

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

Verifiable
Random Function

Public-Key
Encryption

Collision-Resistant
Hash Function

Key Agreement

Oblivious
Transfer

One-Way
Function

Pseudorandom
Generator

Pseudorandom
Function

Digital
Signatures

Commitment
Scheme

Secret-Key
Encryption

Reductionism

Security based on computational hardness

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

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.

Reductionism

Security based on computational hardness

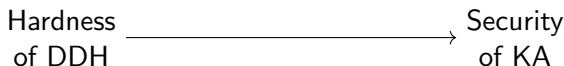
- ▶ $P = NP \implies$ most cryptographic primitives can be broken efficiently.
- ▶ Unconditional security proof $\implies P \neq NP$.
- ▶ Security is based on computational hardness of problems, e.g. number-theory, lattice problems, cyclic groups, etc.
- ▶ Reduction: $\exists \text{PPT } \mathcal{A}_{\text{primitive}}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

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: $\exists \text{PPT } \mathcal{A}_{\text{primitive}} \implies \exists \text{PPT } \mathcal{A}_{\text{problem}}$

Which assumption is best?



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: $\exists \text{PPT } \mathcal{A}_{\text{primitive}} \implies \exists \text{PPT } \mathcal{A}_{\text{problem}}$

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: $\exists \text{PPT } \mathcal{A}_{\text{primitive}} \implies \exists \text{PPT } \mathcal{A}_{\text{problem}}$

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?

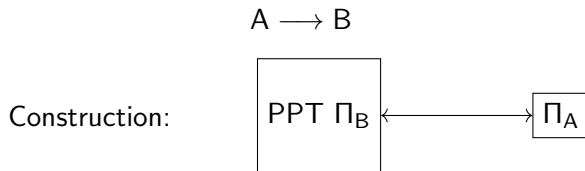
Reductionism

Cryptographic construction/reduction:

$$A \longrightarrow B$$

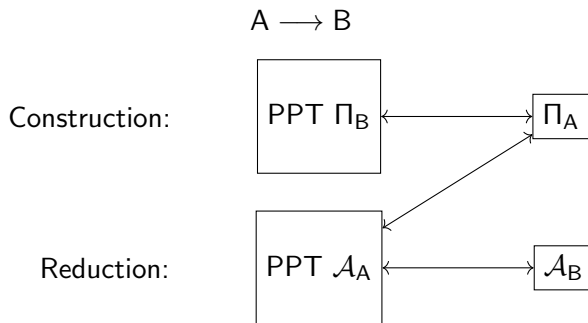
Reductionism

Cryptographic construction/reduction:



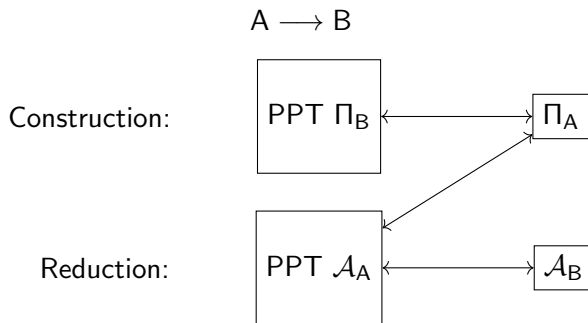
Reductionism

Cryptographic construction/reduction:



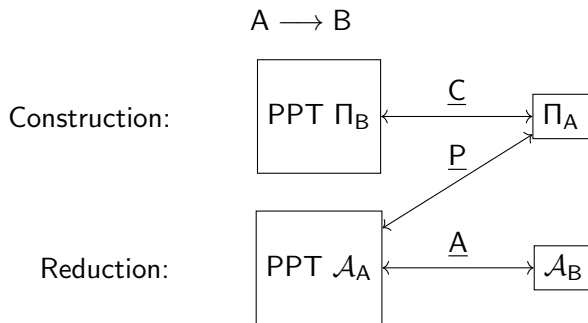
Reductionism

Cryptographic construction/reduction:



Reductionism

Cryptographic construction/reduction:



CAP taxonomy [BBF13]:

<u>C</u> onstruction	<u>A</u> dversary	<u>P</u> rimitive
$\in \{B, N\}$	$\in \{B, N\}$	$\in \{B, N\}$

