**QUEEN'S
UNIVERSITY
BELFAST**

Privacy-Preserving Electronic Ticket Scheme with Attribute-Based Credentials

Han, J., Chen, L., Schneider, S., Treharne, H., & Wesemeyer, S. (2019). Privacy-Preserving Electronic Ticket Scheme with Attribute-Based Credentials. *IEEE Transactions on Dependable and Secure Computing*.
<https://doi.org/10.1109/TDSC.2019.2940946>

Published in:
IEEE Transactions on Dependable and Secure Computing

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
[Link to publication record in Queen's University Belfast Research Portal](#)

Publisher rights
© 2019 IEEE.

This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Privacy-Preserving Electronic Ticket Scheme with Attribute-Based Credentials

Jinguang Han, *Senior Member, IEEE*, Liquan Chen, *Senior Member, IEEE*, Steve Schneider, Helen Treharne and Stephan Wesemeyer

Abstract—Users accessing services are often required to provide personal information, for example, age, profession and location, in order to satisfy access policies. This personal information is evident in the application of e-ticketing where discounted access is granted to visitor attractions or transport services if users satisfy policies related to their age or disability or other defined over attributes. We propose a privacy-preserving electronic ticket scheme using attribute-based credentials to protect users' privacy. The benefit of our scheme is that the attributes of a user are certified by a trusted third party so that the scheme can provide assurances to a seller that a user's attributes are valid. The scheme makes the following contributions: (1) users can buy different tickets from ticket sellers without releasing their exact attributes; (2) two tickets of the same user cannot be linked; (3) a ticket cannot be transferred to another user; (4) a ticket cannot be double spent. The novelty of our scheme is to enable users to convince ticket sellers that their attributes satisfy the ticket policies and buy discounted tickets anonymously. This is a step towards identifying an e-ticketing scheme that captures user privacy requirements in transport services. The security of our scheme is proved and reduced to a well-known complexity assumption. The scheme is also implemented and its performance is empirically evaluated.

Index Terms—Anonymity, Attribute-based Credentials, Privacy-enhanced Authentication, Electronic Ticket

1 INTRODUCTION

Due to their flexibility and portability, electronic ticket (e-ticket) systems have been extensively investigated by both industry [1], [2] and the academic research communities [3], [4], [5]. E-tickets are attractive to transport operators as well as customers because they can reduce paper costs (tickets can be stored on a hand-held device) and improve customer experience (tickets can be purchased and delivered any time and anywhere). However, the use of e-tickets also raises many questions regarding the privacy of its users due to the possibility of linking different e-ticket transactions to a particular user—in contrast to anonymous paper-based tickets—and thus potentially revealing private information, e.g. working patterns, likely places of work, *etc.*

Customers are increasingly aware of privacy issues especially in light of the newly introduced general data protection regulations (GDPR) [6]. One way to address this is through anonymous authentication which enables users to authenticate without revealing their identities and this approach has been used to protect a user's privacy in many privacy-preserving e-ticket schemes [3], [7], [8], [9], [10], [11]. However, many of these schemes were not formally proven to be secure. Notable exceptions are those proposed

by Arfaoui *et al.* [8] and Rupp *et al.* [12]. Arfaoui *et al.* [8] formally defined their security models for e-ticket schemes, including unforgeability, unlinkability and non-repudiation, but the authors only provided a very high-level proof. Rupp *et al.* [12] formalised their security models of privacy-preserving pre-payments with refunds schemes including transportation authority security and user privacy but the security proof of their scheme was again at a high level. Another requirement of a realistic e-ticket systems is the support for different tickets based on a user's attributes (e.g. age, location, disability, profession, *etc.*), i.e. to offer discounts for, say, students or disabled passengers. However, if not implemented carefully, there is a risk that such a ticket system reveals more information about a user than necessary when purchasing or validating tickets. For example, a student buying a discounted student ticket may end up revealing the university at which she is enrolled and, depending on the student card, even her birthday neither of which is relevant to obtaining the student discount. The minimum proof required is that she can demonstrate that she is a legitimate student. Similarly, a disabled passenger might need to reveal more details about his disability to the ticket seller or verifier than necessary for purchasing or verifying a ticket. Gudymenko [10] and Kerschbaum *et al.* [11] addressed this issue, but their schemes were not proven formally.

Transport operators are naturally concerned about fraudulent use of e-tickets due to the ease with which they can be copied. Double spend or more generally overspend detection, i.e. the process of determining whether a ticket has been used too many times, is therefore also an important feature that an e-ticket scheme should support.

To address the above requirements, this paper proposes a new privacy-preserving e-ticket scheme using attribute-

- J. Han is with the Centre for Secure Information Technologies (CSIT), Institute of Electronics, Communications and Information Technology (ECIT), Queen's University Belfast, Belfast, Northern Ireland, BT3 9DT, United Kingdom, and also with the Surrey Centre for Cyber Security, Department of Computer Science, University of Surrey, Guildford, Surrey, GU2 7XH, United Kingdom. E-mail: j.han@qub.ac.uk
- L. Chen, S. Schneider, H. Treharne and S. Wesemeyer are with the Surrey Centre for Cyber Security, Department of Computer Science, University of Surrey, Guildford, Surrey, GU2 7XH, United Kingdom. E-mail: {liquan.chen, s.schneider, h.treharne, s.wesemeyer}@surrey.ac.uk

based credentials which supports issuing different tickets depending on a user's attributes. Our scheme protects an honest user's privacy while allowing for the de-anonymisation of users who try to use their tickets more than once (double spend detection). It is also a general e-ticket system and can be used in various application scenarios including:

- mobility as a service transport tickets (e.g. rail, bus, etc.) where age, disability, profession, affiliation, etc. might determine the prices of tickets;
- one-off token for Internet services (e.g. print service, download service for multimedia, etc.) where age, affiliation, membership might determine the service/access level;
- e-voting where age, nationality, voting district, etc. might determine the voting ballot that should be issued;
- event tickets (e.g. concert, tourist attractions, conferences, etc.) where age, affiliation, disability, etc. might determine the ticket price/access rights.

1.1 Contributions

In this paper, we propose a new attribute-based e-ticket scheme. The main contributions of our scheme are: (1) **Attribute-based Ticketing**: users can buy different tickets depending on their certified attributes without releasing their exact details; (2) **Unlinkability**: two tickets of the same user cannot be linked; (3) **Untransferability**: a ticket can only be used by the ticket holder and cannot be transferred to another user; (4) **Double Spend Detection**: a ticket cannot be double spent and the identities of users who try to double spend tickets can be revealed.

The novelty of our scheme is to enable users to convince ticket sellers that their attributes satisfy the ticket policies and buy discounted tickets anonymously. Our scheme thus offers a natural as well as flexible way of representing user attributes, e.g. to obtain an age based discount, a user would expect to prove that her age is in a certain range, while for a disability discount, she would want to demonstrate her impairment is contained within the set of recognised disabilities. Furthermore, a user's attributes are additionally certified by a trusted third party thereby allowing a user's claimed attributes to also be verified.

The theoretical contribution is that the security of the proposed scheme is formally proven and reduced to a well-known complexity assumption. The scheme is also implemented and performance timings are given.

1.2 Related Work

Mut-Puigserver *et al.* [4] surveyed numerous e-ticket systems and summarised their various functional requirements (e.g. expiry date, portability, flexibility, etc.) and security requirements (e.g. integrity, authentication, fairness, non-overspending, anonymity, transferability, unlinkability, etc.). E-ticket schemes are classified into different types: transferable tickets [5], [7], untransferable tickets [3], [13], multi-use tickets [3], [4] and single-use tickets [3], [5], [7], [14]. Our scheme falls into the untransferable, single-use tickets categories while providing anonymity, unlinkability, non-overspending and flexibility.

We now compare our scheme with a number of other schemes. In these schemes, blind signatures [15], group signatures [16], anonymous credentials [17] and pseudonyms [16], [18] were used to protect user privacy.

E-Ticket Schemes from Blind Signatures. In a blind signature scheme, a user can obtain a signature on a message without the signer knowing the content. Based on the blind signature scheme proposed by Chaum [15], Fan and Lei [19] proposed an e-ticket system for voting in which each voter can vote in different elections using only one ticket. Song and Korba [9] proposed an e-ticket scheme to protect users' privacy and provide non-repudiation in pay-TV systems. Quercia and Hailes [20] proposed an e-ticket scheme for mobile transactions using Chaum's blind signature scheme [15] to generate both limited-use and unlimited-use tickets. Rupp *et al.* [12], [21] proposed privacy-preserving prepayments with refunds schemes derived from Chaum's scheme [22] and Boneh *et al.*'s short signature scheme [23]. In their scheme, trip authorisation tokens were generated using Chaum's blind signatures, while Boneh *et al.*'s short signature scheme was used to implement the privacy-preserving aggregation of refunds. Milutinovic *et al.* [3] proposed an e-ticket scheme which combines the partial blind signature scheme proposed by Abe *et al.* [24], Pedersen's secret sharing commitment scheme [25] and Camenisch *et al.*'s anonymous credential scheme [26] to protect user privacy. All these schemes can protect user privacy and provide ticket unlinkability, but, unlike our scheme, they do not support de-anonymisation after double spending nor ticket untransferability.

E-Ticket Schemes from Group Signatures. A group signature enables a user to sign a message on behalf of the group without exposing his identity, while the group manager can release the identity of the real signer. Nakanishi *et al.* [27] proposed an electronic coupon (e-coupon) scheme where the group signature scheme [28] was used to provide anonymity and unlinkability. Vives-Guasch [29] proposed an automatic fare collection (AFC) system in which the group signature scheme proposed by Boneh *et al.* [30] was used to provide unlinkability and revocable anonymity. These schemes can implement anonymity, de-anonymity, ticket unlinkability and ticket untransferability, but, unlike our scheme, they do not support privacy-preserving attribute-based ticketing. While Gudymenko in [10] addressed user privacy as well as differently priced tickets in his e-ticket scheme and used group signatures to make tickets unlinkable, no formal security models and security proofs were presented.

