# PLAN DU PROJET

Introduction

1. Contexte (on parle succinctement de ce qu’est un réseau communautaire et on prend le cas d’une communauté universitaire
2. Présentation du projet
3. Qu’est-ce que le protocole Signal
4. Historique
5. Caractéristiques (forces, modèles scientifiques et faiblesses)
6. Usage du protocole
7. Influence du protocole
8. Comparaison/Pourquoi le protocole signal
9. Méthodes utilisées (spécification des besoins, conception, implémentation, test, déploiement (modèle en cascade))
10. Analyse
11. Conception
12. Implémentation
13. Difficultés rencontrées
14. Perspectives

Références

Annexes

Guide de déploiement et guide user

Conclusion

# QUELQUES INFOS INTERESSANTES

Le Signal Protocol, anciennement connu sous le nom de TextSecure Protocol, est un protocole cryptographique (en) non-fédéré pouvant être utilisé pour chiffrer de bout en bout des appels vocaux et vidéo1 ainsi que des conversations par messagerie instantanée2. Il a été développé par Open Whisper Systems en 20132 et a été introduit pour la première fois dans l'application open source TextSecure, devenue par la suite Signal. Il a depuis été implémenté dans d'autres applications telles WhatsApp3, Facebook Messenger (en mode « conversation secrète ») et Google Allo (en « mode incognito »).

Le protocole combine l'algorithme double ratchet avec des prekeys et un triple échange de clés Diffie-Hellman (3-DH)4, ainsi que Curve25519, Advanced Encryption Standard et Keyed-hash message authentication code comme primitives5.

Le protocole est open-source et sous licence GPL-3.0. Le code source est disponible sur https://github.com/signalapp

Les premières versions du protocole étaient implémentées dans les applications TextSecure et RedPhone, développées par Open Whisper Systems. Après le rachat de la startup par Twitter en 2011, le code des applications a été libéré sur GitHub.

TextSecure et RedPhone sont fusionnées en une application, Signal, en 2014. Le protocole est alors nommé Axolotl. C'est en mars 2016 qu'il prend son nom actuel de Signal Protocol, par souci de clarté[7](https://fr.wikipedia.org/wiki/Signal_Protocol#cite_note-7).

Les principaux développeurs du protocole, Trevor Perrin et Moxie Marlinspike, reçoivent le prix Levchin en 2017. Le professeur d'université Dan Boneh, président du jury, estime que le développement du protocole a été décisif pour diffuser la cryptologie au grand public, ce qui aurait pu prendre sinon « plusieurs décennies supplémentaires »

29.11.2020 LAST WEEK, WITH little fanfare, Google announced a change that could soon make its 2 billion Android users worldwide far harder to surveil: The tech giant says it's rolling out a beta version of its Android messaging app that will now use end-to-end encryption by default. That level of encryption, while limited to one-on-one conversations, is designed to prevent anyone else from eavesdropping—not phone carriers, not intelligence agencies, not a hacker who has taken over the local Wi-Fi router, not even Google itself will have the keys to decrypt and read those billions of messages.

The news isn't just a win for global privacy. It's also a win for one particular encryption system: the Signal protocol, which is well on its way to accounting for a majority of the world's real-time text conversations. As this protocol becomes the de facto standard for encrypted messaging in most major services, it's worth understanding what sets it apart from other forms of end-to-end encrypted messaging.

You might already know Signal thanks to the popular end-to-end encrypted text messaging app by the same name, created by cypherpunk Moxie Marlinspike and in recent years hosted by the nonprofit Signal Foundation. Signal, the app, has an unparalleled reputation for security and privacy, with high-profile endorsements from NSA whistleblower Edward Snowden and WhatsApp founder Brian Acton, who left WhatsApp in 2018 to serve as the Signal Foundation's executive director.

But the underlying crypto system that Marlinspike designed and on which Signal is built, known as the Signal protocol, has spread far beyond its eponymous app. WhatsApp first adopted the Signal protocol in 2014 to end-to-end encrypt all messages between Android phones, in what Marlinspike told WIRED was "the largest deployment of end-to-end encryption ever." WhatsApp switched it on by default for all billion-plus users two years later. Shortly thereafter, Google rolled out end-to-end encryption via the Signal protocol as an opt-in feature for its now-defunct Allo messenger and in its Duo video chat service. Facebook followed by adding it as an opt-in "Secret Conversations" feature in Facebook Messenger a few months later. Google's decision to integrate the Signal protocol into Android's messaging app by default represents the biggest new collection of phones to adopt the standard in years, with hundreds of millions more devices

Alors pourquoi les géants de la technologie du monde ont-ils tous choisi Signal comme protocole de chiffrement de prédilection ? Sa caractéristique la plus remarquable, selon Matthew Green, professeur d'informatique et cryptographe à Johns Hopkins, est la façon dont il met en œuvre ce que l'on appelle le « secret avancé parfait ». Avec la plupart des systèmes de cryptage, lorsqu'une application est installée sur un téléphone, elle crée une paire de clés permanente qui sert à crypter et décrypter les messages : une clé « publique » qui est envoyée au serveur de messagerie et qui servira à identifier l'utilisateur, et une clé "privée" qui ne quitte jamais le téléphone de l'utilisateur. Cependant, si cette clé privée est compromise, comme si quelqu'un pirate ou s'empare de votre téléphone, tous vos messages sont potentiellement vulnérables au déchiffrement. Même si vous avez supprimé des messages de votre téléphone, la clé peut déchiffrer tous les messages chiffrés que les indiscrets ont réussi à enregistrer lorsqu'ils ont initialement voyagé sur le réseau.

"Chaque fois que vous envoyez un message, votre clé est mise à jour", explique Green. "Cela signifie que si votre téléphone est volé à l'heure X, tout message que vous envoyez avant l'heure X devrait toujours être en sécurité." Cette assurance fait défaut, note Green, dans iMessage d'Apple, une autre application de messagerie populaire qui utilise un cryptage de bout en bout mais n'offre pas une confidentialité de transmission parfaite.

Mais le système de cryptage sous-jacent conçu par Marlinspike et sur lequel Signal est construit, connu sous le nom de protocole Signal, s'est étendu bien au-delà de son application éponyme. WhatsApp a adopté pour la première fois le protocole Signal en 2014 pour crypter de bout en bout tous les messages entre les téléphones Android, dans ce que Marlinspike a déclaré à WIRED était "le plus grand déploiement de cryptage de bout en bout jamais réalisé". WhatsApp l'a activé par défaut pour tous les milliards d'utilisateurs deux ans plus tard. Peu de temps après, Google a déployé le cryptage de bout en bout via le protocole Signal en tant que fonctionnalité d'inscription pour son ancien messager Allo et dans son service de chat vidéo Duo. Facebook a suivi en l'ajoutant en tant que fonctionnalité « Conversations secrètes » dans Facebook Messenger quelques mois plus tard. La décision de Google d'intégrer le protocole Signal dans l'application de messagerie d'Android par défaut représente la plus grande nouvelle collection de téléphones à adopter la norme depuis des années, avec des centaines de millions d'appareils supplémentaires.

<https://signal.org/docs/>

<https://github.com/signalapp/libsignal-protocol-java>

https://medium.com/@justinomora/demystifying-the-signal-protocol-for-end-to-end-encryption-e2ee-ad6a567e6cb4