PROTECT: Privacy-preserving Contact Tracing for COVID-19 with Homomorphic Encryption

Yongdae An, Seungmyung Lee, Seungwoo Jung, Howard Park, Yongsoo Song, Taehoon Ko

Submitted to: Journal of Medical Internet Research
on: January 30, 2021

Disclaimer: © The authors. All rights reserved. This is a privileged document currently under peer-review/community review. Authors have provided JMIR Publications with an exclusive license to publish this preprint on it's website for review purposes only. While the final peer-reviewed paper may be licensed under a CC BY license on publication, at this stage authors and publisher expressively prohibit redistribution of this draft paper other than for review purposes.

Table of Contents

PROTECT: Privacy-preserving Contact Tracing for COVID-19 with Homomorphic Encryption

Yongdae An[1, 2] BSc; Seungmyung Lee[2] MS; Seungwoo Jung[2] BSc; Howard Park[2] MA; Yongsoo Song[3*] PhD; Taehoon Ko[4*] PhD

[1]Department of Industrial Engineering Seoul National University Seoul KR
[2]Desilo Inc. Seoul KR
[3]Microsoft Research Redmond US
[4]Department of Medical Informatics The Catholic University of Korea Seoul KR
[*]these authors contributed equally

Corresponding Author:
Taehoon Ko PhD
Department of Medical Informatics
The Catholic University of Korea
222 Banpo-daero
Seocho-gu
Seoul
KR

Abstract

Background: Various techniques are employed in order to support contact tracing, which has been shown to be highly effective against the pandemic of coronavirus disease 2019 (COVID-19). To apply the technology, either the quarantine authorities should provide the location history COVID-19 patients, or all people should provide their own location history. This inevitably makes people either the patient location history or personal location history of the public, leading to the privacy protection issue of information release for the public good against privacy exposure risks.

Objective: The objective of this study is to develop an effective contact tracing system without exposing the location information between the user and the quarantine authorities with COVID-19 patient location history.

Methods: We propose a new protocol called PRivacy Oriented Technique for Epidemic Contact Tracing (PROTECT) that securely shares the location information of patients with users by using the Brakerski/Fan-Vercauteren (BFV) homomorphic encryption scheme, along with a new secure proximity computation method for it.

Results: We have developed a mobile application for the end-user and a web service for the quarantine authorities by applying the proposed method and have verified their effectiveness. Proposed application and web service compute the existence of intersections between the encrypted location history of COVID-19 patients released by the quarantine authorities and the user location history saved on the local device. We also show that the developed contact tracing application can identify whether the user is in contact with patients within a reasonable time on smartphones.

Conclusions: The developed method that shares the location information encrypted with homomorphic encryption is a new method for contact tracing without exposing the location information of the COVID-19 patients and the users. Homomorphic encryption is difficult to apply to practical issues despite its high security value. This study, however, has designed a system applicable to a reasonable size using the BFV scheme, and developed it to an operable format. The developed application and web service can help contact tracing for not only COVID-19, but also other various epidemics.

(JMIR Preprints 30/01/2021:26371)
DOI: https://doi.org/10.2196/preprints.26371

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?
✓ **Please make my preprint PDF available to anyone at any time (recommended).**

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**
Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Original Paper

PROTECT: Privacy-preserving Contact Tracing for COVID-19 with Homomorphic Encryption

Background: Various techniques are employed in order to support contact tracing, which has been shown to be highly effective against the pandemic of coronavirus disease 2019 (COVID-19). To apply the technology, either the quarantine authorities should provide the location history COVID-19 patients, or all people should provide their own location history. This inevitably makes people either the patient location history or personal location history of the public, leading to the privacy protection issue of information release for the public good against privacy exposure risks.
Objective: The objective of this study is to develop an effective contact tracing system without exposing the location information between the user and the quarantine authorities with COVID-19 patient location history.
Methods: We propose a new protocol called PRivacy Oriented Technique for Epidemic Contact Tracing (PROTECT) that securely shares the location information of patients with users by using the Brakerski/Fan-Vercauteren (BFV) homomorphic encryption scheme, along with a new secure proximity computation method for it.
Results: We have developed a mobile application for the end-user and a web service for the quarantine authorities by applying the proposed method and have verified their effectiveness. Proposed application and web service compute the existence of intersections between the encrypted location history of COVID-19 patients released by the quarantine authorities and the user location history saved on the local device. We also show that the developed contact tracing application can identify whether the user is in contact with patients within a reasonable time on smartphones.
Conclusions: The developed method that shares the location information encrypted with homomorphic encryption is a new method for contact tracing without exposing the location information of the COVID-19 patients and the users. Homomorphic encryption is difficult to apply to practical issues despite its high security value. This study, however, has designed a system applicable to a reasonable size using the BFV scheme, and developed it to an operable format. The developed application and web service can help contact tracing for not only COVID-19, but also other various epidemics.

Trial Registration: None

Keywords: COVID-19; homomorphic encryption; privacy-preserving contact tracing; PROTECT protocol; GPS data; mobile application; web service

Introduction

Background

Since the first coronavirus disease of 2019 (COVID-19) patient was reported in Wuhan on December 8th, 2019, the whole world has been under the COVID-19 pandemic situation. According to WHO, as of January 25th, 2021, the number of COVID-19 patients worldwide is about 97 million, 2.1 million of which are reported to have been fatal [1]. As COVID-19 spreads rapidly, the public is suffering from growing anxiety and concern [2]. COVID-19 has incapacitated the existing medical system with its high communicability and fatality rate, and until a vaccination comes about, the only available countermeasures are traditional control measures, namely, case isolation, contact tracing and quarantine, physical distancing, decontamination, and personal hygiene [3].

Therefore, it is imperative to understand the propagation route and timing in order to take appropriate measures within the right timing. For example, when 97 COVID-19 patients were confirmed at a call center in South Korea in March 2020, the Korea Center for Disease Control and Prevention (KCDC) and the local government formed a joint response team and carried out an epidemiologic investigation with contact tracing [4]. At the time, the team identified and analyzed 1,145 people, and further investigated their surroundings to prevent COVID-19 from spreading. Thanks to such active efforts on COVID-19 quarantine, despite the early onset of COVID-19 pandemic, South Korea shows a significantly smaller number of COVID-19 patients and lower fatality rate compared to other countries.

Prior Work

Ferretti et al. used a renewal equation formulation to develop a mathematical model to determine the speed and volume for effective screening and contact tracing necessary to stop the spread of epidemics and quantify other propagation routes [5]. According to this study, if the self-isolation of an individual who has been in contact with a COVID-19 patient is delayed by 3 days, no parameter combinations can achieve epidemic control. The study of Ferretti has mathematically proved that the epidemic can be far more effectively controlled when the isolation is executed immediately or with a delay of 1 to 2 days. Accordingly, this study explains that if a contact tracing application is used by a sufficient number of people, an epidemic can be controlled by maintaining temporary information about close proximity among individuals and notifying the contacts to induce isolation.

An active measure against the COVID-19 pandemic requires telehealth screening and management, remote testing, and such, but privacy regulations may pose barriers to such information propagation. Accordingly, there are claims that privacy regulations should be relaxed for health information exchange under the COVID-19 pandemic situation [6]. Despite the effectiveness of COVID-19 patient tracing and contact tracing using digital tools, however, there are potential privacy leakage risks [7]. As a matter of fact, there have been privacy infringements in the name of the public interest in Korea during the early days of quarantine, where personal information such as gender, age, residence, and place of work was released altogether, leading to unwanted outing incidents [8].

To resolve such issues, applications and technologies are being developed that digitally execute contact tracing while protecting privacy [9]. There are cases where the Global Positioning System (GPS) or Bluetooth information of mobile device users were collected in a centralized manner while attributing temporary identifiers [10, 11]. Also, there are distributed models which store the personal location history on the local mobile device only, and computes the distance if a patient approaches near [12]. Both methods, however, are effective only if a majority of users install the application and allow the transmission of one another’s data, and in turn increases privacy risks [13]. There also exist cryptography solutions for privacy protection, such as the technology developed by Apple and Google, using secure multi-party computation without relying on a trusted server, or sending anonymous encrypted or random messages [14]. The study of Gvili, however, claims that the said approach by Apple and Google may be vulnerable to several types of security attacks [15].

Goal of This Study

This study intends to propose the PRivacy Oriented Technique for Epidemic Contact Tracing (PROTECT) protocol for digital contact tracing with perfect privacy protection by using homomorphic encryption. The system proposed in this study exchanges the location data in the encrypted state between the user and the quarantine authorities. The PROTECT protocol makes it possible to identify whether the user has been in contact with COVID-19 patients with the encrypted location information only by developing a novel secure proximity combination technique. This method differs from the privacy protection of existing contact tracing methods in that it identifies the contacts with encrypted distances, and thus it can identify whether the user has been in contact with COVID-19 patients without exposing the location information of the user. It can be said to be a privacy-preserving technique of a higher order.

The composition of this study is as follows. In Section 2, we propose a new algorithm for proximity computation and the PROTECT protocol which utilizes this algorithm. In Section 3, we introduce the quarantine application and web service that we have developed to apply the proposed PROTECT protocol to COVID-19 and verify that the proposed protocol is practical through experimentation. Finally, in Section 4, we discuss the major results of the study and its differences from previous studies and its limitations.

Methods

The key to a privacy-preserving contact tracing system is to achieve the perfect protection of the location information of not only the patient, but also the user, along with the ability to check for proximity. To achieve this, this study utilized homomorphic encryption and proximity in a discrete grid system to develop a new secure proximity computation method, and proposes a new protocol called PROTECT which applies such method to deliver data safely among the user, quarantine authorities, and the patient.

Secure proximity computation

The basic method to check for proximity is to compute the distance between two known locations, but this gives rise to unnecessary location privacy issues [16]. Zhong et al. have proposed three methods that achieves privacy-secured proximity computation by employing additive homomorphic encryption [17]. The secure proximity computation used in PROTECT, the protocol proposed in this study, is inspired by the technique used in the Pierre protocol. Pierre protocol maps the exact location information to the predefined grid areas, and substitutes the proximity calculation problem to the calculation of whether the grids are identical or adjacent. One can tell whether the two locations are in the same grid or in adjacent grids, but one does not gain information about the two locations. The PROTECT protocol utilizes homomorphic encryption in a novel way such that it does not expose any information other than proximity, yet is able to perform a high-level computation that can be put into practice immediately.

HE and BFV

Homomorphic encryption is a cryptosystem which supports computation on encrypted data. The result of encrypted computation is also a ciphertext whose decryption is the same as if we performed the operation over plain data. Homomorphic encryption has a broad application in cloud environments since it can be used to outsource storage and computation without data leakage.

