Off-the-Record Messaging

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#searchInput)

**Off-the-Record Messaging** (**OTR**) is a [cryptographic protocol](https://en.wikipedia.org/wiki/Cryptographic_protocol) that provides encryption for [instant messaging](https://en.wikipedia.org/wiki/Instant_messaging) conversations. OTR uses a combination of [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) [symmetric-key algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) with 128 bits key length, the [Diffie–Hellman key exchange](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange) with 1536 bits group size, and the [SHA-1](https://en.wikipedia.org/wiki/SHA-1) hash function. In addition to [authentication](https://en.wikipedia.org/wiki/Authentication) and [encryption](https://en.wikipedia.org/wiki/Encryption), OTR provides [forward secrecy](https://en.wikipedia.org/wiki/Forward_secrecy) and [malleable encryption](https://en.wikipedia.org/wiki/Malleability_(cryptography)).

The primary motivation behind the protocol was providing [deniable authentication](https://en.wikipedia.org/wiki/Deniable_authentication) for the conversation participants while keeping conversations confidential, like a private conversation in real life, or [off the record](https://en.wikipedia.org/wiki/Journalism_sourcing#Using_confidential_information) in [journalism sourcing](https://en.wikipedia.org/wiki/Journalism_sourcing). This is in contrast with cryptography tools that produce output which can be later used as a verifiable record of the communication event and the identities of the participants. The initial introductory paper was named "Off-the-Record Communication, or, Why Not To Use [PGP](https://en.wikipedia.org/wiki/Pretty_Good_Privacy)".[[1]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-not-pgp-1)

The OTR protocol was designed by cryptographers [Ian Goldberg](https://en.wikipedia.org/wiki/Ian_Goldberg) and [Nikita Borisov](https://en.wikipedia.org/wiki/Nikita_Borisov) and released on 26 October 2004.[[2]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-10th-anniversary-2) They provide a client [library](https://en.wikipedia.org/wiki/Library_(computer_science)) to facilitate support for instant messaging client developers who want to implement the protocol. A [Pidgin](https://en.wikipedia.org/wiki/Pidgin_(software)) and [Kopete](https://en.wikipedia.org/wiki/Kopete) plugin exists that allows OTR to be used over any IM protocol supported by Pidgin or Kopete, offering an [auto-detection](https://en.wikipedia.org/wiki/Opportunistic_encryption) feature that starts the OTR session with the buddies that have it enabled, without interfering with regular, unencrypted conversations. Version 4 of the protocol[[3]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-version-4-3) is currently[[*when?*](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Dates_and_numbers#Chronological_items)] being designed by a team led by Sofía Celi, and reviewed by Nik Unger and Ian Goldberg. This version aims to provide online and offline deniability, to update the cryptographic primitives, and to support [out-of-order delivery](https://en.wikipedia.org/wiki/Out-of-order_delivery) and asynchronous communication.



**Contents**

* [1History](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#History)
* [2Implementation](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Implementation)
* [3Authentication](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Authentication)
* [4Limitations](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Limitations)
* [5Client support](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Client_support)
  + [5.1Native (supported by project developers)](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Native_(supported_by_project_developers))
  + [5.2Via third-party plug-in](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Via_third-party_plug-in)
  + [5.3Confusion with Google Talk "off the record"](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Confusion_with_Google_Talk_%22off_the_record%22)
* [6See also](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#See_also)
* [7References](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#References)
* [8Further reading](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#Further_reading)
* [9External links](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#External_links)

History[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=1)]

OTR was presented in 2004 by Nikita Borisov, Ian Avrum Goldberg, and Eric A. Brewer as an improvement over the OpenPGP and the S/MIME system at the "Workshop on Privacy in the Electronic Society" (WPES).[[1]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-not-pgp-1) The first version 0.8.0 of the reference implementation was published on 21 November 2004. In 2005 an analysis was presented by Mario Di Raimondo, Rosario Gennaro, and Hugo Krawczyk that called attention to several vulnerabilities and proposed appropriate fixes, most notably including a flaw in the key exchange.[[4]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Secure_OTR-4) As a result, version 2 of the OTR protocol was published in 2005 which implements a variation of the proposed modification that additionally hides the public keys. Moreover, the possibility to fragment OTR messages was introduced in order to deal with chat systems that have a limited message size, and a simpler method of verification against man-in-the-middle attacks was implemented.[[5]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-v2-5)

