

ROBERT : un protocole de suivi des contacts respectueux de la vie privée ¹

Inria, France ²
Fraunhofer AIESEC, Allemagne

18 avril 2020

Les applications de suivi des contacts

Le virus COVID-19 est difficile à détecter car de nombreuses personnes peuvent être porteuses, et donc contagieuses, sans le savoir et avant même d'en ressentir les symptômes. D'où un risque important de transmission du virus à de nombreuses personnes de leur entourage.

Le principal objectif des applications mobiles de suivi des contacts est d'informer les personnes qu'elles se sont trouvées à proximité de porteurs du virus COVID-19 même si ceux-ci ne présentaient pas de symptômes et n'avaient pas été testés au moment de ce contact.

Pour ce faire, l'application mobile peut utiliser une communication à courte distance en Bluetooth (disponible sur tous les téléphones portables modernes) afin de détecter quand deux utilisateurs sont proches. De telles applications permettent ensuite aux utilisateurs de savoir qu'ils ont été en contact avec des porteurs du virus COVID-19. Le fait de garantir les normes les plus élevées en matière de protection de la vie privée et de sécurité est une condition sine qua non d'adoption de ce type d'application. Dans ce document nous proposons une solution -- le protocole ROBERT (acronyme anglais de [ROBust and privacy-presERving proximity Tracing](#)) -- qui peut être utilisée pour construire de telles applications mobiles de suivi des contacts.

Le protocole ROBERT s'inscrit dans le cadre de l'initiative PEPP-PT ([Pan European Privacy-Preserving Proximity Tracing](#)), dont le but principal est de permettre le développement de solutions de suivi de contacts respectueuses des normes européennes en matière de protection des données, de vie privée et de sécurité, dans le cadre d'une réponse plus globale à la pandémie.

Principes relatifs à la sécurité et à la protection de la vie privée

Pour les applications de suivi des contacts, il est primordial de garantir la protection de la vie privée des utilisateurs et la sécurité des données traitées tout en apportant les fonctionnalités les plus efficaces pour limiter la propagation du virus. Ces exigences sont essentielles pour leur

¹ Ce document est en phase avec les spécifications techniques du protocole ROBERT, version 1.0 : <https://github.com/ROBERT-proximity-tracing>

² Travail collaboratif d'Inria conduit par l'équipe PRIVATICS.

assurer une légalité et favoriser leur acceptabilité par les citoyens qui doivent être libres de les installer mais aussi les désinstaller à tout moment. Nous ne traitons pas ici de l'efficacité de ces applications car elles doivent être calibrées et évaluées en collaboration avec des épidémiologistes. Nous nous concentrons sur les questions de sécurité et de respect de la vie privée.

Pour protéger la vie privée des utilisateurs, les applications de suivi des contacts doivent respecter les principes de proportionnalité et de pertinence du traitement des données personnelles, conformément au RGPD, et ne traiter que les informations nécessaires à l'accomplissement de leur finalité. En particulier, les applications de suivi des contacts ne devraient pas collecter de données de géolocalisation mais plutôt s'appuyer sur la collecte de pseudonymes temporaires.

Les applications de suivi des contacts doivent également fournir les plus hautes garanties en matière de respect de la vie privée des utilisateurs, tant vis à vis des autorités centrales, que des autres utilisateurs ou d'acteurs tiers malicieux. Plus important encore, ces applications ne doivent pas pouvoir être transformées en outils d'espionnage par leurs utilisateurs, notamment pour savoir si des personnes séjournant, travaillant, ou vivant dans un endroit spécifique ont été diagnostiquées positives pour le virus COVID-19.



Ces applications doivent être sécurisées et fonctionner même en présence d'utilisateurs ou de tiers malveillants qui chercheraient à interférer dans le protocole ou entraver leur fonctionnement.

Enfin, ces applications doivent comporter un mécanisme permettant de les désactiver dès qu'elles ne sont plus nécessaires, c'est-à-dire à la fin de la pandémie, ou à la demande de leur utilisateur.