Some Cryptographic Primitives

Verifiable
Random Function

Public-Key
Encryption

Collision-Resistant
Hash Function

Key Agreement

Oblivious
Transfer

One-Way
Function

Pseudorandom
Generator

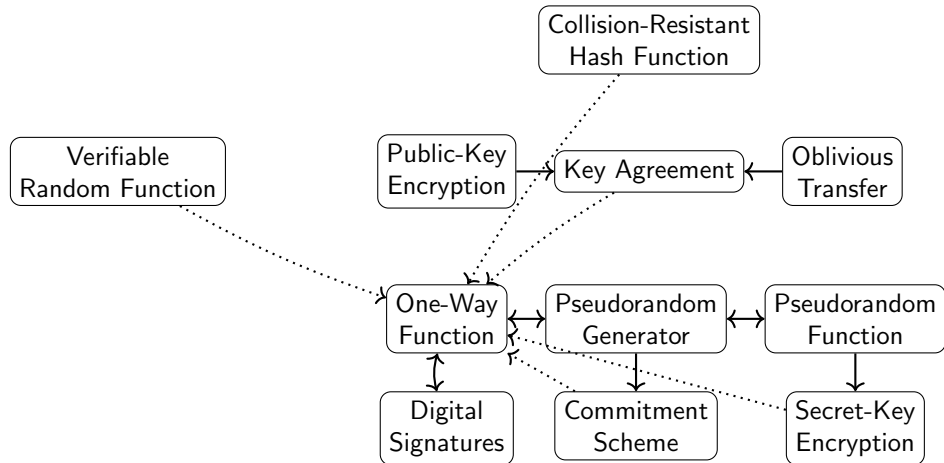
Pseudorandom
Function

Digital
Signatures

Commitment
Scheme

Secret-Key
Encryption

Some Cryptographic Primitives



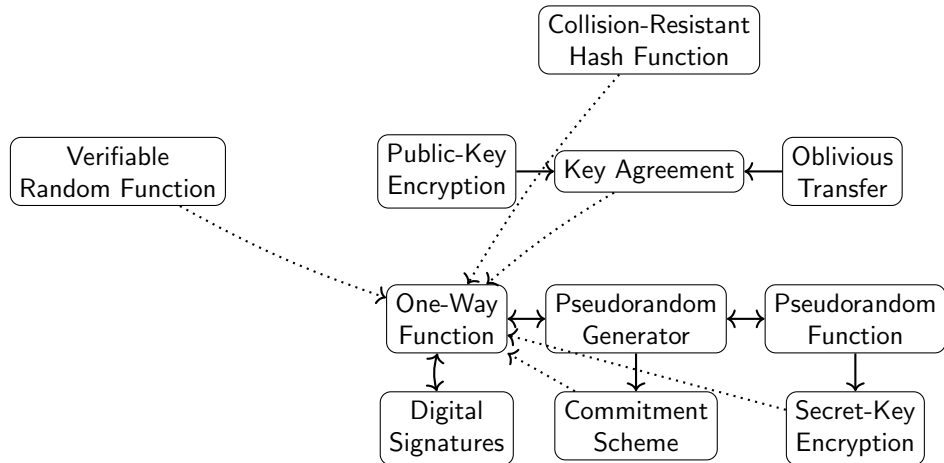
Separations

Separations

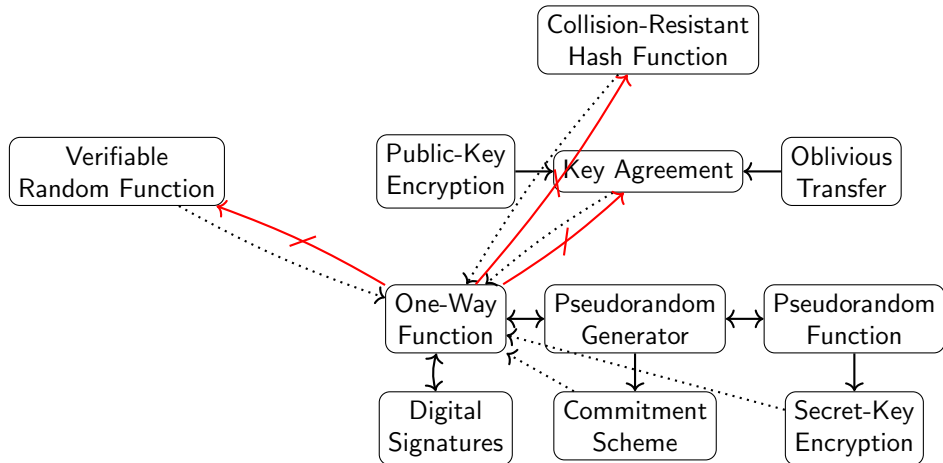
Oracle separations [IR90; IR89; HR04]

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

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: $\text{OWF} \not\leq \text{KA}$.

Separations

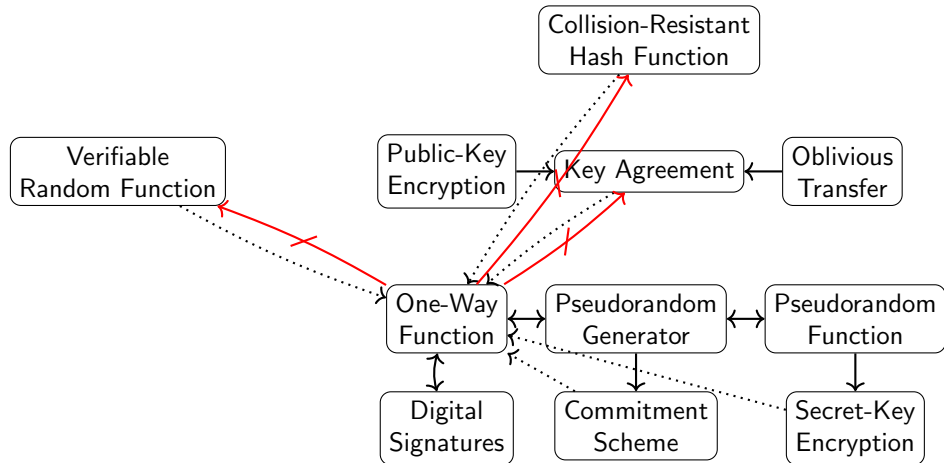
Oracle separations [IR90; IR89; HR04]

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

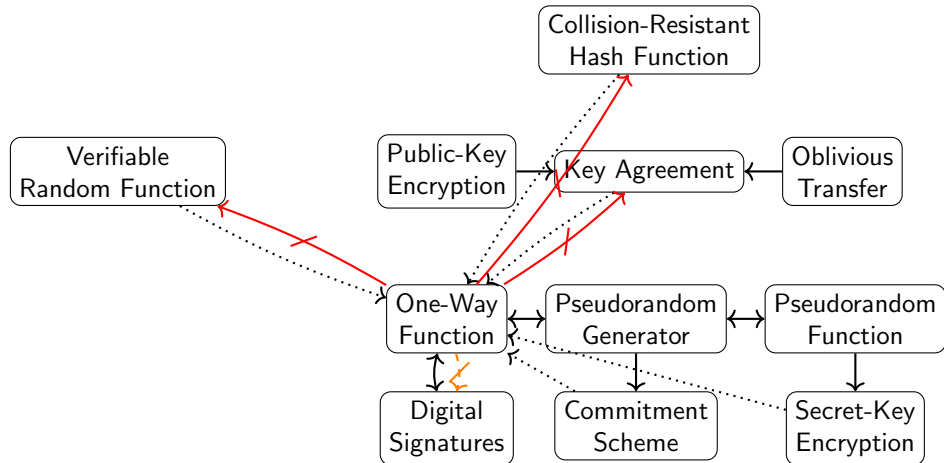
Meta-reductions [BV98; Cor02; Pas11]

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

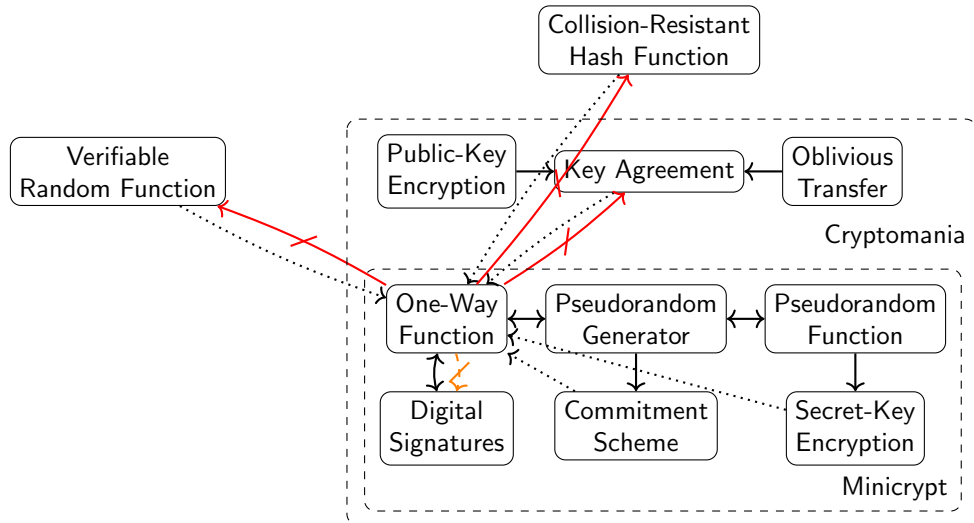
Some Cryptographic Primitives



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 unbiased 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:

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

Definition of VRF

Verifiable Random Function [MRV99]

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

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

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:

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

Properties

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

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

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

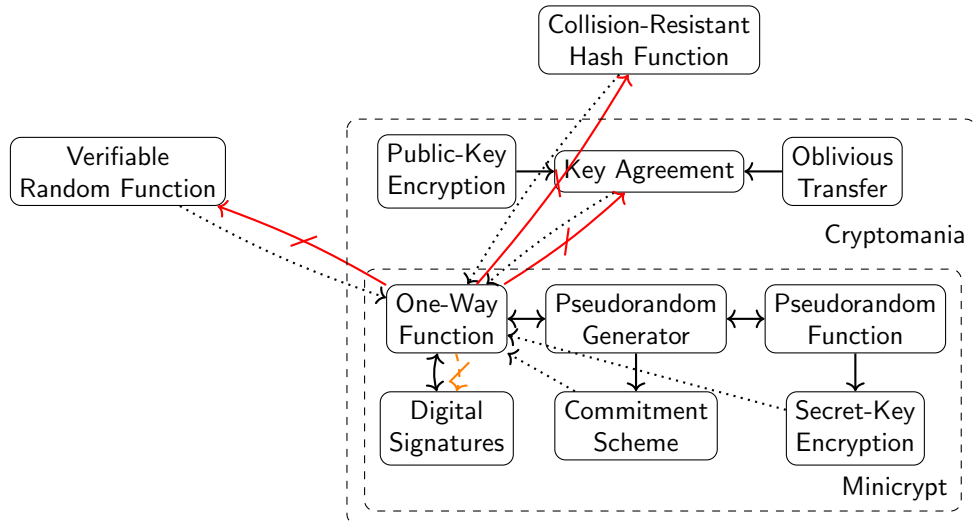
Meta-reductions for VRFs [BHK⁺22]

- ▶ 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.

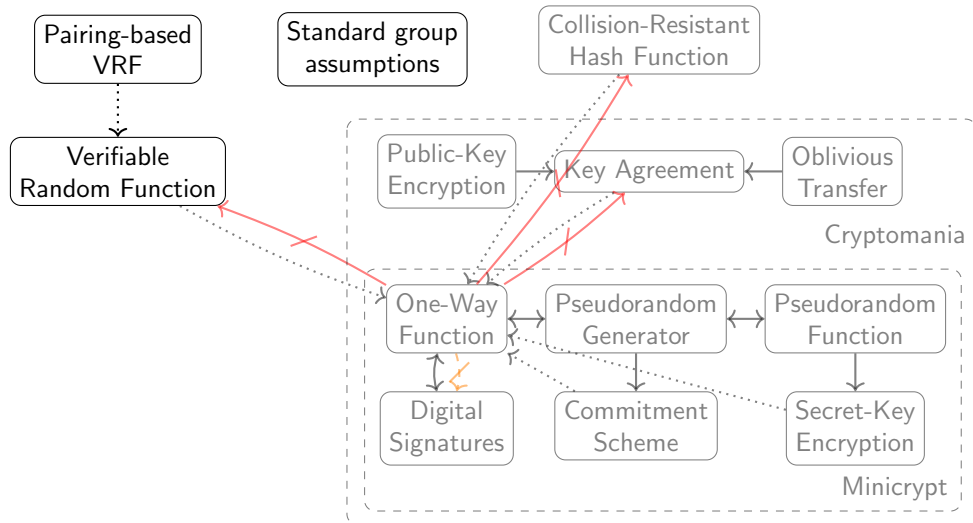
(Non-)black-box reductions for unbiisable VRFs [Bra25]

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

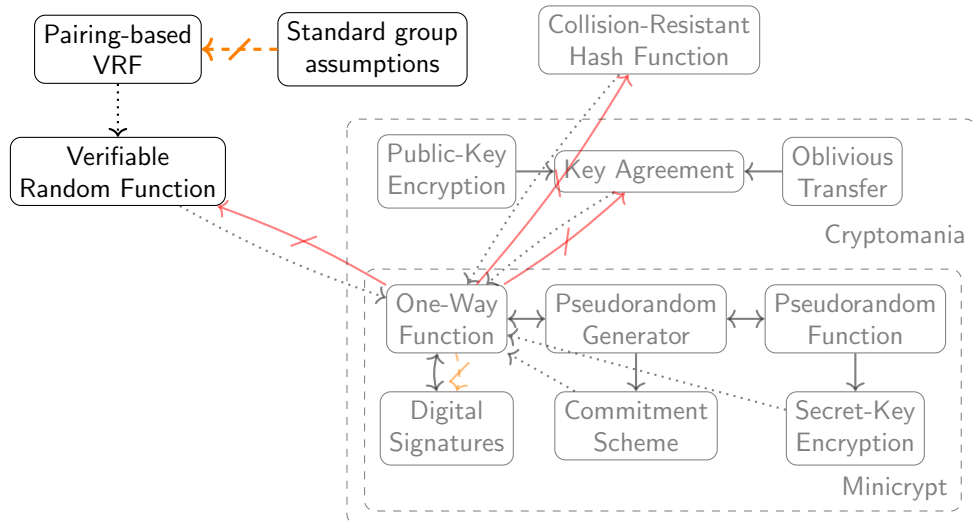
Some Cryptographic Primitives [Imp95]



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 unbiased VRFs [Bra25]

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

Contributions

Meta-reductions for VRFs [BHK⁺22]

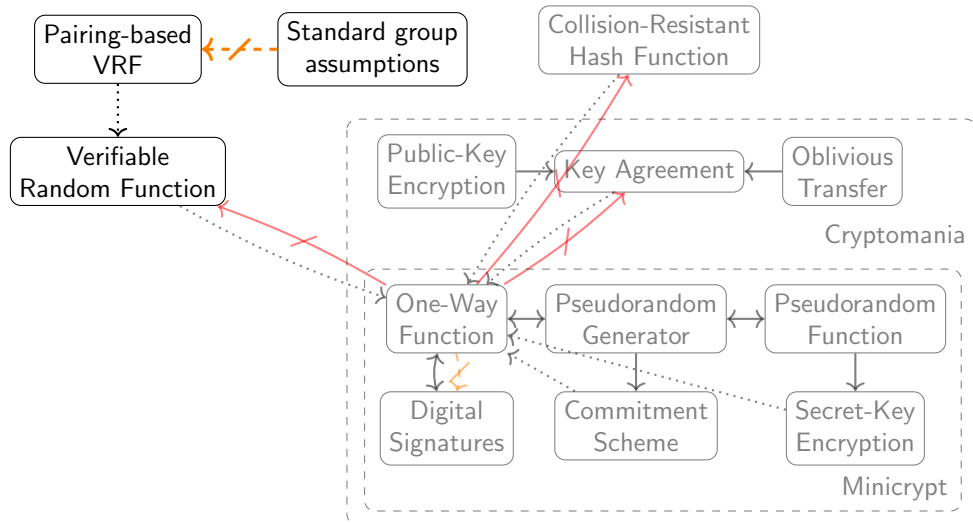
- ▶ Rules out algebraic NBN-reductions from various non-interactive assumptions to pairing-based VRFs with short proofs.
- ▶ For a set of natural VRFs constructions:
the shorter the VRF proof, the stronger the assumption needed.

