Anonymously Transferable Constant-Size E-Tickets

Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud

École normale supérieure, LIENS - CNRS - INRIA, Paris, France
http://www.di.ens.fr/{~fuchsbau,~pointche,~vergnaud}

Abstract. We propose a new blind certification protocol that provides interesting properties while remaining efficient. It falls in the Groth-Sahai framework for WI proofs, thus extended to a certified signature it immediately yields non-frameable group signatures. We then use it to build an e-ticketing system that guarantees anonymity of users and transferability of tickets without increasing their size. In case of abuse, anonymity can be revoked by an authority, which is crucial to prevent double-spending.

1 Introduction

1.1 Motivation

The issue of anonymity in electronic transactions was introduced for e-cash and e-mail in the early 1980's by Chaum, with the famous primitive of blind signatures [Cha83,Cha84]: a signer accepts to sign a message, without knowing the message itself, and without being able to later link the message-signature pair to the transaction it originated from. In e-cash systems, the message is a serial number to make a coin unique. The main security property is resistance to "one-more forgeries" [PS00], which guarantees the signer that after t transactions a user cannot have more than t valid signatures.

Blind signatures have thereafter been widely used for many variants of e-cash systems; in particular *fair* blind signatures [SPC95], which allow to provide revocable anonymity. They deter from abuse since in such a case the signer can ask an authority to reveal the identity of the defrauder. In order to allow the signer to control some part of the message to be signed, *partially* blind signatures [AO00] have been proposed.

Another important primitive for anonymity are group signatures [Cv91], enabling a user to sign as a member of a group without leaking any more information about his identity. Strong security models have been defined [BMW03,BSZ05], considering dynamic groups in which the group manager is not fully trusted: one thus requires that the latter cannot frame honest users.

For e-cash systems, the classical scenario is between a bank, a user and a merchant/shop: the user withdraws money from the bank and can then spend it in a shop. The latter must deposit it at the bank to get its account credited. Literature tries to improve the withdrawal and the spending processes, e.g. with divisible e-cash [EO94,CG07]. However, for many applications, such as e-tickets or coupons [NHS99], transferability [OO90,OO92] is a more important property. It is known that the size of coins grows linearly in the number of transfers [CP92], a drawback we will avoid in our construction.

1.2 Contributions

Our first result is the definition and efficient pairing-based instantiation of a new primitive, which we call *partially-blind certification*. A protocol allows an issuer to interactively issue a *certificate* to a user, of which parts are then only known to the user and cannot be associated to a particular protocol execution by the issuer. The certificates are unforgeable in that from q runs of the protocol with the issuer cannot be derived more than q valid certificates. We then give two applications of the primitive:

- In order to achieve unlinkability in group signatures, a common approach is the following: Using a signing key provided by the group manager, a user produces a signature, encrypts it and adds proofs for its validity. For this method to work efficiently in the standard model, these signing keys have to be constructed carefully. In [BW07] for example, it is the group manager that constructs the entire signing key—which means that he can impersonate (*frame*) users.

Groth [Gro07] achieves *non-frameability* by using *certified signatures* [BFPW07]: The user chooses a verification key which is signed by the issuer. A signature produced with the corresponding signing key together with the verification key and the issuer's signature on it can then be verified under the issuer's key. Security of his instantiation however relies on an unnatural assumption. We avoid this by noting the following: it is not necessary that the user choose the verification key, as long as he can be sure that the private key contains enough entropy. Since the blind component of our certificates can serve as signing key, our construction applies immediately to build non-frameable group signatures (see Sect. 4).
- Second, in e-cash, the serial number of a coin needs to contain enough entropy to avoid collisions, but again the user need not control it entirely. Partially-blind certificates are applicable here too.

1.3 Constant-Size Transferable Anonymous E-Cash

The instantiation we give of our new primitive allows it to be combined with the results of Groth and Sahai [GS08], which is crucial to our main contribution: an efficient standard-model anonymous e-cash system (we will rather speak of tickets than coins) in the classical three-party scenario with novel features. First, the tickets are transferable while remaining constant in size. We achieve this by using a new method to trace double spenders: we have the users keep *receipts* when receiving tickets instead of storing all information about transfers inside the ticket itself.[1]

Second, partial blindness of our certificates provides strong notions of anonymity: a user remains anonymous even w.r.t. to an entity issuing tickets *and* able to detect double spendings. Moreover, tickets are unlinkable to anyone except—of course—the authority that checks for double-spendings. We give an overview of the system before getting back to its security properties.

- The participants of the system are the following: the group manager (that registers members within the system), the issuer (generating tickets), users (that buy, sell or spend tickets), providers of the service the tickets are issued for, the double-spending detector, and an opener to reveal the identity of double-spenders.[2]
- In order to buy a ticket, a user runs a protocol with the issuer, after which she holds a ticket and a receipt to be kept even after selling or spending the ticket (to defend herself against wrongful accusation of double-spending).[3]
- Another protocol allows users to sell tickets to other users who, besides the ticket, also get a receipt, which they keep too.
- To spend the ticket, the user interacts with a service provider. The latter will then give the ticket to the double-spending detector, who checks if it had already been spent. If this is the case, the opener traces back the ticket via the receipts in order to reveal the double spender.

The system satisfies the following security notions:

- Any user who spends a ticket twice is detected.
- As long as a user keeps all his receipts, he cannot not be wrongfully accused of double spending, even if everyone else colludes against him.
- As long as a received ticket was not spent twice, a user remains anonymous even against collusions of the manager, the issuer, the double-spending detector, service providers, and other users.
- Transfers of tickets are unlinkably anonymous to collusions possibly comprising the manager, the issuer, service providers, and other users.

[1] The amount of data a user has to deal with is thus proportional to the number of tickets he bought, rather than the path a ticket took until reaching the user.

[2] The opener might also detect double spendings; we separate the roles nonetheless in order to enable a company implementing an e-ticketing system to check for double spendings itself and only ask the opening authority to trace if a fraud was detected. Moreover, in an implementation, a company will impersonate various protagonists at once. We separate them to generalize the model and provide stronger security guarantees.

[3] If one assumes a validity period for tickets (after which the issuing key is changed), it suffices to keep a receipt only as long as the respective ticket is valid.

Our construction is secure in the standard security model (i.e., without relying on the random oracle idealization [BR93])[4] and its security is based on a new (though very natural) assumption that holds in the generic group model [Sho97].

1.4 Organization of the Paper

In the next section, we state the employed assumptions. In Sect. 3, we describe our new *Partially-Blind Certification* primitive, and apply it to group signatures in Sect. 4. In Sect. 5, we extend some techniques of Groth-Sahai, introducing re-randomization of encryptions and proofs for relations of encryptions under different keys. In Sect. 6, we combine everything to construct our e-ticketing system.

2 Assumptions

We present the assumptions on bilinear groups on which our security results build. A *bilinear group* is a tuple $(p, \mathbb{G}, \mathbb{G}_T, e, G)$ where $(\mathbb{G}, +)$ and $(\mathbb{G}_T, \cdot)$ are two cyclic groups of order p, G is a generator of $\mathbb{G}$, and $e\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate bilinear map: $\forall\, U, V \in \mathbb{G}\ \forall\, a, b \in \mathbb{Z}\colon\ e(aU, bV) = e(U, V)^{ab}$, and $e(G, G)$ is a generator of $\mathbb{G}_T$.

The first two of the following assumptions are classical [DH76,BBS04]. The third is a simple extension of the Hidden Strong Diffie-Hellman Problem proposed by Boyen and Waters in [BW07].

Definition 1. *The* Computational Diffie-Hellman (CDH) Assumption *states that the following problem is intractable:*[5] *given* $(G, \alpha G, \beta G) \in \mathbb{G}^3$*, for* $\alpha, \beta \in \mathbb{Z}_p$*, output* $\alpha\beta G$*.*

Definition 2. *The* Decisional Linear (DLIN) Assumption *states that the following problem is intractable: given* $(U, V, G, \alpha U, \beta V, \gamma G) \in \mathbb{G}^5$*, decide whether* $\gamma = \alpha + \beta$ *or not.*

Definition 3. *The* q-Double Hidden Strong Diffie-Hellman (DHSDH) Assumption *states that the following problem is intractable: given* $(G, H, K, \Gamma = \gamma G) \in \mathbb{G}^4$ *and* $q - 1$ *tuples*

$$\big(X_i = x_i G,\ X_i' = x_i H,\ Y_i = y_i G,\ Y_i' = y_i H,\ A_i = \tfrac{1}{\gamma + x_i}(K + y_i G)\big) \qquad \text{for } x_i, y_i \leftarrow \mathbb{Z}_p^*$$

for $i = 1, \ldots, q-1$*, output a new tuple* $\big(X = xG,\ X' = xH,\ Y = yG,\ Y' = yH,\ A = \tfrac{1}{\gamma + x}(K + yG)\big)$.

Note that a tuple (X, X', Y, Y', A) has the above format if and only if it satisfies

$$e(X, H) = e(G, X') \qquad e(Y, H) = e(G, Y') \qquad e(A, \Gamma + X) = e(K + Y, G)$$

Remark 4. Boneh and Boyen [BB04] introduce the Strong Diffie-Hellman (SDH) assumption in bilinear groups that states that given a $(q+1)$-tuple $(G, \gamma G, \gamma^2 G, \ldots, \gamma^q G) \in \mathbb{G}^{q+1}$ for a random $\gamma \in \mathbb{Z}_p^*$, it is infeasible to output a pair $(x, \frac{1}{\gamma + x} G) \in \mathbb{Z}_p \times \mathbb{G}$. Hardness of SDH implies hardness of the following two problems (the first implication is proven in [BB04], the second in Appendix B):

(I) Given $G, \gamma G \in \mathbb{G}$ and $q - 1$ distinct pairs $(x_i, \frac{1}{\gamma + x_i} G) \in \mathbb{Z}_p \times \mathbb{G}$, output a *new* pair $(x, \frac{1}{\gamma + x} G) \in \mathbb{Z}_p \times \mathbb{G}$.

