Journal of
Cybersecurity
and Privacy

MDPI

Article

A Gap Analysis of the Adoption Maturity of Certificateless Cryptography in Cooperative Intelligent Transportation Systems

Hannes Salin [1],* and Martin Lundgren [2]

[1] School of Information and Engineering, Dalarna University, Röda Vägen 3, SE-781 70 Borlänge, Sweden
[2] School of Informatics, University of Skövde, SE-541 31 Skövde, Sweden; martin.lundgren@his.se
* Correspondence: hasa@du.se

Abstract: Cooperative Intelligent Transport Systems (C-ITSs) are an important development for society. C-ITSs enhance road safety, improve traffic efficiency, and promote sustainable transportation through interconnected and intelligent communication between vehicles, infrastructure, and traffic-management systems. Many real-world implementations still consider traditional Public Key Infrastructures (PKI) as the underlying trust model and security control. However, there are challenges with the PKI-based security control from a scalability and revocation perspective. Lately, certificateless cryptography has gained research attention, also in conjunction with C-ITSs, making it a new type of security control to be considered. In this study, we use certificateless cryptography as a candidate to investigate factors affecting decisions (not) to adopt new types of security controls, and study its current gaps, key challenges and possible enablers which can influence the industry. We provide a qualitative study with industry specialists in C-ITSs, combined with a literature analysis of the current state of research in certificateless cryptographic in C-ITS. It was found that only 53% of the current certificateless cryptography literature for C-ITSs in 2022–2023 provide laboratory testing of the protocols, and 0% have testing in real-world settings. However, the trend of research output in the field has been increasing linearly since 2016 with more than eight times as many articles in 2022 compared to 2016. Based on our analysis, using a five-phased Innovation-Decision Model, we found that key reasons affecting adoption are: availability of proof-of-concepts, knowledge beyond current best practices, and a strong buy-in from both stakeholders and standardization bodies.

Keywords: C-ITS; certificateless cryptography; crypto-readiness

Citation: Salin, H.; Lundgren, M. A Gap Analysis of the Adoption Maturity of Certificateless Cryptography in Cooperative Intelligent Transportation Systems. *J. Cybersecur. Priv.* **2023**, *3*, 591–609. https://doi.org/10.3390/jcp3030028

Academic Editors: Ki-Hyun Jung and Luis Javier García Villalba

Received: 29 June 2023
Revised: 1 August 2023
Accepted: 11 August 2023
Published: 1 September 2023

1. Introduction

Information security plays an increasingly important role for organizations' operation and development. The car industry, the context in which this study takes place, is no exception. Development of connected cars, autonomous driving, and cooperative intelligent transport systems are but some recent examples of technologies whose operation rely on continuous information sharing, and security from theft and wrongful manipulation [1]. Information security management is the practice of providing confidentiality, integrity, and availability (or the CIA triad) to information and information systems in a systematic way by identifying, selecting, and introducing security controls [2,3]. These security controls can be "any process, policy, procedure, guideline, practice or organizational structure, which can be administrative, technical, management, or legal in nature which modify information security risk" ([4], p. 2). Security controls are typically identified and selected as a result of a risk assessment, often requiring a broad set of skills and know-how [5–7], as it aims to maximize resource allocation as well as benefit the security controls offered in assisting (rather than burdening) organizational operation and development [8]. However, adoption of new security controls often means changes to the organization's environment, which is not always perceived as useful, depending on the organization's change-readiness [9].

While perceived usefulness and adoption of security controls have been addressed in numerous studies (e.g., [8,10–12]) and have been described as a fertile ground for additional research [13], the focus has mainly been on the change recipients. That is to say, the end-user of the security controls, such as employees within the organization who are affected by the controls in their day-to-day work. Considering that many incidents, malicious or otherwise, have been reported to be directly (or indirectly) the result of end-users' avoidance or ignorance of security controls [8], it has made sense to study factors affecting change-readiness among recipients, to better cope with advances in security controls. However, less attention has been paid to the affective factors among the change agents. That is to say, those responsible for selecting and implementing the security controls in the first place [14]. Especially when considering new, or innovative, types of security controls based on technology that is not (yet) considered common practice. This presents a gap in the literature on information security management, and to an extent, risk management.

In addressing this gap, this study draws on Technology Readiness Levels [15] and an Innovation-Decision Model [16] to study the cognitive and affective factors when considering new security controls in relation to the controls' technological maturity. While security controls may refer to a wide array of proactive and reactive initiatives, in this study, the focus is on cryptography—and in particular, public-key-based cryptography. The reason for picking such a relatively narrow type of security control is twofold. First, cryptography is a mature and widely applied security control with well-defined best practices and standards [17]. One such example is Public-Key Infrastructure (PKI), which is a common framework to govern and issue cryptographic keys as digital certificates. Second, cryptography is, at the same time, under constant development with new innovations to be considered. One such example is the development of certificateless public key cryptography—as an alternative to PKI—which has shown to be advantageous in some instances, such as privacy and latency [18]. Because of this duality, public-key-based cryptography serves as a good candidate to study attitudes and interventions regarding adoption of new (cryptographic) security controls. The car industry is a relevant setting to examine change-readiness, as recent developments—such as in cooperative intelligent transport systems—face new operational security challenges that rely heavily on secure and private communication with low latency. Moreover, road infrastructure stakeholders are also important in this setting due to their natural connection and collaboration with the car industry.

The contribution of this study is therefore twofold. First, this study provides an overview of the current development in certificateless cryptography within intelligent transport systems, and analyzes it based on the Technology Readiness Levels. Second, building upon this insight, the study furthers the research on security management, and security control identification and selection by studying affecting factors among decision makers when deciding on new, innovative security controls.

The remainder of this study is organized as follows. Section 2 discusses current cryptographic systems in Intelligent Transport Systems, while Section 3 presents certificateless cryptography and how it has been applied to Intelligent Transport Systems. In Sections 4 and 5, the Innovation-Decision Model and Technology Readiness are presented, respectively. Section 6 presents the research approach and how Technology Readiness has been used to investigate the maturity in certificateless cryptography, based on reviewing the existing literature, and how the Innovation-Decision Model was used as a lens to study cognitive and affective factors when considering certificateless cryptography as a security control in relation to its technological maturity. This is followed by Section 7, which present the empirical results from the literature review and interviews. Finally, Section 8 discusses the result while the conclusion, under Section 9, highlights the study's findings and implications.

2. Cryptographic Systems in Intelligent Transport Systems

Decades of research in cooperative intelligent transport systems (C-ITSs) still has not fully harmonized technical solutions for certain security-related challenges. One such challenge is how to setup and manage secret keys used within the eco-system of stationary and moving nodes in a C-ITS system. Different pilots and proof-of-concept projects such as Nordic Way [19] and C-ROADS [20] have chosen to implement traditional PKI architectures. This approach is also chosen for the railway side of C-ITS, where the European Rail Traffic Management System (ERTMS) is one of the major initiatives using PKI [21]. Additionally, the European Telecommunications Standards Institute (ETSI) has drafted a set of technical standardization documents detailing PKI-based solutions for vehicle C-ITS systems [22]. Although PKI is a solid architecture from many perspectives, the deployment of such a solution has some drawbacks if the architecture scales rapidly and there are large volumes of dynamically used key-pairs; the scalability and revocation challenges are still prevalent in the C-ITS domain [23]. For an eco-system that needs to issue, manage, and revoke hundreds or even thousands of new key-pairs every hour, e.g., an inner-city cross-road area during rush hour, a C-ITS system must be both computationally efficient and reliable. Also, for cross-border scenarios where a set of secret keys for a vehicle are issued in one domain or country, the approaching domain needs a way to handle those keys securely, both for verification and revocation.

Security within C-ITSs, often associated with Vehicular Ad-Hoc Networks (VANET) and Vehicle-To-Anything (V2X) communication, is still an emerging area with needs for standardization and harmonization, even enforced in the European Union via EU directives [24]. In the eco-system of vehicles and infrastructure, several technology stacks must be considered. For example, the usage of 5G and cellular technology, but also short-range communication using IEEE 1609.x and IEEE 802.11p standards [25,26], e.g., the WAVE stack. Moreover, different layers of these protocols must also be considered from a cryptographic perspective. For example, design choices needs to be made if a certain signature functionality should be available on the application layer or incorporated closer to the physical layers for speed, security and performance. Several initiatives and projects towards cybersecurity within these areas are ongoing, e.g., the U.S. Department of Transportation's Intelligent Transportation Systems Joint Program Office has several projects [27], and the European Telecommunications Standards Institute (ETSI) has several ITS security standardizations ongoing, particularly regarding privacy and trust model architecture [22].

3. Certificateless Cryptography

Certificate-based cryptography, also known as Public Key Infrastructure (PKI) cryptography, is a method of secure communication that uses digital certificates to establish trust between parties. It is based on the concept of public key cryptography, in which each user has a public key and a private key. These are used for data encryption and signatures. A digital certificate is a digital document that contains a user's public key and a set of identifying information, such as the user's name, address, and other identifying information. The certificate is signed by a trusted third party known as a certificate authority (CA), who attests to the authenticity of the public key and the identity of the user.

Certificateless cryptography (CLC) or certicateless public key cryptography (CL-PKC) is an alternative method of secure communication that does not rely on digital certificates. One of the main differences between certificate-based and CL-PKC is the way trust is established between parties. In a typical PKI, trust is established through the use of the CA who verifies the identity of users and attests to the authenticity of their public keys; thus, being able to issue the certificates. In CL-PKC, trust is established through the use of mathematical algorithms and protocols that eliminate the need for a trusted third party.

The notion of CL-PKC was first discussed by Al-Riyami and Paterson [18]. Primarily, CL-PKC is used for authentication and key agreement protocols and it eliminates the key escrow problem (KEP), as well as challenges with certificate management such as scalability and revocation. In a CL-PKC system, the *Key Generation Center* (KGC) is the node that generates a user's public and private keys partially, which the user then uses to complete the key-pair generation. The user typically seeds the KGC with some secret value or identity string, then called Identity-Based Cryptography (IBC), for further partial key generation. For this reason, the KGC will not contain any of the final keys and, thus, no certificates are needed as in traditional PKI. A conceptual depiction of a CL-PKC is provided in Figure 1.

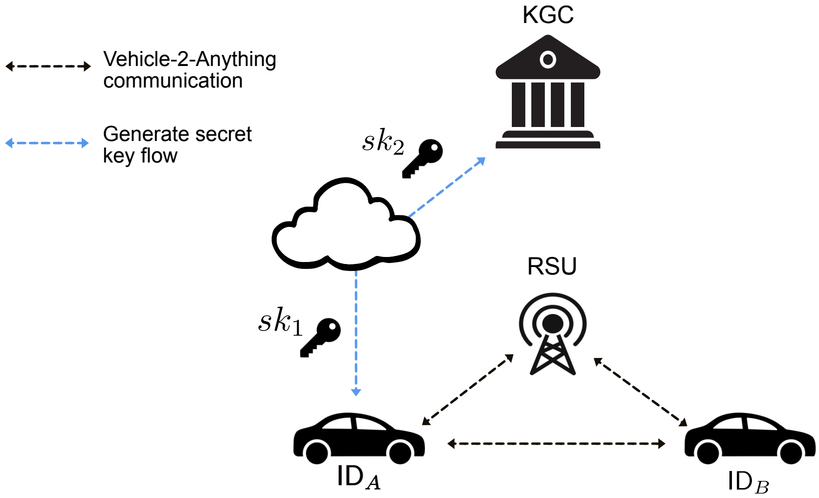

Figure 1. Conceptual system architecture of a CL-PKC setup with a KGC and two users ID_A and ID_B. To generate a secret key, the user needs to make a collaborative computation with the KGC, i.e., generating and combining sk_1 and sk_2.

The KEP refers to a situation where a trusted third party, known as the key escrow agent, has access to the private keys of the users in a cryptographic system. This creates potential security and privacy concerns, as the key escrow agent can potentially decrypt or forge messages, making users vulnerable to unauthorized access [18]. In a traditional PKI, the KEP is not inherent, as users generate their own private keys. However, PKIs rely on certificates to bind public keys to user identities, which can be cumbersome to manage and validate. While IBC simplifies key management by eliminating the need for certificates, it introduces the KEP as the trusted authority has access to all users' private keys. CL-PKC combines the benefits of both PKI and IBC while eliminating the KEP by separating the key generation process between the user and the KGC. At the same time, CL-PKC avoids the complexity of certificate management in traditional PKI systems, offering a more efficient and secure solution for key management and authentication in cryptographic protocols.

In certificate-based cryptography, a malicious third party can impersonate the CA and issue fake certificates, allowing them to intercept and read encrypted messages (e.g., DigiNotar [28]), whereas in CL-PKC, there is no central authority that can be impersonated, making it more difficult for an attacker to intercept and read encrypted messages. Additionally, CL-PKC is more efficient in terms of computation and communication, as it does not involve certificate management and certificate revocation. Hence, it reduces the computational and communication overhead and makes it suitable also for environments with low-powered IoT devices [29]. There is no standard security requirement notion for C-ITS and VANET in the academic literature; however, we have identified a set of commonly frequent categorizations based on the work in [30–32]. Naturally, the CIA triad is a basis, i.e., a security model that emphasizes confidentiality, integrity, and availability of data. Specific attack types for C-ITS relates to tracability, pseduonimzation and unlinkability; all referring to protect the privacy and integrity of participating vehicles.

4. Innovation-Decision Model

The adoption process of innovations (such as identifying, choosing, and implementing one security control over another, like CL-PKC over traditional PKI) can be described as proposed by the five-phased Innovation-Decision Model [16]. This model can help shed light upon what stage and under what conditions an innovation was first discovered by an individual (e.g., a decision maker on security controls), and how decisions to either adopt or reject that innovation was made, as well as potential reinforcements of that decision. Note that innovation with regard to the Innovation-Decision Model does not necessarily mean a new invention. Indeed, the innovation might have been known for many years. Rather, it refers to a technology, process, method, etc., that is previously unknown to a particular individual (read 'decision maker'). This individual can, faced with this innovation and in contrast to current best-practices, norms, and knowledge, decide to either adopt or reject this (new) solution [33]. The Innovation-Decision Model five phases are: knowledge, persuasion, decision, implementation, and confirmation. Each one of these phases is depicted in Figure 2 and further described below.

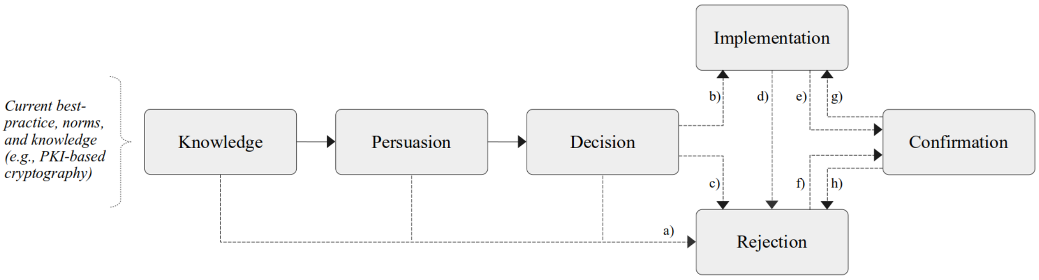

Figure 2. The Innovation-Decision Model with its five phases, adapted based on Rogers [16].

Knowledge —This phase of the model occurs when an individual first learns about the existence of an innovation (e.g., an idea, method, or practice) [16]. Some limited understanding of how the innovation works is gained in this phase which can be divided into three knowledge types. First, the innovation must not be new per se; it can have been invented a long time ago, but is perceived as new to the individual. This type of knowledge is known as 'awareness-knowledge', and can motivate individuals to learn more about the innovation [33]. For example, by gaining 'how-to-knowledge'—which is the next knowledge type—in which additional practical knowledge is sought to better understand the innovation and its uses. Last is 'principles-knowledge', where the individual not only knows how an innovation works, but also why it works, which increases the chances of effective use and adoption [33].

Persuasion—At the persuasion phase, the individual forms a favorable or unfavorable attitude towards the innovation [16]. That is to say, knowing how and why an innovation work does not necessarily mean an individual will or will not adopt it. Other, external, and more feeling-centered factors may affect the decision [33]. For example, social influences from peers and colleagues can affect the attitude towards and opinion about the innovation. The persuasion phase follows the knowledge phase, as individuals shape their attitude towards the innovation after they know about it [33].

Decision—The decision phase is where the individual engages in activities that lead to a decision being made on whether to adopt or reject the innovation [16]. While the decision to adopt or reject the innovation can be made at any point in the innovation-decision process (see step 'a' in Figure 2), this phase also captures two types of rejection as being either active or passive [33]. An active rejection means the individual has tried the innovation and considered adopting it but later decides not to (see step 'b' and 'd' in Figure 2), while a passive rejection means the individual never considered adopting the innovation in the first place (see step 'c' in Figure 2) [33].

Implementation—If the innovation is decided for adoption, this phase captures the innovation put into practice and the potential consequences thereof (see step 'b' in Figure 2) [16,33].

