Jinguang Han*, Liqun Chen, Steve Schneider, Helen Treharne, and Steve Wesemeyer

PPETS-FGP: Privacy-Preserving Electronic Ticket Scheme with Fine-Grained Pricing

Abstract: Electronic tickets (e-tickets) are electronic versions of paper tickets, which enable users to access intended services and improve services' efficiency. Generally, to buy discounted tickets, users must convince ticket sellers that their attributes (i.e. age, profession, location) satisfy the ticket price policies. Hence, privacy issues have been the primary concerns of e-tickets users. In this paper, a privacy-preserving electronic ticket scheme with fine-grained pricing (PPETS-FGP) is proposed to protect users' privacy and implement fine-grained pricing. The proposed PPETS-FGP scheme captures the following features: (1) Users can buy different price tickets from ticket sellers without releasing their exact attributes; (2) Two tickets of the same user cannot be linked; (3) Tickets cannot be transferred and double spent; (4) The security of the proposed PPETS-FGP is formally proven and reduced to well-known (q-strong Diffie-Hellman) complexity assumption. To the best of our knowledge, it is the *first* provable e-ticket system where both privacy-preserving and fine-grained pricing are addressed.

Keywords:

DOI Editor to enter DOI
Received ..; revised ..; accepted ...

1 Introduction

Due to their flexibility and portability, electronic tickets (e-tickets) systems have already been focused on extensively by industries [4, 5, 37] and academic research communities [47, 48, 59]. E-tickets are substituting paper tickets as they can reduce paper costs and improve customers' experiences. Nevertheless, various data breach events show that privacy protection is essential in digital world. For example, On September 9, 2017, Equifax which is one of the largest credit bureaus in the United States said that an application vulnerability on one of their websites led to a data breach [10]. 143 million users' personal information were exposed, including social security numbers, birth dates, addresses. Especially, 209,000 users' credit card data was released. In 2014, eBay reported that 145 million users' information was stolen, including names, emails, passwords, addresses, phone numbers and birth dates [9].

Privacy issues have been the primary concern of users. Therefore, it is imperative that any smart ticketing system is secure and preserves customer privacy. To protect users' privacy in smart ticketing systems, anonymous authentication and fine-grained pricing are required. Anonymous authentication enables users to authenticate without revealing their identities. Users with different attributes benefit from the fine-grained pricing.

In e-ticket systems, different users may buy different tickets depending on policies and their attributes. To purchase special tickets, users must provide information about the attributes related to the discount, e.g. age, professional, location, *etc.* Therefore, users' privacy is being challenged and potentially exposed. Hence, privacy-preserving e-ticket schemes (PPETs) were proposed [6, 38, 39, 42, 47, 57]. However, none of these schemes were formally proven. Hence, there still is a big gap between PPETSs and real e-ticket systems. This paper aims to bridge this gap by proposing a privacy-preserving e-ticket scheme with fine-grained pricing (PPETS-FGP) to protect users' privacy and implement fine-grained pricing.

The proposed PPETS-FGP is a general e-ticket system and can be used into various application scenarios where privacy issues are concerned, such as Internet forums [1, 2], internet information services (IIS) [46], rail [54], gig [35], *etc.* Some Internet forums support anonymous posting, for example 4chan [1] and 5chan [2]. In these forums, there are some active boards, such as social news, cooking, computers, *etc.*, and different types of membership, such as premium, common, *etc.*

***Corresponding Author: Jinguang Han:** Surrey Centre for Cyber Security, Department of Computer Science, University of Surrey, Guildford, Surrey, GU2 7XY, United Kingdom, E-mail: j.han@surrey.ac.uk

Liqun Chen, Steve Schneider, Helen Treharne, Steve Wesemeyer: Surrey Centre for Cyber Security, Department of Computer Science, University of Surrey, Guildford, Surrey, GU2 7XY, United Kingdom, E-mail: {liqun.che, s.schneider, h.treharne, s.wesemeyer}@surrey.ac.uk

BY-NC-ND

When registering to the forum, a user needs to convince the server that he/she satisfies the its policy (age>18) and get a e-ticket (token) from the server. When, posting a comment, the user needs to convince the board manager that he/she is authorized to do it. The web sever IIS 7 [46] developed by Microsoft supports anonymous authentication. <anonymousAuthentication> enable the web server to process the authentication requests from anonymous users. Meanwhile, the server uses <authorization> to determine what sources users can access. There are some filters who control access to the services, including authorization filter, resource filter, action filter, exception filter and result filter. When accessing a service, the filter checks whether the user is authorizeed to access it. In rail, to buy a discounted ticket, users must show his/her special attributes to the ticket seller, for example disability, children, *etc.* Then, the ticket seller issues a discounted ticket to the user according to his/her attributes. When boarding the train, the user must convince the guard that he/she has obtained a ticket. In gig [35], there are four types of members: adult (over 21), student (18-21), junior (under 18) and associate. Prior to going to the club, a user should buy a ticket according to his/her member type. When entering the club, the user need show his/her ticket to the access door. For simplicity, this paper is developed in the rail case.

1.1 Related Work

So far, PPETSs with distinct features have been proposed. In these schemes, blind signature [26], group signature [28], anonymous credential [27] and pseudonym [28, 45] were used to protect users' privacy. Mut-Puigserver *et al.* [48] surveyed e-ticket systems, and summarised functionality and security requirements in e-ticket systems. Functionality requirements include expire date, reduced size, portability, flexibility, *etc.* Security requirements include integrity, authentication, fairness, non-overspending, anonymity, transferability, unlinkability, *etc.* In this paper, we mainly focus on flexibility, non-overspending, anonymity, transferability and unlinkability. E-ticket schemes are classified into different types: transferable tickets [39, 59], untransferable tickets [40, 47], multi-use tickets [47, 48] and single-use tickets [39, 47, 50, 59].

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 message. Based on the blind signature scheme proposed by Chaum [26], Fan and Lei [31] proposed an e-ticket system for voting. In [31], each voter can vote for a sequence of voting using only one ticket. Song and Korba [57] proposed an e-ticket scheme to protect users' privacy and provide non-repudiation in pay-TV systems. Quercia and Hailes [53] proposed an e-ticket scheme for mobile transactions. In [53], the blind signature [26] was adopted to generate tickets and two types of tickets were considered, namely limited-use tickets and unlimited-use tickets. Rupp *et al.* [55, 56] proposed privacy-preserving pre-payments with refunds (P4R) schemes which were derived from the blind signature scheme [16] and the short signature [14]. In this scheme, trip authorisation tokens were generated by using the blind signature scheme [16], while the short signature scheme [14] was used to implement the privacy-preserving aggregation of refunds. Milutinovice *et al.* [47] proposed an e-ticket scheme where the partial blind signature scheme [3], commitment scheme [51] and anonymous credential [20] were explored together to protect users' privacy.

E-Ticket Schemes from Group Signatures. A group signature enables a user to sign on 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.* [49] proposed an electronic coupon (e-coupon) scheme where the group signature scheme [23] was used to provide anonymity and unlinkability. Vives-Guasch [58] proposed an automatic fare collection (AFC) system where the group signature scheme [15] was used to provide unlinkability and revocable anonymity. Gudymenko [38] addressed users' privacy and fine-grained billing issues in e-ticket schemes, and used group signatures to make tickets untraceable. Nevertheless, in [38], there were no formal security models and security proofs.

E-Ticket Schemes from Anonymous Credentials. In an anonymous credential scheme, a user can prove to a verifier that he/she has obtained a credential without releasing any other information to the latter. Heydt-Benjamin *et al.* [39] introduced anonymous credentials, e-cash and proxy re-encryption schemes into e-ticket systems to enhance security and privacy in public transport systems. In [39], passive RFID transponders and higher powered computing devices are required. Arfaoui *et al.* [6] first modified the signature scheme proposed in [12] 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 combing the modified signature with the anonymous credential scheme [21]. In [6], a user can anonymously use an m-ticket at most

k times, otherwise he/she is revoked by the revocation authority.

E-Ticket Schemes from Pseudonyms. A pseudonym allows users to interact with multiple organisations anonymously and unlinkably by proving a statement about his/her relationship with others. Fujimura and Nakajima[33] proposed a general-purpose e-ticket framework where anonymity was achieved by using pseudonym schemes [30, 34]. Jorns *et al.* [41] first proposed a pseudonym scheme which can be implemented on constrained devices, and then used it to protect users' privacy in e-ticket systems. Kuntze and Schmidt [43] 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.* [60] proposed a lightweight e-ticket scheme and addressed exculpability and reusability. In [60], a pseudonym was adopted to provide unlinkability of users' transactions. Kerschbaum *et al.* [42] considered the privacy-preserving billing issue in e-ticket schemes and applied pseudonyms to provide transactions' unlinkability.

E-Ticket from Special Devices. There are other e-ticket schemes designed using special devices, including personal trusted device (PTD) [29], trusted platform module (TPM) [43], mobile handsets (i.e. smart phones) [44], *etc.*

1.2 Contributions

E-ticket schemes attract lots of research attentions due to their flexibility and portability. Nevertheless, privacy issues have been the primary concern of users. PPETs have been proposed, but these schemes were not formally treated in terms of security models and proofs, except [6]. Arfaoui *et al.* [6] formally defined the security models for e-ticket schemes, including unforgeability, unlinkability and non-frameability, but the security proofs in [6] were sketchy. Rupp [56] formalised the security models of privacy-preserving pre-payments with refunds schemes including transportation authority (TA) security and users' privacy, while the security of the proposed scheme was not fomally reduced to well known complexity assumptions, instead of relying the security of the adopted blind signature [16] and the short signature [14]. [38] and [42] addressed privacy-preserving pricing issue, but these schemes were not proven. Hence, how to construct a provable PPETS-FGP is still a challenging and interesting problem.

In this paper, we propose a new e-ticket scheme to implement privacy protection and fine-grained pricing. The proposed scheme provides the following features: (1) For a service, different users can buy different price tickets without releasing their exact attributes; (2) Two tickets of the same user cannot been linked; (3) Tickets cannot been transferred and double spent; (4) The security of the proposed scheme is formally proven and reduced to well-know (q-strong Diffie-Hellman) complexity assumptions. To the best of our knowledge, it is the *first* provable e-ticket scheme where both privacy-preserving and fine-grained pricing are addressed.

1.3 Organisation

The remainder of this paper is organised as follows. In Section 2, the preliminaries used throughout this paper are introduced. The concrete construction and security analysis of our PPETS-FGP are presented in Section 3 and Secion 4, respectively. Finally, Section 6 concludes this paper.

2 Preliminaries

In this section, the preliminaries used throughout this paper are described. All notation used in this paper are explained in Table 1.

2.1 Formal Definition

A PPETS-FGP 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;
- U registers to CA, obtains anonymous credentials from CA, purchases tickets from S, and proves the possession of tickets to V;
- S registers to CA and sells tickets to U according to the ticket price policies;
- V validates the tickets provided by U and detects whether a ticket is double spent.

The workflow of our PPETS-FGP is presented in Fig. 1.

A PPETS-FGP is formally defined as follows:

Table 1. Notation

1^ℓ	A security number
CA	A central authority
S	A ticket seller
U	A user
V	A ticket verifier
ID_U	The identity of U
ID_S	The identity of S
A_U	The attributes of U
PoK	Proof of knowledge
σ_S	A credential of S
σ_U	A credential of U
$Ticket_U$	A ticket of U
VP	A valid period
H	A cryptographic hash function
$\mathbb{P}$	A universal set of price policies
$\mathbb{P}_i$	The i-th policy
$\mathbb{P}_U$	The policies satisfied by U
I_{i_j}	The j-th item in policy $\mathbb{P}_i$
$A_U \models I_{i_j}$	A_U satisfies the item I_{i_j}
$[a, b]$	A range between integers a and b
$x \xleftarrow{R} X$	x is randomly selected from the set X
$A(x) \rightarrow y$	y is obtained by running the algorithm $A(\cdot)$ with input x
$\mathcal{KG}(1^\ell)$	A secret-public key pair generation algorithm
$\mathcal{BG}(1^\ell)$	A bilinear group generator
$\epsilon(\ell)$	A negligible function in ℓ

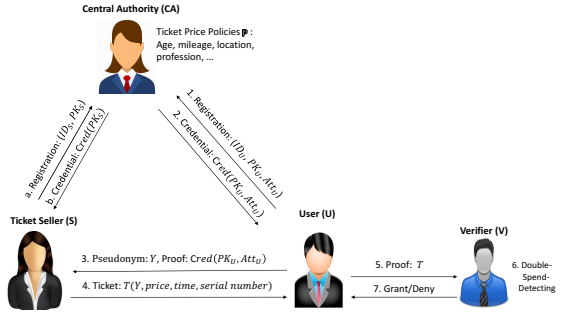

Fig. 1. The Model of Our PPETS-FGP

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

– Registration(S$(ID_S, SK_S, PK_S, params) \leftrightarrow$ CA$(MSK, PK_S, params)) \rightarrow (\sigma_S, (ID_S, PK_S))$/ (U$(ID_U, A_U, SK_U, PK_U, params) \leftrightarrow$ CA$(MSK, PK_U, params)) \rightarrow (\sigma_U, (ID_U, PK_U))$. This algorithm is an interactive algorithm executed between S and CA or U and CA. This algorithm consists of the following two sub-algorithms: S's registration SRegistration and U's registration URegistration.

SRegistration(S$(ID_S, SK_S, PK_S, params) \leftrightarrow$ CA$(MSK, PK_S, params)) \rightarrow (\sigma_S, (ID_S, PK_S))$. S runs $\mathcal{KG}(1^\ell) \rightarrow (SK_S, PK_S)$ to generate a secret-public key pair (SK_S, PK_S), inputs his/her identity ID_S, the secret-public key pair (SK_S, PK_S) and the public parameters $params$, and outputs a credential σ_S which is generated by CA. CA inputs its master secret key, the public key PK_S and the public parameters $params$, and outputs (ID_S, PK_S).

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 $\mathcal{KG}(1^\ell) \rightarrow (SK_U, PK_U)$ to generate a secret-public key pair (SK_U, PK_U), inputs his/her 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 which is generated by CA. CA inputs the master secret key MSK, U's attributes A_U, 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$(SK_S, PK_S, Ps_U, \mathbb{P}, Price, VP, Serv, params)) \rightarrow (T_U, (Ps_U, Service))$. This is an interactive algorithm executed between U and S. U inputs his secret-public key pair (SK_U, PK_U), attributes A_U, credential σ_U, a pseudonym Ps_U, the ticket price policies $\mathbb{P}$, the valid period VP, a service $Service$ and the public parameters $params$, and outputs a ticket T_U. S inputs his secret-public key pair (SK_S, PK_S), U's pseudonym Ps_U, the ticket price policies $\mathbb{P}$, the ticket price $Price$, the valid period time VP, the service $Service$ and the public parameters $params$, and outputs $(Ps_U, Service)$.

– Ticket-Validating(U$(SK_U, Ps_U, T_U, VP, Serv, params) \leftrightarrow$ V$(VP, Serv, params)) \rightarrow (0/1, (Serv, Trans))$. This is an interactive algorithm executed between U and V. U inputs his secret-public key pair (SK_U, PK_U), ticket T_U, the valid period VP, the service $Serv$ and the public parameters $params$, and output 1 if the ticket T_U is valid; otherwise it outputs 0 to indicate fail. V inputs the valid period VP, the service $Serv$ and the public parameters $params$, and outputs $(Serv, Trans)$ where $Trans$ is the transcript of the ticket validation.

– Double-Spend-Detecting$(Trans, params) \rightarrow (PK_U, \perp)$. V inputs the transcript $Trans$ and the public parameters $params$ and outputs U's public key PK_U if U double uses a ticket; otherwise it outputs $\perp$ to indicate that there is no double use ticket.