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

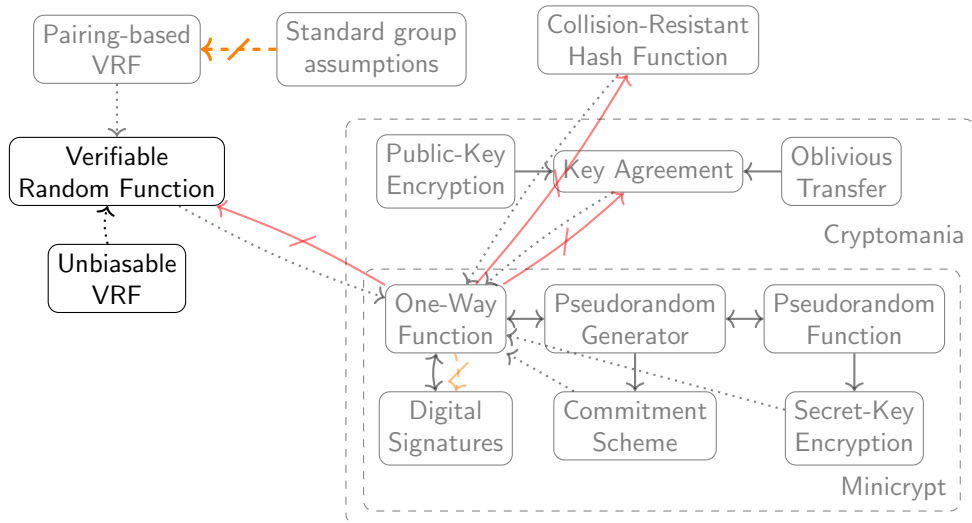
- ▶ BBB-reduction: injective OWF, CRH, VRF \implies unbiisable VRF (subexp. loss)
- ▶ BNN-reduction: injective OWF, VRF \implies unbiisable VRF (poly. loss)

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

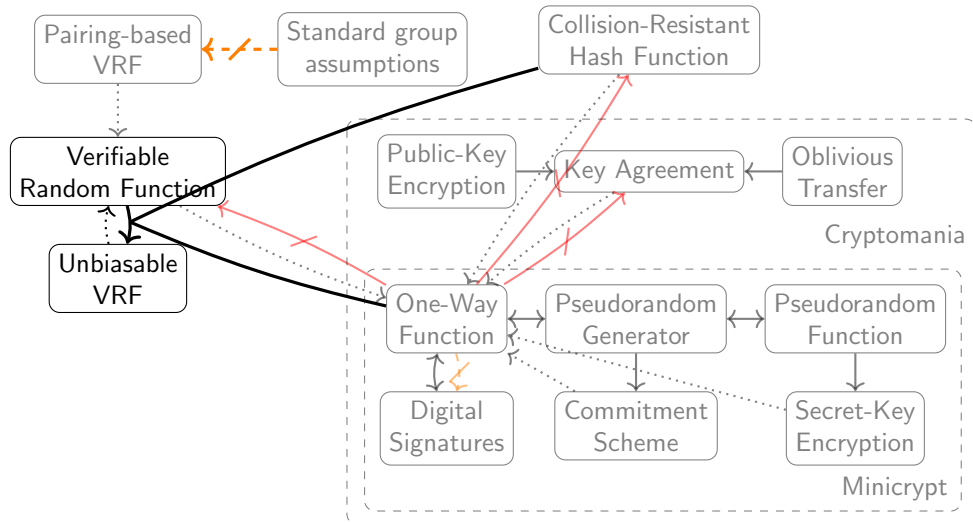
Some Cryptographic Primitives



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 unbiisable VRFs [Bra25]

- ▶ BBB-reduction: injective OWF, CRH, VRF \implies unbiisable VRF (subexp. loss)
- ▶ BNN-reduction: injective OWF, VRF \implies unbiisable 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.

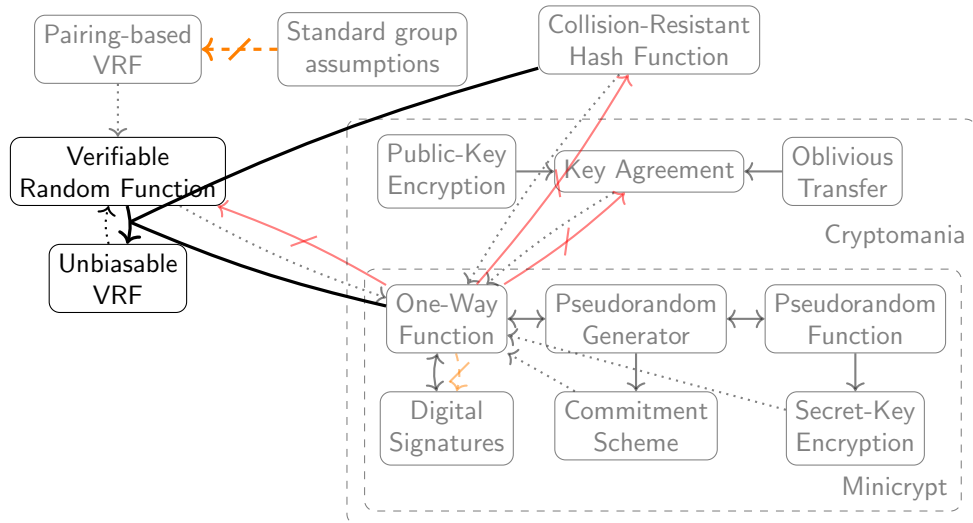
(Non-)black-box reductions for unbiisable VRFs [Bra25]

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

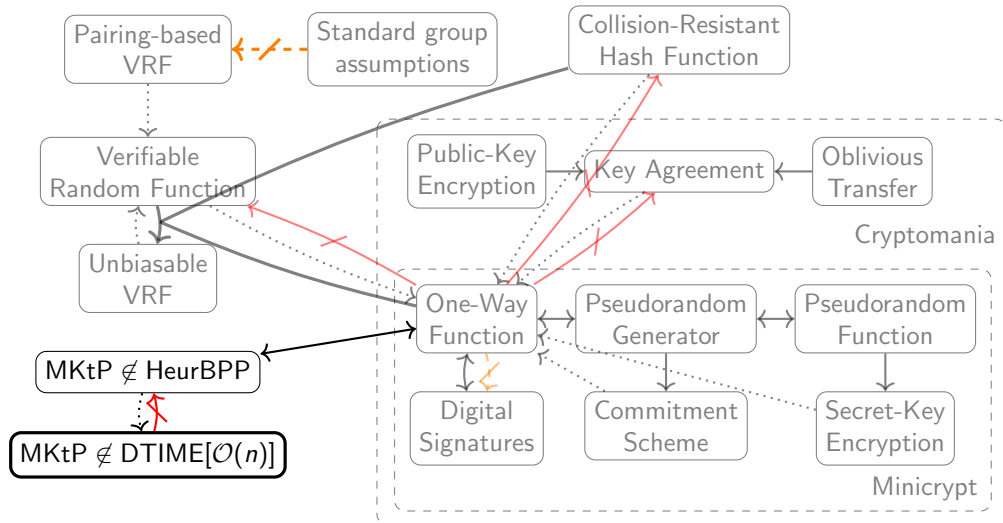
Non-black-box lower bounds for Levin–Kolmogorov complexity [Bra24]

