PRIME Research

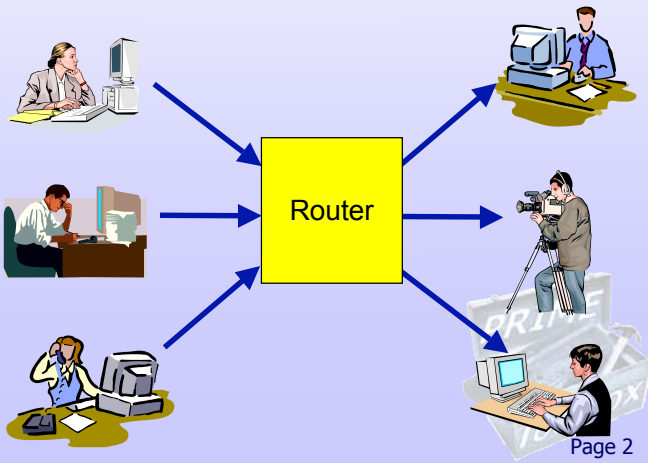
Low Latency Anonymous Communication

Karlstad, 25 September 2006

Carlos Aguilar Melchor, Yves Deswarte
LAAS-CNRS, Toulouse
deswarte@laas.fr

Anonymous Communciations

- **Traffic Analysis: an IP @ is a sensitive information**
  - **Identifying a user**
  - **Identifying the user's location**
  - **Server address = topics of interest**
- **Classical Solution: MIX = deciphering router**



Attacks and Countermeasures

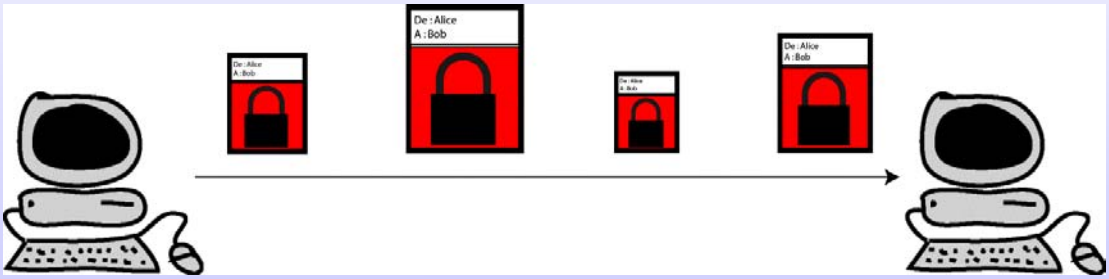
- Malicious MIX => multiple MIXes
- Correlations => many users -> large anonymity sets
  padding traffic
  prevent global observation (distribution)
  --> weak unobservability
- Cascades : ex. JAP in Dresden
  - User throughput: ~100 Kbits/s
  - User perceived latency : < 3 s
- MIX-nets: ex. TOR
  - User throughput: from 0 to 2 Mb/s (average ~500 Kb/s)
  - User perceived latency : very variable: 1 to 10 s

New applications: low latency

- Case study: VoIP
  - Throughput: 8 to 32 Kb/s (codecs G729-EV)
  - RTT: 250 ms max (recommendation ITU)
- New solutions ?
  - One "anonymous communication server" rather than passing through several MIXes
  - More efficient communications (e.g., LAN)
  - Risk of "global observer" => strong unobservability
  - Possibly small anonymity groups

Primitives (1): Ciphered Padding

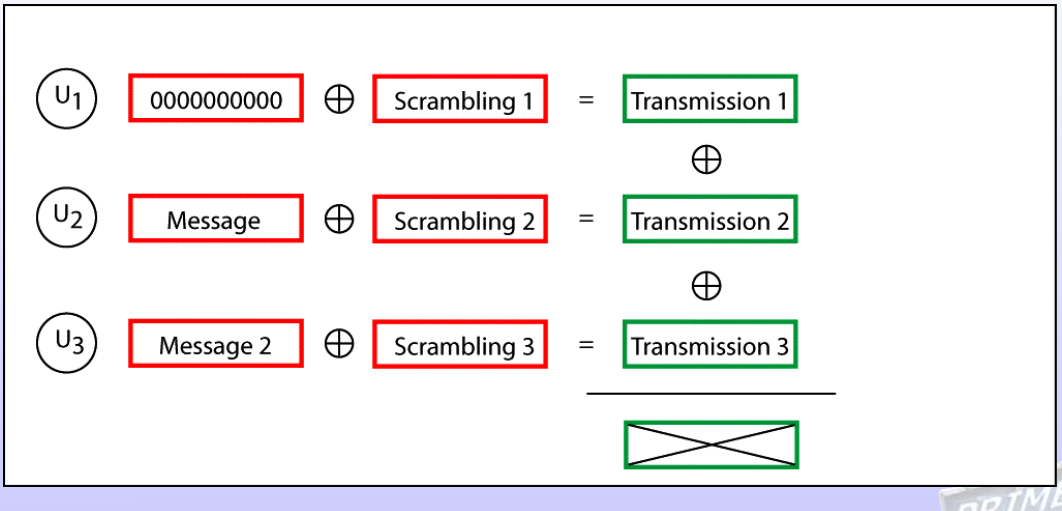
- **Constant transmission**
  - **Fixed size messages**
  - **Either real enciphered messages or padding**



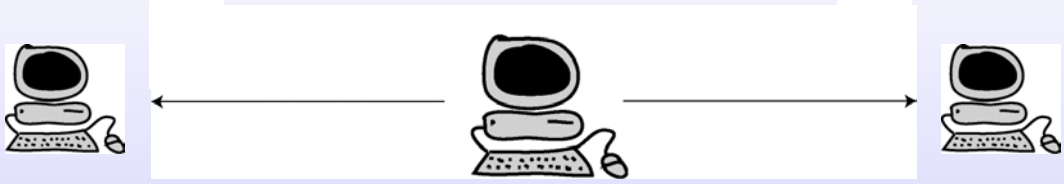
Primitives (1): Ciphered Padding

- **Constant transmission**
  - **Fixed size**
  - **Either real enciphered messages or padding**

Primitives (2): Superposed Sending

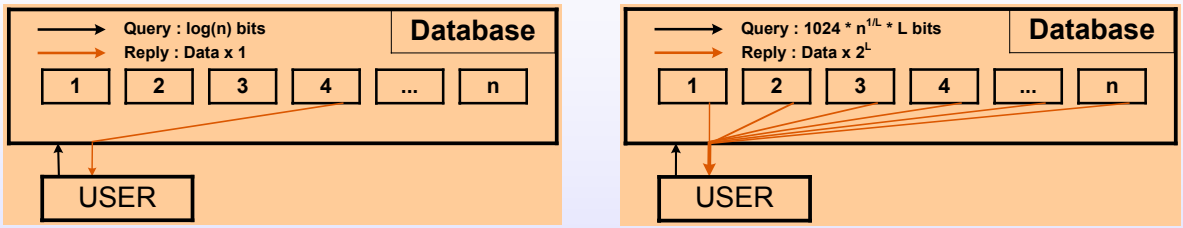


Primitives (3): Broadcast with implicit addressing



- **Broadcast the whole network**
- **Include a mark for the destination to recognize which messages it should receive**

Primitives (4): PIR Protocols



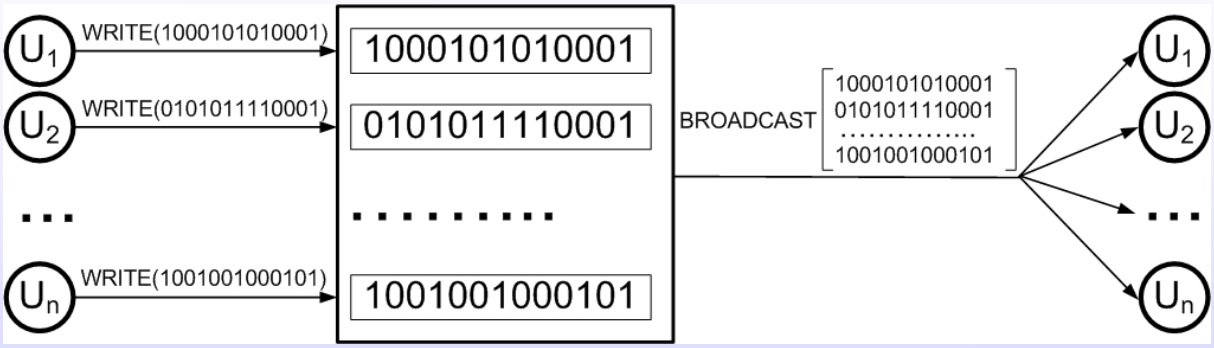
- Enable to retrieve one object
  - Without indicating which object
  - With a small expansion factor (< 2)
- Replace broadcast with implicit addressing
  - Unobservable reception
  - Reduce strongly communication costs
  - Increase strongly computation cost

Low Latency Anonymous Communications

- Possible combinations

	Broadcast with implicit @	PIR
Ciphered padding	EBBS	pMIX
Superposed sending	DC-net server	pDC-net

EBBS: enciphering bulletin-board system

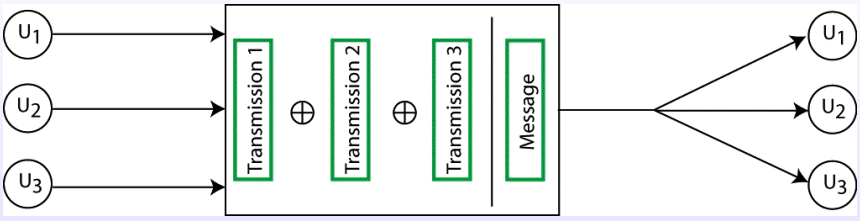


- Each user is assigned a slot
- Ciphered padding, rounds
- Expansion factor in reception = n

EBBS and VoIP

- Useful throughput/user : 10 Kb/s
- Comsumed bandwidth:
  - Less than 10% of each user's available bandwidth
  - In any case, less than 1 Mb/s
- LAN => 100 users max
- Internet
  - ADSL (R: 1 Mb/s, T: 128 Kb/s) => 10 users
  - UMTS (R: 384 Kb/s, T: 64 Kb/s) => 3 to 4 users

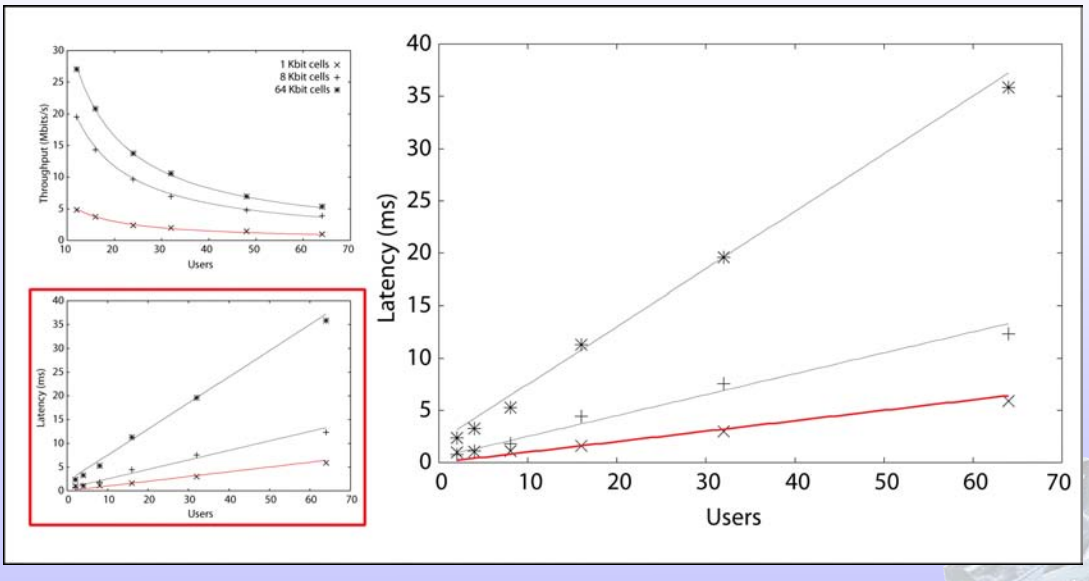
DC-net Server



- **Co-operation of independent, asynchronous agents**
  - **Theoretical performance evaluation: very difficult**
  - **Experiments were necessary**
    - **Cluster: optimal performance**
    - **Operational network (LAAS): realistic performance**

DC-net Server experiment

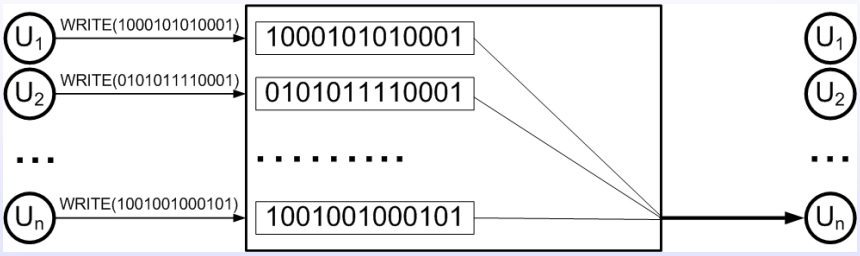
- **On LAAS network:**



DC-net Server and VoIP

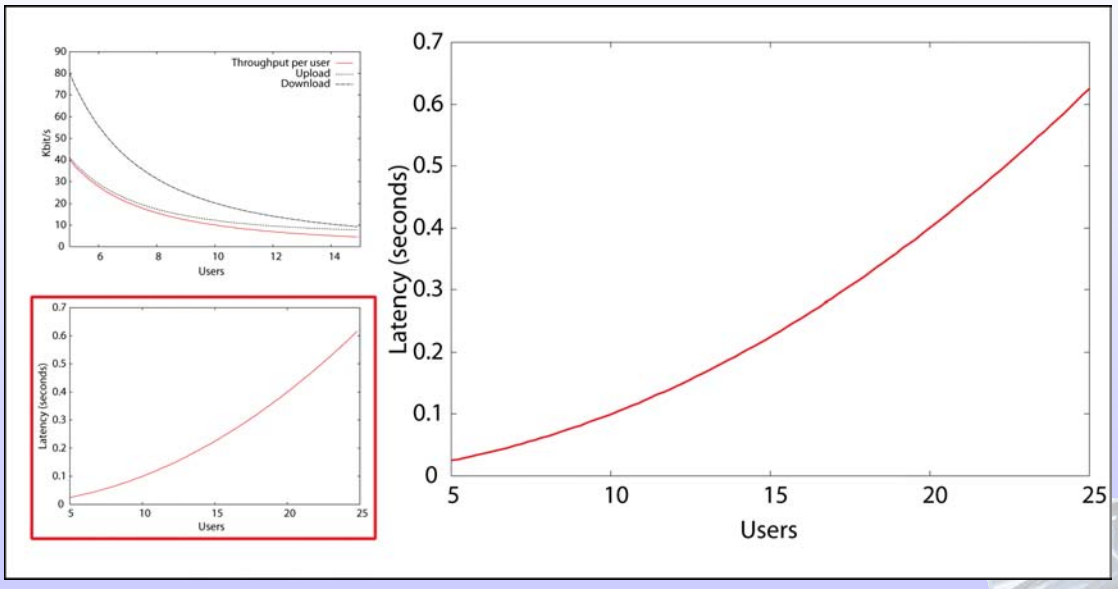
- **LAN: several 100s of users**
- **Internet**
  - **Latency: very inefficient (rounds)**
  - **Transmission bandwidth (xDSL, UMTS, EDGE, …)**

pMIX



- **A slot per user (transmission)**
- **1 PIR reply per destination (n)**
- **Each PIR computation cost: % DB size = % n (+ ~1 modular multiplication/bit)**
- **=> Computation cost % n^2**

pMIX performance

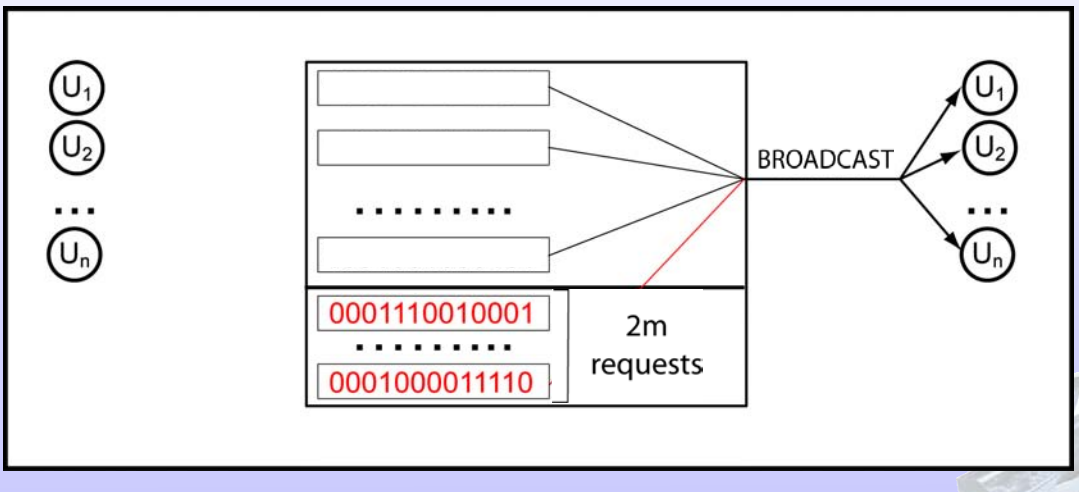


pMIX results

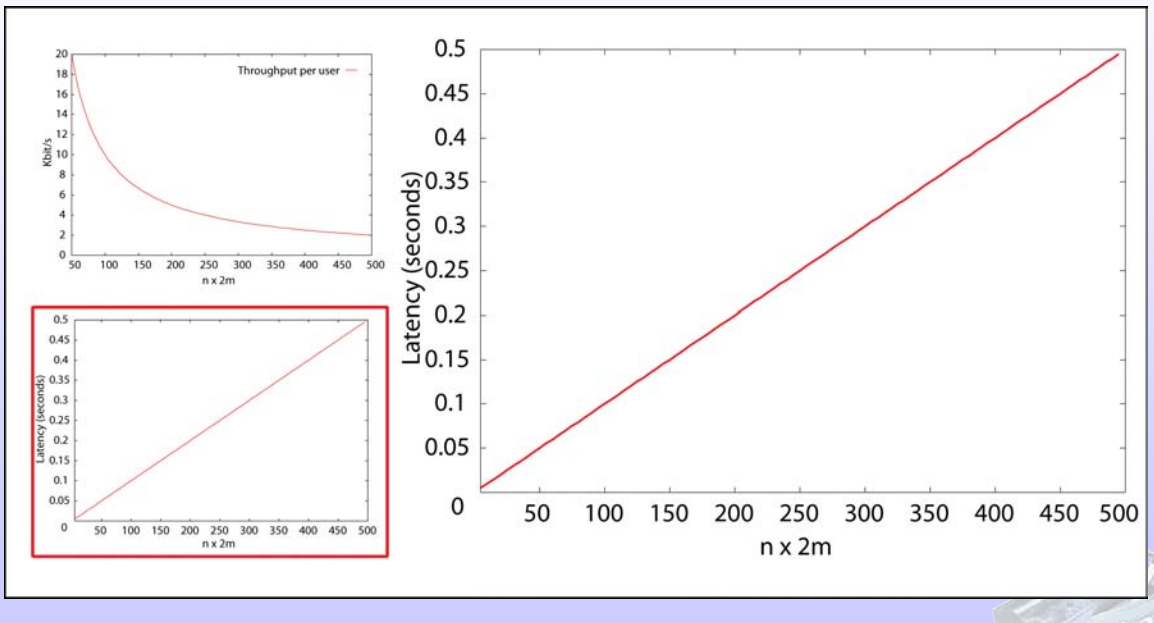
- **Low bandwidth per user, but % computation power**
- **Computation cost very excessive if > 10s users**
- **Much more efficient PIR protocols ?**
  Domingo-Ferrer:
  - **Reasonable up to 250 users**

Variant of pMIX: apMIX

- **1 PIR reply per active communication**
  - **PIR requests sent by superposed sending**



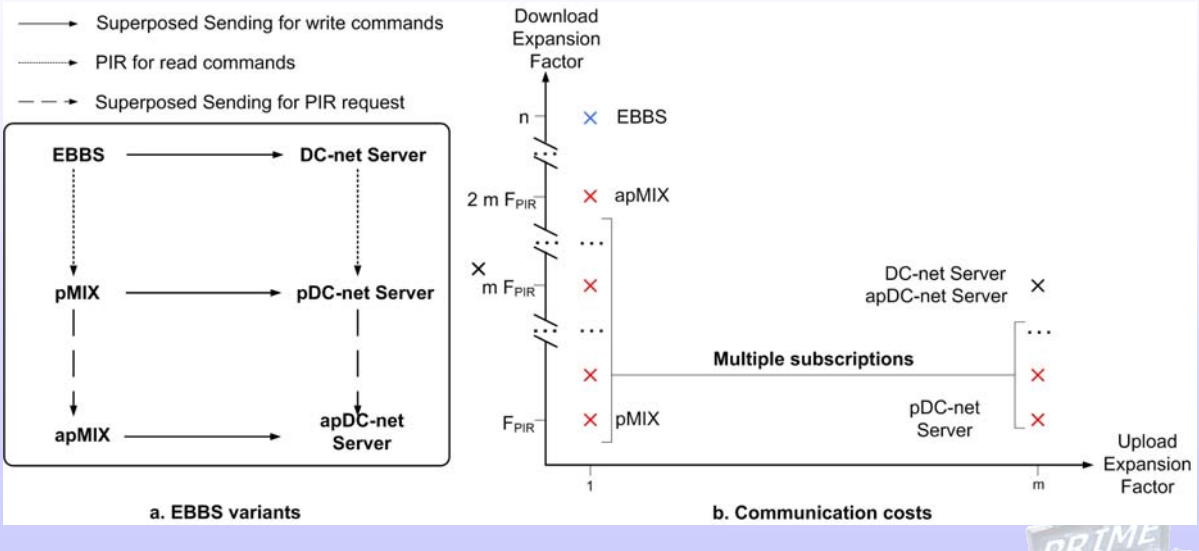
apMIX performance



apMIX and VoIP

- **Each CPU can manage (m.n ~50):**
  - **~ 50 users**
  - **1 active communication**
  - **8 cpus -> 100 users, 4 simultaneous communications**
- **Transmission expansion factor: ~1**
- **Reception expansion factor: 2m*F (m = # active coms)**
  - **LAN : m ≤ 50**
  - **ADSL : m ≤ 5**
  - **UMTS : m ≤ 2**

Other variants



Summary: VoIP

- **LAN**

	DC-net server	EBBS	apMIX
n =# users	100s	100	50/cpu
m =# act. coms	2000/n	n/2	1/cpu
Exp. Factor (t|r)	m|m	1|n	1|2m*F

- **Internet (ADSL)**

	EBBS	pMIX	apMIX
n =# users	10	10	50/cpu
m =# act. coms	n/2	n/2	1/cpu
Exp.F.client (t|r)	1|n	1|F	1|2m*F
Exp.F.serv (r|t)	n|n^2	n|F*n	n|2m*n*F