Optical PUF for Vehicles *Non-Forwardable* Authentication

by

Shlomi Dolev, Łukasz Krzywiecki, Nisha Panwar, Michael Segal

The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel

Technical Report #15-02

February 2015

Optical PUF for Vehicles *Non-Forwardable* Authentication

(Extended Version)

Shlomi Dolev[1] Łukasz Krzywiecki[2] Nisha Panwar[1] Michael Segal[3]

[1] Department of Computer Science, Ben-Gurion University of the Negev, Israel.
{dolev, panwar}@cs.bgu.ac.il. *
[2] Institute of Mathematics and Computer Science, Wroclaw University of Technology, Poland.
lukasz.krzywiecki@pwr.wroc.pl. †
[3] Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Israel.
segal@cse.bgu.ac.il.

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. However, these warning messages must associate an authentication factor such that verifier authenticates the message origin via visual binding. Apparently, vehicle to vehicle communication is vulnerable to message forwarding and thereby allowing an incorrect visual binding with the malicious vehicle. We introduce the *non-forwardable authentication* to avoid the adversary coalition attack scenario for a secure vehicle to vehicle communication. Accordingly, the group of adversaries impose fabricated vehicle attributes in order to impersonate the intended sender and reroute the eavesdropped messages. Therefore, the verifier misidentify one of these adversaries as the authentic vehicle instead of actual sender. We propose to utilize spontaneous optical response verification and establish a session secret key with the original remote vehicle, exchanging messages routed through a resembling and adversarial vehicle. Thus, the communicating parties identify another vehicle as the one they secretly communicate with over wireless radio channel, which in turn can cause hazardous situations. These optical response are generated through hardware means such as a certified Physically Unclonable Function (PUF) device embedded on front and rear of the vehicle and must be verified against a pre-certified fresh pairs of challenges and responses, for the same vehicle. Furthermore, vehicles utilize an out-of-band optical communication channel to exchange the physically unclonable function stimulated optical challenge and corresponding response from the sender and receiver, respectively. It is important to mention that the pre-certified response must be verified against a certified physically unclonable function stimulated immediate optical response rather the image of pre-recorded optical response, for the specific peer 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.

Keywords: Authentication, certificate, optical communication, challenge response pairs, verification.

* 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).

† Partially supported by funds of the Institute of Mathematics and Computer Science, Technical University of WrocŁaw, project (#S40012/I-18).

1 Introduction

Vehicle networks [13, 35, 15] allows a safe and efficient maneuvering among the vehicles. Smart vehicles are equipped with wireless radio devices and comply with the Dedicated Short Range Communication (DSRC) IEEE 1609 and Wireless Access in Vehicular Environment (WAVE) 802.11p [1, 5]. Therefore, vehicles are customized to predict a crash event ahead of time through ultrasonic and infrared radars, optical detection and ranging sensors and night vision camera [42]. Our protocol is secure to create an information rich map of the surrounding vehicles and attribute the messages arriving through the radio to the correct vehicle in the map. Such an up-to-date map may assist real-time decisions on driving actions, e.g., accelerating, decelerating, or lane changing. Once the vehicle have established a secure session with a near by vehicle, the map can be updated using the information received over the radio channel, attributing the responsibility of any malfunctioning to the authenticated party.

We propose to achieve 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., conventional radio channel and optical channel. Wireless radio communication is widely supported by the smart handheld cellular 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 provide a precise location information of the original signal source. Recently, authors in [44] 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) still the source of signal origination is unknown. The dispersed nature of the radio signals provokes the incorrect binding between radio signals and the physical spot of signal origination. Our scheme ensures a correct binding between radio signals and its physical spot of origination.

We utilize the inherent directed nature of optical communication to produce *optical fingerprints* in association with a secure radio communication. Optical communication (or equivalent technology for having clear geographic mapping of the communicating entity monolithically coupled with the information received) is an important ingredient in our proposed architecture. The directed nature of the optical channel eliminates the possibility of an adversary in the line of sight between mutually authenticating 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] based security infrastructure immune against coalition attack scenario as presented in this paper. Vehicles authenticate a peer vehicle over radio channel to be the same vehicle as visualized over optical channel. We propose a PUF based solution that can withstand more sophisticated adversaries than in previous works [7, 8].

Problem statement. We consider an adversary coalition attack scenario [8] 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. Furthermore, the messages are routed through a group of malicious vehicles that looks similar as the intended sender/receiver. The malicious vehicles communicate over a separate communication channel. Therefore, the intended sender/receiver that owns a certificate (binding vehicle attributes and public key) and is actually far away from the communication range would be 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 [7] and dynamic attribute [8] based authentication is not sufficient to avoid the coalition attack scenario and requires *non-forwardable* authentication techniques. Specifically, a technique that would prevent the verifier to visually misidentify the attacker (that only forwards messages) with the original authenticator (that produces the authentication messages).

