Identity-based Conditional Privacy-Preserving Authentication Scheme Resistant to Malicious Subliminal Setting of Ephemeral Secret

Patryk Kozieł, Łukasz Krzywiecki and Damian Stygar
Department of Computer Science, Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology, Poland

Keywords: Authentication, Bilinear Pairing, Elliptic Curve, Vehicular Ad-hoc Networks, Ephemeral Secret Setting, Ephemeral Secret Leakage.

Abstract: In this paper we propose a modification of the Identity Based *Conditional Privacy-Preserving Authentication Scheme* (CPPA), which is based on Schnorr *Signature Scheme* (*SS*). The applicability and the security of the scheme is mainly considered in Intelligent Transportation Systems. We discuss scenarios with subliminal malicious setting of a ephemeral secret. We present a new, stronger security model for the scheme in which we allow the adversary to choose random values used during signing process. We define the *SS* to be secure if the advantage of the adversary in this model is negligible. Finally we prove the security of the modified Identity Based CPPA in our stronger model.

1 INTRODUCTION

In recent years Vehicular Sensor Networks (VSNs) have became an interest of a lot of researchers. They provide a lot of opportunities for modern transportation. Collecting information in real time can support traffic management and driving safety, especially in heavy traffic scenarios, road defects or bad weather conditions. There exist many propositions for cryptographic schemes applicable to VSNs (e.g. (Li et al., 2018)). Vehicular Ad-Hoc Network (VANET) is a subset of Mobile Ad-Hoc Network (MANET), a network that is continuously self-configuring and does not have a fixed infrastructure. VANET supports communication between vehicles (V2V) and between vehicles and road side units (V2I). Two of the crucial features we require from such networks in the context of cryptography are security and privacy preserving of the identities of the participants. VANET is mainly used for providing safety related information and traffic conditions. Traffic management directly impacts driving comfort and safety. We can easily imagine scenarios in which maliciously altered traffic-related data causes dangerous circumstances on the road. Hence the legitimacy of the messages is one of our primary concerns.

1.1 Problem Statement and Motivation

It is very prevalent in cryptographic schemes to use *ephemeral* values, i.e. values drawn randomly from some sets and used in subsequent processing. We are mainly interested in scenarios in which an adversary (who we will call *forger* from this moment on) has the ability to learn how ephemeral secrets are produced or inject them by herself. In particular some implementations of the pseudo-random number generators (PRNG) can be prone to attacks (e.g. (Dorrendorf et al., 2007)) or even deliberately constructed maliciously. It is also known that certification of hardware for cryptographic purposes can be a long and costly process, so many small producers choose cheap, but rather not trustworthy devices available on the market.

Many PRNGs are constructed in such a way that if the attacker learns the current state of the generator, then she can also predict its future outputs. A very basic example is Linear Congruential Generator (LCG). Breaking of this generator is often presented for students as an exercise.

Ephemeral leakage can often result in ability to forge signatures, impersonation or discovery of a secret key. This is why there is a lot of research on the security of PRNGs. However, we propose a different approach in which the security of the generator is not crucial anymore.

Kozieł, P., Krzywiecki, Ł. and Stygar, D.
Identity-based Conditional Privacy-Preserving Authentication Scheme Resistant to Malicious Subliminal Setting of Ephemeral Secret.
DOI: 10.5220/0007954204920497
In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019)*, pages 492-497
ISBN: 978-989-758-378-0

In the context of VSNs we are mainly concerned with situations where protocols are executed using untrustworthy devices, e.g. not certificated or maybe not updated by the manufacturer but claiming to meet the security standards.

In this paper we focus on the Identity Based *Conditional Privacy-Preserving Authentication Scheme* (He et al., 2015) in scenarios with the injecting/leaking of the ephemerals. We provide a new security model with ephemeral leakage, propose a modification of that scheme, and prove that it is a secure solution in our proposed model. We chose to research on this particular scheme because we noticed that improvement (in a sense of protection against ephemeral leakage) is possible and can be formally proved. We devote this paper entirely to this scheme because any modifications of secure schemes require a very careful analysis to ensure that current security features are not compromised.

1.2 Contribution

The contribution of the paper is the following:

- We propose a new security model for Identity-Based Conditional Privacy Preserving Authentication Schemes, stronger than the usual one. In this model the forger is able to choose and inject ephemerals in the signing process.
- **We propose a modification** of Identity-Based Conditional Privacy-Preserving Authentication Scheme from (He et al., 2015), originally not secure in scenarios with ephemeral leakage/injection. We prove the security of the modification in the strong model.