(II) Given $G, K, \gamma G \in \mathbb{G}$ and $q - 1$ distinct triples $\big(x_i, y_i, \frac{1}{\gamma + x_i}(K + y_i G)\big) \in \mathbb{Z}_p^2 \times \mathbb{G}$, output a *new* triple $\big(x, y, \frac{1}{\gamma + x}(K + yG)\big) \in \mathbb{Z}_p^2 \times \mathbb{G}$.

The Hidden SDH problem defined in [BW07] is a variant of Problem (I), where instead of giving the x_i's explicitly, they are given as $(x_i G, x_i H)$. Similarly, the goal is to output a new triple $(xG, xH, \frac{1}{\gamma + x} G)$. Now the Double Hidden SDH assumption (Definition 3) transforms Problem (II) the same way: instead of being given explicitly, x_i and y_i are given as $(x_i G, x_i H, y_i G, y_i H)$. See Appendix A for a discussion on the various assumptions derived from SDH and their relations.

[4] Note that in our context, due to re-randomization of encryptions (cf. Sect. 6.2 for details), it seems even impossible to replace the Groth-Sahai techniques with the Fiat-Shamir heuristic [FS87] to improve efficiency at the expense of relying on the random oracle model.

[5] We say that a computational problem is *intractable* if no probabilistic polynomial-time (p.p.t.) adversary can solve it with non-negligible probability. A decisional problem is *intractable* if no p.p.t. adversary can decide it with probability of non-negligibly more than $1/2$.

Experiment $\mathsf{Exp}^{\mathsf{blindness}-b}_{\mathsf{Sign}^*}(k)$
$(pk, info) \leftarrow \mathsf{Sign}^*(\mathtt{FIND}, k)$
$\sigma_0\ (\neq\perp) \leftarrow \mathsf{User}^{\mathsf{Sign}^*}(info, pk)$
$\sigma_1\ (\neq\perp) \leftarrow \mathsf{User}^{\mathsf{Sign}^*}(info, pk)$
$b' \leftarrow \mathsf{Sign}^*(\mathtt{GUESS}, \sigma_b)$
`RETURN` b'

(1) Partial Blindness

Experiment $\mathsf{Exp}^{\mathsf{forge}}_{\mathsf{User}^*}(k)$
$(pk, sk) \leftarrow \mathsf{Setup}(k)$
$(info, \sigma_1, \ldots, \sigma_\ell) \leftarrow \mathsf{User}^{*\mathsf{Sign}(sk,\cdot)}(pk)$
`IF` $\forall i \in \{1, \ldots, \ell\}, \mathsf{Verif}(pk, info, \sigma_i) =$ `accept`
`AND` $\ell > \ell_{info}$ `RETURN` 1

where ℓ_{info} is the number of executions of the certificate issuing protocol where Sign outputs `completed`, given *info* as input.

(2) Unforgeability

Fig. 1. Security experiments for partially-blind certificates

3 Partially-Blind Certification

3.1 Model

Definition 5. *A* partially-blind certification scheme *is a 4-tuple* $(\mathsf{Setup}, \mathsf{Sign}, \mathsf{User}, \mathsf{Verif})$ *of (interactive) probabilistic polynomial-time Turing machines (PPTs) such that:*

- Setup *is a PPT that takes as input an integer* k *and outputs a pair* (pk, sk) *of* public *(resp.* secret*)* key*.* k *is called the* security parameter*.*
- Sign *and* User *are interactive PPTs such that* User *takes as inputs a public key* pk *and a bit string* $info$ *and* Sign *takes as input a matching secret key* sk *and* $info$*.* Sign *and* User *engage in the* certificate issuing protocol *and when they stop,* Sign *outputs* `completed` *or* `not-completed` *while* User *outputs* $\perp$ *or a bit-string* σ*.*
- Verif *is a deterministic polynomial-time Turing machine that on input a public key* pk *and a pair of bit strings* $(info, \sigma)$ *outputs either* `accept` *or* `reject`*.*

For all $k \in \mathbb{N}$*, all pairs* (pk, sk) *output by* $\mathsf{Setup}(k)$*, if* Sign *and* User *follow the certification issuing protocol with input* $(sk, info)$ *and* $(pk, info)$ *respectively, then* Sign *outputs* `completed` *and* User *outputs a bit string* σ *that satisfies* $\mathsf{Verif}(pk, info, \sigma) =$ `accept`*.*
A pair $(info, \sigma)$ *is termed* valid with regard to pk *if on input* $(pk, info, \sigma)$ Verif *to output* `accept`*, in which case, we say that* σ *is a* certificate *for* pk *with* common information *info.*

Partial Blindness. To define partial blindness, we consider the game (i.e., random experiment) among an adversarial signer Sign^* and two honest users User_0 and User_1 presented in Figure 1 (1).

- We define the advantage of Sign^* in breaking partial blindness by its advantage in distinguishing the two above experiments (with $b = 0$ or $b = 1$):

$$\mathsf{Adv}^{\mathsf{blindness}}_{\mathsf{Sign}^*}(k) \ := \ \Pr[\mathsf{Exp}^{\mathsf{blindness}-1}_{\mathsf{Sign}^*}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{blindness}-0}_{\mathsf{Sign}^*}(k) = 1] \ ,$$

  where the probability is taken over the coin tosses made by User_0, User_1 and Sign^*.
- The scheme $(\mathsf{Setup}, \mathsf{Sign}, \mathsf{User}, \mathsf{Verif})$ is said to be *partially blind* if no adversary Sign^* running in probabilistic polynomial time has a non-negligible advantage $\mathbf{Adv}^{\mathsf{blindness}}_{\mathsf{Sign}^*}$.

Unforgeability. To define unforgeability, we introduce the game among an adversarial user User^* and an honest signer Sign presented in Figure 1 (2).

- We define the *success* of User^* in this game by $\mathbf{Succ}^{\mathsf{unforge}}_{\mathsf{User}^*}(k) := \Pr[\mathsf{Exp}^{\mathsf{forge}}_{\mathsf{User}^*}(k) = 1]$, where the probability is taken over the coin tosses made by User^*, Setup and Sign.
- The scheme $(\mathsf{Setup}, \mathsf{Sign}, \mathsf{User}, \mathsf{Verif})$ is said to be *unforgeable* if no adversary User^* running in probabilistic polynomial time has a non-negligible success $\mathbf{Succ}^{\mathsf{unforge}}_{\mathsf{User}^*}$.

Remark 6. In the random experiment $\mathsf{Exp}^{\mathsf{forge}}_{\mathsf{User}^*}$, depending on the security model, the executions of the certificate issuing protocol are run sequentially or in a concurrent and interleaving way.

Let Com be commitments to elements in $\mathbb{Z}_p$ (cf. Remark 7)

(1) User Choose $r, y_1 \leftarrow \mathbb{Z}_p$, compute and send

$$C_r = \mathsf{Com}(r), \quad C_y = \mathsf{Com}(y_1), \quad R_1 := r(K + y_1 G), \quad T := rG$$

and zero-knowledge proofs of knowledge of r and y_1 satisfying the relations.

(2) Sign Choose $y_2, x \leftarrow \mathbb{Z}_p$ and compute $R := R_1 + y_2 T$ (note that $R = r(K + yG)$ with $y := y_1 + y_2$.)

Send $\left(S_1 := \frac{1}{\gamma + x} R,\ S_2 := xG,\ S_3 := xH,\ S_4 := y_2 G,\ S_5 := y_2 H\right)$

(3) User Check that S is correctly formed:

$$e(S_1, \Gamma + S_2) \stackrel{?}{=} e(R, G) \qquad e(S_2, H) \stackrel{?}{=} e(G, S_3) \qquad e(S_4, H) \stackrel{?}{=} e(G, S_5)$$

If so, compute a certificate

$$\left(A := \tfrac{1}{r} S_1,\ X := S_2,\ X' := S_3,\ Y := y_1 G + S_4 = yG,\ Y' := y_1 H + S_5 = yH\right)$$

Fig. 2. Partially-blind certificate-creation protocol.

3.2 Instantiation

Let $G, H, K \in \mathbb{G}$ be public parameters, define the signer's key pair as $sk := \omega \in \mathbb{Z}_p$ and $pk = \Omega := \omega G$. A certificate on common information $info = x \in \mathbb{Z}_n$, is defined as

$$\mathsf{Crt}(\omega, x, y) \ := \ \left\{ A = \frac{1}{\omega + x}(K + yG) \qquad \begin{array}{ll} X = xG & Y = yG \\ X' = xH & Y' = yH \end{array} \right.$$

for $y \leftarrow \mathbb{Z}_p$. It satisfies:

$$e(X, H) = e(G, X') \qquad e(Y, H) = e(G, Y') \qquad e(A, \Omega + X) = e(K + Y, G) \tag{1}$$

Figure 2 depicts an efficient protocol to interactively generate such a certificate on common information $info = x$ between the signer (issuer) and the user that partially controls y: at the end, the signer has no information about y, except that it is uniformly distributed.

Remark 7. In the first round of the User protocol, one can either use interactive Schnorr-like zero-knowledge proofs [Sch90] together with Pedersen's commitments. Then extraction is only possible for constant-depth concurrency [Oka06]. If one wants full concurrency, Linear commitments (which are extractable) and the GOS technique [GOS06] can be used for the non-interactive zero-knowledge proofs.

