Ethical identity, ring VRFs, and zero-knowledge continuations

Jeffrey Burdges, Oana Ciobotaru, Handan Kılınç Alper, Alistair Stewart, and Sergey Vasilyev

Web 3.0 Foundation

April 30, 2023

Abstract. We introduce a new cryptographic primitive, aptly named *ring verifiable random functions (ring VRF)*, which provides an array of uses, especially in anonymous credentials. Ring VRFs are (anonymized) ring signatures that prove correct evaluation of an authorized signer's PRF, while hiding the specific signer's identity within some set of possible signers, known as the ring.

We discover a family of ring VRF protocols with surprisingly efficient instantiations, thanks to our novel *zero-knowledge continuation* technique. Intuitively our ring VRF signers generate two linked proofs, one for PRF evaluation and one for ring membership. An evaluation proof needs only a cheap Chaum-Pedersen DLEQ proof, while ring membership proof depends only upon the ring itself. We reuse this ring membership proof across multiple inputs by expanding a Groth16 trusted setup to rehide public inputs when rerandomizing the Groth16. Incredibly, our fastest amortized ring VRF needs only eight $\mathcal{G}_1$ and two $\mathcal{G}_2$ scalar multiplications, making it the only ring signature with performance competitive with group signatures.

We discuss applications that range across the anonymous credential space:

As in proof-of-personhood work by Bryan Ford, et al., a ring VRF output acts like a unique pseudo-nonymous identity within some desired context, given as the ring VRF input, but remains unlinkable between different contexts. These unlinkable but unique pseudonyms provide a better balance between user privacy and service provider or social interests than attribute based credentials like IRMA ("I Reveal My Attributes") credentials.

Ring VRFs support anonymously rationing or rate limiting resource consumption that winds up vastly more flexible and efficient than purchases via money-like protocols.

We define the security of ring VRFs in the universally composable (UC) model and show that our protocol is UC secure.

1 Introduction

We introduce an anonymous credential flavor called ring verifiable random functions (ring VRFs), in essence ring signatures that anonymize signers but also prove evaluation of the signers' PRFs. Ring VRFs provide a better foundation for anonymous credentials across a range of concerns, including formalization, optimizations, the nuances of use-cases, and miss-use resistance.

Along with some formalizations, we address three questions within the unfolding ring VRF story:

1. What are the cheapest SNARK proofs?
   Ones users reuse without reproving.
2. How can identity be safe for general use?
   By revealing nothing except users' uniqueness.
3. How can ration card issuance be transparent?
   By asking users trust a public list, not certificates.

Ring VRFs: A ring signature proves only that its actual signer lies in a "ring" of public keys, without revealing which signer really signed the message. A *verifiable random function* (VRF) is a signature that proves correct evaluation of a PRF defined by the signer's key.

A *ring verifiable random function* (ring VRF) is a ring signature, in that it anonymizes its actual signer within a ring of plausible signers, but also proves correct evaluation of a pseudo-random function (PRF) defined by the actual signer's key. Ring VRF outputs then provide linking proofs between different signatures iff the signatures have identical inputs, as well as pseudo-randomness.

As this pseudo-random output is uniquely determined by the signed message and signer's actual secret key, we can therefore link signatures by the same signer if and only if they sign identical messages. In effect, ring VRFs restrict anonymity similarly to but less than linkable ring signatures do, which makes them multi-use and contextual.

We define the security of ring VRFs in both the standard model and in the universally composable (UC) [9,10] model. We show that our ring VRF protocol is secure in the UC model.

In §6, we build extremely efficient and flexible ring VRFs by amortizing a "zero-knowledge continuation" that unlinkably proves ring membership of a secret key, and then cheaply proving individual VRF evaluations.

Zero-knowledge continuations: Rerandomizable zkSNARKs like Groth16 [21] admit a transformation of a valid proof into another valid but unlinkable proof of the exact same statement. In practice, rerandomization never gets deployed because the public inputs link different usages, breaking privacy.

We demonstrate in §6 a simple transformation of any Groth16 zkSNARK into a *zero-knowledge continuation* whose public inputs involve opaque Pedersen commitments, with cheaply rerandomizable blinding factors and proofs. These zero-knowledge continuations then prove validity of the contents of Pedersen commitments, but can now be reused arbitrarily many times, without linking the usages.

In brief, we adjust the trusted setup of the Groth16 to additionally produce an independent blinding factor base for the Groth16 public input, along with an absorbing base that cancels out this blinding factor in the Groth16 verification. As our public inputs involve opaque Pedersen commitments, they now require proofs-of-knowledge resentment of to [8].

As recursive SNARKs might remain slow, we expect zero-knowledge continuations via rerandomization become essential for zkSNARKs used in identity and elsewhere outside the crypto-currency space.

Identity uses: An identity system can be based upon ring VRFs in an natural way: After verifying an identity requesting domain name in TLS, our user agent signs into the session by returning a ring VRF signature whose input is the requesting domain name, so their ring VRF output becomes their unique identity at that domain (see §9).

At this point, our requesting domain knows each users represents distinct ring members, which prevents Sybil behavior, and permits banning specific users. At the same time, users' activities remain unlinkable across different domains

In essence, ring VRF based credentials, if correctly deployed, only prevent users being Sybil, but leak nothing more about users. We argue this yields diverse legally and ethically straightforward identity usages.

As a problematic contrast, attribute based credential schemes like IRMA ("I Reveal My Attributes") credentials [7] are being marketed as an online privacy solution, but cannot prevent users being Sybil unless they first reveal numerous attributes. Attribute based credentials therefore provide little or no privacy when used to prevent abuse.

Abuse and Sybil prevention is not merely the most common use cases for anonymous credentials, but in fact define the "general" use cases for anonymous credentials. IRMA might improve privacy when used as "special purpose" credential in narrower situations of course, but overall attribute based credentials should *never* be considered fit for general purpose usage.

Aside from general purpose identity being problematic for attribute based credentials, our existing offline processes often better protect users' privacy and human rights than adopting online processes like IRMA. In particular, there are many proposals by the W3C for attribute based credential usage in [27], but broadly speaking they all bring matching harmful uses.

As an example, the W3C wants users to be able to easily prove their employment status, ostensibly so users could open bank accounts purely online. Yet, job application sites could similarly demand these same proofs of current employment, a discriminatory practice. Average users apply for jobs far more often than they open bank accounts, so credentials that prove current employment do more harm than good.

An IRMA deployment should prevent this abusive practice by making verifiers prove some legal authorization to request employment status, or other attributes, before user agents prove their attributes. Indeed IRMA deployments need to regulate IRMA verifiers, certainly by government privacy laws, or ideally by some more aggressive ethics board, but this limits their flexibility and becomes hard internationally.

Ring VRFs avoid these abuse risks by being truly unlinkable, and thus yield anonymous credentials which safely avoid legal restrictions.

Any ethical general purpose identity system should be based upon ring VRFs, not attribute based credentials like IRMA.

We credit proof-of-personhood parties by Bryan Ford, et al. [16,5] with first espousing the idea that anonymous credentials should produce contextual unique identifiers, without leaking other user attributes.

As a rule, there exist simple VRF variants for all anonymous credentials, including IRMA [7] or group signatures [24]. We focus exclusively upon ring VRFs for brevity, and because alone ring VRFs contextual linkability covers the most important use cases.

Rationing uses: A rate limiting or rationing system should provide users with a stream of single-use anonymous tokens that each enable consuming some resource. As a rule, cryptographers always construct these either from blind signatures ala [12], or else from OPRFs like PrivacyPass [14], both of which have an $O(n)$ issuance phase.

Ring VRFs yield rate limiting or rationing systems with no issuance phase: We first place into the ring the public keys for all users permitted to consume resources, perhaps all legal residents within some country. We define single-use tokens to be ring VRF signatures whose VRF input consists of a resource name, an approximate date, and a bounded counter. Now merchants reports each anonymous token back to some authority who enforces rate limits by rejecting duplicate ring VRF outputs. (See §10)

In other words, our rate limiting authority treats outputs like the "nullifiers" in anonymous payment schemes. Yet, ring VRF nullifiers need only temporarily storage, as eventually one expires the date in the VRF input. Asymptotically we thus only need $O(\texttt{users})$ storage vs the $O(\texttt{history})$ storage required by anonymous payment schemes like ZCash and blind signed tokens.

We further benefit from the "ring" credential format too, as opposed to certificate based designs like group signatures: We expect a degree of fraud whenever deploying purely certificate based systems, as witnessed by the litany of fraudulent TLS and covid certificates. Ring VRFs help mitigate fraudulent certificate concerns because the ring is a database and can be audited.

We know governments have ultimately little choice but to institute rationing in response to shortages caused by climate change, ecosystem collapse, and peak oil. Ring VRFs could help avoid ration card fraud, and thereby reduce social opposition, while also protecting essential privacy.

As an important caveat, ring VRFs need heavier verifiers than single-use tokens based on OPRFs [14] or blind signatures, but those credentials' heavy issuance phase represents a major adoption hurdle. A ring VRF systems issue fresh tokens almost non-interactively merely by adjusting allowed VRF input on resource names, dates, and bounds. This reduces complexity, simplifies scaling, and increases flexibility.

In particular, if governments issue ration cards based upon ring VRFs then these credentials could safely support other use cases, like free tiers in online services or games, and advertiser promotions, as well as identity applications like prevention of spam and online abuse.

In this, we need authenticated domain separation of products or identity consumers in queries to users' ring VRF credentials. We briefly discuss some sensible patterns in §10.2 below, but overall authenticated domain separation resemble TLS certificates except simpler in that roots of trust can self authenticate if root keys act as domain separators.

2 Protocol overview

As a beginning, we introduce the ring VRF interface, give a simple unamortized non-interactive zero-knowledge (NIZK) protocol that realizes the ring VRF properties discussed later in our UC model, and give some intuition for our later amortization trick. Similar to VRF [26], a ring VRF construction needs:

- $\mathsf{rVRF.KeyGen} : (1^\lambda) \mapsto (\mathsf{sk}, \mathsf{pk})$ algorithm, which creates a random secret key sk and associated public key pk;
- $\mathsf{rVRF.Eval} : (\mathsf{sk}, \mathsf{input}) \mapsto \mathsf{out}$ which deterministically computes the VRF output out from a secret key sk and a message input.

We demand a pseudo-randomness property from Eval. In our construction in §5, $\mathsf{rVRF.KeyGen}$ and $\mathsf{rVRF.Eval}$ resemble EC VRF like [28,29,19].

Different than VRF, a ring VRF scheme has the following algorithms operate directly upon set of public keys ring:

- $\mathsf{rVRF.Sign} : (\mathsf{sk}, \mathsf{ring}, \mathsf{input}) \mapsto \sigma$ returns a ring VRF signature σ for an input input.
- $\mathsf{rVRF.Ver} : (\mathsf{ring}, \mathsf{input}, \sigma) \mapsto \mathsf{out} \vee \perp$ returns either an output out or else failure $\perp$.

Ring VRFs differ from VRFs in that they do not expose a specific signer, and instead prove the signer's key lies in ring, much like how ring signatures differ from signatures. Ring VRFs differ from ring signatures in that the verification process of Ring VRFs outputs the evaluation output out of the signer if the signature is verified with ring. So the ring signature actually proves that out is the evaluation output of the signer.

After success verification, our verifier should be convinced that $\mathsf{pk} \in \mathsf{ring}$, that $\mathsf{out} = \mathsf{rVRF.Eval}(\mathsf{sk}, \mathsf{input})$ for some $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{rVRF.KeyGen}$. We demand anonymity meaning that the verifier learns nothing about the signer except that the signer's evaluation value of the signed message input is out and the signer's public key is in ring.

In other words, this simplified ring VRF could be instantiated by making $\mathsf{rVRF.Eval}$ a pseudo-random (hash) function, and using a NIZK for a relation

$$\mathcal{R}_{\mathsf{rvrf}} = \left\{ (\mathsf{out}, \mathsf{input}, \mathsf{ring}); (\mathsf{sk}, \mathsf{pk}) \;\middle|\; \begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{rVRF.KeyGen}, \quad \mathsf{pk} \in \mathsf{ring} \\ \mathsf{out} = \mathsf{rVRF.Eval}(\mathsf{sk}, \mathsf{input}) \end{array} \right\}$$

The zero-knowledge property of the NIZK ensures that our verifier learns nothing about the specific signer, except that their key is in the ring and maps input to out. Importantly, pseudo-randomness also says that out is an identity for the specific signer, but only within the context of input.

Aside from proving an evaluation using $\mathsf{rVRF.Eval}$, we always need $\mathsf{rVRF.Sign}$ and $\mathsf{rVRF.Ver}$ to sign some associated data ass, as otherwise the ring VRF signature become unmoored and permits replay attacks. As an example, our identity protocol below in §9 yields the same ring VRF outputs each time the same user logs into the same site, which suffers replay attacks unless ass binds the ring VRF signature to the TLS session.

Ring VRFs cannot so easily be combined with another signatures, which makes ass essential, but thankfully our ring VRF construction in in §5 expose ass exactly like EC VRFs should do .

If one used the rVRF interface described above, then one needs time $O(|\mathsf{ring}|)$ in $\mathsf{rVRF.Sign}$ and $\mathsf{rVRF.Ver}$ merely to read their ring argument, which severely limits applications. Instead, ring signatures run asymptotically faster by replacing the ring argument with a set commitment to ring, roughly like what ZCash does [22]. Therefore, we introduce the following algorithms for rVRF.

- $\mathsf{rVRF.CommitRing} : (\mathsf{ring}, \mathsf{pk}) \mapsto (\mathsf{comring}, \mathsf{opring})$ returns a commitment for a set ring of public keys, and optionally the opening opring if $\mathsf{pk} \in \mathsf{ring}$ as well.
- $\mathsf{rVRF.OpenRing} : (\mathsf{comring}, \mathsf{opring}) \mapsto \mathsf{pk} \vee \perp$ returns a public key pk, provided opring correctly opens the ring commitment $\mathsf{comring}$, or failure $\perp$ otherwise.

We thus replace the membership condition $\mathsf{pk} \in \mathsf{ring}$ in the above relation and NIZK by the opening condition $\mathsf{pk} = \mathsf{rVRF.OpenRing}(\mathsf{comring}, \mathsf{opring})$ for some known opring.

Although an asymptotic improvement, our opening $\mathsf{rVRF.OpenRing}$ based condition invariably still winds up being computationally expensive to prove inside a zkSNARK. We solve this obstacle in §6 by introducing *zero-knowledge continuations*, a new zkSNARK technique built from rerandomizable Groth16s [21] and designed for SNARK composition and reuse.

As a step towards this, we split the relation $\mathcal{R}_{\mathsf{rvrf}}$ into a relation $\mathcal{R}_{eval}$ for rVRF evaluation and a relation $\mathcal{R}_{\mathtt{ring}}$, which enforces our computationally expensive condition $\mathsf{pk} = \mathsf{rVRF.OpenRing}(\mathsf{comring}, \mathsf{opring})$. We want to reuse the proof for $\mathcal{R}_{\mathtt{ring}}$ across multiple rVRF signatures, so anonymity requires we rerandomize a Groth16 SNARK for $\mathcal{R}_{\mathtt{ring}}$ ala [3, Theorem 3, Appendix C, pp. 31]. Yet, we must connect together the NIZKs for the two languages $\mathcal{R}_{eval}$ and $\mathcal{R}_{\mathtt{ring}}$ that we define below informally. We do this by passing pk from $\mathcal{R}_{\mathtt{ring}}$ to $\mathcal{R}_{eval}$, which demands some hiding commitment compk to pk.

$$\mathcal{R}_{eval} = \left\{ (\mathsf{out}, \mathsf{input}, \mathsf{ass}, \mathsf{compk}); \mathsf{sk} \;\middle|\; \begin{array}{l} \mathsf{out} = \mathsf{rVRF.Eval}(\mathsf{sk}, \mathsf{input}), \\ \mathsf{compk} \text{ commits to } \mathsf{sk} \end{array} \right\}$$

$$\mathcal{R}_{\texttt{ring}} = \left\{ (\mathsf{compk}, \mathsf{comring}); (\mathsf{sk}, \mathsf{pk}) \;\middle|\; \begin{array}{l} \mathsf{compk} \text{ commits to } \mathsf{sk} \text{ with public key} \\ \mathsf{pk} = \mathsf{rVRF.OpenRing}(\mathsf{comring}, \mathsf{opring}) \end{array} \right\}$$

In §5, we introduce an extremely efficient NIZK for $\mathcal{R}_{eval}$, which also provides an essential proof-of-knowledge for compk.

3 Preliminaries

We briefly establish elliptic curve notion and recall some standard definitions and assumptions.

3.1 Elliptic curves

We obey mathematical and cryptographic implementation convention by adopting additive notation for elliptic curve and multiplicative notation for elliptic curve scalar multiplications and pairing target groups.

All object implicitly depend a security parameter λ. All protocols therefore have an implicit parameter generation algorithm, which output their hash functions, elliptic curves, and some independent base points on the elliptic curves.

We need an elliptic curve $\mathbb{G}$ over a field of characteristic q, equipped with a type III pairing $e : \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$, where the groups $\mathbf{G}_1 \le \mathbb{G}[\mathbb{F}_q]$, $\mathbf{G}_2 \le \mathbb{G}[\mathbb{F}_{q^2}]$, and $\mathbf{G}_T \le \mathbb{F}^*_{q^{12}}$ all have prime order $p \approx 2^{2\lambda}$.

We write $\mathbf{G}$ when discussing the Chaum-Pedersen DLEQ proofs, which do not employ pairings, but $\mathbf{G}$ always denotes $\mathbf{G}_1$ eventually. We avoid pairing unfriendly assumptions like DDH of course, but really we employ the algebraic group model (AGM) throughout.

We sweep cofactor concerns under the rug when discussing Groth16, where our pairings demand deserialization prove group membership in $\mathbf{G}_1$ or $\mathbf{G}_2$. We explicitly multiply by the effective cofactor h when doing Chaum-Pedersen DLEQ proofs though, as not doing so risks miss-reading by implementers. Yet, this becomes redundant if deserialization proves group membership, meaning $h = 1$.

We also let $\mathbb{J}$ denote a ZCash Sapling style "JubJub" Edwards curve over $\mathbb{F}_p$, with distinguished subgroup $\mathbf{J}$ of prime order $p_{\mathbf{J}}$, so that SNARKs on $\mathbb{G}$ prove $\mathbf{J}$ arithmetic relatively cheaply. Aside from Jubjub, we optionally want a "sister" Edwards curve $\mathbb{G}'$, with a subgroup $\mathbf{G}$ of the same order p as $\mathbf{G}_1$, but which lacks any pairing.

We let $H_p : \{0,1\}^* \to \mathbb{F}_p$ and $H_{\mathbf{G}'} : \{0,1\}^* \to \mathbf{G}'$ denote a hash-to-scalar and a hash-to-curve with ranges $\mathbb{F}_p$ and $\mathbf{G}'$, respectively, always modeled as random oracles. We only ever hash-to-$\mathbb{G}'$ because hash-to-$\mathbf{G}_1$ create a miss-use footgun for an anonymity protocol. Also hash-to-$\mathbb{G}'$ is faster. We let H' denote the hash to the VRF output space, usually a key derivation function plus a stream cipher, also modeled as a random oracle.

All our security proofs ignore these underlying elliptic curve concerns, so $\mathbf{G}_1 = \mathbf{G}'$ and cofactors are ignores. All hashes are random oracles. DDH is hard in $\mathbf{G}_1$ and $\mathbf{J}$. AGM is used for $\mathbb{G}$ in Groth16 sections, or wherever is convenient.

3.2 Zero-knowledge proofs

We let $\mathcal{R}$ denote a polynomial time decidable relation, so the language $\mathcal{L} = \{x \mid \exists \omega (x;\omega) \in \mathcal{R}\}$ lies in NP. All non-interactive zero-knowledge proof systems have some setup procedure `Setup` that takes some implicit parameters and some "circuit" description of $\mathcal{R}$, and may produces a structured reference string (SRS). We discuss SRSes and their toxic waste in §6 but SRSes remain implicit in our notation.

A non-interactive proof system for $\mathcal{L}$ consists of Prove and Ver PPT algorithms

- $\mathsf{NIZK}_\mathcal{R}.\mathsf{Prove}(x;\omega) \mapsto \pi$ creates a proof π for a witness and statement pair $(x;\omega) \in \mathcal{R}$.
- $\mathsf{NIZK}_\mathcal{R}.\mathsf{Ver}(x;\pi)$ returns either true of false, depending upon whether π proves x.

which satisfy the following completeness, zero-knowledge, and knowledge soundness definitions.

We always describe circuits as languages $\mathcal{L}$ and write $\mathsf{NIZK}_\mathcal{L}$ for two reasons: All SNARK circuits have many logic wires in $\mathcal{R}$ other than the public input wires x and the secret input witness wires ω. An existential quantifiers $\exists$ more clearly distinguishs public inputs x from secret input witnesses ω than tuple position. We also benefited from language in the preceding informal exposition, which did not always require specifying ω.

Definition 1. *We say* $\mathsf{NIZK}_\mathcal{R}$ *is* complete *if* $\mathsf{Ver}(x, \mathsf{Prove}(x;\omega))$ *succeeds for all* $(x;\omega) \in \mathcal{R}$.

Definition 2. *We say* $\mathsf{NIZK}_\mathcal{R}$ *is* zero-knowledge *if there exists a PPT simulator* $\mathsf{NIZK}_\mathcal{R}.\mathsf{Simulate}(x) \mapsto \pi$ *that outputs proofs for statement* $x \in L$ *alone, which are computationally indistinguishable from legitimate proofs by* Prove*, i.e. any non-uniform PPT adversary* V^* *cannot distinguish pairs* $(x;\pi)$ *generated by* Simulate *or by* Prove *except with odds negligible in* λ *(see [3, Def. 9, §A, pap. 29]).*

Definition 3. *We say* $\mathsf{NIZK}_\mathcal{R}$ *is* (white-box) knowledge sound *if for any non-uniform PPT adversary* P^* *who outputs a statement* $x \in \mathcal{L}$ *and proof* π *there exists a PPT extractor algorithm* Extract *that white-box observes* P^* *and if* $\mathsf{Ver}(x;\pi)$ *holds then* Extract *returns an* ω *for which* $(x;\omega) \in \mathcal{R}$ *(see [3, Def. 7, §A, pap. 29]).*

Our zero-knowledge continuations in §6 demand rerandomizing existing zk-SNARKs, which only Groth16 supports [21]. We therefore introduce some details of Groth16 [21] there, when we tamper with Groth16's SRS and `Setup` to create zero-knowledge continuations.

