LETTER

Randomized Certificate Replacement with Bounded Collateral Damage*

Dae Hyun YUM^{†a)}, *Member*

SUMMARY To accomplish secure communication in vehicular networks, public key infrastructure (PKI) can be employed. However, traditional PKI systems are not suitable because a unique certificate is assigned to each vehicle and thus no anonymity is guaranteed. In the combinatorial certificate schemes, each vehicle is assigned multiple certificates from a shared certificate pool and each certificate in the pool is assigned to multiple vehicles to achieve a level of anonymity. When a certificate assigned to a misbehaving vehicle is revoked, a certificate replacement procedure is executed to all vehicles sharing the certificate. To replace the revoked certificate, a randomized certificate replacement scheme probabilistically assigns different certificates to different vehicles, which can reduce collateral damage caused by repeatedly misusing a certificate and its replacement certificates. Unfortunately, previous randomized certificate replacement schemes allow unbounded collateral damage; a finite number of certificate replacements cannot detect the misbehaving vehicle with certainty. To address this problem, we propose a new randomized certificate replacement scheme with bounded collateral damage.

key words: PKI, privacy, anonymity, certificate revocation

1. Introduction

With vehicular networks, vehicle users can avoid traffic jams and enjoy improved road safety through various traffic- and safety-related applications. However, if the vehicles' privacy cannot be preserved, drivers will not participate in the vehicular networks. To encourage drivers' participation, privacy-preservation techniques that protect vehicles' identity should be employed [1], [2]. However, a conventional certificate (e.g., the ITU-T X.509 standard and IETF RFC 5280) includes plaintext information about the subject of the certificate which adversaries can use to track a vehicle and to determine which messages are from the vehicle.

The challenge for designing a privacy-preserving PKI is to make certificates anonymous while meeting other design goals such as achieving high scalability and robustness [3]. For example, the highest level of anonymity can be easily achieved when all vehicles use the same certificate. However, revoking the certificate will require changes to all vehicles, making the system unscalable. Furthermore, detecting misbehaving vehicles will also be extremely diffi-

cult, which means the system is not robust.

To achieve a level of anonymity, combinatorial certificate schemes assign each certificate to a large enough group of vehicles so that it will be difficult for adversaries to link a certificate to any particular vehicle [3]–[6]. After a certificate authority (CA) creates a shared certificate pool, each certificate in the pool is assigned to multiple vehicles and each vehicle is assigned multiple certificates. When a certificate needs to be revoked, the CA revokes the certificate by posting its identifier (e.g., a serial number) on a certificate revocation list (CRL) and making the CRL available to all vehicles. The CA removes each revoked certificate from the shared certificate pool and assigns a replacement certificate to vehicles that share the revoked certificate. Certificate-revocation collateral damage refers to the problem that when a certificate assigned to a misbehaving vehicle is revoked, all the other vehicles sharing this certificate will also not be able to use it [3]. The more vehicles share each certificate, the more collateral damage will occur when a certificate is revoked. Since anonymity is achieved by sharing each certificate among multiple vehicles, there is a tradeoff between anonymity and collateral damage.

To reduce collateral damage caused by repeatedly misusing a certificate and its replacement certificates, a randomized certificate replacement scheme assigns probabilistically different replacement certificates to vehicles that shared a revoked certificate. This spreads the collateral damage across a different group of vehicles and a misbehaving vehicle increasingly distinguishable each time it revokes a certificate and requests a replacement certificate. Unfortunately, previous randomized certificate replacement schemes allow unbounded collateral damage [3]. This is because randomized certificate replacement schemes choose a replacement certificate randomly from a certificate set and therefore the same replacement certificate could be chosen for vehicles that shared a revoked certificate. In other words, no finite number of certificate replacements can detect with 100% probability a misbehaving vehicle that repeatedly misuses a certificate and its replacement certificates.