3.3 Security Results

Theorem 8. *Under the DHSDH assumption, the above certificates are unforgeable.*

Proof. Let User^* be an adversary impersonating corrupt users running up to $q - 1$ times the issuing protocol and then outputting q different valid certificates. We build $\mathcal{B}$ solving q-DHSDH with the same probability by simulating the signer: $\mathcal{B}$ gets a q-DHSDH-instance $\left(G, H, K, \Gamma, (A_i, X_i, X'_i, Y_i, Y'_i)_{i=1}^{q-1}\right)$. It sets the public parameters so that it can extract r and y_1 used in R_1 and T from the commitments (or it rewinds User^* in case we use interactive zero-knowledge proofs). In each issuing, User^* first sends $(C_{r,i}, C_{y,i}, R_{1,i}, T_i)$ and proofs of correctness. If the proofs are correct, $\mathcal{B}$ extracts r_i, $y_{1,i}$ from $C_{r,i}$, $C_{y,i}$, resp., and sends $\left(S_{1,i} := r_i A_i,\ S_{2,i} := X_i,\ S_{3,i} := X'_i,\ S_{4,i} := Y_i - y_{1,i} G,\ S_{5,i} := Y'_i - y_{2,i} H\right)$. Finally, $\mathcal{B}$ checks the q certificates and forwards any one different from the ones from the DHSDH-instance to its own challenger. □

Theorem 9. *Under the DLIN assumption, the above certificates are partially blind.*

Proof. Consider Sign^*, which after two executions of the blind issuing protocol can decide to which one a given Y' corresponds. We build $\mathcal{B}$ deciding DLIN with half of the success probability of Sign^*.

$\mathcal{B}$ gets a DLIN-instance (H, G, T, Z, K, R_1), i.e., it has to decide whether

$$R_1 \stackrel{?}{=} (\log_H Z + \log_G K)\, T \tag{2}$$

It gives Sign^* the triple (G, H, K) as public parameters and a perfectly hiding key for Com and gets Γ, the issuer's public key from Sign^*. Next, $\mathcal{B}$ flips a coin $b \leftarrow \{0, 1\}$ and simulates two users running the issuing protocol. The simulation of user $(1-b)$ is honest, whereas the simulation of user b is performed by sending:

- random values for C_r and C_y and simulated proofs of correctness
- R_1 and T from its DLIN instance

After getting back $S = (S_1, \ldots, S_5)$ in this bth run, $\mathcal{B}$ checks its correctness and gives Sign^* the following: $Y' := Z + S_5$ with Z from its DLIN instance. Finally Sign^* outputs a guess b' and $\mathcal{B}$ returns 1 iff $b = b'$. Note that $\mathcal{B}$ can verify correctness of S without knowledge of y_1 and r by checking $e(S_1, \Gamma + S_2) = e(R, G)$, $e(S_2, H) = e(G, S_3)$, and $(S_4, H) = e(G, S_5)$.

- If the instance was not a linear tuple then Z is independently random, so Sign^*'s success probability is $1/2$.
- If (H, G, T, Z, K, R_1) is linear, then with $y_1 = \log_H Z$, $\kappa = \log_G K$, and $r = \log_G T$, we have $R_1 = (y_1 + \kappa)T$ by (2). Furthermore, for public parameters (G, H, K), we have

  $$T = rG \qquad R_1 = (y_1 + \kappa)T = (y_1 + \kappa)rG = r(K + y_1 G) \qquad Z = y_1 H$$

  which means that $Y' = Z + S_5$ is the last component of a correctly produced certificate from run b. Sign^* outputs $b' = b$ thus with its success probability in the blindness game. □

4 A Fully-Secure Group Signature from Partially-Blind Certificates

As a first application of the certification protocol from Sect. 3.2, we show how to construct *fully-secure* dynamic group signatures (in the sense of [BSZ05], in particular satisfying non-frameability and CCA-anonymity) without random oracles.

We construct a *certified-signature* scheme, to which can then be applied Groth's [Gro07] methodology of transforming certified signatures into group signatures using Groth-Sahai NIZK [GS08] and Kiltz' tag-based encryption [Kil06], both relying exclusively on the DLIN assumption.

The resulting scheme is less efficient than that from [Gro07]; however, it is based on a more natural assumption, while at the same time being of the same order of magnitude—especially compared to the first instantiations of fully-secure signatures in the standard model (e.g., [Gro06]). We think of the scheme as somehow being the "natural" extension of [BW07] in order to satisfy non-frameability.

Certified Signature. Our certified signature is constructed from a certificate (A, X, X', Y, Y') by using (Y, Y') as a pair of public and secret key for Waters' signature scheme [Wat05]. A certified signature consists thus of the first four components of the certificate prepended to a Waters signature. Note that what is called *cert* in [Gro], corresponds to (A, X, X') here, and (vk, sk) would be (Y, Y'). The scheme is given in Fig. 3.

Groth [Gro07] gives several security criteria that a certified signature has to satisfy in order to be transformable into a secure group signature scheme. We show that our construction satisfies them.

Theorem 10. *The certified-signature scheme in Fig. 3 is perfectly correct, unfakeable under the DHSDH assumption, and existentially unforgeable under chosen-message attack under the CDH assumption.*

Let $(U_i)_{i=0}^n \in \mathbb{G}^{n+1}$ be part of the public parameters; let Ω be the issuer's public key.

Certificate Generation. Run the blind issuing protocol in Fig. 2, except that the authority sends a commitment of $S_4 = y_2 G$ before phase (1) and opens it in phase (2).

Signing. For a message $M = (m_1, \ldots, m_n) \in \{0,1\}^n$, denote $\mathcal{F}(M) := U_0 + \sum_{i=1}^n m_i U_i$. Given a certificate $C = (A, X, X', Y, Y')$, a signature on M using randomness $s \in \mathbb{Z}_p$ is defined as

$$\mathsf{Sig}(C, M\,;\, s) \;:=\; (A, X, X', Y, Y' + s\mathcal{F}(M), -sG) \;.$$

Verification. A certified signature (A, X, X', Y, Z, Z') on message M is verified by checking

$$e(X,H) = e(G,X') \qquad e(Y,H) = e(G,Z)\, e(Z', \mathcal{F}(M)) \qquad e(A, \Omega + X) = e(K + Y, G)$$

Fig. 3. Chosen-message secure certified signature

Proof. (1) Unfakeability means that after running various instances of the issuing protocol with the issuer, no user is able to produce a valid tuple (A, X, X', Y, Z, Z') with a Y different from the obtained certificates. The proof works similarly to that of Theorem 8 with the following modifications: $\mathcal{B}$ chooses $\mu_i \leftarrow \mathbb{Z}_p$ and sets the public parameters $U_i := \mu_i G$ for $0 \le i \le n$. In the issuing protocol, $\mathcal{B}$ simulates the additional commitment at the beginning. From a valid (A, X, X', Y, Z, Z') returned by $\mathcal{A}$, $\mathcal{B}$ can then extract a new certificate by setting $Y' := Z + (\mu_0 + \sum m_i \mu_i) Z'$.

(2) Existential unforgeability under chosen-message attack (EUF-CMA) follows from partial blindness of certificates and security of Waters-signatures, which is implied by CDH (Def. 1): Let $\mathcal{A}$ be an adversary impersonating the issuer and mounting a chosen-message attack. We construct $\mathcal{B}$ against EUF-CMA of Waters-signatures. $\mathcal{B}$ is given a Waters public key V. When $\mathcal{A}$ sends a commitment to S_4 in the first phase of certificate generation, $\mathcal{B}$ extracts S_4 from it. It then chooses r and sends C_r, C_y (perfectly hiding), $R_1 := r(K + V - S_4)$, and $T := rG$. If $\mathcal{A}$ returns a valid tuple, $\mathcal{B}$ can compute an (incomplete) certificate $(A := \frac{1}{r} S_1,\ X := S_2, X' := S_3, Y := V)$ which suffices to answer the signing queries, as $\mathcal{B}$ can get the last two components by querying its own oracle. When $\mathcal{A}$ returns a successful forgery, $\mathcal{B}$ returns the last two components to its own challenger. □

5 New Techniques For Groth-Sahai Proof Systems

5.1 Preliminaries

We briefly review the relevant parts of [GS08]: Witness-indistinguishable (WI) proofs that elements in $\mathbb{G}$ that were committed to via *linear commitments* satisfy *pairing-product equations*. We refer to the original work for more details and proofs.

Let $P \in \mathbb{G}$ be a generator. We define a key for *linear commitments*. Choose $\alpha, \beta, r_1, r_2, r_3 \in \mathbb{Z}_p$ and define $U = \alpha P$, $V = \beta P$, and

$$\mathbf{u}_1 := (U, 0, P) \qquad \mathbf{u}_2 := (0, V, P) \qquad \mathbf{u}_3 := (W_1, W_2, W_3) \tag{3}$$

where $W_1 := r_1 U$, $W_2 := r_2 V$, for random $r_1, r_2 \leftarrow \mathbb{Z}_p$, and W_3 is either

- soundness setting: $W_3 := (r_1 + r_2) P$
- witness indistinguishable setting: $W_3 := (r_1 + r_2 - 1) P$

A commitment to a group element $X \in \mathbb{G}$ under commitment key $ck = (U, V, W_1, W_2, W_3)$ using randomness $(s_1, s_2, s_3) \leftarrow \mathbb{Z}_p^3$ is defined as (with $\iota(X) := (0, 0, X)$)

$$\mathsf{Com}(ck, X;\, s_1, s_2, s_3) := \iota(X) + \sum_{i=1}^{3} s_i \mathbf{u}_i = (s_1 U + s_3 W_1,\ s_2 V + s_3 W_2,\ X + s_1 P + s_2 P + s_3 W_3) \;.$$

Note that in the soundness setting, given the *extraction key* $ek := (\alpha, \beta)$, one can extract the committed value from a commitment $\mathbf{c} = (c_1, c_2, c_3)$:

$$\begin{aligned}\mathsf{Extr}((\alpha,\beta),\mathbf{c}) &:= c_3 - \tfrac{1}{\alpha}c_1 - \tfrac{1}{\beta}c_2 \\ &= X + (s_1 + s_2 + s_3(r_1+r_2))P - \tfrac{1}{\alpha}(s_1 + s_3 r_1)U - \tfrac{1}{\beta}(s_2 + s_3 r_2)V) = X \ ,\end{aligned}$$

since $\frac{1}{\alpha}U = P$ and $\frac{1}{\beta}V = P$. On the other hand, in the WI setting we have (with $s_1' := s_1 + s_3 r_1$ and $s_2' = s_2 + s_3 r_2$): $\mathbf{c} = (s_1' U, s_2' V, X + (s_1' + s_2' - s_3)P)$, which is equally distributed for every X. The two settings are indistinguishable by DLIN since for soundness (W_1, W_2, W_3) is an encryption of 0, whereas in the WI setting it encrypts $-P$.