E-Ticket Schemes from Anonymous Credentials. In an anonymous credential scheme, a user can prove to a verifier that she has obtained a credential without releasing any other information. Heydt-Benjamin *et al.* [7] used anonymous credentials, e-cash and proxy re-encryption schemes to enhance the security and privacy of their public transport e-ticket systems. Arfaoui *et al.* [8] modified the signature scheme proposed by Boneh *et al.* in [31] to eliminate expensive pairing operations in the verification phase, and then proposed a privacy-preserving near field communication (NFC) mobile ticket (m-ticket) system by combining their modified signature with the anonymous credential scheme proposed by Camenisch *et al.* [32]. In their scheme, a user can anonymously use an m-ticket at most k times, otherwise the user

is revoked by the revocation authority. These schemes can implement anonymity, ticket unlinkability as well as ticket untransferability, but, unlike our scheme, do not support privacy-preserving attribute-based ticketing. Additionally, the security of these schemes was not formally proven.

E-Ticket Schemes from Pseudonyms. Pseudonyms allow a user to interact with multiple organisations anonymously and potentially without linkability. Fujimura and Nakajima [33] proposed a general-purpose e-ticket framework where anonymity was achieved by using pseudonym schemes [34], [35]. Jorns *et al.* [36] proposed a pseudonym scheme which could be implemented on constrained devices, and then used it to protect users' privacy in e-ticket systems. Kuntze and Schmidt [37] proposed a scheme to generate pseudonym tickets by using the identities embedded in attestation identity keys (AIKs) certified by the privacy certificate authority (PCA). Vives-Guasch *et al.* [38] proposed a light-weight e-ticket scheme using pseudonyms which also addressed exculpability (i.e. a service provider cannot falsely accuse a user of having overspent her ticket, and the user is able to demonstrate that she has already validated the ticket before using it) and reusability (i.e. a ticket can be used a predefined number of times). In [38], pseudonyms were used to provide unlinkability of users' transactions. Kerschbaum *et al.* [11] considered the privacy-preserving billing issue in e-ticket schemes and applied pseudonyms to provide unlinkability of user transactions. These schemes can implement anonymity, ticket unlinkability as well as ticket untransferability, but, unlike our scheme, they do not support privacy-preserving attribute-based ticketing. Furthermore, the security of these schemes was not formally proven.

E-Tickets from Special Devices. There are other e-ticket schemes designed around special devices, including personal trusted device (PTD) [39], trusted platform module (TPM) [37], mobile handsets [40], *etc.* Unlike our scheme, these schemes require special devices and do not enable de-anonymisation after double spending a ticket nor do they support privacy-preserving attribute-based ticketing.

We compare our scheme with related schemes in Table 1, in terms of unlinkability, untransferability, double spend detection, de-anonymisation, attribute-based ticketing and security proof, where -- indicates that security was not considered by the authors of the respective schemes.

The European Telecommunications Standards Institute (ETSI) [41], [42] released two specifications on attribute-based encryption (ABE) which can be used to securely protect personal data and implement fine-grained access control. In an ABE scheme, a message is encrypted by using a set of attributes so that only the users whose attributes match those in the ciphertext can decrypt it and see the message. As specified in [42], ABE supports offline access control. However, in our scheme, a user can only authenticate to an online verifier. Furthermore, an issued credential enables a user to prove that she holds required attributes without revealing them.

1.3 Organisation

The remainder of this paper is organised as follows. In Section 2, the preliminaries used throughout this paper are

described. The construction of our scheme is presented in Section 4. In Section 5, the performance of our scheme is evaluated. Section 6 presents the security proof of our scheme. Finally, Section 7 concludes this paper.

2 PRELIMINARIES

In this section, the preliminaries used throughout this paper are introduced. The most important notation is summarised in Table 2. We define a function $\epsilon(x)$ is negligible if for any $k \in \mathbb{N}$, there exists an N_k such that $\epsilon(y) \leq \frac{1}{y^k}$ for all $y > N_k$.

2.1 Bilinear Groups

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_\tau$ be cyclic group with prime order p . A map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_\tau$ is a bilinear map if the following properties are satisfied [43]:

- 1) **Bilinearity.** For all $g \in \mathbb{G}_1$, $h \in \mathbb{G}_2$ and $x, y \in \mathbb{Z}_p$, $e(g^x, h^y) = e(g^y, h^x) = e(g, h)^{xy}$;
- 2) **Non-degeneration.** For all $g \in \mathbb{G}_1$ and $h \in \mathbb{G}_2$, $e(g, h) \neq 1_\tau$ where 1_τ is the identity element in $\mathbb{G}_\tau$;
- 3) **Computability.** For all $g \in \mathbb{G}_1$ and $h \in \mathbb{G}_2$, there exists an efficient algorithm to compute $e(g, h)$.

Note that Galbraith, Paterson and Smart [44] classified pairings into three basic types: Type-I: $\mathbb{G}_1 = \mathbb{G}_2$; Type-II: $\mathbb{G}_1 \neq \mathbb{G}_2$ and there exists an efficient map $\psi : \mathbb{G}_1 \rightarrow \mathbb{G}_2$; Type-III: $\mathbb{G}_1 \neq \mathbb{G}_2$ but there is no efficient map between $\mathbb{G}_1$ and $\mathbb{G}_2$. Our scheme is based on the Type-I pairing which is used to construct the signature below.

In the case that $\mathbb{G}_1 = \mathbb{G}_2$, e is called symmetric bilinear map. Let $\mathcal{BG}(1^\ell) \rightarrow (e, p, \mathbb{G}, \mathbb{G}_\tau)$ be a symmetric bilinear group generator which takes as input a security parameter 1^ℓ and outputs a bilinear group $(e, p, \mathbb{G}, \mathbb{G}_\tau)$ with prime order p and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_\tau$.

2.2 Complexity Assumptions

Definition 1. (q -Strong Diffie-Hellman (SDH) Assumption [31]) Let $\mathcal{BG}(1^\ell) \rightarrow (e, p, \mathbb{G}, \mathbb{G}_\tau)$, g be a generator of $\mathbb{G}$ and $x \xleftarrow{R} \mathbb{Z}_p$. We say that the q -strong Diffie-Hellman assumption holds on $\mathbb{G}$ if for all probabilistic polynomial time (PPT) adversary $\mathcal{A}$ given $(g, g^x, \dots, g^{x^q})$ can output a pair $(c, g^{\frac{1}{x+c}})$ with negligible probability, namely $\text{Adv}_{\mathcal{A}}^{q\text{-SDH}} = \Pr \left[\mathcal{A}(g, g^x, \dots, g^{x^q}) \rightarrow (x, g^{\frac{1}{x+c}}) \right] \leq \epsilon(\ell)$, where $c \in \mathbb{Z}_p$.

The security of the following two signatures used in our scheme and thus our overall security can be shown to reduce to this complexity assumption.

2.3 Zero-Knowledge Proof

In this paper, we use zero-knowledge proof of knowledge protocols to prove knowledge of statements about discrete logarithms [45], including discrete logarithm, equality, product, disjunction and conjunction. We follow the notation proposed in [28] and formalised in [46]. By $\text{PoK} \left\{ (\alpha, \beta, \gamma) : A = g^\alpha h^\beta \wedge \tilde{A} = \tilde{g}^\alpha \tilde{h}^\gamma \right\}$, we denote a zero-knowledge proof of knowledge of α, β and γ such that $A = g^\alpha h^\beta$ and $\tilde{A} = \tilde{g}^\alpha \tilde{h}^\gamma$ hold in groups $\mathbb{G}$ and $\tilde{\mathbb{G}}$ simultaneously, where $\mathbb{G} = \langle g \rangle = \langle h \rangle$ and $\tilde{\mathbb{G}} = \langle \tilde{g} \rangle = \langle \tilde{h} \rangle$. Conventionally, the values in the parenthesis (α, β, γ) denote quantities of knowledge which is being proven, while the other values are public to the verifier.

TABLE 1
The Comparison Between Our Scheme and Related Schemes

Schemes	Unlinkability	Untransferability	Double Spend Detection	De-anonymisation	Attribute-based Ticketing	Security Proof
[3]	✓	✓	✓	✗	✗	Sketch
[9]	✓	✗	✓	✗	✗	Sketch
[27]	✓	✓	✓	✓	✗	Sketch
[29]	✓	✓	✓	✓	✗	Sketch
[10]	✓	✓	✓	✓	✗	--
[19]	✓	✓	✓	✗	✗	Sketch
[20]	✓	✗	✓	✓	✗	Sketch
[12], [21]	✓	✓	✓	✗	✗	Sketch
[7]	✓	✓	✓	✗	✗	Sketch
[8]	✓	✓	✓	✓	✗	Sketch
[36]	✓	✓	✗	✗	✗	--
[37]	✓	✓	✓	✓	✗	--
[38]	✓	✓	✓	✓	✗	--
[11]	✓	✓	✓	✓	✗	Sketch
Our Scheme	✓	✓	✓	✓	✓	Reduction

TABLE 2
Notation

1^ℓ	A security number
$\epsilon(\ell)$	A negligible function in ℓ
CA	A central authority
S	A ticket seller
U	A user
V	A ticket verifier
H	A cryptographic hash function
$\mathbb{P}$	A universal set of ticket policies
$\mathbb{P}_U$	The policies satisfied by U
$\mathbb{R}_j$	The j -th range policy
$\mathbb{S}_i$	The i -th set policy
I_{ij}	The j -th item in $\mathbb{S}_i$
σ_S	A credential of S
σ_U	A credential of U
A_U	The attributes of U
ID_U	The identity of U
ID_S	The identity of S
PoK	Proof of knowledge
Ps_U	A pseudonym of U
$Serv$	The services requested by U
VP_X	A validity period for X
MSK	The master secret key of the system
$params$	The public parameters of the system
$Price$	The price of a ticket
$Ticket_U$	A ticket of U
$Trans_T$	A proof transcript of the ticket $Ticket_U$
$\mathcal{KG}(1^\ell)$	A secret-public key pair generation algorithm
$\mathcal{BG}(1^\ell)$	A bilinear group generator
$x \xleftarrow{R} X$	x is randomly selected from the set X
$A(x) \rightarrow y$	y is obtained by running the algorithm $A(\cdot)$ with input x
$A_U \models I_{ij}$	A_U satisfies the item I_{ij}
(SK_S, PK_S)	A secret-public key pair of S
(SK_U, PK_U)	A secret-public key pair of U

2.4 Boneh-Boyen (BB) Signature

In 2004, Boneh and Boyen [31] proposed a short signature scheme. This scheme was used to construct efficient set-membership proof and range proof [47]. In this paper, we use this signature scheme to generate tags for the ticket policies. The scheme works as follows:

KeyGen. Let $\mathcal{BG}(1^\ell) \rightarrow (e, p, \mathbb{G}, \mathbb{G}_\tau)$ and g_1, g_2 be generators of $\mathbb{G}$. The signer generates a secret-public key pair (x, Y) where $x \xleftarrow{R} \mathbb{Z}_p$ and $Y = g_2^x$.

