II. PRESENTATION DU PROTOCOLE SIGNAL

1. HISTORIQUE

Le développement du protocole signal a été lance par Trevor Perrin et Moxie Marlinspike en 2013. La première version du protocole, TextSecure V1, était basee sur la messagerie Off-the-record (OTR) qui est un protocole de cryptage combinant l’algorithme de clé symétrique AES avec une longueur de clé de 128 bits, un échange de clés Diffie-Hellman et la fonction de hashage SHA-1.

Le 24 fevrier 2014, Open Whisper Systems a introduit TextSecure v2, Il a apporté la prise en charge de la communication Asynchrone (« messages hors ligne ») en tant que nouvelle fonctionnalité majeure, ainsi qu'une meilleure résilience avec un ordre déformé des messages et une prise en charge plus simple des conversations avec plusieurs participants.

La troisième version du protocole, TextSecure v3, a apporté quelques modifications aux primitives cryptographiques et au protocole filaire. En mars 2016, les développeurs ont renommé le protocole en protocole de signal.

1. QU’ES CE QUE LE PROTOCOLE SIGNAL ?

Le protocole Signal est un protocole cryptographique non fédéré qui peut est utilise pour fournir un cryptage de bout en bout pour les appels vocaux et les conversations de messagerie instantanée. Plusieurs applications à code source fermé implémente le protocole, telles que WhatsAppp, qui est crypte les conversations de plus d'un milliard de personnes dans le monde ou Google qui fournit un cryptage de bout en bout par défaut à toutes les conversations basées sur RCS (Rich Communication Service. Facebook Messenger dit également offrir le protocole pour les conversations secrètes facultatives, tout comme Skype pour ses conversations privées. Signal comprend plusieurs propriétés de sécurité peu courantes (telles que « futur secret » ou « sécurité post-compromis »), activées par une nouvelle technique appelée cliquet dans laquelle les clés de session sont mises à jour à chaque message envoyé.

Le protocole combine l’algorithme Double Ratchet, des pré-clés et une triple poignée de main Diffie-Hellman (X3DH) à courbe elliptique et utilise Curve25519, AES-256 et HMAC-SHA256.

1. FONCTIONNEMENT DU PROTOCOLE SIGNAL

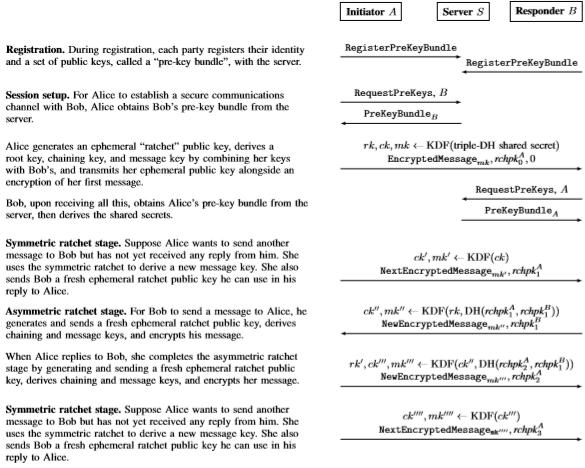
Le protocole Signal vise à envoyer des messages cryptés d'une partie à une autre. À un niveau élevé, Signal est un protocole de canal sécurisé asynchrone, avec des clés calculées par un protocole AKE (Authenticated Key Exchange) à plusieurs étapes, entre un initiateur Alice, un répondeur Bob, à l'aide d'un serveur de distribution de clés qui ne fait que stocker et relayer les informations entre les parties, mais n'effectue aucun calcul.

Signal suppose que chaque partie dispose d'une paire de clés publique/privée à long terme, appelée clé d'identité. Cependant, étant donné que les parties peuvent être hors ligne à tout moment, les solutions standard d'échange de clés authentifiées (AKE) ne peuvent pas être directement appliquées. Par exemple, l'utilisation de l'échange de clés DH (Diffie-Hellman) pour obtenir le secret de transmission parfaite nécessite que les deux parties fournissent de nouvelles clés DH (Diffie-Hellman) éphémères, mais le destinataire peut être hors ligne au moment de l'envoi.