1.3 Previous Work

In VANETs, privacy and message integrity is a widely researched concept. The legitimacy of the traffic related messages is crucial for safe traffic management. On the other hand, we require that a vehicle which sends traffic information cannot be tracked (privacy), except in the situations when it provides malicious information. Then some trusted third party should be able to discover the identity of such vehicle. That is the motivation for supporting conditional privacy and anonymous message authentication. Currently, there exist Conditional Privacy-Preserving Authentication schemes, e.g. ECPP (Lu et al., 2008), CPAS (Shim, 2012), RAISE (Zhang et al., 2008), PCPA (Ming and Shen, 2018). Usually the security of ephemeral values or leakage consequences are not discussed by the authors. The discussion on the leakage of the ephemeral key and countermeasures have been shown for Schnorr Identification Scheme (Krzywiecki, 2016) and for Okamoto Identification Scheme (Krzywiecki and Kutylowski, 2017).

The paper is organized in the following way. In Section 2 we recall Identity-Based Conditional Privacy-Preserving Authentication Scheme. In Section 3.3.2 we introduce our stronger security model which includes the ephemeral setting by the forger. In section 3 we propose the modified version of Identity-Based CPPA, and prove its security in our model.

2 IDENTITY-BASED CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION SCHEME

2.1 Preliminaries and Notation

Let $\mathcal{G}(1^\lambda)$ be a (randomized) group generation algorithm that takes as an input 1^λ, and outputs a tuple $\mathbb{G} = (G_1, G_2, G_T, g, \hat{g}, q)$, where q is a prime number, $G_1 = \langle g \rangle$, $G_2 = \langle \hat{g} \rangle$, $|G_1| = |G_2| = q$, and G_T is another group of prime order q. Let x be a private key of the system and $X = g^x$ be a public key. Let V denote the real identity of a vehicle. AID denotes an anonymous identity of a vehicle which consists of two elements $\{W, \overline{W}\}$. Let $\mathcal{H}_1 : G_1 \to \mathbb{Z}_q^*$, $\mathcal{H}_2 : \{0,1\}^* \to \mathbb{Z}_q^*$, $\mathcal{H}_3 : \{0,1\}^* \times \{0,1\}^* \times G_1 \times \{0,1\}^* \to \mathbb{Z}_q^*$, $\mathcal{H}_4 : G_1 \times \mathbb{Z}_q^* \to G_2$ represent four secure hash functions. We will use the following operations: $\oplus$ - XOR and "," - string concatenation inside a hash. Let m denote an element from the set of all possible messages $\mathcal{M}$.
Bilinear Map: Let G_1, G_2, G_T be groups of a prime order q. We define $\hat{e} : G_1 \times G_2 \to G_T$ as a bilinear pairing such that the following condition holds:
1) *Bilinearity*: $\forall a, b \in \mathbb{Z}_q^*, \forall g_1 \in G_1, \forall g_2 \in G_2$: $\hat{e}(g_1^a, g_2^b) = \hat{e}(g_1, g_2)^{ab}$.
2) *Non-degeneracy*: $\hat{e} \neq 1$.
3) *Computability*: $\hat{e}$ is efficiently computable.
The *Discrete Logarithm* (DL) Assumption: For any probabilistic polynomial time (PPT) algorithm $\mathcal{A}_{\mathsf{DL}}$ it holds that:
$\Pr[\mathcal{A}_{\mathsf{DL}}(\mathbb{G}, g^x) = x \mid \mathbb{G} \leftarrow \mathcal{G}(1^\lambda), x \xleftarrow{\$} \mathbb{Z}_q^*] \leq \varepsilon_{\mathsf{DL}}(\lambda)$, where $\varepsilon_{\mathsf{DL}}(\lambda)$ is negligible.
The *Computational Diffie-Hellman* (CDH) Assumption: For any probabilistic polynomial time (PPT) algorithm $\mathcal{A}_{\mathsf{CDH}}$ it holds that:
$\Pr[\mathcal{A}_{\mathsf{CDH}}(\mathbb{G}, g^x, g^y) = g^{xy} \mid \mathbb{G} \leftarrow \mathcal{G}(1^\lambda), x \xleftarrow{\$} \mathbb{Z}_q^*, y \xleftarrow{\$} \mathbb{Z}_q^*] \leq \varepsilon_{\mathsf{CDH}}(\lambda)$, where $\varepsilon_{\mathsf{CDH}}(\lambda)$ is negligible.
The *Decisional Diffie-Hellman* Oracle ($\mathcal{O}_{\mathsf{DDH}}$) denotes the (PPT) algorithm, which for $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda), x \in$

