2-Tree or not 2-Tree

Rump Session, Asiacrypt 2013

Who? Sanjay Bhattacherjee
Palash Sarkar

From? Applied Statistics Unit
Indian Statistical Institute, Kolkata

When? December 3, 2013
Pay-TV Subscription

Only a subscribed user is privileged to decrypt the broadcast.
The Subset Difference Scheme

... due to Naor-Naor-Lotspiech (CRYPTO, 2001)

assumes an underlying full binary tree

Level Numbers

0 1 2 3 4

15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
**Generalization of the NNL-SD scheme**

The $k$-SD scheme assumes a full $k$-ary tree instead of binary. Example for $k = 3$, $n = 27$.

Subsets are of the form $S_i,\{j_1,...,j_c\}$ where nodes $j_1, \ldots, j_c$ are siblings in the subtree of $i$. 
\(k\)-SD PERFORMANCE

User Storage

\[
\ell_0 = \lceil \log_k n \rceil
\]

\(\chi_k = \text{\#cyclotomic cosets modulo } 2^k - 1.\)

\[
(\chi_k - 2)\ell_0(\ell_0 + 1)/2
\]

is \(\min(2r - 1, n - r, \lceil n/k \rceil).\)
Impact of $k$-SD scheme

Plot for MHL

Sanjay Bhattacherjee; Palash Sarkar (ISI, Kolkata)
The $k$-ary tree SD scheme improves MHL for $r/n > \delta_k$ (a threshold value for a given $k$).

**In Theory**

... we have a hierarchy of optimization between the NNL-SD scheme and the Power Set scheme.

**Practically**

In applications like Pay-TV

... where the sessions change very frequently

... the number of revoked users is moderate

the communication cost can be improved.
Any Questions?
email: sanjayb_r@isical.ac.in
Cryptology ePrint Archive: Report 2013/786