Cryptology ePrint Archive: Report 2011/330

Simple and Asymptotically Optimal t-Cheater Identifiable Secret Sharing Scheme

Ashish Choudhury

Abstract: In this paper, we consider the problem of k-out-of-n secret sharing scheme, capable of identifying t cheaters. We design a very simple k-out-of-n secret sharing scheme, which can identify up to t cheaters, with probability at least 1 - \epsilon, where 0 < \epsilon < 1/2, provided t < k / 2. This is the maximum number of cheaters, which can be identified by any k-out-of-n secret sharing scheme, capable of identifying t cheaters (we call these schemes as Secret Sharing with Cheater Identification (SSCI)). In our scheme, the set of all possible i^{th} share V_i satisfies the condition that |V_i| = |S| / \epsilon^{3n}, where S denotes the set of all possible secrets. Moreover, our scheme requires polynomial computation.

In EUROCRYPT 2011, Satoshi Obana presented two SSCI schemes, which can identify up to t < k / 2 cheaters. However, the schemes require |V_i| \approx (n (t+1) 2^{3t-1} |S|) / \epsilon and |V_i| \approx ((n t 2^{3t})^2 |S|) / (\epsilon^2)$ respectively. Moreover, both the schemes are computationally inefficient, as they require to perform exponential computation in general. So comparing our scheme with the schemes of Obana, we find that not only our scheme is computationally efficient, but in our scheme the share size is significantly smaller than that of Obana. Thus our scheme solves one of the open problems left by Obana, urging to design efficient SSCI scheme with t < k/2.

In CRYPT0 1995, Kurosawa, Obana and Ogata have shown that in any SSCI scheme, |V_i| \geq (|S| - 1) / (\epsilon) + 1. Though our proposed scheme does not exactly matches this bound, we show that our scheme {\it asymptotically} satisfies the above bound. To the best of our knowledge, our scheme is the best SSCI scheme, capable of identifying the maximum number of cheaters.

Category / Keywords: cryptographic protocols /

Date: received 17 Jun 2011

Contact author: partho31 at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110622:200815 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]