Au lieu de cela, Signal implémente un protocole de transmission asynchrone, en exigeant des destinataires potentiels qu'ils envoient au préalable des lots de clés publiques éphémères, lors de l'enregistrement ou ultérieurement. Lorsque l'expéditeur souhaite envoyer un message, il obtient des clés pour le destinataire auprès d'un serveur intermédiaire (qui agit uniquement comme un tampon) et exécute un protocole de type AKE en utilisant les clés à long terme et éphémères pour calculer une clé de chiffrement du message. Cette configuration de base est ensuite étendue en rendant les clés de message dépendantes de tous les échanges précédemment effectués entre les parties, en utilisant une combinaison de mécanismes de « cliquetis » pour former des « chaînes ». De nouvelles valeurs aléatoires et secrètes sont également introduites dans les calculs à différents points, inuent sur les futures clés de message calculées par les partenaires communicants.

Signal est un protocole d'échange de clés authentifié en plusieurs étapes, les principales étapes sont les suivantes :

* **Inscription :** Lors de l'installation (et périodiquement par la suite), Alice et Bob enregistrent indépendamment leur identité auprès d'un serveur de distribution de clés et téléchargent des clés publiques à long terme, à moyen terme et éphémères.
* **Configuration de la session :** Alice demande et reçoit un ensemble de clés publiques de Bob du serveur de distribution de clés et les utilise pour configurer une session de messagerie de longue durée et établir des clés de chiffrement symétriques initiales. C'est ce qu'on appelle la poignée de main TripleDH ou X3DH.
* **Messagerie synchrone (mises à jour asymétriques à cliquet) :** Lorsqu'Alice veut envoyer un message à Bob (ou vice versa) et vient de recevoir un message de Bob, elle échange des valeurs Difﬁe–Hellman avec Bob, générant de nouveaux secrets partagés et les utilise pour commencer de nouvelles chaînes de clés de message. Chaque opération DH est une étape du « cliquet asymétrique » (et se déroule strictement à la manière d'un ping-pong).
* **Messagerie asynchrone (alias à cliquet symétrique) :** Lorsqu'Alice veut envoyer un message à Bob (ou vice versa) mais n'a pas reçu de message de Bob depuis son dernier message envoyé à Bob, elle dérive une nouvelle clé de chiffrement symétrique de son état précédent à l'aide d'un PRF. Chaque application PRF est une étape du « cliquet symétrique ».



**Fig 1 :** **Flux de messages d'un exemple Exécution de signal entre deux clients A et B via un serveur S**

1. PROPRIETES

Le protocole fournit la confidentialité, l'intégrité, l’authentification, la cohérence des participants, la validation de la destination, le secret de transmission, la sécurité post-compromis (alias secret futur), la préservation de la causalité, la dissociation des messages, la répudiation des messages, la répudiation de la participation et l'Asy chronicité. Il ne garantit pas la préservation de l'anonymat et nécessite des serveurs pour le relais des messages et le stockage du matériel à clé publique. Le protocole de signal prend également en charge les discussions de groupe cryptées de bout en bout. Le protocole de discussion de groupe est une combinaison d'un double cliquet par paire et d'un cryptage multicast. En plus des propriétés fournies par le protocole one-to-one, le protocole de discussion de groupe fournit la cohérence du locuteur, la résilience dans le désordre, la résilience des messages abandonnés, l'égalité de calcul, l'égalité de confiance, la messagerie de sous-groupe.

1. INFLUENCES

Le protocole signal a eu une influence sur d'autres protocoles cryptographiques en ce sens qu’en mai 2016, Viber a déclaré que son protocole de cryptage est une implémentation personnalisée qui « utilise les mêmes concepts » que le protocole signal, de même que Les développeurs de Forsta.

