

Oracle Separation in Cryptography

Ahto Buldas

Cybernetica AS / TU / TTU

Agenda

Overview:

- Cryptographic Constructions and Security Proofs
- Black-Box Constructions and Their Role in Cryptography
- How Oracle Separation is used to rule out black-box constructions
- Some separation results (including our recent work)

Problem:

- Current separation results only hold in the uniform polynomial security model.

Our Result (joint work with Margus Niitsoo and Sven Laur):

- We show how to extend all previous results to non-uniform security model.

Cryptographic Constructions and Security Proofs

Complex cryptographic protocols P are often built from simpler cryptographic primitives f .

Security Proof: If the protocol P^f can be broken somehow then also the primitive f can be broken.

Security Proof: If there is an efficient adversary A that breaks P^f then we can construct an efficient adversary B (based on A) that breaks f .

If f is believed to be secure then P^f must also be secure!

Black-Box Reductions

Security proofs for the constructed protocols that do not use the internal structure of the primitives are called *black-box reductions*.

This is the most common way to reason about security – almost all security proofs for efficient cryptographic constructions utilize black-box reductions.

Still, the security of certain cryptographic constructions cannot be established with black-box reductions.

This means that a very clever proof construction is necessary if the reduction can be achieved at all.

As very few of these "clever" constructions are known, the power and limits of black-box reductions are of great interest to cryptographers.

Definition of Primitives: Functionality

An *instance* of a cryptographic primitive is an atomic object f that provides access to computational services.

Example. Encryption primitive as an object f with three member functions $f.gen$, $f.enc$ and $f.dec$ that satisfy the obvious restriction

$$\forall (pk, sk) \leftarrow f.gen(n), \forall m \in \{0, 1\}^n : m = f.dec(sk, f.enc(pk, m)) .$$

f can be represented as a single function $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ because the first few bits of the input can determine the member function.

A *cryptographic primitive* is a class \mathcal{P} of functions that satisfy certain functionality requirements.

Definition of Primitives: Adversaries and Security

To be useful, a primitive \mathcal{P} must satisfy a certain security criterion that involves an *adversary* A . Adversaries can also be viewed as functions $A: \{0, 1\}^* \rightarrow \{0, 1\}^*$.

Each primitive \mathcal{P} is characterized by the *advantage function* $\text{Adv}_k^{\mathcal{P}}(\cdot)$, which for every instance f of \mathcal{P} , an adversary A , and the security parameter k returns the *advantage* $\text{Adv}_k^{\mathcal{P}}(A, f) \in [0, 1]$.

A *breaks* f iff $\text{Adv}_k^{\mathcal{P}}(A, f) \neq k^{-\omega(1)}$.

f is *secure* iff $\text{Adv}_k^{\mathcal{P}}(A, f) = k^{-\omega(1)}$ for every poly-time A .

Types of Black-Box Reductions

Definition. A *fully black-box reduction* $\mathcal{P} \xRightarrow{f} \mathcal{Q}$ is determined by two poly-time oracle machines P and S , satisfying the next two conditions:

- *Construction:* if f implements \mathcal{Q} then P^f implements \mathcal{P} ;
- *Guarantee:* if A breaks P^f as \mathcal{P} then $S^{A,f}$ breaks f as \mathcal{Q} .

Definition. A *semi-black-box reduction* $\mathcal{P} \xRightarrow{s} \mathcal{Q}$ is determined by a poly-time oracle machine P , satisfying the next two conditions:

- *C:* if f implements \mathcal{Q} then P^f implements \mathcal{P} ;
- *G:* for any poly-time A , there exists a poly-time B such that if A^f breaks P^f as \mathcal{P} , then B^f breaks f as \mathcal{Q} .

Definition. A *variable semi-black-box reduction* $\mathcal{P} \xRightarrow{v} \mathcal{Q}$: for any $f \in \mathcal{Q}$:

- *C:* there exists a poly-time oracle machine P^f that implements \mathcal{P} ;
- *G:* for any poly-time A , there exists a poly-time B such that if A^f breaks P^f as \mathcal{P} , then B^f breaks f as \mathcal{Q} .

Oracles in Complexity Theory

An *oracle* is an arbitrary function $\mathcal{O} : \{0, 1\}^* \rightarrow \{0, 1\}^*$.

Oracle machine $M^{\mathcal{O}}$ is a Turing machine that can call \mathcal{O} almost "for free".

Example. Polynomial hierarchy is defined based on oracle machines.

Relative worlds: For any oracle \mathcal{O} , we can develop a theory of efficient computations, where P is replaced with $P^{\mathcal{O}}$. Many results of Complexity Theory stay valid in this case. We say that they *relativize*.

Fact 1. Diagonalization arguments relativize.

Fact 2. There exists an oracle \mathcal{O} relative to which $P^{\mathcal{O}} = NP^{\mathcal{O}}$.

Implication: Diagonalization is insufficient for showing that $P \neq NP$.

Oracle Separation in Cryptography

Goal: to show that there exist no black-box reductions from \mathcal{P} to \mathcal{Q} .

Fact. Black-box reductions relativize!

Hence, to show that there exist no black-box reductions from \mathcal{P} to \mathcal{Q} , it is sufficient to find an oracle \mathcal{O} relative to which there exist secure instances of \mathcal{Q} but no secure instances of \mathcal{P} .

Some Oracle Separation Results

1989 Impagliazzo-Rudich: Finding a black-box reduction from key establishment to one-way permutations is at least as hard as proving $P \neq NP$.

1998 Simon: There exist no black-box reductions from collision-free hash functions to one-way permutations.

...

Our results:

2004 Buldas-Saarepera: The security of unbounded hash-then-publish time-stamping schemes cannot be proved with black-box arguments.

2007 Buldas-Jürgenson: Collision-free hash functions cannot be constructed from secure time-stamping schemes.

2008 Buldas-Niitsoo: Secure unbounded time-stamping schemes cannot probably be constructed from collision-free hash functions via black-box reductions.

Practical Separations Use Randomized Oracles

Most separation results are based on randomized oracles $\mathcal{O} \leftarrow \Omega$, which are later converted to a deterministic instances by a clever choice of random coins. So, we have two steps:

Separation on average: for every poly-time oracle machine A :

$$\mathbf{E}_{\mathcal{O} \leftarrow \Omega} \left[\text{ADV}_k^{\mathcal{O}}(A^{\mathcal{O}}, f^{\mathcal{O}}) \right] = k^{-\omega(1)} ,$$

but no $P^{\mathcal{O}} \in \mathcal{P}$ is secure relative to any \mathcal{O} in the range of Ω .

Oracle Extraction: there is a fixed oracle \mathcal{O} for which no uniform poly-time A can break $f^{\mathcal{O}}$.

Oracle Extraction Idea

Theorem. If $\mathbf{E}_{\vartheta \leftarrow \Omega} [\text{ADV}_k(A^\vartheta, f^\vartheta)] = \epsilon_A(k) = k^{-\omega(1)}$ for every uniform poly-time A , then there is an oracle ϑ so that $\text{ADV}_k(A^\vartheta, f^\vartheta) = k^{-\omega(1)}$ for every uniform poly-time A .

Proof. Markov inequality implies $\Pr_{\vartheta} [\text{ADV}_k(A^\vartheta, f^\vartheta) > k^2 \cdot \epsilon_A(k)] \leq 1/k^2$.

Let E_k be the event that $\text{ADV}_k(A^\vartheta, f^\vartheta) > k^2 \cdot \epsilon_A(k)$. As $\sum_k \Pr [E_k] \leq \sum_k \frac{1}{k^2} < \infty$, the Borel-Cantelli lemma implies

$\Pr_{\vartheta} [\text{"ADV}_k(A^\vartheta, f^\vartheta) > k^2 \cdot \epsilon_A(k) \text{ for infinitely many } k\text{-s"}] = \Pr [E_\infty] = 0$.

Let Ω_A be the set of ϑ -s for which E_∞ happens. Ω_A has measure zero for any A . As there are countably many A -s, $\cup_A \Omega_A$ also has measure zero. Hence, the $\Omega_0 = \Omega \setminus (\cup_A \Omega_A)$ is non-empty and there is ϑ such that for every uniform poly-time oracle machine A and for sufficiently large k we have $\text{ADV}_k(A^\vartheta, f^\vartheta) \leq k^2 \cdot \epsilon_A(k) = k^{-\omega(1)}$.

Limits of Oracle Extraction

Many practical primitives are required to be secure in the *non-uniform security model*.

Non-uniform reductions use machines that have polynomial *advice strings* for every input length k .

There are uncountably many advice string families $\{a_k\}_{k \in \mathbb{N}}$.

Hence, oracle extraction fails in the non-uniform security model.

Counter Example

Let $\mathbf{E}_{\mathcal{O} \leftarrow \Omega} [\text{ADV}_k(A^{\mathcal{O}}, f^{\mathcal{O}})] = k^{-\omega(1)}$ for every non-uniform poly-time A .

Define an oracle \mathcal{A} relative to which f is totally insecure as \mathcal{Q} . Add \mathcal{A} to \mathcal{O} but protect \mathcal{A} with "passwords":

- During $\mathcal{O} \leftarrow \Omega$ pick random "password" strings $\{a_k\}_{k \in \mathbb{N}}$ (parts of \mathcal{O}).
- Oracle calls $\mathcal{O}(a_k, \dots)$ "release" \mathcal{A} , i.e. there is a poly-time A so that:

$$\text{ADV}_k(A^{\mathcal{O}(a_k, \dots)}, f^{\mathcal{O}}) = 1 \neq k^{-\omega(1)} .$$

Hence, for any fixed \mathcal{O} , there is a non-uniform poly-time machine with advice $\{a_k\}_{k \in \mathbb{N}}$ that breaks $f^{\mathcal{O}}$.

- \mathcal{O} will refuse to break $f^{\mathcal{O}}$ if \mathcal{O} is called with incorrect a_k .

So, in the non-uniform model it is possible that $f^{\mathcal{O}}$ is secure on average relative to random oracle \mathcal{O} but still, $f^{\mathcal{O}}$ is insecure relative to any particular choice of \mathcal{O} .

Main Improvement Ideas

Guarantee conditions of the form: "If A breaks P^f as \mathcal{P} then $S^{A,f}$ breaks f as \mathcal{Q} " *are too weak*. We strengthen the definitions to a reasonable extent:

Poly-preserving reductions. There is a *poly-preserving* fully black-box reduction of primitive \mathcal{P} to a primitive \mathcal{Q} if there is a pair (P, S) of poly-time machines so that:

- For any function f that implements \mathcal{Q} , the machine P^f implements \mathcal{P} .
- There is $c > 0$ so that for any f and A : $\text{Adv}_k(S^{A,f}, f) \geq [\text{Adv}_k(A, P^f)]^c$.

We show that oracle extraction step is unnecessary for ruling out all poly-preserving non-uniform black-box reductions.

Separation on Average: New Separation Theorem

Theorem. If for every pair (P, S) of poly-time oracle machines there is a distribution $(A, f) \leftarrow \Omega$ of oracle pairs and a polynomial $q(k)$ such that:

- (1) f implements \mathcal{Q} , for all pairs (A, f) in the range of Ω ;
 (2) if for large enough k , if P^f implements \mathcal{P} for all $(A, f) \leftarrow \Omega$ then

$$\mathbf{E}_{(A, f) \leftarrow \Omega} [\text{ADV}_k(A, P^f)] \geq \frac{1}{q(k)}.$$

- (3) for every poly-time oracle S : $\mathbf{E}_{(A, f) \leftarrow \Omega} [\text{ADV}_k(S^{A, f}, f)] = k^{-\omega(1)}$;

then there exist no power- c fully-black-box reductions (uniform or non-uniform) of \mathcal{P} to \mathcal{Q} .

Proof Sketch of the New Separation Theorem

Let (P, S) be a fully black-box reduction of \mathcal{P} to \mathcal{Q} . By assumptions, there exists a polynomial $q(k)$ and a distribution Ω with the properties (1-3).

By (1), for every (A, f) in the range of Ω , f implements \mathcal{Q} and from the construction condition it follows that P^f implements \mathcal{P} .

By (2), $\mathbf{E}_{(A,f) \leftarrow \mathcal{D}} [\text{ADV}_k(A, P^f)] \geq \frac{1}{q(k)}$ and by the guarantee condition $\text{ADV}_k(S^{A,f}, f) \geq \text{ADV}_k(A, P^f)^c$ where we can choose $c \geq 1$ as it only decreases the left side. Hence,

$$\begin{aligned} \mathbf{E}_{(A,f) \leftarrow \Omega} [\text{ADV}_k(S^{A,f}, f)] &\geq \mathbf{E}_{(A,f) \leftarrow \Omega} [\text{ADV}_k(A, P^f)^c] \\ &\geq \mathbf{E}_{(A,f) \leftarrow \Omega} [\text{ADV}_k(A, P^f)]^c \geq \frac{1}{q^c(k)} \neq k^{-\omega(1)}. \end{aligned}$$

Conclusions

Almost all known separation results will generalize to poly-preserving reductions in the non-uniform model. For example,

- There are no non-uniform poly-preserving black-box reductions from collision-free hash functions to one-way permutations.
- There are no non-uniform poly-preserving black-box reductions from key establishment schemes to one-way permutations.
- ...

Open Questions and Further Work

Can we obtain efficiency upper-bounds for reductions in the polynomial and exact security models?

Sometimes, in practical reductions, state machines are used to model the separation oracles. For which class of reductions such a separation is sufficient?