# Formal Analysis of V2X Revocation Protocols

Jorden Whitefield[1], Liqun Chen[1], Frank Kargl[2], Andrew Paverd[3],
Steve Schneider[1], Helen Treharne[1(✉)], and Stephan Wesemeyer[1]

[1] Department of Computer Science, University of Surrey, Guildford, UK
{J.Whitefield,Liqun.Chen,S.Schneider,H.Treharne,S.Wesemeyer}@surrey.ac.uk
[2] Ulm University, Ulm, Germany
frank.kargl@uni-ulm.de
[3] Aalto University, Espoo, Finland
andrew.paverd@ieee.org

**Abstract.** Research on vehicular networking (V2X) security has produced a range of securitymechanisms and protocols tailored for this domain, addressing both security and privacy. Typically, the security analysis of these proposals has largely been informal. However, formal analysis can be used to expose flaws and ultimately provide a higher level of assurance in the protocols. This paper focusses on the formal analysis of a particular element of security mechanisms for V2X found in many proposals, that is the revocation of malicious or misbehaving vehicles from the V2X system by invalidating their credentials. This revocation needs to be performed in an unlinkable way for vehicle privacy even in the context of vehicles regularly changing their pseudonyms. The REWIRE scheme by Förster et al. and its subschemes PLAIN and R-TOKEN aim to solve this challenge by means of cryptographic solutions and trusted hardware. Formal analysis using the TAMARIN prover identifies two flaws: one previously reported in the lierature concerned with functional correctness of the protocol, and one previously unknown flaw concerning an authentication property of the R-TOKEN scheme. In response to these flaws we propose OBSCURE TOKEN (O-TOKEN), an extension of REWIRE to enable revocation in a privacy preserving manner. Our approach addresses the functional and authentication properties by introducing an additional key-pair, which offers a stronger and verifiable guarantee of successful revocation of vehicles without resolving the long-term identity. Moreover O-TOKEN is the first V2X revocation protocol to be co-designed with a formal model.

**Keywords:** Ad hoc networks · Authentication · Security verification · V2X

## 1 Introduction

The term Intelligent Transportation Systems (ITS) denotes the on-going trend to include information and communication technologies (ICT) in vehicles and transportation infrastructure in order to enable safer, coordinated, environmentally

G. Livraga and C. Mitchell (Eds.): STM 2017, LNCS 10547, pp. 147–163, 2017.
DOI: 10.1007/978-3-319-68063-7_10

friendly, and smarter transportation networks [35]. Having smarter transportation systems typically involves extending the communication capabilities between the involved entities.

This goes by the term "Vehicle-to-X (V2X)" communication and involves various forms of ad-hoc and cellular networking among vehicles and traffic infrastructure. Security and privacy in V2X have played an important role right from the start [22].

In particular, anonymity is a requirement in a V2X network as various privacy issues arise from the frequent and real-time broadcasting of the position of vehicles in an ITS [31], as otherwise mobility patterns can easily be identified. This makes tracking and profiling of entities possible, which can be used to systematically collect and infer private information. Pseudonym certificates (pseudonyms) [25] are the most commonly applied way to address privacy concerns and are also foreseen in emerging standards.

Schaub et al. [31] discuss various requirements for such a pseudonym system and Petit et al. [25] survey a large body of existing work and from there identify an abstract pseudonym life cycle which is comprised of five main phases: issuance, use, change, resolution and revocation. Within an ITS architecture there are three trusted third parties that support the life cycle of pseudonyms: a certification authority (CA), a provider of pseudonyms (PP), and a revocation authority (RA). The CA issues long-term credentials to vehicles. The PP is responsible for handing out shorter-lived pseudonym certificates. The RA receives and collects information such as reports on misbehaviour, takes decisions to revoke a misbehaving entity, and implement this revocation by whatever means a specific scheme foresees.

Effective revocation has been identified as a challenge [29] due to the decentralised nature of vehicle networks and the ability of vehicles to change their active pseudonyms.

*Related Work.* Pseudonym revocation techniques have largely been based on the distribution of certificate revocation lists (CRLs) [25,29], such that when a misbehaving vehicle is revoked an updated CRL is broadcast to all vehicles. Several approaches have been taken to optimise the protocols and distribution process of CRL delivery [10,13,15,17,20,24]. However, these approaches often either revoke only one pseudonym of a vehicle – thereby missing the goal of removing a misbehaving vehicle completely – or they create a way of linking pseudonyms – then hurting privacy protection.

Bißmeyer et al. [2] propose the CORPA protocol that allows conditional pseudonym resolution which preserves the privacy.

Raya et al. propose an infrastructure-based revocation protocol [29], which remotely deletes keys in a trusted component. Their protocol requires that a vehicle's identity is known to perform revocation, in combination with a CRL – again a clear drawback with respect to privacy.

Schaub et al. propose $V$-Tokens [30], which introduces embedding vehicle resolution information directly into pseudonyms. A V-Token is a ciphertext field in the pseudonym certificate that is created from a vehicle's identity, the

CA's identity and a randomisation factor $r$ all encrypted with the RA's public key. In this scheme multiple trusted parties need to collaborate to resolve the pseudonym, which then reveals a vehicle's identity that is used for revocation. In case of a revocation, this therefore violates the privacy of vehicles, as resolution of their pseudonym to an identity is required.

Förster et al. propose PUCA [11], a pseudonym scheme based on anonymous credentials where privacy of the vehicle owner has absolute priority and no way exists for resolving pseudonyms. PUCA foresees no way of credential revocation. However, the same authors then also propose REWIRE [12], a modular revocation mechanism within a decentralised network which is not relying on the resolution approach that can be used to introduce revocation in PUCA. Instead, REWIRE assumes on-board Trusted Components (TC) in vehicles to support revocation.

A series of EU research projects, e.g., SeVeCom [23], EVITA [33] and PRECIOSA [26] have investigated securing V2X architectures using TCs. The recent project PRESERVE [27] has even prototyped this in an ASIC for secure ITS. Feiri et al. [9] propose to use TCs to store pseudonyms in secure storage and use a physical-unclonable function (PUF) to reduce the need for large amounts of secure storage. Based on such earlier work, it seems a reasonable assumption that hardware security modules (HSMs) are available as trust anchors, as done in the specification of our O-TOKEN approach.

In this paper we explore the two versions of the REWIRE protocols [12], which are referred to as REWIRE PLAIN and R-TOKEN. This protocol represents the current state of the art of those proposed for revocation in V2X architectures. No revocation protocol has been deployed in vehicles as yet.

*Contribution.* In this paper, we describe the formalisation of the revocation protocols proposed by Förster et al. [12], which was done using multiset rewriting as supported by the TAMARIN prover. These protocols have not previously been formally analysed. We present definitions of functional correctness and authentication as properties of the protocols. Our formal analysis reveals that the PLAIN model does not preserve functional correctness, specifically that a vehicle is not guaranteed to be revoked and therefore could continue to participate in communication messages within an ITS. This formally confirms a flaw that was observed by Förster et al. [12]. Our analysis of the R-TOKEN protocol identifies a hitherto unknown flaw: that it does not guarantee authentication properties, in particular it does not guarantee that the confirmation of revocation actually came from the intended vehicle. This new unknown weakness is acknowledged by the authors of the R-TOKEN protocol as a flaw.

The insights gained from the formal modelling motivated our proposal for a new protocol. We therefore develop a new protocol which proposes improvements to the REWIRE protocols that ensures correct revocation of an entity under any pseudonym without requiring resolution even if its active pseudonym has changed by the time of revocation. In this paper we refer to our new protocol as the OBSCURE TOKEN (O-TOKEN) protocol. Its novelty is the inclusion of an additional asymmetric key pair for signature, used to augment the pseudonyms that are utilised within message exchanges for verifiable revocation. The new protocol is shown to preserve all the desired authentication and functional correctness properties. Our proposed protocol, similar to the previous protocols discussed in this paper, requires a trusted device at the car which will engage in the revocation protocol and on completion can be trusted to erase all of the pseudonyms that the car may have available.

Due to limited space, we will not present the details of the TAMARIN model rules and lemmas in this paper. The models of the three protocols presented in this paper have been made available [34].

*Structure.* This paper is organised as follows: Section 2 presents a revocation scenario. Section 3 introduces TAMARIN, together with the security notation used throughout the paper and the modelling assumptions made in our symbolic models. Section 4 defines formal models and evaluates the existing REWIRE protocols. Section 5 presents our new enhanced REWIRE protocol and its analysis and Section 6 finally provides conclusions and identifies preservation of privacy properties as an area of future analysis for revocation protocols.

## 2 System Model and Revocation Scenario

The process of revocation for the existing REWIRE protocols and our O-TOKEN protocol follows the same pattern shown in Fig. 1. Figure 1 illustrates the three main authorities in an ITS, namely the CA, the PP and the RA, and how vehicles interact with them. The purpose of these authorities and vehicles in a revocation scenario is as follows:

- The CA and PP issue long-term certificates and pseudonyms respectively to vehicles and may optionally implement a resolution mechanism to allow linking back pseudonyms to long-term IDs.
- Vehicles in the ITS communicate with other participants. They monitor each others behaviour using misbehaviour detection mechanisms [14] and may issue reports of vehicle misbehaviour to the RA.
- The RA collects misbehaviour reports from participating vehicles in an ITS, and takes a decision to revoke reported pseudonyms. It then creates and broadcasts signed revocation messages to the misbehaving vehicle.
- Vehicles receive and process revocation commands to revoke their pseudonyms, and send confirmations back to the RA.

The REWIRE protocols and our variant has the following steps: In step 1 vehicle $V_1$ obtains a long-term certificate from the CA enabling it to obtain pseudonyms. In step 2 $V_1$ obtains pseudonyms from the PP to communicate securely with other vehicles including vehicle $V_2$. Steps 1 and 2 are not part of a revocation protocol itself, rather they are part of the issuance phase of pseudonyms. During the communication in the ITS, vehicle $V_1$ will receive messages from $V_2$ under a pseudonym which could be changed frequently. $V_2$ will apply misbehaviour detection mechanisms [14] in order to detect indications of faulty or malicious behaviour. Examples of such mechanisms may detect spoofed positions or incorrect speeds reported in messages.

