Transaction Systems with Untraceability

Subodh Sharma

Subhashis Banerjee

IIT Delhi, Computer Science Department

Transaction Systems

Requirements

- Identity verification: provides an answer to the question ”Who are *you*?”.
  - Rests on the notion of digital identity.
  - Common examples: User ID, Public keys, ATM or Smart Cards, Aadhaar, etc.
  - Example of ID verification: KYC
- Authentication: A challenge-response process that provides proof of claim of identity!
  - Common authenticators: Passwds, OTPs, PINS, Private Keys
- The overall mechanism to conduct transactions
  - Transaction confidentiality and integrity
  - Unapproved profiling and tracking
  - Appropriate authorisations to prevent fraud

Fundamental Assumptions for Privacy

- Authentication without consentshould never be possible
- Unapproved profiling, tracking and surveillance of individuals should not be possible
- Unauthorised linking of identities should not be allowed

Digital identity and its verification

- Used in almost every modern digital transaction system: UPI, DBT, etc.
- Each organisation maintains its information to identify its clients.
  - How to trust the digital identity? Assumption that the mapping between the digital identity and the person to whom it belongs is safe! Is that enough?
  - Eg: Banks may seek residence proof to open an account; to rent an apartment one may need show bank account. How do we break this cyclic dependency?
- Even if a trusted ID authority exists:
  - How do we avoid sybils and other forms of fraud?
  - How do we know ensure no excess information is communicated during authentication?
  - How do we avoid organisation to perform linking/tracing w/o consent

Authentication

Message Authentication

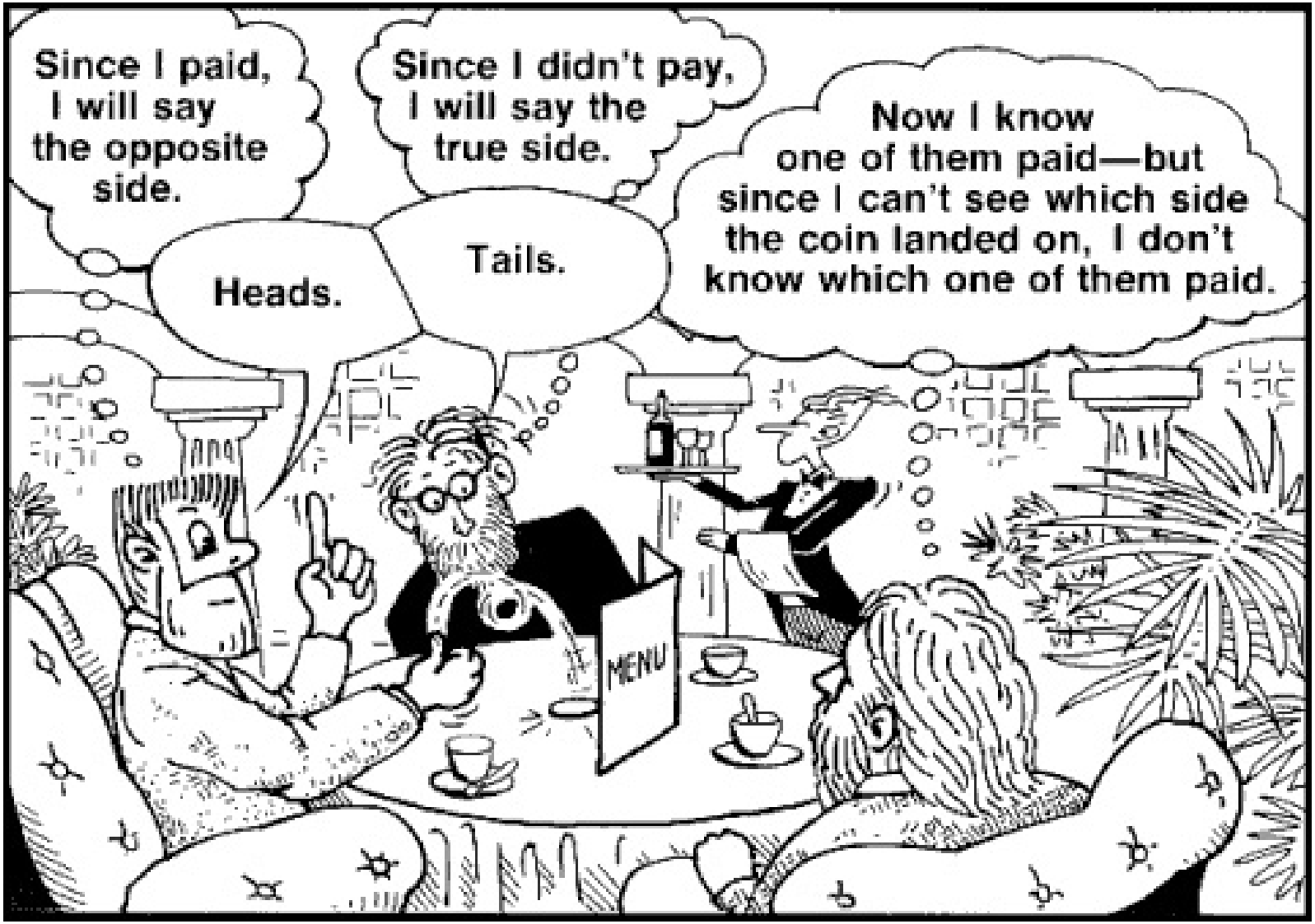
- How to convince a recipient that message was actually sent by the claimed sender and is not tampered
- Message authentication codes (used in private key setting): unforgeable, partial non-repudiation.
- Digital signatures (used in public key setting) in combination with collision-resistant hash functions.
- Challenge-response based authentication protocols such as Kerberos

