Xue, Haiyang; Li, Bao; Lu, Xianhui; Wang, Kunpeng; Liu, Yamin
On the lossiness of $2^k$-th power and the instantiability of rabin-OAEP.


Summary: Seurin (PKC 2014) proposed the $2^{-\Phi/4}$-hiding assumption which asserts the indistinguishability of Blum Numbers from pseudo Blum Numbers. In this paper, we investigate the lossiness of $2^k$-th power based on the $2^k - \Phi/4$-hiding assumption, which is an extension of the $2 - \Phi/4$-hiding assumption. And we prove that $2^k$-th power function is a lossy trapdoor permutation over Quadratic Residuosity group. This new lossy trapdoor function has $2k$-bits lossiness for $k$-bits exponent, while the RSA lossy trapdoor function given by Kiltz et al. (Crypto 2010) has $k$-bits lossiness for $k$-bits exponent under $\Phi$-hiding assumption in lossy mode. We modify the square function in Rabin-OAEP by $2^k$-th power and show the instantiability of this Modified Rabin-OAEP by the technique of Kiltz et al. (Crypto 2010). The Modified Rabin-OAEP is more efficient than the RSA-OAEP scheme for the same secure bits. With the secure parameter being 80 bits and the modulus being 2048 bits, Modified Rabin-OAEP can encrypt roughly 454 bits of message, while RSA-OAEP can roughly encrypt 274 bits.

Keywords: Rabin; OAEP; Lossy trapdoor function; $\Phi$-hiding
doi:10.1007/978-3-319-12280-9_3