TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Faculty of Computer Science Chair of Privacy and Data Security

Protection of the User's Privacy in Ubiquitous E-ticketing Systems based on RFID and NFC Technologies

Ivan Gudymenko

Status talk, 12 June 2013

Outline

Outline

Target Area

- Ubiquitous Computing (UbiComp);
  - Based on RFID/NFC;
- Focus on electronic ticketing (e-ticketing).

  $\rightarrow$ **Privacy protection**.

E-ticket Taxonomy and Dissertation Focus

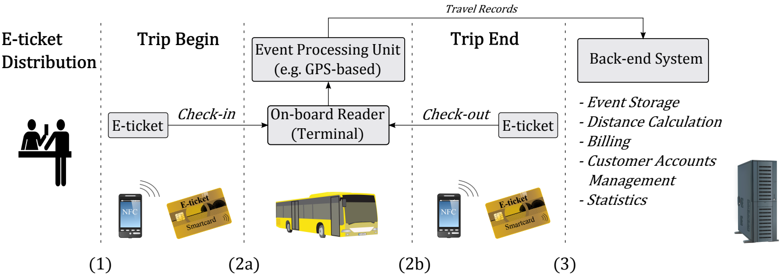
- E-ticket
  - 1. Online ticket
  - 2. Smart ticket
    - public transport
    - event ticketing
      - sport events
      - concerts
    - fitness & leisure
      - fitness studios
      - ski pass

- Focus on public transport

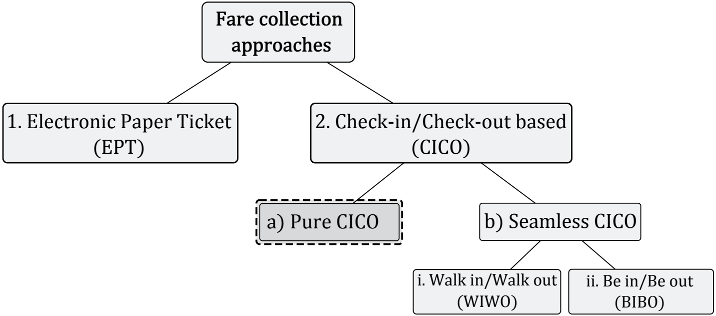
E-ticketing in Public Transport

[Courtesy of MünsterscheZeitung.de]

E-ticketing: A General Application Scenario



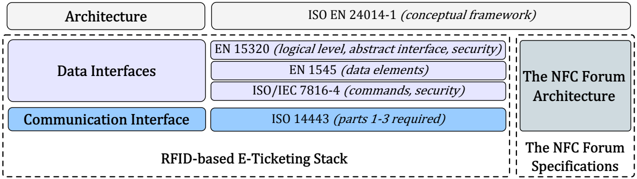
Fare Collection Approaches in E-ticketing



- Focus on CICO-based systems

E-ticketing: Technologies and Standards

- RFID-based stack (proximity cards);
- NFC stack (NFC-enabled devices);
- Recently, CIPURSE by OSPT (Open Standard for Public Transport).



Target Area: Summary

- E-ticketing systems for public transport;
- "Smart ticket" (as opposed to online ticket);
- CICO for automated fare collection;
- Underlying technologies: RFID/NFC.

E-ticketing: Concerns

- **For transport companies**
  - High system development/deployment costs;
  - Lack of well-standardized solutions;
  - New infrastructure is a high risk investment;
  - Possibly low Return of Investment (ROI).
- **For customers**
  - Reluctance to using a conventional system in a new way;
  - **Privacy concerns:**
    - Ubiquitous customer identification;
    - Customer profiling (esp. unconsented);
    - Increased surveillance potential.

Outline

Privacy Protection: Motivation

- Rising privacy concerns in public;
- Motivation to invest in privacy for transport companies;
- **A privacy-preserving solution** is of mutual benefit for both parties:
  - Higher acceptance among customers;
  - Transport companies retain competitiveness.

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.

$\rightarrow$ A **cross-layered** set of countermeasures required.

Protecting User Privacy: Problems

- Customer privacy is not in primary focus of standardization effort;
- Several tailor-made solutions (in add-on fashion);
- No holistic approach treating privacy from an outset (in real systems)

$\rightarrow$ *Privacy by Design is required.*

A Privacy-preserving E-ticketing System: Reqs

(1) **Privacy**

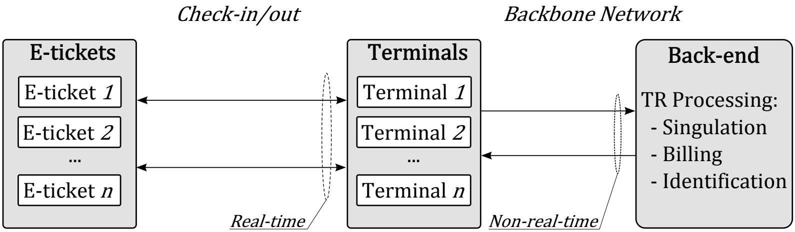
(a) **Against terminals**	Identification:	*no*
	Correlation:	*no*
(b) **Against back-end**	Identification:	*no*
	Correlation:	*yes*
(c) **Against observers**	PII Derivation:	*no*

(2) **Billing**

(a) **Regular Billing**	Regular billing support
(b) **Billing Correctness**	In accordance with fare policy

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

A General System Architecture and Requirements: An Overview



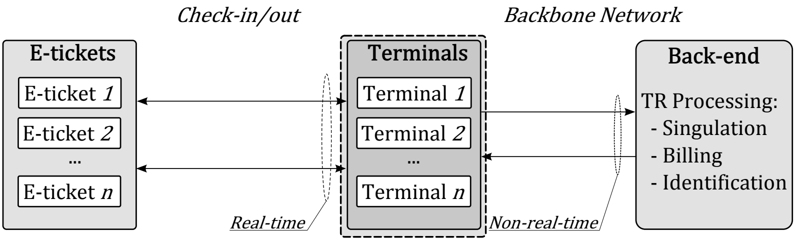
A General System Architecture and Requirements: An Overview (1)

(1) **Privacy**

(a) **Against terminals**

Identification: *no*

Correlation: *no*

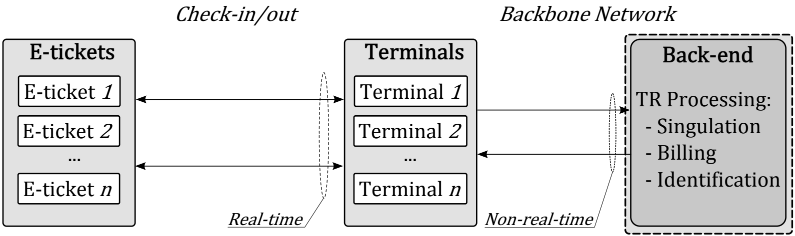


A General System Architecture and Requirements: An Overview (2)

(1) Privacy

(b) Against back-end

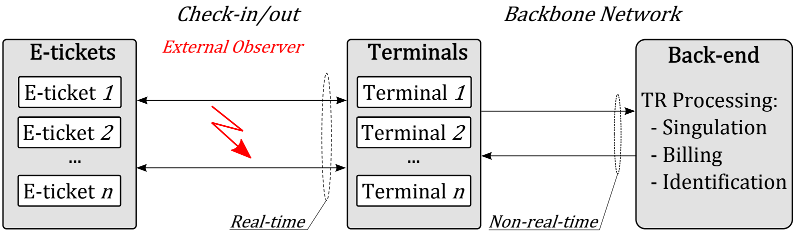
Identification:	*no*
Correlation:	*yes*



A General System Architecture and Requirements: An Overview (3)

(1) **Privacy**

(c) **Against observers** PII Derivation: *no*

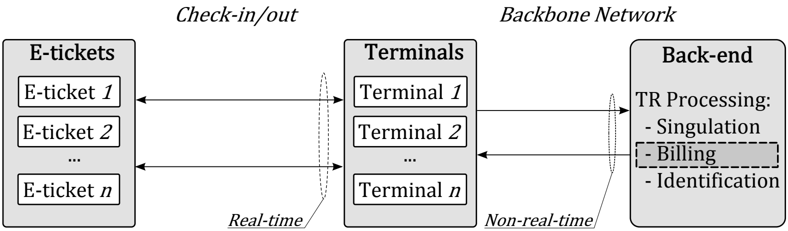


A General System Architecture and Requirements: An Overview (4)

(2) **Billing**

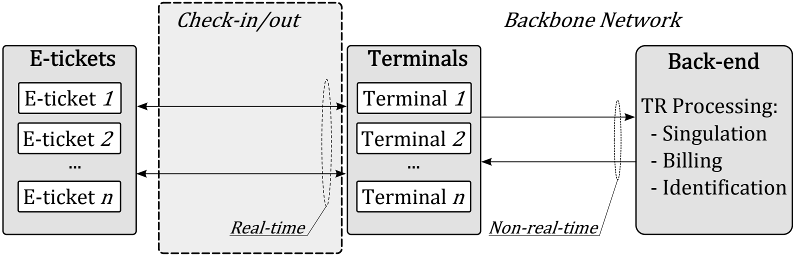
(a) **Regular Billing** — Regular billing support

(b) **Billing Correctness** — In accordance with fare policy



A General System Architecture and Requirements: An Overview (5)

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



Main Goals/Research Questions

RQ: *How to build a privacy-preserving e-ticketing system with the following properties?*

(1) Loose-coupling between front-end and back-end (scaling);

(2) Offline e-ticket validation at the terminal side:

- Valid e-tickets remain anonymous to the terminal;
- Invalid e-tickets must be rejected.

(3) Privacy-preserving travel records processing in back-end:

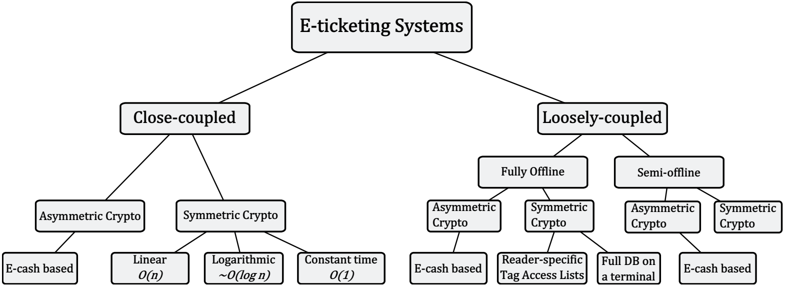
- With regular billing support for personalized tickets;
- Preventing direct identification (pseudonymization).

Outline

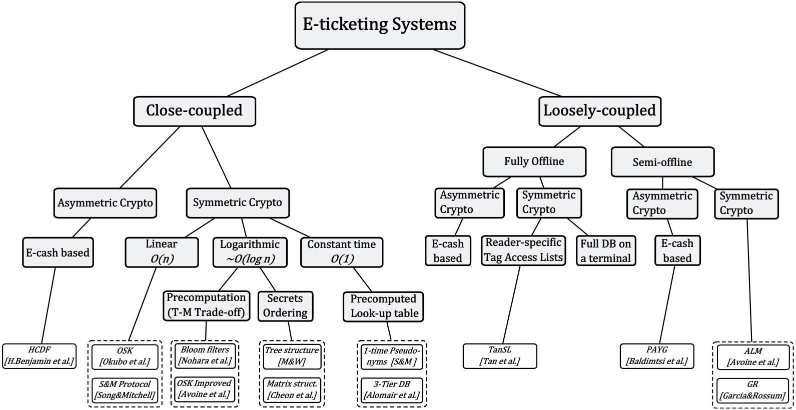
Important Evaluation Criteria

- Mutual authentication between terminals and e-ticket;
- E-ticket anonymity/untraceability against terminals;
- Trust assumptions (esp. concerning terminals);
- Back-end coupling (close/loose);
- Regular billing support.