Confirmation—The last step of the process is the confirmation phase, in which the individual seeks reinforcement of an adoption or rejection decision already made [16].

The decision to adopt or reject may be reversed at this point if the individual is exposed to conflicting messages about the innovation (i.e., combinations between the steps 'e' or 'f' and 'g' or 'h' in Figure 2) [16]. Rejection at this point may also be the result of either having identified an even better innovation to adopt instead, or if the implementation was not performing satisfactorily [33].

5. Technology Readiness

In order to generate a gap analysis with a focus on measuring the technological readiness of CLC and CL-PKC, for the C-ITS domain specifically, a technology readiness framework is needed. Several frameworks for technology readiness have been used in previous research and in industry, e.g., the well-known *Technology Readiness Levels* (TRL) developed by the National Aeronautics and Space Administration (NASA) [15]. Several other types of different frameworks can be used to measure an organization's readiness to adopt a new technology, with different perspectives; the Technology Readiness Index (TRI) measures an organization's readiness to adopt new technology by assessing its technological infrastructure, human resources, and organizational culture [34], or the Technology Acceptance Model (TAM) assess the attitudes and perceptions of an organization's members towards the technology [35]. The TAM framework evaluates an organization's perceptions of the technology's ease of use and usefulness, and how these perceptions influence its adoption. No cryptography readiness frameworks, aimed for C-ITSs or similar domains, exists. However, due to the increasing interest in quantum computing, several frameworks and readiness strategies for adopting post-quantum secure cryptography have been proposed [36,37].

6. Research Approach

Our conducted research consisted of four primary phases: literature analysis, technology readiness assessment, interview phase and final analysis. The literature analysis provided necessary data from academic literature which was used in the second phase, where an initial technology readiness assessment was conducted in order to construct a relevant interview scheme for the subsequent phase. The goal with the interview phase was both to measure the technology readiness assessment with the industry, and to triangulate further what missing components there may be for CLC in C-ITS to have a stronger adoption. Finally, the analysis phase concludes the gap analysis in total. We consider parameters such as technology readiness level, theoretical differences in cryptographic properties, and trends of the academic literature development in the field. A complete overview of the chosed research approach is shown in Figure 3.

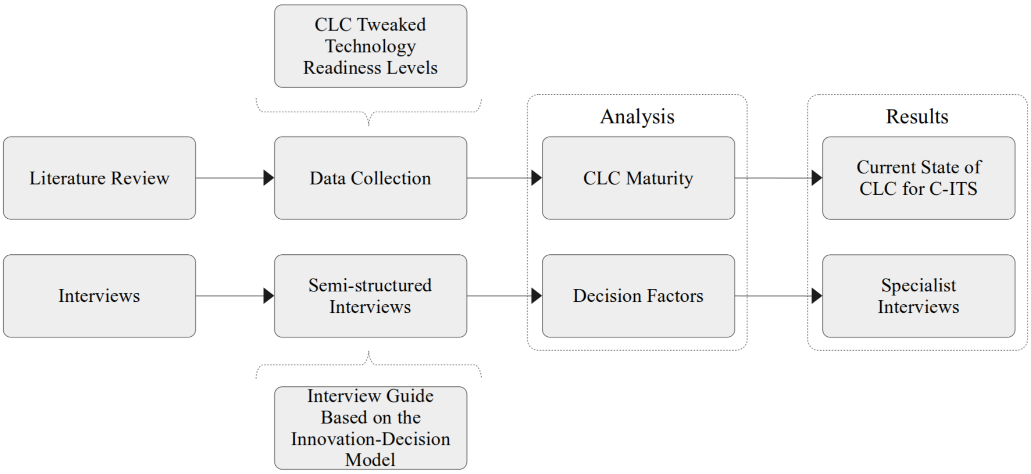
CLC Tweaked Technology Readiness Levels
Analysis
Results
Literature Review
Data Collection
CLC Maturity
Current State of CLC for C-ITS
Interviews
Semi-structured Interviews
Decision Factors
Specialist Interviews
Interview Guide Based on the Innovation-Decision Model

Figure 3. An overview of the research approach.

6.1. Literature Analysis

The review process was modeled after Levy and Ellis's approach [38] and consisted of two consecutive activities: gathering articles and extracting relevant information, followed by analyzing and presenting the findings. IEEE Xplore, ACM Digital Library, and Google Scholar were used to gather articles, with a search strategy that combined the terms "Certificateless", "CLC", "VANET", "Vehicular", "V2X", "C-ITS". The set of articles was then narrowed down into categories based on the search strings "Authentication", "Aggregated signatures", "Key agreement" and "Signcryption". To determine inclusion, the article titles and abstracts were examined. Also, in parallel to the search phase, we collected surveys and literature reviews into a separate set, from which we snowballed articles that was in scope with the inclusion criteria. Only English-language articles that addressed aspects falling within the definition of CLC in C-ITSs were kept. Moreover, we only considered articles published in the time frame of 2022–2023 to limit the scope into a more current view of the topics. However, we provide a lightweight analysis on articles between 2016–2023 to understand trends in the research area over time. The remaining articles were then divided among the authors and processed as follows:

1. Each article was scored with CLC technical readiness level points (CLC-TRL) using the proposed translation table found in Table 1.
2. The aggregated scoring of CLC-TRL for each specified sub-field in CLC was computed where the final score was a majority scoring, i.e., if the majority of the articles had score n, that would be the final scoring.
3. Each author processed step 1 and step 2 independently, then cross-checked the results and summarized the final CLC-TRL assessment.

Table 1. Translation table of NASA TRL into corresponding CLC in C-ITS levels.

NASA TRL	CLC in C-ITS Translation: CLC TRL
TRL 1: basic principles	Only theoretical work is proposed, very few papers in the field.
TRL 2: technology concept	Theoretical work combined with comparative analysis with other technologies are given.
TRL 3: first experiments	There are several proof-of-concepts in at least a laboratory environment or simulations.
TRL 4: validation in lab	There are several proof-of-concepts using corresponding or similar C-ITS equipment, but not used in real infrastructure.
TRL 5: validation on site	Proof-of-concepts exists where the technology is tested in real C-ITS equipment in study- or pre-pilot sites.
TRL 6: component validation	Protocols are implemented and partially tested at real pilot C-ITS sites with real traffic.
TRL 7: system validation	Protocols are implemented and fully tested at real pilot C-ITS sites with real traffic.
TRL 8: tested and implemented	Protocols are implemented and fully tested at real pilot C-ITS sites with real traffic, and evidence for feasibility is presented.
TRL 9: proven in mission	Protocols are implemented and ready for scaled deployment in operating C-ITS sites.

The reason for step 2, to use majority scoring instead of mean values, is to avoid large discrepancies between very small and very large scores, since the focus is on identifying how far the most mature research has reached, regardless of the quantity of published articles. In practice, this also meant the authors examined each extraction and discussed the motivation thereof to resolve any differences.

6.2. Technology Readiness Levels

We used the NASA TRL framework [15] for assessing a set of pre-defined areas within CLC for C-ITSs: authentication, aggregated signatures, key agreement and signcryption. Each area is analyzed using the TRL, where each area consists of a set of articles found in the literature analysis phase. The TRL levels were transformed into the CLC in C-ITSs context using the translation provided in Table 1. There are nine levels in the framework, where TRL 1 is the lowest and TRL 9 is the highest. TRL 1 indicates that scientific research is just beginning and any results can be viewed for future research. TRL 2 corresponds to when the basic principles have been studied, and there is little or no proof-of-concepts for the technology at this level. TRL 3 corresponds to when the technology is actively researched; usually proof-of-concepts are constructed. The next level, TRL 4, is when the proof-of-concept is further advanced, and TRL 5 is a continuation of TRL 4 but with more extensive and more developed implementations, e.g., realistic simulations and tests are conducted. TRL 6 corresponds to a fully functional prototype of the technology. TRL 7 technology requires the prototype to be demonstrated in a space environment, i.e., in a realistic environment. TRL 8 means the technology is tested and ready for implementation, and TRL 9 corresponds to when the technology is "flight proven" during a successful application (mission as it is stated in the framework).

6.3. Empirical Data Collection and Analysis

Empirical data were collected by conducting interviews to capture the adoption of CLC in C-ITSs. Interviews were selected to obtain a first-person account of the social reality of the subject [39]. In this case, the interviews were used to provide insights into affecting factors when deciding on new, innovative cryptographic security controls. Selected for interviews were three subject experts. These three were selected because of their involvement with either regulation of or standardization within C-ITSs and, therefore, in a position to elaborate on potential, future directions and security controls. All interviews were recorded and lasted approximately half an hour each. The interviewed subject specialists are described in Table 2 below.

Table 2. Overview of the interviewees.

Interviewee	Role	Experience
Alpha	Digital strategist ITS/C-ITS	Cybersecurity, ITS/C-ITS > 20 years
Beta	PKI specialist	Cybersecurity, PKI, C-ITS > 10 years
Gamma	C-ITS specialist	IT-architecture, ITS/C-ITS > 5 years

To enable a more natural conversation, semi-structured interviews were used. The structure of the interviews took inspiration from the laddering technique, so as to gain a richer understanding of underlying reasoning and motives. The laddering technique implies that the interviewer repeatedly asks additional, elaborating type of questions and follow up on answers given in order to find nuances in the answers [40]. To help direct the interviews, an interview guide was developed that consisted of a series of questions based around the five phases from the Innovation-Decision Model. A snippet from the interview guide with respect to the decision phase is illustrated below.

- *What are the reasons for (not) adopting new cryptographic systems (e.g., certificate-less) to ITS?*
    - *What motivates the adoption of (new) cryptographic systems for ITS?*
    - *If you were to decide today, would you be in favor of implementing certificate-less cryptography in ITS? Why or why not?*
    - *Do you think these motivations/reasons may change in the future?*
        - *Why do(n't) you think this will happen?*
- *Have you ever experienced that a decision to adopt a cryptographic system was later reversed (e.g., going from adoption to rejection, or the other way around)?*
    - *What was the reason for reversing the decision?*
    - *Why do you think that argument was made?*
    - *What would have needed to be different for this decision (not) to have been made?*

After the interviews, the recordings were partially transcribed and analyzed in two steps. First, the transcripts were analyzed using concept-driven coding to extract relevant answers into the five phases of the Innovation-Decision Model. Next, the extracted data under each phase were then lifted into a new document where differences and similarities between answers were identified and synthesized into a coherent result.

7. Results

The current state of research in CLC for C-ITSs is presented in Section 7.1 as the result of the literature review, while the analysis of the interviews is presented in Section 7.2. Table 3 provides an overview of the identified gaps in CLC along with how these gaps could be closed. These gaps were grouped into three key reasons affecting adoption of CLC for C-ITSs: availability of proof-of-concepts, knowledge beyond current best-practices, and a strong buy-in from both stakeholders and standardization bodies.

Seen from the Innovation-Decision Model, the findings suggest a mismatch between the academic gaps and the practical gaps. Based on the interviews, it was shown that, in practice, gaps mostly circulated around the knowledge and persuasion phases, which can be said to ultimately contribute to a passive rejection (i.e., that the decision maker never considered adopting the innovation in the first place) during a decision phase. Meanwhile, gaps identified in the academic literature circulated around the implementation and confirmation phases, particularly in providing insights on consequences and suitability for CLC in a C-ITS production like environment and context.

Table 3. Overview of the identified and grouped gaps and what could be done, going forward, to address each gap.

Gaps	Description	Going Forward
Proof-of-Concepts	Various concepts of CLC-based solutions have been proposed, such as for authentication [41–58], aggregated signing [44,59–64], key agreement [65,66], and signcryption [67–73]. However, common for these proposals is that they have either been tested in a controller lab environment [42,47,48,59,64,74] or only theoretically [41,43,45,49,50,52,53,60,62,63,65–67,73,75], typically using a desktop or laptop computer. This has lead to quite similar, theoretical performances as they are based on matching setups (e.g., using MIRACL lib. Omnet++, Veins simulations, etc.); even more so when the same PoC are used between authors [43–45,52,53,67]. Hence, little is still known about performance in a production-like environment and context.	Based on the interviews, one way of going forward to counter this gap would be to encourage collaborative (government and/or international funded) C-ITS project initiatives in which new technological advancements can be developed, tested and assessed. Such initiatives could provide an alternative source of cryptography knowledge in the organisations and aid buy-in for testing new technologies and PoC among practitioners and stakeholders alike.
Best-Practices	A clearly identified gap is the lack of professional and academic-level cryptography knowledge in the organization; from the interviews, this was frequently mentioned as a barrier for further developments of new security mechanisms. Practitioners from interview Alpha, Beta, and Gamma, stayed à jour with new developments in cryptography by Internet searches and third-party providers recommendations, which tended to gravitate around already-established best-practices.	Beyond employee training, education, and recruitment of relevant competences within organisations, science communication plays a role in affecting the practitioners individual 'awareness-knowledge'. Bridging academia and industry—e.g., by extended networking and increased collaboration between industry and academia—could, similarly, influence standardization projects.
Stakeholders and Standardization	Although the academic research in CLC for C-ITSs is increasing, there is little overlap with standardization bodies, which are typically focused on traditional solutions. As noted from the interviews, stakeholders tend to rely on approved standardization requirements, which could therefore affect a broader comprehension, development and adoption of CLC-systems by the industry.	Further harmonization of terms, security models, nomenclature, and grouping of protocols in CLC for C-ITSs is needed to better bridge industry, standardization bodies, and academic work on the topic.

7.1. Current State of Research in CLC for C-ITS

In this section we will detail the current theoretical work of CLC, specifically for C-ITSs. The amount of research in CLC is massive. A quick search on "*certificateless cryptography*", "*CLC*" and "*CL-PKC*" in Scopus, Google Scholar, Springer Link, IEEE Xplore and similar databases gives several thousand hits. It is more difficult to extract the exact number of papers addressing C-ITS since several papers only use VANET or V2X as illustrative scenarios, where the essence of the research is the mathematical framework rather than the applicability. Therefore, we applied a filtering process during the synthesis of the collected data, where the inclusion criteria was to have either (or both) a proof-of-concept implementation and a significant detailed part of the paper related to VANET, V2X or other related C-ITS concepts. From the analysis we grouped the remaining articles into Authentication, Aggregated signatures, Key agreement and Signcryption. Although most of the articles refer to authentication solutions, our grouping provides a more detailed distinction of proposed techniques. In the main category Authentication single-signature solutions were in the majority. We summarize the findings in Table 4. We note that there exists no surveys for CLC-based security solutions for C-ITSs specifically. However, some surveys are included in Table 4 if they partially included papers relevant for the intersection of C-ITSs and CLC, and in that case, the proportion of schemes implemented are only counted from the set of CLC-based schemes mentioned in the survey.

Table 4. Overview of the current subfields of CLC for C-ITS-related areas, separated into level of PoC implementations, year and Technical Readiness Level (TRL) score.

Subfield	PoC Lab	PoC Industry	Reference Data	CLC-TRL
2023 Q1				
Authentication	33%	0%	[41–46]	3
Aggregated signatures	66%	0%	[59,60,75]	3
Key agreement	0%	0%	[65]	1
Signcryption	0%	0%	[67]	2
2022				
Authentication	66%	0%	[47–57,76]	3
Aggregated signatures	60%	0%	[61–64,77]	3
Key agreement	0%	0%	[66]	1
Signcryption	100%	0%	[68–72]	4
Surveys			[32,78,79]	

In the analyzed time frame of 2022–2023 there was no proof-of-concept implementations on-site, i.e., corresponding to level 5 in CLC TRL. The majority of implementations, and, thereby, performance analysis of CLC schemes, were made on laptops and/or PC clients with varying specifications in both Ubuntu and Windows. The most-used programming library for the cryptographic operations was MIRACL, e.g., in [46,59–61,67,68]. A few projects, e.g., [60,61,68], also used network traffic simulations for testing the protocols communication complexity; the most used simulation tool was Omnet++. The majority of the remaining found research that included performance analysis did not have customized implementations but instead referred to other articles and used their results to theoretically compute their own protocol's execution time. This would yield a CLC-TRL not higher than 3. We also examined the trend of published CLC-based solutions in C-ITSs. We conducted a second literature search for articles between 2016–2023 and used a lightweight filtering process where we did not classify articles into sub-fields (authentication, signcryption and so on). The publication trend of these papers is presented in Figure 4, and we see clearly that the number of publications in this area increases over time. The articles in 2023 were collected up to and including Q1 of 2023.