Signing. To sign on a message $m \in \mathbb{Z}_p$, the signer computes the signature as $\sigma = g_1^{\frac{1}{x+m}}$.

Verifying. To verify whether σ is a signature on the message m , the verifier checks $e(\sigma, Y g_2^m) \stackrel{?}{=} e(g_1, g_2)$.

Theorem 1. (Boneh and Boyen [31]) This signature scheme is $(q_S, \epsilon(\ell))$ -secure against existentially forgery under the weak chosen message attacks if the $(q, \epsilon'(\ell))$ -SDH assumption holds on $(e, p, \mathbb{G}, \mathbb{G}_\tau)$, where q_S is the number of signing queries made by the adversary $\mathcal{A}$, $q > q_S$ and $\epsilon'(\ell) = \epsilon(\ell)$.

2.5 Signature with Efficient Proof Protocol

Au *et al.* [48] proposed a signature with an efficient proof protocol scheme and referred to it as BBS+ signature. In this paper, we use their signature scheme to issue credentials to users and ticket sellers and to generate tickets for users. This scheme works as follows:

KeyGen. Let $\mathcal{BG}(1^\ell) \rightarrow (e, p, \mathbb{G}, \mathbb{G}, \mathbb{G}_\tau)$ and $(h, g_0, g_1, \dots, g_{n+1})$ be generators of $\mathbb{G}$. The signer generates a secret-public key pair (x, Y) where $x \xleftarrow{R} \mathbb{Z}_p$ and $Y = h^x$.

Signing. To sign on $(m_1, m_2, \dots, m_n) \in \mathbb{Z}_p^n$, the signer selects $w, s \xleftarrow{R} \mathbb{Z}_p$ and computes $\sigma = (g_0 g_1^s g_2^{m_1} \dots g_{n+1}^{m_n})^{\frac{1}{x+w}}$. The signature on $(m_1, m_2, \dots, m_n)$ is (w, s, σ) .

Verifying. To verify whether (w, s, σ) is a valid signature on $(m_1, m_2, \dots, m_n)$, the verifier checks $e(\sigma, Y h^w) \stackrel{?}{=} e(g_0 g_1^s g_2^{m_1} \dots g_{n+1}^{m_n}, h)$.

Proof of the Signature. To prove (w, s, σ) is a signature on $(m_1, m_2, \dots, m_n)$, the prover selects $r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$, and computes $A_1 = \sigma g_2^{r_1}$ and $A_2 = g_1^{r_1} g_2^{r_2}$. Let $t_1 = w r_1$ and $t_2 = w r_2$. We utilise Au *et al.*'s [48] honest-verifier zero-knowledge proof of knowledge protocol, Π , as follows:

$$\text{PoK} \left\{ \begin{array}{l} (r_1, r_2, t_1, t_2, w, s, \sigma, m_1, \dots, m_n) : A_2 = g_1^{r_1} g_2^{r_2} \wedge \\ A_2^w = g_1^{t_1} g_2^{t_2} \wedge \frac{e(A_1, Y)}{e(g_0, h)} = e(g_1, h)^s \cdot e(A_1, Y)^{-w} \cdot \\ e(g_2, h)^{r_1 w} \cdot e(g_2, Y)^{r_1} \cdot \prod_{i=2}^{n+1} e(g_i, h)^{m_i - 1} \end{array} \right\}.$$

Theorem 2. (Au *et al.* [48]) This signature with an efficient proof protocol is $(q_S, \epsilon(\ell))$ -existentially unforgeable under the adaptively chosen message attacks if the

$(q, \epsilon'(\ell))$ -SDH assumption holds on $(e, p, \mathbb{G}, \mathbb{G}_\tau)$, where q_S is the number of signing queries made by the adversary $\mathcal{A}$, $q > q_S$ and $\epsilon(\ell)' > q \cdot \epsilon(\ell)$.

3 FORMAL DEFINITIONS AND SECURITY MODELS

In this section, we provide the formal definitions and security models of our scheme which will be used to verify its security.

3.1 Formal Definitions

Our scheme consists of the following four entities: central authority CA, user U, ticket seller S and ticket verifier V. CA authenticates U and S, and issues anonymous credentials to them; S registers to the CA, obtains anonymous credentials from the CA, and sells tickets to U in accordance with the ticket policies; U registers to the CA, obtains anonymous credentials from the CA, purchases tickets from S, and proves the possession of tickets to V; V validates the tickets provided by U and detects whether a ticket is double spent.

The interactions between the different entities in our scheme is shown in Fig. 1. The algorithms associated with these interactions are formally defined as follows:

Setup $(1^\ell) \rightarrow (MSK, params, \mathbb{P})$. CA inputs a security parameter 1^ℓ , and outputs the master secret key MSK , the public parameters $params$ and a universal set of ticket policies $\mathbb{P}$.

Registration. This algorithm consists of the following two sub-algorithms: S's registration **SRegistration** and U's registration **URegistration**.

- 1) **SRegistration** $(S(ID_S, SK_S, PK_S, params) \leftrightarrow CA(MSK, PK_S, params)) \rightarrow (\sigma_S, (ID_S, PK_S))$. S runs the key generation algorithm $\mathcal{KG}(1^\ell) \rightarrow (SK_S, PK_S)$ to generate his secret-public key pair (SK_S, PK_S) , inputs his identity ID_S , his secret-public key pair (SK_S, PK_S) and the public parameters $params$, and outputs a credential σ_S . CA inputs his secret key MSK , S's public key PK_S and the public parameters $params$, and outputs (ID_S, PK_S) .
- 2) **URegistration** $(U(ID_U, A_U, SK_U, PK_U, params) \leftrightarrow CA(MSK, A_U, PK_U, params)) \rightarrow (\sigma_U, (ID_U, PK_U))$. U runs the key generation algorithm $\mathcal{KG}(1^\ell) \rightarrow (SK_U, PK_U)$ to generate his secret-public key pair (SK_U, PK_U) , inputs his identity ID_U , his attributes A_U , his secret-public key pair (SK_U, PK_U) and the public parameters $params$, and outputs a credential σ_U . CA inputs the master secret key MSK , U's attributes A_U , U's public key PK_U and the public parameters $params$, and outputs (ID_U, PK_U) .

Ticket-Issuing $(U(SK_U, PK_U, A_U, \sigma_U, Ps_U, \mathbb{P}, VP, Serv, params) \leftrightarrow S(SK_S, PK_S, Ps_U, \mathbb{P}, Price, VP, Serv, params)) \rightarrow (Ticket_U, (Ps_U, Service))$. This is an interactive algorithm executed between U and S. U inputs his secret-public key pair (SK_U, PK_U) , his attributes A_U , his credential σ_U , a pseudonym Ps_U , the ticket policies $\mathbb{P}$, a valid period VP , the selected services $Serv$ and the public

parameters $params$, and outputs a ticket $Ticket_U$. S inputs his secret-public key pair (SK_S, PK_S) , the pseudonym Ps_U , the ticket policies $\mathbb{P}$, the ticket price $Price$, the valid period VP , the selected services $Serv$ and the public parameters $params$, and outputs $(Ps_U, Serv)$.

Ticket-Validating $(U(SK_U, Ps_U, Ticket_U, VP, Serv, params) \leftrightarrow V(VP, Serv, params)) \rightarrow (0/1, (Serv, Trans_T))$. This is an interactive algorithm executed between U and V. U inputs his secret-public key pair (SK_U, PK_U) , his ticket $Ticket_U$, the valid period VP , the selected services $Serv$ and the public parameters $params$, and outputs 1 if $Ticket_U$ is valid; otherwise it outputs 0 to indicate a failure. V inputs the valid period VP , the selected services $Serv$ and the public parameters $params$, and outputs $(Serv, Trans_T)$.

Double-Spend-Detecting $(Trans_T, params) \rightarrow (PK_U, \perp)$. V inputs a proof transcript $Trans_T$ and the public parameters $params$ and outputs U's public key PK_U if U has used a ticket twice; otherwise it outputs $\perp$ to indicate that no double spend is found.

