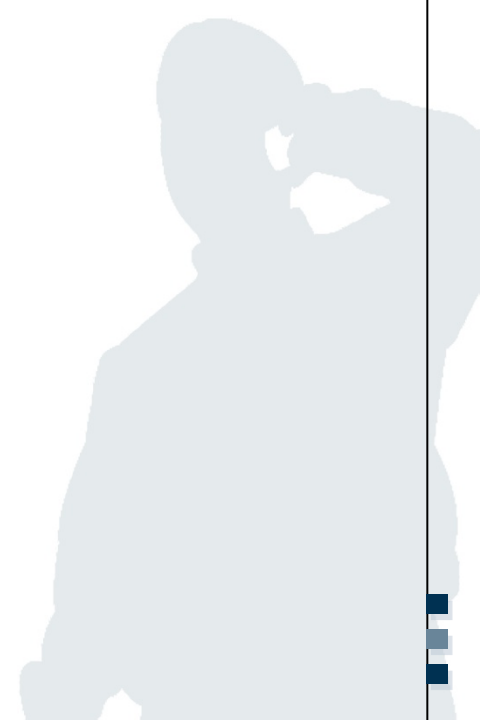


**Information and Communications
Security (WS 2014/15)**

Exam preparation session

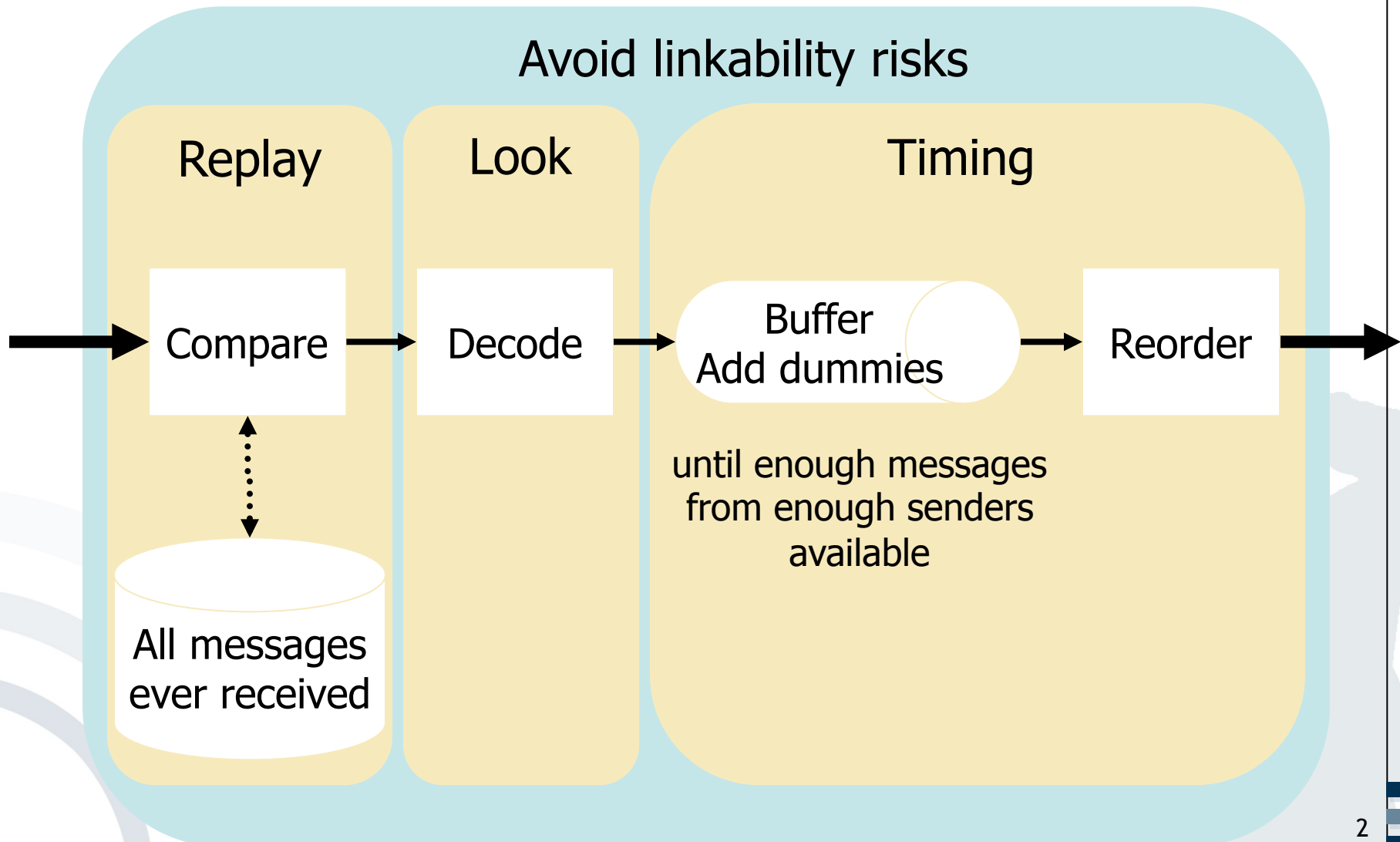
Prof. Dr. Kai Rannenberg
M.Sc. Fatbardh Veseli
M.Sc. Ahmed S. Yesuf
M.Sc. Christopher Schmitz

Deutsche Telekom Chair for
Mobile Business & Multilateral Security
Goethe University Frankfurt a. M.
www.m-chair.de

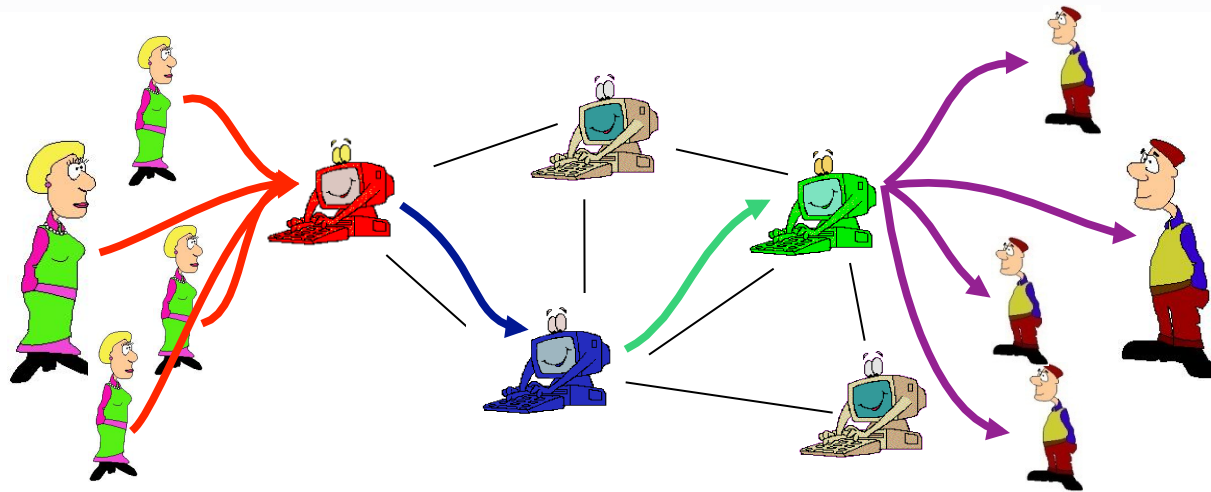


Can you explain this picture please?

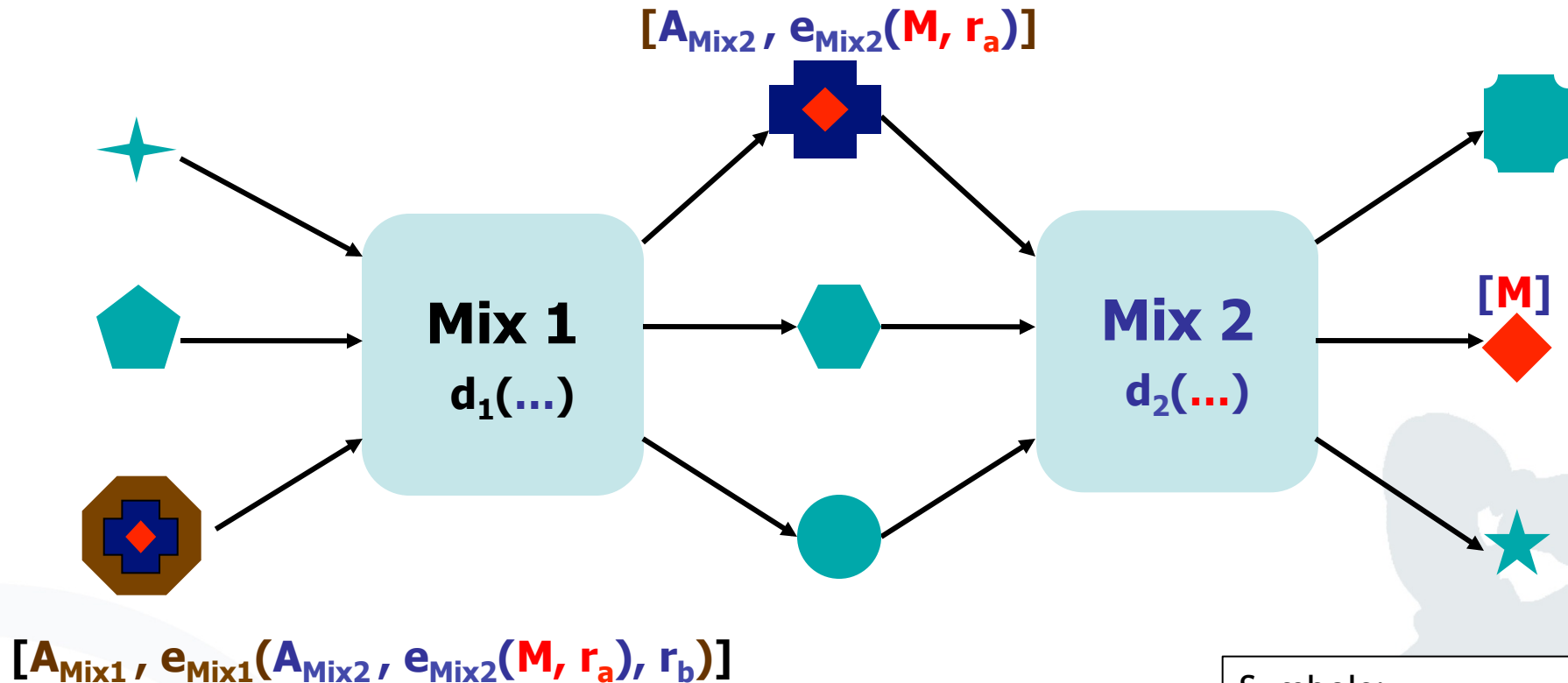
Mixes - Internally



Mixes and Onion Routing



- *Communication is anonymised by multiple mix servers, also called onion routers.*
 - *Both onion routing and JAP are based on the same Mix concept.*



- Decode, buffer, reorder, and resend incoming messages
- Protect **unlinkability** of input / output messages
- Protect **unobservability** of connections and relations
- No single point of trust / failure

[Chaum1981]

Symbols:

A address

e() encryption function

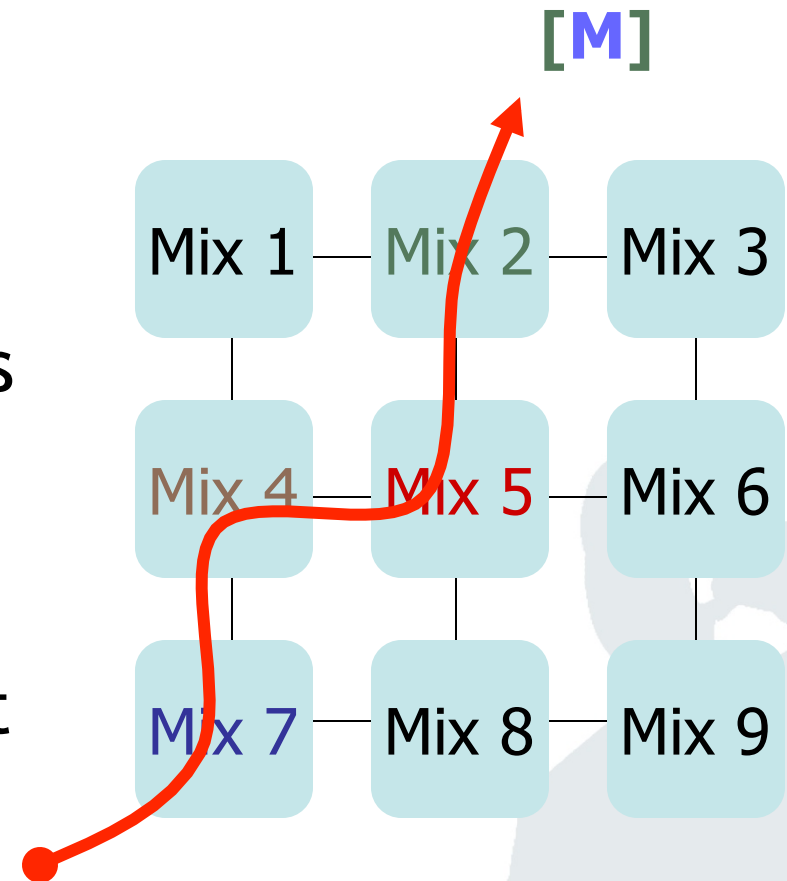
d() decryption function

M core message

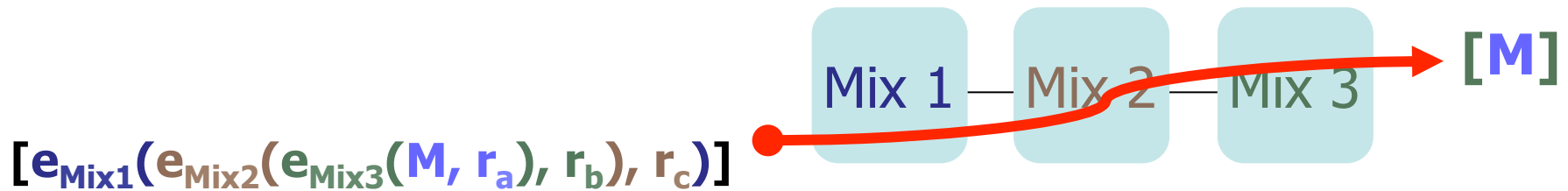
r random value

[] message boundary

- Choose the way of your message through the mixes!
- Protection guaranteed as long as one chosen mix withstands attacks.
- Free path results in additional confusion, but smaller anonymity set.



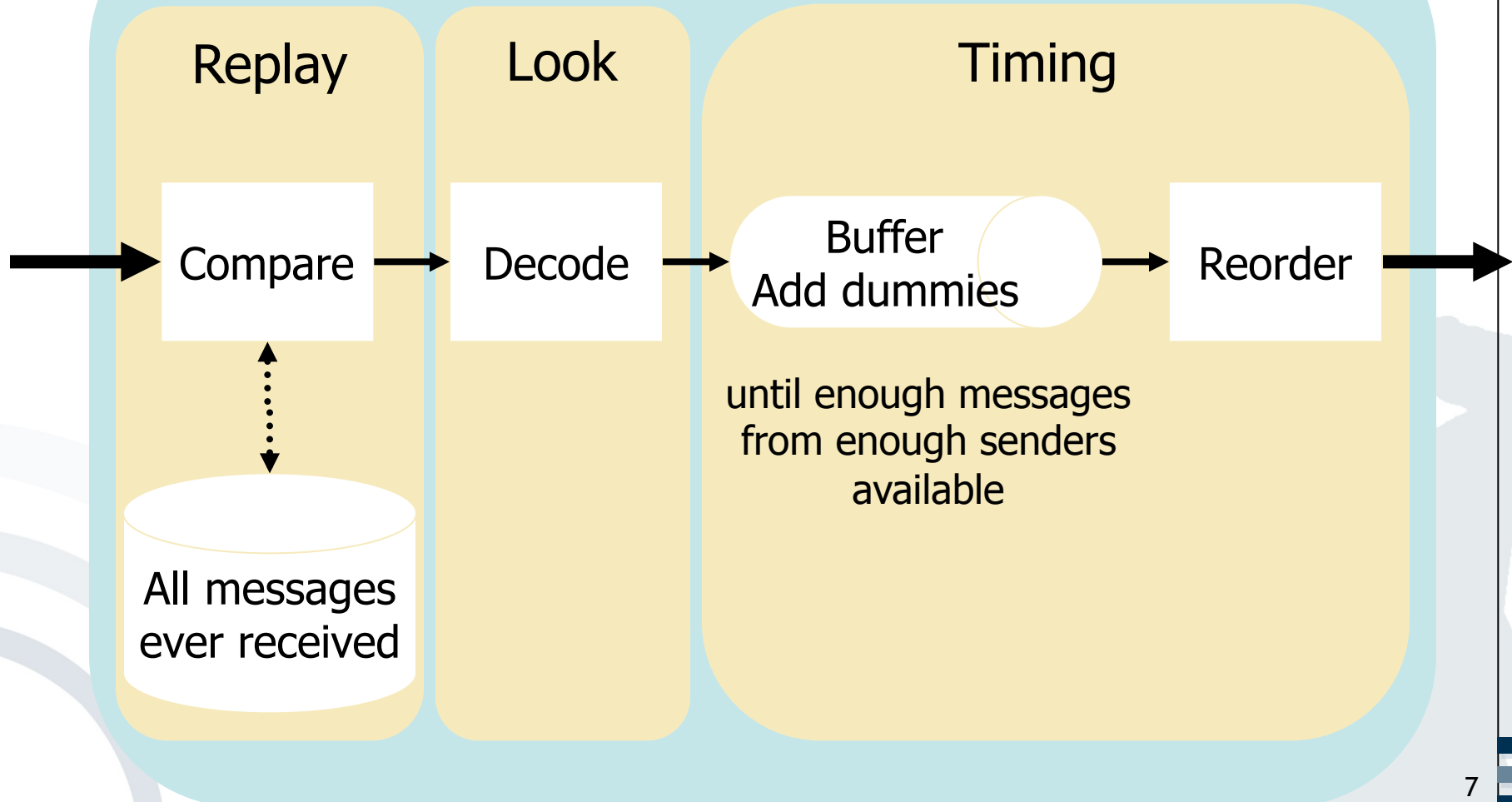
$[A_{\text{Mix7}}, e_{\text{Mix7}}(A_{\text{Mix4}}, e_{\text{Mix4}}(A_{\text{Mix5}}, e_{\text{Mix5}}(A_{\text{Mix2}}, e_{\text{Mix2}}(M, r_a), r_b), r_c), r_d)]$



- Fixed Path through the network
- No mix addresses required in messages
- All traffic flows over the same mixes.
- Protection guaranteed as long as one mix withstands attacks

Mixes - Internally

Avoid linkability risks



- Shouldn't the solution in Exercise 1 (Authentication) be:
 - a. 62^n instead of 36^n ?
 - b. $26 \times 10 \times 62^{n-2}$ instead of 62^n ?

- Well spotted! The solution provided in the website was not identical to the presentation done in the Exercise session. It contained a solution to a different task.
- The solution presented in the class was correct.
- The solution file has been updated in the website.

- Assume that you are only allowed to use a combination of letters and numbers to construct a password. For the letters, let us assume we are using the English alphabet.
 - a. How many different passwords are possible if a password is exactly n characters long, and passwords are not case sensitive?
 - b. How about when we have a distinction between case-sensitive and non-case-sensitive characters?

a) Password combinations:

- Step by step:
 - Each character can be either a letter or a number.
 - Each letter can have 26 possible values.
 - Each number can have 10 possible values.
- If password is 1-character long, we can have
One of the 26 letters OR one of the 10 numbers =
$$\underline{26 + 10 = 36}$$

different options.
- For 2 characters, we have
$$(Letter\ or\ number) * (Letter\ or\ number) =$$
$$\underline{36 * 36 = 36^2}$$
- For 3 characters, we have
$$\underline{36 * 36 * 36 = 36^3}$$
- ...
- For n characters, we can have
$$\underline{36 * 36 * 36 * \dots * 36\ (n\text{-times}) = 36^n}$$

different combinations.

b) Password combinations:

We have n characters for the password and each one can be an uppercase letter, or lowercase letter or a digit.

Each character can possibly have

$$\underline{26 + 26 + 10 = 62}$$

different values.

For n characters, $\underline{62^n}$ different combinations can be used as a password.

Lecture 5:

1. Can you show the multiplicative inverse of d please?

2. How do you get $e = 17$? Is it because of $e = n - ((p-1)(q-1))$? And why is $d = 53$? Can the sender of a message choose d by his own? Are for d only prime numbers possible?*

- To encrypt a message M , using a public key (e, n) , proceed as follows (e and n are a pair of positive integers):
 - First represent the message as an integer between 0 and $n-1$ (break long messages into a series of blocks, and represent each block as such an integer).
 - Then encrypt the message by raising it to the e^{th} power modulo n .
 - The result (the ciphertext C) is the remainder of M^e divided by n .
 - The encryption key is thus the pair of positive integers (e, n) .

- To decrypt the ciphertext, raise it to another power d , again modulo n .
- The decryption key is the pair of positive integers (d, n) .
- Each user makes his encryption key public, and keeps the corresponding decryption key private.

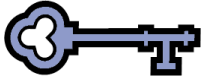
RSA Encryption/Decryption Summary

- $C \equiv E(M) \equiv M^e \pmod{n}$,
for a message M
- $M \equiv D(C) \equiv C^d \pmod{n}$,
for a ciphertext C

- You first compute n as the product of two primes p and q .
- $n=p*q$
- These primes are very large “random” primes.
- Although you will make n public, the factors p and q will be effectively hidden from everyone else due to the enormous difficulty of factoring n .
- This also hides the way, how d can be derived from e .

- You then choose an integer d to be a large, random integer which is relatively prime to $(p-1)*(q-1)$.
- That is, check that d satisfies:
 - The greatest common divisor of d and $(p-1)*(q-1)$ is 1.
 - $\gcd(d, (p-1)*(q-1))=1$

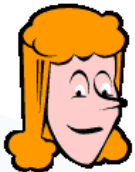
- The integer e is finally computed from p, q , and d to be the “multiplicative inverse” of d , modulo $(p-1)*(q-1)$.
- Thus we have
$$e*d \equiv 1 \pmod{(p-1)*(q-1)}.$$



Public
(e,n)



Private
(d,n)



Alice

- Let $p=7$ and $q=11$.
- Then $n=77$.
- Alice chooses $d=53$, so $e=17$.
- $\gcd(d, (p-1)*(q-1)) = \gcd(53, (7-1)*(11-1)) = \gcd(53, 60) = 1$
- $e*d \bmod (p-1)*(q-1) = 901 \bmod 60 = 1$

- Bob wants to send Alice the message „Hello World“
- Each plaintext character is represented by a number between 00(A) and 25 (Z).
- Therefore, we have the plaintext as:
07 04 11 11 14 26 22 14 17 11 03



Bob

- Using Alice's public key the ciphertext is:
 - $07^{17} \bmod 77 = 28$
 - $04^{17} \bmod 77 = 16$
 - $11^{17} \bmod 77 = 44$
 - ...
 - $03^{17} \bmod 77 = 75$
- Or 28 16 44 44 42 38 22 42 19
44 75



Bob

28 16 44 44
42 38 22
42 19 44 75



Alice

- Alice decrypts the ciphertext by calculating:
 - $28^{53} \bmod 77 = 07$
 - $16^{53} \bmod 77 = 04$
 - $44^{53} \bmod 77 = 11$
 - ...
 - $75^{53} \bmod 77 = 03$
- Or: 07 04 11 11 14 26 22 14
17 11 03 = “Hello World”

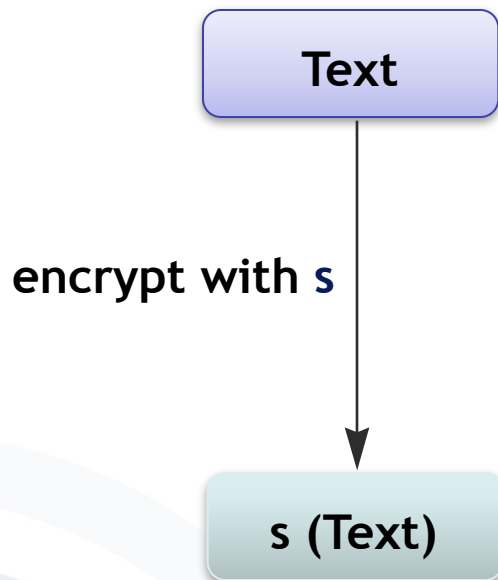
1. What is meant by "mistakenly generalized" in Lecture 6, slide 9? Does it mean, that the hash function is missing?

- **RSA: Rivest, Shamir, Adleman**
 - Asymmetric encryption system which also can be used as a signature system via “inverted use”,
 - Message encrypted with the private key (= signing key) gives the signature,
 - Decoding with the public key (=testing key) has to produce the message.

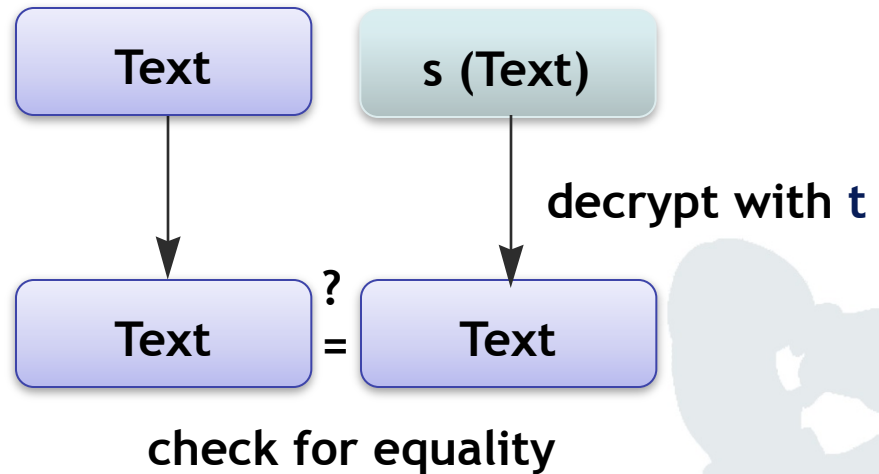
[Rivest et al. 1978]
- **DSA: Digital Signature Algorithm**
 - Determined in the Digital Signature Standard of the NIST (USA),
 - Based on discrete logarithms (Schnorr, ElGamal),
 - Key length is set to 1024 bit.

Asymmetric Signature System (Simplified Example RSA)

Sender / Signer

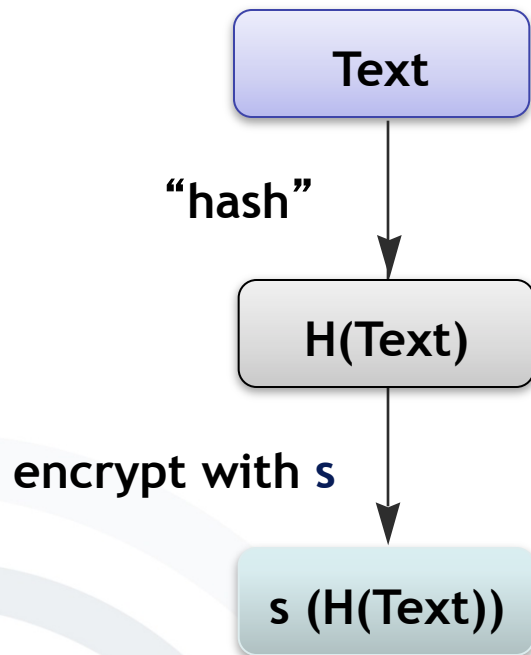


Addressee / Verifier

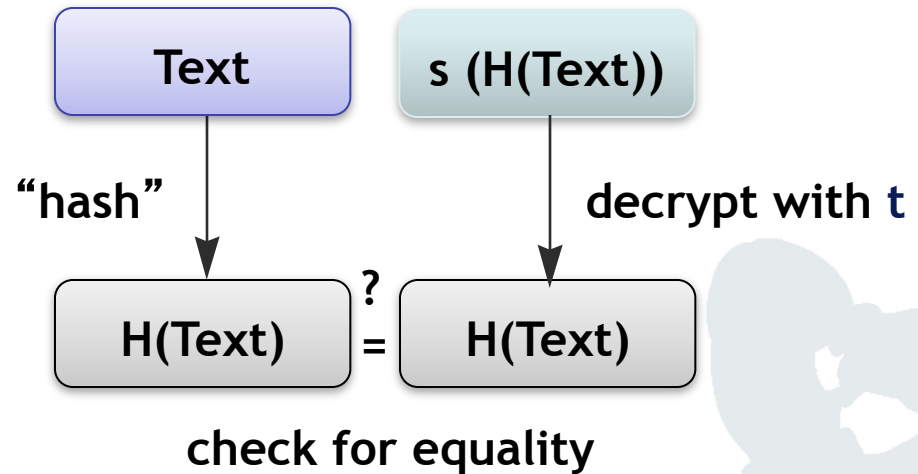


- ➡ Signing key **s** only with the sender, test key **t** public
- ➡ Example is often mistakenly generalized.

Sender / Signer



Addressee / Verifier



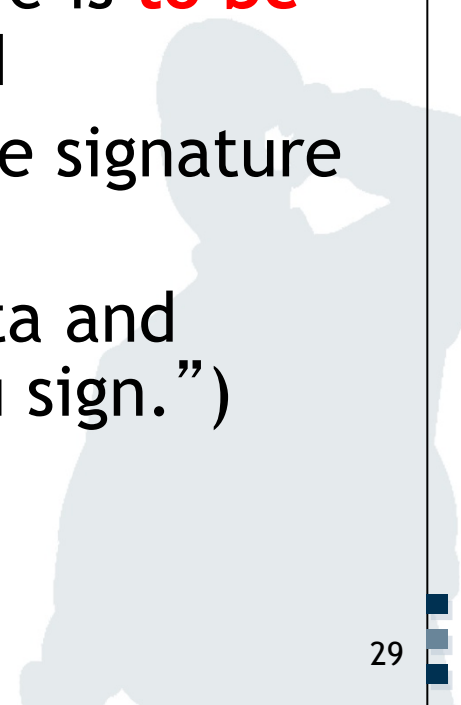
- ➡ Signing key s only with the sender, test key t public
- ➡ Example is often mistakenly generalized.

Lecture 6:

1. "Clearly notify the signer that a signature is created before the signature is created"?

Example: display of data (§ 17(2)) [SigG01]

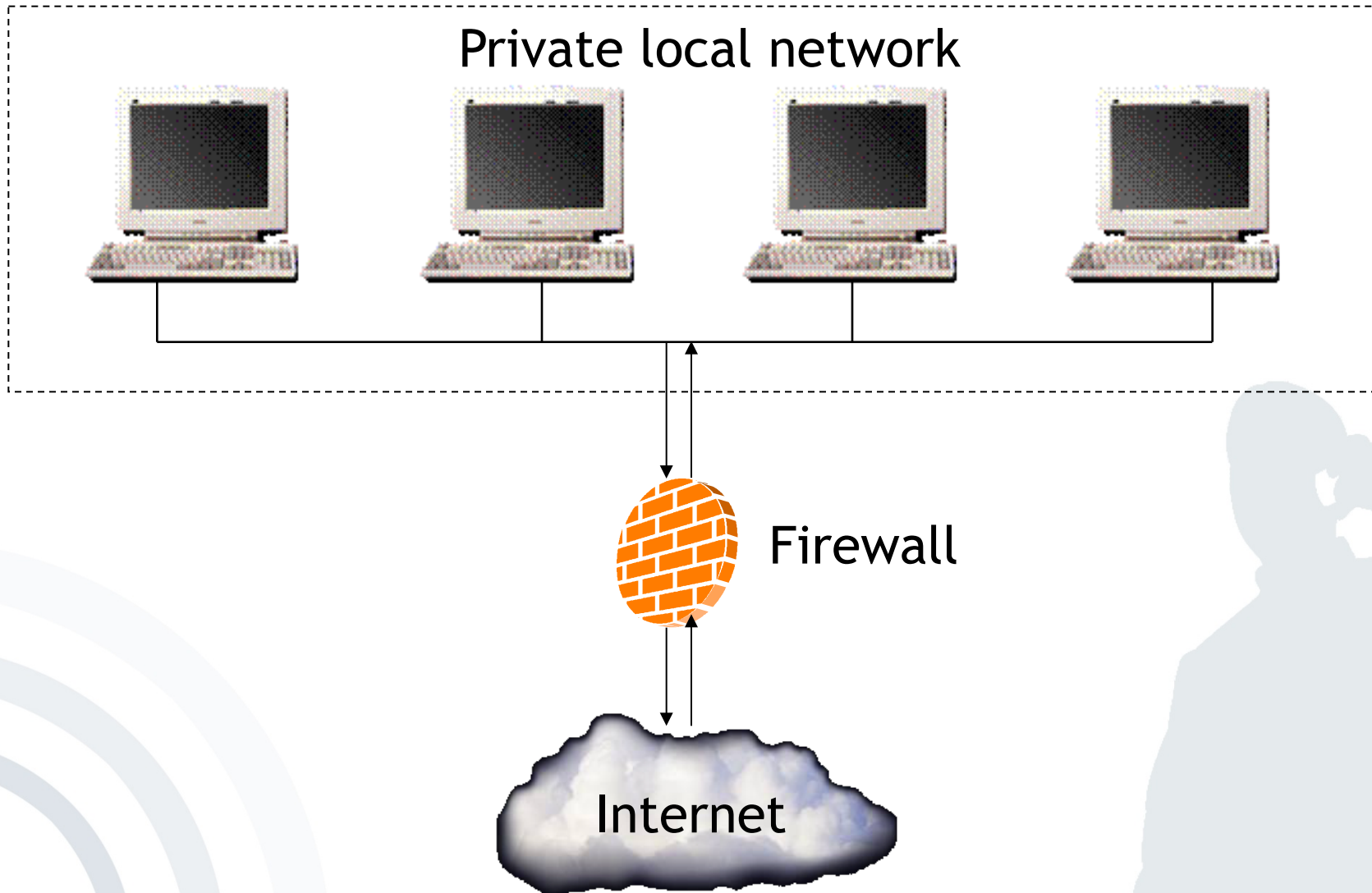
The signature component must:

- Clearly notify the signer that a signature is **to be** created *before* the signature is created
 - Make clearly perceptible which data the signature refers to
 - Secure the accordance of displayed data and signed data (“What you see is what you sign.”)
- 
- A light blue silhouette of a person's head and shoulders, facing right, positioned in the lower right area of the slide. The person appears to be looking at a device or document.

Lecture 10

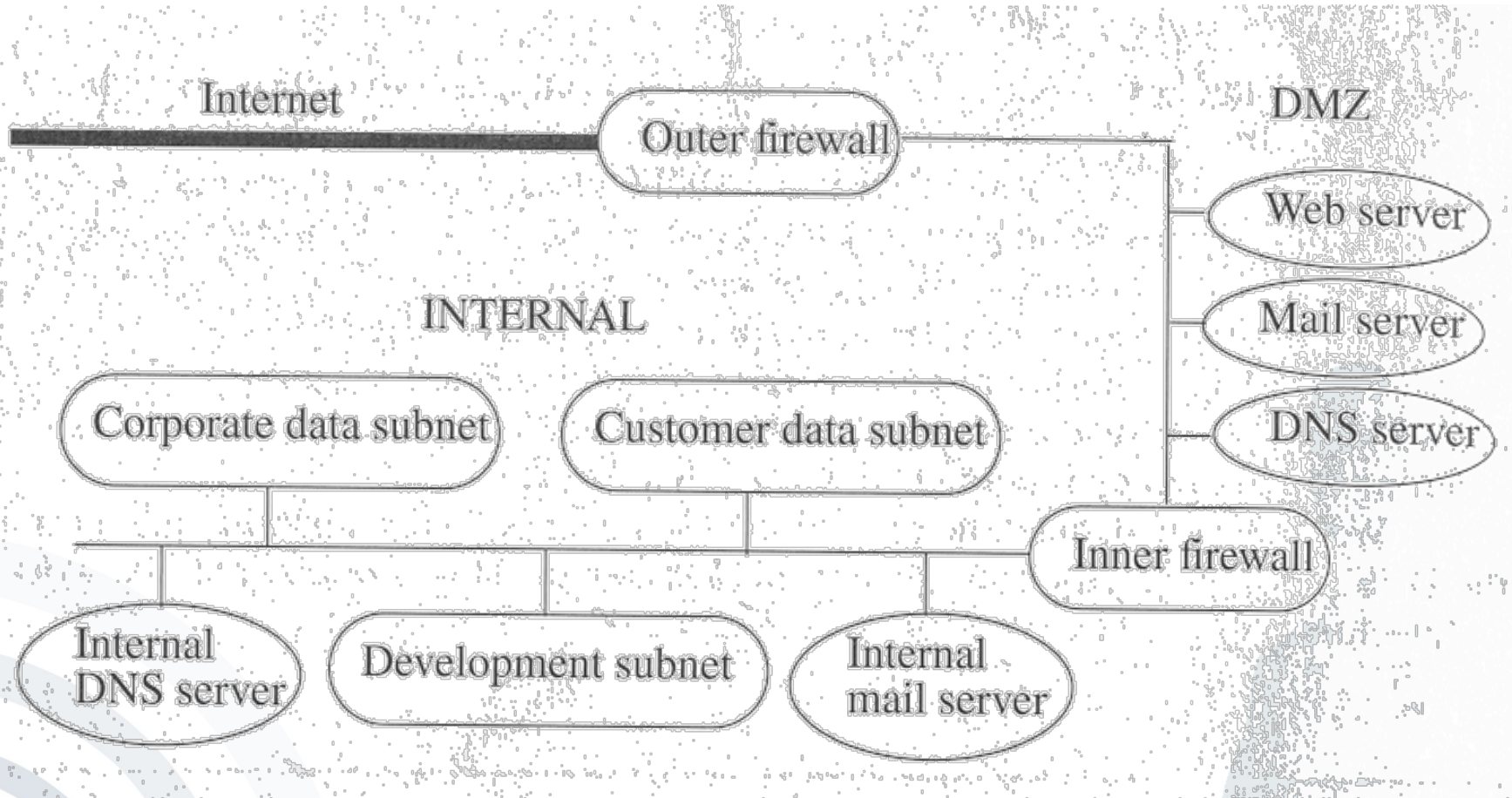
1. What is the difference between a firewall and a demilitarized zone? What are advantages/disadvantages?

- „A firewall is an internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be *inside* the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be *outside* the firewall).“ [RFC 2828]

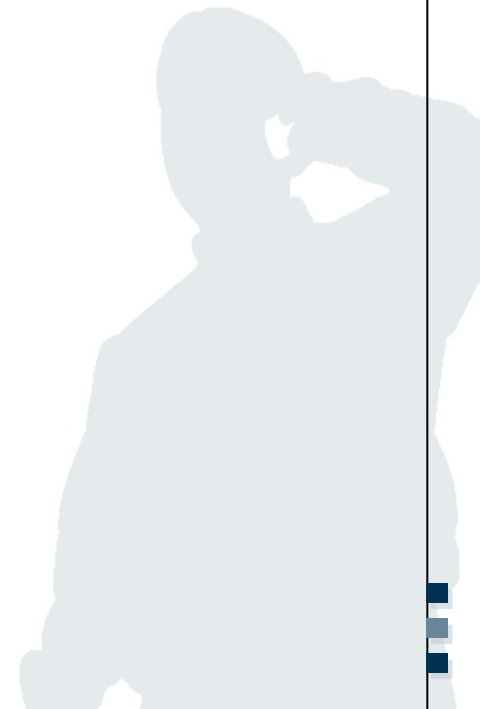


- The DMZ is a portion of a network, that separates a purely internal network from an external network. [Bi05]
- The “outer firewall” sits between the Internet and the internal network.
- The DMZ provides limited public access to various servers.
- The “inner firewall” sits between the DMZ and the subnets not to be accessed by the public.

Network using a DMZ



- *Can you explain the Chinese wall model again, please? Here I can't understand, why on slide 43, lecture 3, a subject is able to access data from two different companies; what is about preventing the conflict of interest in this context?*



- The Chinese Wall (CW) model is a model of a security policy that refers equally to confidentiality and integrity.
- It describes policies that involve a conflict of interest in business.
- The environment of a stock exchange or investment house is the most natural environment for this model.
- In this context, the goal of the model is to prevent a conflict of interest in which a trader represents two clients.

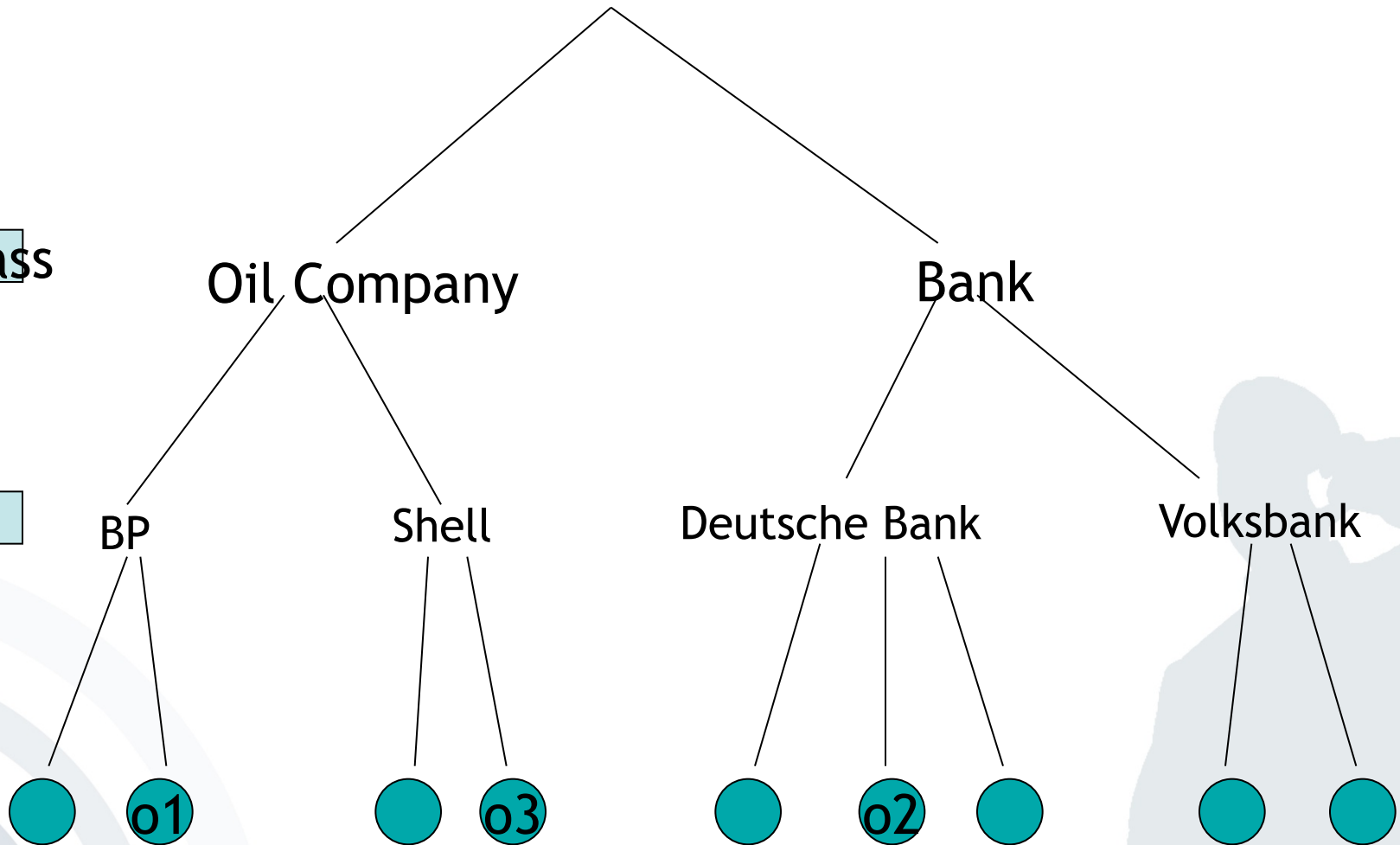
- The ***objects*** of the database are items of information related to a company.
- A ***company dataset (CD)*** contains objects related to a single company.
- A ***conflict of interest (COI)*** class contains the datasets of companies in competition.

- s can read o if and only if any of the following holds:
 1. There is an object o' such that s has accessed o' and $CD(o') = CD(o)$.
 2. For all objects o' , $o' \in PR(s)$
 $\Rightarrow COI(o') \neq COI(o)$
 3. o is a sanitized object.

$PR(s)$ are the files already opened by s .

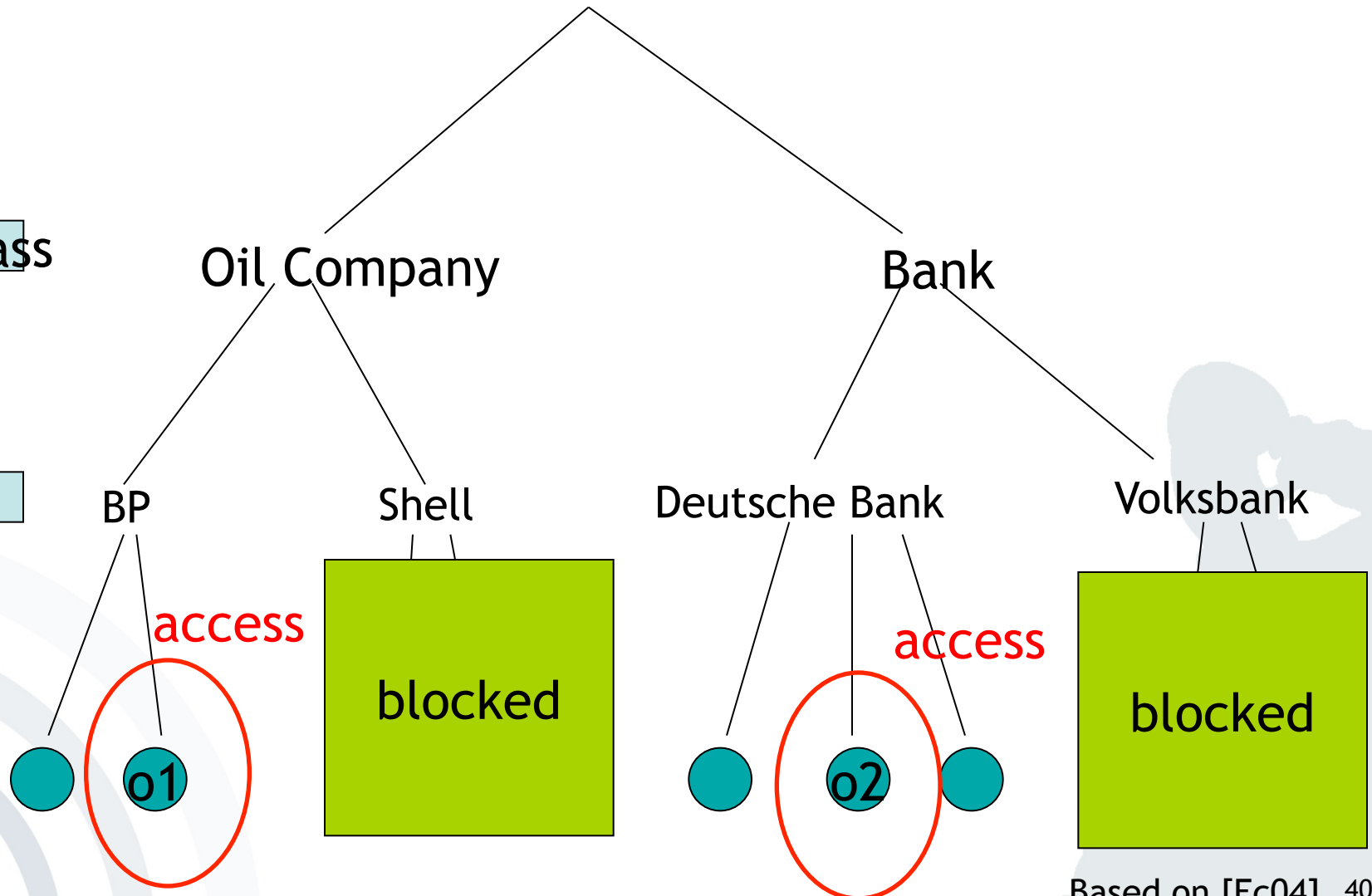
COI class

CD

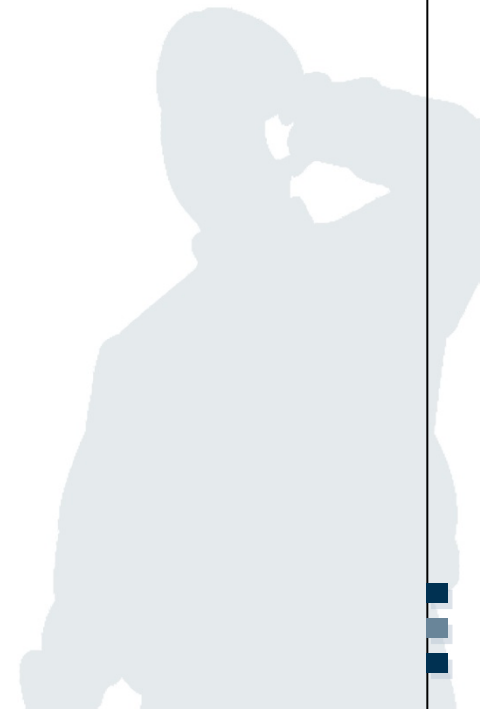


COI class

CD



- *Can you show one more example for how to create a role based access control security model?*

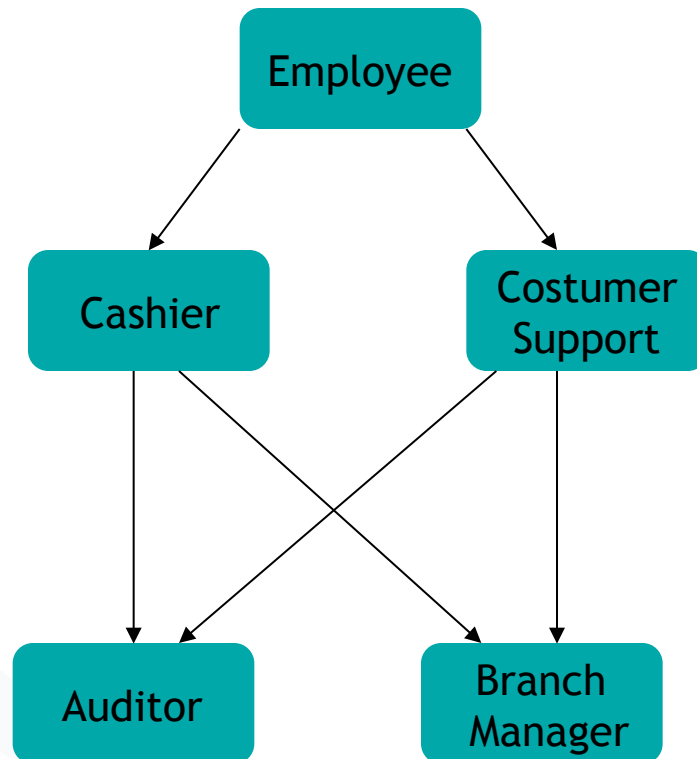


- The ability or need, to access information may depend on one 's job functions.
- This suggests associating access with the particular job of the user.

- A role is a collection of job functions. Each role r is authorized to perform one or more transactions. The set of authorized transactions for r is written $trans(r)$.
- The active role of a subject s , written $actr(s)$, is the role that s is currently performing.
- The authorized roles of a subject s , written $authr(s)$, is the set of roles that s is authorized to assume.
- The predicate $canexec(s,t)$ is true if and only if the subject s can execute the transactions t at the current time.

- If a subject can execute at least one transaction, then the subject has an active role.
 - This binds the notion of execution of a transaction to the role rather than to the user.
- The subject must be authorized to assume its active role.
 - It cannot assume an unauthorized role.
- A subject cannot execute a transaction for which its current role is not authorized.

Example 1: Bank

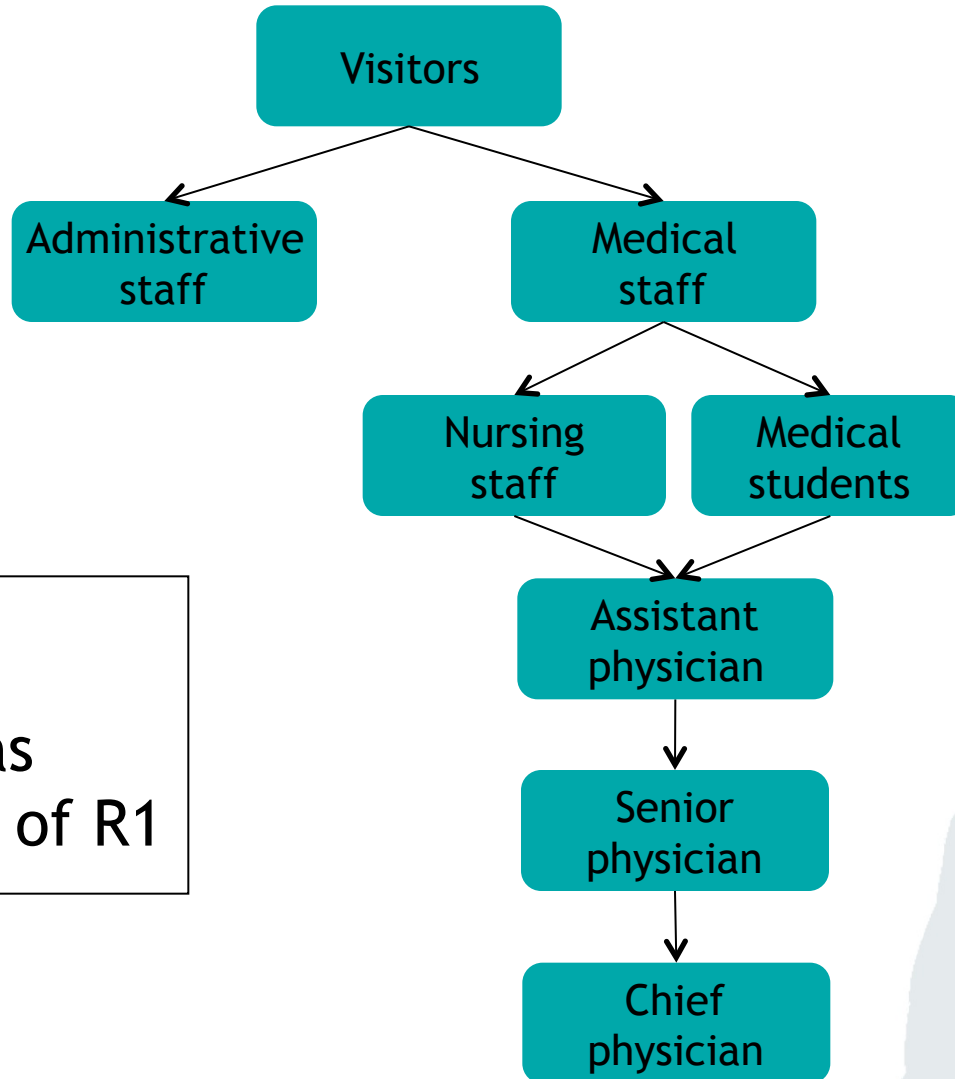


Customer

role

$R1 \rightarrow R2$, R2 has
also the rights of R1

Example 2: Hospital



role

$R1 \rightarrow R2$, R2 has
also the rights of R1

- Please explain Idemix and U-Prove again, especially in the context of Zero-Knowledge Proves.

- How can Alice prove to Bob that she knows a secret S without disclosing the secret to Bob or a third person?

Example: Where is Walter?



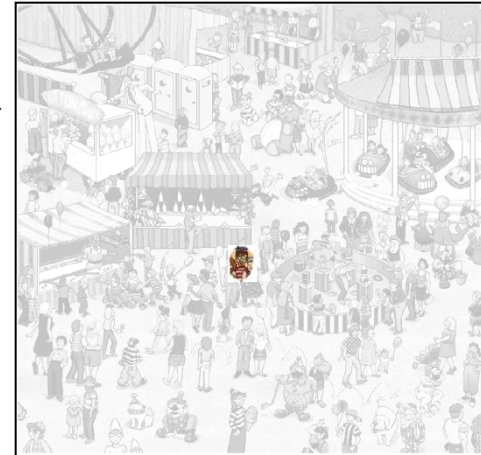
I know where
Walter is.