In the last decade, there have been significant improvements in efficiency of homomorphic encryption. Currently lattice-based schemes such as Brakerski-Gentry-Vaikuntanathan (BGV) [18], Brakerski/Fan-Vercauteren (BFV) [19, 20], Torus Fully Homomorphic Encryption (TFHE) [21] and Cheon-Kim-Kim-Song (CKKS) [22] are showing the best performance in practice, but they provide different functionality. In this work, we focus on the BFV scheme since the proximity of COVID-19 patient movements is calculated in the discrete grid system, which will be discussed later. In this system, the proximity is determined by the operation over integral vectors. The BFV scheme is efficient for vectorized operations over the integers, while the CKKS scheme is more appropriate for approximate computations. We provide a simplified description of BFV as follows.

The BFV scheme consists of five polynomial-time algorithms Setup, Enc, Dec, Add, and Mult. Note that we use symmetric-encryption which is faster and has better noise growth compared to the public-key variant.

- $\mathsf{Setup}(1^{\lambda})$: For the security parameter λ, choose a parameter set and sample a secret key sk. Parameters include the dimension n and the plaintext modulus p.
- $\mathrm{Enc}(sk, m)$: It takes as the input the secret key sk and a plaintext $m=(m_1, \ldots, m_n) \in Z_p^n$ which is an n-dimensional vector over the finite field Z_p, and returns a ciphertext c.
- $\mathrm{Dec}(sk, c)$: It decrypts the ciphertext c using the secret key sk and returns a plaintext m.
- $\mathrm{Add}(c, c')$: It outputs the addition of given ciphertexts.
- $\mathrm{Mult}(c, c')$: It performs the multiplication between give n ciphertexts and returns the result.

The BFV scheme satisfies the homomorphic property if parameters are chosen properly. In other words, if c, c' are encryptions of m, m', then $\mathrm{Add}(c, c')$ and $\mathrm{Mult}(c, c')$ are encryptions of $m+m'$ and $m \odot m'$, respectively, where $m \odot m' = (m_1 m_1', \ldots, m_n m_n')$ denotes the Hadamard (component-wise) multiplication of two vectors. For simplicity, we will write $\mathrm{Add}(c, c') = c + c'$ and $\mathrm{Mult}(c, c') = c * c'$.

Proximity in Discrete Grid System

In this study, we converted the two location points to a hexagonal grid system and defined that two points that belong to the same or adjacent grids are “proximate”. The proximity between locations in a continuous space, e.g., Euclidean space must be checked with comparison operations, and such computation is expensive in a homomorphically encrypted system. The proximity in a discrete space, however, can be computed with a few equality checks, which can be efficiently calculated over encrypted data.

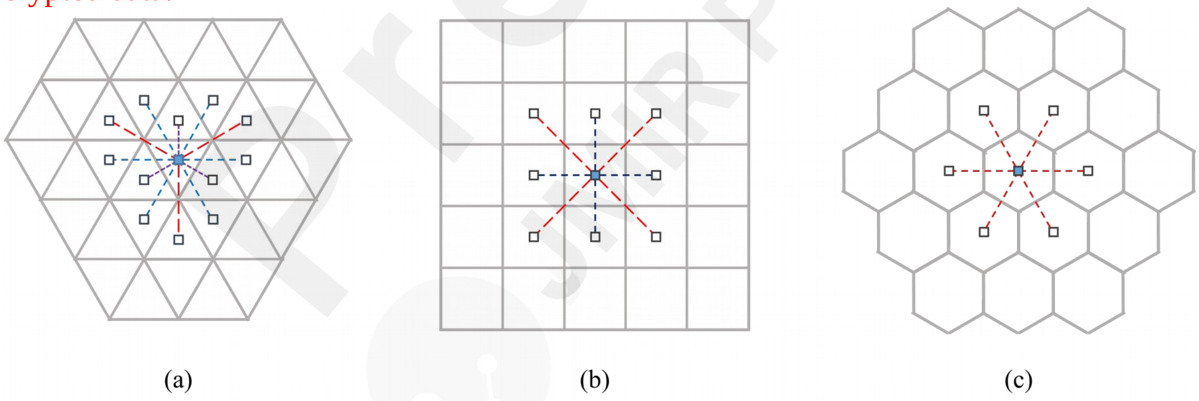


Figure 1. Comparison of triangular, square and hexagonal grids: (a) triangles, (b) squares, (c) hexagons.

We choose the hexagonal grid system to transform the continuous location information into discrete grids. A hexagonal grid system allows for a simpler definition of neighborhood than triangular or square grids do so as to reduce the computation overhead. As shown in Figure 1, to define a neighbor, it takes 3 classes in a triangular grid system and 2 classes in a square grid system, but just 1 class in a hexagonal grid system.

The transportation network company Uber Technologies, Inc. introduced a discrete global grid system called ‘H3: Hexagonal Hierarchical Spatial Index’ that is based on multi-resolution hexagonal grids [23]. As shown in Figure 2, H3 provides the local IJ coordinate system for hexagons, which specifies a hexagonal area adjacent to the specified origin with I-axis and J-axis at an angle of 120 degrees.

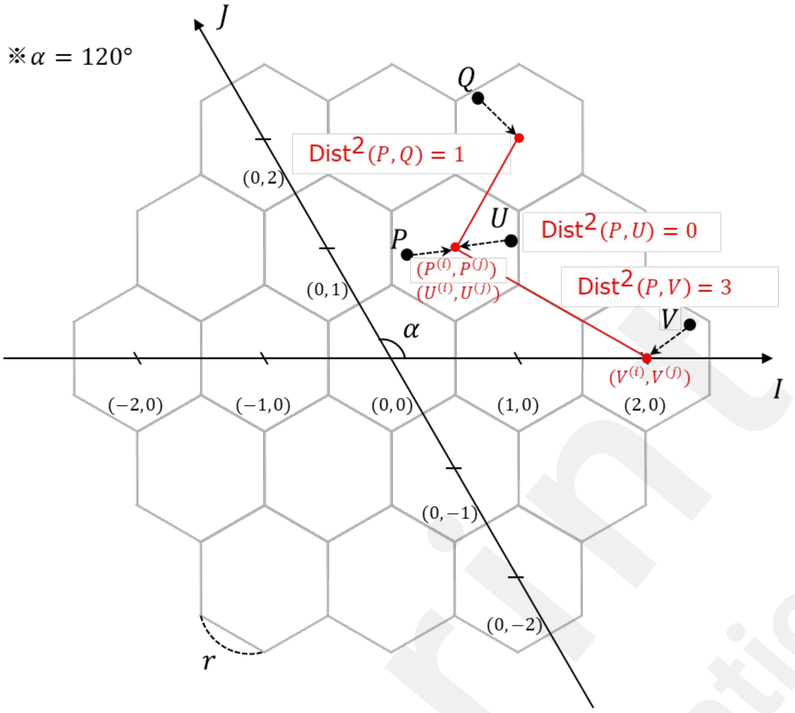


Figure 2. Local IJ coordinates of a hexagonal grid system with a side length of r.

We denote by $H:R^2 \longrightarrow Z^2, (x,y) \longmapsto (i,j)$ the transformation into the hexagonal grid system with a side length of r. In other words, it returns the IJ coordinate of the hexagon which an input point belongs to. Some examples are shown in Figure 2.

We also define a metric function $\mathrm{Dist}^2(\cdot,\cdot):R^2 \longrightarrow Z$, $(P,Q) \longmapsto \frac{1}{3r^2}\|H(P)-H(Q)\|^2$, which can be computed by $\mathrm{Dist}^2(P,Q)=(P^{(i)}-Q^{(i)})^2-(P^{(i)}-Q^{(i)})(P^{(j)}-Q^{(j)})+(P^{(j)}-Q^{(j)})^2$ where $H(P)=(P^{(i)},P^{(j)}), H(Q)=(Q^{(i)},Q^{(j)}) \in Z^2$.

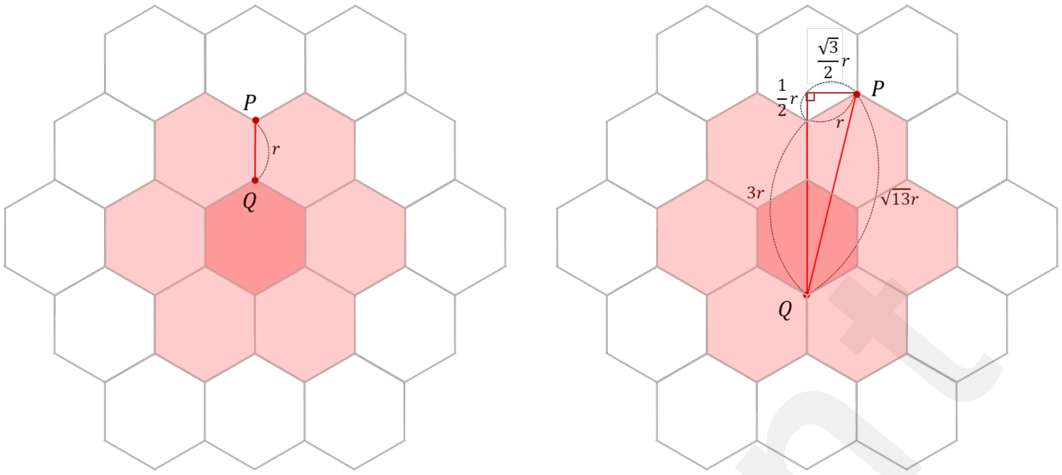
We use the metric Dist^2 to determine the proximity between two locations. Our definition of proximity in H3 is whether the hexagonal grids corresponding to two locations P and Q are identical or adjacent to each other, or equivalently, $\mathrm{Dist}^2(P,Q)=0$ or $\mathrm{Dist}^2(P,Q)=1$. In the following, we present two properties of Dist^2 to convince that this is a reasonable quantity on which we can make a proper judgement.

Figure 3 shows two extreme examples where $\mathrm{Dist}^2(P,Q)$ is relatively large/small compared to the Euclidean distance $\|P-Q\|$. In Figure 3(a), the Euclidean distance between two points is r but $\mathrm{Dist}^2(P,Q)>1$. Meanwhile, we have $\|P-Q\|=\sqrt{13}r$ and $\mathrm{Dist}^2(P,Q)=1$ in the case of Figure 3(b). In application of contact tracing, the primary goal is to detect all contact cases, so the side length r should be set sufficiently large based on if-then statements in Textbox 1.

In case of a highly contagious epidemic such as COVID-19, a single patient may cause a re-proliferation, and thus the examination scope should be rather conservatively set to be broad. WHO recommends massive testing to all suspected cases for COVID-19 [24]. The OECD also recommends that countries conduct as many tests for COVID-19 as possible, even if they are expensive [25]. The OECD projected that the cost of testing would be much less than the cost of a national lockdown situation [26].

Textbox 1. Relationship between the approximated distance $\mathrm{Dist}^2(P,Q)$ and the Euclidean distance $\|P-Q\|$

1. If $\text{Dist}^2(P,Q) \le 1$, then $\|P-Q\| < \sqrt{13}r$
2. If $\|P-Q\| < r$, then $\text{Dist}^2(P,Q) \le 1$



(a) (b)

Figure 3. Distance between two points P, Q on hexagonal girds with a side length of r: (a) when the distance between P and Q is slightly greater than r and they are not deemed proximate, (b) when the distance between P and Q is slightly less than $\sqrt{13}r$ and they are deemed proximate.

