Security and Cryptography 2021

Mirosław Kutyłowski

IX. PRIVACY

Protection of personal data and GDPR

- declared as fundamental right in EU, but technically fundamental for cybersecurity
    - identity theft e.g. for financial criminality
    - mobbing, discrimination, social abuse
    - lack of protection is a threat for economy and national security

Frameworks

- GDPR – EU and European Economic Area, adopted by many countries, some recognized as equivalent by EU
- Privacy Shield: https://www.privacyshield.gov/
- California Consumer Privacy Act
- Schrems II verdict of *Court of Justice of the European Union*

Privacy in communication

- one can hide payload communication
- it is not trivial how to hide **who is communicating with whom**
- this is a sensitive data

protection methods:

- broadcast channel
- token ring
- dining cryptographers -DC nets
- onion protocols and TOR

Dining Cryptographers

- protecting the source of a 1-bit message. One of cryptographers is sending a 0 or 1.
- protocol for 3 cryptographers sitting at a round table:
  1. each pair of neighbors establish a shared bit at random
  2. each cryptographer that is not transmitting computes XOR of the bits shared with the neighbors,
  3. the sender computes the same XOR but swaps it if the bit transmitted is 1
  4. each cryptographer reveals his result
  5. the message is the XOR of the bits published:
     - if the message is 0, then each shared bit occurs twice:

$$(b_{\mathrm{AB}} \oplus b_{\mathrm{BC}}) \oplus (b_{\mathrm{BC}} \oplus b_{\mathrm{CA}}) \oplus (b_{\mathrm{CA}} \oplus b_{\mathrm{AB}}) = 0$$

     - otherwise, one of the bits is swapped: e.g. we have

$$(b_{\mathrm{AB}} \oplus b_{\mathrm{BC}}) \oplus (b_{\mathrm{BC}} \oplus b_{\mathrm{CA}} \oplus 1) \oplus (b_{\mathrm{CA}} \oplus b_{\mathrm{AB}}) = 1$$

Communication steganography–

Hiding communication in innocent traffic

Idea: hiding data in innocent data transmitted (e.g. images, sound, protocol execution data)

steganography versus watermarking:

watermarking is not annoying but hard to remove, steganography is invisible

typical applications: copyright protection, DRM,

steganography in images

1. original picture taken – name: stego image
2. marking algorithm (maybe with a secret key) applied to message and the stego image
3. outcome transmitted/published
4. retreiving the covered message

invisibility: without a key impossible to decide whether there is a message hidden

Concrete techniques for image/video/audio steganography:

- changing LSB bits of gray scale
- JPEG encoding: cosinus transform, high frequency components are manipulated anyway for compression
- other digital transforms
- echoing
- audio encoding: transformation and assigning coefficients to waves – manipulations of certain coefficients undetectable for listeners

Problems

- multiple stego images
- transformations to remove stego, especially fragile: stego messages as ciphertexts
- artefacts due e.g. to the block based transformations

watermarking/stegography in network flow:

- different ways of encoding (e.g. a change is 1 no change encodes 0)
- all random parameters transmitted in clear may contain watermarks
- simple timing: interpacket delays, departure times
- mean balancing:
  - $2d$ probes divided into two sets A and B.
  - the expected values of A and B are the same with no watermarking
  - changing the characteristics so that expected values differ in some direction (the direction is the watermarked value)

- sources of mean balancing watermarks:
  - interpacket delays
  - interval centroid: divide into $2d$ intervals, in each compute mean arrival time
  - interval counting: divide into $2d$ intervals, in each compute the number of packets

- size: packet size (harder if block encryption applied), object size (https, malicious Javascript generating watermarked size data)
- network rate:
  - one can influence it with dummy packets
  - burst traffic
- response times in transmission, packet order etc

Defense against steganography:

(sometimes problematic or illegal due to intelectual property rights)

i. compression

ii. transforms and random distortions

iii. stretching (Stirmark)

iv. printing and scanning, input to an analog device and digitalize again

effectiveness measured by relative entropy:

$$D(P_1 \| P_2) = \sum_{q \in \mathrm{space}} \Pr_1(q) \cdot \log \frac{\Pr_1(q)}{\Pr_2(q)}$$

relative entropy of plaintexts and hidden text should be smaller than some small ϵ

Anonymity via mixing: A mixer

messages $m_1, m_2, \ldots, m_k$ go through a mixer A:

- message m_i sent encrypted with the public key of A

$$C_i := \mathrm{Enc}(\mathrm{PK}_A, m_i)$$

- A decrypts $C_1, \ldots, C_k$ and forwards them to their destinations

Conditions:

encryption might be secure but nevertheless one can link the ciphertexts with the decrypted texts:

- message size
- timing

So:

- all messages should have the uniform size
- A should collect them all, decrypt and send them in a random order

Onion Routing

an attempt to hide the sender and the destination of a message – hiding in a crowd of messages

onion creation:

an onion created for a route going through servers $A, B, C, ..., Z$ to the final destination Γ

$$O_1 = \mathrm{Enc}_A(B, \mathrm{Enc}_B(C, \mathrm{Enc}_C(...(\mathrm{Enc}_Z(\Gamma, M))....)))$$

(by encryption Enc_X we mean encryption with the public key of X)

Onion Routing

onion processing:

- O_1 sent from the origin machine to A,
- server A decrypts with its private key and gets B and

$$O_2 = \mathrm{Enc}_B(C, \mathrm{Enc}_C(\ldots(\mathrm{Enc}_Z(\Gamma, M))\ldots.))$$

- A sends O_2 to B
- server B decrypts O_2 with its private key and gets C and $O_3 = \mathrm{Enc}_C(\ldots(\mathrm{Enc}_Z(\Gamma, M))\ldots.)$
- the process is continued in the same way …
- … until server Z finds Γ, M and forwards the message M to machine Γ

each processing steps is like peeling off one layer of an onion

Onion processing

Limitations

- **idea**: if two or more onions enter a server at the same time, get partially decrypted, then forwarded, then it is impossible to say which incomming onion corresponds to which outcoming onion - **node mixing**

- **traffic analysis:** assigning probabilities to permutations ($\pi(i)=j$ means that the ith sender has a message to the jth receiver)

- **it is not enough to say that** $\pi(i)=j$ **with ppb** $\approx\frac{1}{n}$:
  - let us assume that the adversary knows that π is a circular shift
  - assume that the adversary gets extra knowledge:
    - ”if source i is talking to destination j, then $i+1$ is talking to destination $j+1$”

  however, still $\Pr(\pi(i)=j)=\frac{1}{n}$

Question: necessary length of the onions?

analytical results for restricted case of n senders and n receivers, messages sent simultaneously:

- $O(\log^2 n)$ if the adversary has a full knowledge of the system (not likely to have a better estimation unless ... big progres in math), **assumption:** uniform distribution for choosing destinations
- $O(\log n)$ if the adversary can see only a constant fraction of nodes, **assumption**: sender i may have non-uniform distribution of destination points
- it is easy to see that $\Omega(\log n)$ is necessary

meaning of the results:

traffic analysis does not improve our prior knowledge in a significant way (e.g. if we know in advance that source i always sends to destination j, then onions cannot hide this fact)

the guarantees are given in terms of **total variation distance** of two probability distributions:

$\|\pi,\mu\| = \frac{1}{2}\sum_{\omega\in\Omega}|\pi(\omega)-\mu(\omega)|$, where Ω is the set of all events

Problems with onions

- **replay attacks**: just send the same onion (or partially decrypted onion) for the 2nd time: the same subonions will appear along the forwarding path

  defense: universal reencryption, example based on ElGamal encryption:

  - ciphertext of m:

    $(\beta^r, m \cdot g^r, \beta^s, g^s)$ for r, s chosen at random

  - renecryption:

    1. choose α, β at random
    2. replace (y_1, y_2, y_3, y_4) by $(y_1 \cdot {y_3}^{\alpha}, y_2 \cdot y_4^{\alpha}, y_3^{\beta}, y_4^{\beta})$

       thereby we get $(\beta^{r+\alpha s}, m \cdot g^{r+\alpha s}, \beta^{s\beta}, g^{s\beta})$

       if order of the group is a prime number, then this is equivalent with choosing $(\beta^{r'}, m \cdot g^{r'}, \beta^{s'}, g^{s'})$ for random r', s'

- **local view**: not all users have the same list of servers

  then: **long routes do not improve anonimity**. Toy example:

  - give user A a list of servers with 50% of servers used by nobody else
  - no matter how long is the routing path designed by A, it is likely that close to destination the path goes through a rogue server
  - a few destinations available from this rogue server (50% of cases the rogue server sends directly to the destination)
  - an onion going through the rogue server originates from the attacked source

- **timing at nodes**: delays necessary

  defense: collecting enough onions and flashing them at once. (slowdown!!!)

- **sparse traffic** means no protection

TOR

- free BSD licence
- connection based protocol, new connection established periodically (“10 minutes or so”)
- routes limited to 3 TOR nodes

- onion based forwarding the symmetric keys

  i each node on the path learns only the predecessor and the successor

  ii the path established step by step:

  - after establishing a subpath $X_0, X_1, ..., X_k$ the subpath is used to send an encrypted message over the channel to X_k stating that the next node is X_{k+1}.
  - the sender and X_{k+1} negotiate a new connection key via DH key exchange

  iii after making a connection the message is encrypted symmetrically with the keys:

$$\text{AES}_{\text{relay1}}(\text{AES}_{\text{relay2}}(\text{AES}_{\text{relay3}}(m)))$$

  each relay node removes one layer

  iv the messages back to the sender: instead of decryption: encryption with keys shared with the sender. The sender has to decrypt the onion

Problems:

- exit node knows the plaintext
- traffic correlation
- application level attacks
- Heartbleed - change of public keys, some clients use old keys, ...

Other issues:

- many authorities fight against TOR as it helps to escape the control

Onion Routing - Warning: Rogue Encryption

PSEUDONYMIZATION

Symmetric methods:

- **hashing the identifier:** $\text{pseudonym} = \text{Hash}(\text{identifier})$

  problem: it is impossible to compute the identifier from the pseudonym, however hashing all possible identifiers and brute force reveals the link between the pseudonym and identifier

- **encryption with a (secret) symmetric key:** unlinkability, however the user cannot compute the pseudonym himself and the owner of the secret key can link all pseudonyms

- **hashing with a key:** as above, the party holding the secret key has to perform brute force to link back the pseudonym to the identifier

Asymmetric pseudonymization methods:

- **based on Diffie Hellman Problem**:
  - a **domain** (service provider, database, etc) holds a pair of keys $(d, D = g^d)$
  - a user Alice holds a pair $(x, X = g^x)$
  - the **pseudonym** of Alice corresponding to D is $g^{x \cdot d}$, which is computed as X^d by the domain manager, and D^x by the user
  - nobody but the user and the domain manager can compute the pseudonym:

    for a 3rd person deciding whether X^d corresponds to X in domain D requires solving DDH Problem

- **a variant based on domain and a central Authority:**
  - the key d is not known to the domain authority
  - $d = d_A + d_{\mathrm{domain}}$, where d_A is known by the authority and d_{domain} is known by the domain manager
  - steps of generating the pseudonym by the authority:
    1. the Authority computes $X' := X^{d_A}$ and presents X' to the domain manager
    2. the domain manager computes pseudonym as $(X')^{d_{\mathrm{domain}}}$
  - linking a pseudonym with the starting public key is a reverse process but **both the domain manager and the Authority must participate** in it

- **a variant from German personal identity cards (Restricted Identification):**
  - **pseudonym** of a user with public key $X = g^x$ is $\mathrm{Hash}(D^x)$
  - **pseudonym presentation:** by the ID card over a secure channel,
    - no proof that the pseudonym is correct
    - but a smart card can create only one pseudonym per domain
  - **revocation:** by computing $\mathrm{Hash}((X^{d_A})^{d_{\mathrm{domain}}})$ jointly by the Authority and the domain manager and putting the result on the **blacklist**
  - blacklisting a black sheep based on the domain pseudonym requires brute force and recomputing all pseudonyms
- more flexibility, if pairing groups are available but be careful: DDH might be easy and so the above methods do not work

Advantages and disadvantages of Restricted Identification:

- different pseudonyms generated automatically is
  - user friendly
  - makes re-identification based solely on data related to the pseudonym much harder
- problems:
  - converting a pseudonym in domain D_1 to a pseudonym in domain D_2 might be hard or infeasible, and require cooperation with the user and/or an authority

    (problem area: moving pseudonymized medical records)

DATABASES and PRIVACY for QUERIES

the main problem is answering queries: does a query result disclose personal data?

Approach 1: **anonymity set**

- a query accepted if the number of record used to answer the query is at least k (and each concerns a different person)
- the method is naive: the attack is to ask for two sets of records: one including Alice and one excluding Alice to know the value for Alice

Approach 2: **differential privacy**

classify the algorithms (queries)

algorithm A satisfies ϵ-differential privacy, if for any two databases D and D' that differ by elimination of one record:

- for any subset S of the image of A:

$$\Pr(A(D) \in S) \leq e^{\epsilon} \cdot \Pr(A(D') \in S)$$

  where the probability is over the random choices of A

Then:

- $\epsilon = 0$ is the ideal for privacy: as $e^0 = 1$ and the probabilities are exactly the same, but the result does not depend on the database contents (noise)
- so it is necessary to find balance between privacy (ϵ as small as possible) and information in the response (ϵ as big as possible)

Problem with outliers

with some records that have very different values it is hard to keep promise of *differential privacy*

solution: disregard them (as private data leak anyway) and concentrate on the rest

e.g.:

1. disregard a few entries that are outliers
2. for differential privacy take only those elements that have at least k neighbors in some sense

PSEUDONYMOUS SIGNATURES

Application areas:

- while having the pseudonyms, how to authenticate digital data? Digital signatures would solve the problem

- implementing GDPR rights in practice: a data subject can authenticate the request (e.g. for data rectification) in a database with pseudonyms by sending a request with a signature corresponding to the pseudonym

BSI Pseudonymous Signature:

- **keys:**
  - domain parameters D_M and a pair of global keys $(\mathrm{PK}_M, \mathrm{SK}_M)$
  - public key $\mathrm{PK}_{\mathrm{ICC}}$ for a group of eIDAS tokens, the private key $\mathrm{SK}_{\mathrm{ICC}}$ known to the issuer of eIDAS tokens
  - assigning the private keys for a user:

    the issuer chooses $\mathrm{SK}_{\mathrm{ICC},2}$ at random, then computes $\mathrm{SK}_{\mathrm{ICC},1}$ such that

    $$\mathrm{SK}_{\mathrm{ICC}} = \mathrm{SK}_{\mathrm{ICC},1} + \mathrm{SK}_M \cdot \mathrm{SK}_{\mathrm{ICC},2}$$
  - a sector (domain) holds private key $\mathrm{SK}_{\mathrm{sector}}$ and public key $\mathrm{PK}_{\mathrm{sector}}$.
  - a sector has revocation private key $\mathrm{SK}_{\mathrm{revocation}}$ and public key $\mathrm{PK}_{\mathrm{revocation}}$
  - sector specific identifiers $I^{\mathrm{sector}}_{\mathrm{ICC},1}$ and $I^{\mathrm{sector}}_{\mathrm{ICC},2}$ for the user:

    $$I^{\mathrm{sector}}_{\mathrm{ICC},1} = (\mathrm{PK}_{\mathrm{sector}})^{\mathrm{SK}_{\mathrm{ICC},1}}$$

    $$I^{\mathrm{sector}}_{\mathrm{ICC},2} = (\mathrm{PK}_{\mathrm{sector}})^{\mathrm{SK}_{\mathrm{ICC},2}}$$

- **signing:** with keys $\mathrm{SK}_{\mathrm{ICC},1}$, $\mathrm{SK}_{\mathrm{ICC},2}$ and $I_{\mathrm{ICC},1}^{\mathrm{sector}}$ and $I_{\mathrm{ICC},2}^{\mathrm{sector}}$ for $\mathrm{PK}_{\mathrm{sector}}$ and message m
    - i choose K_1, K_2 at random
    - ii compute
        - $Q_1 = g^{K_1} \cdot (\mathrm{PK}_M)^{K_2}$
        - $A_1 = (\mathrm{PK}_{\mathrm{sector}})^{K_1}$
        - $A_2 = (\mathrm{PK}_{\mathrm{sector}})^{K_2}$
    - iii $c = \mathrm{Hash}(Q_1, I_{\mathrm{ICC},1}^{\mathrm{sector}}, A_1, I_{\mathrm{ICC},2}^{\mathrm{sector}}, A_2, \mathrm{PK}_{\mathrm{sector}}, m)$

      (variant parameters omitted here)
    - iv compute
        - $s_1 = K_1 - c \cdot \mathrm{SK}_{\mathrm{ICC},1}$
        - $s_1 = K_2 - c \cdot \mathrm{SK}_{\mathrm{ICC},2}$
    - v output (c, s_1, s_2)

- **verification:**

  compute

  - $Q_1 = (\mathrm{PK}_{\mathrm{ICC}})^c \cdot g^{s_1} \cdot (\mathrm{PK}_M)^{s_2}$
  - $A_1 = (I^{\mathrm{sector}}_{\mathrm{ICC},1})^c \cdot (\mathrm{PK}_{\mathrm{sector}})^{s_1}$
  - $A_2 = (I^{\mathrm{sector}}_{\mathrm{ICC},2})^c \cdot (\mathrm{PK}_{\mathrm{sector}})^{s_2}$
  - recompute c and check against the c from the signature

- why it works?

$$(\mathrm{PK}_{\mathrm{ICC}})^c \cdot g^{s_1} \cdot (\mathrm{PK}_M)^{s_2} = (\mathrm{PK}_{\mathrm{ICC}})^c \cdot g^{K_1} \cdot (\mathrm{PK}_M)^{K_2} \cdot g^{-c \cdot \mathrm{SK}_{\mathrm{ICC},1}} \cdot (\mathrm{PK}_M)^{c \cdot \mathrm{SK}_{\mathrm{ICC},2}}$$

$$= (\mathrm{PK}_{\mathrm{ICC}})^c \cdot g^{K_1} \cdot (\mathrm{PK}_M)^{K_2} \cdot g^{-c \cdot \mathrm{SK}_{\mathrm{ICC},1}} \cdot (g)^{-c \cdot \mathrm{SK}_M \cdot \mathrm{SK}_{\mathrm{ICC},2}}$$

$$= (\mathrm{PK}_{\mathrm{ICC}})^c \cdot g^{K_1} \cdot (\mathrm{PK}_M)^{K_2} \cdot g^{-c \cdot \mathrm{SK}_{\mathrm{ICC}}} = g^{K_1} \cdot (\mathrm{PK}_M)^{K_2} = Q_1$$

- there is a version without A_1, A_2 and the pseudonyms $I^{\mathrm{sector}}_{\mathrm{ICC},1}, I^{\mathrm{sector}}_{\mathrm{ICC},2}$

- **Problems:**
  - the authorities know the private keys (there is a way to solve it when the user gets two pairs of keys on the device and takes their linear combination)
  - breaking into just 2 devices reveals the system keys
  - possible to create a trapdoor for enabling to link pseudonyms
    - apart from $\mathrm{SK}_{\mathrm{ICC}} = \mathrm{SK}_{\mathrm{ICC},1} + \mathrm{SK}_M \cdot \mathrm{SK}_{\mathrm{ICC},2}$ there is a another relationship for the user u

$$x_u = \mathrm{SK}_{\mathrm{ICC},1} + s_u \cdot \mathrm{SK}_{\mathrm{ICC},2}$$

    - x_u and s_u are dedicated for user u - maybe not in the database but derived from a secret key, say Z
    - domain trapdoor: $T_{\mathrm{domain},u} = \mathrm{PK}_{\mathrm{domain}}^{x_u}$ and s_u (it can be derived from Z alone)
    - then one can conclude that nym_1 and nym_2 correspond to user u, if:

$$T_{\mathrm{domain},u} = \mathrm{nym}_1 \cdot \mathrm{nym}_2^{s_u}$$

ANONYMOUS CREDENTIALS

two commercial products (libraries): Idemix (IBM) and UProve (Microsoft)

some details concerning Idemix

components:

- **actors:** issuer, recipient, verifier, trusted party
- **attributes**: for each attribute there is: `name`, `value` and `type`. The types are `int`, `string`, `date`, `enum` (enumeration). The attributes concern the recipient.
- **credentials**: given by the issuer to the recipient
  - i known (A_k): the issuer knows the value of an attribute
  - ii commited (A_c): the issuer knows a commitment to the attribute but not the commitment itself
  - iii hidden (A_h): the attribute is completely hidden to the issuer

- **keys:**
  - single master key for each user (m_1)
  - single master key for the Issuer – for creation of CL signatures
- **pseudonyms:**
  - a single domain pseudonym for a user per domain: generated as as

    $$\mathrm{dom}^{m_1}$$

    where dom is the public key of a domain, and m_1 is the user's master key
  - pseudonyms are unlinkable

Cryptographic schemes used by Idemix

CL signatures:

- RSA group, special choice of primes: $p = 2p' + 1$, $q = 2q' + 1$, where p' and q' are primes
- choose at random quadratic residues: $R_1, ..., R_l, Z, S$
- public key: $(n, R_1, ..., R_l, Z, S)$, private key: p, q (enabling computation of roots $\mod n$)
- security based on **Strong RSA assumption**: it is infeasibile to compute e-roots for $e > 2$
- signature for messages $m_1, ..., m_l$:
  - choose v at random and a prime $e > 2$ of length higher than each $m_1, ..., m_l$
  - $A := ((Z / (S^v \cdot \prod R_i^{m_i}))^{1/e}$
  - the signature is (A, e, v)
- verification: check if

$$Z = A^e \cdot S^v \cdot \prod R_i^{m_i} \quad ?$$

Issuing a certificate for values $m_1, ..., m_l$

- somewhat complicated since the Issuer can learn only some attributes to be signed
- **method**: a two-party protocol to compute CL signature of the Issuer, algorithm draft:
  - the user chooses v' at random and computes $U := S^{v'} \cdot \prod R_i^{m_i}$ apart from known attributes that are not included in the product $\prod R_i^{m_i}$
  - the user creates a ZKP that U computed in this way, in particular that
    - the user knows hidden attributes
    - the user uses the same attributes as commited
  - the issuer checks the ZKP proofs
  - the issuer chooses at random: v'' and a prime e
  - the issuer computes

$$Q := Z / (U \cdot S^{v''} \cdot \prod_{\mathrm{known}\, m_i} R^{m_i}) \text{ and } A := Q^{1/e}$$

  - (A, e, v'') is sent to the user together with a ZKP proof of corectness
  - the user computes $v := v' + v''$, checks the proof and validity of signature (A, e, v)

Presenting a credential

complicated: also involves proofs over encrypted values and the range of attributes. Some attributes may be revealed, but some must stay hidden. Moreover, **the certificate must not be revealed** (to ensure unlinkability) .

some details for verification of certificate without revealing it:

- value $\widetilde{m}_i$ is chosen for each hidden attribute m_i, that is, $i \in A_{\bar{r}}$
- the user chooses r_A at random and randomizes (A, e, v):
  - $A' := A \cdot S^{r_A}$, $v' := v - e \cdot r_A$
- so called t-values computed:
  - chosen at random: $\tilde{e}$,$\tilde{v}'$
  - $\tilde{Z} := (A')^{\tilde{e}} \cdot S^{\tilde{v}'} \cdot \prod R^{\widetilde{m}_i}$
- these t-values $\tilde{Z}$ and t values from other proofs plus some other data are hashed to get challenge c
- signatures components (s-values) are derived:
  - $\hat{e} := \tilde{e} + c \cdot e$
  - $\hat{v}' := \tilde{v}' + c \cdot v'$
  - $\hat{m}_i := \widetilde{m}_i + c \cdot m_i$

Credential verification - based on recomputation of t-values and recomputing c.

$\tilde{Z}$ recomputed as:

$$(A')^{\hat{e}} \cdot \prod_{i \in A_{\bar{r}}} R_i^{\widehat{m_i}} \cdot S^{\hat{v}'} / \left(\frac{Z}{\prod_{i \notin A_{\bar{r}}} R^{m_i}} \right)^c$$

- we remove from Z the expressions R^m that correspond to the known attributes
- what is left will cancel the $c \cdot e$, $c \cdot v'$, $c \cdot m_i$ when using the exponents $\hat{e}$, $\hat{v}'$, $\hat{m}_i$

ranges have to be checked, etc

...

IDENTIFICATION

running wireless communication protocol may enable tracing a user.

Threats:

- explicit exchange of identifiers: an eavsdropper learns who is communicating with whom
- strong cryptographic proofs created during identification: can be misused for proving presence to the third parties

elimination of explicit identifiers:

- at each communication round Alice and Bob create random nonce (nonces) for the next round
- even more secure: if n is such a nonce, then Alice uses n' where n' is the same as n except for a limited number of bits at random positions

  (so the adversary has to follow Alice and Bob without long interruptions)

deniability:

- the idea is that a transcript of a communication (including the answer from the Prover created with his private key) can be simulated

  consequence: a third party has no grounds to believe the communication transcript presented to him

- **wrong example:** challenge-response algorithm with digital signature:

  1. the Verifier selects x at random and sends to the Prover
  2. the Prover returns his signature s over x

  unfortunately: s can serve as a proof of the claim of the Verifier: "I have talked to Prover" if x is a signature of the Verifier or somthing that only could be created by the Verifier

- **good example:** static Diffie-Hellman protocol

- **good example:** Stinson-Wu for Prover with the key pair $(a, A = g^a)$

  1. Verifier chooses x at random, computes $X := g^x$ and $Y := \mathrm{Hash}(A^x)$
  2. Verifier sends X, Y to Prover
  3. Prover computes $Z := X^a$ and aborts if $Y \neq \mathrm{Hash}(Z)$
  4. Prover sends Z
  5. Verifier accepts iff $Z = A^x$

Stinson-Wu protocol

- Stinson-Wu does not create an oracle for DH Problem, Verifier must send a challege for which *somebody* knows x
- it is untrue that Verifier must know x:

`Preparation:`

  - Eve creates correct X, Y as well as $\mathrm{Enc}_{\mathrm{Hash}(Z)}(x)$
  - Eve sends these data to Verifier

Identification:

  - Verifier sends X, Y to Prover
  - Prover computes $Z := X^a$ and aborts if $Y \neq \mathrm{Hash}(Z)$
  - Prover sends Z
  - Verifier computes $\mathrm{Hash}(Z)$ and uses it as a key to decrypt and derive x
  - Verifier accepts iff $Z = A^x$

Proof of Interaction: **Verifier returns x to Eve as a proof of interaction with Prover**

Anonymous Transactions

idea:

- transactions records publicly available in a distributed ledger (DLT) $\Rightarrow$ undeniability, no backdating, possibility to detect double spending (if...) , anti Money Laundering (if...) ...
- however, we must not create a public Big Brother

core mechanism for digital currencies:

cash hides money flow, this should be the key property of digital money as well

examples below will be taken from Monero

User keys and hidden recipient

user keys (EC notation):

- private keys a, b
- public keys: $A = a \cdot G$, $B = b \cdot G$
- sometimes (a, B) revealed (tracking key) – if the transactions have to be deanonymized

Creating transaction with a hidden recipient: (Alice sends to Bob)

- Alice fetches the public key (A, B)
- Alice chooses r at random, $R := r \cdot G$
- Alice generates one-time public key $P := \mathrm{Hash}(r \cdot A) \cdot G + B$
- Alice uses P as a one-time destination key for the transaction containing metadata R

Receiving a transaction by Bob

- Bob tries each transaction posted:
  - → compute $P' := \mathrm{Hash}(a \cdot R) \cdot G + B$
  - → if this is the right transaction, then $P = P'$ and Bob knows it is for him
- Bob calculates the one-time private key:

$$x = \mathrm{Hash}(a \cdot R) + b$$

- Bob can spend the money obtained in the transaction by signing with x

Remarks:

1: Receiving a transaction possible with (a, B), while (a, B) does not enable to compute x

2: Still only a partial anonymity: using x and the public key P would indicate who has got transaction with P from Alice

One time ring signatures

idea:

- instead of signing with x and showing P, a ring signature created:
  - a set of public keys $P_1, P_2, \ldots., P_m$ from transactions chosen at random (transaction value must be the same)
  - x used for signing
- any two ring signature of this kind created with x will be linked immediately

Goals achieved:

- double spending exposed
- m-anonymity concerning where the e-coin comes from

Creating one-time ring signature

for key pair (x, P)

1. compute image key

$$I := x \cdot \mathrm{Hash}(P)$$

2. choose a ring of keys $\mathcal{P}(P_{0,\ldots}, P_n)$ where $P_s = P$ for some s
3. choose $q_0, \ldots, q_n$ at random
4. choose $w_0, \ldots, w_n$ at random, except for w_s
5. calculate for $i \neq s$

$$L_i := q_i \cdot G + w_i \cdot P_i$$

6. calculate $L_s := q_s \cdot G$
7. calculate for $i \neq s$

$$R_i := q_i \cdot \mathrm{Hash}(P_i) + w_i \cdot I$$

8. calculate $R_s := q_s \cdot \mathrm{Hash}(P_s)$

9. calculate the non-interactive challenge:

$$c := \mathrm{Hash}(\mathrm{message}, L_0, ..., L_n, R_0, ..., R_n)$$

10. calculate individual components:

    - for $i \neq s$: $c_i = w_i,$ and $r_i = q_i$

    - $c_s := c - \sum_{i \neq s} c_i$

    - $r_s := q_s - c_s \cdot x$

11. output signature $(I, c_0, ..., c_n, r_0, ..., r_n)$

Verification

L_i recomputed as $L_i' := r_i \cdot G + c_i \cdot P_i$

R_i recomputed as $R_i' := r_i \cdot \mathrm{Hash}(P_i) + c_i \cdot I$

test:

$$\sum c_i = \mathrm{Hash}(\mathrm{message}, L_0', ..., L_n', R_1', ..., R_n')$$

Linking:

via the same I

Concept used:

to close the ring somewhere a schnorr signature must be created that applies to two generators simultaneously:

- P_s (which is hidden)
- I (which is explicit)

Many extensions possible (e.g. a transaction signed with multiple keys)