Optical PUF for *Non-Forwardable* Vehicle Authentication

Shlomi Dolev[a,*], Łukasz Krzywiecki[b,**], Nisha Panwar[a], Michael Segal[c]

[a] *Department of Computer Science, Ben-Gurion University of the Negev, Israel.*
[b] *Institute of Mathematics and Computer Science, Wrocław University of Technology, Poland.*
[c] *Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Israel.*

Abstract

Modern vehicles are configured to exchange warning messages through IEEE 1609 Dedicated Short Range Communication over IEEE 802.11p Wireless Access in Vehicular Environment. Essentially, these warning messages must associate an authentication factor such that the verifier authenticates the message origin via visual binding. Interestingly, the existing vehicle communication incorporates the message forward-ability as a requested feature for numerous applications. On the contrary, a secure vehicular communication relies on a message authentication with respect to the sender identity. Currently, the vehicle security infrastructure is vulnerable to message forwarding in a way that allows an incorrect visual binding with the malicious vehicle, i.e., messages seem to originate from a malicious vehicle due to non-detectable message relaying instead of the actual message sender. We introduce the *non-forwardable authentication* to avoid an adversary coalition attack scenario. These messages should be identifiable with respect to the immediate sender at every hop. According to a coalition attack scenario, the group of adversaries in coalition adopt the fabricated attributes of a target vehicle and resembles it to be alike. The adversaries in coalition then reroute the eavesdropped messages in order to impersonate the target vehicle. We propose to utilize immediate optical response verification in association with the authenticated key exchange over radio channel. These optical response are generated through hardware means, i.e., a certified Physically Unclonable Function device embedded on the front and rear of the vehicle. To the best of our knowledge, this is the first work proposing a solution based on physically unclonable function for a secure *non-forwardable* vehicle to vehicle authentication. In addition a formal correctness sketch is derived using Strand Space methodology.

Keywords: Authentication, certificate, wireless radio channel, optical channel, challenge response pairs, verification.

1. Introduction

Vehicle networks [17, 44, 20] provide safe and efficient maneuvering among the vehicles and across the road. Smart vehicles are equipped with wireless radio devices and comply with

[*] Partially supported by Orange Labs under external research contract number 0050012310-C04021, the Rita Altura Trust Chair in Computer Sciences, Lynne and William Frankel Center for Computer Sciences, and Israel Science Foundation (grant number 428/11).

[**] The research was financed by the Polish National Science Centre decision (DEC-2013/08/M/ST6/00928), project HARMONIA.

Email addresses: dolev@cs.bgu.ac.il (Shlomi Dolev), lukasz.krzywiecki@pwr.wroc.pl (Łukasz Krzywiecki), panwar@cs.bgu.ac.il (Nisha Panwar), segal@cse.bgu.ac.il (Michael Segal)

the Dedicated Short Range Communication (DSRC) IEEE 1609 [1, 8] and Wireless Access in Vehicular Environment (WAVE) 802.11p [55]. Furthermore, vehicles are customized to predict a crash event ahead of time through ultrasonic and infrared radars, detection vs ranging optical-sensors, and a night vision camera [53]. A decentralized multi-channel communication is standardized in IEEE 1609.4 [7]. Our protocol is secure to create an information rich map of the surrounding vehicles and correspondingly attribute these messages (arriving through the radio) to the correct vehicle in the map. Such an up-to-date map would assist in real-time decision making, e.g., accelerating, decelerating, or lane changing. Once the vehicle has established a secure session with a near-by vehicle the map can be updated using the information received over the radio channel, thereby, attributing the responsibility of any malfunctioning.

Wireless radio communication is widely supported by the portable user devices. There exists a sufficient number of Authenticated Key Exchange (AKE) protocols for a secure wireless communication. Interestingly, the majority of these AKE protocols are implemented over the radio channel for identifying a valid public key holder and establishing a session key. However, these approaches do not suffice for a more sophisticated form of a coalition attack. In order to avoid such attacks a correct mapping to the actual vehicle in secret session is necessary. Subsequently, a location-information rich map can provide a precise identification of the original source. Recently, authors in [56] have presented a *far proximity* identification approach by measuring overall multipath propagation effect. Although, it estimates that a specific target is at least a certain distance away (conceptually quite opposite to the existing distance bounding protocols [5]), however, the source of signal origination is still unidentifiable and seems to comply with the certified credentials. In particular, the dispersed nature of the radio signals might impose an incorrect binding between the session messages and the actual source of the message. Our scheme promises a correct binding between the session messages (over a wireless radio channel) and correspondingly identifiable source of the message (certified attribute holder). We propose to achieve a secure *binding property* with respect to vehicles and corresponding communication channels. Vehicles that identify themselves on an auxiliary channel establish a secure communication over another channel, i.e., an optical and radio channel, respectively.

We utilize the (inherently) directed nature of optical channel to produce *optical fingerprints* in association with a secure radio channel. Optical communication (or an equivalent technology for a clear geographic mapping and to identify communicating vehicle monolithically-coupled with the information received) is an important ingredient in our proposed scheme. The directed nature of the optical communication channel eliminates the possibility of an adversary, present in the line of sight between mutually authenticated vehicles. However, the optical communication or directed microwaves alone are not sufficient and requires additional assumptions to enable the existing DSRC IEEE 1609.2 [2] infrastructure immune against a coalition attack, as presented in this paper. Vehicles authenticate a peer vehicle over radio channel to be the same vehicle as visually identified over the optical channel. Our PUF based solution can withstand more sophisticated adversarial coalition attacks than in previous works [11, 10]. We omit a formal proof specification using Strand Space methodology from this extended abstract.

Problem statement. We will consider an adversary coalition attack scenario [10] in vehicle networks. Accordingly, adversaries forward the messages between the intended sender and receiver, without decrypting the messages. Sender and receiver verifies the visual attributes and the location. However, it is difficult to identify whether the intended sender and receiver are present within the communication range or not. Apparently, messages are routed through a group of malicious vehicles that looks similar as the intended sender/receiver. The malicious vehicle might communicate over a separate communication channel. Therefore, the intended sender and receiver that own a valid certificate (binding vehicle attributes and public key) are actually far away from the communication range still connected through an adversary coalition channel. The term adversary coalition denotes the fact that adversary is allowed to forward and re-route messages towards a second adversary via separate channel. The static [11] and dynamic attribute [10] based authentication is not sufficient to avoid the coalition attack scenario. Evidently, a *non-forwardable* authentication technique must be augmented to the static and dynamic schemes. Specifically, the technique should prevent the verifier to visually misidentify the attacker (that only forwards messages) with the original authenticator (that actually produced the authentication messages).

Apparently, some ad-hoc solutions such as timing analysis, radio fingerprinting, regular mirror and holographic mirror identification, potentially seems to immune against the coalition attack scenario. We further elaborate these solutions with respect to the inapplicability against a coalition attack scenario. It must be noticed that the coalition attack is unavoidable within the existing state of vehicle to vehicle security standards IEEE 1609.2 [2]. Interestingly, neither the wireless radio nor the optical communication channel, individually is enough to provide a complete solution against the coalition attack scenario. We require a dynamic scheme for immediate commitment verification that would not remain static for a long time. Our goal is to couple the communicating vehicles within the scope of multiple channels such as an optical and radio channel. An optical channel is essential during the authentication phase and the radio channel resumes beyond the authentication phase for the authenticated message exchange. Therefore, the proposed authentication approach utilizes a non-forwardable fingerprint from the peer vehicle. A Physically Unclonable Function (PUFs) [35] device is used to produce these output responses and a supplementary optical communication is used to convey PUF input and verify PUF output. Consequently, optical PUF assisted *unforgeable fingerprints* provide a robust vehicle identification.

Strawman Solutions. Interestingly, the wireless radio and the optical communication, individually is not enough to provide a complete solution against the coalition attack scenario. The following native solutions might seem to solve the problem but only to a certain extent.

Timing analysis: Optical communication channels have been used recently to measure the dynamic primitives [29, 34] of any moving target. Moreover, a round trip delay measurement for the optical beam is another estimate that assists to verify the partner in communication. Accordingly, the sender estimates that the receiver is not farther then few meters away and therefore should not take more than the threshold time to access. In the existing literature this concept is also known as distance bounding and round trip delay estimation [6]. Thus, the sender and receiver might be assured that the communication is uninterrupted and also point-to-point (in case of optical communication). However, the underlying communication protocols suffer packet loss, congestion and delay over the wireless radio channel. Therefore, the packet round trip time estimation might lead to an incorrect distance estimation. A sufficient number of security protocols are available that might prevent the adversary to fake a lower latency, still, the adversary can fake a larger distance or round trip latency by intentionally delaying the message forwarding. Therefore, it might lead to an incorrect delay or distance estimation among the actual sender and receiver.

Radio fingerprinting: According to the property of wireless radio fingerprinting, radio signals generated at every device must incorporate an unique distinguishable property [46, 45, 4]. Therefore, the radio waves generated at a particular vehicle retains these *consistent* and *unique* traits during every communication interaction. However, the radio fingerprinting approach does not ensure the *non-forwardable* authentication due to the lack of point-to-point communication. The communicating vehicles might not be able to create a mutual visual binding with respect to fingerprints received over the radio channel. Our approach provides this worthy combination of *unforgeable fingerprints* and *visual bindings* with the sender of those fingerprints.

Regular mirrors: An optical communication channel such as laser beam can be used to convey the commitment data through beam modulations. The receiving vehicle must be configured with a reflective mirror on which the laser beam modulations are received and interpreted. Therefore, the commitment data conveyed through point-to-point beam modulation seems to be secure and confidential to the recipient vehicle. However, the reflective mirror does not contribute beyond the beam modulation decoding. In addition, a recipient vehicle cannot distinguish between the beam reflection originated at intended sender or the reflection-of-reflection (reflection originated at the middle adversary, mimicking the original reflection from the intended sender). An adversary nearby can record the laser beam modulations originated from the other vehicle and might also generate the same modulations. Therefore, the beam modulations and the commitment data is vulnerable to subliminal message rerouting and forwarding. Furthermore, there is no binding between the optical and wireless radio channel and is not a complete solution against an adversary coalition attack scenario.

Holograms: A hologram can be installed at the vehicle front and rear surface. The hologram is subjected to an optical beam in order to verify the validity of the hologram and the corresponding vehicle identity. A specific certified hologram would generate a correspondingly unique reflection for every vehicle identity. Apparently, the solutions based on a certified hologram response verification resolves the true vehicle identity and appears to be a quite relevant solution for the attack scenarios into consideration. However, in this solution the hologram retains and processes a specified Challenge Response Pair (CRP) only and the pairing remains fixed for every verification round. Furthermore, a mighty adversary can reveal the CRP by analyzing it over a period of time because the response remains static irrespective of the static and dynamic attributes of the vehicle.

The problem requires a dynamic solution for the immediate commitment verification in which CRPs are not static. Our solution proposed in this paper verifies the immediate processing of an optical beam through an unclonable device known as a Physically Unclonable Function (PUF) [35, 36, 13, 15, 52]. PUFs are hardware devices that are configured to produce a unique response corresponding to a unique and sufficiently diverse challenge. The verifier compares these PUF generated response patterns against the certified response received over the wireless radio channel. The PUF generated spontaneous wireless signatures enable a secure binding between the optical and wireless radio communication channel. Evidently, our PUF based solution is rigorous and resistant towards the above mentioned coalition attack scenario.

