Cryptology ePrint Archive: Report 2011/480

Complete Tree Subset Difference Broadcast Encryption Scheme and its Analysis

Sanjay Bhattacherjee and Palash Sarkar

Abstract: The Subset Difference (SD) method proposed by Naor-Naor-Lotspeich is the most popular broadcast encryption (BE) scheme. It is suitable for real-time applications like Pay-TV. It has been suggested for use by the AACS standard for digital rights management in Blu-Ray and DVD discs. The SD method assumes the number of users to be a power of two. (1) We propose the Complete Tree Subset Difference (CSD) method that subsumes the SD method by allowing arbitrary number of users in the system. All the results obtained in this work for the CSD scheme hold good for the SD scheme by assuming the number of users to be the next power of two. (2) Given the importance of the SD scheme, its detailed combinatorial analysis is of practical interest. We find recurrences for the CSD scheme to count the number of possible ways r users in the system of n users can be revoked to result in a transmission overhead (header length) of h. The header length h of a broadcast is an important efficiency parameter in BE. The usefulness of these recurrences is demonstrated by generating exhaustive data of the above count, obtaining bounds on the header length and various other interesting results some of which are difficult to prove without the recurrences. (3) An $O(r \log{n})$ time algorithm is proposed to compute the expected header length in the CSD scheme for n users in the system, r out of which are revoked. This algorithm is of practical interest in its own right, for efficiency and performance analysis of the CSD scheme. Using this algorithm, we show that for practical values of n and r, the transmission efficiency of the CSD scheme is better than the SD scheme. For n a power of two and a fixed $r \geq 2$, we obtain an upper bound on the expected header length and show that this bound is also the limit as $n \rightarrow \infty$.

Category / Keywords: Broadcast encryption; combinatorial analysis; recurrences; probabilistic analysis; expected header length; asymptotic analysis

Date: received 6 Sep 2011

Contact author: sanjayb_r at isical ac in

Available formats: PDF | BibTeX Citation

Version: 20110908:103136 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]