

Protocollo Signal

Elena Tonini, Matr.727382

Università degli Studi di Brescia

A.A. 2021/2022

2022-04-29

SIGNAL

Protocollo Signal

Elena Tonini, Matr.727382

Università degli Studi di Brescia

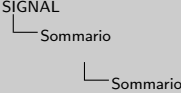
A.A. 2021/2022

Sommario I

- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp VS Telegram
- 5 Bibliografia

- 1. Sommario
- 2. Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3. Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4. Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp VS Telegram
- 5. Bibliografia

2022-04-29



- Sommario I
- 1. Sommario
- 2. Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3. Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4. Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp VS Telegram
- 5. Bibliografia

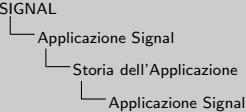
Applicazione Signal

Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.

2022-04-29



Applicazione Signal
Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.

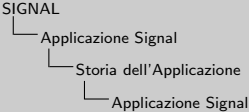
Applicazione Signal

Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.

2022-04-29



Applicazione Signal
Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.

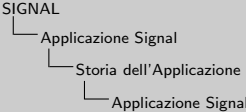
Applicazione Signal

Storia dell'Applicazione

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal.

Nel 2013 Marlinspike fonda il progetto open-source **Open Whisper Systems**, grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come applicazione Chrome), per poi rilasciarlo anche per Windows, Mac e Linux nel 2017.

2022-04-29



Nel 2011 Twitter acquista Whisper Systems e Marlinspike diventa capo della cybersecurity del social media. Nel 2013 Marlinspike abbandona Twitter e fonda la OWS.

Nello stesso anno inizia a lavorare al protocollo Signal insieme al fondatore di WhatsApp Trevor Perrin.

Applicazione Signal
Storia dell'Applicazione

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal.

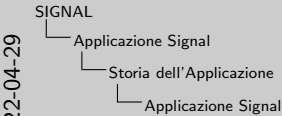
Nel 2013 Marlinspike fonda il progetto open-source Open Whisper Systems, grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come applicazione Chrome), per poi rilasciarlo anche per Windows, Mac e Linux nel 2017.

Applicazione Signal

Storia dell'Applicazione

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal.

Nel 2013 Marlinspike fonda il progetto open-source **Open Whisper Systems**, grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come applicazione Chrome), per poi rilasciarlo anche per Windows, Mac e Linux nel 2017.



Nel 2011 Twitter acquista Whisper Systems e Marlinspike diventa capo della cybersecurity del social media. Nel 2013 Marlinspike abbandona Twitter e fonda la OWS.

Nello stesso anno inizia a lavorare al protocollo Signal insieme al fondatore di WhatsApp Trevor Perrin.

Applicazione Signal
Storia dell'Applicazione

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal.

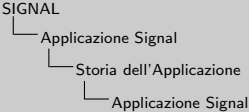
Nel 2013 Marlinspike fonda il progetto open-source **Open Whisper Systems**, grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come applicazione Chrome), per poi rilasciarlo anche per Windows, Mac e Linux nel 2017.

Applicazione Signal

Storia dell'Applicazione

Nel febbraio 2018 Marlinspike e il co-fondatore di WhatsApp Brian Acton fondarono la **Signal Foundation**, il cui obiettivo è il supporto e l'accelerazione della diffusione della comunicazione privata e sicura. [1]

2022-04-29



1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Applicazione Signal

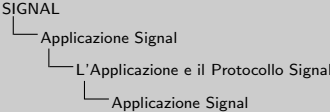
L'Applicazione e il Protocollo Signal

Nel 2013, dopo la fondazione di OWS, i fondatori Marlinspike e Trevor Perrin iniziarono a lavorare al **Protocollo Signal**.

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione implementabile anche da altri servizi.

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.

2022-04-29



Applicazione Signal
L'Applicazione e il Protocollo Signal

Nel 2013, dopo la fondazione di OWS, i fondatori Marlinspike e Trevor Perrin iniziarono a lavorare al **Protocollo Signal**.

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione implementabile anche da altri servizi.

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.

Applicazione Signal

L'Applicazione e il Protocollo Signal

Nel 2013, dopo la fondazione di OWS, i fondatori Marlinspike e Trevor Perrin iniziarono a lavorare al **Protocollo Signal**.

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione implementabile anche da altri servizi.

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.



Applicazione Signal
L'Applicazione e il Protocollo Signal

Nel 2013, dopo la fondazione di OWS, i fondatori Marlinspike e Trevor Perrin iniziarono a lavorare al **Protocollo Signal**.

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione implementabile anche da altri servizi.

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.

Applicazione Signal

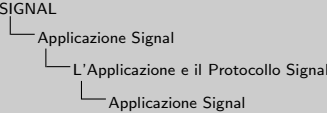
L'Applicazione e il Protocollo Signal

Nel 2013, dopo la fondazione di OWS, i fondatori Marlinspike e Trevor Perrin iniziarono a lavorare al **Protocollo Signal**.

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione implementabile anche da altri servizi.

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.

2022-04-29



Applicazione Signal

L'Applicazione e il Protocollo Signal

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

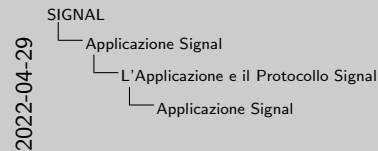
Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Tra le più note implementazioni (parziali) del protocollo troviamo:

- **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- **Duo:** protezione delle videochat
- **Skype:** conversazioni private dal 2018
- **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]



- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

Applicazione Signal
L'Applicazione e il Protocollo Signal

Tra le più note implementazioni (parziali) del protocollo troviamo:

- Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
- Allo: rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- Duo: protezione delle videochat
- Skype: conversazioni private dal 2018
- WhatsApp: tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]

Applicazione Signal

L'Applicazione e il Protocollo Signal

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

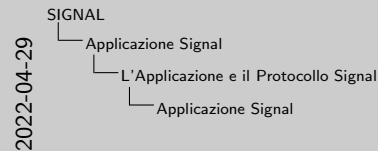
Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Tra le più note implementazioni (parziali) del protocollo troviamo:

- **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- **Duo:** protezione delle videochat
- **Skype:** conversazioni private dal 2018
- **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]



- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

Applicazione Signal
L'Applicazione e il Protocollo Signal

Tra le più note implementazioni (parziali) del protocollo troviamo:

- **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- **Duo:** protezione delle videochat
- **Skype:** conversazioni private dal 2018
- **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]

Applicazione Signal

L'Applicazione e il Protocollo Signal

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ▶ **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- ▶ **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- ▶ **Duo:** protezione delle videochat
- ▶ **Skype:** conversazioni private dal 2018
- ▶ **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]



- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

Applicazione Signal
L'Applicazione e il Protocollo Signal

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ▶ **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- ▶ **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- ▶ **Duo:** protezione delle videochat
- ▶ **Skype:** conversazioni private dal 2018
- ▶ **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]

Applicazione Signal

L'Applicazione e il Protocollo Signal

- Tra le più note implementazioni (parziali) del protocollo troviamo:
- **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
 - **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
 - **Duo:** protezione delle videochat
 - **Skype:** conversazioni private dal 2018
 - **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]



- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

Applicazione Signal

L'Applicazione e il Protocollo Signal

Tra le più note implementazioni (parziali) del protocollo troviamo:

- **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- **Duo:** protezione delle videochat
- **Skype:** conversazioni private dal 2018

« WhatsApp » tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]

Applicazione Signal

L'Applicazione e il Protocollo Signal

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ▶ **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- ▶ **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- ▶ **Duo:** protezione delle videochat
- ▶ **Skype:** conversazioni private dal 2018
- ▶ **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]



- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

Applicazione Signal
L'Applicazione e il Protocollo Signal

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ▶ **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- ▶ **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- ▶ **Duo:** protezione delle videochat
- ▶ **Skype:** conversazioni private dal 2018

» WhatsApp: tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]

Applicazione Signal

L'Applicazione e il Protocollo Signal

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ▶ **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- ▶ **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- ▶ **Duo:** protezione delle videochat
- ▶ **Skype:** conversazioni private dal 2018
- ▶ **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]



- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

Applicazione Signal
L'Applicazione e il Protocollo Signal

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ▶ **Facebook:** introdusse la feature *Secret Conversations* per gli utenti di Facebook Messenger nel luglio 2016
- ▶ **Allo:** rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- ▶ **Duo:** protezione delle videochat
- ▶ **Skype:** conversazioni private dal 2018
- ▶ **WhatsApp:** tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[2], [1]

Applicazione Signal

L'Applicazione e il Protocollo Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

Inoltre, conversazioni già avvenute non possono essere protette applicando il protocollo ex post.
[3]



La dichiarazione delle conversazioni come “private” avviene in genere per selezione esplicita da parte dell'utente e non di default.

WhatsApp implementa automaticamente la crittografia end-to-end sia per le chat private che per quelle di gruppo, tuttavia se si vuole verificare che le conversazioni siano private è necessario che entrambe le persone che partecipano alla conversazione selezionino la chat di interesse, clicchino sul nome del contatto, selezionino l'opzione “Crittografia” e scannerizzino il codice QR che viene presentato sul dispositivo dell'altro utente oppure confrontino i numeri a 60 cifre presentati.

Applicazione Signal
L'Applicazione e il Protocollo Signal

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

Inoltre, conversazioni già avvenute non possono essere protette applicando il protocollo ex post.
[3]

Applicazione Signal

L'Applicazione e il Protocollo Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

Inoltre, conversazioni già avvenute non possono essere protette applicando il protocollo ex post.
[3]



La dichiarazione delle conversazioni come “private” avviene in genere per selezione esplicita da parte dell'utente e non di default.

WhatsApp implementa automaticamente la crittografia end-to-end sia per le chat private che per quelle di gruppo, tuttavia se si vuole verificare che le conversazioni siano private è necessario che entrambe le persone che partecipano alla conversazione selezionino la chat di interesse, clicchino sul nome del contatto, selezionino l'opzione “Crittografia” e scannerizzino il codice QR che viene presentato sul dispositivo dell'altro utente oppure confrontino i numeri a 60 cifre presentati.

Applicazione Signal
L'Applicazione e il Protocollo Signal

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

Inoltre, conversazioni già avvenute non possono essere protette applicando il protocollo ex post.
[3]

Applicazione Signal

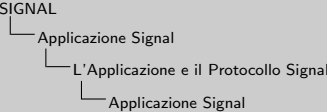
L'Applicazione e il Protocollo Signal

La sicurezza garantita dall'implementazione del protocollo è relativa al fatto che tutti i prodotti OWS sono incentrati sulla privacy degli utenti, infatti:

- ▶ Salvano solo le informazioni strettamente necessarie
- ▶ Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra gli utenti (grazie alla crittografia end-to-end)

[1]

2022-04-29



Applicazione Signal
L'Applicazione e il Protocollo Signal

La sicurezza garantita dall'implementazione del protocollo è relativa al fatto che tutti i prodotti OWS sono incentrati sulla privacy degli utenti, infatti:
▶ Salvano solo le informazioni strettamente necessarie
▶ Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra gli utenti (grazie alla crittografia end-to-end)
[1]

Applicazione Signal

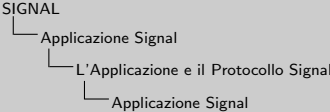
L'Applicazione e il Protocollo Signal

La sicurezza garantita dall'implementazione del protocollo è relativa al fatto che tutti i prodotti OWS sono incentrati sulla privacy degli utenti, infatti:

- ▶ Salvano solo le informazioni strettamente necessarie
- ▶ Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra gli utenti (grazie alla crittografia end-to-end)

[1]

2022-04-29



Applicazione Signal
L'Applicazione e il Protocollo Signal

La sicurezza garantita dall'implementazione del protocollo è relativa al fatto che tutti i prodotti OWS sono incentrati sulla privacy degli utenti, infatti:

- ▶ Salvano solo le informazioni strettamente necessarie
- ▶ Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra gli utenti (grazie alla crittografia end-to-end)

[1]

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

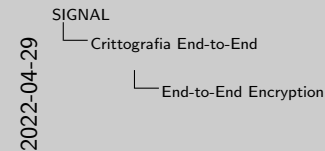
3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia



End-to-End Encryption

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come *plaintext*.

In linea di massima E2EE garantisce che potenziali *eavesdroppers* non possano accedere alle chiavi necessarie per decifrare la conversazione. [4]

Dati protetti da crittografia sono tali per cui solamente le persone autorizzate possono leggerne il contenuto in chiaro, mentre per tutti gli altri utenti si tratta di dati presentati in un formato non leggibile.

Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione, gli Internet provider e utenti malevoli.

La E2EE si assicura inoltre che le comunicazioni tra due endpoint siano sicure.

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come *plaintext*.

In linea di massima E2EE garantisce che potenziali *eavesdroppers* non possano accedere alle chiavi necessarie per decifrare la conversazione. [4]

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

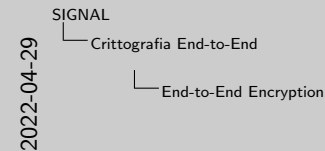
3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia



End-to-End Encryption

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come *plaintext*.

