

# Lightweight Privacy Preserving Authentication and Encryption Scheme for V2X

Key Policy Attribute Based Encryption *for V2X*

---

Vikhyath Sai Kothamasu (cs20btech11056)

December 19, 2022

Indian Institute of Technology Hyderabad

# Table of contents

1. Introduction
2. Related Work
3. Design Goals
4. Preliminaries
5. Originally Proposed Scheme
6. Modified Scheme
7. Conclusion

# Introduction

---

- Vehicle-To-Everything (V2X) is communication between a vehicle and any entity that may affect, or may be affected by, the vehicle. It is a key component in Cooperative Intelligent Transportation Systems (C-ITS).

# Introduction

- Vehicle-To-Everything (V2X) is communication between a vehicle and any entity that may affect, or may be affected by, the vehicle. It is a key component in Cooperative Intelligent Transportation Systems (C-ITS).
- It is a new generation of information and communication technology (ICT) that enables vehicles to communicate with adjacent peers and roadside infrastructures and is becoming increasingly important as the world is progressing towards autonomous driving.

short  
too  
long sentence

# Introduction

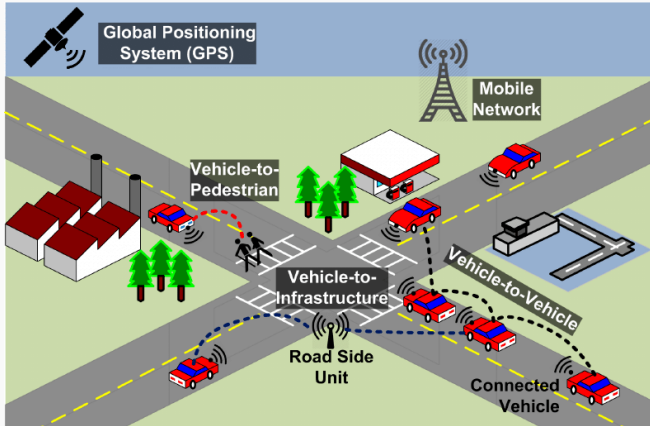


Figure 1: V2X setup

*Picture courtesy*

- V2X vehicles rely on continuous transmission of on-road traffic information via Cooperative Awareness Messages (CAMs)

- V2X vehicles rely on continuous transmission of on-road traffic information via Cooperative Awareness Messages (CAMs)
- Communication occurs over open insecure networks.



- V2X vehicles rely on continuous transmission of on-road traffic information via Cooperative Awareness Messages (CAMs)
- Communication occurs over open insecure networks.
- Vehicles do not want to be profiled since it might expose personal information like location and finally result in the user's identification.

- V2X vehicles rely on continuous transmission of on-road traffic information via Cooperative Awareness Messages (CAMs)
- Communication occurs over open insecure networks.
- Vehicles do not want to be profiled since it might expose personal information like location and finally result in the user's identification.
- Many traditional authentication systems are unsuitable for V2X due to bandwidth restrictions in C-ITS guidelines for CAMs.

- Pseudonym certificates are used by the European Telecommunications Standards Institute (ETSI) and the U.S. Department of Transportation (US-DOT) for anonymous V2X authentication.

## Mechanism:

- Each vehicle has a pool of pseudonyms, and each vehicle signs communications with a distinct pseudonym from the pool to verify them.

Mechanism:

- Each vehicle has a pool of pseudonyms, and each vehicle signs communications with a distinct pseudonym from the pool to verify them.
- Since pseudonym certificates are transient, updating them enables the vehicle to evade being traced for a lengthy period of time.

# Pseudonym Based Models

## Mechanism:

- Each vehicle has a pool of pseudonyms, and each vehicle signs communications with a distinct pseudonym from the pool to verify them.
- Since pseudonym certificates are transient, updating them enables the vehicle to evade being traced for a lengthy period of time.
- There are a few hybrid techniques that combine pseudonyms with other authentication methods including message authentication codes (MACs) and group signatures, but they do not totally preserve anonymity.

