A Location-Privacy Platform for Smartphone Apps

Saikat Guha, Mudit Jain, Venkat Padmanabhan
(Microsoft Research India)

Location-Privacy Problem

- “[TaintDroid OSDI’10] studied **30 popular Android** applications that use location, camera, microphone data. [They] found that **15 send users' location information to remote advertisement or analytics servers**.”

+37.4179, -121.9094

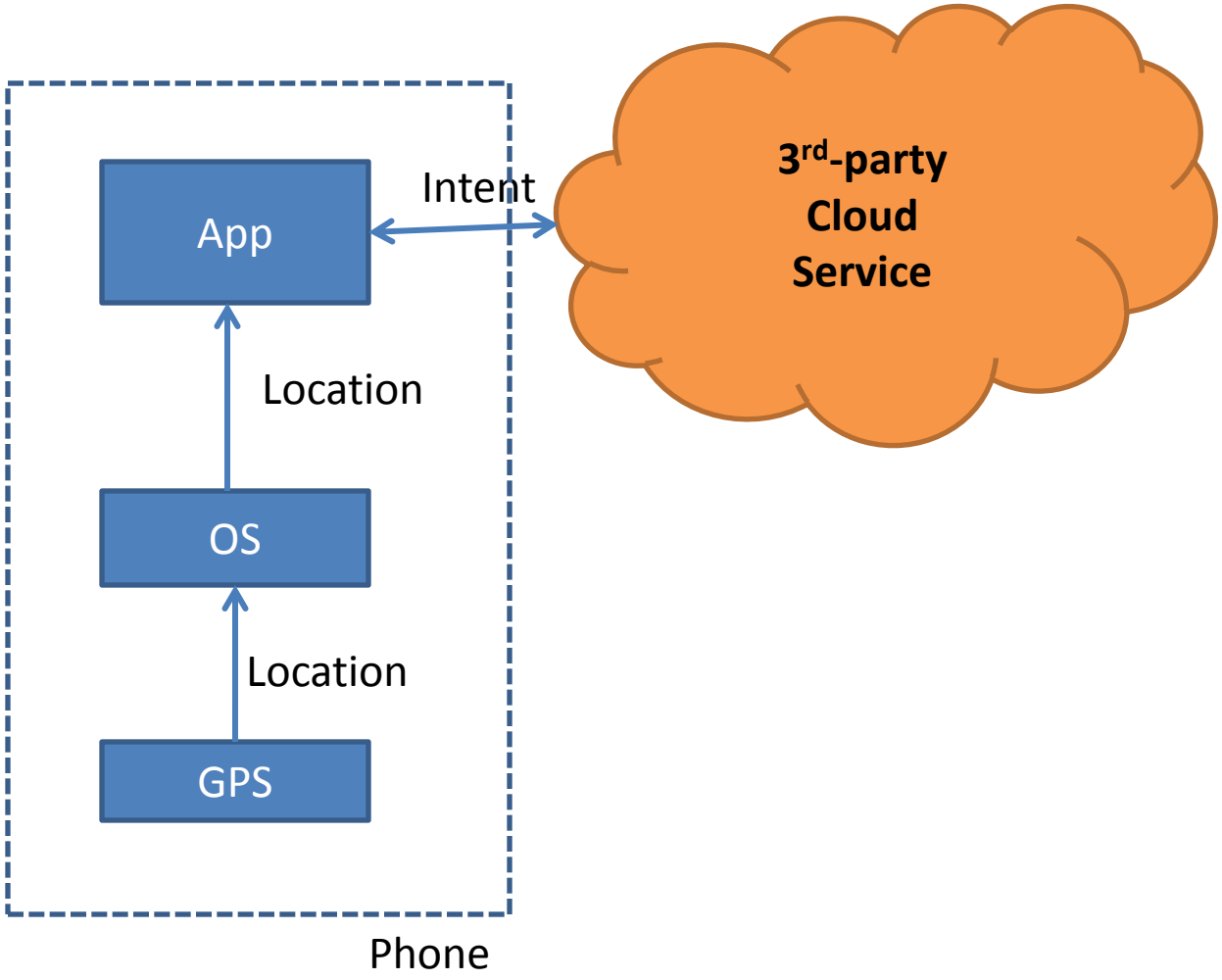
Location-Privacy Problem

- “[TaintDroid OSDI’10] studied **30 popular Android** applications that use location, camera, microphone data. [They] found that **15 send users' location information to remote advertisement or analytics servers**.”

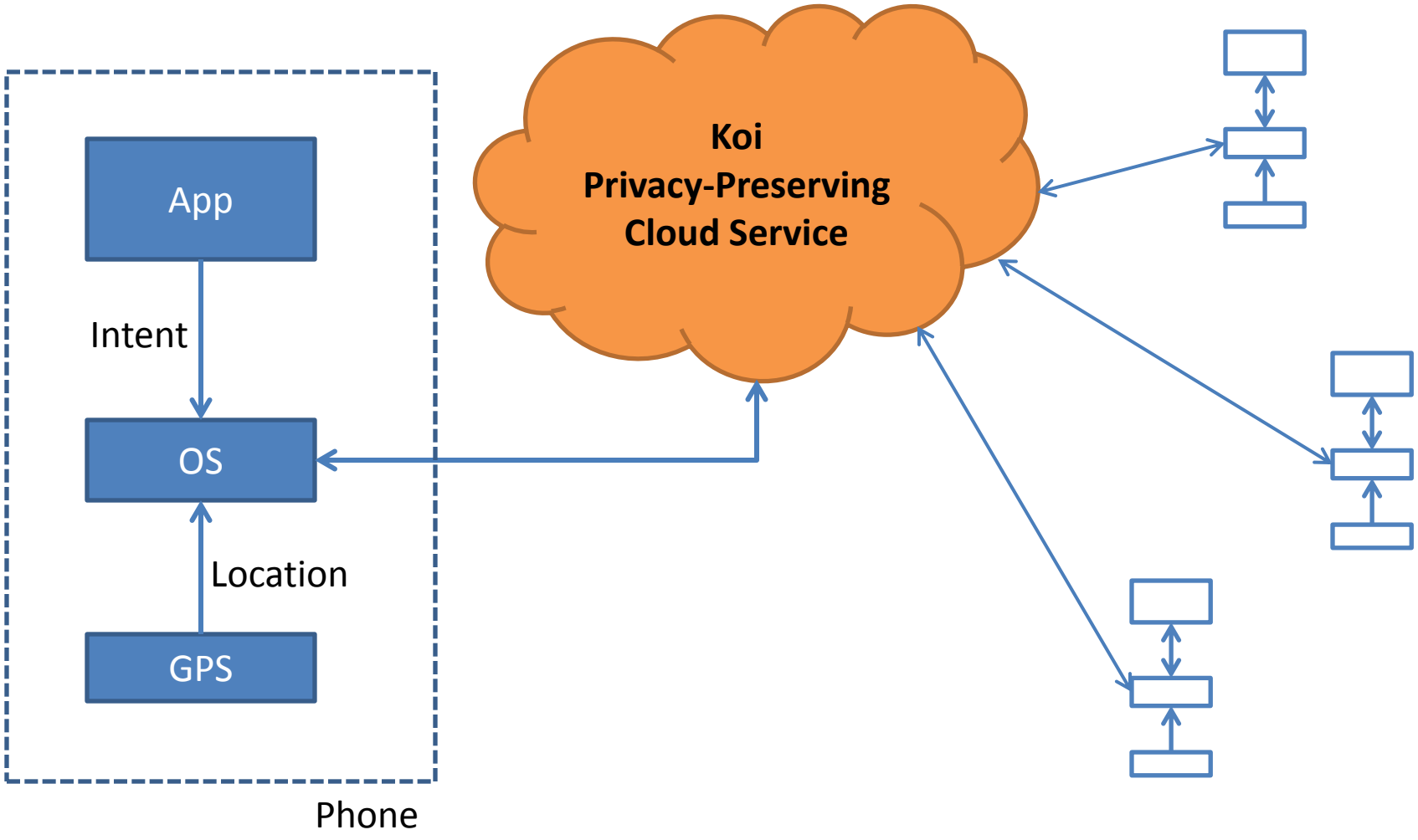
Privacy-Problem on Mobiles

- App developers are given raw low-level data
  - Need 3rd-party libraries to synthesize useful representations
  - 3rd party libraries need to contact cloud
- Once app gets lat-long, OS cannot control what app does with it.

Today: Big Picture



Koi: Big Picture



Koi: Raise Level of Abstraction

- For the app developer:
  - Triggers and callback based API
  - Rich specification of triggers, e.g.,
    - “Within 5 blocks from Bob’s current location”
    - “At any grocery store”
- Platform support:
  - Privacy-preserving cloud service to support this abstraction.

Defining Privacy

- K-anonymity, L-diversity, Differential Privacy
  - Applicable to learning
  - Not applicable to fine-grained personalization

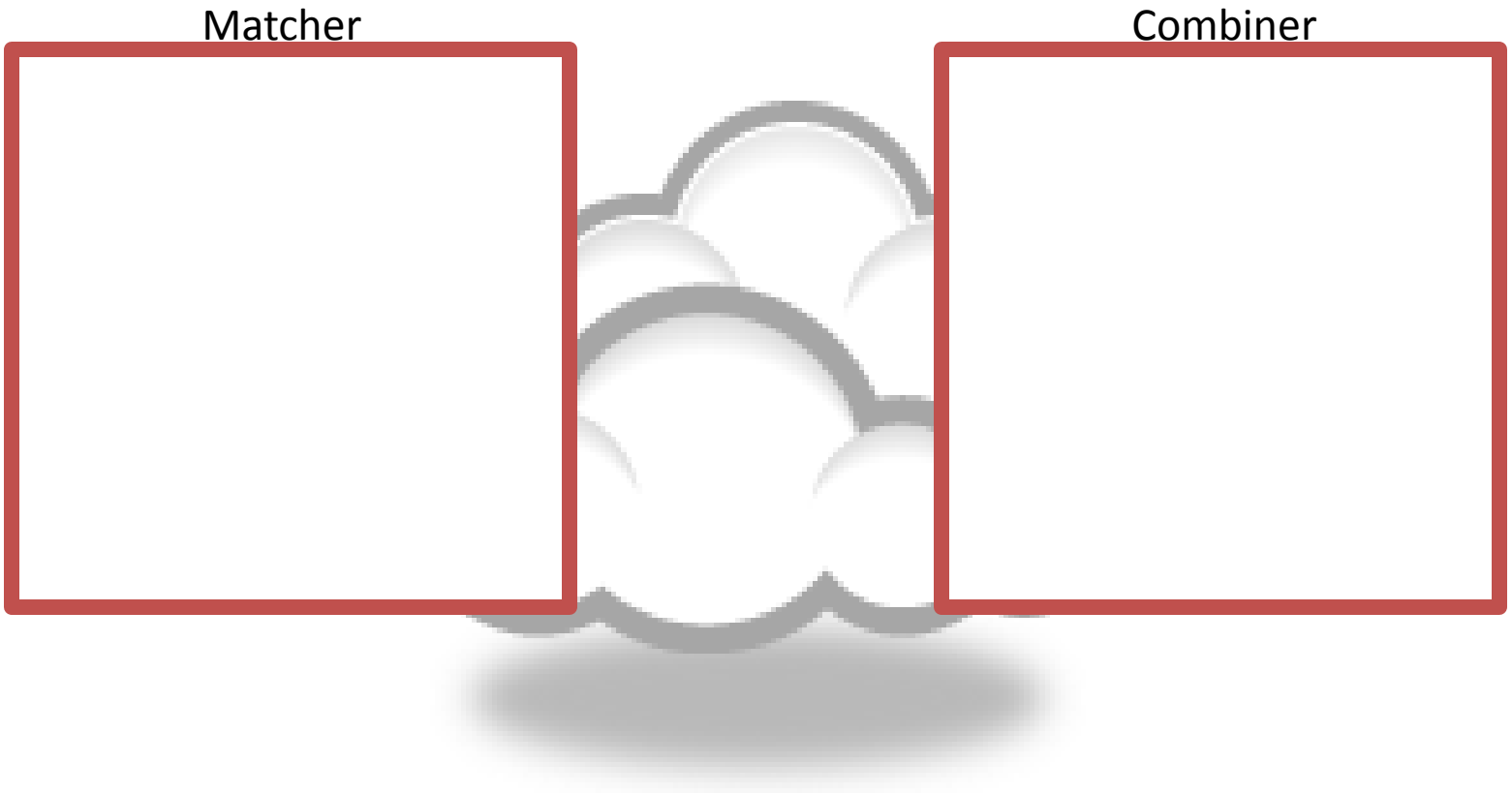
- Unlinkability
  - "Saikat is looking for Bail-bonds" (private)
  - "Someone is looking for Bail-bonds" (*not-private*)
  - "Saikat is looking for something" (*not-private*)

Location-Based Advertising

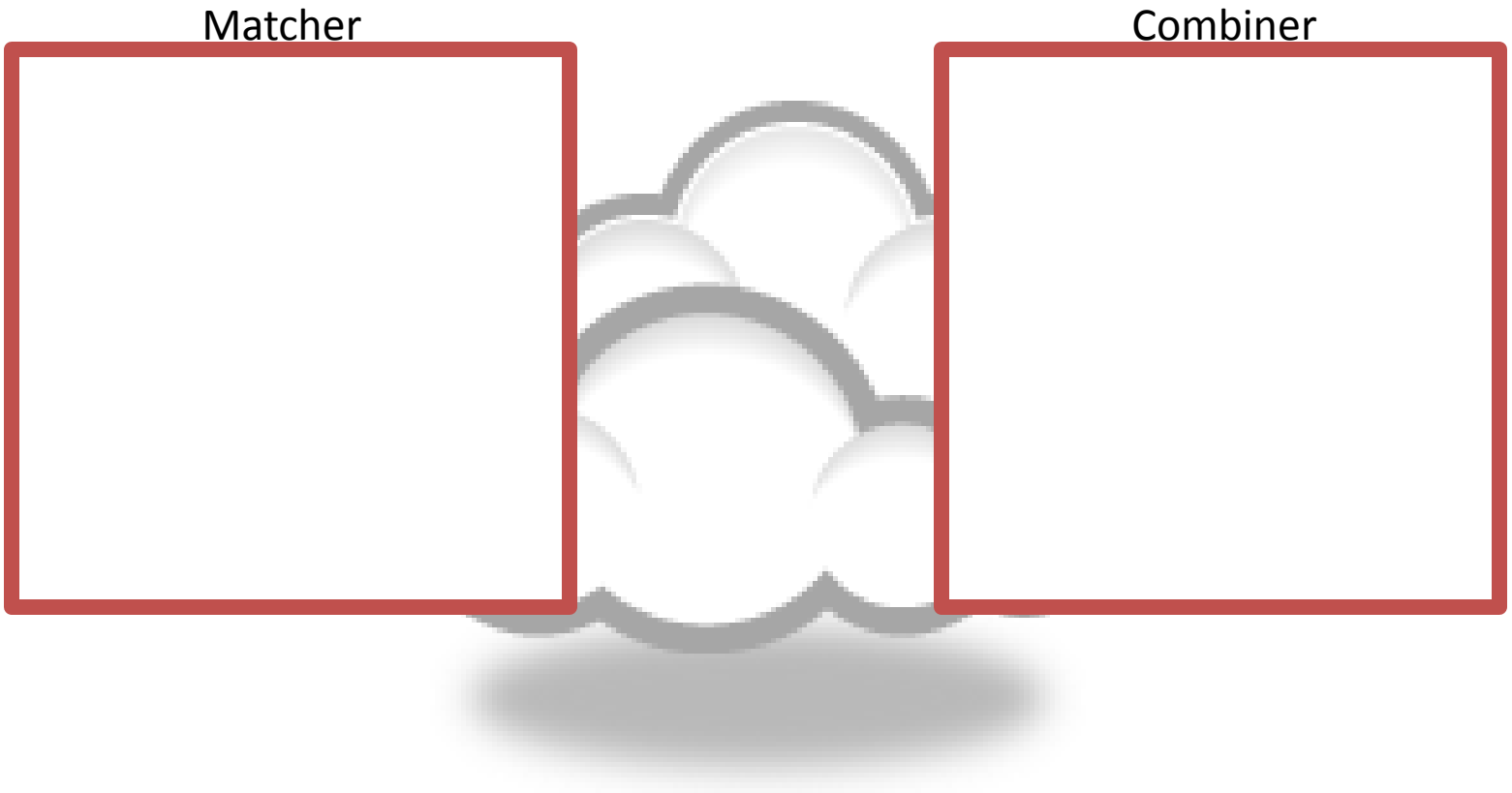

```
I = CreateItem("ZigZag")
I.AddAttr("Bail-Bond")
I.AddLocAttr("N 2nd St., San Jose, CA")
```


```
T = CreateTrigger(callback)
T.AddAttr("Bail-Bond")
T.AddLocAttr("cur loc + 5blk", True)
```

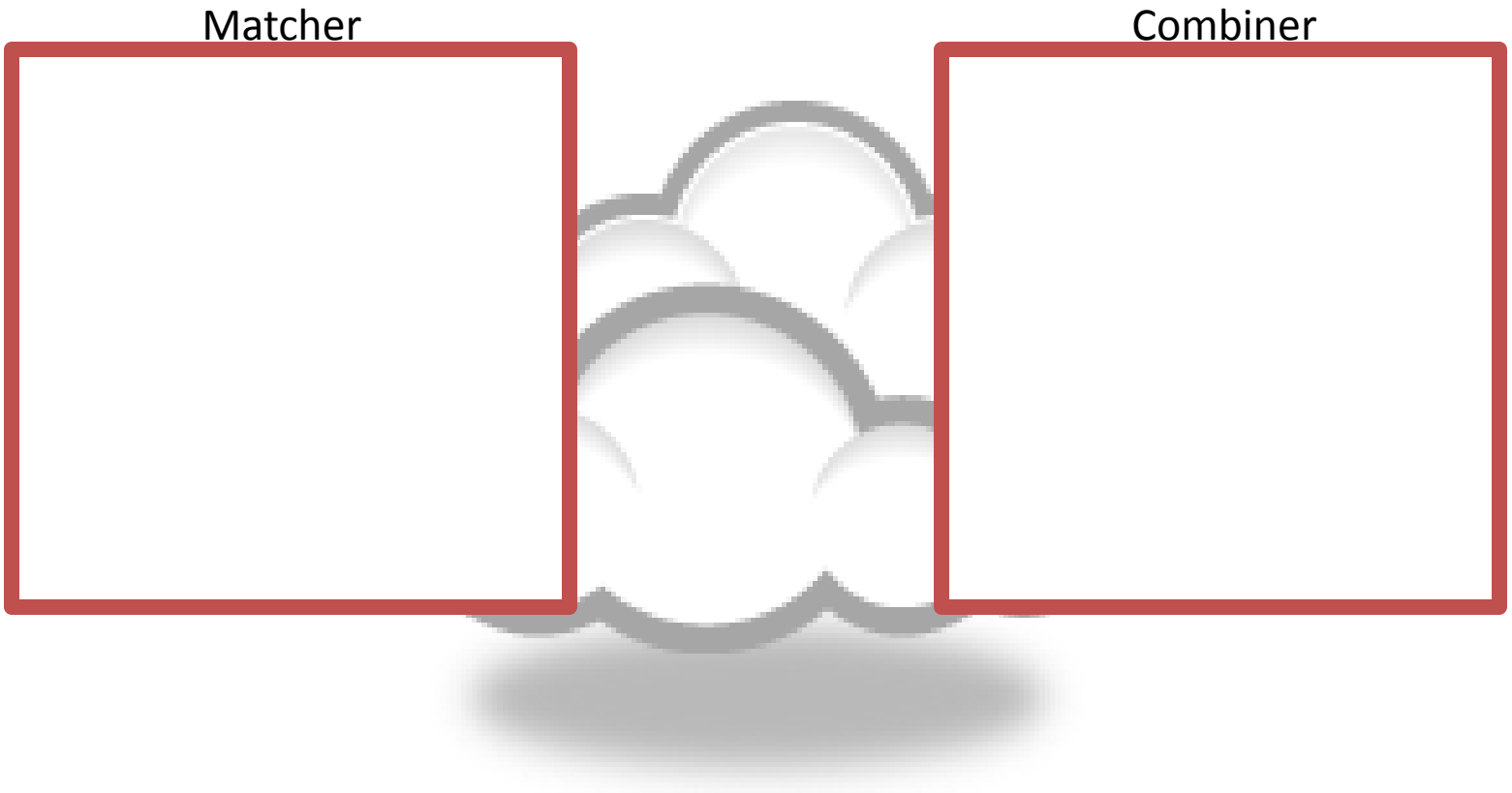
Koi: Privacy-Preserving Matching



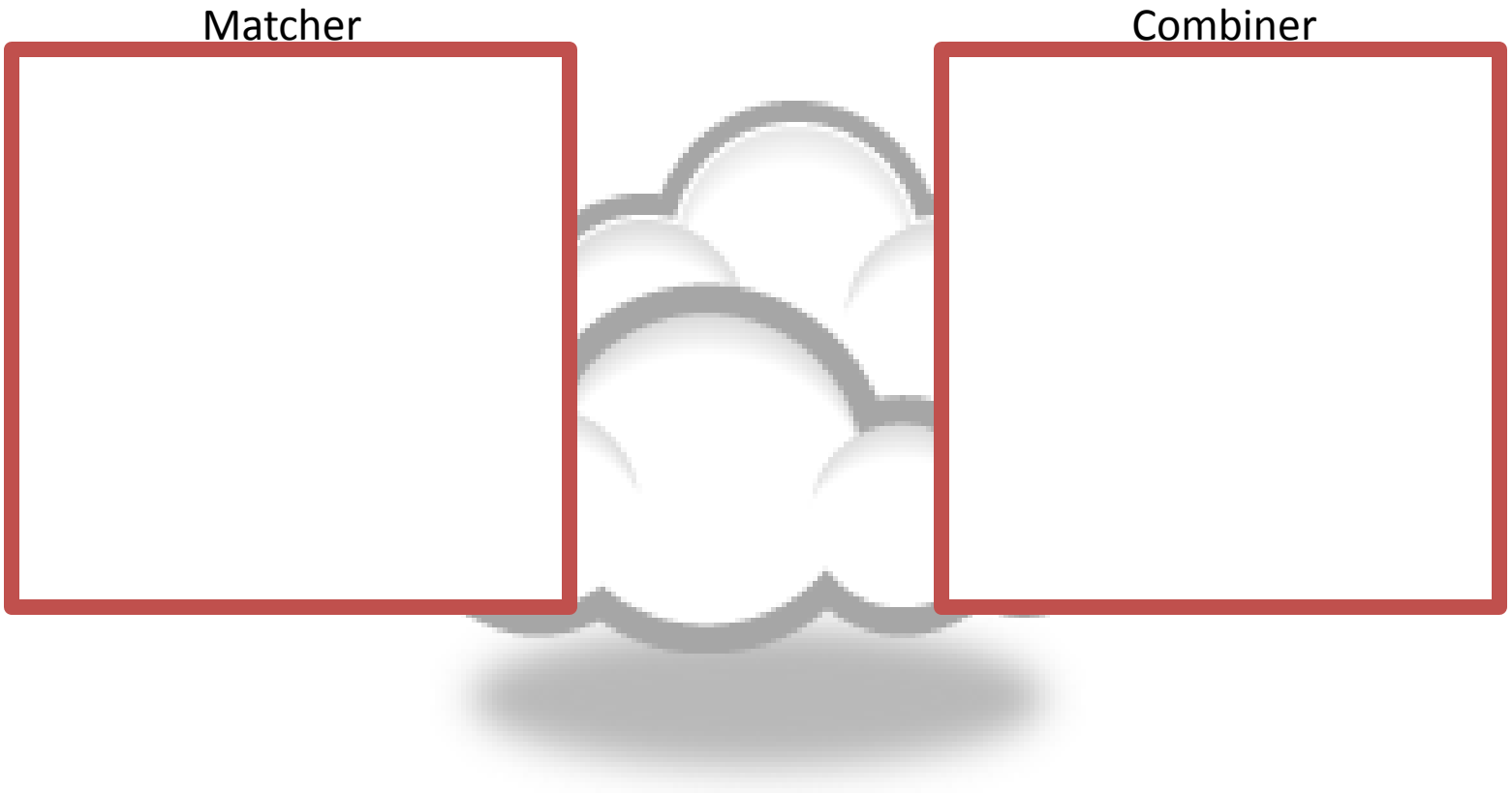
Koi: Privacy-Preserving Matching



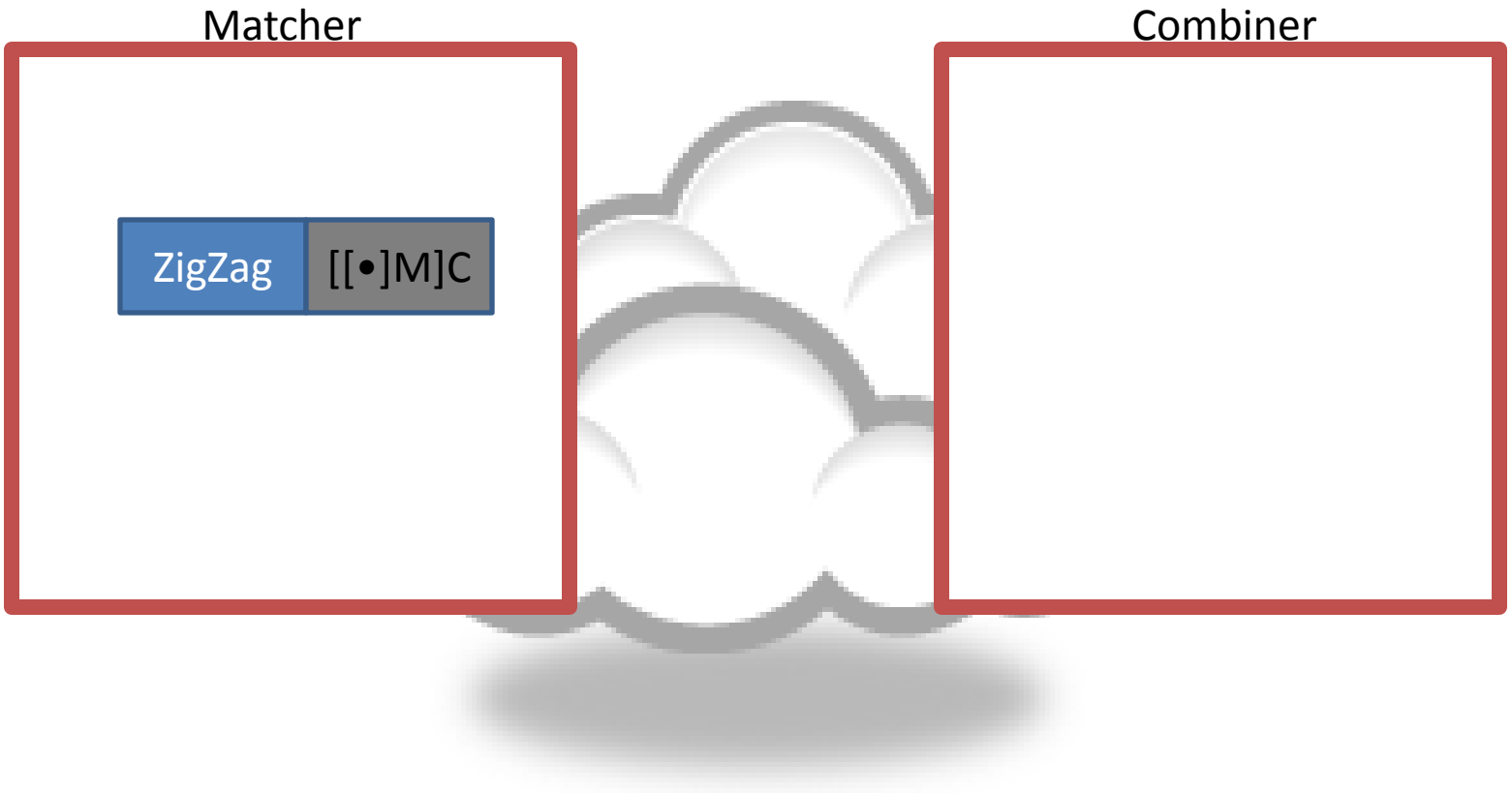
Koi: Privacy-Preserving Matching



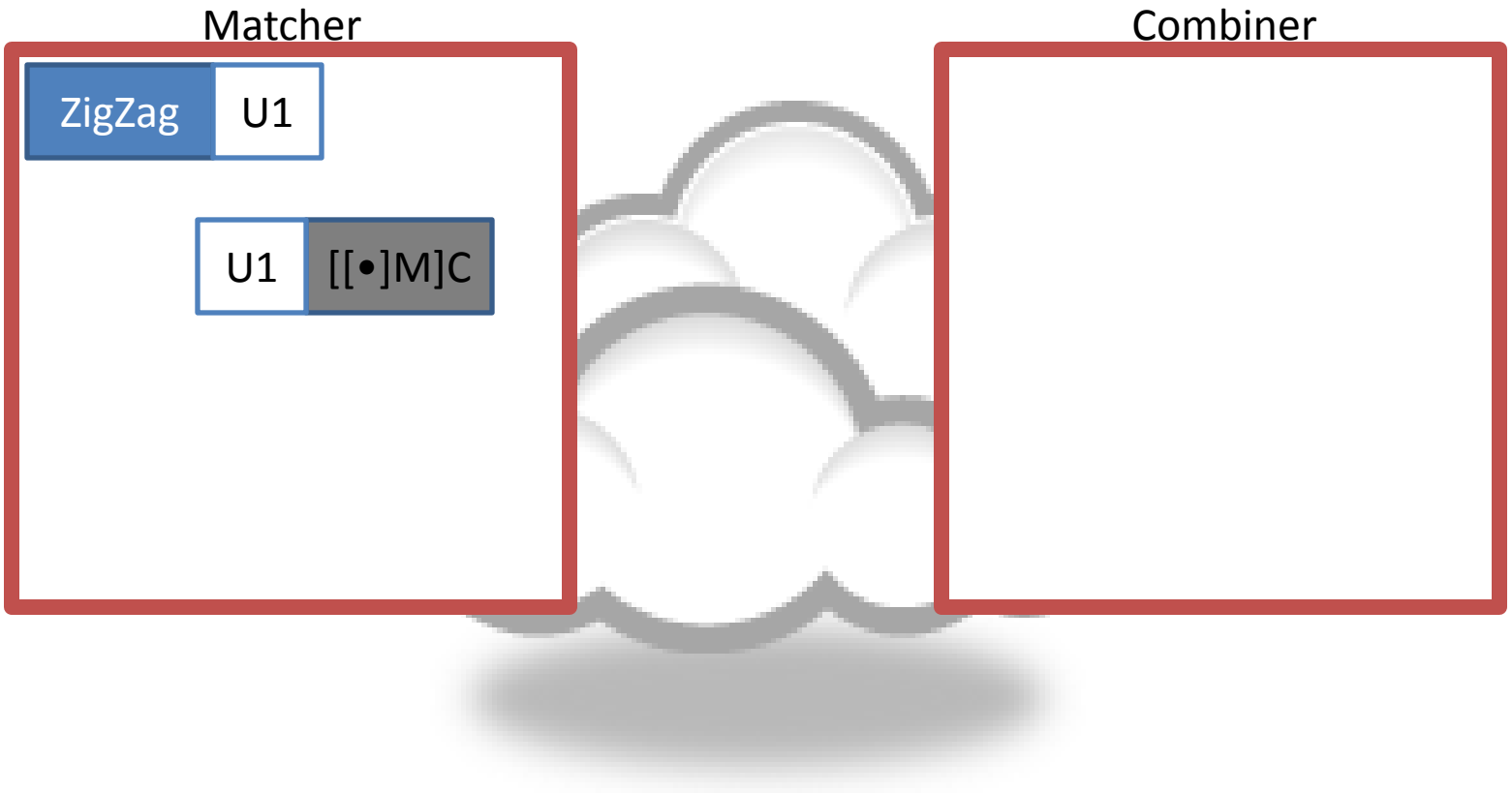
Koi: Privacy-Preserving Matching



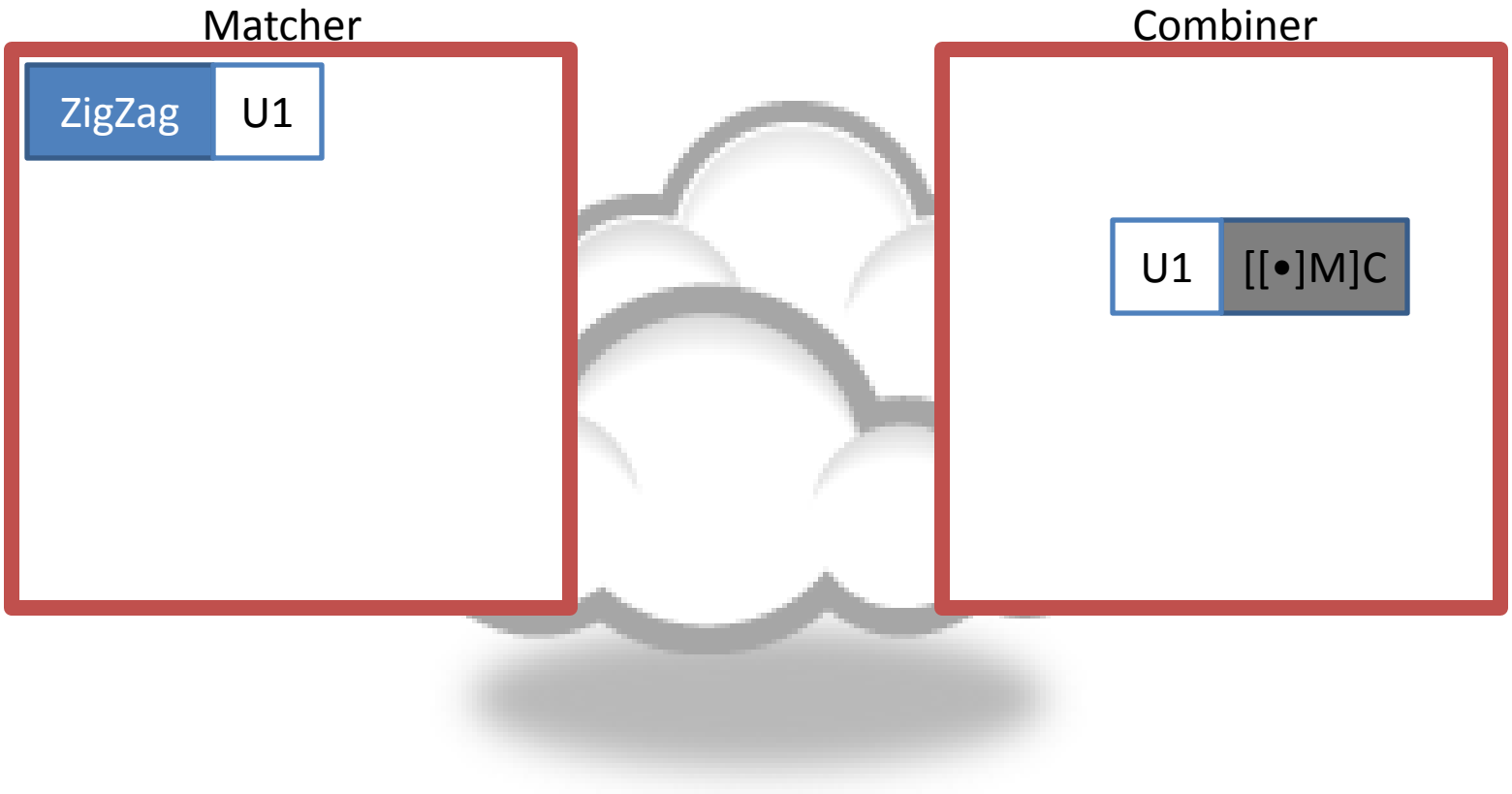
Koi: Privacy-Preserving Matching



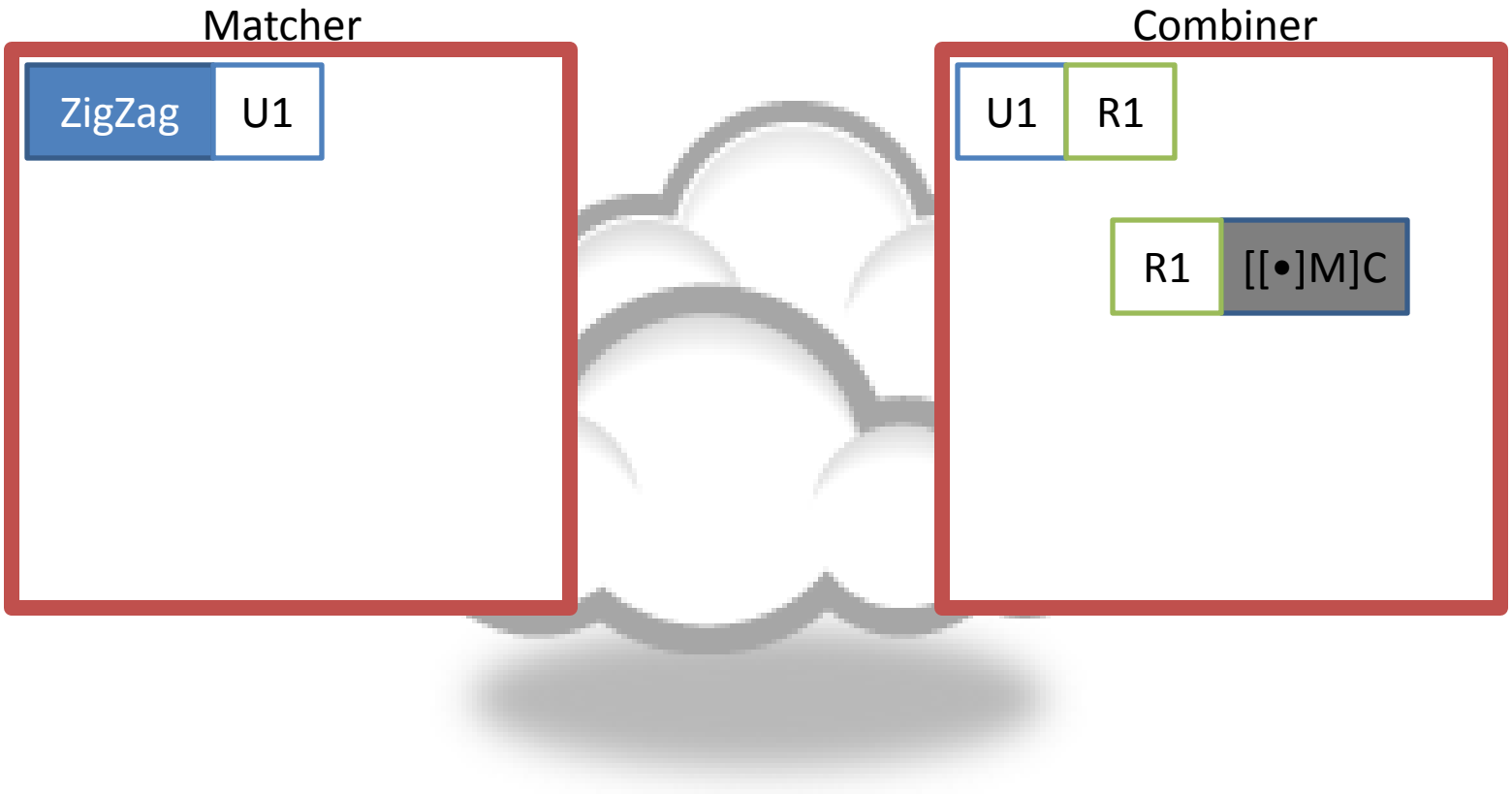
Koi: Privacy-Preserving Matching



Koi: Privacy-Preserving Matching



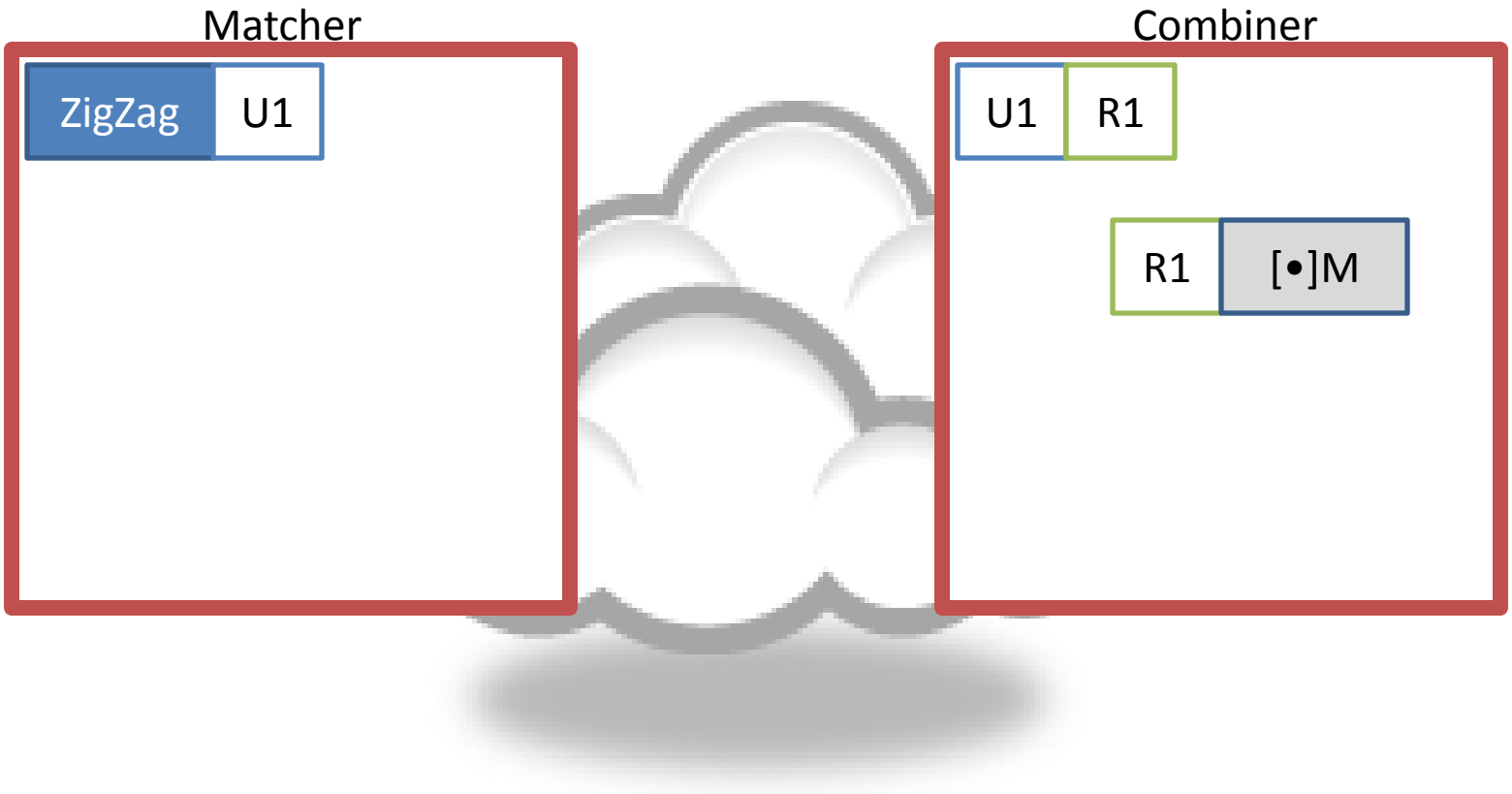
Koi: Privacy-Preserving Matching



ZigZag	Bail-Bond	N 2nd St.

Saikat	Bail-Bond	“cur loc” + 5blk

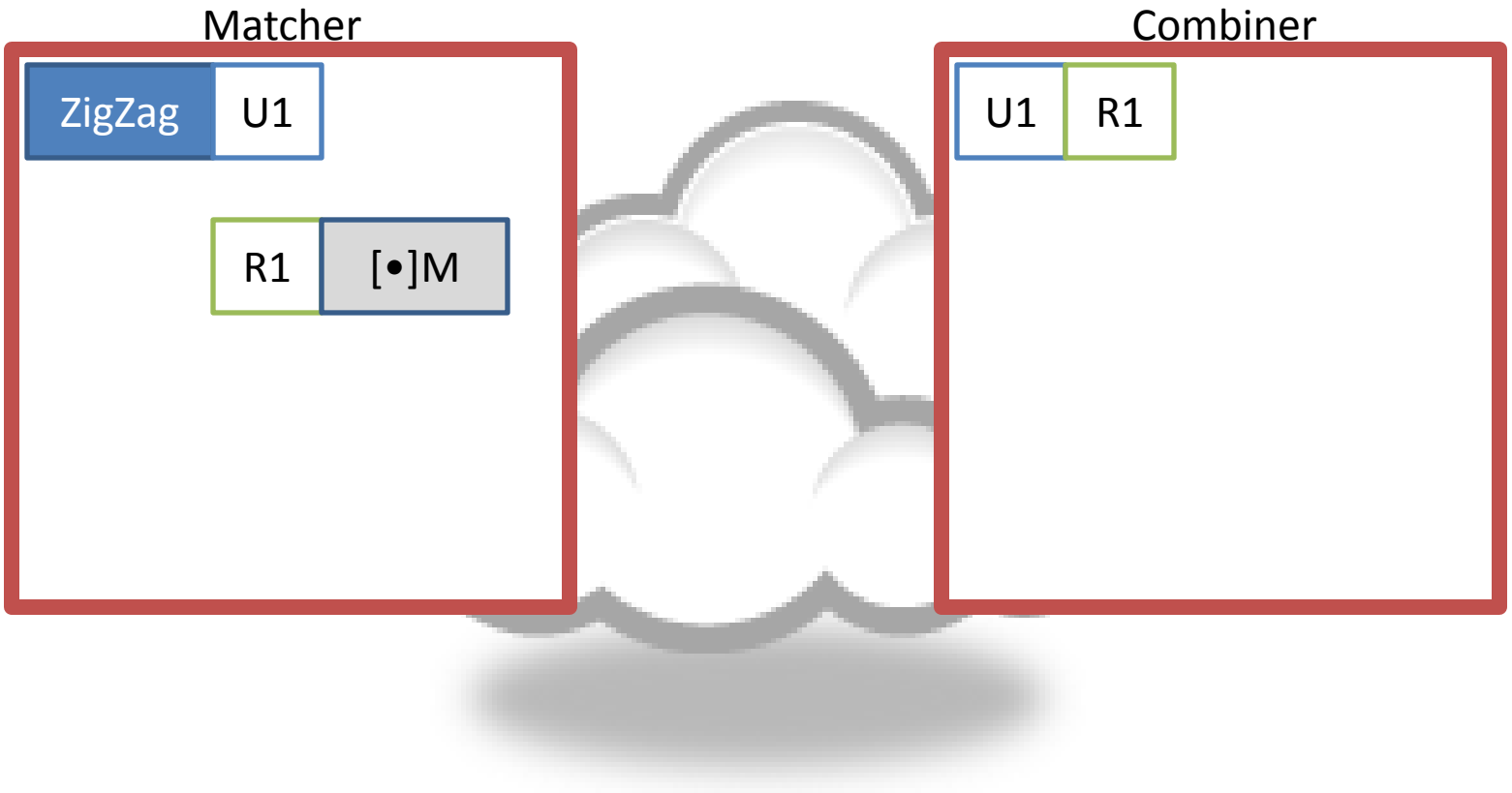
Koi: Privacy-Preserving Matching



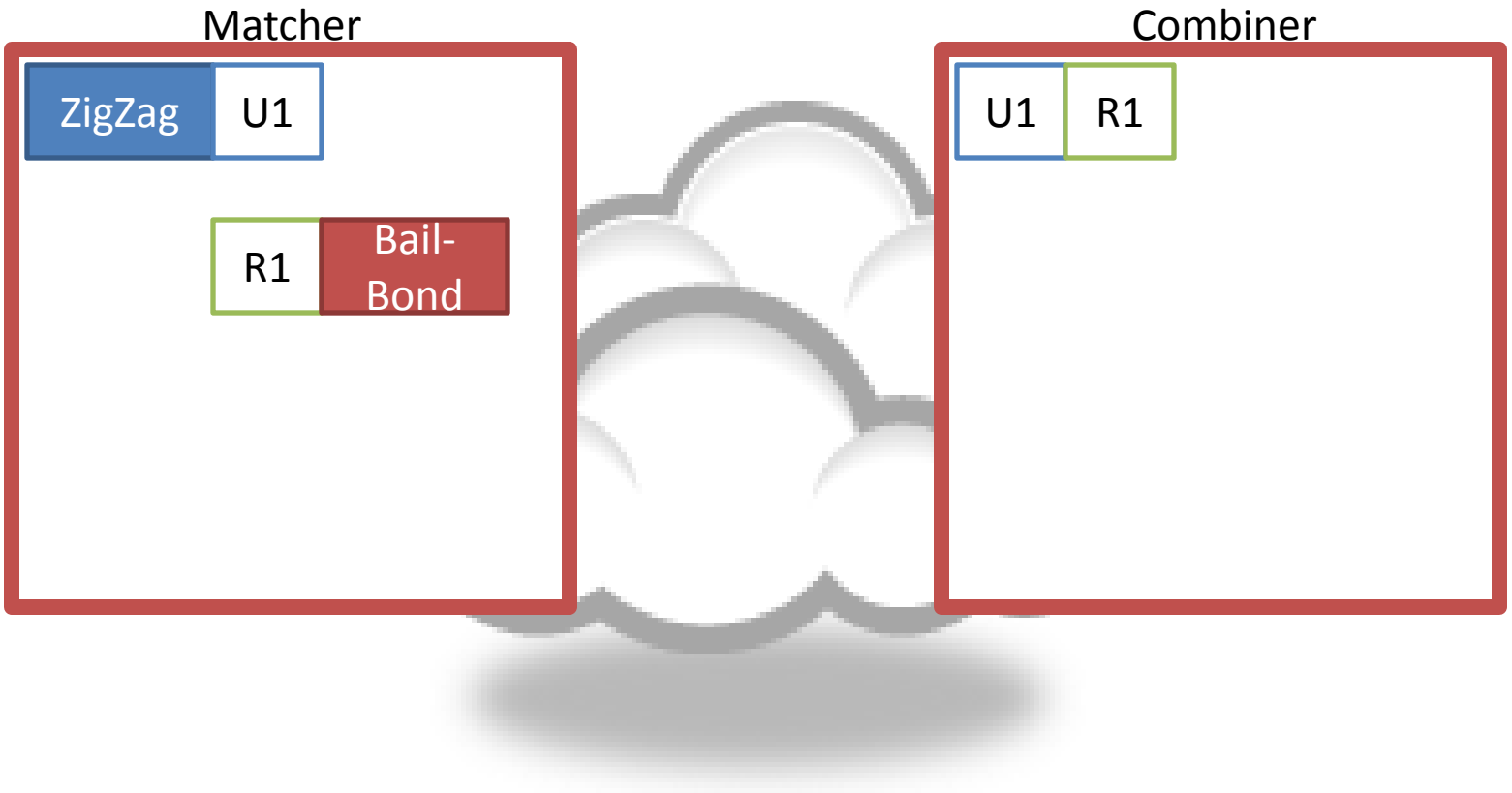
ZigZag	Bail-Bond	N 2nd St.