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

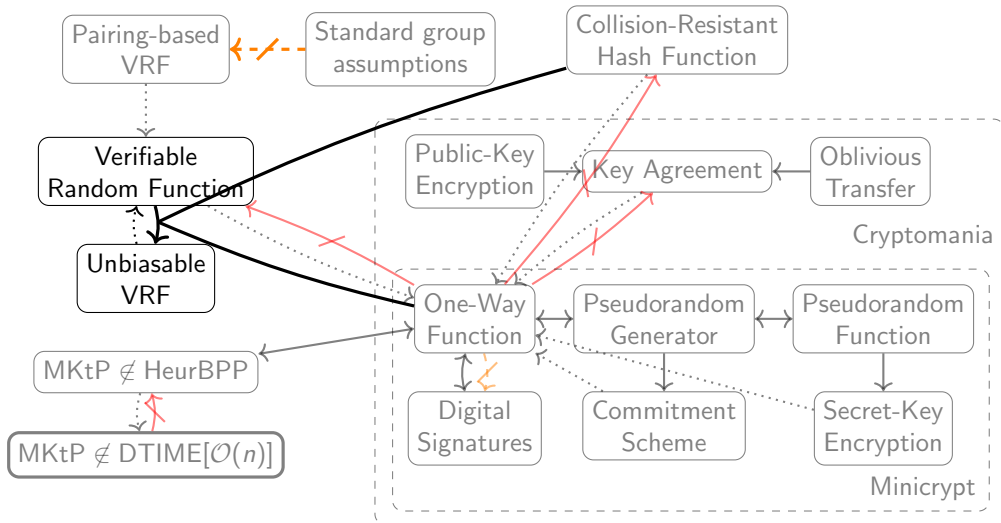
Some Cryptographic Primitives



Some Cryptographic Primitives



Some Cryptographic Primitives



Definition of VRF

Verifiable Random Function [MRV99]

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

- ▶ $\text{Gen}(1^\lambda) \rightarrow (\text{vk}, \text{sk})$
- ▶ $\text{Eval}(\text{sk}, x) \rightarrow (y \in \{0, 1\}^*, \pi)$
- ▶ $\text{Verify}(\text{vk}, x, y, \pi) \rightarrow \{0, 1\}$

Properties

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

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

Definition of VRF

Verifiable Random Function [MRV99]

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

- ▶ $\text{Gen}(1^\lambda) \rightarrow (\text{vk}, \text{sk})$
- ▶ $\text{Eval}(\text{sk}, x) \rightarrow (y \in \{0, 1\}^*, \pi)$
- ▶ $\text{Verify}(\text{vk}, x, y, \pi) \rightarrow \{0, 1\}$

Properties

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

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

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

Simplified Unbiasability Game

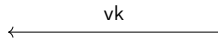
$$\mathcal{C}(1^\lambda)$$

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

Simplified Unbiasability Game

$$\mathcal{C}(1^\lambda)$$

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



Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$

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

$\xleftarrow{\text{vk}}$

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

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

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

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

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$

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

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

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

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

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

\xleftarrow{vk}

$\xrightarrow{y_b}$

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$

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

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

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

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

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

$\leftarrow vk$

$y_b \rightarrow$

$\leftarrow b'$

Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$

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

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

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

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

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

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

$\leftarrow \text{vk}$

$\text{---} y_b \text{---} \rightarrow$

$\leftarrow b' \text{---}$

Construction Overview

Construction [Bra24]

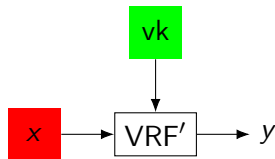
$$\left(\begin{array}{c} \text{VRF} \\ \text{one-way permutation (OWP)} \\ \text{collision-resistant hash function (CRH)} \end{array} \right) \implies \text{unbiasable VRF}$$

Construction Overview

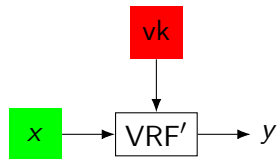
Construction [Bra24]

$$\left(\begin{array}{c} \text{VRF} \\ \text{one-way permutation (OWP)} \\ \text{collision-resistant hash function (CRH)} \end{array} \right) \Rightarrow \text{unbiasable VRF}$$

