learning," *Proc of Asiacrypt 2001*, pp. 369-384, 2001.

[10] C. Hazay, Y. Lindell, "Efficient obliv ious polynomial evaluation with simulation-based security," http://eprint.iacr.org/2009/459.pdf.

[11] Huafei Zhu, Feng Bao, "Augmented oblivious polynomial evaluation protocol and its applications," *Computer Security – ESORICS 2005*, pp. 222-230, 2005.

[12] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *Proc of Eurocrypt1991*, pp. 223-238, 1991.

[13] R. Tonicelli, A. C. A. Nascimento, R. Dowsley, J. M. Quade, H. Imai, G. Hanaoka, A. Otsuka, "Information Theoretically Secure Oblivious Polynomial Evaluation: Model, Bounds, and Constructions," *Information Security and Privacy*, pp. 62-73, 2004.

[14] R. Tonicelli, A. C. A. Nascimento, R. Dowsley, J. M. Quade, H. Imai, G. Hanaoka, A. Otsuka, "Information-Theoretically Secure Oblivious Polynomial Evaluation in the Commodity-Based Model," http://eprint.iacr.org/2009/270.pdf

[15] A. Otsuka, A. C. A. Nascimento, H. Imai, "Unconditionally Secure Polynomial Evaluation And Its Application To Electronic Voting," *IEIC Technical Report, Vol.104, No. 200*, pp. 157-164, 2004.

[16] H. Vanishree, K.George, "A Novel Unconditionally Secure Oblivious Polynomial Evaluation Protocol" *Proc of IWISA 2009*, pp. 450-452, 2009.

[17] WANG Qqinglong, Xu Li, "Cryptanalysis on a Novel Unconditionally Secure Oblivious Polynomial Evaluation Protocol," http://eprint.iacr.org/2012/478.pdf

[18] Hong-Da Li, Dong-Yao Ji, Deng-Guo Feng, Bao Li, "Oblivious Polynomial Evaluation," *Journal of computer science and technology. Vol.19, No.4*, pp. 550-554, 2004.

[19] G. Brassard, C. Cr ́epeau, J.M. Robert, "All-or-nothing disclosure of secrets," *Proc of Advances in Cryptology - CRYPTO '86*, pp. 234-238, 1986.

[20] D. Bleichenbacher, P. Nguyen, "Noisy polynomial interpolation and noisy Chinese remaindering," *Proc of Eurocrypt 2000*, pp. 53 –69, 2000.