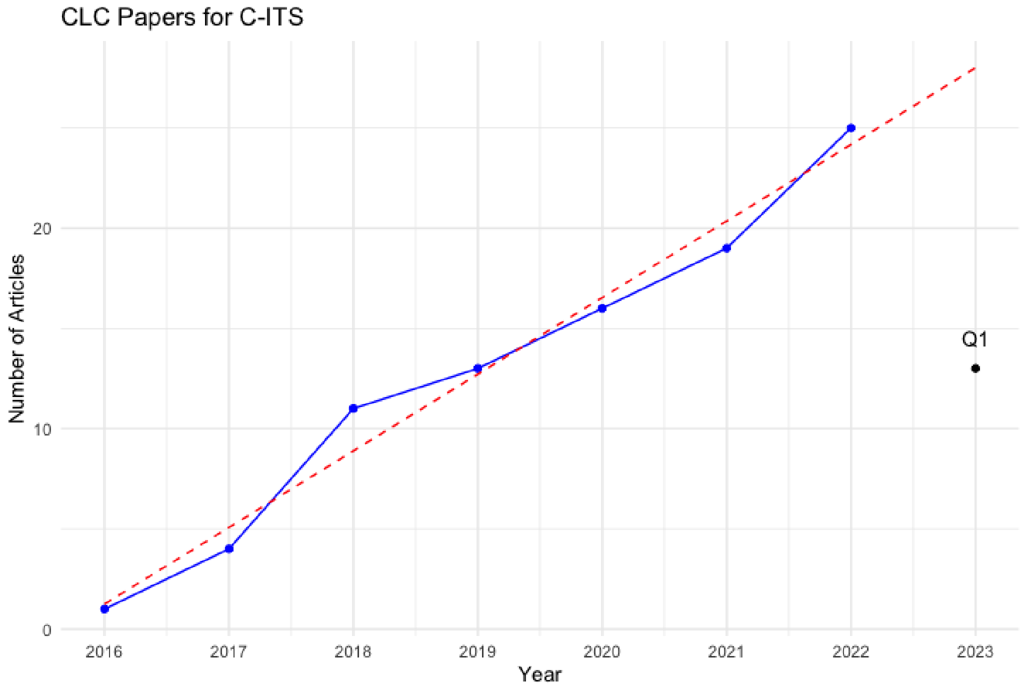

Figure 4. Trend analysis of CLC in C-ITSs articles over time, using linear regression to predict the number of articles for 2023. Q1 marks the number of articles collected up to and including Q1 2023.

7.2. Specialist Interviews

7.2.1. Interviewee Alpha

Interviewee "Alpha" possesses a multifaceted background in system development, IT architecture, and robotics engineering. However, Alpha's involvement in C-ITSs came later in their career. Alpha also has experience in cybersecurity. When confronted with the concept of CLC, Alpha did not have prior knowledge of it, and similar to Beta, would utilize the Internet to source information about it. Alpha identified significant challenges in C-ITSs and cryptographic technologies, specifically concerning the limitations of resources. These constraints often manifest as performance issues, such as difficulties related to hardware computations. Alpha saw parallels between these challenges and those faced in robotics, particularly in terms of securing data and maintaining performance as devices become interconnected. The future of these issues, however, remained unclear to Alpha. For instance, Alpha pondered the impact of further advancements in quantum computing. Alpha also speculated that the evolution of technology, like quantum computing and cloud services, might necessitate different types of security controls. The adoption of these new security controls could prove challenging, owing to the difficulty in distinguishing between quality requirements and business requirements. Moreover, performance issues stemming from new security controls might also act as deterrents to their adoption.

According to Alpha, one of the keys to successfully integrating new security controls in their organization would be securing buy-in from standardization bodies. Alpha stressed the need for the organization to recruit personnel with competence and knowledge in cryptography. This would facilitate a better understanding and faster adoption of new security controls. Furthermore, involvement and active participation in innovation are crucial for the success of the organization. Alpha also pointed out that a significant barrier to the adoption of new controls is the organization's tendency to adhere to previously approved security solutions (e.g., traditional PKI solutions). Another crucial factor for embracing innovation, Alpha indicated, falls on the management's responsibility. The ability to understand and encourage innovation could be pivotal in driving the organization's work towards adopting new security controls.

7.2.2. Interviewee Beta

The interviewee, henceforth referred to as "Beta", possesses extensive experience in the field of IT-security, with a specific focus on authentication and PKI. Beta did not exhibit any prior knowledge of CLC and would use Google to gather information. From Beta's experience, there is a general tendency toward sluggish adoption of novel security technologies. This was attributed not only to technological challenges but also political considerations. Beta suggested that monetary factors often played a significant role, meaning there is interest from the market in what standards and solutions there should be. Within Beta's C-ITS projects, there had not been any discussions concerning the replacement of conventional PKI systems. Beta expressed the belief that, if compelling evidence were presented, showing that a new security technology provides considerable advantages over PKI, the market could potentially accept the idea of adoption. Beta explained that proof-of-concept is a highly effective method for promoting the integration of new technologies. The need for organizations to accumulate knowledge and comprehension of emerging technologies was a point Beta strongly emphasized. Simultaneously, Beta highlighted the importance of creating buy-in within these organizations as a key-factor. Beta noted that new technology must be "*easily consumed*", implying that it should be comprehensible and straightforward to implement in the organization. Beta proposed that any new security technology should be measured in terms of its maintenance costs and the extent to which it enhances the level of security. Beta mentioned that one of the major challenges in this process is the lack of coordination when it comes to introducing new ideas within the organization. In current international projects, the standard practice for implementing proof-of-concepts with regard to trust is to use PKI. According to Beta, it remains uncertain whether innovation is necessary in dealing with trust-related challenges within C-ITS, or if the market's commitment to PKI solutions is robust enough to incubate the expansion of CLC and other new technologies.

7.2.3. Interviewee Gamma

Interviewee "Gamma" has a background in IT-architecture and has worked in different technical and project management roles within the C-ITS domain. Gamma was unfamiliar with the concept of CLC. To gain information about CLC, Gamma would leverage the current professional cybersecurity network, including resources like DigiCert. Gamma highlighted that current C-ITS initiatives demonstrate a satisfactory focus on cybersecurity. However, this focus does not typically include cryptography, but instead emphasizes the necessity for digital signatures and technical standards. In some C-ITS projects, proof-of-concepts are carried out for security controls; however, only including traditional PKI solutions (i.e., not to evaluate novel security controls).

A potential barrier to the adoption of new security controls, according to Gamma, lies in the organization becoming reliant on proprietary security solutions. To avoid this, Gamma advocates for the use of open solutions that allow market-driven development. For an organization to successfully adopt new security controls, Gamma underscores the need for knowledge and competence in cryptography. This expertise should extend to system developers possessing proficiency in these areas. Further, Gamma concludes that the security organization in the company must also champion and understand these new solutions, facilitating buy-in from decision makers and stakeholders. Gamma suggested that the vehicle industry, being generally slow to adapt, must willingly accept new security controls to expedite their adoption. In addition, standardization bodies need to be involved, considering the industry's heavy reliance on these standards. For any innovative security solutions to gain traction, Gamma insists that the benefits must be clearly articulated, justifying why it surpasses traditional PKI. Consequently, convincing organizations to test and adopt new security solutions could be quite challenging. Finally, Gamma stated that, in order to gauge the effectiveness of new technologies, metrics should be established to assess the costs of maintaining and developing it, as well as the business model it promotes.

7.3. Interview Summary

The main key takeaways from the interviews are summarized in Table 5.

Table 5. Summary of the key takeaways from the interviews.

Id	Key Takeaway
1	It is crucial to have individuals with competency in cryptography within the organization, to not only understand but also drive and push innovation, despite the complexities of these new technologies.
2	The involvement and support of standardization bodies are indispensable for ensuring a wide acceptance and implementation of new security controls.
3	A factor that slows down the willingness and ability to adopt new security controls such as CLC is the lack of key takeaways 1 and 2.
4	Organizations can become stuck with previously implemented and accepted security solutions, e.g., traditional PKI, hence do not tend to explore new options that are not officially accepted (in standardization documents).
5	Improved proof-of-concepts of CLC-based solutions are needed, to speeding up adoption of such new security controls.

8. Discussion

Our analysis identified three main gaps in the adoption maturity of CLC-based C-ITS solutions, based on the literature analysis and the industry practitioner interviews. We discuss each gap in the subsequent subsections, providing insights from the collected data in how to bridge the gaps and what factors influence the measured CLC-TRL level.

8.1. Gap 1: Proof of Concepts

We note that 0% of the summarized research in Table 4 contained onsite proof-of-concept implementations. Instead, most implementations were on laptops in laboratory environments or simulations. This suggests that CLC is not yet ready for the first stages of industry adoption, since the interviewees confirmed that proof-of-concepts is one of the key success factors for further adoption of new technology. Moreover, a detailed review of the implementation descriptions in the literature analysis shows an unsatisfactory level of reproducibility and comparability since many implementation details are left out, and very few articles share source code. Several articles leave out testing and performance evaluation in realistic environments as future work (e.g., [31,47,52,55,64]). Also, several articles referred to a small set of previous articles that carried out implementations of the crypto operations used in some of the CLC protocols, and used these to theoretically compute performance metrics (e.g., [43–45,60,67]). Only a handful of the articles did simulations of network traffic, where most implementations focused on the crypto computations. These findings suggest that a closing of the gap relies on creating a buy-in in the industry where future implementations are relevant. As suggested by the interview data, increased knowledge in cryptography on the industry side, and more involvement of cybersecurity expertise from academia in international C-ITS projects are needed for enable more prototyping.

