

The Price of Verifiability: Lower Bounds for Verifiable Random Functions

Nicholas Brandt

Julia Kastner

Dennis Hofheinz

Akin Ünal

Department of Computer Science
ETH Zurich
Zurich, Switzerland

`{nicholas.brandt,hofheinz,julia.kastner,akin.uenal}@inf.ethz.ch`

November 10, 2022

Verifiable Random Functions

Verifiable Random Functions

- ▶ $\text{Gen}(1^\lambda) \mapsto (\text{vk}, \text{sk})$
- ▶ $\text{Eval}(\text{sk}, x) \mapsto (\mathbf{y}_x, \pi_x)$

Verifiable Random Functions

Verifiable Random Functions

- ▶ $\text{Gen}(1^\lambda) \mapsto (\text{vk}, \text{sk})$
- ▶ $\text{Eval}(\text{sk}, x) \mapsto (\mathbf{y}_x, \pi_x)$
- ▶ $\text{Vfy}(\text{vk}, x, \mathbf{y}, \pi) \mapsto b \in \{0, 1\}$

Verifiable Random Functions

Verifiable Random Functions

- ▶ $\text{Gen}(1^\lambda) \mapsto (\text{vk}, \text{sk})$
- ▶ $\text{Eval}(\text{sk}, x) \mapsto (\mathbf{y}_x, \pi_x)$
- ▶ $\text{Vfy}(\text{vk}, x, \mathbf{y}, \pi) \mapsto b \in \{0, 1\}$

Guarantees:

- ▶ Pseudorandomness as for standard PRFs even given vk and Eval queries!

Verifiable Random Functions

Verifiable Random Functions

- ▶ $\text{Gen}(1^\lambda) \mapsto (\text{vk}, \text{sk})$
- ▶ $\text{Eval}(\text{sk}, x) \mapsto (\mathbf{y}_x, \pi_x)$
- ▶ $\text{Vfy}(\text{vk}, x, \mathbf{y}, \pi) \mapsto b \in \{0, 1\}$

Guarantees:

- ▶ Pseudorandomness as for standard PRFs even given vk and Eval queries!
- ▶ Unique Provability:
For all possible vk (not necessarily generated by Gen), all preimages x , all images $\mathbf{y}_1, \mathbf{y}_2 \in \mathbb{G}$ and all possible proofs π_1, π_2 it holds that

$$\text{Vfy}(\text{vk}, x, \mathbf{y}_1, \pi_1) = 1 \wedge \text{Vfy}(\text{vk}, x, \mathbf{y}_2, \pi_2) = 1 \implies \mathbf{y}_1 = \mathbf{y}_2$$

Motivation

Some applications of VRFs

- ▶ Resettable ZK proofs
- ▶ Lottery systems
- ▶ Updatable ZK databases
- ▶ Transaction escrow schemes
- ▶ E-cash systems
- ▶ Blockchain

Related Work

Selected VRF constructions

Reference	$ vk $	$ \pi $	assumption	remark
[Lys02]	2λ	λ	q -type	
[DY05]	2	1	q -type	small inputs
[HJ16]	$O(\lambda)$	$O(\lambda)$	DLIN	
[Koh19]	$\text{poly}(\lambda)$	κ	DLIN	$\kappa \in \omega(1)$

Related Work

Selected VRF constructions

Reference	$ vk $	$ \pi $	assumption	remark
[Lys02]	2λ	λ	q -type	
[DY05]	2	1	q -type	small inputs
[HJ16]	$O(\lambda)$	$O(\lambda)$	DLIN	
[Koh19]	$\text{poly}(\lambda)$	κ	DLIN	$\kappa \in \omega(1)$

Related Work

Selected VRF constructions

Reference	$ vk $	$ \pi $	assumption	remark
[Lys02]	2λ	λ	<i>q-type</i>	
[DY05]	2	1	<i>q-type</i>	small inputs
[HJ16]	$O(\lambda)$	$O(\lambda)$	DLIN	
[Koh19]	$\text{poly}(\lambda)$	κ	DLIN	$\kappa \in \omega(1)$

Do standard assumptions yield VRFs with constant-size proofs?

Related Work

Selected VRF constructions

Reference	$ vk $	$ \pi $	assumption	remark
[Lys02]	2λ	λ	q -type	small inputs
[DY05]	2	1	q -type	
[HJ16]	$O(\lambda)$	$O(\lambda)$	DLIN	$\kappa \in \omega(1)$
[Koh19]	$\text{poly}(\lambda)$	κ	DLIN	

Do standard assumptions yield VRFs with constant-size proofs?

- ▶ In general: ???

Related Work

Selected VRF constructions

Reference	$ vk $	$ \pi $	assumption	remark
[Lys02]	2λ	λ	q -type	small inputs
[DY05]	2	1	q -type	
[HJ16]	$O(\lambda)$	$O(\lambda)$	DLIN	$\kappa \in \omega(1)$
[Koh19]	$\text{poly}(\lambda)$	κ	DLIN	

Do standard assumptions yield VRFs with constant-size proofs?