3.3 Universal Composability (UC) Model

We define the security of ring VRFs in the UC model [9,10]. In a nutshell, Canetti [9,10] defines the UC model as follows:

A protocol ϕ in the UC model is an execution between distributed interactive Turing machines (ITM). Each ITM has a storage to collect the incoming messages from other ITMs, adversary $\mathcal{A}$ or the environment $\mathcal{Z}$. $\mathcal{Z}$ is an entity to represent the external world outside of the protocol execution. The environment $\mathcal{Z}$ initiates ITM instances (ITIs) and the adversary $\mathcal{A}$ with arbitrary inputs and then terminates them to collect the outputs. We identify an ITI with its session identity sid and its ITM's identifier pid. In this paper, when we call an entity as a party in the UC model we mean an ITI with the identifier $(\mathsf{sid}, \mathsf{pid})$.

We define the ideal world where there exists an ideal functionality $\mathcal{F}$ and the real world where a protocol ϕ is run as follows:

Real world: $\mathcal{Z}$ initiates ITMs and $\mathcal{A}$ to run the protocol instance with some input $z \in \{0,1\}^*$ and a security parameter λ. After $\mathcal{Z}$ terminates the protocol instance, we denote the output of the real world by the random variable $\mathsf{EXEC}(\lambda, z)_{\phi,\mathcal{A},\mathcal{Z}} \in \{0,1\}$. Let $\mathsf{EXEC}_{\phi,\mathcal{A},\mathcal{Z}}$ denote the ensemble $\{\mathsf{EXEC}(\lambda, z)_{\phi,\mathcal{A},\mathcal{Z}}\}_{z\in\{0,1\}^*}$.

Ideal world: $\mathcal{Z}$ initiates ITMs and a simulator Sim to contact with the ideal functionality $\mathcal{F}$ with some input $z \in \{0,1\}^*$ and a security parameter λ. $\mathcal{F}$ is trusted meaning that it cannot be corrupted. Sim forwards all messages forwarded by $\mathcal{Z}$ to $\mathcal{F}$. The output of execution with $\mathcal{F}$ is denoted by a random variable $\mathsf{EXEC}(\lambda, z)_{\mathcal{F},\mathsf{Sim},\mathcal{Z}} \in \{0,1\}$. Let $\mathsf{EXEC}_{\mathcal{F},\mathsf{Sim},\mathcal{Z}}$ denote the ensemble $\{\mathsf{EXEC}(\lambda, z)_{\mathcal{F},\mathsf{Sim},\mathcal{Z}}\}_{z\in\{0,1\}^*}$.

Definition 4 (UC-Security of ϕ). *Given a real world protocol ϕ and an ideal functionality $\mathcal{F}$ for the protocol ϕ, we call that ϕ is UC-secure i.e., ϕ UC-realizes $\mathcal{F}$, if for all PPT adversaries $\mathcal{A}$, there exists a simulator* Sim *such that for any environment $\mathcal{Z}$,* $\mathsf{EXEC}_{\phi,\mathcal{A},\mathcal{Z}}$ *is indistinguishable from* $\mathsf{EXEC}_{\mathcal{F},\mathsf{Sim},\mathcal{Z}}$.

4 Security Model of Ring Verifiable Random Function

In this section, we define formally a ring VRF scheme and model its security in the UC model.

Definition 5 (Ring VRF). *A ring VRF scheme is defined with public parameters pp generated by a setup algorithm* $\mathsf{rVRF.Setup}(1^\lambda)$ *and with the following algorithms.*

- $\mathsf{rVRF.KeyGen}(pp) \to (\mathsf{sk}, \mathsf{pk})$*: It is a PPT algorithm and generates a secret key and public key pair* $(\mathsf{sk}, \mathsf{pk})$ *given input pp.*
- $\mathsf{rVRF.Eval}(\mathsf{sk}_i, \mathsf{input}) \to y$*: It is a deterministic polynomial time algorithm and outputs an evaluation value $y \in \mathcal{S}_{eval}$ given input* sk_i *and* input. *Here, $\mathcal{S}_{eval}$ is the domain of evaluation values and defined in pp.*

The following algorithms need an input $\mathsf{ring} = \{\mathsf{pk}_1, \mathsf{pk}_2, \ldots, \mathsf{pk}_n\}$ *that we call ring:*

- $\mathsf{rVRF.CommitRing}(\mathsf{ring}, \mathsf{pk}) \rightarrow (\mathsf{comring}, \mathsf{opring})$*: It is a PPT algorithm and outputs a commitment of* ring *with the opening* opring *given input* ring *and* $\mathsf{pk} \in \mathsf{ring}$*.*
- $\mathsf{rVRF.OpenRing}(\mathsf{comring}, \mathsf{opring}) \rightarrow \mathsf{pk}$*: It is a PPT algorithm and outputs a public key* pk *given input* $\mathsf{comring}$ *and* opring*.*
- $\mathsf{rVRF.Sign}(\mathsf{sk}_i, \mathsf{comring}, \mathsf{opring}, \mathsf{input}, \mathsf{ass}) \rightarrow \sigma$*: It is a PPT algorithm and outputs a ring signature* σ *that signs a message* $\mathsf{input} \in \{0,1\}^*$ *and an associated data* $\mathsf{ass} \in \{0,1\}^*$ *with* sk_i *for* $\mathsf{comring}$ *if .*
- $\mathsf{rVRF.Ver}(\mathsf{comring}, \mathsf{input}, \mathsf{ass}, \sigma) \rightarrow (b, y)$*: It is a deterministic polynomial time algorithm and outputs* $b \in \{0,1\}$ *and* $y \in \mathcal{S}_{eval} \cup \{\perp\}$*.* $b = 1$ *means verified and* $b = 0$ *means not verified.*

We note that all algorithms above have pp as part of their input even if we do not always explicitly write it.

We note that $\mathsf{rVRF.CommitRing}$ and $\mathsf{rVRF.OpenRing}$ are optional algorithms of a ring VRF scheme. If they are not defined, we should let $\mathsf{comring} = \mathsf{ring}$ and $\mathsf{opring} = \mathsf{pk}$. $\mathsf{rVRF.CommitRing}$ and $\mathsf{rVRF.OpenRing}$ are functional for a succinct verification process in case of having large set of ring.

The security properties that we want to achieve in a ring VRF scheme are informally as follows: *correctness* meaning that when an honest signer with key $(\mathsf{sk}_i, \mathsf{pk}_i)$ outputs σ by running $\mathsf{rVRF.Sign}(\mathsf{sk}_i, \mathsf{comring}, \mathsf{opring}, \mathsf{input}, \mathsf{ass})$, $\mathsf{rVRF.Ver}(\mathsf{comring}, \mathsf{input}, \mathsf{ass}, \sigma)$ must output $b = 1$ and y which is equal to $\mathsf{rVRF.Eval}(\mathsf{sk}_i, \mathsf{input})$ if and only if $\mathsf{rVRF.OpenRing}(\mathsf{comring}, \mathsf{opring}) \rightarrow \mathsf{pk}_i \in \mathsf{ring}$, *randomness* meaning that an evaluation value is random and independent from the message and the public key, *determinism* meaning that $\mathsf{rVRF.Eval}$ is deterministic, *anonymity* meaning that $\mathsf{rVRF.Sign}$ does not give any information about its signer, *unforgeability* meaning that an adversary should not forge a ring signature and *uniqueness* meaning that number of verified evaluation values should not be more than the number of the keys in the ring.

We could define all these security properties formally in the standard model but this might cause the composability issues when the ring VRF protocol composed with other protocols. Considering the applications of ring VRF protocol, we want to achieve stronger security guarantees in different environments. Therefore, we define the security of a ring VRF scheme in the UC model in Section 4.1.

One can consider a ring VRF scheme is a combination of a VRF scheme and a ring signature scheme where $\mathsf{rVRF.Eval}$ is similar to Eval algorithm of a VRF scheme and $\mathsf{rVRF.Sign}$ is similar to Sign algorithm of a ring signature scheme. The subtle difference is in $\mathsf{rVRF.Ver}$ that works similar to both Ver of ring signature and VRF schemes. $\mathsf{rVRF.Ver}$ does not need the signer's public key to verify a ring signature as in a ring signature scheme but it outputs the signer's evaluation value for every verified signature. If y is generated independent from the signer's key, $\mathsf{rVRF.Ver}(\mathsf{ring}, \mathsf{input}, \mathsf{ass}, \sigma)$ does not reveal any identity of the signer except that the signer's key is in the ring.

We remark that the output of $\mathsf{rVRF.Eval}$ does not depend on a ring. Therefore, if a signer P with key sk signs a message input for ring and later wants to reveal that it signed input for ring, P should sign input with another ring $\{\mathsf{sk}\}$. Since the verification of both signatures outputs the same evaluation value, the verifier can be convinced that P signed the both signatures. Hence, a ring VRF scheme can link the identities of the signers if it is necessary.

4.1 Ring Verifiable Random Function in the UC Model

We introduce a ring VRF functionality $\mathcal{F}_{\mathsf{rvrf}}$ to model execution of a ring VRF protocol in the ideal world. In other words, we define a ring VRF protocol in the case of having a trusted entity $\mathcal{F}_{\mathsf{rvrf}}$. There are many straightforward ways of defining a ring VRF protocol in the ideal world satisfying the desired security properties. However, defining simple and intuitive functionality while being as expressive and realizable in the real world execution is usually at odds [9]. Therefore, we have a lengthy $\mathcal{F}_{\mathsf{rvrf}}$ (See Figure 1) which satisfies the security properties that we expect from a ring VRF scheme and at the same time faithful to the reality as possible. For the sake of clarity and accessibility, we split each execution part of $\mathcal{F}_{\mathsf{rvrf}}$ while we introduce our functionality. The composition of all parts is in Figure 1 in Appendix. We first describe how $\mathcal{F}_{\mathsf{rvrf}}$ works and then show which security properties it achieves.

$\mathcal{F}_{\mathsf{rvrf}}$ has tables to store the data generated from the requests from honest parties and the adversary Sim. The table `verification_keys` keeps the keys of parties. The other table `anonymous_key_map` stores an anonymous key that corresponds to an evaluation input of a party with a key pk. We note that the real execution of a ring VRF (Definition 5) does not have a concept of an anonymous key but $\mathcal{F}_{\mathsf{rvrf}}$ needs this internally to execute the verification of a ring signature. Related to anonymous keys, $\mathcal{F}_{\mathsf{rvrf}}$ also stores all anonymous keys of all malicious signatures for a ring and input in a table $\mathcal{W}$. Finally, $\mathcal{F}_{\mathsf{rvrf}}$ stores the evaluations values of a party in `evaluations`. In a nutshell, given pk and input, $\mathcal{F}_{\mathsf{rvrf}}$ generates an anonymous key W as explained below and sets `anonymous_key_map`$[\mathsf{input}, W]$ to pk. Then, it generates an evaluation value y as explained below and sets `evaluations`$[\mathsf{input}, W]$ to y. In short, given honestly generated secret, public key pair $(\mathsf{sk}, \mathsf{pk})$ in the real world, the algorithm $\mathsf{rVRF.Eval}(\mathsf{sk}, \mathsf{input})$ that outputs evaluation value corresponds to generating an anonymous key W for $\mathsf{pk}, \mathsf{input}$ and obtaining the evaluation value stored in `evaluations`$[\mathsf{input}, W]$ in the ideal world. The functionality of all these tables and anonymous key will be more clear while we explain $\mathcal{F}_{\mathsf{rvrf}}$ in detail. $\mathcal{F}_{\mathsf{rvrf}}$ consists of the following execution parts.

Key Generation: Whenever an honest party requests a key, $\mathcal{F}_{\mathsf{rvrf}}$ obtains a key pair (x, pk) from Sim. $\mathcal{F}_{\mathsf{rvrf}}$ stores them if they have not been recorded. If it is the case, $\mathcal{F}_{\mathsf{rvrf}}$ gives only pk to the honest party. $\mathcal{F}_{\mathsf{rvrf}}$ will later use x during signature generation of this honest party. One can imagine x as a secret key and pk as a public key. We note that it is not a problem in the ideal model that the adversary generates the secret key because a signature generated by an honest key can be valid if and only if the corresponding honest party requests it as it is guaranteed during the verification process of $\mathcal{F}_{\mathsf{rvrf}}$.

[Key Generation.] upon receiving a message $(\mathsf{keygen}, \mathsf{sid})$ from a party P_i, send $(\mathsf{keygen}, \mathsf{sid}, \mathsf{P}_i)$ to the simulator Sim. Upon receiving a message $(\mathsf{verificationkey}, \mathsf{sid}, x, \mathsf{pk})$ from Sim, verify that x, pk has not been recorded before for sid i.e., there exists no (x', pk') in `verification_keys` such that $x' = x$ or $\mathsf{pk}' = \mathsf{pk}$. If it is the case, store in the table `verification_keys`, under P_i, the value x, pk and return $(\mathsf{verificationkey}, \mathsf{sid}, \mathsf{pk})$ to P_i.

Corruption: Sim can corrupt any honest party at any time. So, $\mathcal{F}_{\mathsf{rvrf}}$ provides security against adaptive adversary.

[Corruption:] upon receiving $(\mathsf{corrupt}, \mathsf{sid}, \mathsf{P}_i)$ from Sim, remove (x_i, pk_i) from `verification_keys`$[\mathsf{P}_i]$ and store them to `verification_keys` under Sim. Return $(\mathsf{corrupted}, \mathsf{sid}, \mathsf{P}_i)$.

Malicious Ring VRF Evaluation: This part of $\mathcal{F}_{\mathsf{rvrf}}$ is for Sim in case of Sim wants to evaluate an input for a malicious key. For this, it should provide to $\mathcal{F}_{\mathsf{rvrf}}$ an input input, a malicious key pk and an anonymous key W. Then, $\mathcal{F}_{\mathsf{rvrf}}$ evaluates input with pk if an anonymous key $W' \neq W$ is not assigned to input and pk before. If it is the case, it returns an evaluation value `evaluations`$[\mathsf{input}, W]$ which is selected randomly. The reason of conditioning on a unique anonymous key for input and pk is to prevent Sim to obtain more than one evaluation values corresponding to input and pk. This is necessary to have a uniqueness property. We remark that it is possible that Sim obtains the same evaluation value of input with two different malicious public keys $\mathsf{pk}_i, \mathsf{pk}_j$ by sending $(\mathsf{eval}, \mathsf{sid}, \mathsf{pk}_i, W, \mathsf{input})$ and $(\mathsf{eval}, \mathsf{sid}, \mathsf{pk}_j, W, \mathsf{input})$. However, this does not break the uniqueness property.

[Malicious Ring VRF Evaluation.] upon receiving a message $(\mathsf{eval}, \mathsf{sid}, \mathsf{pk}_i, W, \mathsf{input})$ from Sim, if pk_i is recorded under an honest party's identity or if there exists $W' \neq W$ where `anonymous_key_map`$[\mathsf{input}, W'] = \mathsf{pk}_i$, ignore the request. Otherwise, record in the table `verification_keys` the value pk_i under Sim if pk_i is not in `verification_keys`.
If `anonymous_key_map`$[\mathsf{input}, W]$ is not defined before, set `anonymous_key_map`$[\mathsf{input}, W] = \mathsf{pk}_i$ and let $y \leftarrow\$ \mathcal{S}_{eval}$ and set `evaluations`$[\mathsf{input}, W] = y$.
In any case (except ignoring), obtain $y =$ `evaluations`$[\mathsf{input}, W]$ and return $(\mathsf{evaluated}, \mathsf{sid}, \mathsf{input}, \mathsf{pk}_i, W, y)$ to P_i.

We remark that once Sim obtains an anonymous key W of input and honest key pk, Sim can learn the evaluation of input with pk without knowing the pk

via malicious ring VRF evaluation i.e., send the message $(\mathsf{eval}, \mathsf{sid}, \mathsf{pk}_i, W, \mathsf{input})$ where pk_i is a malicious verification key. Here, if W is an anonymous key of $\mathsf{input}, \mathsf{pk}$, $\mathcal{F}_{\mathsf{rvrf}}$ returns $\mathtt{evaluations}[\mathsf{input}, W]$ even if $\mathsf{pk} \neq \mathsf{pk}_i$. We note that this leakage does not contradicts the desired security properties and helps us to prove our ring VRF protocol realizes $\mathcal{F}_{\mathsf{rvrf}}$.

Honest Ring VRF Signature and Evaluation: This part of $\mathcal{F}_{\mathsf{rvrf}}$ works for honest parties who evaluate input and generate a ring signature for a ring. An honest party P_i should provide to $\mathcal{F}_{\mathsf{rvrf}}$ a ring consisting of set of public keys, its own public key pk_i, optionally an associated data ass and a message input to be signed and evaluated. Then, $\mathcal{F}_{\mathsf{rvrf}}$ generates the evaluation value of input and pk_i and signs input with associated data ass for given ring if $\mathsf{pk}_i \in \mathsf{ring}$. The evaluation for honest parties works as follows: If $\mathcal{F}_{\mathsf{rvrf}}$ does not select an anonymous key for input and pk_i before, it samples randomly an anonymous key W and samples randomly the evaluation value y. The ring signature generation works as follows: $\mathcal{F}_{\mathsf{rvrf}}$ runs a PPT algorithm $\mathsf{Gen}_{sign}(\mathsf{ring}, W, x, \mathsf{pk}, \mathsf{ass}, \mathsf{input})$ and obtains the ring signature σ. It records $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$ for the verification process where 1 indicates that σ is a valid ring signature of input and ass generated for ring with the anonymous key W.

[**Honest Ring VRF Signature and Evaluation.**] upon receiving a message $(\mathsf{sign}, \mathsf{sid}, \mathsf{ring}, \mathsf{pk}_i, \mathsf{ass}, \mathsf{input})$ from P_i, verify that $\mathsf{pk}_i \in \mathsf{ring}$ and that there exists a public key pk_i associated to P_i in $\mathtt{verification\_keys}$. If it is not the case, just ignore the request. If there exists no W' such that $\mathtt{anonymous\_key\_map}[\mathsf{input}, W'] = \mathsf{pk}_i$, let $W \leftarrow\!\!\$\ \mathcal{S}_W$ and let $y \leftarrow\!\!\$\ \mathcal{S}_{eval}$. If there exists W where $\mathtt{anonymous\_key\_map}[\mathsf{input}, W]$ is defined, then abort. Here, $\mathcal{S}_W$ is the domain of honest anonymous keys. Otherwise, set $\mathtt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_i$ and set $\mathtt{evaluations}[\mathsf{input}, W] = y$.
In any case (except ignoring and aborting), obtain W, y where $\mathtt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_i$ and $\mathtt{evaluations}[\mathsf{input}, W] = y$ and run $\mathsf{Gen}_{sign}(\mathsf{ring}, W, x, \mathsf{pk}, \mathsf{ass}, \mathsf{input}) \rightarrow \sigma$. Record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$. Return $(\mathsf{signature}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, y, \sigma)$ to P_i.

Malicious Requests of Signatures: If Sim provides $\mathsf{ring}, W, \mathsf{ass}, \mathsf{input}$, Sim obtains all valid and stored ring signatures of input and ass generated for ring with an anonymous key W.

[**Malicious Requests of Signatures.**] upon receiving a message $(\mathsf{signs}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input})$ from Sim, obtain all existing valid signatures σ such that $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$ is recorded and add them in a list $\mathcal{L}_\sigma$. Return $(\mathsf{signs}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \mathcal{L}_\sigma)$ to Sim.

Ring VRF Verification: This part of $\mathcal{F}_{\mathsf{rvrf}}$ is to check whether a ring signature of σ signs input and ass for ring with anonymous key W. This part should correspond to $\mathsf{rVRF.Ver}$ in the real world ring VRF protocol. Therefore, $\mathcal{F}_{\mathsf{rvrf}}$ first checks various conditions to decide whether the signature is valid. If the signature is verified, $\mathcal{F}_{\mathsf{rvrf}}$ outputs $b = 1$ and $y = \mathtt{evaluations}[\mathsf{input}, W]$. Otherwise, it outputs $b = 0$ and $y = \perp$.

For the verification of the signature, $\mathcal{F}_{\mathsf{rvrf}}$ first checks its records to see whether this signature is verified or unverified in its records i.e., checks whether $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, b']$ is recorded (See C1). If it is recorded, $\mathcal{F}_{\mathsf{rvrf}}$ lets $b = b'$ to be consistent. Otherwise, it checks whether W is an anonymous key of an honest party generated for input (See C2). If it is the case, $\mathcal{F}_{\mathsf{rvrf}}$ checks its records whether this honest party requested signing input and ass for ring. If there exists such record i.e., $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, ., 1]$, it stores the new signature σ as a valid signature in its records and lets $b = 1$. Remark that Sim can create arbitrary verified signatures that sign any input and ass for ring with W once the honest party owning W has requested signing input and ass for ring. This does not break the forgeability property because the honest party has already signed for it. If none of the above conditions (C1 and C2) holds, it means that σ could be a signature generated for a malicious party. Therefore, $\mathcal{F}_{\mathsf{rvrf}}$ asks about it to Sim and Sim replies with an indicator b_{Sim} showing that σ is valid or not and a public key $\mathsf{pk}_{\mathsf{Sim}}$. Then, $\mathcal{F}_{\mathsf{rvrf}}$ checks various conditions to prevent Sim forging and violating the uniqueness. To prevent forging, it lets directly $b = 0$, if $\mathsf{pk}_{\mathsf{Sim}}$ is a key of an honest party. If $\mathsf{pk}_{\mathsf{Sim}}$ is not an honest key, then $\mathcal{F}_{\mathsf{rvrf}}$ checks its table $\mathcal{W}[\mathsf{input}, \mathsf{ring}]$ which stores the anonymous keys of valid malicious signatures of input for ring. If the number of anonymous keys in $\mathcal{W}[\mathsf{input}, \mathsf{ring}]$ is greater than or equal to the number of malicious keys in ring, then $\mathcal{F}_{\mathsf{rvrf}}$ invalidates σ by letting $b = 0$. This condition guarantees uniqueness meaning that the number of verifying evaluation values that Sim can generate for $\mathsf{input}, \mathsf{ring}$ is at most the number of malicious keys in ring. If the number of malicious anonymous keys of valid signatures does not exceed the number of malicious keys in ring, then $\mathcal{F}_{\mathsf{rvrf}}$ checks whether W is a unique anonymous key assigned to $\mathsf{input}, \mathsf{pk}_{\mathsf{Sim}}$ as in the "Malicious Ring VRF Evaluation". If W is unique then $\mathcal{F}_{\mathsf{rvrf}}$ lets $b = b_{\mathsf{Sim}}$.

After deciding b, $\mathcal{F}_{\mathsf{rvrf}}$ records it as $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, b]$ to be able to reply with the same b for the same verification query later. If $b = 1$, $\mathcal{F}_{\mathsf{rvrf}}$ returns $\mathtt{evaluations}[\mathsf{input}, W]$ as well.

[Ring VRF Verification.] upon receiving a message $(\mathsf{verify}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma)$ from a party, do the following:

C1 If there exits a record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, b']$, set $b = b'$.
C2 Else if $\texttt{anonymous\_key\_map}[\mathsf{input}, W]$ is an honest verification key and there exists a record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma', 1]$ for any σ', then let $b = 1$ and record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$.
C3 Else relay the message $(\mathsf{verify}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma)$ to Sim and receive back the message $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma, b_{\mathsf{Sim}}, \mathsf{pk}_{\mathsf{Sim}})$. Then check the following:
1. If $\mathsf{pk}_{\mathsf{Sim}}$ is an honest verification key, set $b = 0$.
2. Else if $W \notin \mathcal{W}[\mathsf{input}, \mathsf{ring}]$ and $|\mathcal{W}[\mathsf{input}, \mathsf{ring}]| \geq |\mathsf{ring}_{mal}|$ where ring_{mal} is a set of malicious keys in ring, set $b = 0$. .
3. Else if there exists $W' \neq W$ where $\texttt{anonymous\_key\_map}[\mathsf{input}, W'] = \mathsf{pk}_{\mathsf{Sim}}$, set $b = 0$.
4. Else set $b = b_{\mathsf{Sim}}$.

In the end, record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 0]$ if it is not stored. If $b = 0$, let $y = \perp$. Otherwise, do the following:

- if $W \notin \mathcal{W}[\mathsf{input}, \mathsf{ring}]$, add W to $\mathcal{W}[\mathsf{input}, \mathsf{ring}]$.
- if $\texttt{evaluations}[\mathsf{input}, W]$ is not defined, set $\texttt{evaluations}[\mathsf{input}, W] \leftarrow\$ \mathcal{S}_{eval}$, $\texttt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_{\mathsf{Sim}}$. Set $\texttt{evaluations}[\mathsf{input}, W] = y$.
- otherwise, set $y = \texttt{evaluations}[\mathsf{input}, W]$.

Finally, output $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma, y, b)$ to the party.

In real-world ring VRF, the verification algorithm outputs the corresponding evaluation value of the signer. Therefore, $\mathcal{F}_{\mathsf{rvrf}}$ outputs the signer's evaluation value if the signature is verified. However, it achieves this together with the anonymous key which is not defined in the ring VRF in the real world. If $\mathcal{F}_{\mathsf{rvrf}}$ did not define an anonymous key for each signature, then there would be no way that $\mathcal{F}_{\mathsf{rvrf}}$ determines the signer's key and outputs the evaluation value because σ does not need to be associated with the signer's key for the sake of anonymity. Therefore, $\mathcal{F}_{\mathsf{rvrf}}$ maps a random and independent anonymous key to each input and pk so that this key behaves as if it is the verification key of the signature. Since it is random and independent from input and pk, it does not leak any information about the signer during the verification but it still allows $\mathcal{F}_{\mathsf{rvrf}}$ to distinguish the signer.

$\mathcal{F}_{\mathsf{rvrf}}$ achieves the following security properties. We note that when we say the evaluation value of $(\mathsf{input}, \mathsf{pk}_i)$, we mean $\texttt{evaluations}[\mathsf{input}, W]$ where $\texttt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_i$.

Randomness: The evaluation value of $(\mathsf{input}, \mathsf{pk}_i)$ is randomly selected independent from $(\mathsf{input}, \mathsf{pk}_i)$ for keys pk_i and input's. The evaluation value of pairs in

$\{(\mathsf{input}, \mathsf{pk}_i)\}$ with an anonymous key W provided by Sim is randomly selected independent from $\{(\mathsf{input}, \mathsf{pk}_i)\}$ for all malicious keys pk_i and input's.

Evaluation of $(\mathsf{input}, \mathsf{pk}_i)$ where pk_i is an honest key is generated by first assigning a random anonymous key W to it and then assigning a random evaluation value y to (input, W). So, honest evaluations are always random and independent from $(\mathsf{input}, \mathsf{pk}_i)$. Malicious evaluation value of pairs $\{(\mathsf{input}, \mathsf{pk}_i)\}$ with the same anonymous W is $\mathtt{evaluations}[\mathsf{input}, W]$ which is sampled randomly and independently from $\{(\mathsf{input}, \mathsf{pk}_j)\}$ by $\mathcal{F}_{\mathsf{rvrf}}$.

Determinism: Once evaluation value of $(\mathsf{input}, \mathsf{pk}_i)$ is unique and cannot be changed.

The evaluation value of $(\mathsf{input}, \mathsf{pk}_i)$ where pk_i is honest is unique and cannot be changed for honest parties because the anonymous key of it selected only once. Similarly, The evaluation value of $(\mathsf{input}, \mathsf{pk}_i)$ where pk_i is malicious is unique and cannot be changed because $\mathcal{F}_{\mathsf{rvrf}}$ does not allow Sim to select two different anonymous keys for $(\mathsf{input}, \mathsf{pk}_i)$ and to update the anonymous key.

Unforgeability: If an honest party with a public key pk never signs a message input and an associated data ass for a ring ring, then no party can generate a forgery of input and ass for ring signed by pk. Formally, if an honest party with pk never sends a message $(\mathsf{sign}, \mathsf{sid}, \mathsf{ring}, \mathsf{pk}, \mathsf{ass}, \mathsf{input})$ for any $\mathsf{ring}, \mathsf{input}, \mathsf{ass}$, then no party can create a record in $\mathcal{F}_{\mathsf{rvrf}}$ such that $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$ where $\mathtt{anonymous\_key\_map}[\mathsf{input}, \mathsf{pk}] = W$.

Sim cannot create a forgery by sending a message $(\mathsf{sign}, \mathsf{sid}, \mathsf{ring}, \mathsf{pk}, \mathsf{ass}, \mathsf{input})$ to $\mathcal{F}_{\mathsf{rvrf}}$ because $\mathcal{F}_{\mathsf{rvrf}}$ checks whether the sender's key is pk to generate a signature. Another way for Sim to create a forgery is by sending an honest key $\mathsf{pk}_{\mathsf{Sim}}$ in C3 in Figure 1. However, it is not allowed by $\mathcal{F}_{\mathsf{rvrf}}$ in the condition C3-2 neither.

Uniqueness: We call that an evaluation value y for a message input is verified for ring, if there exists a signature σ such that $\mathcal{F}_{\mathsf{rvrf}}$ returns $(y, 1)$ for a query $(\mathsf{verify}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma)$ for any anonymous key W and associated data ass. The uniqueness property guarantees that the number of verified evaluation values via signatures for a message input and ring is not more than $|\mathsf{ring}|$.

If $\mathcal{F}_{\mathsf{rvrf}}$ outputs $(1, y)$, it means that there exists a record $[\mathsf{input}, ., W, \mathsf{ring}, \sigma, 1]$ and $y = \mathtt{evaluations}[\mathsf{input}, W]$, $\mathtt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}$. If pk is an honest key, then it means that $\mathsf{pk} \in \sigma$ because $\mathcal{F}_{\mathsf{rvrf}}$ generates a signature for an honest party with a key if $\mathsf{pk} \in \mathsf{ring}$. Let's assume that there exist more verified evaluation values for ring

The evaluation value of $\mathsf{input}, \mathsf{pk}_i$ is unique and fixed thanks to the determinism. Uniqueness is broken if the number of verified evaluation values of input for ring is greater than the number of anonymous keys that verify a signature that signs input for ring. Assume that there exist t different verified evaluation values $\mathcal{Y} = \{y_1, y_2, \ldots, y_t\}$ of a message input for ring where $|\mathsf{ring}| = t - 1$. This implies that for each $y_i \in \mathcal{Y}$, there exists a record $[\mathsf{input}, \mathsf{ass}_i, W_i, \mathsf{ring}, \sigma_i, 1]$ such that $\mathtt{evaluations}[\mathsf{input}, W_i] = y_i$ where $\mathtt{anonymous\_key\_map}[\mathsf{input}, W_i] = \mathsf{pk}_i$ and $W_i \neq W_j$ for all $i, j \in [1, t]$. We know from the determinism property

$\mathsf{pk}_i \neq \mathsf{pk}_j$ for all $i \neq j \in [1, t]$. If pk_i is an honest key, it means that σ_i is not a forgery so $\mathsf{pk}_i \in \mathsf{ring}$. Therefore, each honest evaluation value in $\mathcal{Y}$ maps to one honest public key in ring meaning that honest evaluation values in $\mathcal{Y}$ is at most $|\mathsf{ring} \setminus \mathsf{ring}_{mal}| = n_h$. If pk_i is not an honest verification key, $W_i \in \mathcal{W}[\mathsf{input}, \mathsf{ring}]$ since $\mathcal{F}_{\mathsf{rvrf}}$ adds W_i to $\mathcal{W}[\mathsf{input}, \mathsf{ring}]$ whenever it creates such record for a malicious signature. $\mathcal{F}_{\mathsf{rvrf}}$ makes sure that in the condition C3-1 that $\mathcal{W}[\mathsf{input}, \mathsf{ring}] \leq |\mathsf{ring}_{mal}| = n_m$. Therefore, $t \leq n_h + n_m = |\mathsf{ring}|$ which is a contradiction.

We note that Sim in our functionality can generate a valid ring signature σ that signs input with a malicious key pk for ring where the malicious key is not in ring i.e., $\mathcal{F}_{\mathsf{rvrf}}$ can have a record for a malicious signature σ such that $[\mathsf{input}, ., W_i, \mathsf{ring}, \sigma, 1]$ and $\texttt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk} \notin \mathsf{ring}$. However, it cannot create signatures of input for ring which $\mathcal{F}_{\mathsf{rvrf}}$ verifies and outputs more than $|\mathsf{ring}_{mal}|$ different evaluation values.

Anonymity: An honest signature σ signs a message input verified by a ring and anonymous key W does not give any information about its signer except that its key is in pk if input is not signed by the same signer before for any other ring. We define this formally with the anonymity game below. We note that we cannot define and verify this property in $\mathcal{F}_{\mathsf{rvrf}}$ as the other properties because it depends on how Gen_{sign} is defined.

Definition 6 (Anonymity). *We define the anonymity game against a special environment $\mathcal{D}$ which plays the following anonymity game. $\mathcal{F}_{\mathsf{rvrf}}$ satisfies anonymity, if any PPT distinguisher $\mathcal{D}$ has a negligible advantage in λ to win the anonymity game defined as follows: We define the anonymity game between a challenger and $\mathcal{D}$. $\mathcal{D}$ accesses a signing oracle $\mathcal{O}_{Sign}$ and $\mathcal{F}_{\mathsf{rvrf}}$ simulated by the challenger as described in Figure 1.*

- *Given the input $'\mathsf{keygen}'$, $\mathcal{O}_{Sign}$ sends $(\mathsf{keygen}, \mathit{sid})$ to the challenger and obtains a verification key pk. Then, it stores pk to a list $\mathcal{K}$ and outputs pk.*
- *Given the input $'(\mathsf{pk}, \mathsf{ring}, \mathsf{ass}, \mathsf{input})'$, $\mathcal{O}_{Sign}$ sends $(\mathsf{sign}, \mathit{sid}, \mathsf{ring}, \mathsf{pk}, \mathsf{ass}, \mathsf{input})$ to the challenger and receives $(\mathsf{signature}, \mathit{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, y, \sigma)$ if $\mathsf{pk} \in \mathsf{ring}$. Then $\mathcal{O}_{Sign}$ stores input to a list $\mathsf{signed}[\mathsf{pk}]$. It outputs (σ, W). Otherwise, it outputs $\perp$.*

At some point, $\mathcal{D}$ sends $(\mathsf{ring}, \mathsf{pk}_0, \mathsf{pk}_1, \mathsf{input}, \mathsf{ass})$ to the challenger where $\mathsf{pk}_0, \mathsf{pk}_1 \in \mathsf{ring}$, $\mathsf{input} \notin \mathsf{signed}[\mathsf{pk}_0]$ and $\mathsf{input} \notin \mathsf{signed}[\mathsf{pk}_1]$. Challenger lets $b \leftarrow_r \{0, 1\}$. Then it gives the input $(\mathsf{pk}_b, \mathsf{ring}, \mathsf{input}, \mathsf{ass})$ to $\mathcal{O}\mathsf{Sign}$ and receives either $\perp$ or (σ, W). If it is (σ, W), it sends (σ, W) to $\mathcal{D}$ as a challenge. If $\mathcal{D}$ sends $'(\mathsf{pk}, \mathsf{ring}, \mathsf{ass}, \mathsf{input})'$ to $\mathcal{O}_{Sign}$ where $\mathsf{pk} = \mathsf{pk}_0$ or $\mathsf{pk} = \mathsf{pk}_1$, it loses the game. During the game if $\mathcal{D}$ outputs $b' = b$, $\mathcal{D}$ wins.

We remark that $\mathcal{D}$ generates keys of honest parties and forwards them via dummy adversaries in the ideal model. So, Gen_{sign} of $\mathcal{F}_{\mathsf{rvrf}}$ should be defined in a way that it preserves the anonymity even if $\mathcal{D}$ generates the keys.

5 Ring VRF construction

We now construct our ring VRF contruction with an efficient evaluation proof, which we call the Pedersen VRF and denote PedVRF. PedVRF instantiates the NIZK for the relation $\mathcal{R}_{\texttt{eval}}$ introduced in a general form in §2. In this section we focus upon Pedersen VRF and relations describing its SNARK for ring membership and we discuss the zero-knowledge continuation that makes the overall ring VRF efficient in the next section.

Our construction works with public parameters $pp = (p, \mathbf{G}, G, K, \mathcal{S}_{eval} = \mathbb{F}_p)$ generated by $\mathsf{rVRF.Setup}(1^\lambda)$. Here, p is a prime number and the order of the group $\mathbf{G}$ which has generators G, K. It deploys random oracles $H_p, H : \{0,1\}^* \to \mathbb{F}_p$, $H_{\mathbf{G}} : \{0,1\}^* \to \mathbf{G}$ and H_{ring} for constructing a Merkle tree.

Pedersen VRF: We construct PedVRF similarly to [28,29,19], except we replace the public key by a Pedersen commitment $\mathsf{sk}\, G + \mathsf{b}\, K$ to the secret key sk. We do not expose a public key from KeyGen, nor inject the public key in Eval.

– $\mathsf{PedVRF.KeyGen} : pp \mapsto \mathsf{sk}$ where $\mathsf{sk} \leftarrow\!\!\$\, \mathbb{F}_p$.
– $\mathsf{PedVRF.Eval} : (\mathsf{sk}, \mathsf{input}) \mapsto H(\mathsf{input}, \mathsf{preout})$ where $\mathsf{preout} = \mathsf{sk}\, H_{\mathbf{G}}(\mathsf{input})$

We add an algorithm to obtain a Pedersen commitment to the secret key sk.

– $\mathsf{PedVRF.CommitKey} : \mathsf{sk} \mapsto (b, \mathsf{compk})$ where $\mathsf{b} \leftarrow\!\!\$\, \mathbb{F}_p$ is a blinding factor and $\mathsf{compk} = \mathsf{sk}\, G + \mathsf{b}\, K$ is a Pedersen commitment.

Our Sign and Ver algorithms of PedVRF correspond to the Prove and Ver algorithms of a Chaum-Pedersen DLEQ proof for relation $\mathcal{R}_{eval}$, instantiated by a Fiat-Shamir transform of a sigma protocol.

$$\mathcal{R}_{eval} = \left\{ \begin{array}{l|l} (\mathsf{compk}, \mathsf{preout}, \mathsf{inbase}); & \mathsf{compk} = \mathsf{sk}\, G + \mathsf{b}\, K, \\ (\mathsf{sk}, \mathsf{b}) & \mathsf{preout} = \mathsf{sk}\, H_{\mathbf{G}}(\mathsf{input}) \end{array} \right\}.$$

– $\mathsf{PedVRF.Sign} : (\mathsf{sk}, \mathsf{b}, \mathsf{input}, \mathsf{ass}) \mapsto \sigma$ Compute $\mathsf{preout} := \mathsf{sk}\, H_{\mathbf{G}}(\mathsf{input})$ and $\mathsf{compk} = \mathsf{sk} G + \mathsf{b} K$. Let $r_1, r_2 \leftarrow\!\!\$\, \mathbb{F}_p$ and compute $R = r_1 G + r_2 K, R_m = r_1 H_{\mathbf{G}}(\mathsf{input})$ and $c = H_p(\mathsf{ass}, \mathsf{input}, \mathsf{compk}, \mathsf{preout}, R, R_m)$. Finally compute $s_1 = r_1 + c\, \mathsf{sk}$ and $s_2 = r_2 + c\, \mathsf{b}$. Return the signature $\sigma = (\mathsf{preout}, R, R_m, s_1, s_2)$.
– $\mathsf{PedVRF.Ver} : (\mathsf{compk}, \mathsf{input}, \mathsf{ass}, \sigma) \mapsto \mathsf{out} \vee \perp$ Parse $\sigma = (\mathsf{preout}, R, R_m, s_1, s_2)$ and compute $c = H_p(\mathsf{ass}, \mathsf{input}, \mathsf{compk}, \mathsf{preout}, R, R_m)$. If $R = s_1 G + s_2 K - c\, \mathsf{compk}$ and and $R_m = s_1 H_{\mathbf{G}}(\mathsf{input}) - c\, \mathsf{preout}$, then return $H(\mathsf{input}, \mathsf{preout})$, which equals $\mathsf{PedVRF.Eval}(\mathsf{sk}, \mathsf{input})$, or return failure $\perp$ otherwise.

We remark that PedVRF becomes almost EC VRF if we demand $\mathsf{b} = r_2 = 0$ in Sign.

The Ring VRF Construction: We now describe how our construction works in combination with PedVRF and a commitment scheme Com.

- $\mathsf{rVRF.KeyGen}$ returns as secret key $\mathsf{sk}, r \leftarrow\$ \mathbb{F}_p$ and pk as public key where $\mathsf{pk} = \mathsf{Com.Commit}(\mathsf{sk}, r)$. We note that pk can be alternatively defined as $\mathsf{pk} = \mathsf{sk}G$ according to the SNARK used for $\mathcal{R}_{\mathtt{ring}}$. In this case, we would not have r as a part of the secret key. We provide one optimal public key design in §6.3 for our SNARK used for $\mathcal{R}_{\mathtt{ring}}$.
- $\mathsf{rVRF.Eval}((\mathsf{sk}, r), \mathsf{input})$ runs $\mathsf{PedVRF.Eval}(\mathsf{sk}, \mathsf{input})$. We remark that the evaluation value is generated with *only* the first part of the secret key which is sk.
- $\mathsf{rVRF.CommitRing} : (\mathsf{ring}, \mathsf{pk}) \mapsto (\mathsf{comring}, \mathsf{opring})$ Compute a Merkle tree root $\mathsf{comring}$ with the random oracle H_{ring} considering the elements of ring as leaves and generate a Merkle tree path opring that verifies $\mathsf{pk} \in \mathsf{ring}$.
- $\mathsf{rVRF.OpenRing} : (\mathsf{comring}, \mathsf{opring}) \mapsto \mathsf{pk}$ Verify that the root computed via Merkle tree path opring is $\mathsf{comring}$. If it is the case, output $\mathsf{pk} \in \mathsf{opring}$. Otherwise, output $\perp$.
  We choose the ring commitment scheme so the $\mathsf{rVRF.OpenRing}$ invocation is relatively SNARK friendly in our ring membership relation $\mathcal{R}_{\mathtt{ring}}$. We note that an alternative ring commitment scheme where $\mathsf{comring} = \mathsf{ring}$ and $\mathsf{opring} = \mathsf{pk}$.

The Sign and Ver for our rVRF are a combination of Sign and Ver from PedVRF and Prove and Ver from $\mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}$, as follows:

- $\mathsf{rVRF.Sign} : ((\mathsf{sk}, r), \mathsf{comring}, \mathsf{opring}, \mathsf{input}, \mathsf{ass}) \mapsto \rho$ returns a ring VRF signature $\rho = (\mathsf{compk}, \pi_{\mathtt{ring}}, \sigma, \mathsf{comring})$ if opring is a correct opening of $\mathsf{comring}$. In this, $(\mathsf{b}, \mathsf{compk}) \leftarrow \mathsf{PedVRF.CommitKey}(\mathsf{sk})$, $\pi_{\mathtt{ring}} \leftarrow \mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}.\mathsf{Prove}((\mathsf{compk}, \mathsf{comring}); \mathsf{b}, \mathsf{opring}, \mathsf{pk}, \mathsf{sk}, r)$ where $\mathsf{ass}' \leftarrow \mathsf{ass} \mathbin{+\!\!+} \pi_{\mathtt{ring}} \mathbin{+\!\!+} \mathsf{comring}$, $\sigma \leftarrow \mathsf{PedVRF.Sign}(\mathsf{sk}, \mathsf{b}, \mathsf{input}, \mathsf{ass}')$. we instantiate $\mathcal{R}_{\mathtt{ring}}$ with

$$\mathcal{R}_{\mathtt{ring}} = \left\{ \begin{array}{c|c} (\mathsf{compk}, \mathsf{comring}); & ((\mathsf{pk}, \mathsf{compk} - \mathsf{b}\,K); (\mathsf{sk}, r)) \in \mathcal{R}_{\mathsf{pk}} \\ (\mathsf{b}, \mathsf{opring}, \mathsf{pk}, \mathsf{sk}, r) & \mathsf{pk} = \mathsf{rVRF.OpenRing}(\mathsf{comring}, \mathsf{opring}) \end{array} \right\}.$$

  where $\mathcal{R}_{\mathsf{pk}} = \{(\mathsf{pk}, X); (\mathsf{sk}, r) : \mathsf{sk} = \mathsf{Com.Open}(\mathsf{pk}; \mathsf{sk}, r), X = \mathsf{sk}G\}$.

