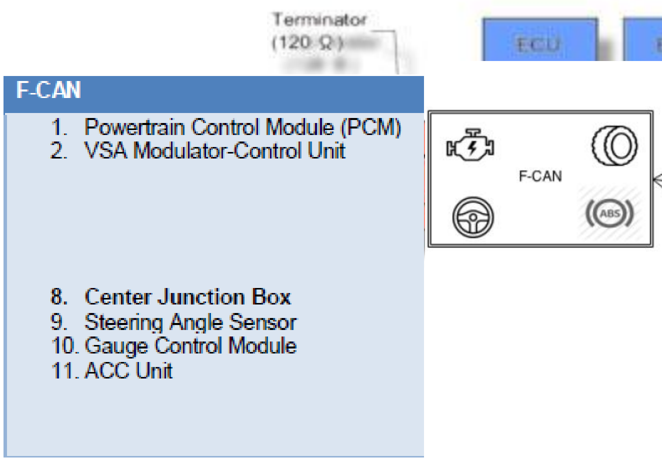
# PHYSICAL LAYER GROUP KEY AGREEMENT FOR AUTOMOTIVE CONTROLLER AREA NETWORK

Shalabh Jain
Jorge Guajardo
*Robert Bosch LLC*
*Research and Technology Center*
*Security and Privacy Group*

# Introduction
# What is CAN



- **C**ontroller **A**rea **N**etwork
  - – The primary communication network inside a car
  - – Several **E**lectronic **C**ontrol **U**nits (ECUs – door, seats, park assist) connected in a ring topology using a 2 wire bus – broadcast medium
  - – Simple differential signaling across the wires to transmit binary values.





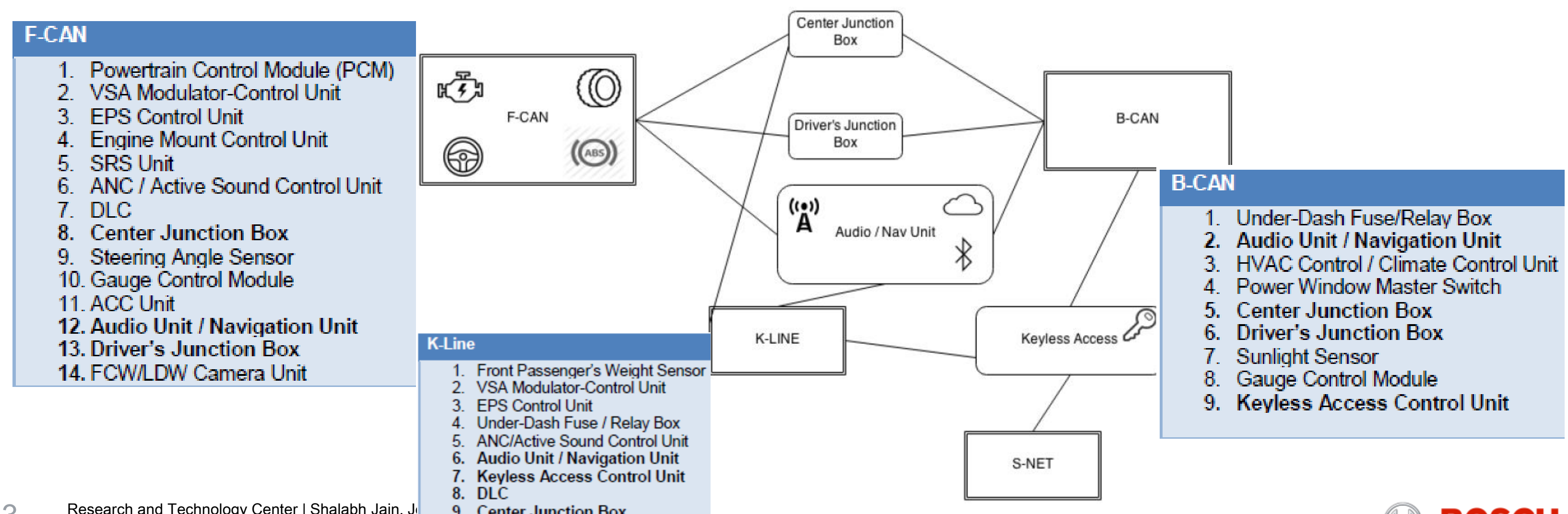



* CAN network picture: http://ww2.ac-poitiers.fr/sciences-ingenieur-sti/spip.php?article87

# Introduction
# What is CAN

What my labmate's car looks like – 2014 Accord*

- **C**ontroller **A**rea **N**etwork
  - The primary communication network inside a car
  - Several **E**lectronic **C**ontrol **U**nits (ECUs – door, seats, park assist) connected in a ring topology using a 2 wire bus
  - Simple differential signaling across the wires to transmit binary values.







