Verifying Certificate Revocation Status for Short Key Lengths in Vehicle Communication Systems

Eun-Gi Kim
Information and Communication Engineering, Hanbat National University, Daejeon City, Republic of Korea.
egkim@hanbat.ac.kr

Correspondence should be addressed to Eun-Gi Kim : egkim@hanbat.ac.kr

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202404046
Received 08 May 2023; Revised from 26 October 2023; Accepted 15 March 2024.
Available online 05 April 2024.

Abstract – This paper proposes and analyzes a ticket-based OCSP protocol for efficient certificate revocation checking in vehicle communication systems. The IEEE WAVE standard for vehicular networks requires real-time processing of Basic Safety Messages (BSMs) exchanged between vehicles. Traditional OCSP revocation checking can introduce delays. The proposed approach distributes OCSP responses as tickets valid for a road section. Vehicles use shorter keys extracted from the tickets for faster cryptographic processing. Experiments compare processing times for signature generation and verification with different elliptic curves. The results show the proposed technique provides faster revocation checking. This allows time-critical vehicle-to-vehicle message processing at high rates under computational constraints. The ticket-based OCSP mechanism enhances security while meeting real-time requirements in vehicular networks.

Keywords – Certificate, Revocation Status, Short Key, Vehicle Communication, Ticket Based OCSP.

I. INTRODUCTION

With the increasing use of the Internet, individuals and businesses have been able to send and store more personal information and important data online. This has led to increased privacy attacks by hackers and cybercriminals, and security threats have become more serious than ever before. The importance of security has become more and more essential to prevent negative effects such as personal information leakage, financial fraud, and intellectual property rights violations. Individuals should keep their personal information secure online by applying security measures such as secure password use, double authentication, and encrypted network connections [1]. Companies must protect customer data and business secrets from attacks such as hacking, data leakage, and ransomware. The importance of corporate security is also emphasized in financial-related activities such as Internet banking, e-commerce, and online transactions. With the spread of mobile devices and the advent of smart home systems, the security of home networks has also become very important. Therefore, governments and businesses should protect public services and infrastructure by strengthening investment and manpower in cybersecurity, and users should carefully manage the rights setting of smartphone apps and the scope of personal information disclosure on social media. The importance of security is expected to continue to grow, and individuals and businesses must raise security awareness and take continuous protection measures [2].

Public key infrastructure (PKI) refers to an integrated security infrastructure used in public key-based encryption systems. PKI supports public key encryption technology and provides security features such as authentication, key management, encryption, and electronic signature. PKI generates a pair of public keys and private keys, and public keys are publicly available and private keys must be kept confidentially by individuals. In PKI, certificate authority (CA) is responsible for issuing certificates and identifying servers or individuals. A certificate includes public key and identity information, and digital signatures from certification bodies are included to ensure reliability. PKI can guarantee document integrity and denial prevention through digital signature, in which case, it provides reliable signature by signing documents with private keys and verifying them with public keys. PKI provides standards for issuing and managing SSL/TLS certificates for secure website access, and supports security in various applications on the Internet, online transactions, email protection, and VPN connections. PKI is an essential security infrastructure for companies, government agencies, and financial institutions to protect important information and ensure the reliability of electronic services [3, 4, 5].

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are protocols used to provide data security and safety in Internet communication. SSL/TLS encrypts communication between clients and servers and ensures data

integrity and authentication to prevent data tampering or eavesdropping in the middle of the network, and for this purpose, public key encryption and symmetric key encryption are used in combination. After safely exchanging symmetric keys with public key encryption, data is efficiently encrypted using symmetric keys. SSL/TLS supports the HTTPS (HTTP Secure) protocol to enhance the security of websites, which encrypts communication between web browsers and web servers. The server receives a certificate from the CA and provides the certificate to the client during the SSL/TLS connection establishment process, and the client verifies the certificate to verify the server's identity. SSL/TLS supports a variety of encryption protocols and algorithms, and is updated to maintain security if any security vulnerabilities are found in the industry. SSL/TLS provides various security features such as authentication, encryption, and data integrity verification to protect users' personal information and sensitive data, and is used in various Internet services such as online payments, Internet banking, email communication, and virtual private network (VPN), providing a secure online experience to users. SSL/TLS is recognized as an essential component of network security, and both businesses and individuals should properly implement SSL/TLS on their websites and applications to enhance security [6, 7].