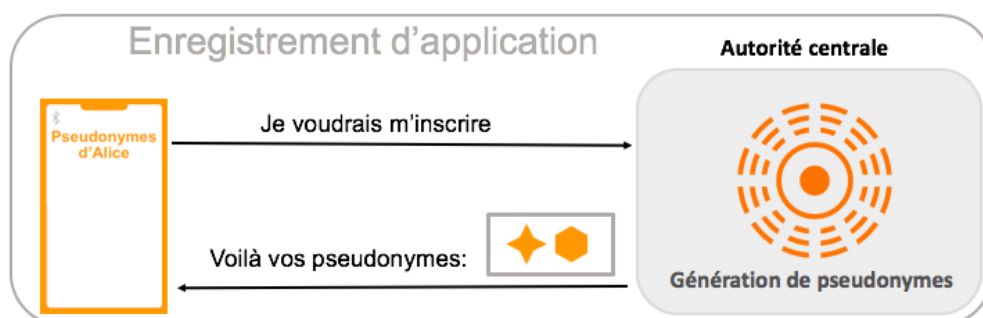
Le protocole ROBERT: un protocole de suivi des contacts respectueux de la vie privée

Nous proposons le protocole ROBERT (ROBust and privacy-presERving proximity Tracing) qui peut être utilisé par des applications pour un suivi des contacts respectueux de la vie privée. Pour détecter si deux utilisateurs se sont trouvés à proximité l'un de l'autre, l'application peut s'appuyer sur les communications à courte portée de la technologie sans fil Bluetooth.

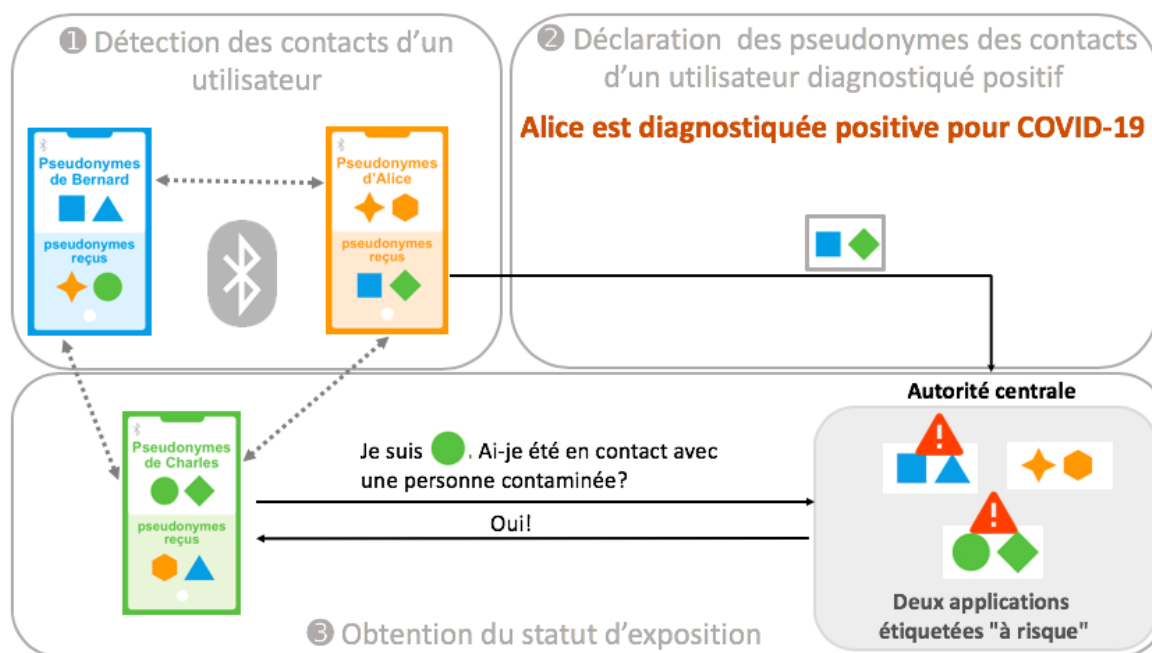
L'utilisateur installe volontairement sur son téléphone portable une application mobile qui utilise ROBERT. Lors de l'installation, l'application s'enregistre auprès de l'autorité centrale. Cette dernière génère un ensemble de pseudonymes temporaires et les partage avec l'application de l'utilisateur. On peut considérer ces pseudonymes comme des "faux noms" temporaires associés à l'application de l'utilisateur. En pratique, ces pseudonymes ressemblent à des nombres aléatoires ; dans ce document, par souci de simplicité, nous utiliserons des formes géométriques.

