Galindo, David

Compact hierarchical identity-based encryption based on a Harder decisional problem. (English) Zbl 1375.94126

Int. J. Comput. Math. 92, No. 3, 463-472 (2015).

Summary: We generalize the decisional problem that was used to prove the security of a well-known hierarchical identity-based encryption scheme by Boneh, Boyen and Goh [*D. Boneh* et al., Eurocrypt 2005, Lect. Notes Comput. Sci. 3494, 440–456 (2005; Zbl 1137.94340)]. We argue that our new problem is strictly harder than the original problem, and thus the security of the aforementioned cryptographic primitive is laid on even stronger foundations.

MSC:

94A60 Cryptography
68P25 Data encryption (aspects in computer science)
68Q17 Computational difficulty of problems (lower bounds, completeness, difficulty of approximation, etc.)

Keywords:

hierarchical identity-based encryption; hard problems; decisional assumptions; standard model; generic model

Full Text: DOI

References:

[1] DOI: 10.1007/978-3-540-74835-9_10 · Zbl 05314723 · doi:10.1007/978-3-540-74835-9_10
[2] DOI: 10.1007/978-3-540-39927-8_28 · doi:10.1007/978-3-540-39927-8_28
[3] DOI: 10.1007/3-540-49649-1_30 · doi:10.1007/3-540-49649-1_30
[4] DOI: 10.1007/978-3-540-24676-3_14 · doi:10.1007/978-3-540-24676-3_14
[5] DOI: 10.1007/3-540-44647-8_13 · doi:10.1007/3-540-44647-8_13
[6] DOI: 10.1007/11426639_26 · Zbl 1137.94340 · doi:10.1007/11426639_26
[7] DOI: 10.1007/3-540-39200-9_16 · doi:10.1007/3-540-39200-9_16
[8] DOI: 10.1007/11761679_1 · Zbl 1129.94017 · doi:10.1007/11761679_1
[9] DOI: 10.1007/s00145-009-9047-0 · Zbl 1195.94052 · doi:10.1007/s00145-009-9047-0
[10] DOI: 10.1007/3-540-36178-2_34 · Zbl 1065.94547 · doi:10.1007/3-540-36178-2_34
[11] DOI: 10.1007/3-540-46035-7_31 · doi:10.1007/3-540-46035-7_31
[12] DOI: 10.1007/10722028_23 · doi:10.1007/10722028_23
[13] DOI: 10.1007/3-540-45311-3_32 · doi:10.1007/3-540-45311-3_32
[14] DOI: 10.1007/11745853_18 · doi:10.1007/11745853_18
[15] DOI: 10.1016/j.dam.2005.03.030 · Zbl 1092.94024 · doi:10.1016/j.dam.2005.03.030
[16] DOI: 10.1007/978-3-540-78440-1_21 · Zbl 1162.94382 · doi:10.1007/978-3-540-78440-1_21
[17] DOI: 10.1007/978-3-642-00468-1_13 · Zbl 1227.94064 · doi:10.1007/978-3-642-00468-1_13
[18] Shamir A., in Proceedings of CRYPTO 1984 pp 47– (1984)
[19] DOI: 10.1007/978-3-540-70583-3_46 · Zbl 1155.94385 · doi:10.1007/978-3-540-70583-3_46
[20] DOI: 10.1007/s00145-004-0313-x · Zbl 1075.94011 · doi:10.1007/s00145-004-0313-x
[21] S. Wolf,Information-theoretically and computationally secure key agreement in cryptography, Ph.D. diss., ETH Zürich, 1999.