Certificate can be revoked due to expiration, leakage of private keys, and reliability problems of certification authorities, and certificate revocation means canceling or discarding the validity of certificate. The revoked certificate is no longer reliable, and encrypted communication using it must be stopped. Certificate revocation is carried out by CA, which uses the revoked Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP), an online status verification protocol. The CRL is a periodically updated list, and the entry allows you to download the CRL in advance to check whether the certificate is discarded. OCSP is a protocol that checks the status of certificates in real time and is used by clients to verify the validity of certificates. Certificate revocation prevents potential security threats arising from the leakage of private keys in certificates and ensures user safety. Web browsers and other client applications must verify the certificate by downloading the CRL or accessing the OCSP responder. Validation of certificates is important to maintain secure communication, and users should carefully perform validation to avoid encrypted communication by unreliable certificates [8, 9].

In this study, we proposed a method of applying the OCSP protocol in an automobile communication system and a method of efficiently authenticating messages through this process and analyzed its performance.

II. PKI AND CERTIFICATE

PKI Structure and Applications

Public Key Infrastructure (PKI) is a security infrastructure based on public key encryption systems that includes digital certificates, public and private keys, certification authorities, and certificate management. This structure is used for secure communication, data protection, and identification, and is utilized in a variety of security applications such as web browsing, email security, and electronic signature [10].

Components of PKI

The PKI components are as follows

Public and private key

In PKI, private key is a secret key for information security and is used to encrypt data and generate digital signatures. The public key is paired with a private key, used for data decryption and digital signature verification, and is publicly shared by others.

Certificate Authority (CA)

The CA is a trusted third-party organization that plays an important role in issuing and managing digital certificates. These certificates are used for public key-based encryption and digital identification, and the CA maintains security by verifying user and server identifications.

Certificate

In PKI, digital certificates include public and private keys, and are reliable documents in digital form to verify the integrity of information and sender identity. This enables secure communication and data exchange, and is issued and managed by the CA.

Certificate chain

In PKI, the certificate chain is a key component of forming a trust scheme and refers to the structure in which multiple certificates are connected. It forms a chain from the root CA to the intermediate CA and the end user's digital certificate, which is verified by the signature of the previous CA at each stage. These chains establish the reliability of digital certificates and ensure the security of data communication.

Fig 1 shows an example of a certificate chain. As shown in the figure, the root CA has its own root certificate, which is self-signed. Root CA uses its own certificate to sign the certificate of B, the sub intermediate CA. Intermediate CA B

uses its own certificate to sign the certificate of entity B. Users who want to verify B's certificate should verify B's certificate using A's public key and B's certificate using root CA's public key.

Certificate Revocation List (CRL)
The CRL is a list used by PKI that is used to track digital certificates that are invalid before expiration. The CRL is periodically updated by the CA to check invalid certificates to prevent security flaws.

PKI Applications
PKI is used to provide security and reliability in a variety of applications. Some major PKI applications include.

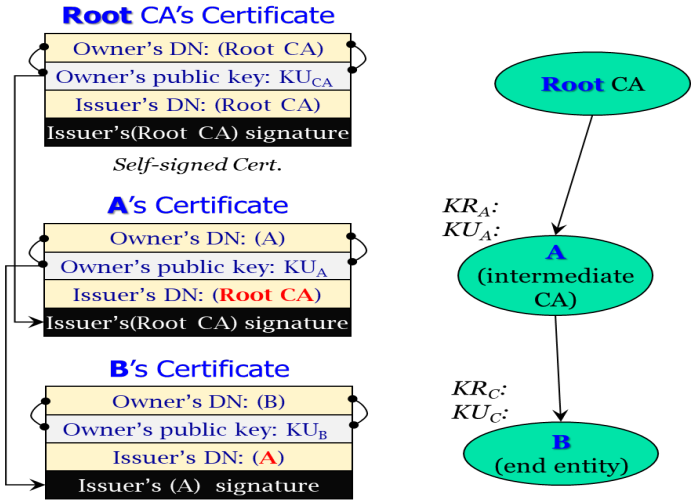


Fig 1. Example of Certificate Chain.

SSL/TLS communications
PKI is used in Secure Socket Layer/Transport Layer Security (SSL/TLS) communication, enabling secure web browsing and data transfer. SSL/TLS protocols utilize public and private keys to identify communication partners and encrypt data to prevent eavesdropping and data tampering, and PKI's CA issues SSL/TLS certificates to ensure website reliability.

Email Protection
PKI can be used for email security. Certificates issued by CAs can be used to ensure the integrity and confidentiality of e-mails. For example, Secure/Multipurpose Internet Mail Extensions (S/MIME) utilizes PKI to encrypt and sign e-mail messages and attachments.

Web authentication and login protection
PKI can be used to enhance user authentication and login security. The user can prove his or her identity using his or her private key and certificate, and the service provider can verify the user's identity through this. This enables secure web application authentication and login.

Virtual Private Network (VPN)
PKI can be used to enhance the security of VPN connections. Communication between VPN clients and servers is protected using public key-based encryption. The client and the server exchange their respective certificates and mutually identify them.