Definition 1. *A privacy-preserving electronic ticket scheme with fine-grained pricing (PPETS-FGP) is correct if*

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

and

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

2.2 Security Models

The security of PPETS-FGP is defined by using the simulation-based definition as introduced in [18, 22, 25, 36]. This security model is similar to the universal composability model [24, 52], but not exactly the same [18]. The simulation-based model is defined by the indistinguishability between the following real world experiment and ideal world experiment.

The Real-World Experiment. We first present how the PPETS-FGP works where the central authority CA, the ticket seller S and the user U and the ticket verifier V are honest. The entities controlled by the real-world adversary $\mathcal{A}$ can deviate arbitrarily from their behaviours described below. CA runs $\mathsf{Setup}(1^\ell) \rightarrow (MSK, params, \mathbb{P})$ to generate the master secret key msk, system public parameters $params$ and the universal set of ticket price polices $\mathbb{P}$, 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 $\mathcal{KG}(1^\ell) \rightarrow (SK_S, PK_S)$, 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 SRegistation 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 $\mathcal{KG}(1^\ell) \rightarrow (SK_U, PK_U)$, 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 $\tilde{b} \in \{0,1\}$ to $\mathcal{E}$ to show whether the URegistation 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 $Service$. If the ticket issue is successful, U sends a bit $\check{b} \in \{0,1\}$ to $\mathcal{E}$ to show the Ticket-Issuing algorithm succeed $(\check{b} = 1)$ or failed $(\check{b} = 0)$.

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 first 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 is not been double spent.

The Ideal-World Experiment. In the ideal world experiment, there are the same entitles as those 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 SCL, a user credential list UCL, a ticket list UTL for each user and a ticket validating list TVL.

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 SCL 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 $(\mathsf{U}', A_{U'})$ into UCL and sends $\tilde{\nu}$ to U'; otherwise, TP sends $\tilde{\nu} = 0$ to S' to indicate failure.

When receiving a ticket issuing message $(ticket\_issuing, A_{U'}, VP, Service)$ from U', TP sends $(ticket\_issuing, \mathsf{U}', A_{U'}, VP, Service)$ to S' and obtains a bit $\hat{\nu} \in \{0, 1\}$ from S'. If $\hat{\nu} = 1$, TP adds $(\mathsf{U}', A_{U'}, VP, Service)$ into UTL, 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 $T_{U'} \in UTL$. If so, TP sends a bit $\bar{\nu} = 1$ to U' and puts $T_{U'}$ into UVL. If $\bar{\nu} = 0$, TP' sends $\bar{\nu} = 0$ to indicate failure.

When receiving a double spend detecting message $(double\_spend\ \_detecting, T_{U'})$ from U', TP checks whether $T_U \in UVL$. If it is, TP returns $\check{\nu} = 1$ to U' to indicate it is double spend; otherwise, $\check{\nu} = 0$ is returned to show it is not double spent.

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

Definition 2. *Let* $\mathbf{Real}_{\mathcal{E},\mathcal{A}}(\ell)$ *be the probability that the enviornment* $\mathcal{E}$ *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 the PPETS-FGP if*

$$|\mathbf{Real}_{\mathcal{E},\mathcal{A}}(\ell) - \mathbf{Ideal}_{\mathcal{E},\mathcal{A}'}(\ell)| \leq \epsilon(\ell).$$

Security Properties. It is obvious that the ideal-world experiment can provide the following properties.

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 he/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.

Seller's Security. U' cannot generate a ticket on behalf of the seller S'. Even if U' colludes potentially other users and V', they cannot forge a valid ticket.

Therefore, both user's privacy and seller's security can be achieved in the real-world experiment due to the indistinguishability between the real-world experiment and ideal-world experiment.

2.3 Bilinear Group

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_\tau$ be cyclic group with prime order p. A map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_\tau$ is a bilinear group if the following properties are satisfied [13]:

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 $e(g, h)$.

In the case that $\mathbb{G}_1 = \mathbb{G}_2$, e is called symmetric bilinear map. Let $\mathcal{BG}(1^\ell) \to (e, p, \mathbb{G}, \mathbb{G}_\tau)$ 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 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\tau$.

2.4 Complexity Assumptions

Definition 3. (q-Strong Diffie-Hellman (SDH) Assumption [12]) *Let* $\mathcal{BG}(1^\ell) \to (e, p, \mathbb{G}, \mathbb{G}_\tau)$*,* g *be a generator*

of $\mathbb{G}$ *and* $x \overset{R}{\leftarrow} \mathbb{Z}_p$. *We say that q-strong Diffie-Hellman assumption holds on* $\mathbb{G}$ *if for all probabilistic polynomial time (PPT) adversary* $\mathcal{A}$ *given* $(g, g^x, g^{x^2}, \cdots, g^{x^q})$ *can output a pair* $(c, g^{\frac{1}{x+c}})$ *with negligible probability, namely* $Adv_{\mathcal{A}}^{q-SDH} = \Pr\left[\mathcal{A}(g, g^x, g^{x^2}, \cdots, g^{x^q}) \rightarrow (x, g^{\frac{1}{x+c}})\right] \leq \epsilon(\ell)$, *where* $c \in \mathbb{Z}_p$.

2.5 Zero-Knowledge Proof

In this paper, we use zero-knowledge proof of knowledge protocols to prove knowledge of statements about discrete logarithms [11], including discrete logarithm, equality, product, disjunction and conjunction. We follow the notation proposed in [23] and formalised in [19]. 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 $\tilde{A} = \tilde{g}^{\alpha} \tilde{h}^{\gamma}$ holds 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 which knowledge is being proven, while the other values are public to the verifier.

2.6 Boneh-Boyen (BB) Signature

In 2004, Boneh and Boyen [12] proposed a short signature scheme. This scheme was used to construct efficient set-membership proof and range proof [17]. In this paper, we use this signature scheme to generate tags for ticket price policies. This 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 $x \overset{R}{\leftarrow} \mathbb{Z}_p$ 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 $e(\sigma, Y g_2^m) \overset{?}{=} e(g_1, g_2)$.

Theorem 1. *The Boneh-Boyen signature is* $(T, q_S, \epsilon(\ell))$*-secure against existentially forgery under the weak chosen message attacks if the* $(T', q, \epsilon'(\ell))$*-strong Diffie-Hellman (SDH) assumption holds on* $(e, p, \mathbb{G}, \mathbb{G}_{\tau})$, *where* q_S *is the number of signing queries made by the adversary* $\mathcal{A}$, $q > q_S, \epsilon'(\ell) = \epsilon(\ell)$ *and* $T' = \mathcal{O}(T)$ *[12].*

2.7 Signature with Efficient Protocol

Au *et al.* [7] proposed a signature with efficient protocol scheme and named it as BBS+ signature. This signature scheme is used to issue credentials to users and ticket sellers, and generate tickets for users in our PPETS-FGP. This scheme works as follows.

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

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

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

Theorem 2. *This signature with efficient protocol is* $(T, q_S, \epsilon(\ell))$*-existentially unforgeable under the adaptively chosen message attacks if the* $(T', q, \epsilon'(\ell))$*-strong Diffie-Hellman (SDH) assumption holds on* $(e, p, \mathbb{G}, \mathbb{G}_{\tau})$, *where* q_S *is the number of signing queries made by the adversary* $\mathcal{A}$, $q > q_S$, $\epsilon(\ell)' > q\epsilon(\ell)$ *and* $T' = \mathcal{O}(T)$ *[7].*

Proof of The Signature. To prove (w, s, σ) is a signature on $(m_1, m_2, \cdots, m_n)$, the prover selects $r_1, r_2 \overset{R}{\leftarrow} \mathbb{Z}_p$, 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 $t_2 = w r_2$. The proof protocol Π is as follows:

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

Theorem 3. Π *is an honest-verifier zero-knowledge proof of knowledge protocol with special soundness [7].*

3 PPETS-FGP: Privacy-Preserving Electronic Ticket System with Fine-Grained Pricing

In this section, we describe the formal construction of our PPETS-FGP scheme. Our scheme is derived from the signature with efficient protocol scheme [7], set-

membership proof scheme and range proof scheme [17], commitment scheme [51] and e-cash [8]. In [17], a value can be proven in a set or a range, while the value is not certified by a trusted party and multiple sets and ranges were not considered simutanously. In [8], a double spend user can be detected, but users' attributes were not addressed.

Challenges. When using the range proof and set-membership proof [17] to construct our PPETS-FGP, there are some technical challenges: (1) The values (i.e. ages, mileages) which users prove to ticket sellers should be certified by a trusted authority; otherwise, users can buy discounted tickets which they do not have the corresponding attributes; (2) To protect users' privacy and implement untransferability, tickets are generated by using anonymous credential schemes and include users' personal information. Hence, detecting double spend users is difficult since two proofs of one ticket cannot be linked and the verifier does not have any information of users; (3) Range proof and set-membership proof can be used simultaneously to prove that values included in a credential are in some sets and ranges, especially there are multiple range policies and set policies.

Techniques. To overcome the hurdles above, the following techniques are adopted: (1) The signature scheme [7] is used to certified users' attribute values (i.e. age, mileage, profession, location, *etc.*). As a result, all the values which are included in the credentials and need to be proven can be expressed in discrete logarithm formules, then can be proven using the zero-knowledge proof of knowledge protocol [11]; (2) To detect double spend users, each ticket is bound with a serial number and the public trace technique in [8] is used. If there are two transcripts including the same serial number, the double spend user can be detected and revoked by releasing his/her identity (public key); (3) Various tags are constructed to support both range proofs and set-membership proofs.

3.1 High-Level Overview

In e-ticket systems, ticket prices mainly depend on two kinds of policies: range policies and set policies. The range policies include attributes, for example age, mileage, *etc.*; while the set policies consist of various other attributes, such as profession, disability, location, *etc.* In this paper, we focus on both range policies and set policies. Each policy determins a price, such as 50% off policy, 30% off policy, *etc.* For example, in UK, users can by 30% off ticket using 16-25 railcards [54] if: (1) they are between 16 to 25; (2) they are over 25, but full-time students. Our PPETS-FGP works as follows.

Setup. CA publishes the ticket price polices $\mathbb{P} = \{\mathbb{R}_1, \cdots, \mathbb{R}_{N_1}, \mathbb{P}_1 \cdots, \mathbb{P}_{N_2}\}$. Let $\{\mathbb{R}_1, \cdots, \mathbb{R}_{N_1}\}$ be range policies and $\{\mathbb{P}_1, \cdots, \mathbb{P}_{N_2}\}$ be set policies. Suppose that the longest interval length in $\{\mathbb{R}_1, \cdots, \mathbb{R}_{N_1}\}$ is $[0, q^k)$, $\mathbb{R}_l = [c_l, d_l]$ and $\mathbb{P}_i = \{I_{i_1}, I_{i_2}, \cdots, I_{\varsigma_i}\}$ consists of ς (> 1) items[1], for $l = 1, \cdots, N_1$ and $i = 1, 2, \cdots, N_2$.

CA selects secret keys $(x, y, \mu_1, \mu_2, \cdots, \mu_{N_2})$ where x is used to generate credentials for users, y is used to generates tags for the range policies and μ_i is used to generate tags for set policies where $i = 1, 2, \cdots, N_2$. CA publishes the range proof tags $(h_0, h_1, \cdots, h_{q-1})$, N set policy tags $(\tilde{\eta}_1, \tilde{\eta}_2, \cdots, \tilde{\eta}_{N_2})$ and $\varsigma \times N$ item tags $\left((\eta_{i_j})_{j=1}^{\varsigma}\right)_{i=1}^{N}$.

Registration. S generates a secret-public key pair (x_s, Y_S), authenticates himself/herself to CA. If the authentication is successful, CA issues a credential $Cred_S = (c_s, r_s, \sigma_S)$ to S, where $\sigma_S = (g_0 Y_S \mathfrak{g}^{r_s})^{\frac{1}{x+c_s}}$. (c_s, r_s, σ_S) is a BBS+ signature on x_s and S's public key Y_S is inlcuded. Later, S can convince U that he/she is authorised by proving the possession of $Cred_S$ and Y_S is included in $Cred_S$.

U generates a secret-public key pair (x_u, Y_U), submits his/her attributes A_U which enable him/her to get special tickets, and authenticates himself/herself to CA. A_U consists of U's age, mileage, profession, location, *etc.* If the authentication is successful, CA issues a credential $Cred_U = (c_u, r_u, \sigma_U)$ to A_U, where $\sigma_U = \left(g_0 Y_U R \mathfrak{g}^{r'} \prod_{l=1}^{N_1} \hat{g}_l^{a_l} \prod_{i=1}^{N_2} \eta_i^{H(I_{i_j})}\right)^{\frac{1}{x+c_u}}$, a_l is the vale of U's attribute in the range policy $\mathbb{R}_l$ for $l = 1, \cdots .N_1$. (c_u, r_u, σ_U) is a BBS+ signature on $\left(x_u, (a_l)_{l=1}^{N_1}, (H(I_{i_j}))_{i=1}^{N_2}\right)$. $Cred_U$ includes U's public key Y_U and attributes A_U, and enables U to prove that his/her attributes have been certified by CA.

Ticket Issuing. To resist illegal entities to collect users' private information, S proves to U that he/she is authorised by CA using $Cred_S$. If the proof is successful, U generates a pseudonym $Y = \xi^{x_u} g_1^d$ where x_u is his/her secret key and d is a random number, and proves to S that he/she holds attributes which enable he/she to buy a discounted ticket and are certified by CA. If the proof is successful, S selects $d', s_u, \omega_u \xleftarrow{R} \mathbb{Z}_p$, and generates a ticket $Ticket_U = (d_u, s_u, \omega_u, \psi_u, T_u)$ for U, where where

1 If there exists a policy $\mathbb{P}_j$ consisting of $\tilde{\varsigma}$ ($\tilde{\varsigma} < \varsigma$) items, we can add $\varsigma - \tilde{\varsigma}$ dummy items to $\mathbb{P}_j$ for $j = 1, 2, \cdots, N$.

$d_u = d + d'$, $T'_U = (g_0 Y g_1^{d'} g_2^{s_u} g_3^{\psi_u})^{\frac{1}{x_s+\omega_u}}$, s_u is a serial number, $\psi_u = H(\mathbb{P}_U||Price||Serv||VP)$, $\mathbb{P}_U$ is a set consists of the names of range policies and set policies satisfied by U and required by V, $Price$ is the ticket price, $Serv$ are the services which U wants to access and VP is the valid period of the ticket. Actually, (s_u, ω_u, T_u) is a BBS+ signature on (x_u, d_u, ψ_u).

Ticket Validation. U initializes an empty table $Table_U$ to store the identity information of V and V initializes $Table_V$ to store the authentication transcript from U. To use a ticket, U first checks that whether $H(ID_V)$ exists in $Table_U$, where ID_V is the identity of the verifier V; If not, U proves to V the possession of the ticket $Ticket_U$ by using a proof transcript $Trans$ and updates $Table_U = Table_U \cup \{(H(ID_V), r)\}$ where r is the challenge from V; otherwise, U aborts. If the proof is successful, V grants the service to U and updates $Table_V = Table_V \cup \{Trans\}$; otherwise, V denies the request. The ticket $Ticket_U$ is untransferable and single-use.

Double Spend Detecting. To detect whether a ticket is being double spent, V checks whether there exist two transcripts $trans$ which includes the same serial number. If it is, the ticket is being double spent and V can reveal the public key of U using the two transcripts; otherwise, it is a fresh ticket.

3.2 Construction

The construction of our PPETS-FGP is described in Fig. 2, Fig. 3, Fig. 4, Fig. 5 and Fig. 6.

In addition, this scheme also addresses the security and privacy issues which are covered in the next two properties.

Transaction Unlinkability. When buying a ticket, U proves to S that he/she holds the attributes required by the discounted ticket without releasing them and provides a pseudonym to S. Later, U proves to V that he/she has obtained a ticket which includes his/her pseudonym. Since all proofs are zero-knowledge, two tickets of the same user cannot be linked by CA, S and V, even if they can collude.

Ticket Untransferability. Both tickets and pseudonyms includes users' secret keys x_u. When using a ticket $Ticket_U$, U needs to prove the knowledge of x_u and the possession of $Ticket_U$. Hence, tickets are untransferable.

Dynamic Policy Update. If the seller S needs to specify/update some policies, he/she contacts the central authority CA to update the public parameters $params$. As a result, when buying a ticket, the user U proves to S that his/her attributes satisfy the updated policies by using updated $params$. In the case that the verifier V needs to specify/update some policies, he/she contacts the CA to update the public parameters $params$. Then, S will generate tickets according to the updated policies. Whether U needs to update his/her credential $Credent_U$ depends on whether his/her attributes satisfy the updated policy. For example, suppose that Alice is 16 years old. If the policy is changed from [12,18] to be [15,20], Alice can still use her credential; while if the policy is changed from [12, 18] to be [18,25], Alice needs to update her credential.

Correctness. The proposed PPETS-FGP in Fig. 2, Fig. 3, Fig. 4, Fig. 5 and Fig. 6 is correct as the following equations hold.

$$\begin{aligned}
&e(Q, \tilde{g}) = e(\sigma_S \vartheta^z, g^x) \\
&= e((g_0 g_1^{H(VP)} Y_S \mathfrak{g}^{r_s})^{\frac{1}{x+c_S}}, g^x) \cdot e(\vartheta, \tilde{g})^z \\
&= e((g_0 g_1^{H(VP)} Y_S \mathfrak{g}^{r_s})^{\frac{x+c_S-c_S}{x+c_S}}, g) \cdot e(\vartheta, \tilde{g})^z \\
&= e((g_0 g_1^{H(VP)} Y_S \mathfrak{g}^{r_s}), g) \cdot e(\sigma_S \vartheta^z, g)^{-c_S} \cdot \\
&\quad e(\vartheta, g)^{-c_S z} \cdot e(\vartheta, \tilde{g})^z \\
&= e(g_0, g) \cdot e(g_1, g)^{H(VP)} \cdot e(\rho, g)^{x_S} \cdot e(\mathfrak{g}, g)^{r_s} \cdot \\
&\quad e(Q, g)^{-c_S} \cdot e(\vartheta, g)^{-c_S z} \cdot e(\vartheta, \tilde{g})^z.
\end{aligned} \tag{1}$$

Hence, we have

$$\begin{aligned}
&\frac{e(Q, \tilde{g})}{e(g_0, g) \cdot e(g_1, g)^{H(VP)}} = e(\rho, g)^{x_S} \cdot e(\mathfrak{g}, g)^{r_s} \cdot \\
&e(Q, g)^{-c_S} \cdot e(\vartheta, g)^{-c_S z} \cdot e(\vartheta, \tilde{g})^z.
\end{aligned} \tag{2}$$

Let $\Delta = g_0 \cdot e(g_1, g)^{H(VP)} Y_U \mathfrak{g}^{r_u} \prod_{l=1}^{N_1} \hat{g}_l^{a_l} \prod_{i=1}^{N_2} \eta_i^{H(I_{i_j})}$, we have

$$\begin{aligned}
&e(C, \tilde{g}) = e\left(\Delta^{\frac{1}{x+c_u}} \vartheta^\alpha, g^x\right) \\
&= e\left(\Delta^{\frac{x+c_u-c_u}{x+c_u}}, g\right) \cdot e(\vartheta, \tilde{g})^\alpha \\
&= e\left(\Delta, g\right) \cdot e\left(\Delta^{\frac{-c_u}{x+c_u}}, g\right) \cdot e(\vartheta, \tilde{g})^\alpha \\
&= e\left(\Delta, g\right) \cdot e\left(\Delta^{\frac{-c_u}{x+c_u}} \vartheta^{-c_u \alpha}, g\right) \cdot e(\vartheta, g)^{c_u \alpha} \cdot e(\vartheta, \tilde{g})^\alpha \\
&= e\left(\Delta, g\right) \cdot e\left(C, g\right)^{-c_u} \cdot e(\vartheta, g)^{c_u \alpha} \cdot e(\vartheta, \tilde{g})^\alpha \\
&= e(g_0, g) \cdot e(g_1, g)^{H(VP)} \cdot e(\xi, g)^{x_u} \cdot e(g, \mathfrak{g})^{r_u} \cdot \\
&\prod_{l=1}^{N_1} e(\hat{g}_l, g)^{a_l} \cdot \prod_{i=1}^{N_2} e(\eta_i, g)^{H(I_{i_j})} \cdot e(C, g)^{-c_u}.
\end{aligned}$$

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

CA runs $\mathcal{BG}(1^\ell) \rightarrow (e, p, \mathbb{G}, \mathbb{G}_\tau)$. Suppose that the longest interval length in $\{\mathbb{R}_1, \cdots, \mathbb{R}_{N_1}\}$ is $[0, q^k)$ where $q \in \mathbb{Z}_p$ and $p > 2q^k + 1$. Let $g, g_0, g_1, g_2, g_3, \hat{g}_1, \hat{g}_2, \cdots, \hat{g}_{N_1}, h, \mathfrak{g}, \eta, \xi, \rho, \vartheta, \eta_1, \eta_2, \cdots, \eta_{N_2}$ 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 $x, y, \mu_1, \mu_2, \cdots, \mu_{N_2} \xleftarrow{R} \mathbb{Z}_p$ and computes $\tilde{g} = g^x, \tilde{h} = h^y, h_0 = h^{\frac{1}{y}}, h_1 = h^{\frac{1}{y+1}}, h_2 = h^{\frac{1}{y+2}}, \cdots, h_{q-1} = h^{\frac{1}{y+q-1}}, \tilde{h}_0 = h^{q^0}, \tilde{h}_1 = h^q, \cdots, \tilde{h}_{k-1} = h^{q^{k-1}}, \tilde{\eta}_1 = \eta_1^{\mu_1}, \tilde{\eta}_2 = \eta_2^{\mu_2}, \cdots, \tilde{\eta}_{N_2} = \eta_{N_2}^{\mu_{N_2}}$ and $\left(\eta_{i_1} = \eta^{\frac{1}{\mu_i + H(I_{i_1})}}, \eta_{i_2} = \eta^{\frac{1}{\mu_i + H(I_{i_2})}}, \cdots, \eta_{i_\varsigma} = \eta^{\frac{1}{\mu_i + H(I_{i_\varsigma})}}\right)_{i=1}^{N_2}$.

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

Fig. 2. Setup Algorithm

Ticket Seller S		Central Authority CA
Selects $x_s \xleftarrow{R} \mathbb{Z}_p$ and computes $Y_S = \rho^{x_s}$.		
Computes the proof Π_S^1 : PoK$\{x_s : Y_S = \rho^{x_s}\}$.	$\xrightarrow{ID_S, Y_S, \Pi_S^1}$	Selects $c_s, r_s \xleftarrow{R} \mathbb{Z}_p$ and computes
Verifies $e(\sigma_S, \tilde{g}g^{c_s}) \stackrel{?}{=} e(g_0, g) \cdot e(g_0, g_1)^{H(VP)}$ $\cdot e(Y_S, g) \cdot e(g, \mathfrak{g})^{r_s}$.	$\xleftarrow{c_s,\ r_s,\ \sigma_S}$	$\sigma_S = (g_0 g_1^{H(VP)} Y_S \mathfrak{g}^{r_s})^{\frac{1}{x+c_s}}$, where VP is a valid period.
Keeps the credential $Cred_S = (c_s, r_s, \sigma_S)$.		

User U		Central Authority CA
Selects $x_u \xleftarrow{R} \mathbb{Z}_p$ and computes $Y_U = \xi^{x_u}$.		
Selects $r \xleftarrow{R} \mathbb{Z}_p$ and compute $R = \mathfrak{g}^r$.		
Computes the proof Π_U^1 : PoK $\{(x_u, r) : Y_U = \xi^{x_u} \ \wedge \ R = \mathfrak{g}^r\}$.	$\xrightarrow[A_U, \Pi_U^1]{ID_U, Y_U, R,}$	Selects $c_u, r' \xleftarrow{R} \mathbb{Z}_p$ and computes $\sigma_U =$
Computes $r_u = r + r'$.	$\xleftarrow{(c_u, r', \sigma_U)}$	$\left(g_0 g_1^{H(VP)} Y_U R \mathfrak{g}^{r'} \prod_{l=1}^{N_1} \hat{g}_l^{a_l} \prod_{i=1}^{N_2} \eta_i^{H(I_{i_j})}\right)^{\frac{1}{x+c_u}}$
Verifies $e(\sigma_U, \tilde{g}g^{c_u}) = e(g_0, g) \cdot e(g_0, g_1)^{H(VP)}$. $e(\xi, g)^{x_u} \cdot e(\mathfrak{g}, g)^{r_u} \cdot \prod_{l=1}^{N_1} e(\hat{g}_l, g)^{a_l}$. $\prod_{i=1}^{N_2} e(\eta_i, g)^{H(I_{i_j})}$.		where VP is a valid period, $a_l \in A_U \models \mathbb{R}_l$ and $A_U \models I_{i_j}$.
Keeps the credential $Cred_U = (c_u, r_u, \sigma_U)$.		Stores $(ID_U, A_U, Y_U, \sigma_U)$.

Fig. 3. Registration Algorithm

$$e(\vartheta, g)^{c_u \alpha} \cdot e(\vartheta, \tilde{g})^{\alpha}. \tag{3}$$

Hence,

$$\frac{e(C, \tilde{g})}{e(g_0, g) \cdot eg_1, g^{H(VP)}} = e(\xi, g)^{x_u} \cdot e(g, \mathfrak{g})^{r_u} \cdot \prod_{l=1}^{N_1} e(\hat{g}_l, g)^{a_l} \cdot \prod_{i=1}^{N_2} e(\eta_i, g)^{H(I_{i_j})} \cdot e(C, g)^{-c_u} \cdot e(\vartheta, g)^{c_u \alpha} \cdot e(\vartheta, \tilde{g})^{\alpha}. \tag{4}$$

$$e(A_{w_i}, \tilde{h}) = e(h^{\frac{t_i}{y+w_i}}, h^y) = e(h^{\frac{t_i y + t_i w_i - t_i w_i}{y+w_i}}, h) = e(h, h)^{t_i} \cdot e(h^{\frac{t_i}{y+w_i}}, h)^{-w_i} = e(h, h)^{t_i} \cdot e(A_i, h)^{-w_i}. \tag{5}$$

$$e(A'_{w_i}, \tilde{h}) = e(h^{\frac{t'_i}{y+w'_i}}, h^y) = e(h^{\frac{t'_i y + t'_i w_i - t'_i w'_i}{y+w'_i}}, h) = e(h, h)^{t'_i} \cdot e(h^{\frac{t'_i}{y+w_i}}, h)^{-w'_i} = e(h, h)^{t'_i} \cdot e(A_i, h)^{-w'_i}. \tag{6}$$

User: U

Ticket Seller: S

Selects $z, v \xleftarrow{R} \mathbb{Z}_p$ and computes
$Q = \sigma_S \vartheta^z$, $Z = g^z \vartheta^v$, $Z^{c_s} = g^{z'} \vartheta^{v'}$
$(z' = zc_s, v' = vc_s)$.

$\xleftarrow{\Pi_S^2}$

Computes the proof Π_S^2 :
PoK $\Big\{ (c_s, r_s, \sigma_S, z, v) : Z = g^z \vartheta^v \wedge$
$Z^{c_s} = g^{z'} \vartheta^{v'} \wedge \frac{e(Q,\tilde{g})}{e(g_0,g) \cdot e(g_1,g)^{H(VP)}} =$
$e(\rho, g)^{x_s} \cdot e(\mathfrak{g}, g)^{r_s} \cdot e(Q, g)^{-c_s} \cdot e(\vartheta, g)^{c_s z} \cdot$
$e(\vartheta, \tilde{g})^z \Big\}$.

Selects $d, \alpha, \beta, \gamma_1, \gamma_2, \cdots, \gamma_{N_1}, t_{l_0}, t_{l_1}, \cdots, t_{l_{k-1}}$,
$t'_{l_0}, t'_{l_1}, \cdots, t'_{l_{k-1}}, e_1, e_2, \cdots, e_{N_2} \xleftarrow{R} \mathbb{Z}_p$.
Computes $C = \sigma_U \vartheta^\alpha, D = g^\alpha \vartheta^\beta, D^{c_u} = g^{\alpha'} \vartheta^{\beta'}$,
$Y = \xi^{x_u} g_1^d, \Big(Z_l = g^{\gamma_l} h^{a_l}$, $(A_{w_{l_i}} = h^{t_{l_i}}_{w_{l_i}}$,
$A'_{w_{l_i}} = h^{t'_{l_i}}_{w'_{l_i}})_{i=0}^{k-1})_{l=1}^{N_1}$, $\Big(B_{i_j} = \eta_{i_j}^{e_i}\Big)_{i=1}^{N_2}$,
where $\alpha' = \alpha c_u, \beta' = \beta c_u$.
Let $a_l \in A_U$, $a_l \in [c_l, d_l)$,
$a_l - c_l, a_l - d_l + q^k \in [0, q^k)$.
Let $a_l - c_l = \sum_{i=0}^{k-1} w_{l_i} q^i$,
$a_l - d_l + q^k = \sum_{i=0}^{k-1} w'_{l_i} q^i$,
where $w_{l_i}, w'_{l_i} \in [0, 1, \cdots, q-1]$.

Computes the proof Π_U^2 :
PoK $\Big\{ \Big(x_u, c_u, r_u, d, \alpha, \beta, \alpha', \beta', \Big(a_l, (t_{l_i}, t'_{l_i}, w_{l_i},$
$w'_{l_i})_{i=0}^{k-1}\Big)_{l=1}^{N_1}, (e_i, H(I_{i_j})_{i=1}^{N_2}\Big) :$ $Y = \xi^{x_u} g_1^d$
$\wedge Z_l = g^{\gamma_l} h^{a_l} \wedge D = g^\alpha \vartheta^\beta \wedge D^{c_u} = g^{\alpha'} \vartheta^{\beta'}$
$\wedge \frac{e(C,\tilde{g})}{e(g_0,g) \cdot e(g_1,g)^{H(VP)}} = e(\xi, g)^{x_u} \cdot e(\mathfrak{g}, g)^{r_u} \cdot$
$\prod_{l=1}^{N_1} e(\hat{g}_l, g)^{a_l} \cdot \prod_{i=1}^{N_2} e(\eta_i, g)^{H(I_{i_j})} \cdot$
$e(C, g)^{-c_u} \cdot e(\vartheta, g)^{\alpha'} \cdot e(\vartheta, \tilde{g})^\alpha$
$\wedge \Big(Z_l h^{-c_l} = g^{\gamma_l} \prod_{i=0}^{k-1} \tilde{h}_i^{w_{l_i}}$
$\wedge Z_l h^{-(d_l - q^k)} = g^{\gamma_1} \prod_{i=0}^{k-1} \tilde{h}_i^{w'_{l_i}}$
$\wedge (e(A_{w_{l_i}}, \tilde{h}) = e(h,h)^{t_{l_i}} \cdot e(A_{w_{l_i}}, h)^{-w_{l_i}})_{i=0}^{k-1}$
$\wedge (e(A'_{w_{l_i}}, \tilde{h}) = e(h,h)^{t'_{l_i}} \cdot e(A'_{w_{l_i}}, h)^{-w'_{l_i}})_{i=0}^{k-1})_{l=1}^{N_1}$
$\wedge \Big(e(B_{i_j}, \tilde{\eta}_i) = e(\eta, \eta_i)^{e_i} \cdot e(B_{i_j}, \eta_i)^{H(I_{i_j})}\Big)_{i=1}^{N_2} \Big\}$

$\xrightarrow{\Pi_U^2, Y}$

Selects $d', s_u, \omega_u \xleftarrow{R} \mathbb{Z}_p$ and computes
$T_U = (g_0 Y g_1^{d'} g_2^{s_u} g_3^{\psi_u})^{\frac{1}{x_s + \omega_u}}$ where s_u is a serial number, $\psi_u = H(\mathbb{P}_U || Price ||$ Serv$||$VP), $\mathbb{P}_U$ consists of the names of range polices and set policies satisfied by U and required by V, $Serv$ are the services which U wants to access and VP is a valid period.