BOSCH

* C Valasek, C Miller, A Survey of Remote Automotive Attack Surfaces

# Introduction
## What are the problems?

- Internal vehicular networks have become complex
  - More ECUs attached to the network
  - Several external interfaces with public networks – cellular, Bluetooth, USB
- ECUs design sensitive to cost – not much over-provisioning
  - Limited processing
  - Limited bandwidth
- Automobile operations are timing critical – latency sensitive operations
- Current automotive security state – in early stages of adoption

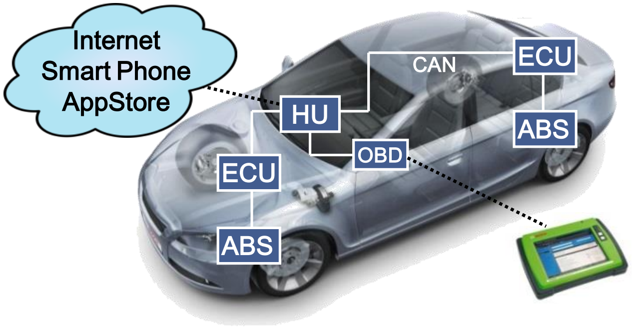
# Introduction
## Demonstrated attacks

### Bluetooth Pairing
Sniffing telematics unit's MAC address and brute-forcing PIN allows to pair attacker's Bluetooth device.

### Smart phone exploit of Bluetooth stack vulnerability
Malicious App on the user's (paired) smart phone can execute arbitrary code on the car's telematics unit.

### Exploit of media file (WMA) parser vulnerability
Malicious WMA file plays fine on PC but allows to send out arbitrary CAN messages when played in car's media player.

### Exploit of vulnerabilities in voice modem code
Dialing the car's number from an office phone and playing a malicious MP3 file into the receiver allows to compromise the car.




### Hijacking Wi-Fi Pass-Thru Device
Hijacking pass-thru device via Wi-Fi lets pass-thru device send arbitrary CAN messages when connected to the car.


(*) Koscher et al: **Experimental Analysis of a Modern Automobile**, S&P 2010
Checkoway et al.: **Comprehensive Experimental Analyses of Automotive Attack Surface,** USENIX Security, Aug. 2011.

# Introduction
## Demonstrated attacks - Jeep attack


Remote-attack demonstration by security researchers on a Jeep Cherokee


Encrypt all traffic – minimize information leakage

Authenticate the sender – prevent interaction between critical and non-critical groups

- Key components of the attack
  - Reverse engineer the CAN messages sent by individual ECUs – no encryption
  - Compromise a single ECU on the network – inject spurious messages as another ECU – no authentication



BOSCH

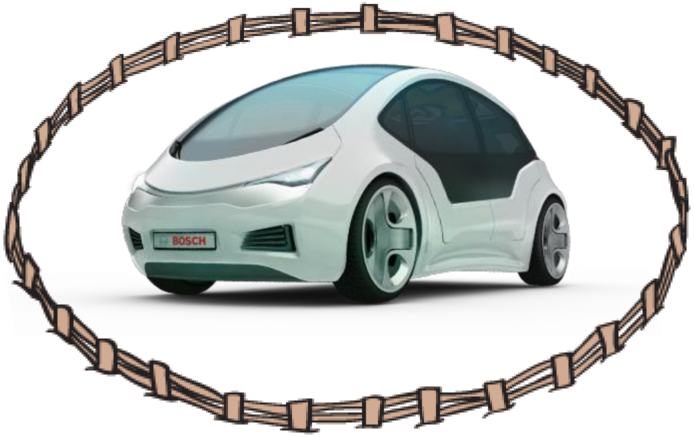
# Introduction
## Current automotive trend

1. Adding new interfaces – new methods to access internal methods
2. Provide security mechanisms on the interfaces

Advantages of this

**Quick to add**– minimal changes to internal architecture

**Utilize well known solutions** – Solution for traditional network interfaces




**What happens when the fence is breached?**

**Additional security inside the fence with minimal changes?**

**PLUG-AND-SECURE MODULES –** Authenticate and encrypt traffic

Utilize internal device properties – efficient solution tailored to device

# Introduction
## Requirements from Potential Solutions

- Establishing a **symmetric key** – fundamental requirement for any security

**Plug-and-Secure scheme for the CAN bus**

- **Require group keys** – for communication between logically connected entities


Research and Technology Center | Shalabh Jain, Jorge Guajardo Merchan | 06/01/2016

# Plug and Secure Scheme
## In a nutshell

- Establishing a **symmetric key** – fundamental requirement for any security
- PnS enables simple pairwise key generation and exchange between two parties
- PnS enables simple key updates (re-keying)

- **Require fast and efficient re-keying**
- Negligible hardware and software overhead
- On-the fly scheme – no storage requirements