In 2007 [Olivier Goffart](https://en.wikipedia.org/w/index.php?title=Olivier_Goffart&action=edit&redlink=1) published mod\_otr[[6]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-6) for [ejabberd](https://en.wikipedia.org/wiki/Ejabberd), making it possible to perform [man-in-the-middle attacks](https://en.wikipedia.org/wiki/Man-in-the-middle_attack) on OTR users who don't check key fingerprints. OTR developers countered this attack by introducing [socialist millionaire protocol](https://en.wikipedia.org/wiki/Socialist_millionaires) implementation in libotr. Instead of comparing key checksums, knowledge of an arbitrary shared secret can be utilised for which relatively low [entropy](https://en.wikipedia.org/wiki/Entropy_(information_theory)) can be tolerated by using the [socialist millionaire protocol](https://en.wikipedia.org/wiki/Socialist_millionaires).[[7]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-WPES'07-7)

Version 3 of the protocol was published in 2012. As a measure against the repeated reestablishment of a session in case of several competing chat clients being signed on to the same user address at the same time, more precise identification labels for sending and receiving client instances were introduced in version 3. Moreover, an additional key is negotiated which can be used for another data channel.[[8]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-v3-8)

Several solutions have been proposed for supporting conversations with multiple participants. A method proposed in 2007 by Jiang Bian, Remzi Seker, and Umit Topaloglu uses the system of one participant as a "virtual server".[[9]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-BianSekerTopaloglu-9) The method called "Multi-party Off-the-Record Messaging" (mpOTR) which was published in 2009 works without a central management host and was introduced in [Cryptocat](https://en.wikipedia.org/wiki/Cryptocat) by Ian Goldberg et al.[[10]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-mpOTR-10)

In 2013, the [Signal Protocol](https://en.wikipedia.org/wiki/Signal_Protocol) was introduced, which is based on OTR Messaging and the [Silent Circle Instant Messaging Protocol](https://en.wikipedia.org/wiki/Silent_Circle_Instant_Messaging_Protocol) (SCIMP). It brought about support for asynchronous communication ("offline messages") as its major new feature, as well as better resilience with distorted order of messages and simpler support for conversations with multiple participants.[[11]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-SoK-11) [OMEMO](https://en.wikipedia.org/wiki/OMEMO), introduced in an Android XMPP client called [Conversations](https://en.wikipedia.org/w/index.php?title=Conversations_(software)&action=edit&redlink=1) in 2015, integrates the [Double Ratchet Algorithm](https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm) used in Signal into the instant messaging protocol [XMPP](https://en.wikipedia.org/wiki/XMPP) ("Jabber") and also enables encryption of file transfers. In the autumn of 2015 it was submitted to the [XMPP Standards Foundation](https://en.wikipedia.org/wiki/XMPP_Standards_Foundation) for standardisation.[[12]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-OMEMO-XEP-12)[[13]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-OMEMO-Jingle-13)

Currently, version 4 of the protocol has been designed. It was presented by Sofía Celi and Ola Bini on PETS2018.[[14]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-no-evidence-14)

Implementation[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=2)]

In addition to providing encryption and authentication — features also provided by typical public-key cryptography suites, such as [PGP](https://en.wikipedia.org/wiki/Pretty_Good_Privacy), [GnuPG](https://en.wikipedia.org/wiki/GNU_Privacy_Guard), and [X.509](https://en.wikipedia.org/wiki/X.509) ([S/MIME](https://en.wikipedia.org/wiki/S/MIME)) — OTR also offers some less common features:

* [Forward secrecy](https://en.wikipedia.org/wiki/Forward_secrecy): Messages are only [encrypted](https://en.wikipedia.org/wiki/Encrypted) with temporary per-message [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) keys, negotiated using the [Diffie–Hellman key exchange](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange) protocol. The compromise of any long-lived cryptographic keys does not compromise any previous conversations, even if an attacker is in possession of [ciphertexts](https://en.wikipedia.org/wiki/Ciphertext).
* [Deniable authentication](https://en.wikipedia.org/wiki/Deniable_authentication): Messages in a conversation do not have [digital signatures](https://en.wikipedia.org/wiki/Digital_signature), and after a conversation is complete, anyone is able to forge a message to appear to have come from one of the participants in the conversation, assuring that it is impossible to prove that a specific message came from a specific person. Within the conversation the recipient can be sure that a message is coming from the person they have identified.

Authentication[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=3)]

As of OTR 3.1, the protocol supports mutual authentication of users using a shared secret through the [socialist millionaire](https://en.wikipedia.org/wiki/Socialist_millionaire) protocol. This feature makes it possible for users to verify the identity of the remote party and avoid a [man-in-the-middle attack](https://en.wikipedia.org/wiki/Man-in-the-middle_attack) without the inconvenience of manually comparing [public key fingerprints](https://en.wikipedia.org/wiki/Public_key_fingerprint) through an outside channel.

Limitations[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=4)]

Due to limitations of the protocol, OTR does not support multi-user group chat as of 2009[[15]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-multi-party-15) but it may be implemented in the future. As of version 3[[8]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-v3-8) of the protocol specification, an extra symmetric key is derived during authenticated key exchanges that can be used for secure communication (e.g., encrypted [file transfers](https://en.wikipedia.org/wiki/File_transfer)) over a different channel. Support for encrypted audio or video is not planned. ([SRTP](https://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol) with [ZRTP](https://en.wikipedia.org/wiki/ZRTP) exists for that purpose.) A project to produce a protocol for multi-party off-the-record messaging (mpOTR) has been organized by [Cryptocat](https://en.wikipedia.org/wiki/Cryptocat), [eQualitie](https://en.wikipedia.org/w/index.php?title=EQualitie&action=edit&redlink=1), and other contributors including Ian Goldberg.[[10]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-mpOTR-10)[[16]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-mpOTR-Plan-16)

Since OTR protocol v3 (libotr 4.0.0) the plugin supports multiple OTR conversations with the same buddy who is logged in at multiple locations.[[17]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-libotr4-17)

Client support[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=5)]

|  |  |
| --- | --- |
| **libotr** | |
| [**Developer(s)**](https://en.wikipedia.org/wiki/Software_developer) | [OTR Development Team](https://otr.cypherpunks.ca/people.php) |
| [**Stable release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | 4.1.1 / 9 March 2016; 4 years ago |
| **Written in** | [C](https://en.wikipedia.org/wiki/C_(programming_language)) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Cross-platform](https://en.wikipedia.org/wiki/Cross-platform) |
| [**Type**](https://en.wikipedia.org/wiki/Software_categories#Categorization_approaches) | [Software Library](https://en.wikipedia.org/wiki/Software_Library) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [LGPL](https://en.wikipedia.org/wiki/GNU_Lesser_General_Public_License) v2.1+[[18]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-libotr_license-18) |
| **Website** | <https://otr.cypherpunks.ca/index.php#downloads> |

**Native (supported by project developers)**[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=6)]

These clients support Off-the-Record Messaging out of the box.

