Számítógép hálózatok, osztott rendszerek

8: Anonimitás

Motiváció

- Közösség
  - Szólásszabadság csak akkor lehetséges, ha a felszólalóra az nem járhat negatív következménnyel
  - Így csak egy anonim felszólalónak valódi szólásszabadsága van
- Szerzői jog megsértés
  - Számítógéppel könnyű másolni (legtöbbször számítógéppel történik)
  - Szerzői jogok korlátozzák a másolást
  - File megosztók felhasználói nem akarnak büntethetők lenni
- Diktatúra
  - Elnyomó rendszerek egy előfeltétele az információ és a vélemények kontrollálása tematizáló hatalom, vélemény hatalom
  - Publikálás anélkül hogy félni kelljen a megtorlástól
- Demokráciák
  - bizonyos álláspontok képviselése nem legitim, pl.
  - közösség elleni uszítás (Btk. 332§)
  - bizonyos szexuális tartalmak
  - politikai nézetek (pl. fasiszta, kommunista, szaparatista, …)
- Anonimizáló P2P hálózatoknak biztosítani kell minden felhasználó személyi jogainak védelmét és anonimitását más felhasználók veszélyeztetése nélkül

Terminológia

- Danezis, Diaz: A Survey of Anonymous Communication Channels
- Pfitzmann, Hansen: Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology

- Anonimitás (Pfitzmann-Hansen 2001)
  - nem azonosíthatóság egy nagyobb halmazon belül, az anonimitási halmazon belül
  - Az anonimitási halmaz lehet egy P2P hálózat összes peer-je
    - De lehet más halmaz is, egy kisebb vagy egy még nagyobb halmaz

Terminológia

- Összekapcsolhatatlanság (Unlinkability)
  - Abszolut (ISO15408)
    - „biztosítja, hogy egy felhasználó több erőforrást vagy szolgáltatást használjon, anélkül, hogy mások képesek legyenek összekapcsolni ezeket a használatokat“
  - Relatív
    - Egy támadó nem tudhat meg többet a használatok közötti kapcsolatról a rendszer megfigyelésével
    - a-priori knowledge = a-posteriori knowledge

Terminológia

- Megfigyelhetetlenség (Unobservability)
  - Az érdeklődés védett
  - Bármely szolgáltatás használata vagy annak nem használata nem deríthető ki egy megfigyelő(támadó) által
- Pszeudonimitás
  - Pszeudonim használata azonosítóként
  - Megtartja a hozzárendelhetőséget és megbízhatóságot az anonimitás megtartásával

Támadások

- Denial-of-Service támadások (DoS)
  - vagy elosztott DoS (DDoS)
  - egy vagy sok peer kér egy dokumentumot
  - A peer-ek lelassulnak vagy teljesen leállnak
- Sybil támadás
  - Egy támadó sok „fake” peer-t hoz létre új IP címekkel
  - Vagy a támadó egy bot-net-et irányít
- Protokoll gyengeségeinek kihasználása
- Rosszindulatú peer-ek általi elidegenítés (infiltration)
  - Bizánci tábornokok
- Időzítési támadások
  - Üzenetek lelassulnak
  - Kommunikációs vonal lelassul
  - Egy kapcsolat létesíthető küldő és fogadó között
- Megfertőzés támadás
  - Hamis információ rendelkezésre bocsájtása
  - Rossz routing tábla, rossz index file, stb…
- Eclipse támadás
  - Egy peer környezetének megtámadása
  - Egy peer szeparálása
  - Egy „fake” környezet felépítése