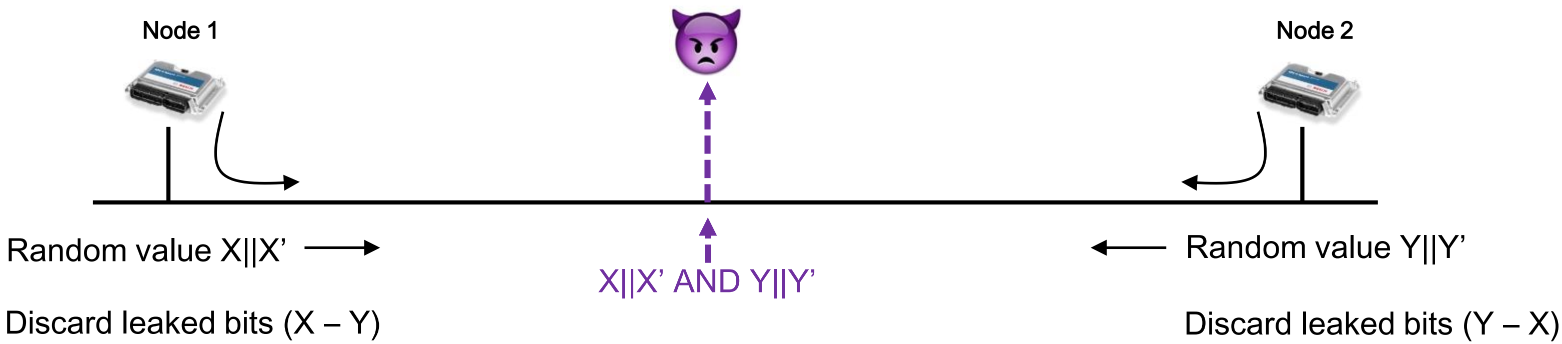
- **Require group keys**
- Extension of basic PnS to generate group keys
- Extension of basic PnS for authentication among participants

# Plug and Secure Scheme
## Basic Protocol

- Two nodes simultaneously writing to the CAN bus effectively compute the logical AND operation


| Node 1 | Node 2 | Bus output |
|---|---|---|
| ~~0~~ | ~~0~~ | ~~0~~ |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| ~~1~~ | ~~1~~ | ~~1~~ |

- Two party unauthenticated protocol – Plug and Secure [Mueller'15]



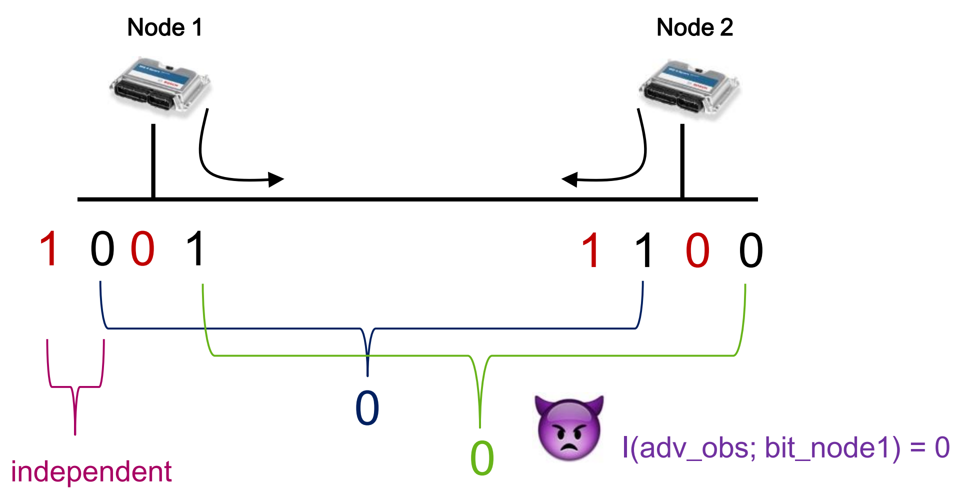

SECRET SHARED KEY


Research and Technology Center | Shalabh Jain, Jorge Guajardo Merchan | 06/01/2016

# Plug and Secure Scheme

## Basic Protocol ~ Unauthenticated Diffie-Hellman

- Stronger security guarantees – against unbounded passive adversaries




| Node 1 | Node 2 | Bus output |
|---|---|---|
| ~~0~~ | ~~0~~ | ~~0~~ |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| ~~1~~ | ~~1~~ | ~~1~~ |