For the sake of readability and consistency with the original work, we stick to the abstract notation from [GS08], which we sketch briefly:

- For a vector $\vec{\mathcal{X}} = (\mathcal{X}_1, \ldots, \mathcal{X}_n)^\top \in \mathbb{G}^n$, let $\vec{\mathcal{X}} \cdot \vec{\mathcal{Y}} := \prod_{i=1}^n e(\mathcal{X}_i, \mathcal{Y}_i)$.
- Bold letters denote triples, e.g., $\mathbf{d} = (d_1, d_2, d_3) \in \mathbb{G}^{1\times 3}$, $\vec{\mathbf{d}}$ denotes a column vector of triples, thus a matrix in $\mathbb{G}^{n\times 3}$. Furthermore, define $\widetilde{F}(\mathbf{c}, \mathbf{d}) := \big[e(c_i, d_j)\big]_{i,j=1,3} \in \mathbb{G}_T^{3\times 3}$. In $\mathbb{G}_T^{n\times 3}$, "+" denotes entry-wise multiplication of matrix elements. Define $\mathbf{c} \bullet \mathbf{d} := \sum_{i=1}^n \big(\tfrac{1}{2}\widetilde{F}(c_i, d_i) + \tfrac{1}{2}\widetilde{F}(d_i, c_i)\big)$.

A *pairing-product equation* is an equation for variables $\mathcal{Y}_1, \ldots, \mathcal{Y}_n \in \mathbb{G}$ of the form

$$\prod_{i=1}^n e(\mathcal{A}_i, \mathcal{Y}_i) \prod_{i=1}^n \prod_{j=1}^n e(\mathcal{Y}_i, \mathcal{Y}_j)^{\gamma_{i,j}} \ = \ t_T \ ,$$

with $\mathcal{A}_i \in \mathbb{G}$, $\gamma_{i,j} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$. Setting $\Gamma := \big[\gamma_{i,j}\big]_{i,j=1,\ldots,n} \in \mathbb{Z}_p^{n\times n}$, this can be written as

$$(\vec{\mathcal{A}} \cdot \vec{\mathcal{Y}})\,(\vec{\mathcal{Y}} \cdot \Gamma\vec{\mathcal{Y}}) \ = \ t_T \ . \tag{4}$$

Define $H_1 := \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $H_2 := \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}$, $H_3 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$, and for $t_T \in \mathbb{G}_T$, let $\iota_T(t_T) := \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & t_T \end{bmatrix}$.

Let $\vec{\mathbf{d}}$ be a vector of commitments to $\vec{\mathcal{Y}}$, i.e., $\vec{\mathbf{d}} := \iota(\vec{\mathcal{Y}}) + S\vec{\mathbf{u}}$ with $S \leftarrow \mathbb{Z}_p^{n\times 3}$ and $\iota(\vec{\mathcal{Y}}) := [\iota(\mathcal{Y}_i)]_{i=1,\ldots,n}$. The proof that the committed values satisfy (4) is defined as

$$\Phi \ := \ S^\top \iota(\vec{\mathcal{A}}) + S^\top \Gamma \iota(\vec{\mathcal{Y}}) + S^\top \Gamma^\top \iota(\vec{\mathcal{Y}}) + S^\top \Gamma S \vec{\mathbf{u}} + \sum_{i=1}^3 r_i H_i \vec{\mathbf{u}} \qquad \text{with } r_i \leftarrow \mathbb{Z}_p, \tag{5}$$

and satisfies

$$\iota(\vec{\mathcal{A}}) \bullet \vec{\mathbf{d}} + \vec{\mathbf{d}} \bullet \Gamma\vec{\mathbf{d}} \ = \ \iota_T(t_T) + \vec{\mathbf{u}} \bullet \Phi \ . \tag{6}$$

Soundness and WI of the proofs. In the WI setting, let $\vec{\mathbf{c}}$ and $\vec{\mathbf{d}}$ be commitments to $\vec{\mathcal{X}}$ and $\vec{\mathcal{Y}}$, resp., which both satisfy (4). Then Φ and Φ' constructed as in (5) for $\vec{\mathbf{c}}$ and $\vec{\mathbf{d}}$, resp., are equally distributed. In the soundness setting, given $\vec{\mathbf{d}}$ satisfying (6) for any Φ, one can extract $\vec{\mathcal{Y}}$ satisfying (4).

5.2 New Techniques I: Commitment Re-randomization and Proof Updating

As observed by [FP08] and [BCC+08], commitments of this form can be *re-randomized* and the corresponding proofs adapted without knowledge of the committed values and the used randomness: Given a commitment $\vec{\mathbf{d}}$, set $\vec{\mathbf{c}} := \vec{\mathbf{d}} + \widetilde{S}\vec{\mathbf{u}}$, for $\widetilde{S} \leftarrow \mathbb{Z}_p^{n\times 3}$, and *update* the proof Φ for $\vec{\mathbf{d}}$ to $\widetilde{\Phi}$ for $\vec{\mathbf{c}}$:

$$\widetilde{\Phi} \ := \ \Phi + \widetilde{S}^\top \iota(\vec{\mathcal{A}}) + \widetilde{S}^\top \Gamma\vec{\mathbf{d}} + \widetilde{S}^\top \Gamma^\top \vec{\mathbf{d}} + \widetilde{S}^\top \Gamma \widetilde{S}\vec{\mathbf{u}} + \sum \widetilde{r}_i H_i \vec{\mathbf{u}} \qquad \text{with } \widetilde{r}_i \leftarrow \mathbb{Z}_p. \tag{7}$$

The pair $(\vec{\mathbf{c}}, \widetilde{\Phi})$ satisfies (6) and some computation shows that $\widetilde{\Phi}$ is constructed as in (5) for $\vec{\mathbf{c}}$ being a commitment to $\vec{\mathcal{Y}}$ using randomness $S + \widetilde{S}$. (In particular (7) yields the same $\widetilde{\Phi}$ as (5) if in the latter the randomness used is $r_i + \alpha_i + \widetilde{r}_i$, where r_i is the randomness of Φ and the α_i are such that $A := \widetilde{S}^\top \Gamma^\top S - S^\top \Gamma \widetilde{S} = \sum \alpha_i H_i$. Such α_i exist because A satisfies $\vec{\mathbf{u}} \bullet A\vec{\mathbf{u}} = 0$ and the H_i's are a basis for the matrices of this form; cf. [GS08, Chapter 4]).

5.3 New Techniques II: Linear Equations and Different Commitment Keys

Consider two commitments under *different* commitment keys $\mathbf{c}$, $\mathbf{d}$ of Y, Z, resp. We show that the plaintexts satisfy

$$e(H, Y) \;=\; e(G, Z) \;. \tag{8}$$

Unlike for general equations, the proof for linear equations reduces to 3 group elements:[6] After committing to Y via $\mathbf{c} = \iota(Y) + \sum_{i=1}^{3} s_i \mathbf{u}_i$ (and for the time being considering Z as a constant), the proof for Y satisfying (8) is $\pi := (s_1 H, s_2 H, s_3 H)$ and is verified by checking

$$\begin{array}{rcl} e(H, c_1) & = & e(\pi_1, U)\, e(\pi_3, W_1) \\ e(H, c_2) & = & e(\pi_2, V)\, e(\pi_3, W_2) \end{array} \qquad\qquad e(H, c_3) \;=\; e(G, Z)\, e(\pi_1, P)\, e(\pi_2, P)\, e(\pi_3, W_3) \tag{9}$$

Re-randomization. Given $(\mathbf{c}, \pi)$, we can re-randomize the commitments and update the proofs (which replaces randomness s_i by $\tilde{s}_i := s_i + s'_i$):

$$\begin{array}{lll} c'_1 := c_1 + s'_1 U + s'_3 W_1 & c'_2 := c_2 + s'_1 V + s'_3 W_2 & c'_3 := c_3 + s'_1 P + s'_2 P + s'_3 W_3 \\ \pi'_1 := \pi_1 + s'_1 H & \pi'_2 := \pi_2 + s'_2 H & \pi'_3 := \pi_3 + s'_3 H \end{array}$$

The second variable. We now commit to Z under commitment key $\overline{\mathbf{u}}$ constructed from $\overline{U}$, $\overline{V}$, $\overline{W}_1$, $\overline{W}_2$, $\overline{W}_3$, and prove that Z satisfies the last equation in (9)—of which we now regard all other elements as constant. Letting $\mathbf{d} := \mathsf{Com}(\overline{u}, Z\,;\, \overline{s}_1, \overline{s}_2, \overline{s}_3)$ and $\overline{\pi} := (\overline{s}_1 G, \overline{s}_2 G, \overline{s}_3 G)$ we get the following relations:

$$\begin{array}{rcl} e(G, d_1) & = & e(\overline{\pi}_1, \overline{U})\, e(\overline{\pi}_3, \overline{W}_1) \\ e(G, d_2) & = & e(\overline{\pi}_2, \overline{V})\, e(\overline{\pi}_3, \overline{W}_2) \\ e(G, d_3) & = & e(H, c_3)\, e(\pi_1, P)^{-1}\, e(\pi_2, P)^{-1}\, e(\pi_3, W_3)^{-1}\, e(\overline{\pi}_1, P)\, e(\overline{\pi}_2, P)\, e(\overline{\pi}_3, \overline{W}_3) \end{array}$$

Putting it together. Given $\mathbf{c}, \mathbf{d}, \pi, \overline{\pi}$, we can verify that Y, the value committed to in $\mathbf{c}$ under $\mathbf{u}$, and Z, the value committed to in $\mathbf{d}$ under $\overline{\mathbf{u}}$, satisfy (8) by checking:

$$\begin{array}{rcl@{\qquad}rcl} e(H, c_1) & = & e(\pi_1, u_{1,1})\, e(\pi_3, u_{3,1}) & e(G, d_1) & = & e(\overline{\pi}_1, \overline{u}_{1,1})\, e(\overline{\pi}_3, \overline{u}_{3,1}) \\ e(H, c_2) & = & e(\pi_2, u_{2,2})\, e(\pi_3, u_{3,2}) & e(G, d_2) & = & e(\overline{\pi}_2, \overline{u}_{2,2})\, e(\overline{\pi}_3, \overline{u}_{3,2}) \end{array} \tag{10}$$

$$e(G, d_3)\, e(\pi_1, u_{1,3})\, e(\pi_2, u_{2,3})\, e(\pi_3, u_{3,3}) \;=\; e(H, c_3)\; e(\overline{\pi}_1, \overline{u}_{1,3})\, e(\overline{\pi}_2, u_{2,3})\, e(\overline{\pi}_3, \overline{u}_{3,3})$$

Correctness, soundness, and witness-indistinguishability follow from a hybrid argument applied to two instances of Groth-Sahai proofs. Moreover, the commitments can be independently re-randomized and the proofs updated, since the proof for Y does not depend on Z and vice versa.

5.4 New Techniques III: Proofs that Commitments Open to the Same Value

Given the extraction key, one can prove that two commitments open to the same value without knowledge of the randomness used when committed. We start by showing how to prove that a commitment (c_1, c_2, c_3) opens to zero: given the extraction key $ek = (\alpha, \beta)$ define the proof as $(\pi_1 := \frac{1}{\alpha} c_1, \pi_2 := \frac{1}{\beta} c_2)$. It satisfies the following relations:

$$e(\pi_1, U) = e(c_1, P) \qquad\qquad e(\pi_2, V) = e(c_2, P) \qquad\qquad c_3 = \pi_1 + \pi_2$$

It is easily seen that the proofs are perfectly correct and perfectly sound. In addition, they do not leak information about the opener's secret key, since they can be produced without knowledge of ek, given the randomness used to commit and the "trapdoor" (r_1, r_2) for the W_i's: $c_1 = s_1 U + s_3 W_1 = \alpha(s_1 + s_3 r_1) P$, thus $\pi_1 = (s_1 + s_3 r_1) P$, and similarly $\pi_2 = (s_2 + s_3 r_2) P$.

Now to show that $\mathbf{c}$ and $\mathbf{d}$ are two commitments to the same value, it suffices to prove that $\mathbf{c} - \mathbf{d}$ opens to 0.

[6] See Sect. 6.1 of the full version of [GS08].

$\mathbf{Exp}_{\mathcal{A}}^{\text{anon-iss}}(k)$

- Experiment plays: honest users $\mathcal{U}_1$ and $\mathcal{U}_2$
- $\mathcal{A}$ impersonates: $\mathcal{M}$, $\mathcal{I}$, $\mathcal{D}$, $\mathcal{O}$, users
- $\mathcal{U}_1$ and $\mathcal{U}_2$ run Join with $\mathcal{A}$ impersonating $\mathcal{M}$
- $b \leftarrow \{0,1\}$; $\mathcal{A}$ receives the ticket of $\mathcal{U}_b$
- $\mathcal{A}$ wins if it guesses b correctly

$\mathbf{Exp}_{\mathcal{A}}^{\text{trace-DS}}(k)$

- Experiment plays: honest $\mathcal{I}$, $\mathcal{M}$
- $\mathcal{A}$ impersonates: users
- gets keys: ok, dk (thus $\mathcal{O}$, $\mathcal{D}$ semi-honest[a])
- $\mathcal{A}$ gets oracles Join, Issue, Spend to communicate with $\mathcal{M}$, $\mathcal{I}$ and $\mathcal{D}$, resp.
- The experiment runs Detect and Trace on the spent tickets
- Let q be the number of Issue-oracle calls, let d be the number of Spend calls and a be the number of accusations by Trace. Then $\mathcal{A}$ wins if $a < d - q$

[a] As for the BSZ-model of group signatures, the detector and the opener can be malicious but at least have to follow the protocol of detecting and opening.

$\mathbf{Exp}_{\mathcal{A}}^{\text{anon-sell}}(k)$

- Experiment plays: honest users $\mathcal{U}_1$ and $\mathcal{U}_2$
- $\mathcal{A}$ impersonates: $\mathcal{M}$, $\mathcal{I}$, users
- $\mathcal{U}_1$ and $\mathcal{U}_2$ run Join with $\mathcal{A}$ impersonating $\mathcal{M}$
- $\mathcal{A}$ can ask withdrawals, transfers and spendings of $\mathcal{U}_1$ and $\mathcal{U}_2$.
- $b \leftarrow \{0,1\}$, $\mathcal{U}_b$ runs Sell with $\mathcal{A}$ playing a user.
- $\mathcal{A}$ wins if it guesses b correctly.

$\mathbf{Exp}_{\mathcal{A}}^{\text{non-fram}}(k)$

- The experiment plays an honest user $\mathcal{U}^*$
- $\mathcal{A}$ can impersonate: $\mathcal{M}$, $\mathcal{I}$, $\mathcal{D}$, $\mathcal{O}$, users
- $\mathcal{U}^*$ runs Join with $\mathcal{A}$ impersonating $\mathcal{M}$
- $\mathcal{A}$ can ask the user to withdraw tickets, sell and buy them and spend tickets[a]
- $\mathcal{A}$ wins if it outputs a proof that accuses $\mathcal{U}^*$ of double spending, which $\mathcal{U}^*$ cannot contest.[b]

[a] $\mathcal{U}^*$ behaves honestly, so if he is asked to spend more tickets than he withdrew he refuses.

[b] A malicious open can accuse an honest user of not having a receipt, which the latter counters by showing it.

Fig. 4. Security experiments for e-ticketing

6 Anonymously Transferable Tickets from Certificates

6.1 Formal Model

In an e-ticketing system, there are the following protagonists: *users* $\mathcal{U}_i$ that—after registering—can buy, sell and spend tickets, the *manager* $\mathcal{M}$, authorizing users to join the system, the *issuer* $\mathcal{I}$, able to issue tickets, *service providers* $\mathcal{P}_i$ to which tickets are spent, the *double-spending detector* $\mathcal{D}$, that can detect if a ticket was spent twice, and the *opener* $\mathcal{O}$, able to trace double spenders. The system comprises the following protocols and algorithms:

Setup	A protocol between $\mathcal{M}$ (who gets mk), $\mathcal{I}$ (who gets ik), $\mathcal{D}$ (who gets dk), and $\mathcal{O}$ (who gets ok). The protocol also outputs the public parameters pp.
Join	A protocol between a user and $\mathcal{M}$ that registers the user to the system and gives him usk.
Issue	A protocol permitting $\mathcal{I}$ to issue a ticket to a user.
Sell	A protocol between users $\mathcal{U}_1$ and $\mathcal{U}_2$, where $\mathcal{U}_1$ sells a ticket to $\mathcal{U}_2$.
Spend	A protocol between a user and a service provider to spend a ticket.
Detect	An algorithm enabling $\mathcal{D}$ to check for double spendings.
Trace	A protocol conducted by $\mathcal{O}$ in order to trace a double spender.

We define the following security notions for our e-ticketing system: *Traceability (of double spenders)* states that for each time a user spends a ticket more than once he will be accused. *Non-frameability* guarantees that even if everyone else colludes against an honest user, he cannot be wrongfully accused of double spending. *Anonymity of issuing:* means that not even the issuer colluding with the double-spending detector can tell to which issuing a ticket corresponds. *Anonymity of selling (or spending)* ensures that when selling/spending a ticket one remains anonymous even with respect to the issuer and malicious users the ticket was sold by.

With the experiments detailed in Fig. 4, we say an e-ticketing system is traceable, non-frameable, etc., if no p.p.t. adversary can win the respective game with non-negligible probability (non-negligibly more than $1/2$ for the anonymity notions).

6.2 Instantiation

Overview. The tickets in our system are certificates from Sect. 3, whose partial blindness guarantees that the issuer does not know their last component C_5. They were constructed so that their verification relations fall in the Groth-Sahai methodology [GS08]; the user can thus encrypt (in Groth-Sahai terminology: commit to) the ticket and prove validity. Moreover, each time the ticket is transferred, the receiver can re-randomize the encryption (cf. Sect. 5.2), which guarantees anonymity and unlinkability.

Now, to check for double spendings, the detector will get the decryption key to compare encrypted certificates. However, this straight-forward approach would not guarantee user anonymity when issuer and detector collude; we proceed thus as follows: The different components of the ticket are encrypted under *different* keys (cf. Sect. 5.3 on how to construct the corresponding proofs). The detector gets the key to decrypt the last (secret) component only, which suffices to detect double spending.

The receipts are group signatures, the signing keys for which the users get when joining the system. This guarantees traceability of double spenders, while preserving anonymity (only the opener, holding the group-signature opening key, can reveal users' identities). When transferring or spending a ticket, the user must thus sign it first.

In case a double spending is detected, the opener can trace back the paths the certificate took before reaching the spender, by opening the group signatures. A user that spent or sold a ticket twice is then unable to show two receipts. To guarantee soundness of tracing, we must ensure that each signature corresponds to at most one transfer. We achieve this by adding a nonce, set by the buyer, to the message to be signed by the seller.

Details. Let $\mathcal{GS} = (\mathsf{Setup}_{\mathcal{GS}}, \mathsf{Join}_{\mathcal{GS}}, \mathsf{GSign}_{\mathcal{GS}}, \mathsf{GVer}_{\mathcal{GS}})$ be a dynamic group-signature scheme that is non-frameable.[7] Moreover, let $\mathcal{H}\colon \mathbb{G}^* \to \{0,1\}^n$ be a collision-resistant hash function.

Setup. – Set up a group signature scheme $\mathcal{GS}$ such that $\mathcal{M}$ is the group's issuer (group manager) and $\mathcal{O}$ is the opener. The group verification key gvk is added to pp.
– Produce two keys for linear commitments ck and $ck_{\mathcal{D}}$. The extraction key $ek_{\mathcal{D}}$ corresponding to ck_D is given to $\mathcal{D}$ and $\mathcal{O}$.
– Set up the parameters for the blind certification scheme from Sect. 3. $\mathcal{I}$ gets the certificate issuing key ω, and a group signing key $gsk_{\mathcal{I}}$ for $\mathcal{GS}$.

Join. A user $\mathcal{U}_i$ joins the system by running $\mathsf{Join}_{\mathcal{GS}}$ with $\mathcal{M}$ to obtain her group signing key gsk_i.

Issue. User $\mathcal{U}$ runs the certification protocol (Sect. 3.2) with $\mathcal{I}$ to get $(C_1, \dots C_5) \in \mathbb{G}^5$ satisfying

$$e(C_1, \Omega + C_2) = e(K + C_4, G) \qquad e(C_2, H) = e(G, C_3) \qquad e(C_4, H) = e(G, C_5) \tag{11}$$

Additionally, the issuer gives the user a "receipt" $R_{\mathcal{I}} \leftarrow \mathsf{GSign}_{\mathcal{GS}}(gsk_{\mathcal{I}}, \mathcal{H}(C_1, C_2, C_3, \mathcal{U}))$.[8]
The user verifies the certificate and the signature and produces the following commitments:
– $\mathbf{c}_i := \mathsf{Com}(ck, C_i)$, for $1 \le i \le 4$
– $\mathbf{c}_5 := \mathsf{Com}(ck_{\mathcal{D}}, C_5)$
and proofs Φ_1, Φ_2, Φ_3 for the committed values satisfying the three equation in (11). Φ_1 and Φ_2 are regular Groth-Sahai proofs, for the last equation on commitments under different keys, see Sect. 5.3. We call $(\vec{\mathbf{c}}, \vec{\Phi})$ a *ticket*, and refer to Appendix C for its concrete construction.

Sell / Spend. When $\mathcal{U}_S$ sells a ticket to $\mathcal{U}_B$, she sends $(\vec{\mathbf{c}}, \vec{\Phi})$ and $R \leftarrow \mathsf{GSig}_{\mathcal{GS}}(gsk_{\mathcal{U}_S}, \mathcal{H}(\vec{\mathbf{c}}, \mathcal{U}_B, N))$, where N is a nonce set by $\mathcal{U}_B$. The buyer $\mathcal{U}_B$ checks correctness of $(\vec{\mathbf{c}}, \vec{\Phi})$ and R, re-randomizes $\vec{\mathbf{c}}$ and updates $\vec{\Phi}$ (cf. Sects. 5.2 and 5.3). Spending is defined as selling to $\mathcal{P}$.

Detect. After receiving a ticket, $\mathcal{D}$ uses extraction key $ek_{\mathcal{D}}$ to open $\mathbf{c}_5$: $C_5 := \mathsf{Extr}(ek_{\mathcal{D}}, \mathbf{c}_5)$. He compares the tag C_5 with that of other received tickets to see if a ticket was spent twice, in which case he charges $\mathcal{O}$ to trace the double spender.

[7] Encrypting the certified signatures from Sect. 4 and proving validity by adding a Groth-Sahai proof yields a (CPA-anonymous) non-frameable group signature scheme that does not require any further assumptions.
[8] Abusing notation, we let $\mathcal{U}$ be a unique encoding of the user's identity in $\mathbb{G}$.

Tracing. – If multiple spendings $(\vec{\mathbf{c}}^{(i)}, \vec{\Phi}^{(i)}, R^{(i)})$ with $\mathsf{Extr}(ek_{\mathcal{D}}, \mathbf{c_5}^{(i)}) = C_5^*$ for all i were detected, the opener uses the opening key ok to open the signatures $R^{(i)}$ in order to reveal users $\mathcal{U}_0^{(i)}$.

– Each $\mathcal{U}_0^{(i)}$ has to *prove legal acquisition* of his ticket, which a user $\mathcal{U}$ does as follows:

- If the ticket was obtained from the issuer, show $C = (C_1, \ldots, C_5)$ and the receipt $R_{\mathcal{I}}$. $\mathcal{O}$ accepts if C is valid, $\mathsf{GVer}_{\mathcal{GS}}(gvk, \mathcal{H}(C_1, C_2, C_3, \mathcal{U}), R_{\mathcal{I}}) = 1$ and $C_5 = C_5^*$.
- If the ticket was bought from a user, show the receipt R received with the ticket together with $(\vec{\mathbf{c}}', \vec{\Phi}')$, the received ticket (i.e., before re-randomizing it), and the nonce N. $\mathcal{O}$ accepts if $(\vec{\mathbf{c}}', \vec{\Phi}')$ is valid, $\mathsf{GVer}_{\mathcal{GS}}(gvk, \mathcal{H}(\vec{\mathbf{c}}', \mathcal{U}, N), R) = 1$ and $\mathsf{Extr}(ek_{\mathcal{D}}, \mathbf{c}_5') = C_5^*$.

– In the second case (receipt produced by a user), $\mathcal{O}$ opens R to $\mathcal{U}_1^{(i)}$, who in turn has to prove legal acquisition of the ticket. Moreover, the opener only accepts a receipt if it has not been received before.

– Continuing this process produces chains of users $\mathcal{U}_0^{(i)}, \mathcal{U}_1^{(i)}, \ldots$ which either end with the issuer, or with a user failing to prove legal acquisition—in which case that user is accused.

– Correctness of tracing is proven by proving correctness of opening of group signatures and proving that two commitments contain the same certificate using the techniques from Sect. 5.4.

6.3 Security Results

We briefly argue why our instantiation satisfies the security definitions from Sect. 6.1. Each property follows by a straight-forward reduction to the security of the underlying building blocks.

Traceability of double spenders. Assuming an honest issuer we have (1) every certificate is only issued once with all but negligible probability; (2) by unforgeability of certificates (Theorem 8) and soundness of the WI proofs, opening all d spent tickets leads to at most q different certificates.

Assume, a certificate $C^{(i)}$ was spent $s^{(i)}$ times. Then the tracing algorithm produces $s^{(i)}$ lists of users, beginning with the spenders and linked by their certificates. Unforgeability of group signatures and (1) guarantees that only one such list ends with the issuer. Since $s^{(i)} - 1$ users are thus accused and by (2), we have $a = \sum_{i=1}^{q}(s^{(i)} - 1) = d - q$.

Non-frameability. If $\mathcal{U}^*$ uses a random nonce each time then by collision resistance of $\mathcal{H}$, the probability of receiving the same valid receipt twice is negligible. The user can only be provably accused if he spent/transferred a ticket of which he cannot justify acquisition. Non-frameability of group signatures guarantees that $\mathcal{U}^*$ only has to justify tickets he actually transferred—and for each such ticket he possesses a valid receipt. Note that if a malicious user sells the same ticket (possibly as two different randomizations) twice to $\mathcal{U}^*$ then $\mathcal{U}^*$ has two different signatures (due to the nonce) and can thus justify both tickets.

Anonymity. Anonymity of issuing follows from partial blindness of issuing (indistinguishability of $\mathbf{c}_5$) and witness indistinguishability of the commitments $(\mathbf{c}_1, \ldots, \mathbf{c}_4)$ under key ck. Anonymity of selling follows from WI of commitments under ck and $ck_{\mathcal{D}}$ and anonymity of group signatures.

Acknowledgments

The authors would like to thank the members of the PACE research project for the fruitful discussions that led to the new primitive discussed in this paper. This work was supported by the French ANR 07-TCOM-013-04 PACE Project, the European Commission through the IST Program under Contract ICT-2007-216646 ECRYPT II, and EADS.

References

[AO00] Masayuki Abe and Tatsuaki Okamoto. Provably secure partially blind signatures. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 271–286. Springer, August 2000.

[BB04] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 56–73. Springer, May 2004.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, August 2004.

[BCC+08] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Delegatable anonymous credentials. Cryptology ePrint Archive, Report 2008/428, 2008. http://eprint.iacr.org/.

[BFPW07] Alexandra Boldyreva, Marc Fischlin, Adriana Palacio, and Bogdan Warinschi. A closer look at PKI: Security and efficiency. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *PKC 2007*, volume 4450 of *LNCS*, pages 458–475. Springer, April 2007.

[BMW03] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 614–629. Springer, May 2003.

[BP04] Mihir Bellare and Adriana Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 273–289. Springer, August 2004.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 136–153. Springer, February 2005.

[BW07] Xavier Boyen and Brent Waters. Full-domain subgroup hiding and constant-size group signatures. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *PKC 2007*, volume 4450 of *LNCS*, pages 1–15. Springer, April 2007.

[CG07] Sébastien Canard and Aline Gouget. Divisible e-cash systems can be truly anonymous. In Moni Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 482–497. Springer, May 2007.

[Cha83] David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *CRYPTO'82*, pages 199–203. Plenum Press, New York, USA, 1983.

[Cha84] David Chaum. Blind signature system. In David Chaum, editor, *CRYPTO'83*, page 153. Plenum Press, New York, USA, 1984.

[CP92] David Chaum and Torben P. Pedersen. Transferred cash grows in size. In Rainer A. Rueppel, editor, *EUROCRYPT'92*, volume 658 of *LNCS*, pages 390–407. Springer, May 1992.

[Cv91] David Chaum and Eugène van Heyst. Group signatures. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 257–265. Springer, April 1991.

