Reducing communication cost of (NNL) Broadcast Encryption

Rump Session, ECC 2014

Who? Sanjay Bhattacherjee Palash Sarkar

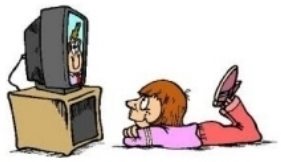
From? Applied Statistics Unit
Indian Statistical Institute, Kolkata

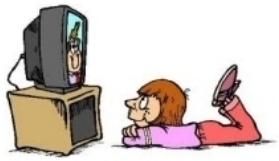
When? October 8, 2014

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)

Patented and used in the AACS standard. It assumes an underlying full binary tree

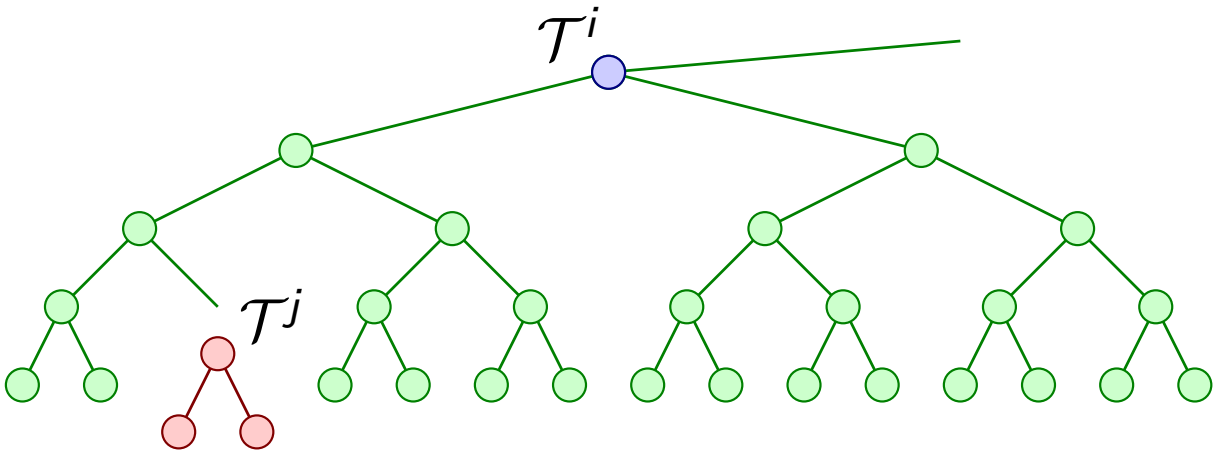
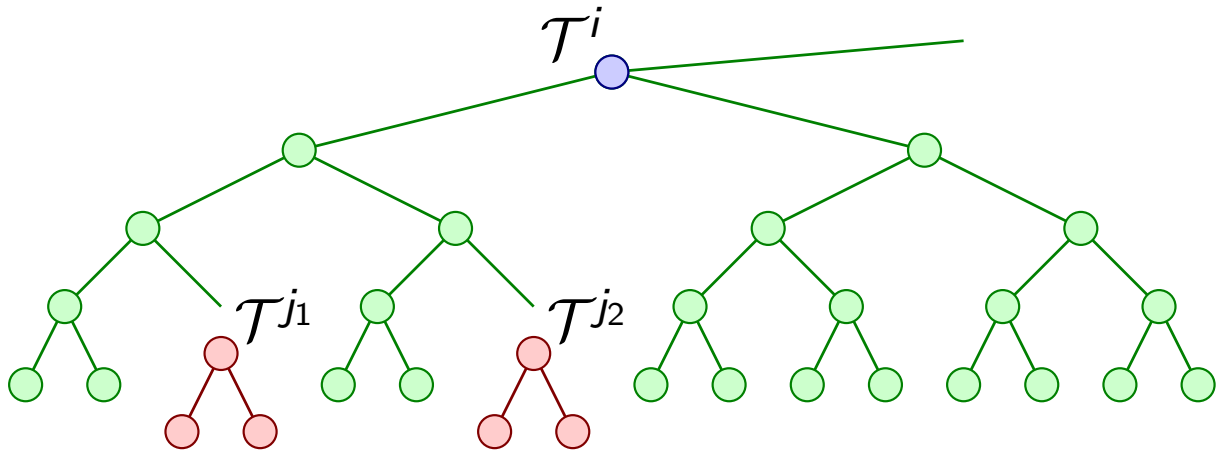


Figure: An example of a subset difference (SD) subset $S_{i,j}$ that has leaves of the subgraph $\mathcal{T}^i \setminus \mathcal{T}^j$.