In linea di massima E2EE garantisce che potenziali *eavesdroppers* non possano accedere alle chiavi necessarie per decifrare la conversazione. [4]

Dati protetti da crittografia sono tali per cui solamente le persone autorizzate possono leggerne il contenuto in chiaro, mentre per tutti gli altri utenti si tratta di dati presentati in un formato non leggibile.

Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione, gli Internet provider e utenti malevoli.

La E2EE si assicura inoltre che le comunicazioni tra due endpoint siano sicure.

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come *plaintext*.

In linea di massima E2EE garantisce che potenziali *eavesdroppers* non possano accedere alle chiavi necessarie per decifrare la conversazione. [4]

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

2022-04-29

SIGNAL

Crittografia End-to-End

End-to-End Encryption

End-to-End Encryption

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come *plaintext*.

In linea di massima E2EE garantisce che potenziali *eavesdroppers* non possano accedere alle chiavi necessarie per decifrare la conversazione. [4]

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come *plaintext*.

In linea di massima E2EE garantisce che potenziali *eavesdroppers* non possano accedere alle chiavi necessarie per decifrare la conversazione. [4]

Dati protetti da crittografia sono tali per cui solamente le persone autorizzate possono leggerne il contenuto in chiaro, mentre per tutti gli altri utenti si tratta di dati presentati in un formato non leggibile.

Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione, gli Internet provider e utenti malevoli.

La E2EE si assicura inoltre che le comunicazioni tra due endpoint siano sicure.

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

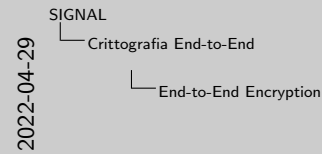
5 Bibliografia

E2EE si basa sulla crittografia *asimmetrica*.

La crittografia **asimmetrica**, o a **chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- ▶ La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- ▶ In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia **simmetrica** utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.



I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in *plaintext* e saranno dunque conservabili solo in *ciphertext*.

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

End-to-End Encryption

E2EE si basa sulla crittografia asimmetrica. La crittografia **asimmetrica**, o a **chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- ▶ La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- ▶ In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia simmetrica utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

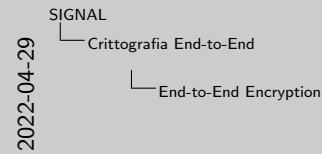
5 Bibliografia

E2EE si basa sulla crittografia *asimmetrica*.

La crittografia **asimmetrica**, o a **chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia **simmetrica** utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.



I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in *plaintext* e saranno dunque conservabili solo in *ciphertext*.

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

End-to-End Encryption

E2EE si basa sulla crittografia asimmetrica. La crittografia **asimmetrica**, o a **chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia simmetrica utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

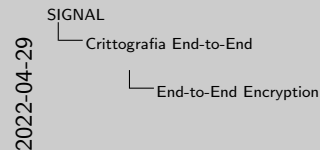
5 Bibliografia

E2EE si basa sulla crittografia *asimmetrica*.

La crittografia **asimmetrica**, o a **chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia **simmetrica** utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.



I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in *plaintext* e saranno dunque conservabili solo in *ciphertext*.

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

End-to-End Encryption

E2EE si basa sulla crittografia *asimmetrica*.
La crittografia **asimmetrica**, o a **chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia *simmetrica* utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp VS Telegram

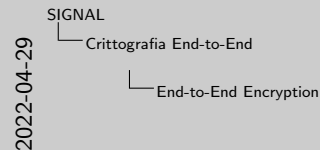
5 Bibliografia

E2EE si basa sulla crittografia *asimmetrica*.

La crittografia **asimmetrica**, o **a chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia **simmetrica** utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.



I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in *plaintext* e saranno dunque conservabili solo in *ciphertext*.

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

End-to-End Encryption

E2EE si basa sulla crittografia *asimmetrica*.
La crittografia **asimmetrica**, o **a chiave pubblica**, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia **simmetrica** utilizza una sola chiave privata per cifrare il *plaintext* e decifrare il *ciphertext*.

End-to-End Encryption

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni Problematiche

4 Signal Protocol

Proprietà

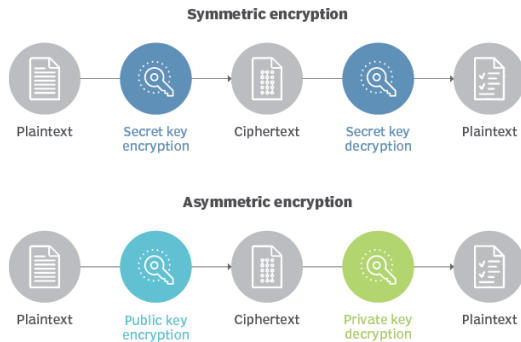
Il protocollo

Difetti di progettazione

Signal VS WhatsApp VS Telegram

5 Bibliografia

Symmetric vs. asymmetric encryption



2022-04-29

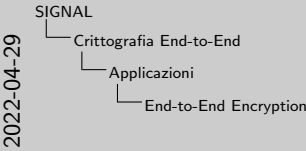
SIGNAL
└─ Crittografia End-to-End
 └─ End-to-End Encryption

End-to-End Encryption



End-to-End Encryption

Applicazioni



End-to-End Encryption

Applicazioni

- **Comunicazioni sicure:** applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- **Gestione password:** a entrambi gli endpoint della comunicazione si trova lo stesso utente, l'unica persona munita di chiave;
- **Data storage:** nei servizi di storage in cloud la E2EE protegge i dati degli utenti anche dall'accesso da parte dei fornitori del servizio in cloud.

[5]

Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [6]
Lavabit, servizio email in passato ritenuto sicuro e oggi non più attivo, nel 2014 consegnò al governo americano le chiavi che utilizzava per proteggere i dati dei propri utenti in occasione delle indagini sul caso Snowden. La compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori avevano accesso al contenuto delle mail scambiate dai propri utenti. [7], [8]
Hushmail, altro email provider dichiarato sicuro, utilizzò le password dei propri utenti per decrittare le email e consegnarle al governo federale in *plaintext*. [9]
Altri sistemi, come per esempio Telegram, non implementano la crittografia end-to-end di default e sono pertanto stati criticati.

In modo particolare Telegram non la implementa né per le chat di gruppo né per i client desktop, oltre al fatto che utilizza il protocollo di crittografia non standard MTProto. [10]

- **Comunicazioni sicure:** applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- **Gestione password:** a entrambi gli endpoint della comunicazione si trova lo stesso utente, l'unica persona munita di chiave;
- **Data storage:** nei servizi di storage in cloud la E2EE protegge i dati degli utenti anche dall'accesso da parte dei fornitori del servizio in cloud.

[5]

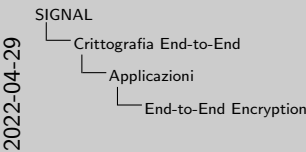
- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp
 - VS Telegram
- 5 Bibliografia

End-to-End Encryption

Applicazioni

- **Comunicazioni sicure:** applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- **Gestione password:** a entrambi gli endpoint della comunicazione si trova lo stesso utente, l'unica persona munita di chiave;
- **Data storage:** nei servizi di storage in cloud la E2EE protegge i dati degli utenti anche dall'accesso da parte dei fornitori del servizio in cloud.

[5]



Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [6]
Lavabit, servizio email in passato ritenuto sicuro e oggi non più attivo, nel 2014 consegnò al governo americano le chiavi che utilizzava per proteggere i dati dei propri utenti in occasione delle indagini sul caso Snowden. La compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori avevano accesso al contenuto delle mail scambiate dai propri utenti. [7], [8]
Hushmail, altro email provider dichiarato sicuro, utilizzò le password dei propri utenti per decrittare le email e consegnarle al governo federale in *plaintext*. [9]
Altri sistemi, come per esempio Telegram, non implementano la crittografia end-to-end di default e sono pertanto stati criticati.

In modo particolare Telegram non la implementa né per le chat di gruppo né per i client desktop, oltre al fatto che utilizza il protocollo di crittografia non standard MTProto. [10]

End-to-End Encryption

Applicazioni

- **Comunicazioni sicure:** applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- **Gestione password:** a entrambi gli endpoint della comunicazione si trova lo stesso utente, l'unica persona munita di chiave;
- **Data storage:** nei servizi di storage in cloud la E2EE protegge i dati degli utenti anche dall'accesso da parte dei fornitori del servizio in cloud.

[5]

End-to-End Encryption

Applicazioni

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

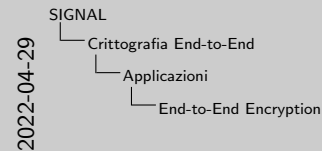
4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

- **Comunicazioni sicure:** applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- **Gestione password:** a entrambi gli endpoint della comunicazione si trova lo stesso utente, l'unica persona munita di chiave;
- **Data storage:** nei servizi di storage in cloud la E2EE protegge i dati degli utenti anche dall'accesso da parte dei fornitori del servizio in cloud.

[5]



Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [6]

Lavabit, servizio email in passato ritenuto sicuro e oggi non più attivo, nel 2014 consegnò al governo americano le chiavi che utilizzava per proteggere i dati dei propri utenti in occasione delle indagini sul caso Snowden. La compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori avevano accesso al contenuto delle mail scambiate dai propri utenti. [7], [8]

Hushmail, altro email provider dichiarato sicuro, utilizzò le password dei propri utenti per decrittare le email e consegnarle al governo federale in *plaintext*. [9]

Altri sistemi, come per esempio Telegram, non implementano la crittografia end-to-end di default e sono pertanto stati criticati.

In modo particolare Telegram non la implementa né per le chat di gruppo né per i client desktop, oltre al fatto che utilizza il protocollo di crittografia non standard MTProto. [10]

End-to-End Encryption

Applicazioni

- **Comunicazioni sicure:** applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- **Gestione password:** a entrambi gli endpoint della comunicazione si trova lo stesso utente, l'unica persona munita di chiave;
- **Data storage:** nei servizi di storage in cloud la E2EE protegge i dati degli utenti anche dall'accesso da parte dei fornitori del servizio in cloud.

[5]

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

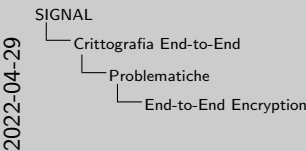
5 Bibliografia

End-to-End Encryption

Problematiche

La E2EE non garantisce di per sé né la sicurezza né la privacy, in quanto i dati trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint. Tuttavia, l'implementazione della E2EE consente di applicare una protezione dei dati migliore della sola crittografia “in transit”.

Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che li conserva finché non vengono recuperati dal destinatario. Anche se protetti da crittografia, essi lo sono solamente in transito, quindi possono essere letti dai provider di servizi.
[11], [5]



In questo modo è possibile monitorare il contenuto dei messaggi (per esempio in cerca di contenuti offensivi o pericolosi) ma si corre anche il rischio che utenti non autorizzati e/o malintenzionati aventi accesso allo storage dei messaggi possano fare un uso improprio dei contenuti.

Nella crittografia “in transit” è possibile o salvare direttamente i messaggi decrittati oppure salvare i dati crittografati e la chiave con cui decrittarli sullo stesso database.

End-to-End Encryption

Problematiche

La E2EE non garantisce di per sé né la sicurezza né la privacy, in quanto i dati trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint. Tuttavia, l'implementazione della E2EE consente di applicare una protezione dei dati migliore della sola crittografia “in transit”.

Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che li conserva finché non vengono recuperati dal destinatario. Anche se protetti da crittografia, essi lo sono solamente in transito, quindi possono essere letti dai provider di servizi.
[11], [5]

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

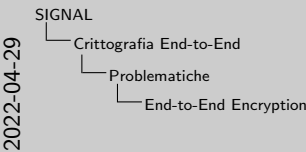
5 Bibliografia

End-to-End Encryption

Problematiche

La E2EE non garantisce di per sé né la sicurezza né la privacy, in quanto i dati trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint. Tuttavia, l'implementazione della E2EE consente di applicare una protezione dei dati migliore della sola crittografia **“in transit”**.

Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che li conserva finché non vengono recuperati dal destinatario. Anche se protetti da crittografia, essi lo sono solamente in transito, quindi possono essere letti dai provider di servizi.
[11], [5]



In questo modo è possibile monitorare il contenuto dei messaggi (per esempio in cerca di contenuti offensivi o pericolosi) ma si corre anche il rischio che utenti non autorizzati e/o malintenzionati aventi accesso allo storage dei messaggi possano fare un uso improprio dei contenuti.

Nella crittografia “in transit” è possibile o salvare direttamente i messaggi decrittati oppure salvare i dati crittografati e la chiave con cui decrittarli sullo stesso database.

End-to-End Encryption
Problematiche

La E2EE non garantisce di per sé né la sicurezza né la privacy, in quanto i dati trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint. Tuttavia, l'implementazione della E2EE consente di applicare una protezione dei dati migliore della sola crittografia **“in transit”**.

Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che li conserva finché non vengono recuperati dal destinatario. Anche se protetti da crittografia, essi lo sono solamente in transito, quindi possono essere letti dai provider di servizi.
[11], [5]

- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp VS Telegram
- 5 Bibliografia

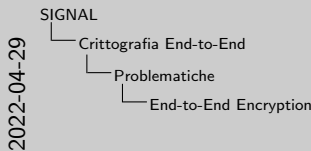
End-to-End Encryption

Problematiche

Ulteriori problematiche:

- ▶ **Endpoint security:** gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ **Attacchi di tipo Man-in-the-Middle:** la conversazione può essere soggetta a *eavesdropping*
- ▶ **Backdoors:** metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

[4], [5]



- Endpoint security: E2EE protegge i dati solo tra i due endpoint; ciò significa che i due endpoint possono essere soggetti ad attacchi;
- Attacchi MITM: anziché forzare la crittografia dei dati, ci si può aspettare un tentativo da parte di terzi malintenzionati di impersonare il destinatario. Essi possono, per esempio, impersonare il destinatario durante lo scambio di chiavi con il mittente, decifrare il messaggio inviato e poi inoltrarlo al vero destinatario senza farsi notare. Una soluzione per questo tipo di attacchi è introdurre un metodo di autenticazione (per es. certification authorities, web of trust, fingerprint numeriche o come QR code)
- Backdoors: nonostante le *backdoors* non siano sempre implementate volutamente, esse possono essere introdotte grazie a *cyber-attacks* e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

End-to-End Encryption

Problematiche

Ulteriori problematiche:

- ▶ **Endpoint security:** gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ Attacchi di tipo Man-in-the-Middle: la conversazione può essere soggetta a *eavesdropping*
- ▶ Backdoors: metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

[4] [5]

End-to-End Encryption

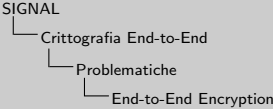
Problematiche

Ulteriori problematiche:

- ▶ **Endpoint security:** gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ **Attacchi di tipo Man-in-the-Middle:** la conversazione può essere soggetta a *eavesdropping*
- ▶ **Backdoors:** metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

[4], [5]

2022-04-29



- Endpoint security: E2EE protegge i dati solo tra i due endpoint; ciò significa che i due endpoint possono essere soggetti ad attacchi;
- Attacchi MITM: anziché forzare la crittografia dei dati, ci si può aspettare un tentativo da parte di terzi malintenzionati di impersonare il destinatario. Essi possono, per esempio, impersonare il destinatario durante lo scambio di chiavi con il mittente, decifrare il messaggio inviato e poi inoltrarlo al vero destinatario senza farsi notare. Una soluzione per questo tipo di attacchi è introdurre un metodo di autenticazione (per es. certification authorities, web of trust, fingerprint numeriche o come QR code)
- Backdoors: nonostante le *backdoors* non siano sempre implementate volutamente, esse possono essere introdotte grazie a *cyber-attacks* e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

End-to-End Encryption

Problematiche

Ulteriori problematiche:

- ▶ **Endpoint security:** gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ **Attacchi di tipo Man-in-the-Middle:** la conversazione può essere soggetta a *eavesdropping*
- ▶ **Backdoors:** metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

[4], [5]

End-to-End Encryption

Problematiche

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

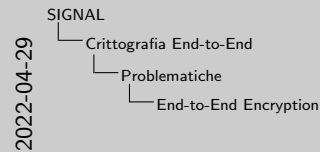
Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Ulteriori problematiche:

- ▶ **Endpoint security:** gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ **Attacchi di tipo Man-in-the-Middle:** la conversazione può essere soggetta a *eavesdropping*
- ▶ **Backdoors:** metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

[4], [5]



- Endpoint security: E2EE protegge i dati solo tra i due endpoint; ciò significa che i due endpoint possono essere soggetti ad attacchi;
- Attacchi MITM: anziché forzare la crittografia dei dati, ci si può aspettare un tentativo da parte di terzi malintenzionati di impersonare il destinatario. Essi possono, per esempio, impersonare il destinatario durante lo scambio di chiavi con il mittente, decifrare il messaggio inviato e poi inoltrarlo al vero destinatario senza farsi notare. Una soluzione per questo tipo di attacchi è introdurre un metodo di autenticazione (per es. certification authorities, web of trust, fingerprint numeriche o come QR code)
- Backdoors: nonostante le *backdoors* non siano sempre implementate volutamente, esse possono essere introdotte grazie a *cyber-attacks* e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

End-to-End Encryption
Problematiche

Ulteriori problematiche:

- ▶ **Endpoint security:** gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ **Attacchi di tipo Man-in-the-Middle:** la conversazione può essere soggetta a *eavesdropping*
- ▶ **Backdoors:** metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

[4], [5]

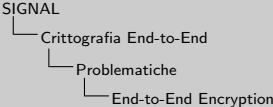
End-to-End Encryption

Problematiche

- **Complessità nel definire gli endpoint:** alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- **Privacy “eccessiva”:** enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- **Metadati visibili**
- Non vi è certezza che E2EE possa funzionare altrettanto bene con l’eventuale introduzione di *quantum computer* che rendano la crittografia obsoleta

[12]

2022-04-29



End-to-End Encryption

Problematiche

- **Complessità nel definire gli endpoint:** alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- Privacy “eccessiva”: enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- Metadati visibili
- Non vi è certezza che E2EE possa funzionare altrettanto bene con l’eventuale introduzione di *quantum computer* che rendano la crittografia obsoleta

[12]

End-to-End Encryption

Problematiche

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

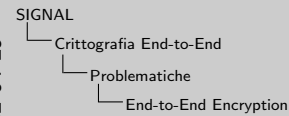
Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

- **Complessità nel definire gli endpoint:** alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- **Privacy “eccessiva”:** enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- **Metadati visibili**
- Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale introduzione di *quantum computer* che rendano la crittografia obsoleta

[12]

2022-04-29



End-to-End Encryption

Problematiche

- **Complessità nel definire gli endpoint:** alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- **Privacy “eccessiva”:** enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti

► Metadati visibili

► Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale introduzione di *quantum computer* che rendano la crittografia obsoleta

[12]

End-to-End Encryption

Problematiche

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

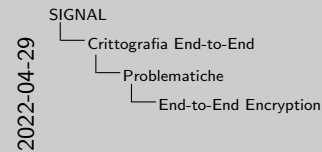
4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

- **Complessità nel definire gli endpoint:** alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- **Privacy “eccessiva”:** enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- **Metadati visibili**
 - Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale introduzione di *quantum computer* che rendano la crittografia obsoleta

[12]



End-to-End Encryption

Problematiche

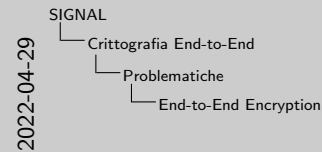
- **Complessità nel definire gli endpoint:** alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- **Privacy “eccessiva”:** enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- **Metadati visibili**

► Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale introduzione di *quantum computer* che rendano la crittografia obsoleta

[12]

End-to-End Encryption

Problematiche



End-to-End Encryption
Problematiche
► Complessità nel definire gli endpoint: alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
► Privacy “eccessiva”: enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
► Metadati visibili
► Non vi è certezza che E2EE possa funzionare altrettanto bene con l’eventuale introduzione di quantum computer che rendano la crittografia obsoleta
[12]

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

- **Complessità nel definire gli endpoint:** alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- **Privacy “eccessiva”:** enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- **Metadati visibili**
- Non vi è certezza che E2EE possa funzionare altrettanto bene con l’eventuale introduzione di *quantum computer* che rendano la crittografia obsoleta

[12]

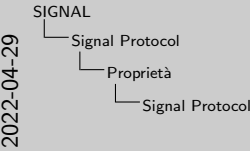
Signal Protocol

Proprietà

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in ambito crittografico:

- **Confidenzialità**
- **Integrità**
- **Autenticità**

Le proprietà CIA spesso vengono accompagnate dalla **non ripudiabilità**



- **Confidenzialità:** dati trasmessi non vengono diffusi a terzi non coinvolti nella conversazione
- **Integrità:** dati trasmessi non danneggiati e/o dispersi
- **Autenticità:** possesso di una chiave da parte di due persone al fine di riconoscere e verificare l'identità dell'altro
- **Non ripudiabilità:** non deve essere possibile negare per es. la propria firma a un documento, per questo spesso è implementata tramite firme digitali

Signal Protocol

Proprietà

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in ambito crittografico:

- **Confidenzialità**
- **Integrità**
- **Autenticità**

Le proprietà CIA spesso vengono accompagnate dalla non ripudiabilità

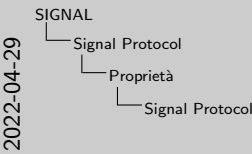
Signal Protocol

Proprietà

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in ambito crittografico:

- **Confidenzialità**
- **Integrità**
- **Autenticità**

Le proprietà CIA spesso vengono accompagnate dalla **non ripudiabilità**



- **Confidenzialità**: dati trasmessi non vengono diffusi a terzi non coinvolti nella conversazione
- **Integrità**: dati trasmessi non danneggiati e/o dispersi
- **Autenticità**: possesso di una chiave da parte di due persone al fine di riconoscere e verificare l'identità dell'altro
- **Non ripudiabilità**: non deve essere possibile negare per es. la propria firma a un documento, per questo spesso è implementata tramite firme digitali

Signal Protocol

Proprietà

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in ambito crittografico:

► **Confidenzialità**

► **Integrità**

► **Autenticità**

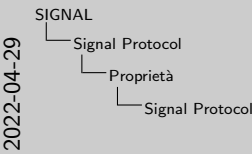
Le proprietà CIA spesso vengono accompagnate dalla **non ripudiabilità**

Signal Protocol

Proprietà

Ulteriori proprietà spesso richieste sono:

- **Forward Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- **Future Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi
- **Cryptographic Deniability:** l'esistenza di un file cifrato o di un messaggio è rinne­gabile, nel senso che un altro utente non può dimostrare che i dati in *plaintext* esistono.



Signal Protocol
Proprietà

Ulteriori proprietà spesso richieste sono:

- **Forward Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- **Future Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi
- **Cryptographic Deniability:** l'esistenza di un file cifrato o di un messaggio rinne­gabile, nel senso che un altro utente non può dimostrare che i dati *plaintext* esistono.

Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica.

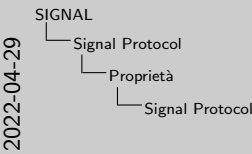
Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che ciò sia vero o meno.

Signal Protocol

Proprietà

Ulteriori proprietà spesso richieste sono:

- **Forward Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- **Future Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi
- **Cryptographic Deniability:** l'esistenza di un file cifrato o di un messaggio è rinnegabile, nel senso che un altro utente non può dimostrare che i dati in *plaintext* esistono.



Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica.

Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che ciò sia vero o meno.

Signal Protocol
Proprietà

Ulteriori proprietà spesso richieste sono:

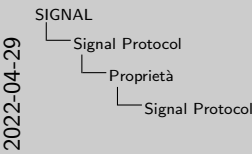
- **Forward Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- **Future Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi
- **Cryptographic Deniability:** l'esistenza di un file cifrato o di un messaggio rinnegabile, nel senso che un altro utente non può dimostrare che i dati *plaintext* esistono.

Signal Protocol

Proprietà

Ulteriori proprietà spesso richieste sono:

- **Forward Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- **Future Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi
- **Cryptographic Deniability:** l'esistenza di un file cifrato o di un messaggio è rinne­gabile, nel senso che un altro utente non può dimostrare che i dati in *plaintext* esistono.



Signal Protocol

Proprietà

Ulteriori proprietà spesso richieste sono:

► **Forward Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti

► **Future Secrecy:** se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi

► **Cryptographic Deniability:** l'esistenza di un file cifrato o di un messaggio è rinne­gabile, nel senso che un altro utente non può dimostrare che i dati in *plaintext* esistono.

Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica.

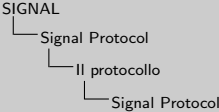
Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che ciò sia vero o meno.

Signal Protocol

Il protocollo

Il protocollo Signal fornisce crittografia end-to-end a sistemi di messaggistica istantanea e di chiamate vocali, combinando l'algoritmo **“Double Ratchet”**, pre-chiavi e un triplo handshake Elliptic-curve Diffie–Hellman (3-DH).

2022-04-29



Signal Protocol
Il protocollo

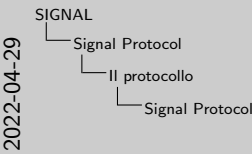
Il protocollo Signal fornisce crittografia end-to-end a sistemi di messaggistica istantanea e di chiamate vocali, combinando l'algoritmo **“Double Ratchet”**, pre-chiavi e un triplo handshake Elliptic-curve Diffie–Hellman (3-DH).

Signal Protocol

Il protocollo

Le specifiche di riferimento sono infatti: [13]

- ▶ **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ **Double Ratchet**: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- ▶ **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.