Saikat	Bail-Bond	"cur loc" + 5blk

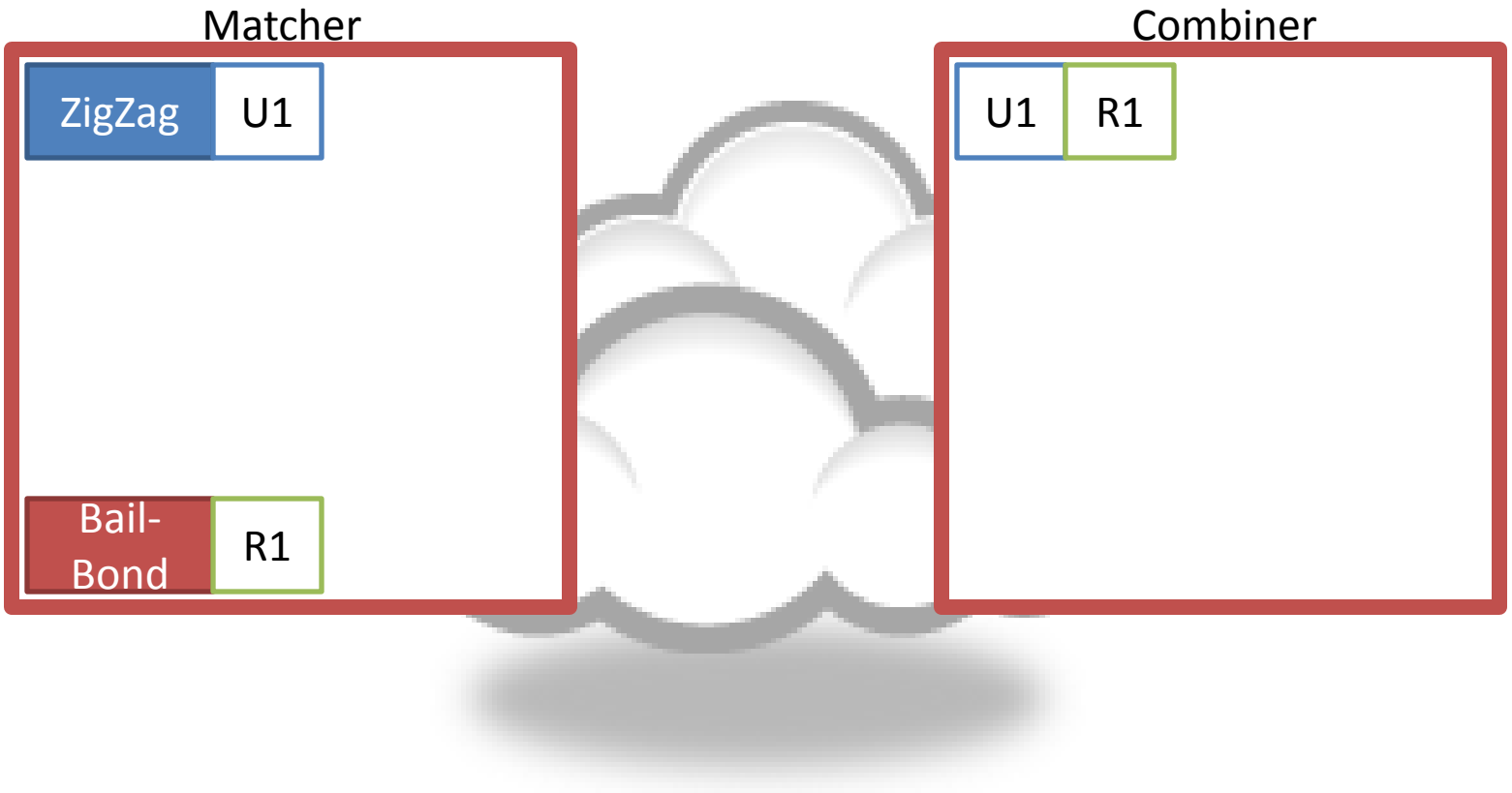
Koi: Privacy-Preserving Matching



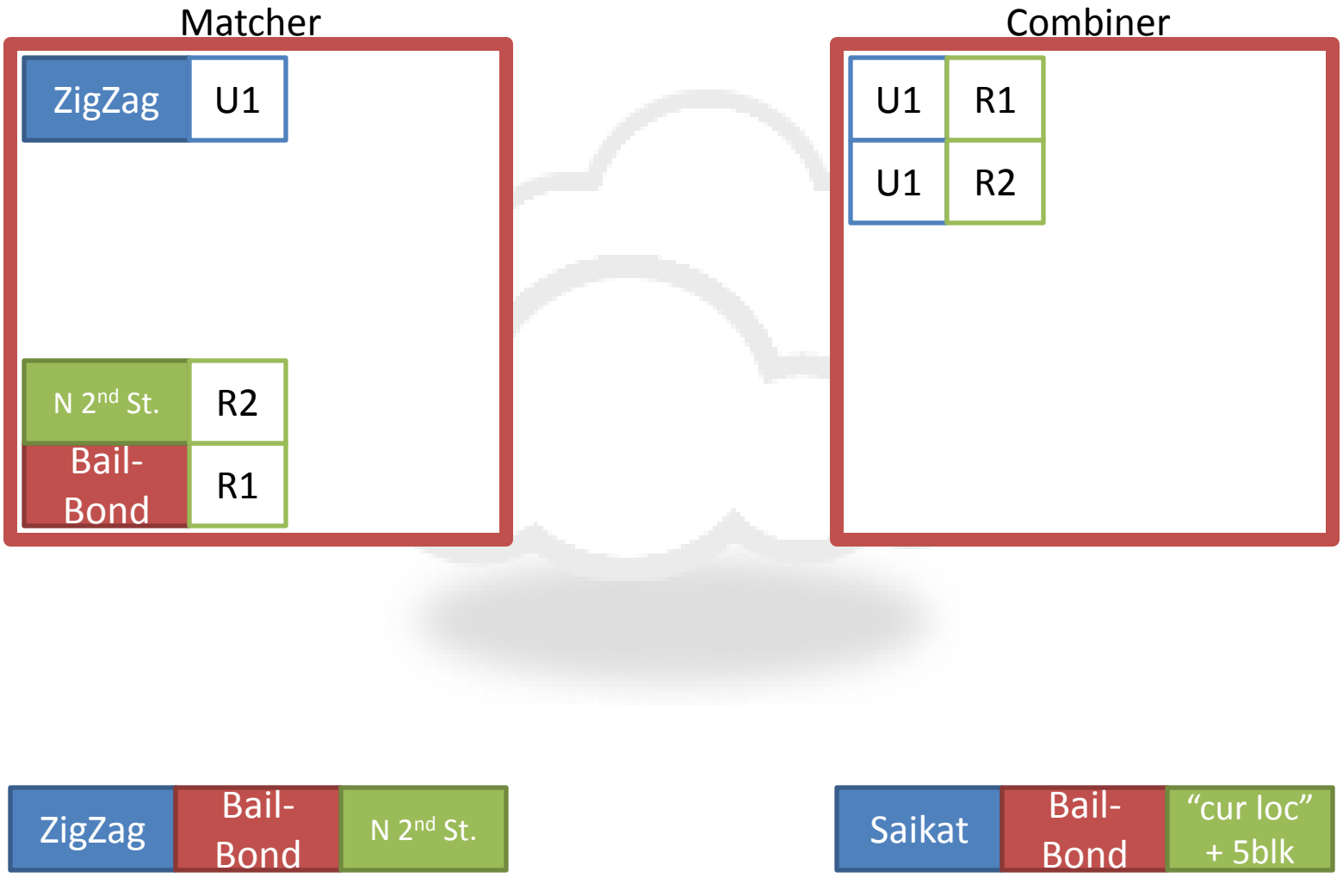
Koi: Privacy-Preserving Matching



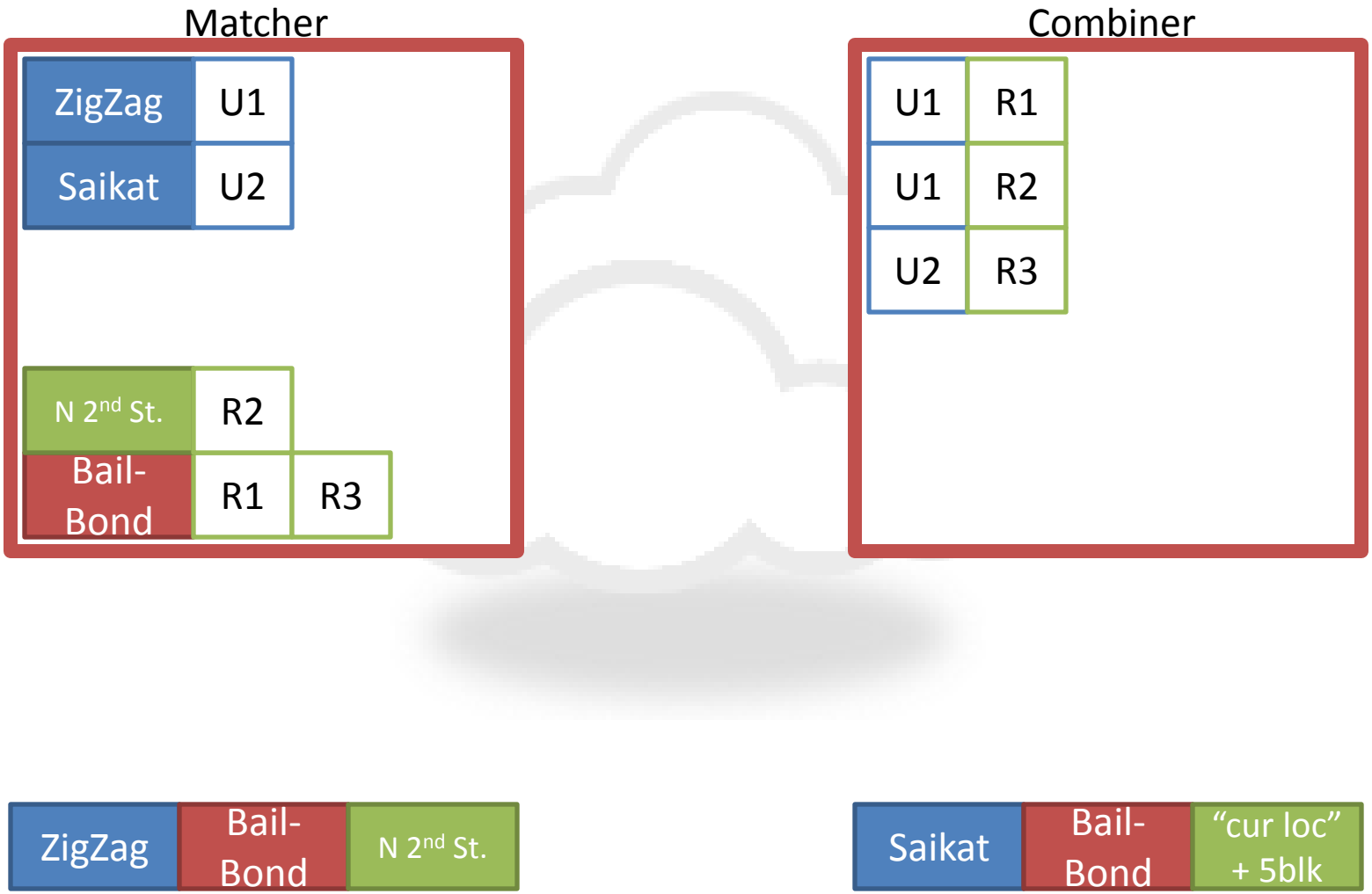
Koi: Privacy-Preserving Matching



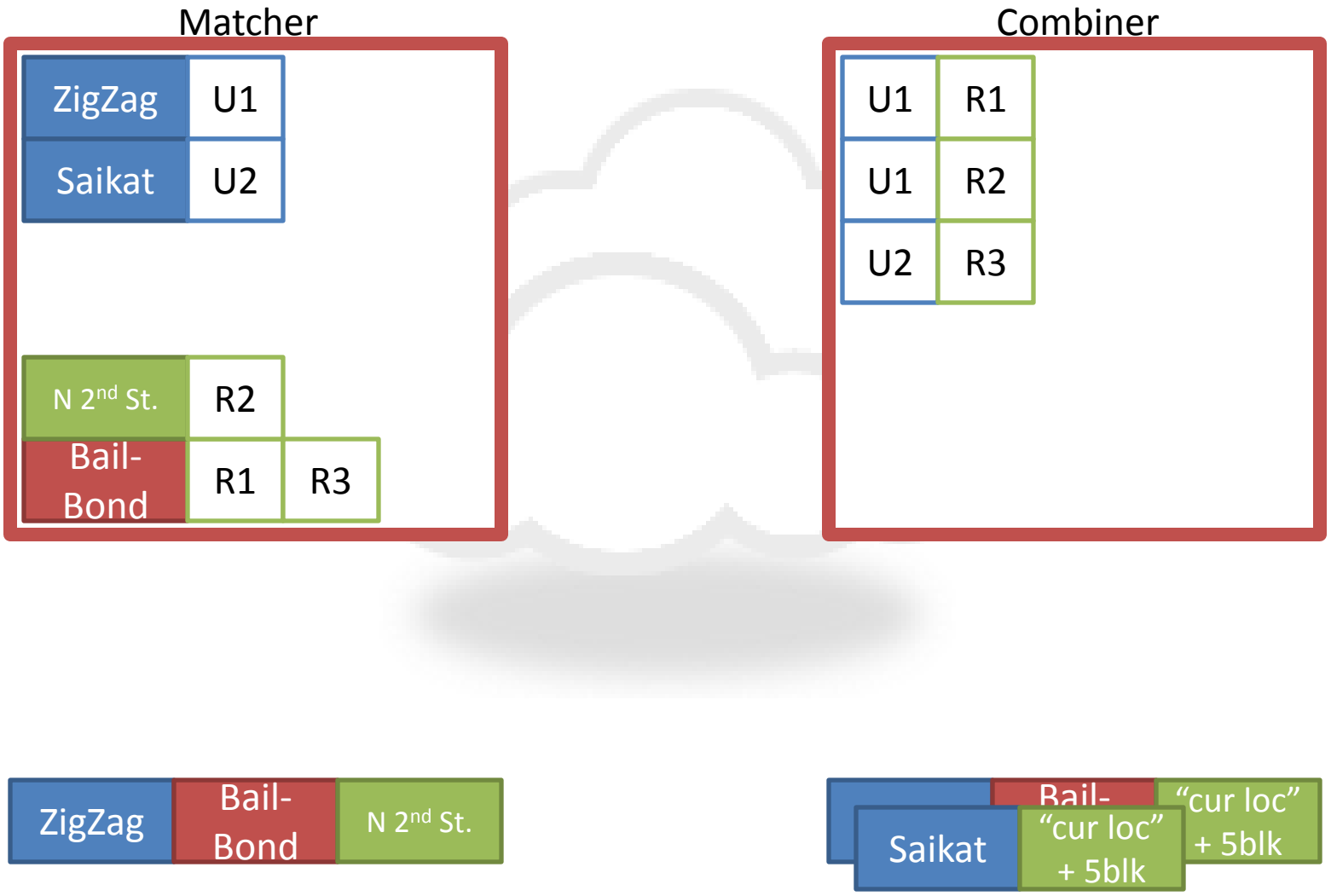
Koi: Privacy-Preserving Matching



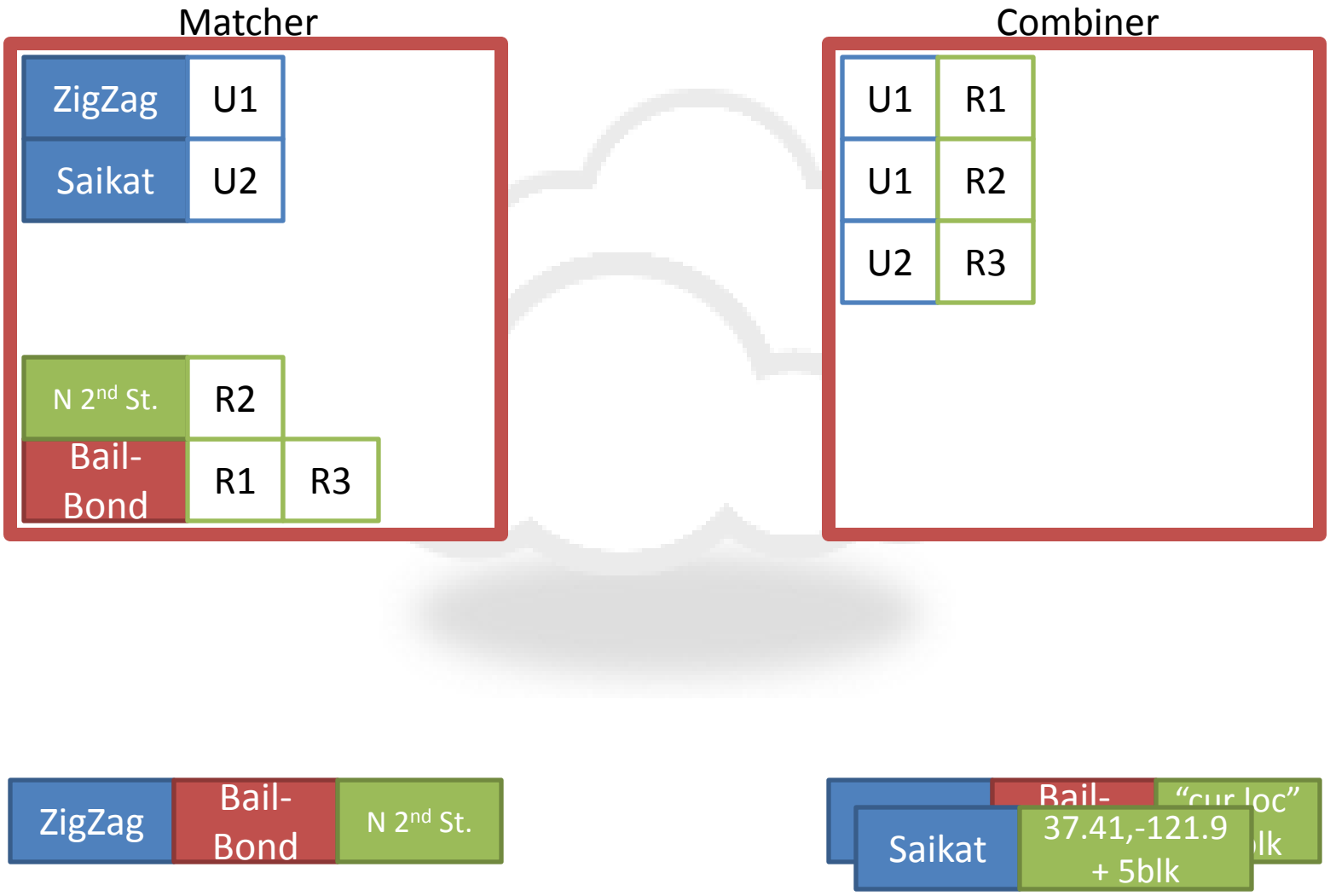
Koi: Privacy-Preserving Matching



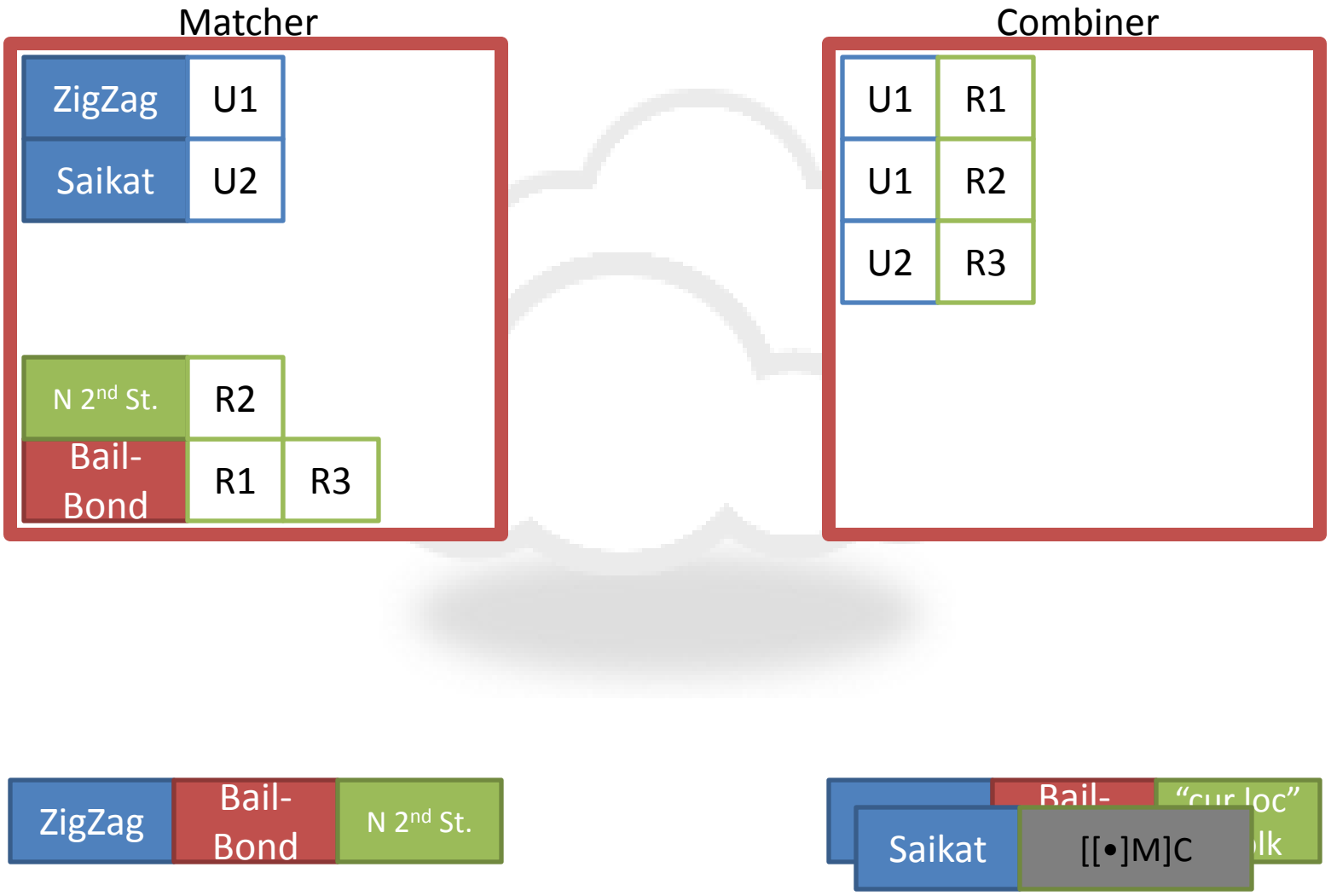
Koi: Privacy-Preserving Matching



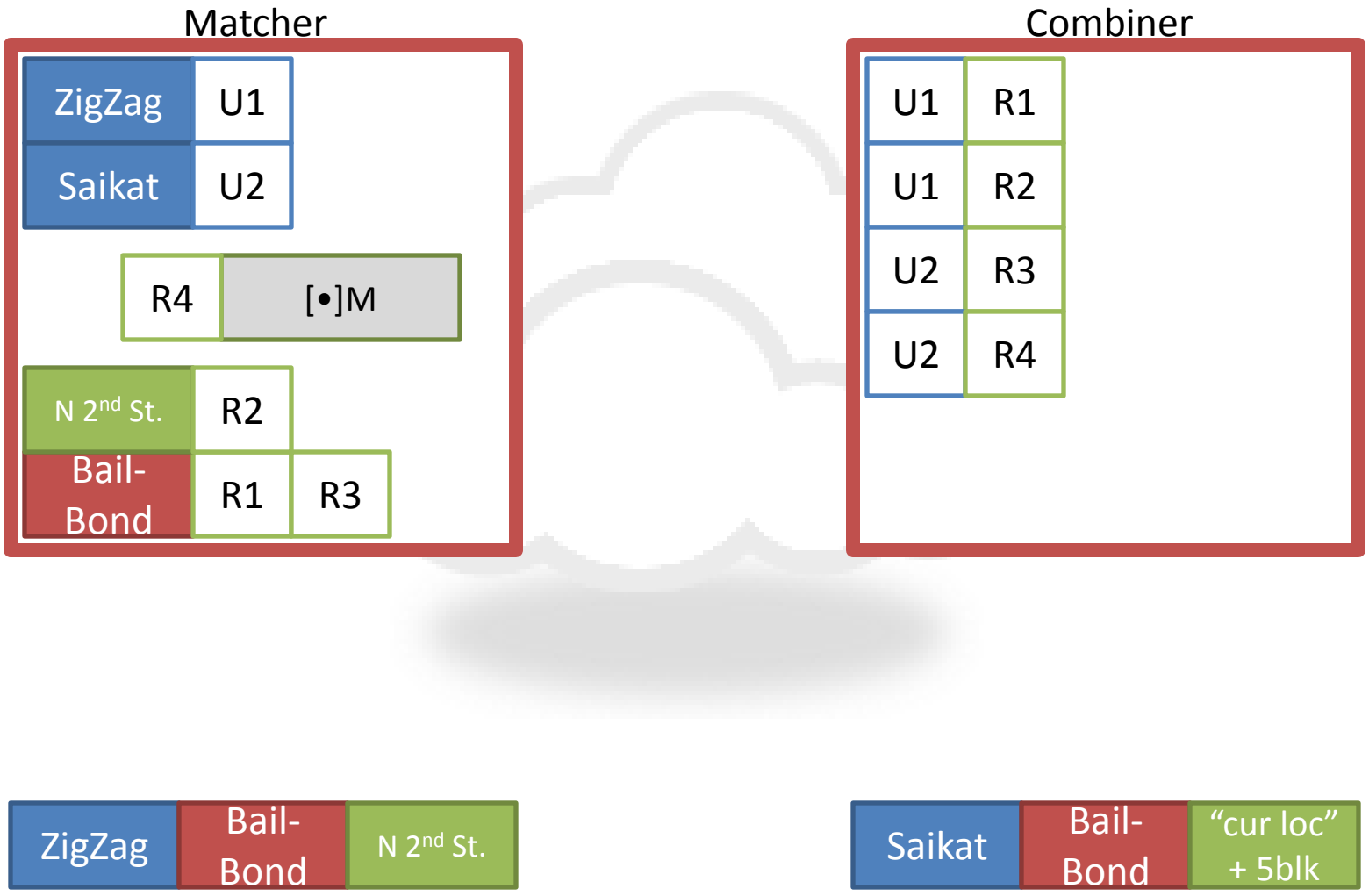
Koi: Privacy-Preserving Matching



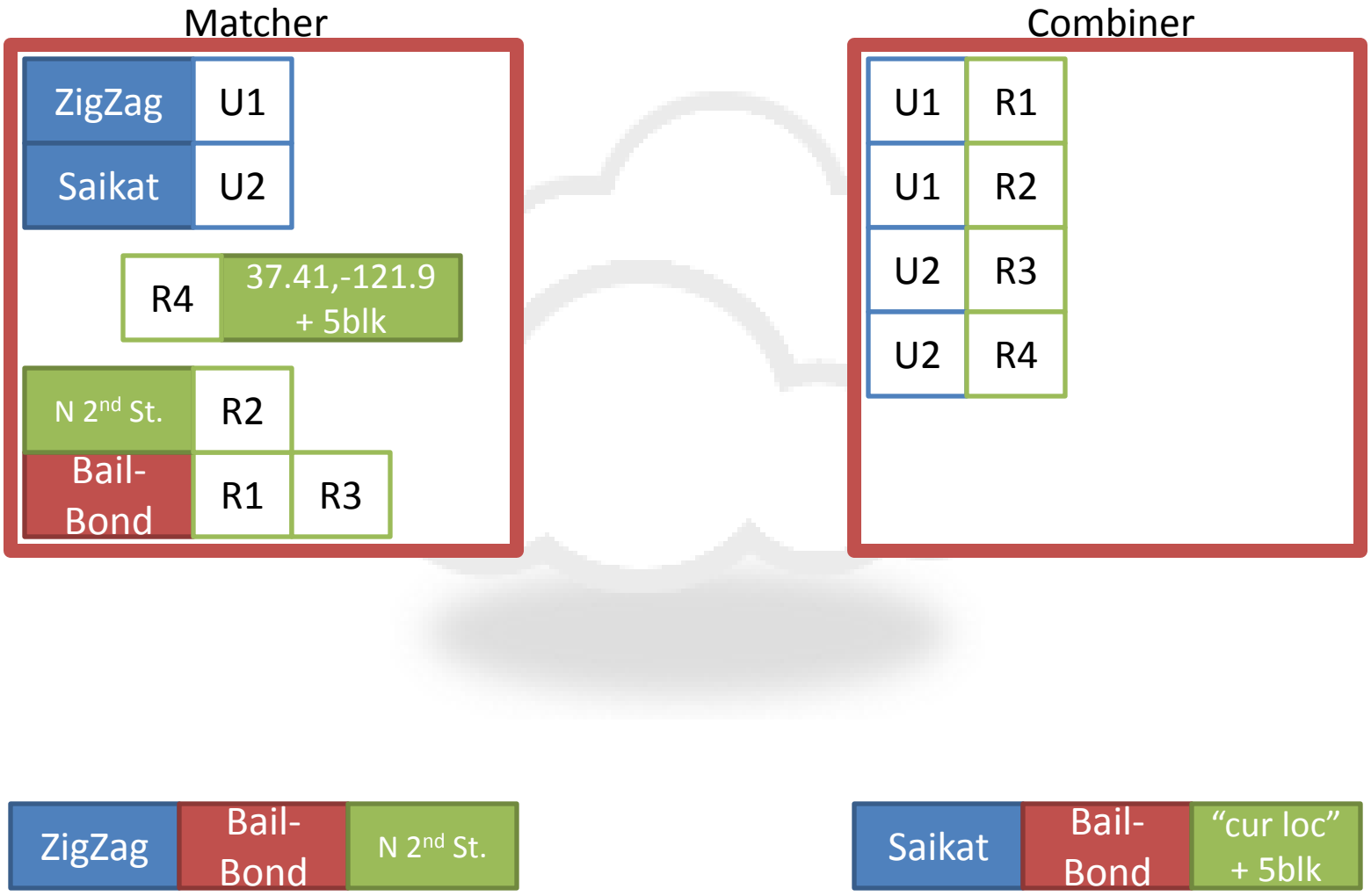
Koi: Privacy-Preserving Matching



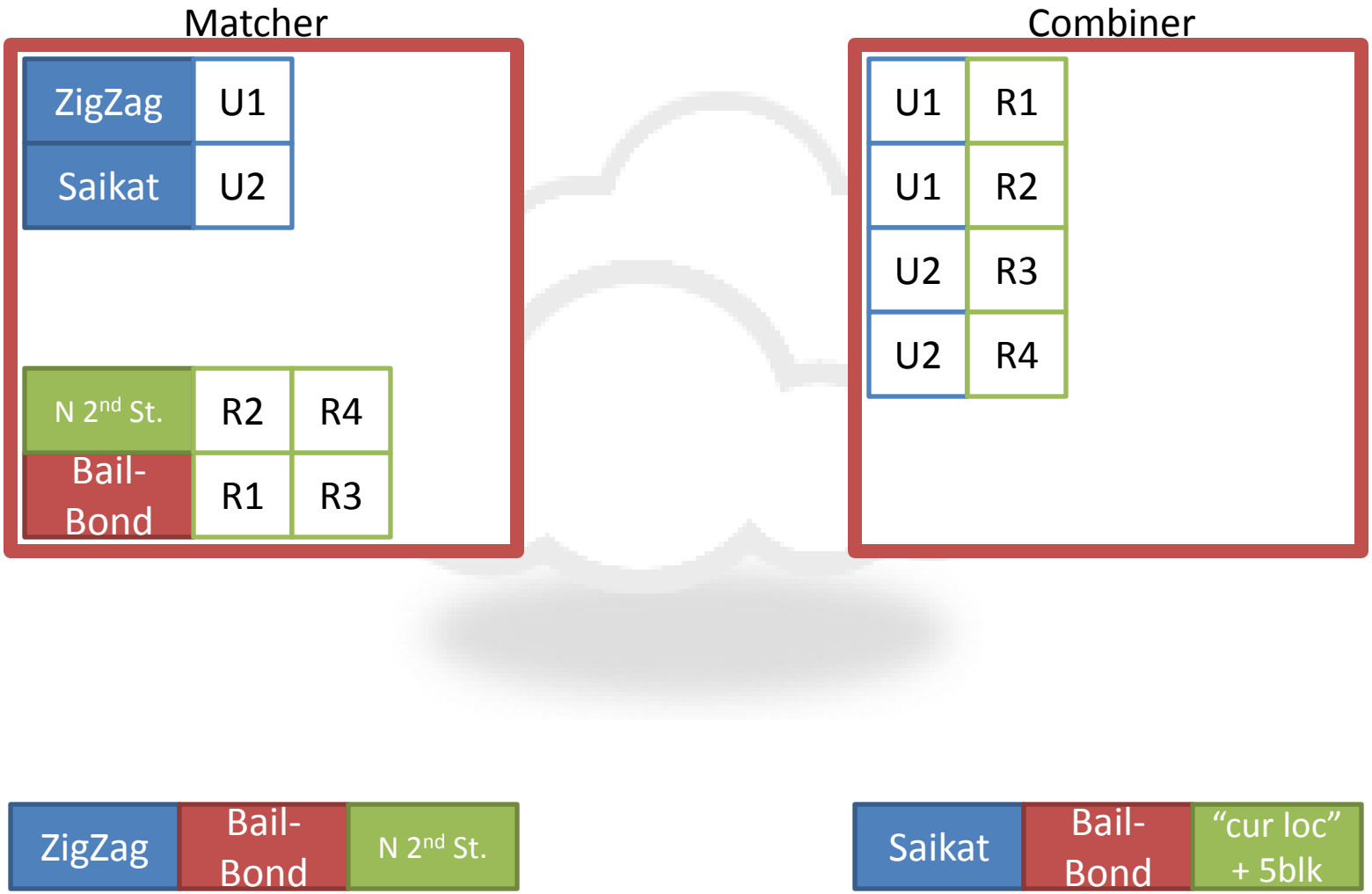
Koi: Privacy-Preserving Matching



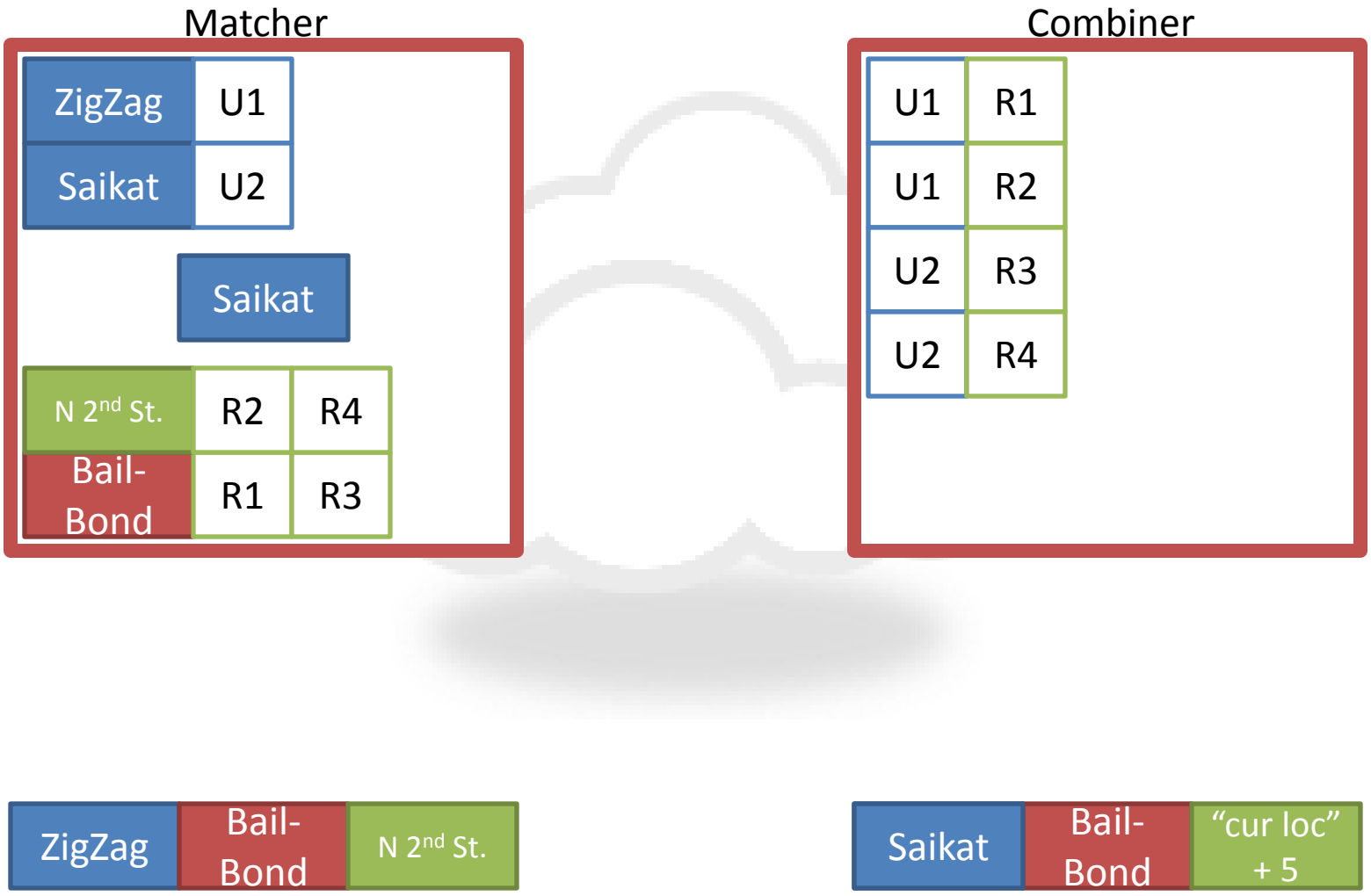
