# Article information:

LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks: ACM Transactions on Embedded Computing Systems: Vol 16, No 3  
<https://dl.acm.org/doi/abs/10.1145/3056506>

# Article summary:

1. LiBrA-CAN is a lightweight broadcast authentication protocol for Controller Area Networks (CAN) that takes advantage of two innovative procedures: splitting keys between nodes and mixing authentication tags.

2. Experiments were performed on state-of-the-art Infineon TriCore controllers, contrasted with low-end Freescale S12X cores, while simulations were provided for the recently released CAN-FD standard.

3. The article discusses a solution based on CAN+ to gain compatibility with existent networks.

# Article rating:

Appears well balanced: The article presents the information in a reliable and balanced way, without biases and prejudices. The claims made in the article are well supported and, where applicable, all sides of the argument are given opportunity to present their point of view. The article appears trustworthy and reliable.

# Article analysis:

The article “LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks” is an informative and well researched piece of work that provides an overview of the security protocols used in vehicular buses such as the widely used Controller Area Network (CAN). The authors provide a detailed description of their proposed protocol, LiBrA-CAN, which is based on efficient symmetric primitives and takes advantage of two innovative procedures: splitting keys between nodes and mixing authentication tags. This results in a higher security level when compromised nodes are in the minority, which is a realistic assumption for automotive networks.

The authors have done an excellent job in providing evidence to support their claims by performing experiments on state-of-the-art Infineon TriCore controllers, contrasted with low-end Freescale S12X cores, while simulations were provided for the recently released CAN-FD standard. They also discuss a solution based on CAN+ to gain compatibility with existent networks.

The article does not appear to be biased or one sided as it presents both sides of the argument equally and provides evidence to support its claims. It also does not appear to contain any promotional content or partiality towards any particular point of view or technology. Furthermore, all possible risks associated with using this protocol are noted and discussed in detail throughout the article.

In conclusion, this article appears to be trustworthy and reliable as it provides detailed information about its subject matter and presents both sides of the argument equally without any bias or promotional content.

# Topics for further research:

* CAN security protocols
* CAN+ compatibility
* Symmetric primitives
* Splitting keys between nodes
* Mixing authentication tags
* Infineon TriCore controllers

# Report location:

<https://www.fullpicture.app/item/65ae1b44bdfd340785521132f6328ffe>