# Pseudonym Based Models

## Drawbacks:

- Ineffective against colluding adversaries and malicious infrastructure.
- Come with additional storage or download costs.
- Transmission of CAMs in plaintext which are easy to intercept.
- Easy to correlate signals from one particular vehicle.
- Hard to identify and locate eavesdropping devices.

Despite this, pseudonyms are still widely employed because they are quicker and more lightweight than more sophisticated authentication schemes and offer higher assurances of anonymity.

- The scheme contains the following entities:
  - Enrollment authority as issuer
  - Vehicles as users
  - Roadside Units (RSUs) as verifiers
- The main cryptographic primitives used in the scheme are:
  - Randomizable signatures
  - Symmetric Key Authenticated Encryption



# Anonymous Authentication

Vehicle proves the possession of credentials to the RSU anonymously using randomizable signatures.

- Vehicle obtains a single long-term credential

Vehicle proves the possession of credentials to the RSU anonymously using randomizable signatures.

- Vehicle obtains a single long-term credential
- On entering a new RSU zone, vehicle randomizes the long-term credential to generate a fresh short-term credential which is used to authenticate itself.

# Anonymous Authentication

Vehicle proves the possession of credentials to the RSU anonymously using randomizable signatures.

- Vehicle obtains a single long-term credential
- On entering a new RSU zone, vehicle randomizes the long-term credential to generate a fresh short-term credential which is used to authenticate itself.
- The short-term credentials cannot be linked to the long-term credentials or between zones.

*this may need explanation*

# Anonymous Authentication

Vehicle proves the possession of credentials to the RSU anonymously using randomizable signatures.

- Vehicle obtains a single long-term credential
- On entering a new RSU zone, vehicle randomizes the long-term credential to generate a fresh short-term credential which is used to authenticate itself.
- The short-term credentials cannot be linked to the long-term credentials or between zones.
- Impossible to identify a vehicle even if any entity colludes with the issuing authority.

# Symmetric Key Authenticated Encryption

Vehicle-to-vehicle communication is confidential when it is encrypted, and plain-text CAM data cannot be misused.

- RSU ties an attribute to the vehicle's credential from which the vehicle derives the secret key which is specific to that zone.

# Symmetric Key Authenticated Encryption

Vehicle-to-vehicle communication is confidential when it is encrypted, and plain-text CAM data cannot be misused.

- RSU ties an attribute to the vehicle's credential from which the vehicle derives the secret key which is specific to that zone.
- To derive a legitimate zone key, one has to be aware of the vehicle's secret upon which the long term credential is generated.

# Symmetric Key Authenticated Encryption

Vehicle-to-vehicle communication is confidential when it is encrypted, and plain-text CAM data cannot be misused.

- RSU ties an attribute to the vehicle's credential from which the vehicle derives the secret key which is specific to that zone.
- To derive a legitimate zone key, one has to be aware of the vehicle's secret upon which the long term credential is generated.
- The vehicle may still be (incorrectly) authorised by the RSU without the secret, but it won't be able to determine the zone key and won't be able to connect with any entities in that zone.

*needed  
for you  
with*

# Symmetric Key Authenticated Encryption

Vehicle-to-vehicle communication is confidential when it is encrypted, and plain-text CAM data cannot be misused.

- RSU ties an attribute to the vehicle's credential from which the vehicle derives the secret key which is specific to that zone.
- To derive a legitimate zone key, one has to be aware of the vehicle's secret upon which the long term credential is generated.
- The vehicle may still be (incorrectly) authorised by the RSU without the secret, but it won't be able to determine the zone key and won't be able to connect with any entities in that zone.
- The vehicles do not need to authenticate each CAM message since only an authenticated vehicle can obtain the secret zone key needed for communication.

may need a picture or flow diagram for a first time listener



## Related Work

---

- Pseudonym Certificate Authentication is preferred because of its efficiency.
- Elliptic Curve Digital Signature Algorithm (ECDSA) is well suited for V2X due to its short signature sizes and efficient verification.
- Direct anonymous attestation is one method based on group signatures that protects confidentiality from cooperating agencies. However, these authentication methods are computationally expensive since they require zero-knowledge proofs of knowledge (ZKPoKs) of signatures.
- Using modified PS signatures as characteristics, Camenisch presented a zone encryption system that draws on dynamic group signatures.

