# The "H-coefficients" Technique in a Nutshell

**Miloslav Homer**

**Jarní škola katedry algebry**

**April 5, 2017**

# Table of Contents

# Introduction

# Real Oracles

- Let $\mathcal{Z} = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ be a cryptosystem.

# Real Oracles

- Let $\mathcal{Z} = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ be a cryptosystem.
- An oracle is an object that takes queries and responds to them.

# Real Oracles

- Let $\mathcal{Z} = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ be a cryptosystem.
- An oracle is an object that takes queries and responds to them.
- We can construct a family of oracles corresponding to this cryptosystem in a following fashion:

# Real Oracles

- Let $\mathcal{Z} = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ be a cryptosystem.
- An oracle is an object that takes queries and responds to them.
- We can construct a family of oracles corresponding to this cryptosystem in a following fashion:
  - Pick a key $K \in \mathcal{K}$

# Real Oracles

- Let $\mathcal{Z} = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ be a cryptosystem.
- An oracle is an object that takes queries and responds to them.
- We can construct a family of oracles corresponding to this cryptosystem in a following fashion:
  - Pick a key $K \in \mathcal{K}$
  - (Encryption) Oracle $R$ corresponding to this key on query $P$ returns $E_K(P)$.

# Real Oracles

- Let $\mathcal{Z} = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ be a cryptosystem.
- An oracle is an object that takes queries and responds to them.
- We can construct a family of oracles corresponding to this cryptosystem in a following fashion:
  - Pick a key $K \in \mathcal{K}$
  - (Encryption) Oracle $R$ corresponding to this key on query $P$ returns $E_K(P)$.
- Define decryption oracles similarly and note we can also define a combination oracle.

# Real Oracles

- Let $\mathcal{Z} = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ be a cryptosystem.
- An oracle is an object that takes queries and responds to them.
- We can construct a family of oracles corresponding to this cryptosystem in a following fashion:
  - Pick a key $K \in \mathcal{K}$
  - (Encryption) Oracle $R$ corresponding to this key on query $P$ returns $E_K(P)$.
- Define decryption oracles similarly and note we can also define a combination oracle.
- We denote the family of them as $\Omega_{Real}$.

# Random Oracles

- In general, an (encryption, decryption) random oracle compatible with cryptosystem $\mathcal{Z}$ is a random function from $P$ to $C$ (or $C$ to $P$).

# Random Oracles

- In general, an (encryption, decryption) random oracle compatible with cryptosystem $\mathcal{Z}$ is a random function from $P$ to $C$ (or $C$ to $P$).
- This may vary depending on the properties of $\mathcal{Z}$, for example when examining block ciphers we require oracles to be random permutations.

# Random Oracles

- In general, an (encryption, decryption) random oracle compatible with cryptosystem $\mathcal{Z}$ is a random function from $P$ to $C$ (or $C$ to $P$).
- This may vary depending on the properties of $\mathcal{Z}$, for example when examining block ciphers we require oracles to be random permutations.
- We denote the family of these as $\Omega_{Random}$.

# Distinguisher

- Let $D$ be a deterministic distinguisher, i.e. a deterministic algorithm which has an oracle $R$ on input.

# Distinguisher

- Let $D$ be a deterministic distinguisher, i.e. a deterministic algorithm which has an oracle $R$ on input.
- The experiment will be conducted in following fashion:

# Distinguisher

- Let $D$ be a deterministic distinguisher, i.e. a deterministic algorithm which has an oracle $R$ on input.
- The experiment will be conducted in following fashion:
  - A coin is flipped. If heads a random element of $\Omega_{Real}$ is chosen as $R$, else chose $R$ as element of $\Omega_{Random}$.

# Distinguisher

- Let $D$ be a deterministic distinguisher, i.e. a deterministic algorithm which has an oracle $R$ on input.
- The experiment will be conducted in following fashion:
  - A coin is flipped. If heads a random element of $\Omega_{Real}$ is chosen as $R$, else chose $R$ as element of $\Omega_{Random}$.
  - $D$ is given access to oracle $R$.

# Distinguisher

- Let $D$ be a deterministic distinguisher, i.e. a deterministic algorithm which has an oracle $R$ on input.
- The experiment will be conducted in following fashion:
  - A coin is flipped. If heads a random element of $\Omega_{Real}$ is chosen as $R$, else chose $R$ as element of $\Omega_{Random}$.
  - $D$ is given access to oracle $R$.
  - $D$ interacts (queries queries, do other computations) with $R$.

# Distinguisher

- Let $D$ be a deterministic distinguisher, i.e. a deterministic algorithm which has an oracle $R$ on input.
- The experiment will be conducted in following fashion:
  - A coin is flipped. If heads a random element of $\Omega_{Real}$ is chosen as $R$, else chose $R$ as element of $\Omega_{Random}$.
  - $D$ is given access to oracle $R$.
  - $D$ interacts (queries queries, do other computations) with $R$.
  - $D$ outputs a bit - 1 denoting that $R \in \Omega_{Real}$, 0 otherwise.

# Advantage

- Define advantage of distinguisher $D$ on cryptosystem $\mathcal{Z}$:

$$\mathrm{Adv}^{\mathcal{Z}}(D) = \Pr\left[R \in \Omega_{Real} \;\&\; D^R = 1\right] - \Pr\left[R \in \Omega_{Random} \;\&\; D^R = 1\right]$$

# Advantage

- Define advantage of distinguisher $D$ on cryptosystem $\mathcal{Z}$:

$$\mathrm{Adv}^{\mathcal{Z}}(D) = \Pr\left[R \in \Omega_{Real} \;\&\; D^R = 1\right] - \Pr\left[R \in \Omega_{Random} \;\&\; D^R = 1\right]$$

- We can also define resource bounded advantage, allowing $D$ to only make $q$ queries.

# Advantage

- Define advantage of distinguisher $D$ on cryptosystem $\mathcal{Z}$:

$$\mathrm{Adv}^{\mathcal{Z}}(D) = \Pr\left[R \in \Omega_{Real} \;\&\; D^R = 1\right] - \Pr\left[R \in \Omega_{Random} \;\&\; D^R = 1\right]$$

- We can also define resource bounded advantage, allowing $D$ to only make $q$ queries.
- We are really interested in resource bounded advantage independent on distinguishers, which can be defined like this:

$$\mathrm{Adv}_q^{\mathcal{Z}} = \max_D \mathrm{Adv}_q^{\mathcal{Z}}(D).$$

# The Path to H-Coefficients

# Views

- From now on a distinguisher $D$ and number of queries $q$ is fixed.

# Views

- From now on a distinguisher $D$ and number of queries $q$ is fixed.
- Define view as set of queries and responses for $R$ that $D$ made during the experiment.

# Views

- From now on a distinguisher $D$ and number of queries $q$ is fixed.
- Define view as set of queries and responses for $R$ that $D$ made during the experiment.
- A typical view $\nu$ therefore looks like this:

$$\nu = \{(P_i, C_i) \mid i \leq q\}\,.$$

# Views

- From now on a distinguisher $D$ and number of queries $q$ is fixed.
- Define view as set of queries and responses for $R$ that $D$ made during the experiment.
- A typical view $\nu$ therefore looks like this:

$$\nu = \{(P_i, C_i) \mid i \leq q\}\,.$$

- We don't care about the order of these queries.

# Views

- From now on a distinguisher $D$ and number of queries $q$ is fixed.
- Define view as set of queries and responses for $R$ that $D$ made during the experiment.
- A typical view $\nu$ therefore looks like this:

$$\nu = \{(P_i, C_i) \mid i \leq q\}\,.$$

- We don't care about the order of these queries.
- We assume that $D$ doesn't repeat queries – this implies that for all $i \neq j$ it holds that $P_i \neq P_j$ or $C_i \neq C_j$.

# Views

- From now on a distinguisher $D$ and number of queries $q$ is fixed.
- Define view as set of queries and responses for $R$ that $D$ made during the experiment.
- A typical view $\nu$ therefore looks like this:

$$\nu = \{(P_i, C_i) \mid i \leq q\}.$$

- We don't care about the order of these queries.
- We assume that $D$ doesn't repeat queries – this implies that for all $i \neq j$ it holds that $P_i \neq P_j$ or $C_i \neq C_j$.
- Denote the set of all views $V$.

# Probability distributions

- Denote $X$ the probability distribution on views induced by *Real* oracles

# Probability distributions

- Denote $X$ the probability distribution on views induced by *Real* oracles
- we therefore ask: given distinguisher $D$ and view $\nu$ how probable it is that $D$ produced view $\nu$ after interaction with a random element from $\Omega_{Real}$?

# Probability distributions

- Denote $X$ the probability distribution on views induced by *Real* oracles
- we therefore ask: given distinguisher $D$ and view $\nu$ how probable it is that $D$ produced view $\nu$ after interaction with a random element from $\Omega_{Real}$?
- Denote this probability $\Pr[X = \nu]$.