Our goal is to couple the communicating vehicles within the scope of multiple channels such as radio channel and optical channel. However, the optical channel is essential during the authentication phase and radio channel resumes beyond the authentication phase for the authenticated message exchange. Therefore, the proposed authentication approach utilizes a non-forwardable fingerprint response from peer vehicle. Moreover, Physical Unclonable Functions (PUFs) [27] device is used to produce these responses and a supplementary optical communication is used to convey and verify these unique responses. Consequently, optical PUF assisted *unforgeable fingerprints* provide a robust vehicle identification.

Strawman Solutions. To give intuition about the criticality of the coalition attack scenarios we present here some ad-hoc solutions that potentially seems to immune against the coalition attack scenario. However, the attack is still unavoidable due to the message forwarding within the existing state of vehicle to vehicle security standards. Interestingly, neither the wireless radio nor the optical communication individually is enough to provide a complete solution against the coalition attack scenario. Furthermore, the following intuitive solutions might seem to solve the problem but only to a certain extent, therefore, we further explore in more detail the pros and cons of these intuitive solutions.

Timing analysis: The optical communication channel is used to measure the dynamic primitives [21, 26] of the moving target. Moreover, a round trip delay measurement for the optical beam is another estimate that assists to verify the partner in communication. Accordingly, sender estimates that the receiver is not farther then few meters away and therefore should not take more than a few seconds to access. In the existing literature the concept is also known as distance bounding and round trip delay estimation [4]. In this case, the sender and receiver might assure 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. Furthermore, assuming that sufficient security protocols are available that might prevent the adversary to fake the lower delay, still, the adversary can fake a larger distance or round trip delay by delaying the message relaying towards the intended recipient. 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 bear an unique distinguishable property [37, 36, 3]. Therefore, the radio waves generated at a particular vehicle retains the *consistent* and *unique* traits. However, the radio fingerprinting approach does not ensure the *non-forwardable* authentication due to the lack of point-to-point nature of the channel. Moreover, 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 binding* 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 reflected. Therefore, the commitment data conveyed through beam modulations seems secure and confidential to recipient vehicle. However, these reflective mirror does not contribute beyond the beam modulation decoding. Moreover, a recipient vehicle cannot distinguish between the beam reflection originated at intended sender and the reflection of reflection (reflection originated at middle adversary, mimicking the original reflection from the intended sender). An adversary nearby can record the laser beam modulations originated from other vehicle and might also generate the same modulations. Therefore, the beam modulations and the commitment data is vulnerable to rerouting and forwarding, subliminally. Furthermore, there is no binding between the optical and wireless radio channel and is not a complete solution against 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 an unique reflection corresponding to vehicle identity. Apparently, the certified hologram response resolves the true vehicle identity and appears to be quite relevant solution for identity resolution as in our case. However, the hologram retains a specified Challenge Response Pair (CRP) which remains fixed for every verification round. Furthermore, a mighty adversary can reveal the CRP by analysing it over a period of time because the response remains static irrespective of the vehicle static and dynamic attributes.

We require a dynamic scheme for commitment verification in which CRPs are no longer static for a long time. It is evident that the property of non-forwardability must be ensured through an instant response verification. Our solution proposed in this paper verifies the immediate processing of optical beam through unclonable device known as Physically Unclonable Function (PUF) [27, 28, 9, 11, 41]. PUFs are hardware devices that

are configured to produce an unique response corresponding to a unique and sufficiently diverse challenge. The verifier compares these PUF generated response pattern against the certified response received over wireless radio channel. Evidently, a PUF based solution is rigorous and resistant towards the above mentioned coalition attack scenario. Therefore, the PUF generated spontaneous wireless signatures enable a secure binding between the optical and wireless radio communication channel.

Physically Unclonable Function (PUF). A PUF device is a hardware primitive that extracts secrets from its physical characteristics acquired during inevitable random variation of fabrication process. Specifically, PUF is a physical instantiation of hash function in a random oracle and is difficult to predict and model the corresponding input of a processed response over PUF. Therefore, PUF devices are immune against the predictable mathematical modeling of underlying challenge-response mapping and strongly ensures the one-way hash property. We denote the function instated inside the hardware PUF device as $\wp$. 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 in a commitment-response verification protocol. These PUFed responses are unique corresponding to the challenge and are extremely difficult to predict without accessing the original PUF device itself. The essential properties [22, 39] 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 [27]. Therefore, we presume that the certified CRPs produced by a PUF device are uniquely paired and sufficiently diverse to distinguish.