  We note that if $\mathsf{pk} = \mathsf{sk}G$ then $\mathcal{R}_{\mathtt{ring}}$ does not need sk, r since $\mathcal{R}_{\mathsf{pk}}$ can be checked without them i.e., check whether $\mathsf{compk} - \mathsf{b}K = \mathsf{pk}$.
- $\mathsf{rVRF.Ver} : (\mathsf{comring}, \mathsf{input}, \mathsf{ass}, \rho) \mapsto \mathsf{out} \vee \perp$ Parses ρ as $(\mathsf{compk}, \pi_{\mathtt{ring}}, \sigma)$, sets $\mathsf{ass}' \leftarrow \mathsf{ass} \mathbin{+\!\!+} \pi_{\mathtt{ring}} \mathbin{+\!\!+} \mathsf{comring}$ and runs $\mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}.\mathsf{Ver}((\mathsf{compk}, \mathsf{comring}); \pi_{\mathtt{ring}})$. If it fails, returns $(0, \perp)$. Otherwise, returns $\mathsf{PedVRF.Ver}(\mathsf{compk}, \mathsf{input}, \mathsf{ass}', \sigma)$.

Appendix A proves our ring VRF construction realizes $\mathcal{F}_{\mathsf{rvrf}}$ in Figure 1. Intuitively, the randomness and the determinism of $\mathsf{rVRF.Eval}$ come from the random oracles H' and $H_{\mathbf{G}'}$. The anonymity of our ring VRF signature comes from the perfect hiding property of Pedersen commitment, the zero-knowledge property of $\mathsf{NIZK}_{\mathcal{R}_{ring}}$ (Lemma 4) and the difficulty of DDH in $\mathbf{G}$ (Lemma 5) so that preout is indistinguishable from a random element in $\mathbf{G}$. The unforgeability and uniqueness come from the fact that CDH is hard in $\mathbf{G}$ (Lemma 6), i.e., for unforgeability, one cannot commit an honest party's secret key without breaking the CDH problem and for the uniqueness, if one can obtain PedVRF signatures such that $\sigma_1 = (\mathsf{preout}_1, \pi_{\mathsf{PedVRF}})$ and $\sigma_2 = (\mathsf{preout}_2, \pi'_{\mathsf{PedVRF}})$ where $\mathsf{preout}_1 \neq \mathsf{preout}_2$ and verified by compk for the message input, then we break a CDH problem in $\mathbf{G}$.

Theorem 1. rVRF *over the group structure* $(\mathbf{G}, p, G, K)$ *realizes* $\mathcal{F}_{\mathsf{rvrf}}$ *in Figure 1 in the random oracle model assuming that* $\mathsf{NIZK}_{\mathcal{R}_{eval}}$ *and* $\mathsf{NIZK}_{\mathcal{R}_{ring}}$ *are zero-knowledge and knowledge sound, the decisional Diffie-Hellman (DDH) problem are hard in* $\mathbf{G}$ *and the commitment scheme* Com *is binding and perfectly hiding.*

6 Zero-knowledge Continuations

In the following, we describe a NIZK for a relation $\mathcal{R}$ where

$$\mathcal{R} = \{(\bar{y}, \bar{z}; \bar{x}, \bar{w}_1, \bar{w}_2) : (\bar{y}, \bar{x}; \bar{w}_1) \in \mathcal{R}_1, (\bar{z}, \bar{x}; \bar{w}_2) \in \mathcal{R}_2\},$$

and $\mathcal{R}_1$, $\mathcal{R}_2$ are some NP relations. Our NIZK is designed to efficiently re-prove membership for relation $\mathcal{R}_1$ via a new technique which we call *zero-knowledge continuation*. In practice, using a NIZK that ensures a zero-knowledge continuation for a subcomponent relation (i.e., in our case $\mathcal{R}_1$) means one essentially needs to create only once an otherwise expensive proof for that subcomponent relation; the initial proof can later be re-used multiple times (just after inexpensive re-randomisations) while preserving knowledge soundness and zero-knowledge of the entire NIZK. Below, we formally define zero-knowledge continuation. In section 6.1 we instantiate it via a *special(ised) Groth16* or $\mathsf{SpecialG}$, and finally, in section 6.3 we use it to build a ring VRF with fast amortised prover time.

In addition, the anonymity property of our ring VRF demands we not only finalise multiple times a component of the zero-knowledge continuation but also each time the result remains unlinkable to previous finalisations, meaning our ring VRF stays zero-knowledge even with a continuation component being reused. We formalise such a more general zero-knowledge property in section 6.1 and give an instantiation of our NIZK fulfilling such a property in section 6.3.

Definition 7 (ZK Continuations). *A zero-knowledge continuation* ZKCont *for a relation* $\mathcal{R}_1$ *with input* $(\bar{y}, \bar{x})$ *and witness* $\bar{w}_1$ *is a tuple of efficient algorithms (*$\mathsf{ZKCont.Setup}$*,* $\mathsf{ZKCont.Preprove}$*,* $\mathsf{ZKCont.Reprove}$*,* $\mathsf{ZKCont.VerCom}$*,* $\mathsf{ZKCont.Ver}$*,* $\mathsf{ZKCont.Sim}$*) such that for implicit security parameter* λ*,*

- $\mathsf{ZKCont.Setup} : (1^\lambda, \mathcal{R}_1) \mapsto (crs, td, pp)$ *a setup algorithm that on input the security parameter outputs a common reference string* crs*, a trapdoor* td *and a list* pp *of public parameters,*

- $\mathsf{ZKCont.Preprove}$: $(crs, \bar{y}, \bar{x}, \bar{w}_1, \mathcal{R}_1) \mapsto (X', \pi', b')$ *constructs commitment* X' *from a vector of inputs* $\bar{x}$ *(called* opaque*) and constructs proof* π' *from vector of inputs* $\bar{y}$ *(called* transparent*),* $\bar{x}$ *and vector of witnesses* $\bar{w}_1$*, and it also outputs* b' *as the opening for* X'*,*
- $\mathsf{ZKCont.Reprove}$: $(crs, X', \pi', b', \mathcal{R}_1) \mapsto (X, \pi, b)$ *finalises commitment* X *and proof* π *and returns an opening* b *for the commitment,*
- $\mathsf{ZKCont.VerCom}$: $(pp, X, \bar{x}, b) \mapsto 0/1$ *verifies that indeed* X *is a commitment to* $\bar{x}$ *with opening (e.g., randomness)* b *and outputs 1 if indeed that is the case and 0 otherwise,*
- $\mathsf{ZKCont.Ver}$: $(crs, \bar{y}, X, \pi, \mathcal{R}_1) \mapsto 0/1$ *outputs* 1 *in case it accepts and* 0 *otherwise,*
- $\mathsf{ZKCont.Sim}$: $(td, \bar{y}, \mathcal{R}_1) \mapsto (\pi, X)$ *takes as input a simulation trapdoor td and statement* $(\bar{y}, \bar{x})$ *and returns arguments* π *and* X*,*

and satisfies perfect completeness for Preprove *and, for* Reprove*, it satisfies knowledge soundness and zero-knowledge as defined below:*
Perfect Completeness for Preprove *For all* $\lambda \in \mathbb{N}$*, for every* $(\bar{y}, \bar{x}; \bar{w}_1) \in \mathcal{R}_1$*:*

$$\begin{aligned} &Pr(\mathsf{ZKCont.Ver}(crs, \bar{y}, X, \pi, \mathcal{R}_1) = 1 \ \wedge \ \mathsf{ZKCont.VerCom}(pp, X, \bar{x}, b) = 1 \mid \\ &\quad (crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1), \\ &\quad (X, \pi, b) \leftarrow \mathsf{ZKCont.Preprove}(crs, \bar{y}, \bar{x}, \bar{w}_1, \mathcal{R}_1)) = 1 \end{aligned}$$

Perfect Completeness for Reprove *For all* $\lambda \in \mathbb{N}$*, for every efficient adversary* A*:*

$$\begin{aligned} &Pr((\mathsf{ZKCont.Ver}(crs, \bar{y}, X', \pi', \mathcal{R}_1) = 1 => \mathsf{ZKCont.Ver}(crs, \bar{y}, X, \pi, \mathcal{R}_1) = 1) \wedge \\ &\quad \wedge \ (\mathsf{ZKCont.VerCom}(pp, X', \bar{x}, b') = 1 => \mathsf{ZKCont.VerCom}(pp, X, \bar{x}, b) = 1) \mid \\ &\quad (crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1), (\bar{y}, \bar{x}, X', \pi', b') \leftarrow A(crs, \mathcal{R}_1), \\ &\quad (X, \pi, b) \leftarrow \mathsf{ZKCont.Reprove}(crs, X', \pi', b', \mathcal{R}_1)) = 1 \end{aligned}$$

Knowledge Soundness *For all* $\lambda \in \mathbb{N}$*, for every benign auxiliary input aux (as per [4]) and every non-uniform efficient adversary* A*, there exists efficient non-uniform extractor* E *such that:*

$$\begin{aligned} &Pr((\mathsf{ZKCont.Ver}(crs, \bar{y}, X, \pi, \mathcal{R}_1) = 1) \ \wedge \ (\mathsf{ZKCont.VerCom}(pp, X, \bar{x}, b) = 1) \wedge \\ &\quad \wedge \ ((\bar{y}, \bar{x}; \bar{w}_1) \notin \mathcal{R}_1) \mid (crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1), \\ &\quad (\bar{y}, \bar{x}, X, \pi, b; \bar{w}_1) \leftarrow A || E(crs, aux, \mathcal{R}_1)) = \mathsf{negl}(\lambda), \end{aligned}$$

where by $(output_A; output_B) \leftarrow A||B(input)$ *we denote algorithms* A*,* B *running on the same input and* B *having access to the random coins of* A*.*

Perfect Zero-knowledge w.r.t. $\mathcal{R}_1$ *For all* $\lambda \in \mathbb{N}$*, for every benign auxiliary input aux, for all* $(\bar{y}, \bar{x}; \bar{w}_1) \in \mathcal{R}_1$*, for all* X'*, for all* π'*, for all* b'*, for every* *adversary A:*

$$
\begin{aligned}
&Pr(A(crs, aux, \pi, X, \mathcal{R}_1) = 1 \mid (crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1),\\
&\quad \mathsf{ZKCont.Ver}(crs, \bar{y}, X', \pi', \mathcal{R}_1) = 1,\\
&\quad (\pi, X, \_) \leftarrow \mathsf{ZKCont.Reprove}(crs, X', \pi', b', \mathcal{R}_1)) =\\
= &Pr(A(crs, aux, \pi, X, \mathcal{R}_1) = 1 \mid (crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1),\\
&\quad \mathsf{ZKCont.Ver}(crs, \bar{y}, X', \pi', \mathcal{R}_1) = 1, (\pi, X) \leftarrow \mathsf{ZKCont.Sim}(td, \bar{y}, \mathcal{R}_1))
\end{aligned}
$$

6.1 Specialised Groth16

Below we instantiate our zero-knowledge continuation notion with a scheme based on Groth16 [21] SNARK; hence, we call our instantiation *specialised Groth16* or SpecialG. But first we need a reminder of the definition of Quadratic Arithmetic Program (QAP) [8], [18].

Definition 8 (QAP). *A Quadratic Arithmetic Program (QAP) $\mathcal{Q} = (\mathcal{A}, \mathcal{B}, \mathcal{C}, t(X))$ of size m and degree d over a finite field $\mathbb{F}_q$ is defined by three sets of polynomials $\mathcal{A} = \{a_i(X)\}_{i=0}^m$, $\mathcal{B} = \{b_i(X)\}_{i=0}^m$, $\mathcal{C} = \{c_i(X)\}_{i=0}^m$, each of degree less than $d-1$ and a target degree d polynomial $t(X)$. Given $\mathcal{Q}$ we define $\mathcal{R}_\mathcal{Q}$ as the set of pairs $((\bar{y}, \bar{x}); \bar{w}) \in \mathbb{F}_q^l \times \mathbb{F}_q^{n-l} \times \mathbb{F}_q^{m-n}$ for which it holds that there exist a polynomial $h(X)$ of degree at most $d-2$ such that:*

$$
(\sum_{k=0}^m v_k \cdot a_k(X)) \cdot (\sum_{k=0}^m v_k \cdot b_k(X)) = (\sum_{k=0}^m v_k \cdot c_k(X)) + h(X)t(X) \quad (*)
$$

where $\bar{v} = (v_0, \ldots, v_m) = (1, x_1, \ldots, x_n, w_1, \ldots w_{m-n})$ and $\bar{y} = (x_1, \ldots, x_l)$ and $\bar{x} = (x_{l+1}, \ldots, x_n)$ and $\bar{w} = (w_1, \ldots, w_{m-n})$.

Given notation provided in section 3, we introduce

Definition 9 (Specialised Groth16 (SpecialG)). *Let $\mathcal{R}_\mathcal{Q}$ be as in Definition 8. Then we call specialised Groth16 for relation $\mathcal{R}_\mathcal{Q}$ the following:*

- SpecialG.Setup : $(1^\lambda, \mathcal{R}_\mathcal{Q}) \mapsto (crs, td, pp)$.
  Let $\alpha, \beta, \gamma, \delta, \tau, \eta \xleftarrow{\$} \mathbb{F}_q^*$. *Let* $td = (\alpha, \beta, \gamma, \delta, \tau, \eta)$.
  Let $crs = ([\bar{\sigma}_1]_1, [\bar{\sigma}_2]_2)$ *where*

$$
\begin{aligned}
\bar{\sigma}_1 = (&\alpha, \beta, \delta, \{\tau_i\}_{i=0}^{d-1}, \left\{\frac{\beta a_i(\tau) + \alpha b_i(\tau) + c_i(\tau)}{\gamma}\right\}_{i=1}^n, \frac{\eta}{\gamma},\\
&\left\{\frac{\beta a_i(\tau) + \alpha b_i(\tau) + c_i(\tau)}{\delta}\right\}_{i=n+1}^m, \left\{\frac{1}{\delta}\sigma^i t(\sigma)\right\}_{i=0}^{d-2}, \frac{\eta}{\delta}),\\
\bar{\sigma}_2 = (&\beta, \gamma, \delta, \{\tau^i\}_{i=0}^{d-1}).
\end{aligned}
$$

  $pp = \left(\left\{\left[\frac{\beta a_i(\tau)+\alpha b_i(\tau)+c_i(\tau)}{\gamma}\right]_1\right\}_{i=l+1}^n, \left[\frac{\eta}{\gamma}\right]_1\right)$.
  Moreover, for simplicity and later use, we call $K_\gamma = \left[\frac{\eta}{\gamma}\right]_1$ *and* $K_\delta = \left[\frac{\eta}{\delta}\right]_1$.

– $\mathsf{SpecialG.Preprove} : (crs, \bar{y}, \bar{x}, \bar{w}_1, \mathcal{R}_\mathcal{Q}) \mapsto (X', \pi', b')$ *such that*

$$b' = 0; r, s \xleftarrow{\$} \mathbb{F}_p; X' = \sum_{i=l+1}^{n} v_i \left[\frac{\beta a_i(\tau) + \alpha b_i(\tau) + c_i(\tau)}{\gamma}\right]_1;$$
$$o = \alpha + \sum_{i=0}^{m} v_i \cdot a_i(\tau) + r \cdot \delta; u = \beta + \sum_{i=0}^{m} v_i \cdot b_i(\tau) + s \cdot \delta;$$
$$v = \frac{\sum_{i=n+1}^{m}(v_i(\beta a_i(\tau) + \alpha b_i(\tau) + c_i(\tau))) + h(\tau)t(\tau)}{\delta} + o \cdot s + u \cdot r - r \cdot s \cdot \delta;$$
$$\pi' = ([o]_1, [u]_2, [v]_1),$$

where $\bar{y} = (x_1, \ldots, x_l)$, $\bar{x} = (x_{l+1}, \ldots, x_n)$, $\bar{w} = (w_1, \ldots, w_{m-n})$, $\bar{v} = (1, x_1, \ldots, x_n, w_1, \ldots, w_{m-n})$ *(same as in Definition 8).*

– $\mathsf{SpecialG.Reprove} : (crs, X', \pi', b', \mathcal{R}_\mathcal{Q}) \mapsto (X, \pi, b)$ *such that*

$$b, r_1, r_2 \xleftarrow{\$} \mathbb{F}_p, X = X' + (b - b')K_\gamma, \pi = (O, U, V),$$
$$O = \frac{1}{r_1}O', U = r_1 U' + r_1 r_2 [\delta]_2, V = V' + r_2 O' - (b - b')K_\delta.$$

where $\pi' = (O', U', V')$.

– $\mathsf{SpecialG.VerCom} : (pp, X, \bar{x}, b) \mapsto 0/1$ *where the output is 1 iff the following holds*

$$X = \sum_{i=l+1}^{n} x_i \left[\frac{\beta a_i(\tau) + \alpha b_i(\tau) + c_i(\tau)}{\gamma}\right]_1 + bK_\gamma,$$

where $\bar{x} = (x_{l+1}, \ldots, x_n)$, $0 \leq l \leq n - 1$.

– $\mathsf{ZKCont.Ver} : (crs, \bar{y}, X, \pi, \mathcal{R}_\mathcal{Q}) \mapsto 0/1$ *where the output is 1 iff the following holds*

$$e(O, U) = e([\alpha]_1, [\beta]_2) \cdot e(X + Y, [\gamma]_2) \cdot e(V, [\delta]_2),$$

where $\pi = (O, U, V)$, $Y = \sum_{i=1}^{l} x_i \left[\frac{\beta a_i(\tau) + \alpha b_i(\tau) + c_i(\tau)}{\gamma}\right]_1$ *and* $\bar{y} = (x_1, \ldots, x_l)$.

– $\mathsf{SpecialG.Sim} : (td, \bar{y}, \mathcal{R}_\mathcal{Q}) \mapsto (\pi, X)$ *where* $x, o, u \xleftarrow{\$} \mathbb{F}_p$ *and let* $\pi = ([o]_1, [u]_2, [v]_1)$ *where* $v = \frac{o \cdot u - \alpha\beta - \sum_{i=1}^{l} x_i(\beta a_i(\tau) + \alpha b_i(\tau) + c_i(\tau)) - x}{\delta}$ *and, by definition* $\bar{y} = (x_1, \ldots, x_l)$. *Note that* π *is a simulated proof for transparent input* $\bar{y}$ *and commitment* $X = [x]_1$.

Notes: First, the trusted setup required by $\mathsf{SpecialG}$ is an extension of that required by original Groth16 [21] by two additional group elements $K_\gamma = [\frac{\eta}{\gamma}]_1$ and $K_\delta = [\frac{\eta}{\delta}]_1$. An identical trusted setup to that used by $\mathsf{SpecialG}$ was used in LegoSNARK [8, Fig. 22] which defines a commit-carrying SNARK based on Groth16. Second, our $\mathsf{SpecialG.Reprove}$ algorithm uses a Groth16 re-randomisation technique for the proof (see [3, Fig. 1] or LegoSNARK [8,

Fig. 22]), but, in addition, SpecialG.Reprove also re-randomises X which is a commitment to a slice of the public input; moreover, in terms of security properties, we appropriately define the zero-knowledge for zk continuations such that even after iteratively applying SpecialG.Reprove zero-knowledge property is preserved for both the witness as well as the public input committed to in X.

Finally, we are ready to prove the following result:

Theorem 2. *Let $\mathcal{R}_Q$ be a relation as per Definition 8 such that additionally $\{a_k(X)\}_{k=0}^{n}$ are linearly independent polynomials. Then, in the AGM [17],* SpecialG *is a zero-knowledge continuation as per definition 7.*

Proof. It is straightforward to prove that SpecialG has perfect completeness for Preprove and perfect completeness for Reprove.

We prove knowledge-soundness (KS) an in Definition 7 by first arguing SpecialG is a commit-carrying SNARK with double binding (cc-SNARK with double binding) as per Definition 3.4 [8]. We use the fact that ccGroth16 as defined by the NILP detailed in Fig.22, Appendix H.5 [8] satisfies that latter definition. Moreover, SpecialG's Setup together with Gen, on one hand, and ccGroth16's *KeyGen*, on the other hand, are the same procedure. Also SpecialG and ccGroth16 share the same verification algorithm. Hence, translating the notation appropriately, SpecialG also satisfies KS of a cc-SNARK with double binding.

Let A_{SpecialG} be an adversary for KS in Definition 7 and define adversary $A_{\mathsf{ccGroth16}}$ for KS in Definition 3.4 [8]:

$$\begin{aligned}&\textit{If}\ \ A_{\mathsf{SpecialG}}(crs, pp, aux, \mathcal{R}_Q)\ \textit{outputs}\ (\bar{y}, \bar{x}, X, \pi, b)\\ &\qquad \textit{then}\ \ A_{\mathsf{ccGroth16}}(crs, aux, \mathcal{R}_Q)\ \textit{outputs}\ (\bar{y}, X, \pi).\end{aligned}$$

Given extractor $E_{\mathsf{ccGroth16}}$ fulfilling Definition 3.4 [8] for $A_{\mathsf{ccGroth16}}$, we construct extractor E_{SpecialG} for A_{SpecialG}

$$\begin{aligned}&\textit{If}\, E_{\mathsf{ccGroth16}}(crs, aux, \mathcal{R}_Q)\ \textit{outputs}\ (\bar{x}^*, b^*, \bar{w}^*)\\ &\qquad \textit{then}\ \ E_{\mathsf{SpecialG}}(crs, aux, \mathcal{R}_Q)\ \textit{outputs}\ \bar{w}^*;\\ &\textit{Otherwise}\ \ E_{\mathsf{ccGroth16}}(crs, aux, \mathcal{R}_Q)\ \textit{outputs}\ \perp.\end{aligned}$$

We show E_{SpecialG} fulfils Definition 7 for A_{SpecialG}. Assume by contradiction that is not the case. This implies there exist auxiliary input aux such that each:

$$\mathsf{ZKCont.Ver}(crs, \bar{y}, X, \pi, \mathcal{R}_Q) = 1\ (10)\ ;\ \mathsf{ZKCont.VerCom}(pp, X, \bar{x}, b) = 1\ (20)$$
$$(\bar{y}, \bar{x}; \bar{w}) \notin \mathcal{R}_Q\ \ (30)$$

hold with non-negligible probability. Since (20) holds with non-negligible probability and verification is identical for SpecialG and ccGroth16, and since $E_{\mathsf{ccGroth16}}$ is an extractor for $A_{\mathsf{ccGroth16}}$ as per Definition 3.4 [8], then each of the two events

$$\textit{VerCommit}^*(pp, X, \bar{x}^*, b^*) = 1\ (40)\ ;\ (\bar{y}, \bar{x}^*; \bar{w}^*) \in \mathcal{R}_Q\ (50)$$

holds with overwhelming probability. Since (20) holds with non-negligible probability and (40) holds with overwhelming probability and together with (ii) from Definition 3.4 [8] we obtain that $\bar{x}^* = \bar{x}$. Since (50) holds with overwhelming probability, it implies $(\bar{y}, \bar{x}; \bar{w}^*) \in \mathcal{R}_{\mathcal{Q}}$ with overwhelming probability which contradicts our assumption, so our claim that $\mathsf{SpecialG}$ does not have KS as per Definition 7 is false.