[Dam92] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 445–456. Springer, August 1992.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[EO94] Tony Eng and Tatsuaki Okamoto. Single-term divisible electronic coins. In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 306–319. Springer, May 1994.

[FP08] Georg Fuchsbauer and David Pointcheval. Encrypting proofs on pairings and its application to anonymity for signatures. Cryptology ePrint Archive, Report 2008/528, 2008. http://eprint.iacr.org/.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, August 1987.

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111. Springer, August 2006.

[Gro06] Jens Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459. Springer, December 2006.

[Gro07] Jens Groth. Fully anonymous group signatures without random oracles. In Kaoru Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 164–180. Springer, December 2007.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–423. Springer, April 2008.

[Kil06] Eike Kiltz. Chosen-ciphertext security from tag-based encryption. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 581–600. Springer, March 2006.

[NHS99] Toru Nakanishi, Nobuaki Haruna, and Yuji Sugiyama. Unlinkable electronic coupon protocol with anonymity control. In Masahiro Mambo and Yuliang Zheng, editors, *ISW'99*, volume 1729 of *LNCS*, pages 37–46. Springer, November 1999.

[Oka06] Tatsuaki Okamoto. Efficient blind and partially blind signatures without random oracles. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 80–99. Springer, March 2006.

[OO90] Tatsuaki Okamoto and Kazuo Ohta. Disposable zero-knowledge authentications and their applications to untraceable electronic cash. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 481–496. Springer, August 1990.

[OO92] Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 324–337. Springer, August 1992.

[PS00] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[Sch90] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 239–252. Springer, August 1990.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, May 1997.

[SPC95] Markus Stadler, Jean-Marc Piveteau, and Jan Camenisch. Fair blind signatures. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 209–219. Springer, May 1995.

[Wat05] Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer, May 2005.

A The Strong Diffie-Hellman Assumptions and the Hidden Variants

We present the Strong Diffie-Hellman Problem for $\mathbb{G}_1 = \mathbb{G}_2$ and variants of it whose hardness follows from that of the original problem.

Definition 11 (The Strong Diffie-Hellman Problem I (SDH-I)). *Given a $(q+1)$-tuple $(G, \gamma G, \gamma^2 G, \ldots, \gamma^q G)$, for a random element $\gamma \in \mathbb{Z}_p$, output a pair $\left(x, A = \frac{1}{\gamma+x} G\right)$, with $x \in \mathbb{Z}_p$. It satisfies $e(A, \Gamma + xG) = e(G, G)$ with $\Gamma = \gamma G$.*

Definition 12 (The Strong Diffie-Hellman Assumption). *The q-SDH assumption states that this problem is intractable for a given q.*

Definition 13 (The Strong Diffie-Hellman Problem II (SDH-II)). *Given $(G, \Gamma = \gamma G)$ and $q-1$ pairs $\left(x_i, A_i = \frac{1}{\gamma+x_i} G\right)$, with $x_i \in \mathbb{Z}_p$ for $i = 1, \ldots, q-1$, output a new pair $\left(x, A = \frac{1}{\gamma+x} G\right)$, with $x \in \mathbb{Z}_p$.*

Lemma 14. *If one can solve the Strong Diffie-Hellman Problem II, then one can solve the Strong Diffie-Hellman Problem I.*

See Appendix B for the proof.

Definition 15 (The Strong Diffie-Hellman Problem III (SDH-III)). *Given $(G, \Gamma = \gamma G, K)$ and $q-1$ triples $\left(x_i, y_i, A_i = \frac{1}{\gamma+x_i}(K + y_i G)\right)$, with $x_i, y_i \in \mathbb{Z}$ for $i = 1, \ldots, q-1$, output a new triple $\left(x, y, A = \frac{1}{\gamma+x}(K + yG)\right)$, with $x, y \in \mathbb{Z}_p$. It satisfies $e(A, \Gamma + xG) = e(K, G) \cdot e(G, G)^y$.*

Lemma 16. *If one can solve the Strong Diffie-Hellman Problem III, then one can solve the Strong Diffie-Hellman Problem I.*

See Appendix B for the proof.

In [BW07], a "hidden" version of SDH-II is defined, where in the pairs (x_i, A_i), the scalar x_i is not given in the clear but as $(x_i G, x_i H)$ for a fixed group generator H. It is easily seen that under the Knowledge of Exponent Assumption [Dam92,BP04], the following problem is equivalent to SDH-II.

Definition 17 (The Hidden Strong Diffie-Hellman Problem (HSDH)). *Given $(G, H, \Gamma = \gamma G)$ and $q-1$ triples $\left(X_i = x_i G, X_i' = x_i H, A_i = \frac{1}{\gamma+x_i} G\right)$, with $x_i \in \mathbb{Z}_p^*$ for $i = 1, \ldots, q-1$, output a new triple $\left(X = xG, X' = xH, A = \frac{1}{\gamma+x} G\right)$, with $x \in \mathbb{Z}_p^*$. It satisfies both*

$$e(X, H) = e(G, X') \qquad e(A, \Gamma + X) = e(G, G).$$

Definition 18 (The Hidden Strong Diffie-Hellman Assumption). *The q-HSDH assumption states that the Hidden Strong Diffie-Hellman II Problem is intractable for a given q.*

We now apply the same methodology to SDH-III, i.e., we give (and expect in a forgery) the two scalars x and y in a hidden form analogously to HSDH.

Definition 19 (The Double Hidden Strong Diffie-Hellman Problem (DHSDH)). *Given* $(G, H, K, \Gamma = \gamma G)$ *and* $q-1$ *tuples* $\left(X_i = x_i G, X'_i = x_i H, Y_i = y_i G, Y'_i = y_i H, A_i = \frac{1}{\gamma + x_i}(K + y_i G)\right)$, *with* $x_i, y_i \in \mathbb{Z}_p^*$ *for* $i = 1, \ldots, q-1$, *output a new tuple*

$$\left(X = xG, X' = xH, Y = yG, Y' = yH, A = \frac{1}{\gamma + x}(K + yG)\right),$$

with $x \in \mathbb{Z}_p^*$. *It satisfies*

$$e(X, H) = e(G, X') \quad e(Y, H) = e(G, Y') \quad e(A, \Gamma + X) = e(K, G) \cdot e(Y, G).$$

Definition 20 (The Double Hidden Strong Diffie-Hellman Assumption). *The q-DHSDH assumption states that the Double Hidden Strong Diffie-Hellman Problem is intractable for a given* q.

B Proofs

Similar proofs can be found in [Oka06], but we recall them for completeness.

Proof (Proof of Lemma 14). Let us be given a $(q+1)$-tuple $(P, \gamma P, \gamma^2 P, \ldots, \gamma^q P)$, for random elements $P \in \mathbb{G}$ and $\gamma \in \mathbb{Z}_p$. We now generate the input for the SDH-II problem: we

- randomly choose $\alpha \in \mathbb{Z}_p$ and $x_i \in \mathbb{Z}_p$, for $i = 1, \ldots, q-1$, such that the x_i's are pairwise distinct;
- set

$$G \leftarrow \alpha \left[\prod_{i=1}^{q-1}(\gamma + x_i)\right] P \qquad \Gamma \leftarrow \gamma G;$$

- simulate the elements, for $i = 1, \ldots, q-1$: $A_i \leftarrow \alpha \left[\prod_{\substack{j=1 \\ j \neq i}}^{q-1}(\gamma + x_j)\right] P$.

  Since $G = (\gamma + x_i)A_i$, we have

$$e(A_i, \Gamma + x_i G) = e(A_i, \gamma G + x_i G) = e(A_i, (\gamma + x_i)G) = e(G, G).$$

  Finally, the forgery (x, A) satisfies

$$x \neq x_i \quad (i = 1, \ldots, q-1), \qquad A = \frac{1}{\gamma + x} G = \frac{\alpha}{\gamma + x} \left[\prod_{i=1}^{q-1}(\gamma + x_i)\right] P = \frac{f(\gamma)}{\gamma + x} P,$$

with

$$f(\gamma) = \alpha \prod_{i=1}^{q-1}(\gamma + x_i) = \alpha \prod_{i=1}^{q-1}((\gamma + x) + (x_i - x)) = \alpha \prod_{i=1}^{q-1}(x_i - x) + (\gamma + x)g(\gamma + x)$$

Therefore,

$$A = \frac{\alpha \prod_{i=1}^{q-1}(x_i - x)}{\gamma + x} P + g(\gamma + x)P$$

Since g is a polynomial of degree at most $q-2$, one can compute $R = g(\gamma + x)P$ from the SDH-I input. If one sets

$$A' = \frac{1}{\alpha \prod_{i=1}^{q-1}(x_i - x)}(A - R) = \frac{1}{\gamma + x} P$$

the pair (x, A') is a solution to the SDH-I problem. □

Proof (Proof of Lemma 16). There are two ways of solving SDH-III by outputting (x, y, A): Either $x \neq x_i$ for all $i = 1, \ldots, q-1$ or $y \neq y_i$ for all i.

A new x. Let us first assume that the adversary is more likely to solve the SDH-III Problem with an x that is different from all the x_i of the input. Then the analysis is similar to the proof of Lemma 14.

