80
06
0b
09 08 07 03 02
06
15
08
4
16
02 03 01
02
1e 01
02
17 80
00
c b4 1d e0 5d e7 6b
24 ea
03 ff
70
b db 6d 61 74 00 04 19 b8 4f b3 d8
3 ec c0 4c 73 e8 a0 88 fb a7 97 e5
7 0a ff 2d 17 61 d1 2a ab ef 07 e1
8 c4 1a cc d0 26 43 67 bd 05 fc 0d
d d5 b0 ed 00 ad 20 8b a8 92 7a e7
a f8 f2 5b 8b 37 6e 63 a4 60 50 ea
2 Sig Subpacket Length
27 Key Flags
b0011 {Sign Data & Certify
5 Sig Subpacket Length
9 Key Expiration Time
31536000 {2016-06-03}
6 Sig Subpacket Length
11 Preferred Symmetric A
x09 x08 x07 x03 x02 {AES-256,AES-192,AES-
6 Sig Subpacket Length
15 Preferred Hash Algori
x08 x02 x09 x0A x0B {SHA-256, SHA-1, SHA-
4 Sig Subpacket Length
22 Preferred Compression
x02 x03 x01 {ZLIB, BZip2, ZIP}
2 Sig Subpacket Length
30 Features
x01 {Modification Detecti
2 Sig Subpacket Length
23 Key Server Preference
x80 {No-modify}
10 Unhashed Subpacket Le
9 Sig Subpacket Length
16 Issuer (OpenPGP Key I
?