Problems:

- Exposure of ”tracing information” leading to unapproved linking.

Unconditional Message Traceability

Problem: Preventing messages from being traced to the sender.



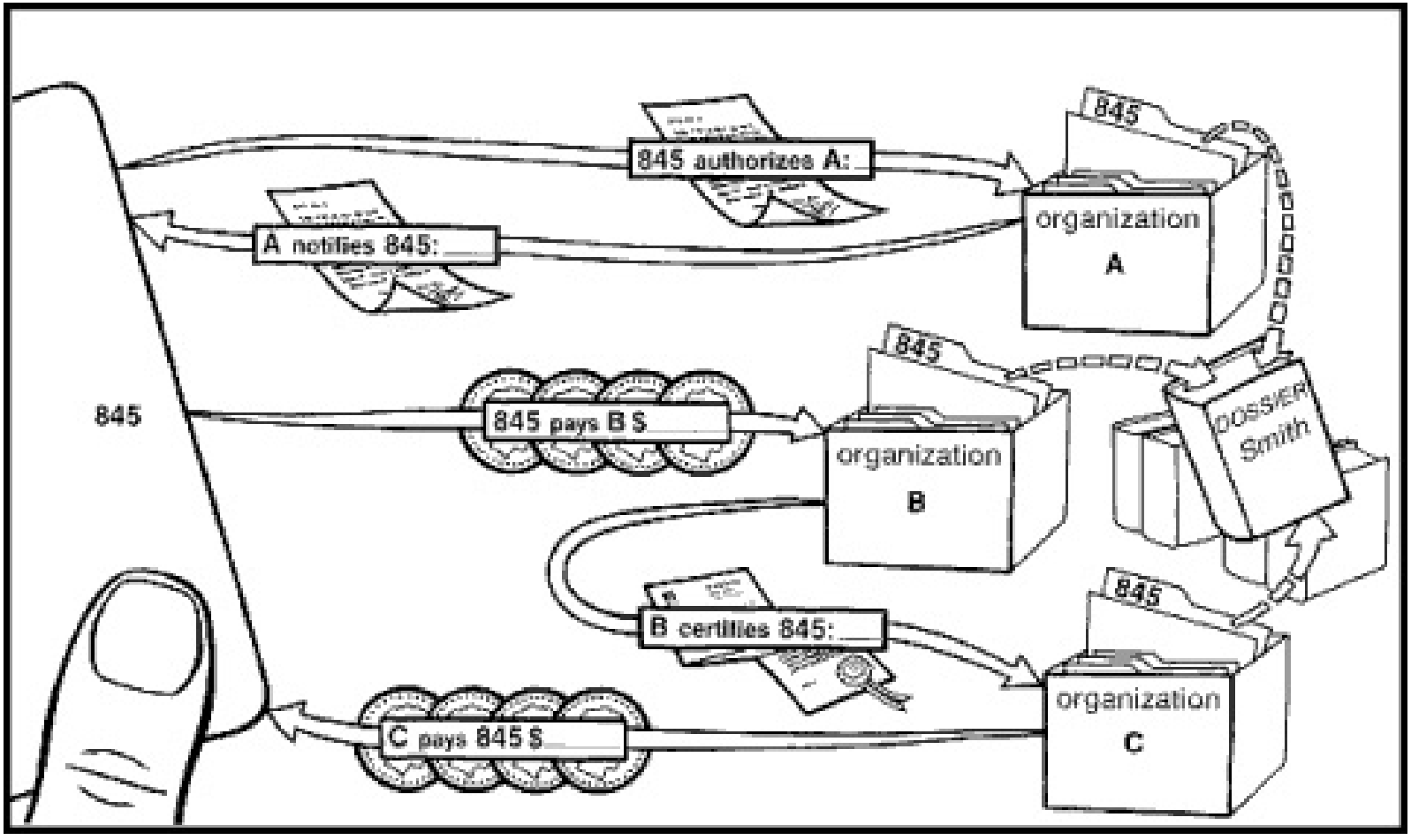
Unconditional Traceability

- Suppose you are invited to dine at a restaurant by two of your friends
- After dinner, the waiter informs that one of you has already paid for the dinner
- If you paid, your friends want to know since they invited you.
- If one of your friends paid, they do not want you to learn which of the two who paid.
- Solution: Your friends flip a coin behind the menu so that they can see but you cannot.
- The one who paid calls out the opposite of the side the coin falls on.
- If both of them call heads/tails, then you have paid.
- This way, the friend who paid sends you an unconditionally untraceable message.

