Journal of Advances and Scholarly Researches in Allied Education
Vol. 21, Issue No. 7, October-2024, ISSN 2230-7540

DOI: https://doi.org/10.29070/zqq83789

Check for updates

Applications and Implementations of Pairing-Free Directed Signature Techniques in Real-World Scenarios

Sajitha V G [1] * , Dr. Dharmendra Saxena [2]

1. Research Scholar, Department of Mathematics, University of Technology, Jaipur, Rajasthan, India
sajithavg1981@gmail.com ,
2. Professor, Department of Mathematics, University of Technology, Jaipur, Rajasthan, India

Abstract: Vehicular Ad-hoc Networks (VANETs), a type of Internet of Things system, allow groups of cars to communicate with one another and with traffic monitoring devices, improving traffic safety and quality of life. In a VANET, vehicles are used by drivers and the system controller to report not only their own status but also that of the road, traffic, and environment. Since VANET networks are open to the public, there is a significant influx and outflow of automobiles. This feature has led to the emergence of two top-tier requirements for VANET security: first, that systems ensuring message security must be quick, and second, that vehicles in a VANET must be held responsible for the accuracy of the information they provide. This study proposes an efficient pairing-free signature technique for VANETs that protects against signer identity fraud, even in situations of insider attacks, without the need for a tamper-proof device.

Keywords: Internet of Things, signature techniques, VANET systems, cryptographic, Digital signature

---------------------------X---------------------------

INTRODUCTION

A message's most crucial component is the sender's signature. A written signature is typically difficult to forge. Consequently, this is an obvious means of verifying the correspondence. Digital signatures and such alternatives are necessary since physical signatures have no value in electronic transmissions. The methods of message transmission across insecure media have been transformed by public key cryptography, which was discovered in 1976 by W. Diffie and M. Hellman. Even on a public and potentially dangerous network like the Internet, previously unknown people may now conduct safe and honest conversations with one another. Consequently, public key approaches are finding more and more uses in cryptography. One of the most crucial cryptographic tools for implementing different authentication and security measures is digital signature schemes that use public key approaches.

Everybody can check the document's signature using the user's public key, but no one can fake it. This is achieved using a digital signature system, which requires a user to have a public key and a private key that correspond to it. Certain uses of digital signatures, like certification, need this kind of self-verification from an authoritative body. The recipient of a signed communication is often the one who is most affected by its contents. This includes circumstances where a signature is required on a medical record, a tax return, or a personal or corporate transaction.

A wants to sign a message m, but B finds it sensitive, and other users are worried about the message as well. In this case, the signature should be designed in a way that only B can directly check it, and when needed, B can also establish its authenticity to any third party C. Directed signatures describe this type of signature. The signature receiver B in a directed signature scheme is completely free to decide how to verify the signature. Without his assistance, no one can verify the signature's legitimacy.

To guarantee data security in unprotected communication networks, digital signatures are among the most critical technologies. Issues with forgery, denial, impersonation, and tampering can be resolved with its help. Many industries, including smart cities [6], transportation, healthcare, and the power grid, rely on digital signatures because they offer reliable identity identification and data sharing services. The public key of the signer is used to confirm the authenticity of a digital signature in conventional systems. Public keys are private pieces of information that represent users' identities in certain real-world contexts (e.g., hospitals, shopping malls). Patients prefer that only their physicians have access to their medical records, while shoppers prefer that no one else has access to their purchase history. Because of this, public verification of the user's signature is not possible.

LITERATURE REVIEW

Zhou, Lifeng et.al. (2022). Medical sensor nodes are used by health care wireless sensor networks (HWMSNs) to collect patient data that can be transmitted to physicians for diagnosis and treatment. A variety of public-channel attacks could jeopardize health information in HWMSNs. Data breaches involving the private information of patients also happen frequently. Therefore, protecting privacy and promoting safe communication are the main priorities of HWMSNs. Zhan and associates. To solve the aforementioned issues, a pairing-free certificateless aggregate signature (PF-CLAS) technique was suggested. However, our cryptanalysis reveals that the malicious medical sensor node (MSNi) could create a fake signature by substituting its public key in the PF-CLAS scheme. Thus, we devise the enhanced PF-CLAS scheme that may accomplish unforgeability, anonymity, and traceability in order to rectify this security issue. Under the Elliptic Curve Discrete Logarithm assumption, the enhanced PF-CLAS scheme can withstand Type I and Type II assaults since we modified the creation of the partial private key. The suggested method is more suited to HWMSNs settings, since it beats comparable CLAS schemes in performance evaluations.