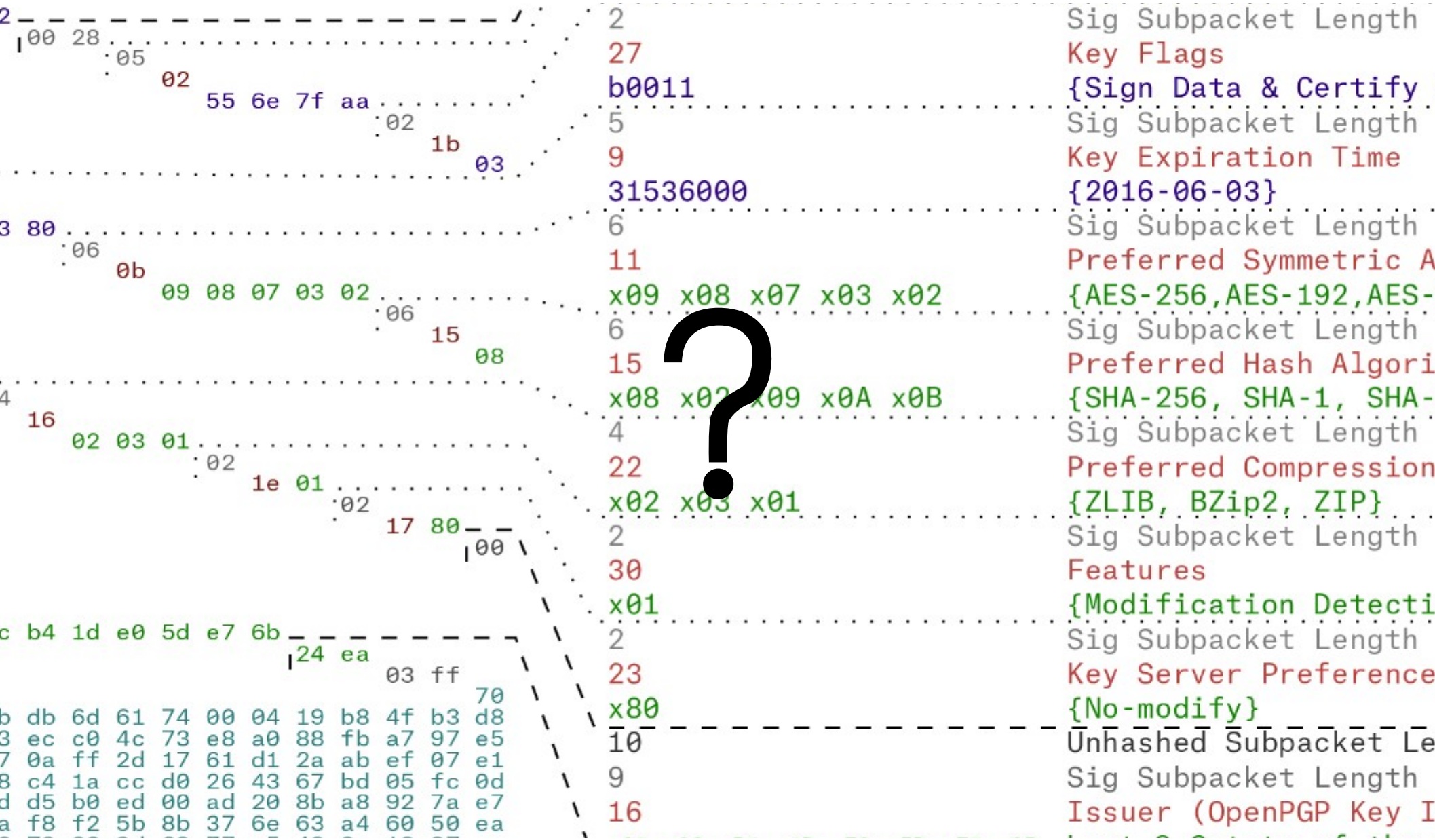

PRISM
KEYSCORE
CTO
Internet Cloud
CIA
The Internet
DoD Network

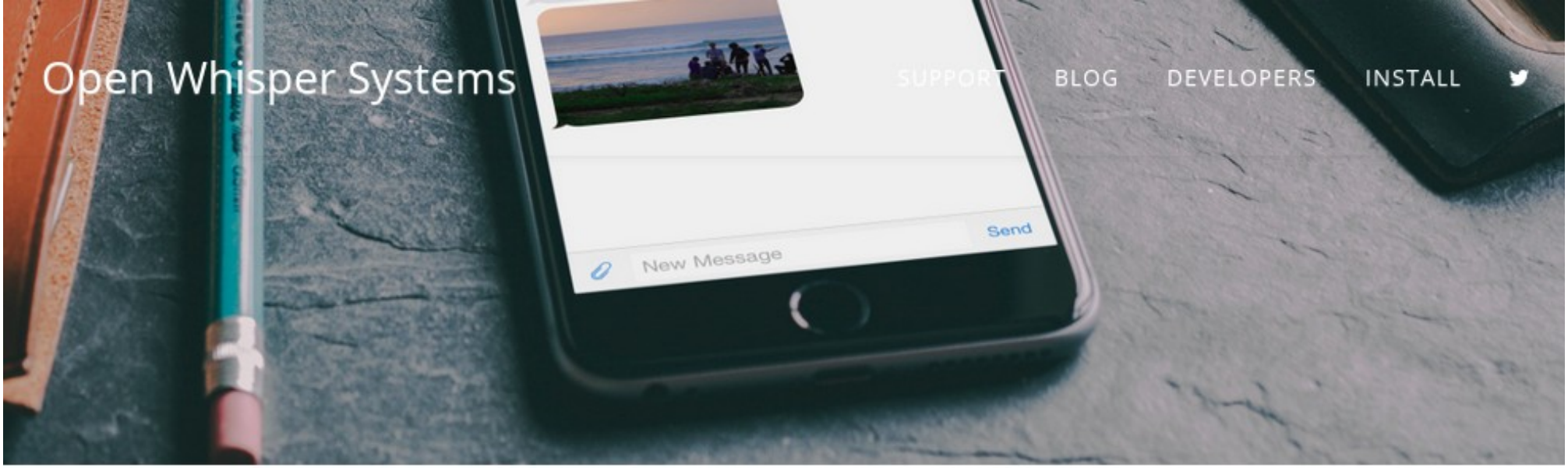

CRYPTO
JPARTY


PGP
TOR
OTR
FTW
CRYPTOPARTY.IN


CRYPTO
JPARTY

CryptoParty is not the solution.


2
00 28
05
02
55 6e 7f aa
02
1b
03
3 80
06
0b
09 08 07 03 02
06
15
08
4
16
02 03 01
02
1e 01
02
17 80
00
c b4 1d e0 5d e7 6b
24 ea
03 ff
70
b db 6d 61 74 00 04 19 b8 4f b3 d8
3 ec c0 4c 73 e8 a0 88 fb a7 97 e5
7 0a ff 2d 17 61 d1 2a ab ef 07 e1
8 c4 1a cc d0 26 43 67 bd 05 fc 0d
d d5 b0 ed 00 ad 20 8b a8 92 7a e7
a f8 f2 5b 8b 37 6e 63 a4 60 50 ea
2 Sig Subpacket Length
27 Key Flags
b0011 {Sign Data & Certify
5 Sig Subpacket Length
9 Key Expiration Time
31536000 {2016-06-03}
6 Sig Subpacket Length
11 Preferred Symmetric A
x09 x08 x07 x03 x02 {AES-256,AES-192,AES-
6 Sig Subpacket Length
15 Preferred Hash Algori
x08 x02 x09 x0A x0B {SHA-256, SHA-1, SHA-
4 Sig Subpacket Length
22 Preferred Compression
x02 x03 x01 {ZLIB, BZip2, ZIP}
2 Sig Subpacket Length
30 Features
x01 {Modification Detecti
2 Sig Subpacket Length
23 Key Server Preference
x80 {No-modify}
10 Unhashed Subpacket Le
9 Sig Subpacket Length
16 Issuer (OpenPGP Key I
?



PRIVACY THAT FITS IN YOUR POCKET

“Use anything by Open Whisper Systems.”

— **Edward Snowden**, Whistleblower and privacy advocate

“Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday.”

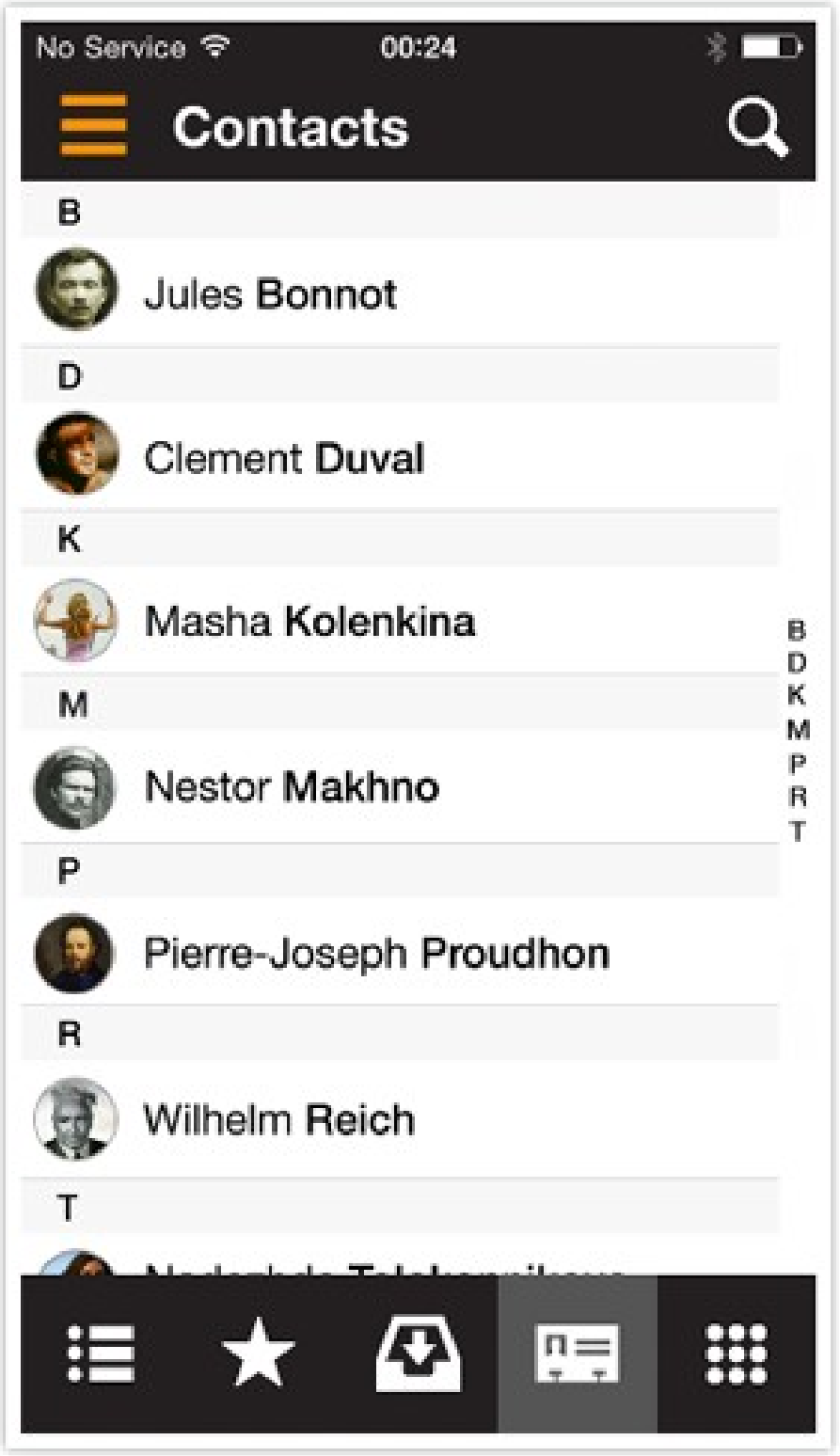
— **Laura Poitras**, Oscar winning filmmaker and journalist

