A Privacy-Preserving E-Ticketing System for Public Transportation Supporting Fine-Granular Billing and Local Validation

Ivan Gudymenko
ivan.gudymenko@mailbox.tu-dresden.de
http://wwwpub.zih.tu-dresden.de/~igudym/

Chair of Privacy and Data Security
Faculty of Computer Science, TU Dresden

11th of September, 2014
OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution
Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution
E-ticketing in Public Transport

[Courtesy of MünsterscheZeitung.de]
**What an E-Ticket is**

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket” at a user device:
  - Smart Card
  - NFC-enabled smart phone
What an E-Ticket is

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket“ at a user device:
  - Smart Card
  - NFC-enabled smart phone
WHAT AN E-TICKET IS

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket” at a user device:
  - Smart Card
  - NFC-enabled smart phone
**What an E-Ticket is**

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket” at a user device:
  - Smart Card
  - NFC-enabled smart phone
WHAT AN E-TICKET IS

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket” at a user device:
  - Smart Card
  - NFC-enabled smart phone
WHAT AN E-TICKET IS NOT

- A widely used “online ticket” (air transport, etc.)
- Pointing to the respective entry in the back-end DB
What an E-Ticket is NOT

- A widely used “online ticket” (air transport, etc.)
- Pointing to the respective entry in the back-end DB

![Online Ticket Image]
WHAT AN E-TICKET IS NOT

- A widely used “online ticket” (air transport, etc.)
- Pointing to the respective entry in the back-end DB
Non-Interactive vs. Interaction-Based

- Non-Interactive

- Interaction-based
  - enable fine-granular billing.
Non-interactive vs. Interaction-based

- Non-interactive

- Interaction-based
  - enable fine-granular billing.
**Non-Interactive vs. Interaction-Based**

- Non-interactive
- Interaction-based
  - enable fine-granular billing.
NON-INTERACTIVE VS. INTERACTION-BASED

- Non-interactive

- Interaction-based
  - enable fine-granular billing.
Non-interactive vs. Interaction-based

- Non-interactive
- Interaction-based
  - enable fine-granular billing.
Non-interactive vs. Interaction-based

- Non-interactive

- Interaction-based
  - enable fine-granular billing.
E-ticketing: A General Application Scenario

Station A  \(\xrightarrow{\text{Trip}}\)  Station B  \(\xrightarrow{\text{Backbone network}}\)  Back-end

Terminal 1 \((\text{Check-in})\)  Terminal 2 \((\text{Check-out})\)

A Privacy-Preserving E-Ticketing System
Ivan Gudymenko
Faculty of Computer Science, TU Dresden
OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution
CONVENTIONAL E-TICKETING SYSTEMS: PRIVACY

- Primary focus on functionality (and security)
- Privacy is often not directly considered
Conventional E-ticketing Systems: Privacy

- Primary focus on functionality (and security)
- Privacy is often not directly considered
Conventional E-ticketing Systems: Privacy

- Primary focus on functionality (and security)
- Privacy is often not directly considered
Privacy Considerations

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification
Privacy Considerations

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification
Privacy Considerations

- Traceability
  - Transactions linkability
- Customer profiling
- Ubiquitous identification
Privacy Considerations

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification
Privacy Considerations

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification
Privacy Considerations

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification
A Privacy-Preserving E-Ticketing System

Ivan Gudymenko

Faculty of Computer Science, TU Dresden

A General System Architecture

Check-in/out

Backbone Network

E-tickets

Real-time

E-ticket 1

E-ticket 2

...

E-ticket n

Terminals

Non-real-time

Terminal 1

Terminal 2

...

Terminal n

Back-end

TR Processing:
- Singulation
- Billing
- Identification
A Privacy-preserving E-ticketing System: Core Requirements
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy

(a) Against terminals

<table>
<thead>
<tr>
<th>Identification</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

(2) Fine-granular billing support

(3) Loose-coupling

(4) Efficiency

(5) Check-in/out events handling

Multilateral security
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy

(a) Against terminals
   Identification: no
   Correlation: no

(b) Against back-end
   Identification: no
   Correlation: yes
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy

(a) Against terminals
   Identification: no
   Correlation: no

(b) Against back-end
   Identification: no
   Correlation: yes

(c) Against observers
   PII Derivation: no
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy

(a) Against terminals
   Identification: no
   Correlation: no

(b) Against back-end
   Identification: no
   Correlation: yes

(c) Against observers
   PII Derivation: no

(2) Fine-granular billing support
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy

(a) Against terminals
- Identification: no
- Correlation: no

(b) Against back-end
- Identification: no
- Correlation: yes

(c) Against observers
- PII Derivation: no

(2) Fine-granular billing support

(3) Loose-coupling
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy

(a) Against terminals
   Identification: no
   Correlation: no

(b) Against back-end
   Identification: no
   Correlation: yes

(c) Against observers
   PII Derivation: no

(2) Fine-granular billing support

(3) Loose-coupling

(4) Efficiency
   Check-in/out events handling
A Privacy-preserving E-ticketing System: Core Requirements

