REFERENCES

[1] Wei L, Wu C, Zhou S. efficient verifier-local revocation group signature schemes with backward unlinkability. Chinese Journal of Electronics, 2009, e90-a(2):379-384.

[2] Dan B, Shacham H. Group signatures with verifier-local revocation. Acm Conference on Computer & Communications Security. 2004.

[3] Chaum, David, and T. P. Pedersen. Wallet Databases with Observers. International Cryptology Conference on Advances in Cryptology 1992.

[4] B. Dan, X. Boyen, E. J. Goh, “Hierarchical identity based encryption with constant size ciphertext”, International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, pp. 440- 456, 2005.

[5] A. Kate, G. M. Zaverucha, I. Goldberg, “Constant-Size Commitments to Polynomials and Their Applications”, Advances in Cryptology - ASIACRYPT 2010 -, International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings. DBLP, pp. 177-194, 2010.

[6] Official Website of The Office of the National Coordinator for Health Information Technology (ONC). (2004). Available: <https://www.healthit.gov/>

[7] Canada Health Infoway. (2001). Available: <https://www.infoway-inforoute.ca/en/>

[8] J. Hu, H.H. Chen, T.W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations", Computer Standards & Interfaces vol. 32, No. 5-6, pp. 274-280, 2010.

[9] S. Benabbas, R. Gennaro, Y. Vahlis, “Verifiable Delegation of Computation over Large Datasets”, Conference on Advances in Cryptology. Springer-Verlag, pp. 111-131, 2011.

[10] D. Catalano, D. Fiore. “Vector Commitments and Their Applications”, Public-Key Cryptography – PKC 2013. Springer Berlin Heidelberg, pp. 55-72, 2013.