A Privacy-Preserving Campus Access Control System

ABSTRACT

During the time of widespread epidemic, many emergency policies are used for epidemic prevention. However, these policies often violate the minimum-privilege principle, and harm people's privacy. The campus access control system is one of them, which keeps track of all personnel's footprint in the school. In this project, we proposed a privacy-preserving campus access control system utilizing suitable group signature schemes. After running some experiments with our implementation, we conclude that it is practical to use our system in schools and other communities to protect people's privacy while maintaining effective epidemic prevention.

1 INTRODUCTION

The coronavirus broke out throughout the world this spring. As a result, most facilities are taking stricter entry control measures, including school campuses. In this semester, National Taiwan University is enforcing access control of campus and buildings too. Whenever a personnel enters a building, he needs to swipe his ID card to authenticate his identity, and the server will log the entry record of the personnel. However, this rises some concern in the student community [8]. The entry record of buildings is similar as GPS positioning, which can harm the privacy of students and professors. On one hand, students may not want the school to be able to view their entire footprint. On the other hand, even if we trust the school, we might not trust the database's security. If malicious parties compromised the server or successfully stole the information from database, they can obtain all the students' and professors' footprints (that is tens of thousands of people). Whether the school should use such measures caused a wide discussion. Some people think that privacy is important, while others think that privacy can be compromised for epidemic prevention. But do privacy and epidemic prevention definitely have to conflict? In this project, we are going to propose a campus access control system that satisfies both privacy and epidemic prevention requirements. That is, a scheme to authenticate personnel anonymously, yet when a personnel is diagnosed, his entry records can be revealed without compromising other people's privacy.

In the current scheme used by National Taiwan University, there are some security problems. First of all, the authentication is not perfect. The card readers in building entrances simply read formatted data out of the card and send it to the school. If malicious visitors or personnel want to fake their identity and enter the building, it is possible to do so by faking a card and its content. Moreover, some card readers in the school only read the bar-code of the ID cards, which is even easier to fake. Secondly, there is no privacy protection at all. All the entry records are sent to the school and stored in the database with the personnel's name. That means privileged people of the school can view all personnel's footprint, while they should not be able to do so normally. In addition, the school's database may not be protected safely (recall that the CEIBA system managed by the school just experienced a severe attack this semester), so it is possible that external attackers can obtain all personnel's footprint.

In this project, we will propose a campus access control system that provides anonymous authentication. That is, the school can verify whether a person is a legitimate personnel, but doesn't know a person's exact identity when authenticating. In case of a confirmed diagnosis event, a more authorized unit should be able to de-anonymize the records and find the patient's footprint and contacts. In addition, our scheme can revoke some personnel's authentication ability for some period of time, so we can reject the patient and his contacts' entry. The core of our scheme is a group signature scheme. We tried two different group signature schemes suitable for our system, and their description is given in section 5. The threat model and assumptions we consider are described in section 3, and the security properties we want to achieve are given in section 4. In section 6, we described our system architecture in detail, while in section 7, we analyzed our system with some experiment results.

2 RELATED WORK

During the coronavirus breakout, governments around the world are taking measures for epidemic prevention. However, the effectiveness of epidemic prevention often has a trade-off with individual's privacy. During this period, security researchers aimed to propose schemes that both consider privacy and epidemic prevention. For example, proximity tracing system is an important measure to identify people who had been in contact with an infected person. An international group of experts proposed a "Decentralized Privacy-Preserving Proximity Tracing" scheme (DP-3T)[1], to provide a efficient, effective, and privacy-preserving proximity tracing system. Inspired by this work, we decide to improve the current campus access control system, which puts students' privacy at risk.

When speaking of authentication, we often think of signatures. However, a signature itself does not provide anonymity. If an authentication scheme only aims to verify whether an individual is a group member, without revealing his identity, we can use group signatures [2–6] and ring signatures [7].

