

# Signal Protocol

The **Signal Protocol** (formerly known as the **TextSecure Protocol**) is a non-federated cryptographic protocol that can be used to provide end-to-end encryption for voice calls, video calls,<sup>[3]</sup> and instant messaging conversations.<sup>[2]</sup> The protocol was developed by Open Whisper Systems in 2013<sup>[2]</sup> and was first introduced in the open-source TextSecure app, which later became Signal. Several closed-source applications have implemented the protocol, such as WhatsApp, which is said to encrypt the conversations of "more than a billion people worldwide".<sup>[4]</sup> Facebook Messenger also say they offer the protocol for optional Secret Conversations, as does Skype for its Private Conversations.

The protocol combines the Double Ratchet algorithm, prekeys, and a triple Elliptic-curve Diffie–Hellman (3-DH) handshake,<sup>[5]</sup> and uses Curve25519, AES-256, and HMAC-SHA256 as primitives.<sup>[6]</sup>

## Signal Protocol

### Communication protocol

<b>Purpose</b>	End-to-end encrypted communications
<b>Developer(s)</b>	Signal Technology Foundation
<b>Based on</b>	OTR, SCIMP <sup>[1]</sup>
<b>Influenced</b>	OMEMO, Matrix <sup>[2]</sup>
<b>OSI layer</b>	Application layer
<b>Website</b>	<a href="https://signal.org/docs">signal.org/docs</a> ( <a href="https://signal.org/docs">https://signal.org/docs</a> )

## Contents

### History

### Properties

[Authentication](#)

[Metadata](#)

### Usage

### Influence

### Implementations

### See also

### References

### Literature

### External links

## History

The Signal Protocol's development was started by Trevor Perrin and Moxie Marlinspike (Open Whisper Systems) in 2013. The first version of the protocol, TextSecure v1, was based on Off-the-Record Messaging (OTR).<sup>[7][8]</sup>

On 24 February 2014, Open Whisper Systems introduced TextSecure v2,<sup>[9]</sup> which migrated to the Axolotl Ratchet.<sup>[7][10]</sup> The design of the Axolotl Ratchet is based on the ephemeral key exchange that was introduced by OTR and combines it with a symmetric-key ratchet modeled after the Silent Circle Instant Messaging Protocol (SCIMP).<sup>[1]</sup> 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.<sup>[11]</sup> The Axolotl Ratchet was named after the critically endangered aquatic salamander Axolotl, which has extraordinary self-healing capabilities. The developers refer to the algorithm as self-healing because it automatically disables an attacker from accessing the cleartext of later messages after having compromised a session key.<sup>[1]</sup>

The third version of the protocol, TextSecure v3, made some changes to the cryptographic primitives and the wire protocol.<sup>[7]</sup> In October 2014, researchers from Ruhr University Bochum published an analysis of TextSecure v3.<sup>[6][7]</sup> Among other findings, they presented an unknown key-share attack on the protocol, but in general, they found that it was secure.<sup>[12]</sup>

In March 2016, the developers renamed the protocol as the Signal Protocol. They also renamed the Axolotl Ratchet as the Double Ratchet algorithm to better differentiate between the ratchet and the full protocol<sup>[13]</sup> because some had used the name Axolotl when referring to the full protocol.<sup>[14][13]</sup>

As of October 2016, the Signal Protocol is based on TextSecure v3, but with additional cryptographic changes.<sup>[7]</sup> In October 2016, researchers from the UK's University of Oxford, Australia's Queensland University of Technology, and Canada's McMaster University published a formal analysis of the protocol, concluding that the protocol was cryptographically sound.<sup>[15][16]</sup>

Another audit of the protocol was published in 2017.<sup>[17]</sup>

## Properties

---

The protocol provides confidentiality, integrity, authentication, participant consistency, destination validation, forward secrecy, post-compromise security (aka future secrecy), causality preservation, message unlinkability, message repudiation, participation repudiation, and asynchronicity.<sup>[18]</sup> It does not provide anonymity preservation and requires servers for the relaying of messages and storing of public key material.<sup>[18]</sup>