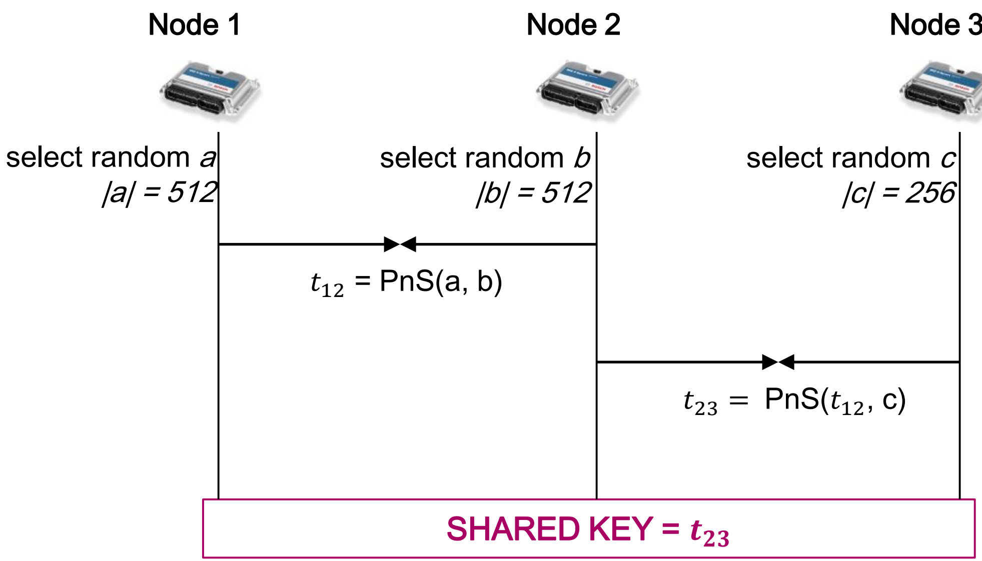
**Information theoretic security**

### Next steps

1. How to utilize this among groups of ECUs?
2. How to include authentication or certification?

# Plug and Secure Scheme
## Extension to Group Protocol

- Utilize the broadcast nature of the medium
  - Pairwise interactions sufficient to establish group keys




**Generate a 128 bit key**

Select random values

Node 1 and Node 2 execute PnS to obtain $t_{12}$
Avg – 256 residual bits

Node 2 and Node 3 execute PnS to obtain $t_{23}$
Avg – 128 residual bits

**No explicit interaction between Node 1 and Node 3**

- Provides information theoretic security
- Not very efficient – Usable bits ~ $b \times 2^{-(num\_nodes - 1)}$


Research and Technology Center | Shalabh Jain, Jorge Guajardo Merchan | 06/01/2016

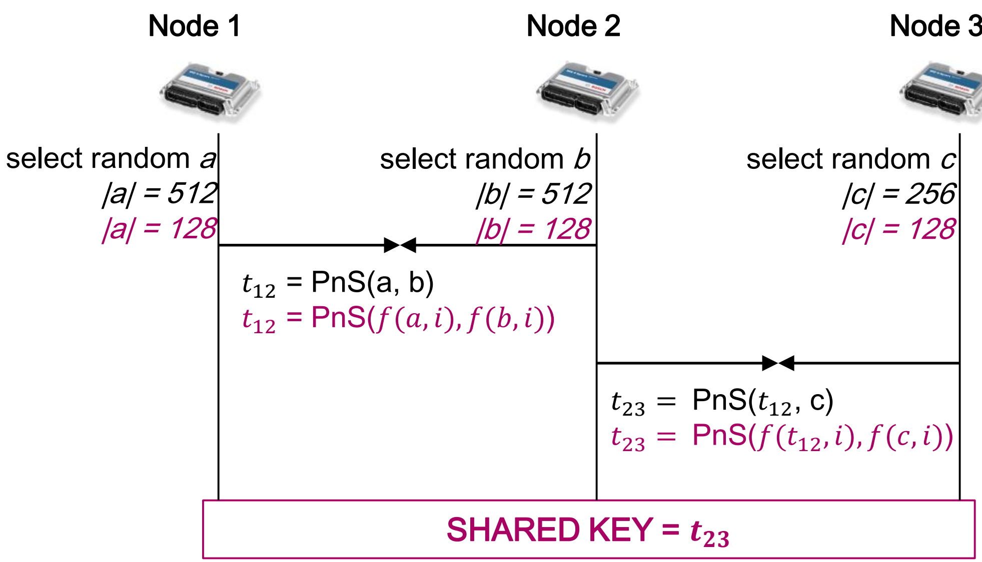
# Plug and Secure Scheme
## Computational model

- Group scheme inefficient – successive stages leak more-and-more bits
  - Provide isolation between successive stages

- Replace random bits by pseudorandom bits
  - Utilize pseudorandom functions for isolation

- Consider the function $f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$
  - For a randomly selected index $k \leftarrow \{0,1\}^n$, the function maps an element from the domain $\{0,1\}^n$ to the range $\{0,1\}^n$.
  - PPT adversary, given oracle access, cannot distinguish between a random function and given instance
  - In practice, can be instantiated by keyed hash function or block cipher