We propose a new randomized certificate replacement scheme with bounded collateral damage. Let γ be the number of vehicles that share a certificate. When a misbehaving vehicle revokes a certificate, we divide the γ vehicles that share the revoked certificate randomly into two groups of the same size and then assign different certificates to the two groups; one replacement certificate is assigned to the vehicles belonging to the first group and another replacement

Manuscript received June 11, 2015.

Manuscript publicized July 27, 2015.

[†]The author is with the Department of Information and Communication Engineering, Myongji University, Yongin, Gyeonggi-do, 449–728, Republic of Korea.

*This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2013R1A1A1009630).

a) E-mail: dhyum@mju.ac.kr

DOI: 10.1587/transinf.2015EDL8133

certificate to the second group. Conceptually, we mix a randomized process with a deterministic process; the grouping process is randomized but the sizes of the resulting groups are deterministic. If a misbehaving vehicle repeatedly revokes a certificate and its replacement certificates, the proposed scheme can detect the vehicle after $\log \gamma + 1$ certificate replacements.

2. Previous Work

In combinatorial certificate schemes (e.g., [3]–[6]), the CA creates a shared certificate pool which consists of N pairs of private and public keys with their certificates. Each vehicle is given n ($\leq N$) certificates with their associated private and public keys from the shared certificate pool. Let V be the number of vehicles. If N is too large (i.e., $N \gg nV$), then each vehicle may be assigned unique n certificates and in this case, no anonymity can be achieved. If N is too small (i.e., $N \simeq n$), the same n certificates may be assigned to all vehicles and no robustness is achieved; e.g., when $N = n$, all vehicles are always assigned the same n certificates and hence, detecting a misbehaving vehicle is hopeless (i.e., complete anonymity is achieved).

When a certificate needs to be revoked, different methods can be used to randomize the replacement certificates [3, Chapter 16].

- IRR (Individually randomized replacement): Each time a vehicle sends a certificate revocation request, the CA randomly selects a certificate from the shared certificate pool as the replacement certificate.
- GRGR (Group revocation with group replacement): The CA revokes $g > 1$ certificates at a time and replaces them with g new certificates. A vehicle that shares x of the g revoked certificates will be given x new certificates selected uniformly at random from the g new certificates.
- FSR (Full set replacement): The CA keeps track of the new certificates it has generated to replace revoked certificates. When there are $g \geq 1$ new certificates in the shared certificate pool, each replacement certificate for a vehicle will be selected with probability p from the g new certificates and with probability $(1 - p)$ from the old certificates in the shared certificate pool.

Since a replacement certificate is chosen in a purely probabilistic manner, all the above methods can suffer from the unbounded collateral damage. Vehicles that shared a revoked certificate can be probabilistically assigned the same (new or old) replacement certificate. If this happens repeated, the level of anonymity for a misbehaving vehicle does not decrease. Therefore, no finite number of certificate replacements can guarantee the detection of the misbehaving vehicle.

3. Mathematical Model

A combinatorial certificate scheme can be described as a

graph $G = (\mathcal{V}, \mathcal{C}, \mathcal{E})$ where $\mathcal{V} = \{v_1, v_2, \dots, v_V\}$ is the vertex set of V vehicles, $\mathcal{C} = \{c_1, c_2, \dots, c_N\}$ is the vertex set of N certificates, and $\mathcal{E}$ is the set of edges (v, c) for $v \in \mathcal{V}$ and $c \in \mathcal{C}$ such that $(v_i, c_j) \in \mathcal{E}$ if and only if the vehicle v_i is assigned the certificate c_j . For each edge $(v_i, c_j) \in \mathcal{E}$, the vertices $\{v_i, c_j\}$ are said to be adjacent to one another. Let $\mathcal{C}(v_i)$ be the subset of $\mathcal{C}$ that consists of certificates adjacent to the vehicle v_i . In other words, $\mathcal{C}(v_i)$ includes the certificates assigned to the vehicle v_i . Similarly, $\mathcal{V}(c_j)$ is the subset of $\mathcal{V}$ that consists of vehicles adjacent to the certificate c_j , which means that $\mathcal{V}(c_j)$ includes the vehicles sharing the certificate c_j . $\mathcal{V}(c_j)$ is called the anonymity set of c_j and the size of the anonymity set $|\mathcal{V}(c_j)|$, which is denoted by $|\mathcal{V}(c_j)|$, indicates the level of anonymity achievable by the certificate c_j . Without loss of generality, we can assume that the size of anonymity set of each certificate is non-zero, i.e., each certificate in $\mathcal{C}$ is assigned to at least one vehicle in $\mathcal{V}$; otherwise, we can simply remove the certificates having an empty anonymity set from $\mathcal{C}$.

