Errata

Corrections to "A Secure Fault-Tolerant Conference-Key Agreement Protocol"

Wen Guey Tzeng

THE above-cited paper appeared in the April 2002 issue of these transactions. The author has submitted the following corrections/clarifications to the paper:

1. In the fault detection stage of Section 4 of the paper, it is obvious that U_i should not broadcast S_i, which is used in ElGamal signature. We should simply delete S_i from the fault detection message since it is not used at all. Therefore, the "Fault detection" stage should be corrected as follows:
   a. In Step 3ai, it should be "Output R_i, K_i."
   b. In Step 3bi, it should be "Wait for U_m's fault detection messages R_m, K_M."
   c. In Step 3biii, it should be "On receiving $R_m, K_M, \cdots$."
2. This is to clarify that following the general practice of deterring the "replay" attack, each broadcast message should have an inseparable stage to show its "timeliness."

REFERENCES

[1] W.G. Tseng, "A Secure Fault-Tolerant Conference-Key Agreement Protocol," *IEEE Trans. Computers*, vol. 51, no. 4, pp. 373-379, Apr. 2002.

• *The author is with the Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 30050. E-mail: tzeng@cis.nctu.edu.tw.*

For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number 111322.