$\mathbb{Z}_q^*, y \in \mathbb{Z}_q^*, z \in \mathbb{Z}_q^*$
$\mathcal{O}_{\mathsf{DDH}}(\mathbb{G}, g^x, g^y, g^z) = 1$ iff $z = xy \mod q$.

The *Computational co-Diffie-Hellman* (CcDH) Assumption: (Saito and Uchiyama, 2004) For any probabilistic polynomial time (PPT) algorithm $\mathcal{A}_{\mathsf{CcDH}}$ it holds that:
$\Pr[\mathcal{A}_{\mathsf{CcDH}}(\mathbb{G}, a, a^x, b) = b^x \mid \mathbb{G} \leftarrow \mathcal{G}(1^\lambda), x \xleftarrow{\$} \mathbb{Z}_q^*, a \in G_1, b \in G_2] \leq \varepsilon_{\mathsf{CcDH}}(\lambda)$, where $\varepsilon_{\mathsf{CcDH}}(\lambda)$ is negligible.

2.2 VANET Model

We model VANET using two layers:

- Upper Layer which consists of:
  - third party Trusted Authority (TA) responsible for generating parameters and loading them to tamper-proof devices in vehicles and discovering the real identities of the vehicles if needed
  - Application Server supporting safety-related applications at the traffic management center.
- Bottom Layer:
  - The Road Side Units (RSUs) - wireless communication devices located at roadside able to communicate with vehicles. It can verify the validity of received messages and sends them to the traffic management center or process them locally.
  - Vehicles equipped an On-Board Unit (OBU) for communication. The OBU is a tamper-proof device. The vehicle communicates wirelessly with RSUs using the OBU.

2.3 Signature Schemes

2.3.1 Identity-based Conditional Privacy-Preserving Authentication Scheme Definition

Definition 1. *Identity-Based Conditional Privacy-Preserving Authentication Scheme* (CPPA) *is a system which consists of five algorithms* (ParGen, KeyGen, AIDGen, AIDSign, Verify)*:*

$\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$**:** *takes the security parameter λ as input, and outputs public parameters available to all users of the system*

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}$**:** *creates a pair of the public key and the secret key of the system and identities of the users.*

$(\mathsf{t}, \mathsf{sk}_t, \mathsf{TempAID}) \leftarrow \mathsf{AIDGen}(\mathsf{V}, \mathsf{password}, \mathsf{sk})$*: verifies identity* V *with provided* password *and creates a timestamp* t *and associated with it secret key* sk_t *based also on the secrey key of the system and anonymous identity* TempAID.

$\sigma \leftarrow \mathsf{AIDSign}(\mathsf{t}, \mathsf{sk}_t, \mathsf{TempAID}, \mathsf{m})$**:** *an algorithm creating a signature over the provided message using private temporary key and the identity. The signature plays roles both authenticating the message and identifying the signer.*

$\mathsf{Verify}(\mathsf{t}, \mathsf{TempAID}, \mathsf{pk}, \mathsf{m}, \sigma)$**:** *an algorithm verifying if signature over given message is valid taking into account the public key, the timestamp and* AID *identity.*

The scheme is actually an extended identification scheme in which a prover together with identifying herself sends authenticated messages at the same time. The algorithms generating the key for the users are assumed to be secure and deployed in tamper-proof devices. In this particular case the security of the scheme depends solely on the security of the signature scheme, so unforgeability of the underlying signature scheme determines if the whole scheme is secure. Our exact modification is actually posing new security requirements for the signature scheme. Therefore in this paper we focus mostly on malicious ephemeral setting in the context of the signature scheme used in the main scheme.

3 MODIFIED IDENTITY-BASED CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION SCHEME

Our proposed modified Identity-Based Conditional Privacy-Preserving Authentication Scheme is depicted in Figure 1 alongside the regular scheme. Points with suffix "mod" come from modified version. The signing procedure requires one exponentiation and one call to hash function more. In the verification procedure one additional call to hash function and two executions of the bilinear pairing are required. In Theorem 3 we show that if an adversary attacking regular version of the scheme knows the ephemeral value from AIDSign, then she can easily compute the private key. Our solution is to mask this ephemeral value in such a way that knowledge of it does not allow to recover the secret key. We propose usage of a bilinear pairing.