Let $G = (\mathcal{V}, \mathcal{C}, \mathcal{E})$ be a combinatorial certificate scheme where $\mathcal{V} = \{v_1, v_2, \dots, v_V\}$ and $\mathcal{C} = \{c_1, c_2, \dots, c_N\}$. Suppose a misbehaving vehicle misused certificate c_k and caused it to be revoked. In a deterministic certificate replacement scheme, the CA revokes c_k by posting its identifier on a CRL and then assigns a replacement certificate $c_k^{(1)}$ to $\mathcal{V}(c_k)$ that shared the revoked certificate c_k . As all vehicles in $\mathcal{V}(c_k)$ receive the same replacement certificate $c_k^{(1)}$, it holds that $\mathcal{V}(c_k) = \mathcal{V}(c_k^{(1)})$. If the misbehaving vehicle subsequently misuses certificate $c_k^{(1)}$ and causes it to be revoked, a replacement certificate $c_k^{(2)}$ will be assigned to all vehicles in $\mathcal{V}(c_k^{(1)})$. If the misbehaving vehicle repeats this pattern t times, it will hold that $\mathcal{V}(c_k) = \mathcal{V}(c_k^{(1)}) = \mathcal{V}(c_k^{(2)}) = \dots = \mathcal{V}(c_k^{(t)})$. It is difficult to detect which vehicle is misbehaving because all the vehicles in group $\mathcal{V}(c_k)$ will appear to have misused the same sequence of certificates as the misbehaving vehicle does. Therefore, a misbehaving vehicle can cause collateral damage to a group of vehicles repeatedly without worrying about being detected.

In a randomized certificate replacement scheme, each certificate replacement is probabilistic [3]. If a misbehaving vehicle misused certificate c_k and caused it to be revoked, then each vehicle (including the misbehaving vehicle) in $\mathcal{V}(c_k)$ receives a replacement certificate chosen randomly from a certificate set which may be composed of the shared certificate pool $\mathcal{C}$ and/or some new certificates. Let $c_k^{(1)}$ be the replacement certificate that is assigned to the misbehaving vehicle. As replacement certificates are randomized, the other vehicles in $\mathcal{V}(c_k)$ may receive the same replacement certificate $c_k^{(1)}$ or different replacement certificates. Therefore, the set $\mathcal{V}(c_k^{(1)})$ of vehicles that share the replacement certificate $c_k^{(1)}$ may be different from the set $\mathcal{V}(c_k)$ of vehicles that shared the revoked certificate c_k . If the misbehaving vehicle subsequently causes certificate $c_k^{(1)}$ to be revoked, the misbehaving vehicle will be assigned a replacement certificate $c_k^{(2)}$ and the other vehicles in $\mathcal{V}(c_k^{(1)})$ will be assigned

$c_k^{(2)}$ or different replacement certificates. If the misbehaving vehicle repeats this pattern t times, collateral damages spread across different groups of vehicles and this makes the misbehaving vehicle distinguishable. Let $c_k^{(0)}$ denote the initial certificate c_k , i.e., $c_k^{(0)} = c_k$. Only the vehicles in the intersection set $\bigcap_{0 \leq i \leq t-1} \mathcal{V}(c_k^{(i)})$ will be requesting replacement certificates for the exact sequence of revoked certificates $c_k^{(0)}, c_k^{(1)}, \dots, c_k^{(t-1)}$. As the value of t increases, the intersection set $\bigcap_{0 \leq i \leq t-1} \mathcal{V}(c_k^{(i)})$ is expected to shrink and the misbehaving vehicle can be detected with high probability.

