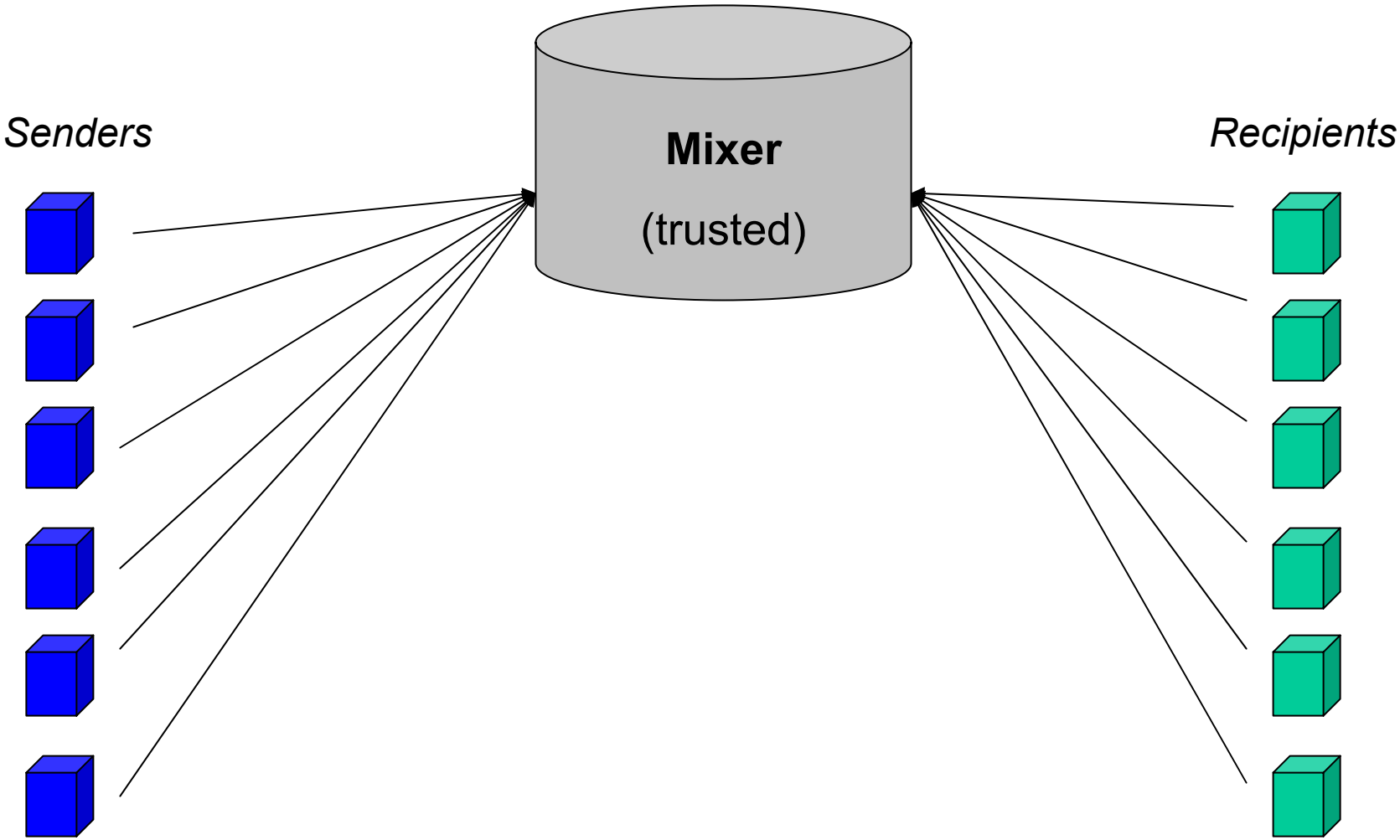
Acid Mixes

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.
  - Chaum (1991): group signatures.
  - Stajano and Anderson (1999): cocaine auction protocol.
- Applications: flexible, but more efficient in targeted communications. For example:
  - Voting systems.
  - Payments.

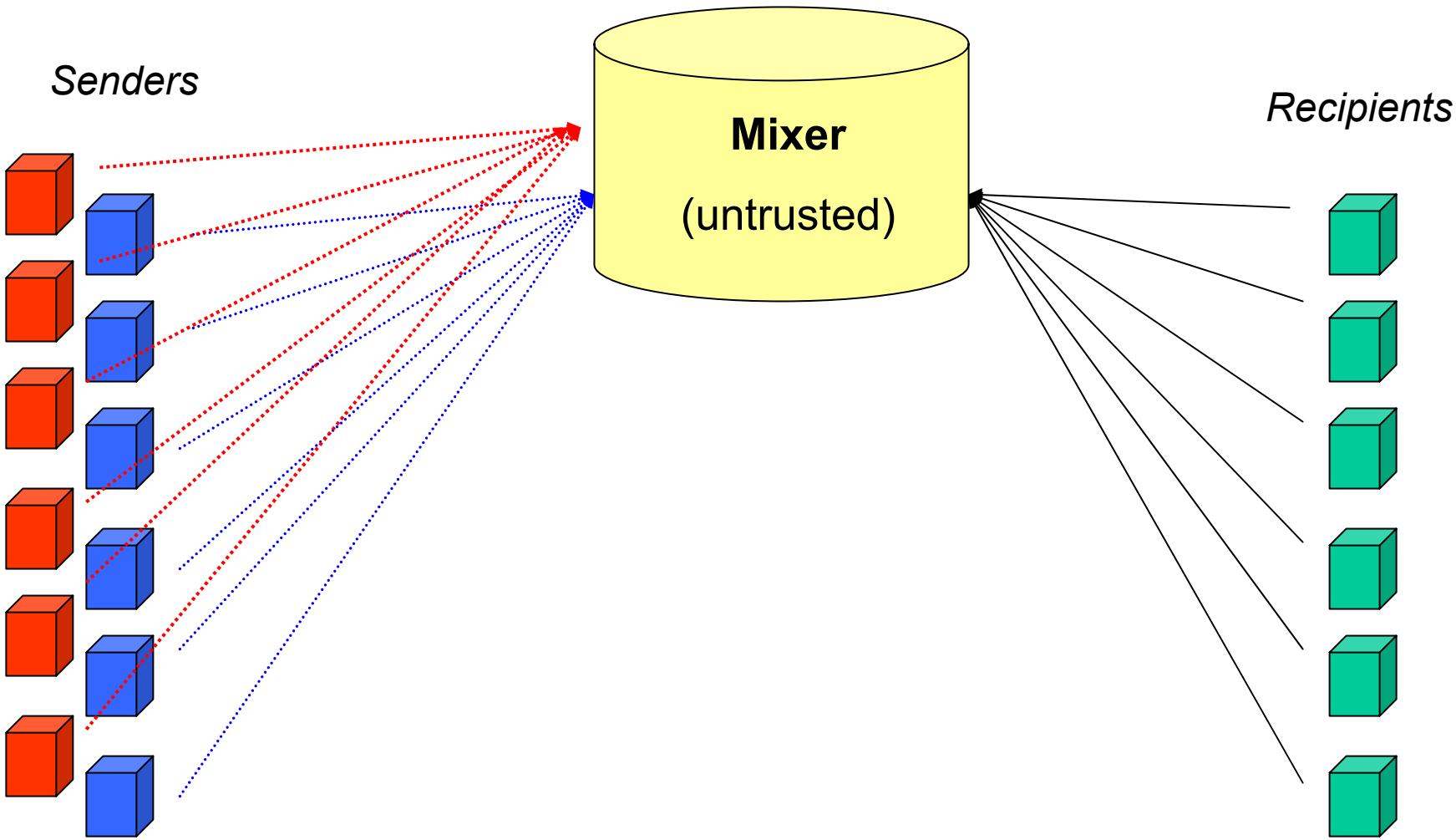
Vanilla mix-net



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 unlinkabilty.
- Voting
  - Receipt free.
  - Universally verifiable.
  - Open-ended ballot question.
  - (caveats.)

For the record

1. $C_{C\_t} \rightarrow F : E_{C\_tPR}\{E_{F\_PB}\{C\_transaction\_id, C\_amount, C\_tPB, C\_tPBT, C\_t\}\}$
2. $F \rightarrow C_{C\_t} : E_{C\_tPB}\{C\_transaction\_id, T^{C\_t}_{1,...,n}\}$
3. $C_{C\_t} \rightarrow * : E_{C\_tPR}\{C\_tPB, n_{C\_t}\}$
4. $[1,2,...,X]_{[1,2,...,X]\_(t+1)} \rightarrow C_{C\_t}$:
   $E_{C\_tPB}\{E_{[1,2,...,X]\_(t+1)PR}\{[1,2,...,X]\_(t+1)\,PB, E_{C\_tPR}\{C\_tPB, n_{C\_t},\}\}\}$
5. $C_{C\_t} \rightarrow F, [1,2,...,X]_{[1,2,...,X]\_(t+1)}$:
   $E_{C\_tPR}\{n_{C\_t}, [C,1,2,...,X]\_(t+1)\,PB, [C,1,2,...,X]\_(t+1)\,PBT\}$
6. $[C,1,2,...,X]_{[C,1,2,...,X]\_t} \rightarrow F, [C,1,2,...,X]_{[C,1,2,...,X]\_(t+1)}$:
   $E_{[C,1,2,...,X]\_tPR}\left\{S, E_{F\_PB}\left\{T^{[C,1,2,...,X]\_t}_{1,...,n_{C\_t}}, [C,1,2,...,X]\_tPRT\right\}\right\}$
7. $F \rightarrow * : E_{F\_PR}\{E_{C\_(t+1)PB}\left\{T^{C\_(t+1)}_{1,...,n_{C\_t}}\right\}, E_{1\_(t+1)PB}\left\{T^{1\_(t+1)}_{1,...,n_{C\_t}}\right\}, ..., E_{X\_(t+1)PB}\left\{T^{X\_(t+1)}_{1,...,n_{C\_t}}\right\}\}$

acquisti@sims.berkeley.edu