Physically Unclonable Function (PUF). The Physically Unclonable function (PUF) was first introduced in [35] as a hardware analogous to the one-way hash functions. We denote the function instated inside the hardware PUF device as $\wp$. Essentially, a PUF is a hardware primitive that represents physical hash functions due to unique physical characteristics. There is no instantiation of any PUF, at least as much intuitive as a mathematical description, except a random oracle model. Specifically, every instantiation of the PUF is considered as another instantiation of a random oracle model. PUF devices are characterized with micro-structural variations. These perplexed structural variations are enforced during the production process, therefore, it is hard to clone the same structural variations. Furthermore, PUFs can be used perfectly in a challenge-response verification protocol. These PUFed responses are correspondingly unique to the paired challenges and are extremely difficult to predict without accessing the original PUF device itself. The essential properties [30, 48] of a basic PUF ($\wp$) are:

- *Unique:* The PUF output is unpredictable due to the unique micro-structural variations. In the existing literature, a PUF device is termed as a physical one-way hash function [35]. Inherently, the CRPs produced by a PUF are uniquely paired and sufficiently diverse to distinguish.
- *Unclonable:* No two PUFs could ever produce same output via cloning. Due to micro-structural

variations it is infeasible to physically clone a PUF. Therefore, the inevitable structural randomness avoids the PUF cloning attacks.

• *Unpredictable:* It is infeasible to predict the consistent response for a random challenge given a set of pre-recorded CRPs. An adversary might stimulate a passive PUF device for a random set of challenges $(c_1, c_2, ...c_\ell)$ and retrieves corresponding responses as $(r_1, r_2, ...r_\ell)$, still it is infeasible to predict a correct response $r_{\ell+1}$ corresponding to an unqueried input challenge $c_{\ell+1}$.

• *One-way:* Given a decoded numeric response r_i and the certified PUF ($\wp$) still it is infeasible to recover the paired challenge c_i that triggered the PUF to generate r_i.

• *Tamper evident:* Any attempt to recover the structural traits of the PUF ($\wp$) would deviate the original structure of $\wp$ and the original challenge-response pairing.

Previous work. According to a PUF authentication scheme [41], an initiator measures the PUFed responses. The responder transmits a shuffled response string that initiator verifies through substring matching. The paper [38] presented a PUF based protocol for secure private-public key pair generation and distribution between Certificate Authority (CA) and vehicles. The authors in [47] presented a challenge-response method to identify the paired device, while both devices are assumed to have a session key. The sender measures the response and receives the same response encrypted with the secret key from the receiver in order to cross verify the measured response. However, to the best of our knowledge, none of these previous works have considered the vehicle coalition attack scenario as a problem. We assume the existence of an out-of-band communication channel [32] to verify the certified static attributes. In [11] a novel vehicle authentication scheme has been proposed which is based on the certified and monolithically-coupled vehicle attributes with the public key. The following work [10] have used a laser communication for additional verification of dynamic attributes is presented. The utility of an auxiliary laser based communication channel regarding the secure device pairing can be found in [31, 24, 33]. It is practically feasible for high speed vehicles to operate laser beams for tracking [29, 50, 34] and secret key establishment [37, 31].

The Physically Unclonable functions (PUF) was first introduced in [35] as a hardware analogous to the one-way hash functions. There are several types of PUFs discussed in literature [36, 15, 14, 16] such as Strong PUFs [36, 15], Controlled PUFs [14], Weak PUFs [16]. There are number of candidates for Strong PUFs implemented on integrated circuits, however, the enhancement in this area is still evolving due to modeling attacks [42]. The proposed scheme utilizes optical PUF as they are secure against cloning [18] and modeling attacks [42]. PUFs are also referred to as Physical Random Functions [13, 15] or Physical One-Way Functions [35, 36], have been used for key establishment [36, 52], identification [36] and authentication [15, 52]. The state-of-art research that ensures the property of unclonability is given in [30, 48]. Moreover, the work in [3] presents the PUF assisted formal security features. A broadcast encryption scheme based on PUF devices is given in [23]. Furthermore, the authors in [39] presented an optical PUF based scheme for challenge-response verification through a manufacturers 2D barcode signature embedded over the PUF device.

Our contribution. In order to mitigate this coalition attack scenario as mentioned in problem-statement and detailed in Section 2, we plan to utilize PUF devices for a *non-forwardable* message authentication that provides:

• *Unique identification:* Vehicles create a visual binding over optical channel through the PUF ($\wp$). The physical challenge stimulus c is processed over an authentic PUF ($\wp$) and spontaneously produces a correspondingly original response r. Therefore, a communicating vehicle can be uniquely identified via PUF verification.

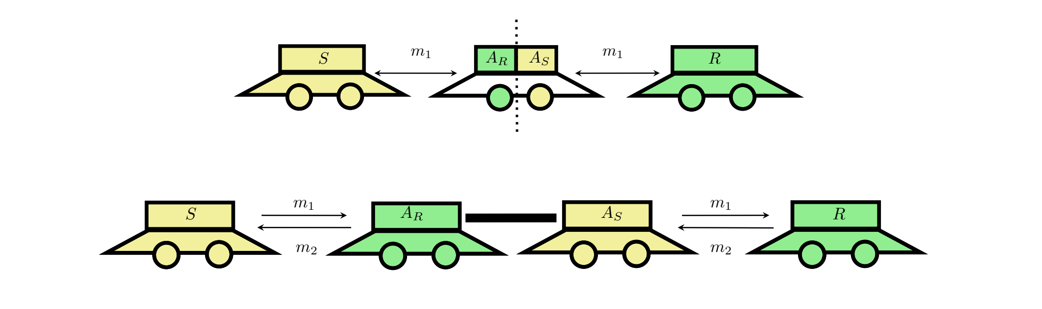

Figure 1: Coalition of adversaries [10].

• *Vehicle authentication:* The AKE execution via certified attributes and the public key over a securely coupled radio channel is an important ingredient in our scheme. Moreover, in this work radio communication is securely coupled with the preliminary optical communication. Thus, the peer vehicle authentication is twofold secure.
• *Non-forwardability:* An adversary cannot forward the messages on behalf of another sender such as without being detected. The sender and the receiver are in direct communication with each other, therefore, the message integrity is ensured.
• *Channel binding:* The sender and receiver create a visual binding through optical communication and establish a secure binding between the wireless radio and optical communication channel. Moreover, the associated AKE protocol enables a secure message exchange over the wireless radio channel.

Outline. Section 2 explains the adversary coalition attack scenario in vehicle to vehicle communication. A detailed description of the PUF assisted vehicle authentication approach is given in Section 3. Security discussion is given in Section 4. A formal correctness proof using Strand Space methodology is given in Section 5. The Section 6 highlights the concluding remarks.

2. Adversary coalition scenario

We provided a solution for the coalition attack scenario as discussed in [10] (see Figure 1). According to the coalition attack scenario, there exists two or more malicious vehicles between the intended sender and the receiver. One of these malicious vehicles impersonates the sender and the other impersonates the receiver by carrying exactly similar static attributes. Moreover, these malicious vehicles communicate over a separate communication channel to relay the acquired messages and coordinate the attack during AKE execution. Although malicious vehicles may not be able to decipher the messages it still can create an illusion of correct visual bindings. The sender believes that it has forwarded the message to the receiver while actually forwarding it to one of the malicious vehicles impersonating the receiver and vice versa. The first scenario in Figure 1 illustrates an adversary in the middle possessing fake visible attributes of both S and R. Therefore, the adversary might forward the message m_1 between S and R through visual misbinding. As the sender S believes A_R to be the actual recipient of the message m_1. However, it is very unlikely that an adversary represents both A_S and A_R in order to impersonate S and R, respectively. It is analogues to the scenario with one vehicle carrying multiple kind of attributes in order to impersonate multiple vehicles at the same time. Nevertheless, the second scenario in Figure 1 illustrates the adversary coalition attack scenario, in which adversaries A_S and A_R communicate over an additional channel and relay the messages m_1 (from sender S) and m_2 (from

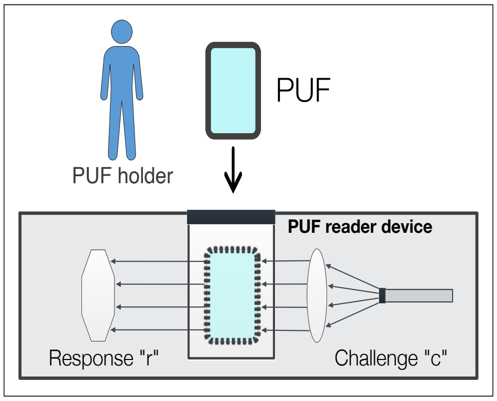

Figure 2: Authorization via PUF device.

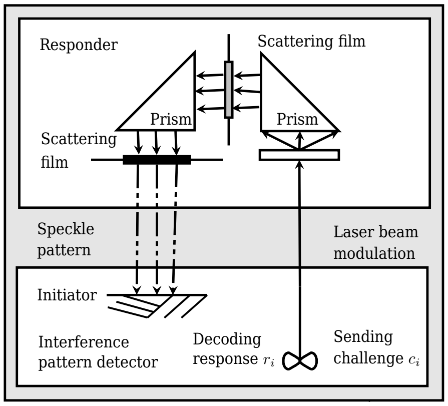

Figure 3: Optical PUF assisted response verification.

recipient R) between S and R (S and R having an illusion of correct visual binding), without deciphering those messages. As a result of which S misinterprets A_R as R and R misinterprets A_S as S. Essentially, the unpredictable but consistent responses produced by a PUF ($\wp$) provides a necessary and sufficient condition to avoid the coalition attack.

3. Physical unclonable function assisted authentication

Regular setup. In a regular setup the optical PUF can have a form of a user card with a transparent film. The film itself is neither crystal-clear nor super smooth. Instead it is covered with a random micro-roughness introduced during its production (e.g. the film is sprayed with micro particles that enables a micro-structural variation over the outer surface). A user authentication requires the user to insert the PUF card into the reader. Then the laser beam, modulated according to the recoded i-th challenge c_i, goes through the film, and the resulting scattered speckle s_i is captured on a photo-diode surface of the reader (see Figure 2). The conventional usage of PUF in the authorization process is divided into two phases:

Setup phase:
- A PUF device ($\wp$) is tested against the vector of challenges $\mathrm{C} = (c_1, c_2, ...c_i, ...c_n)$ and outputs the corresponding vector of responses $\mathrm{R} = (r_1, r_2, ...r_i, ...r_n)$, where n is the size of the vector.
- The PUF device ($\wp$) is handed to the user.

Authentication phase:
- A PUF holder inserts the PUF ($\wp$) into the PUF reader.
- The PUF ($\wp$) is stimulated with the challenge c_i via beam modulation.
- If the answer from the PUF ($\wp$) is equal to the certified response r_i (previously stored or immediately known through the other channel) then the authenticator is accepted.

Vehicles setup. We adapt the regular PUF setup (see Figure 3) for PUF based vehicle authentication. Thus, sender and receiver both are allowed to be distant and the unique responses can be verified through the PUF stimulation.
- The part of the reader device made of the PUF slot (with the PUF inserted inside) and the necessary optics are mounted into the prover vehicle as the authenticator's part.
- The part of the PUF stimulator is made of the laser/Light Emitting Diodes (LEDs) (with respect to indoor vs outdoor applications) and the photo-diode surface verifies the unclonable fingerprints of the prover which must be hardwired to the non-replaceable parts of the vehicle.

$\hat{A}$	Sender	$\hat{B}$	Receiver
$Cert_{\hat{A}}$	Certificate of sender	$Cert_{\hat{B}}$	Certificate of receiver
C	Challenge vector	R	Response vector
c	Challenge bit	r	Numeric response
m	Beam modulation	q	finite number of attempts
S	Speckle response vector	s	Speckle response
I	Initiator vehicle	R	Responder vehicle
t	Active time slot	$Attribute$	Physical static parameters of vehicle
x	Ephemeral secret key of $\hat{A}$	y	Ephemeral secret key of $\hat{B}$
X	Ephemeral public key of $\hat{A}$	Y	Ephemeral public key of $\hat{B}$
a	Static secret key of $\hat{A}$	b	Static secret key of $\hat{B}$
A	Static public key of $\hat{A}$	B	Static public key of $\hat{B}$
f	Function to convert challenge bits	w	Function to convert speckles
H	Public hash algorithm	k	Session key
G	Cyclic group of prime order	ρ	negligible constant
$\mathcal{R}$	Registration authority	$\wp$	Unclonable mathematical function

Table 1: Notations.