## Our Scheme

Proposed Scheme  
(Bisht, Kumar, Francis, Franklin, 21)

- Does not rely on a pseudonym authority.
- Vehicle authenticity is linked to the secret zone key derivation.
- Vehicles communicate using encrypted messages.
- ~~Our~~ <sup>The</sup> system is more effective since we can avoid using ZKPs thanks to authenticated encryption.

## Design Goals

---

# Anonymous Authentication

↓  
g'll make sure  
you come after  
Prashanth & Take  
so you can  
avoid all this.  
Mention it  
one side

We create credentials for the vehicles during enrolment using randomizable signatures. The vehicle's anonymity is maintained by the unforgeability and unlinkability characteristics of randomized signatures.

- Vehicles manage their short-term credentials, shifting the trust from a pseudonym authority to the user. This protects the user's privacy when any issuer colludes with any other entity.
- The credential is also made collusion-resistant by the unlinkability of randomized signatures.

Vehicles communicate via encrypted CAMs, prohibiting the use of CAM data for mass monitoring and profiling.

- Credential verification requires computationally intense ZKPoKs, which can be avoided as authentication is followed by key derivation, which requires a vehicle to know its secret.
- Use of temporary certificates is not required to sign and authenticate each communication.



# Preliminaries

---

# Notations

- $a \xleftarrow{R} X$  :  $a$  is chosen uniformly at random from the set  $X$ .
- $\mathbb{Z}_q$  : Group of integers modulo  $q$ .
- $\mathbb{Z}_q^*$  : Set  $\mathbb{Z}_q \setminus \{0\}$

# Bilinear Pairings

- Let  $G_1 = \langle g_1 \rangle$ ,  $G_2 = \langle g_2 \rangle$  be two additive cyclic groups of prime order  $q$ .
- Let  $\mathbf{G} = \langle g \rangle$  be a multiplicative cyclic group of order  $q$ .
- A bilinear pairing is defined as an efficiently computable map  $e : (G_1 \times G_2) \rightarrow \mathbf{G}$  satisfying the following properties:
  - Bilinearity:  $\forall x, y \in \mathbb{Z}_q^*, P \in G_1, Q, Q_1 \in G_2, e(xP, yQ) = e(P, Q)^{xy}$  and  $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
  - Non-degeneracy:  $e(g_1, g_2) \neq 1_{\mathbf{G}}$  i.e.  $e(g_1, g_2)$  is a generator of  $\mathbf{G}$
- $\mathcal{Gen}(1^k)$  : bilinear pairing group generator for security parameter  $k$  and prime  $q = \Theta(k)$ .
- Let  $(q, e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}) \xleftarrow{R} \mathcal{Gen}(1^k)$  be the asymmetric bilinear pairing group generated uniformly at random by  $\mathcal{Gen}(1^k)$ .
- The scheme works with Type-3 pairing groups: asymmetric pairing groups for which there is no known efficiently computable homomorphism from  $G_1$  to  $G_2$ .

## Co-computational Diffie-Hellman (Co-CDH) assumption

Given  $(q, e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}) \xleftarrow{R} \mathcal{Gen}(1^k)$ ,  $g_1^x, g_2^y$  where  $x, y \xleftarrow{R} \mathbb{Z}_q^*$ , for every PPT adversary  $\mathcal{A}$  there exists a negligible function  $\epsilon(k)$  such that

$$\Pr[\mathcal{A}((q, e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}), g_1^x, g_2^y) \rightarrow g_1^{xy}] \leq \epsilon(k)$$

## Decisional Bilinear Diffie-Hellman (DBDH) assumption

Given  $(q, e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}) \xleftarrow{R} \mathcal{Gen}(1^k)$ ,  $g_1^x, g_2^y, g_2^z$  where  $x, y, z \xleftarrow{R} \mathbb{Z}_q^*$ ,