(1) Privacy

(a) Against terminals
   Identification: no
   Correlation: no

(b) Against back-end
   Identification: no
   Correlation: yes

(c) Against observers
   PII Derivation: no

(2) Fine-granular billing support

(3) Loose-coupling

(4) Efficiency
   Check-in/out events handling

(5) Multilateral security
CORE SYSTEM REQUIREMENTS: INHERENT CONTRADICTIONS

(1) Privacy

(a) Against terminals
   - Identification: no
   - Correlation: no

(b) Against back-end
   - Identification: no
   - Correlation: yes

(c) Against observers
   - PII Derivation: no

(2) Fine-granular billing support

(3) Loose-coupling

(4) Efficiency
   - Check-in/out events handling

(5) Multilateral security
OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution
Related Work/Other Solutions

- Academic solutions: not covering all requirements
- Industry: essentially not interested in privacy preservation
RELATED WORK/OTHER SOLUTIONS

- Academic solutions: not covering all requirements
- Industry: essentially not interested in privacy preservation
\textbf{Related Work/Other Solutions}

- Academic solutions: not covering all requirements
- Industry: essentially not interested in privacy preservation
Core Challenges

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.

- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.
Core Challenges

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.

- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.
Core Challenges

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.

- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.
Core Challenges

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.

- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.
Core Challenges

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.

- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.
CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.

- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.
Core Challenges

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.

- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.
Outline

Introduction

Privacy Issues

State-of-the-Art and Core Challenges

Our Solution
**Adversary Model**

1. *(Outsider)* External observers can observe the communication between terminals and e-tickets (front-end)
   → no PII derivation

2. *(Insider)* Terminals can analyse the logs, may leak information.
   → No tracking and identification of valid e-tickets

3. *(Insider)* Back-end can process all information pieces under its control
   → No direct identification of any e-ticket

→ Insider/outsider with respect to the involvement into the system flow.
Adversary Model

1. (Outsider) **External observers** can observe the communication between terminals and e-tickets (front-end)
   → no PII derivation

2. (Insider) **Terminals** can analyse the logs, may leak information.
   → No tracking and identification of valid e-tickets

3. (Insider) **Back-end** can process all information pieces under its control
   → No direct identification of any e-ticket

→ Insider/outsider with respect to the involvement into the system flow.
Adversary Model

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)
   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.
   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control
   → No direct identification of any e-ticket

→ **Insider/outsider** with respect to the involvement into the system flow.
Adversary Model

1. *(Outsider)* External observers can observe the communication between terminals and e-tickets (front-end)
   → no PII derivation

2. *(Insider)* Terminals can analyse the logs, may leak information.
   → No tracking and identification of valid e-tickets

3. *(Insider)* Back-end can process all information pieces under its control
   → No direct identification of any e-ticket

→ Insider/outsider with respect to the involvement into the system flow.
**Adversary Model**

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ **Insider/outsider** with respect to the involvement into the system flow.
Adversary Model

1. *(Outsider)* External observers can observe the communication between terminals and e-tickets (front-end)
   \[\rightarrow \text{no PII derivation}\]

2. *(Insider)* Terminals can analyse the logs, may leak information.
   \[\rightarrow \text{No tracking and identification of valid e-tickets}\]

3. *(Insider)* Back-end can process all information pieces under its control
   \[\rightarrow \text{No direct identification of any e-ticket}\]

\[\rightarrow \text{Insider/outsider with respect to the involvement into the system flow.}\]
ADVERSARY MODEL

1. *(Outsider)* External observers can observe the communication between terminals and e-tickets (front-end)
   → no PII derivation

2. *(Insider)* Terminals can analyse the logs, may leak information.
   → No tracking and identification of valid e-tickets

3. *(Insider)* Back-end can process all information pieces under its control
   → No direct identification of any e-ticket

→ Insider/outsider with respect to the involvement into the system flow.
Adversary Model

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)
   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.
   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control
   → No direct identification of any e-ticket

→ *Insider/outside* with respect to the involvement into the system flow.
**Solution Building Blocks**

- **Mutual Authentication** (front-end)
  - non-identifiability
  - non-traceability

- **Local Revocation** (front-end)
  - non-identifiability
  - non-traceability

- **Path Reconstruction** (back-end)
  - non-identifiability
  - traceability (singulation)

---

*Privacy-preserving eTicketing System*
**Solution Building Blocks (2)**

**Tools available:**
- Group Signatures
- ZKP of possession of a valid credential

**Tools available:**
- Dynamic Accumulators
- Homomorphic encryption and ZKP of correctness

**Tools available:**
- Predefined Matrix-based
- Private Information Retrieval?
**Solution Building Blocks: Summary**

- **Tools available**:
  - Group Signatures
  - ZKP of possession of a valid credential

- **Tools available**:
  - Dynamic Accumulators
  - Homomorphic encryption and ZKP of correctness

- **Tools available**:
  - Predefined Matrix-based
  - Other approaches?