# Plug and Secure Scheme
## Efficient Group Protocol




**Generate a 128 bit key**

Select random values of 128 bits

Node 1 and Node 2 and nodes Node 2 and Node 3 execute PnS to obtain $t_{12}$ and $t_{23}$

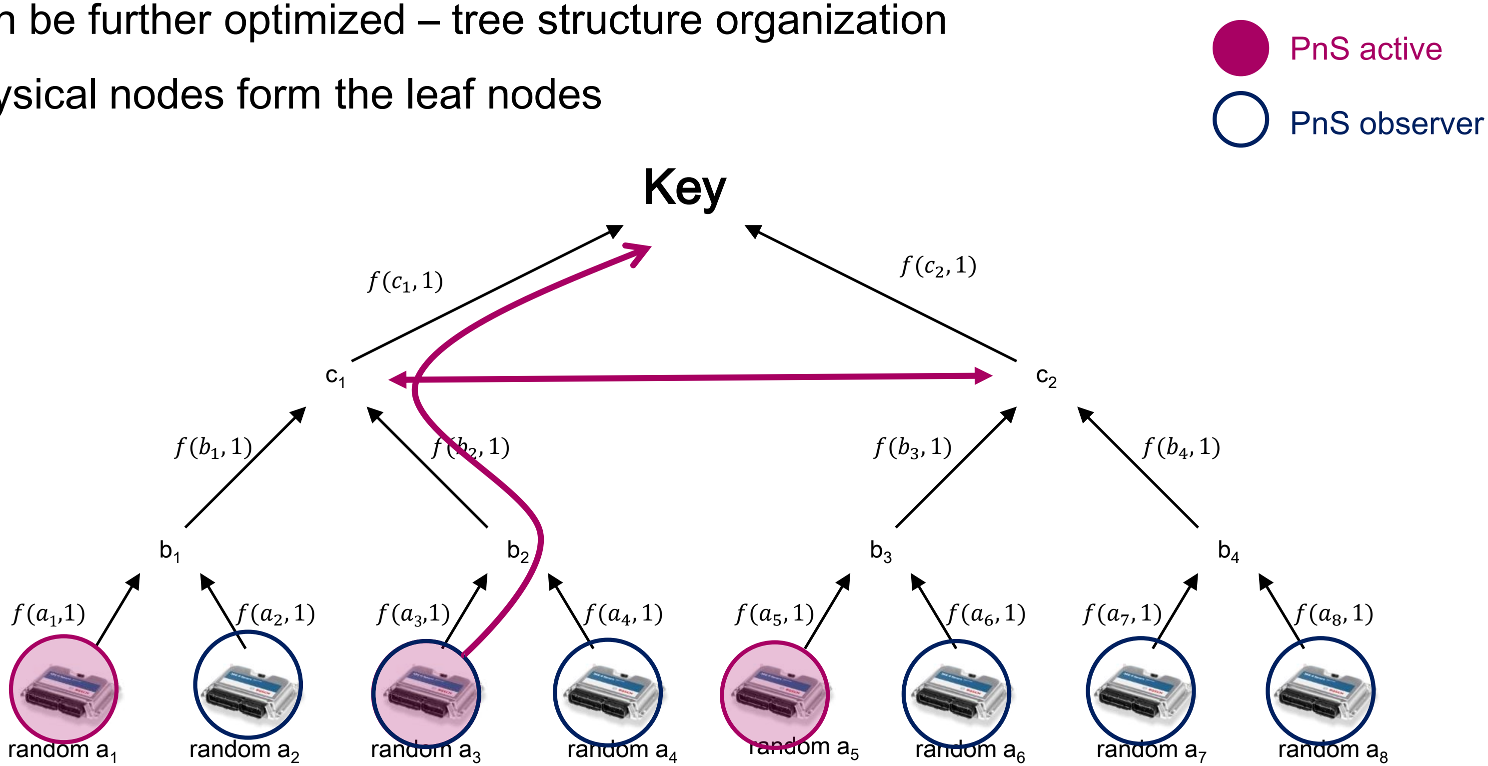
First use $i = 1$. Increment $i$ at each iteration

- Each interaction can generate 128 random bits
- Provides security against computationally bounded passive adversaries
- Has properties such as key independence


Research and Technology Center | Shalabh Jain, Jorge Guajardo Merchan | 06/01/2016

# Plug and Secure Scheme
## Tree based group key

- Can be further optimized – tree structure organization
- Physical nodes form the leaf nodes




- Rekeying – constant complexity


Research and Technology Center | Shalabh Jain, Jorge Guajardo Merchan | 06/01/2016

# Plug and Secure Scheme
## Security against active adversaries

- Ensure communication between the correct parties
  - Group key can be derived only by the correct parties

- Arbitrarily powerful adversary
  - Ability to record, inject and modify messages

- Adversarial access via
  - Remotely compromised ECU
  - Diagnostics (OBD) port
  - Maliciously replaced ECU

No physical probing YET!

