論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Cryptographic Credential Schemes and Their Applications in Contact Tracing
著者(和文)	WangPengfei
Author(English)	Pengfei Wang
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第12832号, 授与年月日:2024年9月20日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12832号, Conferred date:2024/9/20, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（論文博士）
(Dissertation Doctorate)

論　文　要　旨（英文）　（**800**語程度）

Dissertation Summary (approx. 800 words in English)

報告番号 For administrative use only	乙 第　　号	氏　名 Name	Wang, Pengfei

（要　旨）
(Summary)

The outbreak of COVID-19 urges scientists to design contact tracing systems to track close contacts of infectees, because they might still in incubation period (without symptoms). However, ever since contact tracing systems' global-wide implementation, many concerns have arisen.

First, in order to detect nearby users, contact tracing systems use Bluetooth LE to scan surroundings. However, such approach will fail to take environmental factors into consideration (relative humidity, temperature, ventilation, etc.), and environmental factors have been proved by epidemiologists to be capable of impacting virus transmission on an unneglectable degree. Lacking such will yield a large false-positive rate of close contacts involved.

Furthermore, existing contact tracing systems fail to address airborne transmission, which refers to the fact that virus may float in the air for a certain period of time and infect people during that time, without close contact between patient and infectee. Naturally, we need to record geographic location for such non-interactive contact records. However, security frameworks of current contact tracing systems (e.g., privacy preserving contact tracing system by Apple and Google) are not able to include such additional attributes and airborne transmission into secure data generation, transmission, and calculation.

Besides, such systems should have prevented anyone from collecting or modifying user information, but they fail to prevent potential unauthorized access from service providers and do not include service providers into their threat model.

To address all the concerns listed above, an effective contact tracing system will need to be capable of embedding attributes in committed records, having two transmission modes (airborne, droplet), and allowing users conduct tracing independently (because airborne transmission is non-interactive). More importantly, the system needs to maintain confidentiality and integrity -- unauthorized access or modification should be prohibited. Furthermore, the system needs to be scalable -- to ensure performance even in crowded areas, since handshakes of Bluetooth, backbone of most contact tracing systems, takes considerable time to accomplish. We hence designed the two approaches: Environmental Adaptive Contact Tracing System, and Auditable Attribute-Based Credentials Scheme.

Our first attempt is the Environmental Adaptive Contact Tracing System (abbr., EACT). This system is based on decentralized anonymous credential. The construction is built upon the BLS signature and the updatable public key mechanism. This system uses environmental factors influencing particle dynamics, lifetime, to filter scanned results, which lowers the false positive rate. It is a variant of credential systems (decentralized anonymous credential), and thus it is able to carry arbitrary environmental factors. In order to include airborne transmission, we invented discrete

real-time tracking contact-tracing scheme. This system also implements a perfect hiding commitment scheme to disallow multiple identities of the same user.

EACT's software demonstration proves that, because of its non-interactive solution for airborne transmission, its performance is very optimistic. However, vulnerabilities hide beneath EACT's constructions: first, EACT assumes that revealers (e.g., doctors) are semi-honest, and therefore embedding positional and environmental data into records might violate confidentiality as these records, containing sensitive personal identifiable information as mentioned previously, could potentially be accessed and misused by revealers (doctors); second, EACT's two transmission modes' threat models are not compatible, since users in airborne transmission generate records independently in a decentralized manner, while droplet transmission is based on user interactions, and thus issuing one's own records fails to ensure integrity of the system.

Such problems motivate us to turn our eyes to a more unified scheme, which is secure for both transmission modes and threat models of which are compatible to each other. Moreover, we need a scheme to provide better confidentiality to personal identifiable information within positional and environmental data embedded. Therefore, such needs lead us to attribute-based credential schemes, and we hence designed our Auditable Attribute-Based Credentials Scheme.

Auditable Attribute-Based Credentials Scheme (abbr., Auditable ABC) is built upon our auditable public keys (APK) mechanism, which is an extended version of the updatable public key mechanism mentioned previously in EACT. APK adds a new component, auditing key, to the legacy public-private keypair, which allows auditing even if the public key has been updated. Then, we inserted APK into SPS-EQ (Structure-Preserving Signatures on Equivalence Classes) scheme, maintaining SPS-EQ's security definition, to construct our modified SPS-EQ. We thus constructed our Auditable ABC scheme based on 1) such modified SPS-EQ described above, 2) a set-commitment scheme from, and 3) a zero-knowledge proofs of knowledge protocol. Using such construction, we re-designed EACT framework and unified droplet transmission and airborne transmission's threat models, even holding the fact that these two transmissions' natures (interactive and non-interactive) are different.

Despite Auditable ABC's advantages comparing to EACT as described above, according to our software demonstration, although its performance lies in acceptable and reasonable range on real world's perspective, it is still distinctly worse than EACT's performance because of Auditable ABC's interactive nature.

Therefore, we conclude that our two constructions, Environmental Adaptive Contact Tracing System and Auditable Attribute-Based Credentials Scheme, because they are based on different underlying cryptographic schemes: decentralized anonymous credential and attribute-based credential, both have their own advantages and disadvantages as described above. We choose to present both of them in this work with their detailed performance data in our experiment, and their threat model, for researchers or users to compare and decide.

We sincerely hope that our cryptographic scheme can contribute to improved privacy and efficiency in the response to future epidemics, while fervently wishing that such circumstances never arise again.