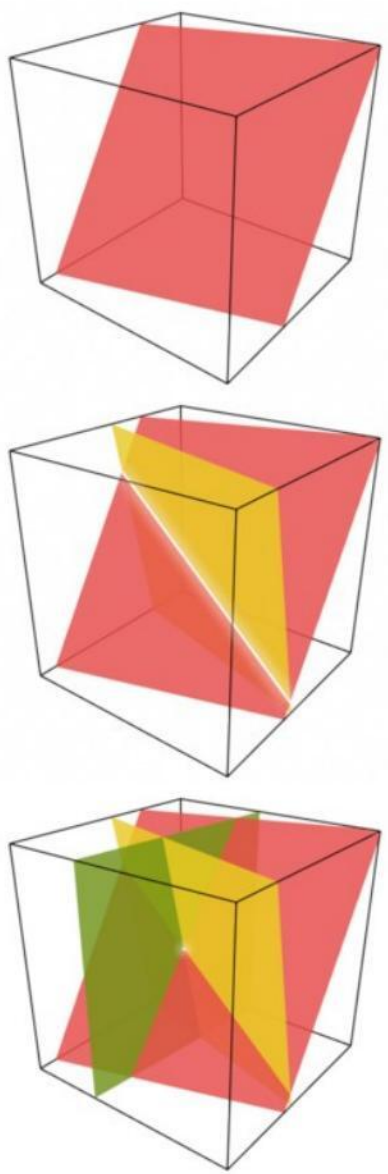
Kryptográfia dióhéjban

- Szimmetrikus kryptografia
  - AES
  - Affin kryptorendszerek
- Nyilvános kulcsó kryptográfia
  - RSA
  - ElGamal
- Digitális szignatúra
- Public-Key-Exchange
  - Diffie-Hellman

- Interaktív bizonyítás rendszerek
  - Zéro-ismeretű bizonyítások (Zero-Knowledge-Proofs)
  - Titok megosztás (Secret Sharing)
  - Biztonságos több-résztvevős számítás (Secure Multi-Party Computation)

Blakley titok megosztás sémája

- George Blakley, 1979
- Feladatok
  - n személy megoszt egy titkot
  - csak akkor lehet megtudni a titkot, ha k személy jelen van
- Blakley sémája
  - A k-dimenziós térben k (lineárisan független) k-1-dimenziós hipersík metszete definiál egy pontot
  - ez a pont a titkos információ
  - k-1 hipersík egy egyenest határoz meg
- Konstrukció
  - Egy harmadik (megbízható) instancia generál egy $x \in R^k$ ponthoz n hipersíkot, melyek közül bármely k lineárisan független