Yang, Lu et.al. (2019). Storage servers may recover publicly encrypted data using searchable public key encryption without disclosing the original data contents. In encrypted data storage systems, it provides an ideal cryptographic answer for decrypting data. A new cryptographic primitive with significant advantages is certificateless cryptography (CLC). It solves the issues with traditional public key cryptosystems' certificate process and identity-based cryptosystems' key escrow problem. Three CLEKS (certificateless encryption with keyword search) methods were proposed in the literature, all inspired by the attractive aspects of CLC. Nevertheless, due to their reliance on expensive bilinear pairing, none of them are appropriate for devices with constrained computational resources and battery life. Therefore, developing a CLEKS technique independent of bilinear pairing is an intriguing and valuable endeavour. We propose a CLEKS technique in this research that does not rely on bilinear pairing. According to our rigorous proof, the technique successfully prevents adaptive chosen-keyword attacks on keyword ciphertext in the random oracle model, assuming the computational Diffie-Hellman issue is difficult. It outperforms earlier pairing-based CLEKS methods, according to efficiency comparisons and simulations. We also provide a quick overview of three enhancements to the CLEKS scheme that was previously presented.

Kumar, Vivek et.al. **(2022).** Among the other main security services, authentication among the different connecting devices in wireless sensor networks while broadcasting is the most important. For faster consumer monitoring and data privacy in an unsecured sensor network, this authentication during broadcasting services enables numerous mobile end-devices to safely and dynamically transmit messages. In order to alleviate the heavy computational burden, this study presents a new identity-based cryptographic technique that uses ElGmal-elliptic-curve cryptography and digital signatures. The goal is to improve the authentication protocol for secure end-user message distribution. Further, the suggested authentication protocol's performance is improved by reducing the size of the signature and encryption key. With the authentication protocol's safe and quick key management, computational complexity is reduced in the end. The comparison between the handover authentication protocol and authentication systems based on bilinear pairings is borne out by the performance study, which also backs up the assertion made before.

Zhang, Fangguo et.al. (2004). Using bilinear pairing on certain elliptic and hyperelliptic curves, Boneh, Lynn, and Shacham (8) presented a short signature scheme (BLS scheme) in Asiacrypt2001. Many further cryptographic systems were suggested, all of which relied on the BLS signature scheme. A hash function that is specific to BLS short signatures is required (6, 1, 8). This hash function is typically inefficient and based on probability. Unlike BLS, our proposed short signature technique employs ordinary cryptographic hash functions like SHA-1 or MD5 and doesn't require specific hash functions. It is derived from bilinear pairings. Along with being more efficient, the technique needs less pairing operations than BLS. We build a ring signature scheme and a novel delegation mechanism using this signature scheme. For both the novel signature scheme and the ring signature scheme in the random oracle model, we provide precise security proofs.

Salin, Hannes. (2021). This paper provides a comprehensive overview of bilinear maps and their applications in contemporary cryptography, namely the theory behind pairing-based encryption and the mathematical assumptions made to support it. Algebraic structures, elliptic curves and divisor theory form the basis of the theory, which allows for the formal definition of pairings. As an example, we examine the well-known Weil pairing in further detail. Further, we describe pairings in detail and provide numerical examples of the definition of pairing-friendly curves and the operation of various cryptographic algorithms.

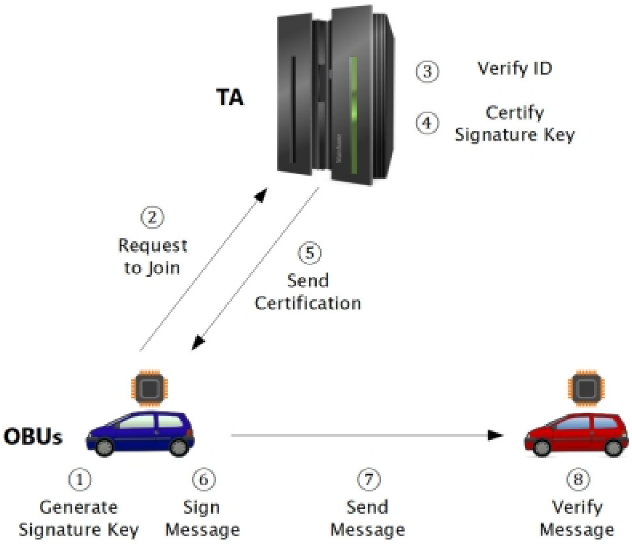
RESEARCH METHODOLOGY

Components

The standard TA-RSU-OBU VANET hierarchy is employed by the suggested design. We will now provide a concise overview of the functions performed by each tier in our system:

1) TA LEVEL

The TA is a state-of-the-art central server that verifies cars seeking to enrol in the system by connecting to official databases. In the event of a disagreement, it is the TA's responsibility to verify the identity of the message signers and validate car keys to prevent vehicles from signing messages under a fake identity. The TA may in fact be composed of several dispersed servers due to practical considerations, but under this theory, they operate as one.



2) RSU LEVEL

In this plan, RSUs are just meant to organise OBUs geographically according to their positions; other than that, they just act as wireless messaging relays between the TA and the vehicles' radio signals.

3) OBU LEVEL

Secure connections with other cars are made possible by OBUs, which are microchips that are put in every vehicle. When cars apply to join the system, OBUs carry the officially-signed certificates needed to authenticate them. In addition to generating and storing keys for message signing, they must communicate with the TA to verify their keys, a prerequisite for creating legitimate signatures.

DATA ANALYSIS

Analysis

Before presenting the suggested strategy, we will thoroughly examine it in relation to the security needs of VANET. Afterwards, we will compare our signature size and performance against other comparable schemes.

Integrity

The suggested method ensures message integrity by feeding the message into the signature hash. If M is changed during transmission, the final signature validation will fail because, when using a cryptographically secure hash function, H(M0 ||T ||B) does not equal H(M||T ||B). A timestamp integrity check is included with the message integrity check to further guarantee that the timestamp cannot be altered without affecting the signature value. This aids in preventing replay attacks.

Authentication

The suggested solution uses TA authentication to stop unauthenticated cars from sending system messages.

Only the TA has the authority to create a valid signature key certification. The public can access GK's value, but in order to obtain x from GK, one must solve the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is expressed as GK = x ∏ P [38]. If a malicious vehicle attempts to create a faked signature key certification, represented as 0 PKi = x 0+a 0H(PKi ‖A 0), the signature validation check will fail.

$$\sigma'_M * P = (\sigma'_{PKi} + y + b * H\ (M|\ |T|\ |B)) * P \qquad (10)$$

where substitution gives:

$$\begin{aligned}
&= ((x' + a' * H(PK_i||A')) + y + b * H(M|\ |T|\ |B)) * P \\
&= (x' + a' * H(PK_i||A') + y + b * H(M|\ |T|\ |B)) * P \\
&= (x' * P + a' * P * H(PK_i||A') + y * P + b * P \\
&\quad *H(M|\ |T|\ |B)) \\
&= GK' + A' * H(PK_i||A') + PK_i + B * H(M||T||B)
\end{aligned}$$

Because GK0, which is determined from the forged signature, does not equal the group public key, GK, the validation will fail.

$$\begin{aligned}
&GK' + A' * H(PK_i||A') + PK_i + B * H(M||T||B) \\
&\qquad \neq GK + A' * H\left(PK_i||A'\right) + PK_i + B * H(M||T||B)
\end{aligned}$$

PRIVACY

The suggested approach protects the privacy of car owners by masking their real-life identities. The TA is the only one who can access the car registration information, and each vehicle in the group is identifiable by its signature key. Due of the random number generator used to produce signature keys, which has nothing to do with the vehicle's identification, no vehicle or RSU can link a signature key to the car's registration information.

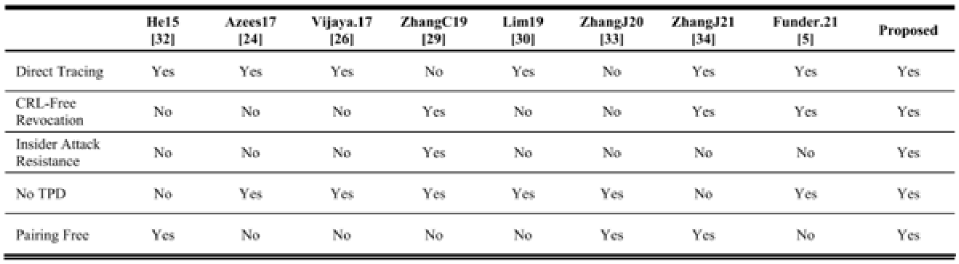
TRACING

Even though no one else can see a car's identification, the TA can easily find out who is behind any suspicious or criminally behaving vehicle according to the planned method. An association between signature keys and car registration data is saved in the TA. In an emergency, this facilitates a simple retrieval of registration details. Toll road charge collecting and vehicle insurance billing are two further examples of services that might benefit from such look-ups.

