



(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2024/0214370 A1**

(43) **Pub. Date: Jun. 27, 2024**

Zeh et al.

(54) **SECURE COMMUNICATIONS USING PRE-GENERATED SUBKEYS**

(52) **U.S. Cl.**
CPC **H04L 63/083** (2013.01)

(71) Applicant: **Infineon Technologies AG**, Nuebiberg (DE)

(57) **ABSTRACT**
The described techniques address issues associated with current secure in-vehicle communication systems, which are required to generate subkeys per each encoded data transmission/reception. These encoded data transmissions/receptions may be in accordance with several different in-vehicle communication protocols, and the requirement of such protocols to generate the subkeys “on-the-fly” may lead to significant processing overhead and latency. The embodiments provided herein address the issue of subkey generation by using a predetermined function to pre-calculate and store the subkeys that are to be used for future encoded data message transmissions/receptions. In this way, the time and overhead required to generate the subkeys may be better and more efficiently managed.

(72) Inventors: **Alexander Zeh**, Muenchen (DE);
Patrick Kresmer, Muenchen (DE);
Andreas Graefe,
Strassblach-Dingharting (DE)

(21) Appl. No.: **18/069,396**

(22) Filed: **Dec. 21, 2022**

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)

900