Pseudorandomness ☒



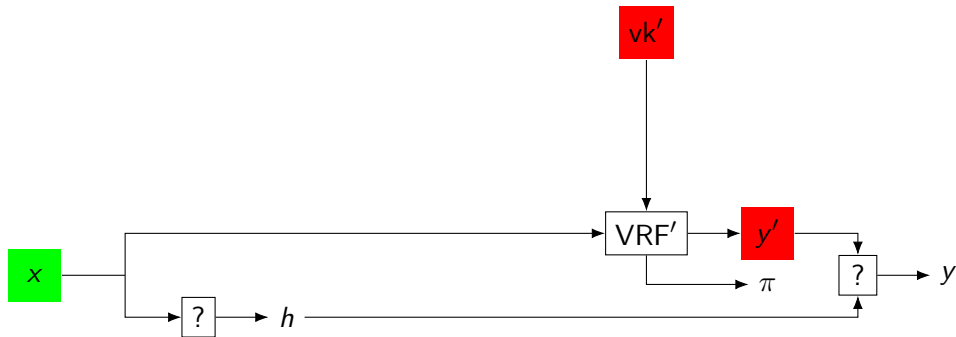
Unbiasability ☐



Construction

Pseudorandomness ☒

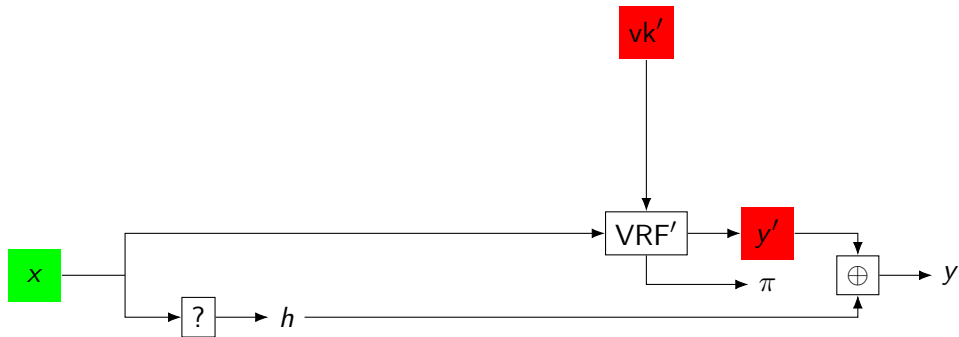
Unbiasability ☐



Construction

Pseudorandomness ☒

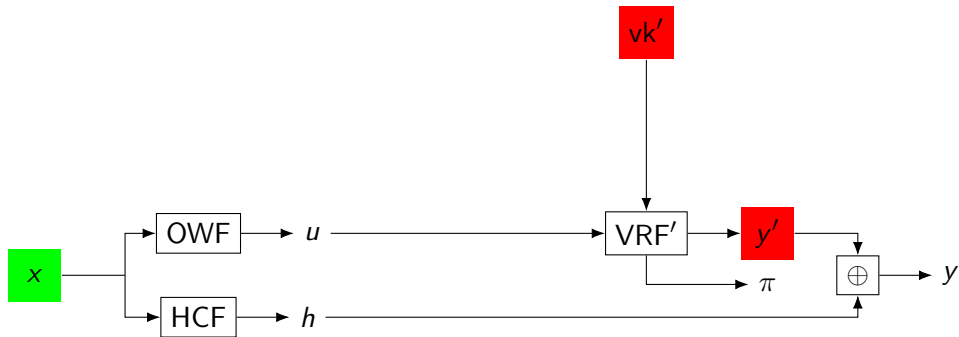
Unbiasability ☐



Construction

Pseudorandomness ☐

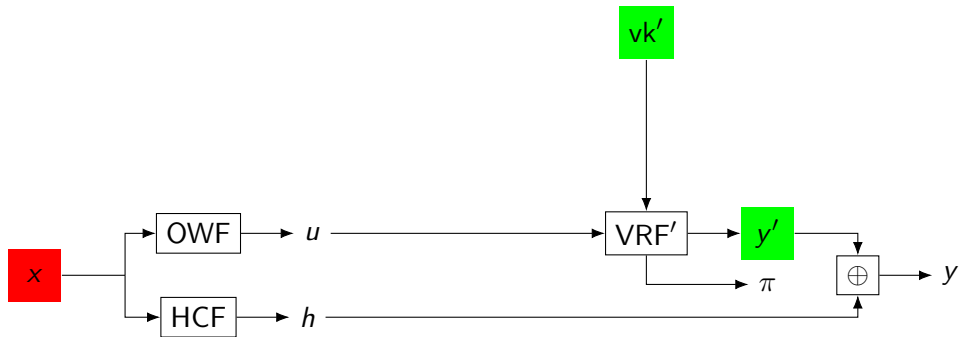
Unbiasability ☒



Construction

Pseudorandomness \square

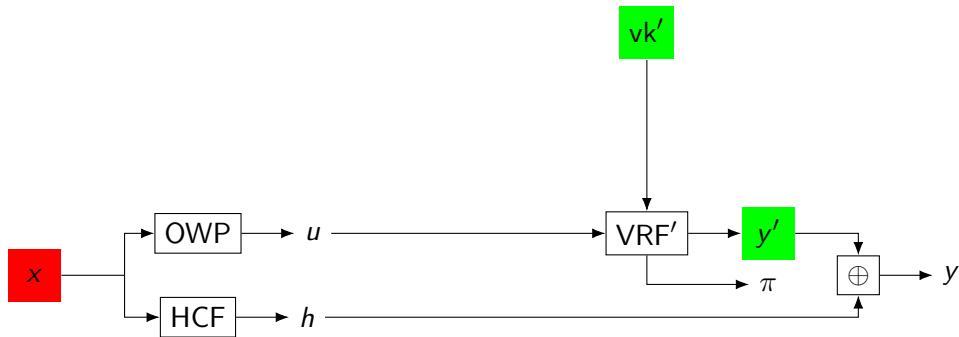
Unbiasability \checkmark



Construction

Pseudorandomness ✓

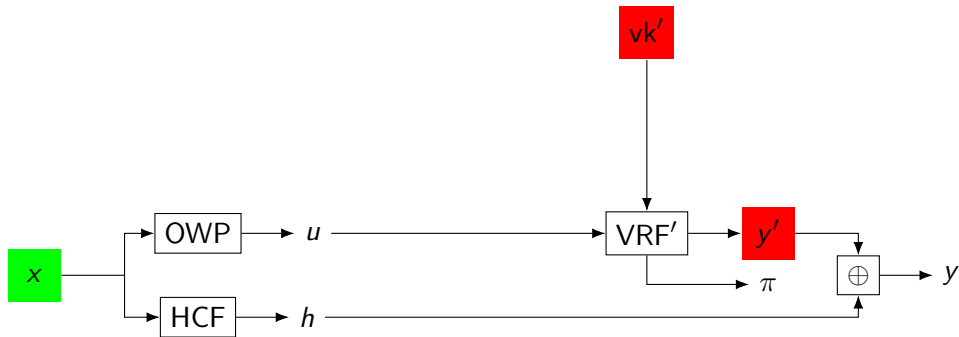
Unbiasability ✓



Construction

Pseudorandomness ☒

Unbiasability ☐



Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$

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

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

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

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

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

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

$\leftarrow \text{vk}$

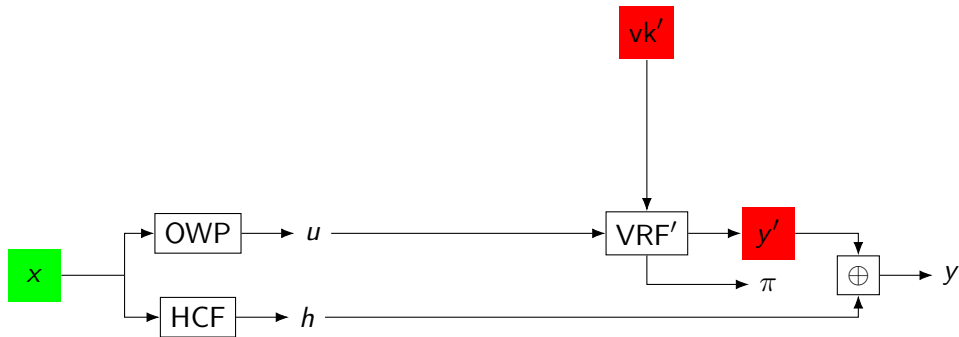
$\text{---} y_b \text{---} \rightarrow$

$\leftarrow b' \text{---}$

Construction

Pseudorandomness ☒

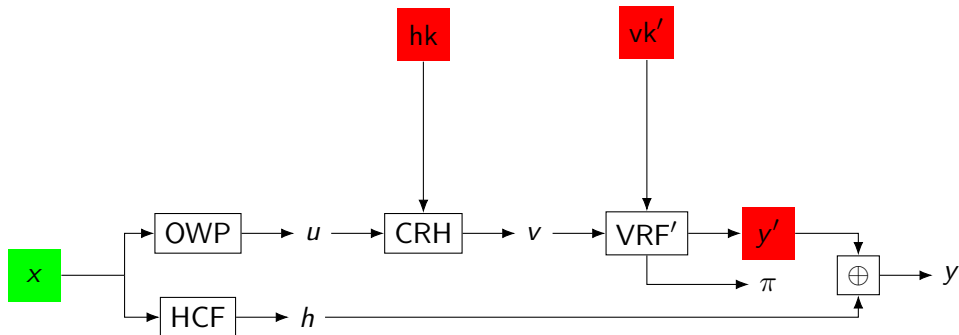
Unbiasability ☐



Construction

Pseudorandomness ✓

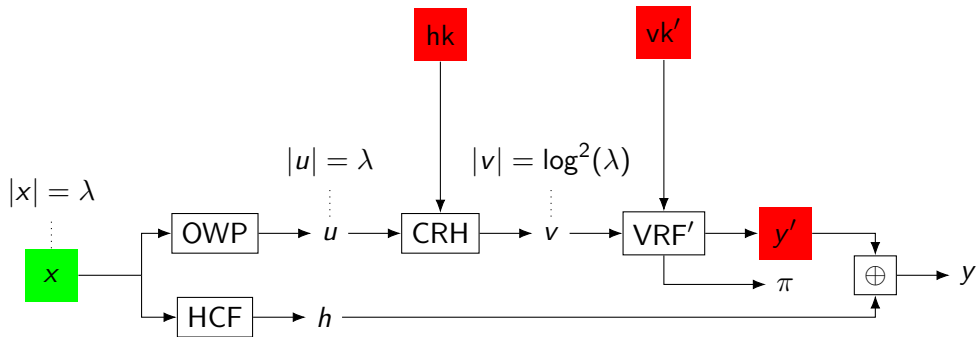
Unbiasability ✓



Construction

Pseudorandomness ✓

Unbiasability ✓



Simplified Unbiasability Game

$\mathcal{C}(1^\lambda)$

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

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

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

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

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

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

$\leftarrow \text{vk}$

$\text{---} y_b \text{---} \rightarrow$

$\leftarrow b' \text{---}$

Simplified Unbiasability Reduction

$\mathcal{C}(1^\lambda)$

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

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

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

$\mathcal{R}(1^\lambda)$

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

\xrightarrow{u}

$\xleftarrow{\text{vk} = (\text{hk}, \text{vk}')} \leftarrow$

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

find $y'_0, \pi' : \text{VRF}'.\text{Verify}(\text{vk}', v, y'_0, \pi') = 1$

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

$\xleftarrow{b'} \leftarrow$