Definition 2. A privacy-preserving electronic ticket scheme with attribute-based credential is correct if

$$\Pr \left[\begin{array}{l} \text{Ticket-} \\ \text{Validating} \\ (U(SK_U, \\ Ps_U, \\ Ticket_U, \\ VP, Serv, \\ params) \\ \leftrightarrow V(VP, \\ Serv, \\ params)) \\ \rightarrow (1, \\ (Serv, \\ Trans_T)) \end{array} \middle| \begin{array}{l} \text{Setup}(1^\ell) \rightarrow (msk, params, \mathbb{P}); \\ \text{SRegistration}(S(ID_S, SK_S, \\ PK_S, params) \leftrightarrow CA(MSK, \\ PK_S, params)) \rightarrow (\sigma_S, (ID_S, \\ PK_S)); \\ \text{URegistration}(U(ID_U, A_U, \\ SK_U, PK_U, params) \leftrightarrow \\ CA(MSK, PK_U, A_U, params)) \\ \rightarrow (\sigma_U, (ID_U, PK_U)); \\ \text{Ticket-Issuing}(U(SK_U, PK_U, \\ A_U, \sigma_U, Ps_U, \mathbb{P}, VP, Serv, \\ params) \leftrightarrow S(SK_S, PK_S, \\ Ps_U, \mathbb{P}, VP, Serv, params)) \\ \rightarrow (Ticket_U, (Ps_U, Serv)); \\ A_U \models \mathbb{P} \end{array} \right] = 1$$

and

$$\Pr \left[\begin{array}{l} \text{Double-} \\ \text{Spend-} \\ \text{Detecting} \\ (Trans_T, \\ params) \\ \rightarrow PK_U \end{array} \middle| \begin{array}{l} \text{Setup}(1^\ell) \rightarrow (msk, params, \mathbb{P}); \\ \text{SRegistration}(S(ID_S, SK_S, \\ PK_S, params) \leftrightarrow CA(MSK, \\ PK_S, params)) \rightarrow (\sigma_S, (ID_S, \\ PK_S)); \\ \text{URegistration}(U(ID_U, A_U, \\ SK_U, PK_U, params) \leftrightarrow \\ CA(MSK, PK_U, A_U, params)) \\ \rightarrow (\sigma_U, (ID_U, PK_U)); \\ \text{Ticket-Issuing}(U(SK_U, PK_U, \\ A_U, \sigma_U, Ps_U, \mathbb{P}, VP, Serv, \\ params) \leftrightarrow S(SK_S, PK_S, Ps_U, \\ \mathbb{P}, VP, Service, params)) \rightarrow \\ (T_U, (Ps_U, Service)); \\ A_U \models \mathbb{P} \wedge T_U \text{ is double spent.} \end{array} \right] = 1.$$

3.2 Security Model

While Universally Composable (UC) security models [49] can offer strong security, it is very difficult to construct

Fig. 1. The Model of our scheme

a scheme which can be shown to provide UC security. To the best of our knowledge, none of the existing smart ticketing schemes was proven in UC security model. Consequently, the security of our scheme is defined by using the simulation-based definition as introduced in [50], [51], [52], [53]. The simulation-based model is defined by the indistinguishability between the following real world and ideal world experiment.

The Real-World Experiment. We first present how our scheme works where the central authority CA, the ticket seller S, the user U and the ticket verifier V are honest. The real-world adversary $\mathcal{A}$ can control S, U and V, but cannot control CA. The entities controlled by $\mathcal{A}$ can deviate arbitrarily from their behaviour described below. CA runs $Setup(1^\ell) \rightarrow (MSK, params, \mathbb{P})$ to generate the master secret key msk , system public parameters $params$ and the universal set $\mathbb{P}$ of ticket polices, and sends $params$ and $\mathbb{P}$ to U, S and V.

When receiving a registration message $(registration, ID_S)$ from $\mathcal{E}$, S executes the seller registration algorithm $SRegistration$ with CA. S runs $KG(1^\ell) \rightarrow (SK_S, PK_S)$, takes as input his identity ID_S , the secret-public key pair (SK_S, PK_S) and the public parameters $params$, outputs a credential σ_S . CA takes inputs his master secret key MSK , S's public key PK_S and the public parameters $params$, and outputs S's identity ID_S and public key PK_S . S sends a bit $b \in \{0, 1\}$ to $\mathcal{E}$ to show whether the $SRegistration$ algorithm succeed ($b = 1$) or failed ($b = 0$).

When receiving a registration message $(registration, ID_U, A_U)$ from $\mathcal{E}$, U executes the user registration algorithm $URegistration$ with CA. U runs $KG(1^\ell) \rightarrow (SK_U, PK_U)$, takes as input his identity ID_U , attributes A_U , secret-public key pair (SK_U, PK_U) and the public parameters $params$, and outputs a credential σ_U . CA takes inputs his master secret key MSK , U's public key PK_U and the public parameters $params$, and outputs U's identity ID_U , attributes A_U and public key PK_U . U sends a bit $b \in \{0, 1\}$ to $\mathcal{E}$ to show whether the $URegistration$ algorithm succeed ($\tilde{b} = 1$) or failed ($\tilde{b} = 0$).

When receiving a ticket issuing message $(ticket$

$_{issuing}, A_U, VP, Service)$ from $\mathcal{E}$, U first checks whether he has got a credential for A_U . If so, U executes the ticket issuing algorithm $Ticket-Issuing$ with S. U takes as inputs his secret-public key pair (SK_U, PK_U) , attributes A_U , a pseudonym Ps_U , his credential σ_U , the valid period VP , the service $Serv$ and the public parameters $params$. S takes as input his secret-public key pair (SK_S, PK_S) , the valid period VP , the service $Serv$ and the public parameters $params$. Finally, U obtains a ticket T_U or $\perp$ to show failure. S outputs U's pseudonym Ps_U and the service $Serv$. If the ticket issuing is successful, U sends a bit $\tilde{b} \in \{0, 1\}$ to $\mathcal{E}$ to show the $Ticket-Issuing$ algorithm succeed ($\tilde{b} = 1$) or failed ($\tilde{b} = 0$).

When receiving a ticket validation message $(ticket_{validating}, T_U, VP, Serv, params)$ from $\mathcal{E}$, U first checks whether he has the ticket T_U which includes the valid period VP and the service $Serv$. If so, U executes the ticket validating algorithm $Ticket-Validating$ with V; otherwise U outputs $\perp$ to show he does not have the ticket T_U . If U has the ticket T_U , he takes as input his secret-public key pair (SK_U, PK_U) , the ticket T_U , the valid period VP , the service $Serv$ and the system public parameters $params$, and outputs a bit $\hat{b} \in \{0, 1\}$ to show whether the ticket is valid ($\hat{b} = 1$) or invalid ($\hat{b} = 0$). V takes input the valid period VP , the service $Serv$ and the public parameters $params$, and outputs the service $Serv$ and the transcript $Trans$. Finally, if $\hat{b} = 1$, U returns *success*; otherwise U returns *fail*.

When receiving a double spend detecting message $(double_spend_detecting, Trans, params)$ from $\mathcal{E}$, V checks that whether there is a $(Trans', params)$ with $Trans = Trans'$. If so, V returns a bit $\bar{b} = 1$ to indicate that it is a double spend ticket; otherwise $\bar{b} = 0$ is returned to show that the ticket has not been double spent.

The Ideal-World Experiment. In the ideal world experiment, there are the same entities as in real world experiment, including the central authority CA' , ticket seller S' , user U' and ticket verifier V' . All communications among these entities must go through a trusted party TP. The behaviour of TP is described as follows. TP maintains four lists which are

initially empty: a ticket seller credential list, a user credential list, a ticket list for each user and a ticket validating list.

When receiving a registration message (*registration*, $ID_{S'}$) from S' , TP sends (*registration*, $ID_{S'}$) to CA' and obtains a bit $\nu \in \{0, 1\}$ from CA' . If $\nu = 1$, TP adds S' into the ticket seller credential list and sends ν to S' ; otherwise, TP sends $\nu = 0$ to S' to indicate failure.

When receiving a registration message (*registration*, $ID_{U'}$, $A_{U'}$) from U' , TP sends (*registration*, $ID_{U'}$, $A_{U'}$) to CA' and obtains a bit $\tilde{\nu} \in \{0, 1\}$ from CA' . If $\tilde{\nu} = 1$, TP adds (U' , $A_{U'}$) into the user credential list and sends $\tilde{\nu}$ to U' ; otherwise, TP sends $\tilde{\nu} = 0$ to S' to indicate failure.

When receiving a ticket issuing message (*ticket_issuing*, Ps_U , $Price$, VP , $Serv$) from U' , TP sends (*ticket_issuing*, Ps_U , $Price$, VP , $Serv$) to S' and obtains a bit $\hat{\nu} \in \{0, 1\}$ from S' . If $\hat{\nu} = 1$, TP adds (U' , $A_{U'}$, Ps_U , $Price$, VP , $Serv$) into the user ticket list, and sends $\hat{\nu}$ to V' ; otherwise, TP sends $\hat{\nu} = 0$ to U' to indicate failure.

When receiving a ticket validating message (*ticket_validating*, $T_{U'}$) from V' , TP checks whether $T_{U'}$ is in the user ticket list. If so, TP sends a bit $\bar{\nu} = 1$ to U' and puts $T_{U'}$ into the ticket validation list TVL ; otherwise, TP sends $\bar{\nu} = 0$ to indicate failure.

When receiving a double spend detecting message (*double_spend_detecting*, $T_{U'}$) from V' , TP checks whether $T_{U'} \in TVL$. If it is, TP returns $\tilde{\nu} = 1$ to U' to indicate it is double spend; otherwise, $\tilde{\nu} = 0$ is returned to show it is not double spend.

The entities CA' , S' , U' and V' in ideal world simply relay the inputs and outputs between $\mathcal{E}$ and TP.

Definition 3. Let $\mathbf{Real}_{\mathcal{E}, \mathcal{A}}(\ell)$ be the probability that the environment $\mathcal{E}$ outputs 1 when running in the real world with the adversary $\mathcal{A}$ and $\mathbf{Ideal}_{\mathcal{E}, \mathcal{A}'}$ be the probability that $\mathcal{E}$ outputs 1 when running in the ideal world with the adversary $\mathcal{A}'$. A set of cryptographic protocols is said to securely implement privacy-preserving electronic ticket scheme with attribute-based credential if $|\mathbf{Real}_{\mathcal{E}, \mathcal{A}}(\ell) - \mathbf{Ideal}_{\mathcal{E}, \mathcal{A}'}(\ell)| \leq \epsilon(\ell)$.

Security Properties. We now look at the security properties of our scheme which the ideal-world experiment can provide.

User's Privacy. S' does not know users' identities and their exact attributes, namely S' only knows that a user buys a ticket for which she has the required attributes. Even if S' colludes with V' and potentially with other users, they can only try to know the attributes required by the ticket policies. Furthermore, two tickets for the same users cannot be linked. Since each user needs to prove that he knows the corresponding secret key included in a ticket when using the ticket, he cannot transfer his tickets to others.

Seller's Security. U' cannot generate a ticket on behalf of the seller S' . Even if U' colludes potentially with other users and V' , they cannot forge a valid ticket. Since a double spend ticket can be detected and the real user can be identified, U' cannot double spend a ticket. Therefore, the seller's security includes both unforgeability, double spend detection and de-anonymization.

