On the Limits of Black-Box Techniques for Minimizing Cryptographic Assumptions

Nicholas Brandt
crypto@nicholasbrandt.de

November 21, 2025

Outline

Preliminaries

- Reductionism underlying modern cryptography

Outline

Preliminaries

- Reductionism underlying modern cryptography
- Relating cryptographic primitives

Outline

Preliminaries

- Reductionism underlying modern cryptography
- Relating cryptographic primitives

Contributions

- Overview

Outline

Preliminaries

- Reductionism underlying modern cryptography
- Relating cryptographic primitives

Contributions

- Overview
- (Non-)black-box construction of unbiasable verifiable random functions (VRFs)

Some Cryptographic Primitives

Collision-Resistant Hash Function

Verifiable Random Function

Public-Key Encryption

Key Agreement

Oblivious Transfer

One-Way Function

Pseudorandom Generator

Pseudorandom Function

Digital Signatures

Commitment Scheme

Secret-Key Encryption

Reductionism

Security based on computational hardness

- $\mathsf{P} = \mathsf{NP} \implies$ most cryptographic primitives can be broken efficiently.
- Unconditional security proof $\implies \mathsf{P} \neq \mathsf{NP}$.

Reductionism

Security based on computational hardness

- $\mathrm{P} = \mathrm{NP} \implies$ most cryptographic primitives can be broken efficiently.
- Unconditional security proof $\implies \mathrm{P} \neq \mathrm{NP}$.
- Security is based on computational hardness of problems, e.g. number-theory, lattice problems, cyclic groups, etc.

Reductionism

Security based on computational hardness

- P $=$ NP $\implies$ most cryptographic primitives can be broken efficiently.
- Unconditional security proof $\implies$ P $\neq$ NP.
- Security is based on computational hardness of problems, e.g. number-theory, lattice problems, cyclic groups, etc.
- Reduction: $\exists \mathrm{PPT} \mathcal{A}_{\mathrm{primitive}} \implies \exists \mathrm{PPT} \mathcal{A}_{\mathrm{problem}}$

Reductionism

Security based on computational hardness

- P $=$ NP $\implies$ most cryptographic primitives can be broken efficiently.
- Unconditional security proof $\implies$ P $\neq$ NP.
- Security is based on computational hardness of problems, e.g. number-theory, lattice problems, cyclic groups, etc.
- Reduction: $\exists \mathrm{PPT} \mathcal{A}_{\mathrm{primitive}} \implies \exists \mathrm{PPT} \mathcal{A}_{\mathrm{problem}}$

Which assumption is best?

$$\text{Hardness of DDH} \longrightarrow \text{Security of KA}$$

Reductionism

Security based on computational hardness

- P $=$ NP $\implies$ most cryptographic primitives can be broken efficiently.
- Unconditional security proof $\implies$ P $\neq$ NP.
- Security is based on computational hardness of problems, e.g. number-theory, lattice problems, cyclic groups, etc.
- Reduction: $\exists \mathrm{PPT} \mathcal{A}_{\mathrm{primitive}} \implies \exists \mathrm{PPT} \mathcal{A}_{\mathrm{problem}}$

Which assumption is best?

Shor [Sho94]

~~Hardness of DDH~~

Security of KA

Reductionism

Security based on computational hardness

- P = NP $\implies$ most cryptographic primitives can be broken efficiently.
- Unconditional security proof $\implies$ P $\neq$ NP.
- Security is based on computational hardness of problems, e.g. number-theory, lattice problems, cyclic groups, etc.
- Reduction: $\exists \mathrm{PPT} \mathcal{A}_{\mathrm{primitive}} \implies \exists \mathrm{PPT} \mathcal{A}_{\mathrm{problem}}$

Which assumption is best?

Shor [Sho94]

~~Hardness of DDH~~

Security of KA

?

Hardness of LWE

Reductionism

What is a minimal assumption for a given primitive?

Reductionism

What is a cryptographic reduction?

Reductionism

Cryptographic construction/reduction:

$$\mathsf{A} \longrightarrow \mathsf{B}$$

Reductionism

Cryptographic construction/reduction:

$$A \longrightarrow B$$

Construction: $\boxed{\Pi_B} \longleftrightarrow \boxed{\Pi_A}$

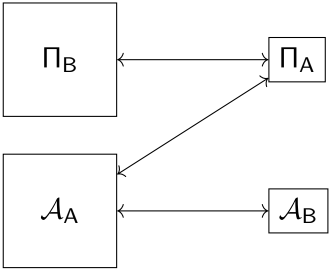
Reductionism

Cryptographic construction/reduction:

$$\mathsf{A} \longrightarrow \mathsf{B}$$

Construction:

Reduction:



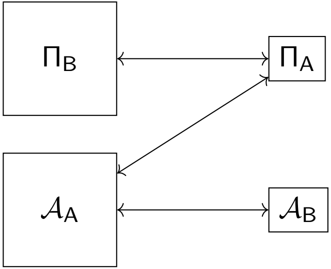
Reductionism

Cryptographic construction/reduction:

$$\mathsf{A} \longrightarrow \mathsf{B}$$

Construction:

Reduction:



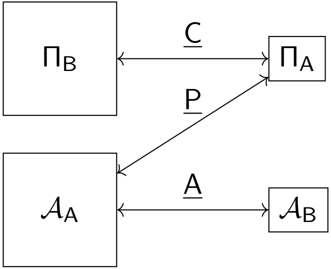
Reductionism

Cryptographic construction/reduction:

$$\mathsf{A} \longrightarrow \mathsf{B}$$

Construction:

Reduction:



CAP taxonomy [BBF13]:

Construction	Adversary	Primitive
$\in \{B, N\}$	$\in \{B, N\}$	$\in \{B, N\}$

Some Cryptographic Primitives

Collision-Resistant Hash Function

Verifiable Random Function

Public-Key Encryption

Key Agreement

Oblivious Transfer

One-Way Function

Pseudorandom Generator

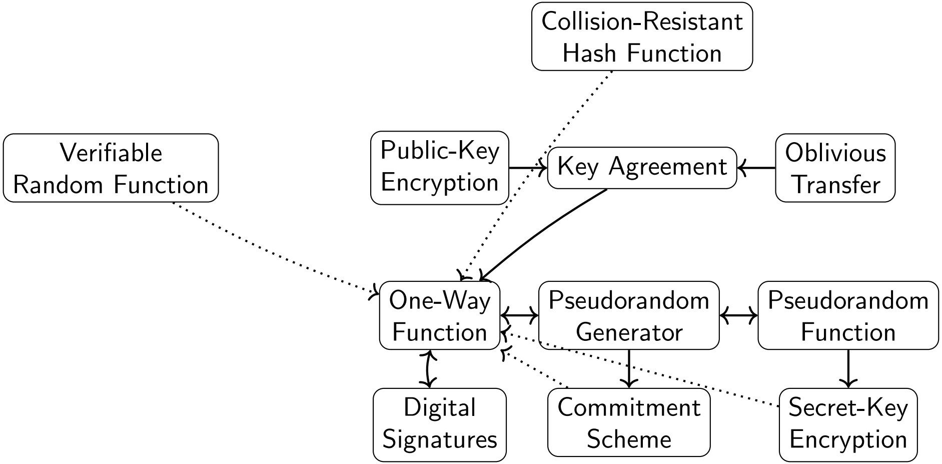
Pseudorandom Function

Digital Signatures

Commitment Scheme

Secret-Key Encryption

Some Cryptographic Primitives



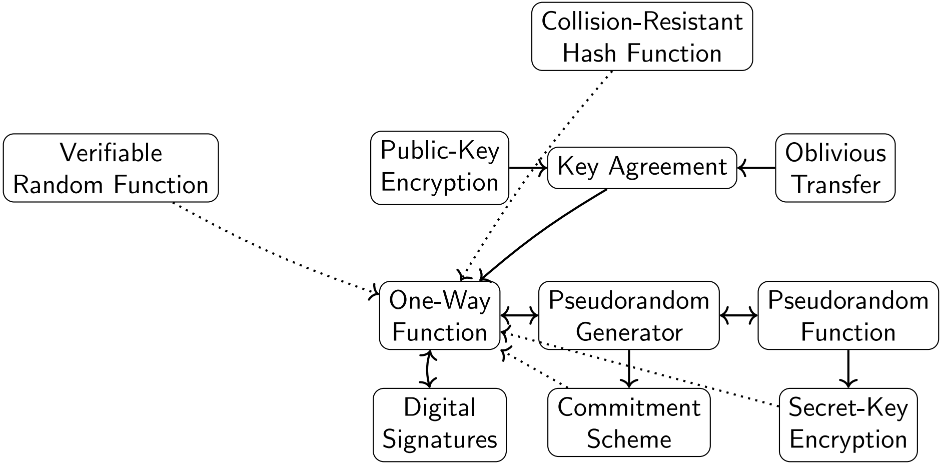
Separations

Separations

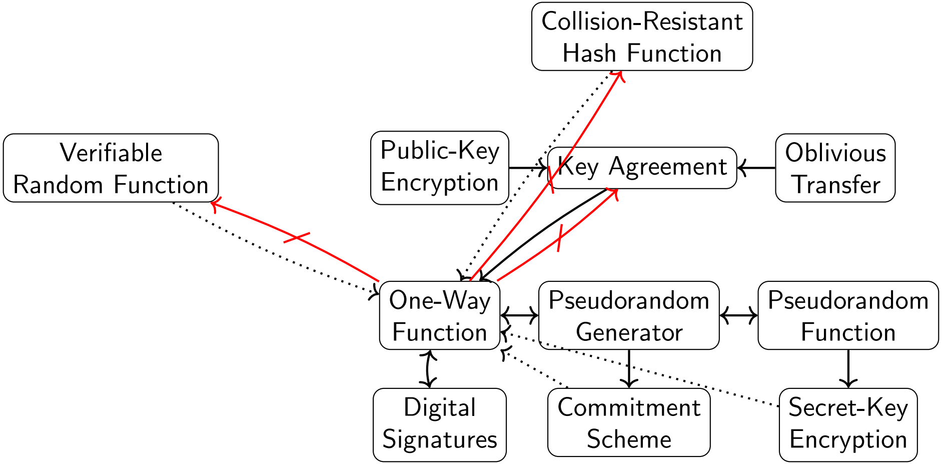
Oracle separations [IR90; IR89; HR04]

- Rules out (in particular) BBB-reductions.
- Relative to some oracle, primitive OWF exists but KA does not: OWF $\not\leq$ KA.

Some Cryptographic Primitives



Some Cryptographic Primitives



Separations

Oracle separations [IR90; IR89; HR04]

- Rules out (in particular) BBB-reductions.
- Relative to some oracle, primitive OWF exists but KA does not: OWF $\not\leq$ KA.

Separations

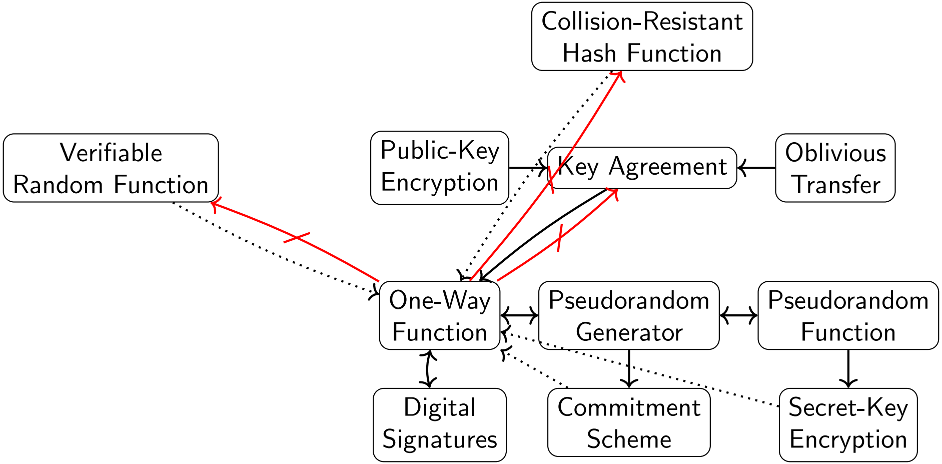
Oracle separations [IR90; IR89; HR04]

- Rules out (in particular) BBB-reductions.
- Relative to some oracle, primitive OWF exists but KA does not: OWF $\not\leq$ KA.

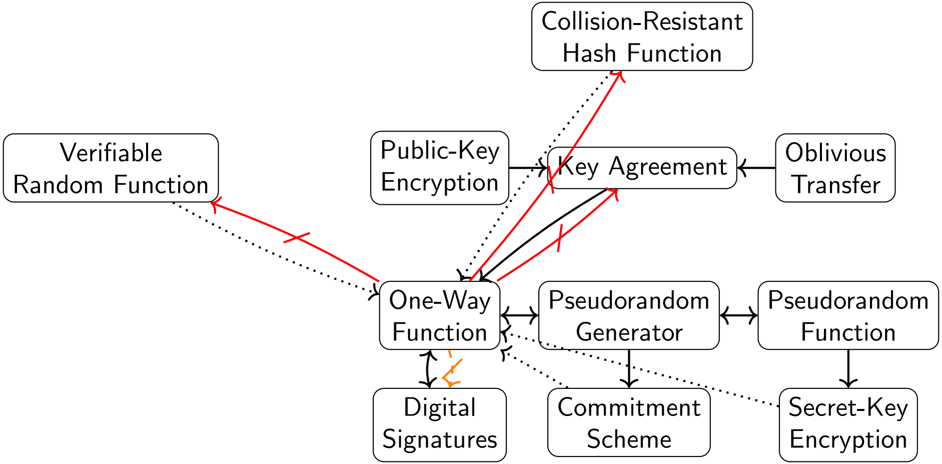
Meta-reductions [BV98; Cor02; Pas11]

- Rules out NBN-reductions.
- Often requires special properties of the reduction (algebraicity, small loss, non-interactive games, etc.).

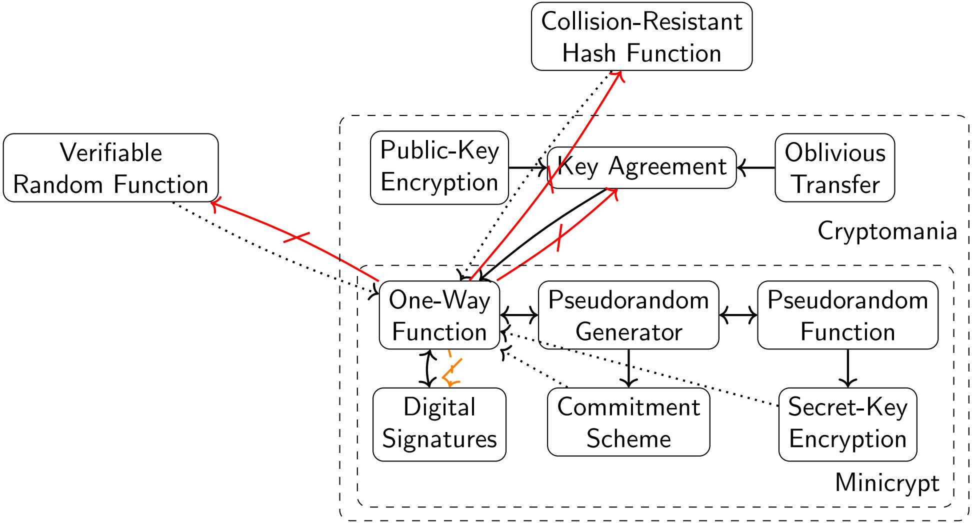
Some Cryptographic Primitives



Some Cryptographic Primitives



Some Cryptographic Primitives [Imp95]



Contributions

Contributions in the thesis

Contributions

Contributions in the thesis

- [BHK+22]: Meta-reductions for VRFs from standard group assumptions

Contributions

Contributions in the thesis

- [BHK$^+$22]: Meta-reductions for VRFs from standard group assumptions
- [Bra25]: (Non-)black-box reductions for unbiasable VRFs

Contributions

Contributions in the thesis

- [BHK$^+$22]: Meta-reductions for VRFs from standard group assumptions
- [Bra25]: (Non-)black-box reductions for unbiasable VRFs
- [Bra24]: Non-black-box lower bounds for Levin–Kolmogorov complexity

Contributions

Contributions in the thesis

- [BHK+22]: Meta-reductions for VRFs from standard group assumptions
- [Bra25]: (Non-)black-box reductions for unbiasable VRFs
- [Bra24]: Non-black-box lower bounds for Levin–Kolmogorov complexity

Other works (not in the thesis)

- [BMM+23]: Tight setup bounds for secure multi-party computation with identifiable abort
- [BHK+24]: Tightly secure blind signatures in pairing-free groups
- [BFM24]: A formal treatment of key transparency
- [BNG+25]: Constrained VRFs from novel pairing-based assumptions

Definition of VRF

Verifiable Random Function [MRV99]

A *verifiable random function* (VRF) consists of three algorithms:

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{vk}, \mathsf{sk})$
- $\mathsf{Eval}(\mathsf{sk}, x) \to (y \in \{0,1\}, \pi)$
- $\mathsf{Verify}(\mathsf{vk}, x, y, \pi) \to \{0,1\}$

Definition of VRF

Verifiable Random Function [MRV99]

A *verifiable random function* (VRF) consists of three algorithms:

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{vk}, \mathsf{sk})$
- $\mathsf{Eval}(\mathsf{sk}, x) \to (y \in \{0,1\}, \pi)$
- $\mathsf{Verify}(\mathsf{vk}, x, y, \pi) \to \{0,1\}$

Properties

- Pseudorandomness: VRF images look random (analog to PRFs).

Definition of VRF

Verifiable Random Function [MRV99]

A *verifiable random function* (VRF) consists of three algorithms:

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{vk}, \mathsf{sk})$
- $\mathsf{Eval}(\mathsf{sk}, x) \to (y \in \{0,1\}, \pi)$
- $\mathsf{Verify}(\mathsf{vk}, x, y, \pi) \to \{0,1\}$

Properties

- Pseudorandomness: VRF images look random (analog to PRFs).
- Unique Provability:

$$\forall \mathsf{vk}, x, y_0, \pi_0, y_1, \pi_1 : \wedge \begin{array}{ll} \mathsf{Verify}(\mathsf{vk}, x, y_0, \pi_0) & = 1 \\ \mathsf{Verify}(\mathsf{vk}, x, y_1, \pi_1) & = 1 \end{array} \implies y_0 = y_1$$

Contributions

Meta-reductions for VRFs [BHK^{+}22]

(Non-)black-box reductions for unbiasable VRFs [Bra25]

Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

Contributions

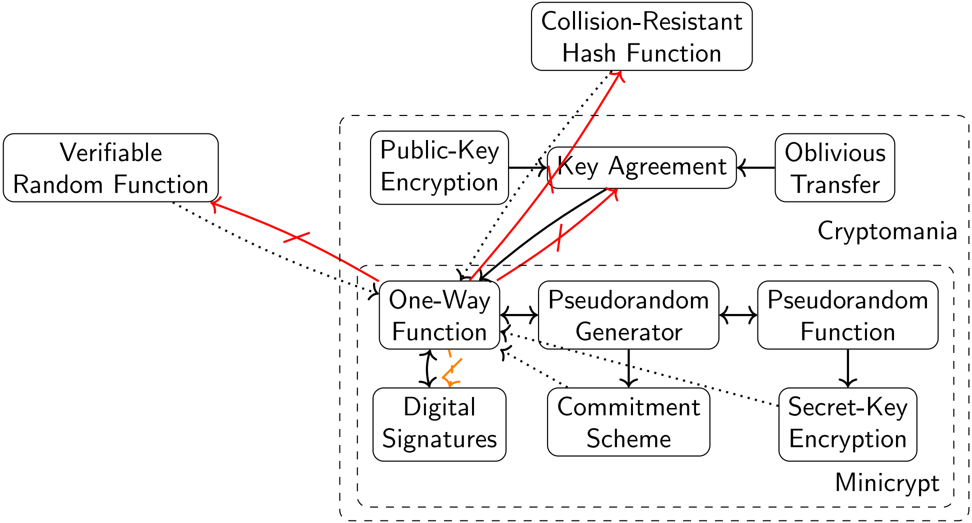
Meta-reductions for VRFs [BHK^{+}22]

- Rules out algebraic NBN-reductions from various non-interactive assumptions to pairing-based VRFs with short proofs.
- For a set of natural VRFs constructions:
  the shorter the VRF proof, the stronger the assumption needed.

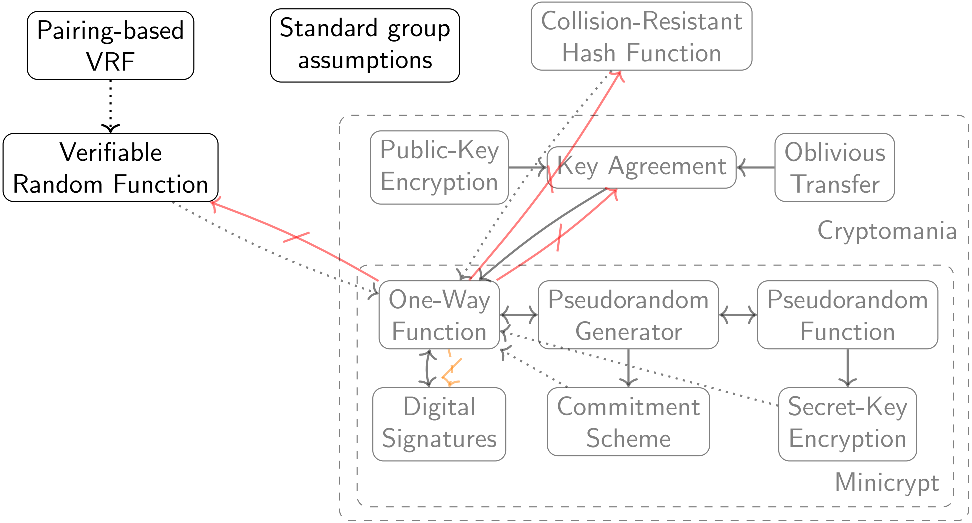
(Non-)black-box reductions for unbiasable VRFs [Bra25]

Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

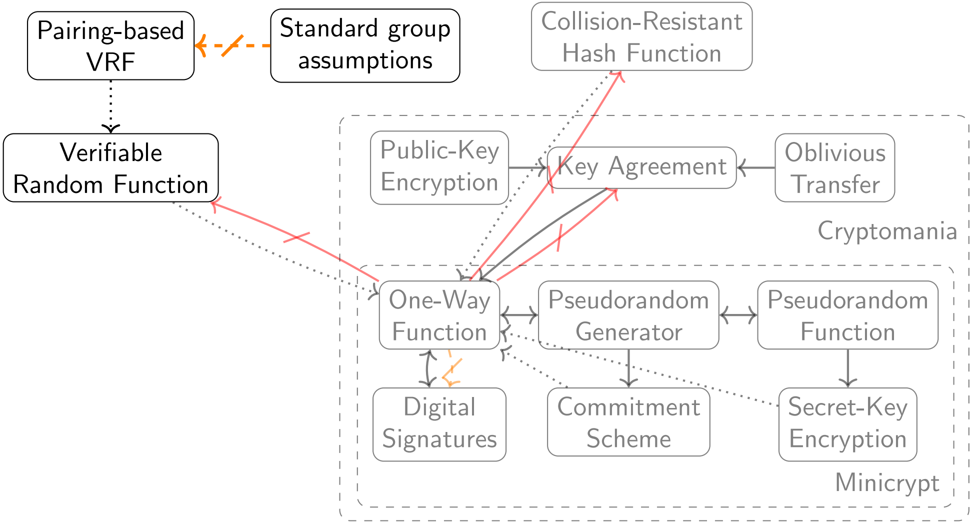
Some Cryptographic Primitives [Imp95]



Some Cryptographic Primitives



Some Cryptographic Primitives



Contributions

Meta-reductions for VRFs [BHK$^+$22]

- Rules out algebraic NBN-reductions from various non-interactive assumptions to pairing-based VRFs with short proofs.
- For a set of natural VRFs constructions:
  the shorter the VRF proof, the stronger the assumption needed.

(Non-)black-box reductions for unbiasable VRFs [Bra25]

Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

Contributions

Meta-reductions for VRFs [BHK$^+$22]

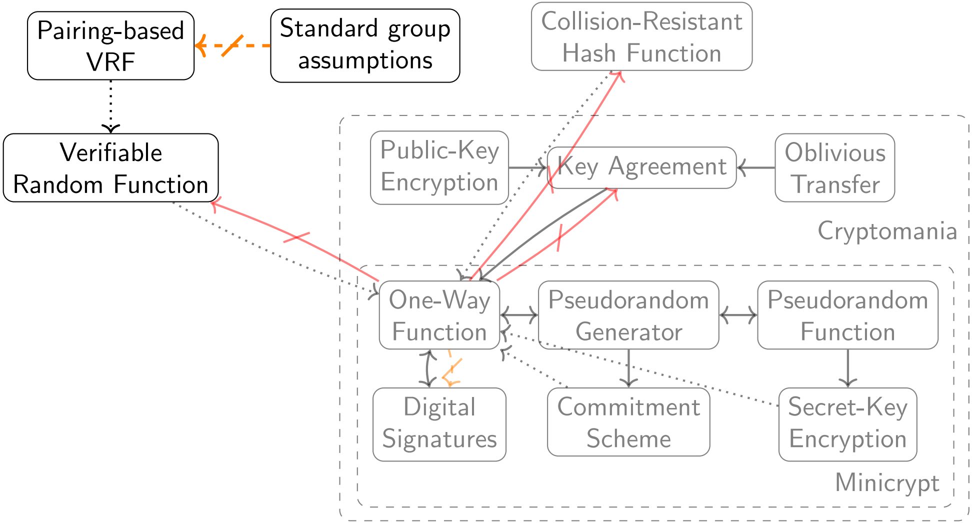
- Rules out algebraic NBN-reductions from various non-interactive assumptions to pairing-based VRFs with short proofs.
- For a set of natural VRFs constructions:
  the shorter the VRF proof, the stronger the assumption needed.

(Non-)black-box reductions for unbiasable VRFs [Bra25]

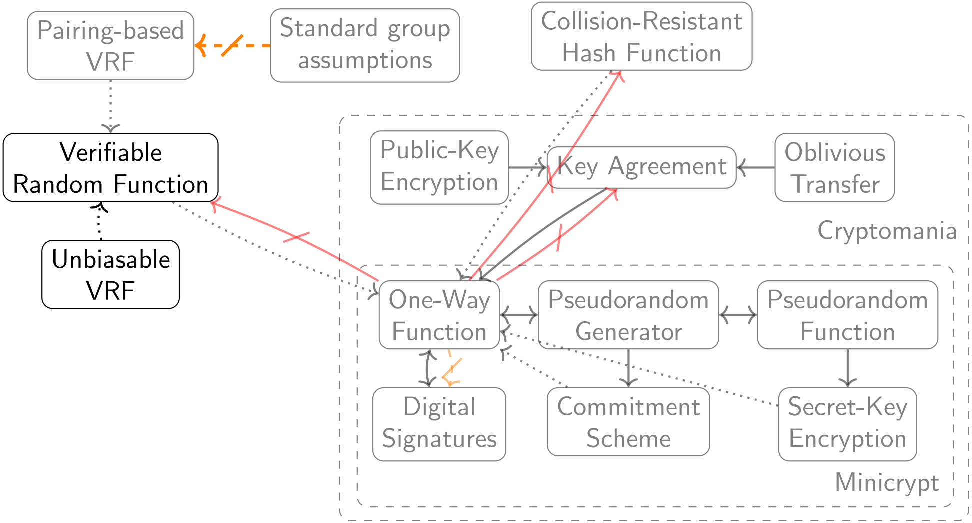
- BBB-reduction: injective OWF, CRH, VRF $\implies$ unbiasable VRF (subexp. loss)
- BNN-reduction: injective OWF, VRF $\implies$ unbiasable VRF (poly. loss)

Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

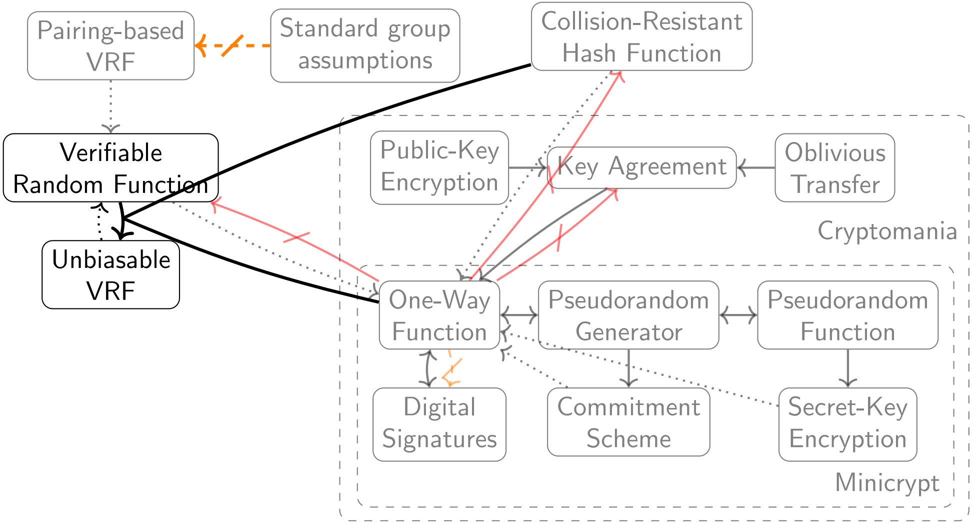
Some Cryptographic Primitives



Some Cryptographic Primitives



Some Cryptographic Primitives



Contributions

Meta-reductions for VRFs [BHK$^+$22]

- Rules out algebraic NBN-reductions from various non-interactive assumptions to pairing-based VRFs with short proofs.
- For a set of natural VRFs constructions:
  the shorter the VRF proof, the stronger the assumption needed.

(Non-)black-box reductions for unbiasable VRFs [Bra25]

- BBB-reduction: injective OWF, CRH, VRF $\implies$ unbiasable VRF (subexp. loss)
- BNN-reduction: injective OWF, VRF $\implies$ unbiasable VRF (poly. loss)

Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

Contributions

Meta-reductions for VRFs [BHK+22]

- Rules out algebraic NBN-reductions from various non-interactive assumptions to pairing-based VRFs with short proofs.
- For a set of natural VRFs constructions:
  the shorter the VRF proof, the stronger the assumption needed.

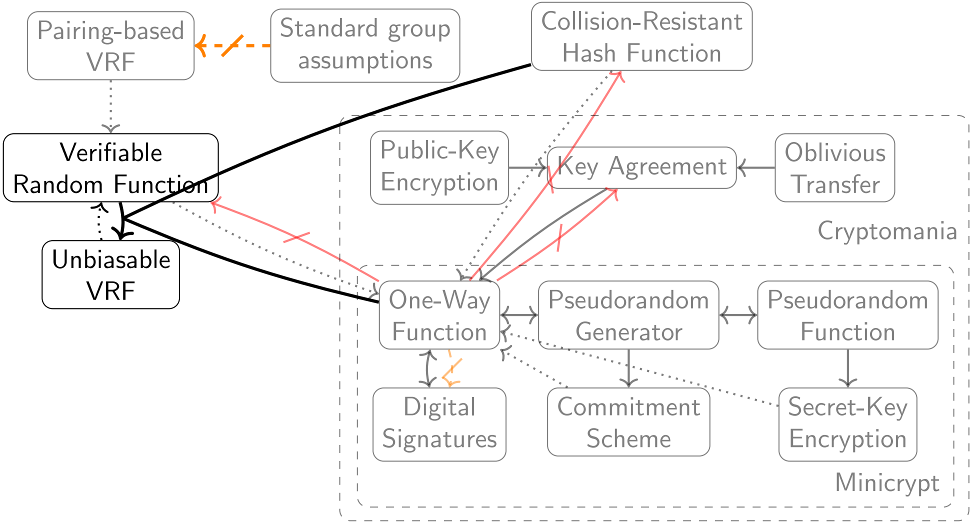
(Non-)black-box reductions for unbiasable VRFs [Bra25]

- BBB-reduction: injective OWF, CRH, VRF $\implies$ unbiasable VRF (subexp. loss)
- BNN-reduction: injective OWF, VRF $\implies$ unbiasable VRF (poly. loss)

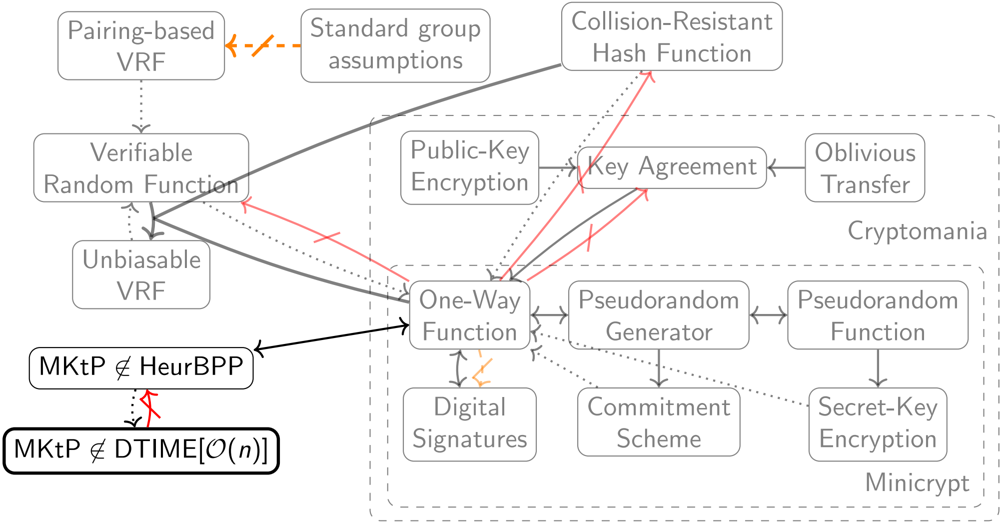
Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

- First unconditional lower bound MKtP $\notin$ DTIME$[\mathcal{O}(n)]$.
- Conditional lower bounds MKtP $\notin$ DTIME$[\mathfrak{t}(n)] \cap \mathrm{Heur}_{0,o(1/\mathfrak{t}(n))}$DTIME$[\mathcal{O}(n)]$.

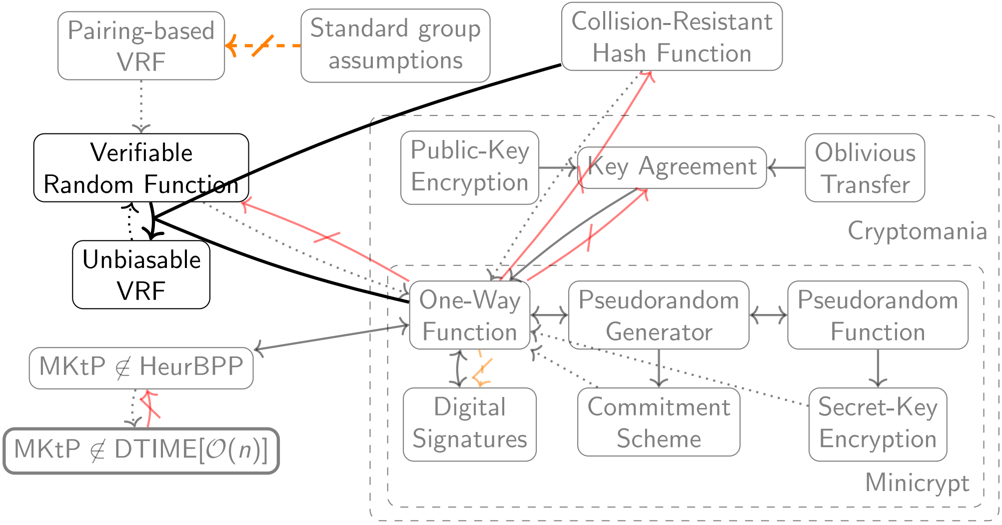
Some Cryptographic Primitives



Some Cryptographic Primitives



Some Cryptographic Primitives



Definition of VRF

Verifiable Random Function [MRV99]

A *verifiable random function* (VRF) consists of three algorithms:

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{vk}, \mathsf{sk})$
- $\mathsf{Eval}(\mathsf{sk}, x) \to (y \in \{0,1\}, \pi)$
- $\mathsf{Verify}(\mathsf{vk}, x, y, \pi) \to \{0,1\}$

Properties

- Pseudorandomness: VRF images look random (analog to PRFs).
- Unique Provability:

$$\forall \mathsf{vk}, x, y_0, \pi_0, y_1, \pi_1 : \bigwedge \begin{array}{ll} \mathsf{Verify}(\mathsf{vk}, x, y_0, \pi_0) & = 1 \\ \mathsf{Verify}(\mathsf{vk}, x, y_1, \pi_1) & = 1 \end{array} \implies y_0 = y_1$$

Definition of VRF

Verifiable Random Function [MRV99]

A *verifiable random function* (VRF) consists of three algorithms:

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{vk}, \mathsf{sk})$
- $\mathsf{Eval}(\mathsf{sk}, x) \to (y \in \{0,1\}, \pi)$
- $\mathsf{Verify}(\mathsf{vk}, x, y, \pi) \to \{0,1\}$

Properties

- Pseudorandomness: VRF images look random (analog to PRFs).
- Unique Provability:

$$\forall \mathsf{vk}, x, y_0, \pi_0, y_1, \pi_1 : \bigwedge \begin{array}{ll} \mathsf{Verify}(\mathsf{vk}, x, y_0, \pi_0) & = 1 \\ \mathsf{Verify}(\mathsf{vk}, x, y_1, \pi_1) & = 1 \end{array} \implies y_0 = y_1$$

- Unbiasability [GS24]:
  random preimage $\implies$ random image even for maliciously chosen vk

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$ $\mathcal{A}(1^\lambda; r_\mathcal{A})$

Simplified Unbiasability Game

$$\mathcal{C}(1^\lambda) \qquad\qquad \xleftarrow{\mathsf{vk}} \qquad\qquad \mathcal{A}(1^\lambda; r_\mathcal{A})$$

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$ $\mathcal{A}(1^\lambda; r_{\mathcal{A}})$

$\xleftarrow{\quad \mathsf{vk} \quad}$

$x \leftarrow \{0,1\}^\lambda$

find y_0, π : $\mathsf{VRF.Verify}(\mathsf{vk}, x, y_0, \pi) = 1$

$y_1 \leftarrow \{0,1\}$

$b \leftarrow \{0,1\}$

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$ $\qquad\qquad$ $\mathcal{A}(1^\lambda; r_\mathcal{A})$

$\xleftarrow{\mathsf{vk}}$

$x \leftarrow \{0,1\}^\lambda$

find y_0, π : $\mathsf{VRF.Verify}(\mathsf{vk}, x, y_0, \pi) = 1$

$y_1 \leftarrow \{0,1\}$

$b \leftarrow \{0,1\}$

$\xrightarrow{y_b}$

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$		$\mathcal{A}(1^\lambda; r_{\mathcal{A}})$
	$\xleftarrow{\quad \mathsf{vk} \quad}$	
$x \leftarrow \{0,1\}^\lambda$ **find** $y_0, \pi : \mathsf{VRF.Verify}(\mathsf{vk}, x, y_0, \pi) = 1$ $y_1 \leftarrow \{0,1\}$ $b \leftarrow \{0,1\}$		
	$\xrightarrow{\quad y_b \quad}$	
	$\xleftarrow{\quad b' \quad}$	

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$ $\qquad\qquad$ $\mathcal{A}(1^\lambda; r_\mathcal{A})$

$$\xleftarrow{\quad \mathsf{vk} \quad}$$

$x \leftarrow \{0,1\}^\lambda$

find $y_0, \pi : \mathsf{VRF.Verify}(\mathsf{vk}, x, y_0, \pi) = 1$

$y_1 \leftarrow \{0,1\}$

$b \leftarrow \{0,1\}$

$$\xrightarrow{\quad y_b \quad}$$

$$\xleftarrow{\quad b' \quad}$$

return $b' \stackrel{?}{=} b$

Construction Overview

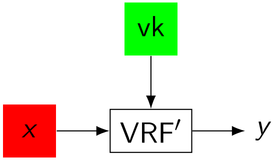
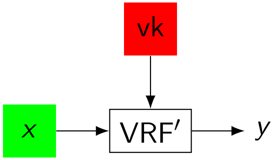
Construction [Bra24]

$$\begin{pmatrix} \text{VRF} \\ \text{one-way permutation (OWP)} \\ \text{collision-resistant hash function (CRH)} \end{pmatrix} \implies \text{unbiasable VRF}$$

Construction Overview

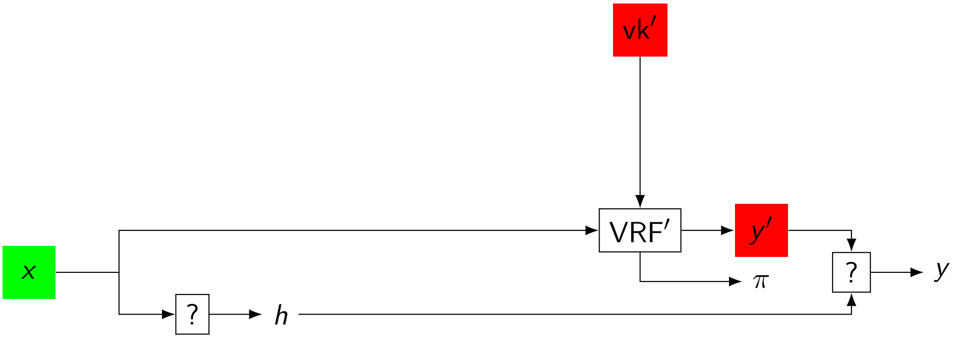
Construction [Bra24]

$$\begin{pmatrix} \text{VRF} \\ \text{one-way permutation (OWP)} \\ \text{collision-resistant hash function (CRH)} \end{pmatrix} \implies \text{unbiasable VRF}$$

Pseudorandomness ☑	Unbiasability □
	

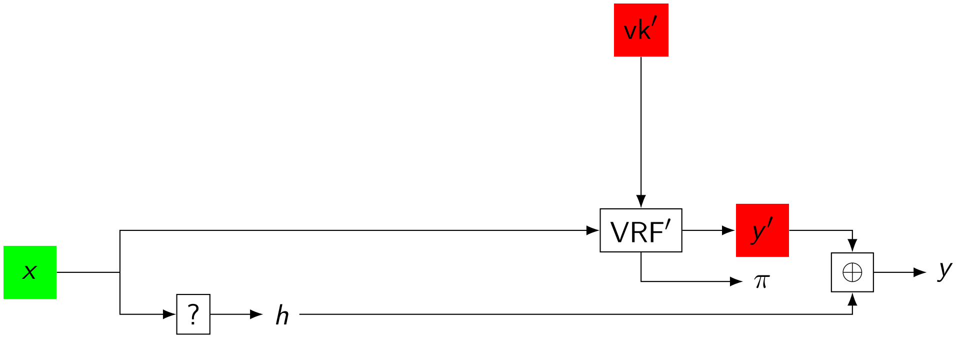
Construction

Pseudorandomness ☑ | Unbiasability ☐



Construction

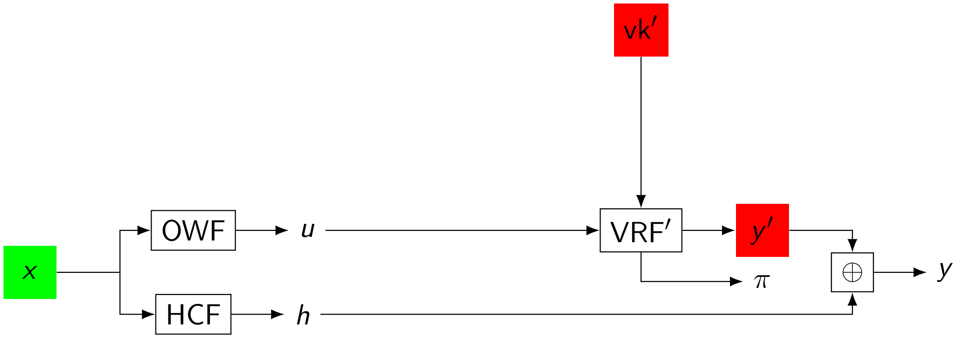
Pseudorandomness ☑ | Unbiasability ☐



Construction

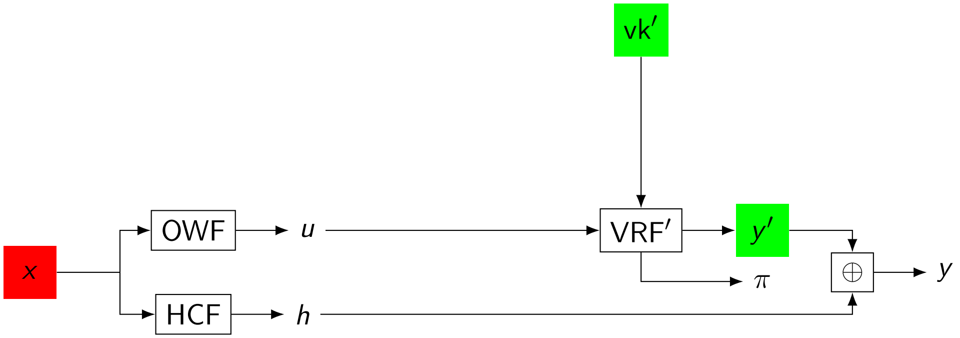
Pseudorandomness ☐

Unbiasability ☑



Construction

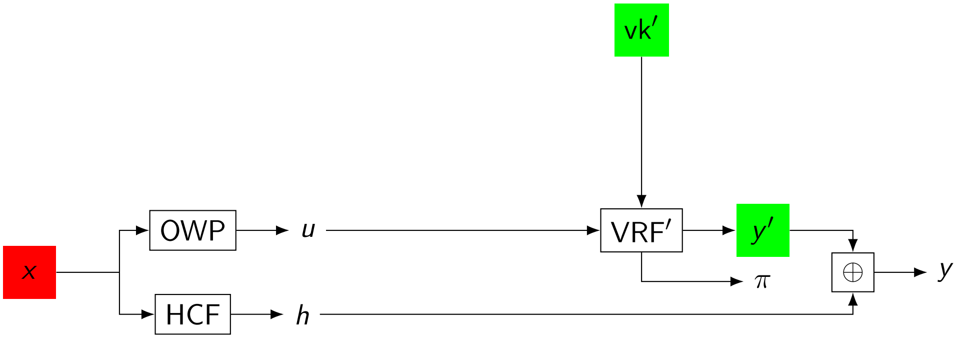
Pseudorandomness ☐ | Unbiasability ☑



Construction

Pseudorandomness ☑

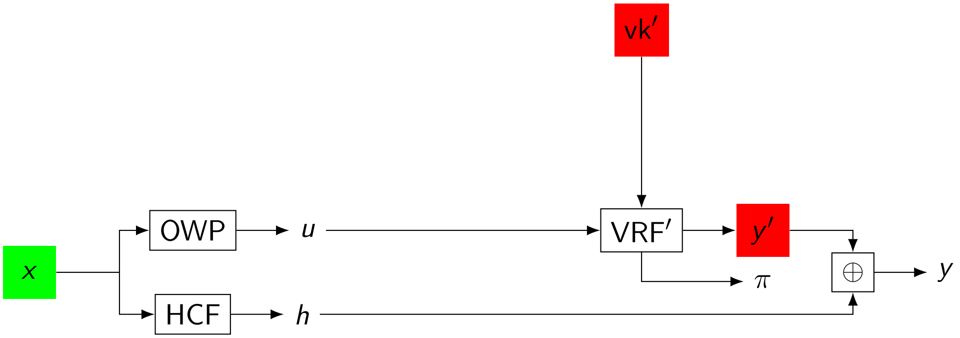
Unbiasability ☑



Construction

Pseudorandomness ☑

Unbiasability ☐



Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$ $\qquad\qquad$ $\mathcal{A}(1^\lambda; r_\mathcal{A})$

$\xleftarrow{\hspace{2em}\mathsf{vk}\hspace{2em}}$

$x \leftarrow \{0,1\}^\lambda$

find $y_0, \pi : \mathsf{VRF.Verify}(\mathsf{vk}, x, y_0, \pi) = 1$

$y_1 \leftarrow \{0,1\}$

$b \leftarrow \{0,1\}$

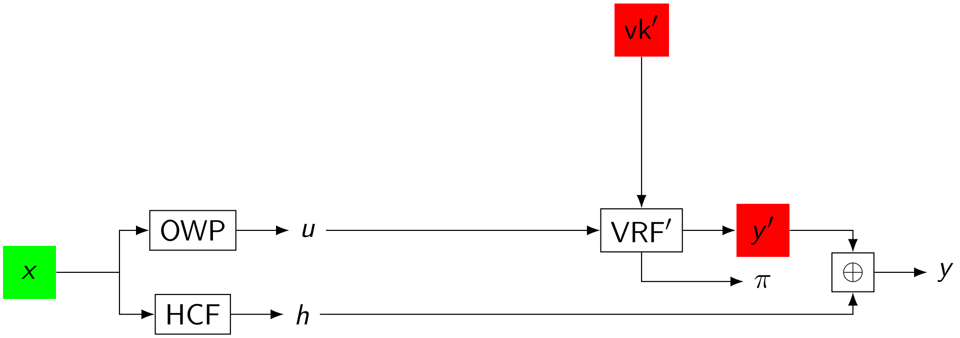
$\xrightarrow{\hspace{2em}y_b\hspace{2em}}$

$\xleftarrow{\hspace{2em}b'\hspace{2em}}$

return $b' \stackrel{?}{=} b$

Construction

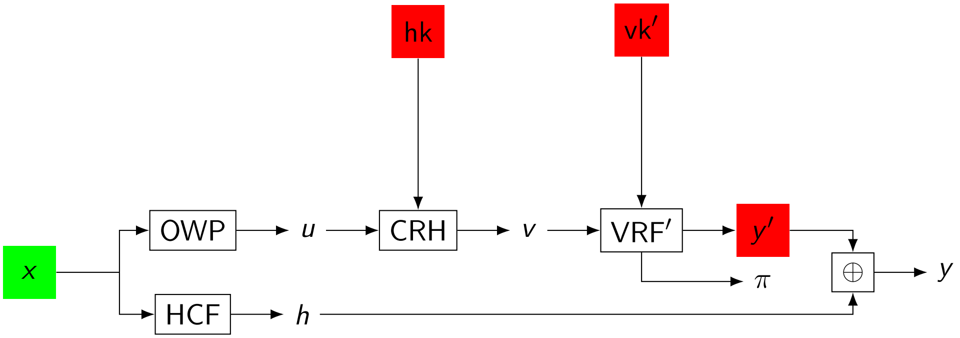
Pseudorandomness ☑ | Unbiasability ☐



Construction

Pseudorandomness ☑

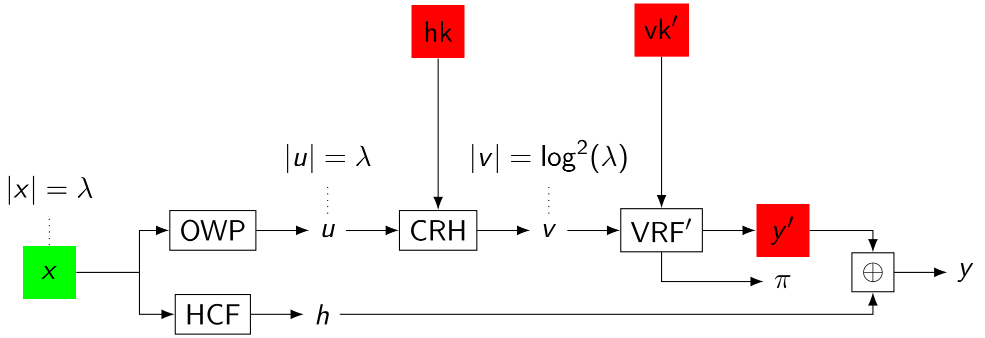
Unbiasability ☑



Construction

Pseudorandomness ☑

Unbiasability ☑



Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$ $\qquad\qquad$ $\mathcal{A}(1^\lambda; r_\mathcal{A})$

$\xleftarrow{\mathsf{vk}}$

$x \leftarrow \{0,1\}^\lambda$

find $y_0, \pi : \mathsf{VRF.Verify}(\mathsf{vk}, x, y_0, \pi) = 1$

$y_1 \leftarrow \{0,1\}$

$b \leftarrow \{0,1\}$

$\xrightarrow{y_b}$

$\xleftarrow{b'}$

return $b' \stackrel{?}{=} b$

Simplified Unbiasability Reduction

$\mathcal{C}(1^\lambda)$		$\mathcal{R}(1^\lambda)$		$\mathcal{A}(1^\lambda; r_{\mathcal{A}})$
$x \leftarrow \{0,1\}^\lambda$				
$u := \mathsf{OWP}(x)$				
$h := \mathsf{HCF}(u)$				
	$\xrightarrow{\quad u \quad}$		$\xleftarrow{\quad \mathsf{vk} = (\mathsf{hk}, \mathsf{vk}') \quad}$	
		$v := \mathsf{CRH}(\mathsf{hk}, u) \in \{0,1\}^{\log^2(\lambda)}$		
		find $y_0', \pi' : \mathsf{VRF}'.\mathsf{Verify}(\mathsf{vk}', v, y_0', \pi') = 1$		
			$\xrightarrow{\quad y := y_0' \overset{!}{=} y' \oplus h \quad}$	
			$\xleftarrow{\quad b' \quad}$	
		if $b' = 0$ **then** $h' := 0$		
		else $h' := 1$		
	$\xleftarrow{\quad h' \quad}$			
return $h' \overset{?}{=} h$				

Simplified Unbiasability Reduction

$\mathcal{C}(1^\lambda)$ | $\mathcal{R}_{\mathsf{ek}'}(1^\lambda)$ | $\mathcal{A}(1^\lambda; r_\mathcal{A})$

$x \leftarrow \{0,1\}^\lambda$

$u := \mathsf{OWP}(x)$

$h := \mathsf{HCF}(u)$

$\xrightarrow{\quad u \quad}$ $\qquad$ $\xleftarrow{\quad \mathsf{vk} = (\mathsf{hk}, \mathsf{vk}') \quad}$

$v := \mathsf{CRH}(\mathsf{hk}, u) \in \{0,1\}^{\log^2(\lambda)}$

$y'_0 := \mathsf{VRF}'.\mathsf{LatEval}(\mathsf{ek}', v)$

$\xrightarrow{\quad y := y'_0 \stackrel{!}{=} y' \oplus h \quad}$

$\xleftarrow{\quad b' \quad}$

if $b' = 0$ **then** $h' := 0$

else $h' := 1$

$\xleftarrow{\quad h' \quad}$

return $h' \stackrel{?}{=} h$

BNN-Reduction with Polynomial Loss [Bra24]

BNN-Reduction with Polynomial Loss [Bra24]

Latent VRF

A VRF VRF' is (perfectly) *latent* if there exists a deterministic polynomial-time algorithm $\mathsf{LatEval}'$ such that

$$\forall \mathsf{vk}' \; \exists \mathsf{ek}' \; \forall x \left(\begin{array}{lcl} y' := \mathsf{LatEval}'(\mathsf{ek}', x) \neq \bot & \Longrightarrow & y' \text{ is the valid image} \\ y' := \mathsf{LatEval}'(\mathsf{ek}', x) = \bot & \Longrightarrow & \text{no valid image exists} \end{array} \right).$$

Simplified Unbiasability Reduction

$\mathcal{C}(1^\lambda)$ | $\mathcal{R}(1^\lambda)$ | $\mathcal{A}(1^\lambda; r_{\mathcal{A}})$

$x \leftarrow \{0,1\}^\lambda$

$u := \mathsf{OWP}(x)$

$h := \mathsf{HCF}(u)$

$\xrightarrow{\quad u \quad}$ $\xleftarrow{\quad \mathsf{vk} = (\mathsf{hk}, \mathsf{vk}') \quad}$

$v := \mathsf{CRH}(\mathsf{hk}, u) \in \{0,1\}^{\log^2(\lambda)}$

find y_0', π' : $\mathsf{VRF}'.\mathsf{Verify}(\mathsf{vk}', v, y_0', \pi') = 1$

$\xrightarrow{\quad y := y_0' \stackrel{!}{=} y' \oplus h \quad}$

$\xleftarrow{\quad b' \quad}$

if $b' = 0$ **then** $h' := 0$

else $h' := 1$

$\xleftarrow{\quad h' \quad}$

return $h' \stackrel{?}{=} h$

BNN-Reduction with Polynomial Loss [Bra24]

Latent VRF

A VRF VRF' is (perfectly) *latent* if there exists a deterministic polynomial-time algorithm $\mathsf{LatEval}'$ such that

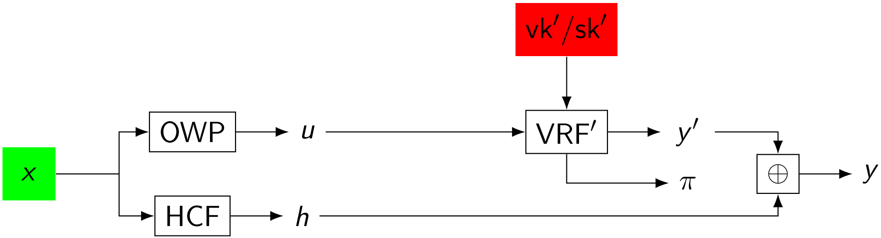
$$\forall \mathsf{vk}' \; \exists \mathsf{ek}' \; \forall x \begin{pmatrix} y' := \mathsf{LatEval}'(\mathsf{ek}', x) \neq \bot & \implies & y' \text{ is the valid image} \\ y' := \mathsf{LatEval}'(\mathsf{ek}', x) = \bot & \implies & \text{no valid image exists} \end{pmatrix}.$$

BNN-Reduction with Polynomial Loss [Bra24]

Latent VRF

A VRF VRF' is (perfectly) *latent* if there exists a deterministic polynomial-time algorithm $\mathsf{LatEval}'$ such that

$$\forall \mathsf{vk}'\ \exists \mathsf{ek}'\ \forall x \left(\begin{array}{lcl} y' := \mathsf{LatEval}'(\mathsf{ek}', x) \neq \bot & \Longrightarrow & y' \text{ is the valid image} \\ y' := \mathsf{LatEval}'(\mathsf{ek}', x) = \bot & \Longrightarrow & \text{no valid image exists} \end{array} \right).$$



Contributions

Meta-reductions for VRFs [BHK$^+$22]

- Rules out algebraic NBN-reductions from various non-interactive assumptions to pairing-based VRFs with short proofs.
- For a set of natural VRFs constructions:
  the shorter the VRF proof, the stronger the assumption needed.

(Non-)black-box reductions for unbiasable VRFs [Bra25]

- BBB-reduction: injective OWF, CRH, VRF $\implies$ unbiasable VRF (subexp. loss)
- BNN-reduction: injective OWF, VRF $\implies$ unbiasable VRF (poly. loss)

Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

- First unconditional lower bound MKtP $\notin$ DTIME$[\mathcal{O}(n)]$.
- Conditional lower bounds MKtP $\notin$ DTIME$[\mathfrak{t}(n)] \cap \mathrm{Heur}_{0,\mathrm{o}(1/\mathfrak{t}(n))}$DTIME$[\mathcal{O}(n)]$.

Conclusion

Conclusion

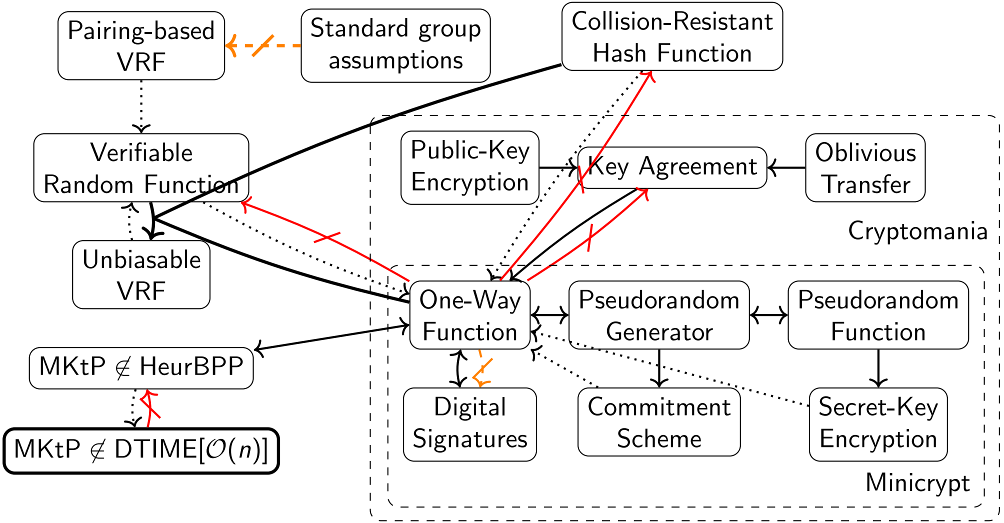
- BBB-constructions are conceptually simple but often lack feasibility or efficiency.
- Separations can formally explain insufficiencies of BBB-constructions.
- Obfuscation-/NIZK/NIWI-based constructions are often NAP.
- CNP-constructions are under-explored (non-black-box use of the adversary).

Construction cookbook

1. Try a BBB-construction.
2. Try a meta-reduction or oracle separation.
3. Try a CNP- or NAP-construction.

Thank you!

Some Cryptographic Primitives



References I

P. Baecher, C. Brzuska, and M. Fischlin. Notions of Black-Box Reductions, Revisited. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 296–315. Springer, Berlin, Heidelberg, December 2013.

N. Brandt, M. Filić, and S. A. Markelon. A Formal Treatment of Key Transparency Systems with Scalability Improvements. Cryptology ePrint Archive, Report 2024/1938, 2024.

N. Brandt, D. Hofheinz, J. Kastner, and A. Ünal. The Price of Verifiability: Lower Bounds for Verifiable Random Functions. In E. Kiltz and V. Vaikuntanathan, editors, *TCC 2022, Part II*, volume 13748 of *LNCS*, pages 747–776. Springer, Cham, November 2022.

N. Brandt, D. Hofheinz, M. Klooß, and M. Reichle. Tightly-Secure Blind Signatures in Pairing-Free Groups. Cryptology ePrint Archive, Report 2024/2075, 2024.

References II

N. Brandt, S. Maier, T. Müller, and J. Müller-Quade. On the Correlation Complexity of MPC with Cheater Identification. In F. Baldimtsi and C. Cachin, editors, *FC 2023, Part I*, volume 13950 of *LNCS*, pages 129–146. Springer, Cham, May 2023.

N. Brandt, M. C. Noval, C. U. Günther, A. Ünal, and S. Wohnig. Constrained Verifiable Random Functions Without Obfuscation and Friends. Cryptology ePrint Archive, Report 2025/1045, 2025.

N. Brandt. Lower Bounds for Levin-Kolmogorov Complexity. In E. Boyle and M. Mahmoody, editors, *TCC 2024, Part I*, volume 15364 of *LNCS*, pages 191–221. Springer, Cham, December 2024.

N. Brandt. Unbiasable Verifiable Random Functions from Generic Assumptions. Cryptology ePrint Archive, Report 2025/766, 2025.

D. Boneh and R. Venkatesan. Breaking RSA May Not Be Equivalent to Factoring. In K. Nyberg, editor, *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 59–71. Springer, Berlin, Heidelberg, 1998.

References III

J.-S. Coron. Optimal Security Proofs for PSS and Other Signature Schemes. In L. R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 272–287. Springer, Berlin, Heidelberg, 2002.

E. Giunta and A. Stewart. Unbiasable Verifiable Random Functions. In M. Joye and G. Leander, editors, *EUROCRYPT 2024, Part IV*, volume 14654 of *LNCS*, pages 142–167. Springer, Cham, May 2024.

S. Hirahara. Unexpected hardness results for Kolmogorov complexity under uniform reductions. In K. Makarychev, Y. Makarychev, M. Tulsiani, G. Kamath, and J. Chuzhoy, editors, *52nd ACM STOC*, pages 1038–1051. ACM Press, June 2020.

C.-Y. Hsiao and L. Reyzin. Finding Collisions on a Public Road, or Do Secure Hash Functions Need Secret Coins? In M. Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 92–105. Springer, Berlin, Heidelberg, August 2004.

References IV

- R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147, 1995.
- R. Impagliazzo and S. Rudich. Limits on the Provable Consequences of One-Way Permutations. In *21st ACM STOC*, pages 44–61. ACM Press, May 1989.
- R. Impagliazzo and S. Rudich. Limits on the Provable Consequences of One-way Permutations. In S. Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 8–26. Springer, New York, August 1990.
- L. A. Levin. Randomness conservation inequalities; information and independence in mathematical theories. *Information and Control*, 61(1):15–37, 1984.
- Y. Liu and R. Pass. On the Possibility of Basing Cryptography on EXP $\neq$ BPP. In T. Malkin and C. Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 11–40, Virtual Event. Springer, Cham, August 2021.

References V

S. Micali, M. O. Rabin, and S. P. Vadhan. Verifiable Random Functions. In *40th FOCS*, pages 120–130. IEEE Computer Society Press, October 1999.

R. Pass. Limits of provable security from standard assumptions. In L. Fortnow and S. P. Vadhan, editors, *43rd ACM STOC*, pages 109–118. ACM Press, June 2011.

H. Ren and R. Santhanam. A Relativization Perspective on Meta-Complexity. In P. Berenbrink and B. Monmege, editors, *39th International Symposium on Theoretical Aspects of Computer Science (STACS 2022)*, volume 219 of *Leibniz International Proceedings in Informatics (LIPIcs)*, 54:1–54:13, Dagstuhl, Germany. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, November 1994.

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

- Levin's notion [Lev84] of Kolmogorov complexity:
$$\mathrm{Kt}(x) := \min\{|\Pi| + \lceil \log(t) \rceil \mid \Pi(\varepsilon) = x \text{ in } t \text{ steps}\}$$
- Set of low-complexity strings: $\mathsf{MKtP} := \{x \mid \mathrm{Kt}(x) \leq |x|\} \in \mathsf{E} := \mathsf{DTIME}[2^{\mathcal{O}(n)}]$
- Liu and Pass [LP21]:
$$\exists\mathsf{OWF} \iff \mathsf{MKtP} \notin \mathsf{HeurBPP}$$
$$\mathsf{BPP} \neq \mathsf{EXP} \iff \mathsf{MKtP} \notin \mathsf{AvgBPP}$$

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

- Levin's notion [Lev84] of Kolmogorov complexity:

$$\mathsf{Kt}(x) := \min\{|\Pi| + \lceil \log(t) \rceil \mid \Pi(\varepsilon) = x \text{ in } t \text{ steps}\}$$

- Set of low-complexity strings: $\mathsf{MKtP} := \{x \mid \mathsf{Kt}(x) \leq |x|\} \in \mathsf{E} := \mathsf{DTIME}[2^{\mathcal{O}(n)}]$
- Liu and Pass [LP21]:

$$\exists \mathsf{OWF} \iff \mathsf{MKtP} \notin \mathsf{HeurBPP}$$
$$\mathsf{BPP} \neq \mathsf{EXP} \iff \mathsf{MKtP} \notin \mathsf{AvgBPP}$$

Our results [Bra24]

- First unconditional lower bound $\mathsf{MKtP} \notin \mathsf{DTIME}[\mathcal{O}(n)]$.

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

- Levin's notion [Lev84] of Kolmogorov complexity:

$$\mathsf{Kt}(x) := \min\{|\Pi| + \lceil \log(t) \rceil \mid \Pi(\varepsilon) = x \text{ in } t \text{ steps}\}$$

- Set of low-complexity strings: $\mathsf{MKtP} := \{x \mid \mathsf{Kt}(x) \le |x|\} \in \mathsf{E} := \mathsf{DTIME}[2^{\mathcal{O}(n)}]$
- Liu and Pass [LP21]:

$$\exists\mathsf{OWF} \iff \mathsf{MKtP} \notin \mathsf{HeurBPP}$$
$$\mathsf{BPP} \neq \mathsf{EXP} \iff \mathsf{MKtP} \notin \mathsf{AvgBPP}$$

Our results [Bra24]

- First unconditional lower bound $\mathsf{MKtP} \notin \mathsf{DTIME}[\mathcal{O}(n)]$.
- Tolerating false-positive error: $\mathsf{MKtP} \notin \mathsf{Heur}_{1/n^2,0}\mathsf{DTIME}[\mathcal{O}(n)]$.

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

- Levin's notion [Lev84] of Kolmogorov complexity:

$$\mathsf{Kt}(x) := \min\{|\Pi| + \lceil \log(t) \rceil \mid \Pi(\varepsilon) = x \text{ in } t \text{ steps}\}$$

- Set of low-complexity strings: $\mathsf{MKtP} := \{x \mid \mathsf{Kt}(x) \leq |x|\} \in \mathsf{E} := \mathsf{DTIME}[2^{\mathcal{O}(n)}]$
- Liu and Pass [LP21]:

$$\exists\mathsf{OWF} \iff \mathsf{MKtP} \notin \mathsf{HeurBPP}$$
$$\mathsf{BPP} \neq \mathsf{EXP} \iff \mathsf{MKtP} \notin \mathsf{AvgBPP}$$

Our results [Bra24]

- First unconditional lower bound $\mathsf{MKtP} \notin \mathsf{DTIME}[\mathcal{O}(n)]$.
- Tolerating false-positive error: $\mathsf{MKtP} \notin \mathsf{Heur}_{1/n^2,0}\mathsf{DTIME}[\mathcal{O}(n)]$.
- In some computational models: $\mathsf{MKtP} \notin \mathsf{DTIME}[\mathcal{O}(n^2)]$.

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

- Levin's notion [Lev84] of Kolmogorov complexity:

$$\mathrm{Kt}(x) := \min\{|\Pi| + \lceil \log(t) \rceil \mid \Pi(\varepsilon) = x \text{ in } t \text{ steps}\}$$

- Set of low-complexity strings: $\mathrm{MKtP} := \{x \mid \mathrm{Kt}(x) \leq |x|\} \in \mathrm{E} := \mathrm{DTIME}[2^{\mathcal{O}(n)}]$
- Liu and Pass [LP21]:

$$\exists \mathrm{OWF} \iff \mathrm{MKtP} \notin \mathrm{HeurBPP}$$
$$\mathrm{BPP} \neq \mathrm{EXP} \iff \mathrm{MKtP} \notin \mathrm{AvgBPP}$$

Our results [Bra24]

- First unconditional lower bound $\mathrm{MKtP} \notin \mathrm{DTIME}[\mathcal{O}(n)]$.
- Tolerating false-positive error: $\mathrm{MKtP} \notin \mathrm{Heur}_{1/n^2,0}\mathrm{DTIME}[\mathcal{O}(n)]$.
- In some computational models: $\mathrm{MKtP} \notin \mathrm{DTIME}[\mathcal{O}(n^2)]$.
- Conditional lower bounds $\mathrm{MKtP} \notin \mathrm{DTIME}[\mathfrak{t}(n)] \cup \mathrm{Heur}_{0,\mathrm{o}(1/\mathfrak{t}(n))}\mathrm{DTIME}[\mathcal{O}(n)]$.

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Hardness of MKtP

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Hardness of MKtP

HeurBPP ($\Leftrightarrow \nexists$OWF) [LP21]

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Hardness of MKtP

HeurBPP ($\Leftrightarrow \nexists$OWF) [LP21]

AvgBPP ($\Leftrightarrow$ BPP $=$ EXP) [LP21]

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Hardness of MKtP

HeurBPP ($\Leftrightarrow \nexists$OWF) [LP21]

AvgBPP ($\Leftrightarrow$ BPP $=$ EXP) [LP21]

Algebrization barrier

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Hardness of MKtP

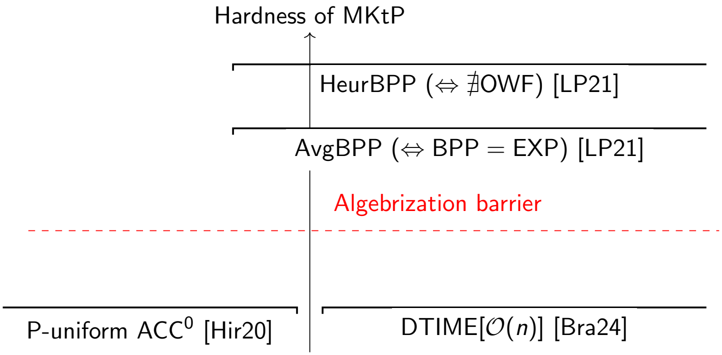
HeurBPP ($\Leftrightarrow \nexists$OWF) [LP21]

AvgBPP ($\Leftrightarrow$ BPP $=$ EXP) [LP21]

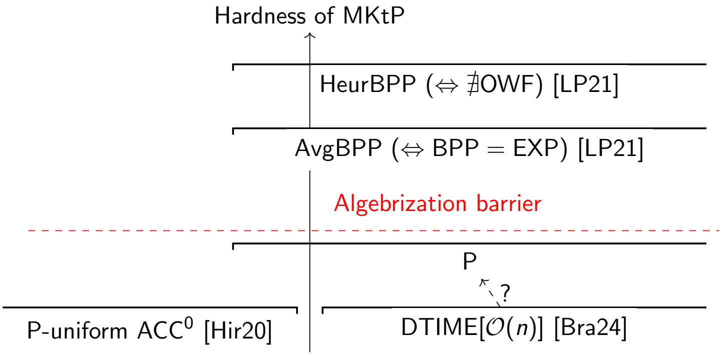
Algebrization barrier

P-uniform ACC^0 [Hir20]

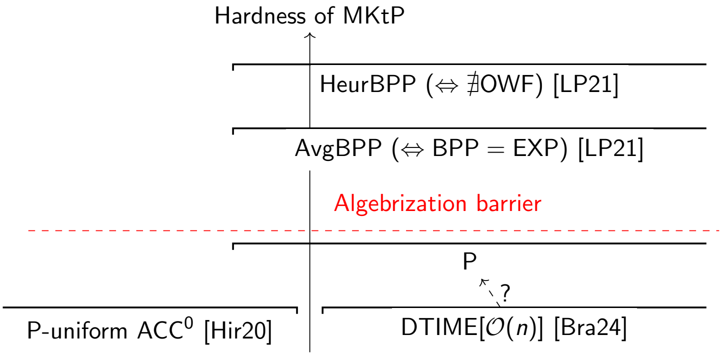
Lower bounds for Levin–Kolmogorov complexity [Bra24]



Lower bounds for Levin–Kolmogorov complexity [Bra24]



Lower bounds for Levin–Kolmogorov complexity [Bra24]



[RS22] oracle: approx. Kt within factor $(1+\epsilon)$ in linear time and BPP $=$ EXP