

Perfect One-Way Hashing and Point Functions Obfuscation

based on CANETTI 97

NIR BITANSKY

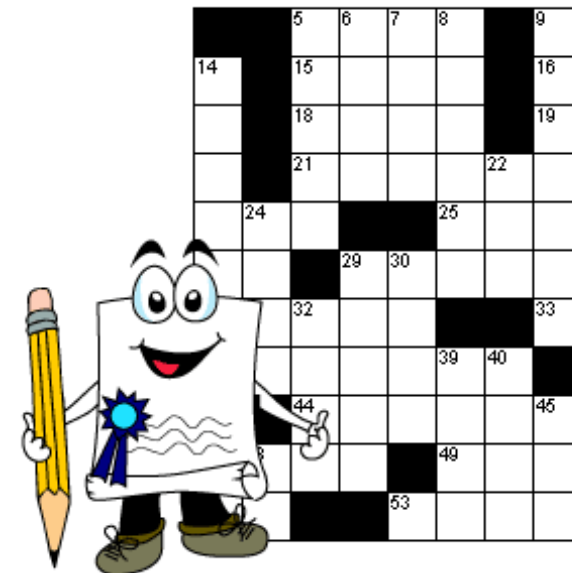
June 15, 2009

A motivating example (CANETTI 97)

- Alice publishes a puzzle in the local newspaper.
- He would like to add a short string which will allow solvers to verify their solution.
- Readers who didn't solve it should gain no helpful information from this string.



(a) Alice



(b) Puzzle

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Any Suggestions?

- How about using a [one way function](#)?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Any Suggestions?

- How about using a **one way function**?
Might leak some of the information on the solution.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Any Suggestions?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- How about using a **one way function**?
Might leak some of the information on the solution.
- How about a **commitment** for the solution?

Any Suggestions?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- How about using a **one way function**?
Might leak some of the information on the solution.
- How about a **commitment** for the solution?
Requires the committer participation in the open phase (or alternatively giving the commitment coins).

Any Suggestions?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- How about using a **one way function**?
Might leak some of the information on the solution.
- How about a **commitment** for the solution?
Requires the committer participation in the open phase (or alternatively giving the commitment coins).
- Can we use some kind of **hashing family**?

Any Suggestions?

- How about using a **one way function**?
Might leak some of the information on the solution.
- How about a **commitment** for the solution?
Requires the committer participation in the open phase (or alternatively giving the commitment coins).
- Can we use some kind of **hashing family**?
Must require certain properties.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Any Suggestions?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- How about using a **one way function**?
Might leak some of the information on the solution.
- How about a **commitment** for the solution?
Requires the committer participation in the open phase (or alternatively giving the commitment coins).
- Can we use some kind of **hashing family**?
Must require certain properties.
- Say we had a **Random Oracle** ?

Any Suggestions?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- How about using a **one way function**?
Might leak some of the information on the solution.
- How about a **commitment** for the solution?
Requires the committer participation in the open phase (or alternatively giving the commitment coins).
- Can we use some kind of **hashing family**?
Must require certain properties.
- Say we had a **Random Oracle** ? Simple solution.

So what do we need?

- Recall our motivating example. **Ideally**, we would like allow the solver to call Alice (or an Oracle), suggest a solution and get a right/wrong answer.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

So what do we need?

- Recall our motivating example. **Ideally**, we would like allow the solver to call Alice (or an Oracle), suggest a solution and get a right/wrong answer.
- Informally, given a (secret) value $x \in D$, we would like to hash it to a new value $\mathcal{H}(x)$ achieving two essential properties:
 - Allow efficient **verification**:
$$\exists V \text{ s.t. } V(y, \mathcal{H}(x)) = \begin{cases} 1 & y = x \\ 0 & o.w. \end{cases}$$
 - **Oracle security** - having $\mathcal{H}(x)$, allows nothing more than an exhaustive search over the entire domain (using the verification algorithm).

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Obfuscation of Point Functions

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- In other words, we would like to construct an **obfuscator** for the family of point functions.

Obfuscation of Point Functions

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- In other words, we would like to construct an **obfuscator** for the family of point functions.
- A **point function** $I_x : \{0, 1\}^* \rightarrow \{0, 1\}$ outputs 1 on input x and 0 on any other input (a.k.a δ -functions).
- We can view our primitive \mathcal{H} as an obfuscator which takes a point-function I_x (or a TM/circuit in which x is explicit), and returns an obfuscation, \mathcal{O}_x given by $\mathcal{O}_x(y) = V(y, \mathcal{H}(x))$.
 - \mathcal{O}_x has the same functionality as I_x .
 - Has the virtual black-box property.
 - Polynomial slow down (efficiency).

Formally Defining Security

Definition 0: *Oracle Simulatability - Virtual Black Box.*

For any poly adversary A there is a poly simulator S such that for any predicate P and any $x \in D$:

$$|\Pr[A(\mathcal{H}(x)) = P(x)] - \Pr[S^{I_x} = P(x)]| \leq \text{neg}(n)$$

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Formally Defining Security

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Definition 0: *Oracle Simulatability - Virtual Black Box.*

For any poly adversary A there is a poly simulator S such that for any predicate P and any $x \in D$:

$$|\Pr[A(\mathcal{H}(x)) = P(x)] - \Pr[S^{I_x} = P(x)]| \leq \text{neg}(n)$$

Remarks:

- Same definition we saw last week.
- To satisfy this we have to let \mathcal{H} be probabilistic (o.w. the adversary learns for example $P(x) = \mathcal{H}_1(x)$). From now on we'll write $\mathcal{H}(x, r)$, $r \in R_n$.
- In fact we'll only achieve a weaker variant.

Defining Security cont'

Definition 1: *Weaker Virtual Black Box*.

For any poly adversary A and any polynomial q there is a poly **non-uniform** simulator $S = S_q$ such that for any poly predicate P and any $x \in D$:

$$\left| \Pr_{A,r} [A(\mathcal{H}(x, r)) = P(x)] - \Pr_S [S^{I_x} = P(x)] \right| \leq \frac{1}{q(n)}$$

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Defining Security cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Definition 1: *Weaker Virtual Black Box*.

For any poly adversary A and any polynomial q there is a poly **non-uniform** simulator $S = S_q$ such that for any poly predicate P and any $x \in D$:

$$\left| \Pr_{A,r}[A(\mathcal{H}(x, r)) = P(x)] - \Pr_S[S^{I_x} = P(x)] \right| \leq \frac{1}{q(n)}$$

- The simulator is allowed to depend on q (the quality of the approximation). BGI 01 rules out general obfuscation also in this case.
- Non-symmetric definition, the simulator is allowed some advise (WEE 05 - required for BB simulators)

Alternative Definition

Definition 2 (attempt 1): *Distributional Indistinguishability*

For any poly A and any distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Alternative Definition

Definition 2 (attempt 1): *Distributional Indistinguishability*

For any poly A and any distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

Does this make any sense?

- What if A just outputs its input?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Alternative Definition

Definition 2 (attempt 1): *Distributional Indistinguishability*

For any poly A and any distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

Does this make any sense?

- What if A just outputs its input? We can distinguish easily using the verification algorithm.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Alternative Definition cont'

Definition 2 (attempt 2): *Distributional Indistinguishability*

For any **binary** poly adversary A and any distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Alternative Definition cont'

Definition 2 (attempt 2): *Distributional Indistinguishability*

For any **binary** poly adversary A and any distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

How about now ?

- What if the support of X_n is small?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Alternative Definition cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Definition 2 (attempt 2): *Distributional Indistinguishability*

For any **binary** poly adversary A and any distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

How about now ?

- What if the support of X_n is small? A can use the verification algorithm to find the hashed value and output its first bit.

Alternative Definitions cont'

Definition: *Well Spread Distribution Ensemble*

Any element has a neg. prob. (super-log min-entropy):

$$\max_x \Pr[X = x] = \text{neg}(n)$$

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Alternative Definitions cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)

Construction

The (r, r^x)

Construction cont'

The (r, r^x)

Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Definition: *Well Spread Distribution Ensemble*

Any element has a neg. prob. (super-log min-entropy):

$$\max_x \Pr[X = x] = \text{neg}(n)$$

Definition 2: *Distributional Indistinguishability*

For any **binary** poly adversary A and any **well spread** distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

Alternative Definitions cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)

Construction

The (r, r^x)

Construction cont'

The (r, r^x)

Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Definition: *Well Spread Distribution Ensemble*

Any element has a neg. prob. (super-log min-entropy):

$$\max_x \Pr[X = x] = \text{neg}(n)$$

Definition 2: *Distributional Indistinguishability*

For any **binary** poly adversary A and any **well spread** distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

Yet Another Definition

Definition 3: *Oracle Indistinguishability*

For any poly distinguisher D and any polynomial p there exist a poly size family $\mathcal{L}_{D,p} = \{L_n\}$ such that for any $x, y \notin L_n$

$$\Pr_r[D(\mathcal{H}(x, r)) = 1] - \Pr_r[D(\mathcal{H}(y, r)) = 1] < \frac{1}{p(n)}$$

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Yet Another Definition

Definition 3: *Oracle Indistinguishability*

For any poly distinguisher D and any polynomial p there exist a poly size family $\mathcal{L}_{D,p} = \{L_n\}$ such that for any $x, y \notin L_n$

$$\Pr_r[D(\mathcal{H}(x, r)) = 1] - \Pr_r[D(\mathcal{H}(y, r)) = 1] < \frac{1}{p(n)}$$

Think of L_n as the set of bad inputs (relatively to D, p)

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Which One Do You Prefer?

- The last definition seems rather convenient. We'll see for example it easily implies Oracle Simulatability (Virtual Black Box).

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Which One Do You Prefer?

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- The last definition seems rather convenient. We'll see for example it easily implies Oracle Simulatability (Virtual Black Box).
- It turns out:

Theorem (CANETTI 97):

All three definitions are equivalent.

The (r, r^x) Construction

- Before proving the equivalence, let us demonstrate a construction which utilizes the DI definition.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

The (r, r^x) Construction

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Before proving the equivalence, let us demonstrate a construction which utilizes the DI definition.
- Let $p = 2q + 1$ be an n -bit safe¹ prime, where q is also a prime.
- Let Q be the order q subgroup of \mathbb{Z}_p^* . Our randomness will be drawn from $R = Q - \{1\}$ (note that any $g \in R$ generates Q).
- Our input domain will be $\mathbb{Z}_q^* = \{1, \dots, q - 1\}$.
- For $x \in \mathbb{Z}_q^*$ we pick a random $r \in R$ and map:

$$x \xrightarrow{\mathcal{H}} (r, r^x)$$

¹Safe means $p - 1$ has a large prime factor, which prevents known discrete log attacks such as Pohlig-Hellman.

The (r, r^x) Construction cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

$$x \xrightarrow{\mathcal{H}} (r, r^x)$$

- Easy verification. $V(x, (a, b)) = 1$ iff $a^x \equiv_p b$.

The (r, r^x) Construction cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

$$x \xrightarrow{\mathcal{H}} (r, r^x)$$

- Easy verification. $V(x, (a, b)) = 1$ iff $a^x \equiv_p b$.
- Public randomness.

The (r, r^x) Construction cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

$$x \xrightarrow{\mathcal{H}} (r, r^x)$$

- Easy verification. $V(x, (a, b)) = 1$ iff $a^x \equiv_p b$.
- Public randomness.
- Why is this secure?

The (r, r^x) Construction cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

$$x \xrightarrow{\mathcal{H}} (r, r^x)$$

- Easy verification. $V(x, (a, b)) = 1$ iff $a^x \equiv_p b$.

- Public randomness.

- Why is this secure?

DDH: Given $g \in R$, and independently chosen $a, b, c \in U(\mathbb{Z}_q^*)$:

$$(g^a, g^b, g^c) \approx_c (g^a, g^b, g^{ab})$$

- We will need a stronger assumption.

