CORRECTION

Correction to: Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5.0 and its countermeasure

Da-Zhi Sun^{1,2,3} • Yi Mu³ • Willy Susilo³

Published online: 11 November 2017
© Springer-Verlag London Ltd. 2017

Correction to: Pers Ubiquit Comput

<https://doi.org/10.1007/s00779-017-1081-6>

Figure 4 contained an error. "Diffie-Hellman key" in step 1c' of Figure 4 should be changed to "Diffie-Hellman keys".

The original article was corrected.

The online version of the original article can be found at <https://doi.org/10.1007/s00779-017-1081-6>

✉ Da-Zhi Sun
sundazhi@tju.edu.cn

¹ Tianjin Key Laboratory of Advanced Networking (TANK), School of Computer Science and Technology, Tianjin University, No. 135, Yaguan Road, Tianjin Haihe Education Park, Tianjin 300350, China

² State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

³ Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia