Cryptology ePrint Archive: Report 2013/213

On (Destructive) Impacts of Mathematical Realizations over the Security of Leakage Resilient ElGamal Encryption

Guangjun Fan and Yongbin Zhou and F.-X. Standaert and Dengguo Feng

Abstract: Leakage resilient cryptography aims to address the issue of inadvertent and unexpected information leakages from physical cryptographic implementations. At Asiacrypt 2010, E.Kiltz et al. [1] presented a multiplicatively blinded version of ElGamal public-key encryption scheme, which is proved to be leakage resilient in the generic group model against roughly 0.50*log(p) bits of arbitrary, adversarially chosen information leakage about the computation, when the scheme is instantiated over bilinear groups of prime order p (denoted BEG^*). Nonetheless, for the same scheme instantiated over arbitrary groups of prime order p (denoted EG^*), no leakage resilience bound is given, and was only conjectured to be leakage resilient. In this paper, we show that, when some of the leakage happens within the computation of pseudo random number generator (PRNG) used by EG^*, the leakage tolerance of EG^* is far worse than expected. We used three instances of internationally standardized PRNGs to analyze the leakage resilience of different mathematical realizations of EG^*, namely ANSI X9.17 PRNG, ANSI X9.31 PRNG using AES-128, and FIPS 186 PRNG for DSA pre-message secrets, respectively. For ANSI X9.17 PRNG and ANSI X9.31 PRNG using AES-128 (resp. DSA PRNG) considered, when the size of p is 1024 bits (resp. 1120 bits), one can successfully recover the long-term secret key x if he learns only 0.2988*log(p) and 0.2832*log(p) (resp. 0.2929*log(p)) bits of leakages of the computation respectively. This shows that mathematical realizations of EG^* can have significant impacts on its leakage resilience. In addition, by presenting non-generic attacks, this paper also gives some upper bounds of the amount of leakages that these mathematical realizations of EG^* can tolerate, and these upper bounds are the best known so far.

Category / Keywords: Leakage Resilient Cryptography, ElGamal Encryption, Mathematical Realization, PRNG, Lattice

Date: received 12 Apr 2013, last revised 14 Apr 2013

Contact author: guangjunfan at 163 com