Errata

of the PhD thesis

Reconciling Information Exchange and Confidentiality

A Formal Approach

by

Wouter Teepe

May 15, 2007

Please report any errors in the thesis, small or big, to Wouter Teepe: `wouter@teepe.com`

Main Errata

1. page xvii, line 6–7, Lotte Douze should be included
2. page xvii, line 30, "cover, which was" should read "cover. The cover was"
3. page 21, subscript of Figure 2.2, line 7, "$O(k \ln \ln \ln n)$" should read $O(k(\ln n)^3)$
4. page 44, line 4, "file" should read "hash value of the file"
5. page 61, line -1, "false belief" should read "unjustified belief"
6. page 62, line 10, "false belief" should read "unjustified belief"
7. page 63, line 17, "false belief" should read "unjustified belief"
8. page 70, line -5, "from $\{X\}_{-K}$" should read "from $\{X\}_{-K}$ only"
9. page 131, Figure 9.7, item 7, "$h_2 = H(I_P, N, P, C)$" should read "$h_2 = H(I_P, P, C)$"
10. page 131, Figure 9.7, item 9, "$H(I_{V_j}, N, P, C)$" should read "$H(I_{V_j}, P, C)$"
11. page 132, Figure 9.8, item 11, "$h_{2_B} = H(I_B, N, B, C_A)$" should read "$h_{2_B} = H(I_B, B, C_A)$"
12. page 132, Figure 9.8, item 13, "$H(I_A, N, B, C_A)$" should read "$H(I_A, B, C_A)$"

Bibliography

Some of the literature references are inaccurate, as they point to preliminary versions of articles. The correct references are given below.

1. [AvdHdV01] should be replaced with [AvdHdV02].
2. [KS04] shoud be replaced with [KS05, Kis06].

[AvdHdV02] Nesria Agray, Wiebe van der Hoek, and Erik P. de Vink. On BAN logics for industrial security protocols. In Barbara Dunin-Kęplicz and Edward Nawarecki, editors, *Proceedings of the Second International Workshop of Central and Eastern Europe on Multi-Agent Systems*, volume 2296 of *Lecture Notes in Artificial Intelligence*, pages 29–36, Berlin / Heidelberg, 2002.

[Kis06] Lea Kissner. *Privacy-Preserving Distributed Information Sharing*. PhD thesis, School of Computer Science, Carnegie Mellon University, July 2006.

[KS05] Lea Kissner and Dawn Song. Privacy-preserving set operations. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 241–257, Berlin, 2005. Springer-Verlag.

Punctuation

There are just minor annoyances.

1. page xv, line 1, “the the” should read “the”
2. page 49, line 4 of footnote 5, “strand-space” should read “strand space”
3. page 55, line 10, “Sect.” should read “Section”
4. page 55, line 12, “Sect.” should read “Section”
5. page 56, line 18, “Sect.” should read “Section”
6. page 61, line 1, “Sect.” should read “Section”
7. page 61, line 6, “Sect.” should read “Section”
8. page 61, line 8, “Sect.” should read “Section”
9. page 62, line 17, “Sect.” should read “Section”
10. page 63, line 17, “Sect.” should read “Section”
11. page 64, line 14, “. . .” should read “· · ·”
12. page 65, line 12, “knows” should read “knows that”
13. page 180, line 3, “Sect.” should read “Section”
14. SIKS Dissertation Series, heading should be on top of the page, and not 4 centimeters down.