A sequence is said to be monotonically decreasing if each term is less than or equal to the one before it. If each consecutive term is strictly less than the previous term, then the sequence is called strictly monotonically decreasing. Consider the sequence of sizes of anonymity sets $(|\mathcal{V}(c_k^{(i)})|)_{0 \leq i \leq t} = (|\mathcal{V}(c_k^{(0)})|, |\mathcal{V}(c_k^{(1)})|, \dots, |\mathcal{V}(c_k^{(t)})|)$. The sequence is not monotonically decreasing because if the replacement certificate $c_k^{(i)}$ happens to be chosen from the initial pool C , i.e., $c_k^{(i)} \in C$, the relation $|\mathcal{V}(c_k^{(i-1)})| < |\mathcal{V}(c_k^{(i)})|$ may hold. Meanwhile, the sequence $(|\bigcap_{0 \leq i \leq j} \mathcal{V}(c_k^{(i)})|)_{0 \leq j \leq t-1} = (|\mathcal{V}(c_k^{(0)})|, |\mathcal{V}(c_k^{(0)}) \cap \mathcal{V}(c_k^{(1)})|, \dots, |\bigcap_{0 \leq i \leq t-1} \mathcal{V}(c_k^{(i)})|)$ is monotonically decreasing because the basic property of intersection $A \cap B \subseteq A$ holds for any sets A and B . To revoke certificate $c_k^{(i)}$, the CA in previous randomized certificate replacement schemes chooses replacement certificates for $\mathcal{V}(c_k^{(i)})$ randomly from a certificate set. Therefore, the same replacement certificate $c_k^{(i+1)}$ can be repeatedly chosen for vehicles in $\mathcal{V}(c_k^{(i)})$ and it can happen that $\mathcal{V}(c_k^{(0)}) = \mathcal{V}(c_k^{(1)}) = \dots = \mathcal{V}(c_k^{(t-1)})$. This in turn implies that the sequence $(|\bigcap_{0 \leq i \leq j} \mathcal{V}(c_k^{(i)})|)_{0 \leq j \leq t-1}$ is constant and the misbehaving vehicle cannot be detected. As any finite number of certificate replacements cannot guarantee, with 100% probability, detection of a misbehaving vehicle that repeatedly misuses a certificate and its replacement certificates, previous randomized certificate replacement schemes allow unbounded collateral damage.

4. Proposed Randomized Certificate Replacement

In the previous randomized certificate replacement schemes, the sequence $(|\bigcap_{0 \leq i \leq j} \mathcal{V}(c_k^{(i)})|)_{0 \leq j \leq t-1}$ is monotonically decreasing but not strictly monotonically decreasing; hence, the sequence can become constant, which allows unbounded collateral damage. In order to guarantee bounded collateral damage, we design a randomized certificate replacement scheme in which the sequence $(|\bigcap_{0 \leq i \leq j} \mathcal{V}(c_k^{(i)})|)_{0 \leq j \leq t-1}$ is strictly monotonically decreasing.

Let $G = (\mathcal{V}, C, \mathcal{E})$ be the proposed scheme where $\mathcal{V} = \{v_1, v_2, \dots, v_V\}$ and $C = \{c_1, c_2, \dots, c_N\}$. For simplicity, we assume that the size of each initial anonymity set is a power of two; for each certificate c_i , there is a non-negative integer d_i such that $|\mathcal{V}(c_i)| = 2^{d_i}$. Our scheme works as follows; when a certificate c_k is required to be revoked, the CA

checks the size of the anonymity set $\mathcal{V}(c_k)$.