The Signal Protocol also supports end-to-end encrypted group chats. The group chat protocol is a combination of a pairwise double ratchet and multicast encryption.<sup>[18]</sup> In addition to the properties provided by the one-to-one protocol, the group chat protocol provides speaker consistency, out-of-order resilience, dropped message resilience, computational equality, trust equality, subgroup messaging, as well as contractible and expandable membership.<sup>[18]</sup>

## Authentication

For authentication, users can manually compare public key fingerprints through an outside channel.<sup>[19]</sup> This makes it possible for users to verify each other's identities and avoid a man-in-the-middle attack.<sup>[19]</sup> An implementation can also choose to employ a trust on first use mechanism in order to notify users if a correspondent's key changes.<sup>[19]</sup>

## Metadata

The Signal Protocol does not prevent a company from retaining information about when and with whom users communicate.<sup>[20][21]</sup> There can therefore be differences in how messaging service providers choose to handle this information. Signal's privacy policy states that recipients' identifiers are only kept on the Signal servers as long as necessary in order to transmit each message.<sup>[22]</sup> In June 2016, Moxie Marlinspike told *The Intercept*: "the closest piece of information to metadata that the Signal server stores is the last time each user connected to the server, and the precision of this information is reduced to the day, rather than the hour, minute, and second."<sup>[21]</sup>

In October 2018, Signal Messenger announced that they had implemented a "sealed sender" feature into Signal, which reduces the amount of metadata that the Signal servers have access to by concealing the sender's identifier.<sup>[23][24]</sup> The sender's identity is conveyed to the recipient in each message, but is encrypted with a key that the server does not have.<sup>[24]</sup> This is done automatically if the sender is in the recipient's contacts or has access to their Signal Profile.<sup>[24]</sup> Users can also enable an option to receive "sealed sender" messages from non-contacts and people who do not have access to their Signal Profile.<sup>[24]</sup> A contemporaneous wiretap of the user's device and/or the Signal servers may still reveal that the device's IP address accessed a Signal server to send or receive messages at certain times.<sup>[23]</sup>

## Usage

---

Open Whisper Systems first introduced the protocol in their TextSecure app. They later merged an encrypted voice calling application called RedPhone into the TextSecure app and renamed it as Signal. RedPhone used ZRTP to encrypt its calls. In March 2017, Signal transitioned to a new WebRTC-based<sup>[3]</sup> calling system that also introduced the ability to make video calls.<sup>[25]</sup> Signal's new calling system uses the Signal Protocol for end-to-end encryption.<sup>[3]</sup>

In November 2014, Open Whisper Systems announced a partnership with WhatsApp to provide end-to-end encryption by incorporating the Signal Protocol into each WhatsApp client platform.<sup>[26]</sup> Open Whisper Systems said that they had already incorporated the protocol into the latest WhatsApp client for Android and that support for other clients, group/media messages, and key verification would be coming soon after.<sup>[27]</sup> On April 5, 2016, WhatsApp and Open Whisper Systems announced that they had finished adding end-to-end encryption to "every form of communication" on WhatsApp, and that users could now verify each other's keys.<sup>[28][29]</sup> In February 2017, WhatsApp announced a new feature, WhatsApp Status, which uses the Signal Protocol to secure its contents.<sup>[30]</sup> In October 2016, WhatsApp's parent company Facebook also deployed an optional mode called Secret Conversations in Facebook Messenger which provides end-to-end encryption using an implementation of the Signal Protocol.<sup>[31][32][33][34]</sup>

In September 2015, G Data Software launched a new messaging app called Secure Chat which used the Signal Protocol.<sup>[35][36]</sup> G Data discontinued the service in May 2018.<sup>[37]</sup>

In September 2016, Google launched a new messaging app called Allo, which featured an optional Incognito Mode that used the Signal Protocol for end-to-end encryption.<sup>[38][39]</sup> In March 2019, Google discontinued Allo in favor of their Messages app on Android.<sup>[40][41]</sup> In November 2020, Google announced that they would be using the Signal Protocol to provide end-to-end encryption by default to all RCS-based conversations between users of their Messages app, starting with one-to-one conversations.<sup>[42][43]</sup>