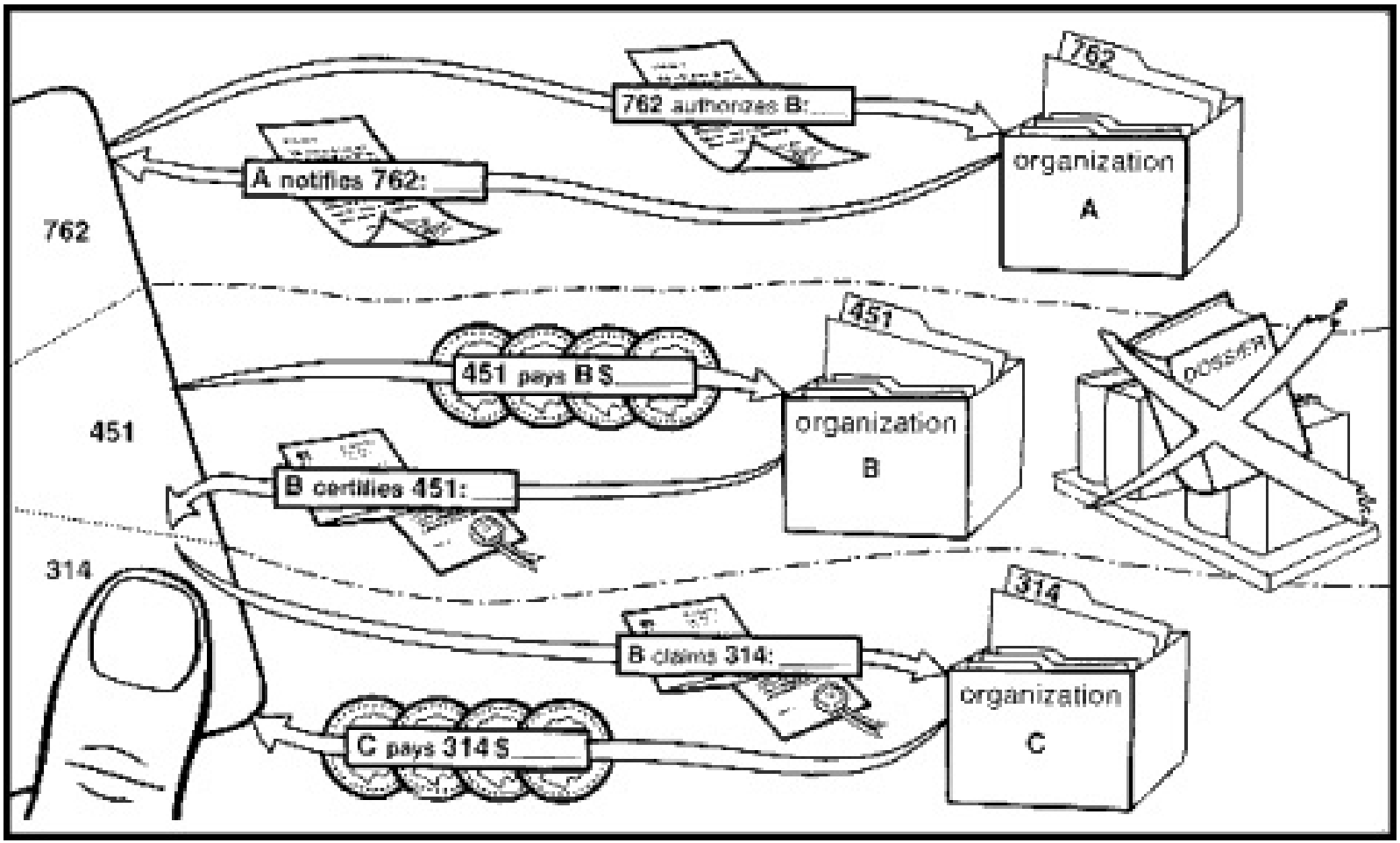
Unconditional Traceability

- Converting this 2-sender 1-receiver system to more general system is provided in: The dining cryptographers problem: Unconditional sender and recipient untraceability. David Chaum
- One such generalization uses additional coins to allow more potential senders at the table, while preventing tracing even by collusion.
- Another breaks long messages into a sequence of parts, each of which is dealt with in a separate round of coin tosses and utterances.

Universal Identifiers

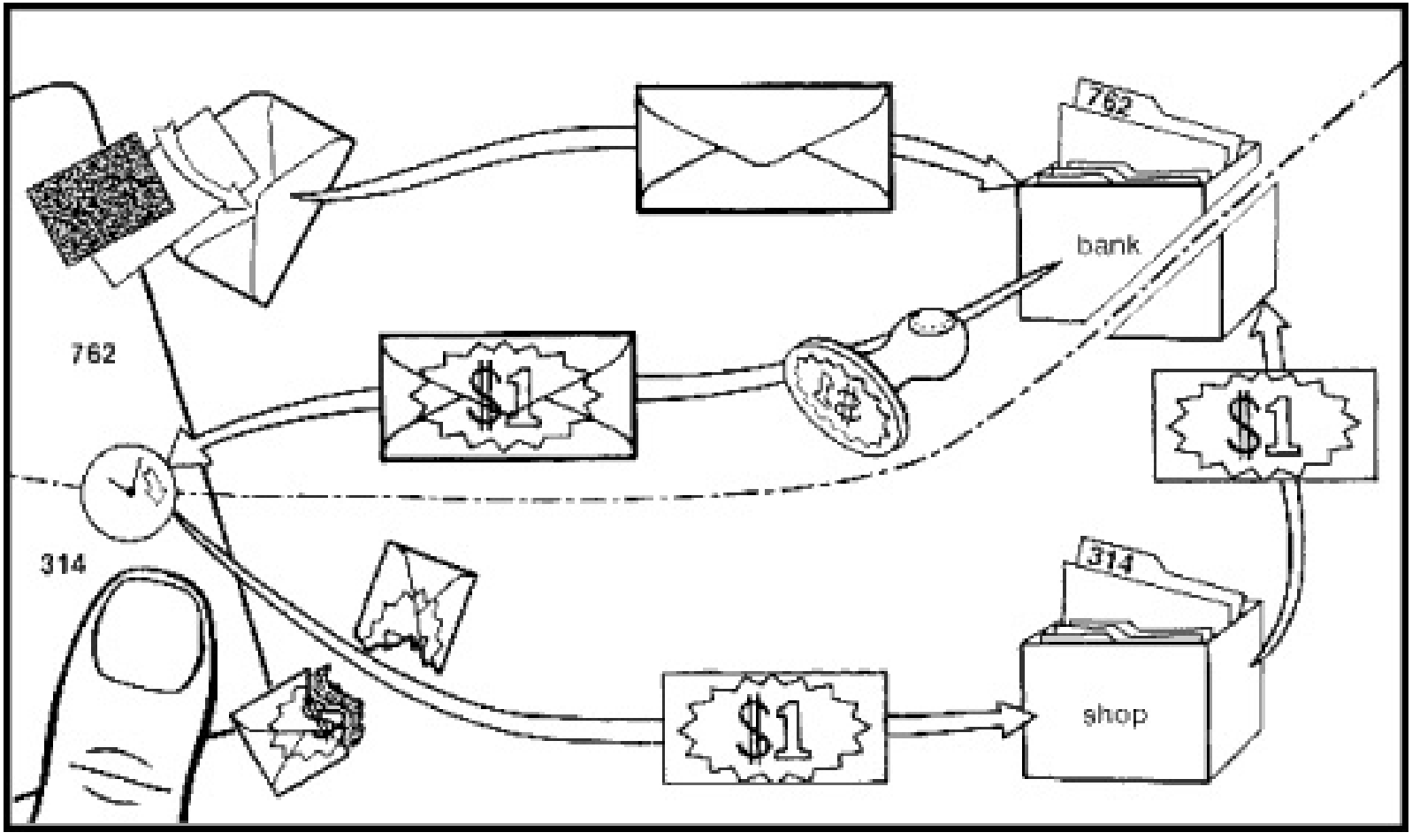


Digital Pseudonyms



Blind Signatures for Untraceable Payments

Consider the analogy:



Blind Signatures for Untraceable Payments

- Suppose that a bank has a special signature mark that it guarantees to be worth one rupee, in the sense that the bank will pay one rupee for any piece of paper with that mark on it
- You take a plain slip of paper sealed in a carbon-lined envelope to the bank and ask to withdraw one ruppe from your account.
- The bank deducts the amount from your account, makes the signature mark on the outside of your envelope, and returns it to you.
- You verify that the signature mark is proper; Later, when you remove the slip from the envelope, it bears the carbon image of the bank's signature mark. You can then buy something for one rupee from a shop, using the signed slip to make payment.
- The shop verifies the carbon image of the bank's signature on the slip before accepting it.

Blind Signatures for Untraceable Payments

Untraceability:

- The bank verifies the signature on the slip submitted for deposit, just as the shop did, and adds a rupee to the shop's account.
- Bank uses the same signature to sign many such envelopes; all slips are "*blinded*" by envelopes; thus. the bank cannot learn from which account the funds were drawn.
- More generally, the bank cannot determine which withdrawal corresponds to which deposit – the payments are untraceable.

Formal Definition of Blind Signature Scheme

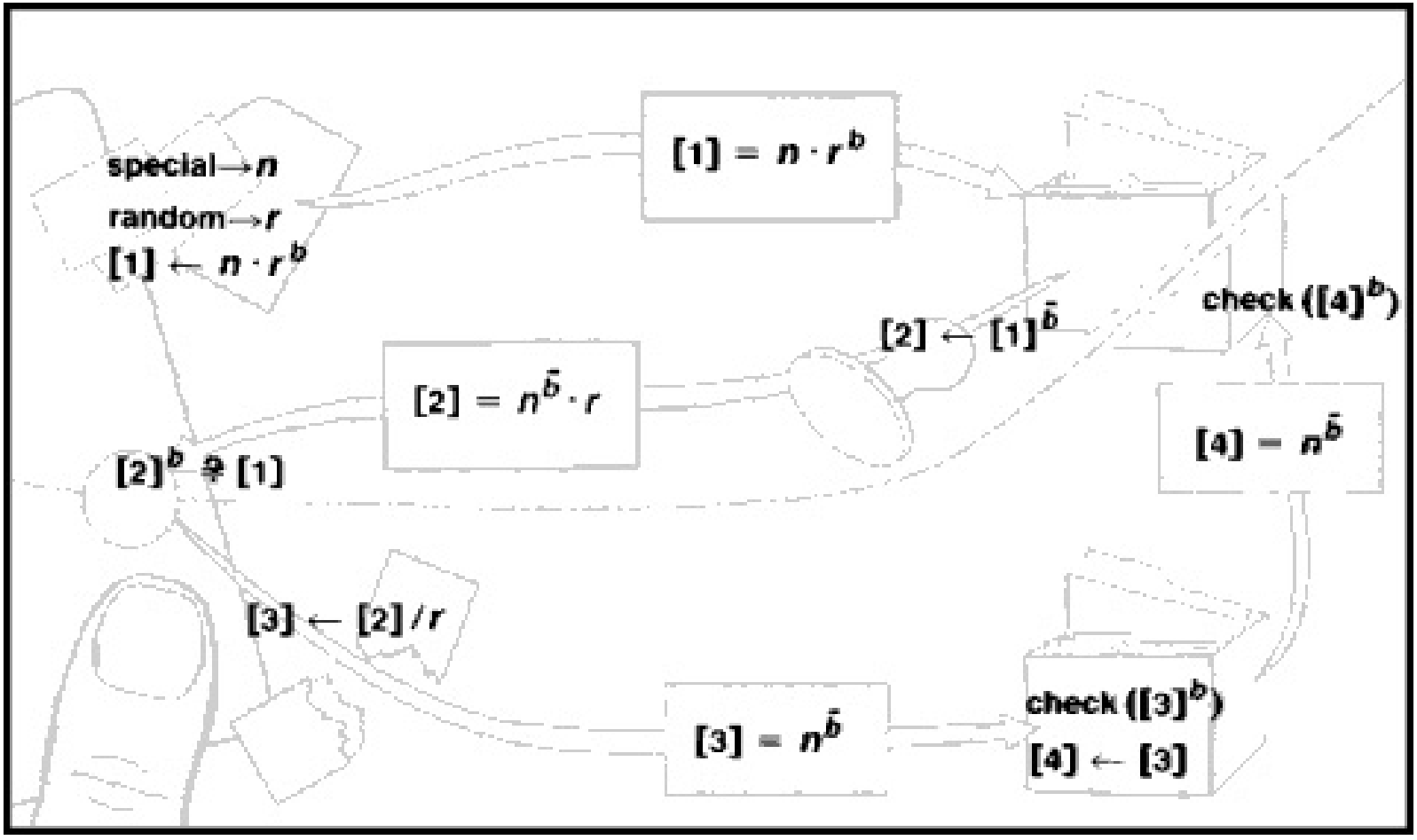
- Key Generation: a P.P.T. algorithm. On input of a security parameter , it outputs a key pair (sk, pk), where sk is the secret key and pk is the public key.
- an interactive and P.P.T. two-party protocol between a signer S and a user U (who receives the signature) with a public key pk as common input. The private input of S is a private key sk, and the private input of U is a message m', which is the blinded version of a message m. At the end of the protocol, U obtains a either the string 'unsuccessful' or a signature σ' on m' as a private output; S obtains the string 'completed' or 'not completed' as private output. U unblinds σ' to obtain σ, the signature on m.
- a deterministic polynomial time algorithm. On input of a message m, a public key pk, and a signature σ, it determines whether σ is a valid signature on with respect to public key pk. If it is valid, the algorithm outputs 'true', otherwise it outputs 'false'

Blind Signature Implementation Using RSA

- S generates public key (e, n) and private key (d, n) using RSA.
- Blinding: U chooses $r \in \mathbb{Z}_n^*$; computes $m' = r^e H(m) \ (mod\ n)$ where $H : \{0,1\}^* \Rightarrow \mathbb{Z}_n^*$ is a one-way hash function.
- Signing: S computes and sends $\sigma' \equiv m'^d \ (mod\ n)$ to U
- Unblinding: U computes $\sigma \equiv \sigma' r^{-1} \ (mod\ n)$
- Verifying: U verifies legitimacy of σ on m by checking whether $\sigma^e \equiv H(m)(mod\ n)$

More efficient scheme was given by Jan Camenisch in 1994 based on Discrete-log problem.

Untraceable Payment with Numbers



Untraceable Payment with Numbers

- First the individual's card computer chooses the digits of n by a physical random process to create the note number n (corresponding to choosing a suitable slip of paper at random in the analogy).
- The card also creates a totally random number r (like choosing an envelope and carbon).
- The card then raises the random number r to the bank's "worth one rupee" public power b, multiplies this by the note number n (like sealing the slip in the envelope), and supplies [1].
- The bank deducts from the account uses the corresponding private power b' to sign the transmission, and returns the result to the card in [2].
- The card verifies that the bank returned exactly the right thing, and obtains the signed note by dividing out the random r (like removing the envelope and carbon).
- The shop checks that [3] is a signed special number, and then forwards a copy [4] to the bank for deposit. The bank checks the signature just as the shop did, and accepts the deposit if the valid note has not already been deposited.

Credential Transactions

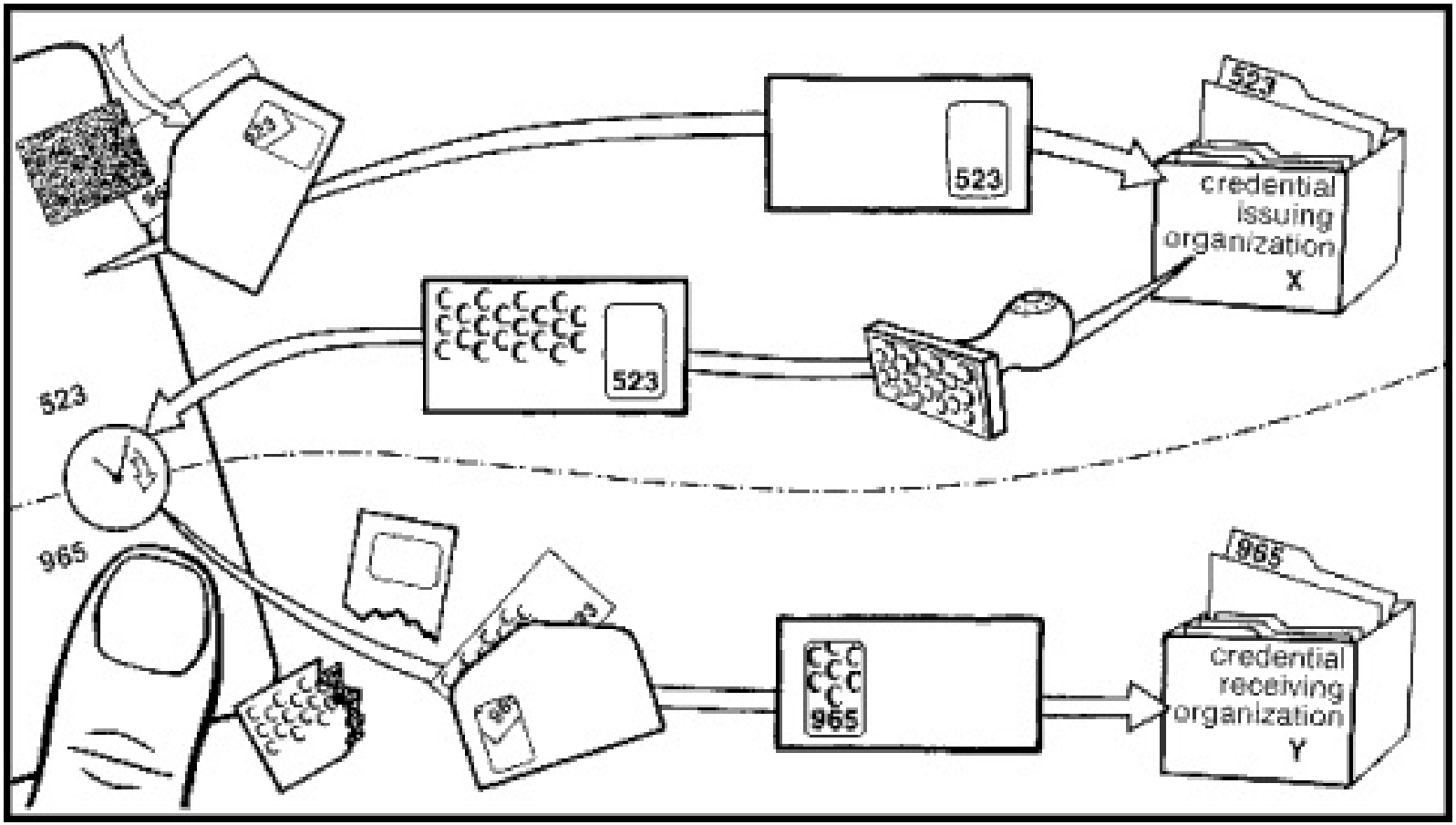
- In their relationships with many organizations, there are legitimate needs for individuals to show credentials. The term ”credentials” is used here to mean statements concerning an individual that are issued by organizations, and are in general shown to other organizations. Eg:?
- Problems:
  - Confirmation of credentials – unnecessary and overly detailed information is demanded. This can be used to link records to certificate holders.
  - Control over credentials that certificates once provided is thus rendered illusory.

Solution

An individual can transform a specially coded credential issued under one pseudonym into a similarly coded form of the same credential, which can be shown under the individual’s other pseudonyms.