• *Unclonable:* No two PUF devices produce same output via cloning. As the micro variations enforced by during the production process ensures the infeasibility of physical cloning. 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 Challenge Response Pairs (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 or raw speckle pattern s_i and the certified PUF device $\wp$ still it is infeasible to derive the corresponding challenge stimulus c_i.

• *Tamper evident:* Any attempt to recover the structural traits of the PUF device $\wp$ would manipulate the original structure of $\wp$ such that the original CRP pairing is not retained any longer.

Previous work. In [32] a PUF authentication scheme has been proposed, accordingly, initiator measures response via PUF stimulation. Responder transmits a shuffled response string that initiator verifies through substring matching. The paper [30] presented a PUF based protocol for secure private-public key pair generation and distribution

between Certificate Authority (CA) and vehicles. Similarly, authors in [38] presented a challenge-response based method to verify the paired device, whereas both the paired devices are assumed to have established a secret key. Sender measures the response and receives the same response encrypted with the secret key from 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.

Our approach provides a non-forwardable vehicle authentication and the key establishment together. Furthermore, we assume the existence of an out-of-band communication channel [24] to verify the certified static attributes. In [7] a novel vehicle authentication scheme based on certified and coupled vehicle attributes with the public key has been proposed. Subsequently, in the following work [8] the use of laser communication channel 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 [23, 18, 25]. Moreover, it is practically feasible for high speed vehicles to operate laser beam for tracking [21, 40, 26] and secret key establishment [29, 23].

The Physically Unclonable functions (PUF) was first introduced in [27] as a hardware analogous to the one-way hash functions. There are several types of PUFs discussed in literature [28, 11, 10, 12]. The proposed scheme utilizes optical PUF as they are secure against cloning [14] and modeling attacks [33]. PUFs are also referred to as Physical Random Functions [9, 11] or Physical One-Way Functions [27, 28], have been used for key establishment [28, 41], identification [28] and authentication [11, 41]. The state-of-art research that ensures the property of unclonability is given in [22, 39]. Furthermore, the authors in [31] presented an optical PUF based scheme for challenge-response verification through a manufacturers 2D barcode signature embedded over the PUF device.

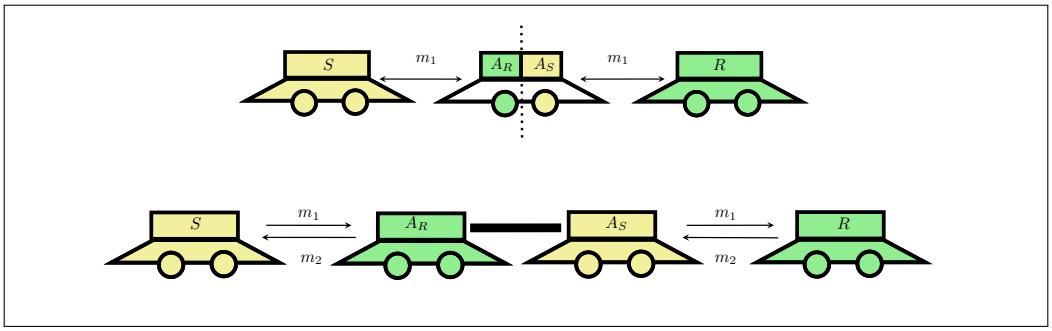

Figure 1: Coalition of adversaries [8].

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

• *Unique identification:* Vehicles create a visual binding with a peer vehicle over optical channel through PUF $\wp$ device. The physical challenge stimulus c is processed over an authentic PUF $\wp$, thereby, producing an original and spontaneous response r from $\wp$. Therefore, a communicating vehicle is uniquely identified via PUF verification.
• *Vehicle authentication:* The proposed approach ensures the unique vehicle authentication due to AKE protocol execution via certified attributes and public key over a securely coupled radio channel. Moreover, radio communication is securely coupled with the preliminary optical communication. Thus, peer vehicle authentication is twofold secure.
• *Non-forwardability:* The adversary cannot forward the messages on behalf of another sender such as without being detected. Sender and receiver are in direct communication with each other, therefore, the message integrity is ensured.
• *Channel binding:* 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 authentication 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. A detailed security discussion is given in Section 4. Further, Section 5 highlights the concluding remarks. Moreover, a detailed formal correctness proof using Strand Space methodology have been omitted from this extended version.

