KU LEUVEN

Distributed Systems - **Assignment**

Content may be borrowed from other resources.
See the last slide for acknowledgements!

Privately (and Unlinkably) Exchanging Messages Using a Public Bulletin Board*

Jaap-Henk Hoepman
Institute for Computing and Information Sciences (ICIS)
Radboud University
the Netherlands
jhh@cs.ru.nl

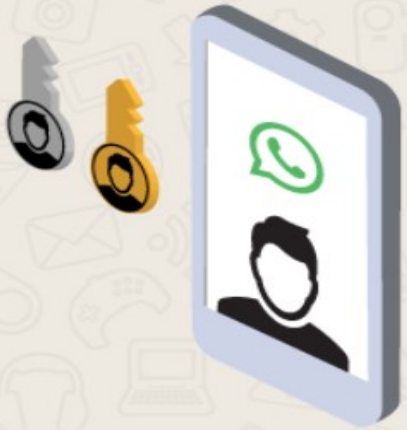
ABSTRACT

We implement a secure and privacy friendly asynchronous unidirectional message transmission protocol using a *public* bulletin board that makes individual send or receive events unlinkable to one another. While the clients must securely run in the user's endpoint device, the bulletin board can be hosted on an arbitrary public cloud at no additional risk. In fact the protocol provides the same unlinkability guarantees as the underlying mixing network. The protocol is efficient, and the central bulletin board can adaptively be scaled and distributed depending on the load. We show how the basic unidirectional protocol can be used to hide the metadata in bidirectional message exchange applications like WhatsApp, and how it can be used to implement a private pres-

a secure contact that allows you to securely and anonymously communicate with that contact at a later stage.

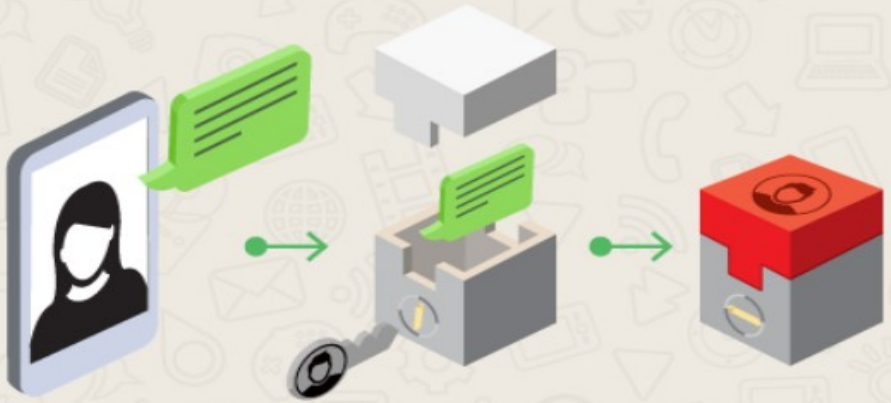
Our research is partly motivated by the following use case. Consider a journalist that wants to stay in touch with (anonymous) contacts and informants in a hostile environment, like a civil war zone or a country with limited protection to journalists (or informants). Exchanging phone numbers to stay in touch is dangerous, as these can be traced back to their owner. Yet even very secure and privacy friendly messaging applications like Signal need such a phone number to create an account and to establish first contact. If you don't even need a phone number to connect to each other, loss or theft of your phone means your contacts cannot be traced (as would be the case if their phone

1 Two keys, public and private are generated when a user opens WhatsApp for the first time. The encryption process takes place on your phone.



2 The private key remains with the user on the phone. The public key is transmitted through the server to the receiver.

3 The public key encrypts the sender's message on the phone even before it reaches the server.



4 The server is only used to transmit the encrypted message. Only the receiver's private key can unlock the message. No third party including WhatsApp can read the message.

WhatsApp

KU LEUVEN

WhatsApp security and privacy properties

- WhatsApp hides the **content** of the communication
- WhatsApp does not hide the sender and recipient (**~metadata**)

- The *social graph* should be protected against externals *and* service provider
- Social graph = who is connected to whom

- Alternative: implementing a peer-to-peer protocol
  - **BUT**: phones do not have fixed IP addresses

- **Proposed solution** ☾ centralized + asynchronous messages

tor network for communication between the server and the client

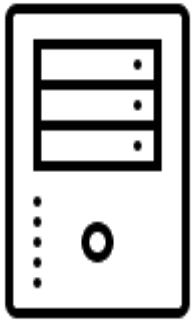
if bob has 1000 connections -> need for 1000 mailboxes

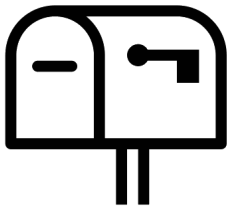
A Simple, but Bad Idea

(k_{AB}, K_{AB})
(s_{AB}, S_{AB})
Bob: S_{BA},K_{BA},
`pqzvqupnbqpmup`

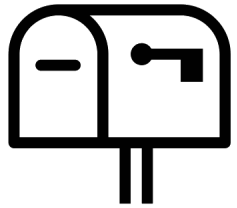
(k_{BA}, K_{BA})
(s_{BA}, S_{BA})
Alice: S_{AB},K_{AB},
`apreiqonvcpaeece`

$\{Sign(Message, s_{AB})\}\ K_{BA}$





`apreiqonvcpaeece`



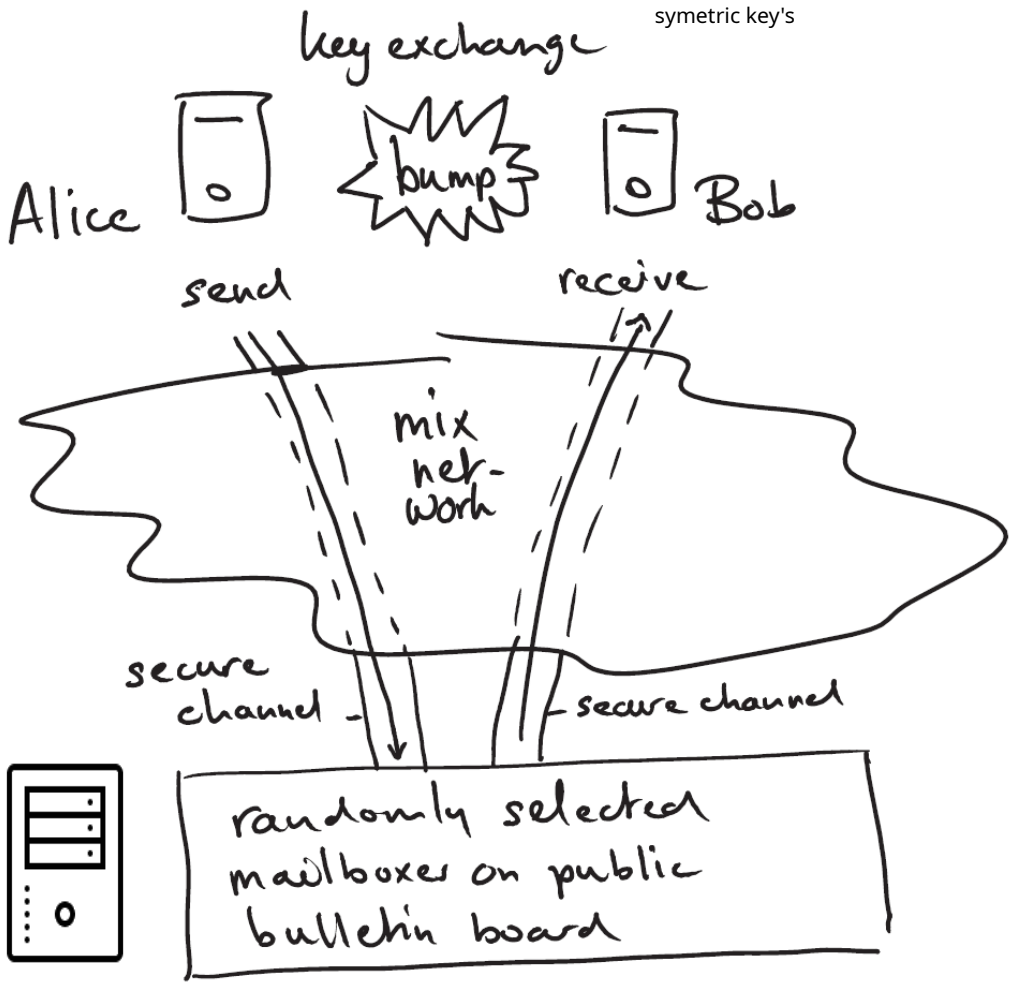
`pqzvqupnbqpmup`

pseudonymous
mail boxes
In the cloud

Assumption: mix network between users and bulletin board service
☹ Server will notice conversations between pseudonymous entities
☹ Alice checks mails at morning ☾ server can link all mailboxes of same user

Social graph reconstruction

Privately (and Unlinkably) Exchanging Messages Using a Public Bulletin Board



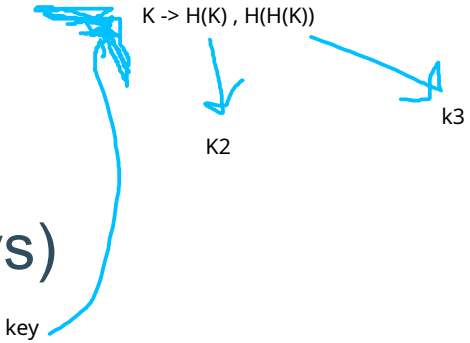
Requirements

- Confidentiality
- Integrity
- Authenticity
- Unlinkability of events
- Unlinkability of relationships
- Forward secrecy
- Availability

