Unbiasable Verifiable Random Functions

Emanuele Giunta[1,2,3], Alistair Stewart[1]

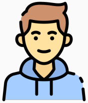
Web3 Foundation, Switzerland.
alistair@web3.foundation

IMDEA Software Institute, Spain.
emanuele.giunta@imdea.org

Universidad Politecnica de Madrid, Spain.

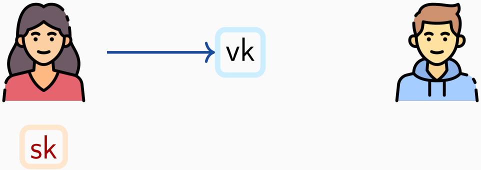
Verifiable Random Functions [MRV99]

VRF.Gen, VRF.Eval, VRF.Vfy



Verifiable Random Functions [MRV99]

VRF.Gen, VRF.Eval, VRF.Vfy

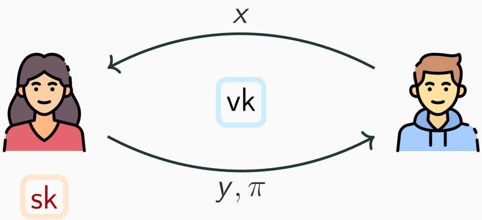


Verifiable Random Functions [MRV99]

VRF.Gen, VRF.Eval, VRF.Vfy

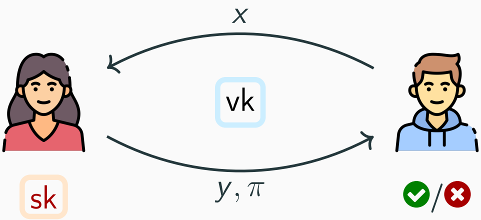
Verifiable Random Functions [MRV99]

VRF.Gen, VRF.Eval, VRF.Vfy

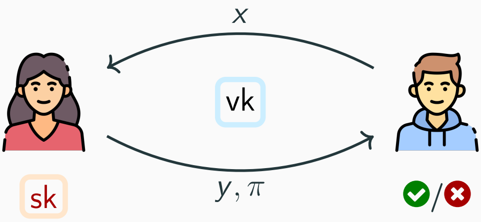


Verifiable Random Functions [MRV99]