Notations. Notations are given in Table 1.

Overview. Initially, communicating vehicles utilize laser and PUF devices for identification purposes. The interaction between a modulated laser beam and the PUF device is to convey the challenge bits. The whole protocol construction utilizes secure binding between the wireless radio and optical communication channel. Consider that every vehicle is configured with a certificate from trusted authorities. The authorities sign the public key of the vehicle along with the additional relevant primitives such as visible static attributes of the vehicle, validity period, sequence number and procedure to verify the signed visible static attributes. Interested readers may refer to [11] for further details about the certificate structure and visible static attributes. The certificate encompasses nonpolitically coupled vehicle public key and static attributes. Therefore, certificates are primarily used for the vehicle authentication and session key derivation. After the completion of an unique vehicle (PUF holder) identification over optical channel and AKE execution over radio channel, both vehicles may switch on to a secure wireless radio session.

Assumptions and settings.

• Vehicles possess a certified PUF from the trusted party.

• Vehicles store certified coupled CRPs in a non-volatile tamper proof memory to ensure the confidentiality.

• The certificate consists of CRPs, visual static attributes such as license number, brand, identification number, public key and validity period as $Cert(c_{i,\hat{A}}, r_{i,\hat{A}}, Attribute_{\hat{A}}, \hat{A}, A, t_{val})$, henceforth, we have used an abstract term $Cert(c_i, r_i)$.

• Certificates are discarded after the one-time use or beyond the validity time t_{val} whichever is earlier. Whereas, the adversary requires at least t_{adv} time to fabricate a specifically queried CRP, exactly as the original PUF would have done.

• The difference between the CRP validity time t_{val} and the current time t_{cur} must be lesser than the time t_{adv}.

Considering the rapid evolution and connectivity among Internet of Things (IoT), modern vehicles are expected to survive longer (physically) but the embedded firmware and crypto-counters inside would be refreshed for every 2-5 years approximately (depending on miles covered). Therefore, we consider the vehicle lifetime in terms of average duration required to upgrade internal firmware and restart crypto-counters.

• In the proposed approach, CRP validity time t_{val} is relaxed to be semi-synchronized and allows a clock drift by $(\pm t_{diff})$ (with respect to the current time). However, we consider a worst case scenario where the PUF modeling attack should be infeasible even in as much time as $|t_{val} - t_{cur} + t_{diff}|$.

- We assume a challenge input to PUF ($\wp$) through an optical medium. The light beam modulation m_i is derived through a deterministic function f that converts the numeric challenge c_i into modulation pattern, denoted as $f(c_i) \rightarrow m_i$.
- The input for an optical PUF ($\wp$) is a modulated light beam m_i and the corresponding output is a scattered speckle response s_i, denoted as $\wp(m_i) \rightarrow s_i$.
- The output s_i from an optical PUF ($\wp$) is captured via photo-diode surface at the receiver and decoded into numeric value r_i, denoted as $w(s_i) \rightarrow r_i$. Importantly, the specialized optical screen distinguishes between the original 3d-speckles and the relayed 2d-image of speckles.

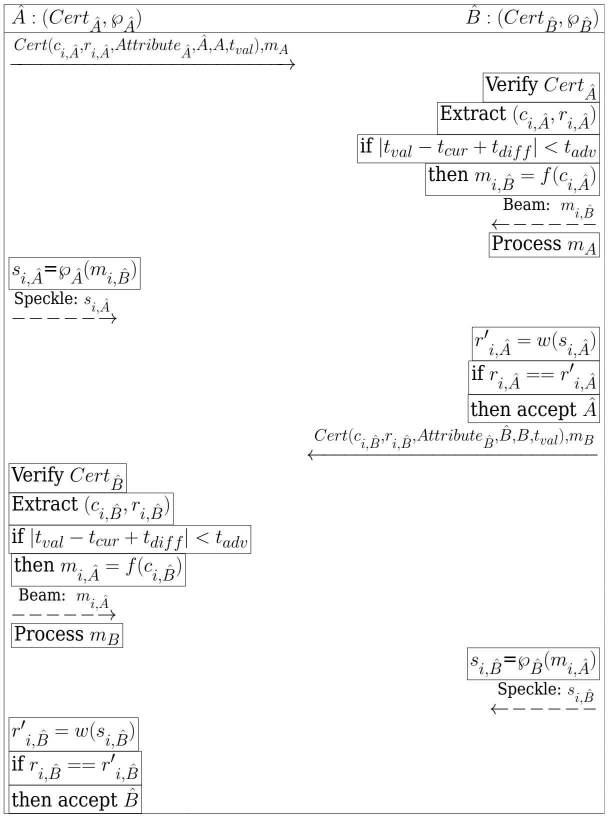
$\hat{A} : (Cert_{\hat{A}}, \wp_{\hat{A}})$
$\hat{B} : (Cert_{\hat{B}}, \wp_{\hat{B}})$
$Cert(c_{i,\hat{A}}, r_{i,\hat{A}}, Attribute_{\hat{A}}, \hat{A}, A, t_{val}), m_A$
Verify $Cert_{\hat{A}}$
Extract $(c_{i,\hat{A}}, r_{i,\hat{A}})$
if $|t_{val} - t_{cur} + t_{diff}| < t_{adv}$
then $m_{i,\hat{B}} = f(c_{i,\hat{A}})$
Beam: $m_{i,\hat{B}}$
Process m_A
$s_{i,\hat{A}} = \wp_{\hat{A}}(m_{i,\hat{B}})$
Speckle: $s_{i,\hat{A}}$
$r'_{i,\hat{A}} = w(s_{i,\hat{A}})$
if $r_{i,\hat{A}} == r'_{i,\hat{A}}$
then accept $\hat{A}$
$Cert(c_{i,\hat{B}}, r_{i,\hat{B}}, Attribute_{\hat{B}}, \hat{B}, B, t_{val}), m_B$
Verify $Cert_{\hat{B}}$
Extract $(c_{i,\hat{B}}, r_{i,\hat{B}})$
if $|t_{val} - t_{cur} + t_{diff}| < t_{adv}$
then $m_{i,\hat{A}} = f(c_{i,\hat{B}})$
Beam: $m_{i,\hat{A}}$
Process m_B
$s_{i,\hat{B}} = \wp_{\hat{B}}(m_{i,\hat{A}})$
Speckle: $s_{i,\hat{B}}$
$r'_{i,\hat{B}} = w(s_{i,\hat{B}})$
if $r_{i,\hat{B}} == r'_{i,\hat{B}}$
then accept $\hat{B}$

Figure 4: The generalized approach.

3.1. Proposed approach

Optical PUF based vehicle identification in association with a simultaneously executing AKE protocol (over the conventional radio channel), is the essence of the proposed approach. The radio channel must enable a secure session key establishment in association with the response verification over the optical channel. It provides a secure binding between the radio channel (with session establishment) and optical channel (with immediate response verification).

Definition 1. *Physically Unclonable Function (PUF): is a physical device that realizes a one-way, collision resistant hash function corresponding to an unique underlying mathematical description. The PUF executes as a separate instance of random oracle model. Each input to a PUF device* *yields a sufficiently diverse output and it is nearly impossible to trace back the specific input value from any given output value.*

The relative variation in each response, corresponding to each challenge is denoted as ε. Therefore, this output response divergence is the parameter to ensure the physical one-way property. We consider the term *sufficiently diverse* in terms of an underlying mathematical function that denotes a surjective (onto) mapping as $\wp : \mathrm{C} \rightarrow \mathrm{R} : \wp(c_i) = r_i$; such that the C domain is large and there exists multiple responses for corresponding challenges at least ε distance apart. Henceforth, any i-th numeric challenge, modulation, speckles and numeric response are denoted as c_i, m_i, s_i, r_i, respectively.

Setup: In this phase we demonstrate the vehicle identification procedure using unclonable devices and the certified credentials such as challenge, response, attributes, identity, public key and validity period. In Figure 4 the regular and dashed arrows denote messages over the wireless radio channel and optical channel, respectively. Also, equations in the boxes are the respective computations on both sides (see Table 1 for notations). The certificate exchange over the wireless radio channel allows the recipient to use a valid CRP for the current active time slot. The recipient uses the certified CRP for PUF stimulation and verification of the correspondingly measured response over the optical channel. However, a vehicle might not be able to locate the corresponding PUF device for which the certificate is available over the wireless radio channel. Therefore, it is necessary to accompany the certificate transmission with visible static attributes of the certificate sender. Thus, the certificate recipient knows a current valid challenge for PUF stimulation and also the location of the PUF device that must be stimulated using that challenge.

Vehicles are configured with a static public key in a tamper proof storage. W.l.o.g. we assume that the AKE protocol via radio channel and optical PUF assisted out-of-band channel are based on regular Diffie-Hellman (DH) [9] key exchange over a secure group $G = \langle g \rangle$. Also the Decisional Diffie-Hellman (DDH) and Computational Diffie-Hellman (CDH) assumption holds. Accordingly, a discrete logarithm function over the DH public values is computationally hard within the cyclic group G. Consider that vehicle $\hat{A}$ is configured with the static public key $A = g^a$ and the PUF $\wp_{\hat{A}}$. Similarly, vehicle $\hat{B}$ has long term public key $B = g^b$ and the PUF $\wp_{\hat{B}}$, here a and b are static secret keys, respectively.

Registration: This phase enables a periodic registration of the vehicles by the assigned authorities. Registration authority $\mathcal{R}$ with the secret key $SK_{\mathcal{R}}$ coins a pseudorandom set of challenges $(c_1, c_2, ...c_i, ...c_n)$ and corresponding responses $(r_1, r_2, ...r_i, ...r_n)$ for the current registration period. Furthermore, while registering vehicle $\hat{A}$, authority $\mathcal{R}$ processes a set of c_i with the configured $\wp_{\hat{A}}$ and obtains a uniquely paired response. In addition, $\mathcal{R}$ certifies these processed challenges and paired numeric responses as $Cert_{\hat{A}}(c_{i,\hat{A}}, r_{i,\hat{A}})$ and configures the vehicle to use these certified CRPs during the authentication phase. For example, $\mathcal{R}$ stores the n number of valid certificates $Cert_{\hat{A}}(c_{1,\hat{A}}, r_{1,\hat{A}}), Cert_{\hat{A}}(c_{2,\hat{A}}, r_{2,\hat{A}}), ...Cert_{\hat{A}}(c_{i,\hat{A}}, r_{i,\hat{A}}),\ ...Cert_{\hat{A}}(c_{n,\hat{A}}, r_{n,\hat{A}})$ of the vehicle $\hat{A}$ on a SD card.

Authentication and session key exchange: This phase considers the interaction among the moving vehicles after the registration and certificate configuration is complete. Vehicles possess certified CRPs of their own PUF device which would be used by the peer vehicle for this PUF stimulation. These certified pairs are used for an immediate response verification within the active time interval. The additional certified parameters are used during the session key establishment.

For example, $\hat{A}$ sends the certificate as $Cert(c_{i,\hat{A}}, r_{i,\hat{A}}, Attribute_{\hat{A}}, \hat{A}, A, t_{val})$ with message m_A over the wireless radio channel. It must be noticed that the message abbreviations m_A and m_B denote the public exponents for key derivation and are processed as per the underlying AKE protocol. Next, $\hat{B}$ receives the certificate $Cert_{\hat{A}}$ and message m_A over the radio channel. $\hat{B}$ extracts the CRP $(c_{i,\hat{A}}, r_{i,\hat{A}})$ from certificate $Cert_{\hat{A}}$ and verifies the validity period as $|t_{val} - t_{cur} + t_{diff}|< t_{adv}$. Vehicle $\hat{B}$ with the public key B stimulates the PUF $\wp_{\hat{A}}$ embedded on the target vehicle $\hat{A}$ using the certified challenge and corresponding beam modulations such as $m_{i,\hat{B}} = f(c_{i,\hat{A}})$. Subsequently, PUF $\wp_{\hat{A}}$ processes the challenge modulation $m_{i,\hat{B}}$ as $s_{i,\hat{A}} = \wp_{\hat{A}}(m_{i,\hat{B}})$. $\hat{B}$ records the optical speckle response $s_{i,\hat{A}}$ from $\wp_{\hat{A}}$ and decodes into the numeric response $r'_{i,\hat{A}} = w(s_{i,\hat{A}})$. The verifier compares this decoded numeric response $r'_{i,\hat{A}}$ over the optical channel with the certified response $r_{i,\hat{A}}$ over the radio channel. After the response verification, $\hat{B}$ accepts $\hat{A}$ as an authentic peer vehicle. Meanwhile, $\hat{B}$ processes the message m_A according to the AKE exponents. Thus, $\hat{B}$ creates a binding between the PUF generated response $r'_{i,\hat{A}}$ and the certified response $Cert_{\hat{A}}(r_{i,\hat{A}})$.