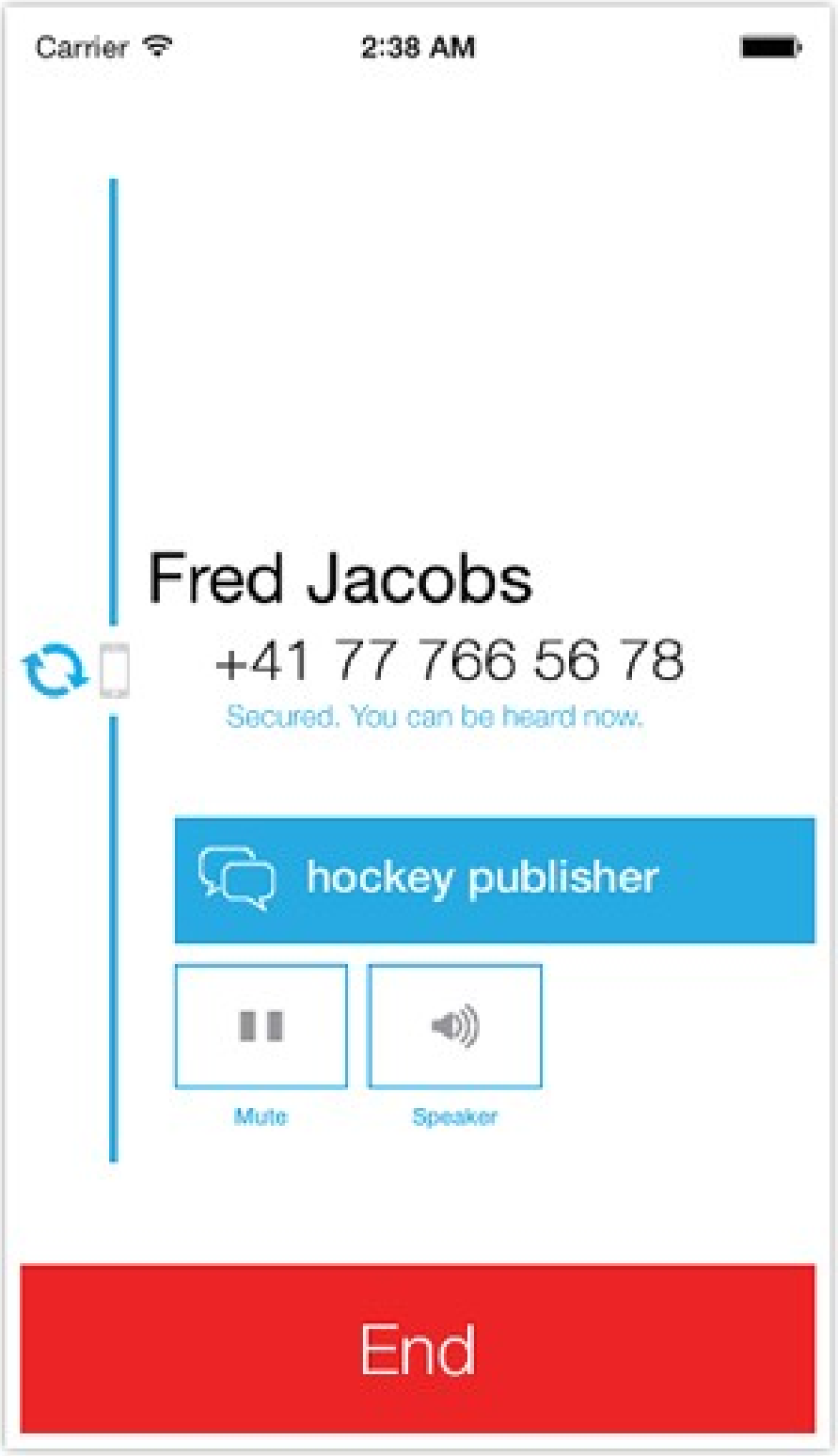
“I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation.”

— **Bruce Schneier**, internationally renowned security technologist

“After reading the code, I literally discovered a line of drool running down my face. It’s really nice.”

— **Matt Green**, Cryptographer, Johns Hopkins University


No Service
00:24
Contacts
B
Jules Bonnot
D
Clement Duval
K
Masha Kolenkina
M
Nestor Makhno
P
Pierre-Joseph Proudhon
R
Wilhelm Reich
T
B D K M P R T


Carrier
2:38 AM
Fred Jacobs
+41 77 766 56 78
Secured. You can be heard now.
hockey publisher
Mute
Speaker
End

Off-the-Record Messaging

Donate

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, *during* a conversation, your correspondent is assured the messages he sees are authentic and unmodified.

- **Perfect forward secrecy**

  If you lose control of your private keys, no previous conversation is compromised.

Primary download: Win32 installer for pidgin-otr 4.0.1 (sig) [other downloads]

News

21 Oct 2014

pidgin-otr 4.0.1 released

This point-release includes the following updates:

- Fix max message size for Novell Groupwise
- New Czech, Finnish, Brazilian Portuguese, Norwegian Bokmål translations. Updated French, Chinese translations.
- The Windows binary has been linked with updated versions of libotr, libgcrypt, and libgpg-error.

libotr 4.1.0 released

This minor-version update includes the following changes:

- Modernized autoconf build system
- Use constant-time comparisons where needed
- Use gcrypt secure memory allocation
- Correctly reject attempts to fragment a message into too many pieces
- Fix a missing opdata when sending message fragments
- Don't lose the first user message when REQUIRE_ENCRYPTION is set
- Fix some memory leaks
- Correctly check for children contexts' state when forgetting a context
- API Changes:
  - Added API functions otrl_context_find_recent_instance and otrl_context_find_recent_secure_instance.

10 Oct 2014

git repos and bugtracker now on otr.im

We now link to the new git repositories and the bugtracker on the community development site, otr.im.

28 Sept 2013

Now running on a new server

We've migrated the OTR website to a new and faster server. (Updated 3 Oct 2013): The URL is now https://otr.cypherpunks.ca/, as we have enabled TLS.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. H

- **Perfect forward secrecy**

  If you lose control of your private keys, no previous conversation is compromised.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. sation to make them look like they came from you. H

- **Perfect forward secrecy**

  If you lose control of your private keys, no previous conversation is compromised.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. sation to make them look like they came from you. H

- **Perfect forward secrecy**

  If you lose control of your private keys us conversation is compromised.

Downloads

OTR library and toolkit

This is the portable OTR Messaging Library, as well as the toolkit to help you forge messages. You need this library in order to use the other OTR software on this page. [Note that some binary packages, particularly Windows, do not have a separate library package, but just include the library and toolkit in the packages below.] The current version is 4.1.0.

README

UPGRADING from version 3.2.x

Source code (4.1.0)

Compressed tarball (sig)

Java OTR library

This is the Java version of the OTR library. This is for developers of Java applications that want to add support for OTR. End users do not require this package. It's still early days, but you can download java-otr version 0.1.0 (sig).

OTR plugin for Pidgin

This is a plugin for Pidgin 2.x which implements Off-the-Record Messaging over any IM network Pidgin supports. The current version is 4.0.1.