3.1 Batch Verification

The original scheme supports also batch verification. Here we omit discussion on this feature. Our modification is also scalable for verification of multiple messages at once. The full modification and the security proof is planned for future research.

Parameters initialization:

$\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$: Let $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$, s.t. DL and CDH assumptions hold.

Key Generation:

1. $\mathsf{KeyGen}()$: $\mathsf{sk} = x \leftarrow \mathbb{Z}_q^*$, $\mathsf{pk} = X = g^x$. Output $(\mathsf{sk}, \mathsf{pk})$.
2. Trusted Authority (TA) assigns a real identity V and a password for each vehicle and pre-loads $\{V, password, x\}$ into its tamper-proof device.
3. The system parameters are sent to all RSUs and vehicles by the TA.

AID generation: (in a tamper-proof device) If V and password are equal to the stored ones then:

1. $w \xleftarrow{\$} \mathbb{Z}_q^*$
2. $W = g^w$
3. $\overline{W} = V \oplus \mathcal{H}_1(X^w)$
4. $h_2 = \mathcal{H}_2(AID||t)$
5. $v = w + h_2 \cdot x$
6. $AID = \{W, \overline{W}\}$
7. sends a tuple $\{AID, v, t\}$ to the vehicle.

AID Signing: The vehicle generates:

1. $r \xleftarrow{\$} \mathbb{Z}_q^*$
2. $R = g^r$
3. $h_3 = \mathcal{H}_3(AID, t, R, m)$
4. $s = v + h_3 \cdot r$
5. sends $\{m, AID, t, R, s\}$ to the verifier

5mod $\hat{g} = \mathcal{H}_4(R, h_3)$

6mod $S = \hat{g}^s$

7mod sends $\{m, AID, t, R, S\}$ to the verifier

Verification: The verifier checks:

1. freshness of t
2. $\{W, \overline{W}\} = AID$
3. $h_2 = \mathcal{H}_2(AID||t)$
4. $h_3 = \mathcal{H}_3(AID, t, R, m)$
5. acceptance if $g^s = W \cdot X^{h_2} \cdot R^{h_3}$

5mod $\hat{g} = \mathcal{H}_4(R, h_3)$

6mod acceptance if $\hat{e}(S, g) = \hat{e}(\hat{g}, WX^{h_2}R^{h_3})$

Figure 1: Identity-Based Conditional Privacy-Preserving Authentication Scheme - Regular and Modified versions.

3.2 Correctness of the Proposed Scheme

Theorem 1 (Correctness)**.** *The Modified Identity-Based Conditional Privacy-Preserving Authentication Scheme, depicted in Figure 1 is correct, that is:*

$$\begin{gathered}\Pr[\mathsf{Verify}(\mathsf{t}, \mathsf{TempAID}, \mathsf{pk}, \mathsf{m}, \sigma) = 1| \\ \sigma \leftarrow \mathsf{AIDSign}(\mathsf{t}, \mathsf{sk}_t, \mathsf{TempAID}, \mathsf{m}), \\ \mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda), \\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(), \\ (\mathsf{t}, \mathsf{sk}_t, \mathsf{TempAID}) \leftarrow \mathsf{AIDGen}(\mathsf{V}, \mathsf{password}, \mathsf{sk})] = 1\end{gathered}$$

Proof. For properly generated keys the produced signature is always accepted by the verifier.

$$\hat{e}(S,g) = \hat{e}(\hat{g}^s, g) = \hat{e}(\hat{g}, g^s) = \hat{e}(\hat{g}, g^{v+h_3*r}) =$$
$$= \hat{e}(\hat{g}, g^{w+h_2x+h_3r}) = \hat{e}(\hat{g}, g^w g^{h_2x} g^{h_3r)} =$$
$$= \hat{e}(\hat{g}, g^w X^{h_2} R^{h_3})$$

□

3.3 Security Analysis

3.3.1 New Stronger Security Model for Signatures

Definition 2 (Signature Scheme)**.** *Signature Scheme* (SiS) *is a system which consists of four algorithms* (ParGen, KeyGen, Sign, Verify)*:*

