World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:11, No:06, 2017

Rounding Technique's Application in Schnorr Signature Algorithm: Known Partially Most Significant Bits of Nonce

Authors : Wenjie Qin, Kewei Lv

Abstract : In 1996, Boneh and Venkatesan proposed the Hidden Number Problem (HNP) and proved the most significant bits (MSB) of computational Diffie-Hellman key exchange scheme and related schemes are unpredictable bits. They also gave a method which is a lattice rounding technique to solve HNP in non-uniform model. In this paper, we put forward a new concept that is Schnorr-MSB-HNP. We also reduce the problem of solving Schnorr signature private key with a few consecutive most significant bits of random nonce (used at each signature generation) to Schnorr-MSB-HNP, then we use the rounding technique to solve the Schnorr-MSB-HNP. We have come to the conclusion that if there is a 'miraculous box' which inputs the random nonce and outputs 2loglogq (q is a prime number) most significant bits of nonce, the signature private key will be obtained by choosing 2logq signature messages randomly. Thus we get an attack on the Schnorr signature private key.

Keywords : rounding technique, most significant bits, Schnorr signature algorithm, nonce, Schnorr-MSB-HNP
Conference Title : ICISC 2017 : International Conference on Information Security and Cryptography
Conference Location : Amsterdam, Netherlands
Conference Dates : June 18-19, 2017