README

Source code (4.0.1)

Compressed tarball (sig)

Windows (4.0.1)

Win32 installer for pidgin 2.x (sig)
Win32 zipfile (manual installation) for pidgin 2.x (sig)

OTR localhost AIM proxy

This software is no longer supported. Please use an IM client with native support for OTR.

This is a localhost proxy you can use with almost any AIM client in order to participate in Off-the-Record conversations. The current version is 0.3.1, which means it's still a long way from done. Read the README file carefully. Some things it's still missing:

- Username/password authentication to the proxy
- Having the proxy be able to use *outgoing* proxies itself
- Support for protocols other than AIM/ICQ
- Configurability of the proxy types and ports it uses

But it should work for most people. Please send feedback to the otr-users mailing list, or to the dev team. You may need the above library packages.

README

Source code (0.3.1)

Compressed tarball (sig)

Windows (0.3.1)

Win32 installer (sig)

OS X (0.3.1)

OS X package

Source Code Repository and Bugtracker

You can find a git repository of the OTR source code, as well as the bugtracker, on the otr.im community development site:

- libotr git repo: https://bugs.otr.im/git/libotr.git ; git://git.otr.im/libotr.git
- pidgin-otr git repo: https://bugs.otr.im/git/pidgin_otr.git ; git://git.otr.im/pidgin_otr.git
- Bugtracker: https://bugs.otr.im

Mailing Lists

If you use OTR software, you should join at least the otr-announce mailing list, and possibly otr-users (for users of OTR software) or otr-dev (for developers of OTR software) as well.

Documentation

Installation and Setup Guides

pidgin-otr tutorial from the Security-in-a-Box project
Video OTR tutorial (by Niels)
Adium, Pidgin & OTR (auf Deutsch, by Christian Franke)

Downloads

OTR library and toolkit

This is the portable OTR Messaging Library, as well as the toolkit to help you forge messages. You need this library in order to use the other OTR software on this page. [Note that some binary packages, particularly Windows, do not have a separate library package, but just include the library and toolkit in the packages below.] The current version is 4.1.0.

README

UPGRADING from version 3.2.x

Source code (4.1.0)

Compressed tarball (sig)

Java OTR library

This is the Java version of the OTR library. This is for developers of Java applications that want to add support for OTR. End users do not require this package. It's still early days, but you can download java-otr version 0.1.0 (sig).

OTR plugin for Pidgin

This is a plugin for Pidgin 2.x which implements Off-the-Record Messaging over any IM network Pidgin supports. The current version is 4.0.1.