# Probability distributions

- Denote $X$ the probability distribution on views induced by *Real* oracles
- we therefore ask: given distinguisher $D$ and view $\nu$ how probable it is that $D$ produced view $\nu$ after interaction with a random element from $\Omega_{Real}$?
- Denote this probability $\Pr[X = \nu]$.
- Similarly denote $Y$ the probability distribution on views induced by *Random* oracles.

# Obtainable views

- A view $\nu$ is obtainable if $\Pr[X = \nu] > 0$.

# Obtainable views

- A view $\nu$ is obtainable if $\Pr[X = \nu] > 0$.
- From now on we only consider obtainable views, i.e. such $\nu$ that at least one of $\Pr[X = \nu], \Pr[Y = \nu]$ is nonzero.

# Obtainable views

- A view $\nu$ is obtainable if $\Pr[X = \nu] > 0$.
- From now on we only consider obtainable views, i.e. such $\nu$ that at least one of $\Pr[X = \nu], \Pr[Y = \nu]$ is nonzero.
- Therefore $V$ is now the set of all obtainable views

# Statistical Distance

Denote $\Delta(X, Y)$ the statistical distance (also called total variation):

$$\begin{aligned}\Delta(X, Y) &= \frac{1}{2} \sum_{\nu \in V} \left| \Pr[X = \nu] - \Pr[Y = \nu] \right|, \\ &= \sum_{\nu:\ \Pr[Y=\nu] > \Pr[X=\nu]} \Pr[Y = \nu] - \Pr[X = \nu], \\ &= \sum_{\nu:\ \Pr[X=\nu] > \Pr[Y=\nu]} \Pr[X = \nu] - \Pr[Y = \nu].\end{aligned}$$

# Upper-Bounding Advantage

- For fixed deterministic distinguisher $D$ we have:

$$\Delta(X, Y) \geq \mathrm{Adv}(D).$$

# Upper-Bounding Advantage

- For fixed deterministic distinguisher $D$ we have:

$$\Delta(X, Y) \geq \mathrm{Adv}(D).$$

- Since $D$ is deterministic, $D$'s decision is based only on view that it produces during experiment.

# Upper-Bounding Advantage

- For fixed deterministic distinguisher $D$ we have:

$$\Delta(X, Y) \geq \mathrm{Adv}(D).$$

- Since $D$ is deterministic, $D$'s decision is based only on view that it produces during experiment.
- That implies $D$'s advantage can be rewritten as:

$$\Pr\left[D(X) = 1\right] - \Pr\left[D(Y) = 1\right].$$

# The Ratio

- Now let's transform statistical distance into something more useful.

$$\Delta(X, Y) = \sum_{\nu:\ \Pr[Y=\nu]>\Pr[X=\nu]} \Pr[Y = \nu] - \Pr[X = \nu]$$

# The Ratio

- Now let's transform statistical distance into something more useful.

$$\Delta(X,Y) = \sum_{\nu:\ \Pr[Y=\nu]>\Pr[X=\nu]} \Pr[Y=\nu] - \Pr[X=\nu]$$

$$= \sum_{\nu:\ \Pr[Y=\nu]>\Pr[X=\nu]} \Pr[Y=\nu]\left(1 - \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)$$

# The Ratio

- Now let's transform statistical distance into something more useful.

$$\begin{aligned}
\Delta(X,Y) &= \sum_{\nu:\ \Pr[Y=\nu]>\Pr[X=\nu]} \Pr[Y=\nu] - \Pr[X=\nu] \\
&= \sum_{\nu:\ \Pr[Y=\nu]>\Pr[X=\nu]} \Pr[Y=\nu]\left(1-\frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right) \\
&= \sum_{\nu\in V} \Pr[Y=\nu]\left(1-\min\left(1,\frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)\right)
\end{aligned}$$

# The Ratio

- Now let's transform statistical distance into something more useful.

$$
\begin{aligned}
\Delta(X, Y) &= \sum_{\nu:\ \Pr[Y=\nu]>\Pr[X=\nu]} \Pr[Y = \nu] - \Pr[X = \nu] \\
&= \sum_{\nu:\ \Pr[Y=\nu]>\Pr[X=\nu]} \Pr[Y = \nu] \left(1 - \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right) \\
&= \sum_{\nu \in V} \Pr[Y = \nu] \left(1 - \min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right) \\
&= 1 - \mathbb{E}_{\nu \in Y}\left[\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right]
\end{aligned}
$$

# Good and Bad Views

- Let $V = V_1 \cup V_2$ be such that $V_1, V_2$ are disjoint.