Two approaches

1. Using inherent robustness of basic PnS
2. Cryptographic guarantees using pre-existing trust relation

# Plug and Secure Scheme
## Security against active adversaries

- PnS has some inherent robustness against active adversaries
- Node impersonation
  - Nodes can monitor the broadcast medium
  - Identify and flag false use of IDs
- Inserting message for active nodes
  - Can only insert by PnS type methods – AND operations
  - No control over inserted message
- Inserting message for observer nodes
  - Negligible probability of acceptance
- Modification of packets
  - Can only change 1 to 0 – solved by key verification
- May be sufficient against active adversaries



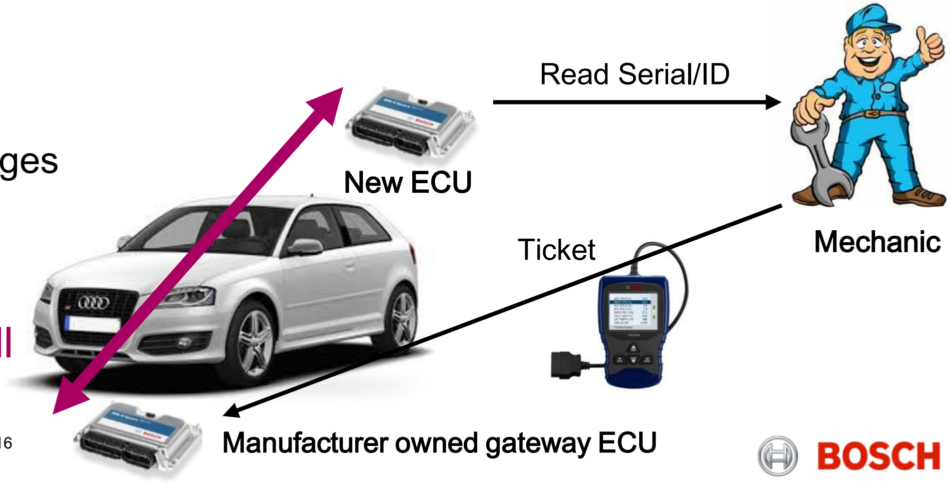
BOSCH

# Plug and Secure Scheme
## Overlay Authentication Architecture

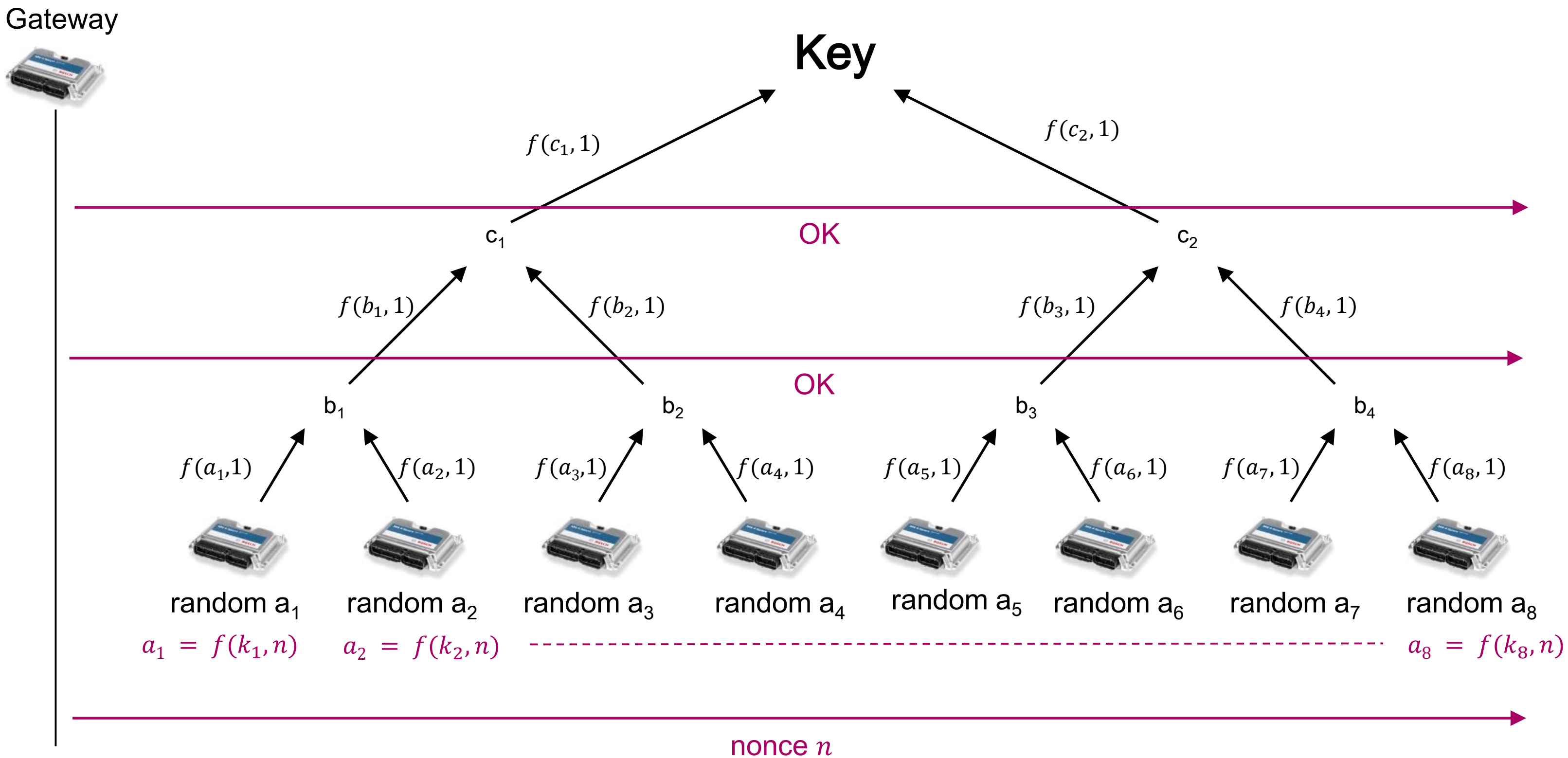
- Extend PnS to support authentication
  - Set up an initial shared secret with the ECUs – proof of identity
- Utilize gateway nodes as root of trust
  - Each ECU shares a trust relationship with the gateway – symmetric key
  - Established during installation or manufacture
- Gateway can have added security extensions to protect keys
- Gateway has knowledge of the group configurations
  - Defined by manufacturer
- Gateway used as monitor
  - Verify the correctness of the messages