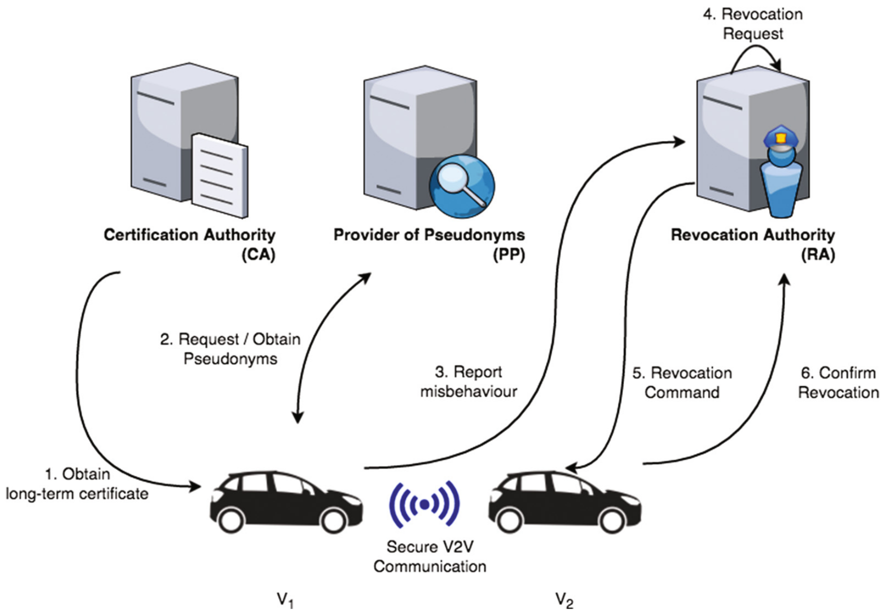

**Fig. 1.** High-level V2X revocation scenario

In such cases, step 3 is triggered by $V_1$ submitting a misbehaviour report to the RA accusing $V_2$ of misbehaviour. Similarly other vehicles may make the same report to the RA against $V_2$ (omitted from the diagram). The RA takes a decision to have $V_2$'s access to the ITS infrastructure revoked if some threshold is reached. Then the RA crafts a report containing the reason for revocation and $V_2$'s current pseudonym (step 4). Following the receipt, a revocation message is broadcast to all vehicles in step 5. $V_2$ receives the designated revocation message and its TC will be triggered to delete all of its pseudonyms. Finally, $V_2$ constructs and sends a confirmation message back to the RA in step 6 to inform the RA all of its pseudonyms were deleted.

## 3 Background and Assumptions

### 3.1 TAMARIN

We model and analyse all three protocols, the PLAIN and R-TOKEN protocols and our new O-TOKEN protocol in Sect. 5 using the TAMARIN prover. For this paper we give a general description of what the TAMARIN tool provides. There are several full introductions to the tool [18,19,32] for further details.

The TAMARIN prover is a symbolic analysis tool that is based on multiset rewriting rules and first order logic. It supports the analysis of security protocols, which are described using multi-set rewrite rules to describe actions corresponding to protocol agents taking part in protocol steps. Protocol messages are modelled as terms which enable cryptographic protocol constructions such as encryption, decryption, signatures and hashing to be expressed. Thus the terms in Table 1 are all expressible in TAMARIN syntax. The global state of the system is captured as a multi-set of Facts, which are expressed as predicates on terms, of the form $F(t_1, \ldots, t_n)$. A rewrite rule, labelled by an action, takes a multi-set of facts, and replaces (or rewrites) them with another multi-set of facts, labelled by an action.

A Dolev-Yao adversary is also built into the tool. The rewrite rules induce a transition system describing the potential executions of (unbounded numbers of) protocol instances in the context of the adversary. The transition system has a formal semantics which underpins the soundness of the tool.

Properties on the actions can be expressed using first-order logic, enabling requirements on executions to be defined. TAMARIN enables the analysis of the transition system with respect to such properties. Authentication properties are typically of the form "for every execution, if action $a_2$ occurs then action $a_1$ must previously have occurred". For example, if $a_2$ corresponds to agent $A$ receiving a confirmation message, and $a_1$ corresponds to $B$ sending that message, then the authentication property is that $A$'s receipt of the message guarantees that $B$ sent it (i.e., it was not spoofed by the adversary). If every execution satisfies this property then the protocol provides the authentication required.

TAMARIN has numerous built-in security theories that abstractly support common cryptographic functions. For example, in this paper we use the *signing* built-in which models a signature scheme. It provides the function symbols `sign` and `verify` such that digital signatures can be verified using the equation: `verify(sign(m, sk), m, pk(sk)) = true`.

### 3.2 Security Notation and Analysis

The notation defined in Table 1 is used across all models in the paper. The last three entries are specific to our new protocol in Sect. 5. The following seven proof goals are considered in this paper to model our correctness requirements.

*G1: Executable* ensures the model is executable and demonstrates successful transmission of all core messages. It is a sanity check of the model's correctness.

*G2: Weak agreement*, defined by Lowe [16], is a form of authentication which guarantees that when an initiator $A$ completes a run of the protocol then it was interacting with another agent $B$ who had also been running the protocol. In the revocation protocols the initiator $A$ is the RA and an agent $B$ is a vehicle.

*G3: Non-injective agreement*, again defined by Lowe [16], adds a further condition to ensure that the two agents, $A$ and $B$, agree on the roles they are taking and agree on the data items used in their message exchange. In our protocols *non-injective agreement* guarantees that the RA and vehicle both agree upon the completion of a run with each other and that in those runs the contents of the received messages correspond to the sent messages.

*G4: Non-injective synchronisation*, defined by Cremers and Mauw [5], is very similar to *non-injective agreement* but additionally requires that the corresponding send and receive messages have to be executed in their expected

**Table 1.** Security notation

| Syntax | | Description |
|---|---|---|
| $V_j$ | | An arbitrary vehicle $j$ |
| $SK_{V_j}$ | $PK_{V_j}$ | Asymmetric key pair for $V_j$ |
| $Ps_{i(V_j)}$ | | $i^{th}$ pseudonym of $V_j$ |
| $SK_{Ps_i(V_j)}$ | $PK_{Ps_i(V_j)}$ | Asymmetric pseudonym key pair for $V_j$'s $i^{th}$ pseudonym |
| $SK_{RA}$ | $PK_{RA}$ | Asymmetric key pair for the RA |
| $\sigma_{Ps_i(V_j)} := \{\| V_j \,\|\|\, PK_{V_j} \,\|\|\, r \,\|\}_{SK_{V_j}}$ | | An R-TOKEN of the $i^{th}$ pseudonym of $V_j$, where $r$ is a nonce |
| $LTK_{V_j}$ | | Long-term symmetric key of a vehicle $V_j$ (replaces asymmetric pair in line 2 above) |
| $SK_{O_{Ps_i(V_j)}}$ | $PK_{O_{Ps_i(V_j)}}$ | Asymmetric key pair for an O-TOKEN, belonging to the$i^{th}$ pseudonym of $V_j$ |
| $\phi_{Ps_i(V_j)} := \{\| SK_{Ps_i(V_j)} \|\}_{LTK_{V_j}}$ | | An O-TOKEN of the $i^{th}$ pseudonym of $V_j$ |

order. This means that in the revocation protocols revoke messages are sent later than receive messages. This means that if a protocol preserves a *non-injective synchronisation* property then the corresponding *non-injective agreement* property will also hold.