NON-REPUDIATION

No vehicle may use a signature key that the TA is not aware of or falsify a certification using the recommended method, which is illustrated in section 2 "Authentication.". More significantly, no vehicle can ever "steal" the signature key from another vehicle.

Table 1: NON-REPUDIATION



	He15 [32]	Azees17 [24]	Vijaya.17 [26]	ZhangC19 [29]	Lim19 [30]	ZhangJ20 [33]	ZhangJ21 [34]	Funder.21 [5]	Proposed
Direct Tracing	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
CRL-Free Revocation	No	No	No	Yes	No	No	Yes	Yes	Yes
Insider Attack Resistance	No	No	No	Yes	No	No	No	No	Yes
No TPD	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Pairing Free	Yes	No	No	No	No	Yes	Yes	No	Yes

while launching an impersonation assault. Not only does a car convey the message M, but it also sends FM, PKi, T, A, and B. The only person who knows the values of σPKi, y, and b is the one who signs the message. You need to solve the ECDLP in order to get the values of y and b from PKi or B. Furthermore, since FM cannot be used to derive FPKi, it remains unknown, as neither y nor b are known. As a result, it is evident that the vehicle will fail if it tries to create a signature using a stolen PKi with randomly assigned values for σPKi and y, where $\sigma0\ M = \sigma0\ PKi + y0 + b0 \prod H(M||T\ ||B\ 0\ )$.

$\sigma\ 0\ M * P = (\sigma\ 0\ PKi + y\ 0 + b\ 0 * H\ M|\ |T\ |\ |B\ 0\ \ ) * P\ (11$

where distribution gives

$= \sigma\ 0\ PKi * P + y\ 0 * P + b\ 0 * P * H(M|\ |T\ |\ |B\ 0$

$= \sigma\ 0\ PKi * P + PK0\ i + B\ 0 * H(M|\ |T\ |\ |B\ 0$

And it can be seen that

$\sigma\ 0\ PKi * P + PK0\ i + B\ 0 * H\ M\ ||T\ ||\ B\ 0$

$6 = GK + A * H\ (PKi\ ||A) + PKi + B\ 0 * H(M||T\ ||B\ 0$

A vehicle cannot claim that their public key was used fraudulently to sign a message in their name since a valid signature can only be generated with knowledge of the corresponding values of σPKi, y, and PKi.

Insider attack resistance

Lastly, the suggested method can withstand insider assaults from other vehicles (as mentioned in sections 2 and 5 of the "Authentications" and "non-repudiation" sections, respectively), as well as the theft of essential material held on the TA. In a lot of VANET setups, the TA is completely reliable as they make or have direct access to all the cars' private keys. Because of the weak security measures, these techniques are susceptible to insider assaults.

While the TA can successfully certify a vehicle's public key as a signature key under the current method, it is unable to do so in the absence of the private key for the vehicle. Thus, not even with the TA's help can vehicles launch a masquerade assault on other vehicles. The signature validation check will fail if a compromised TA or malicious vehicle tries to create a signature without the private key y that matches the signature key that was certified, so that $\sigma\ 0\ M = \sigma PKi + y\ 0 + b * H(M||T\ ||B)$.

$\sigma 0 M * P = (\sigma PKi + y 0 + b * H(M\|T \|B)) * P$

where substitution give

$$\begin{aligned}
&= ((x + a * H(PK_i||A)) + y' + b * H(M||T||B)) * P \\
&= (x + a * H(PK_i||A) + y' + b * H(M||T||B)) * P \\
&= (x * P + a * P * H(PK_i||A) + y' * P + b * P \\
&\quad *H(M||T||B)) \\
&= GK + A * H(PK_i||A) + PK_i' + B * H(M||T||B)
\end{aligned}$$

Even though it's not easy to seize control of a TA, it would be an attractive target for key theft if the TA had the private keys of every vehicle in a VANET. A poorly protected key database might provide cybercriminals access to a large number of compromised keys, allowing them to launch widespread assaults against non-repudiation or Sybil. Under the proposed system, each car would have its own private key. Even if the TA verifies the signature keys, it has to solve the ECDLP before it can get the private keys for the cars. Because of this, the proposed system is much safer than many other VANET schemes that use fully-trusted TA.

