Acid Mixes

Alessandro Acquisti
UC Berkeley
acquisti@sims.berkeley.edu
What is that?

• A variation on mix-net protocols that (attempts to) address reliability and trust issues while maintaining anonymity and preserving ACID properties.

• The variation is, itself, a “mix”:
  • Chaum (1981): mix-nets.
  • Stajano and Anderson (1999): cocaine auction protocol.

• Applications: flexible, but more efficient in targeted communications. For example:
  • Voting systems.
  • Payments.
Vanilla mix-net
Issues discussed in the literature

• Trust.

• Reliability.

• Often, trade-offs between the two.
Vanilla acid mix
More precisely...

- Let users interact...
- ...through untrusted third party (mix)...
- …splitting information...
- …and broadcasting it.
Analysis

• Compare to Chaum (1981) voting mix-net protocol:
  • Candidate sends identification+key (pseudonym) through mix-net, then votes.

• Here:
  • Identification sent separately from key.
  • Mixed through other users.

• How?
  • Stajano and Anderson (1999). Message 3. can be broadcasted anonymously – does not contain identifying information (or, see Pfitzmann and Waidner [1986]).
Strengths, weaknesses, and attacks

• Strengths
  – Untrusted third party.
  – Untrusted senders.
  – Flexible.

• Weaknesses
  – Efficiency (depending on application).

• Attacks
  – Intersection attack.
  – Adversary observes in/out communication and owns some senders: OK.
  – Adversary sees in/out communication and owns all senders ("n-1 attack"): Not OK.
Applications

• (Messaging)
• Payments
  • Sender/buyer unlinkability.
• Voting
  • Receipt free.
  • Universally verifiable.
  • Open-ended ballot question.
  • (caveats.)
For the record

1. \( C_{\perp} \to F : E_{C_{\perp}PB} \{ C_{\text{transaction massage}} , C_{\text{amount}} , C_{\perp PB} , C_{\perp PBT} , C_{\perp} \} \)

2. \( F \to C_{\perp} : E_{C_{\perp}PB} \{ C_{\text{transaction massage}} , T^{C_{\perp}}_{C_{\perp}} \} \)

3. \( C_{\perp} \to \ast : E_{C_{\perp}PR} \{ C_{\perp PB} , n_{C_{\perp}} \} \)

4. \([1, 2, ..., X]_{[1, 2, ..., X]_{(t+1)}} \to C_{\perp} :\)
\[ E_{C_{\perp}PB} \{ E_{[1, 2, ..., X]_{(t+1)}PR} \{ [1, 2, ..., X]_{(t+1)} PB, E_{C_{\perp}PR} \{ C_{\perp PB} , n_{C_{\perp}} \} \} \} \]

5. \( C_{\perp} \to F, [1, 2, ..., X]_{[1, 2, ..., X]_{(t+1)}} :\)
\[ E_{C_{\perp}PR} \{ n_{C_{\perp}} , [C, 1, 2, ..., X]_{(t+1)} PB, [C, 1, 2, ..., X]_{(t+1)} PBT \} \]

6. \([C, 1, 2, ..., X]_{[C, 1, 2, ..., X]_{(t+1)}} \to F, [C, 1, 2, ..., X]_{[C, 1, 2, ..., X]_{(t+1)}} :\)
\[ E_{[C, 1, 2, ..., X]_{(t+1)PR}} \{ S, E_{F_{PB}} \{ T^{C, 1, 2, ..., X}_{C_{\perp}} U^{C, 1, 2, ..., X}_{C_{\perp}} PRT \} \} \]

7. \( F \to \ast : E_{F_{PR}} \{ E_{C_{\perp}(t+1)PB} \{ T^{C_{\perp}(t+1)}_{1, ..., n_{C_{\perp}}} \} , E_{1(t+1)PB} \{ T^{1,t+1}_{1, ..., n_{C_{\perp}}} \} , ..., E_{X(t+1)PB} \{ T^{X_{(t+1)}}_{1, ..., n_{C_{\perp}}} \} \} \)
acquisti@sims.berkeley.edu