The (r, r^x) Construction cont'

Stronger DDH: Let $\{X_q\}$ be a w.s. distribution ens. with domains \mathbb{Z}_q^* . Given $g \in R$, and independently chosen $a \in X_q(\mathbb{Z}_q^*)$, $b, c \in U(\mathbb{Z}_q^*)$:

$$(g^a, g^b, g^c) \approx_c (g^a, g^b, g^{ab})$$

- This assumption obviously implies the previous one (taking $X = U$). Has not been refuted so far.
- Let us show that under this assumption the (r, r^x) construction is secure w.r.t the DI definition.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

DI (reminder): For any binary poly adversary A and any well spread distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

DI (reminder): For any binary poly adversary A and any well spread distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

- Assume there exist a w.s. distribution ens. $\{X_q\}$, a distinguisher D , and a binary adversary A s.t. :

$$\Pr_{x,r}[D(x, A(r, r^x)) = 1] - \Pr_{x,y,r}[D(x, A(r, r^y)) = 1] \geq \delta(n) \quad (1)$$

For infinitely many n 's.

- For a given $g \in Q - \{1\}$ we'll construct A' which distinguishes g^a, g^b, g^c from g^a, g^b, g^{ab} with advantage $\Omega(\delta)$.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

Proof - First Step

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- For $x \in \mathbb{Z}_q^*$, define $P_x = \Pr_r[A(r, r^x) = 1]$.
- Given fact (1):

$$\Pr_{x,r}[D(x, A(r, r^x)) = 1] - \Pr_{x,y,r}[D(x, A(r, r^y)) = 1] \geq \delta$$

We can show that P_x varies significantly as x varies.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- For $x \in \mathbb{Z}_q^*$, define $P_x = \Pr_r[A(r, r^x) = 1]$.
- Given fact (1):

$$\Pr_{x,r}[D(x, A(r, r^x)) = 1] - \Pr_{x,y,r}[D(x, A(r, r^y)) = 1] \geq \delta$$

We can show that P_x varies significantly as x varies.

- Claim: $\Pr_{x,y \in X}[|P_x - P_y| > \frac{\delta}{4}] > \frac{\delta}{4}$. We will denote this event by $I_{x,y}$.

Proof: Consider an experiment where b is a random bit and $x_0, x_1 \in X, r \in R$ are independently drawn from their distributions. The experiment succeeds if:

$$^2 D(x_1, A(r, r^{x_b})) = b$$

²sense - D is more likely to output 1 when both are the same.

Proof - First Step cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?
Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

■ Fact (1):

$$\Pr_{x,r}[D(x, A(r, r^x)) = 1] - \Pr_{x,y,r}[D(x, A(r, r^y)) = 1] \geq \delta$$

- Fact (1) implies $\Pr[succ] \geq \frac{1}{2} + \frac{\delta}{2}$ (conditioning on b).
- On the other hand:

$$\Pr[succ] \leq \underbrace{\Pr[succ | I_{x_0, x_1}^c]}_* + \Pr[I_{x_0, x_1}] \leq \frac{1}{2} + \frac{\delta}{8} + \Pr[I]$$

- (*)Note that given I_{x_0, x_1}^c we have $|P_{x_0} - P_{x_1}| \leq \delta/4$.
Implying that the statistical distance between $A(r, r^{x_1}), A(r, r^{x_0})$ is at most $\delta/4$ and hence $D(x_1, .)$ distinguish w.p. at most $1/2 + \delta/8$.

Proof - First Step cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

■ We have seen that $\Pr_{x,y \in X} [|P_x - P_y| > \frac{\delta}{4}] > \frac{\delta}{4}$.

■ This also implies that $\Pr_{x \in X} [|P_x - P_{y_0}| > \frac{\delta}{8}] > \frac{\delta}{12}$
for any fixed y_0 .

■ **Proof:** If this is not the case then
 $\Pr_{x \in X} [|P_x - P_{y_0}| \leq \frac{\delta}{8}] \geq 1 - \frac{\delta}{12}$ and hence:

$$\Pr_{x,y \in X} [|P_x - P_y| \leq \delta/4] \geq (1 - \delta/12)^2 \geq 1 - \delta/6$$

Contradicting our assumption.

Proof - Distinguishing SDDH

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Given (g^a, g^b, g^z) , distinguish $z = ab$ from $z \in_R \mathbb{Z}_q^*$.

Proof - Distinguishing SDDH

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Given (g^a, g^b, g^z) , distinguish $z = ab$ from $z \in_R \mathbb{Z}_q^*$.
- Let $w = z \cdot b^{-1} \pmod q$. Note that if $z = ab$ then $w = a$. On the other hand if $z \in_R \mathbb{Z}_q^*$ then so is w .
- We will try to estimate P_a, P_w and answer $z = a$ in case they are close and $z = w$ if they're far.