Generalization of the NNL-SD scheme

a-ABTSD scheme

assumes augmented tree structures associated with each internal node.

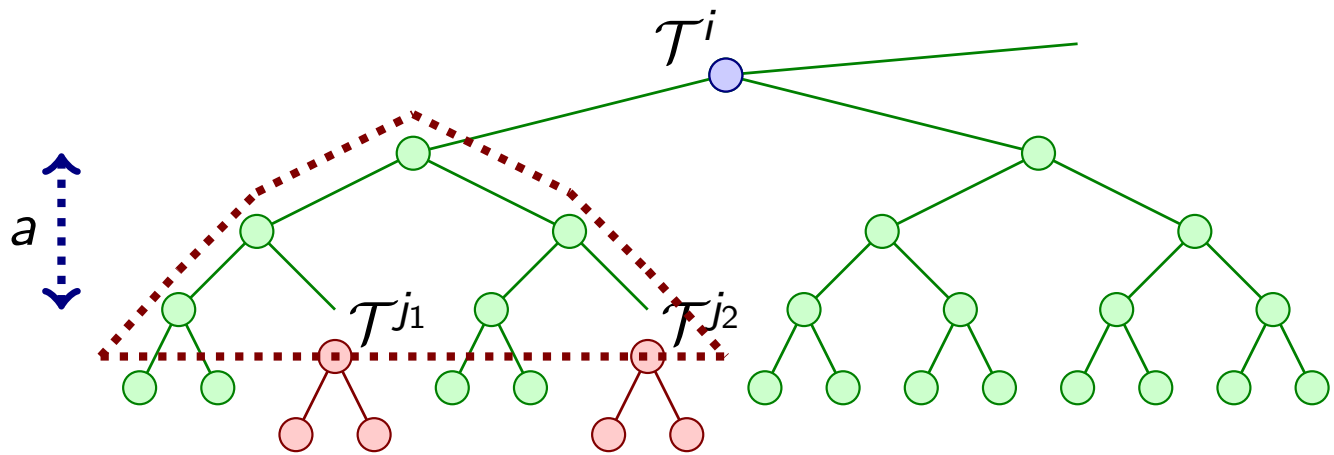


Subsets

are of the form $S_{i,\{j_1,\ldots,j_c\}}$ where nodes $j_1, \ldots, j_c$ are leaf nodes of the augmented tree structure.

Generalization of the NNL-SD scheme

a-ABTSD scheme assumes augmented tree structures associated with each internal node.



Subsets are of the form $S_{i,\{j_1,\ldots,j_c\}}$ where nodes $j_1, \ldots, j_c$ are leaf nodes of the augmented tree structure.

a-ABTSD performance

$a = 1$ is NNL-SD.

$a = 2, 3, 4$ should be good enough for practical purposes.

a-ABTSD performance

$a = 1$ is NNL-SD.
$a = 2, 3, 4$ should be good enough for practical purposes.

Header Length for $a > 1$ is at most as large as $a = 1$ (NNL-SD). (for any revoked set)

