Cryptology ePrint Archive: Report 2011/392

An Efficient Rational Secret Sharing Scheme Based on the Chinese Remainder Theorem (Revised Version)

Yun Zhang, Christophe Tartary and Huaxiong Wang

Abstract: The design of rational cryptographic protocols is a recently created research area at the intersection of cryptography and game theory. At TCC'10, Fuchsbauer \emph{et al.} introduced two equilibrium notions (computational version of strict Nash equilibrium and stability with respect to trembles) offering a computational relaxation of traditional game theory equilibria. Using trapdoor permutations, they constructed a rational t-out-of n sharing technique satisfying these new security models. Their construction only requires standard communication networks but the share bitsize is $2 n |s| + O(k)$ for security against a single deviation and raises to $(n-t+1)\cdot (2n|s|+O(k))$ to achieve $(t-1)$-resilience where k is a security parameter. In this paper, we propose a new protocol for rational t-out-of n secret sharing scheme based on the Chinese reminder theorem. Under some computational assumptions related to the discrete logarithm problem and RSA, this construction leads to a $(t-1)$-resilient computational strict Nash equilibrium that is stable with respect to trembles with share bitsize $O(k)$. Our protocol does not rely on simultaneous channel. Instead, it only requires synchronous broadcast channel and synchronous pairwise private channels.

Category / Keywords: cryptographic protocols / rational cryptography, computational strict Nash equilibrium, stability with respect to trembles, Asmuth-Bloom sharing

Publication Info: the original version has been published by ACISP 2011 and here we make some modifications

Date: received 19 Jul 2011

Contact author: zhan0233 at e ntu edu sg