In group signatures, any member can sign on behalf of the group, but no one except the group manager can recover the signer's identity. This scheme is naturally suitable for our scheme, where we need a anonymous authentication, but identities need to be recoverable in case of a personnel being diagnosed. D. Boneh et al. [2] designed the scheme with two isomorphic groups based on Strong-Deffie-Hellman assumption. G. Ateniese et al. [3] designed the scheme with RSA-modulus group based on Strong-RSA assumption and Decisional-Deffie-Hellman Assumption. But none of them have implementation and evaluation. A recent research by E. mura et al. [5] implemented a scheme similar to [2] on a 455 bits group and shows that each step takes about tens of milliseconds. However, the previous schemes are inconvenient in revocation. J. Bringer and A. Patey [4] designed a scheme similar to [2] with verifier-local revocation. Verifier-Local Revocation (VLR) group signatures, introduced by D. Boneh and H. Shacham [6], are a particular case of dynamic group signature schemes where the revocation process

does not influence the activity of the signers. [4] can temporarily revoke some users in any time period, for example, 14 days. It is suitable for our case to implement the revocation functionality.

Ring signature is used when the members do not want to cooperate, and there is no group manager. Everyone can only verify if the signer is in the ring by the ring members' public keys. R. Rivest et al. [7] designed two ring signature schemes based on RSA and Rabin public key system. Signing a message require many of the ring members' public keys to gain anonymity, which is inefficient in implementation. So our scheme will be built upon a group signature scheme and other common cryptographic primitives.

3 THREAT MODEL AND ASSUMPTION

3.1 The school

We assume the school is not a trusted party. The school is assumed to execute the planned access control system correctly, but they may attempt to identify personnel from the database of entry records. That is, the school is a honest-but-curious party.

3.2 External attackers

External attackers are malicious parties that may attack the school's server or steal information from the database. Privacy data could be valuable to some organizations. In this scheme, our goal is not to protect the security of the school's database, but the privacy of personnel even if the database is leaked.

3.3 Personnel and Visitors

We assume that personnel care about their own privacy, and may want to be dishonest about their footprint even if diagnosed. They might also try to forge identities to prevent their identities being revealed. The access control system stops visitors who want to enter the campus or buildings. Therefore, they might try to forge identities or bypass the authentication system technically. We do not consider physical bypass here.

3.4 CDC

CDC, or the Ministry of Health and Welfare, is in charge of the diagnose and epidemic prevention policies. We assume CDC is a trusted party, who have the power to de-anonymize the entry records, and will not perform any kind of attacks. Furthermore, the link between CDC and school is authenticated. It is reasonable to trust a government ministry, since if we don't trust it, it is nearly impossible to have any epidemic prevention measures that is both effective and privacy-preserving.

4 SECURITY PROPERTIES

4.1 Anonymity

Given a entry record in the database, it should be infeasible to recover the identity of the personnel creating the record. Only the CDC can break the anonymity using the group secret key. When a personnel is diagnosed, the revealed information should be minimum, where only the necessary information is revealed.

4.2 Unlinkability

Given two entry records in the database, it should be infeasible to know whether the two entry records are created by the same personnel.

4.3 Authentication

Although the access control system is anonymous, it should still satisfy authentication requirements. That is, the server(school) will need to be able to verify that the swiped ID card provides a valid identity (an authorized personnel). personnel shouldn't be able to forge another personnel's identity, and visitors should not be able to bypass the authentication.

4.4 Traceability

The authorized unit (CDC) acts as a group manager, and personnel should not be capable of producing signatures that are untraceable by the CDC in case of being diagnosed.

5 GROUP SIGNATURE

5.1 Definition

5.1.1 bilinear group. Let G_1, G_2, G_τ be cyclic groups of prime order p that is safe($(p-1)/2$ is a prime), g_1, g_2 be the generator of G_1, G_2, respectively. And there is a pairing $e : G_1 \times G_2 \rightarrow G_\tau$ that satisfies

(1) bilinear: $e(u^a, v^b) = e(u, v)^{ab}, \forall u \in G_1, \forall v \in G_2, \forall a, b \in \mathbb{Z}$
(2) non-degenerate: $e(g_1, g_2) \neq 1$

5.1.2 q-Strong Deffie-Hellman(q-SDH) problem. Given bilinear group $G_1, G_2, G_\tau, g_1, g_2$, and a q-tuple $(g_2^\gamma, \ldots, g_2^{(\gamma^q)})$, output a pair $(g_1^{1/(\gamma+x)}, x)$.