- **Chosen approach**:
  - A slightly modified certificate-based authentication

- **Chosen approach**:
  - A custom blacklisting scheme

- **Chosen approach**:
  - A custom pseudonymisation scheme

---

**Privacy-preserving eTicketing System**

- **Mutual Authentication (front-end)**
  - non-identifiability
  - non-traceability

- **Local Revocation (front-end)**
  - non-identifiability
  - non-traceability

- **Path Reconstruction (back-end)**
  - non-identifiability
  - traceability (singulation)
A Privacy-Preserving E-Ticketing System

Ivan Gudymenko

Faculty of Computer Science, TU Dresden

23

Solution Outline

- Transport Authority
  - Operates on pseudonyms
  - Can correlate travel records for billing
  - Cannot identify users

- External TTP
  - Does not know user travel patterns
  - Can identify users
  - Performs end user billing

1. (Bill, Pseudonym)
2. (Bill, ID)
3. (Payment, ID)
4. Aggregated Payment

- Information minimization
- Separation of concerns
THE SUGGESTED PRIVACY-PRESERVING FRAMEWORK

Transport Authority (TA)

Check-in/$out

1. SC Establishment
2. Mutual Authent.
3. BL Check

Real-time

Backbone Network

Travel records
Processing:
- Singulation
- Billing

Back-end

Terminals

Terminal 1
Terminal 2
Terminal n

1. SC Establishment
2. Mutual Authent.
3. BL Check

Real-time

Non-real-time

Front-end Interaction
(time critical)

Back-end Processing

Distributed Billing

External TTP

- End User Identification
- End User Billing

External TTP (Bill, ID)

External TTP (Payment, ID)
**Path Reconstruction: Pseudonymisation**

- Privacy-preserving eTicketing System
  - Mutual Authentication (front-end)
    - non-identifiability
    - non-traceability
  - Local Revocation (front-end)
    - non-identifiability
    - non-traceability
  - Path Reconstruction (back-end)
    - non-identifiability
    - traceability (singulation)

**Chosen approach:**
- A slightly modified certificate-based authentication
- A custom blacklisting scheme
- A custom pseudonymisation scheme
A Privacy-Preserving E-Ticketing System

Ivan Gudymenko

Faculty of Computer Science, TU Dresden
Local Revocation Based on Blacklists

Privacy-preserving eTicketing System

Mutual Authentication (front-end)
- non-identifiability
- non-traceability

Local Revocation (front-end)
- non-identifiability
- non-traceability

Path Reconstruction (back-end)
- non-identifiability
- traceability (singulation)

Chosen approach:
- A slightly modified certificate-based authentication

Chosen approach:
- A custom blacklisting scheme

Chosen approach:
- A custom pseudonymisation scheme

Ivan Gudymenko
Faculty of Computer Science, TU Dresden
Local Revocation Based on Blacklists

- Based on the inherent homomorphism of an encryption scheme in use: $p_i^A = E_{k_{ta}}(p_i^T)$;

- Homomorphic property: $E(x \cdot r) = E(x)^r$;

- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow (E(x \cdot r), E(r))$;

- Black list: $\{y : y \in BL\}$;

- Check $SP_j$ against the BL: $\forall y \in BL, E(r) \in SPT : c \leftarrow E(r)^y$
  $c \neq E(x \cdot r) \ \forall c \in C.$
A Privacy-Preserving E-Ticketing System

Ivan Gudymenko

Faculty of Computer Science, TU Dresden

28

**Local Revocation Based on Blacklists**

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}}(P_i^T)$;

- Homomorphic property: $E(x \cdot r) = E(x)^r$;

- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow (E(x \cdot r), E(r))$;

- Black list: $\{y : y \in BL\}$;

- Check $SP_j$ against the BL: $\forall y \in BL, E(r) \in SPT : c \leftarrow E(r)^y$

  $c \neq E(x \cdot r) \ \forall c \in C.$
Local Revocation Based on Blacklists

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}} (P_i^T)$;

- Homomorphic property: $E(x \cdot r) = E(x)^r$;

- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow (E(x \cdot r), E(r))$;

- Black list: $\{y : y \in BL\}$;

- Check $SP_j$ against the BL: $\forall y \in BL, E(r) \in SPT : c \leftarrow E(r)^y$
  $c \overset{?}{=} E(x \cdot r) \forall c \in C.$
Local Revocation Based on Blacklists