Finally, regarding zero-knowledge, it is clear that if $\pi = (O, U, V)$ is part of the output of $\mathsf{SpecialG.Reprove}$, then O and U are uniformly distributed as group elements in their respective groups. This holds, as long as the input to $\mathsf{SpecialG.Reprove}$ is a verifying proof, even when the proof was maliciously generated. Hence, it is easy to check that the output π' of $\mathsf{SpecialG.Sim}$ is identically distributed to a proof π output by $\mathsf{SpecialG.Reprove}$ so the perfect zero-knowledge property holds for $\mathsf{SpecialG}$.

6.2 Putting Together a NIZK and a ZKCont for Proving $\mathcal{R}$

Let ZKCont be a zk continuation for $\mathcal{R}_1$ (from preamble of Section 6) and let $\mathsf{NIZK}_{\mathcal{R}'_2(pp)}$ be a NIZK for $\mathcal{R}'_2(pp)$ (for some public parameters pp) defined by:

$$\mathcal{R}'_2(pp) = \{(X, \bar{z}, pp; \bar{x}, b, \bar{w}_2) : \mathsf{ZKCont.VerCom}(pp, X, \bar{x}, b) = 1 \wedge (\bar{z}, \bar{x}; \bar{w}_2) \in \mathcal{R}_2\},$$

with $\mathcal{R}_2$ from preamble of Section 6. Then we define the system $\mathsf{NIZK}_{\mathcal{R}}$ for relation $\mathcal{R}$ from the preamble of Section 6 as:

- $\mathsf{NIZK}_{\mathcal{R}}.\mathsf{Setup} : (1^\lambda) \mapsto (crs_{\mathcal{R}} = (crs, crs_{\mathcal{R}'_2(pp)}), td_{\mathcal{R}} = (td, td_{\mathcal{R}'_2(pp)}), pp)$ where $(crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1)$, $(crs_{\mathcal{R}'_2(pp)}, td_{\mathcal{R}'_2(pp)}) \leftarrow \mathsf{NIZK}_{\mathcal{R}'_2(pp)}.\mathsf{Setup}(1^\lambda)$
- $\mathsf{NIZK}_{\mathcal{R}}.\mathsf{Prove} : (crs_{\mathcal{R}}, \bar{y}, \bar{z}; \bar{x}, \bar{w}_1, \bar{w}_2) \mapsto (\pi_1, \pi_2, X)$ where
  $(X', \pi'_1, b') \leftarrow \mathsf{ZKCont.Preprove}(crs, \bar{y}, \bar{x}, \bar{w}_1, \mathcal{R}_1)$
  $(X, \pi_1, b) \leftarrow \mathsf{ZKCont.Reprove}(crs, X', \pi'_1, b', \mathcal{R}_1)$
  $\pi_2 \leftarrow \mathsf{NIZK}_{\mathcal{R}'_2(pp)}.\mathsf{Prove}(crs_{\mathcal{R}'_2(pp)}, X, \bar{z}; \bar{x}, b, \bar{w}_2)$
- $\mathsf{NIZK}_{\mathcal{R}}.\mathsf{Ver} : (crs_{\mathcal{R}}, \bar{y}, \bar{z}, \pi_1, \pi_2, X) \mapsto 0/1$ where the output is 1 iff

  $$\mathsf{ZKCont.Ver}(crs, \bar{y}, X, \pi_1, \mathcal{R}_1) = 1 \ \wedge \ \mathsf{NIZK}_{\mathcal{R}'_2(pp)}.\mathsf{Ver}(crs_{\mathcal{R}'_2(pp)}, X, \bar{z}, \pi_2) = 1$$

- $\mathsf{NIZK}_{\mathcal{R}}.\mathsf{Sim} : (td_{\mathcal{R}}, \bar{y}, \bar{z}) \mapsto (\pi_1, \pi_2, X)$ where
  $(\pi_1, X) \leftarrow \mathsf{ZKCont.Sim}(td, \bar{y}, \mathcal{R}_1)$, $\pi_2 \leftarrow \mathsf{NIZK}_{\mathcal{R}'_2(pp)}.\mathsf{Sim}(td_{\mathcal{R}'_2(pp)}, X, \bar{z})$

Lemma 1 (Knowledge-soundness for $\mathsf{NIZK}_{\mathcal{R}}$). *If ZKCont is a zk continuation for $\mathcal{R}_1$ and $\mathsf{NIZK}_{\mathcal{R}'_2(pp)}$ is a NIZK for $\mathcal{R}'_2(pp)$ for some appropriately chosen public parameters pp, then the $\mathsf{NIZK}_{\mathcal{R}}$ construction described above has knowledge-soundness for $\mathcal{R}$.*

Proof. This is easy to infer by linking together the extractors guaranteed for ZKCont and $\mathsf{NIZK}_{\mathcal{R}'_2(pp)}$ due to their respective knowledge-soundness.

Next, we define
Special Perfect Completeness For all $\lambda \in \mathbb{N}$, for every efficient adversary A, for every $(\bar{z}, \bar{x}; \bar{w}_2) \in \mathcal{R}_2$ it holds:

$$\begin{aligned}
Pr(&(\mathsf{ZKCont.Ver}(crs, \bar{y}, X', \pi_1', \mathcal{R}_1) = 1 => \mathsf{ZKCont.Ver}(crs, \bar{y}, X, \pi_1, \mathcal{R}_1) = 1) \wedge \\
&\wedge\ (\mathsf{ZKCont.VerCom}(pp, X', \bar{x}, b') = 1 => \mathsf{ZKCont.VerCom}(pp, X, \bar{x}, b) = 1) \wedge \\
&\wedge\ \mathsf{NIZK}_{\mathcal{R}_2'(pp)}.\mathsf{Ver}(crs_{\mathcal{R}_2'(pp)}, X, \bar{z}, \pi_2) = 1 | \\
&(crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1), \\
&(crs_{\mathcal{R}_2'(pp)}, td_{\mathcal{R}_2'(pp)}) \leftarrow \mathsf{NIZK}_{\mathcal{R}_2'(pp)}.\mathsf{Setup}(1^\lambda, \mathcal{R}_2'(pp)), \\
&(\bar{y}, X', \pi_1', b') \leftarrow A(crs, \mathcal{R}_1), (X, \pi_1, b) \leftarrow \mathsf{ZKCont.Reprove}(crs, X', \pi_1', b', \mathcal{R}_1) \\
&\pi_2 \leftarrow \mathsf{NIZK}_{\mathcal{R}_2'(pp)}.\mathsf{Prove}(crs_{\mathcal{R}_2'(pp)}, X, \bar{z}, \bar{x}, b, \bar{w}_2)) = 1
\end{aligned}$$

Lemma 2 (Special Perfect Completeness). *If* ZKCont *is a zk continuation for* $\mathcal{R}_1$ *and* $\mathsf{NIZK}_{\mathcal{R}_2'(pp)}$ *is a NIZK for* $\mathcal{R}_2'(pp)$ *for some appropriately chosen public parameters* pp*, then the* $\mathsf{NIZK}_\mathcal{R}$ *construction described above has special perfect completeness.*

Proof. This is easy to infer by combining the perfect completeness properties of $\mathsf{NIZK}_{\mathcal{R}_2'(pp)}$ and perfect completeness for ZKCont.Reprove.

Finally, we define

Zero-knowledge after Reusing a ZKCont Proof For all $\lambda \in \mathbb{N}$, for every benign auxiliary input aux, for all $\bar{y}, \bar{x}, \bar{z}, \bar{w}_1, \bar{w}_2$ with $(\bar{y}, \bar{x}; \bar{w}_1) \in \mathcal{R}_1$ and $(\bar{z}, \bar{x}; \bar{w}_2) \in \mathcal{R}_2$, for all X', π_1', π_2, b', for every adversary A it holds:

$$\begin{aligned}
&|Pr(A(crs, aux, \pi_1, \pi_2, X, \mathcal{R}) = 1 \mid (crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1), \\
&\quad (\pi_1, X, _) \leftarrow \mathsf{ZKCont.Reprove}(crs, X', \pi_1', b', \mathcal{R}_1), \\
&\quad \pi_2 \leftarrow \mathsf{NIZK}_{\mathcal{R}_2'(pp)}.\mathsf{Prove}(crs_{\mathcal{R}_2'(pp)}, X, \bar{z}, \bar{x}, b, \bar{w}_2), \\
&\quad \mathsf{ZKCont.Ver}(crs, \bar{y}, X', \pi_1', \mathcal{R}_1) = 1 \wedge \mathsf{ZKCont.VerCom}(pp, X', \bar{x}', b') = 1) \\
&-Pr(A(crs, aux, \pi_1, \pi_2, X, \mathcal{R}) = 1 \mid (crs, td, pp) \leftarrow \mathsf{ZKCont.Setup}(1^\lambda, \mathcal{R}_1), \\
&\quad (\pi_1, \pi_2, X) \leftarrow \mathsf{NIZK}_\mathcal{R}.\mathsf{Sim}(td, \bar{y}, \mathcal{R}_1) \\
&\quad \mathsf{ZKCont.Ver}(crs, \bar{y}, X', \pi_1', \mathcal{R}_1) = 1 \wedge \mathsf{ZKCont.VerCom}(pp, X', \bar{x}', b') = 1)| \\
&\leq \mathsf{negl}(\lambda)
\end{aligned}$$

Lemma 3 (ZK after Reusing a ZKCont Proof). *If* ZKCont *is a zk continuation for* $\mathcal{R}_1$ *and* $\mathsf{NIZK}_{\mathcal{R}_2'(pp)}$ *is a NIZK for* $\mathcal{R}_2'(pp)$ *for some appropriately chosen public parameters* pp*, then the* $\mathsf{NIZK}_\mathcal{R}$ *construction described above has zero-knowledge after reusing a* ZKCont *proof.*

Proof. The statement follows from the perfect zero-knowledge w.r.t. $\mathcal{R}_1$ for ZKCont and the zero-knowledge property of $\mathsf{NIZK}_{\mathcal{R}_2'(pp)}$ w.r.t. $\mathcal{R}_2'(pp)$.

Corollary 1. *If* ZKCont *is a zk continuation for* $\mathcal{R}_1$ *and* $\mathsf{NIZK}_{\mathcal{R}_2'(pp)}$ *is a NIZK for* $\mathcal{R}_2'(pp)$ *for some appropriately chosen public parameters* pp*, then the* $\mathsf{NIZK}_\mathcal{R}$ *construction described above is a NIZK for* $\mathcal{R}$*.*

Proof. Putting together the results of Lemma 1, Lemma 2, Lemma 3 and we obtain the above statement.

6.3 Ring VRFs based on SpecialG

We can apply the results of the previous subsections to construct a ring VRF using $\mathsf{SpecialG}$ that allows a fast amortized ring VRF prover. First, PedVRF has a sigma protocol which proves the relation $\mathcal{R}_{eval}$, where $\mathcal{R}_{eval}$ is the instantiation of relation $\mathcal{R}'_2(pp)$ (for some appropriately chosen public parameters pp). Second, we can use $\mathsf{SpecialG}$ for a relation $\mathcal{R}_1$ similar to $\mathcal{R}_{\mathtt{ring}}$. In fact, we will instantiate $\mathcal{R}_1$ with $\mathcal{R}^{\mathtt{inner}}_{\mathtt{ring}}$.

For the latter, we need an appropriate choice of pk to commit to sk. We use a Pedersen commitment using some Jubjub curve $\mathbb{J}$. $\mathbb{J}$ contains a large subgroup $\mathbf{J}$ of prime order $p_{\mathbf{J}}$. Typically $p_{\mathbf{J}}$ is smaller than p, the order of $\mathbf{G}$, certainly when $\mathbb{J}$ is an Edwards curve with a cofactor. Since $\mathsf{sk} \in \mathbb{F}_p$, we represent it with two $\mathbb{F}_{p_{\mathbf{J}}}$ elements $\mathsf{sk}_0, \mathsf{sk}_1 \leq 2^\lambda$ so that $\mathsf{sk} = \mathsf{sk}_0 + \mathsf{sk}_1\, 2^\lambda \mod p$ for some fixed $(\log_2 p)/2 < \lambda < \log_2 p_{\mathbf{J}}$. $\mathsf{rVRF.KeyGen}$ now samples $\mathsf{sk} \leftarrow\!\!\$\, \mathbb{F}_p$, computes $\mathsf{sk}_1, \mathsf{sk}_2$, samples a blinding factor $d \leftarrow\!\!\$\, \mathbb{F}_{p_{\mathbf{J}}}$ and then returns a blinded Pedersen commitment as the public key $\mathsf{rVRF.pk} = \mathsf{sk}_0\, J_0 + \mathsf{sk}_1\, J_1 + dJ_2$ and the secret key $\mathsf{rVRF.sk} = (\mathsf{sk}_0, \mathsf{sk}_1, d)$. Here $J_0, J_1, J_2 \in \mathbf{J}$ are independent generators.

We thus have a fairly efficient instantiation for $\mathcal{R}_1$ given by

$$\mathcal{R}^{\mathtt{inner}}_{\mathtt{ring}} = \left\{ (\mathsf{comring}, \mathsf{sk}; \mathsf{sk}_0, \mathsf{sk}_1, \mathsf{opring}) \;\middle|\; \mathsf{sk} = \mathsf{sk}_0 + 2^\lambda \mathsf{sk}_1 \wedge \begin{array}{c} \mathsf{OpenRing}(\mathsf{comring}, \mathsf{opring}) \\ = \mathsf{sk}_0 J_0 + \mathsf{sk}_1 J_1 + dJ_2 \end{array} \right\}.$$

Combining $\mathsf{SpecialG}$ for $\mathcal{R}_1$ and the sigma protocol which is part of PedVRF gives a NIZK for relation $\mathcal{R}_{\mathtt{rvrf}}$ (i.e., an instantiation of $\mathcal{R}$ from previous subsections):

$$\mathcal{R}_{\mathtt{rvrf}} = \left\{ \mathsf{out}, \mathsf{input}, \mathsf{comring}; \mathsf{sk}_0, \mathsf{sk}_1, \mathsf{opring} \;\middle|\; \begin{array}{l} \mathsf{OpenRing}(\mathsf{comring}, \mathsf{opring}) \\ \quad = \mathsf{sk}_0 J_0 + \mathsf{sk}_1 J_1 + dJ_2, \\ \mathsf{out} = \mathsf{rVRF.Eval}(\mathsf{sk}_0 + 2^\lambda \mathsf{sk}_1, \mathsf{input}) \end{array} \right\}$$

Efficiency: If we have a $\mathsf{SpecialG}$ proof for $\mathcal{R}_1$ for our pk in a ring defined by $\mathsf{comring}$, to generate a ring VRF proof for the same ring, we need to run $\mathsf{SpecialG.Reprove}$ and $\mathsf{PedVRF.Sign}$. $\mathsf{PedVRF.Sign}$ requires two scalar multiplications on $\mathbb{G}_1$ and two on the same or faster $\mathbb{G}'$, so together with $\mathsf{SpecialG.Reprove}$ costing four scalar multiplications on $\mathbb{G}_1$ and two on $\mathbb{G}_2$, our amortised prover time runs faster than 12 scalar multiplications on typical $\mathbb{G}_1$ curves. We expect the three pairings dominate verifier time, but verifiers also need five scalar multiplications on $\mathbb{G}_1$.

Importantly, our fast ring VRF's amortised prover time now rivals group signature schemes' performance [24]. We hope this ends the temptation to deploy group signature like constructions where the deanonymisation vectors matter.

7 Ring updates

We now discuss the performance of $\pi_{\texttt{fast}}$. Although our $\mathsf{rVRF.Sign}$ runs fast, all users should update their stored zkSNARK $\pi_{\texttt{fast}}$ every time ring changes, but zero knowledge continuations help here too.

7.1 Merkle trees

Our $\mathsf{rVRF}.\{\mathsf{CommitRing}, \mathsf{OpenRing}\}$ could implement a Merkle tree using a zkSNARK friendly hash function like Poseidon [20], giving $O(\log|\mathsf{ring}|)$ prover time. At least one Poseidon [20] provides arity four with only 600 R1CS constraints. We need roughly 700 R1CS constraints for each fixed based scalar multiplication too, so the flavor of $\pi_{\texttt{fast}}$ costs under 12k R1CS constraints for a ring with four billion people.

7.2 Side channels

In $\pi_{\texttt{fast}}$, one might dislike processing secret key material inside the Groth16 prover for $\pi_{\texttt{fast}}$. Adversaries could trigger $\pi_{\texttt{fast}}$ recomputation only by updating the ring, but this still presents a side channel risk.

If concerned, one could address this via a second zk continuation that splits $\pi_{\texttt{fast}}$ into a Groth16 π_{sk} and a Groth16 or KZG π_{pk} for two respective languages:

$$\mathcal{L}^{\texttt{inner}}_{\mathsf{pk}} = \{\, J_{\mathsf{pk}}, \mathsf{comring} \mid \exists \mathsf{opring} \text{ s.t. } J_{\mathsf{pk}} = \mathsf{OpenRing}(\mathsf{comring}, \mathsf{opring}) \,\} \,,$$

$$\mathcal{L}^{\texttt{inner}}_{\mathsf{sk}} = \left\{\, \mathsf{sk}_0 + \mathsf{sk}_1 2^{128}, J_{\mathsf{pk}} \;\middle|\; \exists d \text{ s.t. } J_{\mathsf{pk}} = \mathsf{sk}_0 J_0 + \mathsf{sk}_1 J_1 + d J_2 \,\right\} .$$

We now prove π_{sk} only once *ever* during secret key generation, which largely eliminates any side channel risks. We do ask verifiers compute more pairings, but nobody cares when the VRF verifiers are few in number or institutional, as in many applications. We also ask provers rerandomize both π_{sk} and π_{pk}, but this costs relatively little. Assuming π_{pk} is Groth16 then we need a proof-of-knowledge for the desired structure of J_{pk} too. All totaled this almost doubles the size and complexity of our ring VRF signature.

There is no "arrow of time" among zk continuations per se, but as π_{sk} bridges between the PedVRF and π_{pk}, one might consider the π_{sk}-to-π_{pk} continuation to be "time reversed", in that the "middle" continuation is proved first.

7.3 Polynomial commitments

As π_{pk} became rather simple, there exists an alternative formulation: $\mathsf{comring}$ could be a KZG polynomial commitment [23] to users' J_{pk}s, while π_{pk} itself becomes an opening at a secret location, like Caulk+ [31] or Caulk [34]. We benefit from faster ring updates this way, but pay in increased verifier time and increased marginal prover time.

7.4 Append only rings

As a slight variation, we could build ring using append only structures like some blockchains, in which case we should split $\mathsf{rVRF.OpenRing}$ differently between an inner ring block or epoch proof $\mathcal{L}_{\mathtt{block}}$, which we only prove once like $\pi_{\mathtt{sk}}$ above, and a chain state proof $\mathcal{L}_{\mathtt{chain}}$, which extends this inner ring to the growing blockchain. Now our inner SNARKs pass a $\mathtt{blk}$ parameter, which our zero-knowledge continuation transforms into a opaque commitment $\mathtt{comblk}$, thereby requiring a proof-of-knowledge.

$$\mathcal{L}^{\mathtt{inner}}_{\mathtt{chain}} = \{ \mathtt{blk}, \mathtt{chain} \mid \mathtt{blk} \in \mathtt{chain} \}, \quad \text{and}$$

$$\mathcal{L}^{\mathtt{inner}}_{\mathtt{block}} = \left\{ \mathsf{sk}_0 + \mathsf{sk}_1 2^{128}, \mathtt{blk} \;\middle|\; \begin{array}{c} \mathsf{OpenRing}(\mathtt{blk}, \mathsf{opring}) \\ = \mathsf{sk}_0 J_0 + \mathsf{sk}_1 J_1 + d J_2 \end{array} \right\}.$$

We suggest appending $\mathtt{blk}$ to a polynomial commitment using [33], which then $\mathcal{L}_{\mathtt{chain}}$ blind opens via Caulk+ [31] as above.

7.5 Expiration and revocation

We expect expiration and revocation would be required for append only rings like blockchains, or say a zero-knowledge proof of a certificate.

For expiry, we suggest $\pi_{\mathtt{sk}}$ or $\mathcal{L}_{\mathtt{block}}$ commit to the expiration date alongside the secret key in their X, and then $\pi_{\mathtt{pk}}$ or $\mathcal{L}_{\mathtt{chain}}$ enforce expiration, but really even PedVRF could enforce expiration.

A revocation list could be enforced by a non-membership proof in $\pi_{\mathtt{pk}}$ or $\mathcal{L}_{\mathtt{chain}}$. We expect a revocation list updates only rarely compared with ring itself though, which makes doing this non-membership proof inside some separate zero-knowledge continuation tempting too. A deployment faces should make this choice carefully.

8 Anonymized ring unions

We briefly discuss ring VRFs whose ring consists of the union of several smaller rings, but which hide to which ring the user belongs. In this, we bring out one interesting zero-knowledge continuation technique.

8.1 Identical circuit

As a first step, if all rings use the same circuit, then we hide the ring among several rings using a second zero-knowledge continuation, not unlike §7.2. We could then blind open a polynomial commitment [23] to our $\mathsf{comring}$ choices, Caulk+ [31] or Caulk [34] or similar as in §7.3.

As a special case, if users cannot change their keys too quickly, then one could reduce the frequency with which users reprove their original zero-knowledge by using multiple $\mathsf{comring}$ choices across the history of the same evolving ring database.