VRF.Gen, VRF.Eval, VRF.Vfy



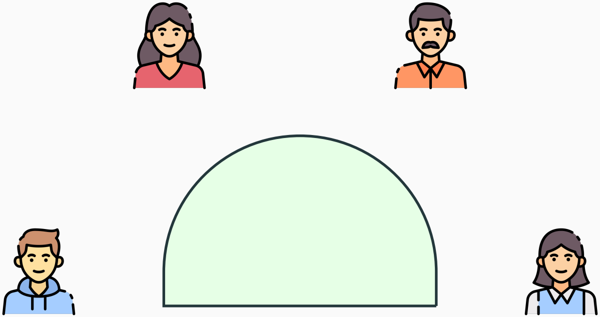
VRF.Gen, VRF.Eval, VRF.Vfy



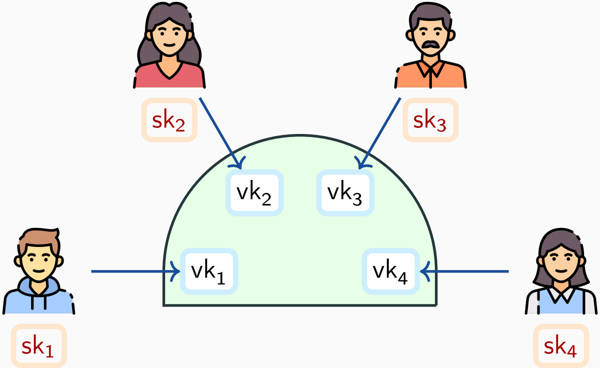
Uniqueness

Pseudorandom

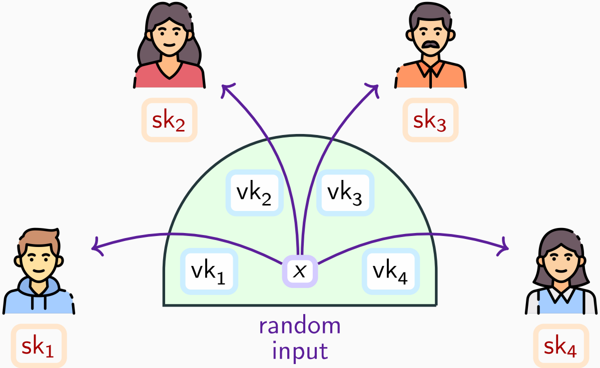
Poker VRF ♡ ♢ ♣ ♠



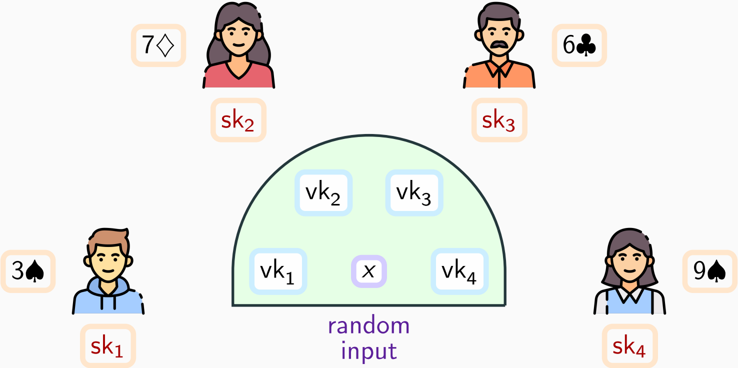
Poker VRF ♡♢♣♠



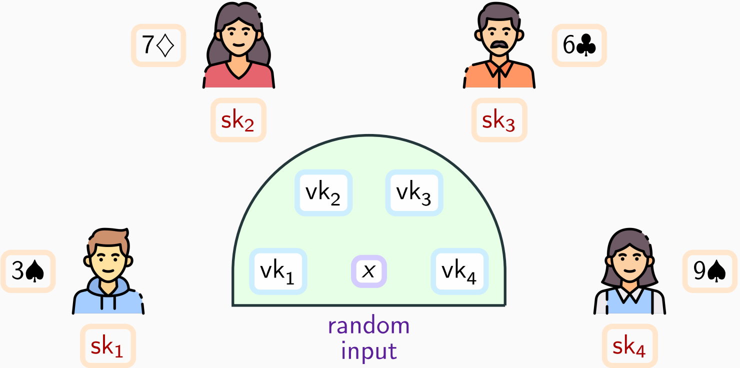
Poker VRF ♡ ♢ ♣ ♠



Poker VRF ♡ ♢ ♣ ♠



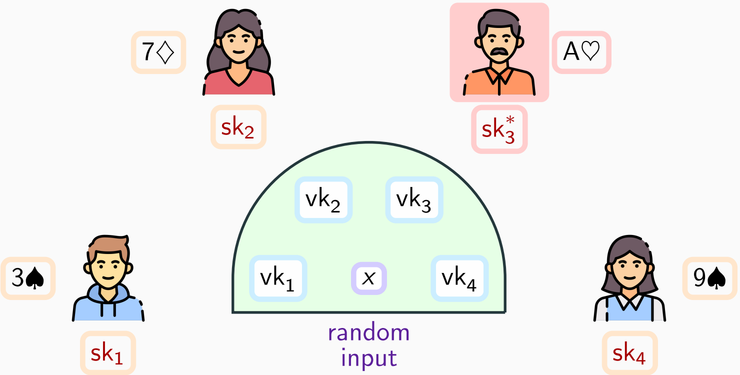
Poker VRF ♡ ♢ ♣ ♠



Unpredictability ✓

Fairness ✗

Poker VRF

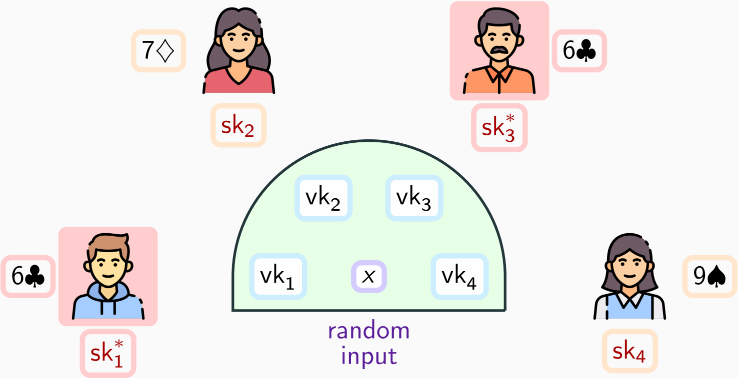


Unpredictability ✔

Fairness ✖

Poker VRF

♡♢♣♠



Unpredictability ✓

Fairness ✗

VRF Unbiasability

[EKS+21]

(Weak) Unbiasability

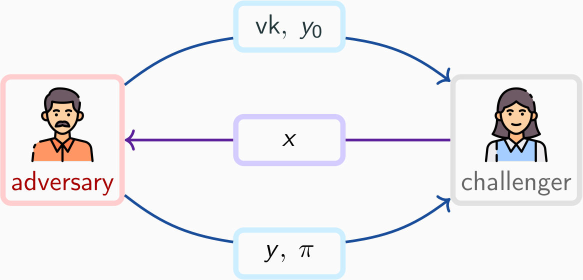
- ✓ Standard model
- ✗ Insufficient for SLE

[DGKR17]

UC-VRF

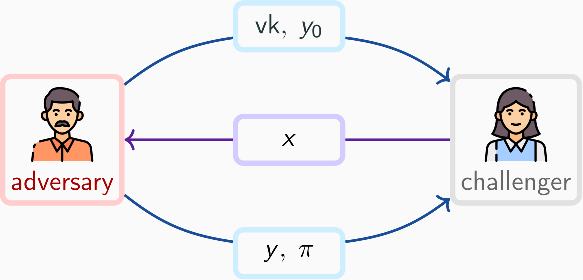
- ✗ Requires ROM
- ✓ Implies SLE

(Weak) Unbiasability [EKS+21]



Win if $y = y_0$ and π is correct.

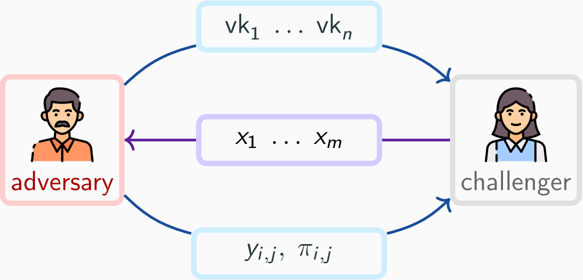
(Weak) Unbiasability [EKS+21]



Win if $y = y_0$ and π is correct.

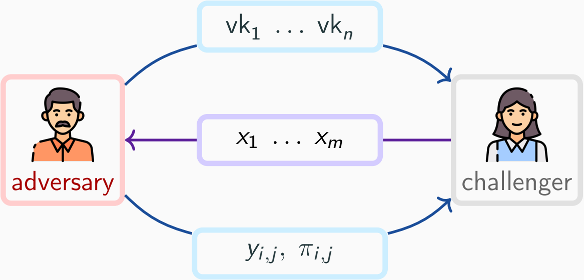
- ✖ Some output bits could be biased
- ✖ Different key's output could be correlated

Unbiasability (First attempt)



Win if $\pi_{i,j}$ are **correct** $y_{i,j}$ are **far** from random.

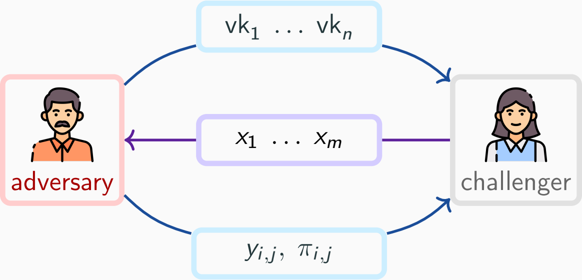
Unbiasability (First attempt)



Win if $\pi_{i,j}$ are **correct** $y_{i,j}$ are **far** from random.

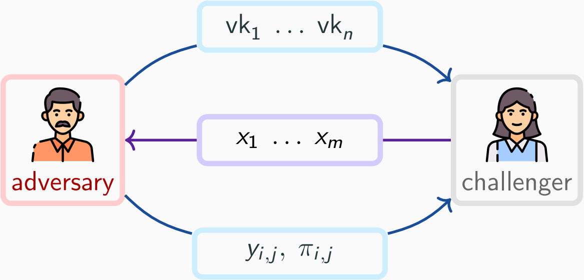
❌ Does not exclude biased vk^* that cannot be evaluated on the full domain

Unbiasability (Second attempt)



1. If $\pi_{i,j}$ is incorrect, **erase** $y_{i,j} \leftarrow \perp$
2. Win if **non-erased** $y_{i,j}$ are **far** from random

Unbiasability (Second attempt)

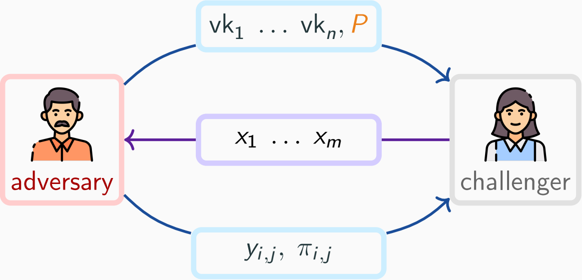


1. If $\pi_{i,j}$ is incorrect, **erase** $y_{i,j} \leftarrow \perp$
2. Win if **non-erased** $y_{i,j}$ are **far** from random

✖ Selective openings are always biased

Unbiasability

[GS24]



1. P is **monotone**[1].
2. If $\pi_{i,j}$ is incorrect, **erase** $y_{i,j} \leftarrow \perp$.
3. Win if $\Pr[P(y) = 1] \gg \Pr[P(z) = 1]$ for a **random** z.