2 Adversary coalition scenario

We provide a solution for the coalition attack scenario as discussed in [8] (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 sender and the other impersonates receiver by carrying exactly similar static attributes. Moreover, these malicious vehicles communicate over a separate communication channel to relay the messages between the intended sender and receiver. Although malicious vehicles may not be able to decipher the messages still it can create an illusion of correct visual binding. The sender believes that it forwards message to receiver while actually forwarding it to one of the malicious vehicle impersonating the receiver and vice versa. The first scenario in Figure 1, illustrates an adversary in the middle possesses fake visible attributes of both S and R. Therefore, 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 message m_1. However, an adversary representing both A_S and A_R that impersonates S and R, respectively, is very unlikely. 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 communicate over an additional channel and relay the messages m_1 (from sender S) and m_2 (from 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. Therefore, PUF $\wp$ produced unpredictable but consistent responses are necessary and sufficient to avoid the coalition attack which is feasible in real life scenarios.

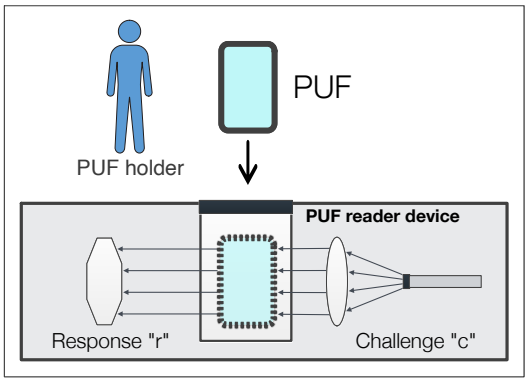

Figure 2: Authorization via PUF device.

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 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 speckles s_i are captured on the sensor part of the reader (see Figure 2). The conventional usage of PUF in authorization process is divided into two phases:

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

Vehicles setup. We adapt the regular PUF setup (see Figure 3) for PUF based vehicle authentication. Thus, verifier and prover both are allowed to be distant and the unique responses can be verified through the PUF stimulation.

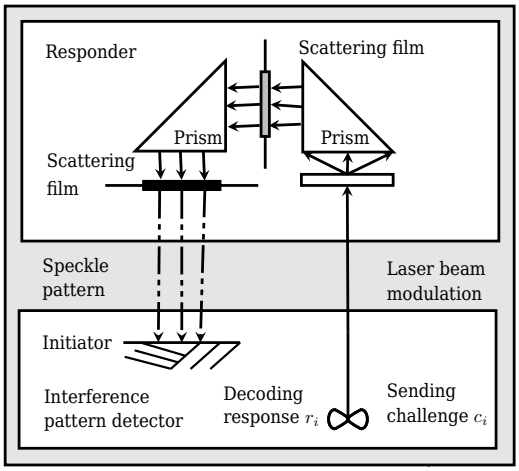

Figure 3: Optical PUF assisted response verification.

• The part of the reader device made of 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 made of the laser and the sensor, verifies the unclonable fingerprints of the prover and must be hardwired to the non-replaceable parts of the verifier vehicle.

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 wireless radio and optical communication channel. Presumably, every vehicle is configured with the certificate from trusted authorities. The authorities sign the public key of the vehicle along with additional relevant primitives such as visible static attributes of the vehicle, validity, sequence number and procedure to verify the signed visible static attributes. Interested readers may refer to [7] 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 independent session key derivation at the sender and receiver, both vehicles may switch on to a secure wireless radio session. A general working of the proposed approach is given in Figure 4.

3.1 Proposed approach

PUF based remote vehicle to vehicle identification over the optical channel assists Authenticated Key Exchange (AKE) over the conventional radio channel. Therefore, the radio channel must enable a secure session key establishment in association with the response verification over optical channel. It necessitates a secure binding between radio

$\hat{A}$	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.

channel (with session establishment) and optical channel (with visual identification). We describe the tamper proof PUF device setup and the registration phase as following:

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 device is considered as a separate instance of random oracle model, therefore, each input to a PUF device yields a sufficiently diverse output and it is nearly impossible to retract the specific input value from any given output value.*

We denote the relative variation in each response corresponding to each challenge as ε. Therefore, this response divergence is the parameter to ensure physical one-way property in a PUF device. 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 C domain is large and there exist 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. We define the assumptions and settings as follows:

Assumptions and settings.

• Vehicles possesses a certified PUF device from the trusted manufacturer.

• Vehicles store certified coupled CRPs in a non-volatile tamper proof memory device and certified CRPs are confidential.

• 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 use an abstract term $Cert(c_i, r_i)$ for brevity.

