

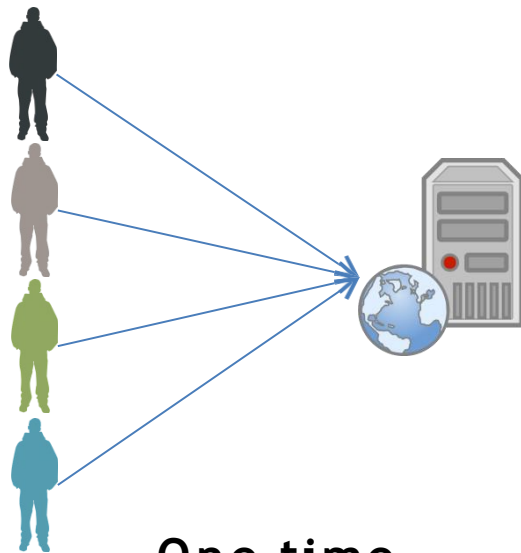
Privacy Enhancing Technologies

Privacy properties: Anonymity

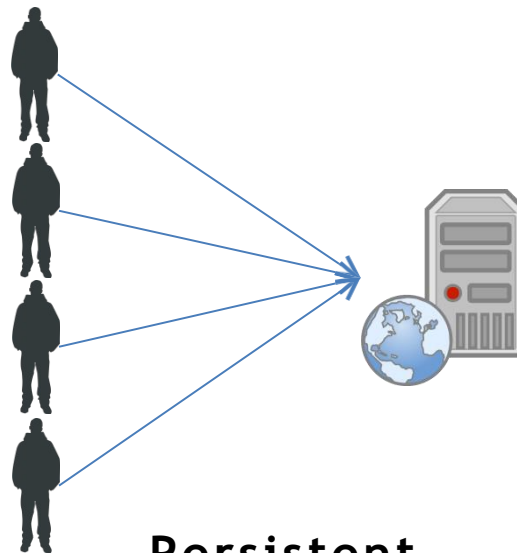
- Hiding link between identity and action/piece of information.
 - Reader of a web page, person accessing a service
 - Sender of an email, writer of a text
 - Person to whom an entry in a database relates
 - Person present in a physical location
- Definitions:
 - Pfitzmann-Hansen (PH) “*Anonymity is the state of being not identifiable within a set of subjects, the anonymity set [...] The anonymity set is the set of all possible subjects who might cause an action*” [[pattern Anonymity set](#)]
 - ISO 29100 “defines anonymity as a characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly”

Privacy properties: Pseudonymity

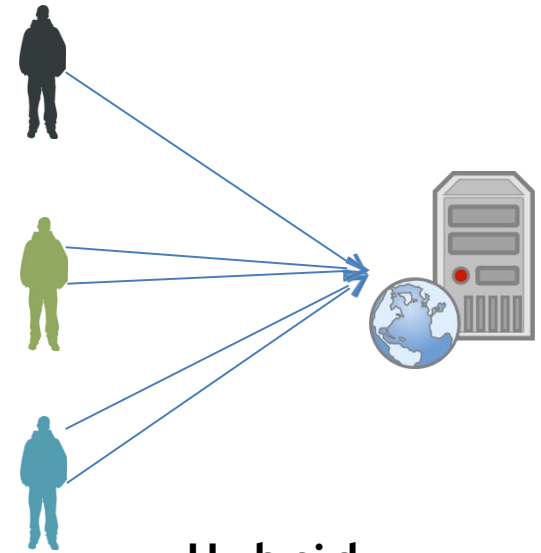
- PH: “Pseudonymity is the use of pseudonyms as IDs [...] A digital pseudonym is a bit string which is unique as ID and which can be used to authenticate the holder” [[pattern Pseudonymous identity](#)]
- ISO15408 “pseudonymity ensures that a user may use a resource or service without disclosing its identity, but can still be accountable for that use. ”



One time
pseudonyms
(Anonymity)



Persistent
pseudonyms
(Identity!)



Hybrid
(Multiple
identities)

Privacy properties: Unlinkability

- Hiding link between two or more actions/identities/info pieces
 - Two anonymous letters written by the same person
 - Two web page visits by the same user
 - Entries in two databases related to the same person
 - Two people related by a friendship link
 - Same person spotted in two locations at different points in time
- Definitions
 - PH “Unlinkability of two or more items means that within a system, these items are no more and no less related than they are related concerning the a-priori knowledge”
 - ISO15408 “unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together”

Privacy properties: Unobservability

Hiding user activity.

- whether someone is accessing a web page
- whether an entry in a database corresponds to a real person
- whether someone or no one is in a given location

Definitions

- PH “*Unobservability is the state of items of interest being indistinguishable from any item of interest at all [...] Sender unobservability then means that it is not noticeable whether any sender within the unobservability set sends.*”
- ISO15408 “unobservability ensures that a user may use a resource or service without others, especially third parties, without being able to observe that the resource or service is being used.”

Privacy properties: **Plausible deniability**

- Not possible to prove a user knows, has done or has said something
 - Off-the-record conversations
 - Resistance to coercion:
 - Not possible to prove that a person has hidden information in a computer
 - Not possible to know that someone has the combination of a safe
 - Possibility to deny having been in a place at a certain point in time
 - Possibility to deny that a database record belongs to a person

Privacy properties

- So far it was about de-coupling identity and actions
- but we could keep identity and hide data
 - Cryptographic security properties
- Differential privacy: a data base looks “almost” the same before and after an event occurs.
 - Special noise

Privacy enhancing technologies

- Technologies that enable users to preserve their privacy
 - In terms of technical properties



- From whom?
 1. Third parties = trust on data controller/processor (or must disclose data)
 - PETs for personal data management [“soft privacy”]
 - Support to Data Protection

Privacy enhancing technologies

- Technologies that enable users to preserve their privacy
 - In terms of technical properties



- From whom?
 1. Third parties = trust on data controller/processor (or must disclose data)
 - PETs for personal data management [“soft privacy”]
 - Support to Data Protection
 2. Data controller/processor = no trust
 - PETs for data disclosure minimization (i.e., minimize trust) [“hard privacy”]

PETs for personal data management

PETs for decision support

- Provide insight in how user's data is being collected, stored, processed and disclosed to the data subject to enable well-informed decisions [[pattern Protection against tracking](#)]
- Transparency-Enhancing Technologies
 - *Google Dashboard*: what personal data is stored and who has access
 - *Collusion (Firefox addon)*: list of entities tracking users
 - *Mozilla Privacy Icons*: simple visual language to make privacy policies more understandable
 - *Privacy Bird (IE Add-on)*: shows user whether webpage complies with her preferred policy based on images
- Challenges
 - How to provide information useful to users
 - How to convey it
 - How to make users understand

PETs for consent support

- Provide users with means to express their privacy preferences and give consent [[pattern Protection against tracking](#)]
- Privacy policies languages (P3P, S4P, SIMPL)
 - Automated processing and comparison with users' preferences
 - Difficult to make unambiguous and inform users (TETs)
 - Difficult to standardize and make them expressive
- Anti-tracking
 - Do Not Track options
 - Browser tag expressing who can collect personal data
 - Track Me Not plugin
 - Renders collection useless

PETs for enforcement support

- Provide users with means to enforce their preferences
- Locally “easy”: blockers (pop-ups, ads, cookies,...)
- Remotely
 - Sticky policies associated to data(e.g., trusted third party stores encryption keys only disclosed in certain cases)
 - Use of trusted hardware (HSMs, TPMs) to process data “out” of the server’s control

PETs for accountability support

- Data controllers should be able to demonstrate compliance with Data Protection.
- Non repudiable logs
 - Backups, distributed logging
 - Forward integrity (hash chains)
- Verifiable Audits
 - Automated tools for log audits

Data Management vs. Minimization

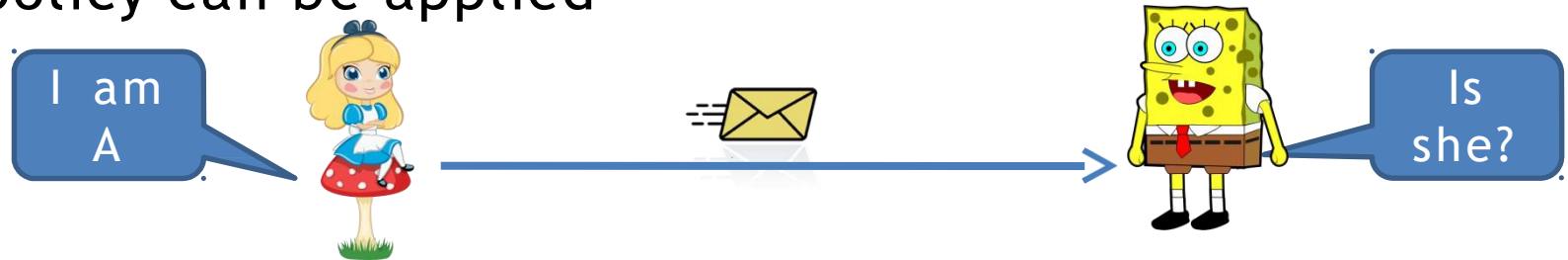
- Previous techniques are applied once personal data has been disclosed
- Aim at:
 - Help the user understand and decide
 - Make data controllers more responsible
- But they cannot guarantee that privacy is not lost
- Can we reduce the amount of data disclosed?

PETs for personal data disclosure minimization

Privacy as confidentiality!

Anonymous credentials

- Authentication is the first step before any security policy can be applied

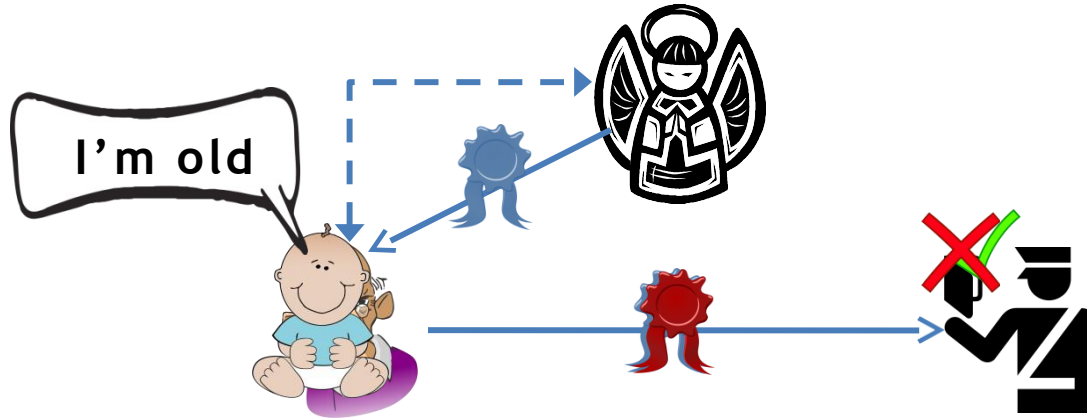


- Makes sense in government, military, even commercial
 - ...but if there is no closed group? (e.g., peer-to-peer)
 - The **Identity Management** concept
- Possible solutions:
 - Private authentication: hide against 3rd parties
 - Anonymous credentials: protect against everybody

Idea behind credentials

- Many transactions involve attribute certificates
 - ID docs: state certifies name, birth dates, address
 - Letter reference: employer certifies salary
 - Club membership: club certifies some status
 - PKI certificate: RRN in Belgian eID, NIF in Spain
- Do you want to show all of them?
- Credential: token certifying one attribute
 - e.g. ticket to the cinema (“i have paid”)
 - Digital credentials: string, boolean attributes, range