Crypto functions

- **Authenticated encryption scheme** (confidentiality, integrity, authenticity)
  - $\{[m||idx||tag]\}_{AB}$ send message , identifier and tag and encrypt it with a secret key used to communicate from A to B
  - $m||idx||tag \approx \mathbf{open}_{AB}(\{[m||idx||tag]\}_{AB})$

opening with a key is with the same key -> symetric encryption



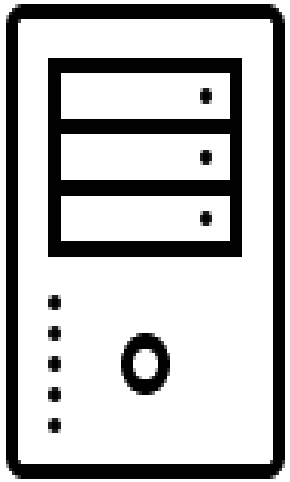
- **Key deriviation function** (generating new keys)
  - KDF(.): K ☾ K
  - Perfect forward secrecy

you could make a new secret key -> you cannot construct the previous key

- **Cryptographic hash function** (preventing deletion of values at will)
  - B(.): T ☾ T

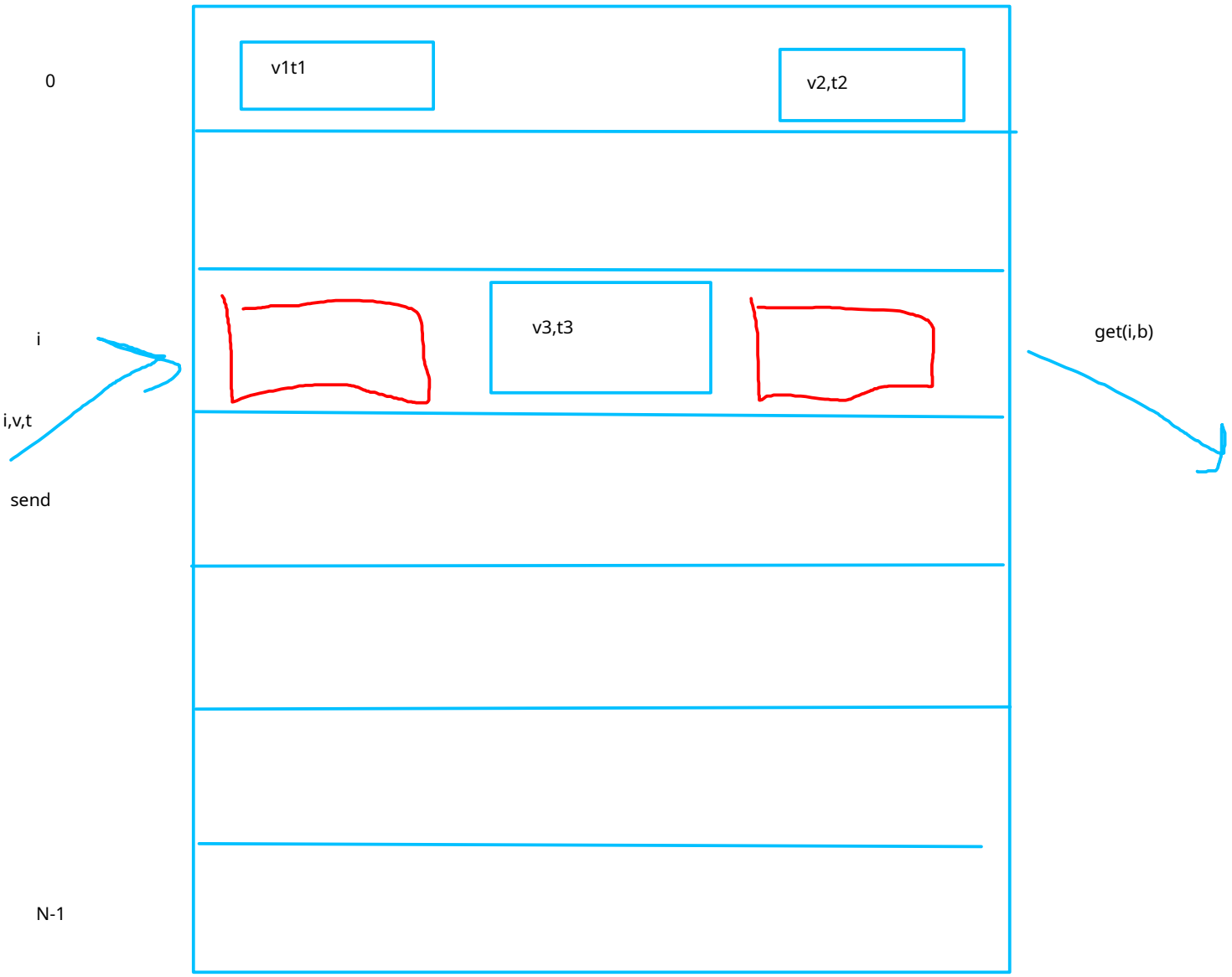
Operations on BB

- Bulletin Board B[] is an array of n cells, indexed by arbitrary integers modulo n
- Each cell B[i] contains a set of value/tag pairs <v,t>



add(i, v, t): Add $\langle v, t \rangle$ to the set at cell i: $B[i] := B[i] \cup \{\langle v, t \rangle\}$.

get(i, b): Let $t = \mathcal{B}(b)$. If $\langle v, t \rangle \in B[i]$ for some value v, return v and remove $\langle v, t \rangle$ from $B[i]$. Otherwise return $\perp$, and leave $B[i]$ unchanged.



i is the entry

board gets the the hash of b : if the ahs corresponds to t , we return v , and if its not present ; then we reutrn nothing

b = tag

$setup_{AB}$

bump : secret key AB from alice to bob , BA is for BOB to alice

$K_{AB}, idx_{AB}, tag_{AB}$
$K_{BA}, idx_{BA}, tag_{BA}$

$K_{AB}, idx_{AB}, tag_{AB}$
$K_{BA}, idx_{BA}, tag_{BA}$

$send_{AB}$ -- $receive_{AB}$

KDF(.) B(.)

$K_{AB}, idx_{AB}, tag_{AB}$

$K_{BA}, idx_{BA}, tag_{BA}$

this is the first entry only[2]

KDF(.) B(.)

$K_{AB}, idx_{AB}, tag_{AB}$

$K_{BA}, idx_{BA}, tag_{BA}$

function $send_{AB}(m)$

random value

$idx' \in_R \{0, \ldots, n-1\}$

$tag' \in_R T$

$u := \{[m \,||\, idx' \,||\, tag']\}_{AB}$

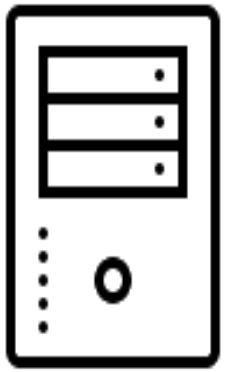