PROTECT (our algorithm)

Protocol Overview

The proposed protocol PROTECT consists of mainly three parties - the user, the quarantine authorities, and the COVID-19 patient. The overall protocol flow is as in Figure 4. The parties exchange individual ID, timestamps, and GPS locations only.

In this study, we assume that the quarantine authorities are semi-honest and that the patient honestly provides his/her location history to them. World Health Organization (WHO) recommends that, as essential surveillance for COVID-19 considering the potential for rapid exponential growth of COVID-19 cases in populations, new cases should be identified, reported, and data included in epidemiological analysis within 24 hours. National authorities should consider including COVID-19 as a mandatory notifiable disease with requirements for immediate reporting [27]. Local and local governments are already collecting information to track and stop the spread of the coronavirus. CDC of the United States published a guideline that the quarantine personnel shall investigate all cases of contacts with COVID-19 patients [28], and South Korea collects the location history of COVID-19 patients and opens them to the public so that those with a high possibility of contact can voluntarily be examined for COVID-19 [29]. Also, it is assumed that all communication in our protocol occurs through a secure channel. When a patient sends his/her data to the authorities or the authorities send the encrypted information to the users, such occurs through a secure channel, so third party attack (e.g., MitM) is not possible.

The definition of each party and further details on the associated events are as follows.

COVID-19 patient

The patient is a user who has been tested positive for COVID-19, and provides his/her two-week GPS location history to the quarantine authorities. At this time, the location information of the patient is not encrypted.

Quarantine Authorities

The quarantine authorities are the subjects that oversee the quarantine system, which may be municipal or national. The quarantine authorities receive the location information provided by the patient, encrypt it, and upload it to the server. Now the encrypted patient location information is then sent to the users who have installed the app. Also, the quarantine authorities receive the result of the computation at the local user device in the encrypted state, decrypt that result, and then send the decrypted result back to the user. In this process, the quarantine authorities have no access to the personal location information stored on the local user device.

User

The user computes, on the individual local device, the proximity between his/her own location information and the encrypted patient location information received from the quarantine authorities. Here, homomorphic encryption makes it possible to execute computation between the encrypted location information and non-encrypted location information. The computation result is encrypted, as shown in Figure 4. The user then sends the encrypted computation result to the quarantine authorities. The user then receives and checks the decrypted computation result from the quarantine authorities, and in case of high risk of infection, gets to follow the quarantine protocol suggested by the government.

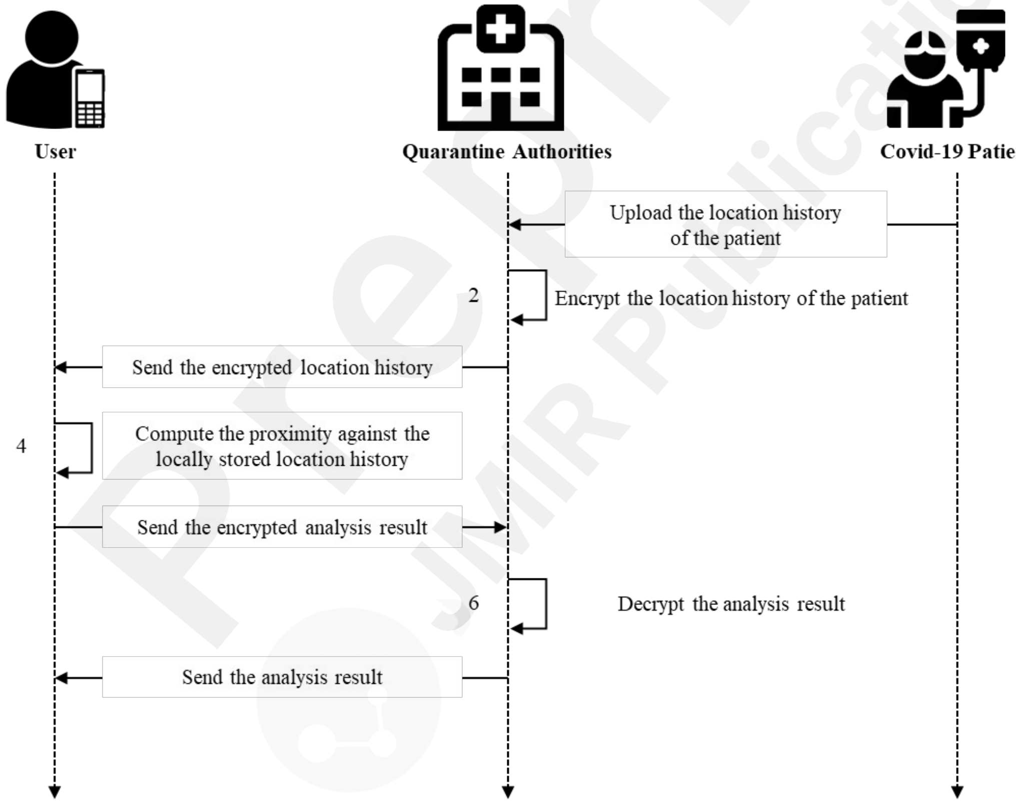

User
Quarantine Authorities
Covid-19 Patient
1
Upload the location history of the patient
2
Encrypt the location history of the patient
3
Send the encrypted location history
4
Compute the proximity against the locally stored location history
5
Send the encrypted analysis result
6
Decrypt the analysis result
7
Send the analysis result

Figure 4. Flow chart for the PROTECT protocol.

Secure proximity computation with BFV and H3

In this section, we provide technical details of proximity computation in the PROTECT protocol. Throughout this section, P_t and Q_t will denote the location data of the COVID-19 patient and the user, respectively. The location data natively includes time information, but we suppose that data is pre-processed and synchronized so that the elements of the same index have the same timestamps.

Before the protocol starts, the quarantine authorities and the user encode their data locally into the IJ coordinate using the H map described in the previous section and generate the vectors

$P^{(i)} = \left(P_1^{(i)}, \ldots, P_n^{(i)}\right), P^{(j)} = \left(P_1^{(j)}, \ldots, P_n^{(j)}\right)$ and $Q^{(i)} = \left(Q_1^{(i)}, \ldots, Q_n^{(i)}\right), Q^{(j)} = \left(Q_1^{(j)}, \ldots, Q_n^{(j)}\right)$, respectively, where $H\left(P_t\right) = \left(P¿¿t^{(i)}, P_t^{(j)}\right)¿$ and $H\left(Q_t\right) = \left(Q¿¿t^{(i)}, Q_t^{(j)}\right)¿$ for $1 \le t \le n$.

BFV encryption

The server sets the parameters for BFV and generates a secret key sk.
The server generates ciphertexts $c^{(i)} \longleftarrow \mathrm{Enc}\left(sk, P¿¿\left(i\right)\right)¿$ and $c^{(j)} \longleftarrow \mathrm{Enc}\left(sk, P¿¿\left(i\right)\right)¿$ using the BFV scheme and sends them to a user.

Secure proximity computation

On receiving the ciphertexts, the user securely computes the proximity between P_t and Q_t. This procedure consists of homomorphic evaluation of the proximity function followed by a ciphertext randomization process.

First of all, the user homomorphically evaluates $\mathrm{Dist}^2\left(P, Q\right)$ by $c_{\mathrm{Dist}^2} := d^{(i)} * d^{(i)} - d^{(i)} * d^{(j)} + d^{(j)} * d^{(j)} = \left(d^{(i)} - d^{(j)}\right)^2 + d^{(i)} * d^{(j)}$ where $d^{(i)} = c^{(i)} - Q^{(i)}$ and $d^{(j)} = c^{(j)} - Q^{(j)}$. This is an encryption of the vector $\left(\mathrm{Dist}^2\left(P_t, Q_t\right)\right)_{1 \le t \le n}$ from the homomorphic property of BFV. Then, she computes and obtains $c_{Prox} = c_{\mathrm{Dist}^2} * \left(c_{\mathrm{Dist}^2} - 1\right)$. In our implementation, we performed two homomorphic multiplications after subtraction, added them, and finally performed one relinearization. Note that c_{Prox} is encrypting $\mathrm{Dist}^2\left(P_t, Q_t\right) * \left(\mathrm{Dist}^2\left(P_t, Q_t\right) - 1\right) = 0$ in the k-th slot, which is zero if and only if $\mathrm{Dist}^2\left(P_t, Q_t\right) = 0$ or $\mathrm{Dist}^2\left(P_t, Q_t\right) = 1$. Hence, if the user sends c_{Prox} back to quarantine authorities (the secret key owner), then they would be able to decrypt the ciphertext and determine the proximity of P_t and Q_t by checking out if $\mathrm{Dist}^2\left(P_t, Q_t\right) * \left(\mathrm{Dist}^2\left(P_t, Q_t\right) - 1\right)$ or not. However, this method is not privacy-preserving since the secret key owner can extract more information from the ciphertext c_{Prox} beyond the proximity.

Hence, the user randomizes the ciphertext c_{Prox} to solve the issue above. She generates a vector $r = \left(r_1, \ldots, r_n\right)$ whose entries r_i are sampled independently and uniformly at random from the set $Z_p \setminus \{0\} = \{1, 2, \ldots, p - 1\}$, and a random encryption of zero c_0 with a large noise parameter. The user outputs the ciphertext $c_{RProx} := r * c_{Prox} + c_0$ and sends it back to the quarantine authorities. Note that the total multiplicative depth of proximity computation is 3.

Decryption

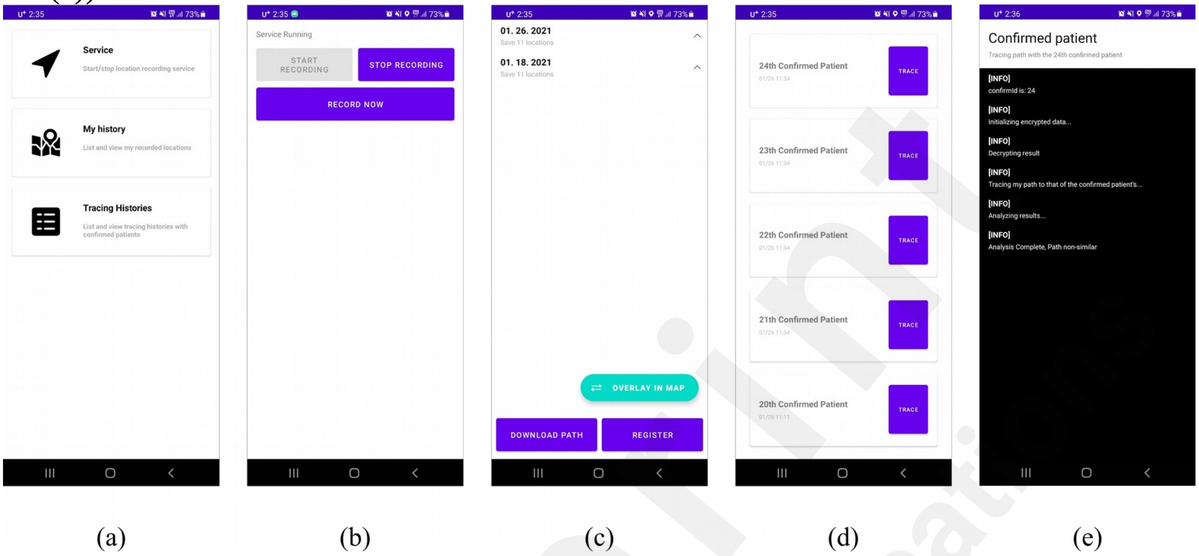
The quarantine authorities decrypt c_{RProx} and obtain $r_t' = r_t * \mathrm{Dist}^2\left(P_t, Q_t\right) * \left(\mathrm{Dist}^2\left(P_t, Q_t\right) - 1\right)$ for $1 \le t \le n$. They conclude that the user has been in contact with a patient at timestamp t if this value is zero. We point out that the quarantine authorities learn nothing from the decrypted value about the user data more than the desired result since r_t' is purely random over $Z_p \setminus \{0\}$ if $\mathrm{Dist}^2\left(P_t, Q_t\right) \neq 0, 1$. Moreover, the ciphertext c_{RProx} itself contains no information beyond r_t' since the user randomized it by adding c_0. Note that the noise parameter of c_0 should exponentially large compared to that of $r * c_{Prox}$ for security proof.

