2-Tree or not 2-Tree

Rump Session, Asiacrypt 2013

Who? Sanjay Bhattacherjee
Palash Sarkar

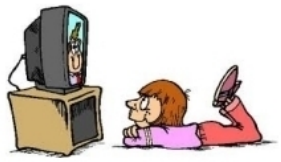
From? Applied Statistics Unit
Indian Statistical Institute, Kolkata

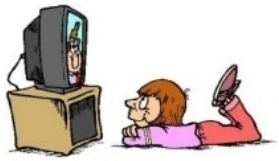
When? December 3, 2013

Pay-TV Subscription

Privileged / Revoked

Only a subscribed user is privileged to decrypt the broadcast.





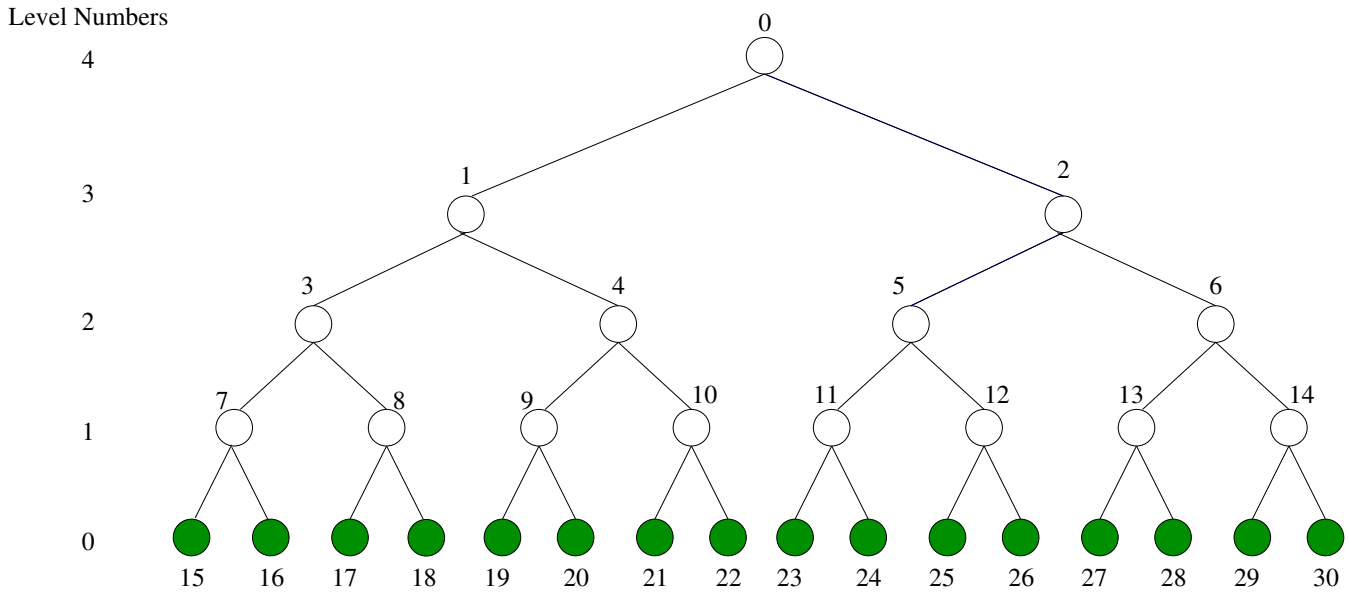
Subscribed User

Unsubscribed User

The Subset Difference Scheme

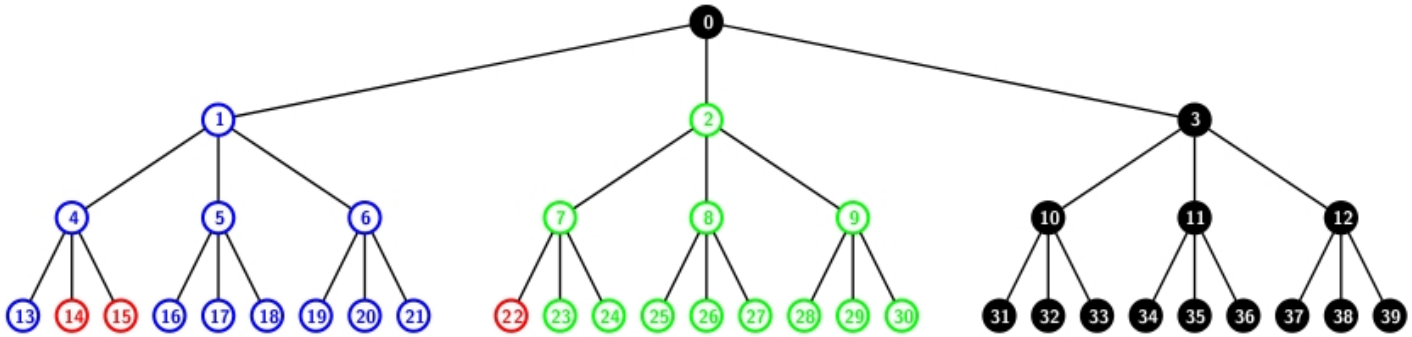
... due to Naor-Naor-Lotspiech (CRYPTO, 2001)

assumes an underlying full binary tree



Generalization of the NNL-SD scheme

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



Subsets are of the form $S_{i,\{j_1,\ldots,j_c\}}$ where nodes $j_1, \ldots, j_c$ are siblings in the subtree of i.