A titre d'illustration simplifiée, pour l'utilisatrice prénommée **Alice** dans le schéma ci-dessous, l'application reçoit plusieurs pseudonymes -- ici  et  -- qui seront utilisés l'un après l'autre. Ce mécanisme permet de protéger sa vie privée et de garantir qu'aucun observateur externe ou

utilisateur de l'application ne pourra relier ces pseudonymes pour la suivre dans le temps. Seul l'utilisateur lui-même et l'autorité centrale peuvent faire le lien entre les pseudonymes d'un utilisateur donné.





Le protocole comporte trois phases principales : la détection des contacts d'un utilisateur, la déclaration des pseudonymes des contacts d'un utilisateur diagnostiqué positif et l'obtention du statut d'exposition.





① Détection des contacts d'un utilisateur

L'application mobile d'**Alice** utilise des communications à courte distance en Bluetooth pour "annoncer" un de ses pseudonymes --  ou  dans notre exemple -- à tout autre utilisateur qui se trouve à proximité immédiate d'**Alice**. Dans l'exemple ci-dessus, l'application d'**Alice** annonce sa présence aux applications de **Bernard** et **Charles**.


L'application mobile de chaque utilisateur, **Alice**, **Bernard** et **Charles**, s'appuie sur des communications Bluetooth pour recueillir tous les pseudonymes des utilisateurs qui se trouvent à proximité. L'application mobile enregistre ensuite ces pseudonymes localement sur le téléphone

portable de chaque utilisateur. Dans notre exemple, **Alice** a rencontré **Bernard** et **Charles** et, par conséquent, leurs pseudonymes,  et , sont enregistrés sur le téléphone portable d' Alice.

② Déclaration des pseudonymes des contacts d'un utilisateur diagnostiqué positif

Si **Alice** est testée positive au COVID-19, elle peut décider, pour aider les personnes qu'elle a côtoyées ces deux dernières semaines, de communiquer anonymement leurs pseudonymes ( et ) à l'autorité centrale. L'autorité centrale reçoit ces pseudonymes **sans aucune information** sur **Alice** : elle n'a **accès ni aux pseudonymes ni aux noms réels des utilisateurs diagnostiqués positifs**. Chaque fois que l'autorité reçoit un pseudonyme correspondant à un contact avec un utilisateur diagnostiqué positif, elle associe une étiquette spéciale "à risque" à l'application correspondant à ce pseudonyme. Dans notre exemple, les applications de **Bernard** et **Charles** sont maintenant étiquetées avec une mention "à risque".

③ Obtention du statut d'exposition

Pour vérifier si **Charles** a été en contact avec des personnes diagnostiqués positifs pour le virus COVID-19 au cours des derniers jours (par exemple deux semaines), son application envoie son pseudonyme actuel, par exemple , à l'autorité centrale. Celle-ci retrouve l'application correspondant à ce pseudonyme et vérifie si elle est mentionnée comme étant "à risque". Il est important de noter que l'autorité ne peut pas identifier les utilisateurs correspondant à ce pseudonyme car cette information n'existe pas.

Si l'autorité constate que la demande enregistrée est marquée comme "à risque" (ce qui est le cas pour **Charles**), elle répond à la demande de l'utilisateur en l'informant qu'il a été au contact d'utilisateurs diagnostiqués positifs pour le virus COVID-19 et, par conséquent, qu'il a été exposé au virus. Sinon, l'autorité informe l'utilisateur qu'il n'a pas été exposé à sa connaissance.

FAQ

Questions générales

Q: Est-ce que le protocole ROBERT est une application pour smartphone ?

Non, le protocole ROBERT n'est pas une application. C'est un protocole de communication, c'est-à-dire une procédure décrivant comment une application doit fonctionner. Il est proposé par des scientifiques, qui travaillent sur la sécurité et la confidentialité des protocoles de communication depuis plus de vingt ans. Différentes applications peuvent utiliser le protocole ROBERT.

Celui-ci est proposé dans le contexte de l'initiative PEPP-PT (Pan European Privacy-Preserving Proximity Tracing), dont le but principal est de permettre le développement de solutions de suivi des contacts garantissant le respect des normes européennes en matière de protection des données, de vie privée et de sécurité.