In January 2018, Open Whisper Systems and Microsoft announced the addition of Signal Protocol support to an optional Skype mode called Private Conversations.<sup>[44][45]</sup>

## Influence

---

The Signal Protocol has had an influence on other cryptographic protocols. In May 2016, Viber said that their encryption protocol is a custom implementation that "uses the same concepts" as the Signal Protocol.<sup>[46][47]</sup> Forsta's developers have said that their app uses a custom implementation of the Signal Protocol.<sup>[48][49]</sup>

The Double Ratchet algorithm that was introduced as part of the Signal Protocol has also been adopted by other protocols. OMEMO is an XMPP Extension Protocol (XEP) that was introduced in the Conversations messaging app and approved by the XMPP Standards Foundation (XSF) in December 2016 as XEP-0384.<sup>[50][2]</sup> Matrix is an open communications protocol that includes Olm, a library that provides for optional

end-to-end encryption on a room-by-room basis via a Double Ratchet algorithm implementation.<sup>[2]</sup> The developers of Wire have said that their app uses a custom implementation of the Double Ratchet algorithm.<sup>[51][52][53]</sup>

## Implementations

---

Signal Messenger maintains the following Signal Protocol libraries under the GPLv3 license on GitHub:

- libsignal-protocol-c (<https://github.com/signalapp/libsignal-protocol-c>): A library written in C with additional licensing permissions for Apple's App Store.
- libsignal-protocol-java (<https://github.com/signalapp/libsignal-protocol-java>): A library written in Java.
- libsignal-protocol-javascript (<https://github.com/signalapp/libsignal-protocol-javascript>): A library written in JavaScript.

There also exist alternative libraries written by third-parties in other languages, such as TypeScript.<sup>[54]</sup>

## See also

---

- Comparison of instant messaging protocols
- Comparison of cryptography libraries

## References

---

1. Marlinspike, Moxie (26 November 2013). "Advanced cryptographic ratcheting" (<https://whispersystems.org/blog/advanced-ratcheting/>). *Signal Blog*. Open Whisper Systems. Archived (<https://web.archive.org/web/20170324070200/https://whispersystems.org/blog/advanced-ratcheting/>) from the original on 24 March 2017. Retrieved 23 September 2016.
2. Ermoshina, Ksenia; Musiani, Francesca; Halpin, Harry (September 2016). "End-to-End Encrypted Messaging Protocols: An Overview". In Bagnoli, Franco; et al. (eds.). *Internet Science*. INSCI 2016. Florence, Italy: Springer. pp. 244–254. doi:10.1007/978-3-319-45982-0\_22 ([https://doi.org/10.1007%2F978-3-319-45982-0\\_22](https://doi.org/10.1007%2F978-3-319-45982-0_22)). ISBN 978-3-319-45982-0.
3. Marlinspike, Moxie (14 February 2017). "Video calls for Signal now in public beta" (<https://whispersystems.org/blog/signal-video-calls-beta/>). *Signal Blog*. Open Whisper Systems. Archived (<https://web.archive.org/web/20170315184106/https://whispersystems.org/blog/signal-video-calls-beta/>) from the original on 15 March 2017. Retrieved 7 April 2017.
4. "WhatsApp's Signal Protocol integration is now complete" (<https://signal.org/blog/whatsapp-complete/>). *Signal*. Signal Blog. 2016. Archived (<https://web.archive.org/web/20210129090529/https://signal.org/blog/whatsapp-complete/>) from the original on 29 January 2021. Retrieved 5 April 2016.
5. Unger et al. 2015, p. 241
6. Frosch et al. 2016
7. Cohn-Gordon et al. 2016, p. 2
8. "Protocol" (<https://web.archive.org/web/20150107094950/https://github.com/WhisperSystems/TextSecure/wiki/Protocol>). Open Whisper Systems. 2 March 2014. Archived from the original (<https://github.com/WhisperSystems/TextSecure/wiki/Protocol>) on 7 January 2015. Retrieved 28 October 2016 – via GitHub.