- If $|\mathcal{V}(c_k)| > 1$, then the CA generates two new replacement certificates and bisects $\mathcal{V}(c_k)$ randomly into two groups of the same size $\frac{|\mathcal{V}(c_k)|}{2}$. The CA assigns one replacement certificate to the vehicles in the first group and the other replacement certificate to the vehicles in the second group. More generally, if $|\mathcal{V}(c_k)|$ is not a power of two, then $\mathcal{V}(c_k)$ can be bisected into two groups of size $\lfloor \frac{|\mathcal{V}(c_k)|}{2} \rfloor$ and $\lceil \frac{|\mathcal{V}(c_k)|}{2} \rceil$.
- If $|\mathcal{V}(c_k)| = 1$, then the CA can identify the vehicle that requested the revocation of c_k . The CA investigates the misbehavior of the vehicle.

Suppose a misbehaving vehicle misused certificate c_k and caused it to be revoked. The CA generates two new replacement certificates $\{c_k^{(1)*}, c_k^{(1)}\}$ and randomly divides $\mathcal{V}(c_k)$, of which the size is larger than one, into two groups of size $\frac{|\mathcal{V}(c_k)|}{2}$. Without loss of generality, we assume that the replacement certificate $c_k^{(1)}$ is assigned to the group which includes the misbehaving vehicle, i.e., the misbehaving vehicle belongs to the group $\mathcal{V}(c_k^{(1)})$. As $\mathcal{V}(c_k)$ is bisected into $\mathcal{V}(c_k^{(1)*})$ and $\mathcal{V}(c_k^{(1)})$, we have $\mathcal{V}(c_k^{(1)}) \subset \mathcal{V}(c_k)$ and $|\mathcal{V}(c_k^{(1)})| = \frac{|\mathcal{V}(c_k)|}{2}$. If the misbehaving vehicle repeats this pattern t times, the following relations hold where $c_k^{(0)} = c_k$.

$$\begin{aligned} \mathcal{V}(c_k^{(t)}) &\subset \mathcal{V}(c_k^{(t-1)}) \subset \dots \subset \mathcal{V}(c_k^{(1)}) \subset \mathcal{V}(c_k^{(0)}) \\ |\mathcal{V}(c_k^{(t)})| &= \frac{|\mathcal{V}(c_k^{(t-1)})|}{2} = \dots = \frac{|\mathcal{V}(c_k^{(1)})|}{2^{t-1}} = \frac{|\mathcal{V}(c_k^{(0)})|}{2^t} \end{aligned}$$

These relations imply that $\bigcap_{0 \leq i \leq t} \mathcal{V}(c_k^{(i)}) = \mathcal{V}(c_k^{(t)})$ and $|\bigcap_{0 \leq i \leq j} \mathcal{V}(c_k^{(i)})| = |\mathcal{V}(c_k^{(j)})| = \frac{|\mathcal{V}(c_k^{(0)})|}{2^j}$. Therefore, the sequence $(|\bigcap_{0 \leq i \leq j} \mathcal{V}(c_k^{(i)})|)_{0 \leq j \leq t-1}$ is strictly monotonically decreasing. If $|\mathcal{V}(c_k^{(0)})| = \gamma = 2^\beta$, then β certificate replacements gives the relation $|\bigcap_{0 \leq i \leq \beta} \mathcal{V}(c_k^{(i)})| = |\mathcal{V}(c_k^{(\beta)})| = \frac{|\mathcal{V}(c_k^{(0)})|}{2^\beta} = 1$ and makes the misbehaving vehicle belong to the anonymity set $\mathcal{V}(c_k^{(\beta)})$ of size one. If the misbehaving vehicle misuses certificate $c_k^{(\beta)}$ and makes it revoked, the CA can detect the misbehaving vehicle. Therefore, the detection of the misbehaving vehicle is guaranteed by $\beta + 1 (= \log \gamma + 1)$ certificate replacements and the bounded collateral damage is achieved. Note that β certificate replacements can detect a misbehaving vehicle in an anonymity set of exponential size 2^β .