# Good and Bad Views

- Let $V = V_1 \cup V_2$ be such that $V_1, V_2$ are disjoint.
- We then examine:

$$\nu \in V_i \Rightarrow \frac{\Pr[X = \nu]}{\Pr[Y = \nu]} \geq 1 - \epsilon_i.$$

# Good and Bad Views

- Let $V = V_1 \cup V_2$ be such that $V_1, V_2$ are disjoint.
- We then examine:

$$\nu \in V_i \Rightarrow \frac{\Pr[X = \nu]}{\Pr[Y = \nu]} \geq 1 - \epsilon_i.$$

- We are free to define classes $V_1, V_2$ as we like.

# Good and Bad Views

- Let $V = V_1 \cup V_2$ be such that $V_1, V_2$ are disjoint.
- We then examine:

$$\nu \in V_i \Rightarrow \frac{\Pr[X = \nu]}{\Pr[Y = \nu]} \geq 1 - \epsilon_i.$$

- We are free to define classes $V_1, V_2$ as we like.
- It is very useful to have one big class for which is the ratio close to one (those would be called "good" iews) and a smaller class for which the ratio is large (call these the "bad" views").

# Epsilons

Then the following holds:

$$1 - \mathbb{E}_{\nu \in Y}\left[\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right]$$

# Epsilons

Then the following holds:

$$1 - \mathbb{E}_{\nu \in Y}\left[\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right]$$
$$= \sum_{\nu \in V} \Pr[Y = \nu]\left(1 - \min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right)$$

# Epsilons

Then the following holds:

$$
\begin{aligned}
&1 - \mathbb{E}_{\nu \in Y}\left[\min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)\right] \\
&= \sum_{\nu \in V} \Pr[Y=\nu]\left(1 - \min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)\right) \\
&= \sum_{\nu \in V_1} \Pr[Y=\nu]\left(1 - \min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)\right) \\
&+ \sum_{\nu \in V_2} \Pr[Y=\nu]\left(1 - \min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)\right)
\end{aligned}
$$

# Epsilons

- And combined with (for $\nu \in V_i$):

$$\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right) \geq 1 - \epsilon_i,$$

# Epsilons

- And combined with (for $\nu \in V_i$):

$$\min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right) \geq 1-\epsilon_i,$$

- we get

$$\sum_{\nu \in V_i} \Pr[Y=\nu]\left(1-\min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)\right) \geq \Pr[Y \in V_i](1-\epsilon_i),$$

# Epsilons

- And combined with (for $\nu \in V_i$):

$$\min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right) \geq 1-\epsilon_i,$$

- we get

$$\sum_{\nu \in V_i} \Pr[Y=\nu]\left(1-\min\left(1, \frac{\Pr[X=\nu]}{\Pr[Y=\nu]}\right)\right) \geq \Pr[Y \in V_i](1-\epsilon_i),$$

- and finally

$$\mathbb{E}_{\nu \in Y}[\ldots] \geq \Pr[Y \in V_1](1-\epsilon_1) + \Pr[Y \in V_2](1-\epsilon_2).$$

# Good and Bad Views part 2

Then we can conclude proposition 5, because:

$$\Delta(X, Y) = 1 - \mathbb{E}_{\nu \in Y}\left[\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right],$$

# Good and Bad Views part 2

Then we can conclude proposition 5, because:

$$\begin{aligned}\Delta(X, Y) &= 1 - \mathbb{E}_{\nu \in Y}\left[\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right], \\ &\geq 1 - \left(\Pr[Y \in V_1](1 - \epsilon_1) + \Pr[Y \in V_2](1 - \epsilon_2)\right),\end{aligned}$$

# Good and Bad Views part 2

Then we can conclude proposition 5, because:

$$\begin{aligned}\Delta(X, Y) &= 1 - \mathbb{E}_{\nu \in Y}\left[\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right], \\ &\geq 1 - \left(\Pr[Y \in V_1](1 - \epsilon_1) + \Pr[Y \in V_2](1 - \epsilon_2)\right), \\ &= \Pr[Y \in V_1]\,\epsilon_1 + \Pr[Y \in V_2]\,\epsilon_2.\end{aligned}$$

# The Main Result

- If we now conclude that $V_1$ is "large" therefore $\Pr[Y \in V_1]$ is approx 1 and that $\epsilon_2$ is also close to one we immediately obtain the main result:

$$\mathrm{Adv}(D) \leq \Delta(X, Y) \leq \epsilon_1 + \Pr[Y \in V_2].$$

# The Main Result

- If we now conclude that $V_1$ is "large" therefore $\Pr[Y \in V_1]$ is approx 1 and that $\epsilon_2$ is also close to one we immediately obtain the main result:

$$\mathrm{Adv}(D) \leq \Delta(X, Y) \leq \epsilon_1 + \Pr[Y \in V_2].$$

- It translates to: Advantage is upper-bounded by probability of "bad" views in ideal world plus the distance between the ratio and one.