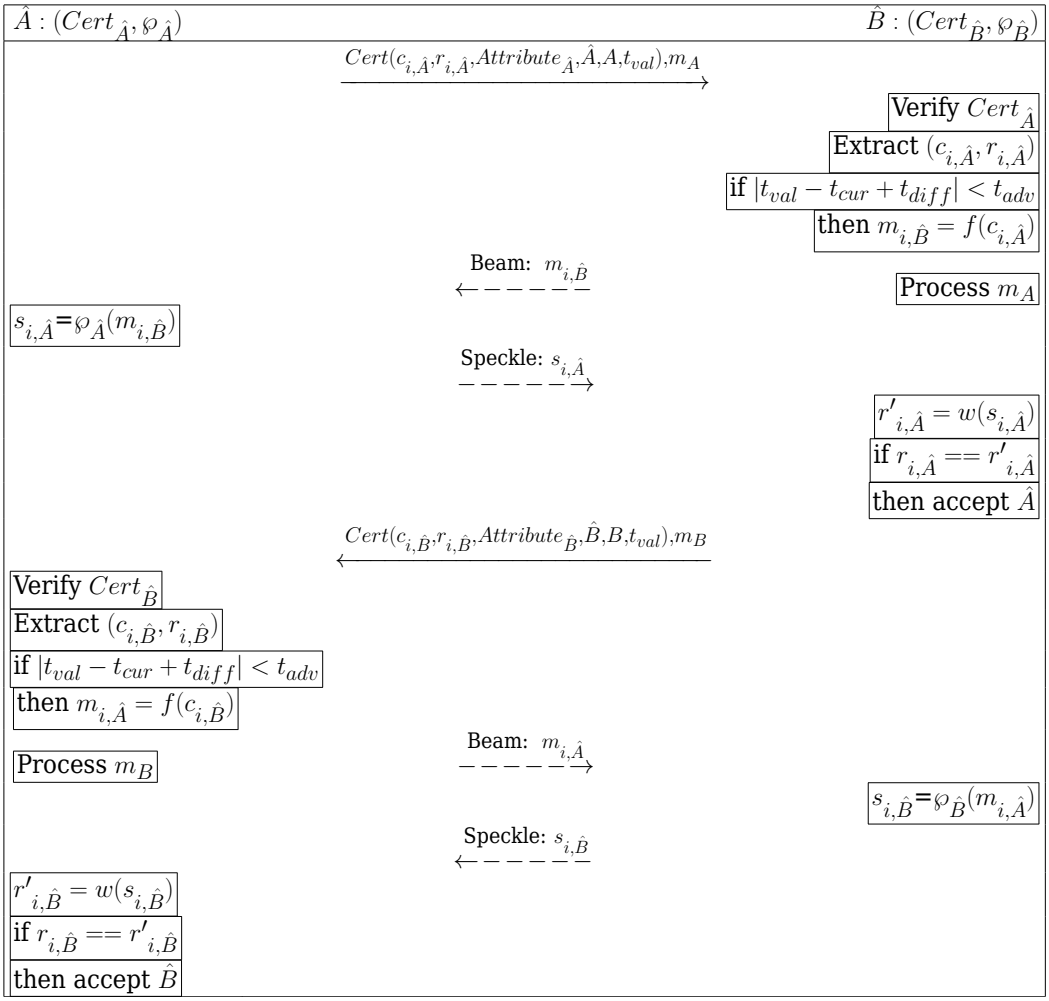

Figure 4: The generalized approach.

• Certificates are discarded after the one-time use or beyond the validity time t_{val} whichever is earlier. Whereas, the adversary requires the least PUF modeling time t_{adv} to model PUF′ that mimics a specific queried CRP.
• The difference between the CRP validity time t_{val} and the current time t_{cur} must be lesser than the estimated PUF modeling time t_{adv}.

Considering the rapid evolution and connectivity among Internet of Things (IoT) modern vehicles would stay longer physically but the firmware updates and crypto-counter restart might be as frequent as nearly 2-5 years (depending on miles covered). Therefore, we consider the vehicle lifetime as the 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 maximum clock drift from current time that is bounded by $(\pm t_{diff})$. Nevertheless, we consider a worst case scenario and accordingly, the PUF modeling attack should be infeasible even in as much time as lesser than $|t_{val} - t_{cur} + t_{diff}|$.
• We consider an optical out of band communication channel in our proposed approach and the challenge input to PUF device is directed through an optical medium. Therefore, the modulation m_i is derived through a deterministic function f that codes the numeric value of the challenge c_i into a combination of beam frequencies and angles, denoted as $f(c_i) \rightarrow m_i$.
• The input for a optical PUF device 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 is captured via optical screens at the receiver and decoded into numeric value r_i, denoted as $w(s_i) \rightarrow r_i$. The specialized optical screen distinguishes the original 3d-speckles and the relayed 2d-image of speckles.