5.1.3 adapted DDH problem. Given a cyclic group G of safe prime order p with generator g and g^a, g^b where $a, b \in \mathbb{Z}_p^*$. Also given u, u^a where u is a generator of a subgroup of $\mathbb{Z}_q^*$(q is a prime) with order $(p-1)/2$. Distinguish $g^{a,b}$ from a random number $z \in G$

5.2 SGS scheme

D. Boneh et al. [2] proposed the Short Group Signature (SGS) scheme. The security of the scheme relies on the difficulty of q-SDH problem. The advantage of the scheme is that it has pretty short signature and high efficiency.

5.2.1 keygen. We generate a random integer pair as group manager's secret key. Choose $h \xleftarrow{r} G_1$, $\xi_1, \xi_2 \xleftarrow{r} \mathbb{Z}_p^*$, and set $u, v \in G_1$ such that $u^{\xi_1} = v^{\xi_2} = h$. Choose $\gamma \xleftarrow{r} \mathbb{Z}_p^*$, and set $w = g_2^\gamma$.

Group secret key $gmsk = (\xi_1, \xi_2)$
Group public key $gpk = (g_1, g_2, h, u, v, w)$

For each user i, choose $x_i \xleftarrow{r} \mathbb{Z}_p^*$ and set $A_i = g_1^{1/(\gamma+x_i)}$

User's private key: $sk_i = (A_i, x_i)$
User's token: A_i

The group manager store A_i for each user.

5.2.2 sign. Given group public key $gpk = (g_1, g_2, h, u, v, w)$, user's private key $sk_i = (A_i, x_i)$, and message M, sign the message as follows:

(1) compute the following values:
choose $\alpha, \beta \xleftarrow{r} \in \mathbb{Z}_p^*$

$\delta_1 = x_i\alpha$, $\delta_2 = x_i\beta$
$T_1 \leftarrow u^\alpha$, $T_2 \leftarrow v^\beta$, $T_3 \leftarrow A_i h^{\alpha+\beta}$
choose $\gamma_\alpha, \gamma_\beta, \gamma_x, \gamma_{\delta_1}, \gamma_{\delta_2} \overset{r}{\leftarrow} \mathbb{Z}_p^*$
$R_1 \leftarrow u^{\gamma_\alpha}$, $R_2 \leftarrow v^{\gamma_\beta}$
$R_3 \leftarrow e(T_3, g_2)^{\gamma_x} e(h, w)^{-\gamma_\alpha - \gamma_\beta} e(h, g_2)^{-\gamma_{\delta_1} - \gamma_{\delta_2}}$
$R_4 \leftarrow T_1^{\gamma_x} u^{-\gamma_{\delta_1}}$, $R_5 \leftarrow T_2^{\gamma_x} v^{-\gamma_{\delta_2}}$

(2) compute the challenge c with hash function H
$c \leftarrow H(M||T_1||T_2||T_3||R_1||R_2||R_3||R_4||R_5)$

(3) construct the values with c:
$s_\alpha \leftarrow \gamma_\alpha + c\alpha$, $s_\beta \leftarrow \gamma_\beta + c\beta$, $s_x \leftarrow \gamma_x + cx_i$,
$s_{\delta_1} \leftarrow \gamma_{\delta_1} + c\delta_1$, $s_{\delta_2} \leftarrow \gamma_{\delta_2} + c\delta_2$

(4) output signature σ
$\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$

5.2.3 verify. Given group public key $gpk = (g_1, g_2, h, u, v, w)$, message M, and signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$, verify the signature as follows:

(1) compute the following value:
$\tilde{R_1} \leftarrow u^{s_\alpha} T_1^{-c}$, $\tilde{R_2} \leftarrow v^{s_\beta} T_2^{-c}$
$\tilde{R_3} \leftarrow e(T_3, g_2)^{s_x} e(h, w)^{-s_\alpha - s_\beta} e(h, g_2)^{-s_{\delta_1} - s_{\delta_2}} (e(T_3, w)/e(g_1, g_2))^c$
$\tilde{R_4} \leftarrow u^{-s_{\delta_1}} T_1^{s_x}$, $\tilde{R_5} \leftarrow v^{-s_{\delta_2}} T_2^{s_x}$

(2) check the challenge c with hash function H
$c \overset{?}{=} H(M||T_1||T_2||T_3||\tilde{R_1}|\tilde{R_2}||\tilde{R_3}||\tilde{R_4}||\tilde{R_5})$

If the signature is valid, the verifier store (M, σ).

5.2.4 open. Given group public key $gpk = (g_1, g_2, h, u, v, w)$, message M, signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ and group secret key $gmsk = (\xi_1, \xi_2)$, trace the signer of the signature as follows:

(1) check if the signature is valid as in *verify* part.

(2) recover signer's token $A = T_3/(T_1^{\xi_1} T_2^{\xi_2})$
and find the user's token A_i that match A.

5.3 VLR scheme

J. Bringer and A. Patey [4] proposed a verifier-local revocation (VLR) group signature scheme. The security of the scheme relies on the difficulty of q-SDH problem and adapted DDH problem. In this scheme, we can temporarily revoke users with a revocation list for a time period. Verifier gets the revocation list and checks if a signature is generated by a revoked signer without knowing the true identity of the signer. However, the group manager has to brute-force search the true identity of a signature, which is slow when we want to find the quarantine personnels.

5.3.1 keygen.

(1) choose $\tilde{g_1}, \hat{g_1} \overset{r}{\leftarrow} G_1$, $\gamma \overset{r}{\leftarrow} \mathbb{Z}_p^*$, and set $w = g_2^\gamma$.

(2) let q be a prime and there is a subgroup of $\mathbb{Z}_q^*$ with order $(p-1)/2$. For time period $1, \ldots, T$, choose time tokens $h[] = h_1, \ldots, h_T \overset{r}{\leftarrow} \mathbb{Z}_q^*$ with order $(p-1)/2$.

(3) compute the following values:
$T_1 = e(g_1, g_2)$, $T_2 = e(\tilde{g_1}, g_2)$, $T_3 = e(\hat{g_1}, g_2)$, $T_4 = e(\hat{g_1}, w)$

(4) choose a security parameter λ.
group public key $gpk = (g_1, g_2, \tilde{g_1}, \hat{g_1}, w, T_1, T_2, T_3, T_4, \lambda, h[])$

(5) for each user i, choose $f_i \overset{r}{\leftarrow} \mathbb{Z}_p^*$, and set $F_i = \tilde{g_1}^{f_i}$. Choose $x_i \overset{r}{\leftarrow} \mathbb{Z}_p^*$ and set $A_i = (g_1 F_i)^{1/(x_i+\gamma)}$.
User's private key: $sk_i = f_i$
User's identity: $id_i = F_i$
User's credential $cre_i = (A_i, x_i)$
The revocation token for user i at time period j is $h_j^{x_i}$. If the user i has to be revoked at time period j, the group manager will put the revocation token into revocation list RL_j.
The group manager store (id_i, cre_i) for each user as $gmsk$.

5.3.2 sign. Given group public key gpk, user's private key $sk_i = f_i$, user's credential $cre_i = (A_i, x_i)$, time period j, and message m.