L'algorithme Double Ratchet qui a été introduit dans le cadre du protocole signal a également été adopté par d'autres protocoles tels que : OMEMO est un protocole d'extension XMPP (XEP) qui a été introduit dans l'application de messagerie Conversations et approuvé par la XMPP Standards Foundation (XSF) en décembre 2016 sous le nom de XEP-0384 et Matrix qui est un protocole de communication ouvert, une bibliothèque qui fournit un cryptage optionnel de bout en. Les développeurs de Wire ont déclaré que leur application utilise une implémentation personnalisée de l'algorithme Double Ratchet également.

1. COMPARAISON DU PROTOCOLE SIGNAL AVEC D’AUTRES PROTOCOLES
2. **OpenPGP**

OpenPGP est un format de stockage de messages et de clés cryptographiques. Il est notamment employé pour sécuriser des messages électroniques. Il convient pour des réseaux de messagerie décentralisés ou lorsque le destinataire est hors-ligne (protocole non interactif). Il permet également d’assurer de la protection de bout en bout, puisque ce sont les messages qui sont chiﬀrés et non le canal de transport de ces derniers. En outre, il est possible d’utiliser OpenPGP pour envoyer des messages à un groupe d’utilisateurs. Pour ce faire, la clé de chiﬀrement du message est chiﬀrée avec les clés publiques de chacun des destinataires. Les clés publiques ainsi utilisées doivent être préalablement créées, et stockées dans des certiﬁcats OpenPGP. Ces certiﬁcats permettent d’associer des identités – éventuellement des pseudonymes – à ces clés publiques. Ces certiﬁcats sont transmis ponctuellement aux autres utilisateurs grâce à des annuaires ou par une remise en main propre. OpenPGP présente cependant des limites, en regard de solutions alternatives spécialisées pour le chiﬀrement de messagerie quasi instantanée. Ainsi, il n’oﬀre pas, de manière inhérente, de conﬁdentialité persistante du fait de la transmission ponctuelle des certiﬁcats : le rafraîchissement des clés est du ressort de l’utilisateur. En outre, pour la protection en intégrité des messages, l’utilisateur n’a le choix qu’entre des solutions imparfaites. L’une est sujette à des attaques par dégradation du niveau de sécurité (downgrade attack) et l’autre use de signatures cryptographiques non répudiables, ce qui n’est pas toujours souhaitable.

1. **Oﬀ-the-Record**

Le protocole Oﬀ-the-Record a été spéciﬁé, pour la première fois, en 2004, sa version la plus récente date de 2012. Ce mécanisme permet l’échange de clés et de messages sécurisés de bout en bout. L’établissement de la session protégée est eﬀectué entre deux parties de manière interactive. Autrement dit, il est nécessaire que les participants soient en ligne simultanément pour l’établissement de cette session. Cette propriété exclut un usage asynchrone, et restreint donc ce protocole à la messagerie instantanée. Le protocole Oﬀ-the-Record présente également une propriété de sécurité qui serait favorable à la vie privée. Ainsi, Oﬀ-the-Record permettrait à un expéditeur de dénier le contenu d’un message, tout en garantissant au destinataire la légitimité et l’intégrité du message reçu. Pour ce faire, les clés utilisées pour calculer des motifs d’intégrité de messages sont divulguées en clair après réception et vériﬁcation de ces messages. Conjuguée à un mode de chiﬀrement malléable et à un clair connu, cette méthode peut permettre à un observateur de forger un message chiﬀré et intègre arbitraire. Cet observateur serait cependant incapable de prouver à un tiers l’authenticité d’un message qu’il détient. Malgré ses nombreux avantages, le protocole Oﬀ-the-Record, tel que spéciﬁé dans sa version la plus récente (3.4), souﬀre d’un problème d’obsolescence cryptographique.