5. Comparison

Recall that there is a tradeoff between collateral damage and anonymity in combinatorial certificate schemes. In this section, we calculate the anonymity levels of the proposed scheme and the previous schemes. Let γ be the number of vehicles that share a certificate. Then, the initial anonymity level of a vehicle with respect to each certificate is γ . Suppose that a misbehaving vehicle repeatedly revokes t certificates $c_k, c_k^{(1)}, \dots, c_k^{(t-1)}$. We investigate, after revocation of

Table 1 Comparison of randomized certificate replacement schemes.

	IRR	GRGR	Ours
Collateral damage	unbounded	unbounded	bounded
Anonymity level	$> \gamma$	$= \gamma$	$\approx \frac{1}{3}\gamma$

the t certificates, the anonymity level of a vehicle (with respect to a replacement certificate) which originally shared c_k . The result is summarized in Table 1.

Because IRR scheme does not generate new certificates, each unrevoked certificate gets shared by more vehicles and anonymity levels increase. GRGR scheme replaces g revoked certificates with g new certificates and thus anonymity levels remain unchanged. The proposed scheme achieves the bounded collateral damage but the anonymity level reduces to approximately one third of the initial anonymity level. Detailed analysis of anonymity levels is given in the following subsections.

5.1 Anonymity Level of the Proposed Scheme

We use the same symbols and notations in Sect. 4. When a misbehaving vehicle causes certificate c_k to be revoked, the CA bisects $\mathcal{V}(c_k)$ of size γ into $\mathcal{V}(c_k^{(1)*})$ and $\mathcal{V}(c_k^{(1)})$ of size $\frac{\gamma}{2}$. If the misbehaving vehicle repeatedly revokes t certificates $c_k, c_k^{(1)}, \dots, c_k^{(t-1)}$, $\mathcal{V}(c_k)$ is partitioned into $t+1$ sets: $\mathcal{V}(c_k^{(1)*}), \mathcal{V}(c_k^{(2)*}), \dots, \mathcal{V}(c_k^{(t)*})$ and $\mathcal{V}(c_k^{(t)})$, where $|\mathcal{V}(c_k^{(i)*})| = \frac{\gamma}{2^i}$ for $1 \leq i \leq t$ and $|\mathcal{V}(c_k^{(t)})| = \frac{\gamma}{2^t}$. In this case, we can compute the expected anonymity level of a vehicle x , which originally belonged to $\mathcal{V}(c_k)$, as follows.

$$\begin{aligned}
& \Pr[x \in \mathcal{V}(c_k^{(1)*})] \cdot \frac{\gamma}{2} + \dots + \Pr[x \in \mathcal{V}(c_k^{(t)*})] \cdot \frac{\gamma}{2^t} \\
& + \Pr[x \in \mathcal{V}(c_k^{(t)})] \cdot \frac{\gamma}{2^t} \\
& = \left(\frac{1}{2} \cdot \frac{\gamma}{2} + \dots + \frac{1}{2^t} \cdot \frac{\gamma}{2^t} \right) + \frac{1}{2^t} \cdot \frac{\gamma}{2^t} \\
& = \left\{ \left(\frac{1}{4} + \dots + \frac{1}{4^t} \right) + \frac{1}{4^t} \right\} \gamma = \left(\frac{\frac{1}{4}(1 - \frac{1}{4^t})}{1 - \frac{1}{4}} + \frac{1}{4^t} \right) \gamma \\
& = \left(\frac{1}{3} + \frac{2}{3} \cdot \frac{1}{4^t} \right) \gamma \approx \frac{1}{3} \gamma
\end{aligned}$$

Therefore, after the misbehaving vehicle revokes t certificates $c_k, c_k^{(1)}, \dots, c_k^{(t-1)}$, the expected anonymity level of a vehicle with respect to a replacement certificate becomes $\frac{1}{3}\gamma$ approximately.

5.2 Anonymity Levels of Previous Schemes

In combinatorial certificate scheme, the CA creates a shared certificate pool of size N . When a certificate is required to be revoked, IRR scheme randomly selects a replacement certificate from the shared certificate pool. If certificate c_k is revoked, a vehicle in $\mathcal{V}(c_k)$ is assigned a random replacement certificate c_i ($\neq c_k$) from the shared certificate pool.

Therefore, each unrevoked certificate c_i in the shared pool becomes shared by $\gamma + \frac{\gamma}{N-1} = \frac{N}{N-1}\gamma$ vehicles, where the first term γ denotes the vehicles which initially share c_i and the second term $\frac{\gamma}{N-1}$ denotes the average number of vehicles in $\mathcal{V}(c_k)$ that are assigned c_i as a replacement certificate. Similarly, if the misbehaving vehicle revokes t certificates, the expected anonymity level of a vehicle becomes $\frac{N}{N-t}\gamma$ ($> \gamma$). When g certificates are required to be revoked, GRGR scheme replaces them with g new certificates. As each vehicle is assigned a replacement certificate randomly from the g new certificates, the expected anonymity level of a vehicle in GRGR scheme is γ . FSR scheme, which is not included in Table 1, is equivalent to IRR when the parameter p is zero and is equal to GRGR when p is one. For $0 < p < 1$, the anonymity level of FSR is between those of IRR and GRGR; precise analysis for the anonymity level of FSR scheme is extremely complicated and is not known.

6. Conclusion

To design a privacy-preserving vehicular PKI, certificates need to be anonymous. An anonymous certificate does not provide information that adversaries can use to identify the subject of the certificate. However, anonymous certificates may allow a misbehaving vehicle to cause collateral damage for a large group of vehicles. To overcome the unbounded collateral damage of the previous randomized certificate replacement schemes, the proposed scheme makes a misbehaving vehicle belong to a strictly smaller anonymity set whenever it causes a certificate to be revoked. In a large-scale vehicular network, each adversary may revoke multiple certificates simultaneously and moreover multiple concurrent adversaries can work together against the PKI system. We are conducting research toward designing a randomized certificate replacement scheme in these more complex scenarios.

References

- [1] R. Lu, X. Lin, Z. Shi, and X.S. Shen, "A lightweight conditional privacy-preservation protocol for vehicular traffic-monitoring systems," *IEEE Intell. Syst.*, vol.28, no.3, pp.62–65, 2013.
- [2] G. Yan, S. Olariu, J. Wang, and S. Arif, "Towards providing scalable and robust privacy in vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol.25, no.7, pp.1896–1906, 2014.
- [3] L. Delgrossi and T. Zhang, *Vehicle Safety Communications: Protocols, Security, and Privacy*, Wiley, 2012.
- [4] R.G. White, S. Pietrowicz, E. van den Berg, G.D. Crescenzo, D. Mok, R. Ferrer, T. Zhang, and H. Shim, "Privacy and scalability analysis of vehicular combinatorial certificate schemes," *The 6th IEEE Conference on Consumer Communications and Networking Conference (CCNC'09)*, pp.1–5, 2009.
- [5] E. van den Berg, T. Zhang, and S. Pietrowicz, "Blend-In: A privacy-enhancing certificate-selection method for vehicular communication," *IEEE Trans. Veh. Technol.*, vol.58, no.9, pp.5190–5199, 2009.
- [6] S. Tengler, S. Andrews, and R. Heft, "Digital certificate pool," United States Patent no.US 7734050 B2, June 8, 2010.