Modeling the Cost Structure of Identity Proofing

Masaki SHIMAOKA[1,2] and Noboru SONEHARA[2,3]

[1] Intelligent Systems Laboratory, SECOM Co., Ltd.

[2] The Graduate University for Advanced Studies

[3] National Institute of Informatics

Agena

- Background
- Qualitative Analysis
- Proposal
- Discussions

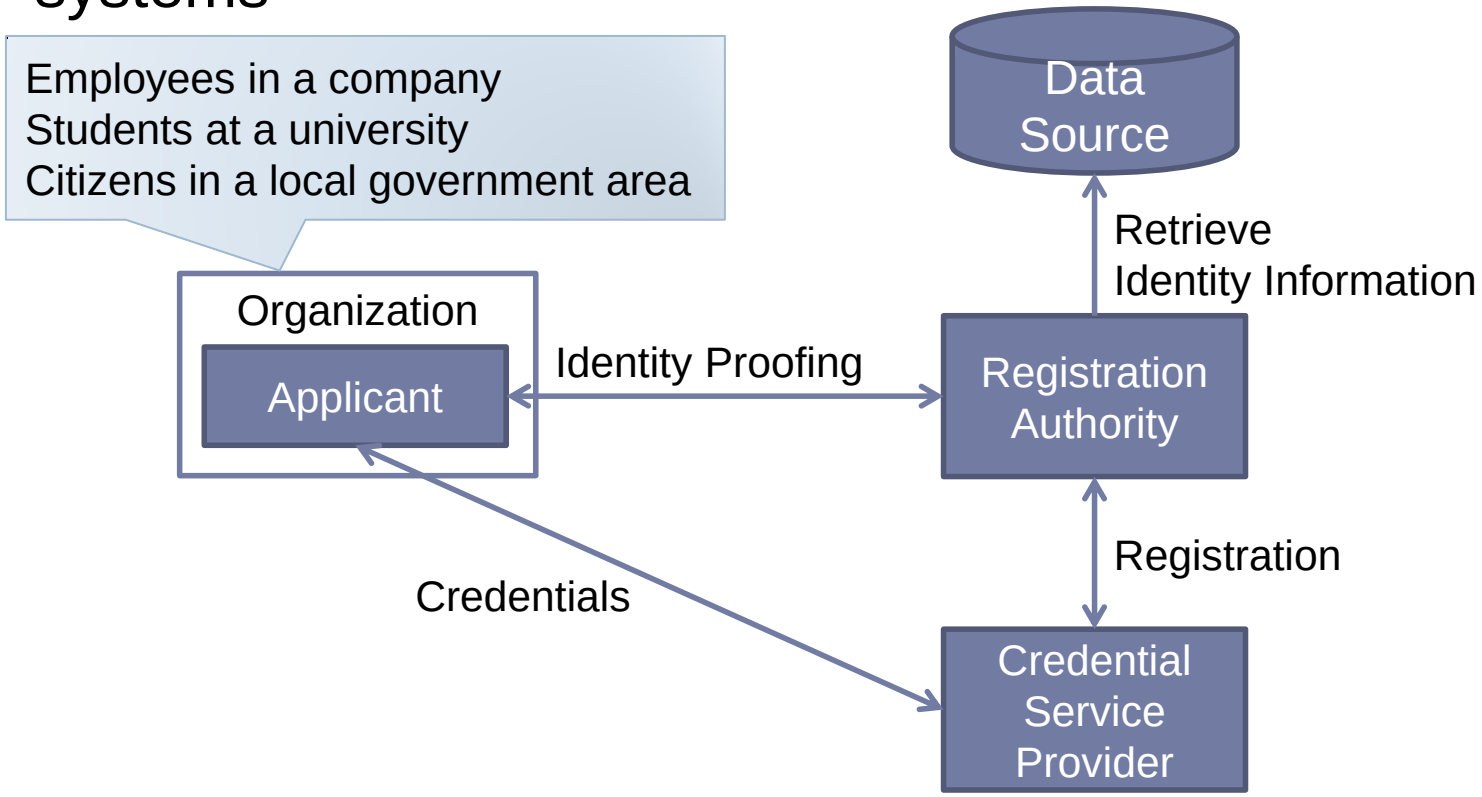
BACKGROUND

Motivations and Objective

- Reducing the operational cost of Identity Management Systems (IdMSs)
  - Several Japanese universities operate campus-wide PKI systems and/or Identity Providers (IdP)
- Quantitative cost structure model is needed
  - For cost estimation, cost evaluation quantitatively
- Our Cost structure model is useful for:
  - designing cost-effective IdMS architectures
  - reducing the cost of running existing operations by readjustment

Identity Proofing

- Process of binding a digital identifier to a real-world entity
- One of key processes in IdMS, especially Authentication systems



Related Works

- Labor Cost structure analysis of PKI (Tanimoto et al.[3,4])
  - Identity proofing is high man-hour rates in operational cost
  - No model developed
- Risk-based security assessment (Argyroudis et al.[17])
  - Security of PKI depends on identity proofing
  - PKI operation costs increases with stricter identity proofing
- Probabilistic model for evaluating operational cost of PKI-based financial transactions(Platis et al.[18])
  - Focused on only revocation and verification process
- Other studies focus on the cost of PKI/IdMS [19-22]
  - Revocation, trust relationship, authentication methods or protocols
  - No study focusing on identity proofing

QUALITATIVE ANALYSIS

Registration Authority types

	Remote RA	Local RA
Identity Proofing Method	Via online channel (e.g., commercial CA for server certs)	With applicant in-person (e.g., enterprise PKI/IdMS)
Location	Outside of organization	Inside of organization
Pros	High labor-efficiency A few operators	Various data sources
Cons	Few data sources	Low Labor efficiency Number of operators
Ideal Use Case	Low operational cost, regardless of data sources	Flexible option of data sources, regardless of operational cost

Data Sources

- Repository of applicants' identity information
- Verification of claimed information is essential
- Authoritative information should be captured

	External resources	Internal resources
Location	Outside of organization	Inside of organization
Accessibility	Both RA	Local RA > Remote RA

Operational cost

- Remote RA
  - Major factors
    - Access cost of data sources per transaction
    - Number of transactions
  - Negligible factors
    - Number of operators
- Local RA
  - Major factors
    - Number of operators
    - Number of transactions
  - Negligible factors
    - Access cost of internal data sources

PROPOSAL

Basic model

$$C = C_u * n + C_k * p$$

C: annual operation cost for identity proofing per CSP

C_u: annual labor cost per operator
Fixed cost, and independent of the number of transactions

C_k: annual non-labor cost per transaction
Transactional cost, and independent of the number of operators
For example, the access charge for a commercial DB

n: number of operators

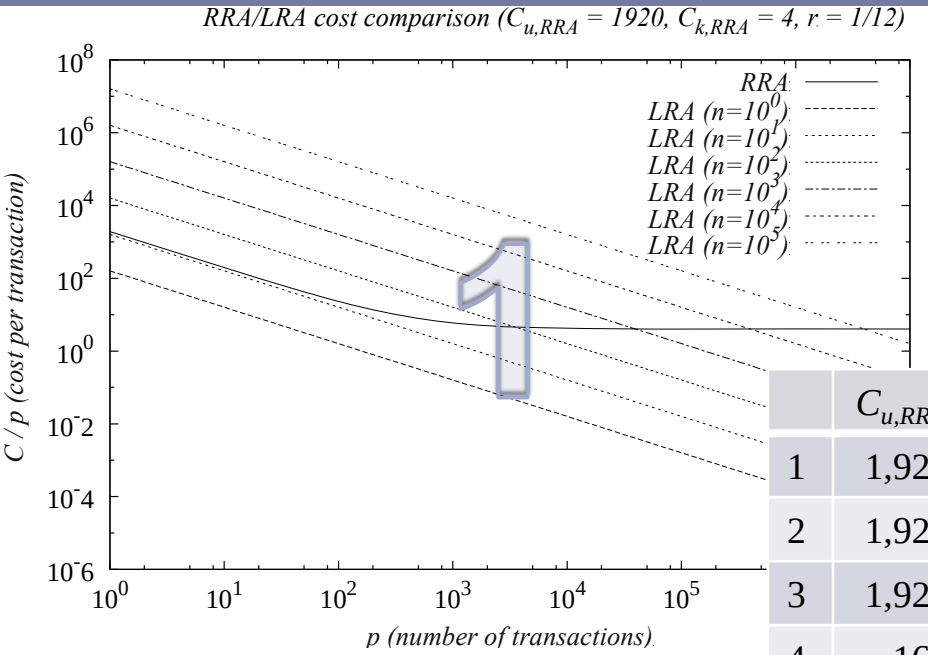
p: number of transactions

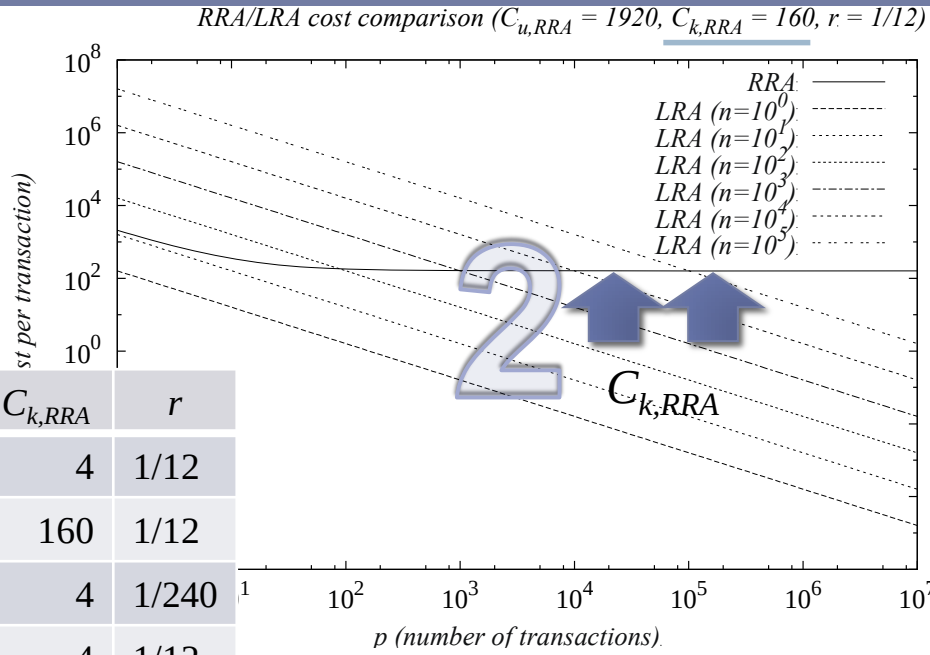
Transaction cost for each RA type

$$C_{RRA}/p = C_{u,RRA}/p + C_{k,RRA}$$

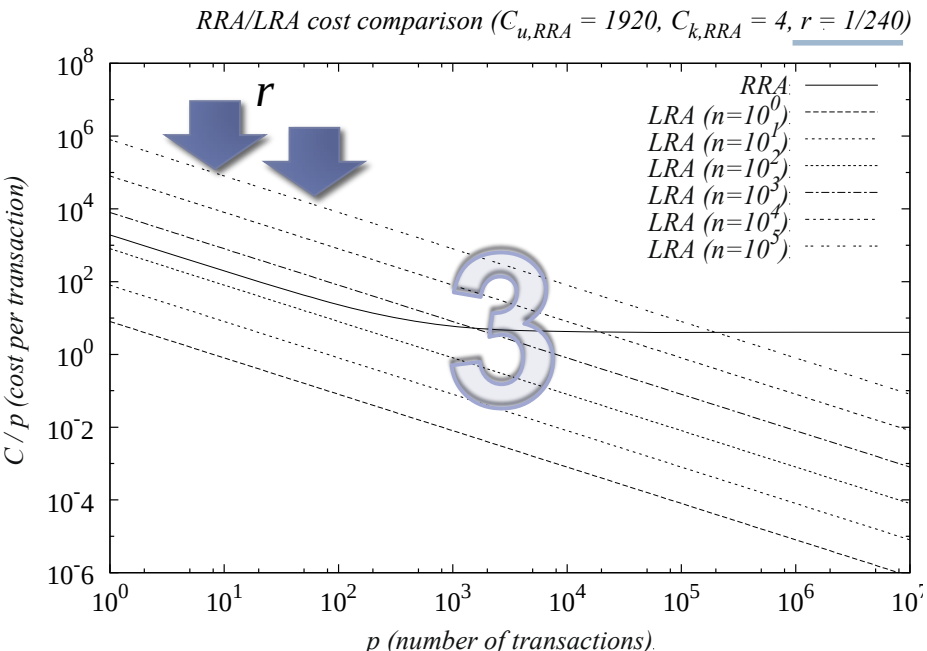
$C_{LRA}/p = C_{u,RRA} * r * n/p$, where r is the ratio of work effort between $C_{u,RRA}$ and $C_{u,LRA}$