a-ABTSD performance

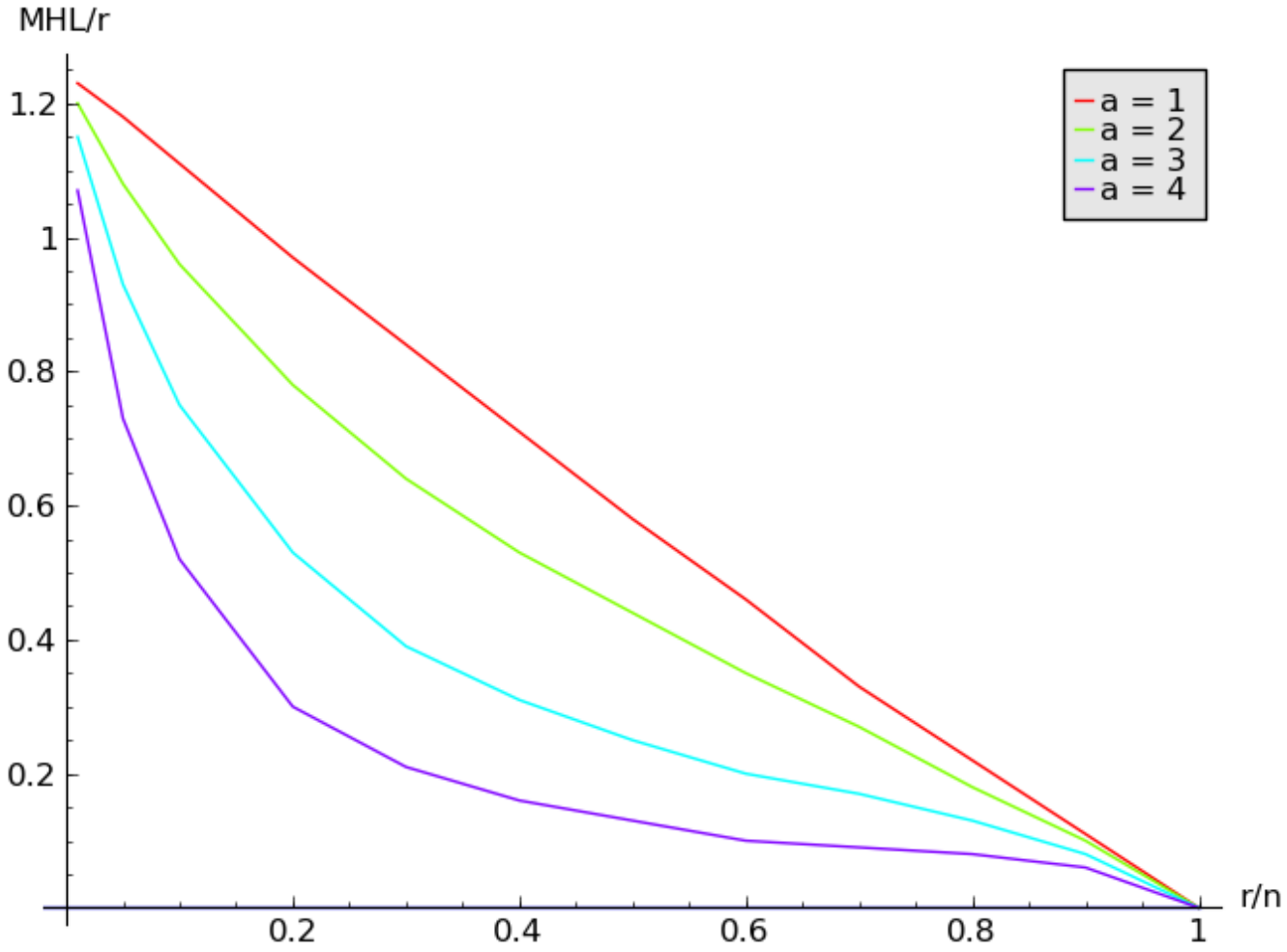
$a = 1$ is NNL-SD.
$a = 2, 3, 4$ should be good enough for practical purposes.

Header Length for $a > 1$ is at most as large as $a = 1$ (NNL-SD). (for any revoked set)

User Storage $1 + \ell_0(\ell_0 + 1)/2 + (\chi_{2^a} - 2)(\ell_0 - a + 2)(\ell_0 - a + 1)/2$
$\ell_0 = \lceil \log_k n \rceil$
$\chi_k = \#$cyclotomic cosets modulo $2^{2^a} - 1$.

Impact of a-ABTSD scheme

Plot for *MHL*



Impact of Generalization

The a-Augmented Binary Tree SD scheme **guarantees** improved mean header length.

Impact of Generalization

The a-Augmented Binary Tree SD scheme **guarantees** improved mean header length.

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

Impact of Generalization

The a-Augmented Binary Tree SD scheme **guarantees** improved mean header length.

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

In Applications (like Pay-TV) that are presumably using the NNL-SD scheme ($a = 1$) currently,
... where the sessions change very frequently
... for $n = 10^8$ and $r = 0.4n$ (using 128-bit keys),
using $a = 2$ saves 6.8MB per session;
using $a = 3$ saves 15.3MB per session;
using $a = 4$ saves 20.9MB per session.

Thank You

Any Questions?

email: sanjayb_r@isical.ac.in

Cryptology ePrint Archive: Report 2014/577