$\xleftarrow{T_U, d', s_u, \omega_u, \psi_u, Service, Price, VP}$

Computes $d_u = d + d'$ and checks
$e(T_U, Y_s \rho^{\omega_u}) \stackrel{?}{=} e(g_0, \rho) \cdot e(Y_U, \rho) \cdot e(g_1, \rho)^{d_u} \cdot$
$e(g_2, \rho)^{s_u} \cdot e(g_3, \rho)^{\psi_u}$.
Keeps the ticket as
$Ticket_U = (d_u, s_u, \psi_u, \omega_u, T'_U$
$\mathbb{P}_U, Price, Service, VP)$

Fig. 4. Ticket Issuing Algorithm

$$
\begin{aligned}
e(B_{i_j}, \tilde{\eta}_i) &= e(\eta_{i_j}^{e_i}, \eta_i^{\mu_i}) = e(\eta^{\frac{e_i}{\mu_i + H(I_{i_j})}}, \eta^{\mu_i}) \\
&= e(\eta^{\frac{e_i \mu_i}{\mu_i + H(I_{i_j})}}, \eta) = e(\eta^{\frac{e_i(\mu_i + H(I_{i_j})) - e_i H(I_{i_j})}{\mu_i + H(I_{i_j})}}, \eta) \\
&= e(\eta, \eta)^{e_i} \cdot e(B_{i_j}, \eta)^{H(I_{i_j})}.
\end{aligned} \tag{7}
$$

$$
\begin{aligned}
e(F, Y_S) &= e((g_0 Y g_1^{d_2} g_2^{s_u} g_3^{\psi_u})^{\frac{1}{x_s + \omega_u}} \vartheta^\pi, \rho^{x_s}) \\
&= e((g_0 Y g_1^{d'} g_2^{s_u} g_3^{\psi_u})^{\frac{x_s + \omega_u - \omega_u}{x_s + \omega_u}}, \rho) \cdot e(\vartheta, Y_S)^\pi \\
&= e(g_0 Y g_1^{d'} g_2^{s_u} g_3^{\psi_u}, \rho) \cdot e((g_0 Y g_1^{d'} g_2^s g_3^{\psi_u})^{\frac{-\omega_u}{x_s + \omega_u}}, \rho) \cdot \\
&\quad e(\vartheta, Y_S)^\pi
\end{aligned} \tag{8}
$$

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

Fig. 5. Ticket Validation Algorithm

If there exit two transcripts $((r, D, E), F, J) \in Table_V$ **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** $E' = \xi^{x_u} H'(ID_V)^{r's_u}$.

To detect the double spend user, V computes $\frac{E^{r'}}{E'^{r}} = \frac{\xi^{x_u r'} H'(ID_V)^{r'rs_u}}{\xi^{x_u r} H'(ID_V)^{r'rs_u}} = \xi^{x_u(r'-r)}$ **and** $Y_U = \xi^{x_u} = (\frac{E^{r'}}{E'^{r}})^{\frac{1}{r'-r}}$.
Hence, U with public key Y_U **is a double spend user.**

Fig. 6. Double Spend Detecting

$$= e(g_0,\rho) \cdot e(\xi,\rho)^{x_u} \cdot e(g_1,\rho)^{d_u} \cdot e(g_2,\rho)^{s_u} \cdot e(g_3,\rho)^{\psi_u}$$
$$e((g_0 Y g_1^{d_2} g_2^{s_u} g_3^{\psi_u})^{\frac{-\omega_u}{x_s+\omega_u}} \vartheta^{-\omega_u\pi}, \rho) \cdot e(\vartheta,\rho)^{\omega_u\pi} \cdot e(\vartheta, Y_S)^{\pi}$$
$$= e(g_0,\rho) \cdot e(\xi,\rho)^{x_u} \cdot e(g_1,\rho)^{d_u} \cdot e(g_2,\rho)^{s_u} \cdot e(g_3,\rho)^{\psi_u}$$
$$e(F,\rho)^{-\omega_u} \cdot e(\vartheta,\rho)^{\omega_u\pi} \cdot e(\vartheta, Y_S)^{\pi}. \tag{9}$$

Hence,

$$\frac{e(F, Y_S)}{e(g_0,\rho) \cdot e(g_3,\rho)^{\psi_u}} = e(\xi,\rho)^{x_u} \cdot e(g_1,\rho)^{d_u} \cdot e(g_2,\rho)^{s_u} \cdot$$
$$e(F,\rho)^{-\omega_u} \cdot e(\vartheta,\rho)^{\omega_u\pi} \cdot e(\vartheta, Y_S)^{\pi}. \tag{10}$$

4 Security Analysis

To prove the security of our PPETS-FGP, indistinguishability between the behaviours of the real-world adversary $\mathcal{A}$ and the behaviours of the ideal-world adversary $\mathcal{A}'$ is proven. 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 as they are meaningless: (1) CA is the only honest party; (2) CA is the only dishonest party; (3) All parties are honest; and (4) All parties are dishonest. Since CA needs to know U's attributes to issue a ticket to him/her, we assume that CA is honest and fully trusted by other entities in the system.

In order to prove the indistinguishability between $\mathcal{A}$ and $\mathcal{A}'$, a sequence of games $\mathbf{Game}_0$, $\mathbf{Game}_1$, $\cdots$,

$\mathbf{Game}_n$ are defined. For each $\mathbf{Game}_i$, we construct a simulator Sim_i that runs $\mathcal{A}$ as a subroutine and provides $\mathcal{E}$'s view, for $i = 0, 1, \cdots, n$. $\mathbf{Hybrid}_{\mathcal{E},Sim_i}(\ell)$ 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 $\mathbf{Hybrid}_{\mathcal{E},Sim_0} = \mathbf{Real}_{\mathcal{E},\mathcal{A}}$. Sim_n runs $\mathcal{A}'$ in ideal-world experiment, hence $\mathbf{Hybrid}_{\mathcal{E},Sim_n}(\ell) = \mathbf{Ideal}_{\mathcal{E},\mathcal{A}'}(\ell)$. Therefore,

$$
\begin{aligned}
&|\mathbf{Real}_{\mathcal{E},\mathcal{A}}(\ell) - \mathbf{Ideal}_{\mathcal{E},\mathcal{A}'}| \leq \\
&\left|\mathbf{Real}_{\mathcal{E},\mathcal{A}}(\ell) - \mathbf{Hybrid}_{\mathcal{E},Sim_1}\right| + \\
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_1} - h\mathbf{Hybrid}_{\mathcal{E},Sim_2}\right| + \cdots + \\
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_{n-2}} - \mathbf{Hybrid}_{\mathcal{E},Sim_{n-1}}\right| + \\
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_{n-1}} - \mathbf{Hybrid}_{\mathcal{E},Sim_n}\right|.
\end{aligned}
$$

Theorem 4. *Our privacy-preserving electronic ticket scheme with fine-grained pricing (PPETS-FGP) described in Fig. 2, Fig. 3, Fig. 4, Fig. 5 and Fig. 6 securely implements the PPETS-FGP functionality if the q-strong Diffie-Hellamn assumption (q-SDH) holds on the bilinear group* $(e, p, \mathbb{G}, \mathbb{G}_\tau)$.

Lemma 1. (Users' Privacy) *For all environments* $\mathcal{E}$ *and all real-world adversaries* $\mathcal{A}$ *who statically controls the ticket seller* S *and verifier* V*, there exists a ideal-word adversary* $\mathcal{A}'$ *such that*

$$|\mathbf{Real}_{\mathcal{E},\mathcal{A}}(\ell) - \mathbf{Ideal}_{\mathcal{E},\mathcal{A}'}(\ell)| \leq 2^{\frac{1}{\ell}}.$$

The proof of **Lemma 1** is referred to the Appendix A.1.

Lemma 2. (Seller's 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 a ideal-word adversary* $\mathcal{A}'$ *such that*

$$
\begin{aligned}
&|\mathbf{Real}_{\mathcal{E},\mathcal{A}}(\ell) - \mathbf{Ideal}_{\mathcal{E},\mathcal{A}'}(\ell)| \leq \frac{q_T}{2^\ell} + \frac{q_v}{2^\ell} + \\
&\frac{1}{q_I} Adv_{\mathcal{A}}^{q_I\text{-}SDH}(\ell) + Adv_{\mathcal{A}}^{(q+1)\text{-}SDH}(\ell) + \\
&Adv_{\mathcal{A}}^{(\varsigma+1)\text{-}SDH}(\ell) + \frac{1}{q_T} Adv_{\mathcal{A}}^{q_T - SDH}(\ell) + \\
&\frac{1}{q_V} Adv_{\mathcal{A}}^{q_V - SDH}(\ell).
\end{aligned}
$$

where q_T*,* q_I*,* q_V *are the number of ticket issue queries made by* $\mathcal{A}$*, credential queries made by* $\mathcal{A}$ *and ticket validation queries made by* $\mathcal{A}$*, respectively.*

The proof of **Lemma 2** is referred to the Appendix A.2.

5 Future Work

The proposed PPETS-FGP is a general e-ticket scheme. In future, key research aspects are: (1) the efficiency of the scheme in its implementation and performance will be improved; (2) simplified version of the proposed PPETS-FGP will be considered so that it can be used in practical scenarios.

6 Conclusions

To protect users' privacy in e-ticket schemes, PPETSs have been proposed, however they have not previously been treated formally. This paper presents the first formal treatment of a PPETS scheme. Furthermore it introduces new features of such a scheme, to implement fine-grained pricing while protecting users' privacy. The distinct features of our PPETS-FGP are as follows: (1) For a service, different users can buy different price tickets without releasing their exact attributes; (2) Two tickets of the same user cannot be linked; (3) Tickets cannot be transferred and double spent; (4) The security of the proposed scheme was formally proven, and reduced to well-known (q- SDH) complexity assumptions.

References

[1] 4chan. What is 4chan, 2013.

[2] 5ch.net. 5channel, 2017.

[3] M. Abe and T. Okamoto. Provably secure partially blind signatures. In *CRYPTO 2000*, pages 271–286. Springer, 2000.

[4] U. Airlines. Customer data privacy policy, 2017.

[5] B. Airways. British airways e-ticket for amadeus users, 2004.

[6] 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 2015*, pages 25–45. DE GRUYTER, 2015.

[7] M. H. Au, W. Susilo, and Y. Mu. Constant-size dynamic k-taa. In *SCN 2006*, pages 111–125. Springer, 2006.

[8] M. H. Au, W. Susilo, and Y. Mu. Practical anonymous divisible e-cash from bounded accumulators. In *FC 2008*, pages 287–301. Springer, 2008.

[9] BBC. ebay faces investigations over massive data breach, 2014.

[10] BBC. Massive equifax data breach hits 143 million, 2017.

[11] M. Bellare and O. Goldreich. On defining proofs of knowledge. In *CRYPTO 1992*, pages 390–420. Springer, 1992.

[12] D. Boneh and X. Boyen. Short signatures without random oracles. In *EUROCRYPT 2004*, pages 56–73. Springer,

2004.
[13] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO 2001*, pages 213–22. Springer, 2001.
[14] D. Boneh, B. Lynn, and H. Shacham:. Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.
[15] D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In *ACM CCS 2004*, pages 168–177.
[16] S. Brands. Untraceable off-line cash in wallets with observers (extended abstract). In *CRYPTO 1993*, pages 302–318. Springer, 1993.
[17] J. Camenisch, R. Chaabouni, and abhi shelat. Efficient protocols for set membership and range proofs. In *ASIACRYPT 2008*, pages 234–252. Springer, 2008.
[18] J. Camenisch, M. Dubovitskaya, and G. Neven. Oblivious transfer with access control. In *ACM CCS 2009*, pages 131–140. ACM, 2009.
[19] J. Camenisch, A. Kiayias, and M. Yung. On the portability of generalized schnorr proofs. In *EUROCRYPT 2009*, pages 425–442. Springer, 2009.
[20] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT 2001*, pages 93–118. Springer, 2001.
[21] J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *CRYPTO 2004*, pages 56–72. Springer, 2004.
[22] J. Camenisch, G. Neven, and abhi shelat. Simulatable adaptive oblivious transfer. In *EUROCRYPT 2007*, page 573?590. Springer, 2007.
[23] J. Camenisch and M. Stadler. Efficient group signature schemes for large groups. In *CRYPTO 1997*, pages 410–424. Springer, 1997.
[24] R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.
[25] A. D. Caro and V. Iovino. On the power of rewinding simulators in functional encryption. *Designs, Codes and Cryptography*, 84(3):373–399, 2017.
[26] D. Chaum. Blind signatures for untraceable payments. In *Crypto 1982*, pages 199–203. Springer, 1982.
[27] D. Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, E28(10):1030–1044, 1985.
[28] D. Chaum and E. van Heyst. Group signatures. In *EUROCRYPT 1991*, pages 257–265. Springer, 1991.
[29] Y.-Y. Chen, C.-L. Chen, and J.-K. Jan. A mobile ticket system based on personal trusted device. *Wireless Personal Communications*, 40(4):569–578, 2007.
[30] G. Davida, Y. Frankel, Y. Tsiounis, and M. Yung. Anonymity control in e-cash systems. In *FC 1997*, pages 1–16. Springer, 1997.
[31] C.-I. Fan and C.-L. Lei. Multi-recastable ticket schemes for electronic voting. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E81-A(5):940–949, 1998.
[32] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO 1986*, pages 186–194. Springer, 1986.
[33] K. Fujimura and Y. Nakajima. General-purpose digital ticket framework. In *USENIX Workshop on Electronic Commerce 1998*, pages 177–186. USENIX Association, 1998.
[34] E. Gabber, P. B. Gibbons, Y. Matias, and A. Mayer. How to make personalized web browsing simple, secure, and anonymous. In *FC 1997*, pages 17–31. Springer, 1997.
[35] Gig. The arry paye gig, 2010.
[36] M. Green and S. Hohenberger. Blind identity-based encryption and simulatable oblivious transfer. In *ASIACRYPT 2007*, page 265?282. Springer, 2007.
[37] R. D. Group. Rail technical strategy capability delivery plan, 2017.
[38] I. Gudymenko. A privacy-preserving e-ticketing system for public transportation supporting fine-granular billing and local validation. In *SIN 2014*, pages 101–107. ACM, 2014.
[39] T. S. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu. Privacy for public transportation. In *PET 2006*, pages 1–19. ACM, 2006.
[40] IATA. Tansferability of tickets, 2012.
[41] O. Jorns, O. Jung, and G. Quirchmayr. A privacy enhancing service architecture for ticket-based mobile applications. In *ARES 2007*, pages 139–146. IEE, 2007.
[42] F. Kerschbaum, H. W. Lim, and I. Gudymenko. Privacy-preserving billing for e-ticketing systems in public transportation. In *WPES 2013*, pages 143–154. ACM, 2013.
[43] N. Kuntze and A. U. Schmidt. Trusted ticket systems and application. In *SEC 2007*, pages 49–60. IFIP Advances in Information and Communication Technology, 2007.
[44] G.-R. Liu, P. Lin, and Y.-B. Lin. Modeling mobile ticket dispenser system with impatient clerk. *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, 65(12):9931–9941, 2016.
[45] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In *SAC 1999*, pages 184–199. Springer, 1999.
[46] Microsoft. system.webserver, 2016.
[47] M. Milutinovic, K. Decroix, V. Naessens, and B. D. Decker. Privacy-preserving public transport ticketing system. In *DBSec 2015*, pages 135–150. Springer, 2015.
[48] 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*, 31(8):925–939, 2012.
[49] T. Nakanishi, N. Haruna, and Y. Sugiyama. Unlinkable electronic coupon protocol with anonymity control. In *ISW 1999*, pages 37–46. Springer, 1999.
[50] B. Patel and J. Crowcroft. Ticket based service access for the mobile user. In *MobiCom 1997*, pages 223–233. ACM, 1997.
[51] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO 1991*, pages 129–140. Springer, 1991.
[52] B. Pfitzmann and M. Waidner. Composition and integrity preservation of secure reactive systems. In *ACM CCS 2000*, pages 245–254. ACM, 2000.
[53] D. Quercia and S. Hailes. Motet: Mobile transactions using electronic ticket. In *SECURECOMM 2005*, pages 1–10. IEEE, 2005.
[54] N. Rail. 16-25 railcard, 2017.
[55] A. Rupp, F. Baldimtsi, G. Hinterw?lder, and C. Paar. Cryptographic theory meets practice: Efficient and privacy-

preserving payments for public transport. *ACM Transactions on Information and System Security*, 17(3):10:01–10:31, 2015.

[56] A. Rupp, G. Hinterw?lder, F. Baldimtsi, and C. Paar. P4r: Privacy-preserving pre-payments with refunds for transportation systems. In *Financial Cryptography 2013*, pages 205–212. Springer, 2013.

[57] R. Song and L. Korba. Pay-TV system with strong privacy and non-repudiation protection. *IEEE Transactions on Consumer Electronics*, 49(2):408–413, 2003.

[58] 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 *MoMM2010*, pages 387–392. ACM, 2010.

[59] 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 2013 and SETOP 2013*, pages 100–113. Springer, 2013.

[60] 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*, E95.D(1):78–93, 2012.

A Security proofs

A.1 Proof of Lemma 1

Proof. To simplify this proof, let U be a single honest user since $\mathcal{A}$ can simulate other users by himself.

Game-1. When $\mathcal{E}$ first makes ticket-issuing queries, the simulator Sim_1 runs the extractor of the proof of knowledge

$$\text{PoK}\left\{\begin{array}{l}(c_s, r_s, \sigma_S, z, v) : Q = \sigma_S \vartheta^z \wedge Z = g^z \vartheta^v \wedge \\ Z^{c_s} = g^{z'} \vartheta^{v'} \wedge \frac{e(Q,\tilde{g})}{e(g_0,g)\cdot e(g_1,g)^{H(VP)}} = \\ e(\rho, g)^{x_s} \cdot e(\mathfrak{g}, g)^{r_s} \cdot e(Q, g)^{-c_s} \cdot e(\vartheta, g)^{c_s z} \cdot \\ e(\vartheta, \tilde{g})^z\end{array}\right\}.$$

to extract from $\mathcal{A}$ the elements $(x_s, c_s, r_s, \sigma_S, z, v)$ such that $Y_S = \rho^{x_s}$, $\sigma_S = (g_0 Y_s \mathfrak{g}^{r_s})^{\frac{1}{x+c_s}}$, $Q = \sigma_S \vartheta^z$, $Z = g^z \vartheta^v$ and $Z^{c_s} = g^{z c_s} \vartheta^{v c_s}$. If the extractor fails, Sim_1 returns $\mathcal{E}$ with $\perp$ to show the failure; otherwise, Sim_1 runs $\mathcal{A}$ to interact with the honest user. The difference between $\mathbf{Hybrid}_{\mathcal{E},Sim_0}$ and $\mathbf{Hybrid}_{\mathcal{E},Sim_1}$ lies in the knowledge error of the proof of knowledge, hence

$$\left|\mathbf{Hybrid}_{\mathcal{E},Sim_0} - \mathbf{Hybrid}_{\mathcal{E},Sim_1}\right| \leq 2^{\frac{1}{\ell}}.$$

Game-2. The simulator Sim_2 works exactly as Sim_1 except that it lets the honest user U to query a ticket for which his attributes A_U satisfy the ticket policy $\mathbb{P}$, namely $A_U \models \mathbb{P}$. Due to the (perfect) zero-knowledgeness of the proof of knowledge, Sim_2 runs a simulated proof of knowledge:

$$\text{PoK}\left\{\begin{array}{l}\big(x_u, c_u, r_u, d, \alpha, \beta, \alpha', \beta', (a_l, (t_{l_i}, t'_{l_i}, w_{l_i}, \\ w'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1}, (e_i, H(I_{i_j}))_{i=1}^{N_2}\big) : Y = \xi^{x_u} g_1^d \\ \wedge Z_l = g^{\gamma} h^{a_l} \wedge D = g^{\alpha} \vartheta^{\beta} \ \wedge \ D^{c_u} = g^{\alpha'} \vartheta^{\beta'} \\ \wedge \frac{e(C,\tilde{g})}{e(g_0,g)\cdot e(g_1,g)^{H(VP)}} = e(\xi, g)^{x_u} \cdot e(\mathfrak{g}, g)^{r_u} \cdot \\ \prod_{l=1}^{N_1} e(\hat{g}_l, g)^{a_l} \cdot \prod_{i=1}^{N_2} \ e(\eta_i, g)^{H(I_{i_j})} \cdot \\ e(\sigma, g)^{-c_u} \cdot e(\vartheta, g)^{\alpha'} \cdot e(\vartheta, \tilde{g})^{\alpha} \\ \wedge \ \left(Z_l h^{-c_l} = g^{\gamma_1} \prod_{i=0}^{k-1} \tilde{h}_i^{w_{l_i}}\right. \\ \wedge \ Z_l \hat{g}_1^{-(d_l - q^k)} = g^{\gamma_1} \prod_{i=0}^{k-1} \tilde{h}_i^{w'_{l_i}} \ \wedge \\ (e(A_{w_{l_i}}, \tilde{h}) = e(h, h)^{t_l} \cdot e(A_{w_{l_i}}, h)^{-w_{l_i}})_{j=0}^{k-1} \ \wedge \\ (e(A'_{w_{l_i}}, \tilde{h}) = e(h, h)^{t_l} \cdot e(A'_{w_{l_i}}, h)^{-w'_{l_i}})_{j=0}^{k-1})_{l=1}^{N_1} \\ \wedge \ \left.\left(e(B_{i_j}, \tilde{\eta}_i) = e(\eta, \eta)^{e_i} \cdot e(B_{i_j}, \eta)^{H(I_{i_j})}\right)_{i=1}^{N_2}\right.\end{array}\right\}.$$

We have

$$\left|\mathbf{Hybrid}_{\mathcal{E},Sim_1} - \mathbf{Hybrid}_{\mathcal{E},Sim_2}\right| = 0.$$

Game-3. The simulator Sim_3 runs exactly as Sim_2, except that it lets the honest user U to valid his/her ticket. Due to the (perfect) zero-knowledgeness of the proof of knowledge, Sim_3 runs a simulated proof:

$$\text{PoK}\left\{\begin{array}{l}(x_u, d_u, s_u, \omega_u, \pi, \lambda, \pi', \lambda') : D = g^{s_u} \wedge \\ E = \xi^{x_u} H'(ID_V)^{r s_u} \wedge F = T_U \vartheta^{\pi} \wedge \\ J = g^{\pi} \vartheta^{\lambda} \wedge J^{\omega_u} = g^{\pi'} \vartheta^{\lambda'} \wedge \frac{e(F,Y_S)}{e(g_0,\rho)\cdot e(g_3,\rho)^{\psi_u}} \\ = e(\xi, \rho)^{x_u} \cdot e(g_1, \rho)^{d_u} \cdot e(g_2, \rho)^{s_u} \cdot \\ e(F, \rho)^{-\omega_u} \cdot e(\vartheta, \rho)^{\pi'} \cdot e(\vartheta, \rho)^{\pi}\end{array}\right\}.$$

We have

$$\left|\mathbf{Hybrid}_{\mathcal{E},Sim_2} - \mathbf{Hybrid}_{\mathcal{E},Sim_3}\right| = 0.$$

Game-4. According to the real-world advesary $\mathcal{A}$, we construct an ideal-world adversary $\mathcal{A}'$ that plays the simultaneous roles of the seller S' and the verifier V', and incorporate all steps from Game_3. $\mathcal{A}'$ runs $\mathcal{A}$ to obtain system parameters *params*. When receiving a user U' registration query $(registration, ID_{U'}, A_{U'})$ from the trusted third party TP, $\mathcal{A}'$ executes the side of the user U with $\mathcal{A}$. If the credential is valid, $\mathcal{A}'$ sends $\tilde{v} = 1$ to TP and adds $(\mathsf{U}', ID_U, A'_U)$ to the user credential list (UCL); otherwise, $\tilde{\nu} = 0$ is returned. For the first time that it receives a ticket issue query $(ticket\_issuing, A_{U'}, VP, Services)$ from TP, it runs $\mathcal{A}$ to obtain the elements $(x_s, c_s, r_s, \sigma_S, z, v)$. $\mathcal{A}'$ simulates a honest user U's query on $(ticket\_issuing, A_{U'}, VP, Services)$. If the ticket is valid, $\mathcal{A}'$ sends $\hat{\nu} = 1$ to TP adds $(A_{U'}, VP, Services)$

to the user ticket list (UTL); otherwise, $\hat{\nu} = 0$ is returned to show failure. When receiving a ticket validating query $(ticket\_validating, T_U, \mathbb{P}_U, Price, VP)$ from TP, $\mathcal{A}'$ run $\mathcal{A}$ to obtain the transcript $Trans$ of the proof of knowledge of $(x_u, d_u, s, \omega_u, pi, \lambda, \pi', \lambda')$. If $Trans$ is valid, $\mathcal{A}'$ sends a bit $\bar{\nu} = 1$ to TP and adds $(T_U, Services, VP, Trans)$ to the ticket validation list (TVL); otherwise, $\bar{\nu} = 0$ is returned. $\mathcal{A}'$ provides $\mathcal{E}$ exactly the same environment as Sim_3, hence

$$\left|\mathbf{Hybrid}_{\mathcal{E},Sim_4} - \mathbf{Hybrid}_{\mathcal{E},Sim_3}\right| = 0.$$

Therefore, we have

$$\begin{aligned}
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_0} - \mathbf{Hybrid}_{\mathcal{E},Sim_4}\right| \leq \\
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_0} - \mathbf{Hybrid}_{\mathcal{E},Sim_1}\right| + \\
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_1} - \mathbf{Hybrid}_{\mathcal{E},Sim_2}\right| + \\
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_2} - \mathbf{Hybrid}_{\mathcal{E},Sim_3}\right| + \\
&\left|\mathbf{Hybrid}_{\mathcal{E},Sim_4} - \mathbf{Hybrid}_{\mathcal{E},Sim_3}\right| \leq 2^{\frac{1}{\ell}}.
\end{aligned}$$

□

A.2 Proof of Lemma 2

Proof. Our PPETS-FGP prevents users from pooling their credentials, hence we should consider multiple users, some of which are corrupted and some of which are honest.

Game-1. For each ticket issuing query from a corrupted user dictated by $\mathcal{E}$, the simulator Sim_1 runs the extractor for the proof of knowledge

$$\text{PoK}\left\{\begin{array}{l}
\Big(x_u, c_u, r_u, d, \alpha, \beta, \alpha', \beta', (a_l, (t_{l_i}, t'_{l_i}, w_{l_i}, \\
w'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1}, (e_i, H(I_{i_j}))_{i=1}^{N_2}\Big) : Y = \xi^{x_u} g_1^d \\
\wedge\ Z_l = g^{\gamma} h^{a_l} \wedge D = g^{\alpha} \vartheta^{\beta} \ \wedge\ D^{c_u} = g^{\alpha'} \vartheta^{\beta'} \\
\wedge \frac{e(C,\tilde{g})}{e(g_0,g)\cdot e(g_1,g)^{H(VP)}} = e(\xi,g)^{x_u} \cdot e(\mathfrak{g},g)^{r_u} \cdot \\
\prod_{l=1}^{N_1} e(\hat{g}_l, g)^{a_l} \cdot \prod_{i=1}^{N_2}\ e(\eta_i, g)^{H(I_{i_j})} \cdot \\
e(\sigma, g)^{-c_u} \cdot e(\vartheta, g)^{\alpha'} \cdot e(\vartheta, \tilde{g})^{\alpha} \\
\wedge \left(Z_l h^{-c_l} = g^{\gamma_1} \prod_{i=0}^{k-1} \tilde{h}_i^{w_{l_i}}\right. \\
\wedge\ Z_l \hat{g}_1^{-(d_l - q^k)} = g^{\gamma_1} \prod_{i=0}^{k-1} \tilde{h}_i^{w'_{l_i}} \ \wedge \\
(e(A_{w_{l_i}}, \tilde{h}) = e(h,h)^{t_l} \cdot e(A_{w_{l_i}}, h)^{-w_{l_i}})_{j=0}^{k-1} \ \wedge \\
\left.(e(A'_{w_{l_i}}, \tilde{h}) = e(h,h)^{t_l} \cdot e(A'_{w_{l_i}}, h)^{-w'_{l_i}})_{j=0}^{k-1}\right)_{l=1}^{N_1} \\
\wedge \left(e(B_{i_j}, \tilde{\eta}_i) = e(\eta, \eta)^{e_i} \cdot e(B_{i_j}, \eta)^{H(I_{i_j})}\right)_{i=1}^{N_2}
\end{array}\right\}.$$

to extract $(x_u, c_u, r_u, d, \alpha, \beta, \alpha', \beta', (a_l, (t_{l_i}, t'_{l_i}, w_{l_i}, w'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1}, (e_i, H(I_{i_j}))_{i=1}^{N_2})$. If the extractor fails, Sim_1 returns $\perp$ to $\mathcal{E}$ to indicate failure; otherwise, Sim_1 runs $\mathcal{A}$ interacting with the honest ticket seller. The difference between $\mathbf{Hybrid}_{\mathcal{E},Sim_0}$ and $\mathbf{Hybrid}_{\mathcal{E},Sim_1}$ is

$$\left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_0}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_1}}\right| \leq \frac{q_T}{2^{\ell}}$$

where q_T is the number of ticket issue queries.

Game-2. The simulator Sim_2 runs exactly as Sim_1 except that Sim_2 returns $\perp$ to $\mathcal{E}$ if one of the credentials $(c_u, r_u, \sigma_U = C\vartheta^{-\alpha})$ is not generated by the Join algorithm. Actually, $(c_u, r_u, \sigma_U = C\vartheta^{-\alpha})$ is a forged BBS+ signature [7] on $(x_u, a_u, r'_u, ((H(I_{ij})_{A_U \models I_{i_j}})_{i=1}^{N})$. For the case that multiple corrupted users pool their credentials, one of the pooled credentials must have a different x_u when it was issued since only a single x_u is extracted, hence is a forged credential. Due to the security of the signature scheme [7], the difference between $\mathbf{Hybrid}_{\mathcal{E},Sim_2}$ and $\mathbf{Hybrid}_{\mathcal{E},Sim_1}$ is the following lemma.

Claim 1. *We claim that*

$$\left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_2}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_1}}\right| \leq \frac{1}{q_I} Adv_{\mathcal{A}}^{q_I - SDH}(\ell),$$

where q_I is the number of crendentail queries made by the adversary $\mathcal{A}$.

Game-3. The simulator Sim_3 runs exactly as Sim_2, except that $a_l \notin [c_l, d_l]$. In this case, there exists at least one $w_{l_i} \notin [0, 1, \cdots, q-1]$ or $w'_{l_i} \notin [0, 1, \cdots, q-1]$. If $w_{l_i} \notin [0, 1, \cdots, q-1]$ or $w'_{l_i} \notin [0, 1, \cdots, q-1]$, we have $h_{w_i} = A_{w_i}^{\frac{1}{t_i}} = h^{\frac{1}{y+w_i}}$ or $h_{w'_i} = (A'_{w_i})^{\frac{1}{t'_i}} = h^{\frac{1}{y+w'_i}}$ is a forged BB signature [12]. The difference between $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_3}}$ and $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_2}}$ is bounded by the following lemma.