- ▶ In general: ???
- ▶ Pairing-based VRF:

Related Work

Selected VRF constructions

Reference	$ vk $	$ \pi $	assumption	remark
[Lys02]	2λ	λ	<i>q-type</i>	small inputs
[DY05]	2	1	<i>q-type</i>	
[HJ16]	$O(\lambda)$	$O(\lambda)$	DLIN	$\kappa \in \omega(1)$
[Koh19]	$\text{poly}(\lambda)$	κ	DLIN	

Do standard assumptions yield VRFs with constant-size proofs?

- ▶ In general: ???
- ▶ Pairing-based VRF: most constructions use a “consecutive verification” strategy

Related Work

Selected VRF constructions

Reference	$ vk $	$ \pi $	assumption	remark
[Lys02]	2λ	λ	q -type	small inputs
[DY05]	2	1	q -type	
[HJ16]	$O(\lambda)$	$O(\lambda)$	DLIN	$\kappa \in \omega(1)$
[Koh19]	$\text{poly}(\lambda)$	κ	DLIN	

Do standard assumptions yield VRFs with constant-size proofs?

- ▶ In general: ???
- ▶ Pairing-based VRF: most constructions use a “consecutive verification” strategy and images have “rational” form

$$\mathbf{y}_x = \mathbf{g}^{\mathbf{T}} \sigma_x(v_1, \dots, v_n) / \rho_x(v_1, \dots, v_n)$$

Contributions

Do standard assumptions yield VRFs with constant-size proofs?

Contributions

Do standard assumptions yield VRFs with constant-size proofs?

Contributions

1. Verification by (consecutive) pairing equations
 \implies degree of σ_x and ρ_x is at most exponential in proof size

Contributions

Do standard assumptions yield VRFs with constant-size proofs?

Contributions

1. Verification by (consecutive) pairing equations
 \implies degree of σ_x and ρ_x is at most exponential in proof size
2. $\mathcal{O}(\log(\lambda))$ proof size
 \implies polynomial degree
 \implies univariate polynomial-size assumption is insufficient

Contributions

Do standard assumptions yield VRFs with constant-size proofs?

Contributions

1. Verification by (consecutive) pairing equations
 \implies degree of σ_x and ρ_x is at most exponential in proof size
2. $\mathcal{O}(\log(\lambda))$ proof size
 \implies polynomial degree
 \implies univariate polynomial-size assumption is insufficient
3. $\mathcal{O}(1)$ proof size
 \implies constant degree
 \implies small-size assumption is insufficient

Preliminaries

Consecutive Verifiability

$$\begin{array}{cccccc} vk_1 & vk_2 & vk_3 & \pi_1 & \pi_2 & \mathbf{y} \\ [v_1] & [v_2] & [v_3] & [p_1] & [p_2] & [y] \end{array}$$

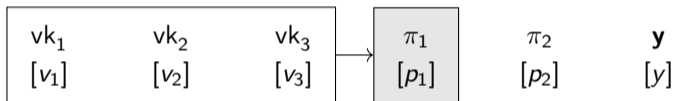
Preliminaries

Consecutive Verifiability

vk_1	vk_2	vk_3	π_1	π_2	y
$[v_1]$	$[v_2]$	$[v_3]$	$[p_1]$	$[p_2]$	$[y]$

Preliminaries

Consecutive Verifiability



$$E_1(v_1, v_2, v_3, p_1) = 0$$

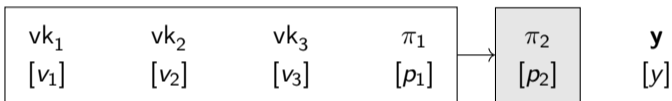
Preliminaries

Consecutive Verifiability

vk_1	vk_2	vk_3	π_1	π_2	y
$[v_1]$	$[v_2]$	$[v_3]$	$[p_1]$	$[p_2]$	$[y]$

Preliminaries

Consecutive Verifiability



$$E_2(v_1, v_2, v_3, p_1, p_2) = 0$$

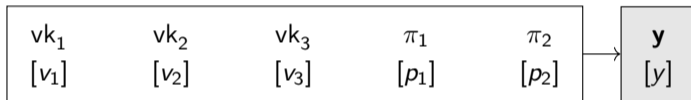
Preliminaries

Consecutive Verifiability

vk_1	vk_2	vk_3	π_1	π_2	y
$[v_1]$	$[v_2]$	$[v_3]$	$[p_1]$	$[p_2]$	$[y]$

Preliminaries

Consecutive Verifiability



$$E_{\mathbf{y}}(v_1, v_2, v_3, p_1, p_2, y) = 0$$

Preliminaries

Consecutive Verifiability

vk_1	vk_2	vk_3	π_1	π_2	y
$[v_1]$	$[v_2]$	$[v_3]$	$[p_1]$	$[p_2]$	$[y]$

Preliminaries

Consecutive Verifiability

vk_1	vk_2	vk_3	π_1	π_2	y
$[v_1]$	$[v_2]$	$[v_3]$	$[p_1]$	$[p_2]$	$[y]$

Technical restriction: p_i only occurs linearly in E_i (y only linear in E_y)

Preliminaries

Notation

- ▶ $\langle \mathbf{g} \rangle = \mathbb{G}$ // source group
- ▶ $\langle \mathbf{g}_T \rangle = \mathbb{G}_T$ // target group
- ▶ $e(\mathbf{g}^a, \mathbf{g}^b) = \mathbf{g}_T^{ab}$ // pairing operation
- ▶ $\text{vk} = (\mathbf{g}^{v_1}, \dots, \mathbf{g}^{v_n})$

Model

Example [DY05]

- ▶ $vk = (\mathbf{g}^1, \mathbf{g}^{v_2})$
- ▶ $\mathbf{y}_x = \mathbf{g}_T^{1/(v_2+x)} = \mathbf{g}_T^y$
- ▶ $\pi_x = \mathbf{g}^{1/(v_2+x)} = \mathbf{g}^{p_1}$

Model

Example [DY05]

▶ $vk = (\mathbf{g}^1, \mathbf{g}^{v_2})$

▶ $\mathbf{y}_x = \mathbf{g}_T^{1/(v_2+x)} = \mathbf{g}_T^y$

▶ $\pi_x = \mathbf{g}^{1/(v_2+x)} = \mathbf{g}^{p_1}$

▶ $\text{Vfy}(vk, x, \mathbf{y}, \pi) = 1 \iff \overbrace{e(vk_1^x \cdot vk_2, \pi) = \mathbf{g}_T}^{(x+v_2) \cdot p_1 = 1} \wedge \overbrace{e(vk_1, \pi) = \mathbf{y}}^{1 \cdot p_1 = y}$

Model

Example [DY05]

- ▶ $vk = (\mathbf{g}^1, \mathbf{g}^{v_2})$
- ▶ $\mathbf{y}_x = \mathbf{g}_T^{1/(v_2+x)} = \mathbf{g}_T^y$
- ▶ $\pi_x = \mathbf{g}^{1/(v_2+x)} = \mathbf{g}^{p_1}$
- ▶ $Vfy(vk, x, \mathbf{y}, \pi) = 1 \iff \overbrace{e(vk_1^x \cdot vk_2, \pi)}^{(x+v_2) \cdot p_1 = 1} = \mathbf{g}_T \wedge \overbrace{e(vk_1, \pi)}^{1 \cdot p_1 = y} = \mathbf{y}$
- ▶ q -Diffie-Hellman inversion assumption:
given $\mathbf{g}, \mathbf{g}^\alpha, \mathbf{g}^{\alpha^2}, \dots, \mathbf{g}^{\alpha^q}$ compute $\mathbf{g}^{1/\alpha}$

Model

Example [DY05]

- ▶ $vk = (\mathbf{g}^1, \mathbf{g}^{v_2})$
- ▶ $\mathbf{y}_x = \mathbf{g}_T^{1/(v_2+x)} = \mathbf{g}_T^y$
- ▶ $\pi_x = \mathbf{g}^{1/(v_2+x)} = \mathbf{g}^{p_1}$
- ▶ $\text{Vfy}(vk, x, \mathbf{y}, \pi) = 1 \iff \overbrace{e(vk_1^x \cdot vk_2, \pi)}^{(x+v_2) \cdot p_1 = 1} = \mathbf{g}_T \wedge \overbrace{e(vk_1, \pi)}^{1 \cdot p_1 = y} = \mathbf{y}$
- ▶ q -Diffie-Hellman inversion assumption:
given $\mathbf{g}, \mathbf{g}^\alpha, \mathbf{g}^{\alpha^2}, \dots, \mathbf{g}^{\alpha^q}$ compute $\mathbf{g}^{1/\alpha}$

- ▶ Verification by a set of “consecutive pairing equations”

Model

Example [DY05]

- ▶ $vk = (\mathbf{g}^1, \mathbf{g}^{v_2})$
- ▶ $\mathbf{y}_x = \mathbf{g}_T^{1/(v_2+x)} = \mathbf{g}_T^y$
- ▶ $\pi_x = \mathbf{g}^{1/(v_2+x)} = \mathbf{g}^{p_1}$
- ▶ $Vfy(vk, x, \mathbf{y}, \pi) = 1 \iff \overbrace{e(vk_1^x \cdot vk_2, \pi)}^{(x+v_2) \cdot p_1=1} = \mathbf{g}_T \wedge \overbrace{e(vk_1, \pi)}^{1 \cdot p_1=y} = \mathbf{y}$
- ▶ q -Diffie-Hellman inversion assumption:
given $\mathbf{g}, \mathbf{g}^\alpha, \mathbf{g}^{\alpha^2}, \dots, \mathbf{g}^{\alpha^q}$ compute $\mathbf{g}^{1/\alpha}$
- ▶ Verification by a set of “consecutive pairing equations”

Model

Example [DY05]

- ▶ $vk = (\mathbf{g}^1, \mathbf{g}^{v_2})$
- ▶ $\mathbf{y}_x = \mathbf{g}_T^{1/(v_2+x)} = \mathbf{g}_T^y$
- ▶ $\pi_x = \mathbf{g}^{1/(v_2+x)} = \mathbf{g}^{p_1}$
- ▶ $Vfy(vk, x, \mathbf{y}, \pi) = 1 \iff \overbrace{e(vk_1^x \cdot vk_2, \pi)}^{(x+v_2) \cdot p_1=1} = \mathbf{g}_T \wedge \overbrace{e(vk_1, \pi)}^{1 \cdot p_1=y} = \mathbf{y}$
- ▶ q -Diffie-Hellman inversion assumption:
given $\mathbf{g}, \mathbf{g}^\alpha, \mathbf{g}^{\alpha^2}, \dots, \mathbf{g}^{\alpha^q}$ compute $\mathbf{g}^{1/\alpha}$
- ▶ Verification by a set of “consecutive pairing equations”
- ▶ \implies Images have “rational” form with small degree:
 $\mathbf{y}_x = \mathbf{g}_T^{\sigma_x(v_1, \dots, v_n) / \rho_x(v_1, \dots, v_n)}$

Model

Example [DY05]

- ▶ $vk = (\mathbf{g}^1, \mathbf{g}^{v_2})$
- ▶ $\mathbf{y}_x = \mathbf{g}_T^{1/(v_2+x)} = \mathbf{g}_T^y$
- ▶ $\pi_x = \mathbf{g}^{1/(v_2+x)} = \mathbf{g}^{p_1}$
- ▶ $Vfy(vk, x, \mathbf{y}, \pi) = 1 \iff \overbrace{e(vk_1^x \cdot vk_2, \pi)}^{(x+v_2) \cdot p_1=1} = \mathbf{g}_T \wedge \overbrace{e(vk_1, \pi)}^{1 \cdot p_1=y} = \mathbf{y}$
- ▶ q -Diffie-Hellman inversion assumption:
given $\mathbf{g}, \mathbf{g}^\alpha, \mathbf{g}^{\alpha^2}, \dots, \mathbf{g}^{\alpha^q}$ compute $\mathbf{g}^{1/\alpha}$
- ▶ Verification by a set of “consecutive pairing equations”
- ▶ \implies Images have “rational” form with small degree:
 $\mathbf{y}_x = \mathbf{g}_T^{\sigma_x(v_1, \dots, v_n) / \rho_x(v_1, \dots, v_n)}$

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)
- ▶ Small degree \implies univariate assumptions are too weak (algebraic reductions)

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)
- ▶ Small degree \implies univariate assumptions are too weak (algebraic reductions)
- ▶ Constant degree \implies short assumptions are too weak (generic reductions)

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)
- ▶ Small degree \implies univariate assumptions are too weak (algebraic reductions)
- ▶ Constant degree \implies short assumptions are too weak (generic reductions)

Takeaway

- ▶ [Koh19] is essentially optimal w.r.t. the proof size based on DLIN

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)
- ▶ Small degree \implies univariate assumptions are too weak (algebraic reductions)
- ▶ Constant degree \implies short assumptions are too weak (generic reductions)

Takeaway

- ▶ [Koh19] is essentially optimal w.r.t. the proof size based on DLIN
- ▶ To improve [Koh19] inherently different verification strategy is necessary

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)
- ▶ Small degree \implies univariate assumptions are too weak (algebraic reductions)
- ▶ Constant degree \implies short assumptions are too weak (generic reductions)

Takeaway

- ▶ [Koh19] is essentially optimal w.r.t. the proof size based on DLIN
- ▶ To improve [Koh19] inherently different verification strategy is necessary
- ▶ Decisional assumptions are inherently stronger than (univariate) computational ones (relative to algebraic reductions)

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)
- ▶ Small degree \implies univariate assumptions are too weak (algebraic reductions)
- ▶ Constant degree \implies short assumptions are too weak (generic reductions)

Takeaway

- ▶ [Koh19] is essentially optimal w.r.t. the proof size based on DLIN
- ▶ To improve [Koh19] inherently different verification strategy is necessary
- ▶ Decisional assumptions are inherently stronger than (univariate) computational ones (relative to algebraic reductions)
- ▶ No algebraic analog of the Goldreich-Levin predicate

Summary

Summary

- ▶ “Consecutive verifiability” \implies rational form of VRF image
- ▶ Short proofs \implies small degree (still exponential)
- ▶ Small degree \implies univariate assumptions are too weak (algebraic reductions)
- ▶ Constant degree \implies short assumption (generic reductions)

Thank you!
ia.cr/2022/762


Takeaway


- ▶ [Koh19] is essentially optimal w.r.t. the proof size based on DLIN
- ▶ To improve [Koh19] inherently different verification strategy is necessary
- ▶ Decisional assumptions are inherently stronger than (univariate) computational ones (relative to algebraic reductions)
- ▶ No algebraic analog of the Goldreich-Levin predicate

References I

 Y. Dodis and A. Yampolskiy. A verifiable random function with short proofs and keys. In S. Vaudenay, editor, *PKC 2005*, volume 3386 of *LNCS*, pages 416–431. Springer, Heidelberg, January 2005.

 D. Hofheinz and T. Jager. Verifiable random functions from standard assumptions. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 336–362. Springer, Heidelberg, January 2016.

 L. Kohl. Hunting and gathering - verifiable random functions from standard assumptions with short proofs. In D. Lin and K. Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 408–437. Springer, Heidelberg, April 2019.

 A. Lysyanskaya. Unique signatures and verifiable random functions from the DH-DDH separation. In M. Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 597–612. Springer, Heidelberg, August 2002.

Formal statements

Theorem

Let p be a superpolynomial group order. Let NICA be a non-interactive computational assumption of size $q \in \text{poly}(\lambda)$. Let $n, d, d_f \in \text{poly}(\lambda)$ and let $f_1, \dots, f_n \in \mathbb{Z}_p[S]$ be some polynomials of degree at most d_f . Let vuf be a rational univariate VUF of evaluation degree d and internal degree d_f over n variables relative to the polynomials f_1, \dots, f_n .

If there exists an algebraic $(t_{\mathcal{B}}, \epsilon_{\mathcal{B}}, r, Q, 1/(Q+1))$ -reduction \mathcal{B} from NICA to the weak Q -selective unpredictability of vuf s.t. $Q \geq q^2 + 1$ and $r \in \text{poly}(\lambda)$, then there exists an adversary \mathcal{M} that $(t_{\mathcal{M}}, \epsilon_{\mathcal{M}})$ -breaks NICA with $\epsilon_{\mathcal{M}} \geq \epsilon_{\mathcal{B}} - 2^{-\lambda}$ and $t_{\mathcal{M}} \leq t_{\mathcal{B}} + \text{poly}(\lambda)$.

Formal statements

Theorem

Let $p = p(\lambda)$ be a superpolynomial group order. Let NICA be some univariate DLog-hard assumption with $l_1, l_2, d_{\text{NICA}} \in \text{poly}(\lambda)$, and polynomials $r_1, \dots, r_{l_1}, t_1, \dots, t_{l_2} \in \mathbb{Z}_p[S]$ of degree at most d_{NICA} . Let $n, d, r \in \text{poly}(\lambda)$. Let vrf be a rational VRF of evaluation degree d with n verification key elements s.t.

$$\forall x \in \mathcal{X} : \sigma_x(\vec{V}) = V_1.$$

If there exists an algebraic $(t_B, \epsilon_B, r, 0, 1)$ -reduction \mathcal{B} (that forwards its group description as part of the verification key) from NICA to the 0-adaptive pseudorandomness of vrf, then there exists an adversary \mathcal{M} that (t_M, ϵ_M) -breaks NICA with $\epsilon_M \geq \epsilon_B - 2^{-\lambda}$ and $t_M \leq t_B + \text{poly}(l_2, d_{\text{NICA}}, d, \log p, r) = t_B + \text{poly}(\lambda)$.

Formal statements

Theorem

Let vuf be a parametrized rational VUF of evaluation degree $d_{\text{vuf}} \in O(1)$. Let NICA be an Uber-assumption of degree $d_{\text{NICA}} \in \text{poly}(\lambda)$ and of size $q \leq \sqrt{\log \log(w)}$ for some $w \in \text{poly}(\lambda)$.

If NICA is hard and $Q > 2 \cdot (1 + \log \log w) \cdot w^{2 \log(d_{\text{vuf}}+1)}$, then there is no generic reduction that can transform an adversary for the weak Q -selective unpredictability of vuf to a NICA solver.

Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

C \mathcal{M} \mathcal{R} \mathcal{A}

Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

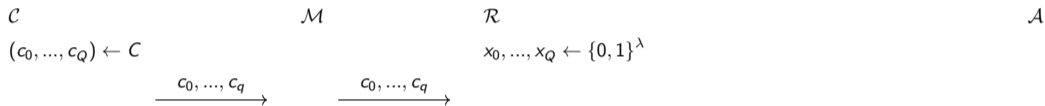
\mathcal{C}	\mathcal{M}	\mathcal{R}	\mathcal{A}
$(c_0, \dots, c_Q) \leftarrow C$		$x_0, \dots, x_Q \leftarrow \{0, 1\}^\lambda$	

Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

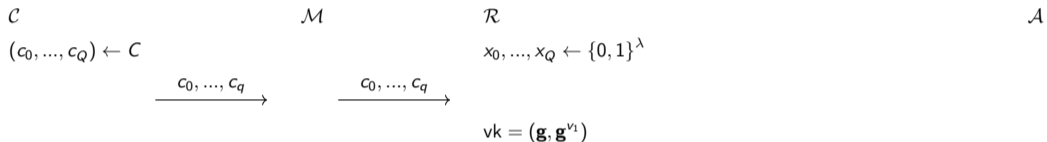


Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

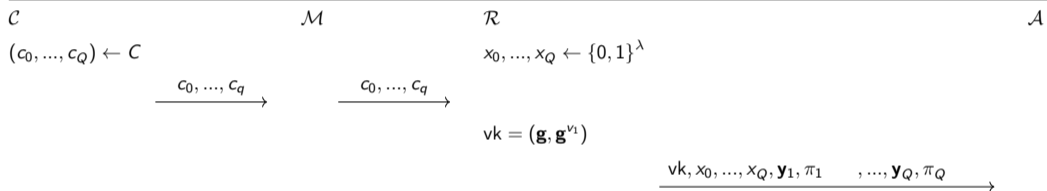


Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

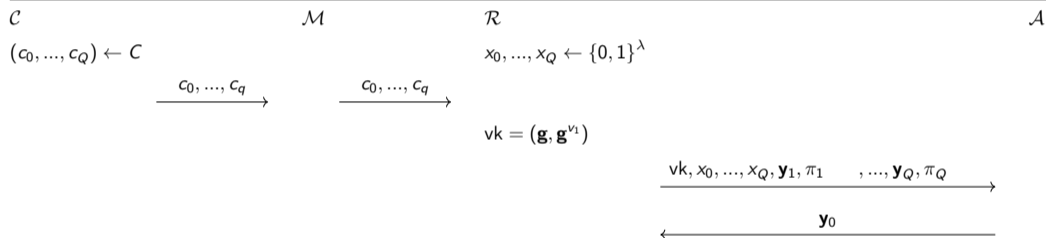


Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

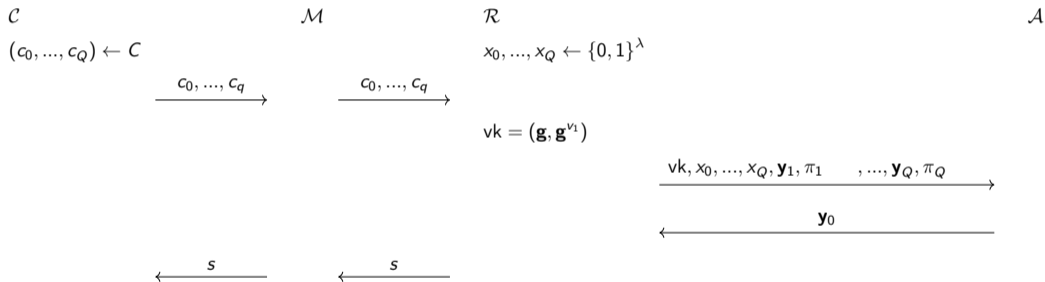


Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

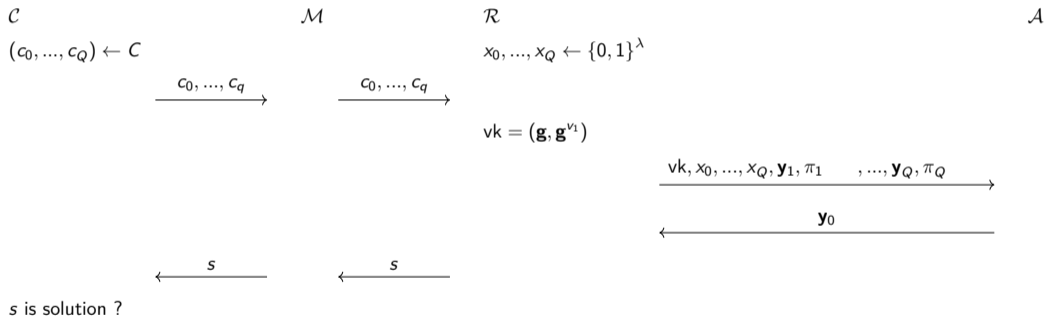


Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability

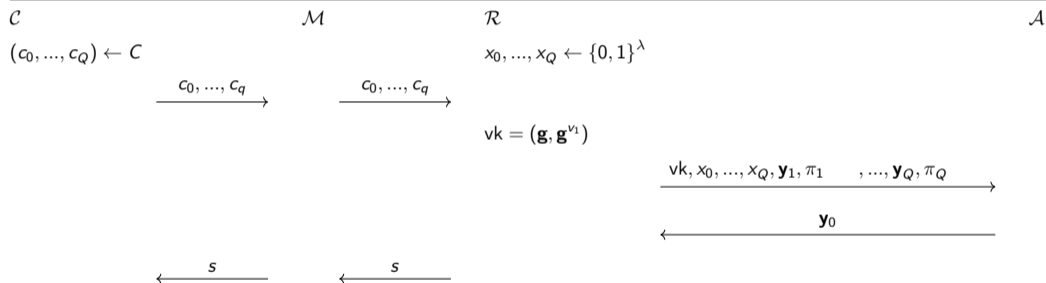


Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability



s is solution ?

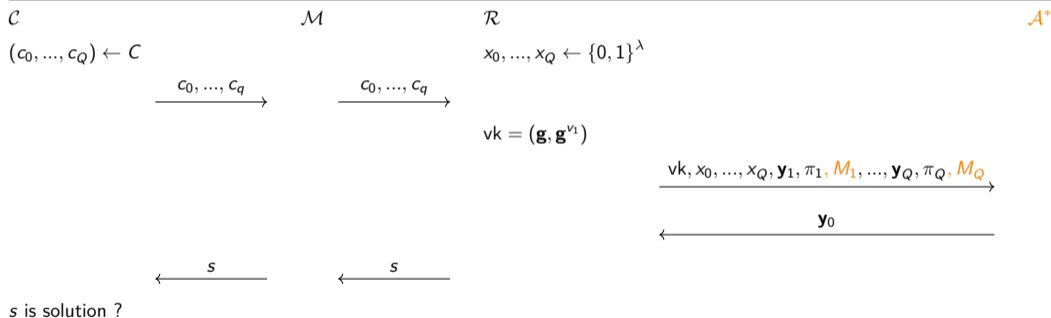
How to simulate an unbounded adversary \mathcal{A} with algebraic representations?

Result

Simplified meta-reduction

polynomial degree \implies polynomial-size assumption is insufficient

Meta-reduction: any q -size assumption C to weak Q -selective unpredictability



How to simulate an unbounded adversary \mathcal{A} with algebraic representations?

Result

Simulating \mathcal{A} with algebraic representations

Result

Simulating \mathcal{A} with algebraic representations

1. Compute $\zeta_i(V) := \sigma_{x_i}(V)/\rho_{x_i}(V) \in \mathbb{Z}_p(V)$ as rational polynomial

Result

Simulating \mathcal{A} with algebraic representations

1. Compute $\zeta_i(V) := \sigma_{x_i}(V)/\rho_{x_i}(V) \in \mathbb{Z}_p(V)$ as rational polynomial
2. If $\zeta_i(V)$ are linearly dependent, i.e., $\exists \alpha \in \mathbb{Z}_p^{Q+1} : \sum_{i=0}^Q \zeta_i(V) \equiv 0$, then predict challenge image as $\mathbf{y}_0 := \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i}$

Result

Simulating \mathcal{A} with algebraic representations

1. Compute $\zeta_i(V) := \sigma_{x_i}(V)/\rho_{x_i}(V) \in \mathbb{Z}_p(V)$ as rational polynomial
2. If $\zeta_i(V)$ are linearly dependent, i.e., $\exists \alpha \in \mathbb{Z}_p^{Q+1} : \sum_{i=0}^Q \zeta_i(V) \equiv 0$, then predict challenge image as $\mathbf{y}_0 := \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i}$
3. If $\zeta_i(V)$ are linearly independent, compute $\alpha \in \mathbb{Z}_p^Q \setminus \{0\}$ s.t. $\sum_{i=1}^Q \alpha_i M_i = 0 \in \mathbb{Z}_p^{(q+1) \times (q+1)}$, then $\mathbf{g}_T^0 = \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i} = \prod_{i=1}^Q \mathbf{g}_T^{\alpha_i \zeta_i(v_1)}$

Result

Simulating \mathcal{A} with algebraic representations

1. Compute $\zeta_i(V) := \sigma_{x_i}(V)/\rho_{x_i}(V) \in \mathbb{Z}_p(V)$ as rational polynomial
2. If $\zeta_i(V)$ are linearly dependent, i.e., $\exists \alpha \in \mathbb{Z}_p^{Q+1} : \sum_{i=0}^Q \zeta_i(V) \equiv 0$, then predict challenge image as $\mathbf{y}_0 := \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i}$
3. If $\zeta_i(V)$ are linearly independent, compute $\alpha \in \mathbb{Z}_p^Q \setminus \{0\}$ s.t. $\sum_{i=1}^Q \alpha_i M_i = 0 \in \mathbb{Z}_p^{(q+1) \times (q+1)}$, then $\mathbf{g}_T^0 = \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i} = \prod_{i=1}^Q \mathbf{g}_T^{\alpha_i \zeta_i(v_1)}$
4. Note $0 = \sum_{i=1}^Q \alpha_i \zeta_i(v_1) \in \mathbb{Z}_p$