9. Donohue, Brian (24 February 2014). "TextSecure Sheds SMS in Latest Version" (<https://threatpost.com/textsecure-sheds-sms-in-latest-version/104456>). *Threatpost*. Archived (<https://web.archive.org/web/20170215020451/https://threatpost.com/textsecure-sheds-sms-in-latest-version/104456/>) from the original on 15 February 2017. Retrieved 14 July 2016.
10. "ProtocolV2" (<https://web.archive.org/web/20141015215356/https://github.com/WhisperSystems/TextSecure/wiki/ProtocolV2>). Open Whisper Systems. 2 March 2014. Archived from the original (<https://github.com/WhisperSystems/TextSecure/wiki/ProtocolV2>) on 15 October 2014. Retrieved 28 October 2016 – via [GitHub](#).
11. Unger et al. 2015
12. Pauli, Darren (3 November 2014). "Auditors find encrypted chat client TextSecure is secure" ([https://www.theregister.co.uk/2014/11/03/how\\_secure\\_is\\_textsecure\\_pretty\\_well\\_secure/](https://www.theregister.co.uk/2014/11/03/how_secure_is_textsecure_pretty_well_secure/)). *The Register*. Archived ([https://web.archive.org/web/20141104060458/http://www.theregister.co.uk/2014/11/03/how\\_secure\\_is\\_textsecure\\_pretty\\_well\\_secure/](https://web.archive.org/web/20141104060458/http://www.theregister.co.uk/2014/11/03/how_secure_is_textsecure_pretty_well_secure/)) from the original on 4 November 2014. Retrieved 4 November 2014.
13. Marlinspike, Moxie (30 March 2016). "Signal on the outside, Signal on the inside" (<https://whispersystems.org/blog/signal-inside-and-out/>). *Signal Blog*. Open Whisper Systems. Archived (<https://web.archive.org/web/20161228221122/https://whispersystems.org/blog/signal-inside-and-out/>) from the original on 28 December 2016. Retrieved 9 April 2016.
14. Cohn-Gordon et al. 2016, p. 1
15. Brook, Chris (10 November 2016). "Signal Audit Reveals Protocol Cryptographically Sound" (<https://threatpost.com/signal-audit-reveals-protocol-cryptographically-sound/121892/>). *Threatpost*. Kaspersky Lab. Archived (<https://web.archive.org/web/20170214222434/https://threatpost.com/signal-audit-reveals-protocol-cryptographically-sound/121892/>) from the original on 14 February 2017. Retrieved 11 November 2016.
16. Cohn-Gordon et al. 2016
17. N. Kobeissi; K. Bhargavan; B. Blanchet (2017). "Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach". *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (<https://hal.inria.fr/hal-01575923/file/KobeissiBhargavanBlanchetEuroSP17.pdf>) (PDF). pp. 435–450. doi:10.1109/EuroSP.2017.38 (<https://doi.org/10.1109%2FEuroSP.2017.38>). ISBN 978-1-5090-5762-7. S2CID 6717546 (<https://api.semanticscholar.org/CorpusID:6717546>). Archived (<https://web.archive.org/web/20180724132029/https://hal.inria.fr/hal-01575923/file/KobeissiBhargavanBlanchetEuroSP17.pdf>) (PDF) from the original on 24 July 2018. Retrieved 29 August 2020.
18. Unger et al. 2015, p. 239
19. Rottermann et al. 2015, p. 5
20. Rottermann et al. 2015, p. 4
21. Lee, Micah (22 June 2016). "Battle of the Secure Messaging Apps: How Signal Beats WhatsApp" (<https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>). *The Intercept*. Archived (<https://web.archive.org/web/20170219051224/https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>) from the original on 19 February 2017. Retrieved 8 October 2016.
22. "Privacy Policy" (<https://whispersystems.org/signal/privacy/>). Open Whisper Systems. n.d. Archived (<https://web.archive.org/web/20170429003356/https://whispersystems.org/signal/privacy/>) from the original on 29 April 2017. Retrieved 8 October 2016.
23. Dan Goodin (30 October 2018). "New Signal privacy feature removes sender ID from metadata" (<https://arstechnica.com/information-technology/2018/10/new-signal-privacy-feature-removes-sender-id-from-metadata/>). *Ars Technica*. Archived (<https://web.archive.org/web/20190328071235/https://arstechnica.com/information-technology/2018/10/new-signal-privacy-feature-removes-sender-id-from-metadata/>) from the original on 28 March 2019. Retrieved 28 March 2019.