- Based on the inherent homomorphism of an encryption scheme in use: \( P_i^A = E_{k_{ta}}(P_i^T) \);

- Homomorphic property: \( E(x \cdot r) = E(x)^r \);

- On validation, an e-ticket presents a tuple to a terminal:
  \( SPT \leftarrow (E(x \cdot r), E(r)) \);

- Black list: \( \{y : y \in BL\} \);

- Check \( SP_j \) against the BL: \( \forall y \in BL, E(r) \in SPT : c \leftarrow E(r)^y \)
  \( c \overset{?}{=} E(x \cdot r) \ \forall c \in C. \)
Local Revocation Based on Blacklists

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_i^t}(P_i^T)$;

- Homomorphic property: $E(x \cdot r) = E(x)^r$;

- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow (E(x \cdot r), E(r))$;

- Black list: $\{y : y \in BL\}$;

- Check $SP_j$ against the BL: $\forall y \in BL, E(r) \in SPT : c \leftarrow E(r)^y$
  $c \neq E(x \cdot r) \ \forall c \in C.$
Local Revocation Based on Blacklists

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}(P_i^T)$;

- Homomorphic property: $E(x \cdot r) = E(x)'$;

- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow (E(x \cdot r), E(r))$;

- Black list: $\{y : y \in BL\}$;

- Check $SP_j$ against the BL: $\forall y \in BL, E(r) \in SPT : c \leftarrow E(r)^y$
  
  $c \overset{?}{=} E(x \cdot r) \quad \forall c \in C.$
Local Revocation Based on Blacklists (2)

Check-in/Check-out

E-tickets
- E-ticket 1
- E-ticket 2
- ...
- E-ticket n

Terminals
- Terminal 1
- Terminal 2
- ...
- Terminal n

1. SC Establishment
2. Mutual Authent.
3. BL Check

Backbone Communication

\{ y : y \in BL \}

\[ SPT \leftarrow (E(x \cdot r), E(r)) \]

\[ E(r)^y \]

\[ y_1 \]

\[ y_2 \]

\[ \vdots \]

\[ y_b \]

if

\[ E(r)^y = E(x \cdot r) \]

reject
LOCAL REVOCATION: BOOSTING PERFORMANCE

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional $k$-anonymous identifier
- Results in partitioned blacklist and $\mathcal{O}(1)$ in the number of blacklisted elements
Local Revocation: Boosting Performance

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional $k$-anonymous identifier
- Results in partitioned blacklist and $O(1)$ in the number of blacklisted elements
Local Revocation: Boosting Performance

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional $k$-anonymous identifier
- Results in partitioned blacklist and $O(1)$ in the number of blacklisted elements
Local Revocation: Boosting Performance

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional $k$-anonymous identifier
- Results in partitioned blacklist and $O(1)$ in the number of blacklisted elements
Local Revocation: Boosting Performance

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional $k$-anonymous identifier
- Results in partitioned blacklist and $O(1)$ in the number of blacklisted elements
Privacy-preserving Mutual Authentication

Mutual Authentication (front-end)
- non-identifiability
- non-traceability

Local Revocation (front-end)
- non-identifiability
- non-traceability

Path Reconstruction (back-end)
- non-identifiability
- traceability (singulation)

Chosen approach:
- A slightly modified certificate-based authentication

Chosen approach:
- A custom blacklisting scheme

Chosen approach:
- A custom pseudonymisation scheme
Privacy-preserving Mutual Authentication

- A variation of the certificate-based authentication
- Alternatively, more profound group signatures can be used

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_e \leftarrow (k_{gr}^+, k_{gr}^-)$</td>
<td>group key pair of an e-ticket;</td>
</tr>
<tr>
<td>$K_t \leftarrow (k_t^+, k_t^-)$</td>
<td>unique key pair of a terminal;</td>
</tr>
<tr>
<td>$K_{ta} \leftarrow (k_{ta}^+, k_{ta}^-)$</td>
<td>unique key pair of a transport authority;</td>
</tr>
</tbody>
</table>
The Developed Prototype

- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250
The Developed Prototype

- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250
The Developed Prototype

- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250
The Developed Prototype

- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250
A SHORT DEMO

- Check-in/check-out session: a video demonstration
Prototype Performance

Execution time vs. the size of the blacklist

Execution time vs. the size of the blacklist

A Privacy-Preserving E-Ticketing System
Ivan Gudymenko
Faculty of Computer Science, TU Dresden
Integration of Our Solution into Real-World Systems

- Can be achieved at a relatively low cost, since:
  - Our solution is based on loose-coupling
  - Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
  - Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry
Integration of Our Solution into Real-World Systems

- Can be achieved at a relatively low cost, since:
  - Our solution is based on loose-coupling
  - Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
  - Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry
Integration of Our Solution into Real-World Systems

- Can be achieved at a relatively low cost, since:

- Our solution is based on loose-coupling

  - Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)

  - Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry
Integration of Our Solution into Real-World Systems

- Can be achieved at a relatively low cost, since:
  - Our solution is based on loose-coupling
  - Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
  - Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry
Integration of Our Solution into Real-World Systems

- Can be achieved at a relatively low cost, since:

- Our solution is based on loose-coupling

- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)

- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry
Integration of Our Solution into Real-World Systems

- Can be achieved at a relatively low cost, since:
  - Our solution is based on loose-coupling
  - Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
  - Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry
Integration of Our Solution into Real-World Systems

- Can be achieved at a relatively low cost, since:

- Our solution is based on loose-coupling

- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
  - E.g., KVP in eTicket Germany (VDV-KA)

- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry
INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
  - Our solution is based on loose-coupling
  - Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
  - Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry
INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
  - Our solution is based on loose-coupling
  - Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
  - Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry
Current Challenges: Concept

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
Current Challenges: Concept

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
**Current Challenges: Concept**

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
Current Challenges: Concept

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
Current Challenges: Concept

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
Current Challenges: Concept

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions
    (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default
CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)
Current Challenges: Implementation

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)
**Current Challenges: Implementation**

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)
CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)
CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)
CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)
CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)
Our solution: Summary

- A privacy-preserving framework for e-ticketing systems
- Satisfies all the requirements
- Goes in line with the adopted attacker model
Our solution: Summary

- A privacy-preserving framework for e-ticketing systems
- Satisfies all the requirements
- Goes in line with the adopted attacker model
Thank you for your attention!

Questions? Comments?
Suggestions?
REFERENCES I


REFERENCES II


Backup Slides
Fare Collection Approaches in E-ticketing

- Focus on CICO-based systems
**A General Application Scenario: Detailed**

- **E-ticket Distribution**
- **Trip Begin**
  - Check-in
  - On-board Reader (Terminal)
- **Event Processing Unit** (e.g. GPS-based)
- **Trip End**
  - Check-out
- **Back-end System**
  - Event Storage
  - Distance Calculation
  - Billing
  - Customer Accounts Management
  - Statistics

---

(1) (2a) (2b) (3)

A Privacy-Preserving E-Ticketing System

Ivan Gudymenko

Faculty of Computer Science, TU Dresden
E-TICKETING: TECHNOLOGIES AND STANDARDS

- RFID-based stack (proximity cards);
- NFC stack (NFC-enabled devices);
- E-ticket Germany: “Core Application” (VDV-KA)

<table>
<thead>
<tr>
<th>Architecture</th>
<th>ISO EN 24014-1 (conceptual framework)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Interfaces</td>
<td>EN 15320 <em>(logical level, abstract interface, security)</em></td>
</tr>
<tr>
<td></td>
<td>EN 1545 <em>(data elements)</em></td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 7816-4 <em>(commands, security)</em></td>
</tr>
<tr>
<td>Communication Interface</td>
<td>ISO 14443 <em>(parts 1-3 required)</em></td>
</tr>
</tbody>
</table>

The NFC Forum Specifications
- Reader/Writer
- Peer-to-Peer
- Card Emulation

The RFID-based E-Ticketing Stack

A Privacy-Preserving E-Ticketing System
Ivan Gudymenko
Faculty of Computer Science, TU Dresden
Why Fine-Granular Billing?

- An important feature (with high potential)
- Enables highly flexible fare polices (loyalty programs, individual discounts, etc.):
  - Essential for a modern public transport market
  - Personalized cards are often a preferred choice due to more services they provide [de Panizza et al., 2010];
- Several real-world systems are already supporting regular billing (Hannover, Phoenix).
**E-ticketing: Main Advantages**

- **For transport companies**
  - decrease in system maintenance costs;
  - significant reduction of payment handling costs;
  - fare dodgers rate improvement;
  - better support of flexible pricing schemes;
  - support of multiapplication/nontransit scenarios;
  - a high interoperability potential.

- **For customers**
  - faster verification of an e-ticket;
  - "pay as you go";
  - flexible pricing schemes;
  - increased usability.
# Fare System in Denmark