Results

In order to apply the PROTECT protocol to COVID-19 contact tracing, we have built an application for the COVID-19 patient and the user and a web service of the quarantine authorities. Also, we empirically verified the practicality of the PROTECT protocol through performance indicators related to resource consumption such as response time, Central Processing Unit (CPU) utilization, and memory consumption on the local device.

User Application

The smartphone application for the user is as shown in Figure 5. The user can enable or disable the service any time at will (Figure 5(b)), and easily check the GPS information stored on the local device by date (Figure 5(c)). Also, the user can conduct comparison with the COVID-19 patient location information received from the quarantine authorities by push, and check the details on the potential contact in case he or she is suspected to have been in contact with a patient (Figure 5(d) , Figure 5(e)).



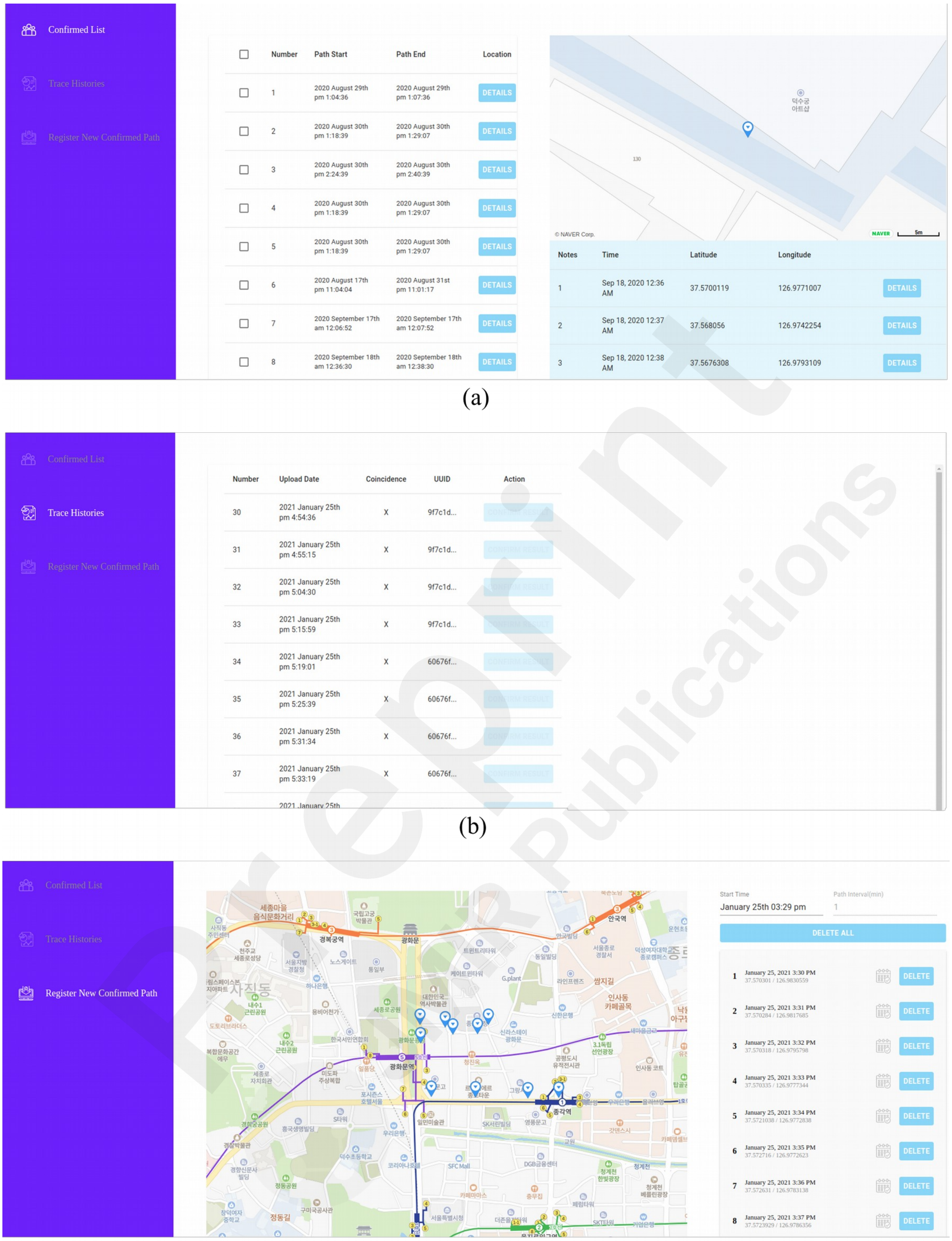
```
[INFO]
confirmId is: 24
[INFO]
Initializing encrypted data...
[INFO]
Decrypting result
[INFO]
Tracing my path to that of the confirmed patient's...
[INFO]
Analyzing results...
[INFO]
Analysis Complete, Path non-similar
```

(a) (b) (c) (d) (e)

Figure 5. Screenshots of the user application: (a) main screen, (b) GPS data recording setup screen, (c) list of GPS data by day stored on the user's local device, (d) list of encrypted GPS data per patient received from the quarantine authorities, (e) location history comparison and result.

Web Service for Quarantine Authorities

The role of the quarantine authorities is to manage the COVID-19 patient information and to propagate the test results. For this, we have built a web service as shown in Figure 6. The quarantine authorities can encrypt the location information provided by the patients and propagate the encrypted information to the users who have installed the application (Figure 6(a)). Also, while the quarantine authorities have no access to the location information of each individual user, they can identify the users who have location information close to the currently registered patient location information through the analysis results uploaded by the users (Figure 6(b)). Also, we also developed a feature where the quarantine authorities can easily register patient location history by manually clicking on the map in case of patient whose two-week location data has not been collected as they have not used this app or for any other reason (Figure 6(c)).



□	Number	Path Start	Path End	Location
□	1	2020 August 29th pm 1:04:36	2020 August 29th pm 1:07:36	DETAILS
□	2	2020 August 30th pm 1:18:39	2020 August 30th pm 1:29:07	DETAILS
□	3	2020 August 30th pm 2:24:39	2020 August 30th pm 2:40:39	DETAILS
□	4	2020 August 30th pm 1:18:39	2020 August 30th pm 1:29:07	DETAILS
□	5	2020 August 30th pm 1:18:39	2020 August 30th pm 1:29:07	DETAILS
□	6	2020 August 17th pm 11:04:04	2020 August 31st pm 11:01:17	DETAILS
□	7	2020 September 17th am 12:06:52	2020 September 17th am 12:07:52	DETAILS
□	8	2020 September 18th am 12:36:30	2020 September 18th am 12:38:30	DETAILS

Notes	Time	Latitude	Longitude	
1	Sep 18, 2020 12:36 AM	37.5700119	126.9771007	DETAILS
2	Sep 18, 2020 12:37 AM	37.568056	126.9742254	DETAILS
3	Sep 18, 2020 12:38 AM	37.5676308	126.9793109	DETAILS

(a)

Number	Upload Date	Coincidence	UUID	Action
30	2021 January 25th pm 4:54:36	X	9f7c1d...	CONFIRM RESULT
31	2021 January 25th pm 4:55:15	X	9f7c1d...	CONFIRM RESULT
32	2021 January 25th pm 5:04:30	X	9f7c1d...	CONFIRM RESULT
33	2021 January 25th pm 5:15:59	X	9f7c1d...	CONFIRM RESULT
34	2021 January 25th pm 5:19:01	X	60676f...	CONFIRM RESULT
35	2021 January 25th pm 5:25:39	X	60676f...	CONFIRM RESULT
36	2021 January 25th pm 5:31:34	X	60676f...	CONFIRM RESULT
37	2021 January 25th pm 5:33:19	X	60676f...	CONFIRM RESULT
	2021 January 25th			

(b)

Start Time: January 25th 03:29 pm

Path Interval(min): 1

1	January 25, 2021 3:30 PM 37.570301 / 126.9830559	DELETE
2	January 25, 2021 3:31 PM 37.570284 / 126.9817685	DELETE
3	January 25, 2021 3:32 PM 37.570318 / 126.9795798	DELETE
4	January 25, 2021 3:33 PM 37.570335 / 126.9777344	DELETE
5	January 25, 2021 3:34 PM 37.5721038 / 126.9772838	DELETE
6	January 25, 2021 3:35 PM 37.572716 / 126.9772623	DELETE
7	January 25, 2021 3:36 PM 37.572631 / 126.9783138	DELETE
8	January 25, 2021 3:37 PM 37.5723929 / 126.9786356	DELETE

(c)

Figure 6. Screenshots of the web service for quarantine authorities: (a) list of confirmed patients GPS data, (b) list of trace histories, (c) register new confirmed patient GPS data.

Performance indicators

To assess the practicality of the application that implements the proposed PROTECT protocol, we have installed the developed application on two smartphone models – Samsung

Galaxy S20 Plus and Note 8 – and conducted performance tests. The detailed specifications of the testing devices are as in Table 1.

Table 1. Specifications of testing devices

	Galaxy S20 plus	Galaxy Note 8
Release Year	2020	2017
Chipset	Samsung Exynos 9 Octa 990	Samsung Exynos 9 Octa 8895
Processor	Octa core (2 x 2.73 GHz Mongoose + 2 x 2.5 GHz Cortex A76 + 4 x 2 GHz Cortex A55)	Octa-core (4 x 2.3 GHz Mongoose M2 + 4 x 1.7 GHz Cortex-A53)
GPU	ARM Mali-G77 MP11	ARM Mali-G71 MP20
RAM	8 GB	6 GB

To satisfy 128-bit security level while maintaining a proper size for computation, the base ring dimension was set to 8192, which indicates that the proximity computation for 8192 time points can be executed simultaneously. At the same time, the computation time for the entire data is determined by the size of the base ring dimension. When GPS data is collected every *t* seconds, the number of time points per person collected over the period of 14 days is $\lceil (60*60*24*14)/t \rceil$. Surely, the larger t gets, the smaller the number of time points to be collected per person gets, and the number of comparison computations is also greatly reduced.