Not the only possible architecture

PKI based solutions may apply as well



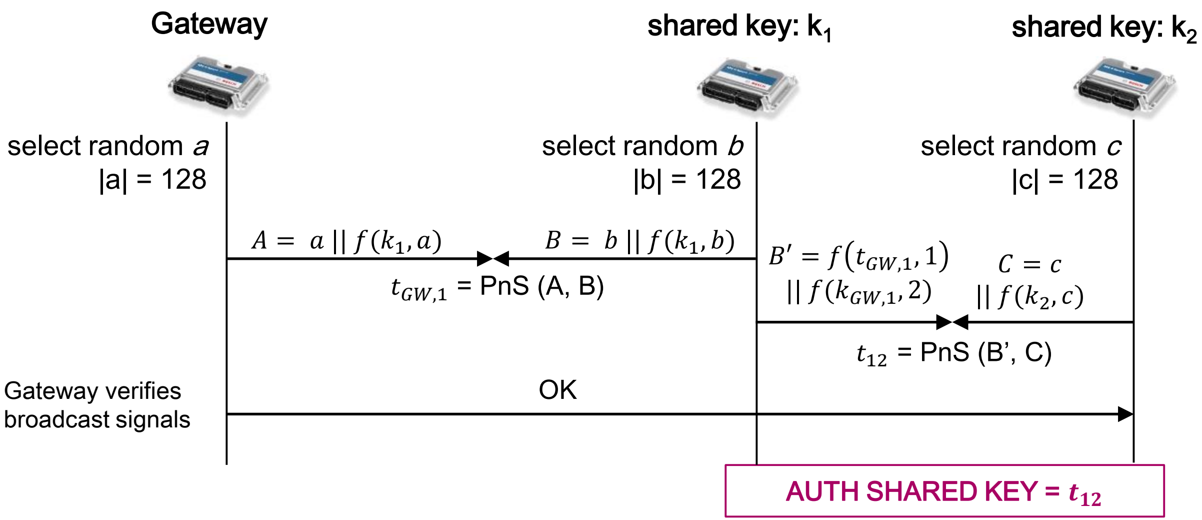
# Plug and Secure Scheme
## Authenticated tree based group key




- All operations can be verified by the gateway
- Lacks perfect forward secrecy – if ECU is compromised, group key recovered

# Plug and Secure Scheme
## Authenticated Group Protocol

- Each node first utilizes fresh randomness
  - Transmit MAC of the random message – in place of pseudorandom inputs




