[23] Mironov I, Stephens-Davidowitz N. Cryptographic reverse firewalls. In: Oswald E, Fischlin M, eds. Proc. of the 34th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2015). Heidelberg: Springer-Verlag, 2015. 657−686.

[24] Boneh D, Halevi S, Hamburg M, Ostrovsky R. Circular-secure encryption from decision Diffie-Hellman. In: Wagner D, ed. Proc. of the 28th Annual Cryptology Conf. (CRYPTO 2008). Heidelberg: Springer-Verlag, 2008. 108−125.

[25] Barak B, Garg S, Kalai YT, Paneth O, Sahai A. Protecting obfuscation against algebraic attacks. In: Nguyen PQ, Oswald E, eds. Proc. of the 33rd Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2014). Heidelberg: Springer-Verlag, 2014. 221−238.

[26] Lindell Y. How to simulate it—A tutorial on the simulation proof technique. IACR Cryptology ePrint Archive: Report 2016/046 (2016), 2016. http://eprint.iacr.org/2016/046.pdf

[27] Bellare M, Hoang VT, Rogaway P. Adaptively secure garbling with applications to one-time programs and secure outsourcing. In: Wang X, Sako K, eds. Proc. of the 18th Int'l Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2012). Heidelberg: Springer-Verlag, 2012. 134−153.

[28] Aiello W, Ishai Y, Reingold O. Priced oblivious transfer: How to sell digital goods. In: Pfitzmann B, ed. Proc. of the 20th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2011). Heidelberg: Springer-Verlag, 2001. 119−135.

[29] Naor M, Pinkas B. Efficient oblivious transfer protocols. In: Proc. of the 12th Annual ACM-SIAM Symp. on Discrete Algorithms. ACM Press, 2001. 448−457.

赵青松(1973－),男,江苏连云港人,博士,讲师,CCF 专业会员,主要研究领域为信息安全和隐私,公钥密码学.

刘西蒙(1988－),男,博士,教授,CCF 专业会员,主要研究领域为应用密码学,数据安全,安全计算,公钥密码学.

曾庆凯(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,分布计算.

徐焕良(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为分布计算,数据科学与计算.