* [Adium](https://en.wikipedia.org/wiki/Adium) ([OS X](https://en.wikipedia.org/wiki/OS_X))
* [Blink SIP client](https://en.wikipedia.org/wiki/Blink_(SIP_client)) ([OS X](https://en.wikipedia.org/wiki/OS_X))
* [BitlBee](https://en.wikipedia.org/wiki/BitlBee) (cross-platform), since 3.0 (optional at compile-time)[[19]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-BitlBee-19)
* [CenterIM](https://en.wikipedia.org/wiki/CenterIM) ([Unix-like](https://en.wikipedia.org/wiki/Unix-like)), since 4.22.2
* [ChatSecure](https://en.wikipedia.org/wiki/ChatSecure) ([iOS](https://en.wikipedia.org/wiki/IOS))
* [Zom Mobile Messenger](https://en.wikipedia.org/wiki/The_Guardian_Project_(software)) ([Android](https://en.wikipedia.org/wiki/Android_(operating_system)))
* [climm](https://en.wikipedia.org/wiki/Climm) ([Unix-like](https://en.wikipedia.org/wiki/Unix-like)), since (mICQ) 0.5.4
* IronChat, based on Xabber ([Android](https://en.wikipedia.org/wiki/Android_(operating_system)))
* [Jitsi](https://en.wikipedia.org/wiki/Jitsi) (cross-platform)
* [Kadu](https://en.wikipedia.org/wiki/Kadu_(software)) ([cross-platform](https://en.wikipedia.org/wiki/Cross-platform)), since 1.0[[20]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Kadu-20)
* [Kopete](https://en.wikipedia.org/wiki/Kopete) ([Unix-like](https://en.wikipedia.org/wiki/Unix-like))[[21]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-kopete-otr_KDE-21)[[22]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-kopete-otr_review-22)
* LeechCraft (cross-platform)[[23]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-leechcraft1-23)[[24]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-leechcraft2-24)
* [MCabber](https://en.wikipedia.org/wiki/MCabber) ([Unix-like](https://en.wikipedia.org/wiki/Unix-like)), since 0.9.4[[25]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-MCabber-25)
* [Profanity](https://en.wikipedia.org/wiki/Profanity_(instant_messaging_client)), since 0.4.1
* [Psi](https://en.wikipedia.org/wiki/Psi_(instant_messaging_client)) ([cross-platform](https://en.wikipedia.org/wiki/Cross-platform))[[26]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Psi-26)
* [Psi+](https://en.wikipedia.org/wiki/Psi_(instant_messaging_client)#History) ([cross-platform](https://en.wikipedia.org/wiki/Cross-platform))[[26]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Psi-26)[[27]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Psi+-27)
* Textual 5 ([OS X](https://en.wikipedia.org/wiki/OS_X)), since 5.1.2
* Xabber ([Android](https://en.wikipedia.org/wiki/Android_(operating_system)))
* [Tkabber](https://en.wikipedia.org/wiki/Tkabber) ([cross-platform](https://en.wikipedia.org/wiki/Cross-platform)), since version 1.1[[28]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Tkabber-28)
* [irssi](https://en.wikipedia.org/wiki/Irssi) , in (future) releases released after August 2018, currently in 'master' repo

**Via third-party plug-in**[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=7)]

[](https://en.wikipedia.org/wiki/File:Off-The-Record_authentication_dialog..png)

Off-The-Record authentication in [Pidgin](https://en.wikipedia.org/wiki/Pidgin_(software)) using [Socialist millionaires](https://en.wikipedia.org/wiki/Socialist_millionaire) protocol

The following clients require a plug-in to use Off-the-Record Messaging.

* [xchat](https://en.wikipedia.org/wiki/Xchat), with a third-party plugin[[29]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-irssi-xchat-29)
* [Miranda IM](https://en.wikipedia.org/wiki/Miranda_IM) ([Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows)), with a third-party plugin[[30]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Miranda-30)
* [Pidgin](https://en.wikipedia.org/wiki/Pidgin_(software)) ([cross-platform](https://en.wikipedia.org/wiki/Cross-platform)), with a plugin available from the OTR homepage[[31]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-Pidgin-31)
* [WeeChat](https://en.wikipedia.org/wiki/WeeChat), with a third-party plugin[[32]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-WeeChat-32)
* [HexChat](https://en.wikipedia.org/wiki/HexChat), for \*nix versions, with a third-party plugin[[33]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-33)

**Confusion with Google Talk "off the record"**[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=8)]

Although Gmail's [Google Talk](https://en.wikipedia.org/wiki/Google_Talk) uses the term "off the record", the feature has no connection to the Off-the-Record Messaging protocol described in this article, its chats are not encrypted in the way described above—and could be logged internally by Google even if not accessible by end-users.[[34]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-GTalk1-34)[[35]](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_note-GTalk2-35)