- Double Ratchet: le due parti derivano nuove chiavi per ogni messaggio in modo tale che chiavi usate in precedenza non possano essere ricavate dalle chiavi successive (grazie alla non invertibilità della funzione *ratchet*)
- X3DH: stabilisce una chiave segreta condivisa da due parti che si autenticano a vicenda basandosi su chiavi pubbliche. X3DH fornisce *forward secrecy* e *cryptographic deniability*

Signal Protocol
Il protocollo

Le specifiche di riferimento sono infatti: [13]

- ▶ **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- » Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- » Sesame: gestisce le sessioni crittografate in ambiente asincrono e multi-device.

Signal Protocol

Il protocollo

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

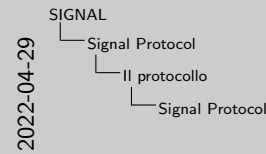
4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Le specifiche di riferimento sono infatti: [13]

- ▶ **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ **Double Ratchet**: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- ▶ **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.



- Double Ratchet: le due parti derivano nuove chiavi per ogni messaggio in modo tale che chiavi usate in precedenza non possano essere ricavate dalle chiavi successive (grazie alla non invertibilità della funzione *ratchet*)
- X3DH: stabilisce una chiave segreta condivisa da due parti che si autenticano a vicenda basandosi su chiavi pubbliche. X3DH fornisce *forward secrecy* e *cryptographic deniability*

Signal Protocol
Il protocollo

Le specifiche di riferimento sono infatti: [13]
▶ **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
▶ **Double Ratchet**: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
▶ **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.

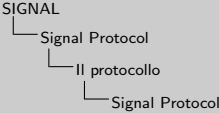
Signal Protocol

Il protocollo

Le specifiche di riferimento sono infatti: [13]

- ▶ **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ **Double Ratchet**: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- ▶ **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.

2022-04-29



- Double Ratchet: le due parti derivano nuove chiavi per ogni messaggio in modo tale che chiavi usate in precedenza non possano essere ricavate dalle chiavi successive (grazie alla non invertibilità della funzione *ratchet*)
- X3DH: stabilisce una chiave segreta condivisa da due parti che si autenticano a vicenda basandosi su chiavi pubbliche. X3DH fornisce *forward secrecy* e *cryptographic deniability*

Signal Protocol
Il protocollo

Le specifiche di riferimento sono infatti: [13]

- ▶ **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ **Double Ratchet**: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- ▶ **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.

Signal Protocol

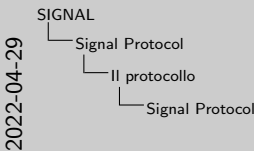
Il protocollo: fasi di funzionamento [14]

► **KEY REGISTRATION:** invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online

► **KEY AGREEMENT:** Alice riceve le chiavi pubbliche di Bob dal server e le usa, insieme alle proprie chiavi private, per generare una chiave segreta condivisa. Invia a Bob un messaggio criptato con questa chiave. Bob, ricevutolo, recupera le chiavi pubbliche di Alice dal server e calcola la stessa chiave segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH

► **CONVERSATION:** Alice e Bob possiedono la chiave segreta condivisa e possono conversare.

- DH ratchet phase
- Symmetric ratchet phase



- KEY REGISTRATION: se Alice vuole iniziare una conversazione con Bob può chiedere al server le sue chiavi pubbliche
- KEY AGREEMENT
- CONVERSATION

N.B. Symmetric ratchet phase e DH ratchet phase verranno meglio analizzati più avanti nel parlare dell'algorithm Double Ratchet.

Signal Protocol

Il protocollo: fasi di funzionamento [14]

- **KEY REGISTRATION:** invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online
- **KEY AGREEMENT:** Alice riceve le chiavi pubbliche di Bob dal server e le usa, insieme alle proprie chiavi private, per generare una chiave segreta condivisa. Invia a Bob un messaggio criptato con questa chiave. Bob, ricevutolo, recupera le chiavi pubbliche di Alice dal server e calcola la stessa chiave segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH
- **CONVERSATION:** Alice e Bob possiedono la chiave segreta condivisa e possono conversare.
 - DH ratchet phase
 - Symmetric ratchet phase

Signal Protocol

Il protocollo: fasi di funzionamento [14]

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

- ▶ **KEY REGISTRATION:** invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online
- ▶ **KEY AGREEMENT:** Alice riceve le chiavi pubbliche di Bob dal server e le usa, insieme alle proprie chiavi private, per generare una chiave segreta condivisa. Invia a Bob un messaggio criptato con questa chiave. Bob, ricevutolo, recupera le chiavi pubbliche di Alice dal server e calcola la stessa chiave segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH
- ▶ **CONVERSATION:** Alice e Bob possiedono la chiave segreta condivisa e possono conversare.
 - ▶ DH ratchet phase
 - ▶ Symmetric ratchet phase



- **KEY REGISTRATION:** se Alice vuole iniziare una conversazione con Bob può chiedere al server le sue chiavi pubbliche
- **KEY AGREEMENT**
- **CONVERSATION**

N.B. Symmetric ratchet phase e DH ratchet phase verranno meglio analizzati più avanti nel parlare dell'algoritmo Double Ratchet.

Signal Protocol

Il protocollo: fasi di funzionamento [14]

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

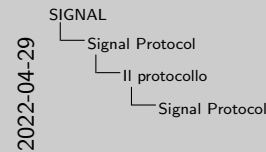
Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

- ▶ **KEY REGISTRATION:** invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online
- ▶ **KEY AGREEMENT:** Alice riceve le chiavi pubbliche di Bob dal server e le usa, insieme alle proprie chiavi private, per generare una chiave segreta condivisa. Invia a Bob un messaggio criptato con questa chiave. Bob, ricevutolo, recupera le chiavi pubbliche di Alice dal server e calcola la stessa chiave segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH
- ▶ **CONVERSATION:** Alice e Bob possiedono la chiave segreta condivisa e possono conversare.
 - ▶ DH ratchet phase
 - ▶ Symmetric ratchet phase



Signal Protocol
Il protocollo: fasi di funzionamento [14]

- ▶ **KEY REGISTRATION:** invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online
- ▶ **KEY AGREEMENT:** Alice riceve le chiavi pubbliche di Bob dal server e le usa, insieme alle proprie chiavi private, per generare una chiave segreta condivisa. Invia a Bob un messaggio criptato con questa chiave. Bob, ricevutolo, recupera le chiavi pubbliche di Alice dal server e calcola la stessa chiave segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH
- ▶ **CONVERSATION:** Alice e Bob possiedono la chiave segreta condivisa e possono conversare.
 - ▶ DH ratchet phase
 - ▶ Symmetric ratchet phase

- **KEY REGISTRATION:** se Alice vuole iniziare una conversazione con Bob può chiedere al server le sue chiavi pubbliche
- **KEY AGREEMENT**
- **CONVERSATION**

N.B. Symmetric ratchet phase e DH ratchet phase verranno meglio analizzati più avanti nel parlare dell'algoritmo Double Ratchet.

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

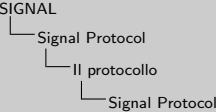
Signal Protocol

Il protocollo: fasi di funzionamento

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa.
Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà criptato con una nuova chiave calcolata in funzione della precedente.
In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la chiave sia compromessa)

2022-04-29



Signal Protocol
Il protocollo: fasi di funzionamento

Symmetric ratchet phase

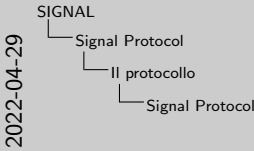
Derivazione di una nuova chiave dalla chiave segreta condivisa.
Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà criptato con una nuova chiave calcolata in funzione della precedente.
In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la chiave sia compromessa)

Signal Protocol

Il protocollo: fasi di funzionamento

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa.
Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà criptato con una nuova chiave calcolata in funzione della precedente.
In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la chiave sia compromessa)



Signal Protocol

Il protocollo: fasi di funzionamento

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa.
Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà criptato con una nuova chiave calcolata in funzione della precedente.
In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la chiave sia compromessa)

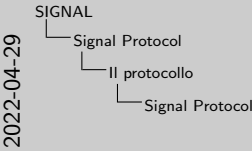
- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo**
 - Difetti di progettazione
 - Signal VS WhatsApp
 - VS Telegram
- 5 Bibliografia

Signal Protocol

Il protocollo: fasi di funzionamento

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa.
Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà criptato con una nuova chiave calcolata in funzione della precedente.
In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la chiave sia compromessa)



Signal Protocol

Il protocollo: fasi di funzionamento

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa.
Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà criptato con una nuova chiave calcolata in funzione della precedente.
In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la chiave sia compromessa)

- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp
 - VS Telegram
- 5 Bibliografia

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Signal Protocol

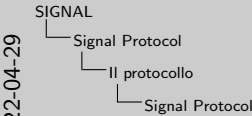
Il protocollo: fasi di funzionamento

Diffie–Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.

Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa queste chiavi per calcolarne una nuova condivisa, inviando poi la propria chiave effimera ad Alice per farle calcolare la chiave condivisa.

La chiave così calcolata verrà usata in una nuova *symmetric ratchet phase* per generare nuove chiavi per i messaggi.



Signal Protocol

Il protocollo: fasi di funzionamento

Diffie–Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.

Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa queste chiavi per calcolarne una nuova condivisa, inviando poi la propria chiave effimera ad Alice per farle calcolare la chiave condivisa.

La chiave così calcolata verrà usata in una nuova *symmetric ratchet phase* per generare nuove chiavi per i messaggi.

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

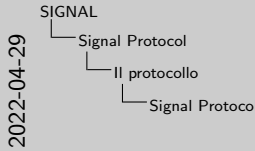
5 Bibliografia

Signal Protocol

Il protocollo: fasi di funzionamento

Diffie–Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.
Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa queste chiavi per calcolarne una nuova condivisa, inviando poi la propria chiave effimera ad Alice per farle calcolare la chiave condivisa.
La chiave così calcolata verrà usata in una nuova *symmetric ratchet phase* per generare nuove chiavi per i messaggi.



Signal Protocol
Il protocollo: fasi di funzionamento

Diffie–Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.
Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa queste chiavi per calcolarne una nuova condivisa, inviando poi la propria chiave effimera ad Alice per farle calcolare la chiave condivisa.
La chiave così calcolata verrà usata in una nuova *symmetric ratchet phase* per generare nuove chiavi per i messaggi.

Signal Protocol

Il protocollo: fasi di funzionamento

Diffie–Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.
Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa queste chiavi per calcolarne una nuova condivisa, inviando poi la propria chiave effimera ad Alice per farle calcolare la chiave condivisa.
La chiave così calcolata verrà usata in una nuova *symmetric ratchet phase* per generare nuove chiavi per i messaggi.

2022-04-29

SIGNAL

Signal Protocol

Il protocollo

Signal Protocol

Signal Protocol

Il protocollo: fasi di funzionamento

Diffie–Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.
Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa queste chiavi per calcolarne una nuova condivisa, inviando poi la propria chiave effimera ad Alice per farle calcolare la chiave condivisa.
La chiave così calcolata verrà usata in una nuova *symmetric ratchet phase* per generare nuove chiavi per i messaggi.

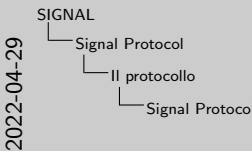
Signal Protocol

Il protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key



STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi private (*secret keys*) sk . Dopodiché scambiano le chiavi pubbliche attraverso un canale e da esse possono derivare una chiave segreta condivisa ssk .

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol

Il protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key

Signal Protocol

Il protocollo: X3DH

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

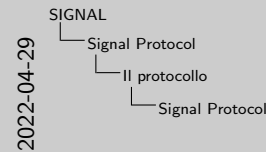
5 Bibliografia

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

[15]

Definizioni:

- Identity key: chiave long-term pubblica
- Ephemereal key: chiave utilizzabile una sola volta
- Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- Signed pre-key: pre-key firmata con l'esponente dell'Identity key



STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi private (*secret keys*) sk . Dopodiché scambiano le chiavi pubbliche attraverso un canale e da esse possono derivare una chiave segreta condivisa ssk .

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol
Il protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [15]

Definizioni:

- Identity key: chiave long-term pubblica
- Ephemereal key: chiave utilizzabile una sola volta
- Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- Signed pre-key: pre-key firmata con l'esponente dell'Identity key

Signal Protocol

Il protocollo: X3DH

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

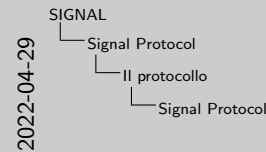
5 Bibliografia

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

[15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key



STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi private (*secret keys*) sk . Dopodiché scambiano le chiavi pubbliche attraverso un canale e da esse possono derivare una chiave segreta condivisa ssk .

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol
Il protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key

Signal Protocol

Il protocollo: X3DH

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

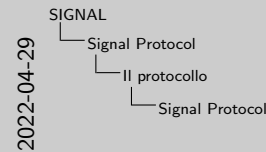
5 Bibliografia

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

[15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key



STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi private (*secret keys*) sk .
Dopodiché scambiano le chiavi pubbliche attraverso un canale e da esse possono derivare una chiave segreta condivisa ssk .