Let us be given a $(q+1)$-tuple $(P, \gamma P, \gamma^2 P, \ldots, \gamma^q P)$, for random elements $P \in \mathbb{G}$ and $\gamma \in \mathbb{Z}_p$. We now generate the input for the SDH-III problem: we

– randomly choose $\alpha, \beta \in \mathbb{Z}_p$ and $x_i, y_i \in \mathbb{Z}_p$, for $i = 1, \ldots, q-1$, such that the (x_i, y_i)'s are pairwise distinct;
– set

$$G \leftarrow \alpha \left[\prod_{i=1}^{q-1}(\gamma + x_i)\right] \cdot P \qquad K \leftarrow \beta G \qquad \Gamma \leftarrow \gamma G$$

– simulate the certificates, for $i = 1, \ldots, q-1$:

$$A_i \leftarrow \alpha(\beta + y_i) \left[\prod_{\substack{j=1 \\ j \neq i}}^{q-1}(\gamma + x_j)\right] P$$

Since $(\gamma + x_i)A_i = (\beta + y_i)G = K + y_i G$, we have

$$e(A_i, \Gamma + x_i G) = e(A_i, \gamma G + x_i G) = e(A_i, (\gamma + x_i)G) = e(K + y_i G, G) = e(K, G)e(G, G)^{y_i}.$$

Finally, a successful output satisfies

$$x \neq x_i \quad (i = 1, \ldots, q), \qquad A = \frac{1}{\gamma + x}(K + yG) = \frac{\beta + y}{\gamma + x}G = \frac{\alpha(\beta + y)}{\gamma + x}\left[\prod_{i=1}^{q-1}(\gamma + x_i)\right] P = \frac{f(\gamma)}{\gamma + x}P,$$

where

$$f(\gamma) = \alpha(\beta + y)\prod_{i=1}^{q-1}(\gamma + x_i) = \alpha(\beta + y)\prod_{i=1}^{q-1}((\gamma + x) + (x_i - x)) = \alpha(\beta + y)\prod_{i=1}^{q-1}(x_i - x) + (\gamma + x)g(\gamma + x)$$

Therefore,

$$A = \frac{\alpha(\beta + y)\prod_{i=1}^{q}(x_i - x)}{\gamma + x}P + g(\gamma + x)P$$

Since g is a polynomial of degree at most $q - 2$, one can compute $R = g(\gamma + x)P$ from the SDH-I input. If one sets

$$A' = \frac{1}{\alpha(\beta + y)\prod_{i=1}^{q}(x_i - x)}(A - R) = \frac{1}{\gamma + x}P$$

the pair (x, A') is a solution to the SDH-I problem.

An already known x. Let us now assume that the adversary most likely solves the SDH-III Problem with $x \in \{x_1, \ldots, x_{q-1}\}$ from the input.

Let us be given a $(q+1)$-tuple $(P, \gamma P, \gamma^2 P, \ldots, \gamma^q P)$, for random elements $P \in \mathbb{G}$ and $\gamma \in \mathbb{Z}_p$. We now generate the input for the SDH-III problem: we

– randomly choose $\alpha, \beta \in \mathbb{Z}_p$ and $(x_i, y_i) \in \mathbb{Z}_p$, for $i = 1, \ldots, q-1$, such that the (x_i, y_i)'s are pairwise distinct;
– choose a random index $k \in \{1, \ldots, q-1\}$, and set (thus implicitly defining a new secret exponent $\omega \leftarrow \gamma - x_k$),

$$G \leftarrow \beta \left[\prod_{\substack{i=1 \\ i \neq k}}^{q-1}(\gamma - x_k + x_i)\right] \cdot P \qquad K \leftarrow (\alpha\gamma - y_k)G \qquad \Gamma \leftarrow (\gamma G) - x_k G = \omega G$$

– simulate the certificates, for $i = 1, \ldots, q-1$:

- for $i = k$, $A_k \leftarrow \alpha G$, which satisfies

$$(\omega + x_k)A_k = \alpha\gamma G = K + y_k G$$

- for $i \neq k$,

$$A_i \leftarrow \beta((y_i - y_k) + \alpha\gamma) \left[\prod_{\substack{j=1 \\ j \neq i,k}}^{q} (\gamma - x_k + x_j) \right] P$$

We have $(\omega + x_i)A_i = ((y_i - y_k) + \alpha\gamma)G = (y_i - y_k)G + K + y_kG = K + y_iG$

Finally, a successful output satisfies

$$(x, y) \neq (x_i, y_i) \quad (i = 1, \ldots, q), \qquad A = \frac{1}{\omega + x}(K + yG)$$

Since we assumed that the x is likely in $\{x_1, \ldots, x_q\}$, and x_k is only used under the formula $\omega = \gamma - x_k$, the probability that $x = x_k$ is $1/q$, in which case

$$A_k = \frac{1}{\gamma}(K + y_kG) \quad A = \frac{1}{\gamma}(K + yG)$$

Then,

$$y_kA - yA_k = \frac{y_k - y}{\gamma}K = \frac{y_k - y}{\gamma}(\alpha\gamma - y_k)\beta \left[\prod_{\substack{i=1 \\ i \neq k}}^{q-1} (\gamma - x_k + x_i) \right] \cdot P = \frac{f(\gamma)}{\gamma}P,$$

with

$$f(\gamma) = (y_k - y)(\alpha\gamma - y_k)\beta \left[\prod_{\substack{i=1 \\ i \neq k}}^{q-1} (\gamma - x_k + x_i) \right] = (y - y_k)y_k\beta \left[\prod_{\substack{i=1 \\ i \neq k}}^{q-1} (x_i - x_k) \right] + \gamma g(\gamma)$$

Since g is a polynomial of degree at most $q - 2$, one can compute $R = g(\gamma)P$ from the SDH-I input. If one sets

$$A' = \frac{1}{(y - y_k)y_k\beta \left[\prod_{\substack{i=1 \\ i \neq k}}^{q-1} (x_i - x_k) \right]} (y_kA - yA_k - R) = \frac{1}{\gamma}P,$$

the pair $(0, A')$ is a solution to the SDH-I problem. □

C The Concrete Form of a Ticket

For concreteness, we give the form of a ticket, i.e., an "encrypted" certificate together with the proof of validity.

Let $ck = (U, V, W_1, W_2, W_3)$, $ck_{\mathcal{D}} = (U', V', W_1', W_2', W_3')$, let $\vec{\mathbf{u}}$ and $\vec{\mathbf{u}}'$ be as in (3), resp.; let $C = (A, X, X', Y, Y')$ be a certificate satisfying (1). We commit to its components

$$\mathbf{c}_A := \iota(A) + \textstyle\sum_{Ai} \mathbf{u}_i \qquad \begin{array}{ll} \mathbf{c}_X := \iota(X) + \sum s_{Xi}\mathbf{u}_i & \mathbf{c}_Y := \iota(Y) + \sum s_{Yi}\mathbf{u}_i \\ \mathbf{c}_{X'} := \iota(X') + \sum s_{X'i}\mathbf{u}_i & \mathbf{c}_{Y'} := \iota(Y') + \sum s_{Y'i}\mathbf{u}'_i \end{array}$$

and prove that the plaintexts satisfy the equations in (1) is satisfied:

Equation 1. $e(X, H) = e(G, X')$, that is $e(H, X)\, e(G^{-1}, X') = 1$ is a linear equation, the proof is thus $\xi := (s_{X1}H + s_{X'1}G^{-1},\ s_{X2}H + s_{X'2}G^{-1},\ s_{X3}H + s_{X'3}G^{-1})$

Equation 2. $e(Y, H) = e(G, Y')$, with Y and Y' encrypted under different keys was discussed in Sect. 5.3, with $Z := Y'$. The proofs are thus $\pi := (s_{Y1}H, s_{Y2}H, s_{Y3}H)$ and $\pi' := (s_{Y'1}G, s_{Y'2}G, s_{Y'3}G)$ and satisfy (10).

Equation 3. $e(A, \Omega + X) = e(K + Y, G)$, that is $e(A, \Omega)\, e(Y, G^{-1})\, e(A, X) = e(K, G)$, which with

$$\vec{\mathcal{Y}} := \begin{bmatrix} A \\ X \\ Y \end{bmatrix} \qquad \vec{\mathcal{A}} := \begin{bmatrix} \Omega \\ 0 \\ G^{-1} \end{bmatrix}, \qquad \Gamma := \begin{bmatrix} 0\,1\,0 \\ 0\,0\,0 \\ 0\,0\,0 \end{bmatrix}, \qquad t_T := e(K, G), \quad \text{and} \quad S = \begin{bmatrix} s_{A1} & s_{A2} & s_{A3} \\ s_{X1} & s_{X2} & s_{X3} \\ s_{Y1} & s_{Y2} & s_{Y3} \end{bmatrix}$$

can be written as $(\vec{\mathcal{A}} \cdot \vec{\mathcal{Y}})\,(\vec{\mathcal{Y}} \cdot \Gamma \vec{\mathcal{Y}}) \;=\; t_T$. Constructing $\Phi \in \mathbb{G}^{3\times 3}$ as in (5), we get

$$\Phi = \begin{bmatrix} s_{A1}s_{X1}U & (s_{A1}s_{X2} + r_1)V & s_{X1}A + s_{A1}X + s_{A1}\Omega + s_{Y1}G^{-1} \\ +(s_{A1}s_{X3} + r_2)W_1 & +(s_{A1}s_{X3} + r_2)W_2 & +(s_{A1}(s_{X1} + s_{X2}) + r_1)P + (s_{A1}s_{X3} + r_2)W_3 \\ (s_{A2}s_{X1} - r_1)U & s_{A2}s_{X2}V & s_{X2}A + s_{A2}X + s_{A2}\Omega + s_{Y2}G^{-1} \\ +(s_{A2}s_{X3} + r_3)W_1 & +(s_{A2}s_{X3} + r_3)W_2 & +(s_{A2}(s_{X1} + s_{X2}) - r_1)P + (s_{A2}s_{X3} + r_3)W_3 \\ (s_{A3}s_{X1} - r_2)U & (s_{A3}s_{X2} - r_3)V & s_{X3}A + s_{A3}X + s_{A3}\Omega + s_{Y3}G^{-1} \\ \quad +s_{A3}s_{X3}W_1 & \quad +s_{A3}s_{X3}W_2 & \quad +(s_{A3}(s_{X1} + s_{X2}) - r_2 - r_3)P + s_{A3}s_{X3}W_3 \end{bmatrix}$$

A ticket is thus of the form $(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_{X'}, \mathbf{c}_Y, \mathbf{c}_{Y'}, \xi, \pi, \pi', \Phi)^\top \in \mathbb{G}^{11\times 3}$.