Préoccupations relatives à la vie privée et à la sécurité

Q : Cette application peut-elle être utilisée par l'autorité centrale pour me pister ou effectuer une surveillance de masse ?

Deux types d'informations doivent être collectées pour pouvoir vous « pister » : (1) un identifiant qui vous est propre (pour détecter que vous êtes la même personne que celle qui a été vue auparavant) et (2) certaines informations personnelles vous concernant. Avec le protocole ROBERT, l'autorité ne reçoit des informations que pendant la phase “déclaration des pseudonymes des contacts d'un utilisateur diagnostiqué positif”, et l'autorité ne reçoit que le pseudonyme d'un utilisateur pendant la phase “obtention du statut d'exposition”. En outre, seul un pseudonyme temporaire est utilisé, et la seule information que l'autorité peut tirer de ce pseudonyme est que la personne correspondante a été exposée (proximité avec un utilisateur diagnostiqué positif). Par conséquent, les pseudonymes ne permettent pas à l'autorité de suivre les utilisateurs.

L'autorité n'apprend pas l'identité réelle d'un utilisateur, qu'il soit diagnostiqué positif (c'est-à-dire testé positif), comme Alice ci-dessus, ou exposé, comme Bernard et Charles. De plus, l'autorité ne peut pas déduire le "graphe de proximité" d'Alice, Bernard ou Charles. Si l'autorité veut effectuer un traçage physique, elle devra déployer des dispositifs de d'écoute (sniffing) ou compromettre le téléphone mobile de l'utilisateur en exploitant une vulnérabilité, ce qui pourrait conduire à une surveillance ciblée mais pas à une surveillance de masse. En outre, ce type de suivi physique est déjà possible en mobilisant d'autres moyens comme la vidéosurveillance, le bornage GSM, ou des dispositifs de suivi dédiés.

Q : Je suis passé près d'une personne dans la rue. Puis-je savoir si cette personne est diagnostiquée positive ou non ?

Non, ce n'est pas possible. Savoir si la personne est **diagnostiquée positive ou non** constituerait une violation de sa vie privée. Le protocole ROBERT garantit que lorsqu'un utilisateur est testé positif, son application est désactivée. La personne peut être invitée - par son professionnel de santé (médecin/généraliste) - à s'isoler pendant deux semaines. Lorsqu'elle se rétablit, le professionnel de santé pourra réactiver son application.

Q : Si mon test est positif, qui peut savoir que j'ai été diagnostiqué(e) positif(ve) ?

Seuls les professionnels de santé qui ont accès aux résultats de vos tests apprendront que vous avez été diagnostiqué(e) positif(ve)(e). Ni l'autorité centrale ni les utilisateurs de l'application n'auront accès aux résultats de votre test. De plus, ils ne pourront pas déduire d'informations sur les personnes diagnostiqués positifs pour le virus COVID-19.

Quand un utilisateur reçoit un message "Vous avez été en contact avec une personne diagnostiquée positive" et qu'il a été en contact avec très peu de personnes (dans notre exemple, Charles a été en contact avec seulement Alice et Bernard) il peut deviner que l'un d'entre eux est diagnostiqué positif. Si ce risque est jugé inacceptable, le protocole ROBERT pourra être doté d'un mécanisme probabiliste permettant de protéger les utilisateurs contre ce type d'inférence. Le choix de tels options dépassent le strict cadre de version courante du protocole ROBERT.

Q : Comment mes pseudonymes sont-ils générés ? Quelqu'un peut-il utiliser mon pseudonyme ? Est-il sécurisé ?

Les pseudonymes temporaires sont générés par l'autorité à l'aide d'une fonction cryptographique sécurisée qui met en jeu une clé secrète associée à votre application et une information temporelle. Ces pseudonymes temporaires sont ensuite transmis de façon sécurisée à votre application et stockés pour un usage future. Seule l'autorité et votre application peuvent y accéder. Les pseudonymes temporaires sont ensuite diffusés en Bluetooth pour informer les application à proximité. Afin de limiter les risques qu'un message contenant votre pseudonyme ne soit réutilisé par un utilisateur malicieux, ce message n'est valide que durant quelques secondes (ce que l'on appelle une "protection anti-rejeu").

Q: Comment le protocole ROBERT garantit-il que l'autorité centrale ne peut pas faire le lien entre mes pseudonymes et moi ?

