# Security Key Generation Technique for Inter-Vehicular Visible Light Communication

Tech ID: 29411 / UC Case 2018-534-0

## BRIEF DESCRIPTION

The invention is a technique that provides a novel, reliable and secure cryptography solution for inter-vehicular visible light communication. Through combining unique data as the road roughness and the driving behavior, a symmetric security key is generated for both communicating vehicles. As the data used is unique to the communicating vehicles only, the generated keys are thus unique, securing a reliable communication channel between both vehicles.

## FULL DESCRIPTION

Visible light communication (VLC) is a rapidly growing wireless optical communication technology, emerging as an attractive alternative for Vehicle to Vehicle (V2V) communication. V2V communication is vital for exchanging data as speed, brake and acceleration for safety operation of vehicles, improving roads' efficiency and reducing traffic jam. However, such communication and data exchange requires a secure and safe channel that is immune to jamming, interception and hacking. A reliable cryptography technique is therefore needed. Current applied algorithms use pre-shared secured keys which are still susceptible to hackers' attacks if they have knowledge of the system. Inventors at UCI provide a novel cryptography technique for inter-vehicular visible light communication. The algorithm combines various environment-unique data including, for example, road roughness and driving behaviors, to generate security keys for the communicating vehicles. The generated keys provide a securely encrypted communication channel between both vehicles, allowing for the exchange of data with no fear of jamming or interception, which will improve the efficiency and security of transportation systems significantly.

## SUGGESTED USES

Secured Vehicle to Vehicle communication

## ADVANTAGES

· Cryptography technique for inter-Vehicular visible light communication

· Utilizing natural driving behavior and road roughness for generating cryptographic security keys

· Eliminates the need for pre-shared security keys, thus system attackers have no access to them even if they have prior knowledge of the system

· Facilitates a secured and reliable Vehicle to Vehicle communication that helps in improving traffic fluidity and road throughput, thus decreasing traffic jam

## PATENT STATUS

| Country | Type | Number | Dated | Case |
|---|---|---|---|---|

## CONTACT

Michael Harpen
mharpen@uci.edu
tel: 949-824-5321.



## OTHER INFORMATION

## CATEGORIZED AS

- » **Optics and Photonics**
  - » All Optics and Photonics
- » **Communications**
  - » Internet
  - » Networking
  - » Optical
  - » Wireless
- » **Security and Defense**
  - » Cyber security

## RELATED CASES

2018-534-0

| | | | | |
|---|---|---|---|---|
| United States Of America | Issued Patent | 11,122,425 | 09/14/2021 | 2018-534 |

## STATE OF DEVELOPMENT

Computer simulations using real-life data provided by the Federal Highway Administration, for the proof of concept.

UCI Beall Applied Innovation

5270 California Avenue / Irvine,CA
92697-7700 / Tel: 949.824.2683