PLOS ONE

CORRECTION

Correction: Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments

Chi-Tung Chen, Cheng-Chi Lee, Iuon-Chang Lin

There are errors in the author affiliations. The correct affiliations are as follows:

Chi-Tung Chen[1], Cheng-Chi Lee[3,4], Iuon-Chang Lin[2,4]

1 Department of Distribution Management (Information Management), National Chin-Yi University of Technology, Taichung, Taiwan, R.O.C. **2** Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei City, Taiwan, R.O.C. **3** Department of Photonics and Communication Engineering, Asia University, Taichung, Taiwan, R.O.C. **4** Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan, R.O.C.

There is an error in Fig 4. Part of the figure is missing. Please see the complete, correct Fig 4 here.

There are errors in the typesetting of the columns in Tables 3 and 4. Please see the correct Tables 3 and 4 here.

Citation: Chen C-T, Lee C-C, Lin I-C (2020) Correction: Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments. PLoS ONE 15(6): e0234631. https://doi.org/10.1371/journal.pone.0234631

Published: June 12, 2020

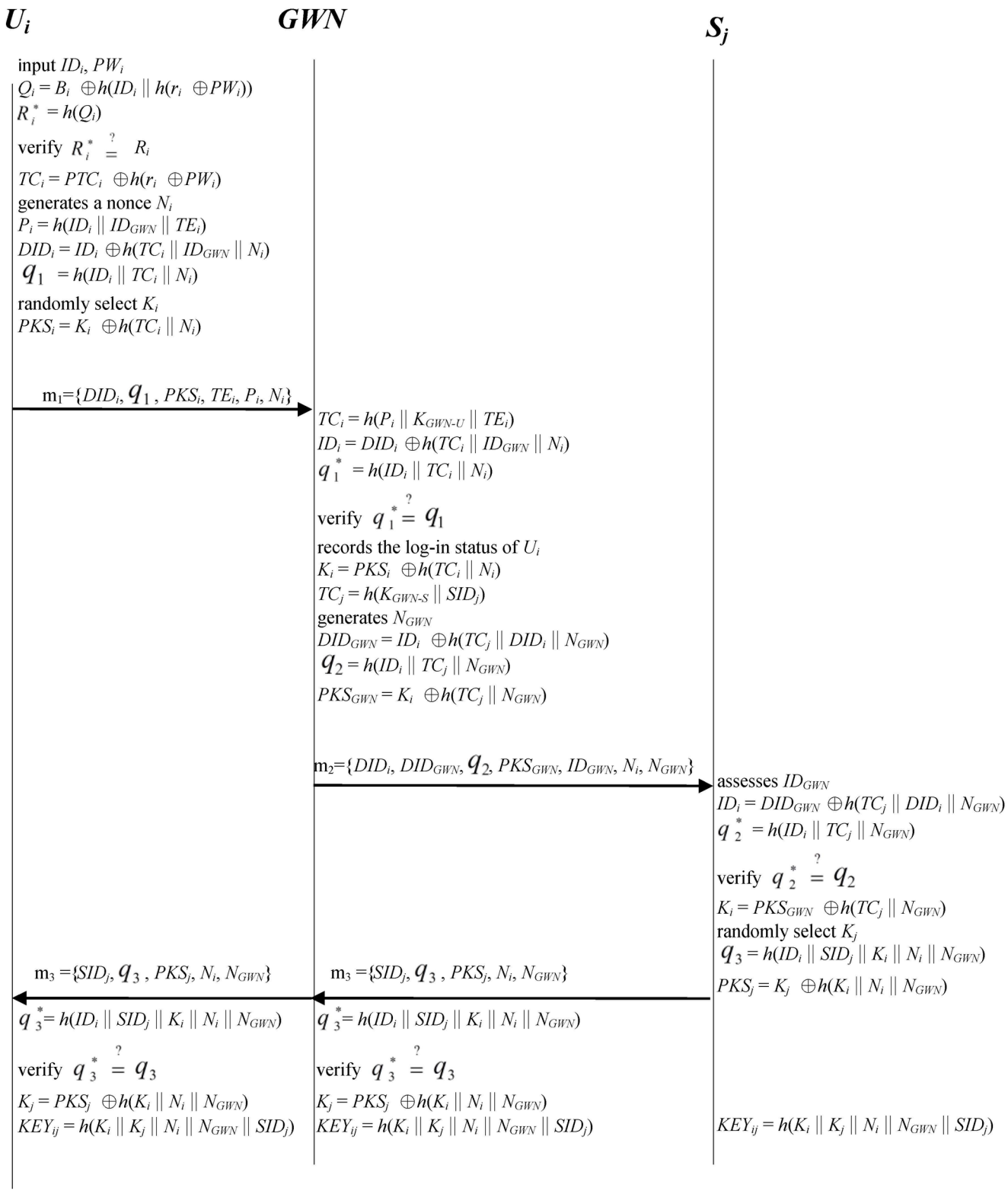

Fig 4. Login phase; authentication and key agreement phase.

https://doi.org/10.1371/journal.pone.0234631.g001

Table 3. Functionality comparison of our scheme with other related schemes.

	Ours	Ostad-Sharif (2019)[2]	Amin et al. (2018)[26]	Chang et al. (20160[27]	Xue et al. (2103)[7]	Yeh et al. (2011)[8]	Khan et al. (2010)[24]	Chen et al. (2010)[25]	Das (2009)[5]
Password protection	Yes	Yes	Yes	No	No	Yes	Yes	No	No
Stolen smart card attack resistance	Yes	Yes	Yes	No	No	No	No	No	No
Masquerade attack resistance	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No
Replay attacks resistance	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Insider attack resistance	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