(1) compute the following values: choose $B \overset{r}{\leftarrow} G_1$ and
$J = B^{f_i}$, $K = B^{x_i}$, $L = B^{h_j^{x_i}}$
choose $a \overset{r}{\leftarrow} \mathbb{Z}_p^*$
$b = ax_i$, $T = A_i \hat{g_1}^a$
choose $r_f, r_x, r_a, r_b, r_1, ..., r_\lambda \overset{r}{\leftarrow} \mathbb{Z}_p^*$
$R_1 = B^{r_f}$, $R_2 = B^{r_x}$, $R_4 = K^{r_a} B^{-r_b}$
$R_3 = e(T, g_2)^{-r_x} T_2^{r_f} T_3^{r_b} T_4^{r_a}$
$(V_l, W_l) = (B^{r_l}, B^{h_j^{r_l}})$ for $l = 1, 2, ..., \lambda$

(2) compute $c = H(B||J||K||L||T||R_1||R_2||R_3||R_4||j||m)$

(3) compute $d = H(c||(V_1, W_1)||...||(V_\lambda, W_\lambda))$

(4) construct the value with c
$s_f = r_f + cf_i$, $s_x = r_x + cx_i$, $s_a = r_a + ca$, $s_b = r_b + cb$

(5) construct the value with d, let b_l be the l^{th} bit of d
$s_l = r_l - b_l x$ for $l = 1, 2, ..., \lambda$

(6) output signature σ
$\sigma = (B, J, K, L, T, c, d, s_f, s_x, s_a, s_b, s_1, ..., s_\lambda)$

5.3.3 verify. Given group public key gpk, message m, signature $\sigma = (B, J, K, L, T, c, d, s_f, s_x, s_a, s_b, s_1, ..., s_\lambda)$, time period j and revocation list RL_j.

(1) check the signature with c:
$R_1' = B^{s_f} J^{-c}$, $R_2' = B^{s_x} K^{-c}$, $R_4' = K^{s_a} B^{-s_b}$
$R_3' = e(T, g_2)^{-s_x} T_2^{s_f} T_3^{s_b} T_4^{s_a} T_1^c e(T, w)^{-c}$
check that $c \overset{?}{=} H(B||J||K||L||T||R_1'||R_2'||R_3'||R_4'||j||m)$

(2) check the signature with d:
let b_l be the l^{th} bit of d
$(V_l', W_l') = (B^{s_l} K^{b_l}, (B^{1-b_l} L^{b_l})^{h_j^{s_l}})$ for $l = 1, 2, ..., \lambda$
check that $d \overset{?}{=} H(c||(V_1', W_1')||...||(V_\lambda', W_\lambda'))$

(3) check revocation:
check that $\forall rt \in RL_j, L \neq B^{rt}$

If the signature is valid, the verifier store (m, σ).

5.3.4 open. Given message m, signature σ, time token $h[]$, time period j, and user's token $x_1, ..., x_n$. For $i = 1, 2, ..., n$, compute $rt_{ij} = h_j^{x_i}$ and check $L \overset{?}{=} B^{rt_{ij}}$. If it holds, output (x_i, id_i).

6 SYSTEM ARCHITECTURE

There are three parties in our system architecture: personnel, the school, and CDC. We need to choose one of the group signature schemes mentioned in the previous section. To enable revocation, we need to choose the VLR group signature scheme. In key generation, we have to generate a group with size equivalent to the total number of personnel in the school. After key generation, the group public key will be published and known by every party, the group manager secret key will be given to CDC, and each personnel will

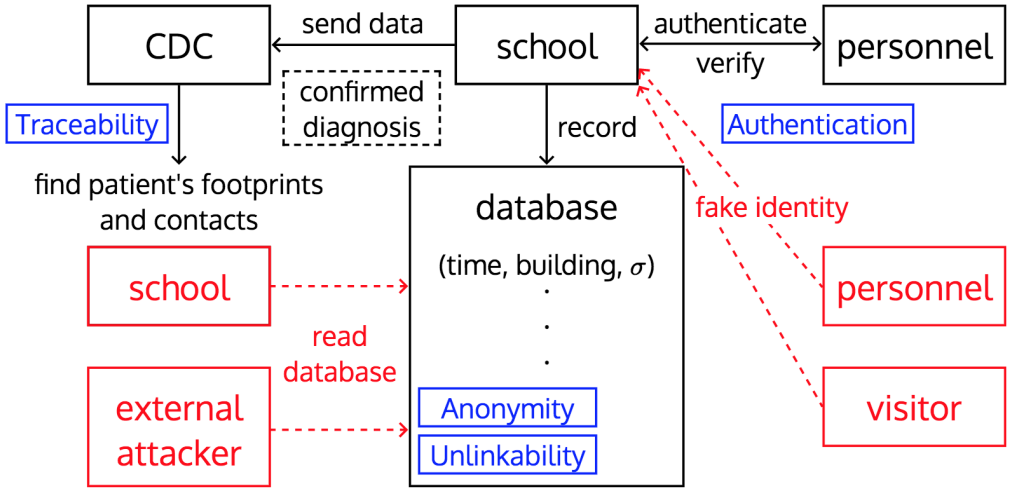

Figure 1: System Architecture, Threat Model, and Security Properties

receive a secret key. The school will control a database that records all the entry records. There are three functionalities of our system:

(1) Since the scheme allows revocation, and the revocation list may be different every day, CDC needs to calculate a revocation list and send it to the school every day. The revocation list is empty if there are no personnel that have been contact with patients. After the school receives the list, it needs to record it for authentication usage today.
(2) When a personnel wants to enter a building, he has to first calculate a signature (using his secret key) of the message containing the current timestamp and the building he is attempting to enter. Then, the personnel sends the message along with the signature to the school. The school will verify that the signature is valid, and the signer is not in the revocation list. If true, the school will allow the entry and record the timestamp, building, and signature into the database. Otherwise, the school will reject the entry.
(3) When there is a confirmed diagnosis case in the school, the CDC will notify the school. Then, the school will send all the entry records within the past 14 days to CDC. Now, CDC will use the group manager secret key to open the records to find the patient's footprint and contacts. Contacts of the patient are those personnel who had been in the same building in the same day with the patient. Next, CDC has to update the revocation list for the next 14 days, adding all the contacts of the patient (and the patient himself) into the lists. At last, CDC will send the patient's footprint and contact to the school, for the school to perform other possible proceeding actions (like sending mails).

The relationship graph of our system architecture, along with visualization of the threat model and security properties are give in figure 1. The software implementation of the proposed system is open-sourced in https://github.com/howard41436/CNS-Final-Project.

7 ANALYSIS

7.1 Security

In our scheme, we assume that CDC is trusted and securely protected. This assumption is reasonable because CDC controls more sensitive private data than the school's database record, and can also investigate more thorough information of the patients. If CDC is not trusted or vulnerable to attack, it is nearly impossible to have any epidemic prevention measures that is privacy-preserving. As long as the link between the school and CDC is authenticated, all of the security properties we needed are guaranteed by the group signature scheme. First of all, during the authentication step, people outside the group do not have secret keys to produce valid signatures of messages. Second, without the group manager secret key, the signatures themselves reveal no information about the true identity of the signer, hence the database is both anonymous and unlinkable as guaranteed by the group signature. At last, the group signature scheme guarantees that any valid signatures can be opened successfully and correctly, so the effectiveness of epidemic prevention will not be decreased.

7.2 Efficiency

A feature of our scheme is that CDC has to be included in our system. So a important question needs to be discussed: how much overhead will we put on CDC? In our scheme, CDC only needs to send the revocation list to the school everyday, and be in charge of finding the patient footprint and contacts when there is a case of confirmed diagnosis. The latter situation happens with low probability (in Taiwan's current situation), and the former can be neglected if no personnel is revoked, which is true most of the time if nobody is diagnosed. Moreover, finding the patient footprint and contacts is indeed CDC's job. The first group signature scheme (SGS) we proposed is more efficient, while the second (VLR) has the revocation ability. To see whether the execution time of the actions are

acceptable, we ran some experiments and analyzed them in the next subsection.