[1] Let x^* be x with some positions erased. Then $P(x^*) \leq P(x)$.

Constructions

Our Constructions

1. VUF to VRF in the Random Oracle Model.

Our Constructions

1. VUF to VRF in the Random Oracle Model.

2. Verifiable Random **Bijection** (VRB) from any VRF + DL.

Our Constructions

1. VUF to VRF in the Random Oracle Model.
2. Verifiable Random **Bijection** (VRB) from any VRF + DL.
3. **Unbiasable VRF** from any VRF + DL* + PRF*.

VUF to VRF transform in the ROM

$F_{\mathsf{sk}} : X \to Y$ **V**erifiable **U**npredictable **F**unction with public key vk.

1st Transform: $F^*_{\mathsf{sk}}(x) = H(F_{\mathsf{sk}}(x), x, \mathsf{vk})$.

2nd Transform: $F^*_{\mathsf{sk}}(x) = H(F_{\mathsf{sk}}(x))$.

VUF to VRF transform in the ROM

$F_{\mathsf{sk}} : X \to Y$ **V**erifiable **U**npredictable **F**unction with public key vk.

$$\textbf{1}^{\textbf{st}}\ \textbf{Transform:} \quad F^*_{\mathsf{sk}}(x) = H\left(F_{\mathsf{sk}}(x), x, \mathsf{vk}\right).$$

$$\textbf{2}^{\textbf{nd}}\ \textbf{Transform:} \quad F^*_{\mathsf{sk}}(x) = H\left(F_{\mathsf{sk}}(x)\right).$$

- Both are VRF in the ROM.
- **First**: Unbiasable for any VUF.
- **Second**: Unbiasable if F_{sk} is collision resistant on random inputs:

VUF to VRF transform in the ROM

$F_{\mathsf{sk}} : X \to Y$ **V**erifiable **U**npredictable **F**unction with public key vk.

$$\textbf{1}^{\textbf{st}}\ \textbf{Transform:} \quad F^*_{\mathsf{sk}}(x) = H\left(F_{\mathsf{sk}}(x), x, \mathsf{vk}\right).$$

$$\textbf{2}^{\textbf{nd}}\ \textbf{Transform:} \quad F^*_{\mathsf{sk}}(x) = H\left(F_{\mathsf{sk}}(x)\right).$$

- Both are VRF in the ROM.
- **First**: Unbiasable for any VUF.
- **Second**: Unbiasable if F_{sk} is collision resistant on random inputs:
    1. $F_{\mathsf{sk}}(x_1) \neq F_{\mathsf{sk}}(x_2)$ for random x_1, x_2.
    2. $F_{\mathsf{sk}_1}(x) \neq F_{\mathsf{sk}_2}(x)$ for random x and $\mathsf{sk}_1 \neq \mathsf{sk}_2$.

Verifiable Random Bijection

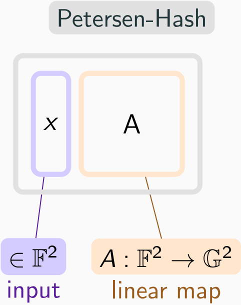
$\mathbb{G}$ prime order group where DL is hard.

Verifiable Random Bijection

$\mathbb{G}$ prime order group where DL is hard.

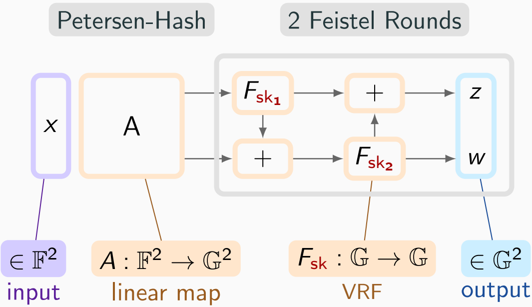
Verifiable Random Bijection

$\mathbb{G}$ prime order group where DL is hard.