Code Signature
PKI can be used to sign code to verify the integrity and reliability of software or code. Software developers use private keys to sign software or code, and users can use public keys to identify the signed code.

In addition, PKI is used to provide security and reliability in various fields such as IoT (Internet of Things), cloud security, digital copyright management, and electronic signature. PKI is used as a key element for effectively implementing and managing public key-based encryption systems.

X.509 certificate structure
Fig 2 shows the structure of the X.509 certificate [10]. X.509 is a standard certificate format used for authentication in PKI that defines the structure and data format of digital certificates. The main fields of the X.509 certificate are as follows.

Version
Specifies the version of the certificate; the current most common version is X.509v3.

Serial Number
A unique serial number of a certificate that is used to identify the certificate.

Signature Algorithm
A digital signature algorithm used for certificates, typically RSA, DSA, ECDSA, etc.

Issuer
Information on the authority that issued the certificate.

Validity Period
Specifies the validity period of a certificate, consisting of the issuance date and expiration date of the certificate.

Subject
Information on the object (person, organization, etc.) that owns the certificate. The Subject field is primarily used to identify the identity of the user, along with the public key.

Public Key
A public key associated with a certificate. The 'subject' and 'public key' fields on the certificate perform the function of binding the user's public key.

Issuer Signature
The signature of a certificate encrypted with the issuing authority's private key. This signature is used to verify the integrity of the certificate and to prove that it is issued by the issuing authority.

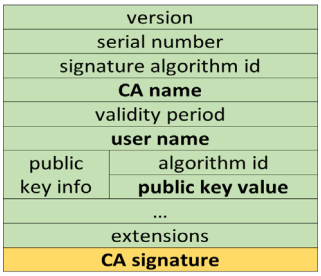


Fig 2. X.509 Certificate Structurex.509 Certificate Structure.

Certificate creation and verification
Fig 3 shows the certificate creation and verification process.

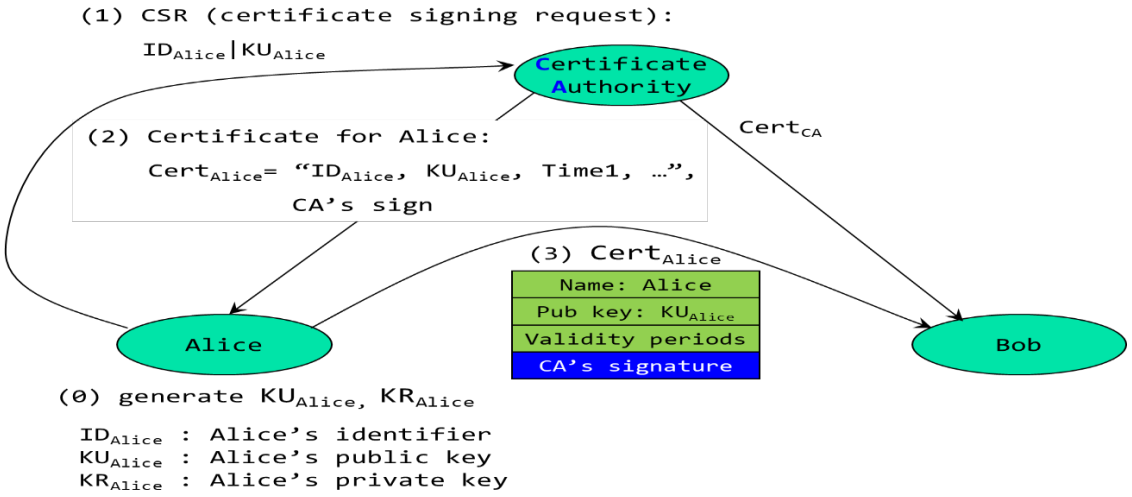


Fig 3. Certificate Creation and Verification.

The certificate generation process is as follows.

Private/public key generation
To generate a certificate, a private key is first generated, and a public key is generated using it.

Certificate signing request (CSR)
Create and deliver CSR to CA to generate certificates. CSR includes the certificate applicant's information and public key.

Certification Authority Review
CA reviews CSR and verifies that it is reliable. In this process, the identity of the requester is verified, and the requester is qualified to obtain a certificate.

Certificate Issuance
After CA reviews the certificate request, issue a new X.509 certificate containing the requester's public key. The certificate contains the signature of the CA, which ensures the integrity of the certificate and provides reliability.

Save Certificates
Certificates are typically stored on the requester's computer or device. Certificates provide public keys and are used to verify the identity of the certificate owner.

The verification process of the X.509 certificate is to verify the validity and reliability of the certificate as follows.