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

else $h' := 1$

$\xleftarrow{h'} \leftarrow$

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

Simplified Unbiasability Reduction

$\mathcal{C}(1^\lambda)$

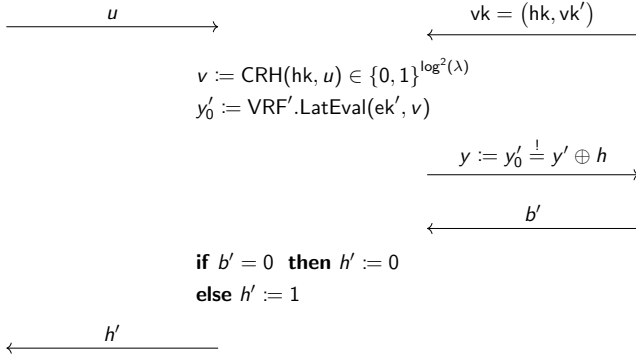
$x \leftarrow \{0, 1\}^\lambda$

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

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

$\mathcal{R}_{\text{ek}'}(1^\lambda)$

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



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 $\text{LatEval}'$ such that

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

Simplified Unbiasability Reduction

$\mathcal{C}(1^\lambda)$

$\mathcal{R}(1^\lambda)$

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

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

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

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

\xrightarrow{u}

$\xleftarrow{\text{vk} = (\text{hk}, \text{vk}')} \leftarrow$

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

find $y'_0, \pi' : \text{VRF}'.\text{Verify}(\text{vk}', v, y'_0, \pi') = 1$

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

$\xleftarrow{b'} \leftarrow$

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

else $h' := 1$

$\xleftarrow{h'} \leftarrow$

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 $\text{LatEval}'$ such that

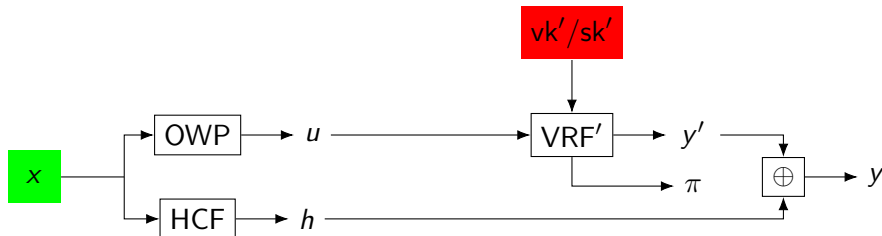
$$\forall vk' \exists ek' \forall x \left(\begin{array}{ll} y' := \text{LatEval}'(ek', x) \neq \perp & \implies y' \text{ is the valid image} \\ y' := \text{LatEval}'(ek', x) = \perp & \implies \text{no valid image exists} \end{array} \right).$$

BNN-Reduction with Polynomial Loss [Bra24]

Latent VRF

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

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



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 unbiisable VRFs [Bra25]

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

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

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

Conclusion

Conclusion

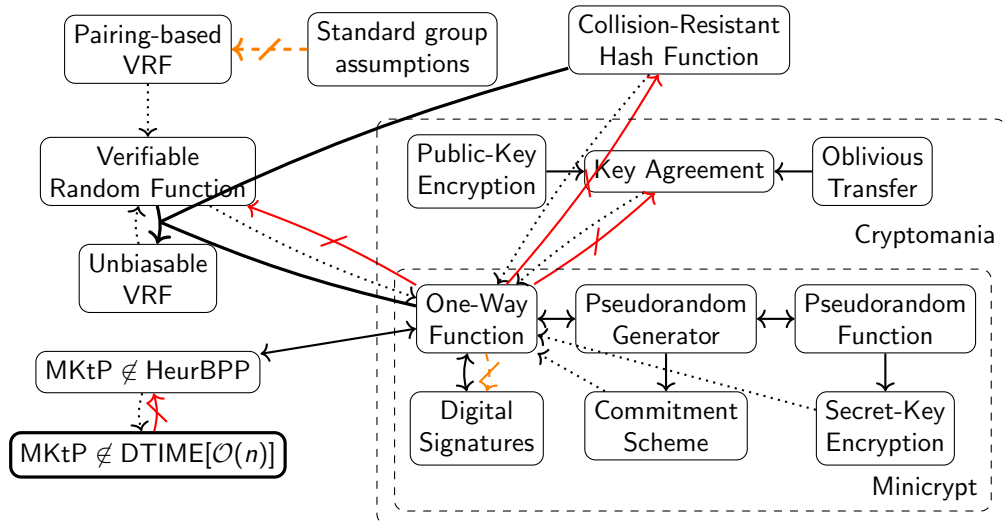
- ▶ BBB-constructions are conceptually simple but often lack feasibility or efficiency.
- ▶ Separations can formally explain insufficiencies of BBB-constructions.
- ▶ Obfuscation-/NIZK/NIWI-based constructions are often NAP.
- ▶ CNP-constructions are under-explored (non-black-box use of the adversary).

