Jackpot: Non-Interactive Aggregatable Lotteries

Nils Fleischhacker, Mathias Hall-Andersen, Mark Simkin, and Benedikt Wagner

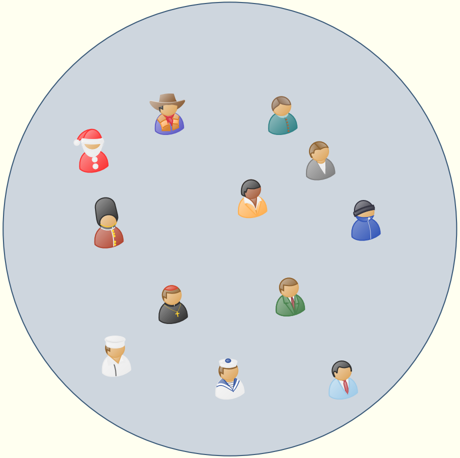
13. December 2024

RUB

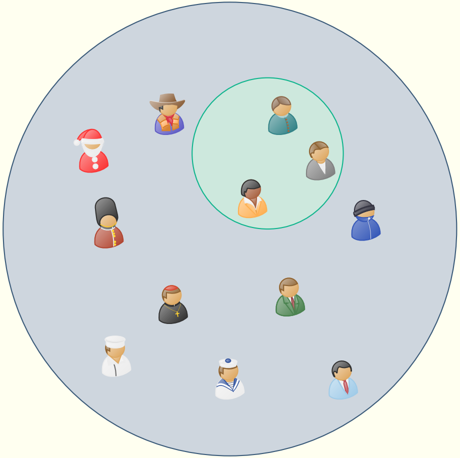
HORST GÖRTZ INSTITUT

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

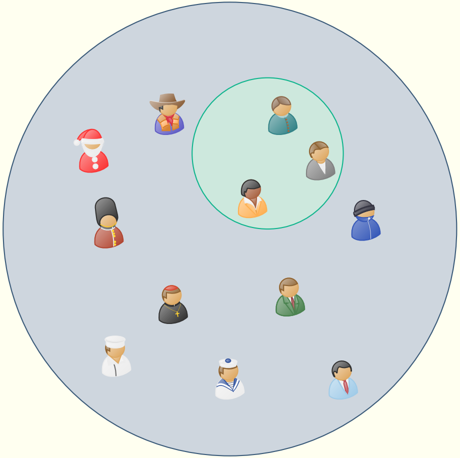
Why Lotteries?



Why Lotteries?



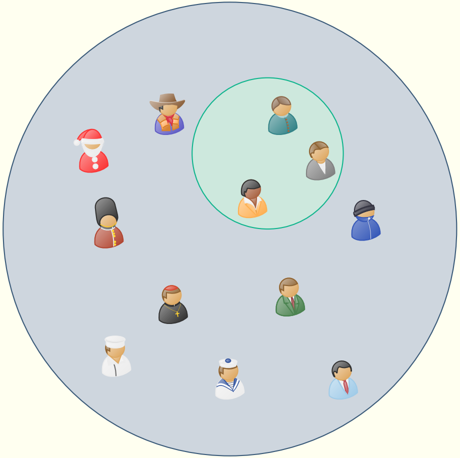
Why Lotteries?



Goal: Select a committee of size $\approx N/k$ such that:

- You can't be selected with probability $> 1/k$.

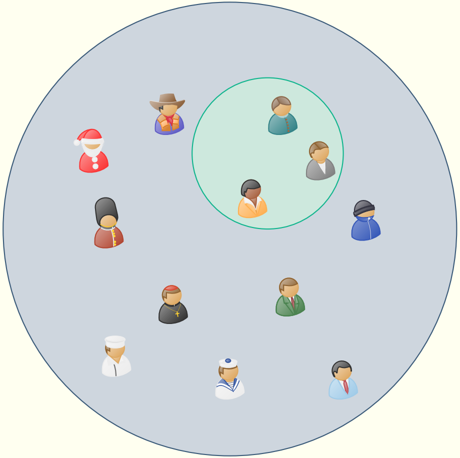
Why Lotteries?