*G5: Revoke after change esists*, defined in this paper, states that if a vehicle changes its pseudonym and a previous pseudonym is revoked, it should still be possible for the vehicle to create a message to confirm the Revocation Authority (RA) that it has taken the action for revocation. This is a sanity check that the a vehicle can be revoked even after a change of pseudonym.

*G6: Order for self revocation (OSR) request received with change all*, defined in this paper, indicates that if a vehicle receives the OSR request, the vehicle will perform the revocation and create a confirmation.

*G7: Revoke with change all*, defined in this paper, states that if a confirmation of a pseudonym revocation is accepted by the RA from a vehicle then that vehicle will have accepted and processed a revocation request from the RA.

### 3.3 Modelling Assumptions

In this section we provide a scope for the protocols and identify the modelling abstractions that are used for the analysis. We assume that for each of the protocol models a registration and enrolment phase has executed, resulting in vehicles holding valid pseudonyms. All vehicles in a network have a Trusted Component (TC) and abstractly this means that (1). vehicle keys cannot be leaked, and (2). vehicles cannot ignore revocation messages. We consider the CA, PP and RA to be distinct roles and in the architecture there is one of each. These roles are all trustworthy and therefore, we remove the possibility of their keys leaking from the analysis.

Steps 1 and 2 in Sect. 2 denotes the issuing of pseudonyms to vehicles by the CA and will be abstractly captured as a rule within our models. A revocation protocol focuses on steps 3, 4, 5 and 6 from Fig. 1. Within the Tamarin model steps 3 and 4 are abstractly represented by a report event which the RA receives. Steps 5 and 6 are described in three rules which focus on the message exchange to revoke a vehicle and a confirmation to affirm the vehicle followed the request. All the formal models in this paper follow this pattern of communication but the format of the messages and the verification that can be performed on the signed messages changes with each protocol.

The Dolev-Yao adversary in our models is in control of the network and other untrusted parts of the system including the vehicles themselves. It is not in control of the TCs of the vehicles and the trusted third parties.

## 4 Rewire Protocols

This section describes our modelling and analysis of the Plain and R-token protocols. Our security and functional correctness analysis shows the following ***main results*** which are weaknesses in the existing protocols:

- If the Plain protocol executes a change of pseudonym, then no confirmation guarantee can be communicated to the RA. Hence even though authentication properties may hold, a misbehaving vehicle may avoid revocation by changing its pseudonym, and so functional correctness will not be guaranteed. While the original paper [12] already identified this issue and addressed it in the R-token version, Tamarin was independently able to discover this problem.
- Following attempted revocation of a vehicle's pseudonym the RA is unable to verify successful confirmation in the R-token scheme, thus none of the authentication properties hold. In particular a confirmation can be spoofed by a malicious agent and accepted by the RA, even when the misbehaving vehicle is not revoked. This flaw was not previously recognised.

### 4.1 REWIRE: Plain

***Modelling.*** Section 3.3 informally identified the steps of a revocation protocol based on the behaviour of an RA and a misbehaving vehicle. We model the protocol roles of the RA and an arbitrary vehicle ($V_j$) in Tamarin by a set of rewrite rules, which correspond to the steps of the protocol. The Plain model has three distinct types of rules to: (1). setup all required key pairs for secure communication, (2). create misbehaviour reports and (3). describe revocation requests and receiving subsequent confirmation.

The heart of the protocol involves an exchange of messages to effect revocation: an Order for Self-Revocation (OSR) request, followed by a confirmation response.

The OSR request message Osr-req [12] is the first message sent to a vehicle, which triggers its revocation process. Osr-req contains the command to revoke,

**Table 2.** Summary of results

| Goal | Content | PLAIN | R-TOKEN | O-TOKEN |
|---|---|---|---|---|
| G1 | `Executable` | ✓ | ✓ | ✓ |
| G2 | `Weak_agreement` | ✓ | × | ✓ |
| G3 | `Noninjective_agreement` | ✓ | × | ✓ |
| G4 | `Noninjective_synchronisation` | ✓ | × | ✓ |
| G5 | `Revoke_after_change_exists` | × | ✓ | ✓ |
| G6 | `Osr_req_received_with_change_all` | N/a | ✓ | ✓ |
| G7 | `Revoke_with_change_all` | N/a | × | ✓ |

the reported misbehaving pseudonym and additional information as to why the revocation occurred. The pseudonym $Ps_{i(V_j)}$ in this protocol is simply $PK_{Ps_{i(V_j)}}$ belonging to $V_j$. OSR-REQ is signed by the RA, and can be verified by receiving vehicles.

$$O\text{SR-REQ} := \{|\ \text{“}revoke\text{”} \ \|\ Ps_{i(V_j)} \ \|\ reason|\}_{SK_{RA}} \tag{1}$$

The OSR-REQ message is received and verified by a $V_j$, and the TC in $V_j$ can identify the pseudonym as belonging to $V_j$. Following this identification the vehicle constructs an OSR-CONF message confirming the command to revoke was followed, and the TC in $V_j$ will flag all available pseudonyms as revoked to prevent their future use in V2X communication. The OSR-CONF message is comprised of two terms: a confirm command and the active reported public pseudonym key.

The message is signed with the corresponding secret pseudonym key.

$$O\text{SR-CONF} := \{|\ \text{“}confirm\text{”} \ \|\ Ps_{i(V_j)} \ |\}_{SK_{Ps_{i(V_j)}}} \tag{2}$$

We model a well formed OSR-REQ message duly signed by the RA and addressed to its current pseudonym. The vehicle verifies that the message came from the RA and contains the vehicle's active pseudonym, before deleting all its pseudonyms and creating the OSR-CONF message signed under the active secret pseudonym key, which is sent back to the RA. The adversary is able to learn the OSR-REQ message terms and the signature. However the adversary cannot modify the contents of the message as the adversary does not posses the RA's secret key. We also model the incoming OSR-CONF message from a $V_j$. The RA verifies the OSR-CONF message is signed with the reported pseudonym $PK_{Ps_{i(V_j)}}$.

***Proof Goals.*** We state several proof goals for our model, G1-G7 discussed in Sect. 3.2, that represent authentication and functional correctness properties. The results of whether each of the numbered proof goals hold are summarised in Table 2. All the goals include predicates requiring that the vehicle's long-term key and secret pseudonym keys are not compromised, and so correct behaviour is dependent on these keys not being compromised.

A successful run of the model guarantees that $V_j$ was running the protocol with the RA. Receipt of the OSR-CONF message represents completion of a run for the RA. An OSR-REQ message is represented by facts from both the RA and vehicle's perspective. The model observes that the RA will have completed a run and verified a confirmation from a vehicle. Furthermore, the vehicle must have received the OSR-REQ message before it is possible for the RA to receive the OSR-CONF message, hence the communication order is preserved. The above proof goals are trace authentication properties demonstrating that the attacker cannot construct OSR-REQ or OSR-CONF messages from its observations. Thus no logical attacks are identified for the PLAIN protocol from our symbolic analysis.

### 4.2 REWIRE: PLAIN with Change of Pseudonym

***Modelling.*** In the PLAIN pseudonym scheme revocation of REWIRE [12], a *change of pseudonym* for a vehicle can occur at any point prior to an OSR-REQ being received. For example, consider a vehicle $V_1$ and two of its pseudonyms $Ps_{1(V_1)}$ and $Ps_{2(V_1)}$ in the following change of pseudonym scenario. When the RA receives a report to revoke $V_1$, it broadcasts the OSR-REQ message containing the misbehaving pseudonym $Ps_{1(V_1)}$, as shown in Fig. 2. However, before an OSR-REQ message is ever received by $V_1$ a change of pseudonym can occur resulting in a new pseudonym now being active. In an naïve implementation, changing to $Ps_{2(V_1)}$ means that the receipt of the OSR-REQ will be ignored as the vehicle has deleted its previous pseudonym. Therefore, no OSR-CONF message will be generated by $V_1$ as the vehicle has deleted its previous pseudonyms and the revocation process will fail. Consequently $V_1$ can continue to misbehave under the new pseudonym $Ps_{2(V_1)}$.

We model the changing of pseudonyms in such a way that the model creates a fresh pseudonym key for an arbitrary vehicle $V_j$. The "can change" fact is included to control when a vehicle can change its current pseudonym. The model concludes by storing the new pseudonym secret key for $V_j$ and outputs the public key of the new pseudonym, which the intruder learns.

***Proof Goals.*** Adding this extra behaviour to the protocol yields another proof goal, G5, discussed in Sect. 3.2. If a vehicle changes its pseudonym and a previous pseudonym is revoked, it should be possible for the vehicle to create an OSR-CONF

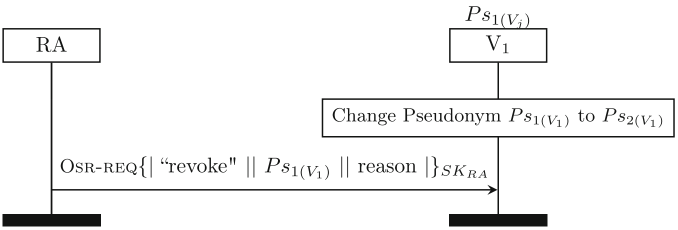

**Fig. 2.** REWIRE: PLAIN pseudonym scheme incomplete run

message. This model fails for the PLAIN protocol, showing that the protocol does not guarantee a successful revocation of a misbehaving vehicle in the presence of changing pseudonyms, and indeed that if a vehicle changes its pseudonym then it can escape revocation. Therefore, the PLAIN protocol is not functionally correct in the context of changing pseudonyms. To address this shortcoming in [11,12] a variant to the PLAIN protocol is proposed, referred to as the R-TOKEN protocol.

### 4.3 REWIRE: R-TOKEN

***Modelling.*** The R-TOKEN variant embeds additional information in pseudonym certificates with the aim of allowing revocation even with changing pseudonyms. This additional information is an R-TOKEN, $\sigma_{Ps_i(V_j)}$, which is constructed from a vehicle's public identity, public key and a nonce $r$, encrypted under a vehicle's secret key. There is a fresh R-TOKEN for each pseudonym. $Ps_{i(V_j)}$ in this protocol is a pseudonym containing $PK_{Ps_i(V_j)}$ and the R-TOKEN $\sigma_{Ps_i(V_j)}$.

It is the purpose of the R-TOKEN to allow a vehicle to later detect whether a revocation request is directed to it, without allowing others to identify the vehicle. By encrypting the R-TOKEN under $SK_{V_j}$, all vehicles must attempt to decrypt the R-TOKEN. Only the correct vehicle can decrypt the R-TOKEN, meaning the revocation was designated for the vehicle and should be executed.

In PUCA and REWIRE a "cut and choose" approach [28] is used to generate the R-TOKEN, but in the model we have simply abstracted this to a fresh value that is encrypted under the secret key of the vehicle.

The R-TOKEN protocol is represented in Fig. 3. The OSR-REQ message is of the same format as the PLAIN protocol where the pseudonym contains the R-TOKEN. Once a vehicle receives an OSR-REQ it attempts to decrypt the R-TOKEN irrespective of its active pseudonym. Only the designated vehicle can decrypt the R-TOKEN since the decryption uses $SK_{V_j}$, others will simply ignore

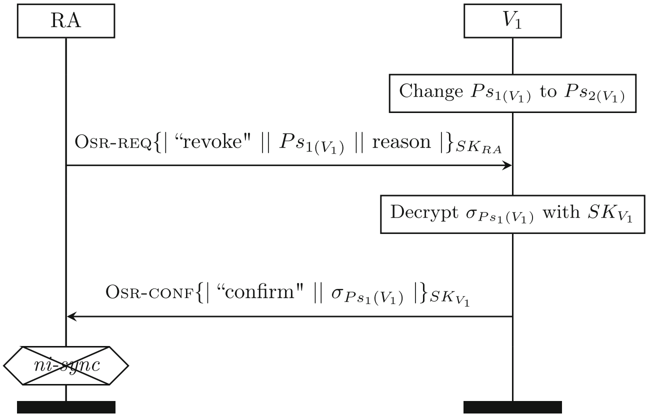

**Fig. 3.** REWIRE: R-TOKEN scheme

the OSR-REQ. The OSR-CONF message now contains the R-TOKEN and not the pseudonym, and the message is signed with the vehicle's secret key.

$$O\text{SR-CONF} := \{\mid \text{"}confirm\text{"} \mid\mid \sigma_{Ps_i(V_j)} \mid\}_{SK_{V_j}} \quad (3)$$

The modelling of the rules for the R-TOKEN protocol is almost identical but there are two important changes. Firstly the model includes having to decrypt the R-TOKEN as an additional action. Secondly, the model is weakened to remove the `verify` step (which checks the correctness of the confirmation $\sigma_{Ps_i(V_j)}$) since the RA is not in possession of the $PK_{V_j}$.

***Proof Goals.*** For consistency we analysed functional correctness. All the proof goals for the PLAIN protocol remain applicable. Proof goal G5 holds because any vehicle can create a confirmation message. Two additional goals are included to analyse the correct behaviour of the vehicle (G6) and RA (G7) in the context of changing pseudonyms, as shown in Table 2. For each goal we again assume that $SK_{V_j}$ is not compromised. The security analysis yields that neither of the authentication properties hold. The adversary is able to intercept the OSR-REQ message and create a OSR-CONF message containing the inferred R-TOKEN. The adversary then generates a fresh secret key which is used to sign the OSR-CONF message. The created OSR-CONF is sent to the RA. The RA accepts the confirmation but cannot verify its authenticity because the $LTK_{V_j}$ is only known to $V_j$ and CA. Therefore, The RA does not obtain a guarantee that it is communicating with a running vehicle.

This flaw in the protocol was not previously recognised, and has been accepted by the designers of the R-TOKEN protocol.

## 5 O-TOKEN Protocol

***Modelling.*** To solve the issue of the RA not being able to verify the confirmation message, OSR-CONF, we propose the O-TOKEN protocol. Note that the O-TOKEN mimics the R-TOKEN closely: the reason for generating different O-TOKENS for each pseudonym is the same as for the R-TOKEN, to ensure unlinkability of the vehicle in question. If the R-TOKEN or O-TOKEN remained the same, it would act as a vehicle identifier.

We replace the R-TOKEN in the previous scheme with a simpler construction: an O-TOKEN for the $i^{th}$ pseudonym of $V_j$, $\phi_{Ps_i(V_j)}$, consisting of an $SK_{O_{Ps_i(V_j)}}$ key which is encrypted under $LTK_{V_j}$. Each O-TOKEN is fresh and associated with one and only one $Ps_{i(V_j)}$ pseudonym.

$$\phi_{Ps_i(V_j)} \ := \ \{\mid SK_{O_{Ps_i(V_j)}} \mid\}_{LTK_{V_j}}$$

The aim of using fresh $SK_{O_{Ps_i(V_j)}}$ keys is to make pseudonyms unlinkable.

The pseudonym also contains one additional field, $PK_{O_{Ps_i(V_j)}}$, which is the corresponding public key for the particular O-TOKEN. Therefore, the pseudonym contains enough information for the RA to verify a received OSR-CONF message and for the vehicle to change its pseudonym.

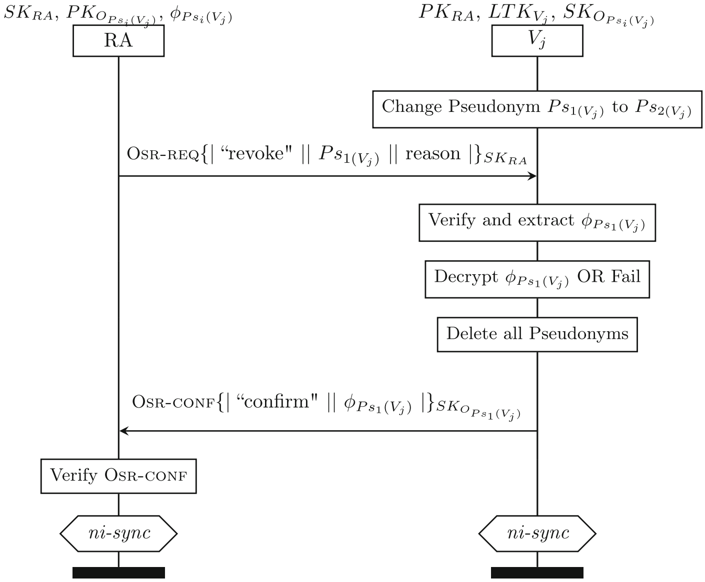

**Fig. 4.** O-TOKEN revocation

A revocation run which uses O-TOKEN is shown in Fig. 4. The OSR-REQ message is of the same format as the other protocols but the pseudonym contains the O-TOKEN. The OSR-CONF message now contains the O-TOKEN and the message is signed with $SK_{O_{Ps_i(V_j)}}$ instead of signing with $LTK_{V_j}$ which the vehicle extracted earlier:

$$O\text{SR-CONF} := \{|\text{"}confirm\text{"} \mid\mid \phi_{Ps_i(V_j)} \;|\}_{SK_{O_{Ps_i(V_j)}}} \tag{4}$$

The subtle change in signing the OSR-CONF message, together with the RA's knowledge of $PK_{O_{Ps_i(V_j)}}$enables the RA to verify the confirmation message.

The modelling of the other rules for the O-TOKEN protocol is largely similar but there are two further changes. Firstly, the rule for receiving the OSR request includes having to decrypt the O-TOKEN as an additional action, Secondly, changing pseudonym behaviour is supported with a new rule, by creating a fresh pseudonym secret key, a fresh $SK_{O_{Ps_i(V_j)}}$ and the newly encrypted O-TOKEN.

***Proof Goals.*** The results for the formal analysis for the O-TOKEN protocol is presented in Table 2 and achieves all desired guarantees. Notably all the authentication properties hold which means that the RA is communicating with the revoked vehicle and can verify the received confirmation, which was not the case with the R-TOKEN protocol. Therefore, all the desired functional correctness properties hold.

## 6 Conclusions and Future Work

The new O-token protocol proposed in this paper allows revocation even if vehicles have changed pseudonym. It also allows the RA to verify a confirmation sent by a vehicle that it has deleted its pseudonyms. The formal analysis establishes that verifying such a confirmation provides a guarantee that the revocation occurred. We have therefore shown through formal analysis that the desired functional correctness and authentication properties hold. The new O-token protocol for Rewire was developed by first formally modelling and analysing the two previous variants of Rewire, then identifying weaknesses in their functional correctness and a failure to meet required authentication properties.

In an implementation of a revocation protocol, heartbeats provide protection against non-delivery of revocation requests by incorporating such requests within the heartbeats. TCs within a vehicle expect heartbeats (which may contain revocation requests), which are generated by the RA. TCs will take appropriate action if they are not received, under the assumption that they have been blocked. Therefore, augmenting a formal analysis with heartbeats will require a more detailed model of a TC and further adversarial behaviour. With respect to the greater level of detail timestamps may also be important in modelling time out behaviour of heartbeats. The inclusion of time may also allow us to model the retention of keys before the deletion of pseudonyms. TC's could also consider storing the last $k$ pseudonyms and the analysis would need to ensure that the adversary could not evade revocation by changing pseudonym at least $k$ times.

Another consideration in an implementation is the handling of cases where no confirmation is sent. If heartbeats are not used then further revocation requests will need to be sent until confirmation is received.

In the analysis, we currently focus on functional correctness and authentication. In future work we will consider generalising the correctness analysis, in particular G5, to include liveness properties such that we could prove a more general property such as "any revocation request must eventually be confirmed". The Tamarin tool chain has been extended in a recent paper by Backes *et al.* [21] to enable verification of liveness properties. Not considered here are privacy requirements such as unlinkability which could likewise merit a formal analysis.

Delaune and Hirschi [7] and Chadha et al. [4] survey various anonymity and privacy related properties, including anonymity, unlinkability and strong secrecy, which can be proved using equivalence-based reasoning. Behavioural equivalence allows us to determine whether two situations are different, in particular whether the confirmation of a revocation came from one vehicle or another. The use of process equivalences to analyse privacy properties can also be seen in Tamarin [1] and in other modelling tools, e.g. ProVerif [3], which has been used successfully to analyse privacy properties [6,8]. Future work will be to explore anonymity and privacy properties of revocation protocols and of other V2X protocols.

Our proposed protocol requires a trusted device at the car which can be trusted to erase all of the pseudonyms that the car may have available. However, it is still under debate whether this is the right trust model for the car. Furthermore, which functions is it reasonable to place within this trusted device, and which cannot be made trustworthy? To answer these questions in a satisfactory way is not straightforward, and to make the vehicle industry reach agreement on a specific trust model is even more demanding. This is an interesting challenge for future work.

**Acknowledgements.** Jorden Whitefield is funded by EPSRC iCASE studentship 15220193 through Thales UK. Thanks to Cas Cremers for detailed discussions on TAMARIN. Thanks also to François Dupressoir and Adrian Waller for detailed feedback, and to the reviewers for their constructive comments.

## References

1. Basin, D.A., Dreier, J., Sasse, R.: Automated symbolic proofs of observational equivalence. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, pp. 1144–1155 (2015)
2. Bißmeyer, N., Petit, J., Bayarou, K.M.: CoPRA: conditional pseudonym resolution algorithm in VANETs. In: 2013 10th Annual Conference on Wireless On-demand Network Systems and Services (WONS), pp. 9–16. IEEE (2013)
3. Blanchet, B., Smyth, B., Cheval, V.: Proverif 1.96: automatic cryptographic protocol verifier, user manual and tutorial (2016). http://prosecco.gforge.inria.fr/personal/bblanche/proverif/manual.pdf
4. Chadha, R., Cheval, V., Ciobâcă, Ş., Kremer, S.: Automated verification of equivalence properties of cryptographic protocols. ACM Trans. Comput. Log. **17**(4), 23:1–23:32 (2016)
5. Cremers, C., Mauw, S.: Operational Semantics and Verification of Security Protocols. Information Security and Cryptography. Springer, Heidelberg (2012)
6. Dahl, M., Delaune, S., Steel, G.: Formal analysis of privacy for vehicular mix-zones. In: Gritzalis, D., Preneel, B., Theoharidou, M. (eds.) ESORICS 2010. LNCS, vol. 6345, pp. 55–70. Springer, Heidelberg (2010). doi:10.1007/978-3-642-15497-3_4
7. Delaune, S., Hirschi, L.: A survey of symbolic methods for establishing equivalence-based properties in cryptographic protocols. J. Log. Algebraic Methods Program. **87**, 127–144 (2017)
8. Fazouane, M., Kopp, H., van der Heijden, R.W., Métayer, D., Kargl, F.: Formal verification of privacy properties in electric vehicle charging. In: Piessens, F., Caballero, J., Bielova, N. (eds.) ESSoS 2015. LNCS, vol. 8978, pp. 17–33. Springer, Cham (2015). doi:10.1007/978-3-319-15618-7_2
9. Feiri, M., Petit, J., Kargl, F.: Formal model of certificate omission schemes in VANET. In: 2014 IEEE Vehicular Networking Conference, VNC 2014, Paderborn, Germany, 3–5 December 2014, pp. 41–44 (2014)
10. Fischer, L., Aijaz, A., Eckert, C., Vogt, D.: Secure revocable anonymous authenticated inter-vehicle communication (SRAAC). In: 4th Conference on Embedded Security in Cars (ESCAR 2006), Berlin, Germany (2006)
11. Förster, D., Kargl, F., Löhr, H.: PUCA: a pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. Ad Hoc Netw. **37**(Part 1), 122–132 (2016). Special Issue on Advances in Vehicular Networks

12. Förster, D., Löhr, H., Zibuschka, J., Kargl, F.: REWIRE - revocation without resolution: a privacy-friendly revocation mechanism for vehicular ad-hoc networks. In: Trust and Trustworthy Computing - 8th International Conference, TRUST 2015, Heraklion, Greece, 24–26 August 2015, Proceedings, pp. 193–208 (2015)
13. Haas, J.J., Hu, Y.C., Laberteaux, K.P.: Efficient certificate revocation list organization and distribution. IEEE J. Sel. Areas Commun. **29**(3), 595–604 (2011)
14. van der Heijden, R.W., Dietzel, S., Leinmüller, T., Kargl, F.: Survey on misbehavior detection in cooperative intelligent transportation systems. CoRR abs/1610.06810 (2016). http://arxiv.org/abs/1610.06810
15. Kondareddy, Y., Di Crescenzo, G., Agrawal, P.: Analysis of certificate revocation list distribution protocols for vehicular networks. In: Global Telecommunications Conference (GLOBECOM 2010), pp. 1–5, IEEE (2010)
16. Lowe, G.: A hierarchy of authentication specifications. In: 10th Computer Security Foundations Workshop, pp. 31–44. IEEE Computer Society (1997)
17. Ma, Z., Kargl, F., Weber, M.: Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications. In: IEEE 68th Vehicular Technology Conference, 2008. VTC 2008-Fall, pp. 1–5. IEEE (2008)
18. Meier, S., Schmidt, B.: Tamarin prover - information security group — eth zurich (2016). http://www.infsec.ethz.ch/research/software/tamarin.html. Accessed 18 Jan 2017
19. Meier, S., Schmidt, B., Cremers, C., Basin, D.: The TAMARIN prover for the symbolic analysis of security protocols. In: Sharygina, N., Veith, H. (eds.) CAV 2013. LNCS, vol. 8044, pp. 696–701. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39799-8_48
20. Michael, E.N., Henry, L.O.: Scalable certificate revocation list distribution in vehicular ad hoc networks. In: GLOBECOM Workshops (GC Wkshps), pp. 54–58. IEEE (2010)
21. Backes, M., Jannik Dreier, S.K., Künnemann, R.: A novel approach for reasoning about liveness in cryptographic protocols and its application to fair exchange. In: 2nd IEEE European Symposium on Security and Privacy (2017)
22. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., Hubaux, J.P.: Secure vehicular communication systems: design and architecture. IEEE Commun. Mag. **46**(11), 100–109 (2008)
23. Papadimitratos, P., Buttyan, L., Hubaux, J.P., Kargl, F., Kung, A., Raya, M.: Architecture for secure and private vehicular communications. In: 2007 7th International Conference on ITS Telecommunications, pp. 1–6. IEEE (2007)
24. Papadimitratos, P.P., Mezzour, G., Hubaux, J.P.: Certificate revocation list distribution in vehicular communication systems. In: Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, pp. 86–87. ACM (2008)
25. Petit, J., Schaub, F., Feiri, M., Kargl, F.: Pseudonym schemes in vehicular networks: a survey. IEEE Commun. Surv. Tutor. **17**(1), 228–255 (2015)
26. PRECIOSA: European commission : Cordis : Projects and results service : Privacy enabled capability in co-operative systems and safety applications (2010). http://cordis.europa.eu/project/rcn/86606_en.html. Accessed 31 Jan 2017
27. PRESERVE: www.preserve-project.eu — preparing secure V2X communication systems (2011). https://preserve-project.eu/. Accessed 31 Jan 2017
28. Rabin, M.O.: Digitalized signatures and public-key functions as intractable as factorization. In: Foundations of Secure Computation, pp. 155–168 (1978)
29. Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.P.: Eviction of misbehaving and faulty nodes in vehicular networks. IEEE J. Sel. A. Commun. **25**(8), 1557–1568 (2007)

30. Schaub, F., Kargl, F., Ma, Z., Weber, M.: V-Tokens for conditional pseudonymity in VANETs. In: 2010 IEEE Wireless Communications and Networking Conference, WCNC 2010, Proceedings, Sydney, Australia, 18–21 April 2010, pp. 1–6 (2010)
31. Schaub, F., Ma, Z., Kargl, F.: Privacy requirements in vehicular communication systems. In: Computational Science and Engineering, CSE 2009, vol. 3, pp. 139–145, IEEE (2009)
32. Schmidt, B., Meier, S., Cremers, C.J.F., Basin, D.A.: Automated analysis of Diffie-Hellman protocols and advanced security properties. In: 25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, 25–27 June 2012, pp. 78–94 (2012)
33. Weyl, B., Henniger, O., Ruddle, A., Seudie, H., Wolf, M., Wollinger, T.: Securing vehicular on-board IT systems: the EVITA project. In: 25th Joint VDI/VW Automotive Security Conference, Ingolstadt, Germany (2009). http://www.evita-project.org/Publications/HRSW09.pdf
34. Whitefield, J., Chen, L., Kargl, F., Schneider, S., Treharne, H., Wesemeyer, S.: Formal analysis of V2X revocation protocols (2017). http://www.computing.surrey.ac.uk/personal/st/H.Treharne/papers/2017/rewire.html
35. Willke, T.L., Tientrakool, P., Maxemchuk, N.F.: A survey of inter-vehicle communication protocols and their applications. IEEE Commun. Surv. Tutor. **11**(2), 3–20 (2009)