24. Lund, Joshua (29 October 2018). "Technology preview: Sealed sender for Signal" (<https://signal.org/blog/sealed-sender/>). *signal.org*. Signal Messenger. Archived (<https://web.archive.org/web/20181124093525/https://signal.org/blog/sealed-sender/>) from the original on 24 November 2018. Retrieved 16 April 2019.
25. Marlinspike, Moxie (13 March 2017). "Video calls for Signal out of beta" (<https://whispersystems.org/blog/signal-video-calls/>). *Signal Blog*. Open Whisper Systems. Archived (<https://web.archive.org/web/20170315175109/https://whispersystems.org/blog/signal-video-calls/>) from the original on 15 March 2017. Retrieved 7 April 2017.
26. Evans, Jon (18 November 2014). "WhatsApp Partners With Open Whisper Systems To End-To-End Encrypt Billions Of Messages A Day" (<https://techcrunch.com/2014/11/18/end-to-end-for-everyone/>). *TechCrunch*. Archived (<https://web.archive.org/web/20141118220338/http://techcrunch.com/2014/11/18/end-to-end-for-everyone/>) from the original on 18 November 2014. Retrieved 14 March 2016.
27. Marlinspike, Moxie (18 November 2014). "Open Whisper Systems partners with WhatsApp to provide end-to-end encryption" (<https://whispersystems.org/blog/whatsapp/>). Open Whisper Systems. Archived (<https://web.archive.org/web/20141118161936/https://www.whispersystems.org/blog/whatsapp/>) from the original on 18 November 2014. Retrieved 14 March 2016.
28. Metz, Cade (5 April 2016). "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People" (<https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/>). *Wired*. Archived (<https://web.archive.org/web/20160405164942/http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/>) from the original on 5 April 2016. Retrieved 5 April 2016.
29. Lomas, Natasha (5 April 2016). "WhatsApp completes end-to-end encryption rollout" (<https://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/>). *TechCrunch*. Archived (<https://web.archive.org/web/20160406010346/http://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/>) from the original on 6 April 2016. Retrieved 5 April 2016.
30. "WhatsApp Status" (<https://blog.whatsapp.com/10000630/WhatsApp-Status>). *WhatsApp*. Facebook. 20 February 2017. Archived (<https://web.archive.org/web/20170223061647/http://blog.whatsapp.com/10000630/WhatsApp-Status>) from the original on 23 February 2017. Retrieved 23 February 2017.
31. Isaac, Mike (8 July 2016). "Facebook to Add 'Secret Conversations' to Messenger App" (<https://www.nytimes.com/2016/07/09/technology/facebook-messenger-app-encryption.html>). *The New York Times*. Archived (<https://web.archive.org/web/20160712043038/http://www.nytimes.com/2016/07/09/technology/facebook-messenger-app-encryption.html>) from the original on 12 July 2016. Retrieved 12 July 2016.
32. "Messenger Starts Testing End-to-End Encryption with Secret Conversations" (<https://newsroom.fb.com/news/2016/07/messenger-starts-testing-end-to-end-encryption-with-secret-conversations/>). Facebook. 8 July 2016. Archived (<https://web.archive.org/web/20180112214633/https://newsroom.fb.com/news/2016/07/messenger-starts-testing-end-to-end-encryption-with-secret-conversations/>) from the original on 12 January 2018. Retrieved 11 January 2018.
33. Greenberg, Andy (8 July 2016). "'Secret Conversations:' End-to-End Encryption Comes to Facebook Messenger" (<https://www.wired.com/2016/07/secret-conversations-end-end-encryption-facebook-messenger-arrived/>). *Wired*. Archived (<https://web.archive.org/web/20160711073318/https://www.wired.com/2016/07/secret-conversations-end-end-encryption-facebook-messenger-arrived/>) from the original on 11 July 2016. Retrieved 12 July 2016.
34. Greenberg, Andy (4 October 2016). "You Can All Finally Encrypt Facebook Messenger, So Do It" (<https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/>). *Wired*. Archived (<https://web.archive.org/web/20170415004558/https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/>) from the original on 15 April 2017. Retrieved 5 October 2016.

