

PHILIPS

sense **and** simplicity

Portable reputation: Proving ownership of reputations across portals

Sandeep S. Kumar & Paul Koster

Information & System Security Group, Philips Research


September 09, 2009

Reputation locked in portals

Congratulations, you've reached Level 2 [Inbox](#) | [X](#)

Yahoo! Answers to xian

[Take me to Yahoo! Answers...](#)



YAHOO! ANSWERS

Clin
Con
 You
 you
 the exclusive group of folks who can rate questions and answers! Check out the chart below. The next step is Level 3, so get those fingers movin'!

[Take me to Yahoo! Answers](#)

Thanks for sharing what you know with the world!
The Yahoo! Answers Team

YOUR NEXT LEVEL IS RIGHT AROUND THE CORNER.

Level	Points Range	Ratings you can give per day	Votes you can give per day	Questions you can ask per day	Answers you can give per day	Comments you can make per day
7	25000+	unlimited	100	unlimited	unlimited	unlimited
6	10000 - 24999	unlimited	100	unlimited	unlimited	unlimited
5	5000 - 9999	unlimited	100	unlimited	unlimited	unlimited
4	2500 - 4999	unlimited	80	20	80	40
3	1000 - 2499	unlimited	60	15	60	30
2	250 - 999	unlimited	40	10	40	20
1	1 - 249	0	20	5	20	10

[Get easy, one click access to your favorites. Make Yahoo! your home page.](#)

Member Profile: 

Feedback Score: 246466
Positive Feedback: 98.1%

Members who left a positive: 251054
 Members who left a negative: 4794
 All positive feedback received: 465634

[Learn about](#) what these numbers mean.

Recent Ratings:

	Past Month	Past 6 Months	Past 12 Months
positive	27322	148302	313701
neutral	618	3127	5053
negative	613	3129	4523

Bid Retractions (Past 6 months): 0







Member since: May-20-04
 Location: United States

- [ID History](#)
- [Items for Sale](#)
- [Visit my Store](#)
- [Add to Favorite Sellers](#)
- [Learn more About Me](#)
- [View my Reviews & Guides](#)

Amazon's Top Customer Reviewers
 The top reviewers have helped millions of their fellow customers make informed purchase decisions on Amazon.com with their consistently helpful, high-quality reviews. Take a minute to explore the reviews written by these customers. They will amaze you.

New Reviewer Rank | **Classic Reviewer Rank**

10,000 customer reviewers | [Previous](#) | [1](#) | [2](#) | ... | [1000](#) | [Next](#) | Sorted by rank (high to low)

Rank	Customer Reviewer	Total Reviews	Helpful Votes	Percent Helpful	Fan Voters
#1	 Mark See all 473 reviews	473	10,568	95%	796
#2	 Beth Cholette See all 1,304 reviews	1,304	14,394	92%	346
#3	 Joanna Daneman See all 2,524 reviews	2,524	41,467	91%	981
#4	 Rebecca Johnson Rebecca Johnson "SeasonedwithLove.com" (Washington State) <small>TOP 10 REVIEWER REAL NAME™ COMMUNITY FORUM 04</small> Contributions Reviews (4,009) · Lists (5) · Guides (7) · Images (34) Helpful votes received on contributions: 89% (32,612 of 36,647) Most used tags (interests in products) spa girl, fitness lifestyle, poetry, music collection, cookbook, kitchen essentials, pretty in pink, marriage... See profile Add to Interesting People	4,009	31,908	89%	960
#5				92%	886
#6				92%	675

- Classic Reviewer Rank**
 Our leaders sorted by the classic
- [Harriet Klausner](#)
 - [Lawrance M. Bernabo](#)
 - [Gail Cooke](#)
 - [Grady Harp](#)
 - [Rebecca Johnson](#)
 - [Donald Mitchell](#)
 - [E. A Solinas](#)
 - [Joanna Daneman](#)
 - [FrKurt Messick](#)
 - [Marc Ruby™](#)

Have questions about Top Reviewers? [Learn more](#)

Please do not reply to this message. This is a service email related to your use of Yahoo! Answers. To learn more about Yahoo!'s user information, including the use of [web beacons](#) in HTML-based email, please read our [Privacy Policy](#). Yahoo! Answers is located at 70 Sunnyvale, CA 94089.
 Copyright © 2007 Yahoo! Inc. All rights reserved. [Terms of Service](#).

How does a Reputation System work?

What is reputation?
Historic behavior

Reputation Systems

- Collect historic behavior
- Aggregate
- Distribute

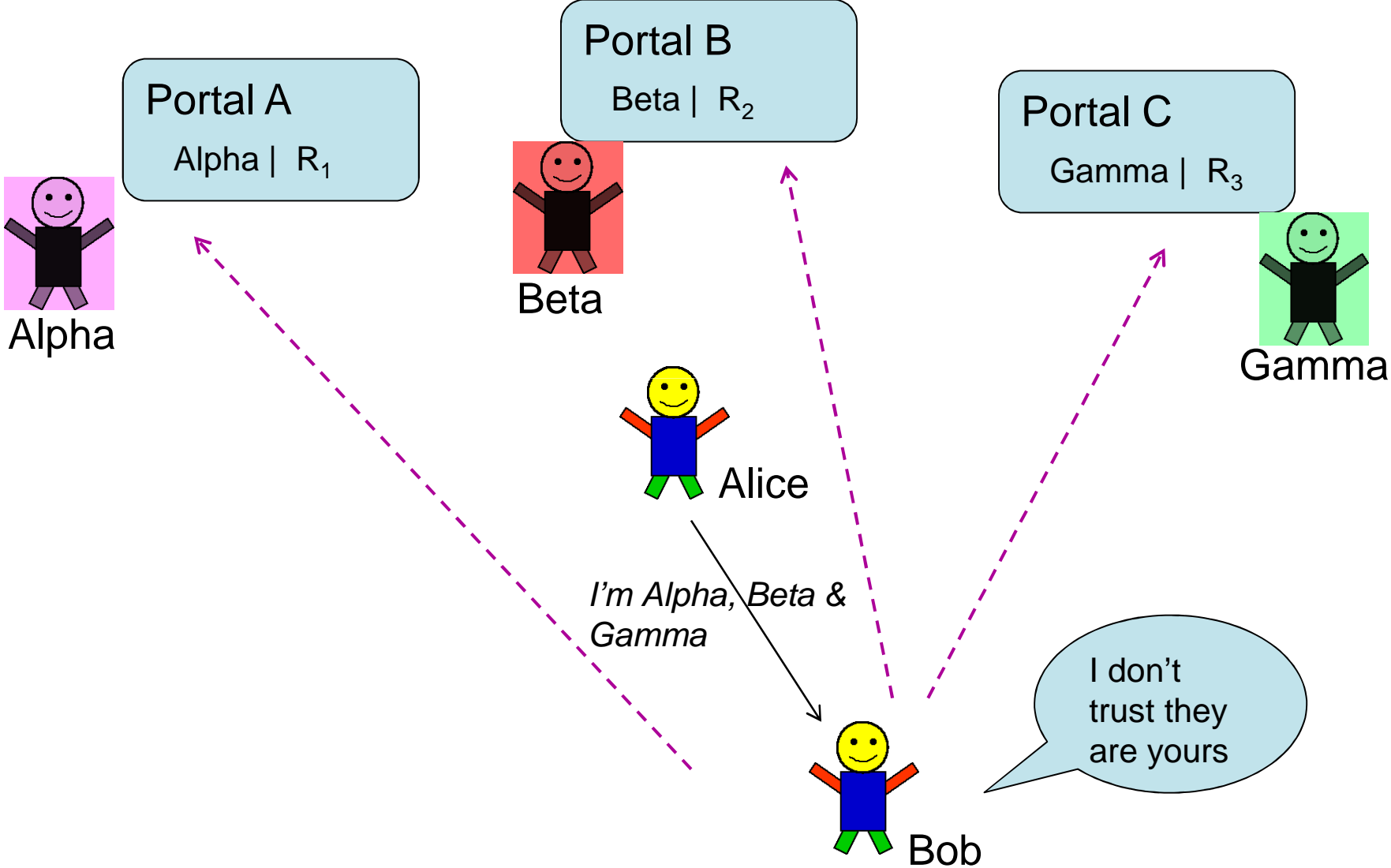
Different reputation system frameworks with different parameters



The reputation dilemma

- Reputation is an important (valuable) ingredient for creation of trust
- Positive reputation is a hard earned
 - Over long time
 - By consistent behavior
 - Observed and guaranteed by a 3rd party (the portal)
- Unfortunately
 - Use of new portals require users to start with no reputation
 - Locks users to their existing portal
- Good for portals ↔ Bad for users

Scenario sketch: Portable reputation



Problem : Portable reputation

- Users would like to combine all their (little positive) reputations at multiple portals to show their trustworthiness
 - All portals cannot be practically expected to use a single Federated Identity provider
 - Portals (often competing) will not actively co-operate in transfer of reputation ratings.
- For privacy reasons, users would ideally not like all his pseudonyms linked by anyone but only the party he intends to interact

Solution sketch: Portable reputation

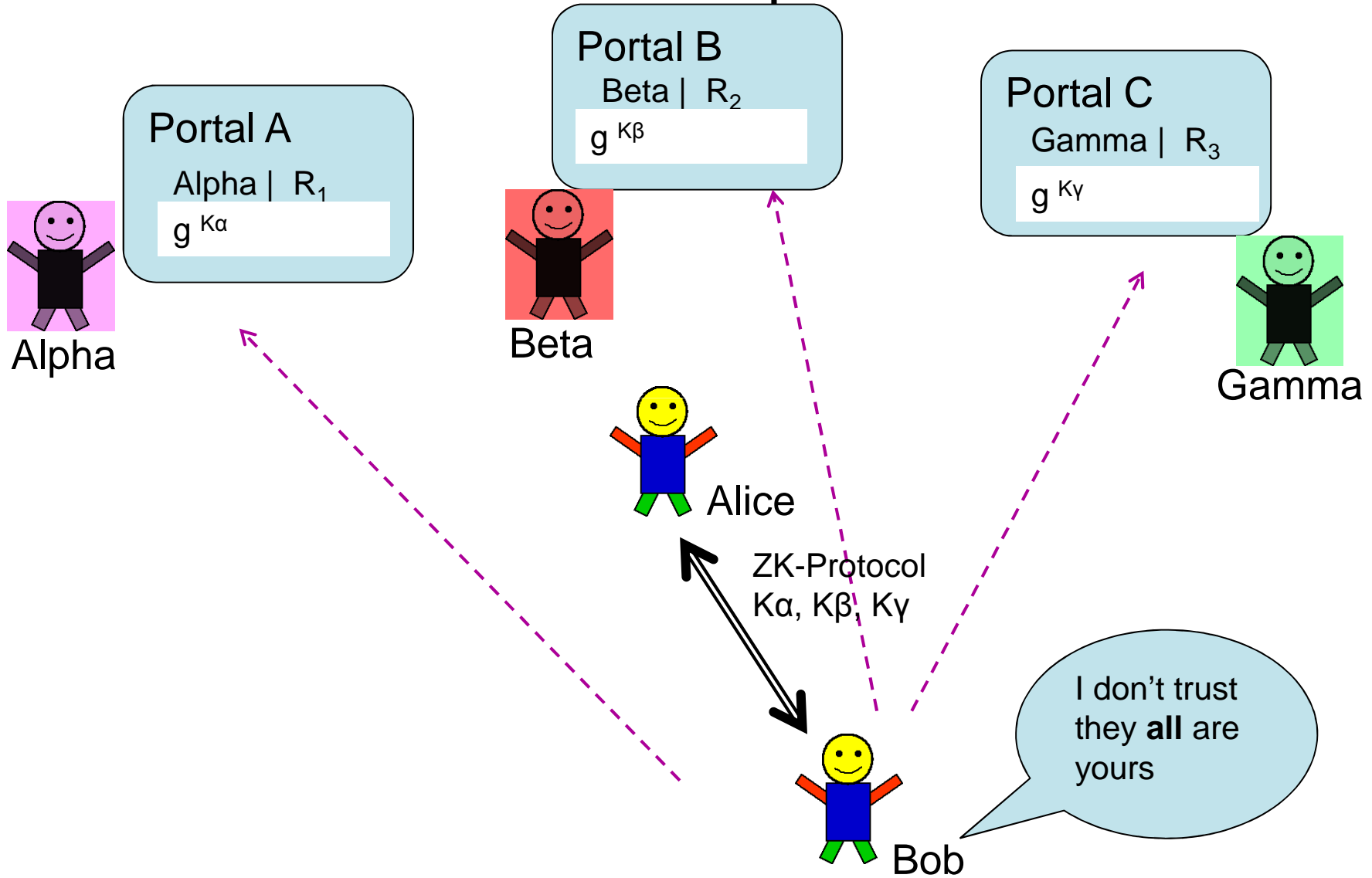
Map problem of portable reputation to the problem of proving ownership of pseudonyms at the different portals

Leave aggregation and weights to attach to each individual reputation to the receiving party.

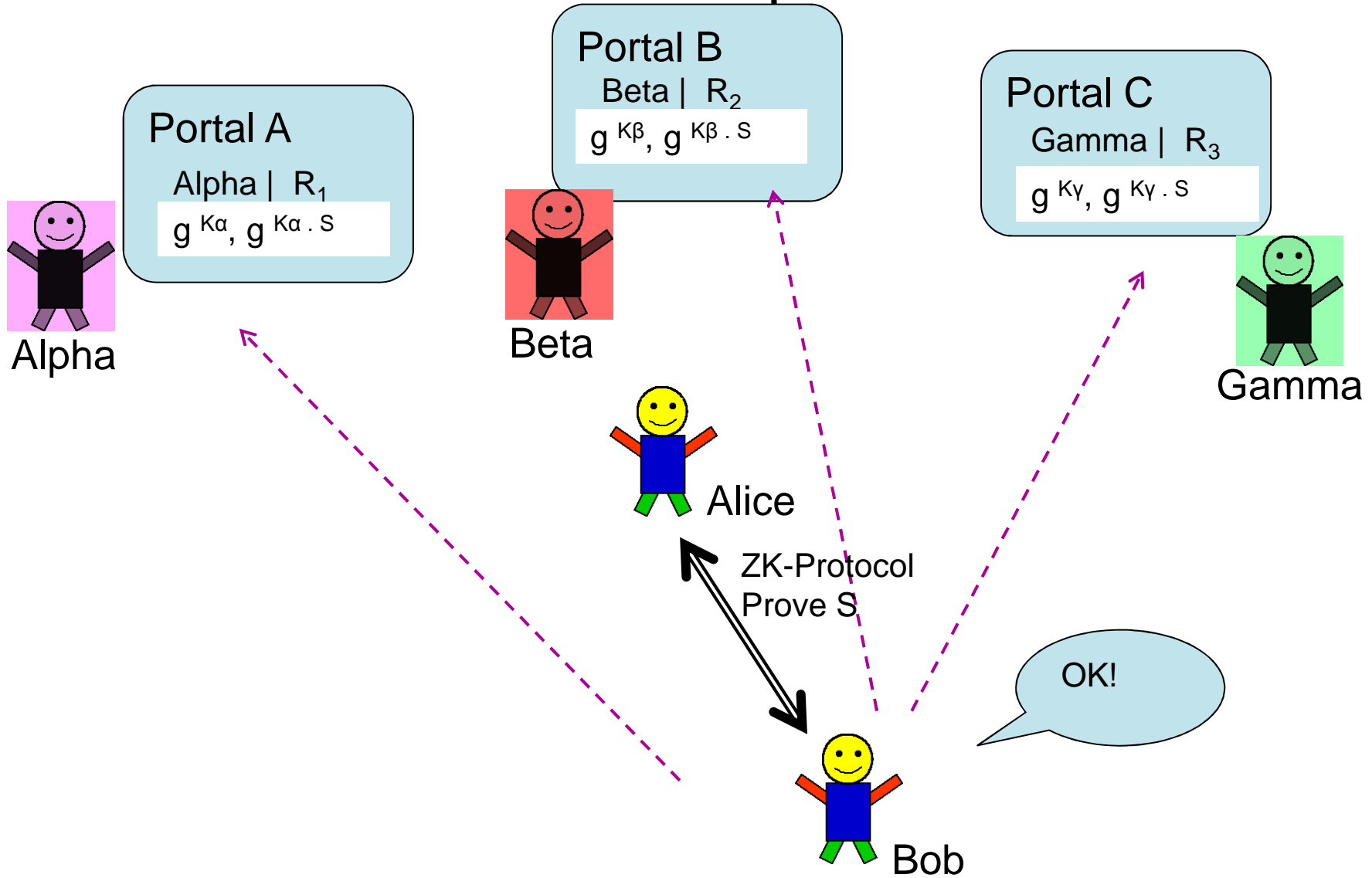
Cryptographic prelims - Discrete Log problems

- Given g^m , finding m hard
- Given g^x and g^y , finding g^{xy} hard

Solution sketch: Portable reputation



Solution sketch: Portable reputation



The protocol

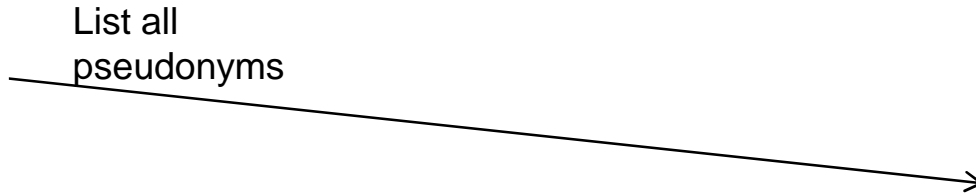
$$C_i = (\hat{c}, \hat{c}) = (g^{K_i}, g^{U_I K_i})$$

Secret K_i and U_I



Alice

List all pseudonyms



fetch



Bob

g^a



$$H[(g^a)^{K_i}] = v_i$$

$$H[(g^{K_i})^a] = \tau_i$$



$$\tau_i = v_i$$



$$H[\omega^{U_I}] = \varphi$$

$$(g^{K_1} * g^{K_2} * \dots * g^{K_n})^b = \omega$$



$$H[(g^{U_I K_1} * g^{U_I K_2} * \dots * g^{U_I K_n})^b] = \rho$$

$$\varphi = \rho$$

Conclusion: Portable reputation

- Allows users to claim their reputation without active cooperation of portals
- Pseudonym privacy by linking is not affected
- Cryptographically secure way to prove reputations actually belong to the user and not borrowed.

PHILIPS