Certificate Acquisition
Certificates are typically provided to clients when HTTPS connections are established on a web server, and the client receives the certificate from the server to initiate verification. (Server Verification)

Certificate parsing
To verify a certificate, the certificate is first parsed to extract the components and information of the certificate.

Certificate chain verification
Most certificates are generated via an intermediate CA under the highest certification authority (Root CA). Therefore, you should check the certificate chain to ensure that it is a certificate signed by a trusted root certificate authority. All certificates in the chain are verified using a trusted certificate store or certificate path algorithm.

Signature verification
The certificate to be verified is signed with the CA's private key, and the verification process uses the CA's public key to verify the signature of the certificate. Signature verification is used to ensure the integrity of the certificate and to verify whether the certificate is tampered with.

Validity check
Certificates include start and end dates, and the verification process checks the validity of the certificate against the current time. Expired certificates cannot be trusted, and verification will fail.

Conformity verification
The conformity verification of a certificate may vary depending on the purpose of use of the certificate. For example, in the case of a web server's certificate, you can check whether it matches the domain name. This will allow you to verify that the certificate is used for the correct server.

Check Certificate Status
Certificates that have not expired may be discarded for some reason. In the process of verifying the certificate, you must go through the process of verifying these revoked certificates.

III. METHODS FOR CERTIFICATE REVOCATION STATUS VERIFICATION

Certificates with remaining validity periods may no longer be usable for a variety of reasons. For example, a certificate may be revoked if the private key is lost or leaked, the identity of the certificate owner has changed, or the certificate is no longer needed. Methods for verifying revoked certificates are as follows.

CRL (Certificate Revocation List)
CRL is issued by a CA and is used to verify the validity of a certificate. The CRL contains a list of revoked certificates. The CRL must be updated whenever a CA revokes a certificate. To achieve this, the CA adds the list of revoked

certificates to the CRL, creates a new CRL, and distributes it. Typically, CRLs are provided on the CA's website or other public means, and verifiers can use these CRLs to check whether a particular certificate has been revoked[11]. After receiving the certificate, the verifier downloads and verifies the CRL of the CA that issued the certificate. The CRL contains information such as the serial number of the revoked certificate and the date and time of revocation. Verifiers can use the CRL to check whether a certificate is valid and to check whether the certificate is included in a list of revoked certificates. If a certificate is listed in a CRL, it is no longer considered trustworthy. CRLs are also signed to prevent forgery and alteration. The CA signs the CRL with its private key to ensure the integrity of the certificate. The verifier can use the CA's public key to check the signature of the CRL and verify that the CRL was properly generated by the CA.

OCSP (Online Certificate Status Protocol)

OCSP is a protocol for checking certificate status in real time, and was developed to overcome the limitations of the CRL method. CRLs have the disadvantage of having to be updated periodically and downloading large lists. In contrast, OCSP can operate efficiently because it can check the status of the certificate in real time. OCSP operates based on the interaction between the client and the CA that issued the certificate [12].

Fig 4 shows the operation of OCSP.

- The client receiving the certificate from the server obtains the OCSP server address of the issuer (i.e., CA) attached to the certificate.
- The client generates an OCSP request and transmits it to the OCSP server (responder). This request includes the serial number of the certificate and other necessary parameters.
- Upon receiving the OCSP request, the OCSP server checks the status of the requested certificate and generates an OCSP response and returns it to the client.
- The client can receive an OCSP response and check the status of the certificate. The response indicates whether the status of the certificate is valid, abolished, or otherwise.
- When the CRL is updated, the CA delivers it to the OCSP server.

The OCSP is efficient because it can check the status of certificates in real time compared to CRL and does not require the need to download a large list of certificates. However, OCSP may have longer response time than CRL because it requires client-server communication.