See also[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=9)]

* [](https://en.wikipedia.org/wiki/File:Free_and_open-source_software_logo_(2009).svg) [Free software portal](https://en.wikipedia.org/wiki/Portal:Free_software)

References[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=10)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-not-pgp_1-0) [***b***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-not-pgp_1-1) [*Nikita Borisov*](https://en.wikipedia.org/wiki/Nikita_Borisov)*,*[*Ian Goldberg*](https://en.wikipedia.org/wiki/Ian_Goldberg)*,*[*Eric Brewer*](https://en.wikipedia.org/wiki/Eric_Brewer_(computer_scientist))*(28 October 2004).*[*"Off-the-Record Communication, or, Why Not To Use PGP"*](https://otr.cypherpunks.ca/otr-wpes.pdf)*(PDF). Workshop on Privacy in the Electronic Society. Retrieved 6 March 2014.*
  2. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-10th-anniversary_2-0) [*Ian Goldberg*](https://en.wikipedia.org/wiki/Ian_Goldberg)*(26 October 2014).*[*[OTR-users] Happy 10th anniversary!*](https://lists.cypherpunks.ca/pipermail/otr-users/2014-October/002515.html)*. Retrieved 27 April 2015.*
  3. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-version-4_3-0) *Sofía Celi, Ola Bini (15 February 2019).*[*"Off-the-Record Messaging Protocol version 4"*](https://github.com/otrv4/otrv4)*.*
  4. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Secure_OTR_4-0) *Mario Di Raimondo; Rosario Gennaro; Hugo Krawczyk (2005).*[*"Secure off-the-record messaging"*](https://www.dmi.unict.it/diraimondo/web/wp-content/uploads/papers/otr.pdf)*(PDF). Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. Association for Computing Machinery: 81–89.*
  5. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-v2_5-0) [*"Off-the-Record Messaging Protocol version 2"*](https://otr.cypherpunks.ca/Protocol-v2-3.1.0.html)*.*
  6. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-6) [*"mod\_otr"*](http://www.ejabberd.im/mod_otr)*.*
  7. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-WPES'07_7-0) *Chris Alexander; Ian Avrum Goldberg (February 2007).*[*Improved User Authentication in Off-The-Record Messaging*](https://cypherpunks.ca/~iang/pubs/impauth.pdf)*(PDF). Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society. New York: Association for Computing Machinery. pp. 41–47.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/1314333.1314340*](https://doi.org/10.1145%2F1314333.1314340)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9781595938831*](https://en.wikipedia.org/wiki/Special:BookSources/9781595938831)*.*
  8. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-v3_8-0) [***b***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-v3_8-1) [*"Off-the-Record Messaging Protocol version 3"*](https://otr.cypherpunks.ca/Protocol-v3-4.0.0.html)*.*
  9. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-BianSekerTopaloglu_9-0) *Jiang Bian; Remzi Seker; Umit Topaloglu (2007).*[*Off-the-Record Instant Messaging for Group Conversation*](https://www.researchgate.net/profile/Remzi_Seker/publication/4272374_Off-the-Record_Instant_Messaging_for_Group_Conversation/links/53fb51d30cf27c365cf09c8a.pdf)*(PDF). IEEE International Conference on Information Reuse and Integration. IEEE.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/IRI.2007.4296601*](https://doi.org/10.1109%2FIRI.2007.4296601)*.*
  10. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-mpOTR_10-0) [***b***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-mpOTR_10-1) *Ian Avrum Goldberg; Berkant Ustaoğlu; Matthew D. Van Gundy; Hao Chen (2009).*[*Multi-party off-the-record messaging*](https://cypherpunks.ca/~iang/pubs/mpotr.pdf)*(PDF). Proceedings of the 16th ACM Computer and Communications Security Conference. Association for Computing Machinery. pp. 358–368.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/1653662.1653705*](https://doi.org/10.1145%2F1653662.1653705)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9781605588940*](https://en.wikipedia.org/wiki/Special:BookSources/9781605588940)*.*
  11. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-SoK_11-0) *Nik Unger; Sergej Dechand; Joseph Bonneau; Sascha Fahl; Henning Perl; Ian Avrum Goldberg; Matthew Smith (2015).*[*"SoK: Secure Messaging"*](http://ieee-security.org/TC/SP2015/papers-archived/6949a232.pdf)*(PDF). Proceedings of the 2015 IEEE Symposium on Security and Privacy. IEEE Computer Society's Technical Committee on Security and Privacy: 232–249.*
  12. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-OMEMO-XEP_12-0) *Straub, Andreas (25 October 2015).*[*"OMEMO Encryption"*](https://web.archive.org/web/20160129003540/https:/xmpp.org/extensions/inbox/omemo.html)*. XMPP Standards Foundation website. Archived from*[*the original*](https://xmpp.org/extensions/inbox/omemo.html)*on 29 January 2016. Retrieved 16 January 2016.*