Let  $D_0 = e(g_1, g_2)^{xyz}$  and  $D_1 = e(g_1, g_2)^c$ , where  $c \xleftarrow{R} \mathbb{Z}_q^*$ , for every PPT adversary  $\mathcal{A}$  there exists a negligible function  $\epsilon(k)$  such that

$$\begin{aligned} &Pr[\mathcal{A}((q, e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}), g_1^x, g_2^y, g_2^z, D_0) = 1] \\ &- Pr[\mathcal{A}((q, e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}), g_1^x, g_2^y, g_2^z, D_1) = 1] \leq \epsilon(k) \end{aligned}$$

# Randomizable Signatures

- Given a randomizable signature  $\sigma$  on a message  $\alpha$ , one can create another fresh valid signature  $\sigma'$  for  $\alpha$ , indistinguishable from  $\sigma$  by raising  $\sigma$  to a scalar  $r$ .
- A user can obtain a signature  $\sigma$  on some secret  $s$  from an issuer and then prove to a verifier that the secret  $\alpha$  is certified by an issuer. The proof remains unlinkable from all the previous times the user proves possession of the certificate to a verifier.

## Originally Proposed Scheme

---

- Setup  $\mathcal{S}(1^k)$  : Given security parameter  $k$ , output the type-3 bilinear pairing parameters  $(e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}) \xleftarrow{R} \mathcal{Gen}(1^k)$ .



- Setup  $\mathcal{S}(1^k)$  : Given security parameter  $k$ , output the type-3 bilinear pairing parameters  $(e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G}) \xleftarrow{R} \mathcal{Gen}(1^k)$ .
- Keygen  $\mathcal{K}(1^k)$  : The issuer generates  $sk = (x, y) \xleftarrow{R} \mathbb{Z}_q^*$  as its secret keys and publishes  $pk = (X = g_2^x, Y = g_2^y)$  as its public keys. The user generates  $(\alpha, \beta) \xleftarrow{R} \mathbb{Z}_q^*$  as its secrets and sends  $req = (a = g_1^\beta, b = a^\alpha)$  to the issuer for obtaining the credential.

- GenCred  $\mathcal{G}(sk, req)$  : The issuer verifies the vehicle and uses its secret keys to compute  $c = a^x, d = (a^\alpha \cdot c)^y = a^{y(\alpha+x)}$  and outputs the signature  $\sigma = (a, b, c, d)$ .

# Authentication Mechanism

- GenCred  $\mathcal{G}(sk, req)$  : The issuer verifies the vehicle and uses its secret keys to compute  $c = a^x, d = (a^\alpha \cdot c)^y = a^{y(\alpha+x)}$  and outputs the signature  $\sigma = (a, b, c, d)$ .
- Verify  $\mathcal{V}(\sigma, pk)$  : This algorithm takes the public keys of the issuer and credential of the user as input and verifies whether  $e(a, X) \stackrel{?}{=} e(c, g_2)$  and  $e(d, g_2) \stackrel{?}{=} e(b \cdot c, Y)$  are satisfied. On successful verification, it outputs 1 (accept), else 0 (reject).

# Correctness

$$\sigma = (a, b = a^\alpha, c = a^x, d = a^{y(\alpha+x)})$$

First verification

$$\begin{aligned} e(a, X) &\stackrel{?}{=} e(c = a^x, g_2) \\ &= e(a, g_2^x) \\ &= e(a, X) \end{aligned}$$

no need.  
explain  
Attribute  
based  
fuzzy

Second verification

$$\begin{aligned} e(d = a^{y(\alpha+x)}, g_2) &\stackrel{?}{=} e(b \cdot c, Y) \\ e(a, g_2)^{y(\alpha+x)} &= e(a^\alpha \cdot a^x, g_2^y) \\ &= e(a, g_2)^{y(\alpha+x)} \end{aligned}$$