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

Vehicles are configured with a static public key in a tamper proof storage and the PUF device. 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) [6] key exchange over a secure group $G = \langle g \rangle$ where 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. For example, vehicle $\hat{A}$ is configured with the static public key $A = g^a$ and the PUF device $\wp_{\hat{A}}$. Similarly, vehicle $\hat{B}$ has long term public key $B = g^b$ and the PUF device $\wp_{\hat{B}}$. Where 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 $\wp_{\hat{A}}$ device and obtains a uniquely paired response. In addition, $\mathcal{R}$ certifies the 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 authentication phase. For example $\mathcal{R}$ stores the 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 moving vehicles after the registration and certificate configuration is completed. Vehicles possess certified CRPs for their own PUF device stimulation. These pairs are used for PUF stimulation and 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 is important to notice 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 $\wp_{\hat{A}}$ embedded on 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 optical channel with an extracted response $r_{i,\hat{A}}$ over 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 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 $\wp_{\hat{B}}$ 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 optical channel with an extracted response $r_{i,\hat{B}}$ over radio channel. After the response verification, $\hat{A}$ accepts $\hat{B}$ as an authentic peer vehicle. In addition, $\hat{A}$ 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. However, there exist a plenty of two round authentication protocols that enable secure session key derivation, e.g., CMQV [43], SMQV [34], NAXOS [19], NAXOS+ [20], SIGMA [16]. Furthermore, these approaches are proven to be secure in CK and eCK model recently. Therefore, we demonstrate the binding between the proposed approach and the existing AKE such as CMQV.

Binding with CMQV: The wireless radio and optical communication channels are used concurrently. The example sequence of messages and computation on both sides are shown in Figure 5. Binding for two authentication channels can be summarized as below:
• Radio channel for establishing a secure session through CMQV.
• Optical channel for PUF authentication 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 static secret key a and b, respectively. We are binding proposed approach with the existing CMQV authentication protocol over 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 wireless radio channel and forwards the certified CRPs along with the attributes, sender identity, static public key, validity period, recipient identity and 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 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 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 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 an extracted response $r_{i,\hat{A}}$ over radio channel. After the response verification, $\hat{B}$ accepts $\hat{A}$ as authentic peer vehicle and derives 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 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 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 numeric response as $r'_{i,\hat{B}} = w(s_{i,\hat{B}})$. The verifier must compare