Koi: Privacy-Preserving Matching



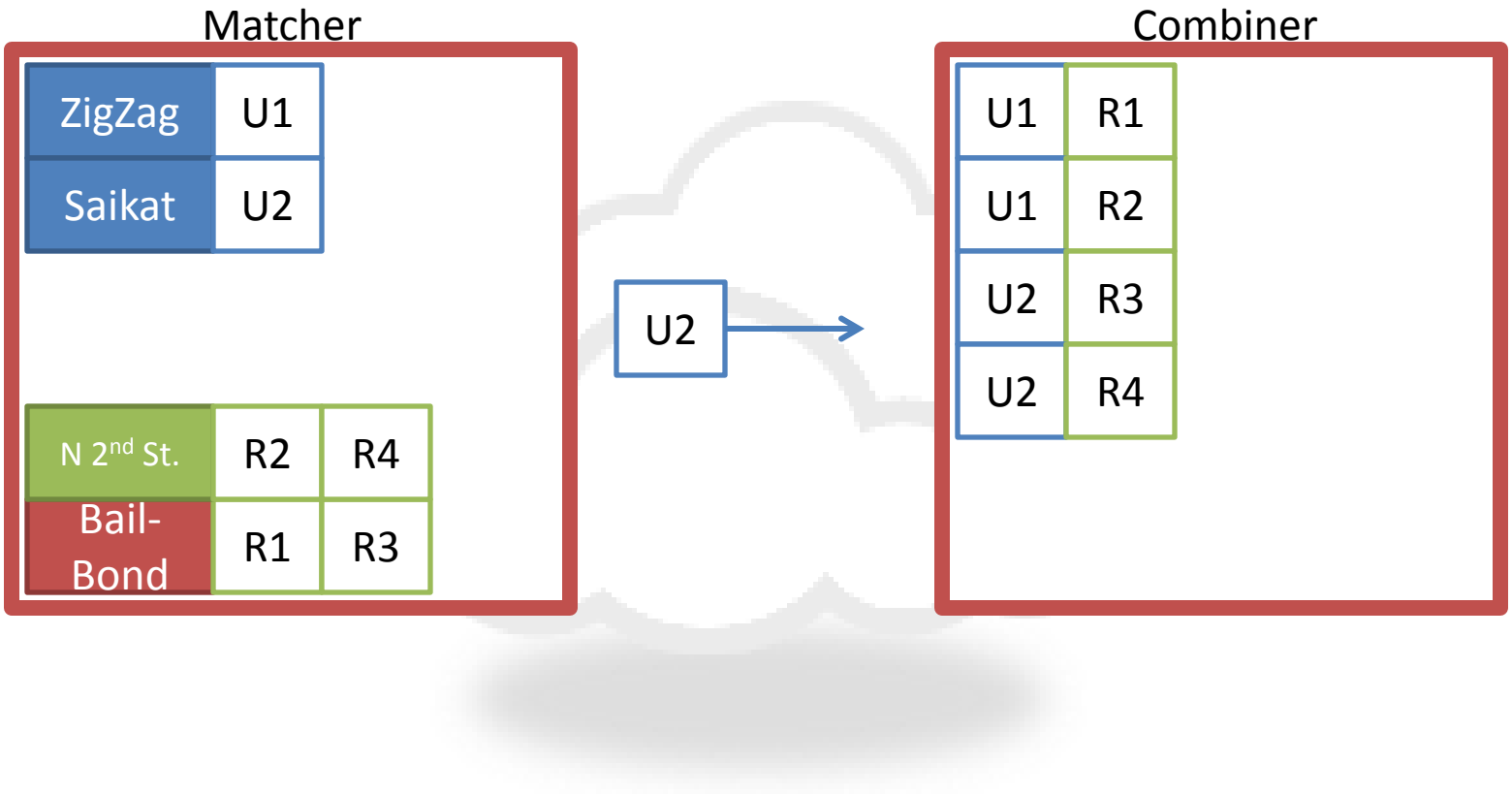
Koi: Privacy-Preserving Matching



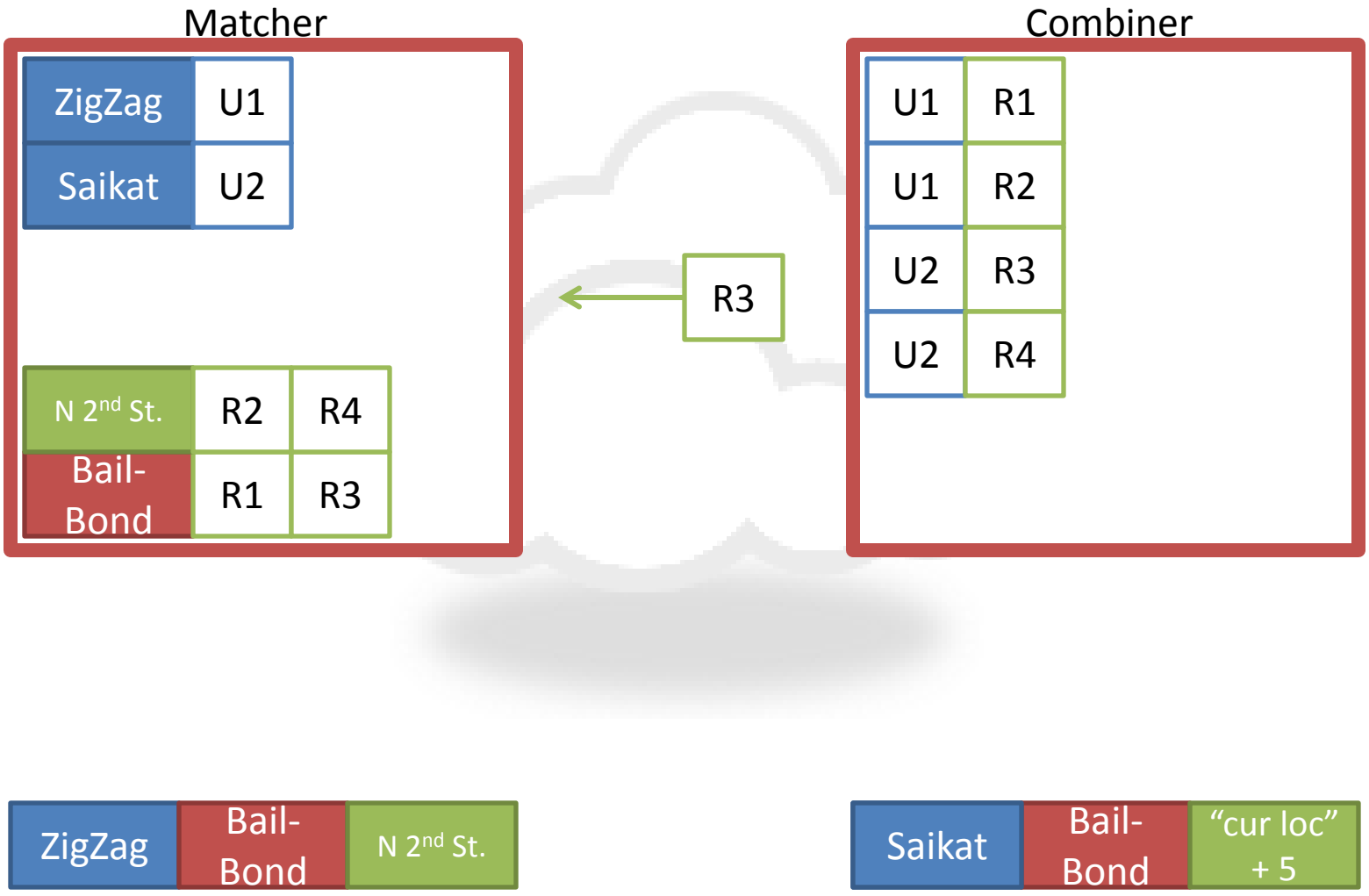
Koi: Privacy-Preserving Matching



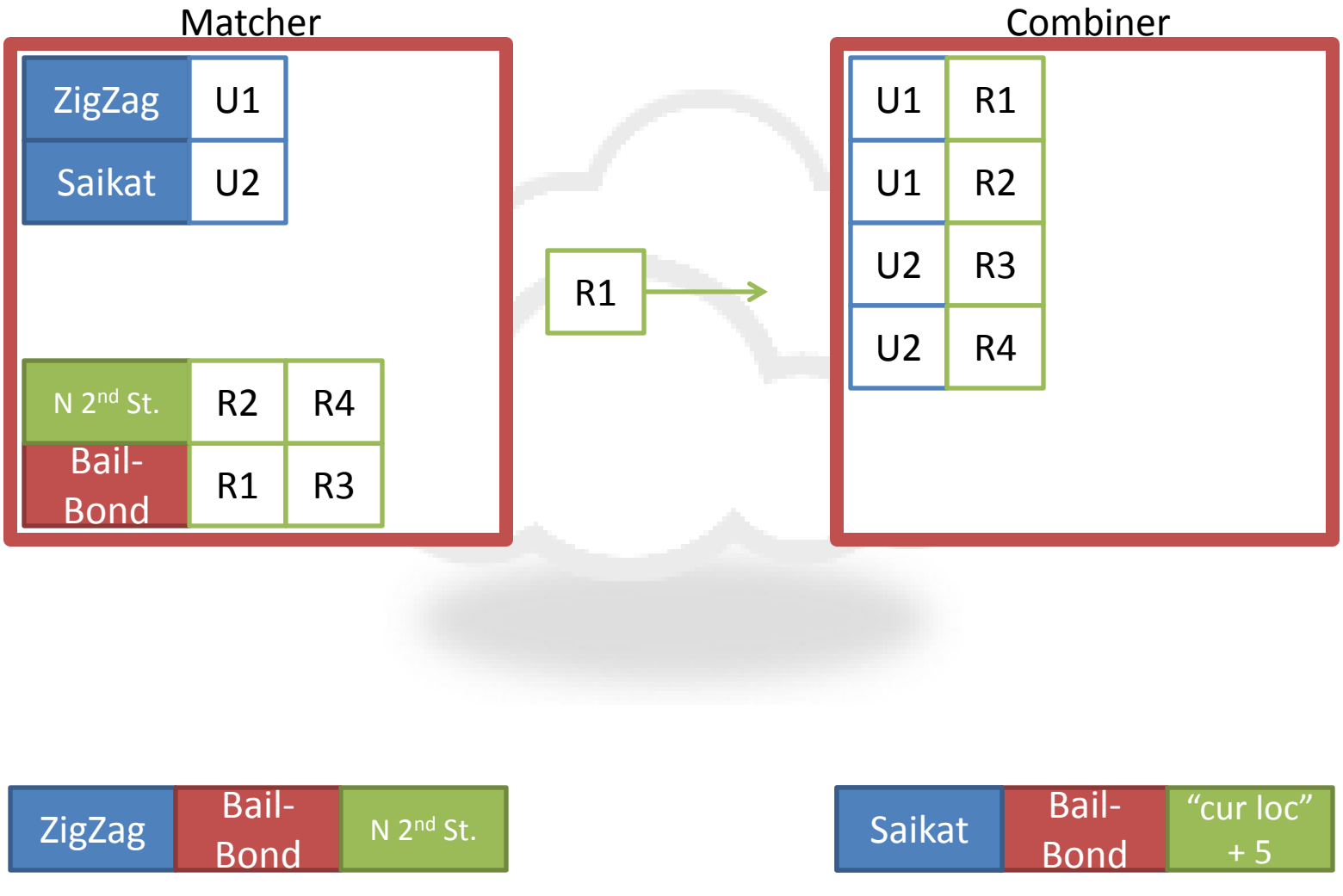
Koi: Privacy-Preserving Matching



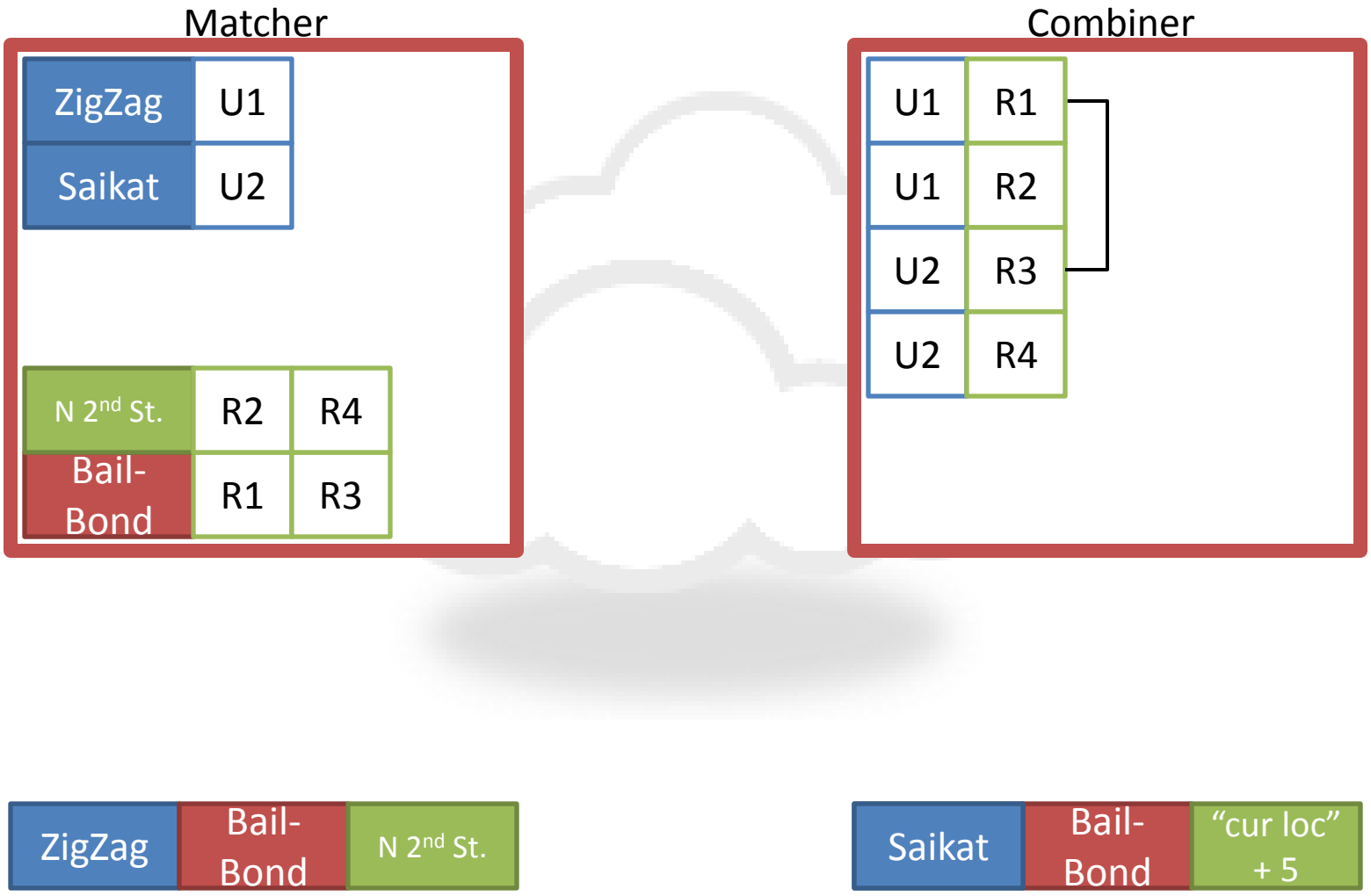
Koi: Privacy-Preserving Matching



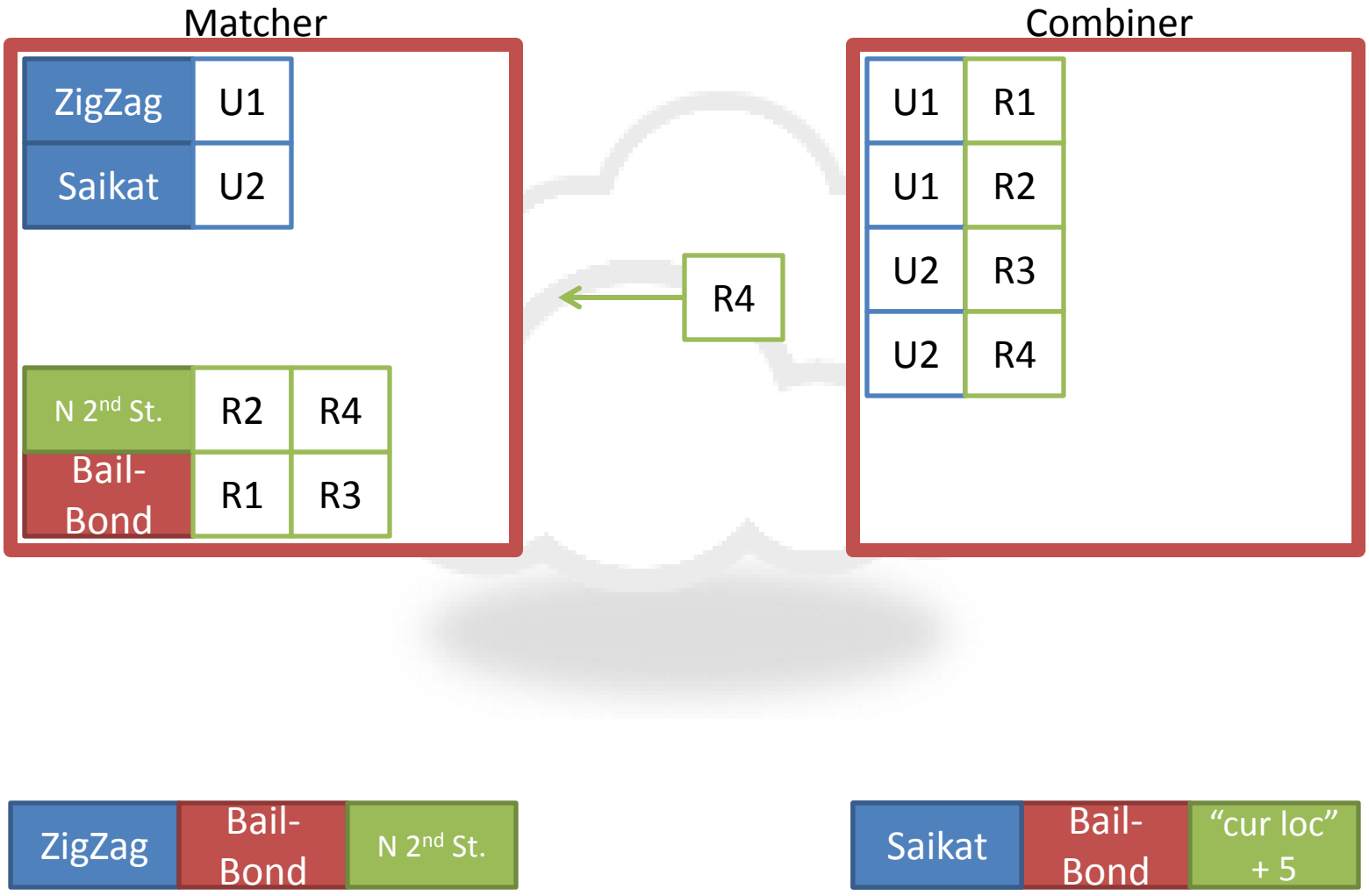
Koi: Privacy-Preserving Matching



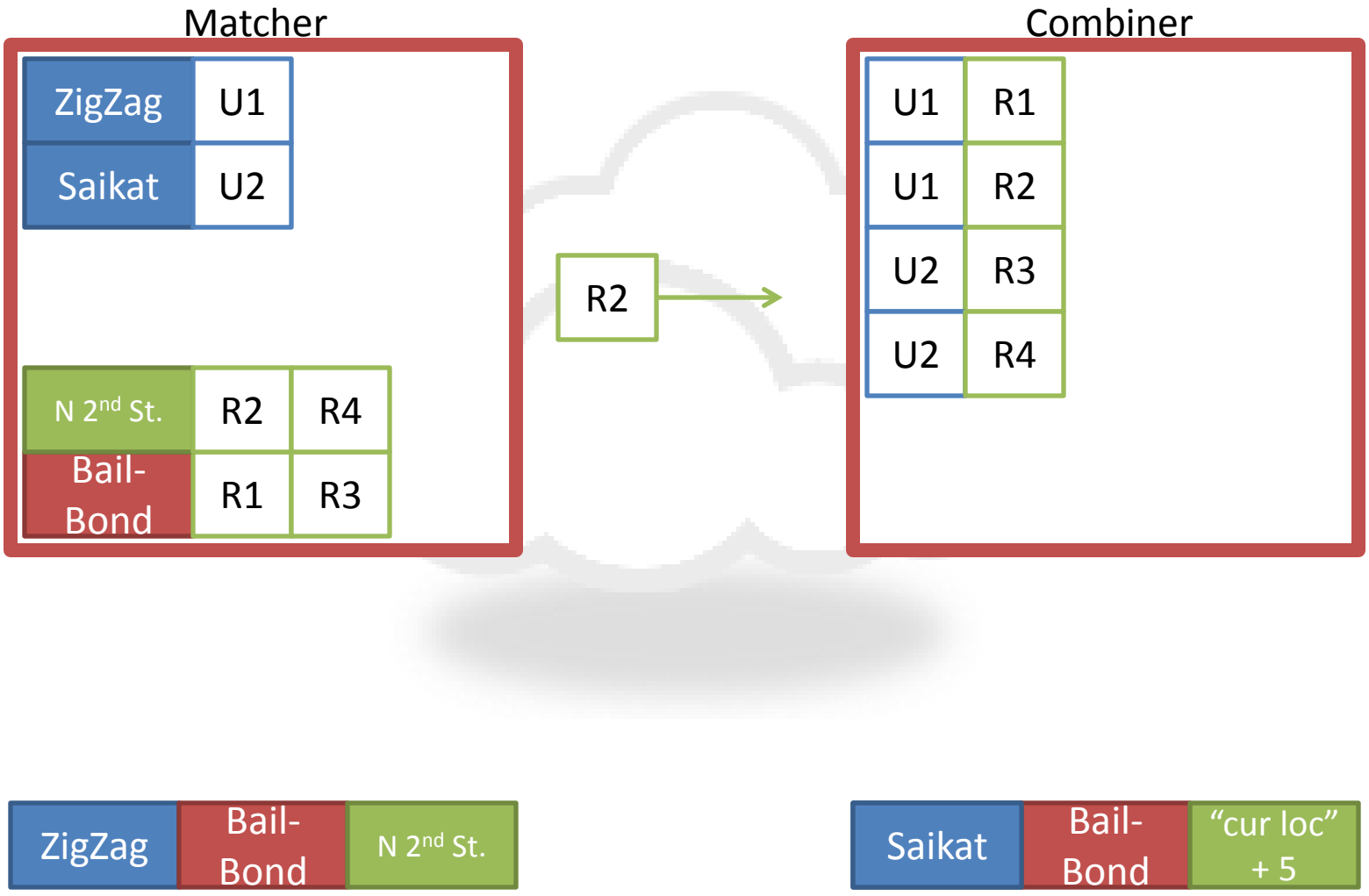
Koi: Privacy-Preserving Matching



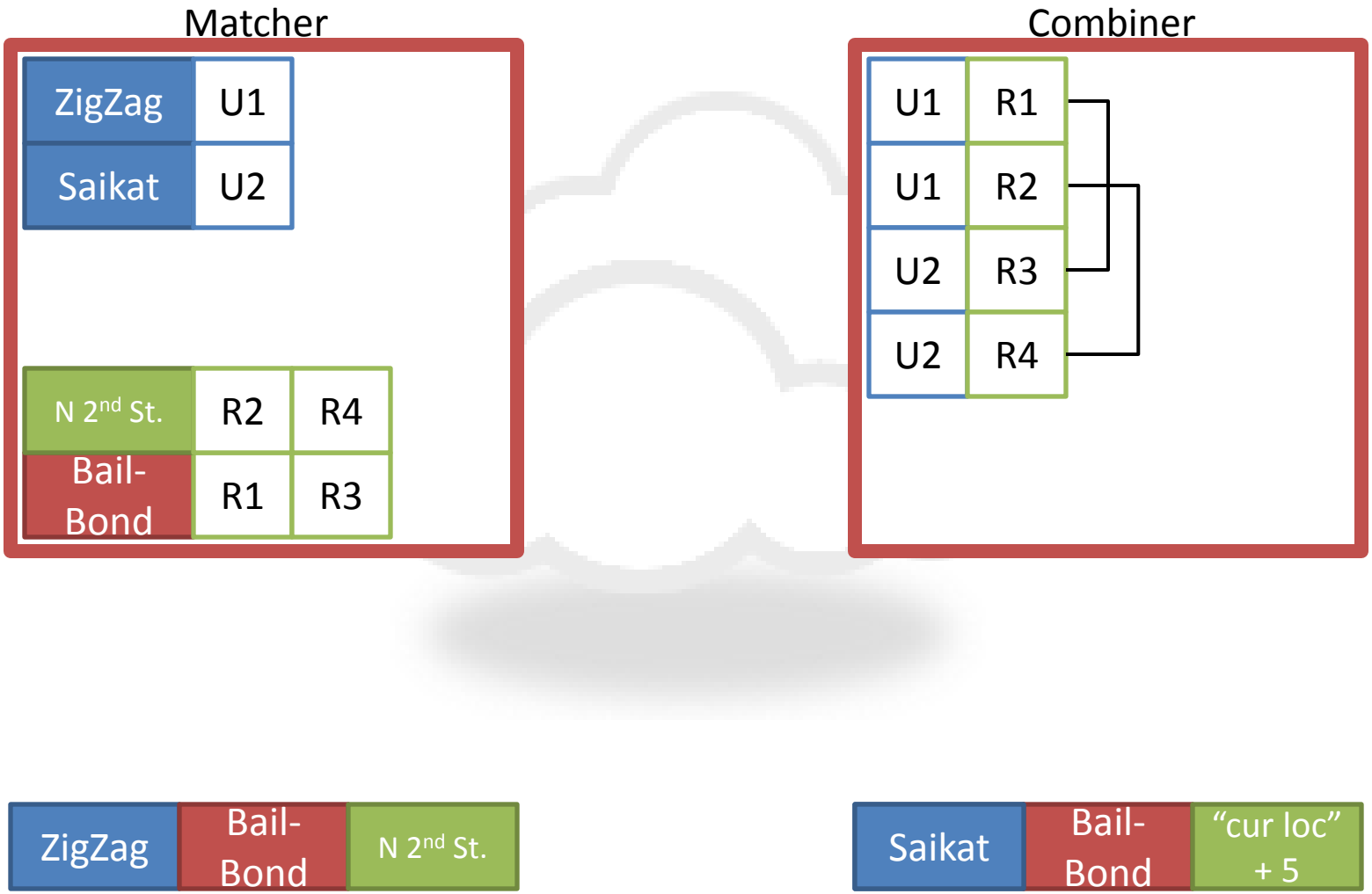
Koi: Privacy-Preserving Matching



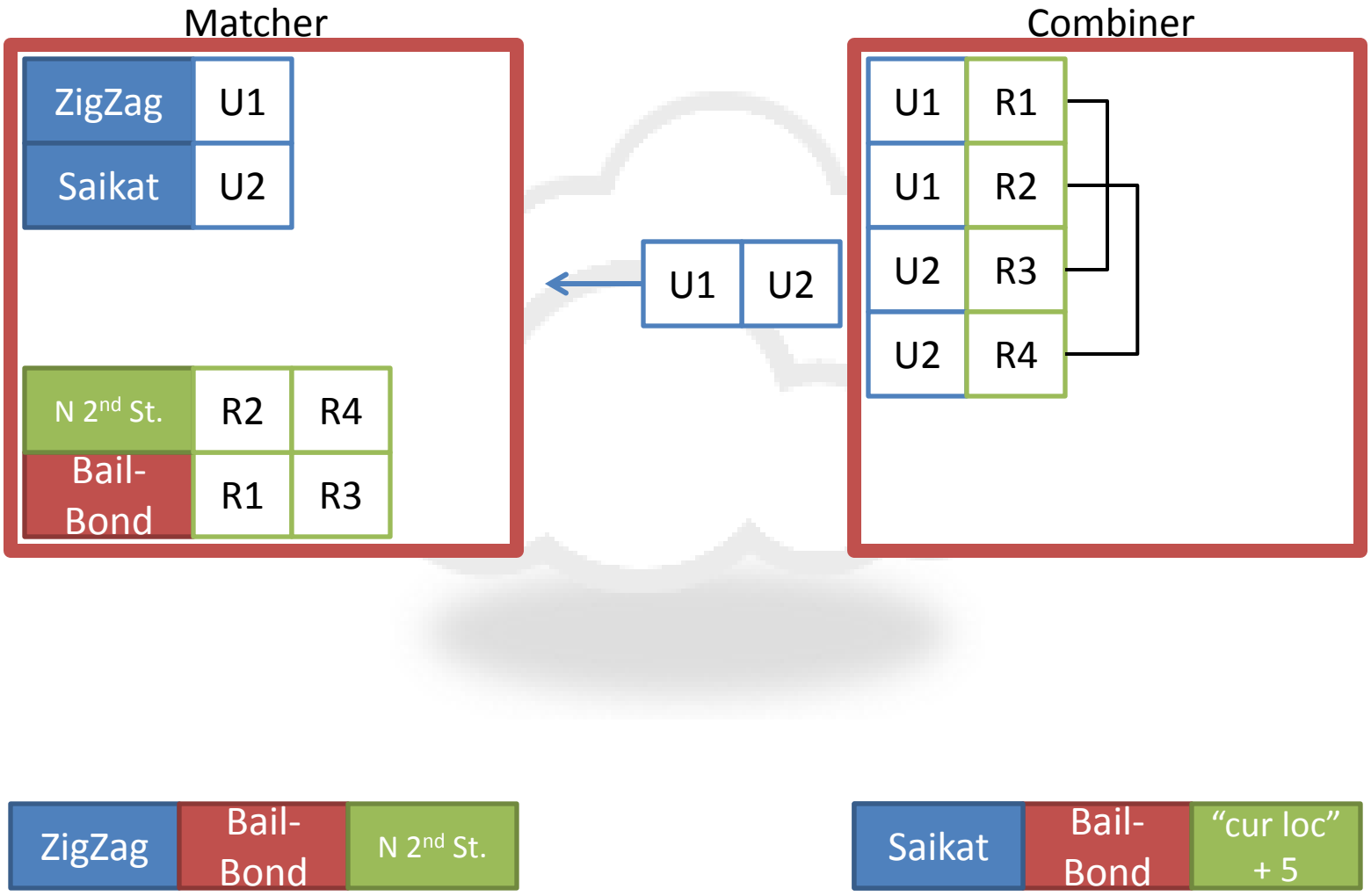
Koi: Privacy-Preserving Matching



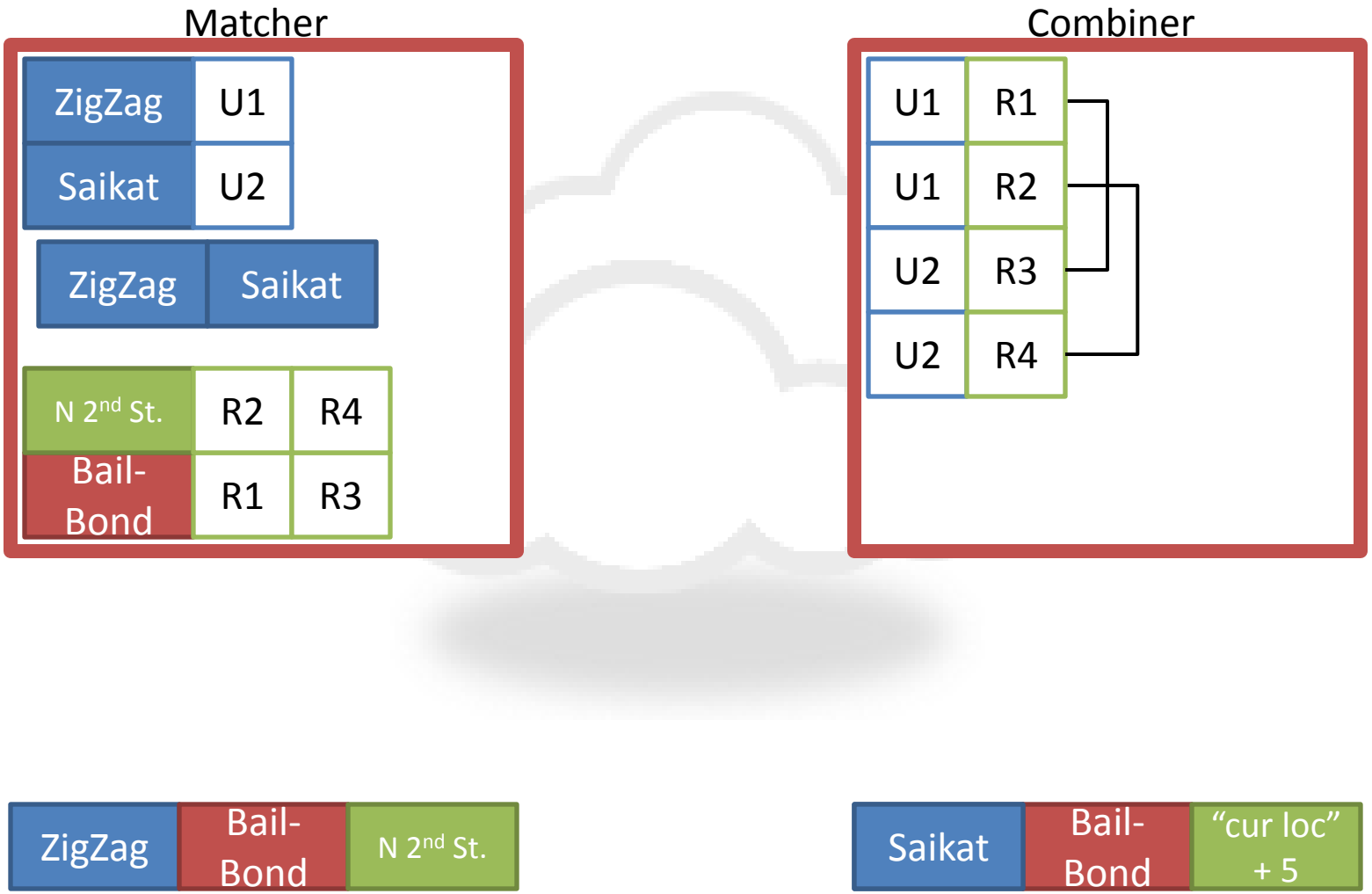
Koi: Privacy-Preserving Matching



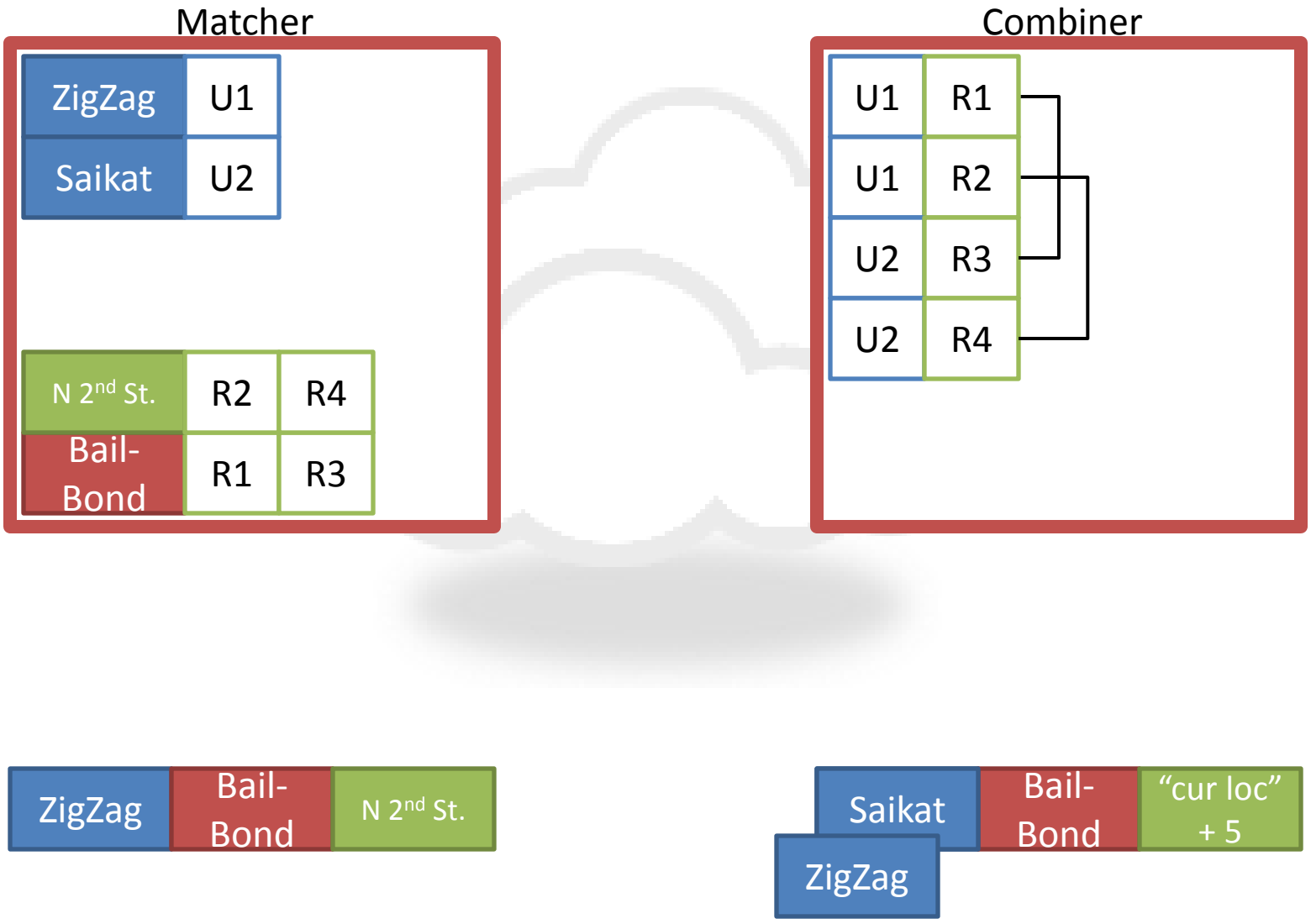
Koi: Privacy-Preserving Matching



Koi: Privacy-Preserving Matching



Koi: Privacy-Preserving Matching



Koi Features

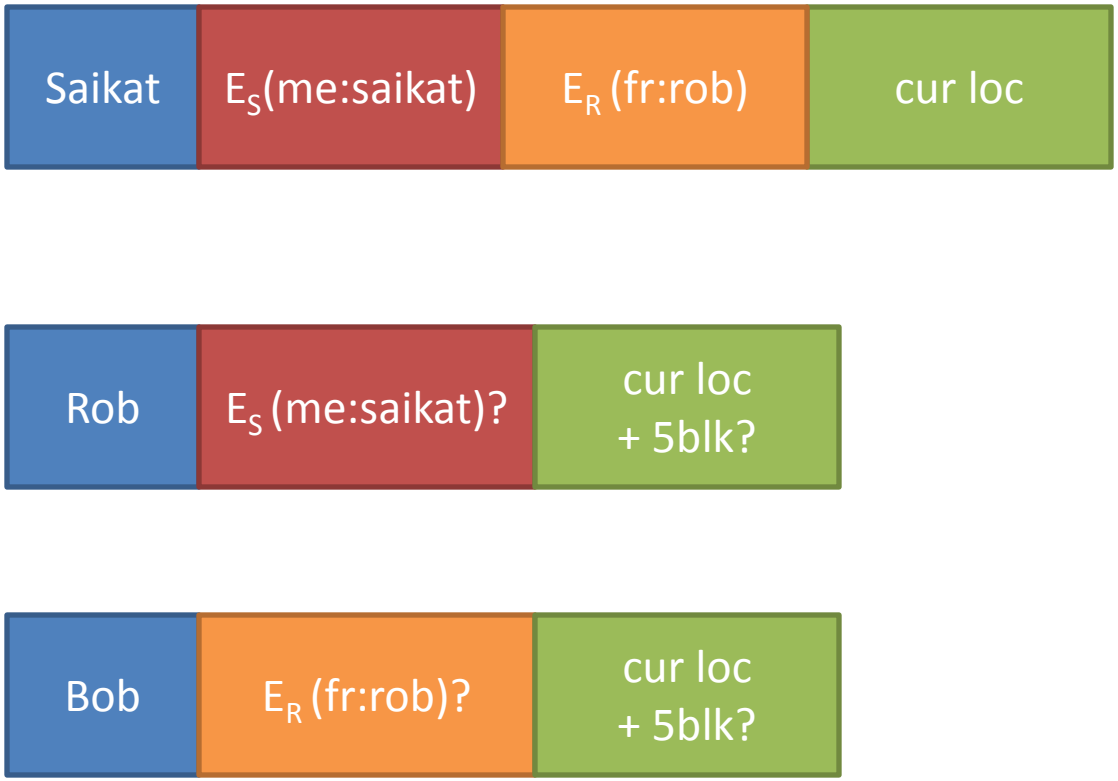
- Matching based on attribute plain-text
  - Location, spelling correction, translation
  - Other semantic transformation
- OS can auto-update location attributes
  - Without waking app up

Koi Applications: Location-Based …

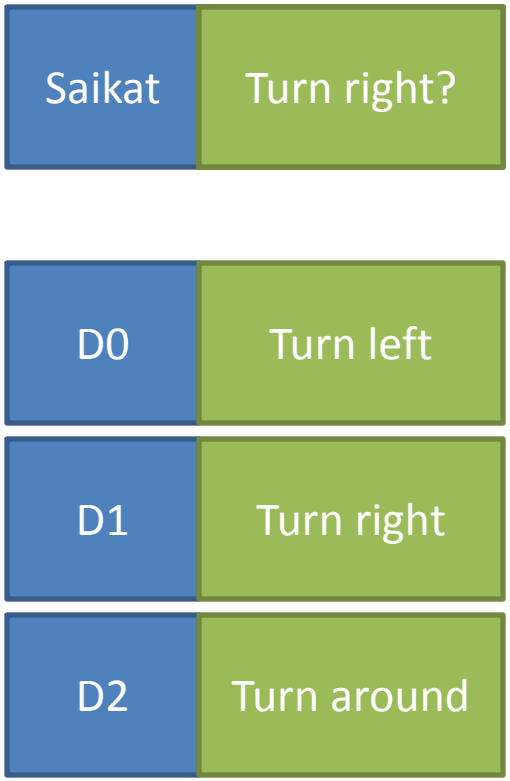
- Advertising
- Content tagging (photos, etc.)
- Search
- Recommendations

- Social networking
- Navigation

Koi: Private Mobile Social Network



Koi: Private Navigation



Privacy-Properties

- Proverif Automated Theorem Prover
- Model Koi protocol in applied pi-calculus
  - Unlinkability (using Proverif secrecy)
  - Adversary (spy channels; Honest-but-Curious)
  - Datastore (using Proverif asynchronous channels)
- Proofs for:
  1. User cannot be linked with attribute
  2. User's multiple attributes cannot be linked
  3. Matched users cannot be linked (extn.)

Malicious Applications

- Filter triggers
  - By location, time-of-day, etc.
- Rate-limit triggers and callbacks
  - Per user, across all users, etc.

- Sybil apps trying to stay under threshold
  - Economic burden (developer key costs $$)

Implementation and Deployment

- Koi Matcher service implemented and publicly deployed
  - REST based API
  - HTML5 (mobile) browsers, and C# bindings
  - Scales well
- Combiner:
  - “Bring-your-own-combiner”
  - Or use our combiner (uhhh…)

Summary

- Current Get-Lat-Long API is bad for privacy
- Koi raises the level of abstraction
  - Simple yet powerful abstraction
  - Easy for app-developers to use
  - Allows platform to provide user privacy
- Proverif is a cool tool

Adoption Incentives

- Up to the platform
- Positive feedback:
  - Higher placement on app marketplace for apps not using legacy location API
- Negative feedback:
  - More nag screens for apps using legacy API
- Enforcement:
  - Block legacy API for free apps

Collusion

- Combiner
  - Allow privacy-advocates (EFF, ACLU), anti-virus companies, certificate agencies (Verisign), non-profits (Mozilla), to run combiner.
  - Their existence entirely dependent on public trust
- Matcher
  - User picks combiner (out of hundreds). Matcher needs to collude with many to be effective. Quickly discovered.