8.2. Gap 2: Best Practices

In general, it was clear from the interviews that an increase in building cryptography knowledge in the organization is needed; this was highlighted by all interviewees. This indicates that, in order to pick up new security technology such as CLC, even in the first stages of innovation, the prerequisite is to hire people skilled in cryptography, or develop the competence in the organization. This underpins what previous studies have noted regarding the increasingly broad expertise required for decision makers of security controls [5–7]. Regardless, this would naturally lead to increased costs, not only in terms of competence development, but also in technology development; an investment which has shown to not always result in a more profitable product [12], thus potentially affecting the decision phase towards a rejection. However, seen from a knowledge phase perspective, the literature analysis indicates that the industry should be able to move towards a decision phase fairly easily if the knowledge barrier is mitigated, since the academic research is mature enough to be pushed towards CLC-TRL 5 and 6. If onsite proof-of-concepts can be implemented, tested, and assessed, a previous rejection may be reversed at this point if the decision maker is exposed to conflicting messages about previous doubts. Although, this most likely requires collaboration with the industry so that relevant hardware can be provided. From the interview data, we conclude that recruitment and/or development of skilled employees in cryptography is necessary to close this gap. Moreover, the data also suggest that more involvement of decision makers and collaboration in the industry towards exploring non-standard solutions (such as traditional PKI) is needed.

8.3. Gap 3: Stakeholders and Standardization

The interviews indicated two main stakeholders for a buy-in regarding CLC and other novel security technologies: upper management and standardization bodies. The management segment must have a buy-in in order for the organization to consider evaluating new technology, and the standardization bodies are crucial for the market since they seem to be very dependent on these bodies. Therefore, even if adequate cryptography competence is gained within the organization, the persuasion phase is crucial—as can be seen from previous studies where top management support has been shown to be key for managing information security in practice [80]. No data from our study indicate whether there is a natural dependency between adequate competence in cryptography and strong buy-in of stakeholders; but, drawing on previous studies on differing risk perceptions, we can suspect these are independent since a buy-in may be more volatile due to individual preferences. Or put differently, knowing about does not necessarily translate into an intent to do [81]. Moreover, the literature analysis suggests that the nomenclature, notation, and grouping of schemes is not fully harmonized; thus, potentially leading to even slower adoption due to a lower level of comprehension. As pointed out by Sripathi Venkata Naga et al. [78] from the literature analysis, future work in investigating notation standards as in what type of CLC solutions there are with regards to type of application scenario, is suggested. Indeed, lacking a common language among information security practitioners have been noted as a major factor that slows down progression within the field [82]. Similar to cybersecurity in general, the importance of harmonization and standardization is crucial [83], we thus hypothesise that an increase in harmonization activities could help to minimize this gap.

8.4. Technology Readiness Assessment

Interestingly, we have identified a distinct increase in academic research of CLC within C-ITSs (see Figure 4), but the TRL is still below onsite proof-of-concept implementations. Simultaneously, there is a need for understanding the cryptography part of CLC in the industry, combined with—as elaborated by interviewee Beta and Gamma—a desire to have clear proofs as to why such technology would be more beneficial than traditional PKI. Since standardization bodies are inclined to default to PKI, that seems to be a strong barrier for the industry to be convinced and spend resources to evaluate new security controls. To conclude: the current level of TRL for CLC in the domain of C-ITSs is low, where our qualitative study indicates a knowledge gap (specifically cryptography) in the industry and the literature analysis indicates a lack of proof-of-concept implementations that can be used for better buy-in of the industry. The identified gaps for CLC in C-ITSs is, then, hindering the field to be mature enough for adoption in the current state of industry and academia.

8.5. Future Research

From the interviews, it is clear that the industry has a knowledge gap in CLC. Moreover, the tendency to search for information of new security controls and technology is not in academia but on the Internet. Can this be a barrier for closing the knowledge gap? Practitioners have not picked up CLC yet, thus it will be very difficult to even find out about CLC even though the fundamental research is solid, i.e., if CLC-TRL 4 is reached. Therefore, research in *how* the knowledge phase can be improved is needed. We also note that the current perception is that standardization bodies influence the adoption (or lack thereof) of new security controls heavily; hence, a better understanding in how the decision making and knowledge phase works within these type of organizations, is needed.

8.6. Threats to Validity

There is a possibility that articles aimed for CL-PKC in C-ITSs scenarios have been missed in the initial literature review phase due to missing keywords in the article or mentioning of string such as "VANET", "V2X" or "C-ITS" in the abstracts and conclusions. Nonetheless, as our analysis was specifically focused on articles targeting the C-ITS context, it is plausible that any missing articles due to the aforementioned threat suggest that the central aspect of those articles merely employs C-ITSs as an example scenario or to illustrate one among several potential use cases. Finally, the accuracy and reliability of data collected through interviews are naturally subject to the respondents' recall ability and perception. There may be biases in the responses that may affect the quality of the data collected.

9. Conclusions

The aim of this study was to explore affective factors for decision makers when selecting and implementing new types of security controls. Certificateless cryptography (CLC) as a security control in Cooperative Intelligent Transport Systems (C-ITSs) was selected as a good candidate to study this phenomenon, since it is still a relatively new technology that has not yet been widely adopted by the industry, but has, at the same time, been subject to academic studies for some time. Factors influencing the decision to adopt or reject this new type of security control were studied by first investigating current advances and gaps in CLC for C-ITSs. This was carried out by reviewing academic articles on the topic and rank them according to a modified version of NASA's Technology Readiness Levels to assess the security controls (practical) maturity. Likewise, in order to study the challenges (or gaps) and enablers that affect readiness and willingness to adopt certificateless cryptography, the five phases of the Innovation-Decision Model was used as a foundation for the interviews held with three domain experts. As a result, three gaps were identified as key reasons affecting adoption. First, it was found that there are few proof-of-concepts that take into account realistic, production like circumstances, but remain theoretical. As such, little is still known about CLC's practical suitability in C-ITS, which does not inspire confidence in buy-in among practitioners and stakeholders alike. Second, it was found that the domain experts' principles-knowledge did not go beyond the security controls currently seen as industry best-practice. Lastly, it was found that there is little overlap between academic research in CLC for C-ITSs and standardization bodies, ultimately affecting the buy-in from both stakeholders and standardization bodies. Additional work is needed to better understand the affective factors for decision makers, and in extension CLC for C-ITSs. To this end, each identified gap is accompanied by suggested areas for future research and can be found in Table 3 'Going Forward' as well as in Section 8.5.

Author Contributions: Conceptualization, H.S. and M.L.; methodology, H.S. and M.L.; resources, H.S.; data curation, H.S. and M.L.; writing—original draft preparation, H.S. and M.L.; writing—review and editing, H.S. and M.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The transcript data supporting this study are not publicly available as the participants of this study did not give written consent for this data to be shared publicly in full. Please contact the corresponding author, H.S, if there are any questions.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

C-ITS	Cooperative ITS
CLC	Certificateless Cryptography
CL-PKC	Certificateless Public Key Cryptography
ITS	Intelligent Transport Systems
TRL	Technology Readiness Level
V2X	Vehicle-to-Anything
VANET	Vehicular Ad-Hoc Network