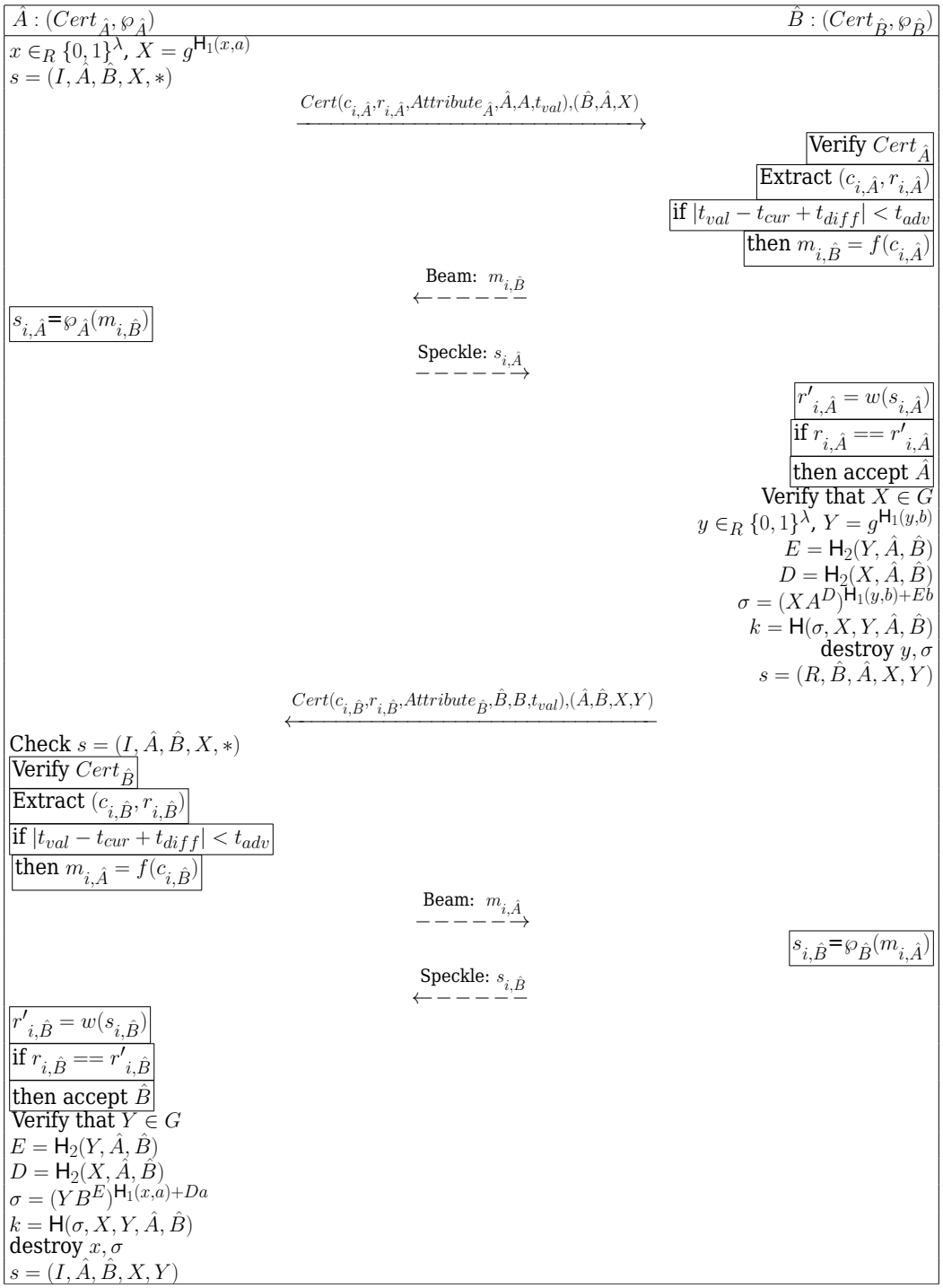

Figure 5: Binding optical PUF verification with CMQV over radio channel.

this decoded numeric response $r'_{i,\hat{B}}$ over optical channel with an extracted 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 $s(I, \hat{A}, \hat{B}, X, Y)$.

Therefore, $\hat{A}$ and $\hat{B}$ can verify the certified response on wireless radio channel and the corresponding optical response over the laser channel. Consequently, the initiator derives a secret exponent E and the receiver derives a secret exponent D by using 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. Furthermore, 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.

4 Security Discussion

Ideally, producing the optical speckle response $r_{i,\hat{A}}$ for the paired challenge $c_{i,\hat{A}}$ is impossible, without using the corresponding PUF device $\wp_{\hat{A}}$. We assume that receiver has to process the original optical response itself to compute the final numeric response value $r_{i,\hat{A}}$. A vehicle receiving a decoded numeric response $r_{i,\hat{A}}$ from the peer vehicle is considered an attack attempt and discarded.

Considering the uncertain factors of the future technology development and potential physical attacks (that are not known currently), we should consider 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 be confidential therefore, we introduce a time parameter t_{adv} that denotes the minimum time an adversary requires to model a PUF clone. We assume that PUF modeling in a time fewer than t_{adv} is negligible and smaller than a parameter ϵ. The modeling attack is analogous to producing a forged hologram that clones the static CRP of an original hologram. Apparently, it is difficult to attack an ongoing session in any ad-hoc scenario. Since the existing AKE protocols avoids an active impersonation. However, a mighty adversary may succeed in modeling the PUF device (for which a few transcripts are known) in a carefully prepared laboratory environment. Moreover, these protocols neither prevent a message forwarding nor create a visual binding.

In addition, we consider that the peer vehicle must exchange their current CRP's (during the session) with each other. An authorization session should utilize challenges that are not publicly known (not known to the attacker) for time longer than t_{val}. Therefore, we require CRPs to be confidential and vehicles spontaneously acquire the current (not older validity period t'_{val}) certified CRP over the wireless radio channel, instead of knowing challenges for future interval beforehand. Other vehicles cannot access CRPs that are certified for a future interval. 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 assumed to own an individual PUF device and using certificates (monolithic binding between public key and static attributes) over radio channel.

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 claim the following properties to 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).

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. 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 [17]:

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

• There is a separate table of input-output pairs (m_i, s_i) associated with each PUF device, empty at the end of the production stage, initialized on its first run 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 specific PUF that generates the spontaneous interference pattern.
• The PUF cannot be cloned in a way that responses for unqueried inputs would be consistent between the clones.