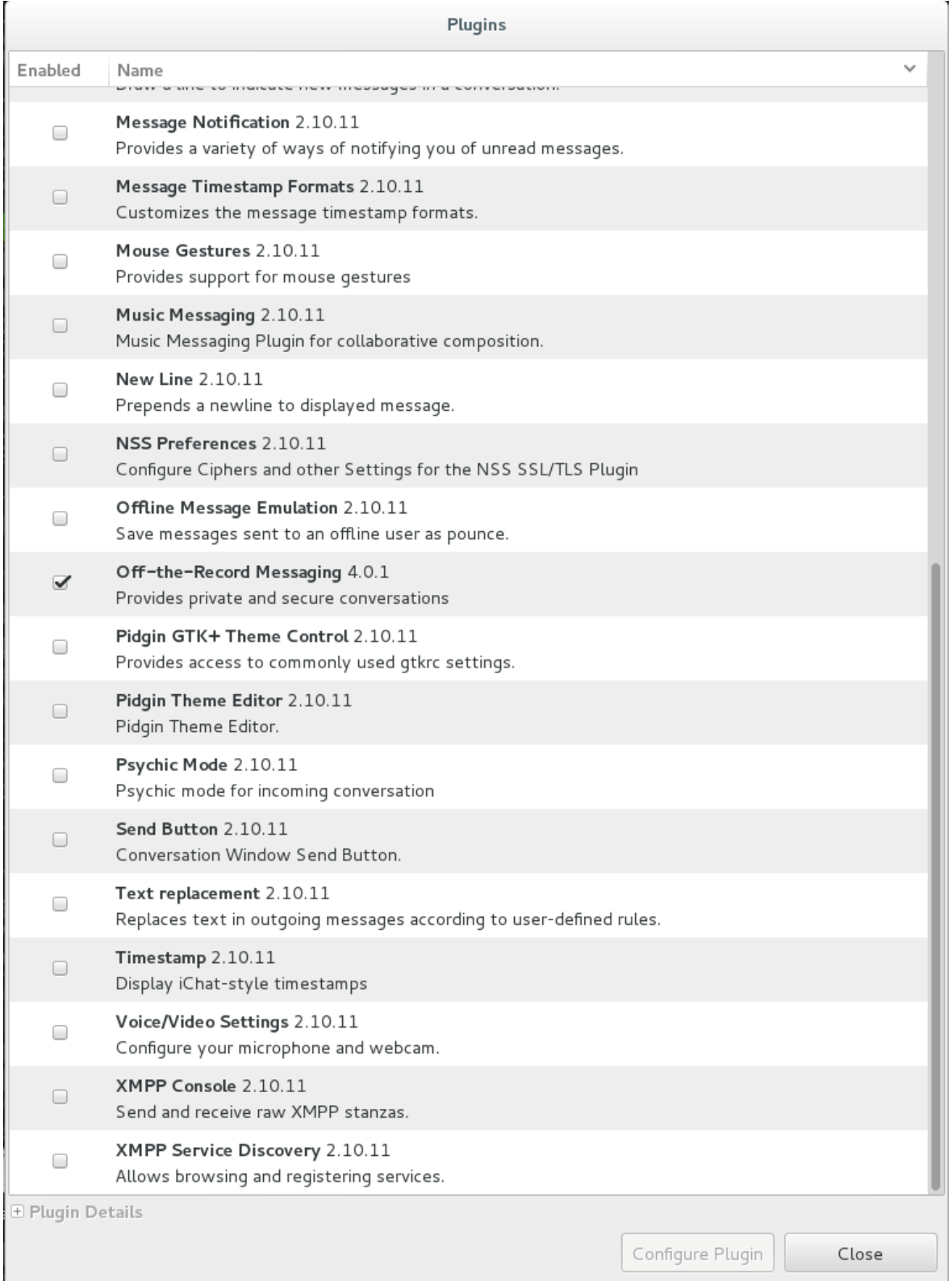
README

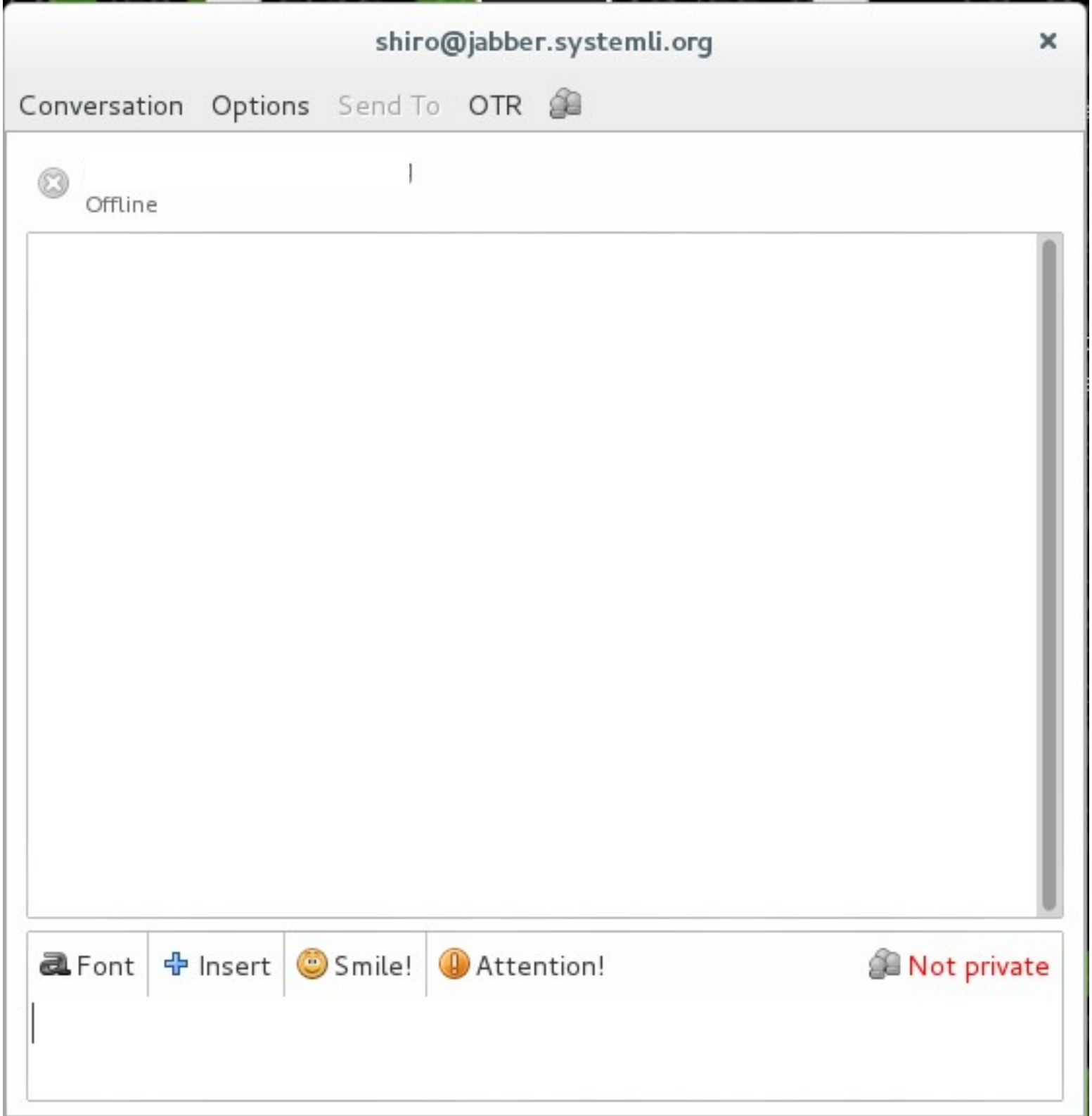
Source code (4.0.1)

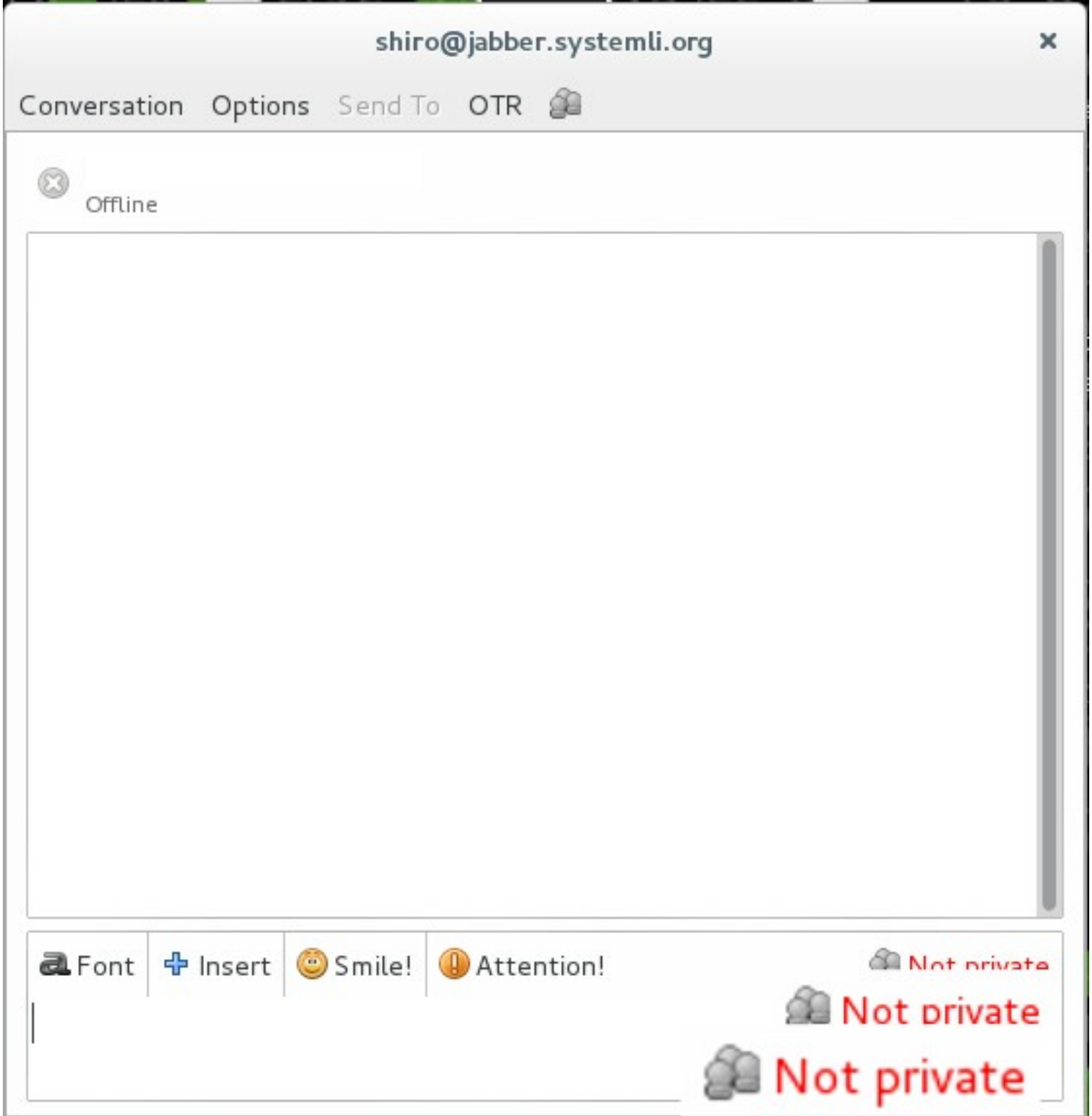
Compressed tarball (sig)

Windows (4.0.1)

Win32 installer for pidgin 2.x (sig)
Win32 zipfile (manual installation) for pidgin 2.x (sig)

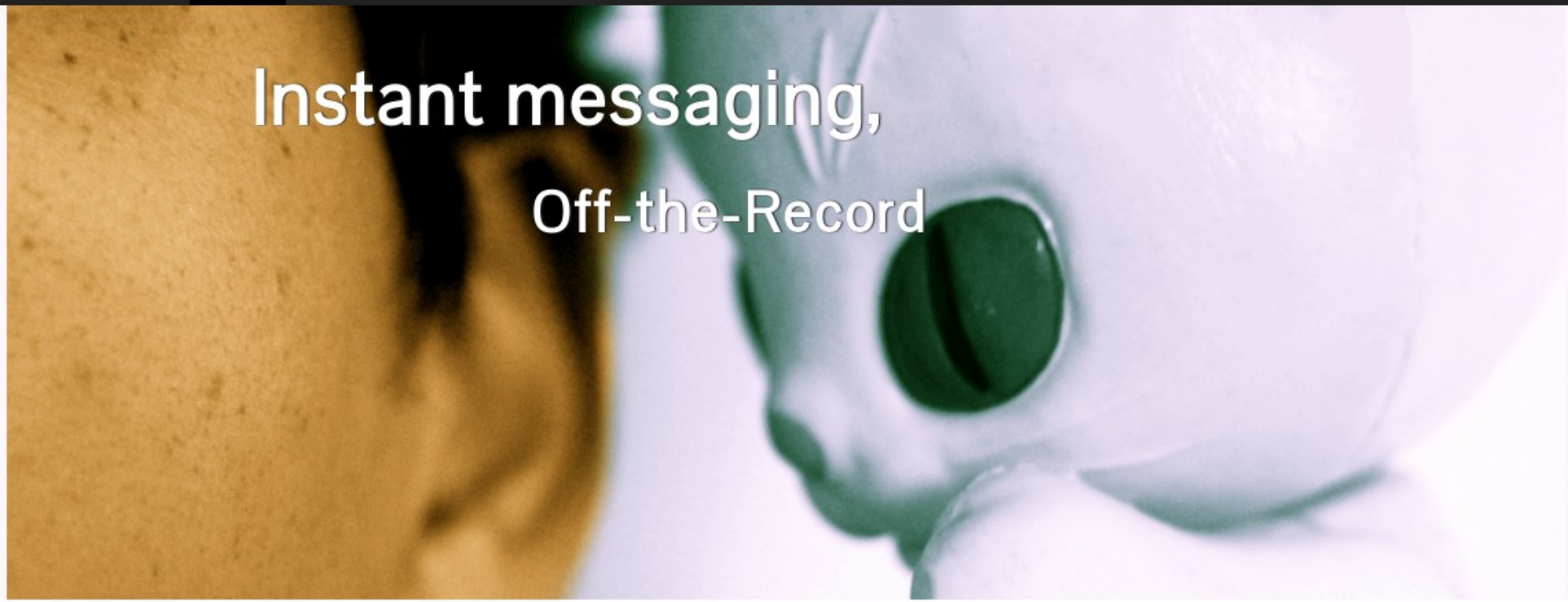

Plugins
Enabled
Name
Message Notification 2.10.11
Provides a variety of ways of notifying you of unread messages.
Message Timestamp Formats 2.10.11
Customizes the message timestamp formats.
Mouse Gestures 2.10.11
Provides support for mouse gestures
Music Messaging 2.10.11
Music Messaging Plugin for collaborative composition.
New Line 2.10.11
Prepends a newline to displayed message.
NSS Preferences 2.10.11
Configure Ciphers and other Settings for the NSS SSL/TLS Plugin
Offline Message Emulation 2.10.11
Save messages sent to an offline user as pounce.
Off-the-Record Messaging 4.0.1
Provides private and secure conversations
Pidgin GTK+ Theme Control 2.10.11
Provides access to commonly used gtkrc settings.
Pidgin Theme Editor 2.10.11
Pidgin Theme Editor.
Psychic Mode 2.10.11
Psychic mode for incoming conversation
Send Button 2.10.11
Conversation Window Send Button.
Text replacement 2.10.11
Replaces text in outgoing messages according to user-defined rules.
Timestamp 2.10.11
Display iChat-style timestamps
Voice/Video Settings 2.10.11
Configure your microphone and webcam.
XMPP Console 2.10.11
Send and receive raw XMPP stanzas.
XMPP Service Discovery 2.10.11
Allows browsing and registering services.
Plugin Details
Configure Plugin
Close


shiro@jabber.systemli.org
Conversation
Options
Send To
OTR
Offline
Font
Insert
Smile!
Attention!
Not private


shiro@jabber.systemli.org
Conversation
Options
Send To
OTR
Offline
Font
Insert
Smile!
Attention!
Not private
Not private
Not private

OTR.im

Home | Clients | Chat | About | Blog



OTR!

OTR, which stands for Off-the-Record messaging is a cryptographic protocol that provides strong encryption for instant messaging conversations. Originally designed by, among others, Ian Goldberg.

Get to know the OTR protocol »

Bugtracker

Help us improve OTR software by filing bugs, triaging bugs or submit patches to solve issues.