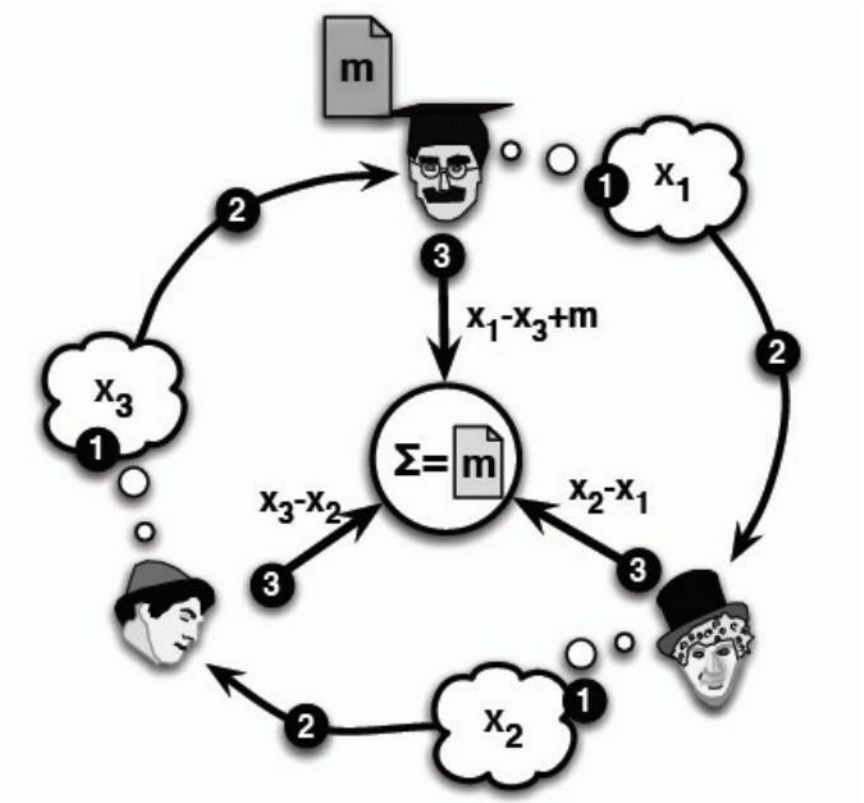


Shamir titok megosztás rendszere

- Adi Shamir, 1979
- Feladat
  - n személy megoszt egy s titkot
  - az n közül k együttesen tudja visszafejteni az s titkot
- Egy megbízható harmadik konstrukciója
  - Válasszunk k-1 random számot $a_1,...,a_{k-1}$
  - Ezek definiálják:
  - $f(x) = s + a_1x + \ldots + a_{k-1}x^{k-1}$
  - Válasszunk n különböző random számot: $x_1, x_2, ..., x_n$
  - Az i. személynek elküldjük: $(x_i,f(x_i))$
- Ha k személy találkozik
  - együtt ki tudják számítani az f függvényt: Egy d-ed fokú valós együtthatós polinomot meghatároz d+1 értéke
  - Ehhez kicserélik az értékeiket és kiszámítják interpolációval
    - Lagrange polinom
- Ha k-1 személy találkozik
  - nem tudják meghatározni a polinomot és így az s titkot
  - bármilyen s érték lehetséges
- Általában Shamir és Blakley sémáját véges testtel alkalmazzák
  - Ez leegyszerűsíti a számítást, elkerüli a kerekítési hibákat, amiket lebegőpontos számításnál fellépnének

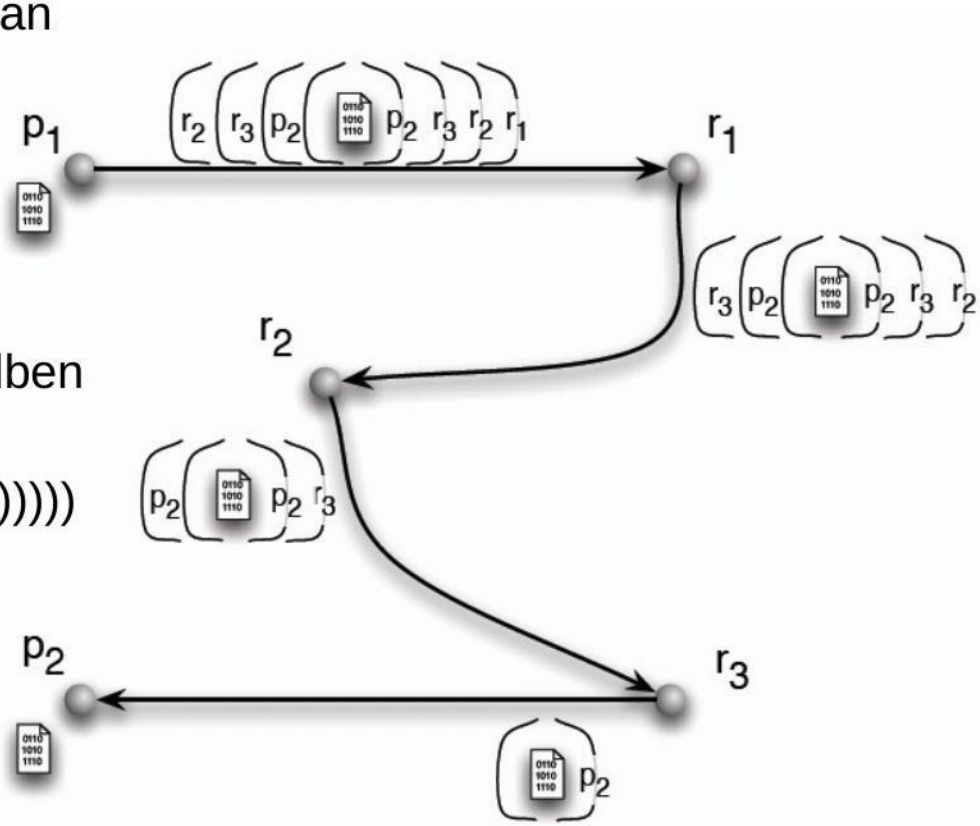
Az vacsorázó kryptográfusok

- Anonim publikálás visszakövethetőség nélkül
- n ≥ 3 kryptográfus ül egy asztalnál
  - Szomszédos kriptográfusok titkosan tudnak egymással kommunikálni
- Minden peer i választ magának egy titkos számot: x_i és ezt elküldi a jobboldali szomszédjának ((i mod n)+1-nek)
- Ha i egy m üzenetet akar publikálni, akkor nyilvánosságra hozza
  - $s_i = x_i - x_{i-1} + m$
- egyébként pedig
  - $s_i = x_i - x_{i-1}$
- Minden peer kiszámítja: $s=s_1+...+s_n$
  - ha s=0, akkor nincs üzenet
  - különben pedig s = m az üzenet



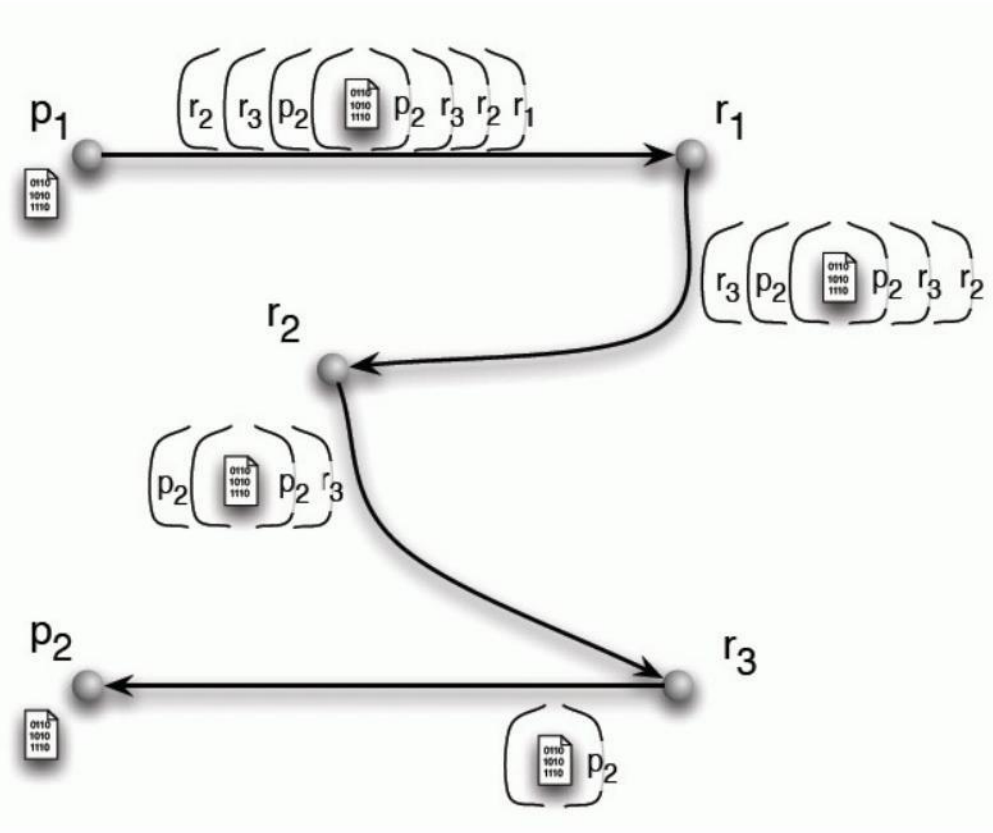
Chaum „mix cascades” módszere

- Minden peer
  - a nyilvános kulcsa ismert a hálózatban
- A küldő p_1 választ egy útvonalat
  - $p_1, r_1, r_2, r_3, ..., r_k, p_2$
- A küldő titkosítja az m üzenetet
  - $p_2, r_k, ... r_3, r_2, r_1$ nyilvános kulcsával ebben a sorrendben
  - és elküldi $f(pk_{r1},(r_2,f(pk_{r2}...f(pk_{rk},(p_2,f(pk_{p2},m)))...)))))$ az r_1 peernek
- r_1 dekódolja a kapott üzenetet, amiből megkapja a következő peer-t r_2-t és továbbküldi r_2-nek
- ...
- amikor p_2 meg kapja az üzenetet, dekódolja



Chaum „mix cascades” módszere

- Az úton egyik peer se tudja
  - hogy hanyadik állomás az úton
  - visszafejteni az eredeti üzenetet
  - ki a végső állomás
- A fogadó nem tudja
  - ki a küldő
- Ezen felül a peer-ek önkéntesen hozzáadhatnak a kerülőutakat a továbbítandó üzenethez
- Chaum Mix Cascades módszere
  - vagy Mix Networks
  - biztonságos mindenféle támadás ellen,
  - de forgalom elemzés ellen nem



TOR -- hagyma routerek

- David Goldschlag, Michael Reed, Paul Syverson, 1998
- Cél
  - Megőrizni a küldő és a fogadó privát szféráját
  - Az átvitt üzenet titkosságát
- Előfeltétel
  - Saját infrastruktúra (Onion Routers)
  - Amelyek kooperálnak
- Módszer
  - Mix Cascades (Chaum)
  - Az üzenetet a köldőtől a fogadóig proxy-kat (onion-routereket) használatáva küldjük
  - Onion-routerek nem előre megmondhatóan választanak routereket közbenső routereknek
  - A küldő, onion-routerek és a fogadó és a cél között az üzenetet szimmetrikus módszerrel titkosítják
  - Minden onion-router csak a következő állomást ismeri
  - Az üzenet „hagyma szerűen” van titkosítva
- TOR úgy értendő mint
  - az Internet Infrastruktúra javítása
  - nem P2P hálózat
  - de gyakran használják P2P hálózatok

További hagyma routereken alapuló munkák

- Crowds
  - Reiter & Rubin 1997
  - Anoním web-böngészés, amely onion-routereken alapul
- Hordes
  - Shields, Levine 2000
  - Alcsoportokat használ az onion-routing javításához
- Tarzan
  - Freedman, 2002
  - Egy P2P anonimizáló hálózat réteg
  - UDP üzeneteket használ és Chaum Mix-et csoportokban az Internet forgalom anonimizálásához
  - „fake” forgalmat is generál időzítés támadások ellen

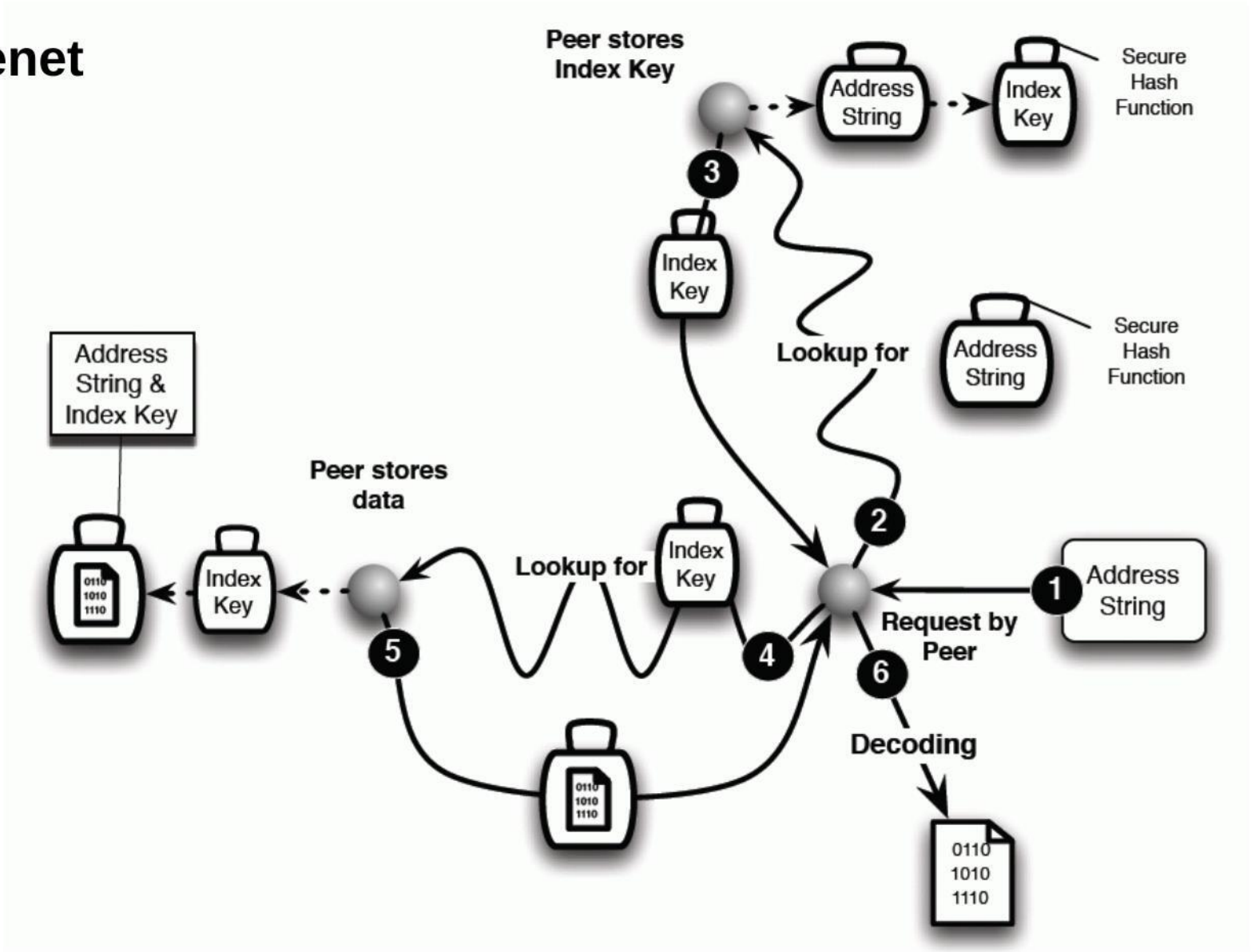
Freenet

- Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore Hong, 2000
- Cél
  - P2P hálózat
  - Lehetővé tesz publikálást, replikálást adat visszakeresést
  - Szerzők és olvasók anonimitása
- A file-ok
  - földrajzi helytől függetlenül kódolva vannak
    - titkosított és pszeudonímmel aláírt index file-ok
    - szerző nem azonosítható
  - Biztosítottak nem autorizált megváltoztatás vagy törlés ellen
  - Olyan kulccsak vannak kódolva, amelyet a tároló peer nem ismer
    - A titkos kulcs valahol máshl van tárolva
  - Replikáltak
    - A keresési útvonalon
    - Ha nem elég a tár, törlődnek “Least Recently Used” (LRU) szabály szerint

Freenet

- Hálózati struktúra
  - Gnutella-hoz hasonló
  - Freenet fokszámeloszlása Pareto (hasonlóan Gnutella-hoz)
- File-ok tárolása
  - Minden file megkereshető, visszakódolható és olvasható a kódolt cím-sztringet használva és az aláírt altér-kulcsot
  - Minden file együtt van tárolva az index kulcsával, de a kódolt cím-sztring nélkül
  - A tároló peer nem tudja ezt a file-t olvasni
    - Hacsak nem próbálja ki az összes lehetséges jelszót (szótár támadás)
- Index file-ok tárolása
  - A cím-string egy kryptografikus hash függvénnyel van kódolva, amely ahhoz a peer-hez vezet, amely tárolja
    - az indexet
    - a cím-sztringet
    - az aláírt altér kulcsot
  - Ezt az index file-t használva megtalálható az eredeti file

Freenet


Peer stores
Index Key
Address
String
Index
Key
Secure
Hash
Function
3
Index
Key
Lookup for
Address
String
Secure
Hash
Function
Address
String &
Index Key
Peer stores
data
2
Index
Key
Lookup for
Index
Key
Address
String
1
Request by
Peer
5
4
6
Decoding
0110
1010
1110
0110
1010
1110

Freenet

- Keresés
  - Legnagyobb lejtés - hegymászás
    - A keresés ahhoz a peer-hez továbbítódik, melynek az ID-je legközelebb van a kereső indexhez
  - TTL mező (azaz hop korlát)
- A file-ok új peer-ekre kerülnek áthelyezésre
  - Ha a kulcsszó hasonló a szomszéd ID-jához
- Új linkek
  - keletkeznek, ha egy keresés közben peer Id-k közötti hasonlóságot derítünk ki

Freenet hatékonysága

- Freenet struktúrája hasonló a Gnutellához
- A keresési idő átlagosan polinomiális

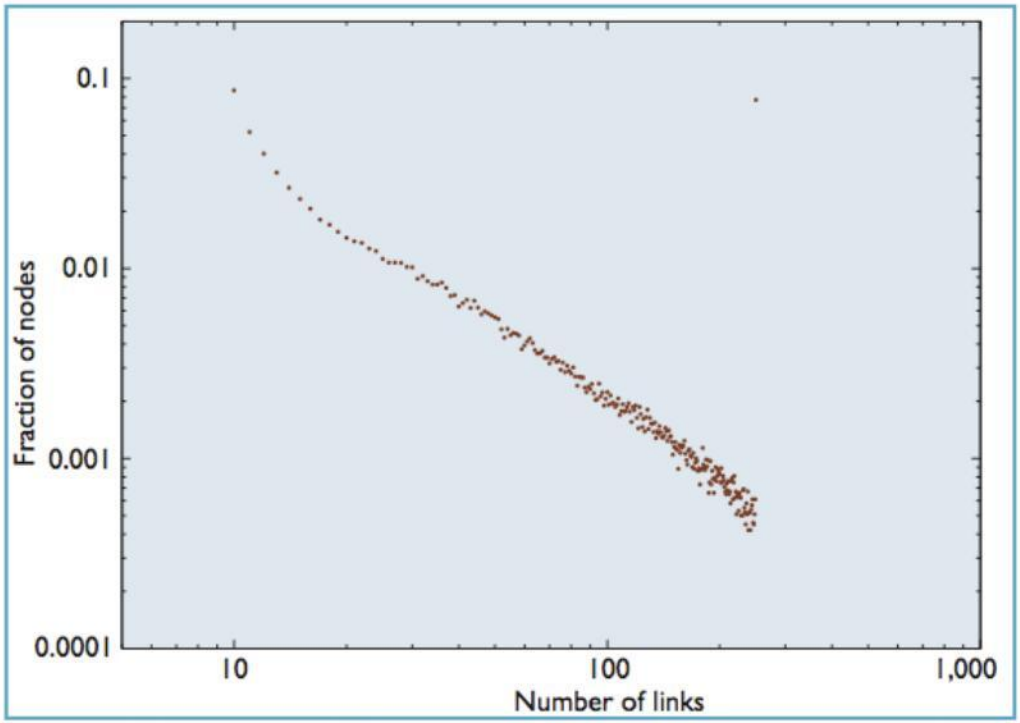


Figure 2. Degree distribution among Freenet nodes. The network shows a close fit to a power-law distribution.

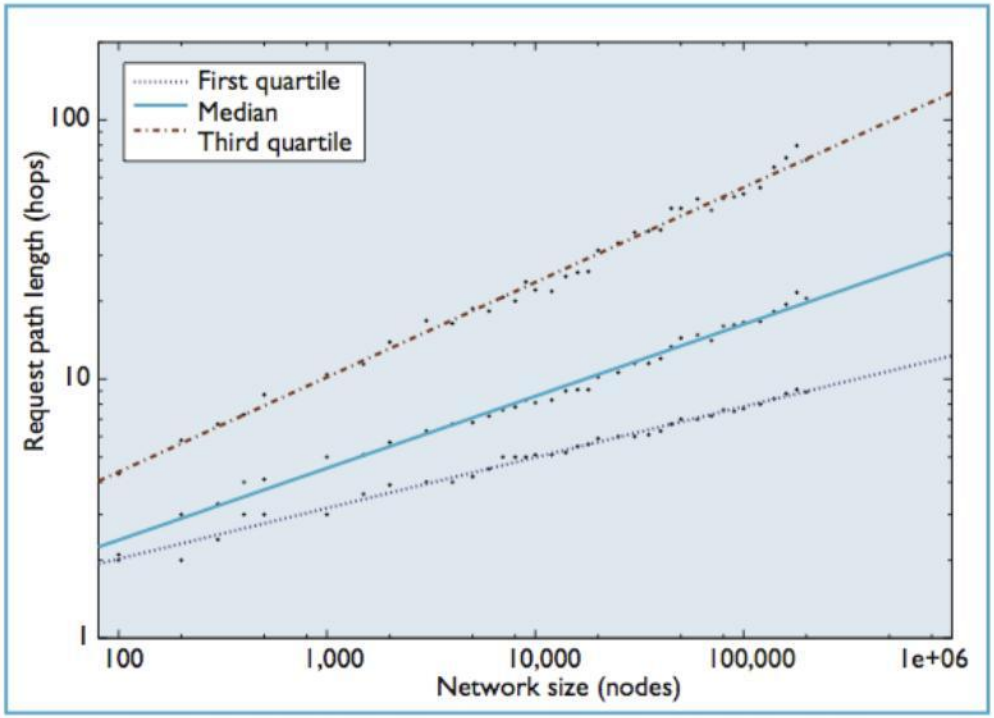


Figure 3. Request path length versus network size. The median path length in the network scales as $N^{0.28}$.

Dark Net & Friend-to-Friend

- Dark-Net egy privát Peer-to-Peer hálózat
  - A tagok megbízhatnak minden más tagban
  - pl.
    - barátok (a valódi világban)
    - sport klub
- Dark-Net a hozzáférés kontroll:
  - titkos címekkel,
  - titkos szoftverrel,
  - jelszó általi autentikálással, vagy
  - központi autentikálással
- Példa:
  - WASTE
    - P2P-Filemegosztás 50 tagig
    - Nullsoft (Gnutella) által
  - CSpace
    - Kademlia használatával