Mo, Ruo; **Ma, Jianfeng**; **Liu, Ximeng**; **Li, Qi**

FABSS: attribute-based sanitizable signature for flexible access structure. (English)

Zbl 1452.94079

Qing, Sihan (ed.) et al., Information and communications security. 19th international conference, ICICS 2017, Beijing, China, December 6–8, 2017. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 10631, 39-50 (2018).

Summary: In the Electronic Health Record (EHR) system, digital signature is utilized to prevent the medical data from being tampered. However, users update their medical data frequently and have to sign these medical data from scratch after updating. Besides, traditional signature attests the identity of the individual signing the records, which leads to vast computation cost and the privacy leakage. In this paper, we obfuscate users identity information with attribute sets and introduce a semi-trusted participant-sanitizer to propose the Flexible Attribute-Based Sanitizable Signature (FABSS) scheme. We prove that our scheme is unforgeable under generic group model. Through comparison, the FABSS scheme not only reduces the users computation overhead, but also supports flexible access structures to implement expressively fine-grained access control.

For the entire collection see [Zbl 1435.68039].

MSC:

94A60 Cryptography

Keywords:

flexible attribute-based access control; sanitizable signature; unforgeability; anonymity; information privacy

Full Text: DOI

References:

[1] Ateniese, G., Chou, D.H., de Medeiros, B., Tsudik, G.: Sanitizable signatures. In: di Vimercati, S.C., Syverson, P., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 159-177. Springer, Heidelberg (2005). https://doi.org/10.1007/11555827_10

[2] Brzuska, C., Fischlin, M., Freudenreich, T., Lehmann, A., Page, M., Schelbert, J., Schröder, D., Volk, F.: Security of sanitizable signatures revisited. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 317-336. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00468-1_18 · Zbl 1227.94073

[3] Brzuska, C., Fischlin, M., Lehmann, A., Schröder, D.: Unlinkability of sanitizable signatures. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 444-461. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_26 · Zbl 1281.94076

[4] Canard, S., Laguillaumie, F., Milhau, M.: Trapdoor sanitizable signatures and their application to content protection. In: Bellovin, S.M., Gennaro, R., Keromytis, A., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 258-276. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68914-0_16 · Zbl 1315.94064

[5] Lai, J., Ding, X., Wu, Y.: Accountable trapdoor sanitizable signatures. In: Deng, R.H., Feng, T. (eds.) ISPEC 2013. LNCS, vol. 7863, pp. 117-131. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38033-4_9 · Zbl 1315.94084

[6] Miyazaki, K., Hanaoka, G., Imai, H.: Digitally signed document sanitizing scheme based on bilinear maps. In: Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, pp. 343-354 (2006)

[7] Yuen, T.H., Susilo, W., Liu, J.K., Mu, Y.: Sanitizable signatures revisited. In: Franklin, M.K., Hui, L.C.K., Wong, D.S. (eds.) CANS 2008. LNCS, vol. 5339, pp. 80-97. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89641-8_6 · Zbl 1362.94059

[8] Agrawal, S., Kumar, S., Shareef, A., Rangan, C.P.: Sanitizable signatures with strong transparency in the standard model. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Inscrypt 2009. LNCS, vol. 6151, pp. 93-107. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16342-5_7 · Zbl 1281.94068

[9] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of 13th ACM Conference on Computer and Communications Security, pp. 89-98 (2006)

[10] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334 (2007)

[11] Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376-392. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19074-2_24 · Zbl 1284.94093

[12] Li, J., Au, M.H., Susilo, W., Xie, D., Ren, K.: Attribute-based signature and its applications. In: Proceedings of 5th ACM Symposium on Information, Computer and Communications Security, pp. 60-69 (2010)

[13] Okamoto, T., Takashima, K.: Efficient attribute-based signatures for non-monotone predicates in the standard model. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 35-52. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_3 · Zbl 1291.94194

[14] Su, J., Cao, D., Zhao, B., Wang, X., You, I.: ePASS: an expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things. Future Gener. Comput. Syst. 33, 11-18 (2014)

[15] Rao, Y.S., Dutta, R.: Efficient attribute-based signature and signcryption realizing expressive access structures. Int. J. Inf. Secur. 15, 81-109 (2016)

[16] Li, J., Chen, X., Huang, X.: New attribute-based authentication and its application in anonymous cloud access service. Int. J. Web Grid Serv. 11, 125-141 (2015)

[17] Liu, X., Ma, J., Xiong, J., Ma, J., Li, Q.: Attribute based sanitizable signature scheme. J. Commun. 34, 148-155 (2013)

[18] Xu, L.