4 CONSTRUCTION OF OUR SCHEME

In this section, we describe the formal construction of our scheme. Our scheme uses a number of ideas and concepts from Au *et al.*'s signature with efficient protocol scheme [48], Camenisch *et al.*'s set-membership proof scheme and range proof scheme [47], Pedersen's commitment scheme [25] and Au *et al.*'s e-cash [54] scheme. In particular, we incorporated Au *et al.*'s signature scheme which enables a user to obtain a signature on a committed block of attributes and prove the knowledge of the signature in zero-knowledge. This is to issue credentials to users and ticket sellers and to generate tickets for users. We adapt Camenisch *et al.* [47]'s set-membership proof and range proofs schemes to prove a user's attributes. In our scheme, these attributes are additionally certified by a trusted third party as well. Pedersen's commitment scheme is used in our scheme to hide the knowledge which a prover needs to prove. Lastly we incorporate Au *et al.*'s [54] approach to detect and de-anonymise a double spend user.

Construction challenges: The schemes described in [25], [47], [48], [54] form the basis of our construction, the challenge is to combine and adapt them such that the resulting scheme provides the following three additional features: (1) The attributes (e.g. age, disability, *etc.*) which a user needs to prove to a ticket seller must be certified by a trusted third party or otherwise users could simply buy discounted tickets using attributes which they do not possess. To address this, Au *et al.*'s signature scheme [48] is used to certify a user's attributes. (2) Tickets need to be untransferable and unlinkable while doublespend detection must be possible. Thus our tickets are generated using anonymous credentials (unlinkability) which include a user's personal information (untransferability). To detect a double spend user, each ticket includes a serial number. If two tickets have the same serial number, the public trace technique proposed by Au *et al.* in [54] is used to reveal the user's identity (via her public key). (3) To provide a high degree of flexibility for setting ticket policies, both range policies and set policies must be available for use. Users can then use their certified attributes to demonstrate membership of multiple range and set policies, e.g. to get a young-persons discount, a frequent traveller bonus as well as a disability reduction.

4.1 High-Level Overview

In our e-ticket system, the type of tickets can be influenced by two kinds of policies: range and set. Range policies might include attributes like age, number of journeys made, salary, *etc.*; while set policies might consist of various other attributes, such as profession, disability, location, *etc.*

Setup. Figure 2 shows how the scheme is initialised. The ticket price polices $\mathbb{P}$ is set to $\mathbb{P} = \{\mathbb{R}_1, \dots, \mathbb{R}_{N_1}, \mathbb{S}_1, \dots, \mathbb{S}_{N_2}\}$ where $\{\mathbb{R}_1, \dots, \mathbb{R}_{N_1}\}$ are the supported range policies and $\{\mathbb{S}_1, \dots, \mathbb{S}_{N_2}\}$ are the supported set policies. The CA selects the following secret keys $MSK = (x, y, \mu_1, \dots, \mu_{N_2})$ where x is used to generate credentials for users of the system, y is used to generate tags identifying the range policies and the μ_i ($i = 1, \dots, N_2$) are used to generate tags identifying the set policies. The CA then publishes the public parameters *params* which include the ticket price policy $\mathbb{P}$ together with the range and set policy tags.

CA publishes the ticket price policies $\mathbb{P} = \{\mathbb{R}_1, \dots, \mathbb{R}_{N_1}, \mathbb{S}_1, \dots, \mathbb{S}_{N_2}\}$ where $\mathbb{R}_l = [c_l, d_l]$ is a range policy (i.e. age, mileage) and $\mathbb{S}_i = \{I_{i_1}, I_{i_2}, \dots, I_{i_\varsigma}\}$ is a set policy (i.e. location, profession, disability) and consists of ς items I_{i_j} for $l = 1, 2, \dots, N_1$ and $i = 1, 2, \dots, N_2$.

CA runs $\mathcal{BG}(1^\ell) \rightarrow (e, p, \mathbb{G}, \mathbb{G}_\tau)$. Suppose that the longest interval length in $\{\mathbb{R}_1, \dots, \mathbb{R}_{N_1}\}$ is $[0, q^k]$ where $q \in \mathbb{Z}_p$ and $p > 2q^k + 1$. Let $g, g_0, g_1, g_2, g_3, \hat{g}_1, \hat{g}_2, \dots, \hat{g}_{N_1}, h, \mathfrak{g}, \eta, \xi, \rho, \vartheta, \eta_1, \eta_2, \dots, \eta_{N_2}$ be generators of $\mathbb{G}$, $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$ and $H' : \{0, 1\}^* \rightarrow \mathbb{G}$ be two cryptographic hash functions.

CA selects $x, y, \mu_1, \mu_2, \dots, \mu_{N_2} \xleftarrow{R} \mathbb{Z}_p$ and computes $\tilde{g} = g^x, \tilde{h} = h^y, h_0 = h^{\frac{1}{y}}, h_1 = h^{\frac{1}{y+1}}, h_2 = h^{\frac{1}{y+2}}, \dots, h_{q-1} = h^{\frac{1}{y+q-1}}, \tilde{h}_0 = h^{q^0}, \tilde{h}_1 = h^q, \dots, \tilde{h}_{k-1} = h^{q^{k-1}}, \tilde{\eta}_1 = \eta_1^{\mu_1}, \tilde{\eta}_2 = \eta_2^{\mu_2}, \dots, \tilde{\eta}_{N_2} = \eta_{N_2}^{\mu_{N_2}}$ and $\left(\eta_{i_1} = \eta^{\frac{1}{\mu_i + H(I_{i_1})}}, \eta_{i_2} = \eta^{\frac{1}{\mu_i + H(I_{i_2})}}, \dots, \eta_{i_\varsigma} = \eta^{\frac{1}{\mu_i + H(I_{i_\varsigma})}} \right)_{i=1}^{N_2}$.

The secret key of CA is $MSK = (x, y, \mu_1, \mu_2, \dots, \mu_{N_2})$ and the public parameters are $params = (e, p, \mathbb{G}, \mathbb{G}_\tau, g, g_0, g_1, g_2, \hat{g}_1, \hat{g}_2, \dots, \hat{g}_{N_1}, h, \mathfrak{g}, \eta, \xi, \rho, \tilde{g}, \tilde{h}, h_0, h_1, \dots, h_{q-1}, \tilde{h}_0, \tilde{h}_1, \dots, \tilde{h}_{k-1}, \eta_1, \eta_2, \dots, \eta_{N_2}, \tilde{\eta}_1, \tilde{\eta}_2, \dots, \tilde{\eta}_{N_2}, (\eta_{i_1}, \eta_{i_2}, \dots, \eta_{i_\varsigma})_{i=1}^{N_2})$.

Fig. 2. Setup Algorithm

Registration. The steps involved in the registration process are shown in Figure 3. The registration of a seller S requires S to generate a secret-public key pair (x_s, Y_S) . He sends Y_S to the CA as well as a proof of knowledge Π_S^1 to demonstrate he knows the secret key x_s . Using some out-of-band channel, S authenticates himself to the CA and provides evidence that he is allowed to operate as a seller. If Π_S^1 is valid and the authentication is successful, the CA generates a credential σ_S which is a BBS+ signature including the public key Y_S as well as a validity period VP_S for it. These details are then sent back to S who verifies that the CA has authorized him as a seller by validating the credential σ_S .

In the case of a user registration, a user U generates a secret-public key pair (x_u, Y_U) and submits her public key Y_U together with a proof of knowledge Π_U^1 showing that she knows the secret key x_u . She also sends the CA the list of attributes A_U (e.g. age, profession, location, etc.) which allow her to get discounted tickets. Again, using an out-of-band channel, she authenticates herself to the CA and provides evidence for the claimed attributes. If Π_U^1 holds, the authentication is successful and the CA is satisfied with the provided evidence, it generates a credential σ_U which is a BBS+ signature scheme including the public key Y_U , its validity period VP_U as well as the corresponding attributes A_U . These details are sent back to U who uses them to verify that she is now a legitimate user of the system and that her attributes have been certified by the CA.

Ticket Issuing. Figure 4 shows the details of the ticket issuing phase. Let $\mathbb{P}_U$ consists of the names of range policies and set policies satisfied by U . In order to prevent attackers from collecting users' private information, a seller S first needs to prove to U that he is authorised by the CA. This is done by constructing a proof of knowledge Π_S^2 of the seller's credential σ_S . If the proof holds, the user U proceeds by generating a new pseudonym Y which involves her secret key x_u and constructs a proof of knowledge Π_U^2 of Y . This proof shows to S that the CA has certified her as a legitimate user who has the claimed attributes which entitle her to buy the ticket corresponding to her provided attributes. After S has successfully verified her proof, he constructs a ticket T_U applying a BBS+ signature scheme which includes the user's

pseudonym Y , the applicable range and set policies of the user relevant to the ticket, a serial number to enable double spend detection as well as the ticket's price and validity period VP_T . Note that while the ticket price and its validity period are included in the construction of T_U , they are just free text entries and should only be used when price and validity periods are required by the application context, e.g. when the validity period is important, S should check the user's credential valid period VP_U and make sure that the ticket valid period VP_T is no later than VP_U . T_U together with its associated details is then sent back to the user who can use the information together with the public key of the seller Y_S to verify the validity of the information. Note that our scheme provides *ticket unlinkability* due to the use of user pseudonyms which prevents the seller S as well as any verifier V from linking any two tickets requested by the same user even if they collude.