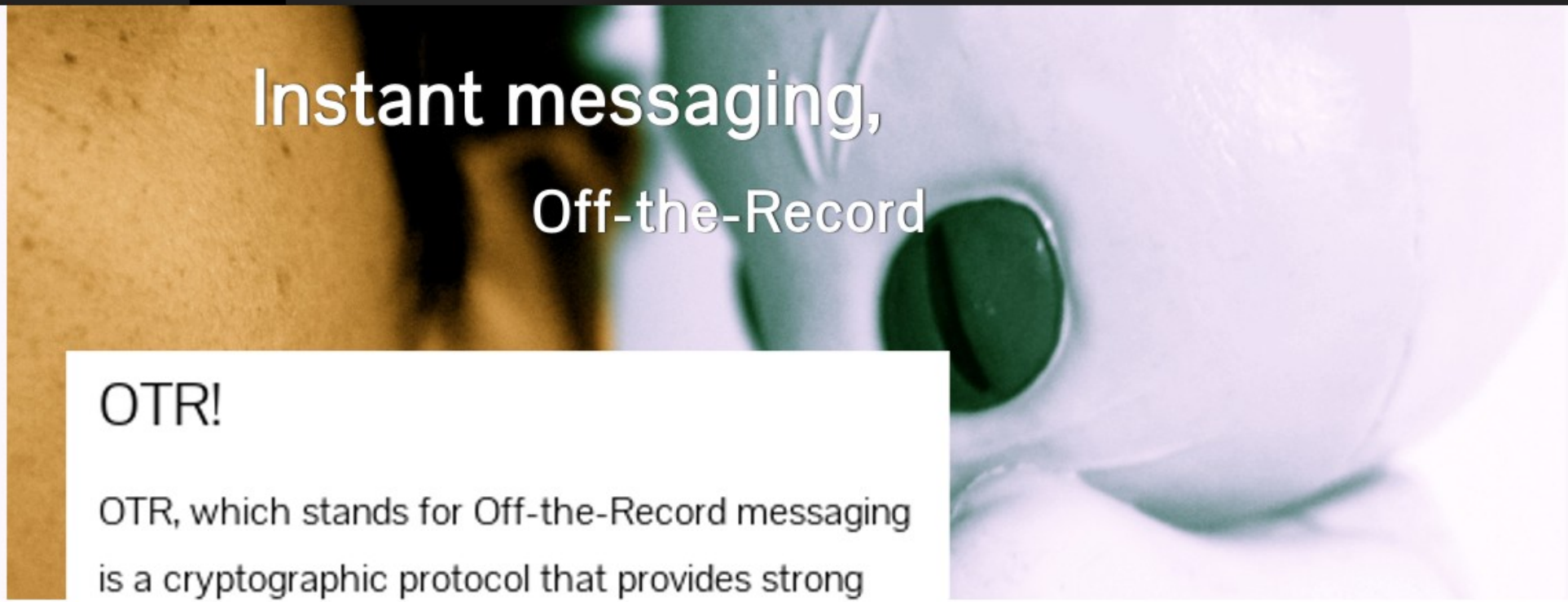
Contribute to the bugtracker »

Reaching developers

Many of the OTR enthusiasts and developers idle on the #OTR channel on the OFTC IRC network. Feel free to join, lurk or discuss..

IRC webchat »

OTR.im Home Clients Chat About Blog



OTR!

OTR, which stands for Off-the-Record messaging is a cryptographic protocol that provides strong encryption for instant messaging conversations. Originally designed by, among others, Ian Goldberg.

Get to know the OTR protocol »

OTR

OTR, v
is a cry
encryp
Origina
Goldbe

Get to know the OTR protocol »

Reaching developers

Many of the OTR enthusiasts and developers idle on the #OTR channel on the OFTC IRC network. Feel free to join, lurk or discuss..

IRC webchat »

Off-the-Record Messaging

Donate

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, *during* a conversation, your correspondent is assured the messages he sees are authentic and unmodified.

- **Perfect forward secrecy**

  If you lose control of your private keys, no previous conversation is compromised.

Primary download: Win32 installer for pidgin-otr 4.0.1 (sig) [other downloads]

News

21 Oct 2014

pidgin-otr 4.0.1 released

This point-release includes the following updates:

- Fix max message size for Novell Groupwise
- New Czech, Finnish, Brazilian Portuguese, Norwegian Bokmål translations. Updated French, Chinese translations.
- The Windows binary has been linked with updated versions of libotr, libgcrypt, and libgpg-error.

libotr 4.1.0 released

This minor-version update includes the following changes:

- Modernized autoconf build system
- Use constant-time comparisons where needed
- Use gcrypt secure memory allocation
- Correctly reject attempts to fragment a message into too many pieces
- Fix a missing opdata when sending message fragments
- Don't lose the first user message when REQUIRE_ENCRYPTION is set
- Fix some memory leaks
- Correctly check for children contexts' state when forgetting a context
- API Changes:
  - Added API functions otrl_context_find_recent_instance and otrl_context_find_recent_secure_instance.

10 Oct 2014

git repos and bugtracker now on otr.im

We now link to the new git repositories and the bugtracker on the community development site, otr.im.

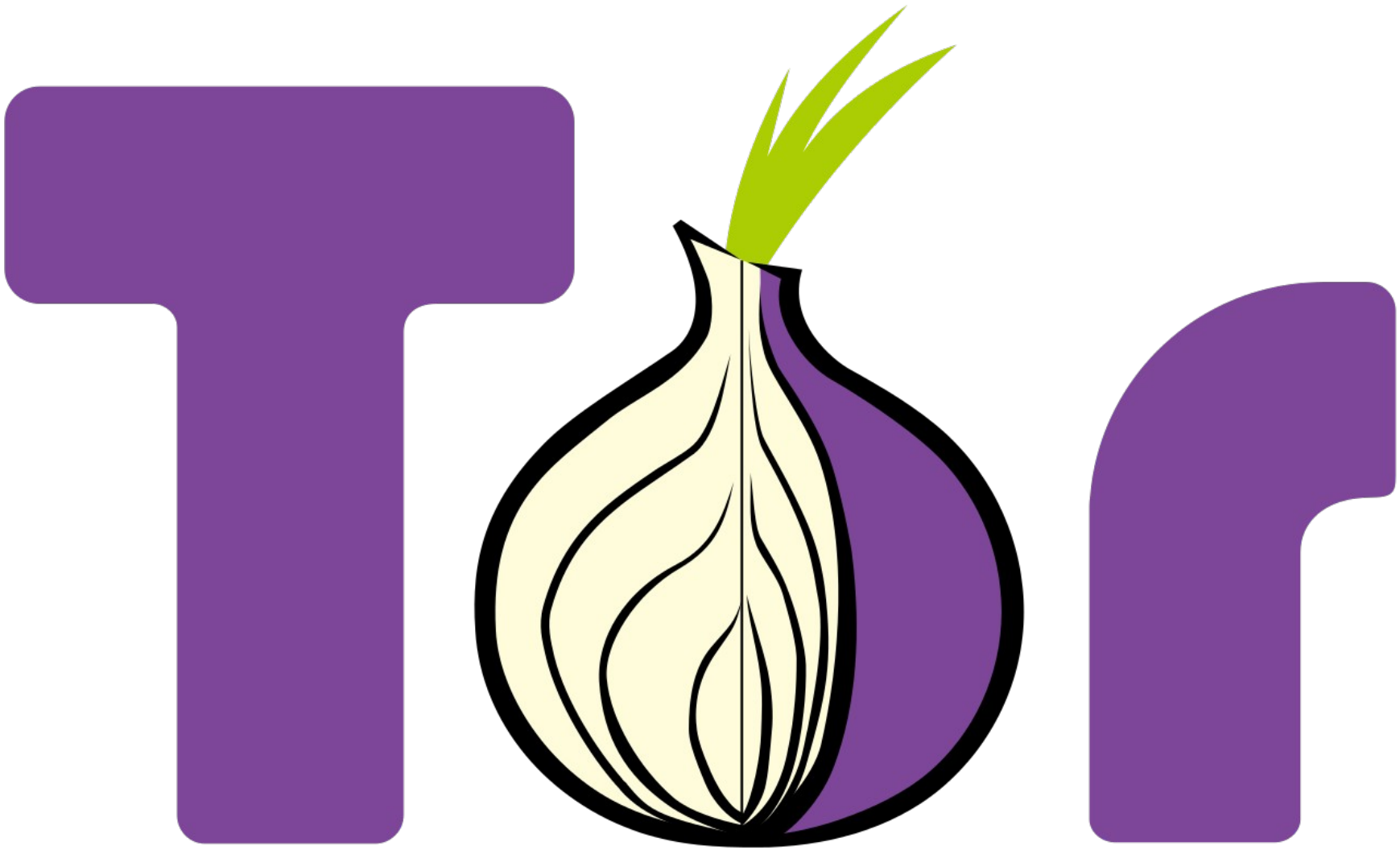
28 Sept 2013

Now running on a new server

We've migrated the OTR website to a new and faster server. (Updated 3 Oct 2013): The URL is now https://otr.cypherpunks.ca/, as we have enabled TLS.