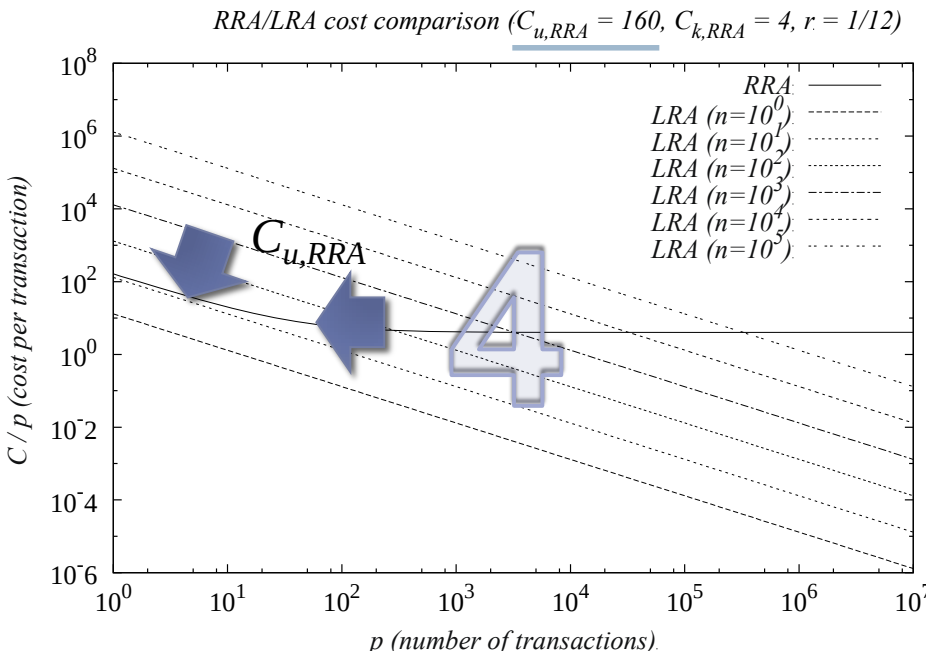
- Assumptions
  - RRA:
    $n = 1$, since $n << C_{k,RRA}$ when p is large
  - LRA:
    $C_{u,LRA}$ is smaller than $C_{u,RRA}$
    $C_{k,LRA}$ is negligible, since $C_{k,RRA} >> C_{k,LRA}$





	$C_{u,RRA}$	$C_{k,RRA}$	r
1	1,920	4	1/12
2	1,920	160	1/12
3	1,920	4	1/240
4	160	4	1/12





Reasonability of Base Parameters

- $C_{u,RRA}$ = *1,920 man-hours*
  - Cost per person per year for a full-time operator to perform identity proofing
- $C_{k,RRA}$ = *4 man-hours*
  - Derived from the following:
    - Representative price of a commercial server certificate: 62,500JPY
    - Cost rate of a certificate is 0.8, and half of the cost is $C_{k,RRA}$
    - Cost of remote RA operator: 6,250JPY /man-hour
- *r = 1/12*
  - Assumes a local RA operator works 160 hours per year per person to perform identity proofing

Evaluations

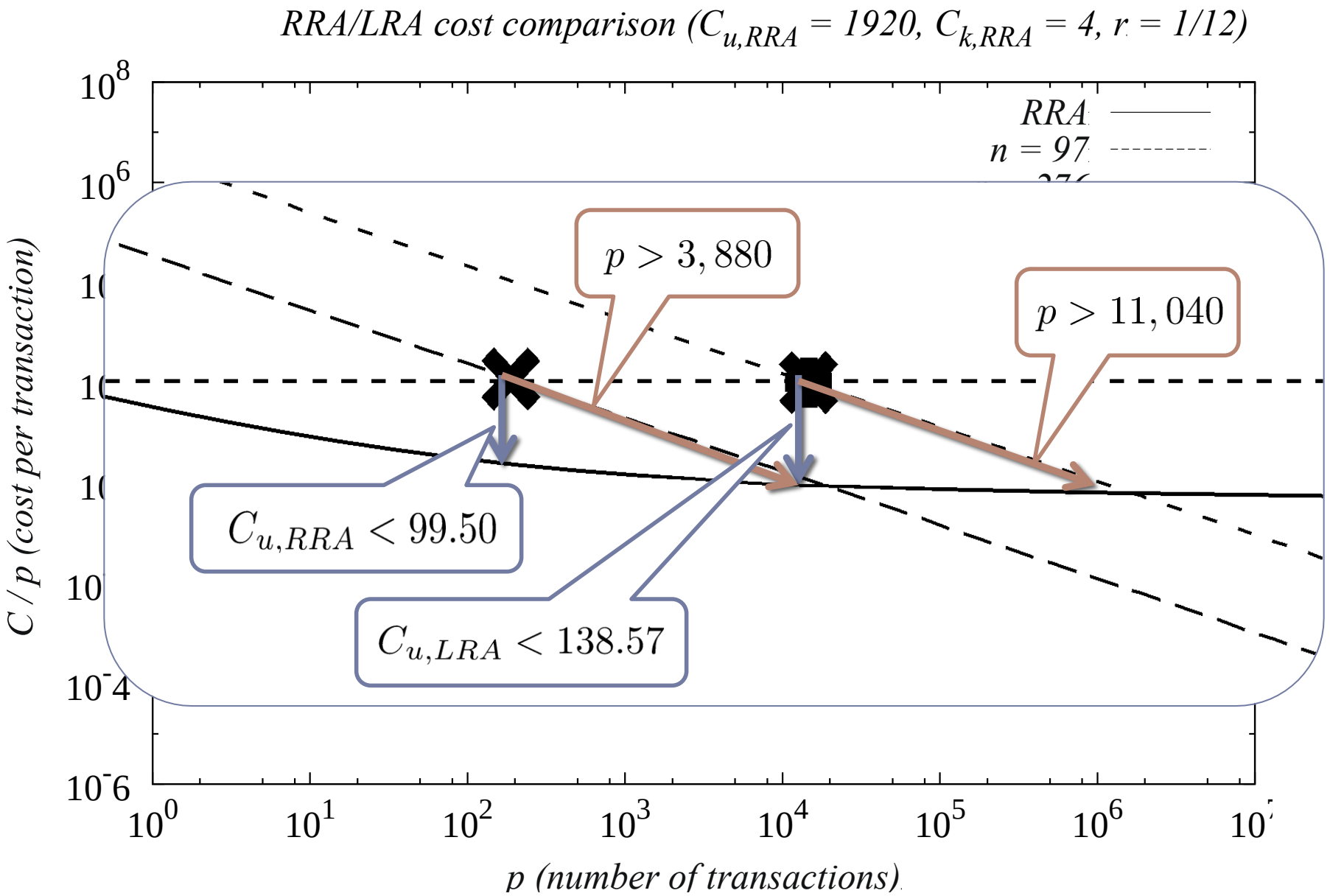
- Remote RAs have the cost advantage when
  - $n > 1$ and small p, depending on n
- Local RAs have the cost advantage when:
  - Small p as $C_{k,RRA}$ increases (2nd figure)
  - Small p and large n as r decreases (3rd figure)
  - Small p as $C_{u,RRA}$ decreases (4th figure)
- Both RA types can reduce C / p as $C_{u,RRA}$ decreases(4th figure)

DISCUSSIONS

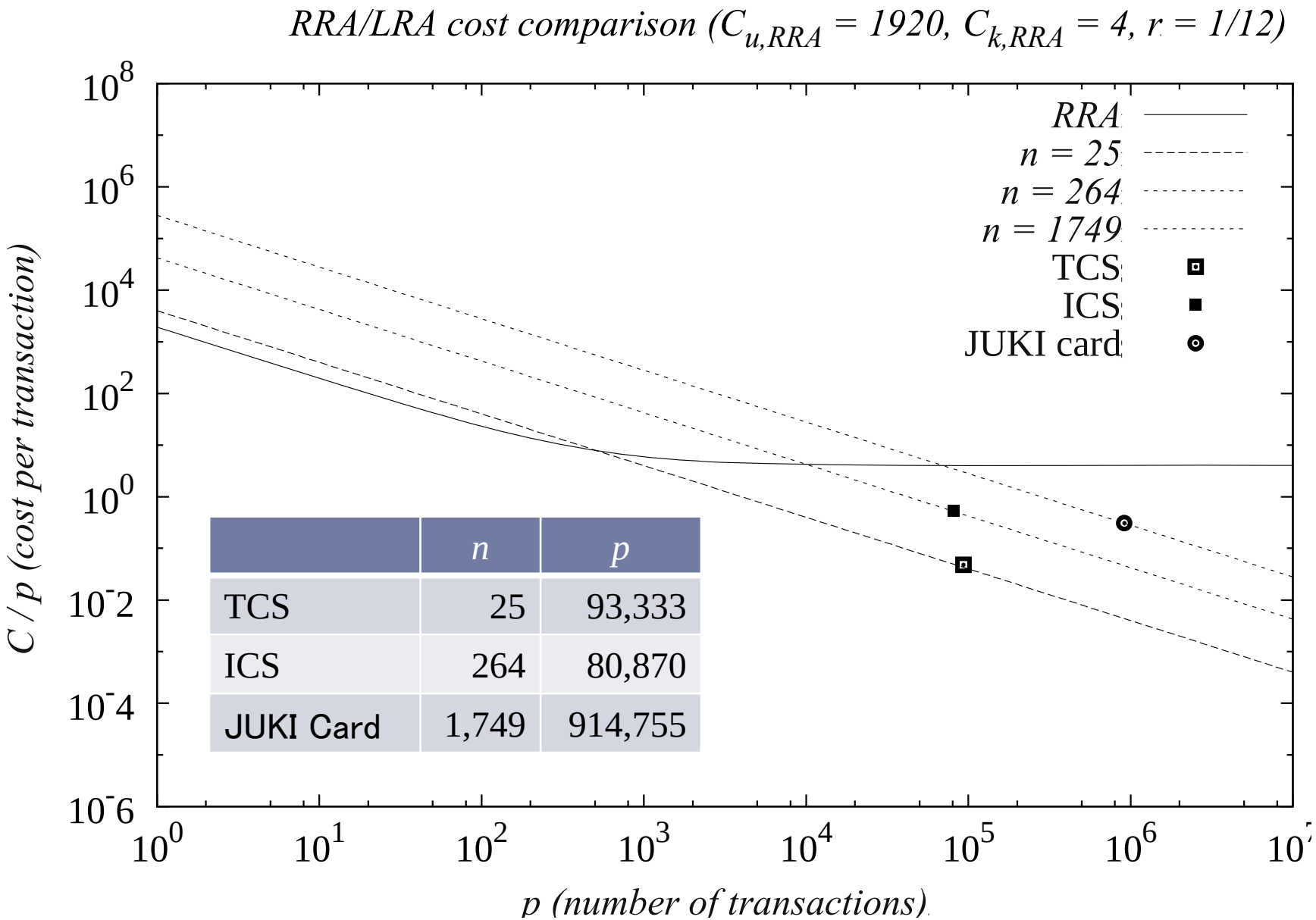
Validity of the model

- Existing CSPs used to validate our model:
  - University PKI (UPKI) Project
    - Operated by National Institute of Informatics in Japan
    - Issues server certificates to academic institutions in Japan
  - TERENA Certificate Service (TCS)
    - Operated by TERENA in Europe (basically)
    - Issues server certificates to institutions participating in TERENA
  - InCommon Certificate Service (ICS)
    - Operated by InCommon in North America
    - Issues server certificates to institutions participating in InCommon
  - JUKI Card
    - Operated by Japanese local government
    - National ID Card for interested Japanese citizens

Modeling the UPKI Project



Modeling TCS, ICS, JUKI card



	n	p
TCS	25	93,333
ICS	264	80,870
JUKI Card	1,749	914,755

Applications

- Simulate variable changes for an existing RA to minimize cost

- Minimize local RA costs by:
  - Increase p to satisfy the following inequality:
    - $\Delta n * C_{u,RRA} * r / C_{k,RRA} < \Delta p$
  - Decrease r without increasing p
- Minimize remote RA costs by:
  - decrease $C_{k,RRA}$

- On a new IdMS, estimate the break-even point of:
  - $C_{k,RRA}$ for a remote RA
  - p or n for a local RA

Conclusion

- Proposed the cost structure model of identity proofing
- Evaluated its applicability by modeling some existing CSPs

- The proposed model is applicable not only to PKIs, but also to other IdMSs.
- Our model is useful as:
  - A tool for optimizing the cost-performance of an IdMS that is constrained by its choice of RA type
  - A quantitative method for evaluating and comparing existing systems

Future Work

- Horizontal Improvements
  - Verify the applicability of our model by applying to other large-scale IdMS
- Vertical Improvements
  - Improve the details of our model by introducing more parameters representing an actual system

Questions?