Ticket Validation. Figure 5 depicts the steps to validate a ticket. The user U initializes an empty table $Table_U$ to store the identity information of any verifier V . The purpose of this table is to ensure that a verifier can only ask for a ticket once to prevent an honest user from being de-anonymised by a malicious verifier. The verifier V , on the other hand, initializes an empty table $Table_V$ to store the authentication transcript from U to determine if a ticket has already been used (i.e. double spend detection). The ticket verification process is started by the verifier sending a fresh nonce r and its identity ID_V to the user. It is assumed that there is some out-of-band channel which allows the user to "authenticate" the verifier, e.g. it is a guard on the train or a gate at the entrance of the platform, etc. U first checks that V does not yet have an entry in $Table_U$. If an entry exists, U aborts the process to avoid de-anonymisation. Otherwise, she proceeds to send V a "ticket transcript", $Trans_T$, of her ticket $Ticket_U$, which includes a zero-knowledge proof of knowledge Π_U^3 . The transcript should convince V that she is a legitimate user who is in the possession of a valid ticket $Ticket_U$. Because $Ticket_U$ includes the user's secret key x_u as part of her pseudonym Y , knowledge of which needs to be demonstrated as part of Π_U^3 . Our scheme ensures *ticket untransferability* assuming U 's private key has not been

Fig. 3. Registration Algorithm

compromised. Moreover, the transcript also incorporates V 's nonce r to prevent simple replay attacks. U completes her part in the validation process by updating her $Table_U$ storing V 's identity together with r . If V can successfully verify U 's ticket transcript, V grants her access to the service and updates $Table_V$ with $Trans_T$; otherwise, V denies the request.

Double Spend Detecting. Figure 6 shows the double spend detection process. To determine whether a ticket is being double spent, V checks $Table_V$ for another ticket transcript $Trans_U$ with the same serial number D . If there is, the ticket is being double spent and V can de-anonymise U by extracting her public key Y_U from the two transcripts; otherwise, it is a new ticket.

It is worth pointing out that the construction of our scheme has the following additional benefit.

Limited Dynamic Policy Update. If the seller S needs to either update some policies in $\mathbb{P}$ or create new ones, he can contact the central authority CA to update or create the relevant public parameters $params$. As a result, when buying a ticket, a user U proves to S that his attributes satisfy the updated policies by using the updated $params$ and S will generate tickets according to the updated policies. U only needs to obtain new credentials from the CA if her current attributes do not satisfy the updated policies any more. For example, suppose that Alice is 16 years old. If the seller S requests that the existing policy range of $[12, 18]$ is changed to $[15, 20]$ instead, then Alice can still use her existing credentials. However, if the policy were changed from $[12, 18]$ to $[18, 25]$ instead, then Alice would need to contact the CA to update her credentials.

Correctness. The correctness of our scheme is shown in the full version of this paper [55].

5 BENCHMARKING RESULTS

In this section we evaluate the performance of our scheme. The source code of the scheme's implementation is available at [56] and its performance has been measured on a Dell Inspiron Latitude E5270 laptop with an Intel Core i7-6600U CPU, 1TB SSD and 16GB of RAM running Fedora 27. The implementation makes use of bilinear maps defined over elliptic curves as well as other cryptographic primitives. We used the JPBC library [57] for the bilinear maps and bouncycastle [58] for the other cryptographic required by our scheme. Note that the Java based implementation of the JPBC API [57] was used throughout.

Recall from Section 2 that our scheme requires a Type I symmetric bilinear map, $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. The JPBC library [57] provides three different instances of a symmetric pairing with their Type A, A1 or E pairings. The Type A and A1 pairings are based on the elliptic curve $E : y^2 = x^3 + x$ over the finite field F_p . In both cases, the group $\mathbb{G}$ in is the group of points on the elliptic curve, $E(F_p)$. The Type E pairing, on the other hand, is based on the Complex Multiplication (CM) method of constructing elliptic curves starting with the Diophantine equation $DV^2 = 4p - t^2$. The details of each construction can be found in [59].

In our implementation, we use the default parameters during the instantiation of the different pairings, e.g. Type A is constructed using $rBits = 160$, $qBits = 512$, Type A1 uses 2 primes of size $qBits = 512$ and Type E is instantiated with $rBits = 160$ and $qBits = 1024$.

Note that according to Table 1 in [60], JPBC's default Type A pairing provides approximately the equivalent of 80-bit symmetric or 1024 RSA-style security. This is sufficient for providing a baseline for taking time measurements.

For the hash functions $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$ and $H' : \{0, 1\}^* \rightarrow \mathbb{G}$ required by our scheme (see Fig 2), we used

Fig. 4. Ticket Issuing Algorithm

SHA256 for H and rely on the implementation of “newElementFromHash()” method in the JPBC library for H' .

5.1 Timings

Table 3 shows the results of the computational time spent in the various phases of our proposed scheme which required more complex computations (i.e. some form of verification using bilinear maps or generation of zero knowledge proofs). The timings shown have been calculated as the average over 20 iterations.

The maximum range interval in this instance was 7 which is covered by the interval $[0, 2^3)$ and thus $k = 3$ in

the set-up algorithm described in Fig 2. The maximum set size used was 10. It is clear from the computations involved in the generation of Π_U^2 (see the full version [55]) that the computational cost of a range proof increases with k while the number of computations for a set membership proof is independent on the size of the set. As such the numbers presented below provide a reasonable lower bound of the computational costs for range proofs assuming that any useful ranges will have at least an interval length of 4 or more.

Table 3 shows the timings for our current implementation of our scheme with 2 small range policies and 4 set

<p>User: U</p> <p>Initializes an empty table: $Table_U$.</p> <p>Checks:</p> <p>(1) If $H(ID_V) \in Table_U$, aborts;</p> <p>(2) If $H(ID_V) \notin Table_U$, goes to the next step.</p> <p>Selects $\pi, \lambda \xleftarrow{R} \mathbb{Z}_p$ and computes</p> <p>$D = g^{s_u}, E = \xi^{x_u} H'(ID_V)^{rs_u}, F = T_U \vartheta^\pi, J = g^\pi \vartheta^\lambda$</p> <p>and $W = J^{\omega_u} = g^{\pi'} \vartheta^{\lambda'}$ where $\pi' = \pi \omega_u$ and $\lambda' = \lambda \omega_u$.</p> <p>Computes the proof Π_U^3:</p> <p>$PoK\{(x_u, d_u, s_u, \omega_u, \pi, \lambda, \pi', \lambda') : D = g^{s_u} \wedge$</p> <p>$P_{SU} = \xi^{x_u} g_1^{d_u} \wedge E = \xi^{x_u} H'(ID_V)^{rs_u} \wedge$</p> <p>$J = g^\pi \vartheta^\lambda \wedge W = J^{\omega_u} = g^{\pi'} \vartheta^{\lambda'} \wedge$</p> <p>$\frac{e(F, Y_S)}{e(g_0, \rho) \cdot e(P_{SU}, \rho) \cdot e(g_3, \rho)^{\psi_u}} = e(g_2, \rho)^{s_u} \cdot e(F, \rho)^{-\omega_u}.$</p> <p>$e(\vartheta, \rho)^{\pi'} \cdot e(\vartheta, \rho)^\pi\}$.</p> <p>The proof transcript is: $Trans_T = ((D, E), F, J, W, \psi_u,$</p> <p>$P_{SU}, \mathbb{P}_U, Price, Serv, VP_T, \Pi_U^3).$</p> <p>Updates: $Table_U = Table_U \cup \{H(ID_V), r\}.$</p>	<p>Ticket Verifier: V</p> <p>Initializes an empty table: $Table_V$.</p> <p>Selects $r \xleftarrow{R} \mathbb{Z}_p$</p> <p>$\xleftarrow{ID_V, r}$</p> <p>Checks $\psi_u \stackrel{?}{=} H(\mathbb{P}_U Price Serv VP_T)$</p> <p>and the proof Π_U^3.</p> <p>Updates: $Table_V = Table_V \cup \{(r, D, E),$</p> <p>$F, J, \psi_u)\}.$</p>
--	--

Fig. 5. Ticket Validation Algorithm

<p>If there exit $((r, D, E), F, J) \in Table_V$ and transcript $((r', D', E'), F', J') \in Table_V$ with $D = D'$ and $E \neq E'$, the ticket with serial number s_u is being double spent. Let $E = \xi^{x_u} H'(ID_V)^{rs_u}$ and $E' = \xi^{x_u} H'(ID_V)^{r's_u}$.</p> <p>To detect the double spend user, V computes $\frac{E^{r'}}{E'^{r'}} = \frac{\xi^{x_u r'} H'(ID_V)^{r' r s_u}}{\xi^{x_u r} H'(ID_V)^{r' r s_u}} = \xi^{x_u (r' - r)}$ and $Y_U = \xi^{x_u} = (\frac{E^{r'}}{E'^{r'}})^{\frac{1}{r' - r}}$.</p> <p>Hence, U with public key Y_U is a double spend user.</p>
--

Fig. 6. Double Spend Detection

TABLE 3
Benchmark results (in ms)

Protocol phase	Entity	(#range policies,#set policies)= (2, 4)		
		Type A	Type A1	Type E
System Initialisation - Central Authority (CA)				
initialise the system	CA	626.05.1	9155.95	2895.25
Issuing phase				
generate PoK Π_S^2	Seller	184.25	2881.8	469.1
verify Π_S^2	User	107.9	1424.95	286.2
generate ticket request, Π_U^2	User	1008.7	17195.95	2847.35
verify Π_U^2	Seller	787.3	11288.0	2166.25
generate ticket	Seller	47.85	583.0	120.3
verify ticket	User	52.5	856.75	158.35
Ticket Verification - Verifier (V)				
generate ticket transcript $Trans_T$	User	241.4	3538.7	707.4
verify transcript	Verifier	214.05	2539.8	649.8
Total system run time				
All phases	All	3659.1	54382.95	11383.1

TABLE 4
Type A: benchmark results for different ranges and set sizes(in ms)

Ticket issuing phase	$k = 5$ [0, 31]	$k = 10$ [0, 1023]	$k = 20$ [0, 1048755]	$s = 10$ { $x 1 \leq x \leq 10$ }	$s = 100$ { $x 1 \leq x \leq 100$ }
range/set proof creation	≈ 512	≈ 961	≈ 1998	≈ 35	≈ 36
range/set proof verification	≈ 367	≈ 599	≈ 1116	≈ 22	≈ 23

policies using the default instantiation of the three different symmetrical pairings available in JPBC. The fastest performance is achieved by the JPBC Type A curve based Type I pairing, where ticket issuing and verification take $\approx 2.2s$ and $\approx 450ms$ respectively.