User pain level: very high.

This needs to change.


Tor

The Benefits of Anonymity Online

The Reality

Internet Service Providers (such as BT and Verizon), websites (such as Google and Facebook), and governments use a common form of Internet surveillance known as IP address tracking to monitor conversations over public networks.

- News sites may promote different articles based on your location.
- Shopping sites may use price discrimination based on your country or institution of origin.
- An average person is tracked by over a hundred companies that sell profiles to advertisers.
- Your social media activity can be revealed and used against you by malicious individuals.

Freedom

The landscape of the Internet is in a constant state of change, and trends in law, policy, and technology threaten anonymity as never before, undermining our ability to speak and read freely online. Countries are watching each other as well as their own citizens, blocking websites, watching traffic content, and restricting important world news.

How Tor Works

Alice encrypts her web page request to Bob three times and sends it to the first relay.

The first relay removes the first encryption layer but doesn't learn that the web page request goes to Bob.

The second relay removes another encryption layer and forwards the web page request.

The third relay removes the last encryption layer and forwards the web page request to Bob, but doesn't know that it comes from Alice.

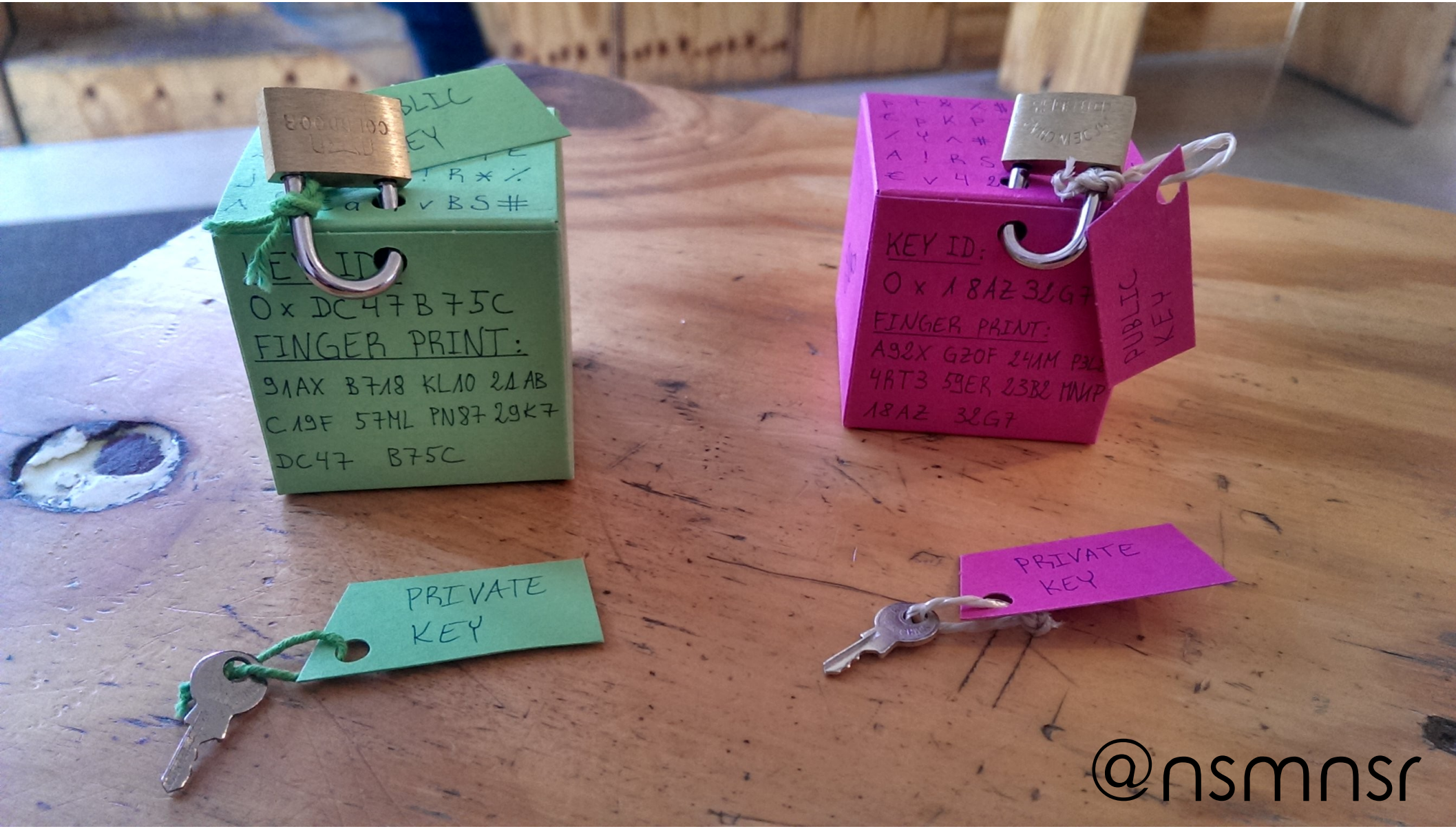
Bob doesn't know that the web page request came from Alice, unless she tells him so.

#1 in Privacy Online

- Tor is free, open source technology, honed over 10 years of research and development by Tor's team of security researchers and software developers.
- Tor is one of the most effective technologies to protect your privacy online and ensure your personal online security stays in your control.

https://www.torproject.org/ +1-781-948-1982


CRYPTO
JPARTY


KEY ID:
0x DC47 B75C
FINGER PRINT:
91AX B718 KL10 21AB
C19F 57ML PN87 29K7
DC47 B75C
PRIVATE KEY
KEY ID:
0x 18AZ 32G7
FINGER PRINT:
A92X GZOF 241M P3L2
4RT3 59ER 23BZ MNP
18AZ 32G7
PUBLIC KEY
PRIVATE KEY
@nsmnsr


CRYPTO
JPARTY

Help us to kill CryptoParty.

CryptoParty, 2pm, Workshop area

OpenFest Sofia, November 2015
@shiromarieke