  13. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-OMEMO-Jingle_13-0) *Gultsch, Daniel (2 September 2015).*[*"OMEMO Encrypted Jingle File Transfer"*](https://xmpp.org/extensions/inbox/omemo-filetransfer.html)*. XMPP Standards Foundation website. Retrieved 16 January 2016.*
  14. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-no-evidence_14-0) *Sofía Celi, Ola Bini (21 July 2018).*[*No evidence of communication: Off-the-Record Protocol version 4*](https://petsymposium.org/2018/files/hotpets/7-bini.pdf)*(PDF). Retrieved 29 November 2018.*
  15. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-multi-party_15-0) *Ian Goldberg (27 May 2009).*[*"multi-party OTR communications? (and other OTR details)"*](http://lists.cypherpunks.ca/pipermail/otr-users/2009-May/001647.html)*. OTR-users mailing list.*
  16. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-mpOTR-Plan_16-0) *Nadim Kobeissi (1 February 2014).*[*"mpOTR Project Plan"*](https://github.com/cryptocat/cryptocat/wiki/mpOTR-Project-Plan)*. Cryptocat wiki on GitHub.*
  17. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-libotr4_17-0) *Ian Goldberg (4 September 2012).*[*"pidgin-otr and libotr 4.0.0 released!"*](https://lists.cypherpunks.ca/pipermail/otr-announce/2012-September/000058.html)*. OTR-announce mailing list.*
  18. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-libotr_license_18-0) [*"Off-the-Record Messaging"*](https://otr.cypherpunks.ca/index.php#faqs)*.*
  19. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-BitlBee_19-0) [*"BitlBee Wiki"*](http://wiki.bitlbee.org/bitlbee-otr)*. Wiki.bitlbee.org. 25 January 2014. Retrieved 15 May 2014.*
  20. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Kadu_20-0) [*"Kadu 1.0 Release Notes"*](https://web.archive.org/web/20161207084931/http:/www.kadu.im/w/English:ReleaseNotes1)*. Archived from*[*the original*](http://www.kadu.im/w/English:ReleaseNotes1)*on 7 December 2016. Retrieved 15 February 2015.*
  21. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-kopete-otr_KDE_21-0) [*"kopete-otr in KDE for 4.1"*](https://web.archive.org/web/20080328080733/http:/kopete-otr.follefuder.org/news.html)*. Archived from*[*the original*](http://kopete-otr.follefuder.org/news.html)*on 28 March 2008.*
  22. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-kopete-otr_review_22-0) [*"kopete-otr review request"*](http://lists.kde.org/?t=120397998900007&r=1&w=2)*.*
  23. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-leechcraft1_23-0) *0xd34df00d.*[*"OTR Plugin"*](https://github.com/0xd34df00d/leechcraft/tree/master/src/plugins/azoth/plugins/otroid)*. Github.com. Retrieved 6 September2017.*
  24. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-leechcraft2_24-0) [*"Short description"*](http://leechcraft.org/plugins-azoth)*. Leechcraft.org. Retrieved 15 May 2014.*
  25. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-MCabber_25-0) [*"source code"*](https://web.archive.org/web/20140517132343/http:/mcabber.com/hg/index.cgi/file/a18e1b488f1c/mcabber/mcabber/otr.c)*. MCabber.com. 25 October 2013. Archived from*[*the original*](http://mcabber.com/hg/index.cgi/file/a18e1b488f1c/mcabber/mcabber/otr.c)*on 17 May 2014. Retrieved 15 May 2014.*
  26. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Psi_26-0) [***b***](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Psi_26-1) [*"OTR Plugin"*](https://github.com/psi-im/plugins/tree/master/generic/otrplugin)*. Github.com. Retrieved 6 September 2017.*
  27. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Psi+_27-0) [*"Psi+ snapshots"*](https://github.com/psi-plus/psi-plus-snapshots/tree/master/plugins/generic/otrplugin)*. Github.com. Retrieved 6 September 2017.*
  28. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Tkabber_28-0) [*"Tkabber OTR Plugin"*](https://web.archive.org/web/20140311093019/https:/svn.xmpp.ru/repos/tkabber/trunk/tkabber-plugins/otr/)*. Archived from*[*the original*](https://svn.xmpp.ru/repos/tkabber/trunk/tkabber-plugins/otr/)*on 11 March 2014.*
  29. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-irssi-xchat_29-0) [*"irssi-otr / xchat-otr plugin"*](http://irssi-otr.tuxfamily.org/)*. 4 February 2019.*
  30. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Miranda_30-0) [*"Miranda OTR Plugin"*](https://code.google.com/p/mirotr/)*.*
  31. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-Pidgin_31-0) [*"OTR plugin for Pidgin"*](https://otr.cypherpunks.ca/#downloads)*.*
  32. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-WeeChat_32-0) [*"OTR plugin for WeeChat"*](https://github.com/mmb/weechat-otr)*. January 2019.*
  33. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-33) [*"TingPing/hexchat-otr"*](https://github.com/TingPing/hexchat-otr)*. GitHub. Retrieved 14 March 2017.*
  34. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-GTalk1_34-0) [*"Chatting off the record - Talk Help"*](https://support.google.com/talk/answer/29291?hl=en)*.*
  35. [**^**](https://en.wikipedia.org/wiki/Off-the-Record_Messaging#cite_ref-GTalk2_35-0) [*"Google Talk - Privacy Policy"*](https://www.google.com/intl/en/policies/privacy/)*.*