Table 4 illustrates the impact of different range and set sizes on the computational effort during the ticket issuing phase using the JPBC Type A curve, where $[0, q^k]$ is the range length and s is the cardinality of the set. It is clear that set membership proofs can be computed much faster than range proofs and their computational cost is independent of the set size whereas for range proofs the computational effort increases linearly with k .

However, range proofs provide an additional benefit which is best illustrated with an example: a young person's age could be either codified in a range policy ($age \in [15, 25]$) or with a set policy ("young person"). Our scheme provides the policy maker with the flexibility to decide which kind of policies should be used. While a set policy is computationally more efficient than a range policy, range policies can potentially accommodate future policy changes. In particular, suppose that Alice is 23 years old and the current young person range policy is given by $age \in [16, 22]$ which means Alice cannot obtain a discount. However, if it is later changed to $age \in [16, 25]$, Alice can still use her existing age attribute of 23 to obtain a young person discount as she can now prove her age falls within the updated range. However, if the set policy approach had been used, Alice would need to return to the CA to update her credentials as she would not have been eligible for her signed "young person" attribute, previously.

Consequently, for any real system, it is important to look at the trade-off between the flexibility that range policies allow in terms of dynamic updates and their more expensive computational cost.

6 SECURITY ANALYSIS

To demonstrate its security, we need to prove indistinguishability between the behaviours of the real-world adversary $\mathcal{A}$ and the behaviours of the ideal-world adversary $\mathcal{A}'$. Given a real-world adversary $\mathcal{A}$, there exist an ideal-world adversary $\mathcal{A}'$ such that no environment $\mathcal{E}$ can distinguish whether it is interacting with $\mathcal{A}$ or $\mathcal{A}'$. The proof is based on sublemmas where different corrupted parties are considered. The following cases are not considered: (1) the CA is the only honest party; (2) the CA is the only dishonest party; (3) all parties are dishonest; and (4) all parties are honest. The first three do not make a sensible system while the last one is trivially secure. Since the CA needs to know U 's attributes to issue her with her credentials, we assume that CA is honest and fully trusted by the other entities.

In order to prove the indistinguishability between $\text{Real}_{\mathcal{E}, \mathcal{A}}(\ell)$ and $\text{Ideal}_{\mathcal{E}, \mathcal{A}'}$, a sequence of games **Game**₀, **Game**₁, $\dots$, **Game** _{n} are defined. For each **Game** _{i} , we construct a simulator Sim_i that runs $\mathcal{A}$ as a subroutine and provides $\mathcal{E}$'s view, for $i = 0, 1, \dots, n$. $\text{Hybrid}_{\mathcal{E}, \text{Sim}_i}(\ell)$ denotes the probability that $\mathcal{E}$ outputs 1 running in the world provided by Sim_i . Sim_0 runs $\mathcal{A}$ and other honest parties in the real-world experiment, hence $\text{Hybrid}_{\mathcal{E}, \text{Sim}_0} =$

$\text{Real}_{\mathcal{E}, \mathcal{A}}$. Sim_n runs $\mathcal{A}'$ in ideal-world experiment, hence $\text{Hybrid}_{\mathcal{E}, \text{Sim}_n}(\ell) = \text{Ideal}_{\mathcal{E}, \mathcal{A}'}$. Therefore,

$$\begin{aligned} |\text{Real}_{\mathcal{E}, \mathcal{A}}(\ell) - \text{Ideal}_{\mathcal{E}, \mathcal{A}'}| &\leq |\text{Real}_{\mathcal{E}, \mathcal{A}}(\ell) - \text{Hybrid}_{\mathcal{E}, \text{Sim}_1}| \\ &+ |\text{Hybrid}_{\mathcal{E}, \text{Sim}_1} - h\text{Hybrid}_{\mathcal{E}, \text{Sim}_2}| + \dots + \\ &|\text{Hybrid}_{\mathcal{E}, \text{Sim}_{n-1}} - \text{Hybrid}_{\mathcal{E}, \text{Sim}_n}|. \end{aligned}$$

Theorem 3. Our privacy-preserving electronic ticket scheme with attribute-based credentials described in Fig. 2, Fig. 3, Fig. 4, Fig. 5 and Fig. 6 is secure if the q -strong Diffie-Hellman assumption (q -SDH) holds on the bilinear group $(e, p, \mathbb{G}, \mathbb{G}_\tau)$.

Theorem 3 is proven by using the following two lemmas.

Lemma 1. (User Privacy) For all environments $\mathcal{E}$ and all real-world adversaries $\mathcal{A}$ who statically control the ticket seller S and verifier V , there exists an ideal-world adversary $\mathcal{A}'$ such that $|\text{Real}_{\mathcal{E}, \mathcal{A}}(\ell) - \text{Ideal}_{\mathcal{E}, \mathcal{A}'}(\ell)| \leq 2^{\frac{1}{t}}$.

The proof of **Lemma 1** is given in the full version of this paper [55]. Since anonymity, ticket unlinkability and ticket untransferability are part of user privacy, they are therefore proved by **Lemma 1**.

Lemma 2. (Seller Security) For all environments $\mathcal{E}$ and all real-world adversaries $\mathcal{A}$ who statically controls the verifier V and one or more users, there exists an ideal-world adversary $\mathcal{A}'$ such that $|\text{Real}_{\mathcal{E}, \mathcal{A}}(\ell) - \text{Ideal}_{\mathcal{E}, \mathcal{A}'}(\ell)| \leq \frac{q_T}{2^t} + \frac{q_V}{2^t} + \frac{1}{q_I} \text{Adv}_{\mathcal{A}}^{q_I\text{-SDH}}(\ell) + \text{Adv}_{\mathcal{A}}^{(q+1)\text{-SDH}}(\ell) + \text{Adv}_{\mathcal{A}}^{(s+1)\text{-SDH}}(\ell) + \frac{1}{q_T} \text{Adv}_{\mathcal{A}}^{q_T\text{-SDH}}(\ell) + \frac{1}{q_V} \text{Adv}_{\mathcal{A}}^{q_V\text{-SDH}}(\ell)$, where q_T , q_I , q_V are the numbers of ticket issue queries, credential queries and ticket validation queries made by $\mathcal{A}$, respectively.

The proof of **Lemma 2** is given in the full version of this paper [55]. Since unforgeability, double spending detection and de-anonymization are included in the seller security, they are therefore proved by **Lemma 2**. Therefore, **Theorem 4** is proven because both **Lemma 1** and **Lemma 2** hold.

7 FUTURE WORK AND CONCLUSIONS

To protect user privacy in e-ticket schemes, various schemes have been proposed but they do not address attribute-based ticketing. Similarly, privacy-preserving attribute-based credential schemes are proposed where attributes can either be elements of a set or within a range but this paper proposes a scheme to support both the use of sets and ranges within the same scheme. The paper has defined such a scheme together with its security model and security proof. The benefit of this scheme is to provide a policy maker with the flexibility to decide which kind of policies should be used. Set policies are computationally more efficient than range policies but the latter could potentially accommodate future policy changes. Currently, our scheme is not suitable for portable devices, e.g. smart phone, tablet, etc., due to its high computation cost and communication overhead.

Our future work will be looking at the impact on the security model and proof when dynamic policy updates are allowed as well as changes to scheme's implementation to improve its performance, e.g. by pre-computing static values where possible and using the C-based PBC library

[61], outsourcing computation [62], [63], verifiable outsourcing computation [64], [65], [66], etc. Another open problem and an interesting area for our future work is to construct a privacy-preserving e-ticket scheme with attribute-based credentials using the most efficient type of pairing, the Type-III pairing.

ACKNOWLEDGEMENT

This work has been supported by the EPSRC Project DICE: "Data to Improve the Customer Experience", EP/N028295/1.