Concurrently, $\hat{B}$ sends the certificate $Cert(c_{i,\hat{B}}, r_{i,\hat{B}}, Attribute_{\hat{B}}, \hat{B}, B, t_{val})$ with the message m_B over the wireless radio channel. Next, $\hat{A}$ receives the certificate $Cert_{\hat{B}}$ and message m_B over the radio channel. Furthermore, $\hat{A}$ extracts the CRP $(c_{i,\hat{B}}, r_{i,\hat{B}})$ from certificate $Cert_{\hat{B}}$ and verifies the validity period as $|t_{val} - t_{cur} + t_{diff}|< t_{adv}$. Vehicle $\hat{A}$ with the public key A stimulates the PUF $\wp_{\hat{B}}$ embedded on target vehicle $\hat{B}$ using the certified challenge and corresponding beam modulations such as $m_{i,\hat{A}} = f(c_{i,\hat{B}})$. Consequently, PUF $\wp_{\hat{B}}$ processes the challenge modulation $m_{i,\hat{A}}$ as $s_{i,\hat{B}} = \wp_{\hat{B}}(m_{i,\hat{A}})$. $\hat{A}$ records the optical speckle response $s_{i,\hat{B}}$ from $\wp_{\hat{B}}$ and decodes into the numeric response $r'_{i,\hat{B}} = w(s_{i,\hat{B}})$. The verifier compares this decoded numeric response $r'_{i,\hat{B}}$ over the optical channel with the certified response $r_{i,\hat{B}}$ over the radio channel. After the response verification, $\hat{A}$ accepts $\hat{B}$ as an authentic peer vehicle. $\hat{A}$ processes the message m_B according to the AKE exponents. Thus, $\hat{A}$ creates a binding between the PUF generated response $r'_{i,\hat{B}}$ and the certified response $Cert_{\hat{B}}(r_{i,\hat{B}})$.

3.2. Adaptation with existing authentication protocols

Our proposed approach promises a binding between the wireless radio communication channel and the auxiliary optical authentication channel. There exists plenty of two round authentication protocols that enable secure session key derivations, e.g., CMQV [54], SMQV [43], NAXOS [25], NAXOS+ [27], SIGMA [21]. These approaches are proven to be secure in the CK and eCK models recently. Therefore, w.l.o.g. we demonstrate the binding between the proposed approach and the existing AKE such as CMQV.

Binding with CMQV: The example sequence of messages and computation on both sides are shown in Figure 5. Binding for the two authentication channels can be summarized as below:

- A Radio channel for establishing a secure session through AKE, i.e., CMQV.
- An Optical channel for PUF identification and visual binding.

Vehicle $\hat{A}$ and $\hat{B}$ coins the corresponding static public key such as $A = g^a$ and $B = g^b$ using the static secret key a and b, respectively. We are binding proposed approach with the existing CMQV authentication protocol over a wireless radio channel. Accordingly, initiator $\hat{A}$ derives a session identifier $s(I, \hat{A}, \hat{B}, X, *)$ where I denotes the initiator vehicle, X denotes the ephemeral public key and $*$ denotes that a corresponding ephemeral public key from responder is required to complete the session. $\hat{A}$ switches onto the wireless radio channel and forwards the certified CRPs along with the attributes, sender identity, static public key, validity period, recipient identity and the ephemeral public key as $Cert(c_{i,\hat{A}}, r_{i,\hat{A}}, Attribute_{\hat{A}}, \hat{A}, A, t_{val}), (\hat{B}, \hat{A}, X)$. After the CRP extraction $(c_{i,\hat{A}}, r_{i,\hat{A}})$ from the certificate $Cert_{\hat{A}}$ and the validity period verification

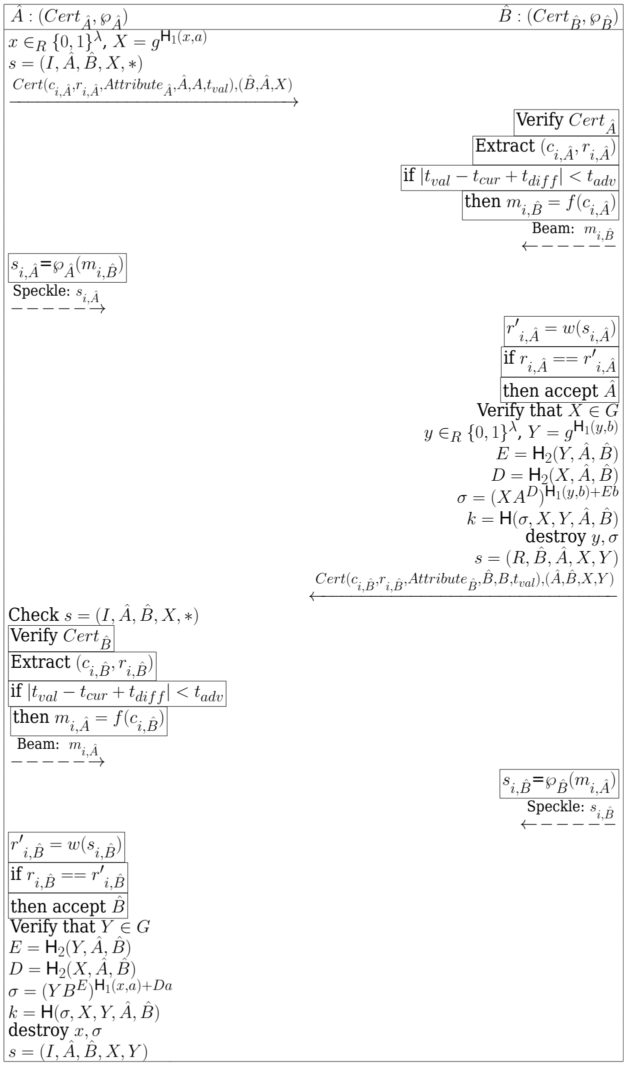
$\hat{A} : (Cert_{\hat{A}}, \wp_{\hat{A}})$
$\hat{B} : (Cert_{\hat{B}}, \wp_{\hat{B}})$
$x \in_R \{0,1\}^\lambda$, $X = g^{\mathsf{H}_1(x,a)}$
$s = (I, \hat{A}, \hat{B}, X, *)$
$Cert(c_{i,\hat{A}}, r_{i,\hat{A}}, Attribute_{\hat{A}}, \hat{A}, A, t_{val}), (\hat{B}, \hat{A}, X)$
Verify $Cert_{\hat{A}}$
Extract $(c_{i,\hat{A}}, r_{i,\hat{A}})$
if $|t_{val} - t_{cur} + t_{diff}| < t_{adv}$
then $m_{i,\hat{B}} = f(c_{i,\hat{A}})$
Beam: $m_{i,\hat{B}}$
$s_{i,\hat{A}} = \wp_{\hat{A}}(m_{i,\hat{B}})$
Speckle: $s_{i,\hat{A}}$
$r'_{i,\hat{A}} = w(s_{i,\hat{A}})$
if $r_{i,\hat{A}} == r'_{i,\hat{A}}$
then accept $\hat{A}$
Verify that $X \in G$
$y \in_R \{0,1\}^\lambda$, $Y = g^{\mathsf{H}_1(y,b)}$
$E = \mathsf{H}_2(Y, \hat{A}, \hat{B})$
$D = \mathsf{H}_2(X, \hat{A}, \hat{B})$
$\sigma = (XA^D)^{\mathsf{H}_1(y,b)+Eb}$
$k = \mathsf{H}(\sigma, X, Y, \hat{A}, \hat{B})$
destroy y, σ
$s = (R, \hat{B}, \hat{A}, X, Y)$
$Cert(c_{i,\hat{B}}, r_{i,\hat{B}}, Attribute_{\hat{B}}, \hat{B}, B, t_{val}), (\hat{A}, \hat{B}, X, Y)$
Check $s = (I, \hat{A}, \hat{B}, X, *)$
Verify $Cert_{\hat{B}}$
Extract $(c_{i,\hat{B}}, r_{i,\hat{B}})$
if $|t_{val} - t_{cur} + t_{diff}| < t_{adv}$
then $m_{i,\hat{A}} = f(c_{i,\hat{B}})$
Beam: $m_{i,\hat{A}}$
$s_{i,\hat{B}} = \wp_{\hat{B}}(m_{i,\hat{A}})$
Speckle: $s_{i,\hat{B}}$
$r'_{i,\hat{B}} = w(s_{i,\hat{B}})$
if $r_{i,\hat{B}} == r'_{i,\hat{B}}$
then accept $\hat{B}$
Verify that $Y \in G$
$E = \mathsf{H}_2(Y, \hat{A}, \hat{B})$
$D = \mathsf{H}_2(X, \hat{A}, \hat{B})$
$\sigma = (YB^E)^{\mathsf{H}_1(x,a)+Da}$
$k = \mathsf{H}(\sigma, X, Y, \hat{A}, \hat{B})$
destroy x, σ
$s = (I, \hat{A}, \hat{B}, X, Y)$

Figure 5: Binding optical PUF verification with CMQV over radio channel.

as $|t_{val} - t_{cur} + t_{diff}| < t_{adv}$, $\hat{B}$ directs the laser beam towards the initiator $\hat{A}$ and forwards the challenge bits $f(c_{i,\hat{A}})$ through the beam modulation $m_{i,\hat{B}}$. At the initiator $\hat{A}$, $\wp_{\hat{A}}$ processes the beam modulations $m_{i,\hat{B}}$ and generates a speckle response as $s_{i,\hat{A}} = \wp_{\hat{A}}(m_{i,\hat{B}})$. Vehicle $\hat{B}$ records the speckle response and decodes a numeric response as $r'_{i,\hat{A}} = w(s_{i,\hat{A}})$. The verifier must compare this decoded numeric response $r'_{i,\hat{A}}$ over optical channel with the certified response $r_{i,\hat{A}}$ over radio channel. After the response verification, $\hat{B}$ accepts $\hat{A}$ as authentic peer vehicle and derives a session identifier $s(R, \hat{A}, \hat{B}, X, Y)$ where R and Y denotes the responder vehicle and corresponding ephemeral public key.

Consequently, $\hat{B}$ switches onto the wireless radio channel and forwards the certified CRP along with the certified attributes, sender identity, static public key, validity period, recipient identity and ephemeral public key as $Cert(c_{i,\hat{B}}, r_{i,\hat{B}}, Attribute_{\hat{B}}, \hat{B}, B, t_{val}), (\hat{A}, \hat{B}, X, Y)$. After the

Protocols	**Iteration cost**	**Efficiency**	**Assumptions**	**Property**
Proposed	2	1	CDH+OoB	Identity binding+ Non-forwardable AKE
HMQV [26, 22]	3	2.5	GDH+CK	wPFS+KCI+AKE
CMQV [54]	3	3	GDH+eCK	wPFS+KCI+LEP+AKE
SMQV [43]	3	2.5	GDH+seCK	Session leakage resilience +AKE

Table 2: Comparison.