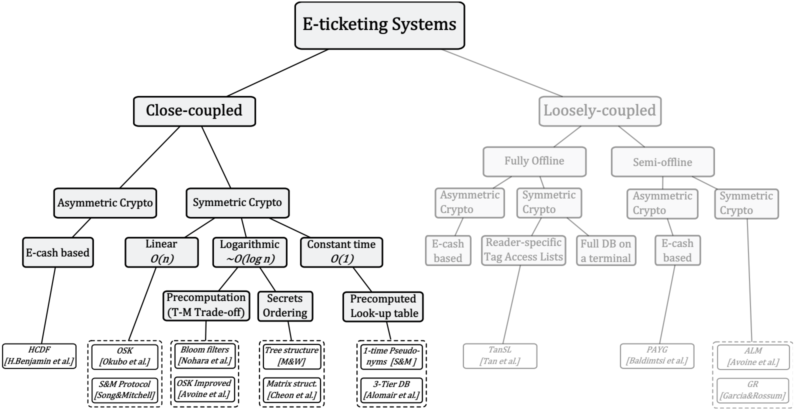
Solutions Taxonomy: Outline



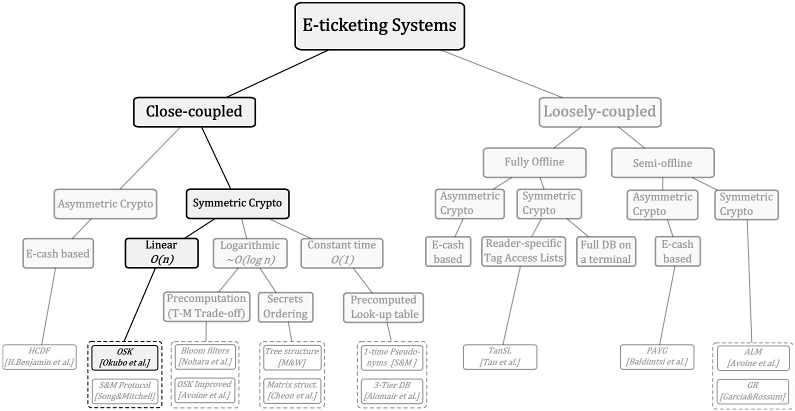
Solutions Taxonomy: Detailed



Solutions Taxonomy: Close-coupled Systems



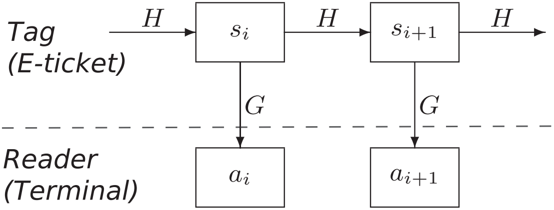
Okubo et al. (OSK Protocol)



[Okubo *et al.*, 2003]

Okubo et al. (OSK Protocol)

- Hash chain-based; two hash functions:
  - $H()$: used for secret refreshment;
  - $G()$: used for untraceability against eavesdroppers.
- Hash chain for the i^{th} tag:
  $F : (i, k) \mapsto r_i^k = G\left(H^{k-1}\left(s_i^{init}\right)\right)$.



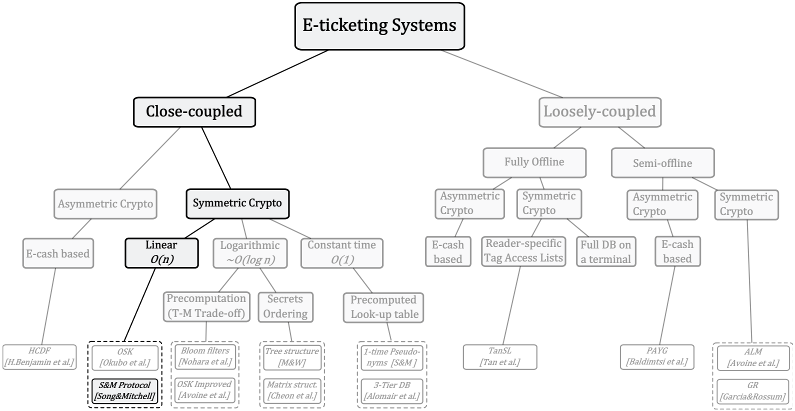
[Okubo *et al.*, 2003]

OSK assessment

- Mutual authentication: *no*
- Untraceability against terminals: *yes*
- Terminals must be trusted: *no*
- Back-end coupling: *tight*
- Regular billing support: *not considered*

- Limited number of validations (by hash chain size k);
- Stateless by design;
- Serious scalability issues: $O(kn)$.

Revised Song & Mitchel's Protocol (RSM)



[Song and Mitchell, 2011]

Revised Song & Mitchel's Protocol (RSM)

- Each tag has a secret s and a pseudonym $t : t = h(s)$;
- A keyed hash function serves for tag identification and authentication (with tag pseudonym t as a key);
- The protocol is stateful;
- Refreshment of tag pseudonym and tag secret on successful *mutual* authentication.

[Song and Mitchell, 2011]

RSM Assessment

• Mutual authentication:	*yes*
• Untraceability against terminals:	*yes*
• Terminals must be trusted:	*no*
• Back-end coupling:	*tight*
• Regular billing support:	*not considered*

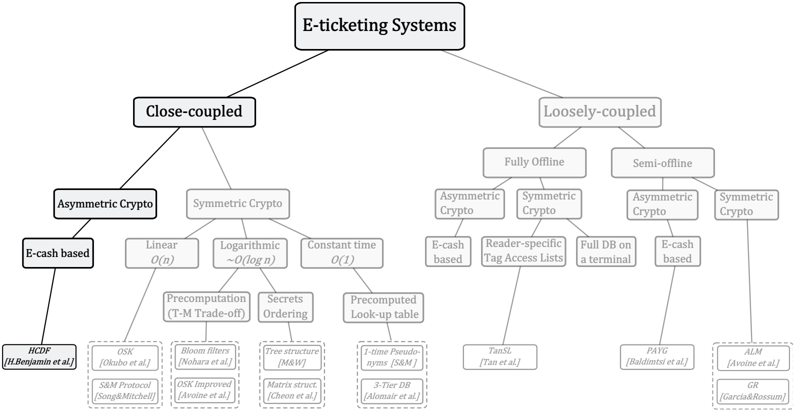
- Scalability issues remain: $O(n)$.

RSM-based One-time Pseudonym Protocol

- Precomputed look-up table of one-time pseudonyms for tag identification:
  - Tag identification complexity $O(1)$;
- Tag authentication is performed similarly to RSM;
- Requires re-initialization when the pseudonyms pool is exhausted.

[Song and Mitchell, 2011]

Heydt-Benjamin *et al.* (HCDF)



[Heydt-Benjamin *et al.*, 2006]

Heydt-Benjamin *et al.* (HCDF)

- Based on e-cash, anonymous credentials, and proxy re-encryption.
- Explicitly considers public transport (a holistic framework);
- Two types of tickets:
  (1) Temporally-bounded;
  (2) Stored-value.

[Heydt-Benjamin *et al.*, 2006]

Heydt-Benjamin *et al.* (HCDF), continued

- On enter:
  - For temporally-bounded tickets: one-show validity credential;
  - For stored value tickets: accept entrance cookie C_E.

- On exit:
  - For temporally-bounded. tickets: the same;
  - For stored value: reveal C_E, calculate price (TA), delete C_E (T).

- On-the-fly price calculation on exit (for stored value ticket).

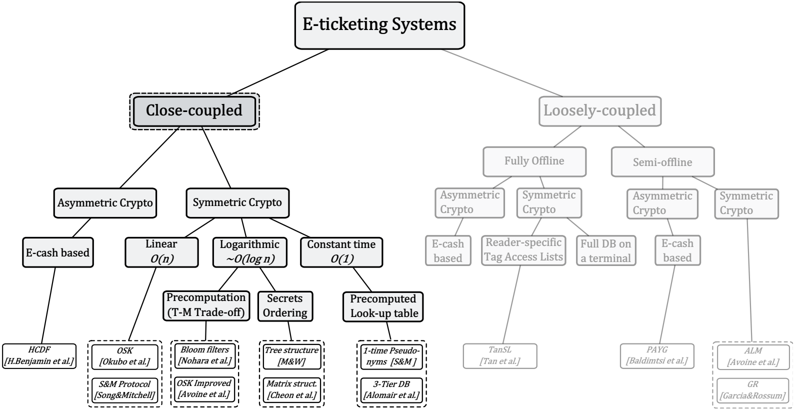
[Heydt-Benjamin *et al.*, 2006]

HCDF Assessment

- Mutual authentication: *no (not explicit)*
- Untraceability against terminals: *yes*
- Terminals must be trusted: *no*
- Back-end coupling: *tight*
- Regular billing support: *no*

- Involves asymmetric crypto on tag (ZKP).

Close-coupled Systems: Summary



Close-coupled Systems: Pros

- Terminal simplicity.
- Less trust in terminals.
- Simple infrastructure.

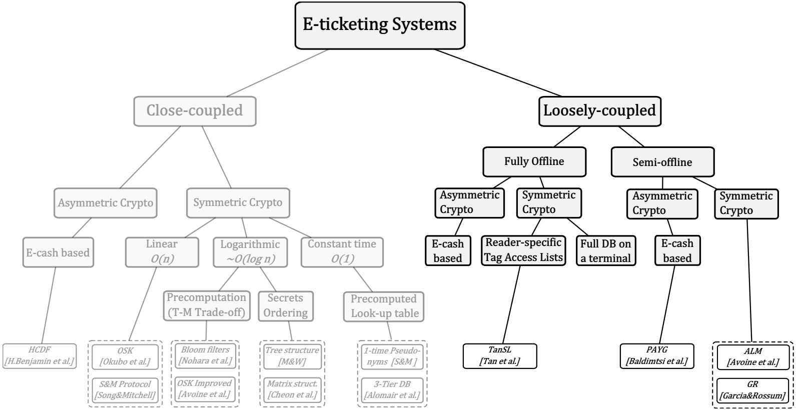
Close-coupled Systems: Contras

- Scaling issues.
- Back-end must be online 24/7.
- Synchronization (statefulness, possibility of DoS attacks).
- Back-end is a bottleneck and single point of failure.

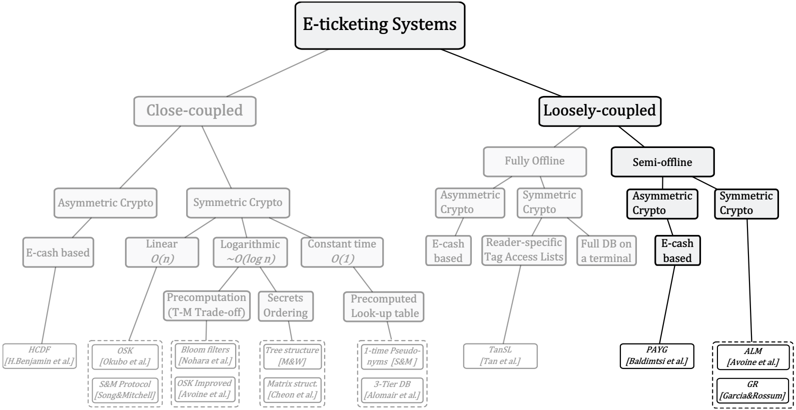
Other Solutions Are Necessary

$\rightarrow$ Some kind of **decentralization** is required.

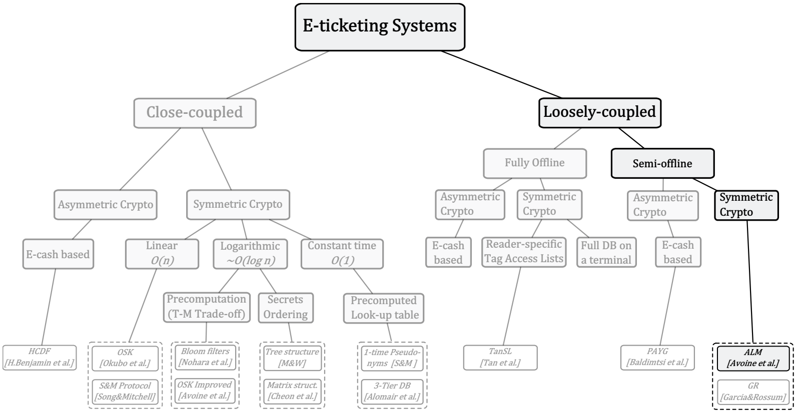
Solutions taxonomy: Loosely-Coupled Systems



Loosely-Coupled Systems: Semi-offline



Avoine *et al.* (ALM)



[Avoine *et al.*, 2009]

Avoine *et al.* (ALM)

- Offline tag validation using challenge response;
- Reader-specific tag identification/authentication tuple sets (TS);
- TS are precomputed by trusted back-end and uploaded to readers;

[Avoine *et al.*, 2009]

Avoine *et al.* (ALM): Keys

- Two key types:
  - Long-term tag-specific key K_T shared between back-end and a tag (is *not* known to readers);
  - Session key k_{TR} is computed on-the-fly by a tag;
- $k_{TR} = f\,(K_T, ID_R, c_R)$
- At the reader side, k_{TR} resides in TS (precomputed);
- k_{TR} is **bounded** to a specific *(reader, tag)* pair.

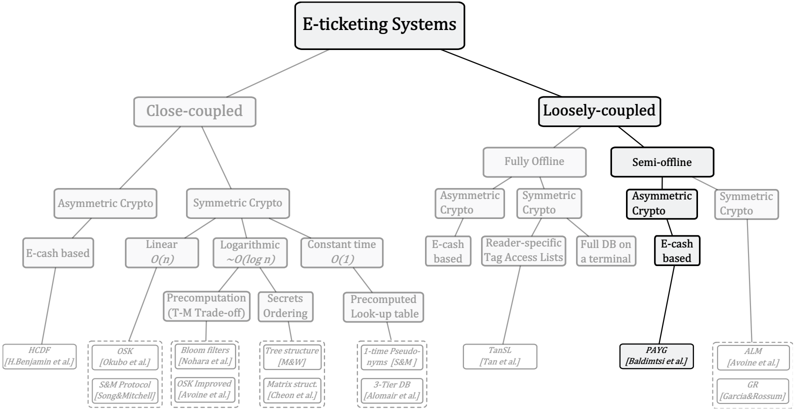
[Avoine *et al.*, 2009]

ALM Assessment

- Mutual authentication: *yes*
- Untraceability against terminals: *no*
- Terminals must be trusted: *yes*
- Back-end coupling: *semi-coupled (counter sync)*
- Regular billing support: *not considered*

- Scalability issues are *shifted* to the reader side:
  - $O(n)$ complexity to locally identify/authenticate a tag.

Baldimtsi *et al.* (PAYG)



[Baldimtsi *et al.*, 2012]

Baldimtsi *et al.* (PAYG)

- Based on e-cash and anonymous credentials;
- Explicitly considers public transport;
- Single trip tickets only;
- Unique ID is encoded into the Trip Authorization Token (TAT) against double spending.
  - The knowledge of the encoded ID must be proved in ZK on check-in.

[Baldimtsi *et al.*, 2012]

Baldimtsi *et al.* (PAYG): System Architecture

- Online vending machines (TAT issuing, refund reimbursement)
- Offline check-in terminals:
  - TAT validity check;
  - Issuance of a Refund Calculation Token (RCT).
- Offline check-out terminals:
  - Terminal-side fare calculation;
  - Refund top-up.
- Variable pricing by attribute encoding;

[Baldimtsi *et al.*, 2012]

PAYG: Issues to Consider

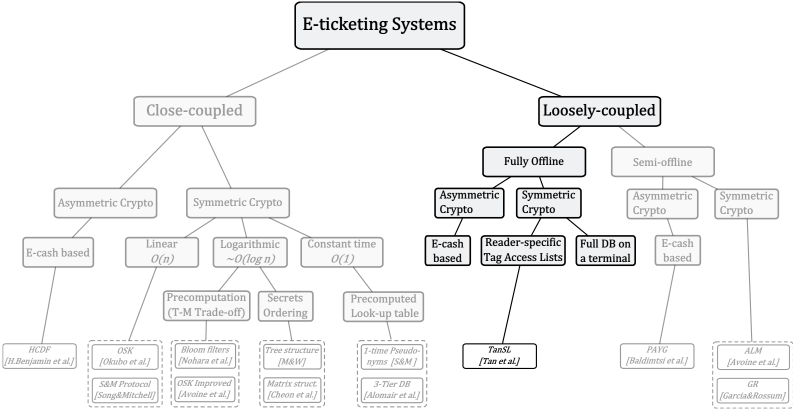
- Refund-based system (refund aggregation into Refund Token);
- Nuisance for users (additional effort for refund reimbursement);
- *All* reimbursed refund tokens must be stored in back-end to prevent refund double spending (for each single trip);
- Actual fare calculation during check-out (no complex pricing schemes possible);

PAYG: Assessment

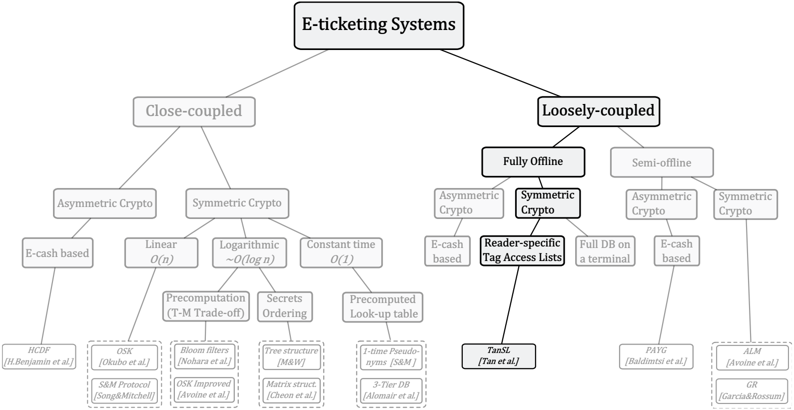
- Mutual authentication: *no*
- Untraceability against terminals: *yes*
- Terminals must be trusted: *no*
- Back-end coupling: *semi-coupled*
- Regular billing support: *no*

- Involves asymmetric crypto on tag (ZKP).

Loosely-Coupled Systems: Fully-offline



Tan *et al.* (TanSL)



[Tan *et al.*, 2007]

Tan *et al.* (TanSL)

- A basis for a more profound protocol
  - ALM by Avoine *et al.*
- Reader-specific tag access list (as in ALM);
- Authentication is *bound* to a concrete *(reader, tag)* pair;
- Fully offline tag identification and authentication;
- No regular secret refreshment (unlike ALM);

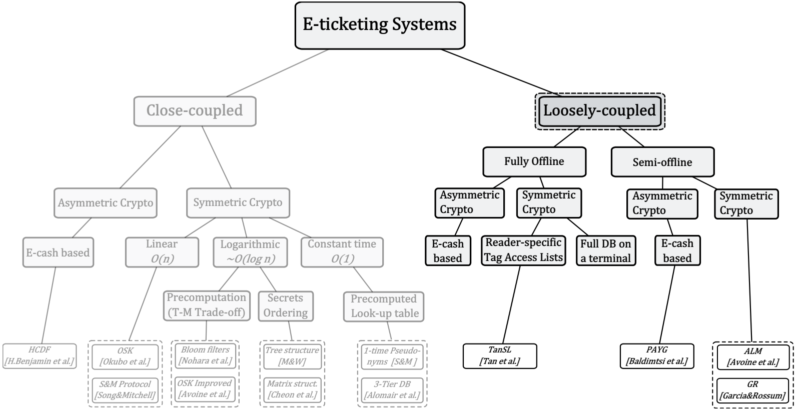
[Tan *et al.*, 2007]

TanSL: Assessment

- Mutual authentication: *yes*
- Untraceability against terminals: *no*
- Terminals must be trusted: *yes*
- Back-end coupling: *fully offline*
- Regular billing support: *not considered*

- Scalability issues are *shifted* to the reader side:
  - $O(n)$ complexity to locally identify/authenticate a tag.

