[Skip to main content](https://webencrypt.org/otr/#content)

[Web Encrypt](https://webencrypt.org/)

* [Index](https://webencrypt.org/)
* [Cryptography](https://webencrypt.org/otr/)
* [Standard](https://webencrypt.org/otr/)
* [Cheat Sheet](https://webencrypt.org/otr/)
* [Organization](https://webencrypt.org/otr/)
* [Tool](https://webencrypt.org/otr/)
* [Online Tool](https://webencrypt.org/otr/)
* [Misc](https://webencrypt.org/otr/)
* [Introduce](https://webencrypt.org/otr/#introduce)
* [Difference between PGP and OTR](https://webencrypt.org/otr/#diffwithpgp)
* [Instant Messaging](https://webencrypt.org/otr/#instantmessaging)
* [Secure Message](https://webencrypt.org/otr/#securemessage)
* [Library](https://webencrypt.org/otr/#library)
* [**Reference**](https://webencrypt.org/otr/#reference)

Introduce

Off-the-Record Messaging (OTR) is a cryptographic protocol that provides encryption for instant messaging conversations. OTR uses a combination of AES symmetric-key algorithm with 128 bits key length, the Diffie–Hellman key exchange with 1536 bits group size, and the SHA-1 hash function. In addition to authentication and encryption, OTR provides forward secrecy and malleable encryption.

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.
* <https://otr.cypherpunks.ca/>
* <https://otr.im/>
* <https://github.com/otrv4/otrv4>
* [Protocol description (version 3)](https://webencrypt.org/otr/attachment/Protocol-v3-4.1.1.html)
* [Protocol description (version 2)](https://webencrypt.org/otr/attachment/Protocol-v2-3.1.0.html)
* [Off-the-Record Communication, or, Why Not to Use PGP](https://webencrypt.org/otr/attachment/otr-codecon.pdf)
* [A User Study of Off-the-Record Messaging](https://webencrypt.org/otr/attachment/otr_userstudy.pdf)
* [Improved User Authentication in Off-The-Record Messaging](https://webencrypt.org/otr/attachment/impauth.pdf)
* [Off-the-Record Communication, or, Why Not To Use PGP](https://webencrypt.org/otr/attachment/otr-wpes.pdf)
* [Off-the-Record Communication, or,  Why Not to Use PGP.PPT](https://webencrypt.org/otr/attachment/otr-wpes.ppt)
* [Off-the-Record Communication, or, Why Not to Use PGP.PDF](https://webencrypt.org/otr/attachment/otr-wpes-present.pdf)
* [Off-the-Record Communication, or, Why Not to Use PGP.PDF](https://webencrypt.org/otr/attachment/otr-codecon.pdf)

Difference between PGP and OTR

|  |  |
| --- | --- |
| **OTR - Off the Record** | **PGP - Pretty Good Privacy** |
| OTR is designed for instant messaging. It initiates a key-exchange between two peers when they are both online. Forward secrecy ensures that, if one of the peers loses control of the long-lived cryptographic keys, no previous conversations can be compromised. | PGP, which stands for “Pretty Good Privacy” was designed for encrypting, decrypting and signing e-mail and data like, texts, files, whole disk partitions. |
| OTR encrypted messages don't contain digital signatures. After a conversation is over, anyone could forge messages which appear to originate from one of the participants of the conversation. Which means that you can't prove the authenticity of the message. However, there is no precedence in any real-life court case with this scenario. | By using PGP for e-mail to exchange messages, at least two or more peers each have an keypair. Now, if you want to verify the key, you can't make use of a protocol as like with OTR. It can only be done by verifying the fingerprint of the peer you want to communicate with, preferrably over a secure channel. |
| OTR implements among others the authentication through the socialist millionaire protocol. This means that, peers can verify each others' identity through the use of a shared secret avoiding a man-in-the-middle attack. Furthermore, users get around the inconvenience of manually comparing each others fingerprints through e.g, an outbound channel over the internet. One can also verify the identity of a peer through comparing fingerprints. | It also comes with digital signatures which are used for message authentication and integrity checking. The latter is only used to see whether the message has been tampered with and if the sender was the real sender. With PGP you can't deny to ever have received the message like you can with OTR. |

Instant Messaging

<https://otr.im/>

Secure Message

CoyIM

<https://coy.im/>  
<https://github.com/coyim/coyim>

CoyIM is a new client for the XMPP protocol. It is built upon https://github.com/agl/xmpp-client and https://github.com/coyim/otr3.

Dark Mail

<https://darkmail.info/>

mailpile

<https://www.mailpile.is/>

Signal

<https://whispersystems.org/docs/specifications/doubleratchet/doubleratchet.pdf>  
<https://whispersystems.org/docs/specifications/x3dh/>  
<https://whispersystems.org/docs/specifications/xeddsa/>  
<https://whispersystems.org/docs/specifications/doubleratchet/>

SMIMP

<http://smimp.org/>  
<https://github.com/smimp/smimp_spec/blob/master/smimp_specification.md>

Library

* Java
  + <https://github.com/jitsi/otr4j> - *Off-the-Record messaging library for Java*

Reference

1. <https://en.wikipedia.org/wiki/Off-the-Record_Messaging>
2. <https://otr.cypherpunks.ca/>
3. <https://whispersystems.org/blog/asynchronous-security/>
4. <https://github.com/WhisperSystems/Signal-iOS/wiki/FAQ>
5. <https://en.wikipedia.org/wiki/Signal_Protocol>
6. <https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_protocols>

*Hatter Jiang, WebEncrypt.Org, My key:*[*https://hatter.in/key*](https://hatter.in/key)*,*[*leave message here*](https://hatter.ink/message/post.jssp?subject=WebEncrypt.org)