Password updating/changing	Yes	No	Yes	Yes	No	No	Yes	No	No
Time synchronization avoidance	Yes	No	No	No	No	Yes	No	No	No
Mutual authentication	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Session key agreement	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
User anonymity	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
GWN bypassing attack resistance	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

https://doi.org/10.1371/journal.pone.0234631.t001

Table 4. Performance comparison of our scheme with other related schemes.

	Ours	Ostad-Sharif (2019)[2]	Amin et al. (2018)[26]	Chang et al. (20160[27]	Xue et al. (2103)[7]	Yeh et al. (2011)[8]	Khan et al. (2010)[24]	Chen et al. (2010)[25]	Das (2009)[5]
【*Computational cost*】									
Authentication phase									
User	$4T_h$	$10T_h$	$13T_h$	$3T_h$	$5T_h$	$2T_{ecc}+1T_h$	$3T_h$	$4T_h$	$3T_h$
GWN	$8T_h$	$14T_h$	$14T_h$	$5T_h$	$11T_h$	$4T_{ecc}+3T_h$	$5T_h$	$5T_h$	$4T_h$
Sensor Node	$3T_h$	$3T_h$	$2T_h$	$1T_h$	$3T_h$	$2T_{ecc}+2T_h$	$2T_h$	$2T_h$	$1T_h$
key agreement phase									
User	$3T_h$	$2T_h$	$1T_h$	$3T_h$	$3T_h$	$1T_h$	- *	- *	- *
GWN	$3T_h$	$3T_h$	$3T_h$	$3T_h$	$3T_h$	$1T_h$	- *	- *	- *
Sensor Node	$3T_h$	$2T_h$	$2T_h$	$4T_h$	$3T_h$	$1T_h$	- *	- *	- *
Total	$24T_h$	$34T_h$	$35T_h$	$19T_h$	$28T_h$	$8T_{ecc}+9T_h$			
【*Communication cost*】									
Transmitted message	4	6	6	4	4	3	4	4	3

* Khan et al. scheme, Chen et al. scheme and Das scheme do not provide the key agreement phase for session key agreement.

https://doi.org/10.1371/journal.pone.0234631.t002

Reference

1. Chen C-T, Lee C-C, Lin I-C (2020) Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments. PLoS ONE 15(4): e0232277. https://doi.org/10.1371/journal.pone.0232277 PMID: 32353049