at entry idx , and we provide the hash of the tag (random number)

$\mathbf{write}(idx_{AB}, u, \mathscr{B}(tag_{AB}))$

$(idx_{AB}, tag_{AB}) := (idx', tag')$

$K_{AB} := \mathrm{KDF}(K_{AB})$

they define the tag and the enrry of the next message



function $receive_{AB}()$

$u := \mathbf{get}(idx_{AB}, tag_{AB})$

if $u \neq \perp$

$\wedge\ (m \,||\, idx' \,||\, tag') := open_{AB}(u)$ is successful

then $(idx_{AB}, tag_{AB}) := (idx', tag')$

$K_{AB} := \mathrm{KDF}(K_{AB})$

return m

else return $\perp$

Advanced features

- Supporting recoverability of corrupted states
- Increasing scalability ☾ partitioning the BB in chunks
- Tackling Denial-of-Service attacks

Assignment

- **Implement the proposed Privacy-Friendly Bulletin Board** (Client + Server application)
  - *Java RMI* as communication technology
  - *Java JCA/JCE* to realise crypto protocols
  - Submit code on github

- **Submit a report** -- max 2 pages -- including following aspects
  - Relevant design decisions (+ extensions) **(0,5 pages)**
  - Detailed SWOT analysis **(1,5 pages)**
  - Link to code on github

Assignment

- **Deadline code and rapport submissie: 11 december 2025**

- **Mondelinge evaluatie (datum: 18 december 2025)**
  - Een demonstratie van de web applicatie [6 min] distributed app is good .
  - Vier vragen rond genomen ontwerpbeslissingen en inzichten aan elke student afzonderlijk [12 min]
  - Eén code sample per student waarover vragen worden gesteld [7 min]

Assignment

- **De evaluatie criteria zijn als volgt:**
  - Volledigheid en creativiteit van de technologische oplevering (30%)
  - Demonstratie van het project (10%)
  - Beantwoorden van vragen rond genomen ontwerpbeslissingen (35% - individueel)
  - Beantwoorden van vraag rond code sample (25% - individueel)

Wie op individuele vragen niet kan antwoorden, kan niet slagen voor dit project.

everyone should understand everything