It is not necessary to use all time points to compare the time points of the user and the patient. The location information can be trimmed through various methods. It is not necessary to compare all time points where the subject has stayed at a single location for a long time, such as sleeping or working. In case many patients occurred at the same location at the same time, a single computation shall suffice. Also, the occasions that the patient has certainly made no contact, such as driving alone, can also be excluded. Such pre-processing can be applied before encryption, by the means of epidemiological investigation when the quarantine authorities collect the location history of the patients.

If the number of data points refined by the quarantine authorities is N, the number of computations (N_{comp}) is $N_{comp} = \lceil N/8192 \rceil$. When the computation time for 8192 time points is $Time_{comp}$, the total time the proximity computation takes for each user ($Total_{¿}$) is $Total_{¿} = Time_{comp} * N_{comp}$.

As for the proposed PROTECT protocol, the computation times may vary depending on the processing power of the user's smart device. The test results for computation time in Samsung Galaxy S20 Plus and Note 8 are as in Table 2.

Table 2. Results of proximity computation tests on testing devices

	Galaxy S20 Plus	Galaxy Note 8
Avg. CPU utilization	2.158%	5.425%
Max. memory consumption during computation	57.57MB	58.6MB
Computation time ($Time_{comp}$ ¿	3.246*s*	6.967 *s*
Size of encrypted data ($TransferSize_{Q \to U}$)	1.08 MB	
Size of encrypted data ($TransferSize_{U \to Q}$)	0.814 MB	

Since S20 Plus has a more powerful processor than that of Note 8, it can be seen that $Time_{comp}$ is smaller. When S20 Plus is to compute 1,000,000 encrypted data points received from the quarantine authorities, $N_{comp} = \lceil 1000000/8192 \rceil = 123$, and $Total_{¿} = Time_{comp} * N_{comp} = 3.246 * 123 = 399.258(s)$. Also, the transfer time between users and quarantine authorities depends on the speed of the network and the size of the transferred data. To account for the difference of the network speed, we checked the size of the transferred data and the results are as in Table 2. In case the quarantine authorities send 8192 encrypted patient location data points to the user, the transferred data size ($Transfer_{¿¿} Q \rightarrow U ¿$) is 1.08 MB on average, and when the user sends the computation result to the quarantine authorities, the data size ($Transfer_{¿¿} U \rightarrow Q ¿$) is 0.814 MB on average. In case of the aforementioned 1,000,000 encrypted data points, $Total_{¿} Q \rightarrow U = Transfer_{¿¿} Q \rightarrow U ¿ N_{comp} = 1.08 * 123 = 132.84(MB) ¿¿$ and $Total_{¿} U \rightarrow Q = Transfer_{¿¿} U \rightarrow Q * N_{comp} = 0.814 * 123 = 100.122(MB) ¿¿$.

Also, the CPU utilization level also varies depending on the processing power of the device. s20 Plus shows a lower average CPU utilization level compared to that of Note 8. In case of memory consumption during computation, there is no significant difference. As for CPU utilization and memory consumption, the proximity computation is repeated in batches of 8192, so the increase in the overall time points does not result in several fold increases.

Discussion

Principal Results

This study proposed the PROTECT protocol, which utilizes homomorphic encryption to protect privacy perfectly while performing contact tracing digitally. For this, a novel secure proximity computation technique has been developed so that the location data can be encrypted and exchanged between the user and the quarantine authorities, while the potential COVID-19 patient contact can be identified with encrypted distances only. This method differs from the privacy protection measures of the existing contact tracing in that it identifies contacts with encrypted distances, enabling a far higher level of privacy-preserving contact tracing. Our proposed protocol assumes the existence of a centralized organization that already collects the location history of patients, and checks for proximity without exposing the location information of the patient to the user or that of the user to the organization. The Bluetooth method proposed by Apple and Google requires adoption by a majority of the population for the contact tracing to take effect. Our proposed protocol, however, can exhibit contact tracing effect for those who have installed the app, no matter how small the number of such people is, provided that the organization encrypts and provides the patient data collected so far. Also, the user does not have to provide his/her location information to the government, which is an advantage against the psychological repulsion, one of the greatest hindrances against spreading such an app.

Also, in order to apply the PROTECT protocol to COVID-19, we built an application for the patients and users, and a web service for the quarantine authorities, and the performance indicators related to resource consumption such as computation time, CPU utilization, and memory consumption verify that it is practical enough to be apply to actual COVID-19 quarantine measures.

Comparison with Contact Tracing in Euclidean Space

Contact tracing in Euclidean space is not secure in terms of privacy. To check for proximity under the Euclidean system, one must first compute the Euclidean distance between the two known locations. This, however, leads to an unnecessary location privacy issue. In order to calculate proximity between the locations of two parties, whoever executes that calculation, be it one of the two parties or an entirely separate third party, he or she must possess the location information of both parties. This implies that at least one party must reveal his/her location information to another party. On the other hand, as previously discussed, the PROTECT protocol can only determine that two locations are in the same or adjacent grid through secure proximity computation.

Since the hexagonal grid system recognizes a wider range as adjacent than the Euclidean distance method, contact tracing in Euclidean space might appear to be more efficient than the PROTECT protocol. Suppose that we need to test everyone who is within r or less Euclidean distance from where the covid-19 patient is located. As shown in Figure 7, if the side length of a single hexagonal grid is $\frac{r}{2}$, the area of 7 hexagonal grids is $\frac{21\sqrt{3}}{2}r^2$. The area of the circle is πr^2, so that the rate (deemed adjacent in the hexagonal grid but not actually adjacent in the Euclidean space) is about 30.9%. If the length of one side of the hexagonal grid is made smaller, this ratio decreases, but the secure computation time in the PROTECT protocol increases. However, the spread of COVID-19 cannot be covered by the Euclidean space. Because COVID-19 is highly contagious, the examination scope should be expanded sufficiently. As mentioned earlier, many international organizations are already recommending mass testing for COVID-19 [25-27]. There are also studies demonstrating that mass testing is highly effective through COVID-19 epidemic simulation [30, 31].

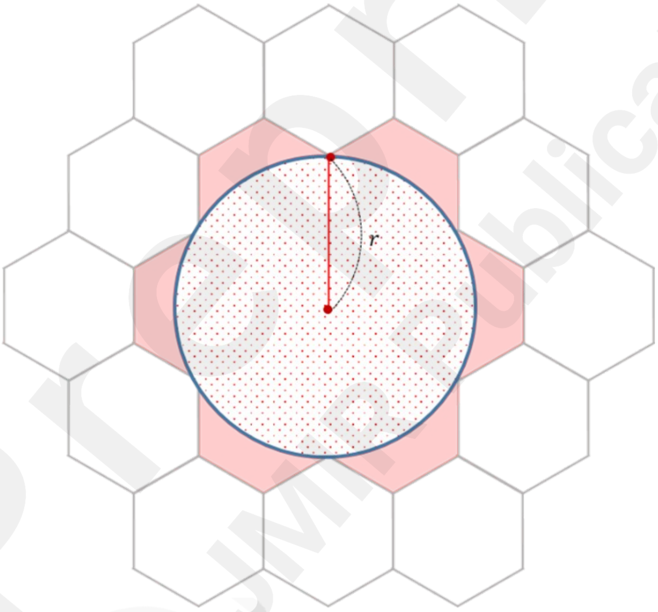


Figure 7. A circle with radius r and 7 hexagons with $\frac{r}{2}$ sides

Limitations

The proposed protocol and system also have limitations shared by all contact tracing methods that make use of digital technologies. There is the limitation of the performance of the smartphone device itself. The accuracy of the GPS location data of each device may vary. GPS, especially, when compared to Bluetooth, is relatively less accurate in an urban setting with many indoor environments and high-rise buildings. Such limitations of the device performance can be complemented by using indoor positioning data such as Wi-Fi and Bluetooth and also the geo-magnetic location measurement techniques. In fact, the indoor positioning data collection technologies have seen much improvement through the advancement of technologies such as fingerprinting.

In this study, all COVID-19 patients are considered. However, in actual quarantine scenarios, one only needs to compare to the patients in the corresponding region, thus reducing the total time. Also, the homomorphically encrypted computation logic was developed in the same language for both the web server and the mobile app. Thus, there were inefficiencies to make it run inside an Android app, such as porting Microsoft SEAL library to WebAssembly with a JavaScript interface and then running it on a JavaScript engine inside a browser. This should be addressed by directly invoking SEAL C++ APIs using JNI (Java Native Interface) for Android applications. The development of a solution of practical level that is applicable to actual quarantine scenarios would be possible by resolving such inefficiencies.

Comparison with Prior Work

In order to prevent the location privacy issue related to the calculation of proximity using location information, Gruteser and Grunwald [32], and Bettini et al. [33] utilized the concept of k-anonymity for location privacy through dummy data. This method can be a useful means to protect location privacy in various location-based services (LBS). However, it is inefficient in the practical setting where the proximity needs to be checked while protecting the location privacy of both parties. Also, Hu et al. [34] proposed a method of calculating the distance using homomorphic encryption and a comparative computation using Geohash. The first method can prevent direct location information exposure through its use of homomorphic encryption, but the location information can be indirectly inferred from the distance information obtained in the end, and thus it cannot be deemed sufficiently safe in terms of location privacy. The second method compares Geohash using homomorphic encryption, and thus is far safer in terms of location privacy. However, it is not practical and/or efficient in terms of computation due to its use of bitwise homomorphic computation.

On the other hand, the secure proximity computation method in this study substitutes the problem of proximity calculation with the computation of identity or adjacency of two grids by mapping the exact location information to a predefined grid system, and then executes the calculation under homomorphic encryption, thus being safe in terms of location privacy and excellent in terms of computation.

Also, from a system-wise perspective, most existing applications, such as TraceTogether of Singapore or COVIDSafe of Australia, are effective only if the users install the app and allow the exchange of data among one another, and has the drawback of increased privacy risks. Moreover, the method proposed by Apple and Google is also vulnerable to several types of security attacks [15]. Above all, the previously mentioned methods become effective only when a majority of users use the app. As for the app and web service based on the proposed PROTECT protocol, however, even if there is only a single user, that user can effectively identify the occurrences of patient contacts as long as the central quarantine authorities have collected the patient location history.

Conclusions

Facing an unprecedented global pandemic situation, the whole world is trying to overcome this crisis by all means. Various IT solutions are being actively suggested in this context. Due to the potential risk of privacy leaks, however, the adoption rates are low and there has been no case of a killer app actively used by many.

