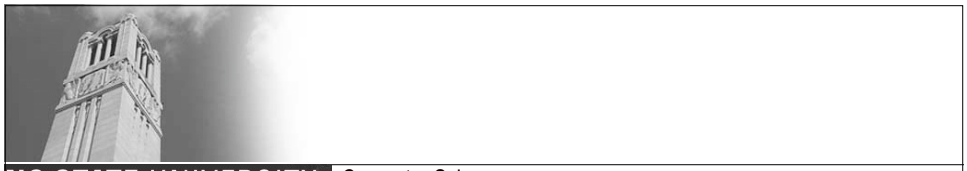


NC STATE UNIVERSITY Computer Science

Coding Constructions for Blacklisting Problems without Computational Assumption

-Donggang Liu

CSC774 Network Security

Outline

- Background
  - Problem
  - Related work
- Proposed Schemes
  - Randomized construction
  - Construction based on polynomials
  - Construction based on algebraic-geometric codes

Problem

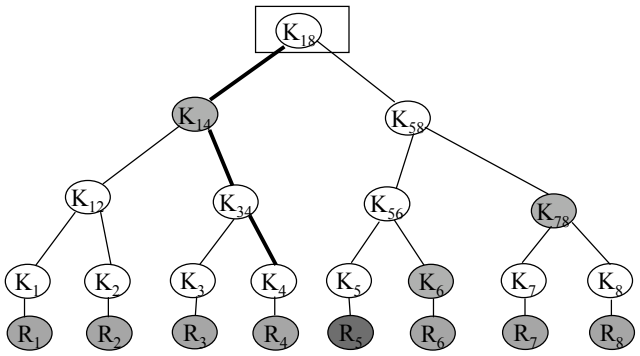
- Secure Communication over broadcast channel
  - One sender, multiple receivers
  - Insecure broadcast channel
  - Receivers may misuse the broadcasted messages
- Issue: how to transmit the data over insecure broadcast channel so that only the select receivers can recovery the content (Broadcast exclusion)

Related work

- Broadcast encryption (by Fiat and Naor 1993)
  - First construct a scheme to exclude a single malicious receiver.
  - Then extend to a scheme to exclude a set of k malicious receivers based on multi-layered hashing techniques and pseudo-random generator
  - Communication overhead $O(k^2 n \log^2 k)$, storage overhead $O(kn^2 \log k)$, where the total number of receivers $N=2^n$
- Other work

Related work (cont'd)

- Logic key hierarchy (wallner et al.)
  - Construct a key tree.
  - Broadcast O(log*N*) messages to update the common key

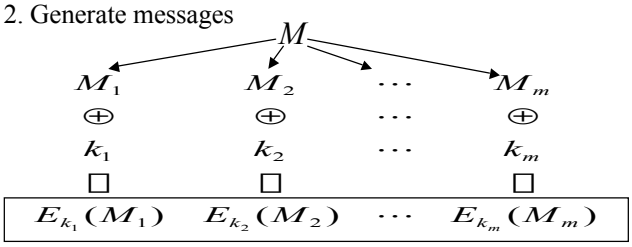


Contributions

- A framework for broadcast exclusion technique
- Based on the above framework, three different schemes are proposed to address this problem. The communication overhead for two of them are totally independent from the total number of receivers

Proposed solutions

- Goal: exclude up to k receivers from the group
- Framework
  - 1. Setup
    - Sender maintains a set of key K=$\{k_1,k_2,\ldots,k_m\}$.
    - Each receiver has a subset of keys in K.
  - 2. Generate messages



  - 3. Broadcast: discards all pieces encrypted by the keys belong to all excluded receivers and broadcasts all the remain pieces

Framework (cont'd)

- The excluded receivers cannot recovery anything from the broadcast messages
- Ensure the following two properties
  - Inner code: The non-excluded receiver can decrypt enough pieces of the message while maximize the total number of receivers we can support.
  - Outer code: Given the number of pieces guaranteed by inner code, the non-excluded receiver can reconstruct the original message M.

Example

- Setup
  - k=1 and K=$\{k_1,\ldots,k_{2n}\}$, totally $2n$ keys.
  - Each receiver i has a different subset S_i of keys from K and $|S_i|=n$. The maximal number of receivers is $\binom{2n}{n}$
- Broadcast:
  - To exclude receiver j, message M is encrypted n times: once using each keys in S but not in set S_j. ($M=M_1=\ldots=M_{2n}$).
- Each non-excluded receiver can decrypt at least one message. But receiver j cannot decryption anything
- The communication overhead is increased by n times

Problems left

- How to design a efficient inner code and outer code scheme
- Inner code:
  - Total key set K and key subset in each receiver i, S_i
  - randomization, polynomial based and AG code based
- Outer code:
  - Simplest: $M=M_1=M_2=\ldots=M_m$. It requires each non-excluded receiver can at least decrypt one piece
  - Erasure code: split M into n redundant pieces so that the original message M can be reconstructed from any k out of n pieces. It requires each non-excluded receiver can decrypt at least k pieces.