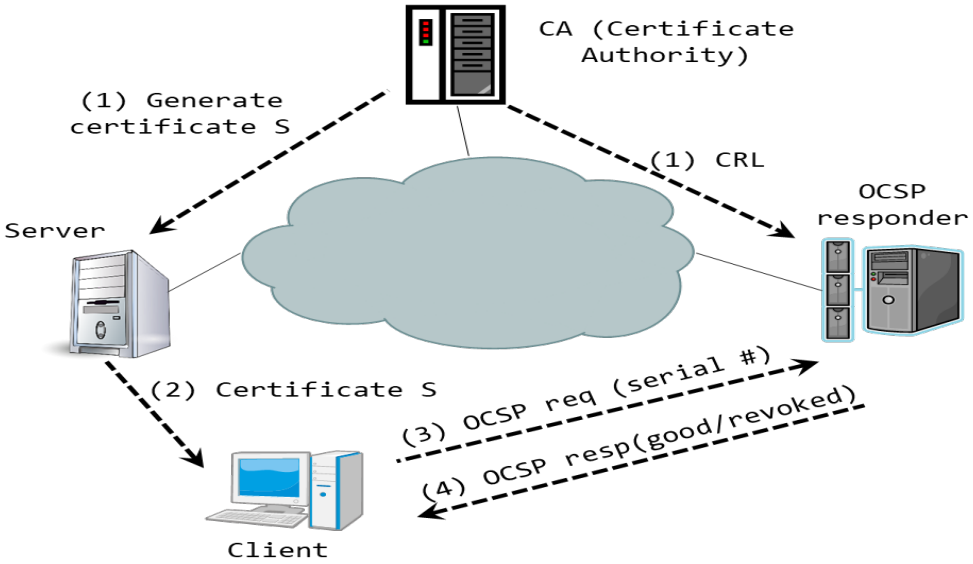


Fig 4. OCSP Operations.

OCSP stapling

OCSP Stapling is a mechanism for quickly checking the status of certificates and operates as part of the OCSP protocol. This method has the advantage of reducing the latency of OCSP requests and responses by providing the status of the certificate directly to the client and enhancing security. In the existing OCSP method, the client must send a request directly to the OCSP server to check the status of the certificate, resulting in additional network round trip delays between the client and the OCSP server. OCSP Stapling is a method in which a web server takes OCSP responses in advance and provides them to clients to address these issues [13]. The server regularly checks the status of the certificate to the OCSP server and caches the verified response. The web server then provides the client with an OCSP response along with the certificate.

The key features of OCSP Stapling include:

Performance improvement

Clients receive OCSP responses directly with certificates from the web server, eliminating additional network round trip delays with the OCSP server, and reducing response time.

Privacy

OCSP Stapling enhances client privacy because clients do not have to connect directly to the OCSP server. The client's IP address or certificate information is not exposed to the OCSP server.

CRLite

CRLite is an efficient method for certificate revocation verification and is a technology jointly developed by Mozilla and Cloudflare. CRLite is used to compress large certificate revocation lists and verify them on the client side. This allows the verifier to efficiently check the status of the certificate and has the advantage of not having to download the entire CRL [14]. The key features of CRLite include:

Centralized Structure

CRLite manages certificate revocation information on a centralized server managed by Mozilla and Cloudflare, and validators can obtain certificate revocation information from one trusted server.

Compressed format

CRLite compresses certificate revocation information and efficiently transmits and stores it. This allows validators to efficiently maintain updates by receiving only small-sized updates instead of downloading the entire CRL list.

Cache-based verification

CRLite uses the local cache to verify the status of the certificate. The validator can periodically update the cache to reduce network delay during the verification process while staying up-to-date.

Here's how CRLite works:

- The CRLite server collects and stores certificate revocation information received from CA in a compressed format.
- The validator periodically downloads small-sized compression updates from the CRLite server to update the local cache.
- After receiving the certificate, the verifier verifies the status of the certificate using the local cache. If the local cache does not contain the certificate or the certificate's status indicates that it is revoked, the verifier may take additional action.

CRLite is much more efficient than downloading the entire CRL. CRL has the problem that the contents of the entire list must be updated periodically and a large list must be downloaded. In contrast, CRLite updates the local cache by downloading only small-sized compressed updates. This helps verifiers maintain up-to-date certificate revocation information with a relatively small amount of data. CRLite is used in the Mozilla Firefox browser and Cloudflare's CDN (Content Delivery Network), and provides real-time certificate revocation information and efficient certificate status verification functions.

IV. TICKET-BASED STAPLED OCSP PROTOCOL FOR VEHICLE COMMUNICATION SYSTEMS

IEEE WAVE (Wireless Access in Vehicular Environments) is a standardized protocol for automotive communication and can be applied to a variety of automotive applications, including autonomous driving, safety communication, entertainment systems, etc.

WAVE uses wireless communication to enable vehicle-to-vehicle communication (V2V), vehicle-to-infrastructure communication (V2I), and vehicle-to-infrastructure communication (V2X). Automotive communication system security supports functions such as confidentiality, integrity, authentication, non-repudiation, and availability.

To support these functions, the IEEE 1609.2 WAVE security standard defines the use of security algorithms such as Electronic Curve Digital Signature Algorithm (ECDSA) and Electronic Curve Integrated Encryption Scheme (ECIES) [15]. Additionally, the IEEE WAVE standard defines BSM (Basic Safety Message) for V2V communication. BSM is designed to use vehicle-to-vehicle communication functions to exchange information about surrounding vehicles and support a variety of safety functions such as collision warning, signal control, and traffic flow management.