8.2 Multi-circuit

We need a new trick if the χ_i come from different circuit's trusted setups. A priori, our zero-knowledge continuation $\pi_{\texttt{fast}}$ fixes some $G = \chi_1$, which reveals the circuit, due to its dependence upon the SRS like

$$\chi_1 = \left[\frac{\beta u_1(\tau) + \alpha v_1(\tau) + w_1(\tau)}{\gamma}\right]_1 .$$

Instead, we propose to stabilize the public input SRS elements across circuits: We choose $\chi_{1,\gamma}$ independently before selecting the circuit or running its trusted setup. We then merely add an SRS element $\chi_{1,\delta}$, for usage in C, that binds our independent $\chi_{1,\gamma}$ to the desired definition, so

$$\chi_{1,\delta} := \left[\frac{\beta u_1(\tau) + \alpha v_1(\tau) + w_1(\tau) - \gamma\chi_{1,\gamma}}{\delta}\right]_1 .$$

At this point, we replace χ_1 by $\chi_{1,\gamma}$ everywhere and our proofs add $\mathsf{comring}\,\chi_{1,\delta}$ to C.

In this way, all ring membership circuits could share identical public input SRS points $\chi_{1,\gamma}$, and similarly χ_0 if desired.

At this point, one still needs to hide the SRS elements $[\delta]_2, [\gamma]_2 \in \mathbf{G}_2$ and $e([\alpha]_1, [\beta]_2) \in \mathbf{G}_T$. We leave this as an exercise to the reader.

9 Application: Identity

Ring VRFs yield anonymous identity systems: After a user and service establish a secure channel and the server authenticates itself with certificates, then the user authenticates themselves by providing an anonymous VRF signature with input input being the service's identity, thus creating an pseudonymous identified session with a pseudonym unlinkable from other contexts.

We expand this identified session workflow with an extra update operation suitable for our ring VRF's amortized prover. We discuss only $\pi_{\texttt{fast}}$ here but all techniques apply to $\pi_{\texttt{sk}}$ and $\pi_{\texttt{pk}}$ similarly.

- *Register* – Adds users' public key commitments into some ring, after verifying the user does not currently exist in ring.
- *Update* – User agents regenerate their stored SNARK $(\mathsf{pk}, \pi^{\texttt{inner}}_{\texttt{fast}})$ using $\mathsf{SpecialG.Preprove}((\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{opring}); (\mathsf{sk}, \mathsf{comring}))$ each time ring changes, perhaps even receiving $\mathsf{comring}$ and opring from some ring management service.
- *Identify* – Our user agent first opens a standard TLS connection to a server input, both checking the server's name is input and checking certificate transparency logs, and then computes the shared session id ass. Our user agent computes the user's identity $\texttt{id} = \mathsf{PedVRF.Eval}(\mathsf{sk}, \mathsf{input})$ on the server id input, Our user agent next rerandomizes $\pi_{\texttt{fast}}$, compk, and b using

$\mathsf{SpecialG.Reprove}(\mathsf{pk}, \pi_{\mathtt{fast}}^{\mathtt{inner}})$, computes $\sigma = \mathsf{PedVRF.Sign}(\mathsf{sk}, \mathsf{b}, \mathsf{input}, \mathsf{ass} \mathbin{+\!\!+} \mathsf{compk} \mathbin{+\!\!+} \pi_{\mathtt{fast}})$, and finally sends the server their ring VRF signature $(\mathsf{compk}, \pi_{\mathtt{fast}}, \sigma)$

– *Verify* – After receiving $(\mathsf{compk}, \pi_{\mathtt{fast}}, \sigma)$ in channel ass, the server named input checks $\mathsf{SpecialG.Ver}(\mathsf{comring}, (\mathsf{compk}, \pi_{\mathtt{fast}}))$, checks the VRF signature, and obtains the user's identity $\mathtt{id}$, ala
$\mathtt{id} = \mathsf{PedVRF.Ver}(\mathsf{compk}, \mathsf{input}, \mathsf{ass} \mathbin{+\!\!+} \mathsf{compk} \mathbin{+\!\!+} \pi_{\mathtt{fast}}, \sigma)$.

9.1 Browsers

We must not link users' identities at different web sites, so user agents should carefully limit cross site resource loading, referrer information, etc. User agents could always load purely static resources, without metadata like cookies or referrer information. At least Tor browser already takes cross site resource concerns seriously, while Safari and Brave may limit invasive cross site resources too.

We somewhat trust the CAs and CT log system with users' identities in the above protocol, in that users could login to a site with fraudulent credentials. We think cross site restrictions limit this attack vector. If stronger defenses are desired then instead of input being the site name, input could be a public "root" key for the specific site, which then also certifies its TLS certificate. Ideally its secret key remains air gaped.

9.2 AML/KYC

We shall not discuss AML/KYC in detail, because the entire field lacks clear goals, and thus winds up being ineffective [30]. We do however observe that AML/KYC typically conflicts with security and privacy laws like GDPR. As a compromise between these regulations, one needs a compliance party who know users' identities, while another separate service party knows the users' activities. We propose a safer and more efficient solution:

Instead our compliance party becomes an identity issuer who maintains a public ring, and privately knows the users behind each public key. As above, identity systems could employ ring freely for diverse purposes. If later asked or subpoenaed, users could prove their relevant identities to investigators, or maybe prove which services they use and do not use.

Interestingly PedVRF could run "backwards" like $H_{\mathbf{G}'}(\mathsf{input}) \neq \mathsf{sk}^{-1}\, \mathsf{preout}$ to show a ring VRF output associated to preout does not belong to the user, without revealing the users' identity $H'(\mathsf{input}, \mathsf{sk}\, H_{\mathbf{G}'}(\mathsf{input}))$ to investigators.

Our applications mostly ignore key multiplicity. AML/KYC demands suspects prove non-involvement using ring VRFs.

Definition 10. *We say* rVRF *is* exculpatory *if we have an efficient algorithm for equivalence of public keys, but a PPT adversary $\mathcal{A}$ cannot find non-equivalent public keys* $\mathsf{pk}_0, \mathsf{pk}_1$ *with colliding VRF outputs.*

A priori, our JubJub representations $\mathsf{sk}_0 J_0 + \mathsf{sk}_1 J_1$ used in §6.3 and §7.2 costs us exculpability from Definition 10.

There is however a natural *exculpable public key* flavor (pk, σ), in which $\sigma = \mathsf{Sign}(\mathsf{sk}, \mathsf{CommitRing}(\{\mathsf{pk}\}, \mathsf{pk}).\mathsf{opring}, \texttt{ring\_name}, "")$. The singleton ring $\{\mathsf{pk}\}$ ensure that $\mathsf{Ver}(\mathsf{CommitRing}(\{\mathsf{pk}\}), \texttt{ring\_name}, "", \sigma)$ uniquely determines the secret key, so exculpability holds if joining the ring requires (pk, σ).

9.3 Moderation

All discussion or collaboration sites have behavioral guidelines and moderation rules that deeply impact their culture and collective values.

Our ring VRFs enables a simple blacklisting operation: If a user misbehaves, then sites could blacklist or otherwise penalizes their site local identity `id`. As `id` remains unlinked from other sites, we avoid thorny questions about how such penalties impact the user elsewhere, and thus can assess and dispense justice more precisely.

At the same time, there exist sites who must forget users' histories eventually, like under some "right to be forgotten" principle, either GDPR compliance or an ethical principle of social mistakes being ephemeral.

We obtain ephemeral identities if input consists of the site name plus the current year and month, or some other approximate date. In this way, users have only one stable `id` within the approximate date range, but they obtain fresh `id`s merely by waiting until the next month.

We could adjust PedVRF to simultaneously prove multiple VRF input-output pairs $(\mathsf{input}_j, \mathtt{id}_j)$. As in [14], we merely delinearize inbase and preout in Sign and Ver like:

$$
\begin{aligned}
x &= H(\mathsf{input}_j, \mathtt{id}_j, \ldots, \mathsf{input}_j, \mathtt{id}_j) \\
\mathsf{inbase} &= \sum_j H_p(x, j)\, \mathsf{inbase}_j \\
\mathsf{preout} &= \sum_j H_p(x, j)\, \mathsf{preout}_j
\end{aligned}
$$

As doing so links these pairs together, we could link together two or more ephemeral identities like this to obtain a semi-permanent identity with user controlled revocation: As login, our site demands two linked input-output pairs given by $\mathsf{input}_1 = \texttt{site\_name} \mathbin{+\!\!+} \texttt{current\_month}$ and $\mathsf{input}_2 = \texttt{site\_name} \mathbin{+\!\!+} \texttt{registration\_month}$, so users could have multiple active pseudo-nyms given by $\mathtt{id}_2$, but only one active pseudo-nym per month, enforced by deduplicating $\mathtt{id}_1$, which still prevents spam and abuse.

If instead our site associates pseudo-nyms to their most recently seen $\mathtt{id}_1$, then we could link adjacent months, meaning input_j is defined by the jth previous month, until reaching a previously used $\mathtt{id}_1$. In this model, pseudo-nyms could be abandoned and replaced, but abandoned pseudo-nyms cannot then be reclaimed without linking intervening dates. Although more costly, sites could permanently bans a few problematic users via the inequality proofs described in §9.2 too.

In these ways, sites encode important aspects of their moderation rules into the ring VRF inputs they demand.

9.4 Reduced pairings

At a high level, we distinguish moderation-like applications discussed above, which resemble classic identity applications like AML/KYC, from rate limiting applications discussed in the next section. In moderation-like applications, ring VRF outputs become long-term stable identities, so users typically reidentify themselves many times to the same sites, reusing the exact same input.

As an optimization, our zero-knowledge continuation could reuse the same compk and $\pi_{\mathtt{fast}}$ for the same input, so that verifiers could memoize their verifications of $\pi_{\mathtt{fast}}$. We spend most verifier time checking the Groth16 pairing equation, so this saves considerable CPU time.

As a concrete example, our coefficients r_1, r_2, b used for rerandomization in §6 could be chosen deterministically like $r_1, r_2, b \leftarrow H(\mathsf{sk}, \mathsf{input})$. In this way, each (helpful) user's $\mathtt{id}$ has a unique $\pi_{\mathtt{fast}}$, which verifiers could memoize by storing $(\mathtt{id}, H(\mathsf{compk} \mathbin{+\!\!+} \pi_{\mathtt{fast}}), \mathtt{dates})$ after their first verification, but then skipping the Groth16 check after merely rechecking the hash $H(\mathsf{compk} \mathbin{+\!\!+} \pi_{\mathtt{fast}})$.

We could risk denial-of-service attacks by users who vary r_1, r_2, b randomly however. We therefore suggest $\mathtt{dates}$ record the last several previous dates when $H(\mathsf{compk} \mathbin{+\!\!+} \pi_{\mathtt{fast}})$ changed. We rate limit or verify more lazily users with many nearby login dates

10 Application: Rate limiting

We showed in §9 how ring VRFs give users only one unique identity for each input input. We explained in §9.3 that choosing input to be the concatenation of a base domain and a date gives users a stream of changing identities. We next discuss giving users exactly $n > 1$ ring VRF outputs aka "identities" per date, as opposed to one unique identity

As a trivial implementation, we could include a counter $k = 1 \ldots n$ in input, so $\mathsf{input} = \mathtt{domain} \mathbin{+\!\!+} \mathtt{date} \mathbin{+\!\!+} k$.

10.1 Avoiding linkage

Our trivial implementation leaks information about ring VRF outputs' ownership by revealing k: An adversary Eve observes two ring VRF signatures with the same $\mathtt{domain}$ and $\mathtt{date}$ so $\mathsf{input}_i = \mathtt{domain} \mathbin{+\!\!+} \mathtt{date} \mathbin{+\!\!+} k_i$ for $i = 1, 2$, but with different outputs out_1 and out_2. If $k_1 \neq k_2$ then Eve learns nothing, but if $k_1 = k_2$ then Eve learns that $sk_1 \neq \mathsf{sk}_2$, maybe representing different users.

We do not necessarily always care if Eve learns this much information, but scenarios exist in which one cares. We therefore briefly describe several mitigation:

If n remains fixed forever, then we could simply let all users register n ring VRF public keys in ring. If n fluctuates under an upper bound N, then we could create N rings ring_i for $i = 1 \ldots N$, and then blind $\mathsf{comring}$ in $\pi_{\mathtt{fast}}$ similarly to §8.

Although simple, these two approaches require users construct n or N different $\pi_{\mathtt{pk}}$ proofs every time ring updates.

Instead of proving ring membership of one public key, $\pi_{\mathtt{pk}}$ could prove ring membership of a Merkle commitment to multiple keys, so users have $\pi^1_{\mathtt{sk}}, \ldots, \pi^N_{\mathtt{sk}}$ for each of their multiple keys.

In principle, there exists ring VRFs that hide parts of their input input, but still fit our abstract formulation in §2. Although interesting, we caution these bring performance concerns not discussed here, so deployments should consider if leaking k suffices.

10.2 Ration cards

As a species, we expect +3°C over the pre-industrial climate by 2100 [1], or more likely above +4°C given tipping points [25]. At these levels, we experience devastating famines as the Earth's carrying capacity drops below one billion people [32]. In the near term, our shortages of resources, energy, goods, water, and food shall steadily worsen over the next several decades, due to climate change, ecosystem damage or collapse, and resource exhaustion ala peak oil. We expect synchronous crop failures around the 2040s in particular [11]. Invariably, nations manage shortages through rationing, like during WWI, WWII, and the oil shocks.

Ring VRFs support anonymous rationing: Instead of treating ring VRF outputs like identities, we treat them like nullifiers which could each be spent exactly once.

We fix a set U of limited resource types, overseen by an authority who certifies verifiers from a key $\mathtt{root}$. We dynamically define an expiry date e_{u,d_0} and an availability n_{u,d_0}, both dependent upon the resource $u \in U$ and current date d_0. We typically want a randomness beacon r_d too, which prevents anyone learning r_d much before date d. As ring VRF inputs, we choose $\mathsf{input} = \mathtt{root} \mathbin{+\!\!+} u \mathbin{+\!\!+} r_d \mathbin{+\!\!+} d \mathbin{+\!\!+} k$ where $u \in U$ denotes a limited resource, d denotes an non-expired date meaning $e_{u,d_0} < d \leq d_0$, and $1 \leq k \leq n_{u,d_0}$. In this way, our rationing system controls both daily consumption via n_{u,d_0} and time shifted demand via expiry time e_{u,d_0}.

Importantly, our rationing system retains ring VRF outputs as nullifiers, filed under their associated date d and resource u, so nullifiers expire once $d \leq e_{u,d_0}$ which permits purging old data rapidly.

We remark that fully transferable assets could have constrained lifetimes too, which similarly eases nullifier management when implements using blind signatures, ZCash sapling, etc. Yet, all these tokens require an explicit issuance stage, while ring VRFs self-issue.

Among the political hurdles to rationing, we know certificates have a considerable forgery problem, as witnessed by the long history of fraudulent covid and

TLS certificates. It follows citizens would justifiably protest to ration carts that operate by simple certificates. Ring VRFs avoid this political unrest by proving membership in a public list.

10.3 Multi-constraint rationing

As in §9.3, we could impose simultaneous rationing constraints for multiple resources $u_1, \ldots, u_k$ by producing one ring VRF signature in which PedVRF proves correctness of pre-outputs for multiple messages $\mathsf{input}_j = \mathtt{root} \mathbin{+\!\!+} u_j \mathbin{+\!\!+} r_d \mathbin{+\!\!+} d \mathbin{+\!\!+} k$ for $j = 1 \ldots k$.

As an example, purchasing some prepared food product could require spending rations for multiple base food sources, like making a cake from wheat, butter, eggs, and sugar.

10.4 Decommodification

There exist many reasons to decommodify important services, like energy, water, or internet, beyond rationing real physical shortages. Ring VRFs fit these cases using similar input formulations.

As an example, a municipal ISP allocates some limited bandwidth capacity among all residents. It allocates bandwidth fairly by verifying ring VRFs signatures on hourly input and then tracking nullifiers until expiry.

Aside from essential government services, commercial service providers typically offers some free service tier, usually because doing so familiarizes users with their intimidating technical product.

Some free and paid tier examples include DuoLingo's hearts on mobile, continuous integration testing services, and many dating sites.

A priori, rate limiting cases benefit from unlinkability among individual usages, not merely at some site boundary like moderation requires. We thus use each ring VRF output only once, which prevents our cashing trick of §9.4 from reducing verifier pairings.

Although rationing sounds valuable enough, we foresee services like ISP, VPNs, or mixnets having many low value transactions. In such cases, ring VRFs could authorize issuing a limited number of fast simple single-use blind issued credentials, like blind signatures ala GNU Taler [6] or PrivacyPass OPRF tokens [14], which both solve the leakage of k above too. In principle, commercial service providers could sell the same tokens, which avoids leaking whether the user uses the free or commercial tier.

10.5 Delegation

Almost all single-use blind signed tokens have an implicit delegation protocol, in which token holders transfer token credentials without sacrificing their own access. As double spending remains possible, delegatees must trust delegators. GNU Taler [6] argues against taxing such trusting transfers, like when parents give their kids spending money, but enforces taxability only when also preventing double spending.

In our rationing scheme, spenders authenticate their specific spending operations inside the associated data ass in a rVRF-AD signature. As doing so requires knowing sk, delegators place enormous trust in delegatees, which likely precludes say parents delegating to children.

We could however achieve delegation by treating the ring VRF like a certificate that authenticates another public key held by the delegatee. In fact, delegators could limit delegatees uses too in this certificate, like how GNU Taler achieves parental restrictions.

We remark that PedVRF has adaptor signatures aka implicit certificate mode: A delegatee learns the full ring VRF signature, but the delegatee hides the blinding factor signature s_1 in PedVRF from downstream recipients, and instead merely prove knowledge of s_1, say via a key exchange or another Schnorr signature with the base point K. EC VRFs lack this mode.

References

1. Climate change 2022: Impacts, adaptation and vulnerability. working group ii contribution to the ipcc sixth assessment report. Cambridge University Press. In Press.
2. Christian Badertscher, Peter Gaži, Iñigo Querejeta-Azurmendi, and Alexander Russell. On uc-secure range extension and batch verification for ecvrf. *Cryptology ePrint Archive*, 2022.
3. Karim Baghery, Markulf Kohlweiss, Janno Siim, and Mikhail Volkhov. Another look at extraction and randomization of groth's zk-snark. In Nikita Borisov and Claudia Diaz, editors, *Financial Cryptography and Data Security*, pages 457–475, Berlin, Heidelberg, 2021. Springer Berlin Heidelberg. `https://ia.cr/2020/811`.
4. Nir Bitansky, Ran Canetti, Omer Paneth, and Alon Rosen. On the existence of extractable one-way functions. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, 2014.
5. Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 23–26, 2017.
6. Jeffrey Burdges, Florian Dold, and Christian Grothoff. Robust and income-transparent online e-cash.
7. Privacy by Design Foundation. Irma docs v0.2.0. `https://irma.app/docs/v0.2.0/overview/`.
8. Matteo Campanelli, Dario Fiore, and Anaïs Querol. Legosnark: Modular design and composition of succinct zero-knowledge proofs. Cryptology ePrint Archive, Paper 2019/142, 2019. `https://eprint.iacr.org/2019/142`.
9. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2000. `https://eprint.iacr.org/2000/067`.
10. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 2001 IEEE International Conference on Cluster Computing*, pages 136–145. IEEE, 2001.

11. Chatham House. Climate change risk assessment 2021.
12. David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology*, pages 199–203, Boston, MA, 1983. Springer US.
13. Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 66–98. Springer, 2018.
14. Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda. Privacy pass: Bypassing internet challenges anonymously. *Proceedings on Privacy Enhancing Technologies*, 2018:164–180, 06 2018.
15. Henry de Valence. It's 255:19am. do you know what your validation criteria are? `https://hdevalence.ca/blog/2020-10-04-its-25519am`.
16. Bryan Ford and Jacob Strauss. An offline foundation for online accountable pseudonyms. In *Proceedings of the 1st Workshop on Social Network Systems*, SocialNets '08, page 31–36, New York, NY, USA, 2008. Association for Computing Machinery.
17. Georg Fuchsbauer, Eike Kiltz, and Julian Loss. The algebraic group model and its applications. Cryptology ePrint Archive, Paper 2017/620, 2017, 2017. `https://eprint.iacr.org/2017/620`.
18. Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct nizks without pcps. Cryptology ePrint Archive, Paper 2012/215, 2012, 2012. `https://eprint.iacr.org/2012/215`.
19. Sharon Goldberg, Leonid Reyzin, Dimitrios Papadopoulos, and Jan Včelák. Verifiable Random Functions (VRFs). Internet-Draft draft-irtf-cfrg-vrf-10, Internet Engineering Task Force, Nov 2021. Work in Progress.
20. Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. Cryptology ePrint Archive, Paper 2019/458, 2019. `https://eprint.iacr.org/2019/458`.
21. Jens Groth. On the size of pairing-based non-interactive arguments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 305–326, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. IACR ePrint Archive 2016/260.
22. Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. ZCash protocol specification. `https://zips.z.cash/protocol/protocol.pdf`. Version 2022.3.8 [NU5], 15 September 2022.
23. Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg. Constant-size commitments to polynomials and their applications. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010*, pages 177–194, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
24. Mark Manulis, Nils Fleischhacker, Felix Günther, Franziskus Kiefer, and Bertram Poettering. Group signatures: Authentication with privacy. BSI, 2011. `https://www.franziskuskiefer.de/paper/GruPA.pdf` and `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/GruPA/GruPA.pdf`.
25. David I. Armstrong McKay, Arie Staal, Jesse F. Abrams, Ricarda Winkelmann, Boris Sakschewski, Sina Loriani, Ingo Fetzer, Sarah E. Cornell, Johan Rockström, and Timothy M. Lenton. Exceeding 1.5°c global warming could trigger multiple climate tipping points. *Science*, 377(6611):286–295, Sep 2022.

26. Silvio Micali, Michael Rabin, and Salil Vadhan. Verifiable random functions. In *40th annual symposium on foundations of computer science (cat. No. 99CB37039)*, pages 120–130. IEEE, 1999.
27. Nate Otto, Sunny Lee, Brian Sletten, Daniel Burnett, Manu Sporny, and Ken Ebert. Verifiable credentials use cases. W3C Working Group Note 24 September 2019. `https://www.w3.org/TR/vc-use-cases/`.
28. Dimitrios Papadopoulos, Duane Wessels, Shumon Huque, Moni Naor, Jan Včelák, Leonid Reyzin, and Sharon Goldberg. Making nsec5 practical for dnssec. Cryptology ePrint Archive, Paper 2017/099, 2017. `https://eprint.iacr.org/2017/099`.
29. Trevor Perrin. The xeddsa and vxeddsa signature schemes. Revision 1, 2016-10-20. `https://signal.org/docs/specifications/xeddsa/`.
30. Ronald F. Pol. Anti-money laundering: The world's least effective policy experiment? together, we can fix it. *Policy Design and Practice*, 3(1):73–94, 2020.
31. Jim Posen and Assimakis A. Kattis. Caulk+: Table-independent lookup arguments. Cryptology ePrint Archive, Paper 2022/957, 2022. `https://eprint.iacr.org/2022/957`.
32. David Spratt. At 4°c of warming, would a billion people survive? what scientists say.
33. Alin Tomescu, Ittai Abraham, Vitalik Buterin, Justin Drake, Dankrad Feist, and Dmitry Khovratovich. Aggregatable subvector commitments for stateless cryptocurrencies. Cryptology ePrint Archive, Report 2020/527, 2020. `https://ia.cr/2020/527`.
34. Arantxa Zapico, Vitalik Buterin, Dmitry Khovratovich, Mary Maller, Anca Nitulescu, and Mark Simkin. Caulk: Lookup arguments in sublinear time. Cryptology ePrint Archive, Paper 2022/621, 2022. `https://eprint.iacr.org/2022/621`.

A Security of Our Ring VRF Construction

Before we start to analyse our protocol, we should define the algorithm Gen_{sign} for $\mathcal{F}_{\mathsf{rvrf}}$ and show that $\mathcal{F}_{\mathsf{vrf}}$ with Gen_{sign} satisfies the anonymity defined in Definition 6. $\mathcal{F}_{\mathsf{rvrf}}$ that rVRF realizes runs Algorithm 1 to generate honest signatures.

Algorithm 1 $\mathsf{Gen}_{sign}(\mathsf{ring}, W, \{X, \mathsf{pk}\}, \mathsf{ass}, \mathsf{input})$

$c, s_1, s_2 \leftarrow\!\$\, \mathbb{F}_p$
$\pi_{eval} \leftarrow (c, s_1, s_2)$
$\mathsf{b} \leftarrow\!\$\, \mathbb{F}_p$
$\mathsf{compk} = xG + \mathsf{b}\, K$
$\mathsf{comring}, \mathsf{opring} \leftarrow \mathsf{rVRF.CommitRing}(\mathsf{ring}, \mathsf{pk})$
$\pi_{ring} \leftarrow \mathsf{NIZK}_{\mathcal{R}_{\mathrm{ring}}}.\mathsf{Prove}((\mathsf{comring}, \mathsf{compk}); (\mathsf{b}, \mathsf{opring}))$
return $\sigma = (\pi_{eval}, \pi_{ring}, \mathsf{compk}, \mathsf{comring}, W)$

Lemma 4. *$\mathcal{F}_{\mathsf{rvrf}}$ running Algorithm 1 satisfies anonymity defined in Definition 6 assuming that $\mathsf{NIZK}_{\mathcal{R}_{\mathrm{ring}}}$ is a zero-knowledge and Pedersen commitment is perfectly hiding.*

$\mathcal{F}_{\mathsf{rvrf}}$ runs a PPT algorithms Gen_{sign} during the execution and is parametrized with sets $\mathcal{S}_{eval}$ and $\mathcal{S}_W$ where $\mathcal{S}_{eval}$ and $\mathcal{S}_W$ generated by a set up function $\mathsf{Setup}(1^\lambda)$.

[Key Generation.] upon receiving a message $(\mathsf{keygen}, \mathsf{sid})$ from a party P_i, send $(\mathsf{keygen}, \mathsf{sid}, \mathsf{P}_i)$ to the simulator Sim. Upon receiving a message $(\mathsf{verificationkey}, \mathsf{sid}, x, \mathsf{pk})$ from Sim, verify that x, pk has not been recorded before for sid i.e., there exists no (x', pk') in `verification_keys` such that $x' = x$ or $\mathsf{pk}' = \mathsf{pk}$. If it is the case, store in the table `verification_keys`, under P_i, the value x, pk and return $(\mathsf{verificationkey}, \mathsf{sid}, \mathsf{pk})$ to P_i.

[Corruption:] upon receiving $(\mathsf{corrupt}, \mathsf{sid}, \mathsf{P}_i)$ from Sim, remove pk_i from $\texttt{verification\_keys}[\mathsf{P}_i]$ and store pk_i to `verification_keys` under Sim. Return $(\mathsf{corrupted}, \mathsf{sid}, \mathsf{P}_i)$.

[Malicious Ring VRF Evaluation.] upon receiving a message $(\mathsf{eval}, \mathsf{sid}, \mathsf{pk}_i, W, \mathsf{input})$ from Sim, if pk_i is recorded under an honest party's identity or if there exists $W' \neq W$ where $\texttt{anonymous\_key\_map}[\mathsf{input}, W'] = \mathsf{pk}_i$, ignore the request. Otherwise, record in the table `verification_keys` the value pk_i under Sim if pk_i is not in `verification_keys`.
If $\texttt{anonymous\_key\_map}[\mathsf{input}, W]$ is not defined before, set $\texttt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_i$ and let $y \leftarrow\$ \mathcal{S}_{eval}$ and set $\texttt{evaluations}[\mathsf{input}, W] = y$.
In any case (except ignoring), obtain $y = \texttt{evaluations}[\mathsf{input}, W]$ and return $(\mathsf{evaluated}, \mathsf{sid}, \mathsf{input}, \mathsf{pk}_i, W, y)$ to P_i.

[Honest Ring VRF Signature and Evaluation.] upon receiving a message $(\mathsf{sign}, \mathsf{sid}, \mathsf{ring}, \mathsf{pk}_i, \mathsf{ass}, \mathsf{input})$ from P_i, verify that $\mathsf{pk}_i \in \mathsf{ring}$ and that there exists a public key pk_i associated to P_i in `verification_keys`. If it is not the case, just ignore the request. If there exists no W' such that $\texttt{anonymous\_key\_map}[\mathsf{input}, W'] = \mathsf{pk}_i$, let $W \leftarrow\$ \mathcal{S}_W$ and let $y \leftarrow\$ \mathcal{S}_{eval}$. If there exists W where $\texttt{anonymous\_key\_map}[\mathsf{input}, W]$ is defined, then abort. Otherwise, set $\texttt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_i$ and set $\texttt{evaluations}[\mathsf{input}, W] = y$.
In any case (except ignoring and aborting), obtain W, y where $\texttt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_i$ and $\texttt{evaluations}[\mathsf{input}, W] = y$ and run $\mathsf{Gen}_{sign}(\mathsf{ring}, W, x, \mathsf{pk}, \mathsf{ass}, \mathsf{input}) \rightarrow \sigma$. Record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$. Return $(\mathsf{signature}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, y, \sigma)$ to P_i.

[Malicious Requests of Signatures.] upon receiving a message $(\mathsf{request}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input})$ from Sim, obtain all existing valid signatures σ such that $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$ is recorded and add them in a list $\mathcal{L}_\sigma$. Return $(\mathsf{requests}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \mathcal{L}_\sigma)$ to Sim.

[Ring VRF Verification.] upon receiving a message $(\mathsf{verify}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma)$ from a party, do the following:

C1 If there exits a record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, b']$, set $b = b'$. (This condition guarantees the completeness and consistency.)

C2 Else if $\texttt{anonymous\_key\_map}[\mathsf{input}, W]$ is an honest verification key and there exists a record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma', 1]$ for any σ', then let $b = 1$ and record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 1]$. (This condition guarantees that if input is signed by an honest party for the ring ring at some point, then the signature is $\sigma' \neq \sigma$ which is generated by the adversary is valid)

C3 Else relay the message $(\mathsf{verify}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma)$ to Sim and receive back the message $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma, b_{\mathsf{Sim}}, \mathsf{pk}_{\mathsf{Sim}})$. Then check the following:

1. If $W \notin \mathcal{W}[\mathsf{input}, \mathsf{ring}]$ and $|\mathcal{W}[\mathsf{input}, \mathsf{ring}]| > |\mathsf{ring}_{mal}|$ where ring_{mal} is a set of malicious keys in ring, set $b = 0$. (This condition guarantees uniqueness meaning that the number of verifying outputs that Sim can generate for $\mathsf{input}, \mathsf{ring}$ is at most the number of malicious keys in ring.).
2. Else if $\mathsf{pk}_{\mathsf{Sim}}$ is an honest verification key, set $b = 0$. (This condition guarantees unforgeability meaning that if an honest party never signs a message input for a ring ring)
3. Else if there exists $W' \neq W$ where $\texttt{anonymous\_key\_map}[\mathsf{input}, W'] = \mathsf{pk}_{\mathsf{Sim}}$, set $b = 0$. (This condition guarantees that there exists a unique anonymous key for each $(\mathsf{input}, \mathsf{pk}_{\mathsf{Sim}})$)
4. Else set $b = b_{\mathsf{Sim}}$.

In the end, record $[\mathsf{input}, \mathsf{ass}, W, \mathsf{ring}, \sigma, 0]$ if it is not stored. If $b = 0$, let $y = \perp$. Otherwise, do the following:

- if $W \notin \mathcal{W}[\mathsf{input}, \mathsf{ring}]$, add W to $\mathcal{W}[\mathsf{input}, \mathsf{ring}]$.
- if $\texttt{evaluations}[\mathsf{input}, W]$ is not defined, set $\texttt{evaluations}[\mathsf{input}, W] \leftarrow\$ \mathcal{S}_{eval}$, $\texttt{anonymous\_key\_map}[\mathsf{input}, W] = \mathsf{pk}_{\mathsf{Sim}}$. Set $y = \texttt{evaluations}[\mathsf{input}, W]$.
- otherwise, set $y = \texttt{evaluations}[\mathsf{input}, W]$.

Finally, output $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma, y, b)$ to the party.

Fig. 1. Functionality $\mathcal{F}_{\mathsf{rvrf}}$.

Proof. We simulate $\mathcal{F}_{\mathsf{rvrf}}$ with Algorithm 1 against $\mathcal{D}$. Assume that the advantage of $\mathcal{D}$ is ϵ. Now, we reduce the anonymity game to the following game where we change the simulation of $\mathcal{F}_{\mathsf{rvrf}}$ by changing the Algorithm 1. In our change, we let $\pi_{ring} \leftarrow \mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}.\mathsf{Simulate}(G, K, \mathbf{G}, \mathsf{comring}, \mathsf{compk})$. Since $\mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}$ is zero knowledge, there exists an algorithm $\mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}.\mathsf{Simulate}$ which generates a proof which is indistinguishable from the proof generated from $\mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}.\mathsf{Prove}$. Therefore, our reduced game is indistinguishable from the anonymity game. Since in this game, no public key is used while generating the proof and W and compk is perfectly hiding, the probability that $\mathcal{D}$ wins the game is $\frac{1}{2}$. This means that ϵ is negligible.

We next show that rVRF realizes $\mathcal{F}_{\mathsf{rvrf}}$ in the random oracle model under the assumption of the hardness of the decisional Diffie Hellman (DDH).

Theorem 3. *Assuming that $H_{\mathbf{G}}, H, H_p, H_{\mathsf{ring}}$ are random oracles, the DDH problem is hard in the group structure $(\mathbf{G}, G, K, p)$ and NIZK algorithms are zero-knowledge and knowledge sound, rVRF UC-realizes $\mathcal{F}_{\mathsf{rvrf}}$ running Algorithm 1 according to Definition 4.*

Proof. We construct a simulator Sim that simulates the honest parties in the execution of rVRF and simulates the adversary in $\mathcal{F}_{\mathsf{rvrf}}$.

- **[Simulation of keygen:]** Upon receiving $(\mathsf{keygen}, \mathsf{sid}, \mathsf{P}_i)$ from $\mathcal{F}_{\mathsf{rvrf}}$, Sim obtains the a secret and public key pair $x = (\mathsf{sk}, r)$ and pk by running $\mathsf{rVRF.KeyGen}$. It adds pk to lists `honest_keys` and `verification_keys` as a key of P_i. In the end, Sim returns $(\mathsf{verificationkey}, \mathsf{sid}, x, \mathsf{pk})$ to $\mathcal{F}_{\mathsf{rvrf}}$. Sim lets $\mathsf{public\_keys}[X] = \mathsf{pk}$ and $\mathsf{secret\_keys}[X] = (\mathsf{sk}, r)$ where $X = \mathsf{sk}G$.
- **[Simulation of corruption:]** Upon receiving a message $(\mathsf{corrupted}, \mathsf{sid}, \mathsf{P}_i)$ from $\mathcal{F}_{\mathsf{rvrf}}$, Sim removes the public key pk from `honest_keys` which is stored as a key of P_i and adds pk to `malicious_keys`.
- **[Simulation of the random oracles:]** We describe how Sim simulates the random oracles $H_{\mathbf{G}}, H, H_p$ against the real world adversaries.
  Sim simulates the random oracle $H_{\mathbf{G}}$ as described in Figure 2. It selects a random element h from $\mathbb{F}_p$ for each new input and outputs hG as an output of the random oracle $H_{\mathbf{G}}$. Thus, Sim knows *the discrete logarithm of each random oracle output of* $H_{\mathbf{G}}$.
  The simulation of the random oracle H is less straightforward (See Figure 3). The value W can be a pre-output generated by $\mathsf{rVRF.Eval}$ or can be an anonymous key of m generated by $\mathcal{F}_{\mathsf{rvrf}}$ for an honest party. Sim does not need to know about this at this point but H should output $\mathtt{evaluations}[m, W]$ in both cases. Sim pretends W as if it is a pre-output. So, Sim first obtains the discrete logarithm h of $H_{\mathbf{G}}(m)$ from the $H_{\mathbf{G}}$'s database and finds out a commitment key $X^* = h^{-1}W$. If $\mathsf{secret\_keys}[X^*]$ is not empty, it replies by a randomly selected value from $\mathbb{F}_p$. Otherwise, Sim checks if $\mathsf{public\_keys}[X^*]$ exists to see whether a corresponding public key of X^* exists. If it does not exist, Sim picks a key pk^* which is not stored in $\mathsf{public\_keys}$ and stores $\mathsf{public\_keys}[X^*] = \mathsf{pk}^*$. In any case, it obtains $\mathtt{evaluations}[m, W]$ by sending

a message $(\mathsf{eval}, \mathsf{sid}, \mathsf{pk}^*, W, m)$ and replies with $\texttt{evaluations}[m, W]$. Remark that if W is a pre-output generated by $\mathcal{A}$, then $\mathcal{F}_{\mathsf{rvrf}}$ matches it with the evaluation value given by $\mathcal{F}_{\mathsf{rvrf}}$. If W is an anonymous key of an honest party in the ideal world, $\mathcal{F}_{\mathsf{rvrf}}$ still returns an honest evaluation value $\texttt{evaluations}[m, W]$ even if Sim cannot know whether W is an anonymous key of an honest party in the ideal world. During the simulation of H, if $\mathcal{F}_{\mathsf{rvrf}}$ aborts, then there exists $W' \neq W$ such that $\texttt{anonymous\_key\_map}[m, W'] = \mathsf{pk}^*$. Remark that it is not possible because if it happens it means that $hX^* = W' \neq W$ where $\mathsf{public\_keys}[X^*] = \mathsf{pk}^*$, but also $W = hX^*$. Therefore, Sim never aborts during the simulation of H.
We note that the anonymous keys for honest parties generated by $\mathcal{F}_{\mathsf{rvrf}}$ are independent from honest commitment keys. Therefore, if $X^* = h^{-1}W$ is an honest verification key, Sim returns a random value because $\texttt{evaluations}[m, W]$ is not defined or will not be defined in $\mathcal{F}_{\mathsf{rvrf}}$ in this case except with a negligible probability. If it ever happens i.e., if $\mathcal{F}_{\mathsf{rvrf}}$ selects randomly $W = hX^*$, $\mathcal{Z}$ distinguishes the simulation via honest signature verification in the real world. So, this case is covered in our simulation in Figure 4.

Oracle $H_{\mathbf{G}}$
Input: m
if
$\texttt{oracle\_queries\_gg}[m] = \perp$
$h \leftarrow\$ \mathbb{F}_p$
$P \leftarrow hG$
$\texttt{oracle\_queries\_gg}[m] := h$
else:
$h \leftarrow \texttt{oracle\_queries\_gg}[m]$
$P \leftarrow hG$
return inbase

Fig. 2. The random oracle $H_{\mathbf{G}}$

Oracle H
Input: m, W
if $\texttt{oracle\_queries\_h}[m, W] \neq \perp$
return $\texttt{oracle\_queries\_h}[m, W]$
$P \leftarrow H_{\mathbf{G}}(m)$
$h \leftarrow \texttt{oracle\_queries\_gg}[m]$
$X^* := h^{-1}W$ // candidate commitment key
if $\mathsf{secret\_keys}[X^*] = \perp$
if $\mathsf{public\_keys}[X^*] = \perp$
$\mathsf{pk}^* \leftarrow\$ \mathbf{G}$
$\mathsf{public\_keys}[X^*] \leftarrow \mathsf{pk}^*$
send $(\mathsf{eval}, \mathsf{sid}, W, \mathsf{public\_keys}[X^*], m)$ **to** $\mathcal{F}_{\mathsf{rvrf}}$
if $\mathcal{F}_{\mathsf{rvrf}}$ ignores: ABORT
receive $(\mathsf{evaluated}, \mathsf{sid}, W, m, y)$ **from** $\mathcal{F}_{\mathsf{rvrf}}$
$\texttt{oracle\_queries\_h}[m, W] := y$
else:
$y \leftarrow\$ \mathbb{F}_p$
$\texttt{oracle\_queries\_h}[m, W] := y$
return $\texttt{oracle\_queries\_h}[m, W]$

Fig. 3. The random oracle H

The simulation of the random oracle H_p (See Figure 4) checks whether the random oracle query $(\mathsf{ring}, m, W, \mathsf{compk}, R, R_m)$ is an $\mathcal{R}_{eval}$ verification query before answering the oracle call. For this, it checks whether $\mathcal{F}_{\mathsf{rvrf}}$ has a recorded valid signature for the message m and the ring ring with the anonymous key W. If there exists such valid signature where compk is part of it,

Sim checks whether the first proof of the signature (c, s_1, s_2) generates R, R_m as in $\mathsf{rVRF.Ver}$ in order to make sure that it is a $\mathcal{R}_{eval}$ verification query. If it is the case, it assigns c as an answer of $H_p(\mathsf{ring}, m, W, \mathsf{compk}, R, R_m)$ so that $\mathcal{R}_{eval}$ verifies. However, if this input has already been set to another value which is not equal to c or W is a pre-output of an honest key, then Sim aborts because the output of the real world for this signature and the ideal world will be different. We remind that if an anonymous key W of an honest party for a message m sampled by $\mathcal{F}_{\mathsf{rvrf}}$ equals to a pre-output generated by $\mathsf{rVRF.Sign}$ for the same honest party's key and the message m, then $\mathcal{Z}$ can distinguish the ideal and real world outputs because the evaluation value in the ideal world and real world for m, W will be different because of the simulation of the random oracle H i.e., $\texttt{oracle\_queries\_h}[m, W] \neq \texttt{evaluations}[m, W]$. Therefore, Sim aborts if it is ever happen.

Oracle H_p
Input: $(\mathsf{ass}', \mathsf{input}, \mathsf{compk}, W, R, R_m)$

parse ass' as $\mathsf{ass} \mathbin{+\!\!+} \pi_{\texttt{ring}} \mathbin{+\!\!+} \mathsf{comring}$
send $(\mathsf{request\_signatures}, \mathsf{sid}, \mathsf{ass}, W, \mathsf{input})$
receive $(\mathsf{signatures}, \mathsf{sid}, \mathsf{input}, \mathcal{L}_\sigma)$
if $\exists \sigma \in \mathcal{L}_\sigma$ where $\mathsf{compk} \in \sigma$ **and** $\mathsf{NIZK}_{\mathcal{R}_{\texttt{ring}}}.\mathsf{Ver}((\mathsf{compk}, \mathsf{comring}); \pi_{\texttt{ring}}) \to 1$
 get $\pi_1 = (c, s_1, s_2) \in \sigma$
 if $R = s_1 G + s_2 K - c\mathsf{compk}, R_m = s_1 H_{\mathbf{G}}(m) - cW$
  $h := \texttt{oracle\_queries\_gg}[m, W]$
  if $\texttt{oracle\_queries\_h\_CP}[\mathsf{ass}, m, \mathsf{compk}, W, R, R_m] = \perp$
   $\texttt{oracle\_queries\_h\_CP}[\mathsf{ass}, m, \mathsf{compk}, W, R, R_m] := c$
  else if $(\texttt{oracle\_queries\_h\_CP}[\mathsf{ass}, m, \mathsf{compk}, W, R, R_m] \neq c$
  or $X^* = h^{-1} W \in \texttt{honest\_keys})$: ABORT
if $\texttt{oracle\_queries\_h\_CP}[\mathsf{ass}, m, \mathsf{compk}, W, R, R_m] = \perp$
 $c \leftarrow\!\!\$\ \mathbb{F}_p$
 $\texttt{oracle\_queries\_h\_CP}[\mathsf{ass}, m, \mathsf{compk}, W, R, R_m] := c$
return $\texttt{oracle\_queries\_h\_CP}[\mathsf{ass}, m, \mathsf{compk}, W, R, R_m]$

Fig. 4. The random oracle H_p

– [**Simulation of** verify] Upon receiving $(\mathsf{verify}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, \mathsf{input}, \sigma)$ from the functionality $\mathcal{F}_{\mathsf{rvrf}}$, Sim runs the two NIZK verification algorithms run for $\mathcal{R}_{eval}, \mathcal{R}_{\texttt{ring}}$ with the input $\mathsf{comring}, \mathsf{input}, \sigma, W$ described in $\mathsf{rVRF.Ver}$ algorithm of ring VRF protocol if σ can be parsed as $(\pi_1, \pi_2, \mathsf{compk}, \mathsf{comring})$. If all verify, it sets $b_{\mathsf{Sim}} = 1$. Otherwise it sets $b_{\mathsf{Sim}} = 0$.
  - If $b_{\mathsf{Sim}} = 1$, it sets $X = h^{-1} W$ where $h = \texttt{oracle\_queries\_gg}[m]$. Then it obtains $\mathsf{pk} = \mathsf{public\_keys}[X]$ if it exists. If it does not exist, it picks a pk which is not stored in $\mathsf{public\_keys}$ and sets $\mathsf{public\_keys}[X] = \mathsf{pk}$. Then sends $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, m, \sigma, b_{\mathsf{Sim}}, \mathsf{public\_keys}[X])$ to $\mathcal{F}_{\mathsf{rvrf}}$ and receives back $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, m, \sigma, y, b)$.