Claim 2. *We claim that*

$$\left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_3}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_2}}\right| \leq Adv_{\mathcal{A}}^{(q+1)-SDH}(\ell).$$

Game-4. The simulator Sim_4 runs exact as Sim_4 except that there exists at least an $I_{i_j} \notin \mathbb{P}_i$. If $I_{i_j} \notin \mathbb{P}_i$, so $B_{i_j}^{\frac{1}{e_i}} = \eta_{i_j} = \eta^{\frac{1}{\eta_i + H(I_{i_j})}}$ is a forged BB signature on $H(i_j)$. The difference between $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_4}}$ and $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_3}}$ is bounded by the following lemma.

Claim 3. *We claim that*

$$\left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_4}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_3}}\right| \leq Adv_{\mathcal{A}}^{(\varsigma+1)-SDH}(\ell).$$

Game-5. The simulator Sim_5 runs exactly as Sim_4 except that Sim_5 returns tickets to $\mathcal{E}$. At the first ticket issuing query dictated by $\mathcal{E}$, Sim_5 runs the simulated proof of knowledge

$$\text{PoK}\left\{\begin{array}{l}
(c_s, r_s, \sigma_S, z, v) : Q = \sigma_S \vartheta^z \wedge Z = g^z \vartheta^v \\
\wedge Z^{c_s} = g^{z'} \vartheta^{v'} \wedge \frac{e(Q,\tilde{g})}{e(g_0,g)\cdot e(g_1,g)^{H(VP)}} = \\
e(\rho, g)^{x_s} \cdot e(\mathfrak{g}, g)^{r_s} \cdot e(Q, g)^{-c_s} \cdot e(\vartheta, g)^{c_s z} \cdot \\
e(\vartheta, \tilde{g})^{z}
\end{array}\right\}.$$

The tickets (d_u, ω_u, T_u) for each ticket issuing query is computed by using the signing oracle in [7]. The following lemma is used to bound the difference between $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_5}}$ and $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_4}}$.

Claim 4. *We claim that*

$$\left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_5}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_4}}\right| \leq \frac{1}{q_T} Adv_{\mathcal{A}}^{q_T-SDH}(\ell).$$

where q_T is the number of ticket issuing queries made by $\mathcal{A}$

Game-6. The simulator Sim_6 runs exactly as Sim_5 except that Sim_6 runs the extractor of the proof of knowledge

$$\text{PoK}\left\{\begin{array}{l}(x_u, d_u, s_u, \omega_u, \pi, \lambda, \pi', \lambda') : D = g^{s_u} \wedge \\ E = \xi^{x_u} H'(ID_V)^{rs_u} \wedge F = T_U \vartheta^{\pi} \wedge \\ J = g^{\pi}\vartheta^{\lambda} \wedge J^{\omega_u} = g^{\pi'}\vartheta^{\lambda'} \wedge \frac{e(F,Y_S)}{e(g_0,\rho)e(g_3,\rho)^{\psi_u}} \\ = e(\xi,\rho)^{x_u} \cdot e(g_1,\rho)^{d_u} \cdot e(g_2,\rho)^{s_u} \cdot \\ e(F,\rho)^{-\omega_u} \cdot e(\vartheta,\rho)^{\pi'} \cdot e(\vartheta,\rho)^{\pi}\end{array}\right\}.$$

to exact from $\mathcal{A}$ the witness $(x_u, d_u, s, \omega_u, \pi, \lambda, \pi', \lambda')$. If the extraction fails, Sim_7 returns $\perp$ to $\mathcal{E}$; otherwise, it continue to run $\mathcal{A}$ interacting with the honest verifier V. The difference between $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_6}}$ and $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_5}}$ is

$$\left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_6}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_5}}\right| \leq \frac{q_V}{2^{\ell}}$$

where q_V is the number of ticket validation queries.

Game-7. The simulator Sim_7 runs exactly as Sim_6 except that Sim_7 returns $\perp$ to $\mathcal{E}$ if at least one of the extracted $(x'_u, d'_u, s', \omega'_u, T'_U, \pi, \lambda, \pi', \lambda')$ was not generated by the Ticket Issuing algorithm. Actually, (ω'_u, T'_U) is a signature on (x_u, d'_u, s'). For multiple users case, one of the pooled tickets must have a different x'_u than when it was issue since only one x_u is extracted, hence (ω'_u, T'_U) is a forged signature on (x'_u, d'_u, s'). The following lemma is used to bound the difference between $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_8}}$ and $\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_7}}$.

Claim 5. *We claim that*

$$\left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_7}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_6}}\right| \leq \frac{1}{q_V} Adv_{\mathcal{A}}^{q_V-SDH}.$$

Game-8. Now, based on the real-world adversary $\mathcal{A}$, we construct an ideal-word adversary $\mathcal{A}'$. $\mathcal{A}'$ runs $\mathcal{A}$ to obtain *params* and Y_S. After receiving a ticket issue query $(ticket\_issuing, A_{U'}, services, VP)$ from TP, $\mathcal{A}'$ runs $\mathcal{A}$ to returns a simulated proof of the knowledge:

$$\text{PoK}\left\{\begin{array}{l}(c_s, r_s, \sigma_S, z, v) : Q = \sigma_S \vartheta^z \wedge Z = g^z \vartheta^v \wedge \\ Z^{c_s} = g^{z'}\vartheta^{v'} \wedge \frac{e(Q,\tilde{g})}{e(g_0,g)\cdot e(g_1,g)^{H(VP)}} = \\ e(\rho,g)^{x_s} \cdot e(\mathfrak{g},g)^{r_s} \cdot e(Q,g)^{-c_s} \cdot e(\vartheta,g)^{c_s z} \cdot \\ e(\vartheta,\tilde{g})^{z}\end{array}\right\}.$$

After having extracted $(x_u, c_u, r_u, d_u, \alpha, \beta, \alpha', \beta', t_1, t_2, \cdots, t_{k-1}, t'_0, t'_1, \cdots, t'_{k-1}, ((e_i, H(I_{i_j}))_{A_U \models I_{i_j}})_{i=1}^{N})$ from $\mathcal{A}$, $\mathcal{A}'$ queries TP to obtain a credential (c_u, r_u, σ_U) for U'. Next, $\mathcal{A}'$ runs $\mathcal{A}$ to generate a BBS+ signature [7] (s_u, ω_u, T_u) on (x_u, d_u). If the signature can be generated correctly, TP returns $\mathcal{A}'$ with a bit $\hat{\nu} = 1$; otherwise $\hat{\nu} = 0$ is returned. After receiving a ticket validation query $(ticket\_validating, T_{U'}, Services, VP)$ from V', $\mathcal{A}'$ runs $\mathcal{A}$ to execute the proof of knowledge

$$\text{PoK}\left\{\begin{array}{l}(x_u, d_u, s_u, \omega_u, \pi, \lambda, \pi', \lambda') : D = g^{s_u} \wedge \\ E = \xi^{x_u} H'(ID_V)^{rs_u} \wedge F = T_U \vartheta^{\pi} \wedge \\ J = g^{\pi}\vartheta^{\lambda} \wedge J^{\omega_u} = g^{\pi'}\vartheta^{\lambda'} \wedge \frac{e(F,Y_S)}{e(g_0,\rho)e(g_3,\rho)^{\psi_u}} \\ = e(\xi,\rho)^{x_u} \cdot e(g_1,\rho)^{d_u} \cdot e(g_2,\rho)^{s_u} \cdot \\ e(F,\rho)^{-\omega_u} \cdot e(\vartheta,\rho)^{\pi'} \cdot e(\vartheta,\rho)^{\pi}\end{array}\right\}.$$

If the proof is correct, TP returns $\mathcal{A}'$ with a bit $\bar{\nu} = 1$ and adds $(\mathsf{U}', T_{U'}, Services, VP)$ into TVL; otherwise, $\bar{\nu} = 0$ is returned. After receiving a double spend detecting query $(double\_spend\_detecting, T_{U'})$ from V', TP checks where $T_{U'}$ is in TVL. If it is, TP returns V' with a bit $\check{\nu} = 1$; otherwise, $\check{\nu} = 0$ is returned. $\mathcal{A}'$ provides $\mathcal{A}$ with the same environment as Sim_7 did, hence we have

$$\mathbf{Hybrid}_{\mathcal{E},Sim_8} = \mathbf{Hybrid}_{\mathcal{E},Sim_7}.$$

Therefore, we have

$$\begin{aligned}&|\mathbf{Real}_{\mathcal{E},\mathcal{A}} - \mathbf{Ideal}_{\mathcal{E},\mathcal{A}'}| = \\ &|\mathbf{Real}_{\mathcal{E},\mathcal{A}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_1}} + \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_1}} - \\ &\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_2}} + \cdots + \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_8}} - \mathbf{Real}_{\mathcal{E},\mathcal{A}'}| \leq \\ &\left|\mathbf{Real}_{\mathcal{E},\mathcal{A}} - \mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_1}}\right| + |\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_1}} - \\ &\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_2}}| + \cdots + \left|\mathbf{Hybrid}_{\mathcal{E},\mathbf{Sim_8}} - \mathbf{Real}_{\mathcal{E},\mathcal{A}'}\right| \leq \\ &\frac{q_T}{2^{\ell}} + \frac{q_v}{2^{\ell}} + \frac{1}{q_I} Adv_{\mathcal{A}}^{q_I-SDH}(\ell) + Adv_{\mathcal{A}}^{(q+1)-SDH}(\ell) + \\ &Adv_{\mathcal{A}}^{(\varsigma+1)-SDH}(\ell) + \frac{1}{q_T} Adv_{\mathcal{A}}^{q_T-SDH}(\ell) + \\ &\frac{1}{q_V} Adv_{\mathcal{A}}^{q_V-SDH}(\ell)\end{aligned}$$

□

Proof of Claim 1. This claim is proven by constructing an algorithm $\mathcal{B}$ that can break the unforgeability under the adaptively chosen message attacks of BBS+ signature [7]. From the security proof presented in [7], there exist a polynomial-time algorithm $\mathcal{B}$ that can break the q_I-SDH assumption with non-negligible advantage.

Suppose that the adversary $\mathcal{A}$ can distinguish **Game-1** and **Game-2**. Given $(\rho, \rho^{x_s}, \rho^{x_s^2}, \cdots, \rho^{x_s^{q_I}})$. $\mathcal{B}$ aims to outpput $(c, \rho^{\frac{1}{x_s+c}})$ where $c \in \mathbb{Z}_p$ and $c \neq -x_s$. Let $Y_S = \rho^{x_s}$.

$\mathcal{B}$ sends q_I messages $(m_1, m_2, \cdots, m_{q_I})$ to the challenger $\mathcal{C}$, and obtains $(\tilde{\sigma}_1, \tilde{\sigma_2}, \cdots, \tilde{\sigma}_{q_I})$ where $\tilde{\sigma}_i = \rho^{\frac{1}{x_s+m_i}}$ and $e(\tilde{\sigma}_i, Y_S\rho^{m_i}) = e(\rho, \rho)$ for $i = 1, 2, \cdots, q_I$. $\mathcal{B}$ selects $\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}, \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \xleftarrow{R} \mathbb{Z}_p$, and computes $g_1 = ((Y_S\rho^{\tilde{\alpha}})^{\tilde{\gamma}}\rho^{-1})^{\frac{1}{\tilde{\beta}}} = \rho^{\frac{(x_s+\tilde{\alpha})\tilde{\gamma}-1}{\tilde{\beta}}}$, $g_0 = \rho^{\tilde{a}}$, $g_2 = g_1^{\tilde{b}}$, $g_3 = g_1^{\tilde{d}}$ and $\xi = g_1^{\tilde{c}}$. $\mathcal{B}$ sends $\mathcal{A}$ the parameters $(\rho, Y_S, g_0, \xi, g_1, g_2, g_3)$.

For q_I ticket issuing queries, $\mathcal{B}$ selects one and referred as query $\tilde{Q} = (\mathbb{P}_U, Price, Services, VP)$. For $q_I - 1$ queries other than query $\tilde{Q}$, $\mathcal{B}$ responses using the $q_I - 1$ pairs (m_i, σ_i) as follows.

Suppose that $\mathcal{A}$ queries a ticket on $(\mathbb{P}_U, Price, Services, VP)$, since $\mathcal{B}$ extracts the knowledge of $(x_u, c_u, r_u, d, \alpha, \beta, \alpha', \beta', (a_l, (t_{l_i}, t'_{l_i}, w_{l_i}, w'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1}, (e_i, H(I_{i_j}))_{i=1}^{N_2})$, $\mathcal{B}$ selects $d', s_u \xleftarrow{R} \mathbb{Z}_p$, and computes $\psi_u = H(\mathbb{P}_U||Price||Services||VP)$ and $t = x_u\tilde{c} + (d' + d) + \tilde{b}s_u + \tilde{d}\psi_u$ and

$$\begin{aligned}
T_U &= (g_0 Y g_1^{d'} g_2^{s_u} g_3^{\psi_u})^{\frac{1}{x_s+m_i}} = (g_0 g_1^{t})^{\frac{1}{x_s+m_i}} = \sigma_i^{\tilde{a}} g_1^{\frac{t}{x_s+m_i}} \\
&= \sigma_i^{\tilde{a}} \rho^{\frac{t((x_s+\tilde{\alpha})\tilde{\gamma}-1)}{\tilde{\beta}(x_s+m_i)}} = \sigma_i^{\tilde{a}} (\rho^{\frac{(x_s+\tilde{\alpha})\tilde{\gamma}-1}{(x_s+m_i)}})^{\frac{t}{\tilde{\beta}}} \\
&= \sigma_i^{\tilde{a}} (\rho^{\frac{(x_s+m_i-m_i+\tilde{\alpha})\tilde{\gamma}-1}{(x_s+m_i)}})^{\frac{t}{\tilde{\beta}}} \\
&= \sigma_i^{\tilde{a}} \rho^{\frac{t\tilde{\gamma}}{\tilde{\beta}}} \sigma_i^{\frac{t((\tilde{\alpha}-m_i)\tilde{\gamma}-1)}{\tilde{\beta}}}
\end{aligned}$$

where $m_i \in \{m_1, m_2, \cdots, m_{q_I}\}$.

For the query $\tilde{Q}$ where $\tilde{Y} = \xi^{\tilde{x}} g_1^{\tilde{d}}$, $\mathcal{B}$ computes $\tilde{\phi} = H(\mathbb{P}_{\tilde{U}}||Price||Services||VP)$ and selects $\tilde{d}', \tilde{s} \in \mathbb{Z}_p$ such that $\tilde{d}' + \tilde{d} + \tilde{c}\tilde{x} + \tilde{b}\tilde{s} + \tilde{d}\tilde{\psi} = \tilde{a}\tilde{\beta}$ and computes

$$\begin{aligned}
\tilde{T} &= (g_0 \tilde{Y} g_1^{\tilde{d}'} g_2^{\tilde{s}} g_3^{\tilde{\psi}})^{\frac{1}{x_s+\tilde{\alpha}}} \\
&= e(g_0 g_1^{\tilde{c}\tilde{x}+\tilde{d}+\tilde{d}'+\tilde{b}\tilde{s}+\tilde{d}\tilde{\psi}})^{\frac{1}{x_s+\tilde{\alpha}}} \\
&= (\rho^{\tilde{a}} \rho^{\frac{((x_s+\tilde{\alpha})\tilde{\gamma}-1)(\tilde{c}\tilde{x}+\tilde{d}+\tilde{d}'+\tilde{b}\tilde{s}+\tilde{d}\tilde{\psi})}{\tilde{\beta}}})^{\frac{1}{x_s+\tilde{\alpha}}} \\
&= (\rho^{\frac{((x_s+\tilde{\alpha})\tilde{\gamma}-1)(\tilde{c}\tilde{x}+\tilde{d}+\tilde{d}'+\tilde{b}\tilde{s})+\tilde{a}\tilde{\beta}}{\tilde{\beta}}})^{\frac{1}{x_s+\tilde{\alpha}}} \\
&= (\rho^{\frac{((x_s+\tilde{\alpha})\tilde{\gamma}-1)\tilde{a}\tilde{\beta}+\tilde{a}\tilde{\beta}}{\tilde{\beta}}})^{\frac{1}{x_s+\tilde{\alpha}}} \\
&= \rho^{\tilde{\gamma}\tilde{a}}
\end{aligned}$$

$\mathcal{B}$ repondes $\mathcal{A}$ with $(\tilde{a}\tilde{\beta} - \tilde{d} - \tilde{c}\tilde{x} - \tilde{b}\tilde{s} - \tilde{d}\tilde{\psi}, \tilde{s}, \tilde{\psi}, \alpha, \tilde{T})$ where $\tilde{\psi} = H(\mathbb{P}_{\tilde{U}}||Price||Services||VP)$. Finally, $\mathcal{A}$ output a forged tickets $(\tilde{d}^*, s^*, \psi^*, \omega^*, T^*)$ for $(\mathbb{P}_{U^*}, price, Services, VP)$ where $\psi^* = H(\mathbb{P}_{U^*}||Price||Services||VP)$, $Y^* = \xi^{x^*} g_1^{d^*}$ and $T^* = (g_0 Y^* g_1^{\tilde{d}^*} g_2^{s^*} g_3^{\psi^*})^{\frac{1}{x_s+\omega^*}}$. $\mathcal{B}$ runs $\mathcal{A}$ to extract (x^*, d^*) from the proof of $\prod^2_{U^*}$. We consider the following three cases.

Case-I $(\omega^* \notin (m_1, m_2, \cdots, m_{q_I}, \tilde{\alpha}))$: Let $t^* = \tilde{c}x^* + d^* + \tilde{d}^* + \tilde{b}s^* + \tilde{d}\psi^*$.

$$\begin{aligned}
T^* &= (g_0 Y^* g_1^{\tilde{d}^*} g_2^{s^*} g_3^{\psi^*})^{\frac{1}{x_s+\omega^*}} \\
&= (g_0 g_1^{\tilde{c}x^*+d^*+\tilde{d}^*+\tilde{b}s^*+\tilde{d}\psi^*})^{\frac{1}{x_s+\omega^*}} \\
&= (\rho^{\tilde{a}} \rho^{\frac{t^*((x_s+\tilde{\alpha})\tilde{\gamma}-1)}{\tilde{\beta}}})^{\frac{1}{x_s+\omega^*}} \\
&= \rho^{\frac{\tilde{a}}{x_s+\omega^*}} \rho^{\frac{t^*((x_s+\tilde{\alpha})\tilde{\gamma}-1)}{\tilde{\beta}(x_s+\omega^*)}} \\
&= \rho^{\frac{\tilde{a}}{x_s+\omega^*}} \rho^{\frac{t^*((x_s+\omega^*-\omega^*+\tilde{\alpha})\tilde{\gamma}-1)}{\tilde{\beta}(x_s+\omega^*)}} \\
&= \rho^{\frac{\tilde{a}}{x_s+\omega^*}} \rho^{\frac{t^*\tilde{\gamma}}{\tilde{\beta}}} \rho^{\frac{t^*(\tilde{\alpha}-\omega^*)\tilde{\gamma}}{\tilde{\beta}(x_s+\omega^*)}} \rho^{\frac{-t^*}{\tilde{\beta}(x_s+\omega^*)}}.
\end{aligned}$$

We have

$$T^* \rho^{\frac{-t^*\tilde{\gamma}}{\tilde{\beta}}} = \rho^{\frac{\tilde{a}\tilde{\beta}+t^*(\tilde{\alpha}-\omega^*)\tilde{\gamma}-t^*}{\tilde{\beta}(x_s+\omega^*)}}$$

and

$$\rho^{\frac{1}{x_s+\omega^*}} = (T^* \rho^{\frac{-t^*\tilde{\gamma}}{\tilde{\beta}}})^{\frac{\tilde{\beta}}{\tilde{a}\tilde{\beta}+t^*(\tilde{\alpha}-\omega^*)\tilde{\gamma}-t^*}}$$

$\mathcal{B}$ outputs $(\omega^*, (T^* \rho^{\frac{-t^*\tilde{\gamma}}{\tilde{\beta}}})^{\frac{\tilde{\beta}}{\tilde{a}\tilde{\beta}+t^*(\alpha^*-\omega^*)\tilde{\gamma}-t^*}})$.

Case-II $(\omega^* = m_i$ and $T^* = T_i)$ or $(\omega^* = \tilde{\alpha}$ and $T^* = \tilde{T})$: These happen with negligible probability except that $\mathcal{A}$ can solves the related discrete logarithms amongst off g_0, g_1, g_2, g_3 and ξ.

Case-III $(\omega^* \in (m_1, m_2, \cdots, m_{q_I}, \tilde{\alpha}))$ and $T^* \neq T_i$ or $T^* \neq \tilde{T}$: If it is, $\omega^* = \tilde{\alpha}$ with the probability $\frac{1}{q_I}$. Let $t^* = \tilde{c}x^* + d^* + \tilde{d}^* + \tilde{b}s^* + \tilde{d}\psi^*$. We have $\rho^{\frac{1}{x_s+\omega^*}} = (T^* \rho^{\frac{-t^*\tilde{\gamma}}{\tilde{\beta}}})^{\frac{\tilde{\beta}}{\tilde{a}\tilde{\beta}-t^*}}$. $\mathcal{B}$ outputs $(\omega^*, (T^* \rho^{\frac{-t^*\tilde{\gamma}}{\tilde{\beta}}})^{\frac{\tilde{\beta}}{\tilde{a}\tilde{\beta}-t^*}})$.

Therefore,

$$\left|\mathbf{Hybrid}_{\mathcal{E},Sim_2}(\ell) - \mathbf{Hybrid}_{\mathcal{E},Sim_1}(\ell)\right| \leq \frac{1}{q_I} Adv_{\mathcal{A}}^{q_I-SDH}(\ell).$$

Proof of Claim 2. This claim is proven by constructing an algorithm $\mathcal{B}$ that can break the unforgeability under the weak chosen message attacks of BB signature [12]. By the security proof given in [12], there exists an polynomial-time algorithm $\mathcal{B}$ that can break the $(q+1)$-SDH assumption with non-negligible advantage.

Suppose that an adversary $\mathcal{A}$ can distinguish **Game-2** and **Game-3**. Given $(h, h^y, h^{y^2}, \cdots, h^{y^{q+1}})$, $\mathcal{B}$ aims to output $(c, h^{\frac{1}{y}})$ where $c \in \mathbb{Z}_p$ and $c \neq -y$. Receiving q messages $\{0, 1, \cdots, q-1\}$ from $\mathcal{A}$, $\mathcal{B}$ computes $f(y) = \prod_{j=0}^{q}(y + j) = \sum_{j=0}^{q} \pi_j y^j$, $yf(y) = \sum_{j=1}^{q+1} \phi_j y^j$ and $f_i(y) = \frac{f(y)}{y+i} = \sum_{j=0}^{q-1} \varpi_j y^j$ where $\pi_0, \cdots, \phi_q, \phi_1, \cdots, \phi_{q+1}, \varpi_0, \cdots, \varpi_{q-1} \in \mathbb{Z}_p$. $\mathcal{B}$ computes $\hat{h} = h^{f(y)} = \prod_{j=0}^{q}(h^{y^j})^{\pi_i}$, $\tilde{h} = \hat{h}^y = h^{yf(y)} = \prod_{j=0}^{q}(h^{y^{j+1}})^{\pi_j}$ and $h_i =$

$\hat{h}^{\frac{1}{y+i}} = h^{\frac{f(y)}{y+i}} \prod_{j=0}^{q-1}(h^{y^j})^{\varpi_i}$ for $i = 0, 2, \cdots, q-1$. $\mathcal{B}$ sends $(\hat{h}, \tilde{h}, h_1, h_2, \cdots, h_q)$ to $\mathcal{A}$. Since $\mathcal{B}$ extracts $(x_u, a_u, c_u, r_u, d_u, \alpha, \beta, \alpha', \beta', (t_i, t_i', \omega_i, \omega_i')_{i=0}^{k-1}, ((e_i, H(I_{i_j}))_{A_U \in I_{i_j}})_{i=1}^{N})$ with $e(A_{w_i}, \tilde{h}) = e(h,h)^{t_i} \cdot e(A_{w_i}, h)^{-w_i}$ and $e(A'_{w_i}, \tilde{h}) = e(h,h)^{t_i} \cdot e(A'_{w_i}, h)^{-w_i'}$. Hence, $h_{w_i} = (A_{w_i})^{\frac{1}{t_i}} = \hat{h}^{\frac{1}{y+w_i}}$ or $h_{w_i} = (A'_{w_i})^{\frac{1}{t_i'}} = \hat{h}^{\frac{1}{y+w_i'}}$. When $w_i \notin \{0, 1, \cdots, k-1\}$, let $f(y) = c(x) \cdot (x + w_i) + \gamma$, where $\gamma \neq 0$ and $c(x) = \sum_{j=0}^{q-1} \varrho_j y^j$ is a $(q-1)$-degree polynomial. We have

$$h_{w_i} = \hat{h}^{\frac{1}{y+w_i}} = h^{\frac{f(y)}{y+w_i}} = h^{\frac{\gamma + c(x)\cdot(x+w_i)}{y+w_i}} = h^{\frac{\gamma}{y+w_i}} \cdot \prod_{j=0}^{q-1}(h^{y^j})^{\varrho_j}$$

and

$$h^{\frac{1}{y+w_i}} = (h_{w_i} \prod_{j=0}^{q-1}(h^{y^j})^{-\psi_j})^{\frac{1}{\gamma}} = ((A_{w_i})^{\frac{1}{t_i}} \prod_{j=0}^{q-1}(h^{y^j})^{-\varrho_j})^{\frac{1}{\gamma}}.$$

Finally, $\mathcal{B}$ outputs $(w_i, h^{\frac{1}{y+w_i}})$. Therefore,

$$\left|\mathbf{Hybrid}_{\mathcal{E},Sim_3} - \mathbf{Hybrid}_{\mathcal{E},Sim_2}\right| \leq Adv_{\mathcal{A}}^{(q+1)-SDH}(\ell).$$

Proofs of Claim 3, 4, 5. The proof of 3 is similar to the proof of Claim 2. The proofs of Claim 4 and 5 is similar as the proof of Claim 1.

B Details of Zero-Knowledge Proofs

The details of zero-knowledge proofs used in our PPETS-FGP are described by using the Fiat-Shamir heuristic [32] as follows.

The Detail of $\prod_S^1$:

The ticket seller S select $t_s \xleftarrow{R} \mathbb{Z}_p$ and $M_S^1 \xleftarrow{R} \mathbb{G}$, and computes $T_S = \rho^{t_s}$, $c = H(M_S^1||Y_S||T_S)$ and $s = t_s - cx_s$. S sends (c, s, M_S^1, Y_S) to CA.

CA verifies $c \stackrel{?}{=} H(M_S^1||Y_S||\rho^s Y_S^c)$.

The Detail of $\prod_U^1$:

U select $\tilde{x}, \tilde{r} \xleftarrow{R} \mathbb{Z}_p$ and $M_U^1 \xleftarrow{R} \mathbb{G}$, and computes $Y_U' = \xi^{\tilde{x}}$, $R' = g^{\tilde{r}}$, $c_1 = H(M_U^1||Y_U||Y_U')$, $c_2 = H(M_U^1||R||R')$, $s_1 = \tilde{x} - c_1 x_u$ and $s_2 = \tilde{r} - c_2 r$. U sends $(M_U^1, Y_U, R, Y_U', R', c_1, c_2, s_1, s_2)$ to CA.

CA verifies $c_1 \stackrel{?}{=} H(M_U^1||Y_U||\xi^{s_1} Y_U^{c_1})$ and $c_2 = H(M_U^1||R||g^{s_2} R^{c_2})$.

The Detail of $\prod_S^2$:

S selects $z, v, \tilde{z}, \tilde{v}, \hat{z}, \hat{v}, \tilde{x}_s, \tilde{v}_s, \tilde{c}_s \xleftarrow{R} \mathbb{Z}_p$ and $M_S^2 \xleftarrow{R} \mathbb{G}$, and computes

$$Q = \sigma_S \vartheta^z,\ Z = g^z \vartheta^v,\ \Gamma = g^{zc_s}\vartheta^{cc_s} = g^{z'}\vartheta^{v'},\ Z' = g^{\tilde{z}}\vartheta^{\tilde{v}},$$

$$\Gamma' = g^{\hat{z}}\vartheta^{\hat{v}},\ \Omega = \frac{e(Q,\tilde{g})}{e(g_0,g)\cdot e(g_1,g)^{H(VP)}},\ \Omega' = e(\rho,g)^{\tilde{x}_s} \cdot e(\mathfrak{g},g)^{\tilde{v}_s} \cdot e(Q,g)^{-\tilde{c}_s} \cdot e(\vartheta,g)^{\hat{z}} \cdot e(\vartheta,\tilde{g})^{\tilde{z}},$$

$$\tilde{c}_1 = H(M_S^2||Z||Z'), \tilde{s}_1 = \tilde{z} - \tilde{c}_1 z, \tilde{s}_2 = \tilde{v} - \tilde{c}_1 v,$$

$$\tilde{c}_2 = H(M_S^2||\Gamma||\Gamma'), \hat{s}_1 = \hat{z} - \tilde{c}_2 z', \hat{s}_2 = \hat{v} - \tilde{c}_2 v',$$

$$\tilde{c}_3 = H(M_S^2||\Omega||\Omega'), \tilde{r}_1 = \tilde{x}_s - \tilde{c}_3 x_s, \tilde{r}_2 = \tilde{v}_s - \tilde{c}_3 r_s,$$

$$\tilde{r}_3 = \tilde{c}_s - \tilde{c}_3 c_s, \tilde{r}_4 = \hat{z} - \tilde{c}_3 z', \tilde{r}_5 = \tilde{z} - \tilde{c}_3 z$$

S sends $(M_S^2, Q, Z, \Gamma, Z', \Gamma', \Omega, \Omega', \tilde{c}_1, \tilde{s}_1, \tilde{s}_2, \tilde{c}_2, \hat{s}_1, \hat{s}_2, \tilde{c}_3, \tilde{r}_1, \tilde{r}_2, \tilde{r}_3, \tilde{r}_4, \tilde{r}_5)$ to U.