CONCLUSION

Using elliptic curves without pairings, this work presents a system for authenticating and signing messages sent within a VANET group. Cars entering a VANET group's service area must first get in touch with a TA in order to sign messages inside the group. The TA will then certify the vehicle's signature key after confirming the vehicle's identity. In the event that a vehicle misbehaves, for example, by giving erroneous location or traffic information, the group keys can be changed to remove the vehicle's ability to sign messages for the group.

Given the need to connect locations and make predictions for VANET anti-collision algorithms, future studies should think about how to protect drivers' privacy while avoiding vehicle monitoring. To avoid message linkage caused by reused signature keys, the suggested technique should be revised in the case that future anti-collision algorithms are able to operate independently of vehicle position monitoring. Furthermore, future schemes should take into account the likelihood of a malevolent TA incorrectly delivering keys to unauthorised cars, even if this system handles the most probable sort of insider attack at the TA level.

References

1. Zhou, Lifeng & Yin, Xinchun. (2022). An improved pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks. PLOS ONE. 17. e0268484. 10.1371/journal.pone.0268484.

2. Yang, Lu & Li, Ji-guo. (2019). Constructing pairing-free certificateless public key encryption with keyword search. Frontiers of Information Technology & Electronic Engineering. 20. 1049-1060. 10.1631/FITEE.1700534.

3. Kumar, Vivek & Ray, Sangram & Sadhukhan, Dipanwita & Karmakar, Jayashree & Dasgupta, Mou. (2022). Enhanced pairing-free identity-based broadcast authentication protocol in WSN using ElGamal ECC. SECURITY AND PRIVACY. 10.1002/spy2.278.

4. Zhang, Fangguo & Safavi-Naini, Reihaneh & Susilo, Willy. (2004). An Efficient Signature Scheme from Bilinear Pairings and Its Applications. 277-290. 10.1007/978-3-540-24632-9_20.

5. Salin, Hannes. (2021). Pairing-Based Cryptography in Theory and Practice.

6. Shams. I. Ben, 2007, "Signature Recognition by Segmentation and Regular Line Detection", In Proceedings of Tencon-2007 IEEE Region 10 Conference, pp. 1-4.

7. Porwik P., 2007, "The compact three stages method of the signature recognition", In Proceedings of the 6th International Conference on Computer Information Systems and Industrial Management Applications, pp. 282 – 287.

8. E. Özgündüz, T. Şentürk, M. Karslıgil, Off-Line Signature Verification and Recognition by Support Vector Machine. EUSIPCO, 2005.

9. Bhattacharyya D., Bandyopadhyay S., Das P., Ganguly D., Mukherjee S., 2008, "Statistical Approach for Offline Handwritten Signature Verification", Journal of Computer Science, 4 (3), pp. 181-185.

10. Madasu VK., Lovell B., Kubik K., 2005, "Automatic Handwritten Signature Verification system for Australian Passports". In Proceedings of Science, Engineering and Technology Summit on Counter-Terrorism Technology, pp. 53-66.

11. Majhi B., Reddy Y. , Babu D., 2006, "Novel Features for Off-line Signature Verification, International", Journal of Computers, Communications and Control , 1(1), pp. 17-24

12. Toscano-Medina K., Sanchez-Perez G., Nakano-Miyatake M., and PerezMeana H., 2001, "On-line signature recognition using feature extraction and multilayer neural networks". Telecom- munications and radio engineering c/c of elektrosviaz' and radio tekhnika, 56(1), pp.58-70.

13. McCabe A., Trevathan J., Read W., 2008, "Neural network-based handwritten signature verification", Journal of Computers, 3(8), pp.9-22.

14. Mautner P., Rohlik O., Matousek V., Kempf J., 2002, "Signature verification using art-2 neural network". In Proceedings of the 9th International Conference on Neural Information Processing.

15. Horvath A., Kovari B., 2010, "Usability of neural networks in off-line signature verification", In Proceedings of 10th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics.