Privacy and Accountability in Networks via Optimized Randomized Mix-nets

Panos Louridas
Greek Research and Technology Network S.A.

Athens, January 31, 2018 – H2020 Clustering Workshop
By Any Other Name...

- Panoramix is the original French name for the druid character in the Asterix stories.
- English translations use Getafix.
- The project is named after the character and his whisk.
Watch our Video!

https://panoramix-project.eu/videos/
What is a Mix-Net?
Mix-net Types

- Re-encryption mix-nets (e-voting)
Mix-net Types

• Decryption mix-nets (networks, messaging, best known example: Tor)
Panoramix Objectives

• Build a mix-net infrastructure for Europe
• make it available
  – build a community around it
• ... and show how it can be used for :
  – (i) e-voting
  – (ii) privacy preserving statistics in the cloud
  – (iii) messaging
Panoramix Partners
E-Voting

• Apply Panoramix to the Zeus e-Voting platform (https://zeus.grnet.gr).
• Use new mix-nets to be able to handle elections with millions of votes.
• Use different mix-nets with different trade-offs.
• Mix-net technology: re-encryption.
• Partner: GRNET.
e-Voting Workflow

Voter → Encrypted Ballot → Ballot Box

Ballot Box → Mixing

Encrypted & Anonymised Ballots → Election Committee

Election Committee → Decrypted Ballots
Privacy-Preserving Statistics

• Allow the collection of data from multiple data sources anonymously.
• Process the data in a privacy-preserving way using differential privacy.
• Mix-net technology: decryption.
• Partner: SAP.
Privacy-Preserving Statistics

Data Sources (IoT) → Collection → Capitalization
Privacy-Preserving Statistics

1. Client(s)
2. Panoramix
3. Server

- Anonymization
  - RSA Encryption
  - Sphinxmix backend

- Mix

- Decryption Analysis
Messaging

- Allow anonymous e-mail communication.
- Mix-net technology: decryption.
- Target: K9Mail (Android), Thunderbird.
- Partner: CCT (Center for the Cultivation of Technology).
Messaging