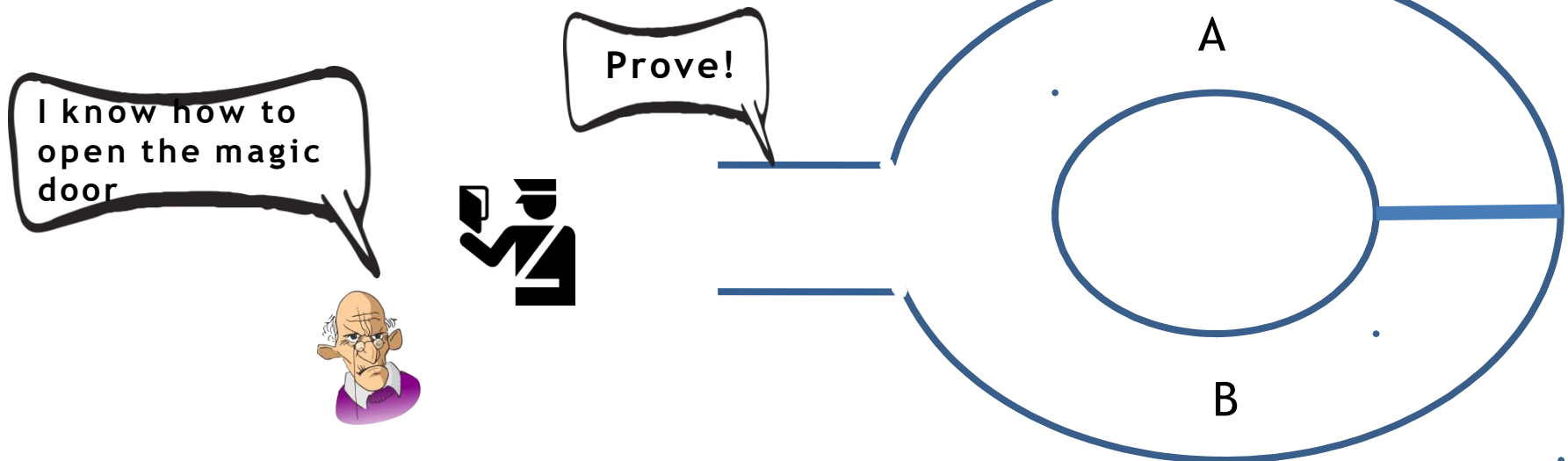
Properties



- **Completeness:** if the statement is true, the verifier will be convinced
- **Zero-knowledge:** if the statement is true no cheating verifier learns anything other than this fact
- **Soundness:** no cheating prover can convince the honest verifier
- **Unlinkability:** two requests cannot be linked to the same user
- Holds even if verifier and prover collide

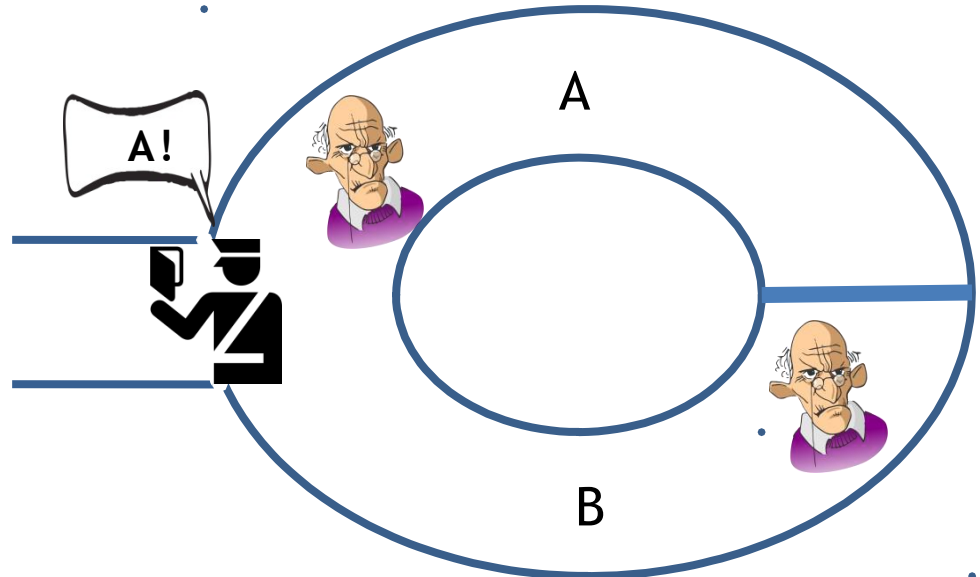
Zero-knowledge proofs

- One party to prove to another that a statement is true, without revealing anything other than the veracity of the statement.
- J.J. Quisquater: "How to Explain Zero-Knowledge Protocols to Your Children"



Zero-knowledge proofs

- One party to prove to another that a statement is true, without revealing anything other than the veracity of the statement.
 - J.J. Quisquater: "How to Explain Zero-Knowledge Protocols to Your Children"
- } If there are doubts repeat!
- } 50% chance
 - } Likelihood decreases



Optional properties

- **Revocation:** some schemes allow for revocation of credential
 - Total revocation
 - Blacklisting
- **Linkability:** some schemes allow to link credential shows
- **Limited shows:** some schemes allow to limit the number of shows
- **Re-identification:** some schemes allow to de-anonymize the subject

PKI vs Anonymous Credentials

PKI

Signed by a trusted issuer
Certification of attributes
Authentication (secret key)
Double-signing detection

No data minimization
Users are identifiable
Users can be tracked
(Signature linkable to other contexts where PK is used)

Anonymous credentials

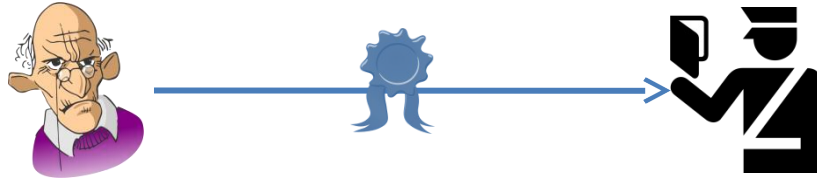
Signed by a trusted issuer
Certification of attributes
Authentication (secret key)
Double-signing detection

Data minimization
Users are anonymous
Users are unlinkable in different contexts

Other privacy-preserving crypto

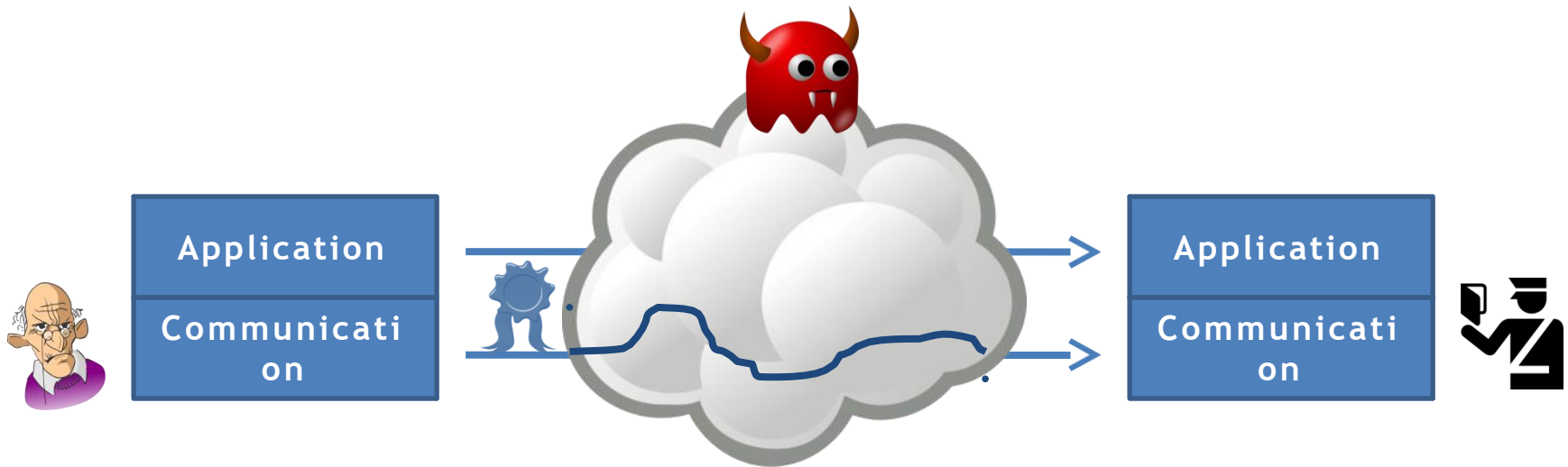
- Private Information Retrieval (Oblivious transfer)
Query databases without revealing query
- Secure Multiparty computation
Group computation where only result is revealed
- Cryptographic commitments
“Vaults” that allow to commit to secret values
- eCash
Digital cash with anonymity and unlinkability properties (like real cash!)
- Private set intersection
Find matching elements in sets without revealing further information

Anonymous communications



- Hidden assumptions
 - Secure channel
 - The channel does not break the privacy property
- But IP is a pseudo-identifier!
 - anonymous credentials are useless in this case...
- Need protection against **traffic analysis**
 - Even if communication is encrypted, traffic data can reveal a lot of information: source, destination, timing, volume, etc.

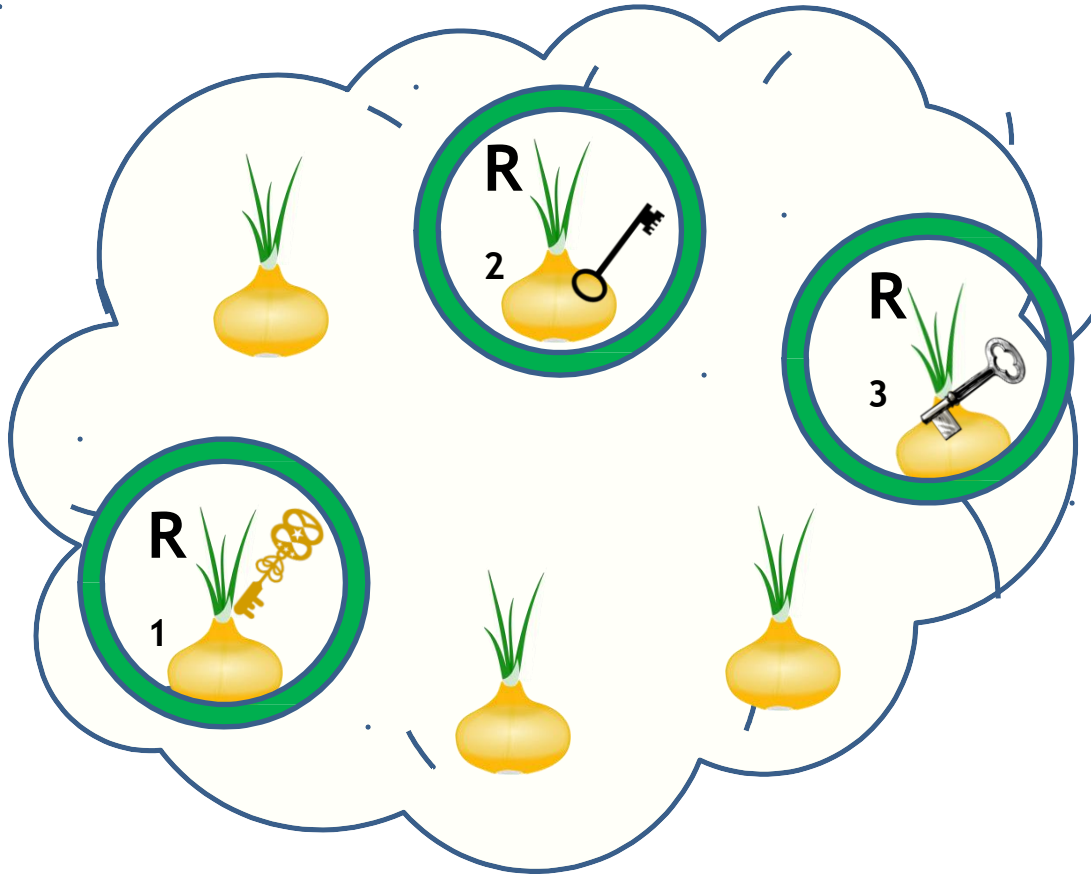
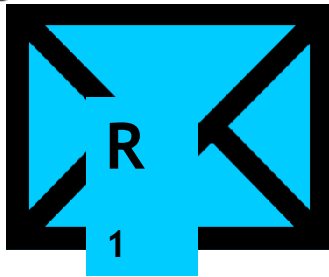
System model



Attacker assumptions

- Attacker abilities:
 - Observe
 - All links (*Global Passive Adversary*)
 - *Some links*
 - Modify, delay, delete or inject messages.
 - Control some nodes in the network.
- Attacker limitations:
 - Cannot break cryptographic primitives.
 - Cannot see inside nodes he does not control.

Onion encryption

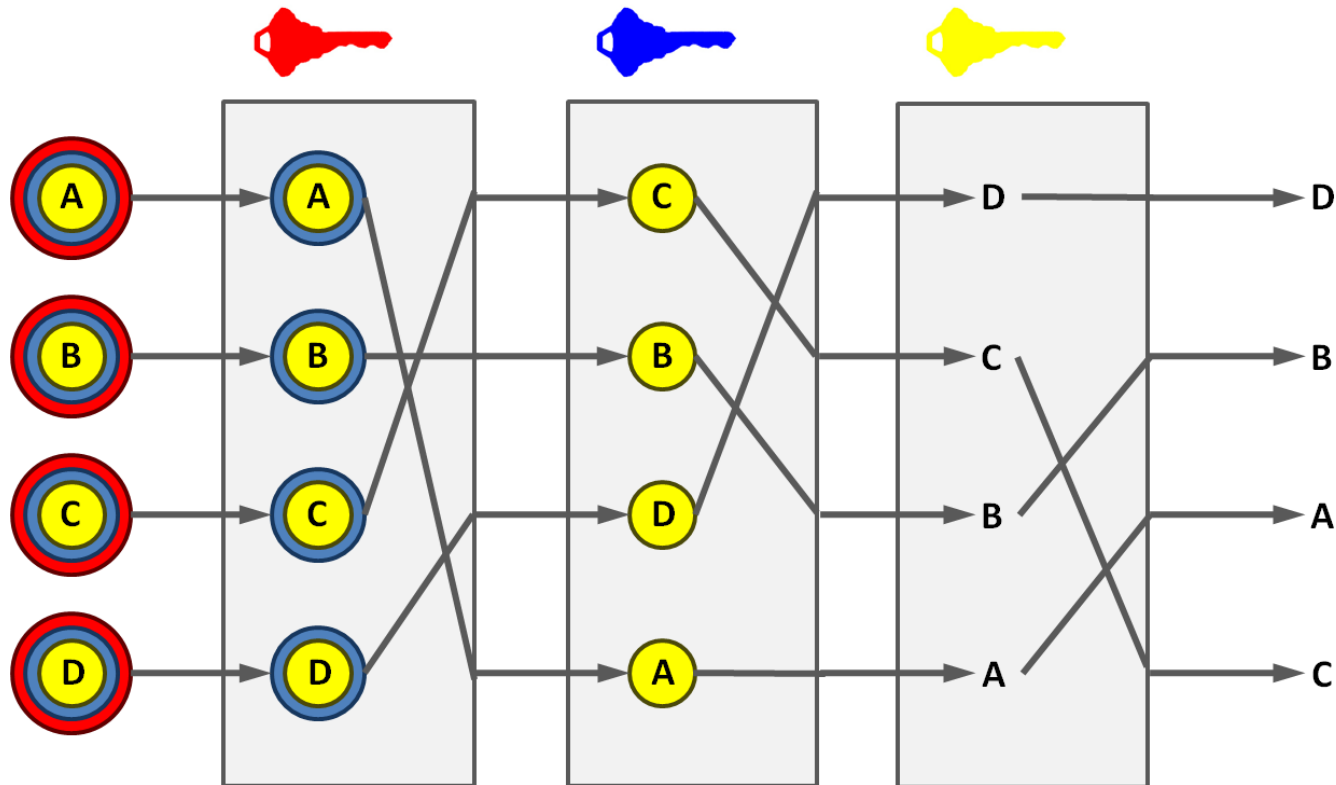


D

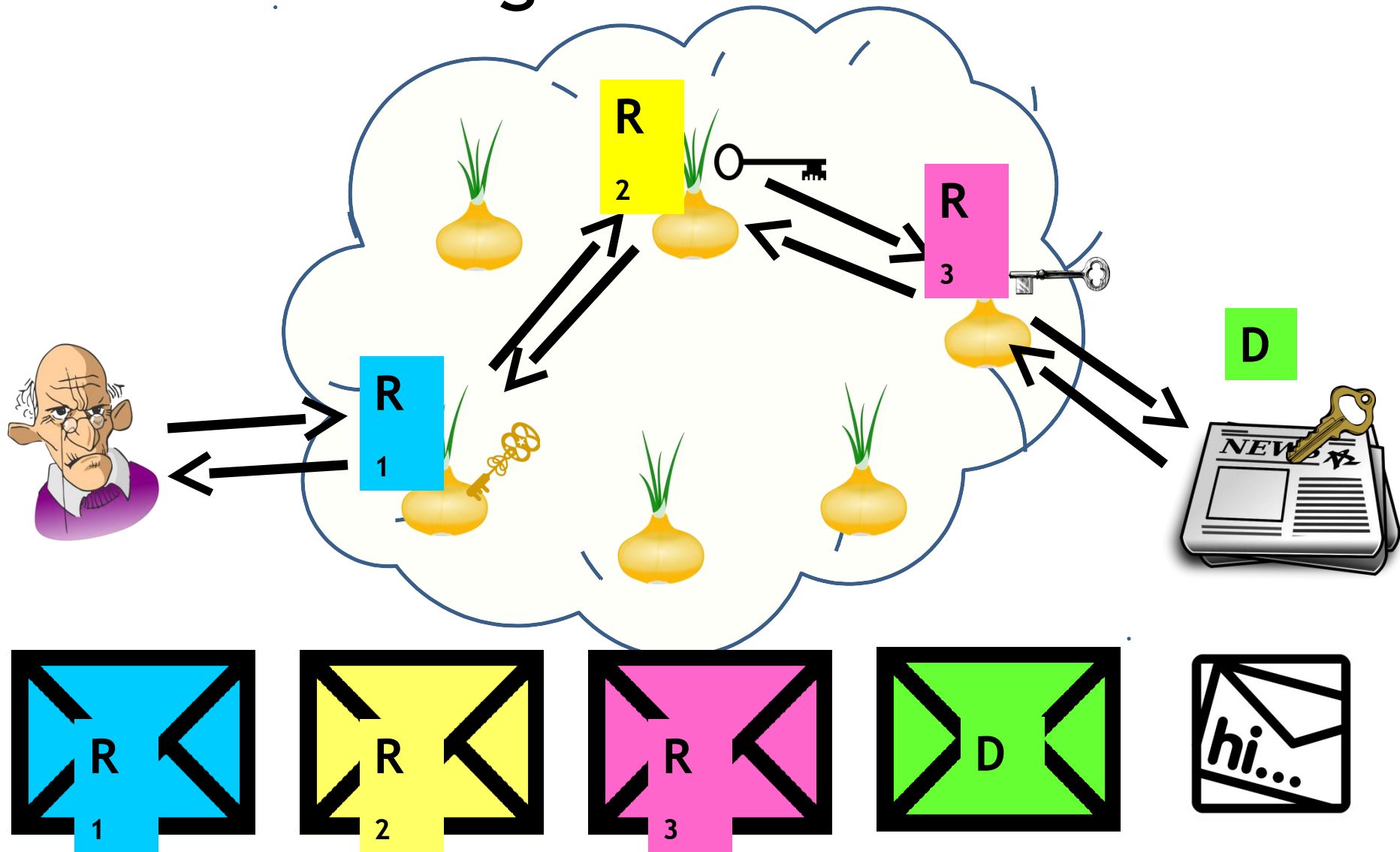


Concept of Mix (Chaum 1982)