* If $b \neq b_{\mathsf{Sim}}$, it means that the signature is not a valid signature in the ideal world, while it is in the real world. So, Sim aborts in this case. If $\mathcal{F}_{\mathsf{rvrf}}$ does not verify a ring signature even if it is verified in the real world, $\mathcal{F}_{\mathsf{rvrf}}$ is in either C3-1, 2 or C3-3. If $\mathcal{F}_{\mathsf{rvrf}}$ is in C3-1, it means that $\mathsf{counter}[m, \mathsf{ring}] > |\mathsf{ring}_m|$. If $\mathcal{F}_{\mathsf{rvrf}}$ is in C3-2, it means that pk belongs to an honest party but this honest party never signs m for ring. So, σ is a forgery. If $\mathcal{F}_{\mathsf{rvrf}}$ is in C3- 3, it means that there exists $W' \neq W$ where $\texttt{anonymous\_key\_map}[m, W'] = \mathsf{pk}$. If $[m, W']$ is stored before, it means that Sim obtained $W' = hX$ where $h = \texttt{oracle\_queries\_h}[m]$ but it is impossible to happen since $W = hX$.
* If $b = b_{\mathsf{Sim}}$, it sets $\texttt{oracle\_queries\_h}[m, W] = y$, if it is not defined before.

- If $b_{\mathsf{Sim}} = 0$, it sets $\mathsf{pk} = \perp$ and sends $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, m, \sigma, b_{\mathsf{Sim}}, X)$ to $\mathcal{F}_{\mathsf{rvrf}}$. Then, Sim receives back $(\mathsf{verified}, \mathsf{sid}, \mathsf{ring}, W, \mathsf{ass}, m, \sigma, \perp, 0)$.

Now, we need to show that the outputs of honest parties in the ideal world are indistinguishable from the honest parties in the real world.

Lemma 5. *Assuming that the DDH problem is hard on the group structure $(\mathbf{G}, G, K)$, the outputs of honest parties in the real protocol rVRF are indistinguishable from the output of the honest parties in $\mathcal{F}_{\mathsf{rvrf}}$.*

Proof. Clearly, the evaluation outputs of the ring signatures in the ideal world identical to the real world protocol because the outputs are randomly selected by $\mathcal{F}_{\mathsf{rvrf}}$ as the random oracle H in the real protocol. The only difference is the ring signatures of honest parties (See Algorithm 1) since the pre-output W and π_1 is generated differently in Algorithm 1 than rVRF.Sign. The distribution of $\pi_{eval} = (c, s_1, s_2)$ and compk generated by Algorithm 1 and the distribution of $\pi_{eval} = (c, s_1, s_2)$ and compk generated by rVRF.Sign are from uniform distribution so they are indistinguishable. So, we are left to show that the anonymous key W selected randomly from $\mathbf{G}$ and pre-output W generated by rVRF.Sign are indistinguishable given pk.

Case 1 ($\mathsf{pk} \neq xG$): If $\mathsf{pk} \neq xG$, then pk is uniformly random and independent from x. Therefore, $\mathcal{Z}$ can distinguish ideal world honest signatures from the real world honest signatures at most with probability $\frac{1}{2}$.

Case 2 ($\mathsf{pk} = xG$): We show this under the assumption that the DDH problem is hard. In other words, we show that if there exists a distinguisher $\mathcal{D}$ that distinguishes honest signatures in the ideal world and honest signatures in the real protocol then we construct another adversary $\mathcal{B}$ which breaks the DDH problem. We use the hybrid argument to show this. We define hybrid simulations H_i where the signatures of first i honest parties are computed as described in rVRF.Sign and the rest are computed as in $\mathcal{F}_{\mathsf{rvrf}}$. Without loss of generality, $\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_{n_h}$ are the honest parties. Thus, H_0 is equivalent to the honest of the ideal protocol and H_{n_h} is equivalent to honest signatures in the real world. We construct an adversary $\mathcal{B}$ that breaks the DDH problem given that there exists an adversary $\mathcal{D}$ that distinguishes hybrid games H_i and H_{i+1} for $0 \leq i < n_h$. $\mathcal{B}$ receives the DDH challenges $X, Y, Z \in \mathbf{G}$ from the DDH game and simulates the game against $\mathcal{D}$ as follows. Then $\mathcal{B}$ runs a simulated copy of $\mathcal{Z}$ and starts to simulate $\mathcal{F}_{\mathsf{rvrf}}$ and Sim for $\mathcal{Z}$. For this, it first runs the simulated copy of $\mathcal{A}$ as Sim does. $\mathcal{B}$ publishes $\mathbf{G}, G = Y, K$ as parameters of the ring VRF protocol. $\mathcal{B}$ generates the public key of all honest parties' key as usual by running $\mathsf{rVRF.KeyGen}$ as Sim does except party P_{i+1}. It lets the public key of P_{i+1} be X.

While simulating $\mathcal{F}_{\mathsf{rvrf}}$, $\mathcal{B}$ simulates the ring signatures of first i parties by running $\mathsf{rVRF.Sign}$ and the parties $\mathsf{P}_{i+2}, \ldots, \mathsf{P}_{n_h}$ by running Algorithm 1 where W is selected randomly. The simulation of P_{i+1} is different. Whenever P_{i+1} needs to sign a message m, it obtains $\mathsf{inbase} = H_{\mathbf{G}}(m) = hY$ from $\texttt{oracle\_queries\_gg}$ and lets $W = hZ$. Then it lets $\mathsf{compk} = X + \mathsf{b}K$, lets $\pi_{\mathtt{eval}} \to \mathsf{NIZK}_{\mathcal{R}_{eval}}.\mathsf{Simulate}(\mathsf{compk}, W, H_{\mathbf{G}}(m))$ and $\pi_{ring} \leftarrow \mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}.\mathsf{Simulate}((\mathsf{comring}, \mathsf{compk}))$. Remark that if (X, Y, Z) is a DH triple (i.e., $\mathsf{DH}(X, Y, Z) \to 1$), P_{i+1} is simulated as in rVRF because $W = x\mathsf{inbase}$ in this case. Otherwise, P_{i+1} is simulated as in the ideal world because W is random. So, if $\mathsf{DH}(X, Y, Z) \to 1$, Sim simulates H_{i+1}. Otherwise, it simulates H_i. In the end of the simulation, if $\mathcal{D}$ outputs i, Sim outputs 0 meaning $\mathsf{DH}(X, Y, Z) \to 0$. Otherwise, it outputs $i+1$. The success probability of Sim is equal to the success probability of $\mathcal{D}$ which distinguishes H_i and H_{i+1}. Since DDH problem is hard, Sim has negligible advantage in the DDH game. So, $\mathcal{D}$ has a negligible advantage too. Hence, from the hybrid argument, we can conclude that H_0 which corresponds the output of honest parties in the ring VRF protocol and H_q which corresponds to the output of honest parties in ideal world are indistinguishable.

This concludes the proof of showing the output of honest parties in the ideal world are indistinguishable from the output of the honest parties in the real protocol.

Next we show that the simulation executed by Sim against $\mathcal{A}$ is indistinguishable from the real protocol execution.

Lemma 6. *The view of $\mathcal{A}$ in its interaction with the simulator* Sim *is indistinguishable from the view of $\mathcal{A}$ in its interaction with real honest parties assuming that CDH is hard in $\mathbf{G}$, $H_{\mathbf{G}}, H, H_p, H_{\mathsf{ring}}$ are random oracles,* $\mathsf{NIZK}_{\mathcal{R}_{eval}}, \mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}$ *are knowledge sound and T_{key} is computationally indistinguishable and binding.*

Proof. The simulation against the real world adversary $\mathcal{A}$ is identical to the real protocol except the output of the honest parties and cases where Sim aborts. We show that the abort cases happen with a negligible probability during the simulation. Sim aborts during the simulation of random oracles H and H_p and during the simulation of verification. We have already explained that the abort case during the simulation of H cannot happen. The abort case happens in the simulation of H_p if $W = hX$ where $X = xG$ or if $\texttt{oracle\_queries\_h\_CP}[\mathsf{comring}, m, W, \mathsf{compk}, R, R_m]$ has already been defined by a value which is different than c. The first case happens in H_p if $\mathcal{F}_{\mathsf{rvrf}}$ selects a random $W \in \mathbf{G}$ for an anonymous key of m, pk for the honest party with the other key X and the random oracle $H_{\mathbf{G}}$ selects a random $h \in \mathbb{F}_p$

where $H_{\mathbf{G}}(m) = hG$ and $W = hX$. Clearly, this can happen with a negligible probability in λ. The second case happens in H_p if $\mathcal{A}$ queries with the input $(\mathsf{comring}, m, W, \mathsf{compk}, R, R_m)$ before $(\pi_1, \pi_2, \mathsf{compk}, \mathsf{comring}, W)$ generated by Gen_{sign}. Since compk is randomly selected by $\mathcal{F}_{\mathsf{rvrf}}$, the probability that $\mathcal{A}$ guesses compk before it is generated is negligible. Now, we are left with the abort case during the verification. For this, we show that if there exists an adversary $\mathcal{A}$ which makes Sim abort during the simulation, then we construct another adversary $\mathcal{B}$ which breaks either the CDH problem or the binding property of $\mathsf{rVRF.KeyGen}$.

Consider a CDH game in a prime p-order group $\mathbf{G}$ with the challenges $G, U, V \in \mathbf{G}$. The CDH challenges are given to the simulator $\mathcal{B}$. Then $\mathcal{B}$ runs a simulated copy of $\mathcal{Z}$ and starts to simulate $\mathcal{F}_{\mathsf{rvrf}}$ and Sim for $\mathcal{Z}$. For this, it first runs the simulated copy of $\mathcal{A}$ as Sim does. $\mathcal{B}$ provides $(\mathbf{G}, p, G, K)$ as a public parameter of the ring VRF protocol to $\mathcal{A}$.

Whenever $\mathcal{B}$ needs to generate a ring signature for m on behalf of an honest party with a public key pk, X, it behaves exactly as $\mathcal{F}_{\mathsf{rvrf}}$ except that it runs Algorithm 2 to generate the signature.

Algorithm 2 $\mathsf{Gen}_{sign}(\mathsf{ring}, W, \{X, \mathsf{pk}\}, \mathsf{ass}, m)$

1: $\mathsf{b} \leftarrow\$ \mathbb{F}_p$
2: $\mathsf{compk} = X + \mathsf{b}\, K$
3: $\pi_{\mathtt{eval}} \leftarrow \mathsf{NIZK}_{\mathcal{R}_{eval}}.\mathsf{Simulate}(\mathsf{compk}, W, H_{\mathbf{G}}(m))$
4: $\mathsf{comring}, \mathsf{opring} \leftarrow \mathsf{rVRF.CommitRing}(\mathsf{ring})$
5: $\pi_{\mathtt{ring}} \leftarrow \mathsf{NIZK}_{\mathcal{R}_{\mathtt{ring}}}.\mathsf{Simulate}(\mathsf{comring}, \mathsf{compk})$
6: **return** $\sigma = (\pi_{eval}, \pi_{ring}, \mathsf{compk}, \mathsf{comring}, W)$

Clearly the ring signature of an honest party outputted by Sim (remember $\mathcal{F}_{\mathsf{rvrf}}$ generates it by Algorithm 1) and the ring signature generated by $\mathcal{B}$ are the same. The only difference is that now $\mathcal{B}$ does not need to set H_p so that $\pi_{\mathtt{eval}}$ verifies because Gen_{sign} in Algorithm 2 does it while simulating the proof for $\mathcal{R}_{eval}$. Therefore, the simulation of H_p is simulated as a usual random oracle by $\mathcal{B}$.

In order to generate the public keys of honest parties, $\mathcal{B}$ picks a random $r_x \in \mathbb{F}_p$ and sets $X = r_x V$. If $\mathsf{rVRF.KeyGen}$ is defined as $\mathsf{pk} = \mathsf{sk}G$, it lets pk be X otherwise it picks a random public key pk . Remark that $\mathcal{B}$ never needs to know the secret key of honest parties to simulate them since $\mathcal{B}$ selects anonymous keys randomly and generates the ring signatures without the secret keys. Since the public key generated by $\mathsf{rVRF.KeyGen}$ is random and independent from the secret key, $\mathcal{B}$'s key generation is indistinguishable from Sim's key generation.

$\mathcal{B}$ simulates $\mathcal{F}_{\mathsf{rvrf}}$ as described but with a difference of the following: whenever $\mathcal{F}_{\mathsf{rvrf}}$ sets up $\mathtt{evaluations}[m, W]$ it queries m, W to the random oracle H described in Figure 5. $\mathcal{B}$ simulates the random oracle H in Figure 5 a usual random oracle. The only difference from the simulation of H by Sim is that $\mathcal{B}$ does not ask for the output of $H(m, W)$ to $\mathcal{F}_{\mathsf{rvrf}}$ but it does not change the simulation because now $\mathcal{F}_{\mathsf{rvrf}}$ asks for it. Remark that since $H_{\mathbf{G}}$ is not simulated as in Figure 2, $\mathcal{B}$ cannot check whether W is an anonymous key generated by an honest secret key or not. However, it does not need this information because H is simulated as a usual random oracle. $\mathcal{B}$ also simulates H_{ring} for the ring commitments as a usual random oracle. Simulation of $H_{\mathbf{G}}$ by $\mathcal{B}$ returns hU instead of hG. The simulation of $H_{\mathbf{G}}$ is indistinguishable from the simulation of $H_{\mathbf{G}}$ in Figure 2.

Oracle H
Input: m, W
if $\texttt{oracle\_queries\_h}[m, W] = \perp$
 $y \leftarrow\$ \{0,1\}^{\ell_{\mathsf{rVRF}}}$
 $\texttt{oracle\_queries\_h}[m, W] := y$
return $\texttt{oracle\_queries\_h}[m, W]$

Fig. 5. The random oracle H

During the simulation, when $\mathcal{A}$ outputs a signature $\sigma = (\pi_{eval}, \pi_{ring}, \mathsf{compk}, \mathsf{comring}, W)$ of message m with ass which is not recorded in $\mathcal{F}_{\mathsf{rvrf}}$'s record, $\mathcal{B}$ runs $\mathsf{rVRF.Ver}(\mathsf{comring}, m, \mathsf{ass}, \sigma)$. If it verifies, it finds the corresponding ring ring of $\mathsf{comring}$ by checking the random oracle H_{ring}'s database. Remark that there exists ring where Merkle tree root of ring is $\mathsf{comring}$ because if it was not the case σ would not verify which also checks π_{ring}. Then it runs the extractor algorithm of $\mathsf{NIZK}_{\mathcal{R}_{\mathsf{ring}}}$ and obtains $X = \mathsf{compk} - \mathsf{b}\,K$ If $\mathsf{pk} = \mathsf{rVRF.OpenRing}(\mathsf{comring}, \mathsf{opring})$ is not an honest key then $\mathcal{B}$ adds W to $\mathcal{W}[m, \mathsf{ring}]$. If pk is not a malicious key but X is generated for honest parties by $\mathcal{B}$ while simulating Sim, $\mathcal{B}$ aborts [1]. The abort case happen with a negligible probability because all the outputs seen by the adversary are independent from X. Otherwise, it runs the extractor algorithm of $\mathsf{NIZK}_{\mathcal{R}_{eval}}$ and obtains $(\hat{\mathsf{sk}}, \hat{\mathsf{b}})$ such that $\mathsf{compk} = \hat{\mathsf{sk}}G + \hat{\mathsf{b}}\,K$ and $W = \hat{\mathsf{sk}}H_{\mathbf{G}}(m)$. If $W \notin \mathcal{W}[m, \mathsf{ring}]$, $\mathcal{B}$ increments $\mathsf{counter}[m, \mathsf{ring}]$ and adds W to $\mathcal{W}[m, \mathsf{ring}]$ for $\mathcal{R}_{\mathtt{ring}}$.

If X is a key which is generated by $\mathcal{B}$ and $X = \hat{\mathsf{sk}}G$, $\mathcal{B}$ solves the CDH problem as follows: $W = \hat{\mathsf{sk}}hU$ where $h = \texttt{oracle\_queries\_gg}[m]$. Since $X = rV$, $W = \hat{\mathsf{sk}}huG = rhuV$. So, $\mathcal{B}$ outputs $r^{-1}h^{-1}W$ as a CDH solution and simulation ends. Remark that this case happens when Sim aborts because of 2.

If $\mathcal{W}[m, \mathsf{ring}] \geq |\mathsf{ring}_{mal}| = t$, $\mathcal{B}$ obtains all the signatures $\{\sigma_i\}_{i=1}^{t}$ that make $\mathcal{B}$ to add an anonymous key to $\mathcal{W}[m, \mathsf{ring}]$. Then it solves the CDH problem as follows: Remark that this case happens when Sim aborts because of 1.

For all $\sigma_j = (\pi_{\mathtt{eval}}, \pi_{\mathtt{ring}}, \mathsf{compk}_j, W_j) \in \{\sigma_i\}_{i=1}^{t}$, $\mathcal{B}$ runs extractor for $\mathcal{R}_{\mathtt{ring}}$ and obtains $\mathsf{opring}_j, \mathsf{b}_j$. Then it obtains the public key $\mathsf{pk}_j = \mathsf{rVRF.OpenRing}(\mathsf{ring}, \mathsf{opring}_j)$ where $\mathsf{pk}_j \in \mathsf{ring}$ and $X_j = \mathsf{compk} - \mathsf{b}K$. Then it adds X_j to a list $\mathcal{X}$ and pk_j to a set $\mathcal{PK}$. One of the following cases happens:

[1] This case never happens if pk is defined $\mathsf{sk}G$

– All X_j in $\mathcal{X}$ are different and $|\mathcal{PK}| \leq t$, $\mathcal{B}$ aborts: Each $\mathsf{pk} \in \mathcal{PK}$ commits to a secret key sk. Since it is a binding commitment there exists one opening r except with a negligible probability. Since $\pi_{\mathtt{ring}}$ verifies in $\mathcal{R}_{\mathtt{ring}}$ whether $\mathcal{R}_{\mathsf{pk}}$ is satisfied, if X_j in $\mathcal{X}$ are different and $|\mathcal{PK}| \leq t$, means that the binding property is broken. Therefore, $\mathcal{B}$ aborts with a negligible probability. We note $\mathcal{B}$ can be in this case only if $\mathsf{pk} \neq \mathsf{sk}G$.
– All X_j in $\mathcal{X}$ are different and $|\mathcal{PK}| > t$: If $\mathcal{B}$ is in this case, it means that there exists one commitment public key $X_a \in \mathcal{X}$ which belongs to an honest party or . Then $\mathcal{B}$ runs the extractor algorithm of $\mathsf{NIZK}_{\mathcal{R}_{eval}}$ and obtains $\hat{\mathsf{sk}}_a, \hat{\mathsf{b}}$ such that $\mathsf{compk}_a = \hat{\mathsf{sk}}_a G + \hat{\mathsf{b}}_a K$ and $W_a = \hat{\mathsf{sk}}_a H_{\mathbf{G}}(m)$. If $\mathcal{B}$ is in this case, $\hat{\mathsf{sk}}_a G \neq X_a$ because otherwise it would solve the CDH as described before. Therefore, $\mathsf{b}_a \neq \hat{\mathsf{b}}_a$. Since $X_a + \mathsf{b}_a K = \hat{\mathsf{sk}}_a G + \hat{\mathsf{b}}_a K$ and $X_a = r_a V$ where r_a is generated by $\mathcal{B}$ during the key generation process, $\mathcal{B}$ obtains a representation of $V = \gamma G + \delta K$ where $\gamma = \hat{\mathsf{sk}}_a r_a^{-1}$ and $\delta = (\hat{\mathsf{b}}_a - \mathsf{b})\, r_a^{-1}$. Then $\mathcal{B}$ stores (γ, δ) to a list rep. If rep does not include another element $(\gamma', \delta') \neq (\gamma, \delta)$, $\mathcal{B}$ rewinds $\mathcal{A}$ to the beginning with a new random coin. Otherwise, it obtains (γ', δ') which is another representation of V i.e., $V = \gamma' G + \delta' K$. Thus, $\mathcal{B}$ can find discrete logarithm of V on base G which is $v = \gamma + \delta\theta$ where $\theta = (\gamma - \gamma')(\delta' - \delta)^{-1}$. $\mathcal{B}$ outputs vU as a CDH solution.
– There exists at least two $X_a, X_b \in \mathcal{X}$ where $X_a = X_b$. $\mathcal{B}$ runs the extractor algorithm of $\mathsf{NIZK}_{\mathcal{R}_{eval}}$ for π_{ring_a} and π_{ring_b} and obtains $(\hat{\mathsf{sk}}_a, \hat{\mathsf{b}}_a)$ and $(\hat{\mathsf{sk}}_b, \hat{\mathsf{b}}_b)$, respectively. Since $W_a \neq W_b$, $\hat{\mathsf{sk}}_a \neq \hat{\mathsf{sk}}_b$. So, $\mathcal{B}$ can obtain two different and non trivial representation of $X_a = X_b$ i.e., $X_a = X_b = \hat{\mathsf{sk}}_a G + (\hat{\mathsf{b}}_a - \mathsf{b}_a)\, K = \hat{\mathsf{sk}}_b G + (\hat{\mathsf{b}}_b - \mathsf{b}_b)\, K$. Thus, $\mathcal{B}$ finds the discrete logarithm of $K = U$ in base G which is $u = \frac{\hat{\mathsf{sk}}_a - \hat{\mathsf{sk}}_b}{\hat{\mathsf{b}}_a - \mathsf{b}_a - \hat{\mathsf{b}}_b + \mathsf{b}_b}$. $\mathcal{B}$ outputs uV as a CDH solution.

So, the probability of $\mathcal{B}$ solves the CDH problem is equal to the probability of $\mathcal{A}$ breaks the forgery or uniqueness in the real protocol. Therefore, if there exists $\mathcal{A}$ that makes Sim aborts during the verification, then we can construct an adversary $\mathcal{B}$ that solves the CDH problem except with a negligible probability.

This completes the security proof of our ring VRF protocol. $\square$