In this study, we develop a new proximity computation algorithm which can identify proximity occurrences without exposing the COVID-19 patient location and the user location to each other by homomorphically encrypting the location. And we propose PROTECT, a privacy-preserving contact tracing protocol using this algorithm. In order to apply this to COVID-19 quarantine, the proposed protocol are implemented as a smartphone application of the user and a web service for the quarantine authorities. Homomorphic encryption of the BFV scheme is employed to design a system applicable to a reasonable scale, and through experiments under various conditions, it is verified that this service is practical enough to be used in a real-world scenario. We hope that this approach that intends to resolve the issue through new technologies contribute to the early discovery and suppression of other potential diseases in future.

Conflicts of Interest

None declared

Abbreviations

BFV: Brakerski/Fan-Vercauteren
BGV: Brakerski-Gentry-Vaikuntanathan
COVID-19: Coronavirus Disease
CKKS: Cheon-Kim-Kim-Song
CPU: Central Processing Unit
GPS: Global Positioning System
KCDC: Korea Center for Disease Control and Prevention
LBS: Location-Based Services
PROTECT: PRivacy Oriented Technique for Epidemic Contact Tracing
TFHE: Torus Fully Homomorphic Encryption

References

1. WHO Coronavirus Disease (COVID-19) Dashboard. URL: https://covid19.who.int/ [accessed 2021-01-25].
2. Lee H, Noh E, Choi S, Zhao B, Nam E. Determining Public Opinion of the COVID-19 Pandemic in South Korea and Japan: Social Network Mining on Twitter. Healthcare Informatics Research 2020 Oct;26(4):335-343. doi:10.4258/hir.2020.26.4.335.
3. Bae Y, Kim K, Choi S, Ko T, Jeong C, Cho B, et al. Information Technology–Based Management of Clinically Healthy COVID-19 Patients: Lessons From a Living and Treatment Support Center Operated by Seoul National University Hospital. Journal of medical Internet research 2020 Jun; 22(6): e19938. doi: 10.2196/19938.
4. Park S, Kim Y, Yi S, Lee S, Na B, Kim C, et al. Coronavirus Disease Outbreak in Call Center, South Korea. Emerging infectious diseases 2020 Aug;26(8):1666-1670. doi: 10.3201/eid2608.201274.
5. Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, et al. Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing. Science 2020 May 08;368(6491). doi: 10.1126/science.abb6936.
6. Lenert L, McSwain B. Balancing Health Privacy, Health Information Exchange, and Research in the Context of the COVID-19 Pandemic. Journal of the American Medical Informatics Association 2020 June;27(6):963-966. doi: 10.1093/jamia/ocaa039.
7. Park S, Choi G, Ko H. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies. Jama 2020 Apr 23;323(21):2129-2130. doi:10.1001/jama.2020.6602.
8. South Korea's Experiment in Pandemic Surveillance. 2020 Apr 13. The Diplomat. URL: https://thediplomat.com/2020/04/south-koreas-experiment-in-pandemic-surveillance/ [accessed 2021-01-25].
9. Wang D, Liu F. Privacy Risk and Preservation For COVID-19 Contact Tracing Apps. arXiv preprint arXiv 2020;2006(15433).
10. A Singapore Government Agency Website - TraceTogether. URL: https://www.tracetogether.gov.sg/ [accessed in 2021-01-25].
11. Bay J, Kek J, Tan A, Hau C, Yongquan L, Tan J, et al. BlueTrace: A privacy-preserving

protocol for community-driven contact tracing across borders. Government Technology Agency-Singapore Technical Report. 2020.

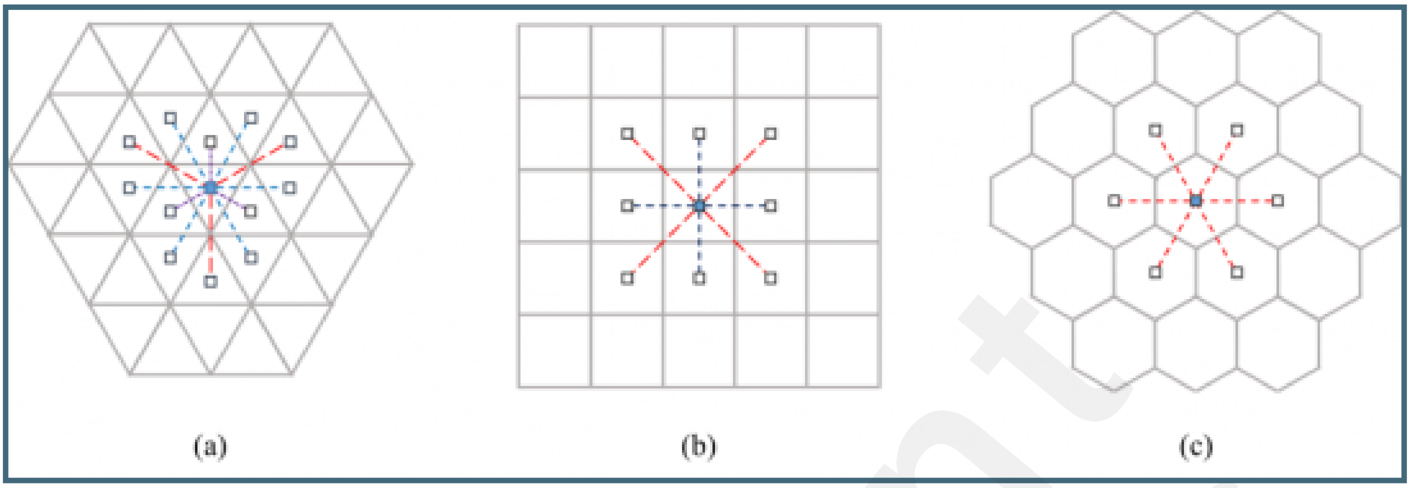
12. COVIDSafe app - Department of Health, Australian Government. URL: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app [accessed in 2021-01-25].
13. Cho H, Ippolito D, Yu Y. Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. arXiv preprint arXiv 2020;2003(11511).
14. Privacy-Preserving Contact Tracing: Apple and Google. URL: https://covid19.apple.com/contacttracing/ [accessed in 2021-01-25].
15. Gvili Y. Security Analysis of the COVID-19 Contact Tracing Specifications by Apple inc. and Google inc. IACR Cryptol ePrint Archive 2020;428.
16. Beresford A, Stajano F. Location privacy in pervasive computing. IEEE Pervasive computing 2003;2(1):46-55. doi: 10.1109/MPRV.2003.1186725
17. Zhong G, Goldberg I, Hengartner U. Louis, lester and pierre: Three protocols for location privacy. In International Workshop on Privacy Enhancing Technologies. Springer, Berlin, Heidelberg 2007 June;62-76. doi: 10.1007/978-3-540-75551-7_5
18. Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory 2014 July;6(3):1-36. doi: 10.1145/2633600
19. Fan J, Vercauteren F. Somewhat Practical Fully Homomorphic Encryption. IACR Cryptol. ePrint Arch., 2012, 144.
20. Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In Annual Cryptology Conference. Springer, Berlin, Heidelberg 2012 August;868-886. doi: 10.1007/978-3-642-32009-5_50
21. Chillotti I, Gama N, Georgieva M, Izabachene M. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In international conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg 2016 December;3-33. doi: 10.1007/978-3-662-53887-6_1
22. Cheon J, Kim A, Kim M, Song Y. Homomorphic encryption for arithmetic of approximate numbers. In International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham 2017 December;409-437. doi: 10.1007/978-3-319-70694-8_15
23. Uber H3. URL: https://eng.uber.com/h3/[accessed in 2020-11-27]
24. World Health Organization. Laboratory testing strategy recommendations for COVID-19: interim guidance. World Health Organization, 2020 March.
25. Allain-Dupré D, Chatry I, Michalun V, Moisio A. The territorial impact of COVID-19: Managing the crisis across levels of government. OECD Policy Responses to Coronavirus, OECD Publishing, Paris 2020 November. doi: 10.1787/d3e314e1-en
26. Scarpetta S, Pearson M, Colombo F, Guanais F. Testing for COVID-19: A way to lift confinement restrictions. OECD Policy Responses to Coronavirus, OECD Publishing, Paris, 2020 May. doi: 10.1787/89756248-en
27. World Health Organization. Surveillance strategies for COVID-19 human infection: interim guidance. World Health Organization , 2020 May.
28. Case Investigation and Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic. URL: https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html[accessed in 2021-03-05]
29. Jung G, Lee H, Kim A, Lee U. Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea. Frontiers in public health 2020 June;8:305. doi: 10.3389/fpubh.2020.00305
30. Giordano G, Blanchini F, Bruno R, Colaneri P, Di Filippo A, Di Matteo A, Colaneri M. Modelling the COVID-19 epidemic and implementation of population-wide interventions in

Italy. Nature medicine 2020 June;26(6):855-860. doi: 10.1038/s41591-020-0883-7
31. Alvarez M, González-González E, Trujillo-de Santiago G. Modeling COVID-19 epidemics in an Excel spreadsheet to enable first-hand accurate predictions of the pandemic evolution in urban areas. Scientific reports 2021 Feb;11(1):4327. doi: 10.1038/s41598-021-83697-w
32. Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the 1st international conference on Mobile systems, applications and services 2003 May;31-42. doi: 10.1145/1066116.1189037
33. Bettini C, Wang X, Jajodia S. Protecting privacy against location-based personal identification. In Workshop on Secure Data Management. Springer, Berlin, Heidelberg 2005 August;185-199. doi: 10.1007/11552338_13.
34. Hu P, Mukherjee T, Valliappan A, Radziszowski S. Homomorphic proximity computation in geosocial networks. In 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE 2016 April;616-621. doi: 10.1109/INFCOMW.2016.7562150

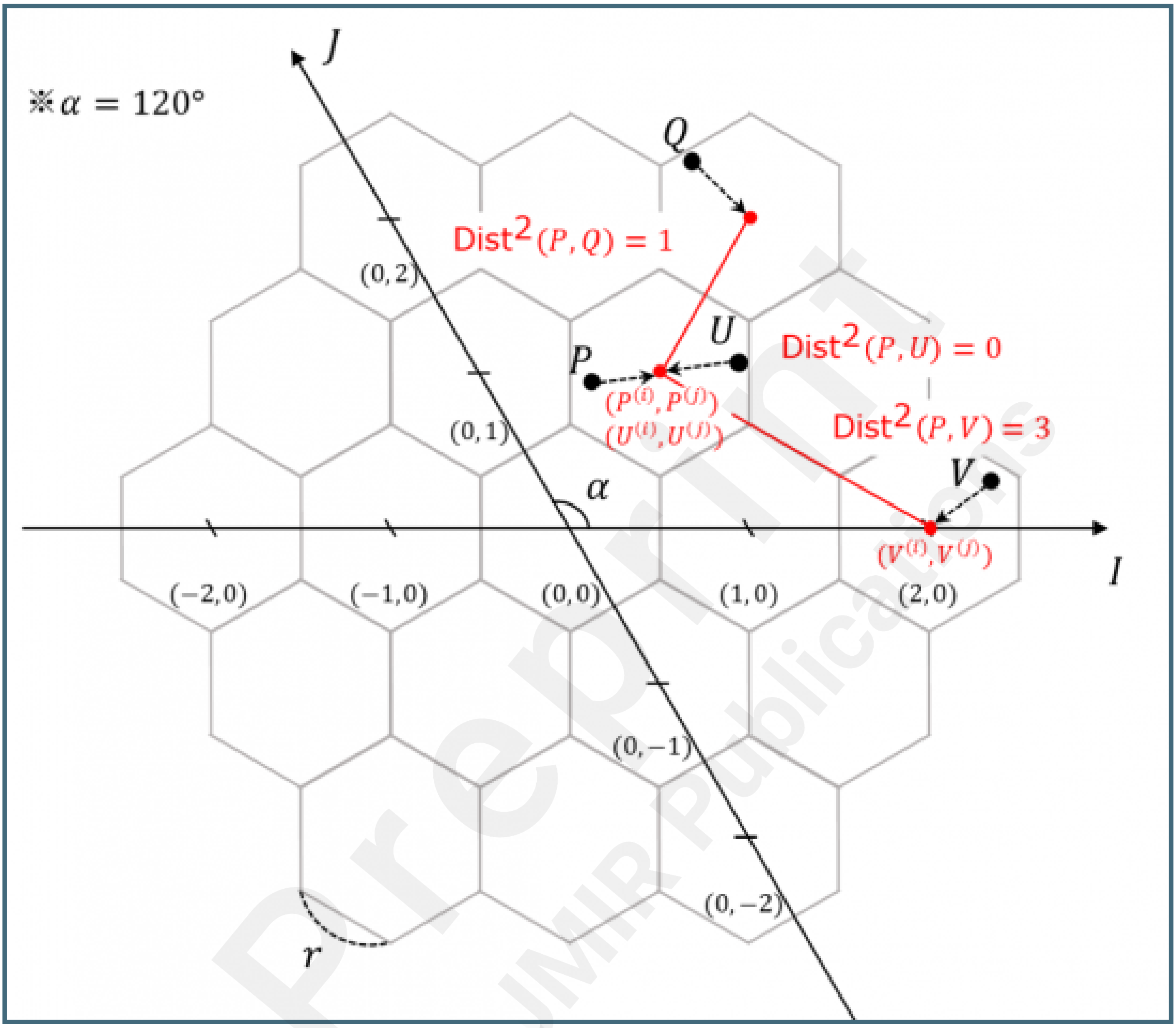
Supplementary Files

Figures

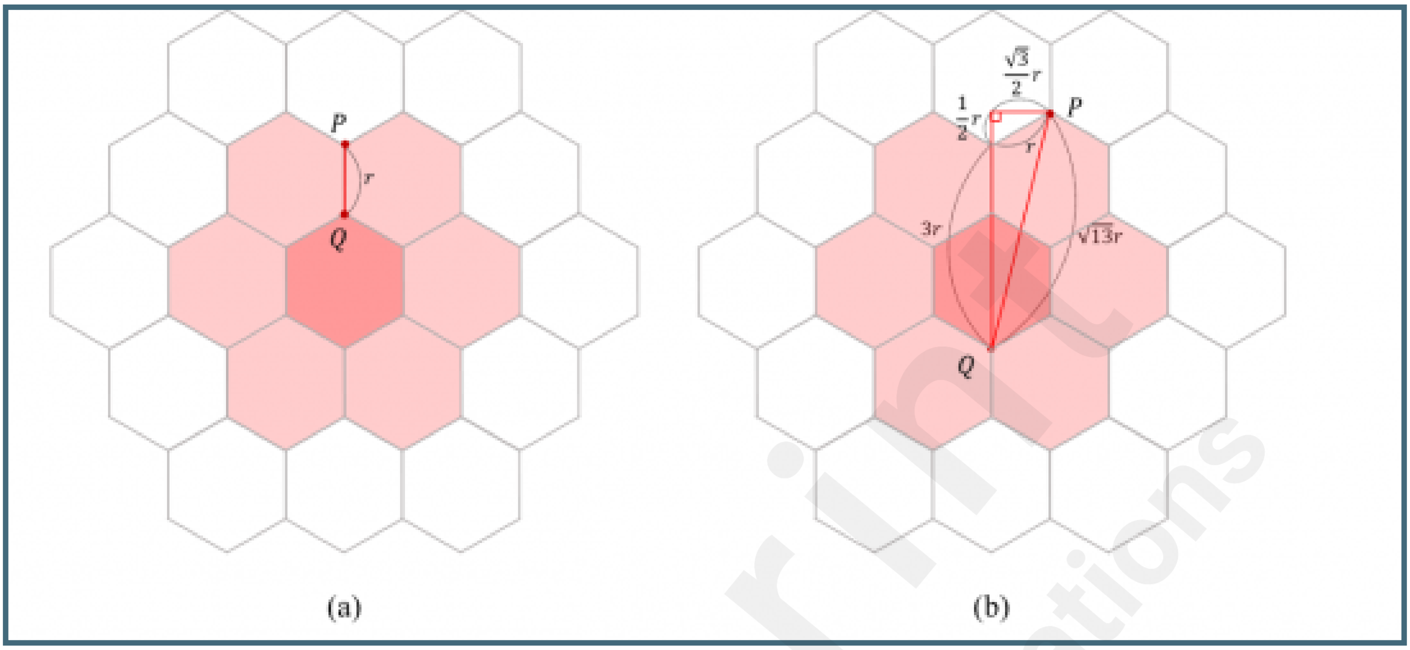
Comparison of triangular, square and hexagonal grids: (a) triangles, (b) squares, (c) hexagons.



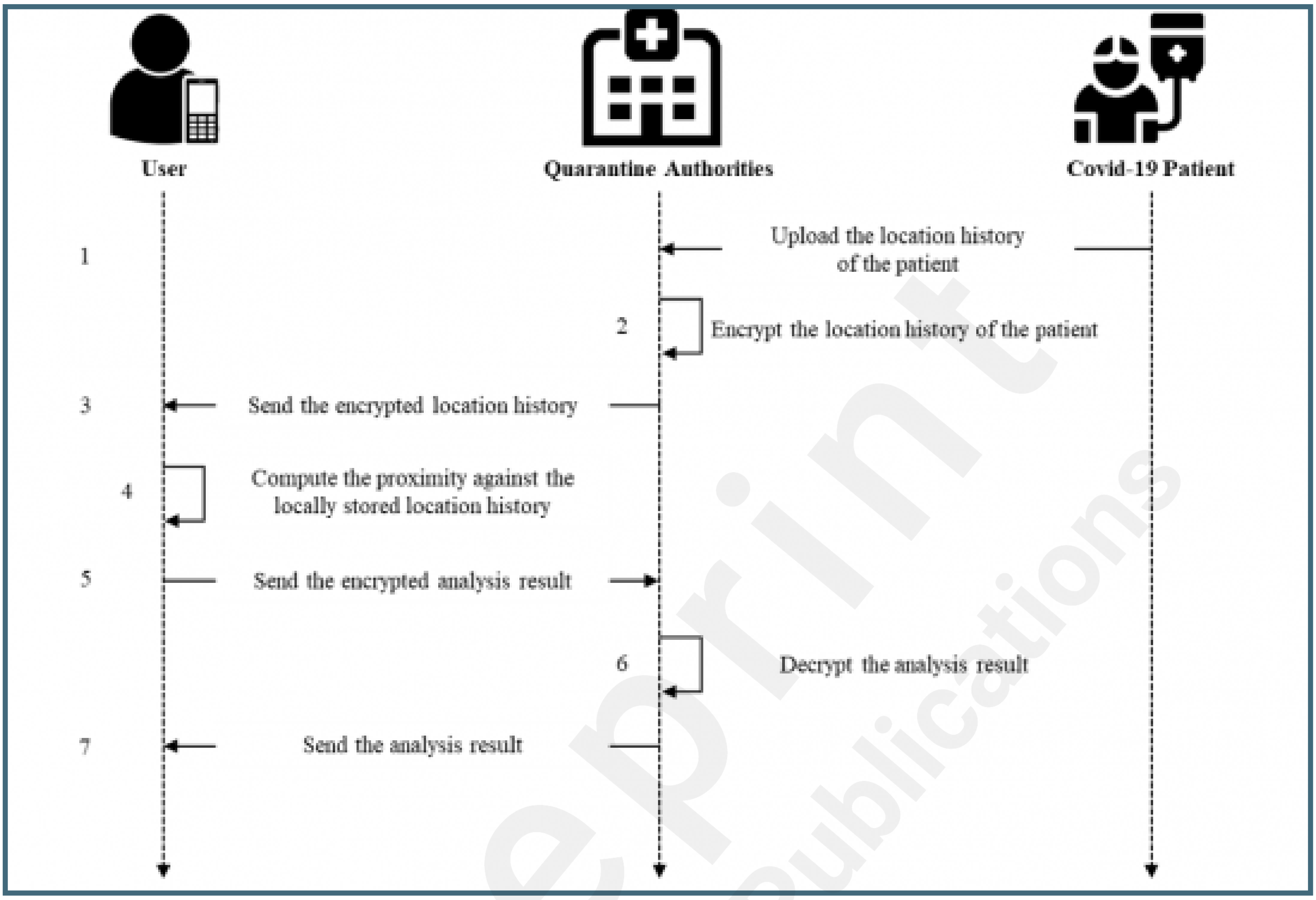
Local IJ coordinates of a hexagonal grid system with a side length of r.