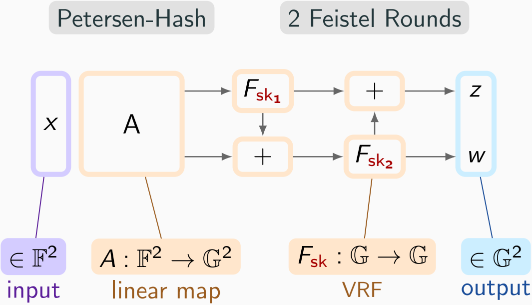
Verifiable Random Bijection

$\mathbb{G}$ prime order group where DL is hard.



Verifiable Random Bijection

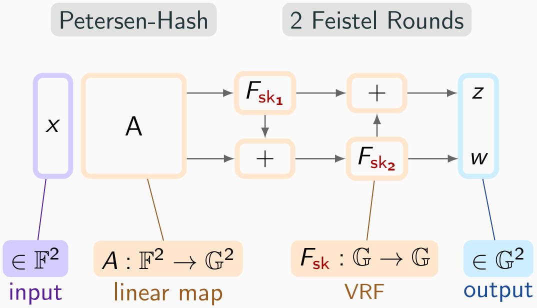
$\mathbb{G}$ prime order group where DL is hard.



✓ Certified bijection

Verifiable Random Bijection

$\mathbb{G}$ prime order group where DL is hard.



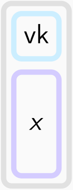
- ✔ Certified bijection
- ✘ Unbiasable only for a single vk!

VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.

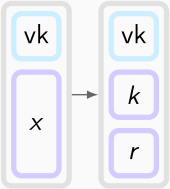
VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.



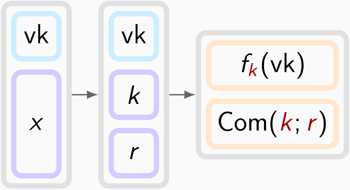
VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.



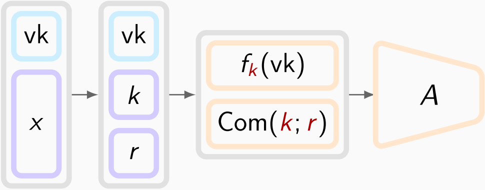
VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.



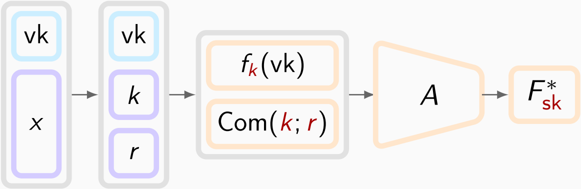
VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.



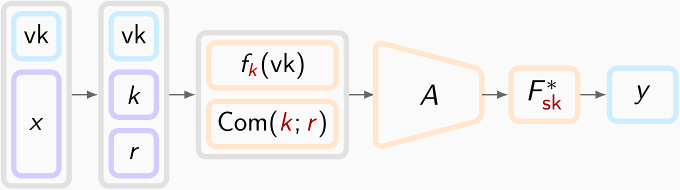
VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.



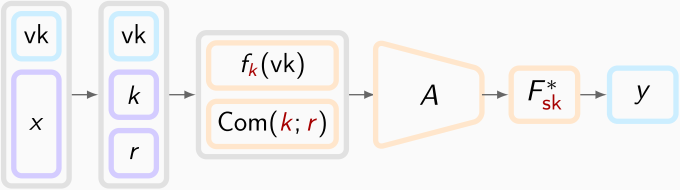
VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.



VRF to UVRF Compiler (simplified)

Let F^*_{sk} be a VRB with verification key vk and f a PRF.



Unbiasable if **DL** and the **PRF** are secure with **preprocessing**.

Conclusions

We provided a new notion of **unbiasability** that is:

- **Sufficient** for applications (e.g. leader election).
- **Satisfied** by existing constructions in the NPROM.
- **Achievable** in the standard model generically.

Conclusions

We provided a new notion of **unbiasability** that is:

- **Sufficient** for applications (e.g. leader election).
- **Satisfied** by existing constructions in the NPROM.
- **Achievable** in the standard model generically.

Open questions:

- Minimal assumptions for UVRF ...or separations?
- Lattice/Isogeny based constructions
- VRB with small domain

Conclusions

We provided a new notion of **unbiasability** that is:

- **Sufficient** for applications (e.g. leader election).
- **Satisfied** by existing constructions in the NPROM.
- **Achievable** in the standard model generically.

Open questions:

- Minimal assumptions for UVRF ...or separations?
- Lattice/Isogeny based constructions
- VRB with small domain

Thanks for your attention!