It is important to mention that the input s_i processed by the sensor 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 (e.g. taken by regular camera). We assume that the sensor is tuned to capture only the predefined

physical characteristics of the scattered speckle in an ad-hoc manner with time less than the adversary modeling time, i.e., $t < t_{adv}$. Therefore, producing the correct vector r_i corresponding to the given c_i is impossible without the original PUF stimulation. We formulate the following assumption:

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

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

there is no adversary that can 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.

As we mentioned earlier 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 will, can produce (in time less than t_{adv}) another PUF'. Such that PUF' outputs 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

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

Apparently, CRPs must be 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. 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. Thus, the certified CRPs remain confidential until the valid interval arrives. 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 bound radio and optical channels. 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 chanel) as I in front of R, during a future session 'k'.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{auth}$
  let $\mathcal{A}(PUF) \leftarrow (T_1, T_2, \ldots T_i, \ldots T_q)_j$
  and $((c_1, r_1), (c_2, r_2), \ldots (c_i, r_i), \ldots (c_\ell, r_\ell))_j \leftarrow \mathcal{A}(PUF)$
  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 $1]$.

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.

• The other possibility around is secure pairing over radio communication but incorrect visual binding among the peer vehicles. It can be summarized as below:

  ◦ *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.

• Another possibility leads to a correct pairing over optical channel. However, the coupled radio channel authentication is interrupted by the adversary. It can further be detailed as follows:

◦ *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.

Nevertheless, the presented 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.

• The most pessimistic possibility is that both channels are influenced by the adversary.

◦ *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.

As an immediate proposition from the above stated theorem 4 is:

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, i.e. the following facts are true:* ◦ *no adversary can be identified to 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 be identified to 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 Conclusion

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. 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.
4. M. Cagalj, S. Capkun, and J. Hubaux. Key agreement in peer-to-peer wireless networks. *Proceedings of the IEEE*, 94(2):467–478, 2006.
5. 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.
6. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
7. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Certificating vehicle public key with vehicle attributes. In *ASCoMS (Architecting Safety in Collaborative Mobile Systems) at SAFECOMP*.
8. 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.
9. B. Gassend. Physical Random Functions. Master's thesis, MIT, 2003.
10. 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.
11. 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.
12. 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.
13. H. Hartenstein and K. Laberteaux. A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, 46(6):164–171, 2008.
14. 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, June 2013.
15. 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.
16. 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.
17. Ł. Krzywiecki and M. Kutylowski. Coalition resistant anonymous broadcast encryption scheme based on puf. In *Trust and Trustworthy Computing*, pages 48–62. 2011.
18. 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.
19. B. LaMacchia, K. Lauter, and A. Mityagin. Stronger security of authenticated key exchange. In *Provable Security*, pages 1–16, 2007.
20. J. Lee and J. Park. Authenticated key exchange secure under the computational Diffie-Hellman assumption. In *IACR Cryptology ePrint Archive*, 2008.
21. 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.
22. 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.
23. R. Mayrhofer and M. Welch. A human-verifiable authentication protocol using visible laser light. In *Availability, Reliability and Security*, pages 1143–1148, 2007.
24. 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.
25. 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.
26. 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.
27. R. S. Pappu. *Physical one-way functions*. PhD thesis, Massachusetts Institute of Technology, March 2001.

28. R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. *Science*, 297:2026–2030, 2002.
29. 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.
30. 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.
31. 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.
32. M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach, and S. Devadas. Robust and reverse-engineering resilient PUF authentication and key-exchange by substring matching. *Emerging Topics in Computing, IEEE Transactions on*, 2(1):37–49, 2014.
33. 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.
34. 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.
35. M. Sichitiu and M. Kihl. Inter-vehicle communication systems: A survey. *Communications Surveys Tutorials,*, pages 88–105, 2008.
36. B. Sieka. Active fingerprinting of 802.11 devices by timing analysis. In *IEEE Consumer Communications and Networking Conference*, pages 15–19, 2006.
37. 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.
38. F. Stajano, F. L. Wong, and B. Christianson. Multichannel protocols to prevent relay attacks. In *Financial Cryptography and Data Security*, pages 4–19. 2010.
39. 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.
40. M. Thuy and F. Leon. Non-linear, shape independent object tracking based on 2d lidar data. In *Intelligent Vehicles Symposium*, pages 532–537, 2009.
41. P. Tuyls and B. Škorić. Strong authentication with physical unclonable functions. In *Security, Privacy, and Trust in Modern Data Management*. 2007.
42. L. Ulrich. Whiter brights with lasers. pages 36–56, 2013.
43. B. Ustaoglu. Obtaining a secure and efficient key agreement protocol from (h)mqv and naxos. In *Designs, Codes and Cryptography*, pages 329–342, 2008.
44. 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.