BSM messages include vehicle location information, speed and acceleration, direction, vehicle identifier, vehicle status, collision warning, lane information, etc. Cars can interact by communicating BSM messages with surrounding vehicles in real time and share driving situations, reducing the risk of collisions between vehicles and improving safety. For example, if a nearby vehicle suddenly stops, the vehicle that receives the information through the BSM message can take appropriate action.

Fig 5 shows the operation of the existing OCSP stapling method.

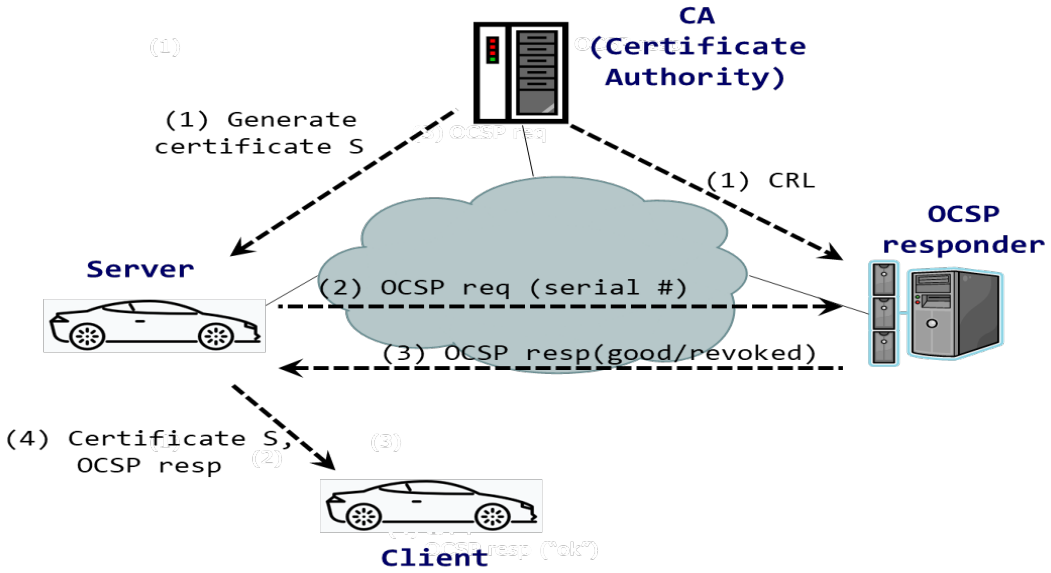


Fig 5. Operation of Traditional OCSP Stapling Method.

In the existing OCSP stapling method, the client receives certificate S and OCSP response from the server and performs the following operations.

- Verify the received server certificate S using the CA's public key
- Verify the received OCSP response message using the OCSP responder's public key
- The public key stored in certificate S is used to verify messages received from the server.

The IEEE WAVE standard defines NIST P-256 and NIST P-384 as the ECC (Elliptic curve cryptography) curve used in this process. The transmission cycle of the BSM message broadcasted from each vehicle may vary depending on the system and operating environment, but is generally known to be 100 msec. Therefore, a running car must be able to process multiple messages sent by cars around it in real time. Therefore, each car must verify dozens of messages per second, and this may be difficult for cars with insufficient processing power. In this study, we proposed a method to solve these problems while applying the OCSP protocol to automobile communication and analyzed its performance.

Fig 6 shows the OCSP operation proposed in this study.

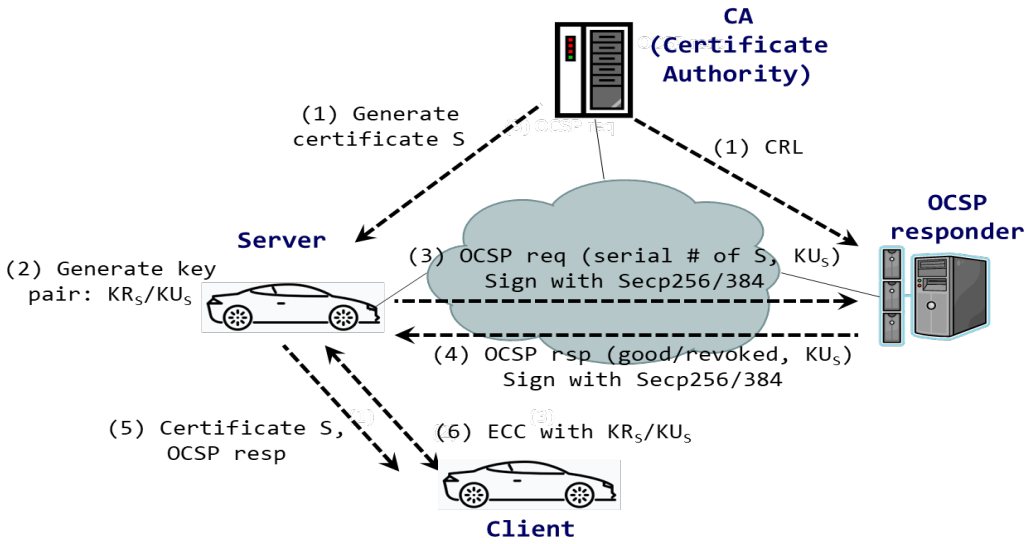


Fig 6. OCSP Operation Proposed in this Study.