$\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$**:** *takes the security parameter λ as input, and outputs public parameters available to all users of the system.*

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}()$**:** *outputs the secret key* sk *and corresponding public key* pk*.*

$\mathsf{Sign}(\mathsf{sk}, m)$**:** *an algorithm creating a signature over the provided message using private key.*

$\mathsf{Verify}(\mathsf{pk}, m, \sigma)$**:** *an algorithm to verify that signature over given message is valid.*

We say that signature scheme is correct if for any pair $(\mathsf{sk}, \mathsf{pk})$:

$$\Pr[\mathsf{Verify}(\mathsf{pk}, m, \sigma) = 1 | \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)] = 1.$$

To address the scenario with ephemeral leakage/injection we propose a new, stronger security model for SiS, based on models introduced in (Krzywiecki, 2016; Krzywiecki and Kutylowski, 2017). In this particular model in the *learning phase* the malicious forger $\mathcal{F}$ has the ability to inject ephemeral secrets to the signing procedure.

Let $\bar{r}$ be a ephemeral secret chosen by $\mathcal{F}$. Signing procedure executed by an honest signer with injected $\bar{r}$ will be denoted by $\mathsf{Sign}^{\bar{r}}$. The signer uses value $\bar{r}$ as its random short term secret key. Let ℓ be the number of executions of Sign method (polynomial in λ).

Definition 3 (Chosen Ephemeral Forger – (CEF))**.** *Let* SiS = (ParGen, KeyGen, Sign, Verify,) *be a signature scheme. We define security experiment* $\mathsf{Exp}_{\mathsf{SiS}}^{\mathsf{CEF},\lambda,\ell}$*:*

`Init` : $\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$, $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}()$.

`Sign Oracle` : *The sign oracle $O_S^{\bar{r}}$ accepts messages m_i, ephemerals $\bar{r}_i$ and outputs corresponding positively verifiable signatures σ_i generated with the $\bar{r}_i$, i.e. $O_S^{\bar{r}_i}(m_i) \rightarrow \sigma_i$, s.t.* $\mathsf{Verify}(m_i, \sigma_i, \mathsf{pk}) = 1$.

The oracle models the device in which the signatures are generated via the algorithm Sign, *with injected ephemerals, controlled externally by the adversary:* $\sigma \leftarrow \mathsf{Sign}^{\bar{r}}(m)$.

`Forger` : *Let the forger* $\mathcal{F}^{O_S^{\bar{r}}}(\mathsf{pk}, \mathsf{par})$, *be the malicious algorithm initialized with the public key* pk *and parameters, having access to the signing oracle* $O_S^{\bar{r}}$. *The forger* $\mathcal{F}^{O_S}$ *issuess a number* ℓ *of queries to* $O_S^{\bar{r}}$ *with the messages of its choice obtaining the corresponding signatures, where* $\bar{r}_i, m_i, \sigma_i$ *denote respectively: the ephemeral values, the message, and the signature in ith oracle query. Let* $\mathcal{R} = \{\bar{r}_1, \ldots, \bar{r}_\ell\}$ $\mathcal{M} = \{m_1, \ldots, m_\ell\}$, *and* $\mathcal{L} = \{\sigma_1, \ldots, \sigma_\ell\}$ *denote the set of the ephemerals, the set of the inputs, and corresponding outputs the oracle processes.*

`Forgery` : *The forger generates a pair:* $(m^*, \sigma^*) \leftarrow \mathcal{F}^{O_S^{\bar{r}}}(\mathsf{pk}, \mathsf{par})$.

We define the advantage of $\mathcal{F}$ *in the experiment* $\mathtt{Exp}_{\mathsf{SiS}}^{\mathsf{CEF},\lambda,\ell}$ *as probability of positive verification:*

$$\mathbf{Adv}(\mathcal{F}, \mathtt{Exp}_{\mathsf{SiS}}^{\mathsf{CEF},\lambda,\ell}) = \\ = \Pr[m^* \notin \mathcal{M}, \mathsf{Verify}(m^*, \sigma^*, \mathsf{pk}) \to 1].$$

We say that the signature scheme is secure if $\mathbf{Adv}(\mathcal{F}, \mathtt{Exp}_{\mathsf{SiS}}^{\mathsf{CEF},\lambda,\ell})) \leq \varepsilon(\lambda)$, *where* $\varepsilon(\lambda)$ *is negligible.*

Theorem 2. *The modified* ModSchnorrSig *Signature scheme, obtained by applying Fiat-Shamir transformation on Identification Scheme from (Krzywiecki, 2016) is secure in* CEF *model, assuming the CcDH hardness and programmable ROM.*

Sketch. Essentially the same as the proof of the security of (Krzywiecki, 2016) scheme, utilizing the Forking Lemma (Pointcheval and Stern, 1996). Omitted due to space constraints (to be included in the future research). □

3.3.2 New Stronger Security Model for CPPA Scheme

Definition 4. *Let* CPPA = (ParGen, KeyGen, AIDGen, AIDSign, Verify) *be a given scheme. We define security experiment* $\mathtt{Exp}_{\mathsf{CPPA}}^{\mathsf{CEF},\lambda,\ell}$:

`Init` : $\mathsf{par} \leftarrow \mathsf{ParGen}(1^\lambda)$, $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}()$.

`AIDGen Oracle` : *The oracle* O_{AIDGen} *accepts identifiers* V *and outputs* AID, v, t. *It models tamper resistant device with the secret key* x, *which produces secret key* v *for pseudonym* AID.

`AIDSign Oracle` : *The oracle* $O_{\mathsf{AIDSign}}^{\bar{r}}$ *accepts messages* m_i, *ephemerals* $\bar{r}_i$ *and outputs corresponding positively verifiable signatures* $\sigma_i = AID, t, R_i, S_i$ *generated with the* $\bar{r}_i$, *i.e.* $O_{\mathsf{AIDSign}}^{\bar{r}_i}(m_i) \to \sigma_i$, *s.t.* $\mathsf{Verify}(m_i, \sigma_i, \mathsf{pk}) = 1$. *The oracle models the device in which the signatures are generated via the algorithm* AIDSign, *with injected ephemerals, controlled externally by the adversary:* $\sigma \leftarrow \mathsf{AIDSign}^{\bar{r}}(m)$.

`Adversary` : *Let the adversary* $\mathcal{A}^{O_{\mathsf{AIDGen}}, O_{\mathsf{AIDSign}}^{\bar{r}}}(\mathsf{pk}, \mathsf{par})$, *be the malicious algorithm initialized with the public key* pk *and parameters, having access to the AID oracle* O_{AIDGen}, *and the signing oracle* $O_{\mathsf{AIDSign}}^{\bar{r}}$. *The* $\mathcal{A}^{O_{\mathsf{AIDGen}}, O_{\mathsf{AIDSign}}^{\bar{r}}}$ *issuess a number* ℓ *of queries to oracles. Let* $A = \{AID_i, v_i, t_i\}_1^\ell$ $\mathcal{R} = \{\bar{r}_i\}_1^\ell$, $\mathcal{M} = \{m_i\}_1^\ell$, *and* $\mathcal{L} = \{\sigma_i\}_1^\ell$ *denote respectively the set of pseudonyms with keys, the set of the ephemerals, the set of the inputs, and the corresponding outputs the oracles processes.*

`Impersonation` : *The adversary generates a pair:* $(m^*, \sigma^*) \leftarrow \mathcal{A}^{O_{\mathsf{AIDGen}}, O_{\mathsf{AIDSign}}^{\bar{r}}}(\mathsf{pk}, \mathsf{par})$.

We define the advantage of $\mathcal{A}$ *in the experiment* $\mathtt{Exp}_{\mathsf{CPPA}}^{\mathsf{CEF},\lambda,\ell}$ *as probability of positive verification:*

$$\mathbf{Adv}(\mathcal{A}, \mathtt{Exp}_{\mathsf{CPPA}}^{\mathsf{CEF},\lambda,\ell}) = \\ = \Pr[m^* \notin \mathcal{M}, AID^* \notin A, \mathsf{Verify}(m^*, \sigma^*, \mathsf{pk}) \to 1].$$

We say that the signature scheme is secure if $\mathbf{Adv}(\mathcal{A}, \mathtt{Exp}_{\mathsf{CPPA}}^{\mathsf{CEF},\lambda,\ell})) \leq \varepsilon(\lambda)$, *where* $\varepsilon(\lambda)$ *is negligible.*

Theorem 3. *The original Identity-Based Conditional Privacy-Preserving Authentication Scheme is not secure in the sense of Definition 4.*

Proof. The adversary $\mathcal{A}$ with the knowledge of ephemeral the $\bar{r}$ is able to compute the secret key of the vehicle $v = s - h_3\bar{r}$. Therefore the adversary can generate positively verifiable signature over any message later on. □

Theorem 4. *Let* CPPA *denote the modified Identity-Based Conditional Privacy-Preserving Authentication Scheme.* CPPA *is secure (in the sense of Definition 4).*

Sketch of the proof. We provide the adversary the access to O_{AIDGen}, and O_{AIDSign} oracles. The oracles can be programmed via standard simulation of Schnorr signatures, and registering the inputs and outputs of hash queries in corresponding ROM tables. The O_{Sign} oracle uses injected ephemerals by forger. The proof is by contradiction. Suppose there is an adversary $\mathcal{A}_{\mathsf{AIDSign}}$ which would authenticate with non-negligible probability without the appropriate secret key obtained from AIDGen procedure. We assume that the advantage of the adversary is non-negligible. In the attack stage, by Forking Lemma, we get two tuples (m, AID, t, R, S_1), (m, AID, t, R, S_2). Subsequently those tuples can be used to obtain $\hat{g}^v$, also with non-negligible probability, for any value $\hat{g}$, provided to the $\mathcal{A}_{\mathsf{AIDSign}}$ adversary as the answer from programmable $\mathcal{O}_{\mathcal{H}_4}$ oracle. Therefore the adversary can be used as a subprocedure by the efficient algorithm $\mathcal{F}_{\mathsf{ModSchnorrSig}}$ that forges the modified Schnorr signature scheme, obtained by Fiat-Schamirr transformation on (Krzywiecki, 2016) scheme. □

3.4 Performance

Additional assessments of complexity were performed. They are not included in this paper due to the space constraint and the fact that they are not essential in the context of this paper, however they were acceptable in real-world applications.

4 CONCLUSION

We modified the Identity-Based CPPA from (He et al., 2015) to a version resistant to ephemeral key setting. This kind of setting can be used by the adversary in scenarios with possible leakage/injection of ephemeral values. In such scenarios a secret key masked by the ephemeral value is not secure even if it is stored in the secure memory module in the device. We proposed the stronger security model to cover that particular scenario and proved the security of the proposed scheme in our model.

ACKNOWLEDGEMENTS

This paper was supported by Wroclaw University of Science and Technology, grant S50129/K1102.

REFERENCES

Dorrendorf, L., Gutterman, Z., and Pinkas, B. (2007). Cryptanalysis of the random number generator of the windows operating system. Cryptology ePrint Archive, Report 2007/419. https://eprint.iacr.org/2007/419.

He, D., Zeadally, S., Xu, B., and Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. In *IEEE Transactions on Information Forensics and Security (Volume: 10 , Issue: 12 , Dec. 2015), August 31, 2015*, pages 2681–2691.

Krzywiecki, L. (2016). Schnorr-like identification scheme resistant to malicious subliminal setting of ephemeral secret. In *In Innovative Security Solutions for Information Technology and Communications - 9th International Conference, October 05, 2016*, pages 137–148.

Krzywiecki, L. and Kutylowski, M. (2017). Security of okamoto identification scheme: a defense against ephemeral key leakage and setup. In *in Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing, April, 2017*, pages 43–50.

Li, C., Zhang, X., Wang, H., and Li, D. (2018). An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks. *Sensors*, 18(1):194.

Lu, R., Lin, X., Zhu, H., Ho, P.-H., and Shen, X. (2008). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, April 13-18, 2008*, pages 1229–1237.

Ming, Y. and Shen, X. (2018). PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks. In *Sensors 2018*.

Pointcheval, D. and Stern, J. (1996). Security proofs for signature schemes. In Maurer, U., editor, *Advances in Cryptology — EUROCRYPT '96*, pages 387–398, Berlin, Heidelberg. Springer Berlin Heidelberg.

Saito, T. and Uchiyama, S. (2004). The co-diffie-hellman problem over elliptic curves. *Reports of the Faculty of Science and Engineering*, 33(1):1–8.

Shim, K.-A. (2012). CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. In *IEEE Trans. Veh. Technol., vol. 61, no. 4, May, 2012*, pages 1874–1883.

Zhang, C., Lin, X., Lu, R., and Ho, P.-H. (2008). RAISE:an efficient rsu-aided message authentication scheme in vehicular communication networks. In *2008 IEEE International Conference on Communications, May 19-23, 2008*, pages 1451–1457.