35. Seals, Tara (17 September 2015). "G DATA Adds Encryption for Secure Mobile Chat" (<https://www.infosecurity-magazine.com/news/g-data-adds-encryption-for-secure/>). *Infosecurity Magazine*. Archived (<https://web.archive.org/web/20160722065627/http://www.infosecurity-magazine.com/news/g-data-adds-encryption-for-secure/>) from the original on 22 July 2016. Retrieved 14 July 2016.
36. "SecureChat" (<https://github.com/GDATASoftwareAG/SecureChat>). G Data. Archived (<https://web.archive.org/web/20170507135213/https://github.com/GDATASoftwareAG/SecureChat>) from the original on 7 May 2017. Retrieved 14 July 2016 – via [GitHub](#).
37. "G DATA Secure Chat wird eingestellt" (<https://www.gdata.de/support/faq/consumer/g-data-secure-chat-wird-eingestellt>) (in German). G DATA Software AG. 18 May 2018. Archived (<https://web.archive.org/web/20190426093244/https://www.gdata.de/support/faq/consumer/g-data-secure-chat-wird-eingestellt>) from the original on 26 April 2019. Retrieved 26 April 2019.
38. Greenberg, Andy (18 May 2016). "With Allo and Duo, Google Finally Encrypts Conversations End-to-End" (<https://www.wired.com/2016/05/allo-duo-google-finally-encrypts-conversations-end-end/>). *Wired*. Archived (<https://web.archive.org/web/20170202161556/https://www.wired.com/2016/05/allo-duo-google-finally-encrypts-conversations-end-end/>) from the original on 2 February 2017. Retrieved 18 May 2016.
39. Gibbs, Samuel (21 September 2016). "Google launches WhatsApp competitor Allo – with Google Assistant" (<https://www.theguardian.com/technology/2016/sep/21/google-whatsapp-all-o-google-assistant>). *The Guardian*. Archived (<https://web.archive.org/web/20190107054254/https://www.theguardian.com/technology/2016/sep/21/google-whatsapp-allo-google-assistant>) from the original on 7 January 2019. Retrieved 21 September 2016.
40. Porter, Jon (12 March 2019). "Google is finally saying goodbye to Allo today" (<https://www.theverge.com/2019/3/12/18261932/google-allo-messaging-app-shutting-down-march-12th-2019>). *The Verge*. Vox Media. Archived (<https://web.archive.org/web/20190312221640/https://www.theverge.com/2019/3/12/18261932/google-allo-messaging-app-shutting-down-march-12th-2019>) from the original on 12 March 2019. Retrieved 26 April 2019.
41. Klainer, Matt (5 December 2018). "The latest on Messages, Allo, Duo and Hangouts" (<https://www.blog.google/products/messages/latest-messages-allo-duo-and-hangouts/>). Archived (<https://web.archive.org/web/20190413210055/https://www.blog.google/products/messages/latest-messages-allo-duo-and-hangouts/>) from the original on 13 April 2019. Retrieved 26 April 2019.
42. Bohn, Dieter (19 November 2020). "Google is rolling out end-to-end encryption for RCS in Android Messages beta" (<https://www.theverge.com/platform/amp/2020/11/19/21574451/android-rcs-encryption-message-end-to-end-beta>). *The Verge*. Vox Media, Inc. Retrieved 28 November 2020.
43. Omara, Emad (November 2020). "Messages End-to-End Encryption Overview" ([https://www.gstatic.com/messages/papers/messages\\_e2ee.pdf](https://www.gstatic.com/messages/papers/messages_e2ee.pdf)) (PDF). *gstatic.com*. Google. Retrieved 28 November 2020.
44. Newman, Lily Hay (11 January 2018). "Skype's Rolling Out End-to-End Encryption For Hundreds of Millions of People" (<https://www.wired.com/story/skype-end-to-end-encryption-voice-text/>). *Wired*. Archived (<https://web.archive.org/web/20180112215711/https://www.wired.com/story/skype-end-to-end-encryption-voice-text/>) from the original on 12 January 2018. Retrieved 13 January 2018.
45. Lund, Joshua (11 January 2018). "Signal partners with Microsoft to bring end-to-end encryption to Skype" (<https://signal.org/blog/skype-partnership/>). *Signal Blog*. Open Whisper Systems. Archived (<https://web.archive.org/web/20200202152037/https://signal.org/blog/skype-partnership/>) from the original on 2 February 2020. Retrieved 13 January 2018.
46. "Viber Encryption Overview" (<https://web.archive.org/web/20160711035838/http://www.viber.com/en/security-overview>). Viber. 3 May 2016. Archived from the original (<https://www.viber.com/en/security-overview>) on 11 July 2016. Retrieved 8 July 2017.