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol
Il protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key

Signal Protocol

Il protocollo: X3DH

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

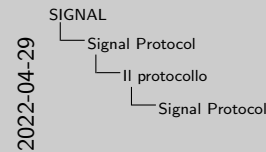
5 Bibliografia

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

[15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key



STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi private (*secret keys*) sk .
Dopodiché scambiano le chiavi pubbliche attraverso un canale e da esse possono derivare una chiave segreta condivisa ssk .

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol
Il protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [15]

Definizioni:

- ▶ Identity key: chiave long-term pubblica
- ▶ Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- ▶ One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire

▶ Signed pre-key: pre-key firmata con l'esponente dell'Identity key

Signal Protocol

Il protocollo: X3DH

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp
VS Telegram

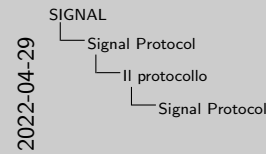
5 Bibliografia

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

[15]

Definizioni:

- Identity key: chiave long-term pubblica
- Ephemereal key: chiave utilizzabile una sola volta
- Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- Signed pre-key: pre-key firmata con l'esponente dell'Identity key



STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi private (*secret keys*) sk . Dopodiché scambiano le chiavi pubbliche attraverso un canale e da esse possono derivare una chiave segreta condivisa ssk .

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol
Il protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.
[15]
Definizioni:

- Identity key: chiave long-term pubblica
- Ephemereal key: chiave utilizzabile una sola volta
- Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
- One-time pre-keys: insiemi di pre-keys condivise col server prima dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- Signed pre-key: pre-key firmata con l'esponente dell'Identity key

Signal Protocol

Il protocollo: X3DH

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

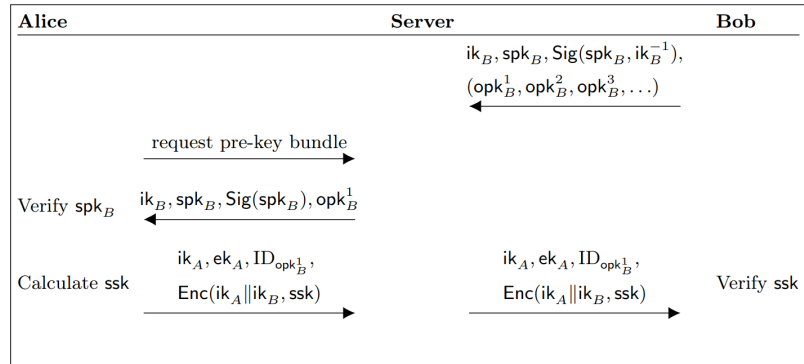
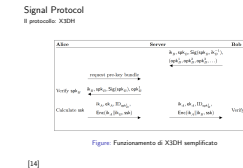
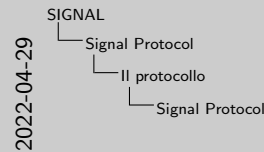


Figure: Funzionamento di X3DH semplificato

[14]



[14]

Perché il protocollo possa funzionare offline ogni utente deve inviare le proprie chiavi pubbliche al server, inviando cioè $ik, spk, Sig(sp, ik^{-1})$ e $(opk^1, opk^2, opk^3, \dots)$.

La ik va inviata una sola volta, la spk va rinnovata periodicamente.

Se Alice vuole iniziare una conversazione richiede al server $ik_B, spk_B, Sig(sp, ik_B^{-1})$ e una delle one-time pre-keys opk_B^x di Bob. Il server poi elimina opk_B^x . Una volta finite le opk_B ad Alice verranno inviate solo le altre chiavi senza opk_B .

Ricevute le chiavi Alice verifica la firma di spk_B e se va a buon fine genera una coppia di chiavi effimere; poi calcola la ssk usando una Key Derivation Function (KDF). Alla fine cancella ek_A^{-1} e tutti i valori k_i generati.

N.B. $DH(x, y)$ è una funzione DH su curva ellittica che calcola una ssk basandosi su due chiavi, mentre $KDF(x)$ è una funzione basata su RFC5869 [18].

Alice invia un messaggio iniziale a Bob contenente $ik_A, ek_A, ID_{opk_B^x}$ (per fargli sapere quale opk_B^x ha usato) e $Enc(ik_A || ik_B, ssk)$.

Bob riceve il messaggio e calcola la ssk nello stesso modo di Alice. Bob decrittà il messaggio inviato da Alice e controlla se il valore di ssk è corretto e in questo caso cancella la opk utilizzata.

Alice e Bob possono ora riutilizzare la stessa ssk per messaggi futuri oppure usare chiavi da essa derivate. [14]

Signal Protocol

Il protocollo: Double Ratchet

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla iniziata tramite X3DH.

[19], [14]

A differenza di X3DH usa una catena KDF, come mostrato in figura 2.

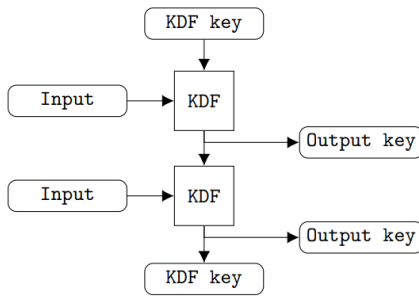
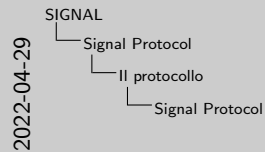


Figure: Catena KDF



2022-04-29

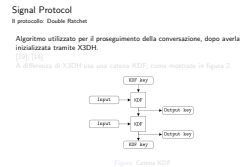


Figure: Catena KDF

La catena KDF usa l'output di una KDF come input per un'altra applicazione della KDF. Ogni *output key* può essere utilizzata per cifrare un messaggio. Tale catena garantisce:

- Resilienza: l'output appare randomico
- Forward secrecy: garantita dalla non-invertibilità della KDF
- Future secrecy: garantita se l'input della KDF $i + 1$ non è il solo output della KDF i . Per garantire ciò è necessario usare un **DH ratchet**

Signal Protocol

Il protocollo: Double Ratchet

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla iniziata tramite X3DH.

[19], [14]

A differenza di X3DH usa una catena KDF, come mostrato in figura 2.

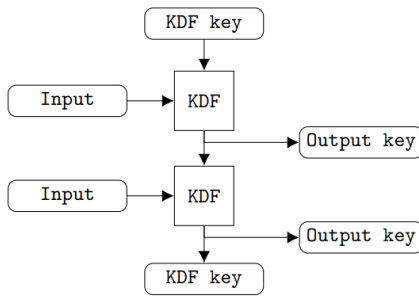
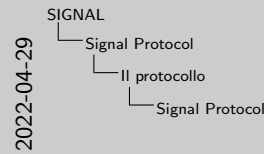


Figure: Catena KDF



2022-04-29



Figure: Catena KDF

La catena KDF usa l'output di una KDF come input per un'altra applicazione della KDF. Ogni *output key* può essere utilizzata per cifrare un messaggio. Tale catena garantisce:

- Resilienza: l'output appare randomico
- Forward secrecy: garantita dalla non-invertibilità della KDF
- Future secrecy: garantita se l'input della KDF $i + 1$ non è il solo output della KDF i . Per garantire ciò è necessario usare un **DH ratchet**

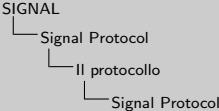
Signal Protocol

Il protocollo: Double Ratchet

Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double ratchet che garantisce sia *forward secrecy* che *future secrecy*.

DH ratchet infatti modifica gli input delle KDF in modo tale che, se anche una chiave venisse compromessa, si sia in grado di ristabilire la segretezza dall'applicazione successiva di una KDF.

2022-04-29



Signal Protocol
Il protocollo: Double Ratchet

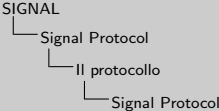
Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double ratchet che garantisce sia *forward secrecy* che *future secrecy*.
DH ratchet infatti modifica gli input delle KDF in modo tale che, se anche una chiave venisse compromessa, si sia in grado di ristabilire la segretezza dall'applicazione successiva di una KDF.

Signal Protocol

Il protocollo: Double Ratchet

Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double ratchet che garantisce sia *forward secrecy* che *future secrecy*.
DH ratchet infatti modifica gli input delle KDF in modo tale che, se anche una chiave venisse compromessa, si sia in grado di ristabilire la segretezza dall'applicazione successiva di una KDF.

2022-04-29



Signal Protocol
Il protocollo: Double Ratchet

Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double ratchet che garantisce sia *forward secrecy* che *future secrecy*.
DH ratchet infatti modifica gli input delle KDF in modo tale che, se anche una chiave venisse compromessa, si sia in grado di ristabilire la segretezza dall'applicazione successiva di una KDF.

Signal Protocol

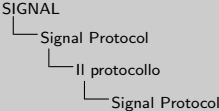
Il protocollo: Double Ratchet

Sia Alice che Bob hanno tre catene KDF da utilizzare:

- ▶ DH ratchet
- ▶ Sending ratchet
- ▶ Receiving ratchet

Ogni volta che Alice vuole inviare un messaggio a Bob aggiornerà la catena *sending ratchet* producendo una nuova chiave di output e invierà a Bob il proprio messaggio cifrato con essa.

2022-04-29



Signal Protocol
Il protocollo: Double Ratchet

Sia Alice che Bob hanno tre catene KDF da utilizzare:

- ▶ DH ratchet
- ▶ Sending ratchet
- ▶ Receiving ratchet

Ogni volta che Alice vuole inviare un messaggio a Bob aggiornerà la catena *sending ratchet* producendo una nuova chiave di output e invierà a Bob il proprio messaggio cifrato con essa.

Signal Protocol

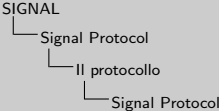
Il protocollo: Double Ratchet

Sia Alice che Bob hanno tre catene KDF da utilizzare:

- ▶ DH ratchet
- ▶ Sending ratchet
- ▶ Receiving ratchet

Ogni volta che Alice vuole inviare un messaggio a Bob aggiornerà la catena *sending ratchet* producendo una nuova chiave di output e invierà a Bob il proprio messaggio cifrato con essa.

2022-04-29



Signal Protocol
Il protocollo: Double Ratchet

Sia Alice che Bob hanno tre catene KDF da utilizzare:

- ▶ DH ratchet
- ▶ Sending ratchet
- ▶ Receiving ratchet

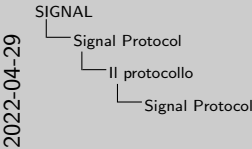
Ogni volta che Alice vuole inviare un messaggio a Bob aggiornerà la catena *sending ratchet* producendo una nuova chiave di output e invierà a Bob il proprio messaggio cifrato con essa.

Signal Protocol

Il protocollo: Double Ratchet

La catena di invio di Alice deve essere sincronizzata con quella di ricezione di Bob e viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DH applicato prima del Double ratchet).

In queste condizioni tuttavia non è ancora garantita la *future secrecy*



Signal Protocol
Il protocollo: Double Ratchet

La catena di invio di Alice deve essere sincronizzata con quella di ricezione di Bob e viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DH applicato prima del Double ratchet).

In queste condizioni tuttavia non è ancora garantita la future secrecy

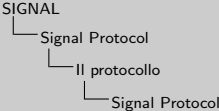
Signal Protocol

Il protocollo: Double Ratchet

La catena di invio di Alice deve essere sincronizzata con quella di ricezione di Bob e viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DH applicato prima del Double ratchet).

In queste condizioni tuttavia non è ancora garantita la *future secrecy*

2022-04-29



Signal Protocol
Il protocollo: Double Ratchet

La catena di invio di Alice deve essere sincronizzata con quella di ricezione di Bob e viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DH applicato prima del Double ratchet).
In queste condizioni tuttavia non è ancora garantita la *future secrecy*

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

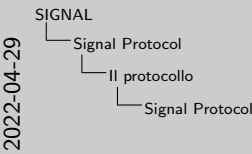
Signal Protocol

Il protocollo: Double Ratchet

Per garantire *future secrecy* Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]



Questo sistema di catene garantisce dunque:

- Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza
- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la sequenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi.

N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

Signal Protocol

Il protocollo: Double Ratchet

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]

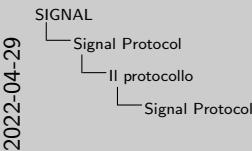
Signal Protocol

Il protocollo: Double Ratchet

Per garantire *future secrecy* Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]



Questo sistema di catene garantisce dunque:

- Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza
- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la sequenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi.

N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

Signal Protocol
Il protocollo: Double Ratchet

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.
Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.
Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]

Signal Protocol

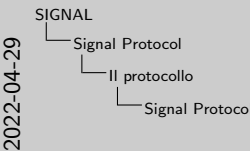
Il protocollo: Double Ratchet

Per garantire *future secrecy* Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene.

Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]



Signal Protocol

Il protocollo: Double Ratchet

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene.

Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]

Questo sistema di catene garantisce dunque:

- Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza
- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la sequenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi.

N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

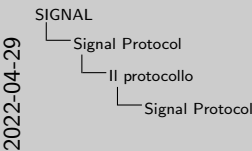
Signal Protocol

Il protocollo: Double Ratchet

Per garantire *future secrecy* Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]



Questo sistema di catene garantisce dunque:

- Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza
- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la sequenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi.

N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

Signal Protocol
Il protocollo: Double Ratchet

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.
Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.
Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [20]

1	Sommario
2	Applicazione Signal
	Storia dell'Applicazione
	L'Applicazione e il Protocollo Signal
3	Crittografia End-to-End
	Applicazioni
	Problematiche
4	Signal Protocol
	Proprietà
	Il protocollo
	Difetti di progettazione
	Signal VS WhatsApp
	VS Telegram
5	Bibliografia

Signal Protocol

Il protocollo: Double Ratchet

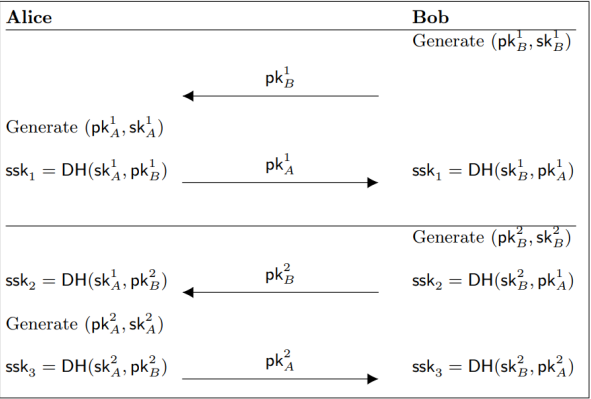


Figure: DH ratchet

2022-04-29

SIGNAL

Signal Protocol

Il protocollo

Signal Protocol

Signal Protocol

Il protocollo: Double Ratchet

Alice	Bob
	Generate (pk_B^1, sk_B^1)
	$\longleftarrow pk_B^1$
Generate (pk_A^1, sk_A^1)	
$ssk_1 = DH(sk_A^1, pk_B^1)$	$\xrightarrow{pk_A^1} ssk_1 = DH(sk_B^1, pk_A^1)$
<hr/>	
	Generate (pk_B^2, sk_B^2)
$ssk_2 = DH(sk_A^1, pk_B^2)$	$\longleftarrow pk_B^2$
Generate (pk_A^2, sk_A^2)	
$ssk_3 = DH(sk_A^2, pk_B^2)$	$\xrightarrow{pk_A^2} ssk_3 = DH(sk_B^2, pk_A^2)$

Figure: DH ratchet

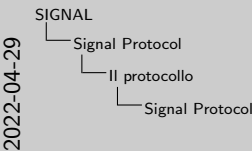
Signal Protocol

Il protocollo: Sesame

L’algoritmo **Sesame** gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.

Ogni dispositivo degli utenti deve tenere traccia di una sessione *attiva* per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione *inattiva*, essa diventa *attiva*.

In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispositivo remoto con cui comunica. [21]



Problemi che si possono generare:

- Alice e Bob possono avere ognuno più dispositivi quindi l'invio di un messaggio da parte di Alice richiede di inviarne una copia a tutti i dispositivi di Bob e a tutti i dispositivi di Alice.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni.
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo. Per il funzionamento del Double Ratchet Alice e Bob devono usare la stessa sessione, quindi devono concordare su quella da utilizzare.
- Alice può resettare lo stato della sessione sul suo dispositivo, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare.

Signal Protocol
Il protocollo: Sesame

L'algoritmo **Sesame** gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.

Ogni dispositivo degli utenti deve tenere traccia di una sessione attiva per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione inattiva, essa diventa attiva.

In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispositivo remoto con cui comunica. [21]

Signal Protocol

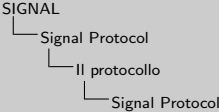
Il protocollo: Sesame

L’algoritmo **Sesame** gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.

Ogni dispositivo degli utenti deve tenere traccia di una sessione *attiva* per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione *inattiva*, essa diventa *attiva*.

In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispositivo remoto con cui comunica. [21]

2022-04-29



Problemi che si possono generare:

- Alice e Bob possono avere ognuno più dispositivi quindi l'invio di un messaggio da parte di Alice richiede di inviarne una copia a tutti i dispositivi di Bob e a tutti i dispositivi di Alice.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni.
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo. Per il funzionamento del Double Ratchet Alice e Bob devono usare la stessa sessione, quindi devono concordare su quella da utilizzare.
- Alice può resettare lo stato della sessione sul suo dispositivo, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare.

Signal Protocol
Il protocollo: Sesame

L'algoritmo **Sesame** gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione. Ogni dispositivo degli utenti deve tenere traccia di una sessione *attiva* per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione *inattiva*, essa diventa *attiva*. In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispositivo remoto con cui comunica. [21]

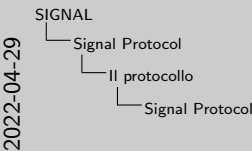
Signal Protocol

Il protocollo: Sesame

L’algoritmo **Sesame** gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.

Ogni dispositivo degli utenti deve tenere traccia di una sessione *attiva* per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione *inattiva*, essa diventa *attiva*.

In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispositivo remoto con cui comunica. [21]



Problemi che si possono generare:

- Alice e Bob possono avere ognuno più dispositivi quindi l'invio di un messaggio da parte di Alice richiede di inviarne una copia a tutti i dispositivi di Bob e a tutti i dispositivi di Alice.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni.
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo. Per il funzionamento del Double Ratchet Alice e Bob devono usare la stessa sessione, quindi devono concordare su quella da utilizzare.
- Alice può resettare lo stato della sessione sul suo dispositivo, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare.

Signal Protocol
Il protocollo: Sesame

L'algoritmo **Sesame** gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.
Ogni dispositivo degli utenti deve tenere traccia di una sessione attiva per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione inattiva, essa diventa attiva.
In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispositivo remoto con cui comunica. [21]

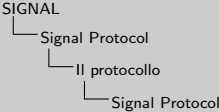
Signal Protocol

Il protocollo: Sesame

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie *one-time pre-keys*, *signed pre-keys* e *identity public key*.
- ▶ Il dispositivo mittente recupera dal server la *identity public key* del dispositivo destinatario, *signed pre-keys* e una *one-time pre-key* se disponibile.
- ▶ X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.

2022-04-29



Signal Protocol
Il protocollo: Sesame

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie *one-time pre-keys*, *signed pre-keys* e *identity public key*.
- ▶ Il dispositivo mittente recupera dal server la *identity public key* del dispositivo destinatario, *signed pre-keys* e una *one-time pre-key* se disponibile.
- ▶ X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.

Signal Protocol

Il protocollo: Sesame

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

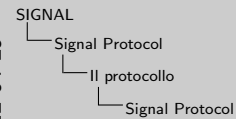
Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie *one-time pre-keys*, *signed pre-keys* e *identity public key*.
- ▶ Il dispositivo mittente recupera dal server la *identity public key* del dispositivo destinatario, *signed pre-keys* e una *one-time pre-key* se disponibile.
- ▶ X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.

2022-04-29



Signal Protocol
Il protocollo: Sesame

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie *one-time pre-keys*, *signed pre-keys* e *identity public key*.
- ▶ Il dispositivo mittente recupera dal server la *identity public key* del dispositivo destinatario, *signed pre-keys* e una *one-time pre-key* se disponibile.
- ▶ X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.

Signal Protocol

Il protocollo: Sesame

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

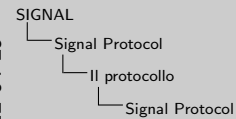
Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie *one-time pre-keys*, *signed pre-keys* e *identity public key*.
- ▶ Il dispositivo mittente recupera dal server la *identity public key* del dispositivo destinatario, *signed pre-keys* e una *one-time pre-key* se disponibile.
- ▶ X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.

2022-04-29



Signal Protocol
Il protocollo: Sesame

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie *one-time pre-keys*, *signed pre-keys* e *identity public key*.
- ▶ Il dispositivo mittente recupera dal server la *identity public key* del dispositivo destinatario, *signed pre-keys* e una *one-time pre-key* se disponibile.
- ▶ X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.

Signal Protocol

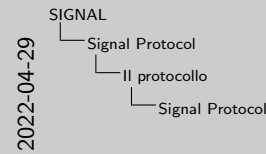
Il protocollo: Sesame

► Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.

► Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH.

► I dispositivi comunicano solo con Double Ratchet.

[21], [14]



Signal Protocol
Il protocollo: Sesame

► Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.

► Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH.

► I dispositivi comunicano solo con Double Ratchet.

[21], [14]

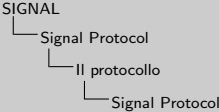
Signal Protocol

Il protocollo: Sesame

- Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.
- Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH.
- I dispositivi comunicano solo con Double Ratchet.

[21], [14]

2022-04-29



Signal Protocol

Il protocollo: Sesame

- Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.
- Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH.

⚠ I dispositivi comunicano solo con Double Ratchet.

[21], [14]

Signal Protocol

Il protocollo: Sesame

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà

Il protocollo

Difetti di
progettazione

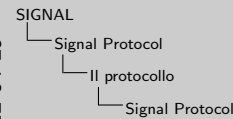
Signal VS WhatsApp
VS Telegram

5 Bibliografia

- Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.
- Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH.
- I dispositivi comunicano solo con Double Ratchet.

[21], [14]

2022-04-29



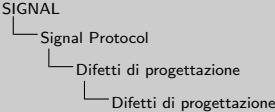
Signal Protocol
Il protocollo: Sesame

- Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.
 - Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH.
 - I dispositivi comunicano solo con Double Ratchet.
- [21], [14]

Difetti di progettazione

Frosch analysis [22]

2022-04-29



- *Export function* [fixed]: la funzione esportava la password necessaria per inviare le *one-time pre-keys* al server in *plaintext* su dispositivi Android
- Vulnerabilità a UKS - *Unknown key-share attack*

I difetti di progettazione individuati in questo paper sono stati ricavati da un'analisi di X3DH e di Double Ratchet separatamente, ma non da un'analisi dell'interazione dei due algoritmi come invece avviene nel protocollo Signal.

UKS
Esempio:
Bob sa che Charlie lo inviterà a una festa. Per fare uno scherzo a Charlie, Bob sostituisce la propria chiave con quella di Dave.
Quando Charlie invita Bob alla festa, Bob inoltrerà il messaggio a Dave.
Dal punto di vista di Dave, sembrerà che Charlie abbia inviato il messaggio.

Charlie penserà di aver invitato Bob, ma avrà in effetti invitato Dave.

- *Export function* [fixed]: la funzione esportava la password necessaria per inviare le *one-time pre-keys* al server in *plaintext* su dispositivi Android
- *Vulnerabilità a UKS - Unknown key-share attack*

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
**Difetti di
progettazione**
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Difetti di progettazione

Cohn-Gordon analysis [23]

L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come oracoli che restituiscono un output simile a un output casuale.

Definiamo questa condizione come *random oracle model*.



Il paper [23] è il primo studio scientifico a riportare un'analisi formale dell'interazione tra X3DH e Double Ratchet.

Difetti di progettazione

Cohn-Gordon analysis [23]

L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come oracoli che restituiscono un output simile a un output casuale.

Definiamo questa condizione come *random oracle model*.

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni

Problematiche

4 Signal
Protocol

Proprietà

Il protocollo

**Difetti di
progettazione**

Signal VS WhatsApp
VS Telegram

5 Bibliografia

Difetti di progettazione

Cohn-Gordon analysis [23]

L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come oracoli che restituiscono un output simile a un output casuale.

Definiamo questa condizione come *random oracle model*.



Il paper [23] è il primo studio scientifico a riportare un'analisi formale dell'interazione tra X3DH e Double Ratchet.

Difetti di progettazione

Cohn-Gordon analysis [23]

L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come oracoli che restituiscono un output simile a un output casuale.

Definiamo questa condizione come *random oracle model*.

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Proprietà
Il protocollo
**Difetti di
progettazione**
Signal VS WhatsApp
VS Telegram

5 Bibliografia

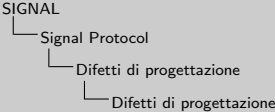
Difetti di progettazione

Cohn-Gordon analysis [23]

L’attacco UKS individuato in [22] non è valido in questo modello.

Non sono stati individuati altri rilevanti difetti di progettazione che generino punti di debolezza nel protocollo.

2022-04-29



UKS è un attacco prevenibile a livello di applicazione (introducendo degli identificativi per gli utenti, e.g. il numero di telefono).

N.B. Gli attacchi possono variare a seconda dell'implementazione fornita del protocollo, ma il protocollo in sé non presenta difetti rilevanti.