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. Wognig. 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 $\text{EXP} \neq \text{BPP}$. 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:

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

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

$$\exists OWF \iff MKtP \notin \text{HeurBPP}$$

$$BPP \neq EXP \iff MKtP \notin \text{AvgBPP}$$

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

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

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

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

$$\exists \text{OWF} \iff \text{MKtP} \notin \text{HeurBPP}$$

$$\text{BPP} \neq \text{EXP} \iff \text{MKtP} \notin \text{AvgBPP}$$

Our results [Bra24]

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

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

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

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

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

$$\exists \text{OWF} \iff \text{MKtP} \notin \text{HeurBPP}$$

$$\text{BPP} \neq \text{EXP} \iff \text{MKtP} \notin \text{AvgBPP}$$

Our results [Bra24]

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

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

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

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

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

$$\exists \text{OWF} \iff \text{MKtP} \notin \text{HeurBPP}$$

$$\text{BPP} \neq \text{EXP} \iff \text{MKtP} \notin \text{AvgBPP}$$

Our results [Bra24]

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

Lower bounds for Levin–Kolmogorov complexity [Bra24]

Context

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

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

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

$$\exists \text{OWF} \iff \text{MKtP} \notin \text{HeurBPP}$$

$$\text{BPP} \neq \text{EXP} \iff \text{MKtP} \notin \text{AvgBPP}$$

Our results [Bra24]

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

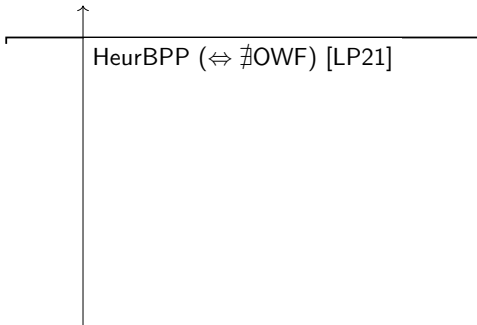
Lower bounds for Levin–Kolmogorov complexity [Bra24]

Hardness of MKtP



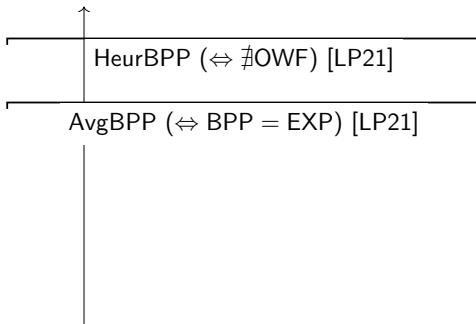
Lower bounds for Levin–Kolmogorov complexity [Bra24]

Hardness of MKtP

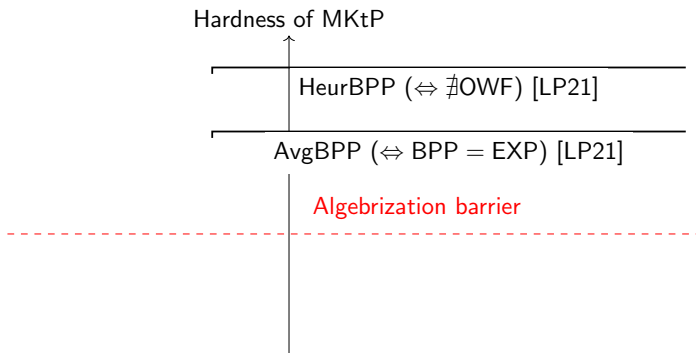


Lower bounds for Levin–Kolmogorov complexity [Bra24]

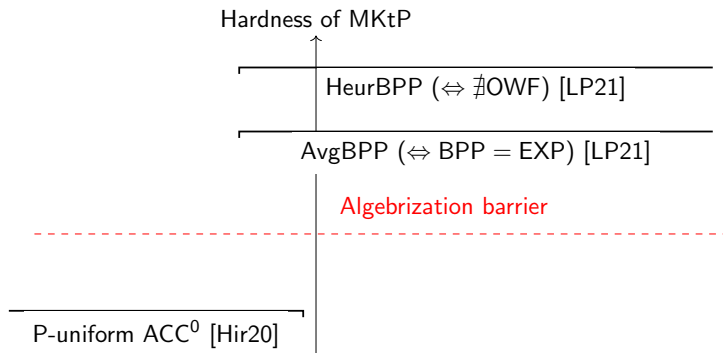
Hardness of MKtP



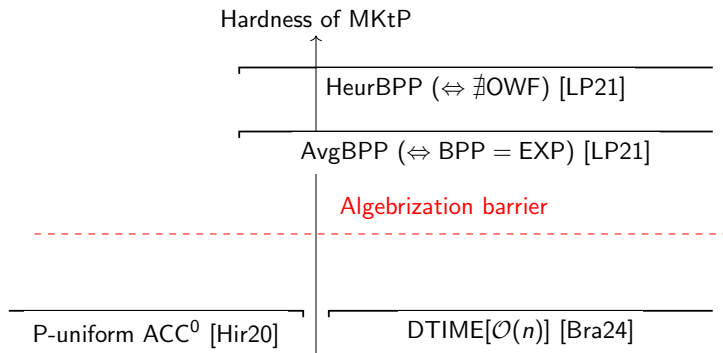
Lower bounds for Levin–Kolmogorov complexity [Bra24]



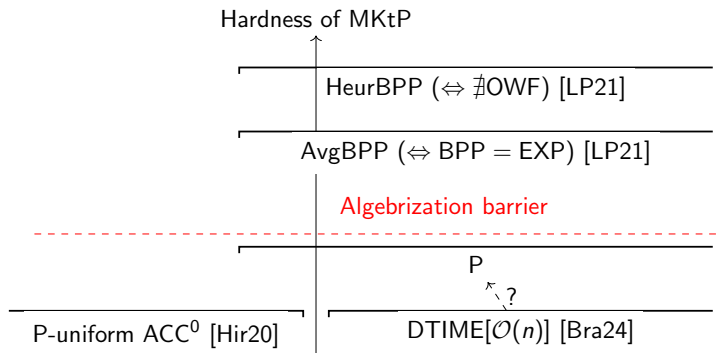
Lower bounds for Levin–Kolmogorov complexity [Bra24]



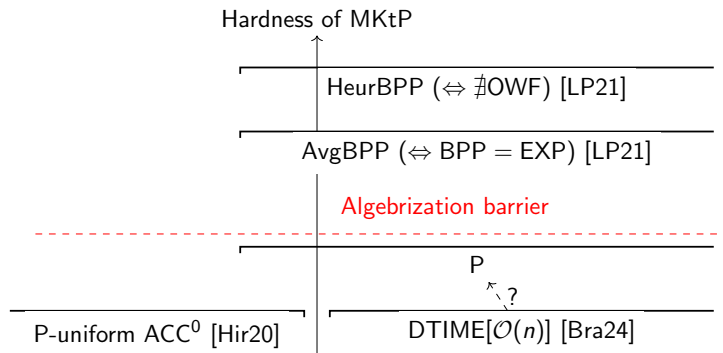
Lower bounds for Levin–Kolmogorov complexity [Bra24]



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 $BPP = EXP$