References

1. Petit, J.; Shladover, S.E. Potential cyberattacks on automated vehicles. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 546–556. [CrossRef]
2. Paulsen, C.; Byers, R. *Glossary of Key Information Security Terms*; Technical Report NIST IR 7298r3; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019. [CrossRef]
3. Lundgren, M.; Bergström, E. Dynamic interplay in the information security risk management process. *Int. J. Risk Assess. Manag.* **2019**, *22*, 212–230. [CrossRef]
4. *ISO/IEC 27005*; Information Technology-Security Techniques -Information Security Risk Management. International Organization for Standardization: Geneva, Switzerland, 2013.
5. Haqaf, H.; Koyuncu, M. Understanding key skills for information security managers. *Int. J. Inf. Manag.* **2018**, *43*, 165–172. . [CrossRef]
6. Anderson, A.B.; Ahmad, A.; Chang, S. Competencies of cybersecurity leaders: A review and research agenda. *ICIS 2022 Proc.* **2022**, *9*, 1967–1983 .
7. Salin, H.; Lundgren, M. Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. *J. Cybersecur. Priv.* **2022**, *2*, 276–291. [CrossRef]
8. Wall, J.D.; Palvia, P.; D'Arcy, J. Theorizing the behavioral effects of control complementarity in security control portfolios. *Inf. Syst. Front.* **2021**, *24*, 1–22 . [CrossRef]
9. Lundgren, M.; Bergström, E. Security-related stress: A perspective on information security risk management. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019; pp. 1–8.
10. Boss, S.R.; Kirsch, L.J.; Angermeier, I.; Shingler, R.A.; Boss, R.W. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *Eur. J. Inf. Syst.* **2009**, *18*, 151–164. [CrossRef]
11. Ogbanufe, O.; Crossler, R.E.; Biros, D. The valued coexistence of protection motivation and stewardship in information security behaviors. *Comput. Secur.* **2023**, *124*, 102960. [CrossRef]
12. Wright, C.S. Software, vendors and reputation: An analysis of the dilemma in creating secure software. In Proceedings of the Trusted Systems: Second International Conference, INTRUST 2010, Beijing, China, 13–15 December 2010; Revised Selected Papers 2; Springer: Berlin/Heidelberg, Germany, 2011; pp. 346–360.
13. Dalal, R.S.; Howard, D.J.; Bennett, R.J.; Posey, C.; Zaccaro, S.J.; Brummel, B.J. Organizational science and cybersecurity: Abundant opportunities for research at the interface. *J. Bus. Psychol.* **2022**, *37*, 1–29. [CrossRef]
14. Bergström, E.; Lundgren, M. Stress amongst novice information security risk management practitioners. *Int. J. Cyber Situational Aware.* **2019**, *4*, 128–154. [CrossRef]
15. Mankins, J.C. Technology readiness levels. *White Pap. April* **1995**, *6*, 1995.
16. Rogers, E.M. *Diffusion of Innovations*; Simon and Schuster: New York, NY, USA, 2010.
17. *NIST SP 800-53*; Security and Privacy Controls for Information Systems and Organizations. Technical Report. Edition: Revision 5. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
18. Al-Riyami, S.S.; Paterson, K.G. Certificateless Public Key Cryptography. In Proceedings of the Advances in Cryptology—ASIACRYPT 2003, Taipei, Taiwan, 30 November–4 December 2003; Laih, C.S., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 452–473.
19. NordicWay 3. NordicWay 2 and NordicWay 3. 2022. Available online: https://www.nordicway.net (accessed on 14 May 2022).
20. C-Roads. C-Roads - The Platform of Harmonised C-ITS Deployment in Europe. 2022. Available online: https://www.c-roads.eu, (accessed on 14 May 2022).
21. UNISIG. On-line Key Management FFFIS: Subset-137. 2015. Available online: https://www.era.europa.eu/system/files/2023-01/sos3_index083_-_subset-137_v100.pdf (accessed on 1 February 2022).
22. European Telecommunications Standards Institute. ETSI TS 102 941 V1.4.1: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. 2021. Available online: https://www.etsi.org/standards (accessed on 23 February 2022).
23. Hammi, B.; Monteuuis, J.P.; Petit, J. PKIs in C-ITS: Security functions, architectures and projects: A survey. *Veh. Commun.* **2022**, *38*, 100531. [CrossRef]

24. European Comission. INTELLIGENT TRANSPORT SYSTEMS—Cooperative, Connected and Automated Mobility (ITS-CCAM) and Electromobility. 2022. Available online: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/intelligent-transport-systems-cooperative-connected-and-automated-mobility-its-ccam-and-0 (accessed on 23 February 2022).
25. IEEE Standard for Information Technology– Local and Metropolitan Area Networks–Specific Requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)* 2010; pp. 1–51. Available online: https://ieeexplore.ieee.org/document/5514475 (accessed on 29 June 2023).
26. *IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013)*; IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. IEEE: Piscataway, NJ, USA, 2019; pp. 1–106. Available online: https://ieeexplore.ieee.org/document/8686445 (accessed on 29 June 2023).
27. US Department of Transportation. Intelligent Transportation Systems Joint Program Office: ITS Cybersecurity Research Program. 2023. Available online: https://www.its.dot.gov (accessed on 28 March 2022).
28. FoxIT. Black Tulip Report of the Investigation into the DigiNotar Certificate Authority Breach. Technical Report, 2012. Available online: https://www.researchgate.net/publication/269333601_Black_Tulip_Report_of_the_investigation_into_the_DigiNotar_Certificate_Authority_breach?channel=doi&linkId=5486fcf80cf268d28f06fa61&showFulltext=true (accessed on 10 August 2023).
29. Malik, M.; Kamaldeep.; Dutta, M. On the Applicability of Certificateless Public Key Cryptography (CL-PKC) for Securing the Internet of Things (IoT). In Proceedings of the International Conference on IoT Inclusive Life (ICIIL 2019), Nitttr Chandigarh, India, 19–20 December 2020.
30. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [CrossRef]
31. Khan, S.; Luo, F.; Zhang, Z.; Rahim, M.A.; Ahmad, M.; Wu, K. Survey on Issues and Recent Advances in Vehicular Public-Key Infrastructure (VPKI). *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1574–1601. [CrossRef]
32. Nayak, P.; Swapna, G. Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview. *Internet Things* **2023**, *21*, 100641. [CrossRef]
33. Sahin, I. Detailed review of Rogers' diffusion of innovations theory and educational technology-related studies based on Rogers' theory. *Turk. Online J. Educ. Technol.-TOJET* **2006**, *5*, 14–23.
34. Parasuraman, A. Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies. *J. Serv. Res.* **2000**, *2*, 307–320. [CrossRef]
35. Holden, R.J.; Karsh, B.T. The Technology Acceptance Model: Its past and its future in health care. *J. Biomed. Inform.* **2010**, *43*, 159–172. [CrossRef]
36. Pandeya, G.R.; Daim, T.U.; Marotzke, A., A Strategy Roadmap for Post-quantum Cryptography. In *Roadmapping Future: Technologies, Products and Services*; Daim, T.U., Ed.; Springer International Publishing: Cham, Switzerland, 2021; pp. 171–207. [CrossRef]
37. Ma, C.; Colon, L.; Dera, J.; Rashidi, B.; Garg, V. CARAF: Crypto Agility Risk Assessment Framework. *J. Cybersecur.* **2021**, *7*, tyab013. [CrossRef]
38. Levy, Y.; Ellis, T.J. A systems approach to conduct an effective literature review in support of information systems research. *Informing Sci.* **2006**, *9*, 81–212. [CrossRef]
39. Schultze, U.; Avital, M. Designing interviews to generate rich data for information systems research. *Inf. Organ.* **2011**, *21*, 1–16. [CrossRef]
40. Reynolds, T.J.; Gutman, J. Laddering theory, method, analysis, and interpretation. *J. Advert. Res.* **1988**, *28*, 11–31.
41. Liu, X.; Wang, Y.; Li, Y.; Cao, H. PTAP: A novel secure privacy-preserving & traceable authentication protocol in VANETs. *Comput. Netw.* **2023**, *226*, 109643. [CrossRef]
42. Genc, Y.; Aytas, N.; Akkoc, A.; Afacan, E.; Yazgan, E. ELCPAS: A new efficient lightweight certificateless conditional privacy preserving authentication scheme for IoV. *Veh. Commun.* **2023**, *39*, 100549. [CrossRef]
43. Wang, Z.; Zhou, Y.; Qiao, Z.; Yang, B.; Gu, C.; Xu, Y.; Zhang, M. An Anonymous and Revocable Authentication Protocol for Vehicle-to-Vehicle Communications. *IEEE Internet Things J.* **2023**, *10*, 5114–5127. [CrossRef]
44. Yan, X.; Ma, M.; Su, R. Efficient Group Handover Authentication for Secure 5G-Based Communications in Platoons. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3104–3116. [CrossRef]
45. Tan, H.; Zheng, W.; Vijayakumar, P. Secure and Efficient Authenticated Key Management Scheme for UAV-Assisted Infrastructure-Less IoVs. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 1–12 . [CrossRef]
46. Zhou, Y.; Cao, L.; Qiao, Z.; Xia, Z.; Yang, B.; Zhang, M.; Zhang, W. An efficient identity authentication scheme with dynamic anonymity for VANETs. *IEEE Internet Things J.* **2023**, *10*, 10052–10065 . [CrossRef]
47. Zhou, X.; Luo, M.; Vijayakumar, P.; Peng, C.; He, D. Efficient Certificateless Conditional Privacy-Preserving Authentication for VANETs. *IEEE Trans. Veh. Technol.* **2022**, *71*, 7863–7875. [CrossRef]
48. Ali, I.; Chen, Y.; Faisal, M.; Li, M., Certificateless Signature-Based Authentication Scheme for Vehicle-to-Infrastructure Communications Using Bilinear Pairing. In *Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks*; Springer Nature: Singapore, 2022; pp. 91–119. [CrossRef]