# Randomizability and Unlinkability

The credential  $\sigma$  can be randomized by selecting  $r \xleftarrow{R} \mathbb{Z}_q^*$  and computing  $\bar{\sigma} = (a^r, b^r, c^r, d^r)$  which is still a valid credential but unlinkable from  $\sigma$ . Verification is as follows:

$$e(a^r, X) \stackrel{?}{=} e(c^r, g_2)$$

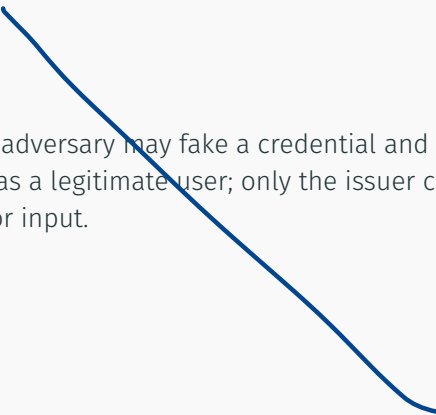
$$e(a, X)^r \stackrel{?}{=} e(c, g_2)^r$$

and

$$e(d^r, g_2) \stackrel{?}{=} e(b^r \cdot c^r, Y)$$

$$e(d, g_2)^r \stackrel{?}{=} e(b \cdot c, Y)^r$$

# Unforgeability



No effective adversary may fake a credential and authenticate themselves as a legitimate user; only the issuer can issue a valid credential for input.

# Key Generation Mechanism

With the RSU, the mechanism enables the authenticated vehicles to construct a symmetric key  $k_v$  for encrypted communication.

- $\text{Keygen } \mathcal{K}(1^k, c = a^x)$  : The key issuing authority generates attribute  $v \xleftarrow{R} \mathbb{Z}_q^*$ . The authority adds the attribute  $v$  to the credential  $\sigma$  by updating  $c$  to  $c' = c^v$  and returns it to the user. The commitment  $V = g_1^v$  is also published for verification of the derived key.

# Key Generation Mechanism

With the RSU, the mechanism enables the authenticated vehicles to construct a symmetric key  $k_v$  for encrypted communication.

- Keygen  $\mathcal{K}(1^k, c = a^x)$ : The key issuing authority generates attribute  $v \xleftarrow{R} \mathbb{Z}_q^*$ . The authority adds the attribute  $v$  to the credential  $\sigma$  by updating  $c$  to  $c' = c^v$  and returns it to the user. The commitment  $V = g_1^v$  is also published for verification of the derived key.
- Derive  $\mathcal{D}(c', \beta)$ : This algorithm derives the symmetric key  $g_1^{xv}$  as follows:  $(c')^{\beta^{-1}} = (a^{xv})^{\beta^{-1}} = (g_1^{\beta \cdot xv})^{\beta^{-1}} = g_1^{xv}$ .



# Key Generation Mechanism

Avoid this as you do not need it for ABE?

With the RSU, the mechanism enables the authenticated vehicles to construct a symmetric key  $k_v$  for encrypted communication.

- Keygen  $\mathcal{K}(1^k, c = a^x)$  : The key issuing authority generates attribute  $v \xleftarrow{R} \mathbb{Z}_q^*$ . The authority adds the attribute  $v$  to the credential  $\sigma$  by updating  $c$  to  $c' = c^v$  and returns it to the user. The commitment  $V = g_1^v$  is also published for verification of the derived key.
- Derive  $\mathcal{D}(c', \beta)$  : This algorithm derives the symmetric key  $g_1^{xv}$  as follows:  $(c')^{\beta^{-1}} = (a^{xv})^{\beta^{-1}} = (g_1^{\beta xv})^{\beta^{-1}} = g_1^{xv}$ .
- Verify  $\mathcal{V}(V, X, g_1^{xv})$  : Verifies whether  $e(V = g_1^v, X = g_2^x) \stackrel{?}{=} e(g_1^{xv}, g_2)$  is satisfied.