CRP extraction $(c_{i,\hat{B}}, r_{i,\hat{B}})$ from the certificate $Cert_{\hat{B}}$ and the validity period verification as $|t_{val} - t_{cur}| < t_{adv}$, $\hat{A}$ directs the laser beam towards the $\hat{B}$ and forwards the challenge bits $f(c_{i,\hat{B}})$ through beam modulation $m_{i,\hat{A}}$. At $\hat{B}$, $\wp_{\hat{B}}$ processes the beam modulations $m_{i,\hat{A}}$ and generates a speckle response as $s_{i,\hat{B}} = \wp_{\hat{B}}(m_{i,\hat{A}})$. Vehicle $\hat{A}$ records the speckle response and decodes the numeric response as ${r'}_{i,\hat{B}} = w(s_{i,\hat{B}})$. The verifier must compare this decoded numeric response ${r'}_{i,\hat{B}}$ over the optical channel with the certified response $r_{i,\hat{B}}$ over radio channel. After the response verification, $\hat{A}$ accepts $\hat{B}$ as authentic peer vehicle and completes the session identifier as $s(I, \hat{A}, \hat{B}, X, Y)$.

$\hat{A}$ and $\hat{B}$ can verify the certified response on the wireless radio channel and the corresponding optical response over the laser channel. The initiator derives a secret exponent E and the receiver derives a secret exponent D by using a publicly known hashing algorithm H_2, identities $(\hat{A}, \hat{B})$ and ephemeral public keys (X, Y). Hence, both parties generate an intermediate secret σ and derive the session key k by using a publicly known hashing algorithm H. Both parties destroy σ and corresponding ephemeral secret keys (x, y) after the session key derivation. The ephemeral secret key x is the random string drawn from the set $\{0, 1\}$ of finite length λ.

In Table 2 a protocol comparison have been shown. The first column *iteration cost* illustrates the number of rounds required in total. All of these protocols in comparison assume the distribution of corresponding public keys as part of pre-processing. Also that this distribution is secure. The actual session establishment requires only two rounds for all of these protocols. Therefore, this column inherently includes at least one more round to process the public key, for all of these protocols. Hence in total at least 3 iterations are required for the public key processing followed by the session establishment. Next, *efficiency* is based on a naive count of exponentiations required at both parties. The *assumptions* explain the assumed model for these protocols. The last column *property* mentioned the specific properties satisfied undre the assumed model.

4. Security Discussion

Considering the uncertain factors of the future communication technology and potential physical attacks that might not be feasible currently, we model the adversarial activity from a future point of view. For example an adversary having access over the PUF device can stimulate it against random challenges. Furthermore, assuming that a *mighty* adversary retrieves certified challenges that is valid for a future interval t_{val}. Then extracts PUF'ed responses corresponding to these retrieved challenges and produces (off-line) equivalent PUF device that generates same CRPs as recovered on-line. Apparently, CRPs must remain confidential until the active time period has arrived. In addition, we consider a time parameter t_{adv} that represents a lower bound on the PUF cloning attack. We assume that PUF modeling in a time fewer than t_{adv} is negligible w.r.t. a security parameter ϵ. The modeling attack is analogous to producing a forged hologram that clones the static CRP of an original hologram. However, a mighty adversary may succeed in modeling the PUF device (for which a few transcripts are known) in a carefully prepared laboratory environment. Apparently, it is difficult to attack an ongoing session in any ad-hoc scenario. Since the existing AKE protocols avoids an active impersonation. Moreover, these protocols neither prevent a message forwarding nor create a visual binding.

In addition, we consider that the peer vehicles exchange only the currently active CRP's during any session. An authorization session should utilize challenges that are not publicly known (not known to the attacker) beyond t_{val}. Therefore, we restrict CRPs to be confidential and vehicles spontaneously acquire the current (not older validity period ${t'}_{val}$) certified CRP over the wireless radio channel. Every vehicle possesses a confidential and pre-certified list of CRPs and discloses it on an immediate interaction request from a peer vehicle. Next, we define the authentication process for vehicles in communication. These vehicles are pre-configured to own an authentic PUF device and certificate (that provides a monolithic binding between public key and static attributes).

Definition 2. *Binding definition:*
• *the initiator vehicle $\hat{A}$ "visualize" and "communicate" to the responder $\hat{B}$ provided: $\hat{A}$ identifies $\wp_{\hat{B}}$. $\hat{B}$ is the holder of the certified public key B. $\hat{A}$ successfully completes AKE protocol with $\hat{B}$ over wireless radio channel.*
• *the responder vehicle $\hat{B}$ "visualize" and "communicate" to the initiator $\hat{A}$ provided: $\hat{B}$ identifies $\wp_{\hat{A}}$. $\hat{A}$ is the holder of the certified public key A. $\hat{B}$ successfully completes AKE protocol with $\hat{A}$ over wireless radio channel.*

The binding property, in definition 2, describes the requirements for a secure association between the key exchange via radio channel and the visual identification via an auxiliary optical communication channel. The following properties hold after a successful protocol termination.
• *Visual binding:* both vehicles have accomplished a successful visual connection within the proximity via optical beam.
• *Secure session key derivation:* both vehicles compute the same session key k. Also the session keys are unique for each session and immune to ephemeral secret leakage (and other similar functionalities as in ECK model).

Subsequently, initiator and responder are assured that the key exchange over wireless radio channel and the mutual identification over optical channel is uniquely mapped. The binding property relies on PUF security therefore to be precise we formulate a set of assumptions. The first assumption is similar to as presented in [23].

Assumption 1 (PUF uniqueness). *Each physically unclonable function device $\wp$ realizes a separate and distinct instance of the random oracle model analogous to a hash function.*

• There is a separate table of input-output pairs (m_i, s_i) associated with each PUF device. That is initialized on its first run, empty at the end of the production stage, and maintained throughout its lifetime. Every time the PUF is tested upon a new distinct input, it returns a new random output and the pair is stored in its table. For inputs previously queried the outputs are consistent with the pairs recorded in the table.
• The optical speckle patterns are unpredictable, unless a specific challenge is processed with the correct authentic PUF to generate the spontaneous interference pattern.
• The PUF cannot be cloned in a way that responses for unqueried inputs would be consistent between the clones.

We assume that the sensor is tuned to capture only the predefined physical characteristics of the scattered speckle in an ad-hoc manner and within the validity time period, i.e., $t_val < t_{adv}$. It is important to mention that the speckle s_i is a physical characteristic of the scattered light (rather than a "flat" two dimensional image). It is analogous to processing the hologram versus processing a "photo" of the hologram for example taken through a regular camera. We formulate the following assumption:

Assumption 2 (PUF Non-forward-ability). *For a given PUF process $\wp$:*

$$c_i, m_i \leftarrow f(c_i),\ s_i \leftarrow \wp(m_i),\ r_i \leftarrow w(s_i)$$

no adversary re-route the $\wp$'s output s_i without possessing original $\wp$ over the respective challenge $m_i \leftarrow f(c_i)$, due to physical characteristics of $\wp$ and s_i.

An attack without the original PUF that produced s_i for the corresponding m_i is negligible in a *reasonable time interval* t_{val}. The term *reasonable time interval* refers to the attack model that allows the attacker to reproduce such an scattered optical speckles s_i's for paired response r_i's in carefully prepared laboratory environment, however, these attacks are considered as infeasible in real life ad-hoc scenarios.

Assumption 3. *No attacker, accessing a specific PUF device and collecting at most ℓ pairs $C = ((c_1, r_1), (c_2, r_2), \ldots (c_i, r_i), \ldots (c_\ell, r_\ell))$, while c_i chosen as per adversary's knowledge, can produce another PUF' within time t_{adv}). Such that PUF' would output the same response as the original PUF, for a specific queried challenge c_j from the set of ℓ pairs. We formalize the following experiment:*

```
Experiment $\mathbf{Exp}_{\mathcal{A}}^{t_{adv},model}$
    let $(c_1, r_1), (c_2, r_2) \ldots (c_i, r_i), \ldots (c_\ell, r_\ell) \leftarrow \mathcal{A}(PUF)$
    generate $c_j$ at random
    $PUF' \leftarrow \mathcal{A}(t_{adv}, C)$
    if ($PUF'(c_j) == PUF(c_j)$)
        return 1
    else return 0
```

the advantage of the adversarial algorithm $\mathcal{A}$ in experiment $\mathbf{Exp}_{\mathcal{A}}^{t_{adv},model}$ is negligible with the probability $\Pr[\mathbf{Exp}_{\mathcal{A}}^{t_{adv},model} = 1] \leq \epsilon_{t_{adv},model}$.

It is mentioned earlier that the certificate consists of a CRP and corresponding validity period. We presume that certificates cannot be forged and are stored in a tamper evident non-volatile memory. Apparently, CRPs must remain confidential and the vehicles must spontaneously acquire the current certified CRP via radio channel. Therefore, peer vehicles cannot access a CRP in advance which is certified for any future interval. Otherwise an adversary that has access over unqueried input challenges for distant future, might use them to stimulate a passive PUF device (e.g. while the vehicle is in parking or in garage), and eventually might launch a successful attack for the certified PUF device.

Now we formulate the experiment, which allows us to state the security of authentication via radio and optical channel binding. W.l.o.g. we set the experiment for initiator authentication.

Definition 3. *We consider the experiment of running an adversary algorithm $\mathcal{A}$ with public keys of parties (I, R) as input. $\mathcal{A}$ is given access to PUF_I for collecting at most ℓ CRP pairs $C = (c_1, r_1), (c_2, r_2), \ldots (c_i, r_i), \ldots (c_\ell, r_\ell)$ and observing at most q transcripts $T = (T_1, T_2, \ldots T_i, \ldots T_q)$, while c_i chosen randomly. Adversary tries to be authenticated (over radio channel) and identified (over optical channel) as I in front of R, during a future session 'k'.*

```
Experiment $\mathbf{Exp}_{\mathcal{A}}^{auth}$
```

```
let $\mathcal{A}(PUF) \leftarrow (T_1, T_2, \ldots T_i, \ldots T_q)$
and $((c_1, r_1), (c_2, r_2), \ldots (c_i, r_i), \ldots (c_\ell, r_\ell)) \leftarrow \mathcal{A}(PUF)$
Run $\pi(\mathcal{A}(T, C), R)_k$
if (R accepts $\mathcal{A}$ as I) then
   return 1
else return 0
```

Then we define the advantage $\mathbf{Adv}(\mathcal{A})$ *of the algorithm* $\mathcal{A}$ *in experiment* $\mathbf{Exp}_{\mathcal{A}}^{auth}$ *as the probability* $\Pr[\mathbf{Exp}_{\mathcal{A}}^{aut}$ *returns* $1]$ *in worst case.*

The protocol execution denoted as $\pi(\mathcal{A}, R)$ represents that the adversary executes protocol as initiator I with the responder R. However, the probability of R accepting $\mathcal{A}$ as authentic I is negligibly small. It must be noticed that an adversary might have recorded messages or certificates over radio channel, during past sessions. Therefore, these transcripts T_i's might be used as a knowledge base (public key or identity) to attack a future session over radio channel.

Theorem 4. *The advantage of* $\mathbf{Adv}(\mathcal{A})$ *is negligibly small.*

Proof. The proposed approach utilizes two separate communication channel for a complete vehicle to vehicle authentication. An adversary might interrupt on either of these channels to prohibit correct authentication and secure vehicle to vehicle pairing. Therefore, both communication channels are equally vulnerable to the possibility of interruption.

• *Real primary and real auxiliary channel:* The primary possibility is without any interruption over both channels. Vehicles create visual binding through optical communication and completes the session key derivation on radio channel with the same peer vehicle. Therefore, the vehicle authentication is secure over both channels.

Furthermore, the following lemma illustrates the impossibility of scenarios other way around.

Lemma 1. *A correct vehicle pairing over the real primary channel is fake without a real auxiliary channel.*

Proof. The proof is straightforward and is attributed to both of the individual channels as if executing independently.

○ *Real primary channel:* The wireless radio channel is non-influenced and $\hat{A}$ completes session key derivation with the intended $\hat{B}$, similarly, $\hat{B}$ completes session key derivation with the intended $\hat{A}$.

○ *Influenced auxiliary channel:* An adversary threatens the optical channel between the peer vehicles within close proximity of each other. Therefore, the initiator $\hat{A}$ identifies a different $\wp_{adv}$ as the $\wp_{\hat{B}}$, or $\hat{B}$ identifies $\wp_{adv}$ as the $\wp_{\hat{A}}$.

Apparently, this situation occurs when the intended peer performs secure AKE protocol over wireless radio channel, nevertheless, the same peer vehicle is not visible on optical channel. Therefore, visible adversary tries to authenticate via optical PUF as one of the peer party that successfully authenticated with AKE over wireless radio channel. The only possible vector of attacks can be summarized as (1) The adversary forges the certificate via extracting the real public keys from *real* secure AKE authentication and combines the extracted values with the influenced PUF response from $\wp_{adv}$. Therefore, the forgery against the certified contents can be used to signing the fake certificates and is against the above stated assumption on certificates. (2) The challenge c_j used in a compromised session j had been previously queried by the adversary and learned r_j leading to successfully produced equivalent PUF' device such that $PUF'(c_j) = PUF(c_j) = r_j$. The event occurrence has a negligible probability $\ell/|C|$, where ℓ is the CRP trials processed by the attacker and $|C|$ denotes the cardinality of the potential challenge set.

Furthermore, considering that adversary occupies an additional knowledge from pre-recorded q transcripts over the radio channel, thus, the probability $(\ell + q)/|C|$ has negligible increment over the earlier estimate. (3) The PUF'ed *responses* were re-routed. However, the assumption 2 illustrates that forging optical pattern in a reasonable time interval is infeasible. (4) The adversary accomplished a PUF clone for the challenge c_j in time smaller than t_{val} that is before the protocol session is expired and the CRPs are still valid for the remaining session. Therefore, an adversary *forwards* the speckle responses from the intended peer that is assumed to be securely paired over the radio channel. However, it violates the underlying Assumption 3. (5) The adversary retrieves CRP from the passive storage of a standalone parked vehicle and learns the unqueried challenges c_j reserved for future interval. Thereby, modeling an equivalent PUF' device such that $PUF'(c_j) = PUF(c_j) = r_j$. This attack scenario violates the assumption about tamper resistant/evident secure storage that is assumed to be configured in secure settings by a certificate distributor and is confidential to the owner. □

Lemma 2. *A correct visual identification over the real auxiliary channel is fake without a real primary channel.*

Proof. In contrast to the lemma and the corresponding impossibility arguments above, here, the impossibility of influenced primary channel is attributed to the security of authenticated key exchange over wireless radio channel.
○ *Influenced primary channel:* The adversary interrupts the communication on radio channel such that ($\hat{A}$ completes session key derivation with the malicious party E assuming that it communicates with $\hat{B}$ for which it verified a PUF stimulated response.
○ *Real auxiliary channel:* Accordingly, vehicles complete a secure authentication on optical channel. Therefore, vehicle $\hat{A}$ identifies $\wp_{\hat{B}}$, and $\hat{B}$ identifies $\wp_{\hat{A}}$ through challenge stimulation and corresponding response decoding.

The malicious influence over the primary channel targets a non-secure AKE execution over wireless radio channel. The only possible vector of attacks can be summarized as (1) The adversary forges the certificate via extracting original numeric response values from *real auxiliary channel*. However, forgery against the certificate contents can be used as the forgery for digitally signing the fake certificates. Therefore, the adversary might combine these extracted response values with the public keys of another party on behalf of which the adversary performs AKE protocol e.g. some corrupted party whose static secrets are known to the adversary. The forgery is against the assumption over pre-certified contents that are distributed securely by the unforgeable certificate authority. (2) The adversary breaks the security of the AKE protocol. Accordingly, adversary performs AKE protocol on behalf of the party whose public key is certified, but without the knowledge of the corresponding secret key. However, the underlying AKE assumption about the static and ephemeral secret keys are based on hard problem CDH. Therefore, if the adversary can perform AKE on behalf of other party than it can be used to break the underlying CDH hard assumption which is in contrast to the security assumptions in eCK model. □

Lemma 3. *A simultaneous adversarial attack on the influenced primary and influenced auxiliary channels is detectable.*

Proof. The proof of this lemma is a byproduct of the Lemma 1 and Lemma 2, combining the impossibility from both channels as below.
○ *Influenced primary channel:* A non-secure authentication on wireless radio channel such that adversary fakes the public key of some other party instead of intended recipient.

○ *Influenced auxiliary channel:* An adversary clones the PUF device and impersonates as other party. In addition, adversary might also use own PUF device with the corresponding unique responses and forges the certificate for these response such that it binds different public key with own PUF generated responses in order to impersonate as other party.

The attacks on both channels together can be deduced as a combination of attacks on either channel (as mentioned earlier in scenario 2 and 3). In the worst case, an adversary is powerful enough to break the security assumptions against the certificate signing authority and the AKE protocol. In addition, adversaries have successfully modeled a PUF clone for both the original initiator and responder. Therefore, a simultaneous attack on multiple channels is based on the underlying hardness of AKE assumption and mathematical modeling of PUF device. □

Theorem 4 is a direct implication of the Lemma 1, 2, and 3. Consequently, an immediate proposition from the Theorem 4 is given as below: □

Proposition 1. *After a successful protocol completion, a peer vehicle identified over the optical channel is the same party with whom the session key was established over the wireless radio channel that is: ○ no adversary can masquerade in front of the initiator $\hat{A}$ as the intended responder $\hat{B}$ - without holding a $\wp_{\hat{B}}$ and a secret key corresponding to the certified static public key B. ○ no adversary can masquerade in front of the responder $\hat{B}$ as the intended initiator $\hat{A}$ - without holding a $\wp_{\hat{A}}$ and a secret key corresponding to the certified static public key A.*

5. Correctness

In this section we present a formal induction proof using Strand Space methodology [49, 12]. The Strand Space methodology has been used earlier for the verification of Diffie-Hellman protocol [19], multi channel security protocol [51]. Accordingly, the verification of security properties such as authentication and secrecy is based on the analysis of mutual interaction between the valid and invalid strands in a specific protocol run.

Formalization The Strand Space model analyzes a legal trace in a bundle such that attacker does not reveal the uniquely originating terms over the channel. Every unique sequential message exchange over the channel is denoted by a unique strand height. Therefore, the initiator and responder both are required to possess a valid strand with respect to the causally related interactions.

Definition 4. *Strand: A strand s is a graph structure generated by the sequence of causally related events such as message transmission and reception. Every node n in a set N is identified by a unique sequential process strand s for every event i.e. $\forall n \in N$: $\exists s_n$.*

Definition 5. *Bundle: A bundle C is a finite, acyclic subgraph structure made of strands and satisfying a partial ordering among the nodes in set N_C.*

Definition 6. *Terms: A set $\mathcal{A}$ of terms is an algebraic structure containing disjoint sets such as plain text, cipher text, encryption keys. Furthermore, compound terms can be generated through multiple or iterative set operations on these disjoint set terms.*

A signed term is represented as a tuple $\langle \delta, t, \upsilon \rangle$ where term $t \in A$ and δt is the signed term sent over channel υ. Terms are either positive or negative signed which represents the transmission or reception of the term, respectively. For example $\langle +, t, \upsilon \rangle$ denotes sending a term t and $\langle -, t, \upsilon \rangle$ denotes receiving a term t over channel υ. Specifically, ($\pm A^*$) represents a finite sequence of signed terms as $\langle \langle \delta_1, t_1 \rangle, ..., \langle \delta_n, t_n \rangle \rangle$. A subterm t' is inductively related with the term t denoted as

$(t' \sqsubset t)$ such that t' preserves the value inside the term t irrespective of join, encryption, decryption and/or hashing operations over the term t.

Definition 7. *Causal precedence: Nodes in set N_C combined with edges $(\rightarrow_C, \Rightarrow_C)$ in a bundle C generates an ordered graph. It represents the sequence of strand height increment $(s_i tos_{i+1})$ on a specific trace such as $\langle s_i, n_j \rangle$ to $\langle s_{i+1}, n_{j+1} \rangle$ for $n_j \rightarrow n_{j+1}$ and $\langle s_i, n_j \rangle$ to $\langle s_{i+k}, n_{j+k} \rangle$ for $n_j \Rightarrow^+ n_{j+1}$.*

Nodes exchange messages along the causally ordered edges denoted as $n_1 \rightarrow n_2$. Assuming that n_1 and n_2 are on different strands and n_1 send term $+t$ on channel before n_2 receives $-t$ the same term on same channel. Similarly, nodes residing on the same strand are causally linked through $n_1 \Rightarrow n_2$ where n_1 is the immediate causal predecessor of n_2 index $\langle s_i, n_1 \rangle \Rightarrow \langle s_{i+1}, n_2 \rangle$. Similarly, $n_1 \Rightarrow^+ n_2$ denotes n_1 precedes n_2 on the same strand except immediately.

Definition 8. *Strand space: A strand space $\sum$ is a causally ordered strand mapped to a sequence of exchanging disjoint terms as $(\pm A^*)$ which represents a complete execution of the protocol.*

Our protocol represents a strand space $\sum$ that encompasses a separate strand for each, the initiator $\hat{A}$, responder $\hat{B}$, and attacker adv as below. The causal node interaction $(n_1, n_4, n_5, n_8, n_9, n_{12})$ with $(n_2, n_3, n_6, n_7, n_{10}, n_{11})$ at the initiator and responder strand $(s_1 tos_6)$, respectively, is depicted in Figure 6. The dashed arrows at the strand (s_1, s_2, s_4, s_5) denote the optical channel and the solid arrows at the strand (s_3, s_6) denote the wireless radio channel.

Proposition 2. *Initiators strand- The initiator $\hat{A}$'s strand is defined with the trace $I_{\hat{A}}(m_{i,\hat{A}}, s_{i,\hat{B}}, m_{i,\hat{B}}, s_{i,\hat{A}}, \hat{A}, \hat{B}, A, B, X, Y)$ as follows:*

$$\langle +Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X), -m_{i,\hat{B}}, +s_{i,\hat{A}}, -Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{A}, \hat{B}, X, Y), +m_{i,\hat{A}}, -s_{i,\hat{B}} \rangle \tag{1}$$

Proposition 3. *Responder strand- The responder $\hat{B}$'s strand is defined with the trace $R_{\hat{B}}(m_{i,\hat{A}}, s_{i,\hat{B}}, m_{i,\hat{B}}, s_{i,\hat{A}}, \hat{A}, \hat{B}, A, B, X, Y)$ as follows:*

$$\langle -Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X), +m_{i,\hat{B}}, -s_{i,\hat{A}}, +Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{A}, \hat{B}, X, Y), -m_{i,\hat{A}}, +s_{i,\hat{B}} \rangle \tag{2}$$

Proposition 4. *Adversary strand- The adversary adv's strand is defined with the trace $adv(\hat{A}, \hat{B}, X, Y)$ as follows:*

$$\begin{array}{lcl}
B & : & Insert\, challenge\, modulations\, \langle -m_{i,\hat{A}}, +m_{i,adv} \rangle \\
R & : & Insert\, recorded\, speckle\, \langle -s_{i,\hat{B}}, +s_{i,adv} \rangle \\
W & : & Insert\, certificate\, \langle -Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X), +Cert(r_{i,\hat{adv}}, \hat{adv}, adv)(\hat{B}, \hat{adv}, X_{adv}) \rangle \\
 & : & \langle -Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{adv}, \hat{B}, X_{adv}, Y), +Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{A}, \hat{B}, X, Y_{adv}) \rangle
\end{array}$$

It must be noticed that the adversary strand (B, W) is depicted with respect to the initiator strand, i.e., adversary insert and replace the modulations and certificates from the initiator strand. Whereas, adversary strand R is to insert and replace the speckles from the responder strand.