Loosely-coupled Systems: Summary



Loosely-coupled Systems: Pros

- Loosely coupled system components
  - Better scaling (compared to close-coupled systems);
- Terminal-side e-ticket validation (efficiency);

Loosely-coupled Systems: Contras

- More intelligence at the terminal side is required;
- Contradicting requirements:
  - Validate e-tickets;
  - Without identifying/tracking them.
- Terminals operate on the tag data containing identifiable information;

$\rightarrow$ Privacy – validation trade-off.

- Decentralized infrastructure is harder to manage (updates, uploads, etc.).

State-of-the-art: Final Overview

Criteria		The most relevant approaches Reviewed						
		PAYG[1]	HCDF[2]	SVW[3]	GR[4]	ALM[5]	OSK[6]	RSMP[7]
Explicitly cons. PT		yes	yes	yes	yes	no	no	no
Anonym. against term.		yes	yes	p	no	no	yes	yes
Untraceab. against term.		yes	yes	p	no	no	yes	yes
Mutual authentication		no	no	no	no	yes	no	yes
Crypto Primitives Used	Symmetric	no	yes	yes	yes	yes	no	yes
	Hash	yes	yes	no	yes	no	yes	yes
	Asymmetric	yes	yes	p	no	no	no	no
Back-end Coupling	Tight	–	yes	–	–	–	yes	yes
	Semi-coupl.	yes	–	–	yes	yes	–	–
	Loose	–	–	yes	–	–	–	–
Tamp. resist. required		∅	∅	p	∅	∅	no	no
Regular billing		no	no	no	∅	∅	∅	∅
Involves extern. device		no	no/p	yes	no	no	no	no
BE is trusted		no	no	yes	yes	yes	yes	yes
ATs are trusted		no	no	yes	yes	yes	no	no
Revocation is possible		yes	yes	yes	yes	yes	yes	yes
Dynamic extensibility		yes	yes	yes	no	no	yes	no

Criteria		The most relevant approaches Reviewed						
		PAYG[1]	HCDF[2]	SVW[3]	GR[4]	ALM[5]	OSK[6]	RSMP[7]
Explicitly cons. PT		yes	yes	yes	yes	no	no	no
Anonym. against term.		yes	yes	p	no	no	yes	yes
Untraceab. against term.		yes	yes	p	no	no	yes	yes
Mutual authentication		no	no	no	no	yes	no	yes
Crypto Primitives Used	Symmetric	no	yes	yes	yes	yes	no	yes
	Hash	yes	yes	no	yes	no	yes	yes
	Asymmetric	yes	yes	p	no	no	no	no
Back-end Coupling	Tight	–	yes	–	–	–	yes	yes
	Semi-coupl	yes	–	–	yes	yes	–	–
	Loose	–	–	yes	–	–	–	–
Tamp. resist. required		∅	∅	p	∅	∅	no	no
Regular billing		no	no	no	∅	∅	∅	∅
Involves extern. device		no	no/p	yes	no	no	no	no
BE is trusted		no	no	yes	yes	yes	yes	yes
ATs are trusted		no	no	yes	yes	yes	no	no
Revocation is possible		yes	yes	yes	yes	yes	yes	yes
Dynamic extensibility		yes	yes	yes	no	no	yes	no

State of the Art: Focused

Criteria	The most relevant approaches Reviewed						
	PAYG[1]	HCDF[2]	SVW[3]	GR[4]	ALM[5]	OSK[6]	RSMP[7]
Anonymity terminals	yes	yes	p	no	no	yes	yes
Untraceability terminals	yes	yes	p	no	no	yes	yes
Mutual authentication	no	no	no	no	yes	no	yes
Close-coupling	no	yes	no	no	no	yes	yes
Regular billing	no	no	no	∅	∅	∅	∅
BE is trusted	no	no	yes	yes	yes	yes	yes
ATs are trusted	no	no	yes	yes	yes	no	no

Legend:

∅ – not considered;
p – partially provided;

Outline

Recall: System 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) **Billing**

(a) **Regular Billing**	Regular billing support
(b) **Billing Correctness**	In accordance with fare policy

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

A **P**rivacy-preserving **E**-ticketing System with Regular **B**illing Support (PEB)

- Protect privacy while allowing various pricing schemes in back-end;
- Pricing schemes are fully independent of system architecture;
- A reasonable trade-off is allowed:
  - *In front-end*. Different sessions between an e-ticket and terminal/s are completely unlinkable;
  - *In back-end*. Back-end may correlate different sessions to an e-ticket *pseudonym*.

Attacker Model

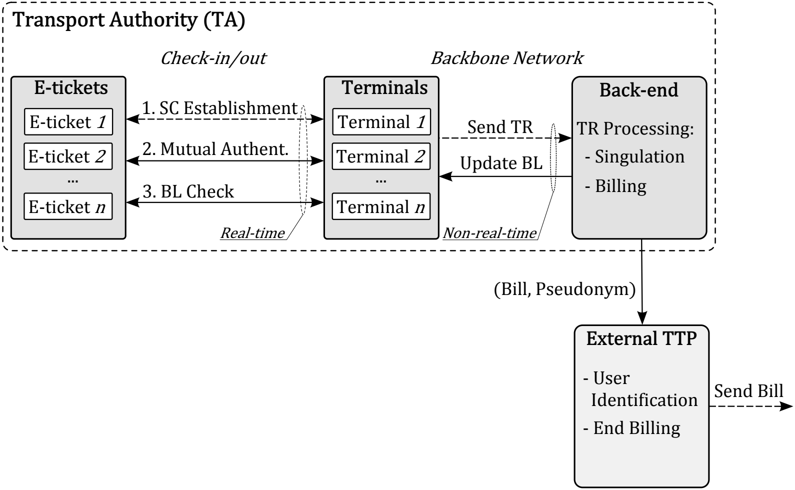
(1) (Outsider) No PII derivation by **external observers** (front-end sessions).

(2) (Insider) No tracking and identification of valid e-tickets by **terminals**.

(3) (Insider) No direct identification by **back-end**.

$\rightarrow$ Insider/outsider with respect to the involvement into the system flow.

PEB: System Architecture



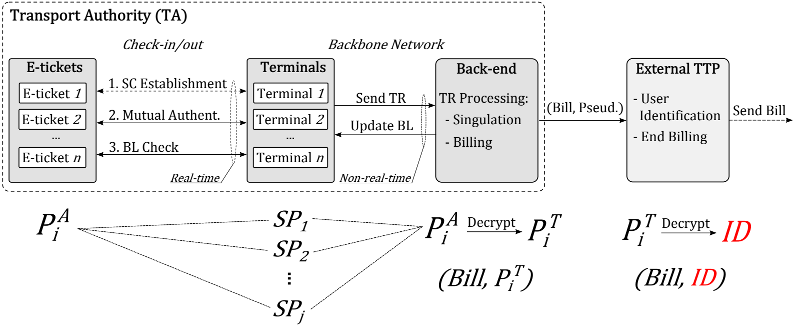
PEB: Pseudonymization

- For each e-ticket, TTP creates a static pseudonym P_i^T;
  - Mapping $P_i^T \mapsto ID$ is kept secret by TTP;
- P_i^T is sent to TA;
- TA includes it into its static pseudonym set: $P_i^T \in P^T$;
- TA, therefore, operates only on pseudonyms in P^T;

PEB: Pseudonymization (continued)

- TA possesses an asymmetric key pair: $\left(k_{ta}^{+}, k_{ta}^{-}\right)$;
- Front-end e-ticket pseudonyms: $P_i^A = E_{k_{ta}^{+}}\left(P_i^T\right)$
  - Required for terminal-side black list checking.
- E-tickets are parameterized with P_i^A;
- E-ticket $\leftrightarrow$ terminal: a session pseudonym on each interaction (anti-tracking): $SP_j = E_{k_{ta}^{+}}\left(P_i^A \cdot r_j\right)$.

PEB: Pseudonymization (continued)



PEB: Privacy-preserving BL Checking

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}\left(P_i^T\right)$;
- Malleability property: $E(x \cdot r) = E(x)^r$;
- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow \big(E(x \cdot r), E(r)\big)$;
- Black list: $\{y : y \in BL\}$;
- Check SP_j against the BL:
  $\forall y \in BL, E(r) \in SPT: \; c \leftarrow E(r)^y$
  $c \stackrel{?}{=} E(x \cdot r) \;\; \forall c \in C.$

BL Checking: A Choice of a Suitable Encryption

- Based on the discrete exponentiation function
- $E(x) = g^x \ (mod\ p)$
- Malleability property:

$$\begin{aligned} E(x \cdot r) &= g^{(x \cdot r)} \\ &= \left(g^x\right)^r \qquad (mod \;\; p) \\ &= E(x)^r. \end{aligned}$$

- Other inherently homomorphic deterministic schemes possible.

PEB: Discussion

- Loosely-coupled system;
- Mutual identification due to group signatures;
- Revocation: black lists:
  - Encrypted black lists possible;
  - Alternatively, dynamic accumulators can be used [8].
- To enhance performance, anonymity set can be reduced in a controllable way;
- Our system fully satisfies the requirements.

State-of-the-art Overview and PEB

Criteria	The most relevant approaches Reviewed							
	PAYG[1]	HCDF[2]	SVW[3]	GR[4]	ALM[5]	OSK[6]	RSMP[7]	**PEB**
Anonymity terminals	yes	yes	p	no	no	yes	yes	**yes**
Untraceability terminals	yes	yes	p	no	no	yes	yes	**yes**
Mutual authentication	no	no	no	no	yes	no	yes	**yes**
Close-coupling	no	yes	no	no	no	yes	yes	**no**
Regular billing	no	no	no	∅	∅	∅	∅	**yes**
BE is trusted	no	no	yes	yes	yes	yes	yes	**no**
ATs are trusted	no	no	yes	yes	yes	no	no	**no**

Legend:

∅ – not considered;
p – partially provided;

Current Progress

- The first results were presented at PECCS-2013 in Barcelona (see [9]);
- The paper presenting the core architecture has been accepted to the IFIP-2013 Summer School.
- Contacts with industry: DVB are interested, Secunet;
- Supervision of two students helping to validate the concept.

Outline

Introduction

Privacy Issues in E-ticketing Systems

Academic Solutions: State of the art

A Privacy-preserving E-ticketing System with Regular Billing Support (PEB)

References

References I

[1] F. Baldimtsi, G. Hinterwalder, A. Rupp, A. Lysyanskaya, C. Paar, and W. P. Burleson, “Pay as you go,” in *Workshop on hot topics in privacy enhancing technologies, HotPETSs 2012*, `http://petsymposium.org/2012/papers/hotpets12-8-pay.pdf`, 2012.

[2] T. S. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu, “Privacy for Public Transportation,” in *Proceedings of the 6th international conference on Privacy Enhancing Technologies*, PET’06, (Berlin, Heidelberg), pp. 1–19, Springer-Verlag, 2006.

[3] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, “User Privacy in Transport Systems Based on RFID E-Tickets,” in *Workshop on Privacy in Location-Based Applications (PILBA 2008)*, vol. 5283 of *Lecture Notes in Computer Sciences*, Springer-Verlag, October 2008.
Malaga, Spain.

[4] F. Garcia and P. Rossum, “Modeling Privacy for Off-Line RFID Systems,” in *Smart Card Research and Advanced Application* (D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, eds.), vol. 6035 of *Lecture Notes in Computer Science*, pp. 194–208, Springer Berlin Heidelberg, 2010.

[5] G. Avoine, C. Lauradoux, and T. Martin, “When Compromised Readers Meet RFID,” in *Information Security Applications* (H. Y. Youm and M. Yung, eds.), vol. 5932 of *Lecture Notes in Computer Science*, pp. 36–50, Springer Berlin Heidelberg, 2009.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic Approach to ”Privacy-Friendly” Tags,” in *In RFID Privacy Workshop*, 2003.

[7] B. Song and C. J. Mitchell, “Scalable RFID security protocols supporting tag ownership transfer,” *Comput. Commun.*, vol. 34, pp. 556–566, apr 2011.

References II

[8] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," in *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '02, (London, UK, UK), pp. 61–76, Springer-Verlag, 2002.

[9] I. Gudymenko, "On Protection of the Users Privacy in Ubiquitous E-ticketing Systems Based on RFID and NFC Technologies," in 3^d *International Conference on Pervasive and Embedded Computing and Communication Systems, PECCS-2013*, pp. 86–91, feb 2013.

[10] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," in *Financial Cryptography 03*, pp. 103–121, Springer-Verlag, 2002.

[11] T.-L. Lim, T. Li, and S.-L. Yeo, "Randomized Bit Encoding for Stronger Backward Channel Protection in RFID Systems," in *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PERCOM '08, (Washington, DC, USA), pp. 40–49, IEEE Computer Society, 2008.

[12] W. Choi and B.-h. Roh, "Backward Channel Protection Method for RFID Security Schemes Based on Tree-Walking Algorithms," in *Computational Science and Its Applications - ICCSA 2006* (M. Gavrilova, O. Gervasi, V. Kumar, C. Tan, D. Taniar, A. Lagan, Y. Mun, and H. Choo, eds.), vol. 3983 of *Lecture Notes in Computer Science*, pp. 279–287, Springer Berlin / Heidelberg, 2006.

[13] T.-L. Lim, T. Li, and S.-L. Yeo, "A Cross-layer Framework for Privacy Enhancement in RFID systems," *Pervasive and Mobile Computing*, vol. 4, no. 6, pp. 889 – 905, 2008.

[14] I. Gudymenko, "Protection of the Users Privacy in Ubiquitous RFID Systems," Master's thesis, Technische Universitt Dresden, Faculty of Computer Science, December 2011.

Thank you for your attention!
Questions? Comments?
Suggestions?

Backup Slides

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.

Generic Countermeasures

Threats	Countermeasures
1. Unintended customer identification:	
a) *Exposure of the customer ID:*	
i. Personal ID exposure (direct)	Privacy-respecting authentication; ID encryption/randomization; access-control functions [10]
ii. Indirect identification	ID encryption
b) *Unencrypted ID during anti-collision*	Randomized bit encoding [11]; bit collision masking [12, 13] (protocol dependent)
c) *PHY-layer identification*	Shielding; switchable antennas [14]
2. Information linkage	Anonymization (in front-end and back-end): threat 1 countermeasures; privacy-respecting data processing
3. Illegal customer profiling	Privacy-respecting data storage (back-end); the same as in threat 1

- Difficult to apply in a **joint** fashion.

Revised Song & Mitchel's Protocol (RSM) [7]

S $[T : s, t, \hat{s}, \hat{t}]$		T $[t]$
Generate r_1		
	$\xrightarrow{r_1}$	
		Generate r_2 $M_1 = t \oplus r_2$ $M_2 = f_t(r_1 \| r_2)$
	$\xleftarrow{r_1, M_1, M_2}$	
Find t in the DB s.t. $M_2 = f_t(r_1 \| (M_1 \oplus t))$ $r_2 = M_1 \oplus t$ $M_3 = s \oplus f_t(r_2 \| r_1)$		
	$\xrightarrow{r_1, M_3}$	
$\hat{s} \leftarrow s$ $\hat{t} \leftarrow t$ $s \leftarrow (s \ll l/4) \oplus (t \gg l/4) \oplus r_1 \oplus r_2$ $t \leftarrow h(s)$		$s = M_3 \oplus f_t(r_2 \| r_1)$ If $h(s) = t$, $t \leftarrow h((s \ll l/4) \oplus (t \gg l/4) \oplus r_1 \oplus r_2)$

HCDF: Session Description

Authorized Reader (F)		Ticket (TX)
	$\xrightarrow{\quad t \quad}$	
		$r \in_R \{0,1\}^{l_n}$ $S \leftarrow t\|\|r$ $C \leftarrow E_{K^+_{TA}}(S)$
	$\xleftarrow{\quad C \quad}$	
$C' \leftarrow RE(C)$ $S \leftarrow D_{K^-_F}(C')$		
	$\xleftrightarrow{E_S(transaction)}$	

- Session key generation: $S \leftarrow t||r$;
- Exchange S using non-expired delegation key (re-encryption);

Avoine *et al.* (ALM)

Reader R		**Tag** T
Id_R, c_R		Id_T, K_T, c_T
$Id_T, k_{TR} = E_{K_T}(Id_R, c_R)$		

$$
\begin{array}{lcl}
(1) & \xrightarrow{Id_R,\ c_R,\ n_R} & \\
 & \xleftarrow{E_{k_{TR}}(n_R, n_T)} & (2) \\
(3) & \xrightarrow{n_T} & (4)
\end{array}
$$

- $TS \leftarrow \{(ID_T, k_{TR})\} \, \forall T$
- $k_{TR} \leftarrow E_{K_T}(ID_R, c_R)$

Tan *et al.* (TanSL)

Reader R		**Tag** T
$Id_R, L = [Id_T : h(Id_R \| \| t_T)]$		Id_T, t_T

(1) $\xrightarrow{\quad request \quad}$

$\xleftarrow{\quad n_T \quad}$ (2)

(3) $\xrightarrow{\quad Id_R,\ n_R \quad}$

$\xleftarrow{\quad Hb,\ ques_R \quad}$ (4)

(5) $\xrightarrow{\quad ans_R,\ ques_T \quad}$

(7) $\xleftarrow{\quad ans_T \quad}$ (6)

Client-Side Fare Calculation: Toll Pricing

- Decentralized approach to *fare calculation;*
- Privacy preservation by client-side fare calculation;
- Enforcement through spot checks, ZKP of the validity of the committed values, etc.;
- The price calculation flow may be fairly complex (involves several noncolluding parties);
- Substantial computational and operational overhead for users;

→ Does not suit well for a target e-ticketing system.