# Lower Bounding the Ratio

# View Compatibility

- We call view $\nu$ compatible with oracle $R$ if for any $(P, C) \in \nu$ it holds that $R(P) = C$.

# View Compatibility

- We call view $\nu$ compatible with oracle $R$ if for any $(P, C) \in \nu$ it holds that $R(P) = C$.
- Given view $\nu$ denote $\text{comp}_\Omega(\nu)$ set of oracles of $\Omega$ that are compatible with view $\nu$.

# View Compatibility

- We call view $\nu$ compatible with oracle $R$ if for any $(P, C) \in \nu$ it holds that $R(P) = C$.
- Given view $\nu$ denote $\text{comp}_\Omega(\nu)$ set of oracles of $\Omega$ that are compatible with view $\nu$.
- This does not imply that if $\nu$ is compatible with $R$ that $D$ produces view $\nu$ when interacting with $R$.

# View Compatibility

- We call view $\nu$ compatible with oracle $R$ if for any $(P, C) \in \nu$ it holds that $R(P) = C$.
- Given view $\nu$ denote $\text{comp}_\Omega(\nu)$ set of oracles of $\Omega$ that are compatible with view $\nu$.
- This does not imply that if $\nu$ is compatible with $R$ that $D$ produces view $\nu$ when interacting with $R$.
- However it implies that when $D$ produced $\nu$ compatible with $R$ then when $D$ interacts with $R$ it produces $\nu$ as well.

# View Compatibility - Illustration

- Let $D$ interact with oracle $R_1$ producing view $\nu = \{(P_i, C_i) | i \leq q\}$.

# View Compatibility - Illustration

- Let $D$ interact with oracle $R_1$ producing view $\nu = \{(P_i, C_i) | i \leq q\}$.
- Say $\nu$ is compatible with $R_2$ then let $D$ interact with $R_2$

# View Compatibility - Illustration

- Let $D$ interact with oracle $R_1$ producing view $\nu = \{(P_i, C_i) | i \leq q\}$.
- Say $\nu$ is compatible with $R_2$ then let $D$ interact with $R_2$
- The first query $D$ makes is the same as when interacting with $R_1$

# View Compatibility - Illustration

- Let $D$ interact with oracle $R_1$ producing view $\nu = \{(P_i, C_i) | i \leq q\}$.
- Say $\nu$ is compatible with $R_2$ then let $D$ interact with $R_2$
- The first query $D$ makes is the same as when interacting with $R_1$
- The response from $R_2$ is also the same, since it is compatible with $\nu$

# View Compatibility - Illustration

- Let $D$ interact with oracle $R_1$ producing view $\nu = \{(P_i, C_i) | i \leq q\}$.
- Say $\nu$ is compatible with $R_2$ then let $D$ interact with $R_2$
- The first query $D$ makes is the same as when interacting with $R_1$
- The response from $R_2$ is also the same, since it is compatible with $\nu$
- By induction $D$ produces the same view when interacting with $R_2$

# Central Insight

Given view $\nu$:

$$\Pr[X = \nu] = \frac{\left|\mathrm{comp}_{\Omega_{Real}}(\nu)\right|}{|\Omega_{Real}|} \text{ and } \Pr[Y = \nu] = \frac{\left|\mathrm{comp}_{\Omega_{Random}}(\nu)\right|}{|\Omega_{Random}|}.$$

# Consequences

Right from the definition of compatibility and the central insight we get:

1. The order in which queries appear in a view $\nu$ does not affect the probability of $\nu$ occuring, only the set of queries does.

# Consequences

Right from the definition of compatibility and the central insight we get:

1. The order in which queries appear in a view $\nu$ does not affect the probability of $\nu$ occuring, only the set of queries does.
2. If two different deterministic distinguishers can obtain $\nu$ with nonzero probability they would obtain $\nu$ with equal probability (even if the order of queries differs).

# Reformulate the ratio

We can therefore transform the ratio:

$$\frac{\Pr[X = \nu]}{\Pr[Y = \nu]} = \frac{|\Omega_{Random}| \left|\text{comp}_{\Omega_{Real}}\right|}{|\Omega_{Real}| \left|\text{comp}_{\Omega_{Random}}\right|}$$

Thank you for your attention.
Do you have any questions?