A stronger notion termed as intensional authentication is introduced in [40]. Similarly, in [28] a hierarchy of authentication is given in terms of properties such as aliveness, weak agreement, non-injective agreement and agreement. Accordingly, the agreement property is the most comprehensive among all while assuring that an initiator executes a recent single round of protocol in correspondence with every recent single round of protocol execution at responder side. However, intensional specification in [40] is stronger and has wider coverage against the possible attack scenarios. Since intensional specification does not deal with the recentness property which is one of the essential properties proposed in hierarchy of authentication [28]. Therefore, our definition of authentication includes the best of both worlds and ensures a spontaneous and mutual bijective authentication and injective secrecy for the security analysis. Moreover, our protocol assures stronger notion of authentication than intensional specification given in [40] as we avoid the misbinding scenario even if adversary is not able to decrypt the messages on a communication channel.

Definition 9. *Bijective authentication (one to one and onto): A protocol ensures bijective authentication when any initiator $\hat{A}$ spontaneously authenticates a specific responder $\hat{B}$ and as a consequence of which the specific responder $\hat{B}$ authenticates the intended initiator $\hat{A}$ uniquely and immediately, i.e. one to one. While, the authenticator $\hat{B}$ retains the authenticity for multiple initiators at the same time i.e. onto.*

We consider the one to one authentication in Lemma 4 and the onto in Lemma 5. Lemma 4 is based on proving that the causal relation among the nodes generates a partially ordered set with unidirectional edges (possible self-loops) and no cycles. In addition, Lemma 5 considers onto relation between the nodes (on separate strands) by showing that at least one causal link is present at any time.

Lemma 4. *Bundle C is a partially ordered structure closed over node set N_C under the relation $(\Re, \preceq)$.*

Proof. Bundle C is a subgraph structure composed of nodes N_C and causal links $(\rightarrow_C, \Rightarrow_C)$ between the nodes. The partial order structure N_C closed under a transitive, antisymmetric and reflexive relation $\Re$ is a weak partial ordering. It is evident that the relation $(\Re, \preceq)$ on N_C is a weakly partial ordered set and every node strand is causally related under $\Re$. Accordingly, $n_1 \preceq n_2 \preceq n_3$ are causally related such that n_1 effects the outcome at n_2 and similarly, n_2 effects the outcome at n_3. Then it can be deduced that n_1 effects the outcome at n_3 denoted as $n_1 \Rightarrow + n_3$. Therefore it is evident that the relation $(\Re, \preceq)$ satisfies the transitivity such that $\forall\, (n_1, n_2, n_3) \in N_C$: If $(n_1, n_2) \in \Re$ and $(n_2, n_3) \in \Re$ then $(n_1, n_3) \in \Re$. Considering nodes (n_1, n_2) closed under the relation $\Re$ such that (n_2, n_1) cannot be in the same relation $\Re$ until and unless $n_1 = n_2$. Thereby, satisfying the antisymmetric property of acyclic N_C under relation $\Re$ i.e. $(n_1, n_2) \in \Re \wedge (n_2, n_1) \in \Re \implies n_1 = n_2$. Apparently, every node strand is causally related to itself such that $\forall\, n \in N_C : (n, n) \in \Re$ and thereby satisfying the reflexivity under the relation $\Re$. □

Lemma 5. *Every non-empty subset of the nodes in N_C in bundle C has at least one causally ordered element that is unique.*

Proof. It is evident that every causally ordered element in a bundle C guarantees the bijective authentication. We consider this induction proof via contradiction. Let us assume that every non-empty subset of the bundle C have multiple causally ordered least elements, i.e., $(N_C, \preceq)$ have nodes n_1 and n_2 both as least element. According to the definition of least element l, $\forall n \in N_C : l \preceq n$ therefore, $\forall n \in N_C : n_1 \preceq n$ and $\forall n \in N_C : n_2 \preceq n$. Subsequently, it follows that $n_1 \preceq n_2$ and $n_2 \preceq n_1$. However, since the relation $(N_C, \preceq)$ is weak partial ordered (see lemma 4) and satisfies antisymmetric relation hence by the antisymmetric property $n_1 = n_2$, which is a contradiction to our initial assumption. Therefore, the least element is unique to every non-empty weak partial ordered subset of bundle C and satisfies that the sender is unique. □

Definition 10. *Injective secrecy: A protocol ensures injective secrecy when any sender $\hat{A}$ reveals a secret π to at most one intended recipient $\hat{B}$ and any third party does not distinguish the random secret π from secret π'.*

In order to illustrate the injective secrecy at each strand, Lemma 6 depicts the secrecy of each term by attributing the unique origination. Lemma 7 depicts the secrecy of each term by attributing the *indistinguishability* to the subterm secrecy perseverance.

Lemma 6. *A term ($\pm A^*$) exchanged on a channel υ belongs to a unique originating node $n \in N_C$.*

Proof. Every signed tuple $\langle\langle\delta_1, t_1\rangle, ..., \langle\delta_n, t_n\rangle\rangle$ exchanged among the regular nodes is bound to occur from a unique origin. The positive δ sign denotes the origin n_1 of term occurrence over the channel and later at the recipient n_2. According to lemma 5 only a unique regular node n_1 could have send it from the sender strand at same trace height i such as $n_1 \rightarrow n_2$. However, in case n_1 is not the immediate predecessor of n_2 such that $n_1 \Rightarrow^+ n_2$ then the signed tuple must have been originated by the strand index $(i-1), (i-2), ..., (i-j)$ or at the first node on initiator strand. Moreover, any subterm $t' \sqsubset \langle\delta_i, t_i\rangle$ originated at n_i is not accessible at any lower strand index n_{i-1} to n_1 see lemma 7. □

Lemma 7. *A predecessor node on the same strand with height $(i - 1 to i - j)$ and term t does not reveal a subterm $t_i \sqsubset t_{i+1}$ on a causally related strand at height $(i + 1)$.*

Proof. An immediate successor i is causally related to every predecessor $i-1, i-2, ..., i-j$. Every unique origination of a term $\pm t_i$ at strand s_i increases the length of strand as s_{i+1}. It is evident that term $t_i \sqsubset t_{i+1}$, however, term t_i is causal predecessor due to a unique origination of term t_{i+1}. Therefore, $t_i \sqsubset t_{i+1} \Leftrightarrow \exists t : (t \in \langle s_i, n_i\rangle \wedge t \in \langle s_{i+1}, n_{i+1}\rangle)$ not vice versa. □

Responder strand verification: Responder strand is given in Equation 2. Every responder strand is causally preceded by an initiator strand. Therefore, responder strand validity and term generation can be verified corresponding to initiator strand.

Lemma 8. *$s_{i,\hat{A}}$ is an unique and unpredictable term from a node n_5 on initiator strand $\langle s_3, n_5\rangle$.*

Proof. A node n_5 on initiator strand $\langle s_3, n_5\rangle$ generates a term $[term(n_5) = +s_{i,\hat{A}}]$ over optical channel. Although the channel is prone to introduce an adversary strand R in which adversary might fake the speckle response as $\langle -s_{i,\hat{A}}, +s_{i,\hat{Adv}}\rangle$. However, an adversary cannot forward the unpredictable response pattern $s_{i,\hat{A}}$ from initiator n_5. The node n_5 is entitled to uniquely generate the term $s_{i,\hat{A}}$. Moreover, earlier node on the same strand $[term(n_1) = +Cert_{hatA}] and [term(n_4) = -m_{i,\hat{A}}] \neq [term(n_4) = +s_{i,\hat{B}}]$ similarly, $term(n_5) \not\leq term(n_1)$ or $term(n_5) \not\leq term(n_4)$. Therefore, node n_4 uniquely generates the term which cannot be relayed further. □

Lemma 9. *Binding between the initiator and responder strand over multiple channels is causally related.*

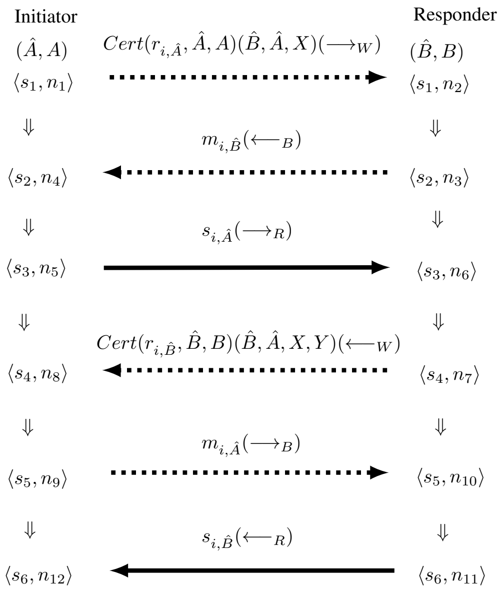
Initiator
Responder
$(\hat{A}, A)$
$Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X)(\longrightarrow_W)$
$(\hat{B}, B)$
$\langle s_1, n_1\rangle$
$\langle s_1, n_2\rangle$
$m_{i,\hat{B}}(\longleftarrow_B)$
$\langle s_2, n_4\rangle$
$\langle s_2, n_3\rangle$
$s_{i,\hat{A}}(\longrightarrow_R)$
$\langle s_3, n_5\rangle$
$\langle s_3, n_6\rangle$
$Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{B}, \hat{A}, X, Y)(\longleftarrow_W)$
$\langle s_4, n_8\rangle$
$\langle s_4, n_7\rangle$
$m_{i,\hat{A}}(\longrightarrow_B)$
$\langle s_5, n_9\rangle$
$\langle s_5, n_{10}\rangle$
$s_{i,\hat{B}}(\longleftarrow_R)$
$\langle s_6, n_{12}\rangle$
$\langle s_6, n_{11}\rangle$

Figure 6: Strand space with causal interactions.

Proof. Responder strand $\langle s_1, n_2\rangle$ receives $[term(n_2) = -Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X)$. Simultaneously, node n_6 over the same strand $\langle s_3, n_6\rangle$ receives $[term(n_6) = -s_{i,\hat{A}}]$. Furthermore, both terms at node n_2 and n_6 are subjected to adversary strand W and R, respectively. Accordingly, adversary might enter into certificate swap strand W as $\langle -Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X), +Cert(r_{i,\hat{adv}}, \hat{adv}, adv)(\hat{B}, \hat{adv}, X_{adv})\rangle$, however, $term(n_6)$ might reveal the certificate swap at n_2. Similarly, adversary might enter into speckle swap strand R as $\langle -s_{i,\hat{B}}, +s_{i,\hat{Adv}}\rangle$, whereas $term(n_2)$ verifies the expected response at node n_6 as $[-term(n_2) \simeq -term(n_6)]$ that certainly originates at $\hat{A}$. □

Lemma 10. *Responder strand $\langle s_4, n_7\rangle$ uniquely originates the term $Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{B}, \hat{A}, X, Y)$.*

Proof. According to lemma 8 responder strand $\langle s_6, n_1 1\rangle$ uniquely generates the commitment response. In addition, lemma 9 infers the causally related terms $term(n_2)$ and $term(n_7)$ that verifies the uniquely generating terms from the initiator strand. Therefore, node n_{11} proves the commitment response generated on the same strand $\langle s_4, n_7\rangle$ as $[term(n_7) = +Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{B}, \hat{A}, X, Y)]$. An adversary might enter into certificate swap strand W as $\langle -Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{adv}, \hat{B}, X_{adv}, Y), +Cert(r_{i,\hat{B}}, \hat{B}, B)(\hat{A}, \hat{B}, X, Y_{adv})\rangle$, however, $term(n_1 2) = -s_{i,\hat{B}}$ and $term(n_1 1) = +s_{i,\hat{B}}$ are causally related nodes on different strands and verifies the commitment $-term(n_8)$. □

Initiator strand verification: Initiator strand is given in Equation 1. The unique term exchange on either channel increases the strand height. Therefore, strand validity can be verified on every unique term generation.