U verifies

$$\tilde{c}_1 \stackrel{?}{=} H(M_S^2||Z||g^{\tilde{s}_1}\vartheta^{\tilde{s}_2}Z^{\tilde{c}_1});$$

$$\tilde{c}_2 \stackrel{?}{=} H(M_S^2||\Gamma||g^{\hat{s}_1}\vartheta^{\hat{s}_2}\Gamma^{\tilde{c}_2});$$

$$\tilde{c}_3 \stackrel{?}{=} H(M_S^2||\Omega||e(\rho,g)^{\tilde{r}_1} \cdot e(\mathfrak{g},g)^{\tilde{r}_2} \cdot e(Q,g)^{-\tilde{r}_3} \cdot e(\vartheta,g)^{\tilde{r}_4} \cdot e(\vartheta,\tilde{g})^{\tilde{r}_5} \cdot \Omega^{\tilde{c}_3}).$$

The Detail of $\prod_U^2$:

U selects $d, \alpha, \beta, (\gamma_l, \tilde{\gamma}_l, \tilde{a}_l, (t_{l_i}, t'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1}, (e_j, \tilde{e}_j, \tilde{e}'_j, \check{e}_j)_{j=1}^{N_2}, \tilde{d},\ \tilde{x}_u, \tilde{r}_u, \tilde{c}_u,\ \tilde{\alpha}, \tilde{\beta}, \tilde{c}, ((\tilde{t}_{l_i}, \tilde{t}'_{l_i}, \tilde{w}_{l_i}, \tilde{w}'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1} \xleftarrow{R} \mathbb{Z}_p$ and $M_U^2 \xleftarrow{R} \mathbb{G}$, and computes

$$C = \sigma_U \vartheta^{\alpha}, D = g^{\alpha}\vartheta^{\beta}, \Phi = D^{c_u} = g^{\alpha c_u}\vartheta^{\beta c_u} = g^{\alpha'}\vartheta^{\beta'},$$

$$Y = \xi^{x_u} g_1^d, \Big(Z_l = g^{\gamma_l} h^{a_l}, Z_l' = g^{\tilde{\gamma}_l} h^{\tilde{a}_l},\ \tilde{Z}_l = g^{\tilde{\gamma}_l} \prod_{i=0}^{k-1} \tilde{h}_i^{\tilde{w}_{l_i}},$$

$$\tilde{Z}_l' = g^{\tilde{\gamma}_l} \prod_{i=0}^{k-1} \tilde{h}_i^{\tilde{w}'_{l_i}}, \big(A_{w_{l_i}} = h_{w_{l_i}}^{t_{l_i}}, A'_{w_{l_i}} = h_{w'_{l_i}}^{t'_{l_i}},$$

$$e(A_{w_{l_i}}, h)^{-w_{l_i}}, \tilde{V}_{l_i} = e(h,h)^{\tilde{t}_{l_i}} \cdot e(A_{w_{l_i}}, h)^{-\tilde{w}_{l_i}},$$

$$V'_{l_i} = e(h,h)^{t'_{l_i}} \cdot e(A'_{w_{l_i}}, h)^{-w'_{l_i}}, \tilde{V}'_{l_i} = e(h,h)^{\tilde{t}'_{l_i}} \cdot e(A'_{w_{l_i}}, h)^{-\tilde{w}'_{l_i}})_{i=0}^{k-1}\Big)_{l=1}^{N_1}, \tilde{D} = g^{\tilde{\alpha}}\vartheta^{\tilde{\beta}},$$

$$\tilde{\Phi} = D^{\tilde{c}} = g^{\tilde{\alpha}'}\vartheta^{\tilde{\beta}'}(\tilde{\alpha}' = \tilde{c}\alpha, \tilde{\beta}' = \tilde{c}\beta), \tilde{Y} = \xi^{\tilde{x}_u} g_1^{\tilde{d}},$$

$$R = \frac{e(C,\tilde{g})}{e(g_0,g)\cdot e(g_1,g)^{H(VP)}},$$

$$R' = e(\xi,g)^{\tilde{x}_u} \cdot e(\mathfrak{g},g)^{\tilde{r}_u} \cdot \prod_{l=1}^{N_1} e(\hat{g}_l, g)^{\tilde{a}_l}.$$

$$\prod_{i=1}^{N_2} e(\eta_i, g)^{\check{e}_i} \cdot e(C, g)^{-\tilde{c}_u} \cdot e(\vartheta, g)^{\tilde{\alpha}'} \cdot e(\vartheta, \tilde{g})^{\tilde{\alpha}},$$
$$\big(B_{i_j} = \eta_{i_j}^{e_i}, W_{i_j} = e(B_{i_j}, \tilde{\eta}_i), \tilde{W}_{i_j} = e(\eta, \eta_i)^{\tilde{e}_i} \cdot$$
$$e(B_{i_j}, \eta_i)^{\tilde{e}'_i}\big)_{i=1}^{N_2},$$
$$\bar{c} = H\big(M_U^2 || Y || \tilde{Y} || D || \tilde{D} || \Phi || \tilde{\Phi} || C || R || R' || Z_1 || \cdots || Z_{N_1} ||$$
$$Z'_1 || \cdots || Z'_{N_1} || B_{1_1} || \cdots || B_{1_\zeta} || \cdots || B_{N_{2_1}} || \cdots || B_{N_{2_\zeta}} ||$$
$$W_{1_1} || \cdots || W_{1_\zeta} || \cdots || W_{2_1} || \cdots || W_{N_{2_\zeta}} || \tilde{W}_{1_1} || \cdots || \tilde{W}_{1_\zeta} ||$$
$$\cdots || \tilde{W}_{N_{2_1}} || \cdots || \tilde{W}_{N_{2_\zeta}}\big),$$

$$\bar{x}_u = \tilde{x}_u - \bar{c}x_u,\ \bar{d} = \tilde{d} - \bar{c}d,\ \bar{r}_u = \tilde{r}_u - \bar{c}r_u,$$
$$(\bar{\gamma}_l = \tilde{\gamma}_l - \bar{c}\gamma_l,\ \bar{a}_l = \tilde{a}_l - \bar{c}a_l)_{l=1}^{N_1},$$
$$(\hat{e}_i = \tilde{e}_i - \bar{c}e_i,\ \hat{e}'_i = \check{e}_i - \bar{c}H(I_{i_j}),\ \hat{e}''_i = \check{e}_i + \bar{c}H(I_{i_j}))_{i=1}^{N_2},$$
$$\bar{c}_u = \tilde{c}_u - \bar{c}c_u,\ \bar{\alpha} = \tilde{\alpha} - \bar{c}\alpha, \bar{\beta} = \tilde{\beta} - \bar{c}\beta, \bar{\alpha}' = \tilde{\alpha}' - \bar{c}\alpha',$$
$$\bar{\beta}' = \tilde{\beta}' - \bar{c}\beta',$$

$$\big(\bar{e}_l = H(M_U^2 || Z_l || Z'_l || \tilde{Z}_l || \tilde{Z}'_l)(\check{\gamma}_l = \tilde{\gamma}_l - \bar{e}_l\gamma_l),$$
$$\check{a}_l = \tilde{a}_l - \bar{e}_l(a_l - c_l), \check{a}'_l = \tilde{a}_l - \bar{e}_l(a_l - d_l + q^k),$$
$$(\bar{w}_{l_i} = \tilde{w}_{l_i} - \bar{e}_l w_{l_i}, \bar{w}'_{l_i} = \tilde{w}'_{l_i} - \bar{e}_l w'_{l_i})_{i=0}^{k-1}\big)_{l=1}^{N_1},$$

$$\big((\bar{d}_{l_i} = H(M_U^2 || A_{w_{l_i}} || A'_{w_{l_i}} || V_{l_i} || V'_{l_i} || \tilde{V}_{l_i} || \tilde{V}'_{l_i}),$$
$$\bar{t}_{l_i} = \tilde{t}_{l_i} - \bar{d}_{l_i} t_{l_i}, \bar{t}'_{l_i} = \tilde{t}'_{l_i} - \bar{d}_{l_i} t'_{l_i}, \hat{w}_{l_i} = \tilde{w}_{l_i} - \bar{d}_{l_i} w_{l_i},$$
$$\hat{w}'_{l_i} = \tilde{w}'_{l_i} - \bar{d}_{l_i} w'_{l_i})_{i=0}^{k-1}\big)_{l=1}^{N_1},$$

U sends S:

$$\big(C, D, \Phi, Y, R, R', (Z_l, Z'_l, \tilde{Z}_l, \tilde{Z}'_l, (\tilde{A}_{w_{l_i}}, \tilde{A}'_{w_{l_i}}, V_{l_i}, \tilde{V}_{l_i}, V'_{l_i},$$
$$\tilde{V}'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1}, (B_{i_j}, W_{i_j}, \tilde{W}_{i_j})_{i=1}^{N_2}, \bar{c}, \bar{x}_u, \bar{d}, \bar{r}_u, \bar{c}_u, \bar{\alpha}, \bar{\beta}, \bar{\alpha}', \bar{\beta}',$$
$$(\bar{e}_l, \bar{\gamma}_l, \bar{a}_l, \check{\gamma}_l, \check{a}_l, \bar{a}'_l)_{l=1}^{N_1}, (\hat{e}_i, \hat{e}'_i)_{i=1}^{N_2}((\bar{w}_{l_i}, \bar{w}'_{l_i}, \hat{w}_{l_i}, \hat{w}'_{l_i}, \bar{d}_{l_i}, \bar{t}_{l_i},$$
$$\bar{t}'_{l_i})_{i=0}^{k-1})_{l=1}^{N_1}\big).$$

S verifies

$$\bar{c} \stackrel{?}{=} H\big(M_U^2 || Y || \xi^{\bar{x}_u} g_1^{\bar{d}} Y^{\bar{c}} || D || g^{\bar{\alpha}} \vartheta^{\bar{\beta}} D^{\bar{c}} || \Phi || g^{\bar{\alpha}'} \vartheta^{\bar{\beta}'} \Phi^{\bar{c}} || C || R ||$$
$$e(\xi, g)^{\bar{x}_u} \cdot e(\mathfrak{g}, g)^{\bar{r}_u} \cdot \prod_{l=1}^{N_1} e(\hat{g}, g)^{\bar{a}_l} \cdot \prod_{i=1}^{N_2} e(\eta_i, g)^{\hat{e}'_i} \cdot e(C, g)^{-\bar{c}_u} \cdot$$
$$e(\vartheta, g)^{\bar{\alpha}'} \cdot e(\vartheta, \tilde{g})^{\bar{\alpha}} \cdot R^{\bar{c}} || Z_1 || \cdots || Z_{N_1} || g^{\bar{\gamma}_1} h^{\bar{a}_1} Z_1^{\bar{c}} || \cdots ||$$
$$g^{\bar{\gamma}_{N_1}} h^{\bar{a}_{N_1}} Z_{N_1}^{\bar{c}} || B_{1_1} || \cdots || B_{1_\zeta} || \cdots || B_{N_{2_1}} || \cdots || B_{N_{2_\zeta}} || W_{1_1} ||$$
$$\cdots || W_{1_\zeta} || \cdots || W_{N_{2_1}} || \cdots || W_{N_{2_\zeta}} || e(\eta, \eta_1)^{\hat{e}_1} \cdot e(B_{1_1}, \eta_1)^{\hat{e}''_1} \cdot$$
$$W_{1_1}^{\bar{c}} || \cdots || e(\eta, \eta_1)^{\hat{e}_1} \cdot e(B_{1_\zeta}, \eta_1)^{\hat{e}''_1} \cdot W_{1_\zeta}^{\bar{c}} || \cdots || e(\eta, \eta_{N_2})^{\hat{e}_{N_2}} \cdot$$
$$e(B_{N_{2_1}}, \eta_{N_2})^{\hat{e}''_{N_2}} \cdot W_{N_{2_1}}^{\bar{c}} || \cdots || e(\eta, \eta_{N_2})^{\hat{e}_{N_2}} \cdot e(B_{N_{2_\zeta}}, \eta_{N_2})^{\hat{e}''_{N_2}}$$
$$\cdot W_{N_{2_\zeta}}^{\bar{c}}\big),$$

$$\big(\bar{e}_l = H\big(M_U^2 || Z_l || g_l^{\check{\gamma}_l} h^{\check{a}_l} (Z_l h^{-c_l})^{\bar{e}_l} || g^{\check{\gamma}_l} \prod_{i=0}^{k-1} \tilde{h}_i^{\bar{w}_{l_i}} (Z_l h^{-c_l})^{\bar{e}_l} ||$$
$$g^{\check{\gamma}_l} \prod_{i=0}^{k-1} \tilde{h}_i^{\bar{w}'_{l_i}} (Z_l h^{-d_1 + q^k})^{\bar{e}_l})\big)_{l=1}^{N_1},$$

$$\Big(\big(\bar{d}_{l_i} = H(M_U^2 || A_{w_{l_i}} || A'_{w_{l_i}} || V_{l_i} || V'_{l_i} || e(h, h)^{\bar{t}_{l_i}} \cdot e(A_{w_{l_i}}, h)^{-\hat{w}_{l_i}} \cdot$$
$$V_{l_i}^{\bar{d}_{l_i}} || e(h, h)^{\bar{t}'_{l_i}} \cdot e(A'_{w_{l_i}}, h)^{-\hat{w}'_{l_i}} \cdot (V'_{l_i})^{\bar{d}_{l_i}})\big)_{i=0}^{k-1}\Big)_{l=1}^{N_1}$$

The Detail of $\prod_U^3$:

U selects $\pi, \lambda, \tilde{x}_u, \tilde{s}_u, \tilde{\pi}, \tilde{\pi}', \tilde{\lambda}', \tilde{\omega}_u, \tilde{d}_u \xleftarrow{R} \mathbb{Z}_p$ and $M_U^3 \xleftarrow{R} \mathbb{G}$, and computes

$$D = g^{s_u}, \tilde{D} = g^{\tilde{s}_u}, E = \xi^{x_u} H'(ID_V)^{rs_u}, \tilde{E} = \xi^{\tilde{x}_u} H(ID_V)^{r\tilde{s}_u},$$
$$F = T_U \vartheta^{\pi}, J = g^{\pi} \vartheta^{\lambda}, \tilde{J} = g^{\tilde{\pi}} \vartheta^{\tilde{\lambda}}, J' = J^{\omega_u} = g^{\pi\omega_u} \vartheta^{\lambda\omega_u},$$
$$\tilde{J}' = J^{\tilde{\omega}_u} = g^{\pi\tilde{\omega}_u} \vartheta^{\lambda\tilde{\omega}_u}, R = \frac{e(F, Y_S)}{e(g_0, \rho) e(g_3, \rho)^{\psi_u}},\ \tilde{R} = e(\xi, \rho)^{\tilde{x}_u} \cdot$$
$$e(g_1, \rho)^{\tilde{d}_u} \cdot e(g_2, \rho)^{\tilde{s}_u} \cdot e(F, \rho)^{-\tilde{\omega}_u} \cdot e(\vartheta, \rho)^{\tilde{\pi}'} \cdot e(\vartheta, Y_S)^{\tilde{\pi}},$$

$$c \stackrel{?}{=} H(M_U^3 || D || E || J || J' || R || \tilde{D} || \tilde{E} || \tilde{J} || \tilde{J}' || R'),$$
$$\bar{s}_u = \tilde{s}_u - cs_u, \bar{x}_u = \tilde{x}_u - cx_u, \hat{s}_u = r\tilde{s}_u - crs_u, \bar{\pi} = \tilde{\pi} - c\pi,$$
$$\bar{\lambda} = \tilde{\lambda} - c\lambda,\ \bar{\omega}_u = \tilde{\omega}_u - c\omega_u,\ \bar{\pi}' = \tilde{\pi}' - c\pi\omega_u \text{ and}$$
$$\bar{d}_u = \tilde{d}_u - cd_u.$$

U sends $(\mathbb{P}_U,\ Price,\ Service,\ VP,\ M^3,\ D,\ E,\ F, J,\ J',\ R,$ $c, \bar{s}_u, \bar{x}_u, \hat{s}_u, \bar{\pi},\ \bar{\lambda}, \bar{\omega}_u, \bar{\pi}', \bar{d}_u)$ to V.

V verifies

$$\psi_u \stackrel{?}{=} H(\mathbb{P}_U || Price || Services || VP),\ R \stackrel{?}{=} \frac{e(F, Y_S)}{e(g_0, \rho) \cdot e(g_3, \rho)^{\psi_u}}$$

and

$$c \stackrel{?}{=} H\big(M_U^3 || D || E || J || J' || R || g^{\bar{s}_u} D^c || \xi^{\bar{x}_u} H'(ID_V)^{\hat{s}_u} E^c || g^{\bar{\pi}} \vartheta^{\bar{\lambda}} J^c$$
$$|| J^{\bar{\omega}_u} J'^c || e(\xi, \rho)^{\bar{x}_u} \cdot e(g_1, \rho)^{\bar{d}_u} \cdot e(g_2, \rho)^{\bar{s}_u} \cdot e(F, \rho)^{-\bar{\omega}_u} \cdot e(\vartheta, \rho)^{\bar{\pi}'} \cdot$$
$$e(\vartheta, Y_S)^{\bar{\pi}} R^c\big).$$