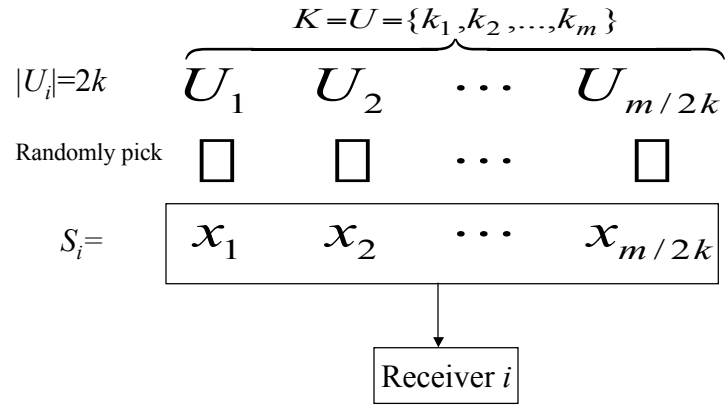
Outer code

- Example of erasure code (k,n): polynomial based scheme
  - Split M into k pieces: M=$v_0|v_1|\ldots|v_{k-1}$, "|" denotes concatenation and construct a polynomial $f(x)$= $v_0+v_1x+\ldots+v_{k-1}x^{k-1}$.
  - Evaluate $f(x)$ at point $\{1,\ldots,n\}$ and get $\{f(1),\ldots,f(n)\}$.
  - If any receiver receives k of $\{f(1),\ldots,f(n)\}$, it knows k point on a $k-1$ degree polynomial f(x). Thus, it can recover $f(x)$ and further recover M

Inner code

- Randomized construction
- Polynomial based
- Algebraic-geometric code based

Randomized construction



Randomized construction (cont'd)

- Theorem 2
  - There exists a universal constant c such that for any t>0, if $N = \exp(\frac{cm}{k(k+1)} \cdot \frac{t}{k+1})$, then the probability that a non-excluded receiver can decrypt at least (m/4k) of the messages is at least 1-exp(-t)

Randomized construction (cont'd)

- Inner code
  - The collusion of no more than *k* excluded receiver cannot recovery anything. Each non-excluded can decrypt at least *m/4k* messages at a high probability.
- Outer code
  - Simplest: communication overhead O(m), storage overhead O(m/2k)
  - (m/4k,m) erasure code: communication overhead reduced to 4*k*, storage overhead O(*m/2k*)=O(*kn*), (N=2^n)

Polynomial based construction

- Let $m=q^2$, where q is a prime number.

$$F_q = \{u_1, u_2, \ldots, u_q\} \rightarrow K = U = F_q^2 = \{< u, v > | u, v \in F_q\}$$

$$\downarrow$$

$$F_{q,d} = \{f(x) = \sum_{i=0}^{t, t \le d} a_i x^i \mid a_i \in F_q\}$$

$$\downarrow$$

$$S_i = \{< u_1, f(u_1) >, \ldots, < u_q, f(u_q) >\}_{d=\frac{q}{2k}, f \in F_{q,d+1}}$$

$$\downarrow$$

Receiver *i*

Polynomial based construction

- Theorem 3
  - With the above construction, the non-excluded receiver can decrypt at least $q/2$ pieces of messages with $N = \exp(\frac{\sqrt{m}\log m}{4k})$

Polynomial based construction (cont'd)

- Inner code
  - The collusion of no more than k excluded receiver cannot recovery anything. Each non-excluded can decrypt at least $q/2$ messages.
- Outer code
  - Simplest: communication overhead blowup O(m), storage overhead O(q)
  - (q/2,m) erasure code: communication overhead blowup is reduced to $2q$=O(kn), storage overhead O(q)=O(kn), ($N=2^n$).

AG code based

- Based on AG code
  - Generate a total key set:

$$K_{|K|=m=s(n)q^2, s(n)=q^{n+1}-q^{n-1}, k=\lfloor q/6 \rfloor}$$

  - Generate a set system:

$$S = \{S_1, \ldots, S_N\} (|S_i| = s(n))$$

$$N = \exp(O(\frac{m \log k}{k^3}))$$

  - After exclude up to *k* receivers, each non-excluded receiver can decrypt at least *s(n)*/2 pieces

AG code based (cont'd)

- Inner code
  - The collusion of no more than k excluded receiver cannot recovery anything. Each non-excluded can decrypt at least s(n)/2 messages.
- Outer code
  - Simplest: communication overhead blowup O(m), storage overhead O(s(n))
  - (s(n)/2,m) erasure code: communication overhead blowup is reduced to $2q^2$=O(k^2), storage overhead O(s(n))=O(*kn*)

Summary

- Proposed a general framework for broadcast exclusion scheme
- With the proposed framework, propose three different scheme. The communication overhead blowup for two of them are independent from the total number of receivers.
  - Randomized construction
  - Polynomial based
  - AG code based

Question?