47. Eyal, Ofir (3 May 2016). "Canada, Germany and Australia are getting e2e encryption" (<https://www.viber.com/en/blog/2016-05-03/canada-germany-and-australia-are-getting-e2e-encryption>). Viber. Archived (<https://web.archive.org/web/20161005083000/http://www.viber.com/en/blog/2016-05-03/canada-germany-and-australia-are-getting-e2e-encryption>) from the original on 5 October 2016. Retrieved 9 October 2016.
48. u/tooker. "r/crypto - Forsta - Signal based messaging platform for enterprises" ([https://www.reddit.com/r/crypto/comments/8b1m6n/forsta\\_signal\\_based\\_messaging\\_platform\\_for/](https://www.reddit.com/r/crypto/comments/8b1m6n/forsta_signal_based_messaging_platform_for/)). *reddit*. Archived ([https://web.archive.org/web/20180502045526/https://www.reddit.com/r/crypto/comments/8b1m6n/forsta\\_signal\\_based\\_messaging\\_platform\\_for/](https://web.archive.org/web/20180502045526/https://www.reddit.com/r/crypto/comments/8b1m6n/forsta_signal_based_messaging_platform_for/)) from the original on 2 May 2018. Retrieved 6 February 2019.
49. "ForstaLabs/libsignal-node" (<https://github.com/ForstaLabs/libsignal-node>). *GitHub*. Forsta Inc. 3 February 2019. Archived (<https://web.archive.org/web/20180613054634/https://github.com/ForstaLabs/libsignal-node>) from the original on 13 June 2018. Retrieved 6 February 2019.
50. Andreas Straub (7 December 2016). "XEP-0384: OMEMO Encryption" (<https://xmpp.org/extensions/xep-0384.html>). *XMPP Standards Foundation website*. Archived (<https://web.archive.org/web/20170225060620/https://xmpp.org/extensions/xep-0384.html>) from the original on 25 February 2017. Retrieved 28 April 2017.
51. "Add attribution" (<https://github.com/wireapp/proteus/blob/develop/src/internal/session.rs#L2>). *GitHub*. Wire Swiss GmbH. 9 May 2016. Archived (<https://web.archive.org/web/20170507135204/https://github.com/wireapp/proteus/blob/develop/src/internal/session.rs#L2>) from the original on 7 May 2017. Retrieved 9 October 2016.
52. "Wire Security Whitepaper" (<https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf>) (PDF). Wire Swiss GmbH. 3 March 2016. Archived (<https://web.archive.org/web/20180910220210/https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf>) (PDF) from the original on 10 September 2018. Retrieved 7 February 2019.
53. Lomas, Natasha (16 December 2016). "Encrypted messaging app Wire adds usernames so you can limit what you share with contacts" (<https://techcrunch.com/2016/12/16/encrypted-messaging-app-wire-adds-usernames-so-you-can-limit-what-you-share-with-contacts/>). *TechCrunch*. Verizon Media. Archived (<https://web.archive.org/web/20190209180036/https://techcrunch.com/2016/12/16/encrypted-messaging-app-wire-adds-usernames-so-you-can-limit-what-you-share-with-contacts/>) from the original on 9 February 2019. Retrieved 8 February 2019.
54. Privacy Research, LLC. "libsignal-protocol-typescript" (<https://github.com/privacyresearchgroup/libsignal-protocol-typescript>). *github.com*. Retrieved 28 November 2020.

## Literature

---


- Cohn-Gordon, Katriel; Cremers, Cas; Dowling, Benjamin; Garratt, Luke; Stebila, Douglas (25 October 2016). "A Formal Security Analysis of the Signal Messaging Protocol" (<https://eprint.iacr.org/2016/1013>). *Cryptology ePrint Archive*. International Association for Cryptologic Research (IACR). Archived (<https://web.archive.org/web/20161228222451/http://eprint.iacr.org/2016/1013>) from the original on 28 December 2016. Retrieved 27 October 2016.
- Ermoshina, Ksenia; Musiani, Francesca; Halpin, Harry (September 2016). "End-to-End Encrypted Messaging Protocols: An Overview". In Bagnoli, Franco; et al. (eds.). *Internet Science*. INSCI 2016. Florence, Italy: Springer. pp. 244–254. doi:10.1007/978-3-319-45982-0\_22 ([https://doi.org/10.1007%2F978-3-319-45982-0\\_22](https://doi.org/10.1007%2F978-3-319-45982-0_22)). ISBN 978-3-319-45982-0.
- Frosch, Tilman; Mainka, Christian; Bader, Christoph; Bergsma, Florian; Schwenk, Jörg; Holz, Thorsten (March 2016). *How Secure is TextSecure?*. 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrücken, Germany: IEEE. pp. 457–472. doi:10.1109/EuroSP.2016.41 (<https://doi.org/10.1109%2FEuroSP.2016.41>). ISBN 978-1-5090-1752-2.



- Rottermanner, Christoph; Kieseberg, Peter; Huber, Markus; Schmiedecker, Martin; Schrittwieser, Sebastian (December 2015). *Privacy and Data Protection in Smartphone Messengers* ([https://www.sba-research.org/wp-content/uploads/publications/paper\\_drafthp.pdf](https://www.sba-research.org/wp-content/uploads/publications/paper_drafthp.pdf)) (PDF). Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services (iiWAS2015). ACM International Conference Proceedings Series. ISBN 978-1-4503-3491-4. Archived ([https://web.archive.org/web/20160327011416/http://www.sba-research.org/wp-content/uploads/publications/paper\\_drafthp.pdf](https://web.archive.org/web/20160327011416/http://www.sba-research.org/wp-content/uploads/publications/paper_drafthp.pdf)) (PDF) from the original on 27 March 2016. Retrieved 25 September 2016.
- Unger, Nik; Dechand, Sergej; Bonneau, Joseph; Fahl, Sascha; Perl, Henning; Goldberg, Ian Avrum; Smith, Matthew (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. pp. 232–249. doi:10.1109/SP.2015.22 (<https://doi.org/10.1109%2FSP.2015.22>). Archived (<https://web.archive.org/web/20160304002758/http://ieee-security.org/TC/SP2015/papers-archived/6949a232.pdf>) (PDF) from the original on 4 March 2016. Retrieved 23 September 2016.
- Rösler, Paul; Mainka, Christian; Schwenk, Jörg (2017). *More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema* (<https://eprint.iacr.org/2017/713>). *Cryptology ePrint Archive*. International Association for Cryptologic Research (IACR). Archived (<https://web.archive.org/web/20190203132148/https://eprint.iacr.org/2017/713>) from the original on 3 February 2019. Retrieved 26 June 2019.

## External links

---

- [Official website](https://signal.org/docs) (<https://signal.org/docs>) 
  - "TextSecure Protocol: Present and Future" (<https://www.youtube.com/watch?v=7WnwSovjYMs>), talk by Trevor Perrin at NorthSec 2015 (video)
- 

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Signal\\_Protocol&oldid=1003529878](https://en.wikipedia.org/w/index.php?title=Signal_Protocol&oldid=1003529878)"

---

This page was last edited on 29 January 2021, at 12:45 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.