# CPA secure encryption scheme

- Setup  $\mathcal{S}(1^k)$  : Execute the key-generation mechanism  $(\mathcal{K}, \mathcal{D}, \mathcal{V})$  to generate the secret key  $k_v = g_1^{xv} = g_1^\gamma$ . The public parameters are  $(e, g_1, g_2, \mathbf{g}, G_1, G_2, \mathbf{G})$  and  $(X = g_2^x, V = g_1^v)$ .
- Encrypt  $\mathcal{E}(M)$  : For message  $M \in \mathbf{G}$ ,
  - select random  $r \in \mathbb{Z}_q$  and compute  $h = g_2^r$
  - compute  $w = e(k_v, h)$
  - ciphertext:  $C = (M \cdot e(k_v, h), h)$
- Decrypt  $\mathcal{D}(C)$  : To decrypt ciphertext  $C = (M \cdot e(k_v, h), h)$ ,
  - compute  $w = e(k_v, h)$
  - $M = \frac{C}{w}$

## Modified Scheme

---

# Attribute Based Encryption

Attribute based encryption (ABE) is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. It provides the ability to determine if data should be decrypted based on various attributes and policies.

bullets



keep  
V2X  
specific  
sample

Figure 2: ABE

# ABE vs other encryption schemes

more intuition than  
this for ABE is  
needed. Spend less  
time on Anonymous  
credentials.

In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based encryption changed this by allowing the public-key to be an arbitrary string. ABE goes one step further and defines the identity not atomic but as a set of attributes.

Make it  
points and  
more intuitive

ABE can be classified into 2 types:

- Ciphertext-Policy ABE (CP-ABE)
- Key-Policy ABE (KP-ABE)

- User's private key is associated with a set of attributes.
- Ciphertext specifies an access policy over a defined universe of attributes within the system.
- A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext.

# CP-ABE example

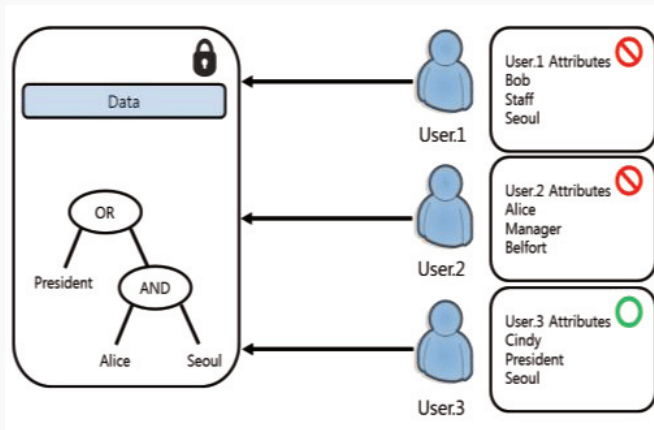


Figure 3: CP-ABE



- Access policy is encoded into the users secret key.
- Ciphertext is computed with respect to a set of attributes.
- A user will be able to decrypt a ciphertext, if and only if the attributes tied with the ciphertext satisfy the policy of his secret key.

# KP-ABE example

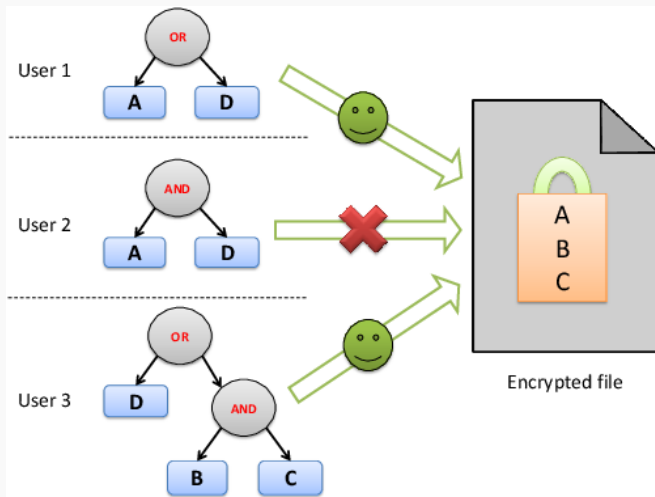


Figure 4: KP-ABE

# Advantages

- Authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data.
- Users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt.
- Collusion resistance - achieved by independently randomizing users' secret keys.

# Collusion Resistance


Example: encrypt a job posting:



Security Threat:



Figure 5: Collusion

-  Cybertwin is the virtual representation and intelligent agent of the vehicle. Vehicle can set access policies and store behavior data or feedback decisions in form of ciphertext on the central cloud. Only those newly created Cybertwins that meet the policies and conditions can legally access the encrypted storage data of the vehicle.
- Suppose vehicles of the same company want to share particular feedback messages which help in improving some algorithms and don't want vehicles of other companies to get this data.
- In case there is an emergency/breakdown, a vehicle would like to automatically send a message regarding its location/issue which should only be available to those of help such as ambulances/police vehicles, etc and no one else.

# Additional Design Goals

We are switching to an ABE setting where instead of standard secret key encryption, the message should not be decrypted by all entities and only by entities having access to certain attributes specified by the ABE scheme.

The messages are tied with attributes which can only be decrypted by users who a sufficient access policy tied to their secret key.

## Additional Setup

↓  
you can start with this by 3<sup>rd</sup> or 4<sup>th</sup> slide

Setup  $\mathcal{S}(\lambda)$  :

- $U$  = Universal set of attributes
- Let  $G_1 = \langle g_1 \rangle$ ,  $G_2 = \langle g_2 \rangle$  be two additive cyclic groups of prime order  $p$ . Let  $G_T = \langle g_T \rangle$  be a multiplicative cyclic group of order  $p$ .
- Bilinear map  $e : G_1 \times G_2 \rightarrow G_T$
- Randomly choose  $\alpha \in \mathbb{Z}_p$  and randomly choose  $t_i \in \mathbb{Z}_p \forall i \in U$
- Public parameters:  $PP = (Y = e(g_1, g_2)^\alpha, \{T_i = g_2^{t_i} | i \in U\})$
- Master Secret Key:  $MSK = (\alpha, \{t_i | i \in U\})$

Keygen  $\mathcal{K}(MSK, \text{access tree})$  : Sets the value of the root node to be  $\alpha(MSK)$  and splits it into shares in a top-down manner.

- OR: if value is  $\delta$ , the split shares are  $\delta$  and  $\delta$ .
- AND: if value is  $\delta$ , choose  $\gamma \in \mathbb{Z}_p$  and then split shares into  $\gamma$  and  $\delta - \gamma$



# Additional Setup

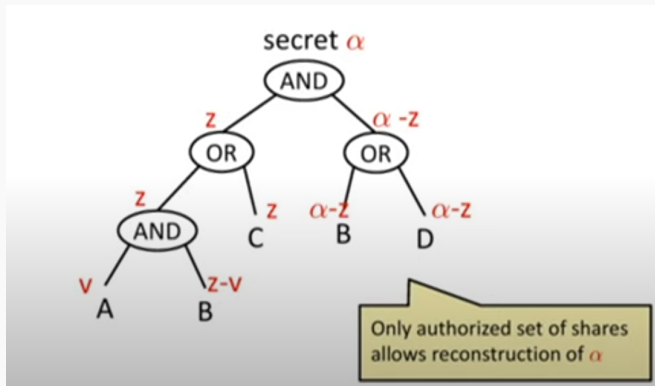


Figure 6: Linear Secret Sharing

# Additional Setup

Randomly choose  $d \in \mathbb{Z}_p$ . For each leaf node  $x$  (the value associated with the node is  $S(x)$ ) and its attached attribute  $t_x$ ,

$$SK_x = g_1^{\frac{S(x)}{t_x}} + g_1^{\frac{d}{t_x}}$$

And the private key:  $SK = (\{SK_x\}, g_2^d)$ .

# Modified Encryption Scheme

## Encrypt $\mathcal{E}(M, A, PP)$

First, we follow the aforementioned scheme to obtain  $M \cdot e(k_v, h)$ . We then select random  $b \in \mathbb{Z}_p$  and raise by  $b$  all the attributes we wish to encrypt the message with. So, our final ciphertext looks like:

$$CT = (A, M \cdot e(k_v, h) \cdot e(g_1, g_2)^{\alpha b}, \{T_i^b = g_2^{t_i b} | i \in A\}, g_1^b)$$

where  $A$  is the set of attributes being tied to the message.

# Modified Decryption Scheme

## Decrypt $\mathcal{D}(CT, PK)$

- Lets say the access structure associated with  $PK$  is  $\Gamma$ .  $CT$  contains  $g_1^b$  and  $PK$  contains  $g_2^d$ . We calculate  $L = e(g_1^b, g_2^d) = e(g_1, g_2)^{bd}$ .
- For a leaf node, if  $\Gamma_w(A) = 1$ , we calculate  $R(w) = e(SK_x, E_x)$  which can be simplified to  $e(g_1, g_2)^{bS(x)} \cdot e(g_1, g_2)^{bd}$ . Dividing the above result by  $L$  calculated before we get  $e(g_1, g_2)^{bS(x)}$ .
- Now, if the attributes satisfy the access structure, the user should be able to obtain  $e(g_1, g_2)^{\alpha b}$  from all the individual shares. So we can obtain  $M \cdot e(k_v, h)$  and continue with the aforementioned decryption and eventually obtain  $M$ .

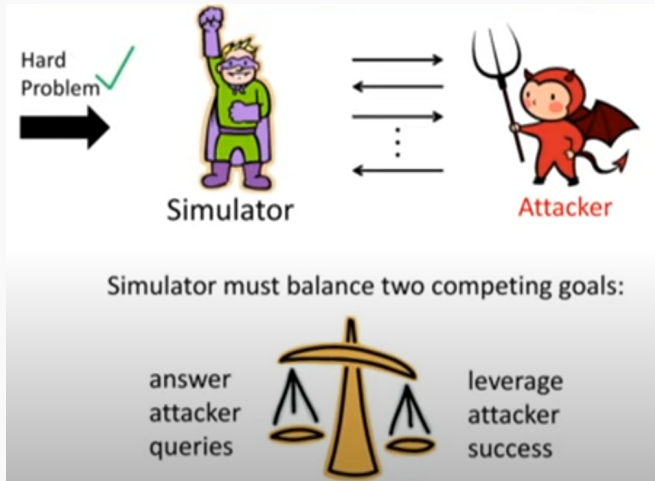


Figure 7: Security

## Decisional Bilinear Diffie-Hellman (DBDH) Assumption

Suppose  $a, b, c, z \in \mathbb{Z}_p$  are chosen at random. The DBDH assumption is that no polynomial time adversary is able to distinguish the tuple  $(A = g_1^a, B = g_2^b, C = g_2^c, Z = e(g_1, g_2)^{abc})$  from the tuple  $(A = g_1^a, B = g_2^b, C = g_2^c, Z = e(g_1, g_2)^z)$  with more than a negligible advantage.

# Theorem

If there exists a poly-time attacker who can break the Key-Policy Attribute Based Encryption scheme with advantage  $\epsilon$ , then the challenger can solve the DBDH problem with advantage  $\frac{\epsilon}{2}$ .

# Proof Outline

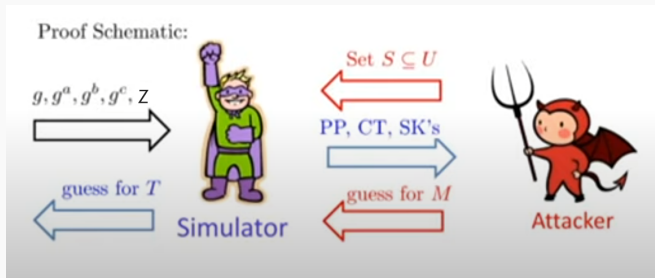


Figure 8: Outline



## Conclusion

---

- We present a privacy-preserving authentication scheme to enable anonymous authentication and resolve confidentiality issues in V2X.
- We also present a way to incorporate attributes into the keys and find ways of encryption based on the access policies defined over the attributes by the vehicle.

Thank you!