In this study, a ticket-based OCSP protocol was proposed to apply the OCSP protocol to automobile communications. The overall operation of the proposed method is as follows.

- OCSP response can be used in a specific section of the road as a ticket.

- The car performing the server role receives a certificate to use from the CA.
- A car that wants to create a ticket generates a public key (KUs) and a private key (KRs) to be used in the section where the ticket is used.
- The server transmits an OCSP request to the OCSP responder at the road entrance of a specific section. The OCSP request transmitted at this time includes the serial number of the certificate S and the generated public key (KUs). The secp256/secp384 curve is used to sign the OCSP request.
- The responder that receives the OCSP request determines whether certificate S is revoked and returns an OCSP response. The OCSP response also includes the KUs sent by the server in the request, along with whether the certificate has been revoked.
- The server operating on a specific section of the road transmits certificate S and OCSP response to the client.
- The OCSP client receives certificate S and OCSP response from the server and performs the following operations.
    - Verify the received server certificate S using the CA's public key
    - Verify the received OCSP response message using the OCSP responder's public key
    - To verify messages received from the server, ECC encryption is performed using the key pair (KRs, KUs) stored in the OCSP response.
- Afterwards, the client and server can quickly perform the encryption operation by performing the encryption operation using a key with a length shorter than scep256/384.

Performance of ticket based stapled OCSP in vehicle communication systems

The ticket-based OCSP method proposed in this study supports signing messages using a shorter key when a car moves in a certain section. In this section, we compared the signature creation and verification time according to various ECC curves. The program for performance analysis was written in C language in OpenSSL 3.1.0 14 to sign and verify 8042 bytes of file data. And, the performance analysis was performed on the Raspberry pi 4 (Broadcom BCM2711, quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz, 4G SDRAM) board.

Fig 7 shows different signature and verification times on various standard ECC curves. It can be seen that the signing and verification time increases as the secret key length increases. As can be seen in the figure, the brainpool series curves [16], secp series curves [17], and prime series curves [18] show similar processing times for similar key lengths. However, as can be seen in **Fig 7 (b)**, prime256v1 shows a shorter processing time compared to curves of other specifications with similar key lengths.

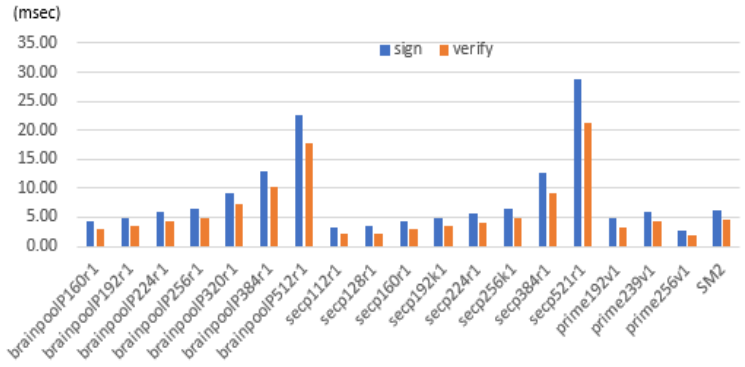
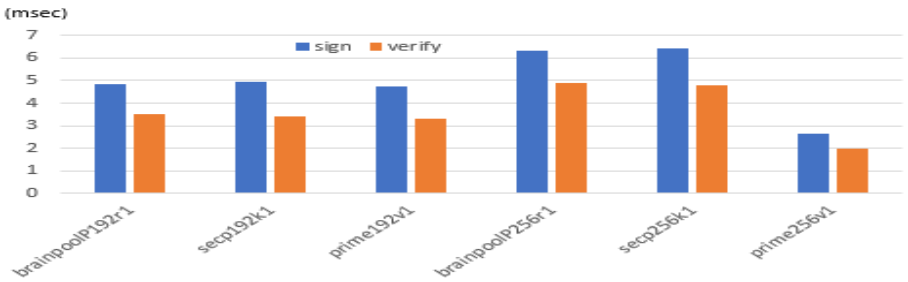


Fig 7a. Signature/Verification Time by Encryption Algorithm



(b) Signature/verification time by key length and encryption algorithm (192/256 bits)

Fig 7. Signature and Verification Time According to Standard ECC Curve.