Further reading[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=11)]

* *Joseph Bonneau; Andrew Morrison (21 March 2006).*[*"Finite-State Security Analysis of OTR Version 2"*](http://www.jbonneau.com/doc/BM06-OTR_v2_analysis.pdf)*(PDF). Retrieved 5 September 2013.*
* *Mario Di Raimondo; Rosario Gennaro & Hugo Krawczyk (2005).*[*"Secure Off-the-Record Messaging"*](http://www.dmi.unict.it/diraimondo/web/wp-content/uploads/papers/otr.pdf)*(PDF). Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society.*[*Association for Computing Machinery*](https://en.wikipedia.org/wiki/Association_for_Computing_Machinery)*. Retrieved 27 August 2013.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Off-the-Record_Messaging&action=edit&section=12)]

* [Official website](https://otr.cypherpunks.ca/)
* [Protocol specification](https://otr.cypherpunks.ca/Protocol-v3-4.1.1.html)
* [Off-the-Record Messaging: Useful Security and Privacy for IM](https://csclub.uwaterloo.ca/media/Off-the-Record%20Messaging:%20Useful%20Security%20and%20Privacy%20for%20IM.html), talk by [Ian Goldberg](https://en.wikipedia.org/wiki/Ian_Goldberg) at the University of Waterloo (video)
* ['Off-the-Record' Instant Messaging Tutorial (encryption, authentication, deniability, ..)](https://www.youtube.com/watch?v=aV6-s9o9bVw) on [YouTube](https://en.wikipedia.org/wiki/YouTube)