k-SD performance

User Storage

$$(\chi_k - 2)\ell_0(\ell_0 + 1)/2$$

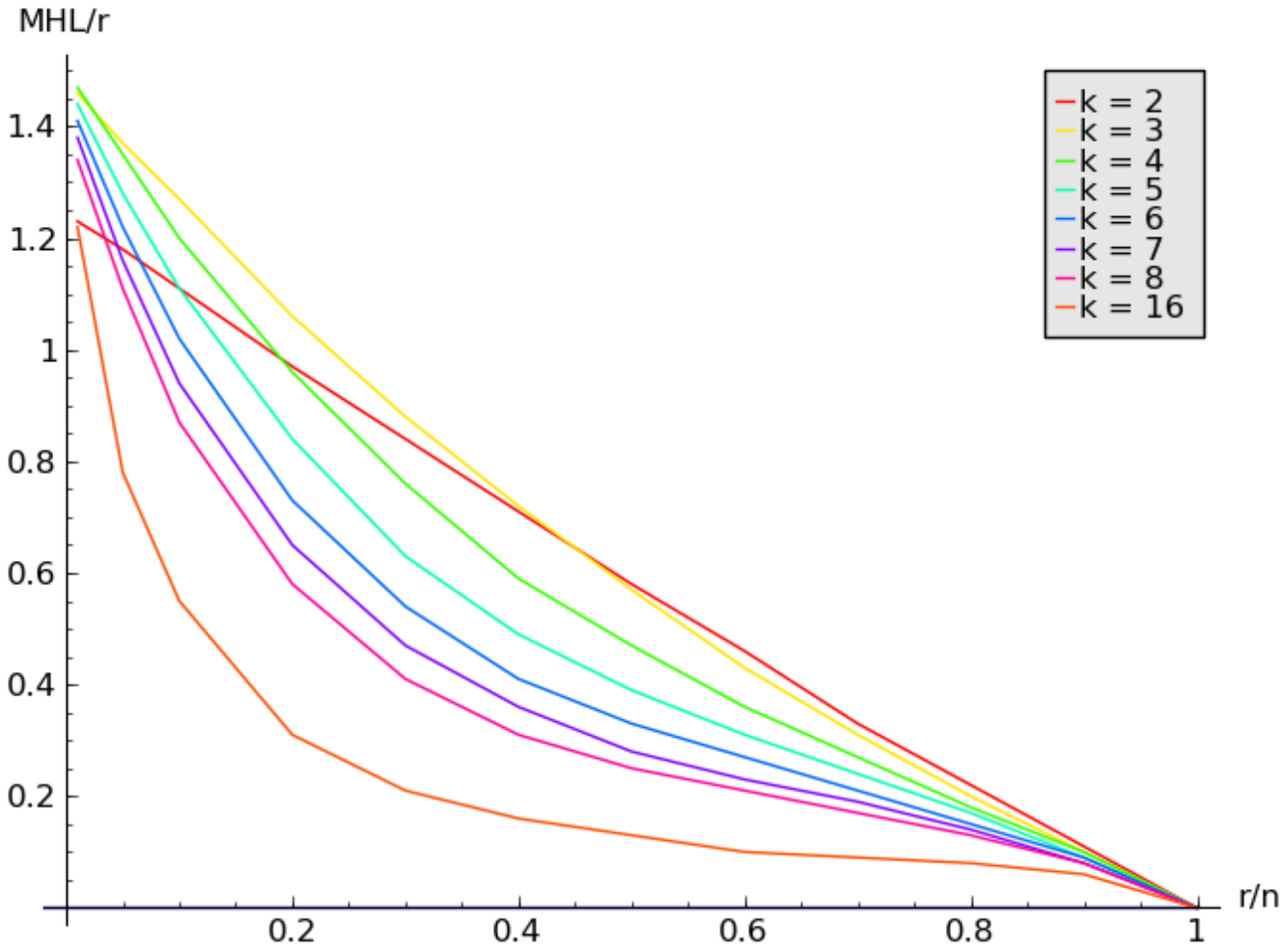
$\ell_0 = \lceil \log_k n \rceil$
$\chi_k = \#$cyclotomic cosets modulo $2^k - 1$.

Maximum header length

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

Impact of k-SD scheme

Plot for *MHL*



Impact of Generalization

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.

Thank You

Any Questions?

email: sanjayb_r@isical.ac.in

Cryptology ePrint Archive: Report 2013/786