Bibliography


[35] Lei Guo, Lincong Zhang Peng, Jingjing Wu, Xiaoying Zhang, Weigang Hou, Jun Zhao,


[73] Yevgeniy Dodis, Rosario Gennaro, Johan Hastad, Hugo Krawczyk, Tal Rabin, “Randomness extraction and key derivation using the CBC, Cascade and HMAC Modes”,
Annual International Cryptology Conference(CRYPTO), 2004, Santa Barbara, California, USA, pp.494-510.