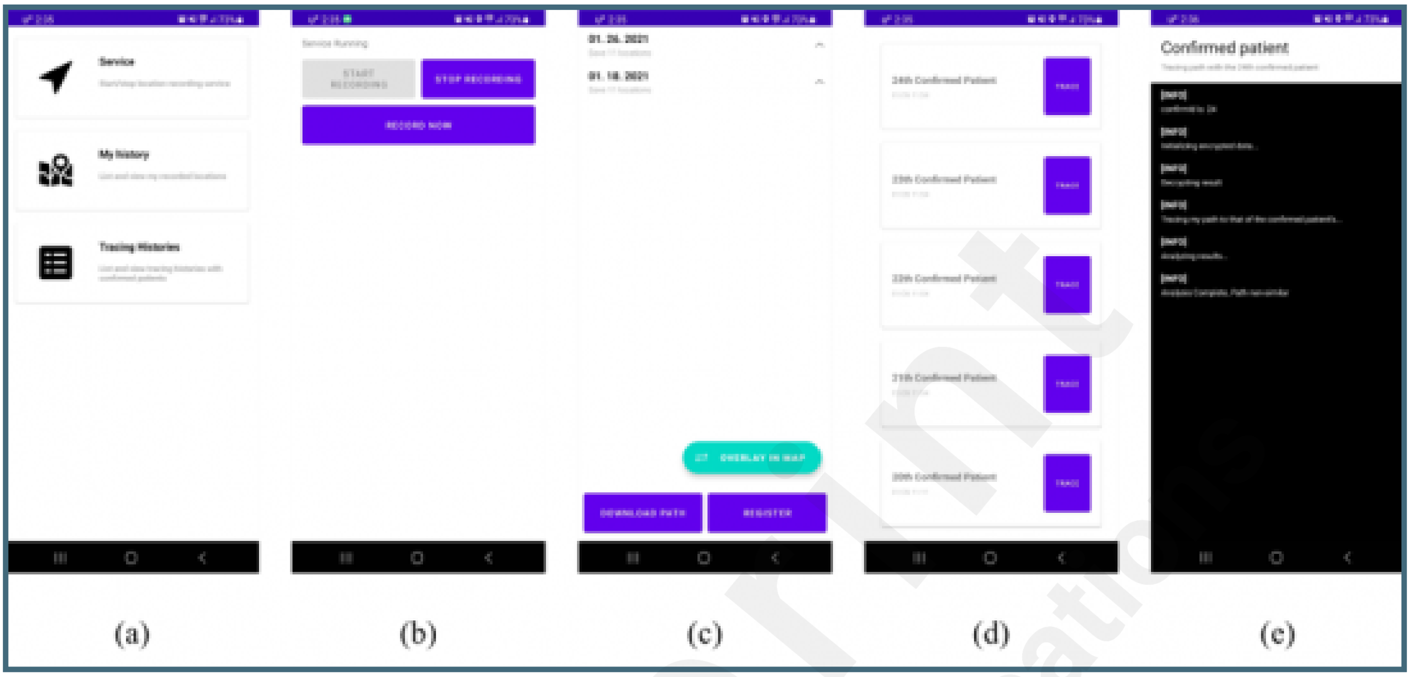
Distance between two points P, Q on hexagonal girds with a side length of r: (a) when the distance between P and Q is slightly greater than r and they are not deemed proximate, (b) when the distance between P and Q is slightly less than ?13 r and they are deemed proximate.



Flow chart for the PROTECT protocol.

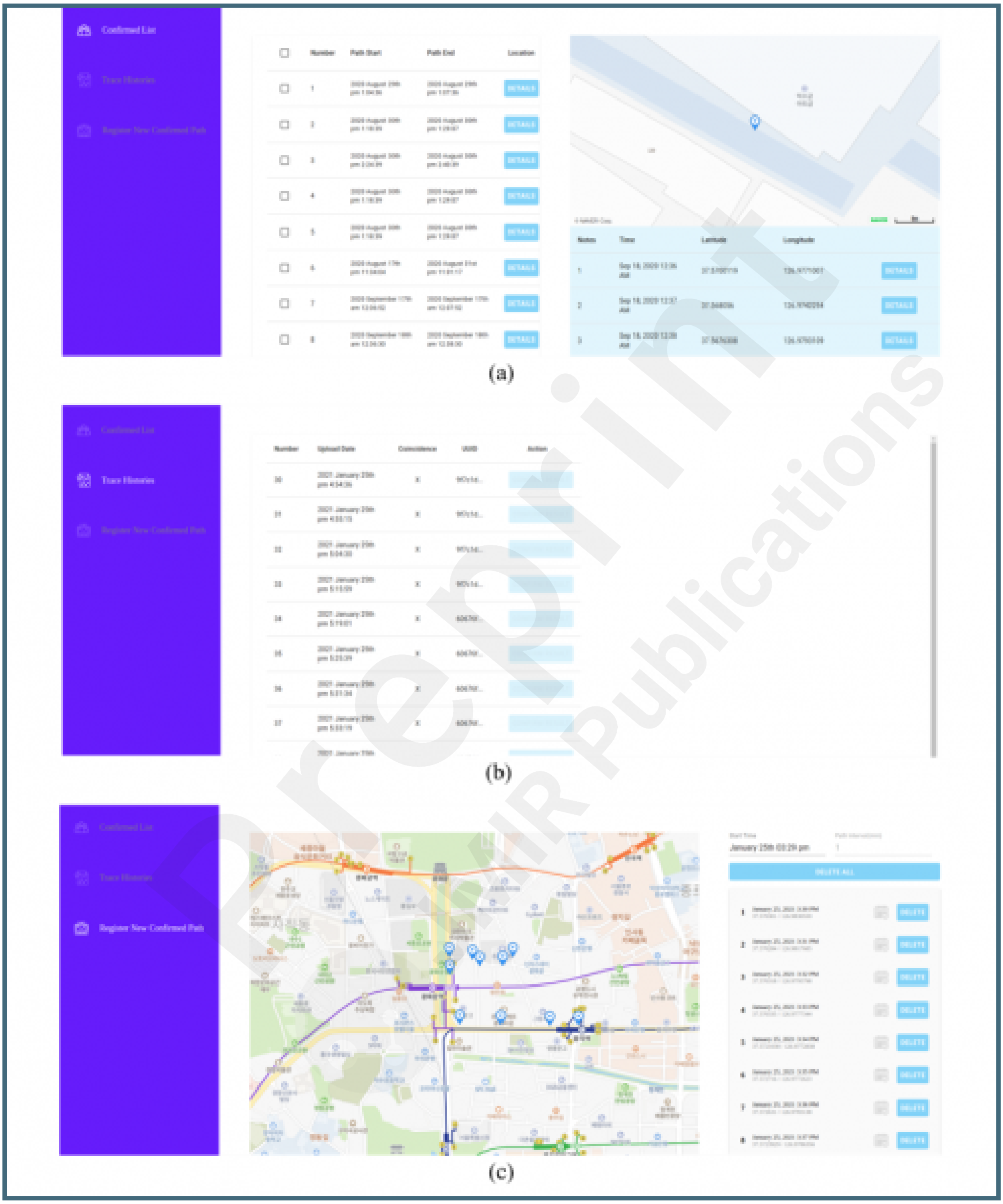

User
Quarantine Authorities
Covid-19 Patient
1
Upload the location history of the patient
2
Encrypt the location history of the patient
3
Send the encrypted location history
4
Compute the proximity against the locally stored location history
5
Send the encrypted analysis result
6
Decrypt the analysis result
7
Send the analysis result

Screenshots of the user application: (a) main screen, (b) GPS data recording setup screen, (c) list of GPS data by day stored on the user's local device, (d) list of encrypted GPS data per patient received from the quarantine authorities, (e) location history comparison and result.

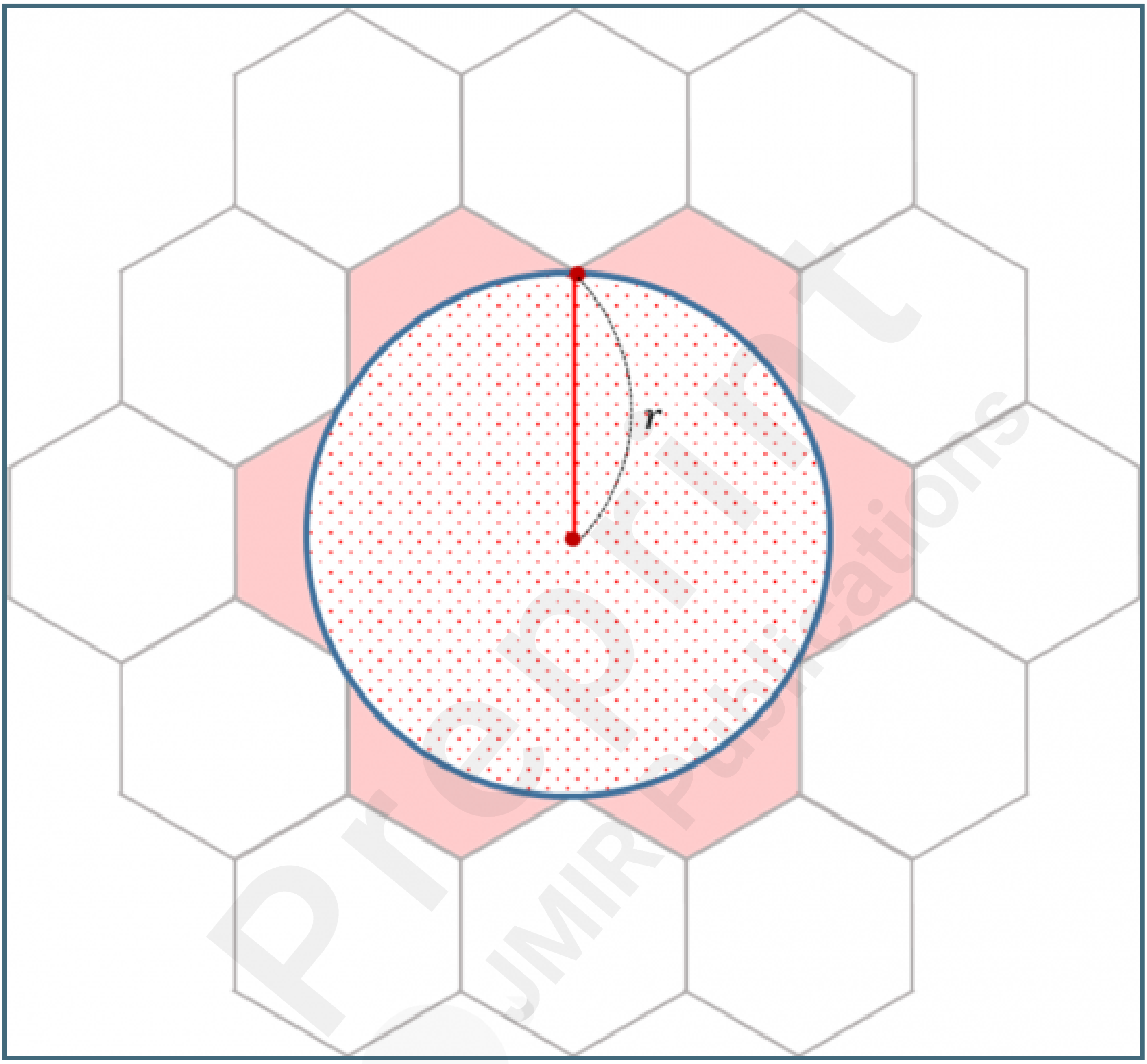


[INFO]
confirmed is: 24
[INFO]
Initializing encrypted data...
[INFO]
Decrypting result
[INFO]
Tracing my path to that of the confirmed patient's...
[INFO]
Analyzing results...
[INFO]
Analysis Complete. Path non-similar

Screenshots of the web service for quarantine authorities: (a) list of confirmed patients GPS data, (b) list of trace histories, (c) register new confirmed patient GPS data.



A circle with radius r and 7 hexagons with r/2 sides.



Multimedia Appendixes

Screenshots of the user application: (a) main screen, (b) GPS data recording setup screen, (c) list of GPS data by day stored on the user's local device, (d) list of encrypted GPS data per patient received from the quarantine authorities, (e) location history comparison and result.
URL: http://asset.jmir.pub/assets/c6d928ae2ae8fcbeaf8ec6460cf11923.png

Screenshots of the web service for quarantine authorities: (a) list of confirmed patients GPS data, (b) list of trace histories, (c) register new confirmed patient GPS data.
URL: http://asset.jmir.pub/assets/53d5d6ab8c3cb08dfe7ff62ee401007d.png