Lemma 11. *Initiator strand $\langle s_2, n_4\rangle$ is causally related with $+term(n_1)$ and $+term(n_3)$.*

Proof. It is evident that $term(n_1)$ and $term(n_3)$ are uniquely generating terms from initiator and responder strand. Moreover, both terms are causally related and unpredictably mapped by the bijective function $\wp_{Responder}$. Therefore, the $[term(n_5) = +s_{i,\hat{A}}]$ is a commitment from initiator strand that is verified with the $term(n_1)$. Furthermore, an adversary might introduce strand R in order to block $term(n_5)$ and insert $term(n_{Adv}) = +s_{i,\hat{Adv}}$. However, the $term(n_{Adv})$ cannot be in correct mapping with $term(n_1)$ and is revealed to node n_6. □

Lemma 12. *A $term(n_1)$ on initiator strand uniquely generates $Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X)]$.*

Proof. The node n_1 generates a certified commitment over the numeric response $r_{i,\hat{A}}$. The original response value is generated at later strand $\langle s_3, n_5 \rangle$. Moreover, $[term(n_5) \not\subseteq (term(n_1), term(n_3))]$ hence is not a subterm originated earlier. Furthermore, the term $[term(n_1) = +Cert(r_{i,\hat{A}}, \hat{A}, A)(\hat{B}, \hat{A}, X)]$ might enter into an adversary strand W but the commitment verification is due on strand $\langle s_3, n_6 \rangle$ that is non-forwardable as per the lemma 9.
□

Lemma 13. *$s_{i,\hat{A}}$ is an unique and unpredictable term from a node n_5 on initiator strand $\langle s_3, n_5 \rangle$.*

Proof. The term $s_{i,\hat{A}}$ from initiator strand $\langle s_3, n_5 \rangle$ is a unique generation. Evidently, $[term(n_5) = +s_{i,\hat{A}}]$ is not a subterm for strand $\langle (n_1, n_5) \rangle$. Moreover, the causal link between strand s_4 and s_5 avoids the adversary strand R, as per the lemma 12 □

Lemma 14. *A uniquely generating $term(n_7)$ compiles the session key on initiator strand $\langle s_4, n_8 \rangle$.*

Proof. According to the lemma 10, the $term(n_7)$ is uniquely generated term and is not a subterm of earlier strands. In lemma 12 and 11, strand $\langle s_1, n_1 \rangle$ and $\langle s_4, n_8 \rangle$ are causally related with the $\langle s_6, n_{12} \rangle$ such that $(n_1 \Rightarrow^+ n_{12})$ and $(n_8 \Rightarrow^+ n_{12})$ are true. Therefore, session key derivation is due n_{12} as $[-term(n_{12}) \simeq (-term(n_1), +term(n_5))]$. □

6. Conclusion and Future Work

In this work, we propose to resolve vehicle to vehicle authentication for adversary coalition attack scenario. The conventional radio communication does not support the location binding and our solution provides this binding via an auxiliary optical channel. We utilize the inherent directed nature of optical communication to stimulate a Physical Unclonable Function (PUF) device. The unique PUF responses are used to verify the vehicle identity. Specifically, initiator vehicle visualize and identify the peer vehicle on optical channel via PUF stimulation. Subsequently, initiator verifies the certified credentials such as public key and numeric optical response over wireless radio channel to establish a secure session.

References

[1] Dedicated Short Range Communications (DSRC) Concept of Operations and ISO Layer Implementation Summary available at URL: http://grouper.ieee.org/groups/scc32/Attachments.html.

[2] Ieee standard for wireless access in vehicular environments security services for applications and management messages. *IEEE Std 1609.2 (Revision of IEEE Std 1609.2-2006)*, pages 1–289, 2013.

[3] F. Armknecht, R. Maes, A. Sadeghi, O.-X. Standaert, and C. Wachsmann. A formalization of the security features of physical functions. In *IEEE Symposium on Security and Privacy (SP)*, 2011.

[4] K. Bonne Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks. In *3rd International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm*, pages 331–340, 2007.

[5] S. Brands and D. Chaum. Distance-bounding protocols. In *Advances in Cryptology EUROCRYPT*, volume 765, pages 344–359. 1994.

[6] M. Cagalj, S. Capkun, and J. Hubaux. Key agreement in peer-to-peer wireless networks. *Proceedings of the IEEE*, 94(2):467–478, 2006.

[7] C. Campolo and A. Molinaro. Multichannel communications in vehicular ad hoc networks: a survey. *IEEE Communications Magazine*, 51(5):158–169, 2013.

[8] Q. Chen, D. Jiang, and L. Delgrossi. IEEE 1609.4 DSRC multi-channel operations and its implications on vehicle safety communications. In *IEEE Vehicular Networking Conference (VNC)*, pages 1–8, 2009.

[9] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[10] S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Dynamic attribute based vehicle authentication. In *13th IEEE International Symposium on Network Computing and Applications*, pages 1–8, 2014.

[11] S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Vehicle authentication via monolithically certified public key and attributes. In *Wireless Networks*, pages 1–18, 2015.

[12] F. J. T. Fábrega. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 1999.

[13] B. Gassend. Physical Random Functions. Master's thesis, MIT, 2003.

[14] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas. Controlled Physical Random Functions. In *Proceedings of the 18th Annual Computer Security Applications Conference*, pages 149–160, 2002.

[15] B. Gassend, D. E. Clarke, M. V. Dijk, and S. Devadas. Silicon physical random functions. In *ACM Conference on Computer and Communications Security*, pages 148–160, 2002.

[16] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls. FPGA intrinsic pufs and their use for ip protection. In *CHES*, pages 63–80, 2007.

[17] H. Hartenstein and K. Laberteaux. A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, 46(6):164–171, 2008.

[18] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert. Cloning physically unclonable functions. In *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 1–6, 2013.

[19] J. Herzog. The diffie-hellman key-agreement scheme in the strand-space model. In *16th IEEE Computer Security Foundations Workshop*, 2003.

[20] E. Hossain, G. Chow, V. C. M. Leung, R. D. McLeod, J. Mišić, V. W. S. Wong, and O. Yang. Vehicular telematics over heterogeneous wireless networks: A survey. *Comput. Commun.*, 33(7):775–793, 2010.

[21] H. Krawczyk. Sigma: The sign-and-mac approach to authenticated Diffie-Hellman and its use in the ike-protocols. In *Advances in Cryptology-CRYPTO*, pages 400–425, 2003.

[22] H. Krawczyk. Hmqv: A high-performance secure diffie-hellman protocol. 3621:546–566, 2005.

[23] Ł. Krzywiecki and M. Kutylowski. Coalition resistant anonymous broadcast encryption

scheme based on puf. In *Trust and Trustworthy Computing*, pages 48–62. 2011.

[24] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun. A comparative study of secure device pairing methods. *Pervasive and Mobile Computing*, 5(6):734 – 749, 2009.

[25] B. LaMacchia, K. Lauter, and A. Mityagin. Stronger security of authenticated key exchange. In *Provable Security*, pages 1–16, 2007.

[26] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone. An efficient protocol for authenticated key agreement. *Designs, Codes and Cryptography*, 28(2):119–134, 2003.

[27] J. Lee and J. Park. Authenticated key exchange secure under the computational Diffie-Hellman assumption. In *IACR Cryptology ePrint Archive*, 2008.

[28] G. Lowe. A hierarchy of authentication specifications. In *10th IEEE Computer Security Foundations Workshop*, 1997.

[29] R. MacLachlan and C. Mertz. Tracking of moving objects from a moving vehicle using a scanning laser rangefinder. In *IEEE Intelligent Transportation Systems Conference*, pages 301–306, 2006.

[30] R. Maes and I. Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security*, pages 3–37. 2010.

[31] R. Mayrhofer and M. Welch. A human-verifiable authentication protocol using visible laser light. In *Availability, Reliability and Security*, pages 1143–1148, 2007.

[32] J. McCune, A. Perrig, and M. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *IEEE Symposium on Security and Privacy*, pages 110–124, 2005.

[33] L. H. Nguyen and A. W. Roscoe. Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. *Journal of Computer Security*, 19(1):139–201, 2011.

[34] A. Noda, M. Hirano, Y. Yamakawa, and M. Ishikawa. A networked high-speed vision system for vehicle tracking. In *IEEE Sensors Applications Symposium (SAS)*, pages 343–348, 2014.

[35] R. S. Pappu. *Physical one-way functions*. PhD thesis, Massachusetts Institute of Technology, 2001.

[36] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. *Science*, 297:2026–2030, 2002.

[37] S. Patel and G. Abowd. A 2-way laser-assisted selection scheme for handhelds in a physical environment. In *Ubiquitous Computing*, pages 200–207. 2003.

[38] J. Y. Petit, C. T. Bösch, M. P. Feiri, and F. Kargl. On the potential of puf for pseudonym generation in vehicular networks. In *IEEE Vehicular Networking Conference*, pages 94–100, 2012.

[39] U. Rhrmair, C. Hilgers, S. Urban, A. Weiershuser, E. Dinter, B. Forster, and C. Jirauschek. Optical PUFs reloaded. Cryptology ePrint Archive, Report 2013/215, 2013.

[40] A. Roscoe. Intensional specifications of security protocols. In *9th IEEE Computer Security Foundations Workshop*, 1996.

[41] M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach, and S. Devadas. Robust and reverse-engineering resilient PUF authentication and key-exchange by substring matching. *IEEE Transactions on Emerging Topics in Computing*, 2(1):37–49, 2014.

[42] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling attacks on physical unclonable functions. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, pages 237–249, 2010.

[43] A. Sarr, P. Elbaz Vincent, and J. Claude Bajard. A new security model for authenticated key agreement. In *Security and Cryptography for Networks*, pages 219–234, 2010.

[44] M. Sichitiu and M. Kihl. Inter-vehicle communication systems: A survey. *Communications Surveys Tutorials,*, pages 88–105, 2008.

[45] B. Sieka. Active fingerprinting of 802.11 devices by timing analysis. In *IEEE Consumer Communications and Networking Conference*, pages 15–19, 2006.

[46] B. Sieka. Using radio device fingerprinting for the detection of impersonation and sybil attacks in wireless networks. In *Security and Privacy in Ad-Hoc and Sensor Networks*, pages 179–192. 2006.

[47] F. Stajano, F. L. Wong, and B. Christianson. Multichannel protocols to prevent relay attacks. In *Financial Cryptography and Data Security*, pages 4–19. 2010.

[48] Katzenbeisser, Stefan and Kocabaş, Ünal and Rožić, Vladimir and Sadeghi, Ahmad-Reza and Verbauwhede, Ingrid and Wachsmann, Christian. PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions Cast in Silicon. In *Cryptographic Hardware and Embedded Systems CHES*, pages 283–301. 2012.

[49] F. Thayer Fabrega, J. Herzog, and J. Guttman. Strand spaces: why is a security protocol correct? In *IEEE Symposium on Security and Privacy*, 1998.

[50] M. Thuy and F. Leon. Non-linear, shape independent object tracking based on 2d lidar data. In *Intelligent Vehicles Symposium*, pages 532–537, 2009.

[51] J. L. Trung Nguyen. Formal analysis of secure device pairing protocols, 2014.

[52] P. Tuyls and B. Škorić. Strong authentication with physical unclonable functions. In *Security, Privacy, and Trust in Modern Data Management*. 2007.

[53] L. Ulrich. Whiter brights with lasers. pages 36–56, 2013.

[54] B. Ustaoglu. Obtaining a secure and efficient key agreement protocol from (h)mqv and naxos. In *Designs, Codes and Cryptography*, pages 329–342, 2008.

[55] R. Uzcategui and G. Acosta-Marum. Wave: A tutorial. *IEEE Communications Magazine*, 47(5):126–133, 2009.

[56] T. Wang, Y. Liu, and J. Ligatti. Fingerprinting far proximity from radio emissions. In *Computer Security - ESORICS*, Lecture Notes in Computer Science, pages 508–525. 2014.