Walter

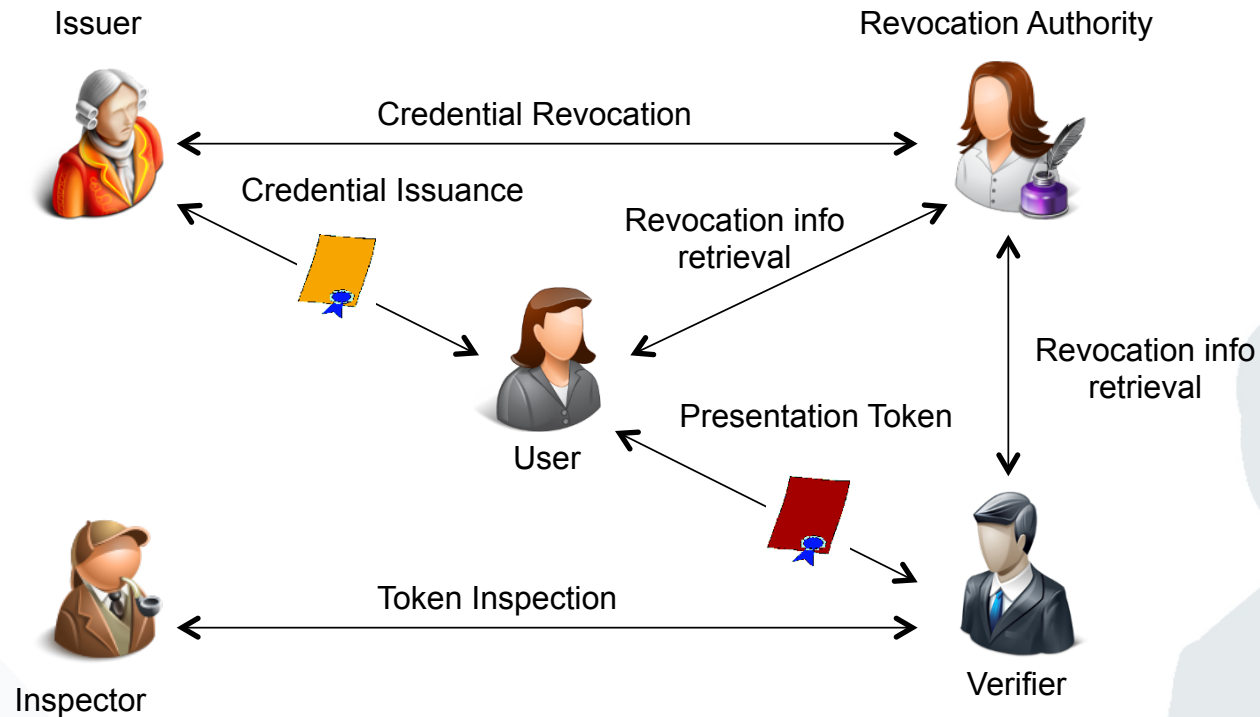
How can I prove this
without disclosing
information?

Example: Where is Walter?

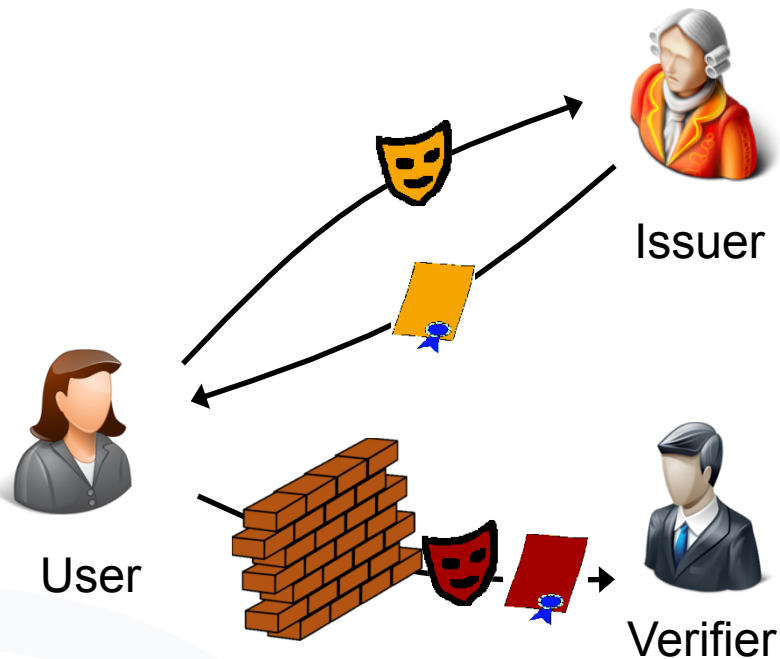


ABC4Trust architecture

Interactions and Entities



Zero-Knowledge Proofs

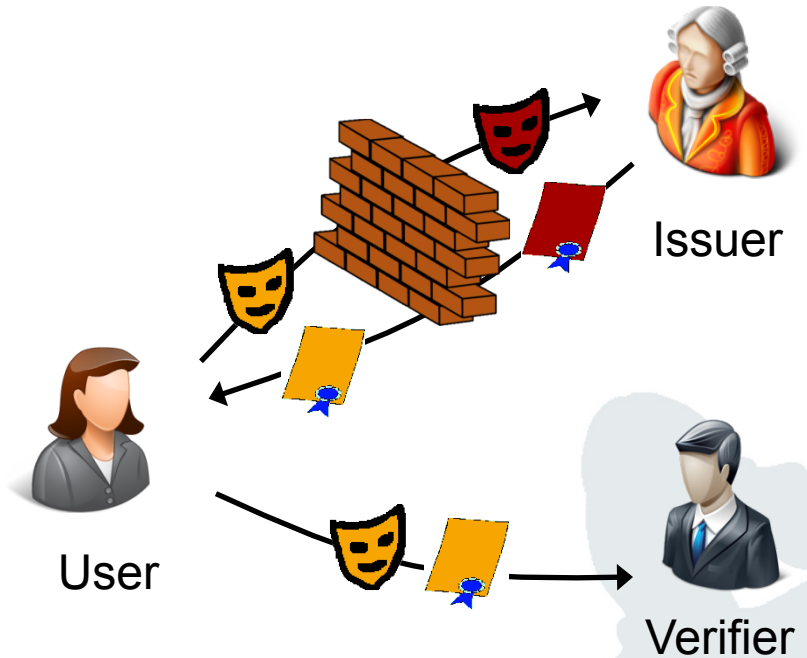


Idemix (Identity Mixer)

Damgard, Camenisch & Lysyanskaya
Strong RSA, pairings (LMRS, q-SDH)

Existing Privacy-ABC Technologies

Blind Signatures



U-Prove

Chaum, Brands et al.
Discrete Logs, RSA,...

- They rely on different cryptographic schemes and have practical differences:
 - U-Prove uses Brands signature scheme [Br00], whereas Idemix uses Camenisch-Lysyanskaya signature scheme.
 - Both rely on a zero-knowledge scheme: for U-Prove, zero knowledge happens is interactive (requires the Issuer), for Idemix it's non-interactive (can be done by the User alone) [CZ13].
 - U-Prove tokens do not provide multiple-presentation unlinkability, Idemix tokens do.

ABC4Trust video on Privacy-ABCs



- www.youtube.com/watch?v=utk4EyoaxAk

- [Bi05] Matt Bishop. Introduction to Computer Security. Boston: Addison Wesley, 2005. pp. 27-35, 62-69, 83-87, 92-94
- [Br00] S. A. Brands, Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. Cambridge, MA, USA: MIT Press, 2000.
- [CL01] J. Camenisch and A. Lysyanskaya, “An efficient system for non-transferable anonymous credentials with optional anonymity revocation,” in Advances in Cryptology EUROCRYPT 2001, ser. Lecture Notes in Computer Science, B. Pfitzmann, Ed. Springer Berlin Heidelberg, 2001, vol. 2045, pp. 93-118. [Online]. Available: <http://dx.doi.org/10.1007/3-540-44987-67>
- [CZ13] M. Chase and G. Zaverucha, “MAC Schemes with Efficient Protocols and Keyed-Verification Anonymous Credentials,” 2013.
- [Ec04] Claudia Eckert. IT-Sicherheit. München, Wien: Oldenbourg, 2004
- [SigG01] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf