# Anonymity in information processing, storage and transmission

Sergey Bezzateev,

bsv@aanet.ru

SUAI, Russia

# Anonimity

**Anonymity** is derived from the Greek word **ἀνωνυμία** - *anonymia*, meaning "without a name" or "namelessness“.

General meaning: personal identity, or personally identifiable information  of that person is not known.

# Anonimity

- Who?
- Where?
- What?

Microsoft : “10 Immutable Laws of Security”

- **Law #9: Absolute anonymity isn't practical, in real life or on the Web**

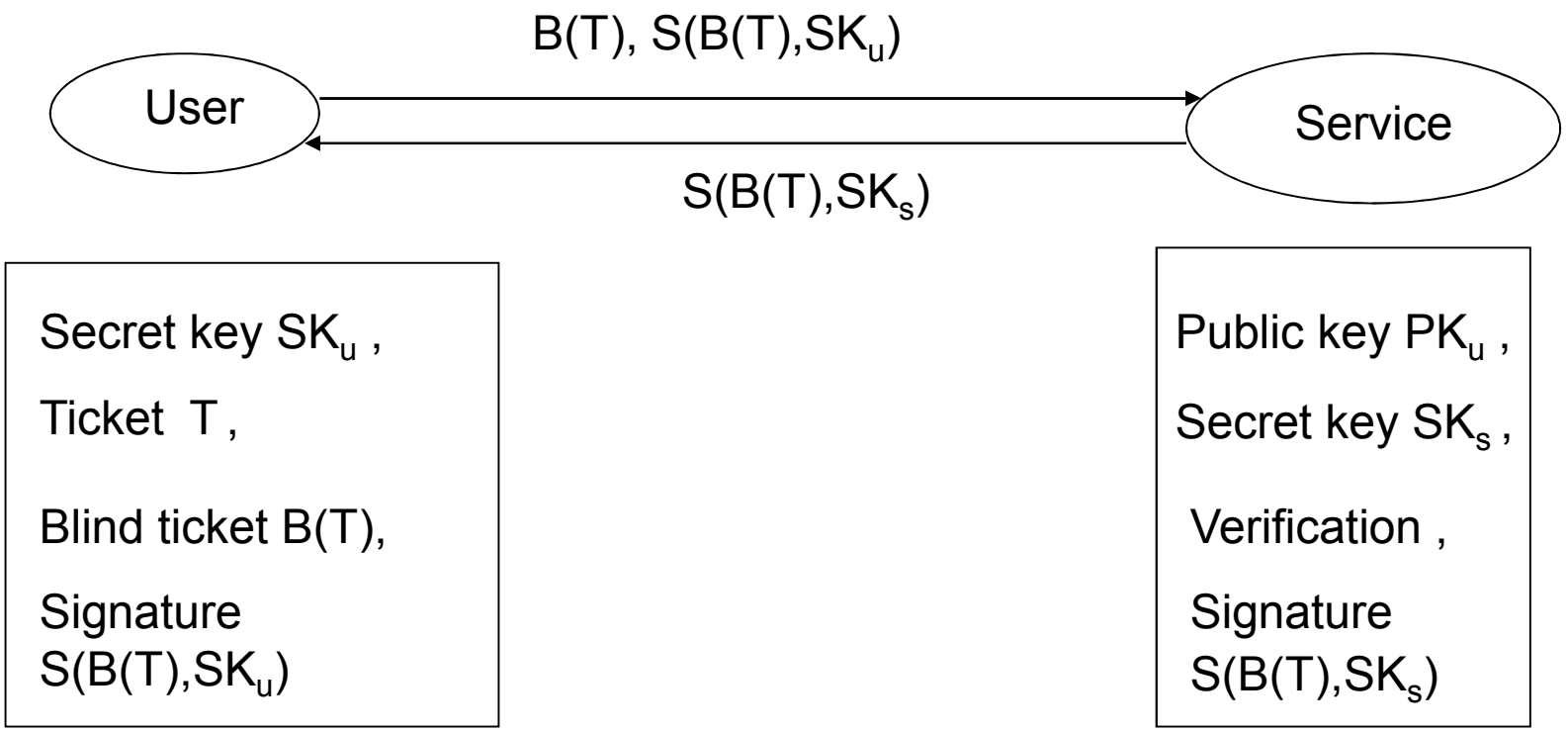
# Instruments

- Blind signature
- Onion functions– $F(k_i, F(k_{i-1}, \ldots F(k_1, x)..)$
- Error correcting codes
- Locally decodable codes

# Problem “WHO?”

- E-voting
- E-commerce
- E-libraries

# Blind ticket



# Blind ticket

*Service*

Verification

$V(B(T), S(B(T),SK_u) , PK_u) = \{true,false\}$

Sign

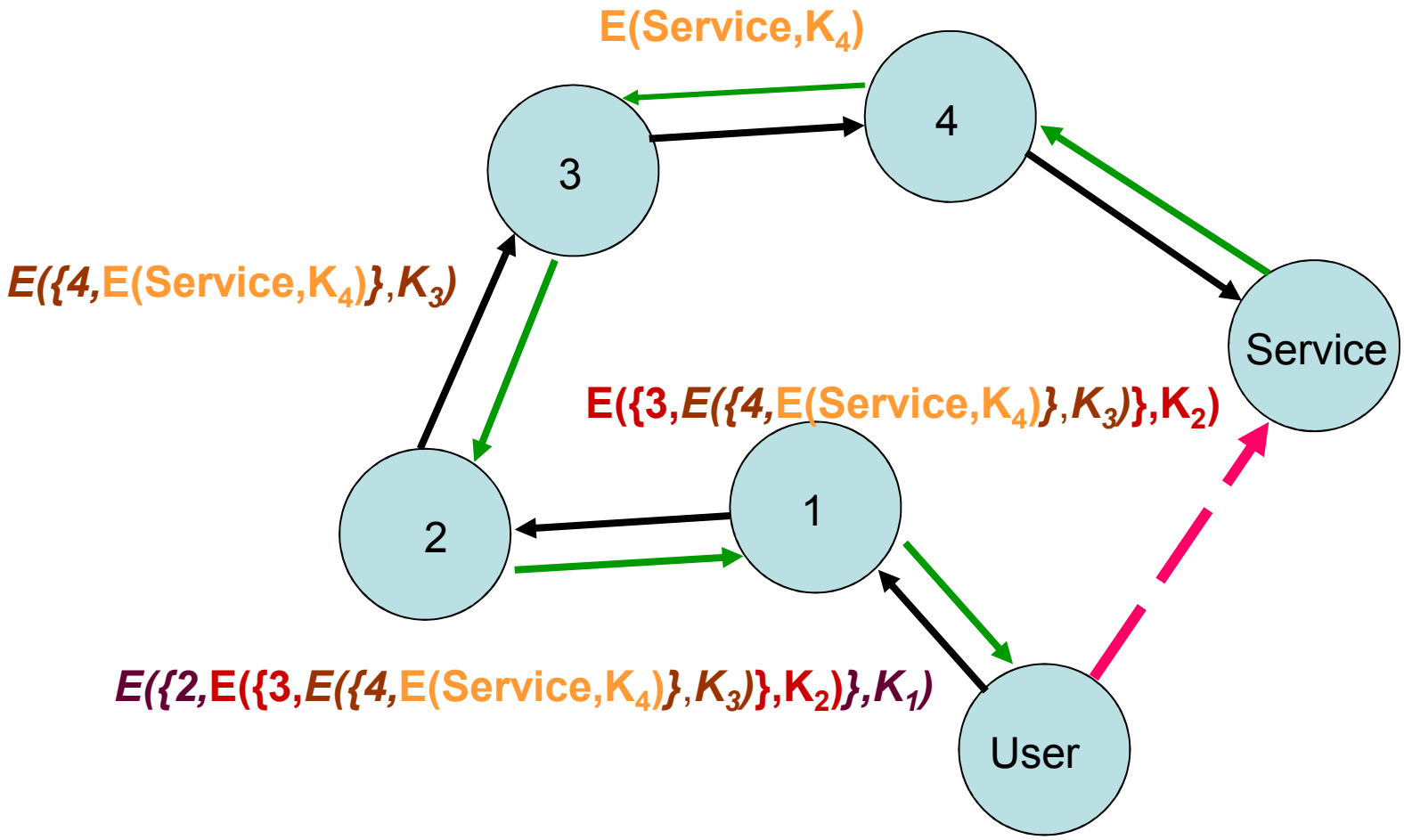
$S(B(T),SK_s)$

*User*

Obtain ticket with signature

$T , S(T,SK_s)$

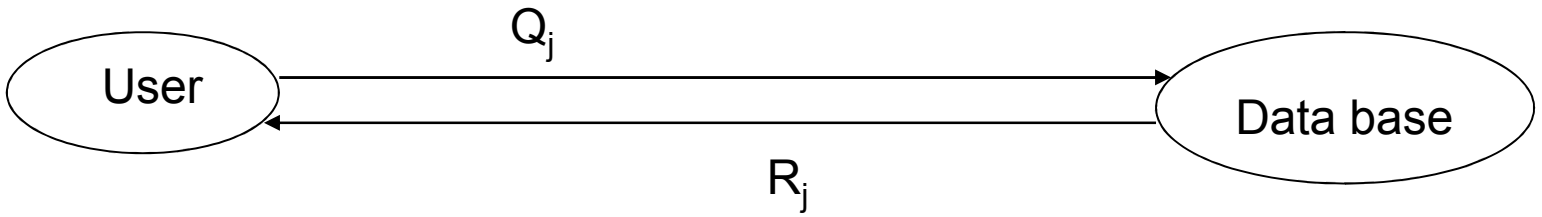
# Problem “WHERE?”



# Problem “WHAT?”

- E-voting
- Hiding calculations ( in cloud computers)
  - Hiding data
  - Hiding functions
- Hiding querying  to databases

# Computational Private Information Retrieval(PIR) Protocol




Decryption key $D_{PIR}$ ,

Choose position j

in database,

Query $Q_j$

$R_j = Q_j(x)$ ,

x – database

or message ,

$R_j$ - response

# Error correcting codes in the PIR protocol

Decryption key – (L,G) and (L,g) – codes.

Message -

$$x=[(a_1+b_1)\cdot P_1, (a_2+b_2)\cdot P_2, \dots, (a_n+b_n)\cdot P_n],$$

where

$a_i$ - any code word from (L,G)-code with minimal distance D,

$b_i$ – information code word from (L,g)-code , $wt(b_i)=d\leq(D-1)/2$,

$P_i$ – permutation matrix,

(L,G)-code is subcode of (L,g)-code.

# Error correcting codes in the PIR protocol

Query – $Q_j = [h_1^*, h_2^*, \ldots, H_j^*, \ldots h_n^*]$

where $h_i^* = A_i \cdot h \cdot P_i$ , h- parity check matrix

for (L,g) code, $A_i$ –random $r \times r^*$ -matrix ,

$H_j^* = A_j \cdot H \cdot P_j$ , H- parity check matrix for (L,G) code,
$A_j$ – nonsingular r x r – matrix,

r*,r – redundancy of (L,g) and (L,G)- codes.

$R_j = Q_j(x) = x \cdot Q_j^T = b_j \cdot H^T \cdot A_j^T$ ,

By using $A_j^{-1}$ and decoding algorithm for (L,G)-code it is easy to restore $b_j$

# THANK YOU!

Questions ???