Difetti di progettazione
Cohn-Gordon analysis [23]

L'attacco UKS individuato in [22] non è valido in questo modello.

Non sono stati individuati altri rilevanti difetti di progettazione che generino punti di debolezza nel protocollo.

Difetti di progettazione

Cohn-Gordon analysis [23]

L’attacco UKS individuato in [22] non è valido in questo modello.

Non sono stati individuati altri rilevanti difetti di progettazione che generino punti di debolezza nel protocollo.



UKS è un attacco prevenibile a livello di applicazione (introducendo degli identificativi per gli utenti, e.g. il numero di telefono).

N.B. Gli attacchi possono variare a seconda dell'implementazione fornita del protocollo, ma il protocollo in sé non presenta difetti rilevanti.

Signal VS WhatsApp VS Telegram

Signal

1

Sommario

2

Applicazione
Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3

Crittografia
End-to-End

Applicazioni

Problematiche

4

Signal
Protocol

Proprietà

Il protocollo

Difetti di
progettazione

Signal VS WhatsApp
VS Telegram

5

Bibliografia

Pro

►

Team indipendente no profit: non vende dati utente per scopi di marketing

►

Open-source

►

Interfaccia personalizzabile

►

Crittografia end-to-end (anche sui metadati)

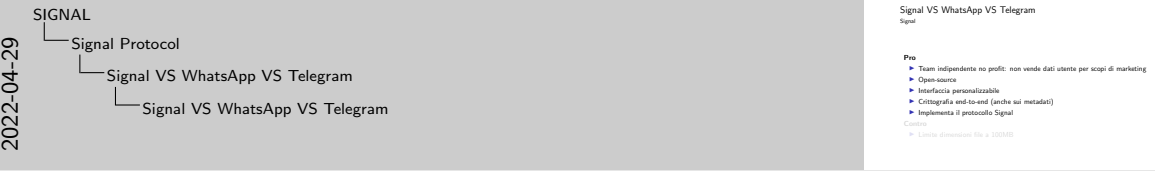
►

Implementa il protocollo Signal

Contro

►

Limite dimensioni file a 100MB



Informazioni raccolte: numero di telefono

Sono in via di sviluppo nuove versioni dell'applicazione che non lo richiedano.

Signal VS WhatsApp VS Telegram

Signal

1

Sommario

2

Applicazione
Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3

Crittografia
End-to-End

Applicazioni

Problematiche

4

Signal
Protocol

Proprietà

Il protocollo

Difetti di
progettazione

Signal VS WhatsApp
VS Telegram

5

Bibliografia

- Pro
- ▶

Team indipendente no profit: non vende dati utente per scopi di marketing
- ▶

Open-source
- ▶

Interfaccia personalizzabile
- ▶

Crittografia end-to-end (anche sui metadati)
- ▶

Implementa il protocollo Signal
- Contro
- ▶

Limite dimensioni file a 100MB



Informazioni raccolte: numero di telefono

Sono in via di sviluppo nuove versioni dell'applicazione che non lo richiedano.

Signal VS WhatsApp VS Telegram

Signal

1

Sommario

2

Applicazione Signal

Storia dell'Applicazione

L'Applicazione e il Protocollo Signal

3

Crittografia End-to-End

Applicazioni

Problematiche

4

Signal Protocol

Proprietà

Il protocollo

Difetti di progettazione

Signal VS WhatsApp VS Telegram

5

Bibliografia

L'applicazione Signal implementa il protocollo omonimo basandosi sulle librerie open-source: GitHub - Signal App

Le versioni per iOS e Android sono strutturate su più livelli:

- ▶ Cryptographic functions layer
- ▶ Protocol library layer
- ▶ Service layer

La versione desktop può essere utilizzata solo in associazione a un dispositivo Android o iOS.



- Dal livello più basso al più alto:
- Cryptographic functions layer: implementazione delle funzioni crittografiche
 - Protocol library layer: usa le funzioni del livello crittografico per implementare il protocollo
 - Service layer: combina le funzioni del livello protocollo per consentire di intraprendere effettivamente le conversazioni.
- VERSIONE DESKTOP:
- All'installazione l'applicazione desktop genera una coppia di chiavi: la chiave pubblica viene presentata come QR code da scannerizzare con l'applicazione mobile. Lo smartphone crittografa l'identity key con la chiave pubblica del client desktop e la comunica al server Signal. Da questo momento l'applicazione desktop può essere usata anche se quella mobile non è in funzione.

Signal VS WhatsApp VS Telegram

Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp VS Telegram

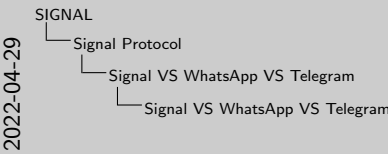
5 Bibliografia

L'applicazione Signal implementa il protocollo omonimo basandosi sulle librerie open-source: GitHub - Signal App

Le versioni per iOS e Android sono strutturate su più livelli:

- Cryptographic functions layer
- Protocol library layer
- Service layer

La versione desktop può essere utilizzata solo in associazione a un dispositivo Android o iOS.



Dal livello più basso al più alto:

- Cryptographic functions layer: implementazione delle funzioni crittografiche
- Protocol library layer: usa le funzioni del livello crittografico per implementare il protocollo
- Service layer: combina le funzioni del livello protocollo per consentire di intraprendere effettivamente le conversazioni.

VERSIONE DESKTOP:

All'installazione l'applicazione desktop genera una coppia di chiavi: la chiave pubblica viene presentata come QR code da scannerizzare con l'applicazione mobile. Lo smartphone crittografa l'identity key con la chiave pubblica del client desktop e la comunica al server Signal. Da questo momento l'applicazione desktop può essere usata anche se quella mobile non è in funzione.

[14]

Signal VS WhatsApp VS Telegram
Signal

L'applicazione Signal implementa il protocollo omonimo basandosi sulle librerie open-source: GitHub - Signal App
Le versioni per iOS e Android sono strutturate su più livelli:

- Cryptographic functions layer
- Protocol library layer
- Service layer

La versione desktop può essere utilizzata solo in associazione a un dispositivo Android o iOS.

Signal VS WhatsApp VS Telegram

Signal

1

Sommario

2

Applicazione
Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3

Crittografia
End-to-End

Applicazioni

Problematiche

4

Signal
Protocol

Proprietà

Il protocollo

Difetti di
progettazione

Signal VS WhatsApp
VS Telegram

5

Bibliografia



Dal livello più basso al più alto:

- Cryptographic functions layer: implementazione delle funzioni crittografiche
- Protocol library layer: usa le funzioni del livello crittografico per implementare il protocollo
- Service layer: combina le funzioni del livello protocollo per consentire di intraprendere effettivamente le conversazioni.

VERSIONE DESKTOP:

All'installazione l'applicazione desktop genera una coppia di chiavi: la chiave pubblica viene presentata come QR code da scannerizzare con l'applicazione mobile. Lo smartphone crittografa l'identity key con la chiave pubblica del client desktop e la comunica al server Signal. Da questo momento l'applicazione desktop può essere usata anche se quella mobile non è in funzione.

Signal VS WhatsApp VS Telegram

WhatsApp

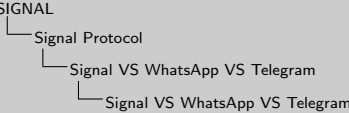
Pro

- Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie
- Implementa il protocollo Signal (l'implementazione in sé è closed-source)
- Interfaccia parzialmente personalizzabile
- 2 miliardi di utenti attivi
- Supporta autenticazione a due fattori

Contro

- Poche impostazioni sulla privacy
- Raccolta dati utente per fini di marketing
- Backup basati su cloud non crittografati, metadati non crittografati

2022-04-29



Informazioni raccolte: numero di telefono, posizione, contatti, abitudini, cronologia di navigazione, cronologia acquisti, dati pubblicitari, ID utente e

dispositivo, indirizzo e-mail, informazioni di pagamento, dati sulle prestazioni e altri contenuti utente

Recente (2019) problema di WhatsApp ha coinvolto numerose chat di gruppo i cui link erano disponibili tramite ricerca Google [bug eliminato a febbraio 2020]

Signal VS WhatsApp VS Telegram
WhatsApp

- Pro**
- Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie
 - Implementa il protocollo Signal (l'implementazione in sé è closed-source)
 - Interfaccia parzialmente personalizzabile
 - 2 miliardi di utenti attivi
 - Supporta autenticazione a due fattori

- Contro**
- Poche impostazioni sulla privacy
 - Raccolta dati utente per fini di marketing
 - Backup basati su cloud non crittografati, metadati non crittografati

Signal VS WhatsApp VS Telegram

WhatsApp

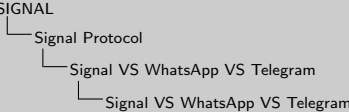
Pro

- Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie
- Implementa il protocollo Signal (l'implementazione in sé è closed-source)
- Interfaccia parzialmente personalizzabile
- 2 miliardi di utenti attivi
- Supporta autenticazione a due fattori

Contro

- Poche impostazioni sulla privacy
- Raccolta dati utente per fini di marketing
- Backup basati su cloud non crittografati, metadati non crittografati

2022-04-29



Informazioni raccolte: numero di telefono, posizione, contatti, abitudini, cronologia di navigazione, cronologia acquisti, dati pubblicitari, ID utente e

dispositivo, indirizzo e-mail, informazioni di pagamento, dati sulle prestazioni e altri contenuti utente

Recente (2019) problema di WhatsApp ha coinvolto numerose chat di gruppo i cui link erano disponibili tramite ricerca Google [bug eliminato a febbraio 2020]

Signal VS WhatsApp VS Telegram
WhatsApp

- Pro**
- Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie
 - Implementa il protocollo Signal (l'implementazione in sé è closed-source)
 - Interfaccia parzialmente personalizzabile
 - 2 miliardi di utenti attivi
 - Supporta autenticazione a due fattori
- Contro**
- Poche impostazioni sulla privacy
 - Raccolta dati utente per fini di marketing
 - Backup basati su cloud non crittografati, metadati non crittografati

Signal VS WhatsApp VS Telegram

WhatsApp

WhatsApp implementa il protocollo Signal basandosi sulle librerie open-source:
GitHub - WhatsApp

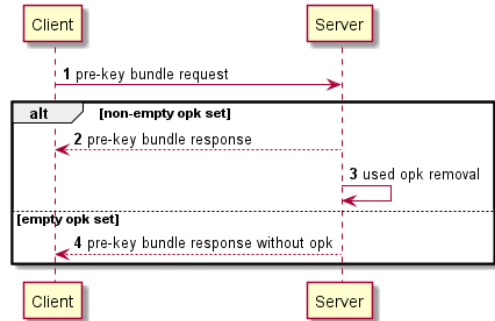
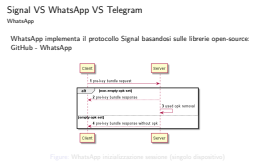


Figure: WhatsApp inizializzazione sessione (singolo dispositivo)



- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp VS Telegram
- 5 Bibliografia

Signal VS WhatsApp VS Telegram

WhatsApp

WhatsApp implementa il protocollo Signal basandosi sulle librerie open-source:
GitHub - WhatsApp

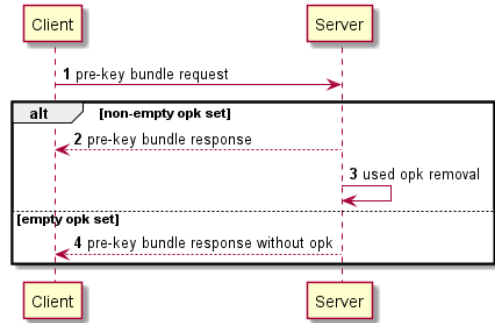
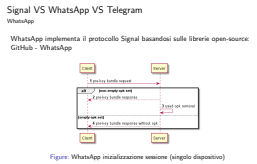


Figure: WhatsApp inizializzazione sessione (singolo dispositivo)



- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp VS Telegram
- 5 Bibliografia

Signal VS WhatsApp VS Telegram

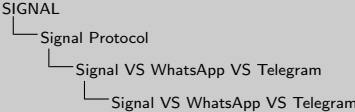
Pro

- Sicurezza: autenticazione a due fattori
- Supporta file di qualsiasi dimensione
- Eliminazione automatica dell'account se inutilizzato per troppo tempo
- Interfaccia personalizzabile

Contro

- Crittografia end-to-end solo per chat segrete, non per chat individuali e di gruppo
- Chat cloud che utilizzano la crittografia client-server: l'azienda ha accesso ai messaggi
- Usa GPS per trovare utenti nelle vicinanze

2022-04-29



Informazioni raccolte: indirizzo IP, dispositivi, cronologia dei nomi utente e contatti.

Messaggi crittografati sul dispositivo utente ma decrittati sui server, ri-crittografati e poi inviati al destinatario per essere decrittati in modo definitivo.

Telegram possiede le chiavi lato server e può teoricamente accedere al contenuto dei messaggi.

Telegram garantisce di non aver condiviso ad oggi alcun dato con terze parti e/o enti governativi.

Signal VS WhatsApp VS Telegram
Telegram

- Pro**
- Sicurezza: autenticazione a due fattori
 - Supporta file di qualsiasi dimensione
 - Eliminazione automatica dell'account se inutilizzato per troppo tempo
 - Interfaccia personalizzabile
- Contro**
- Crittografia end-to-end solo per chat segrete, non per chat individuali e di gruppo
 - Chat cloud che utilizzano la crittografia client-server: l'azienda ha accesso ai messaggi
 - Usa GPS per trovare utenti nelle vicinanze

Signal VS WhatsApp VS Telegram

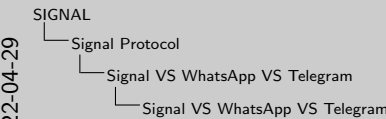
Telegram

Pro

- Sicurezza: autenticazione a due fattori
- Supporta file di qualsiasi dimensione
- Eliminazione automatica dell’account se inutilizzato per troppo tempo
- Interfaccia personalizzabile

Contro

- Crittografia end-to-end solo per chat segrete, non per chat individuali e di gruppo
- Chat cloud che utilizzano la crittografia client-server: l’azienda ha accesso ai messaggi
- Usa GPS per trovare utenti nelle vicinanze



Informazioni raccolte: indirizzo IP, dispositivi, cronologia dei nomi utente e contatti.

Messaggi crittografati sul dispositivo utente ma decrittati sui server, ri-crittografati e poi inviati al destinatario per essere decrittati in modo definitivo.

Telegram possiede le chiavi lato server e può teoricamente accedere al contenuto dei messaggi.

Telegram garantisce di non aver condiviso ad oggi alcun dato con terze parti e/o enti governativi.

Signal VS WhatsApp VS Telegram
Telegram
Pro
<ul style="list-style-type: none">► Sicurezza: autenticazione a due fattori► Supporta file di qualsiasi dimensione► Eliminazione automatica dell’account se inutilizzato per troppo tempo► Interfaccia personalizzabile
Contro
<ul style="list-style-type: none">► Crittografia end-to-end solo per chat segrete, non per chat individuali e di gruppo► Chat cloud che utilizzano la crittografia client-server: l’azienda ha accesso ai messaggi► Usa GPS per trovare utenti nelle vicinanze

Signal VS WhatsApp VS Telegram

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni Problematiche

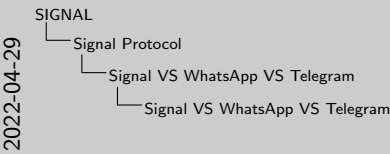
4 Signal Protocol

Proprietà
Il protocollo
Difetti di progettazione
Signal VS WhatsApp VS Telegram

5 Bibliografia

Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal, Telegram utilizza il protocollo proprietario **MTPROTO** per la crittografia dei messaggi.

Essendo a implementazione closed-source non permette l'analisi completa da parte dei ricercatori.



In ambito crittografico è considerata buona norma utilizzare protocolli e algoritmi verificati da un numero di ricercatori o esperti maggiore possibile. Ciò si contrappone alla logica di *security through obscurity* che invece vorrebbe che i protocolli siano tanto più sicuri quanto meno sono stati analizzati.

Per questo motivo protocolli open-source sono in genere preferibili, in quanto è più probabile che vengano rilevati eventuali bug in protocolli analizzati da team più ampi e numerosi.

Signal VS WhatsApp VS Telegram
Telegram

Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal, Telegram utilizza il protocollo proprietario **MTPROTO** per la crittografia dei messaggi.

Essendo a implementazione cloud-source non permette l'analisi completa da parte dei ricercatori.

Signal VS WhatsApp VS Telegram

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

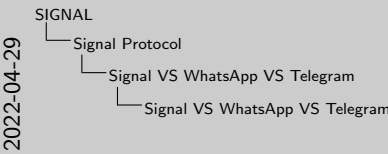
Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal, Telegram utilizza il protocollo proprietario **MTPROTO** per la crittografia dei messaggi.
Essendo a implementazione closed-source non permette l'analisi completa da parte dei ricercatori.



In ambito crittografico è considerata buona norma utilizzare protocolli e algoritmi verificati da un numero di ricercatori o esperti maggiore possibile. Ciò si contrappone alla logica di *security through obscurity* che invece vorrebbe che i protocolli siano tanto più sicuri quanto meno sono stati analizzati.

Per questo motivo protocolli open-source sono in genere preferibili, in quanto è più probabile che vengano rilevati eventuali bug in protocolli analizzati

da team più ampi e numerosi.

Signal VS WhatsApp VS Telegram
Telegram

Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal, Telegram utilizza il protocollo proprietario **MTPROTO** per la crittografia dei messaggi.
Essendo a implementazione closed-source non permette l'analisi completa da parte dei ricercatori.

Signal VS WhatsApp VS Telegram

- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Proprietà
 - Il protocollo
 - Difetti di progettazione
 - Signal VS WhatsApp VS Telegram
- 5 Bibliografia

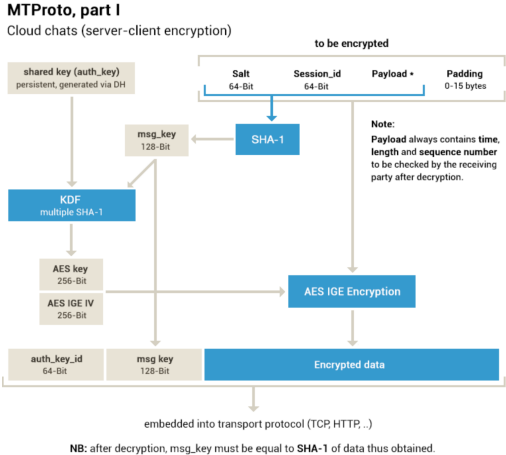
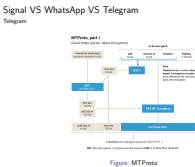
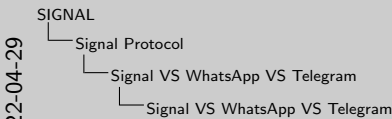


Figure: MTPROTO



Il salt, *session_id* e *payload* del messaggio vengono crittografati con *SHA-1* a creare una *msg_key*.
La *msg_key* viene usata insieme alla *auth_key* come input di una *KDF* che restituisce una chiave *AES* e un vettore di inizializzazione da utilizzare a loro volta come input di una funzione *AES IGE Encryption*.
Da quest'ultima funzione si ottengono i dati crittografati, ai quali vengono aggiunti *auth_key_id* al fine di identificare l'utente e *msg_key*.
Al fine di autenticare il messaggio, una volta decodificato viene comparata la *msg_key* ricevuta con quella computata localmente.[24]

Bibliografia I

1

Sommario

2

Applicazione
Signal

Storia
dell'Applicazione

L'Applicazione e il
Protocollo Signal

3

Crittografia
End-to-End

Applicazioni

Problematiche

4

Signal
Protocol

Proprietà

Il protocollo

Difetti di
progettazione

Signal VS WhatsApp
VS Telegram

5

Bibliografia

D. J. Lumb, “The story of signal,” *Increment*, no. 7, 2018, October.

A. Greenberg, “Hacker lexicon: What is the signal encryption protocol?,” 2020, November 29.

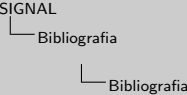
M. Marlinspike, “Whatsapp’s signal protocol integration is now complete,” Apr. 5, 2016.

A. Greenberg, “Hacker lexicon: What is end-to-end encryption?,” 2014, November 15.

“Cos’è la e2ee (end-to-end encryption)?,”

Y. Grauer, “Mr. robot uses protonmail, but it still isn’t fully secure,” 2015, October 7.

2022-04-29



Bibliografia I

D. J. Lumb, “The story of signal,” *Increment*, no. 7, 2018, October.

A. Greenberg, “Hacker lexicon: What is the signal encryption protocol?,” 2020, November 29.

M. Marlinspike, “Whatsapp’s signal protocol integration is now complete,” Apr. 5, 2016.

A. Greenberg, “Hacker lexicon: What is end-to-end encryption?,” 2014, November 15.

“Cos’è la e2ee (end-to-end encryption)?,”

Y. Grauer, “Mr. robot uses protonmail, but it still isn’t fully secure,” 2015, October 7.

Bibliografia II

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End


Applicazioni
Problematiche

4 Signal
Protocol


Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia

 K. Poulsen, “Snowden’s email provider loses appeal over encryption keys,” 2014, April 16.

 B. Gellman and J. Markon, “Edward snowden says motive behind leaks was to expose ‘surveillance state’,” *The Washington Post*, June 10, 2013.

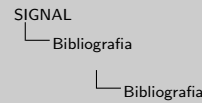
 R. Singel, “Encrypted e-mail company hushmail spills to feds,” 2007, November 7.

 C. M. East, N. A. Program, and C. T. Program, “Why telegram’s security flaws may put iran’s journalists at risk - committee to protect journalists,” 2016, May 1.







 “Cryptography concepts - fundamentals - e3kit — virgil security,” 2020.

 B. Lutkevich and M. Bacon, “end-to-end encryption (e2ee),” June 2021.

2022-04-29



Bibliografia II

-  K. Poulsen, “Snowden’s email provider loses appeal over encryption keys,” 2014, April 16.
-  B. Gellman and J. Markon, “Edward snowden says motive behind leaks was to expose ‘surveillance state’,” *The Washington Post*, June 10, 2013.
-  R. Singel, “Encrypted e-mail company hushmail spills to feds,” 2007, November 7.
-  C. M. East, N. A. Program, and C. T. Program, “Why telegram’s security flaws may put iran’s journalists at risk - committee to protect journalists,” 2016, May 1.
-  “Cryptography concepts - fundamentals - e3kit — virgil security,” 2020.
-  B. Lutkevich and M. Bacon, “end-to-end encryption (e2ee),” June 2021.

Bibliografia III

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia



“Signal documentation,”



D. Van Dam, “Analysing the signal protocol - a manual and automated analysis of the signal protocol,” Master’s thesis, Radboud University, 2019.



M. Marlinspike and T. Perrin, “The x3dh key agreement protocol,” tech. rep., Open Whisper Systems, 2016.



W. Diffie and M. Hellman, “New directions in cryptography,” in *IEEE Transactions on Information Theory*, pp. 644–654, 1976.

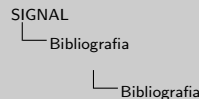


B. Jacobs and J. Daemen, “Computer security: Public key crypto,” 2016.



H. Krawczyk and P. Eronen, “Hmac-based extract-and-expand key derivation function (hkdf),” 2010.

2022-04-29



Bibliografia III

- “Signal documentation.”
- D. Van Dam, “Analysing the signal protocol - a manual and automated analysis of the signal protocol,” Master’s thesis, Radboud University, 2019.
- M. Marlinspike and T. Perrin, “The x3dh key agreement protocol,” tech. rep., Open Whisper Systems, 2016.
- W. Diffie and M. Hellman, “New directions in cryptography,” in *IEEE Transactions on Information Theory*, pp. 644–654, 1976.
- B. Jacobs and J. Daemen, “Computer security: Public key crypto,” 2016.
- H. Krawczyk and P. Eronen, “Hmac-based extract-and-expand key derivation function (hkdf),” 2010.

Bibliografia IV

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia



M. Marlinspike and T. Perrin, “The double ratchet algorithm,” tech. rep., Open Whisper Systems, 2016.



M. Pound, “Double ratchet messaging encryption - computerphile.” Video.



M. Marlinspike and T. Perrin, “The sesame algorithm: Session management for asynchronous message encryption,” tech. rep., Open Whisper Systems, 2017.

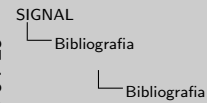


T. Frosch, C. Mainka, C. Bader, F. Bergsma, J. Schwenk, and T. Holz, “How secure is textsecure?,” in *2016 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 457–472, 2016.



K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, “A formal security analysis of the signal messaging protocol,” in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 451–466, 2017.

2022-04-29



Bibliografia IV

- M. Marlinspike and T. Perrin, “The double ratchet algorithm,” tech. rep., Open Whisper Systems, 2016.
- M. Pound, “Double ratchet messaging encryption - computerphile.” Video.
- M. Marlinspike and T. Perrin, “The sesame algorithm: Session management for asynchronous message encryption,” tech. rep., Open Whisper Systems, 2017.
- T. Frosch, C. Mainka, C. Bader, F. Bergsma, J. Schwenk, and T. Holz, “How secure is textsecure?,” in *2016 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 457–472, 2016.
- K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, “A formal security analysis of the signal messaging protocol,” in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 451–466, 2017.

Bibliografia V

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Proprietà
Il protocollo
Difetti di
progettazione
Signal VS WhatsApp
VS Telegram

5 Bibliografia



Telegram.org, “Mtproto mobile protocol. core.,”

2022-04-29

SIGNAL

Bibliografia

Bibliografia

Bibliografia V

Telegram.org, “Mtproto mobile protocol. core.,”