Goal: Select a committee of size $\approx N/k$ such that:

- You can't be selected with probability $> 1/k$.
- Honest participants are selected with $1/k$.

Why Lotteries?

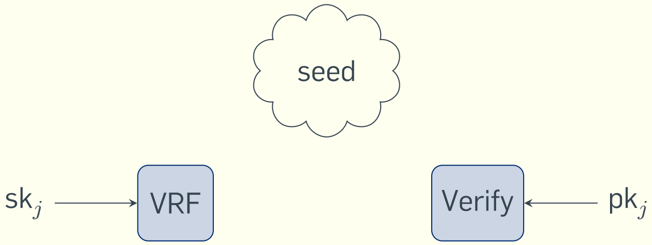


Goal: Select a committee of size $\approx N/k$ such that:

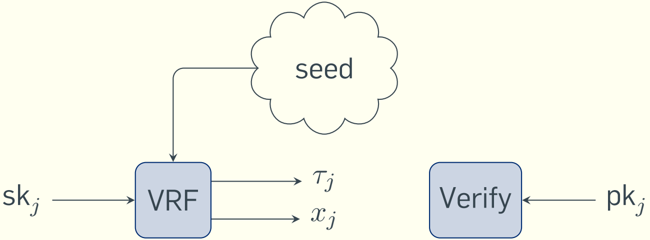
- You can't be selected with probability $> 1/k$.
- Honest participants are selected with $1/k$.
- Participants can't correlate their selection.

A Lottery Using VRFs

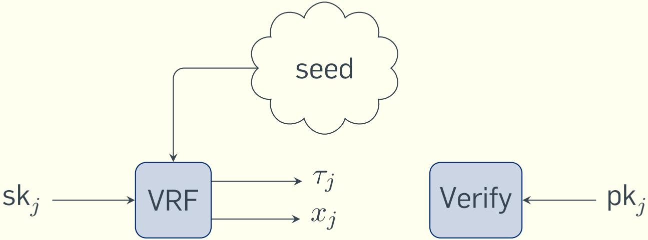
A Lottery Using VRFs



A Lottery Using VRFs

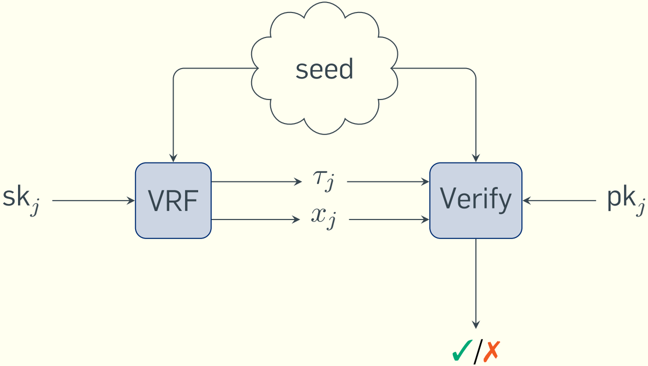


A Lottery Using VRFs



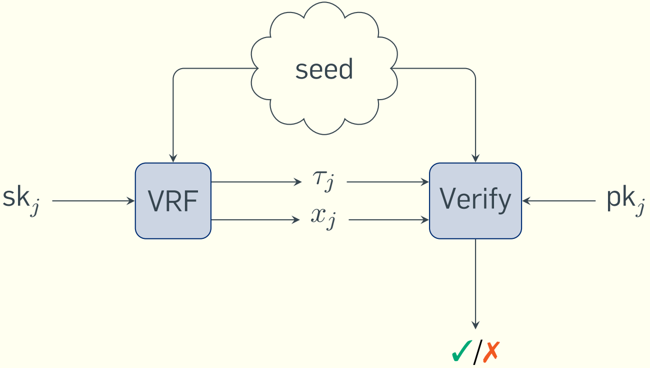
If $x_j \leq t$ you win the lottery.

A Lottery Using VRFs



If $x_j \leq t$ you win the lottery.

A Lottery Using VRFs

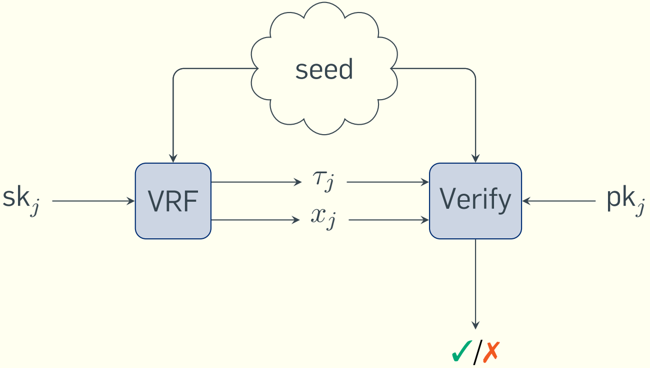


If $x_j \leq t$ you win the lottery.

Problem: Storing the "winning tickets" takes a lot of space.

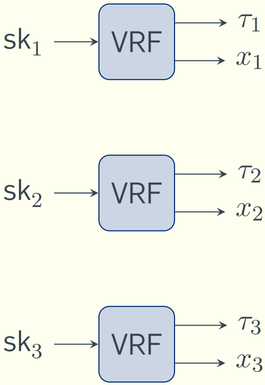
A Lottery Using Small Codomain VRFs

Idea: Use linearly homomorphic VRF with codomain $[k]$.

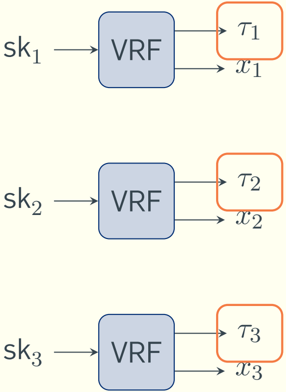


If $x_j = H(i, j, \text{seed})$ you win the lottery.

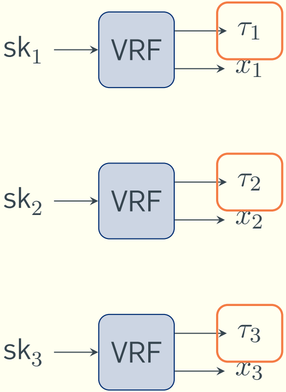
A Lottery Using Small Codomain VRFs



A Lottery Using Small Codomain VRFs

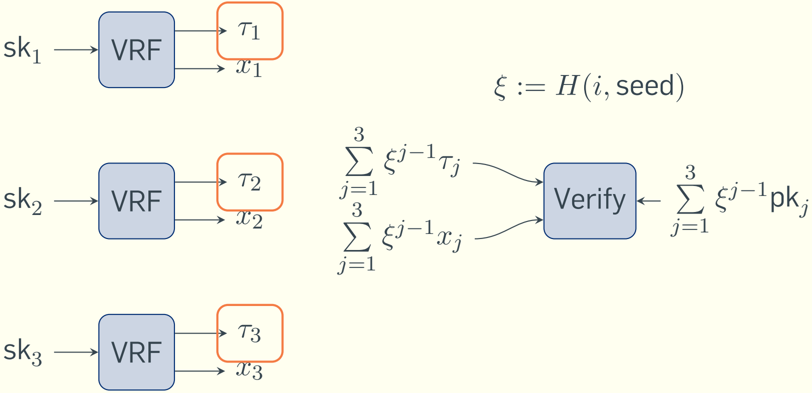


A Lottery Using Small Codomain VRFs

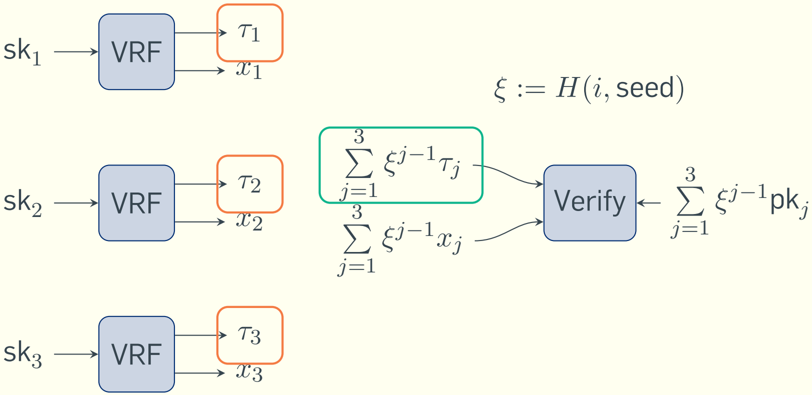


$$\xi := H(i, \mathsf{seed})$$

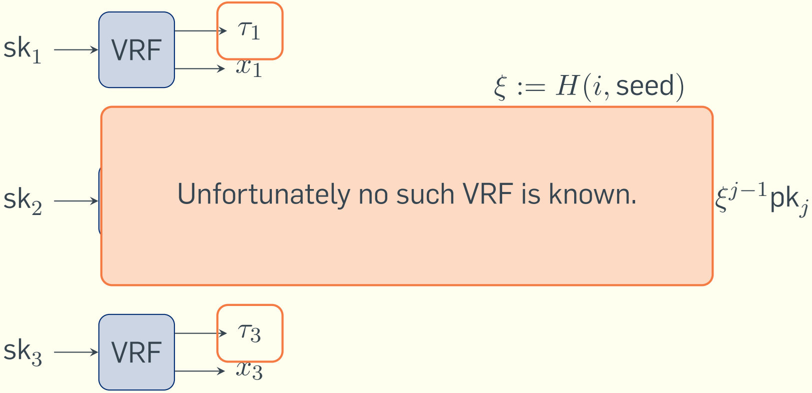
A Lottery Using Small Codomain VRFs



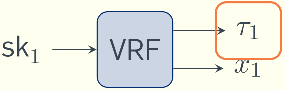
A Lottery Using Small Codomain VRFs



A Lottery Using Small Codomain VRFs

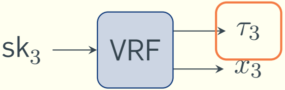


A Lottery Using Small Codomain VRFs



$$\xi := H(i, \mathsf{seed})$$

But what's a VRF other than a vector commitment for long random vectors?



Using a Vector Commitment

$$(\texttt{com}_j, St_j) \leftarrow \mathsf{Com}((x_{j,1}, \ldots, x_{j,\ell}))$$

Using a Vector Commitment

$$(\mathtt{com}_j, St_j) \leftarrow \mathsf{Com}((x_{j,1}, \ldots, x_{j,\ell}))$$

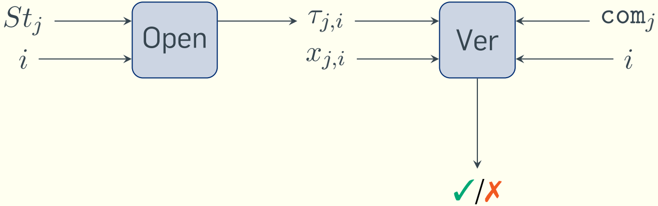
Using a Vector Commitment

$$(\texttt{com}_j, St_j) \leftarrow \mathsf{Com}((x_{j,1}, \ldots, x_{j,\ell}))$$

If $x_{j,i} = H(i, j, \text{seed})$ you win the lottery.

Using a Vector Commitment

$$(\mathtt{com}_j, St_j) \leftarrow \mathsf{Com}((x_{j,1}, \ldots, x_{j,\ell}))$$



If $x_{j,i} = H(i, j, \mathsf{seed})$ you win the lottery.

Using a Vector Commitment

$$(\texttt{com}_j, St_j) \leftarrow \mathsf{Com}((x_{j,1}, \ldots, x_{j,\ell}))$$

Fortunately, we do know of linearly homomorphic vector commitments.
Notably KZG commitments.

✓/✗

If $x_{j,i} = H(i, j, \text{seed})$ you win the lottery.

The Woes of Composability

- Unfortunately we require simulation extractability.

The Woes of Composability

- Unfortunately we require simulation extractability.
- Linearly homomorphic vector commitments are inherently not simulation extractable.

The Woes of Composability

- Unfortunately we require simulation extractability.
- Linearly homomorphic vector commitments are inherently not simulation extractable.
- But: Only openings have to be aggregateable.

The Woes of Composability

- Unfortunately we require simulation extractability.
- Linearly homomorphic vector commitments are inherently not simulation extractable.
- But: Only openings have to be aggregateable.
- Idea: Break homomorphism of commitments but retain it for openings.

A Simulation Extractable VC from KZG

- To commit to a vector $\vec{x}$ of length ℓ:
  1. Choose random polynomial f of degree $\ell + 1$ such that $f(i) = x_i$.
  2. Compute $(\mathtt{com}_{\mathsf{KZG}}, St) \leftarrow \mathsf{KZG.Com}(\mathsf{ck}_{\mathsf{KZG}}, f)$.
  3. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$
  4. Compute $\tau_0 \leftarrow \mathsf{KZG.Open}(\mathsf{ck}_{\mathsf{KZG}}, St, z_0)$.
  5. Full commitment is $(\mathtt{com}_{\mathsf{KZG}}, y_0 = f(z_0), \tau_0)$

A Simulation Extractable VC from KZG

- To commit to a vector $\vec{x}$ of length ℓ:
  1. Choose random polynomial f of degree $\ell + 1$ such that $f(i) = x_i$.
  2. Compute $(\mathtt{com}_{\mathsf{KZG}}, St) \leftarrow \mathsf{KZG.Com}(\mathsf{ck}_{\mathsf{KZG}}, f)$.
  3. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$
  4. Compute $\tau_0 \leftarrow \mathsf{KZG.Open}(\mathsf{ck}_{\mathsf{KZG}}, St, z_0)$.
  5. Full commitment is $(\mathtt{com}_{\mathsf{KZG}}, y_0 = f(z_0), \tau_0)$
- We can verify that commitments are well formed
  1. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$.
  2. Return $\mathsf{KZG.Ver}(\mathsf{ck}_{\mathsf{KZG}}, \mathtt{com}_{\mathsf{KZG}}, z_0, y_0, \tau_0)$

A Simulation Extractable VC from KZG

- To commit to a vector $\vec{x}$ of length ℓ:
  1. Choose random polynomial f of degree $\ell + 1$ such that $f(i) = x_i$.
  2. Compute $(\mathtt{com}_{\mathsf{KZG}}, St) \leftarrow \mathsf{KZG.Com}(\mathsf{ck}_{\mathsf{KZG}}, f)$.
  3. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$
  4. Compute $\tau_0 \leftarrow \mathsf{KZG.Open}(\mathsf{ck}_{\mathsf{KZG}}, St, z_0)$.
  5. Full commitment is $(\mathtt{com}_{\mathsf{KZG}}, y_0 = f(z_0), \tau_0)$
- We can verify that commitments are well formed
  1. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$.
  2. Return $\mathsf{KZG.Ver}(\mathsf{ck}_{\mathsf{KZG}}, \mathtt{com}_{\mathsf{KZG}}, z_0, y_0, \tau_0)$
- Openings are simply openings of the KZG commitment.

A Simulation Extractable VC from KZG

- To commit to a vector $\vec{x}$ of length ℓ:
  1. Choose random polynomial f of degree $\ell + 1$ such that $f(i) = x_i$.
  2. Compute $(\mathtt{com}_{\mathsf{KZG}}, St) \leftarrow \mathsf{KZG.Com}(\mathsf{ck}_{\mathsf{KZG}}, f)$.
  3. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$
  4. Compute $\tau_0 \leftarrow \mathsf{KZG.Open}(\mathsf{ck}_{\mathsf{KZG}}, St, z_0)$.
  5. Full commitment is $(\mathtt{com}_{\mathsf{KZG}}, y_0 = f(z_0), \tau_0)$
- We can verify that commitments are well formed
  1. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$.
  2. Return $\mathsf{KZG.Ver}(\mathsf{ck}_{\mathsf{KZG}}, \mathtt{com}_{\mathsf{KZG}}, z_0, y_0, \tau_0)$
- Openings are simply openings of the KZG commitment.
- Openings can be aggregated.
  1. Derive $\xi := \mathsf{H}'(i, (\mathtt{com}_j)_{j=1}^{L}, (x_j)_{j=1}^{L})$.
  2. Return $\tau := \sum_{j=1}^{L} \xi^{j-1} \tau_j$

A Simulation Extractable VC from KZG

- To commit to a vector $\vec{x}$ of length ℓ:
  1. Choose random polynomial f of degree $\ell + 1$ such that $f(i) = x_i$.
  2. Compute $(\mathtt{com}_{\mathsf{KZG}}, St) \leftarrow \mathsf{KZG.Com}(\mathsf{ck}_{\mathsf{KZG}}, f)$.
  3. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$
  4. Compute $\tau_0 \leftarrow \mathsf{KZG.Open}(\mathsf{ck}_{\mathsf{KZG}}, St, z_0)$.
  5. Full commitment is $(\mathtt{com}_{\mathsf{KZG}}, y_0 = f(z_0), \tau_0)$
- We can verify that commitments are well formed
  1. Derive $z_0 = \mathsf{H}(\mathtt{com}_{\mathsf{KZG}})$.
  2. Return $\mathsf{KZG.Ver}(\mathsf{ck}_{\mathsf{KZG}}, \mathtt{com}_{\mathsf{KZG}}, z_0, y_0, \tau_0)$
- Openings are simply openings of the KZG commitment.
- Openings can be aggregated.
  1. Derive $\xi := \mathsf{H}'(i, (\mathtt{com}_j)_{j=1}^{L}, (x_j)_{j=1}^{L})$.
  2. Return $\tau := \sum_{j=1}^{L} \xi^{j-1} \tau_j$
- Aggregated openings can be verified using the linear homomorphism of KZG.
  1. Individually verify that all commitments are well formed.
  2. Derive $\xi := \mathsf{H}'(i, (\mathtt{com}_j)_{j=1}^{L}, (x_j)_{j=1}^{L})$
  3. Compute $x := \sum_{j=1}^{L} \xi^{j-1} x_j$ and $\mathtt{com} := \prod_{j=1}^{L} \mathtt{com}_{\mathsf{KZG},j}^{\xi^{j-1}}$.
  4. Return $\mathsf{KZG.Ver}(\mathsf{ck}_{\mathsf{KZG}}, \mathtt{com}, i, x, \tau)$.

Comparison

Tickets L	VRF-BLS [B]	Ours [B]	Ratio VRF-BLS/Ours
1	48	80	0.6
16	768	80	9.6
256	12288	80	153.6
1024	49152	80	614.4
2048	98304	80	1228.8

		$L = 1$	$L = 16$	$L = 256$	$L = 1024$	$L = 2048$
Ours	Aggregate [ms]	0.038	0.390	2.377	6.899	14.242
Ours	Ver [ms]	1.413	1.959	3.948	8.875	15.422
VRF-BLS	Ver [ms]	1.663	2.990	7.959	19.010	33.838