V. CONCLUSION

In this paper, we propose a method of applying the OCSP stapling protocol for certificate verification in vehicle communication systems. The existing OCSP stapling protocol has advantages in terms of real-time and efficiency in certificate verification, but has a disadvantage in terms of processing delay time in environments where very frequent message exchanges occur, such as automobile communication systems. In this study, a ticket-based OCSP stapling protocol was proposed to overcome this problem. In the proposed method, similar to the existing stapled OCSP protocol, a certificate and OCSP response to be used in a specific section of the road are created in advance and used as a ticket, eliminating the need for vehicles to perform OCSP communication for certificate verification in real time. This allows vehicles to significantly reduce latency due to certificate verification. In addition, this study used tickets to sign and verify messages with short-length keys, allowing vehicles to perform message authentication at a faster rate. In order to check the processing speed when using short-length keys according to the proposed method, the performance improvement effect was confirmed through an experiment implemented in OpenSSL.

This study is significant in that it suggests a method to support fast processing speed of automobile communication systems. However, when applying the actual system, it is necessary to consider issues such as ticket issuance and management, and key replacement. In the future, it is necessary to evaluate the proposed method in more vehicles and various road environments and study considerations when applying it to an actual system. In the future, we plan to use the results of this study to conduct additional research to increase the security, safety, and efficiency of automobile communication systems.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

[1] M. Curry, B. Marshall, R. E. Crossler, and J. Correia, “InfoSec Process Action Model (IPAM),” ACM SIGMIS Database: the DATABASE for Advances in Information Systems, vol. 49, no. SI, pp. 49–66, Apr. 2018, doi: 10.1145/3210530.3210535.

[2] J. Allen, and J. Westby, "Governing for Enterprise Security (GES) Implementation Guide," *Carnegie Mellon University, Software Engineering Institute's Digital Library*. Software Engineering Institute, Technical Note CMU/SEI-2007-TN-020, 1-Aug-2007 [Online]. Available: https://doi.org/10.1184/R1/6574010.v1. [Accessed: 9-Apr-2024].

[3] Fruhlinger Josh, “What is PKI? And how it secures just about everything online,” CSOOnline. 2021 May.

[4] Adams Carlisle and Lloyd Steve, “Understanding PKI: concepts, standards, and deployment considerations,” Addison-Wesley Professional; 2003. p. 11–15. ISBN 978-0-672-32391-1.

[5] Vacca Jhn R., “Public key infrastructure: building trusted applications and Web services,” CRC Press; 2004. p. 8. ISBN 978-0-8493-0822-2.

[6] E Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” Internet Engineering Task Force. 2008 Aug.

[7] Oppliger Rolf, “SSL and TLS: Theory and Practice,” Artech House; 2016. (2nd ed.), p. 13. ISBN 978-1-60807-999-5.

[8] Nikita Korzhitskii and Niklas Carlsson, “Revocation Statuses on the Internet,” Passive and Active Measurement. PAM 2021. LNCS. Vol. 12671, p. 175–191, 2021 Mar, doi: arxiv.org/abs/2102.04288

[9] S. Wazan et al., “On the Validation of Web X.509 Certificates by TLS Interception Products,” IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 227–242, Jan. 2022, doi: 10.1109/tdsc.2020.3000595.

[10] Carlisle Adams and Steve Lloyd, “Understanding PKI - Concepts, Standards, Deployment and Considerations,” Addison Wesley, 2022 (2nd ed.), ISBN 0-672-32391-5

[11] Q. Wang, D. Gao, and D. Chen, “Certificate Revocation Schemes in Vehicular Networks: A Survey,” IEEE Access, vol. 8, pp. 26223–26234, 2020, doi: 10.1109/access.2020.2970460.

[12] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,” RFC 6960, Internet Engineering Task Force, 2013 June

[13] Y. Pettersen, “The Transport Layer Security (TLS) Multiple Certificate Status Request Extension,” RFC 6961, Internet Engineering Task Force, 2013 June.

[14] J. Larisch, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson, “CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers,” 2017 IEEE Symposium on Security and Privacy (SP), May 2017, doi: 10.1109/sp.2017.17.

[15] "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages," in IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013) , vol., no., pp.1-240, 1 March 2016, doi: 10.1109/IEEESTD.2016.7426684.

[16] M. Lochter and J. Merkle, “Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation,” RFC 5639, Internet Engineering Task Force, 2010 Mar.

[17] “SEC 2: Recommended Elliptic Curve Domain Parameters,” Certicom Research, September 20, 2000, Version 1.0.

[18] NIST SP 800-186, “Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters,” 2023 Feb.