Result

Simulating \mathcal{A} with algebraic representations

1. Compute $\zeta_i(V) := \sigma_{x_i}(V)/\rho_{x_i}(V) \in \mathbb{Z}_p(V)$ as rational polynomial
2. If $\zeta_i(V)$ are linearly dependent, i.e., $\exists \alpha \in \mathbb{Z}_p^{Q+1} : \sum_{i=0}^Q \zeta_i(V) \equiv 0$, then predict challenge image as $\mathbf{y}_0 := \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i}$
3. If $\zeta_i(V)$ are linearly independent, compute $\alpha \in \mathbb{Z}_p^Q \setminus \{0\}$ s.t. $\sum_{i=1}^Q \alpha_i M_i = 0 \in \mathbb{Z}_p^{(q+1) \times (q+1)}$, then $\mathbf{gT}^0 = \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i} = \prod_{i=1}^Q \mathbf{gT}^{\alpha_i \zeta_i(v_1)}$
4. Note $0 = \sum_{i=1}^Q \alpha_i \zeta_i(v_1) \in \mathbb{Z}_p$
5. Define “target polynomial” with root v_1

$$\psi(V) := \rho_{x_1}(V) \cdots \rho_{x_Q}(V) \cdot \sum_{i=1}^Q \alpha_i \zeta_i(V) \quad (1)$$

(2)

Result

Simulating \mathcal{A} with algebraic representations

1. Compute $\zeta_i(V) := \sigma_{x_i}(V)/\rho_{x_i}(V) \in \mathbb{Z}_p(V)$ as rational polynomial
2. If $\zeta_i(V)$ are linearly dependent, i.e., $\exists \alpha \in \mathbb{Z}_p^{Q+1} : \sum_{i=0}^Q \zeta_i(V) \equiv 0$, then predict challenge image as $\mathbf{y}_0 := \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i}$
3. If $\zeta_i(V)$ are linearly independent, compute $\alpha \in \mathbb{Z}_p^Q \setminus \{0\}$ s.t. $\sum_{i=1}^Q \alpha_i M_i = 0 \in \mathbb{Z}_p^{(q+1) \times (q+1)}$, then $\mathbf{gT}^0 = \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i} = \prod_{i=1}^Q \mathbf{gT}^{\alpha_i \zeta_i(v_1)}$
4. Note $0 = \sum_{i=1}^Q \alpha_i \zeta_i(v_1) \in \mathbb{Z}_p$
5. Define “target polynomial” with root v_1

$$\psi(V) := \rho_{x_1}(V) \cdots \rho_{x_Q}(V) \cdot \sum_{i=1}^Q \alpha_i \zeta_i(V) \quad (1)$$

$$= \sum_{i=1}^Q \alpha_i \sigma_{x_i}(V) \prod_{i' \neq i} \rho_{x_{i'}}(V) \in \mathbb{Z}_p[V] \quad (2)$$

Result

Simulating \mathcal{A} with algebraic representations

1. Compute $\zeta_i(V) := \sigma_{x_i}(V)/\rho_{x_i}(V) \in \mathbb{Z}_p(V)$ as rational polynomial
2. If $\zeta_i(V)$ are linearly dependent, i.e., $\exists \alpha \in \mathbb{Z}_p^{Q+1} : \sum_{i=0}^Q \zeta_i(V) \equiv 0$, then predict challenge image as $\mathbf{y}_0 := \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i}$
3. If $\zeta_i(V)$ are linearly independent, compute $\alpha \in \mathbb{Z}_p^Q \setminus \{0\}$ s.t. $\sum_{i=1}^Q \alpha_i M_i = 0 \in \mathbb{Z}_p^{(q+1) \times (q+1)}$, then $\mathbf{gT}^0 = \prod_{i=1}^Q \mathbf{y}_i^{\alpha_i} = \prod_{i=1}^Q \mathbf{gT}^{\alpha_i \zeta_i(v_1)}$
4. Note $0 = \sum_{i=1}^Q \alpha_i \zeta_i(v_1) \in \mathbb{Z}_p$
5. Define “target polynomial” with root v_1

$$\psi(V) := \rho_{x_1}(V) \cdots \rho_{x_Q}(V) \cdot \sum_{i=1}^Q \alpha_i \zeta_i(V) \quad (1)$$

$$= \sum_{i=1}^Q \alpha_i \sigma_{x_i}(V) \prod_{i' \neq i} \rho_{x_{i'}}(V) \in \mathbb{Z}_p[V] \quad (2)$$

6. Factorize $\psi(V)$, find sk v_1 and compute $\mathbf{y}_0 := \text{Eval}(v_1, x_0)$