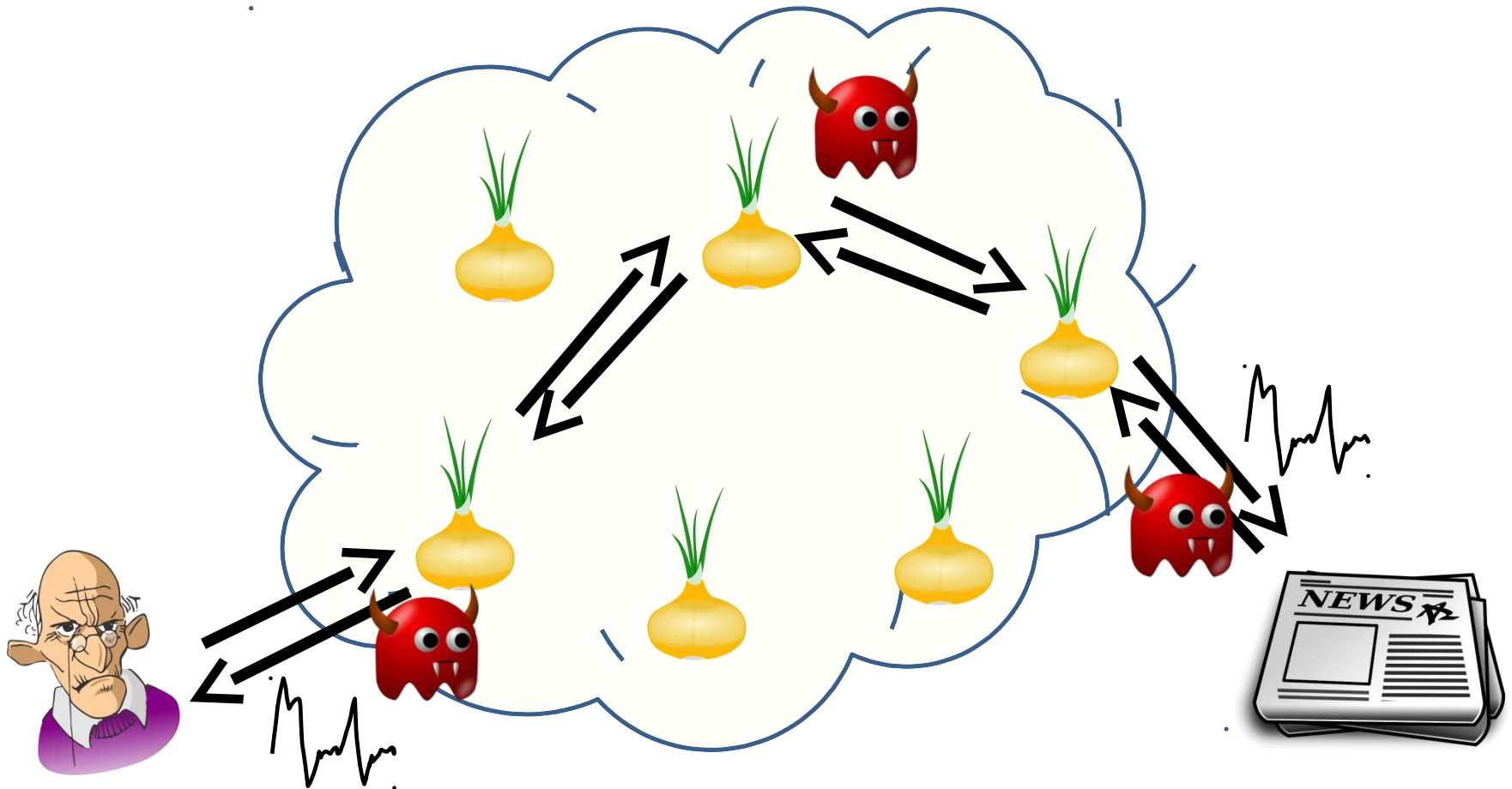
Router that hides
correspondence between
inputs and outputs



Onion Routing



TOR - adversary model



Location Privacy