<table>
<thead>
<tr>
<th>Antal zoner</th>
<th>Voksen (kr)</th>
<th>Barn (kr)</th>
<th>Pensionist (kr)</th>
<th>Ung (kr)</th>
<th>Handicap (kr)</th>
<th>Cykel (kr)</th>
<th>Hund (kr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20,00</td>
<td>10,00</td>
<td>15,00</td>
<td>15,00</td>
<td>10,00</td>
<td>13,00</td>
<td>10,00</td>
</tr>
<tr>
<td>2</td>
<td>20,00</td>
<td>10,00</td>
<td>15,00</td>
<td>15,00</td>
<td>10,00</td>
<td>13,00</td>
<td>10,00</td>
</tr>
<tr>
<td>3</td>
<td>30,00</td>
<td>15,00</td>
<td>22,50</td>
<td>22,50</td>
<td>15,00</td>
<td>13,00</td>
<td>15,00</td>
</tr>
<tr>
<td>4</td>
<td>40,00</td>
<td>20,00</td>
<td>30,00</td>
<td>30,00</td>
<td>20,00</td>
<td>13,00</td>
<td>20,00</td>
</tr>
<tr>
<td>5</td>
<td>50,00</td>
<td>25,00</td>
<td>37,50</td>
<td>37,50</td>
<td>25,00</td>
<td>13,00</td>
<td>25,00</td>
</tr>
<tr>
<td>6</td>
<td>60,00</td>
<td>30,00</td>
<td>45,00</td>
<td>45,00</td>
<td>30,00</td>
<td>15,00</td>
<td>30,00</td>
</tr>
<tr>
<td>7</td>
<td>70,00</td>
<td>35,00</td>
<td>52,50</td>
<td>52,50</td>
<td>35,00</td>
<td>17,50</td>
<td>35,00</td>
</tr>
<tr>
<td>8</td>
<td>80,00</td>
<td>40,00</td>
<td>60,00</td>
<td>60,00</td>
<td>40,00</td>
<td>20,00</td>
<td>40,00</td>
</tr>
<tr>
<td>9</td>
<td>90,00</td>
<td>45,00</td>
<td>67,50</td>
<td>67,50</td>
<td>45,00</td>
<td>22,50</td>
<td>45,00</td>
</tr>
<tr>
<td>10</td>
<td>106,00</td>
<td>53,00</td>
<td>79,50</td>
<td>79,50</td>
<td>53,00</td>
<td>26,50</td>
<td>53,00</td>
</tr>
<tr>
<td>11</td>
<td>122,00</td>
<td>61,00</td>
<td>91,50</td>
<td>91,50</td>
<td>61,00</td>
<td>30,50</td>
<td>61,00</td>
</tr>
<tr>
<td>12</td>
<td>137,00</td>
<td>68,50</td>
<td>102,75</td>
<td>102,75</td>
<td>68,50</td>
<td>34,25</td>
<td>68,50</td>
</tr>
<tr>
<td>13</td>
<td>142,00</td>
<td>71,00</td>
<td>106,50</td>
<td>106,50</td>
<td>71,00</td>
<td>35,50</td>
<td>71,00</td>
</tr>
<tr>
<td>14</td>
<td>147,00</td>
<td>73,50</td>
<td>110,25</td>
<td>110,25</td>
<td>73,50</td>
<td>36,75</td>
<td>73,50</td>
</tr>
<tr>
<td>15</td>
<td>162,00</td>
<td>81,00</td>
<td>121,50</td>
<td>121,50</td>
<td>81,00</td>
<td>40,50</td>
<td>81,00</td>
</tr>
<tr>
<td>16</td>
<td>172,00</td>
<td>86,00</td>
<td>129,00</td>
<td>129,00</td>
<td>86,00</td>
<td>43,00</td>
<td>86,00</td>
</tr>
<tr>
<td>17</td>
<td>182,00</td>
<td>91,00</td>
<td>136,50</td>
<td>136,50</td>
<td>91,00</td>
<td>45,50</td>
<td>91,00</td>
</tr>
<tr>
<td>18</td>
<td>192,00</td>
<td>96,00</td>
<td>144,00</td>
<td>144,00</td>
<td>96,00</td>
<td>48,00</td>
<td>96,00</td>
</tr>
<tr>
<td>19</td>
<td>203,00</td>
<td>101,50</td>
<td>152,25</td>
<td>152,25</td>
<td>101,50</td>
<td>50,75</td>
<td>101,50</td>
</tr>
<tr>
<td>20</td>
<td>209,00</td>
<td>104,50</td>
<td>156,75</td>
<td>156,75</td>
<td>104,50</td>
<td>52,25</td>
<td>104,50</td>
</tr>
<tr>
<td>21</td>
<td>215,00</td>
<td>107,50</td>
<td>161,25</td>
<td>161,25</td>
<td>107,50</td>
<td>53,75</td>
<td>107,50</td>
</tr>
<tr>
<td>22</td>
<td>221,00</td>
<td>110,50</td>
<td>165,75</td>
<td>165,75</td>
<td>110,50</td>
<td>55,25</td>
<td>110,50</td>
</tr>
<tr>
<td>23</td>
<td>225,00</td>
<td>112,50</td>
<td>168,75</td>
<td>168,75</td>
<td>112,50</td>
<td>56,25</td>
<td>112,50</td>
</tr>
<tr>
<td>24</td>
<td>230,00</td>
<td>115,00</td>
<td>172,50</td>
<td>172,50</td>
<td>115,00</td>
<td>57,50</td>
<td>115,00</td>
</tr>
</tbody>
</table>
Generic Privacy Threats in E-ticketing Systems

1. Unintended customer identification:
   a) Exposure of the customer ID:
      i. Personal ID exposure (direct identification);
      ii. Indirect identification through the relevant object’s ID.
   b) Exposure of a non-encrypted identifier during the anti-collision session;
   c) Physical layer identification (RFID fingerprinting).

2. Information linkage;

3. Illegal customer profiling.

→ A cross-layered set of countermeasures required.
### GENERIC COUNTERMEASURES

<table>
<thead>
<tr>
<th>Threats</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Unintended customer identification:</strong></td>
<td></td>
</tr>
<tr>
<td>a) <em>Exposure of the customer ID:</em></td>
<td></td>
</tr>
<tr>
<td>i. Personal ID exposure (direct)</td>
<td>Privacy-respecting authentication; ID encryption/randomization; access-control functions [8]</td>
</tr>
<tr>
<td>ii. Indirect identification</td>
<td>ID encryption</td>
</tr>
<tr>
<td>b) <em>Unencrypted ID during anti-collision</em></td>
<td>Randomized bit encoding [9]; bit collision masking [10, 11] (protocol dependent)</td>
</tr>
<tr>
<td>c) <em>PHY-layer identification</em></td>
<td>Shielding; switchable antennas [12]</td>
</tr>
<tr>
<td><strong>2. Information linkage</strong></td>
<td>Anonymization (in front-end and back-end): threat 1 countermeasures; privacy-respecting data processing</td>
</tr>
<tr>
<td><strong>3. Illegal customer profiling</strong></td>
<td>Privacy-respecting data storage (back-end); the same as in threat 1</td>
</tr>
</tbody>
</table>

- Difficult to apply in a **joint** fashion.
State of the Art

- Real-world systems
- Academic solutions
Real-world systems

- Primary focus on:
  - direct functionality
  - system security
  - resource effectiveness (cost implications)

- Privacy is usually considered in the second place, if at all

- Frequently, privacy is traded-off for efficiency (as far as legislation allows)

- Examples: eTicket Germany (KA), Metrô São Paulo, ...
Loosely-coupled architecture

Tightly-coupled architecture
IMPORTANT EVALUATION CRITERIA

- Mutual authentication between terminals and e-ticket;

- E-ticket anonymity/untraceability against terminals;

- Trust assumptions (esp. concerning terminals);

- Back-end coupling;

- Regular billing support.
A Privacy-Preserving E-Ticketing System

Ivan Gudymenko

Faculty of Computer Science, TU Dresden

56
## Academic Solutions: Assessment

<table>
<thead>
<tr>
<th>Criteria</th>
<th>The most relevant approaches Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymity terminals</td>
<td>yes</td>
</tr>
<tr>
<td>Untraceability terminals</td>
<td>yes</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>no</td>
</tr>
<tr>
<td>Close-coupling</td>
<td>no</td>
</tr>
<tr>
<td>Regular billing</td>
<td>no</td>
</tr>
<tr>
<td>BE is trusted</td>
<td>no</td>
</tr>
<tr>
<td>ATs are trusted</td>
<td>no</td>
</tr>
</tbody>
</table>

**Legend:**

- Ø – not considered;
- p – partially provided;
Requirements: Privacy Against Terminals

(1) Privacy

(a) Against terminals

Identification: no
Correlation: no

Check-in/out

Backbone Network

E-tickets

E-ticket 1
E-ticket 2
... E-ticket n

Real-time

Terminals

Terminal 1
Terminal 2
... Terminal n

Non-real-time

Back-end

TR Processing:
- Singulation
- Billing
- Identification
Requirements: Privacy Against the Back-end

(1) Privacy

(b) Against back-end

Identification: no
Correlation: yes
**Requirements Against Observers**

(1) **Privacy**

(c) **Against observers**  PII Derivation:  *no*
REQUIREMENTS: FINE-GRANULAR BILLING SUPPORT

(2) Fine-granular billing support

- Enabling best price calculation and discounts
- Tariff schemes must be separated from system architecture
Requirements: Loose-Coupling

(3) Loose-coupling

- Large-scale distribution;
- Compatibility to real-world systems (e.g., Metrô São Paulo, Dresdner Verskehrsbetriebe)
**Requirements: Efficiency**

(4) **Efficiency**  
Check-in/out events handling

- Time-critical
- Directly affects customer experience

---

**Check-in/out**

<table>
<thead>
<tr>
<th>E-tickets</th>
<th>Terminals</th>
<th>Back-end</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-ticket 1</td>
<td>Terminal 1</td>
<td>TR Processing:</td>
</tr>
<tr>
<td>E-ticket 2</td>
<td>Terminal 2</td>
<td>- Singulation</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>- Billing</td>
</tr>
<tr>
<td>E-ticket n</td>
<td>Terminal n</td>
<td>- Identification</td>
</tr>
</tbody>
</table>

**Backbone Network**

- Real-time
- Non-real-time

---

A Privacy-Preserving E-Ticketing System  
Ivan Gudymenko  
Faculty of Computer Science, TU Dresden
REQUIREMENTS: MULTILATERAL SECURITY

(5) Multilateral security

- Security goals of transport authority
- Security goals of users
Challenges: Mutual Authentication

1. *Dynamic extensibility.* Support for dynamic accommodation of new e-tickets is a must.


3. *Implications for path reconstruction.* Fully anonymous mutual authentication prohibits path reconstruction in the back-end.

4. *Efficiency.* Advanced methods often have negative efficiency implications and can be resource prohibitive for constrained devices.

→ In our solution, a slightly modified certificate-based approach is chosen.
**Challenges: Local Revocation**

1. Determine (on the fly) if an e-ticket is valid or not

2. Without being able to track or identify e-tickets

3. Valid e-tickets must remain anonymous (to the terminal) and untraceable

4. Cryptographic tools like various cryptographic accumulators do not suit

→ Our solution considers a **custom blacklisting scheme**
CHALLENGES: PATH RECONSTRUCTION

1. The supported fare schemes need to be flexible and extensible
2. It should be possible to combine the rides to issue discounts
3. At the same time, in a privacy-preserving way
4. Simple fare schemes (e.g. matrix-based) allow for privacy-preserving billing with decent privacy properties
   - Efficiency is an issue, though [KHG13]

→ Our solution is based on a special pseudonymisation scheme
LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function

\[ E(x) = g^x \pmod{p} \]

- Homomorphic property:

\[
E(x \cdot r) = g^{x \cdot r} = (g^x)^r \pmod{p} = E(x)^r.
\]

- Okamoto-Uchiyama trapdoor as a private key

- Other inherently homomorphically deterministic schemes possible.
LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function
  - $E(x) = g^x \pmod{p}$

- Homomorphic property:
  $$E(x \cdot r) = g^{(x \cdot r)} = (g^x)^r \pmod{p} = E(x)^r.$$

- Okamoto-Uchiyama trapdoor as a private key

- Other inherently homomorphically deterministic schemes possible.
Local Revocation Based on Blacklists: A Choice of a Suitable Encryption Scheme

- Based on the discrete exponentiation function
  - \( E(x) = g^x \pmod{p} \)
- Homomorphic property:
  - \[ E(x \cdot r) = g^{x \cdot r} = (g^x)^r \pmod{p} = E(x)^r. \]
- Okamoto-Uchiyama trapdoor as a private key
- Other inherently homomorphic deterministic schemes possible.
Local Revocation Based on Blacklists: A Choice of a Suitable Encryption Scheme

- Based on the discrete exponentiation function
  
  \[ E(x) = g^x \pmod{p} \]

- Homomorphic property:
  
  \[
  E(x \cdot r) = g^{(x \cdot r)} \\
  = (g^x)^r \pmod{p} \\
  = E(x)^r.
  \]

- Okamoto-Uchiyama trapdoor as a private key

- Other inherently homomorphically deterministic schemes possible.
Local Revocation Based on Blacklists: A Choice of a Suitable Encryption Scheme

- Based on the discrete exponentiation function

\[ E(x) = g^x \pmod{p} \]

- Homomorphic property:

\[
E(x \cdot r) = g^{(x\cdot r)} \\
= (g^x)^r \pmod{p} \\
= E(x)^r.
\]

- Okamoto-Uchiyama trapdoor as a private key

- Other inherently homomorphic deterministic schemes possible.
Local Revocation Based on Blacklists: A Choice of a Suitable Encryption Scheme

- Based on the discrete exponentiation function
  \[ E(x) = g^x \pmod{p} \]

- Homomorphpic property:
  \[ E(x \cdot r) = g^{(x \cdot r)} = (g^x)^r \pmod{p} = E(x)^r. \]

- Okamoto-Uchiyama trapdoor as a private key

- Other inherently homomorphpic deterministic schemes possible.
## Other Academic Solutions and Ours

<table>
<thead>
<tr>
<th>Criteria</th>
<th>The most relevant approaches Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymity terminals</td>
<td>yes</td>
</tr>
<tr>
<td>Untraceability terminals</td>
<td>yes</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>no</td>
</tr>
<tr>
<td>Close-coupling</td>
<td>no</td>
</tr>
<tr>
<td>Regular billing</td>
<td>no</td>
</tr>
<tr>
<td>BE is trusted</td>
<td>no</td>
</tr>
<tr>
<td>ATs are trusted</td>
<td>no</td>
</tr>
</tbody>
</table>

**Legend:**

- ⌀ – not considered;
- p – partially provided;