REFERENCES

- [1] United Airlines. (2017) Customer data privacy policy. [Online]. Available: <https://www.united.com/web/en-US/content/privacy.aspx>
- [2] Rail Delivery Group. (2017) Rail technical strategy capability delivery plan. [Online]. Available: <https://www.rssb.co.uk/rts/Documents/2017-01-27-rail-technical-strategy-capability-delivery-plan-brochure.pdf>
- [3] M. Milutinovic, K. Decroix, V. Naessens, and B. D. Decker, "Privacy-preserving public transport ticketing system," in *DB-Sec'15*. Springer, 2015, pp. 135–150.
- [4] M. Mut-Puigserver, M. M. Payeras-Capellà, J.-L. Ferrer-Gomila, A. Vives-Guasch, and J. Castellà-Roca, "A survey of electronic ticketing applied to transport," *Computers & Security*, vol. 31, no. 8, pp. 925–939, 2012.
- [5] A. Vives-Guasch, M. M. Payeras-Capellà, M. Mut-Puigserver, J. Castellà-Roca-Roca, and J.-L. Ferrer-Gomilas, "Anonymous and transferable electronic ticketing scheme," in *DPM'13 and SE-TOP'13*. Springer, 2013, pp. 100–113.
- [6] (2016) General Data Protection Regulation. [Online]. Available: <https://eugdpr.org/>
- [7] T. S. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu, "Privacy for public transportation," in *PET'06*. ACM, 2006, pp. 1–19.
- [8] G. Arfaoui, J.-F. Lalande, J. Traoré, N. Desmoulins, P. Berthomé, and S. Gharout, "A practical set-membership proof for privacy-preserving NFC mobile ticketing," in *PoPETs'15*. DE GRUYTER, 2015, pp. 25–45.
- [9] R. Song and L. Korba, "Pay-TV system with strong privacy and non-repudiation protection," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 408–413, 2003.
- [10] I. Gudymenko, "A privacy-preserving e-ticketing system for public transportation supporting fine-granular billing and local validation," in *SIN'14*. ACM, 2014, pp. 101–107.
- [11] F. Kerschbaum, H. W. Lim, and I. Gudymenko, "Privacy-preserving billing for e-ticketing systems in public transportation," in *WPES'13*. ACM, 2013, pp. 143–154.
- [12] A. Rupp, G. Hinterwälder, F. Baldimtsi, and C. Paar, "P4r: Privacy-preserving pre-payments with refunds for transportation systems," in *FC'13*. Springer, 2013, pp. 205–212.
- [13] IATA. (2012) Transferability of tickets. [Online]. Available: <https://www.iata.org/policy/Documents/Transferability.pdf>
- [14] B. Patel and J. Crowcroft, "Ticket based service access for the mobile user," in *MobiCom'97*. ACM, 1997, pp. 223–233.
- [15] D. Chaum, "Blind signatures for untraceable payments," in *Crypto'82*. Springer, 1982, pp. 199–203.
- [16] D. Chaum and E. van Heyst, "Group signatures," in *EURO-CRYPT'91*. Springer, 1991, pp. 257–265.
- [17] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Communications of the ACM*, vol. E28, no. 10, pp. 1030–1044, 1985.
- [18] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf, "Pseudonym systems," in *SAC'99*. Springer, 1999, pp. 184–199.
- [19] C.-I. Fan and C.-L. Lei, "Multi-recastable ticket schemes for electronic voting," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E81-A, no. 5, pp. 940–949, 1998.
- [20] D. Quercia and S. Hailes, "Motet: Mobile transactions using electronic ticket," in *SecureComm'05*. IEEE, 2005, pp. 1–10.
- [21] A. Rupp, F. Baldimtsi, G. Hinterwälder, and C. Paar, "Cryptographic theory meets practice: Efficient and privacy-preserving payments for public transport," *ACM Transactions on Information and System Security*, vol. 17, no. 3, pp. 10:01–10:31, 2015.
- [22] S. Brands, "Untraceable off-line cash in wallets with observers (extended abstract)," in *CRYPTO'93*. Springer, 1993, pp. 302–318.
- [23] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.
- [24] M. Abe and T. Okamoto, "Provably secure partially blind signatures," in *CRYPTO'00*. Springer, 2000, pp. 271–286.
- [25] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *CRYPTO'91*. Springer, 1991, pp. 129–140.
- [26] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *EUROCRYPT'01*. Springer, 2001, pp. 93–118.
- [27] T. Nakanishi, N. Haruna, and Y. Sugiyama, "Unlinkable electronic coupon protocol with anonymity control," in *ISW'99*. Springer, 1999, pp. 37–46.
- [28] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *CRYPTO'97*. Springer, 1997, pp. 410–424.
- [29] A. Vives-Guasch, J. Castellà-Roca, M. M. Payeras-Capella, and M. Mut-Puigserver, "An electronic and secure automatic fare collection system with revocable anonymity for users," in *MoMM'10*. ACM, 2010, pp. 387–392.
- [30] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *ACM CCS'04*, pp. 168–177.
- [31] D. Boneh and X. Boyen, "Short signatures without random oracles," in *EUROCRYPT'04*. Springer, 2004, pp. 56–73.
- [32] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *CRYPTO'04*. Springer, 2004, pp. 56–72.
- [33] K. Fujimura and Y. Nakajima, "General-purpose digital ticket framework," in *USENIX Workshop on Electronic Commerce 1998*. USENIX Association, 1998, pp. 177–186.
- [34] G. Davida, Y. Frankel, Y. Tsiounis, and M. Yung, "Anonymity control in e-cash systems," in *FC'97*. Springer, 1997, pp. 1–16.
- [35] E. Gabber, P. B. Gibbons, Y. Matias, and A. Mayer, "How to make personalized web browsing simple, secure, and anonymous," in *FC'97*. Springer, 1997, pp. 17–31.
- [36] O. Jorns, O. Jung, and G. Quirchmayr, "A privacy enhancing service architecture for ticket-based mobile applications," in *ARES'07*. IEEE, 2007, pp. 139–146.
- [37] N. Kuntze and A. U. Schmidt, "Trusted ticket systems and application," in *SEC'07*. IFIP Advances in Information and Communication Technology, 2007, pp. 49–60.
- [38] A. Vives-Guasch, M. M. Payeras-Capellà, M. Mut-Puigserver, and J. L. Ferrer-Gomila, "A secure e-ticketing scheme for mobile devices with near field communication (NFC) that includes exculpability and reusability," *IEICE Transactions on Information and Systems*, vol. E95.D, no. 1, pp. 78–93, 2012.
- [39] Y.-Y. Chen, C.-L. Chen, and J.-K. Jan, "A mobile ticket system based on personal trusted device," *Wireless Personal Communications*, vol. 40, no. 4, pp. 569–578, 2007.
- [40] G.-R. Liu, P. Lin, and Y.-B. Lin, "Modeling mobile ticket dispenser system with impatient clerk," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9931–9941, 2016.
- [41] ETSI TS 103 458. (2018) Cyber; application of attribute based encryption (abe) for pii and personal data protection on iot devices, wlan, cloud and mobile services - high level requirements. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf
- [42] ETSI TS 103 532. (2018) Cyber; attribute based encryption for attribute based access control. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103500_103599/103532/01.01.01_60/ts_103532v010101p.pdf
- [43] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO'01*. Springer, 2001, pp. 213–222.
- [44] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113–3121, 2008.
- [45] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in *CRYPTO'92*. Springer, 1992, pp. 390–420.
- [46] J. Camenisch, A. Kiayias, and M. Yung, "On the portability of generalized schnorr proofs," in *EUROCRYPT'09*. Springer, 2009, pp. 425–442.

- [47] J. Camenisch, R. Chaabouni, and abhi shelat, "Efficient protocols for set membership and range proofs," in *ASIACRYPT'08*. Springer, 2008, pp. 234–252.
- [48] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in *SCN'06*. Springer, 2006, pp. 111–125.
- [49] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in *FOCS'01*. IEEE, 2001, pp. 136–145.
- [50] J. Camenisch, G. Neven, and A. Shelat, "Simulatable adaptive oblivious transfer," in *EUROCRYPT'07*. Springer, 2007, pp. 573–590.
- [51] M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in *ASIACRYPT'07*. Springer, 2007, pp. 265–282.
- [52] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in *ACM CCS'09*. ACM, 2009, pp. 131–140.
- [53] A. D. Caro and V. Iovino, "On the power of rewinding simulators in functional encryption," *Designs, Codes and Cryptography*, vol. 84, no. 3, pp. 373–399, 2017.
- [54] M. H. Au, W. Susilo, and Y. Mu, "Practical anonymous divisible e-cash from bounded accumulators," in *FC'08*. Springer, 2008, pp. 287–301.
- [55] J. Han, L. Chen, S. Schneider, H. Treharne, and S. Wesemeyer. (2018) Privacy-preserving electronic ticket scheme with attribute-based credentials. [Online]. Available: <https://arxiv.org/abs/1706.03016>
- [56] DICE Project. (2017) Benchmark e-ticket systems (bets). [accessed 18-March-2018]. [Online]. Available: <https://github.com/swesemeyer/BenchmarkingETicketingSystems>
- [57] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011*. Kerkyra, Corfu, Greece, June 28 - July 1: IEEE, 2011, pp. 850–855. [Online]. Available: <http://gas.dia.unisa.it/projects/jpbc/>
- [58] Legion of the Bouncy Castle Inc. Bouncy Castle Crypto APIs. [accessed 19-September-2017]. [Online]. Available: <https://www.bouncycastle.org/>
- [59] B. Lynn, "On the implementation of pairing-based cryptosystems," Ph.D. dissertation, Stanford University Stanford, California, 2007.
- [60] D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," *Journal of cryptology*, vol. 23, no. 2, pp. 224–280, 2010.
- [61] B. Lynn. (2006) The pairing-based cryptography PBC library. [Online]. Available: <https://crypto.stanford.edu/pbc/>
- [62] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in *TCC'05*. Springer, 2005, pp. 264–282.
- [63] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2386 – 2396, 2014.
- [64] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *CRYPTO'10*. Springer, 2010, pp. 465–482.
- [65] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 3184–3195, 2016.
- [66] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 546–556, 2015.

Jinguang Han received his Ph.D from University of Wollongong, Australia, in 2013. He currently is a lecture in the Centre for Secure Information Technologies (CSIT), Institute of Electronics, Communications and Information Technology (ECIT), Queen's University Belfast, UK. His main research interests include cryptography, access control, blockchain, privacy-preserving systems. He is a senior member of the IEEE.

Liqun Chen joined the Department of Computer Science at the University of Surrey as Professor in Secure Systems in 2016. Prior to this appointment, she was a Principal Research Scientist at Hewlett Packard Laboratories in Bristol, UK, which she joined in 1997. Before that she worked at Royal Holloway, University of London, the University of Oxford, and Southeast University in P.R. China. Liqun is a visiting professor at Southeast University. Her research interests include cryptography applied to a broad range of areas in secure systems, such as trusted computing, hardware security, 5G, cloud computing, distributed ledger and Internet of Things, and she is also interested in quantum-resistant cryptographic solutions.

Steve Schneider is the director of the Surrey Centre for Cyber Security, which is recognised by GCHQ as one of the UK's Academic Centres of Excellence in Cyber Security Research. I am also Associate Dean for Research and Enterprise in the Faculty of Engineering and Physical Sciences, having taken the role on in January 2015. I joined the Department of Computer Science in September 2004 and was Head of Department 2004-2010. I was previously in the Department of Computer Science at Royal Holloway, University of London over the period 1994-2004. I gained my doctorate from the University of Oxford, and held post-doctoral positions there prior to joining Royal Holloway.

Helen Treharne is a Reader in Secure Systems in the Department of Computer Science at the University of Surrey. Her main research interests are in data privacy and formal verification. She is leading an interdisciplinary research team on the impact of data privacy on customer experience in the transport domain. Her interests also include the use of trusted computing to improve privacy within secure systems. She is also an expert in formal verification in intelligent transport systems and railway control systems. She was awarded a Royal Academy of Engineering/Leverhulme Trust Senior Research Fellowships during 2013-14 in this area.

Stephan Wesemeyer received his PhD from Exeter in 1997. He worked as research fellow for the Centre for Communication Systems Research (now the Institute for Communication Systems) at the University of Surrey for 18 months before joining an IT consultancy in 1999. After almost 10 years working as an IT consultant, he rejoined the university as a research associate in the Department of Computer Science in 2009. He currently works with Dr Helen Treharne and Prof Steve Schneider on the EPSRC project "Improving customer experience while ensuring data privacy for intelligent mobility".