**Generate a 128 bit key**

Select random values

GW initiates protocol with Node 1

Node 1 executes protocol with Node 2

Gateway verifies the transmission

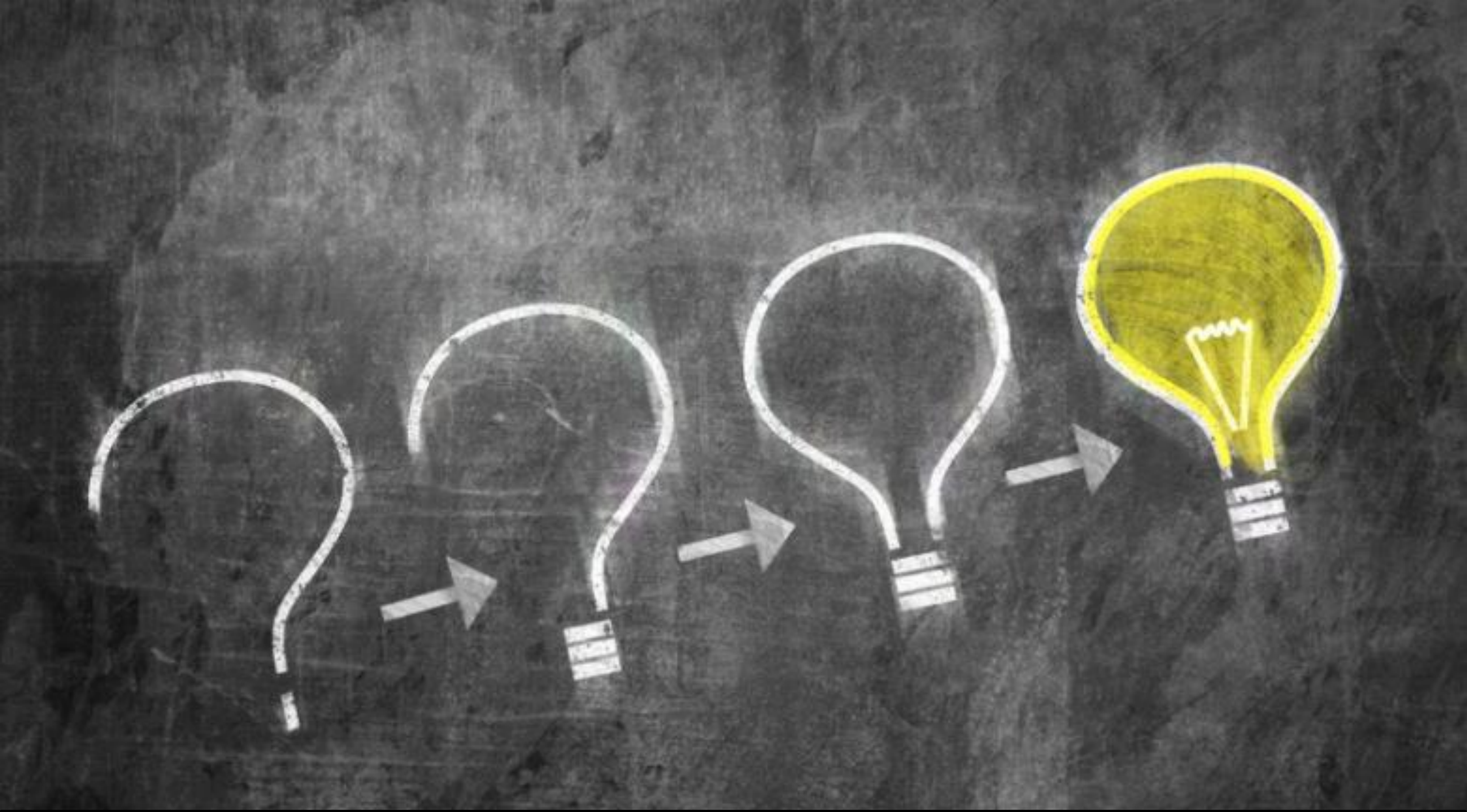
- No overhead due to MAC – PnS requires at least two transmissions
- Provides Perfect Forward Secrecy (PFS)
  - Good feature to have – some ECUs can be easily accessed and compromised
- Linear structure of key agreement scheme



BOSCH

# Plug and Secure Scheme
## Conclusion (and advantages)

- Security against active and passive adversaries
  - Perfect Forward Secrecy, key independence
  - Can have information theoretic guarantees – at cost of efficiency
- Efficient operations
  - Utilize inherent operations of the CAN bus
  - Based on simple cryptographic primitives - PRFs
  - Computationally efficient
  - Number of rounds comparable with optimal schemes in literature
- Computation and bandwidth scaling with key length is linear
- Compared to EC-DH – similar security properties, no expensive group operations
- Can utilize multiple (distributed) gateway
- Adversaries with low level physical access
  - Several interesting attacks and countermeasures possible – in preparation for publication




**Shalabh Jain**

shalabh.jain@us.bosch.com

Bosch Research and Technology Center

Security and Privacy Group

**Jorge Guajardo Merchan**

jorge.guajardomerchan@us.bosch.com

Bosch Research and Technology Center

Security and Privacy Group