49. Zheng, L.; Feng, T. Research on a Vehicle Authentication and Key Transmission Protocol Based on CPN. *Symmetry* **2022**, *14*, 2398. [CrossRef]
50. Imghoure, A.; El-Yahyaoui, A.; Omary, F. ECDSA-based certificateless conditional privacy-preserving authentication scheme in Vehicular Ad Hoc Network. *Veh. Commun.* **2022**, *37*, 100504. [CrossRef]
51. Wang, Y.; Liu, Y.; Tian, Y. ISC-CPPA:Improverd-Security Certificateless Conditional Privacy-Preserving Authentication Scheme With Revocation. *IEEE Trans. Veh. Technol.* **2022**, *71*, 12304–12314. [CrossRef]
52. Yan, X.; Ma, M.; Su, R. A Certificateless Efficient and Secure Group Handover Authentication Protocol in 5G Enabled Vehicular Networks. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 1678–1684. [CrossRef]
53. Mukathe, K.D.; Wu, D.; Ahmed, W. Secure and Efficient Blockchain-Based Certificateless Authentication Scheme for Vehicular Ad-Hoc Networks (VANETs). In Proceedings of the 2022 4th International Conference on Applied Machine Learning (ICAML), Changsha, China, 23–25 July 2022; pp. 302–307. [CrossRef]
54. Gupta, D.S.; Karati, A.; Saad, W.; da Costa, D.B. Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3255–3266. [CrossRef]
55. Palaniswamy, B.; Ansari, K.; Reddy, A.G.; Das, A.K.; Shetty, S. Robust Certificateless Authentication Protocol for the SAE J1939 Commercial Vehicles Bus. *IEEE Trans. Veh. Technol.* **2023**, *72*, 4493–4509. [CrossRef]
56. Jiang, Y.; Zhang, K.; Qian, Y.; Zhou, L. Anonymous and Efficient Authentication Scheme for Privacy-Preserving Distributed Learning. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 2227–2240. [CrossRef]
57. Qi, J.; Gao, T.; Deng, X.; Zhao, C. A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs. *Veh. Commun.* **2022**, *38*, 100535. .: 10.1016/j.vehcom.2022.100535. [CrossRef]
58. Zhao, Y.; Dan, G.; Ruan, A.; Huang, J.; Xiong, H. A Certificateless and Privacy-Preserving Authentication with Fault-Tolerance for Vehicular Sensor Networks. In Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Japan, 30 January–2 February 2021; pp. 1–7. [CrossRef]
59. Liang, Y.; Liu, Y. Analysis and Improvement of an Efficient Certificateless Aggregate Signature With Conditional Privacy Preservation in VANETs. *IEEE Syst. J.* **2023**, *17*, 664–672. [CrossRef]
60. Gong, Z.; Gao, T.; Guo, N. PCAS: Cryptanalysis and improvement of pairing-free certificateless aggregate signature scheme with conditional privacy-preserving for VANETs. *Ad Hoc Netw.* **2023**, *144*, 103134. [CrossRef]
61. Wang, H.; Wang, L.; Zhang, K.; Li, J.; Luo, Y. A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs. *IEEE Access* **2022**, *10*, 15605–15618. [CrossRef]
62. Cahyadi, E.F.; Su, T.W.; Yang, C.C.; Hwang, M.S. A certificateless aggregate signature scheme for security and privacy protection in VANET. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 15501329221080658. [CrossRef]
63. Samra, B.; Fouzi, S. New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET. *Veh. Commun.* **2022**, *34*, 100414. [CrossRef]
64. Chen, Y.; Chen, J. CPP-CLAS: Efficient and Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme for VANETs. *IEEE Internet Things J.* **2022**, *9*, 10354–10365. [CrossRef]
65. Wei, G.; Qin, Y.; Fu, W. Secure and Efficient Certificateless Authentication Key Agreement Protocol in VANET. In *Emerging Information Security and Applications*; Chen, J., He, D., Lu, R., Eds.; Springer Nature Switzerland: Cham, Switzerland, 2022; pp. 160–172.
66. Yang, J.; Li, F.; Zhang, Z. Research on NTRU-based Anonymous Authentication and Key Negotiation Protocol for VANETs. In Proceedings of the 2022 7th International Conference on Cyber Security and Information Engineering (ICCSIE), Brisbane, Australia, 23–25 September 2022; pp. 104–108. [CrossRef]
67. Dai, C.; Xu, Z. Pairing-Free Certificateless Aggregate Signcryption Scheme for Vehicular Sensor Networks. *IEEE Internet Things J.* **2023**, *10*, 5063–5072. [CrossRef]
68. Guo, R.; Xu, L.; Li, X.; Zhang, Y.; Li, X. An Efficient Certificateless Ring Signcryption Scheme With Conditional Privacy-Preserving in VANETs. *J. Syst. Archit.* **2022**, *129*, 102633. [CrossRef]
69. Niu, S.; Shao, H.; Hu, Y.; Zhou, S.; Wang, C. Privacy-Preserving Mutual Heterogeneous Signcryption Schemes Based on 5G Network Slicing. *IEEE Internet Things J.* **2022**, *9*, 19086–19100. [CrossRef]
70. Xie, Z.; Chen, Y.; Ali, I.; Pan, C.; Li, F.; He, W. Efficient and Secure Certificateless Signcryption Without Pairing for Edge Computing-Based Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 5642–5653. [CrossRef]
71. Yang, Y.; Zhang, L.; Zhao, Y.; Choo, K.K.R.; Zhang, Y. Privacy-Preserving Aggregation-Authentication Scheme for Safety Warning System in Fog-Cloud Based VANET. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 317–331. . [CrossRef]
72. Ullah, I.; Khan, M.A.; Khan, F.; Jan, M.A.; Srinivasan, R.; Mastorakis, S.; Hussain, S.; Khattak, H. An Efficient and Secure Multimessage and Multireceiver Signcryption Scheme for Edge-Enabled Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 2688–2697. [CrossRef]
73. Ali, I.; Chen, Y.; Ullah, N.; Afzal, M.; HE, W. Bilinear Pairing-Based Hybrid Signcryption for Secure Heterogeneous Vehicular Communications. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5974–5989. [CrossRef]
74. Altaf, F.; Maity, S. PLHAS: Privacy-preserving localized hybrid authentication scheme for large scale vehicular ad hoc networks. *Veh. Commun.* **2021**, *30*, 100347. [CrossRef]

75. Xiong, W.; Wang, R.; Wang, Y.; Wei, Y.; Zhou, F.; Luo, X. Improved Certificateless Aggregate Signature Scheme Against Collusion Attacks for VANETs. *IEEE Syst. J.* **2023**, *17*, 1098–1109. [CrossRef]
76. Moni, S.S.; Manivannan, D. CREASE: Certificateless and REused-pseudonym based Authentication Scheme for Enabling security and privacy in VANETs. *Internet Things* **2022**, *20*, 100605. [CrossRef]
77. Zheng, H.; Luo, M.; Zhang, Y.; Peng, C.; Feng, Q. A Security-Enhanced Pairing-Free Certificateless Aggregate Signature for Vehicular Ad-Hoc Networks. *IEEE Syst. J.* **2022**, 1–12 . [CrossRef]
78. Sripathi Venkata Naga, S.K.; Yesuraj, R.; Munuswamy, S.; Arputharaj, K. A Comprehensive Survey on Certificate-Less Authentication Schemes for Vehicular Ad hoc Networks in Intelligent Transportation Systems. *Sensors* **2023**, *23*, 2682. [CrossRef] [PubMed]
79. Cahyadi, E.F.; Hwang, M.S. A Comprehensive Survey on Certificateless Aggregate Signature in Vehicular Ad Hoc Networks. *IETE Tech. Rev.* **2022**, *39*, 1265–1276. [CrossRef]
80. Bergström, E.; Lundgren, M.; Ericson, Å. Revisiting information security risk management challenges: A practice perspective. *Inf. Comput. Secur.* **2019**, *27*, 358–372.
81. Lundgren, M. Rethinking capabilities in information security risk management: A systematic literature review. *Int. J. Risk Assess. Manag.* **2020**, *23*, 169–190. [CrossRef]
82. Wangen, G.; Snekkenes, E. A taxonomy of challenges in information security risk management. In Proceedings of the Norwegian Information Security Conference/Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger, Stavanger, Norway, 18–20 November 2013; Akademika Forlag: Bergen, Norway, 2013.
83. Schatz, D.; Bashroush, R.; Wall, J. Towards a more representative definition of cyber security. *J. Digit. Forensics Secur. Law* **2017**, *12*, 8. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.