Basic Credential System

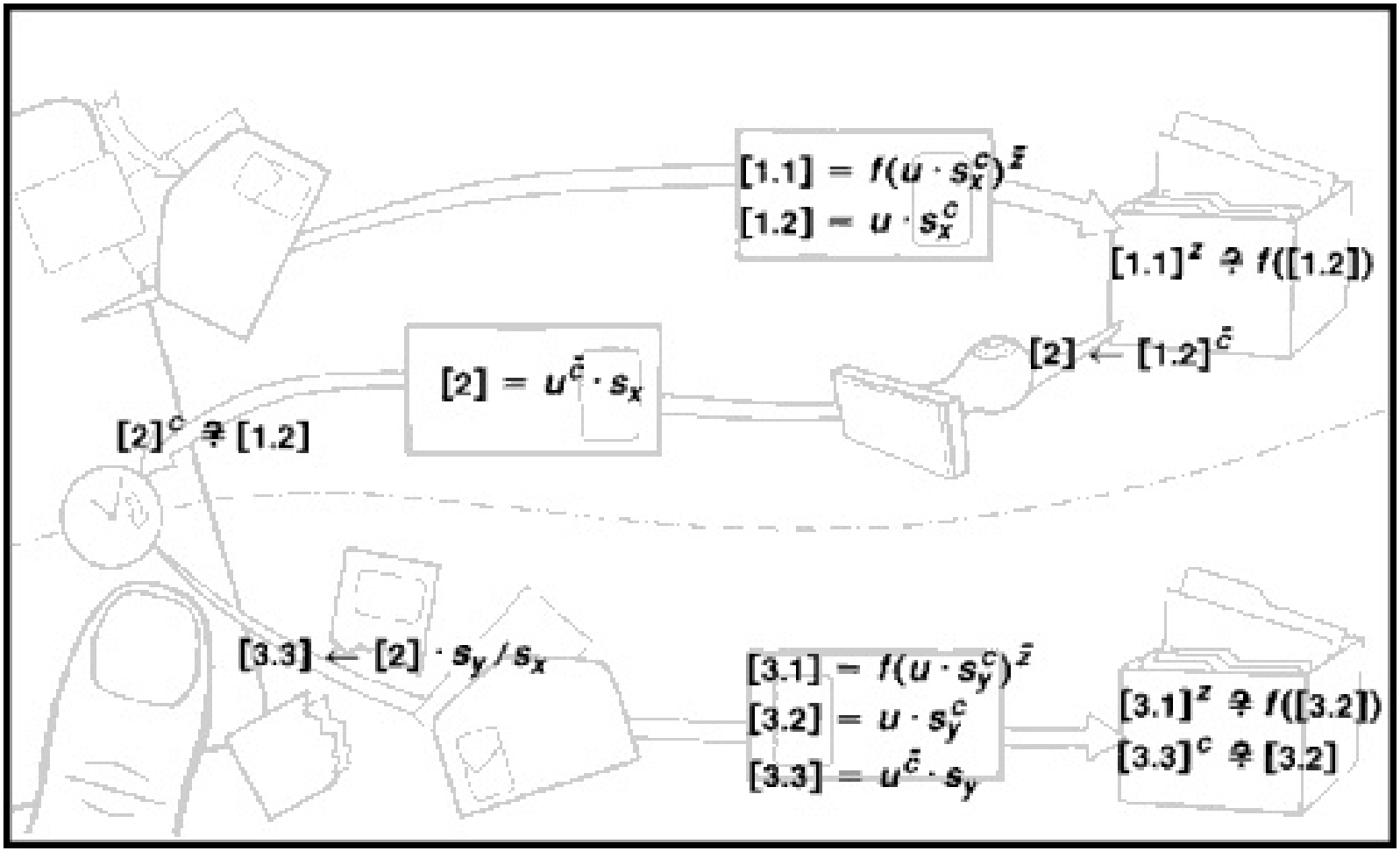
Untraceable Credential Transactions:



Basic Credential System

- Make up numeric pseudonyms at random and write them on a plain slip of paper.
- You put the slip in a carbon-lined envelope with a window exposing only the pseudonym you use with that organization.
- The organization makes a special signature mark in a repeating pattern across the outside of it. This signature pattern is the credential;
- When you get the envelope back from the issuing organization, you verify the credential signature pattern.
- Before showing the credential to another organization, you place the slip in a different envelope with a window position that exposes only the pseudonym you use with that organization, along with some of the adjacent credential signature pattern. The receiving organization can verify, through the window, the pseudonym you use with it as well as the signature pattern.

Untraceable Credential



Discussion on Anonymity

- Unlinkable Anonymity: Organisations cannot map transactions to individuals
- Linkable Anonymity: Allows organisations to identify transactions from the same individual, but the individual's identity is obsucred via *pseudonyms*
- Anonymous credentials: A person can obtain a credential from org. A against their psedunym with A and transform it to identical credential against their pseudonym with org. B.
  - Obtain blind signature from the issuer
  - Use ZKP of knowledge of these signatures to authenticate with a verifier.
- Revoking anonymity under misuse? Are communication channels anonymous? Database anonymisation?

Acknowledgements

- Security without Identification Card Computers to make Big Brother Obsolete Communications of the ACM, vol. 28 no. 10, October 1985 pp. 1030-1044.
- Privacy and security of aadhaar: A computer science perspective September 2017. Economic and political weekly 52(37):93-102