Tous vos pseudonymes sont connus de l'autorité (puisque c'est elle qui les a générés). Toutefois, l'autorité ne dispose d'aucune autre information : ni nom, adresse, numéro de téléphone, identifiant technique du téléphone portable ou géolocalisation, qui pourrait être utilisée pour vous identifier.

Q : Comment puis-je être sûr(e) que toutes les interactions avec l'autorité sont sécurisées et que la réponse que je reçois pour savoir si j'ai été exposé(e) ou non à des utilisateurs diagnostiqués positifs, est fiable ?

L'installation de l'application comporte une phase d'enregistrement au cours de laquelle une clé secrète est générée et partagée entre l'appareil mobile de l'utilisateur et l'autorité. Cette clé est ensuite utilisée pour signer numériquement les messages échangés avec l'autorité. Les signatures numériques sont des schémas mathématiques utilisés pour vérifier l'authenticité des

messages. Elle fournit au destinataire une très forte raison de croire que le message a été créé par un expéditeur connu, et garantit que le contenu du message n'a pas été altéré pendant la transmission. De surcroît les communications entre l'application et l'autorité sont toutes chiffrées.

Fonctionnalité des applications qui mettent en œuvre le protocole ROBERT

Q : Quel type d'information sera envoyé dans le message d'alerte (recommandations, instructions obligatoires) ?

Le protocole ROBERT est conçu pour permettre à une application d'avertir son utilisateur qu'il a été en contact avec des personnes diagnostiqués positifs. Suite à la demande de statut envoyée par l'application à l'autorité, l'utilisateur recevra une réponse (ou un message d'alerte) l'informant qu'il a été en contact ou pas avec des utilisateurs diagnostiqués positifs. Le choix du type d'instructions à transmettre ainsi que de la fréquence à laquelle cette information doit être affichée sur le téléphone portable revient aux professionnels de santé et aux épidémiologistes.

Q : Le message d'alerte peut-il m'indiquer si j'ai été ou non en contact avec un utilisateur diagnostiqué positif au cours des x derniers jours ?

Le protocole actuel est conçu pour renvoyer une réponse "binaire", soit "Oui, vous avez été en contact avec un ou plusieurs utilisateurs diagnostiqués positifs au cours des x derniers jours" ou "Non, pour autant que l'on sache, vous n'avez pas été en contact avec un utilisateur diagnostiqué positif au cours des x derniers jours". Le nombre de jours "x" sera défini par les professionnels de santé et les épidémiologistes.

Q : Combien de temps dois-je interagir avec une personne diagnostiquée positive pour être considéré(e) plus tard comme exposé(e) ? À quelle distance dois-je me trouver ?

Ces choix ne sont pas arrêtés dans l'application et seront définis en accord avec les professionnels de santé et les épidémiologistes.

Accessibilité pour la population

Q : Les personnes qui ne possèdent pas de téléphones portables, comme les enfants, pourront-elles utiliser ce système ?

En effet, les personnes qui ne possèdent pas de téléphone portable ne pourront pas bénéficier d'une application de suivi des contacts si elle n'est disponible que sur téléphone. Cependant, on

peut envisager de créer un dispositif autonome émulant les fonctionnalités de l'application et qui serait utilisable par ces personnes. Cette possibilité est actuellement à l'étude.

Q : Comment les personnes manquant de compétences techniques peuvent-elles télécharger et utiliser l'application ?

L'application sera aussi simple que possible afin de s'assurer que le manque de compétences techniques ne soit pas un obstacle à l'adoption. Les personnes qui ne possèdent pas l'expertise nécessaire pourront être aidées par un parent ou un aidant. A défaut, un appareil dédié qui fonctionne de façon autonome (voir question précédente) pourrait être fourni.

La fonctionnalité Bluetooth

Q : La transmission Bluetooth est-elle sûre ? Quelqu'un peut-il m'écouter ?

Les communications Bluetooth utilisées par le système ne sont pas confidentielles, quiconque peut les observer. Toutefois, les données échangées par Bluetooth se limitent au pseudonyme temporaire anonyme, au temps de transmission et à un code de vérification d'intégrité. Ces informations sont utilisées pour protéger des attaques dites "de re-jeu" (quand le message peut être capté et re-envoyé par l'attaquant, se faisant ainsi passer pour l'utilisateur) : cette attaque ne sera pas possible.