7.3 Experiment result

We simulated the real situation of NTU and evaluated the time cost of each operation. There are about 30000 students in NTU, so we generated 30000 users in keygen. Then we evaluated the authentication time with and without revoked personnel. We assumed that when a diagnosed event is triggered, about 1000 personnel would be quarantined. Since SGS does not have revocation functionality, we did not evaluate the authentication time with revoked personnel. At last, we evaluated the time cost of CDC when a diagnosed event was triggered. We find the patient's footprint in 3000 records and find the quarantine list by opening about 900 records. We implemented on CPU core i5-6200U, and we employed charm python module[9]. Here is our results:

Time cost		
operation	SGS	VLR
keygen	58.539s	82.342s
authentication (no revoked personnel)	0.898s	1.535s
authentication (1000 revoked personnel)	X	2.585s
find quarantine list	12.818s	1945s (32min)

We can see that the authentication time is acceptable, taking less than three seconds even if the revocation list is long as 1000. When finding the quarantine list (contacts of the patient), it takes about 30 minutes on a single CPU core i5-6200U. In practical setting, we estimated that there will be at most 10 times of records to be opened per day, and CDC has to open records of 14 days every time. Therefore, at most 70 CPU hours on a single i5-6200U core is needed, which is achievable in less than an hour with academic-level computational power, not to mention country-level computational power. Therefore, we recommend the VLR group signature for implementation, since revocation is a useful functionality that further protects safety of the campus.

8 DISCUSSION & FUTURE WORK

With regards to the experiment result of our software implementation, we concluded that it is practical to deploy our system in the school. However, before deploying, the hardware implementation has to be decided. If we want to keep using ID cards and card readers, we might require special hardware design and optimization on the card reader, since the ID card itself cannot perform signature calculations. This might be costly and the idea might not be accepted because it is harder to have a "test stage" of our system. Another possibility is to change from swiping cards for entry to swiping QR codes in personnel's phone to initiate communication. The signature calculations can be performed in the phone, and sent to the school. It is easier to directly apply our software implementation this way, and also much easier for testing. For example, we can let the personnel choose which way he wants to enter the building in the testing stage of our system.

Another problem worth discussing is that when finding the patient's contacts, our conditions are too loose so we need to open a lot of signatures. This is because currently a personnel is only required to swipe his card when entering a building, but not when leaving. If the school requires personnel to authenticate when leaving the building too, we can develop a more accurate detection of contacts.

Lastly, since we only survey some of the group signature schemes, we might miss some more suitable group signature schemes for our system. To find the most suitable one, we might need to survey more schemes, compare the efficiency for each of their operations, and also investigate the pros and cons of each schemes. By open-sourcing our work, we hope that the system can be inspected by experts of information security and cryptography. During the severe coronavirus this time, people started to understand that epidemic can really affect our lives in many aspects. We hope that by using our privacy-preserving campus access control system or similar concepts, the school and country could have a better system when epidemic strikes again in the future.

REFERENCES

[1] Decentralized Privacy-Preserving Proximity Tracing. https://github.com/DP-3T/documents

[2] D. Boneh, X. Boyen, H. Shacham. Short group signatures. In M. Franklin, (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg. 2004.

[3] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In M. Bellare, editor, Proceedings of Crypto 2000, volume 1880 of LNCS, pages 255–70. Springer-Verlag, Aug. 2000.

[4] J. Bringer, A. Patey. Backward Unlinkability for a VLR Group Signature Scheme with Efficient Revocation Check. Cryptology ePrint Archive, Report 2011/376 (2011).

[5] K. Emura, T. Hayashi. A revocable group signature scheme with scalability from simple assumptions and its implementation. In L. Chen, M. Manulis, S. Schneider, (eds.) ISC 2018. LNCS, vol. 11060, pp. 442–460. Springer, Cham (2018). 2012, pp. 777–788. ACM Press (2017).

[6] D. Boneh, H. Shacham. Group signatures with verifier-local revocation. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors, ACM Conference on Computer and Communications Security, pages 168–177. ACM, 2004.

[7] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In Proceedings of Asiacrypt 2001, volume 2248 of LNCS, pages 552–65. Springer-Verlag, 2001.

[8] https://sites.google.com/view/ntuprivacy/

[9] https://github.com/JHUISI/charm