Proof - Distinguishing SDDH

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Given (g^a, g^b, g^z) , distinguish $z = ab$ from $z \in_R \mathbb{Z}_q^*$.
- Let $w = z \cdot b^{-1} \pmod q$. Note that if $z = ab$ then $w = a$. On the other hand if $z \in_R \mathbb{Z}_q^*$ then so is w .
- We will try to estimate P_a, P_w and answer $z = a$ in case they are close and $z = w$ if they're far.
- To estimate P_a randomly pick $r_1, \dots, r_\ell \in_R \mathbb{Z}_q^*$, and set $\tilde{P}_a = \frac{1}{\ell} \sum_{i \in [\ell]} A(g^{r_i}, (g^a)^{r_i})$. Note that g^{r_i} is a random generator of Q , hence $\mathbb{E} \tilde{P}_a = P_a$.
- To estimate P_w , set $\tilde{P}_w = \frac{1}{\ell} \sum_{i \in [\ell]} A((g^b)^{r_i}, (g^z)^{r_i})$.
- If $|\tilde{P}_a - \tilde{P}_w| < \delta/24$ output $z = ab$, o.w. $z \in_R \mathbb{Z}_q^*$ (δ is given as advice).

Proof - Distinguishing SDDH finale

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- We choose the number of samples to be $\ell = \frac{n}{\delta^2}$.
- Using Chernoff yields that in case $w = a$ we'll be wrong with negligible probability.
- On the other hand as we saw for any fixed w (and hence also for $w \in_R \mathbb{Z}_q^*$) $|P_w - P_a| > \delta/12$ with noticeable prob. $\Omega(\delta)$. Hence in this case we'll be correct with noticeable probability (Chernoff again).

Equivalence of Definitions - Proof Sketch

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- **DI**: For any binary poly adversary A and any w.s. distribution ensemble $\{X_n\}$:

$$x, A(\mathcal{H}(x, r)) \approx_c x, A(\mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

- **OI**: For any binary poly D and any poly p there is a poly size family $\mathcal{L}_{D,p} = \{L_n\}$ such that for any $x, y \notin L_n$

$$\Pr_r [D(\mathcal{H}(x, r)) = 1] - \Pr_r [D(\mathcal{H}(y, r)) = 1] < \frac{1}{p(n)}$$

- **OS**: For any poly adv. A and any poly q there is a poly n.u. $S = S_q$ s.t. for any predicate P and any distribution X :

$$\left| \Pr_{x \in X, r \in R} [A(\mathcal{H}(x, r)) = P(x)] - \Pr_{x \in X} [S^{I_x} = P(x)] \right| \leq 1/q(n)$$

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Let A be an adversary and q a polynomial. To construct S , consider the set of bad inputs $L = L_{A,q}$ (which exists by the OI definition).
- Given oracle access to I_x , S first checks whether $x \in L$ (by running all of them through the oracle).
- In case $x \in L$, S finds it and can run A on $\mathcal{H}(x, r)$ (with a random r).
- Otherwise, S picks a random (or fixed) $y \notin L$ and runs A on $\mathcal{H}(y, r)$.
- Security follows easily from the OI property.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Assume towards contradiction the existence of a w.s. distribution ens. $\{X\}$, a distinguisher D and a binary A s.t.:

$$\Pr_{x,r}[D(x, A(\mathcal{H}(x, r))) = 1] - \Pr_{x,y,r}[D(x, A(\mathcal{H}(y, r))) = 1] \geq \delta \quad (1)$$

- We'll construct a distribution X' and a predicate B s.t. for any poly simulator S :

$$\Pr_{x \in X', r \in R}[A(\mathcal{H}(x, r)) = B(x)] - \Pr_{x \in X'}[S^{I_x} = B(x)] \geq \Omega(\delta)$$

- Recall that given (1) we defined $P_x = \Pr_r[A(r, r^x) = 1]$ and showed that: $\Pr_{x_0, x_1 \in X}[|P_{x_1} - P_{x_0}| > \frac{\delta}{4}] > \frac{\delta}{4}$.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

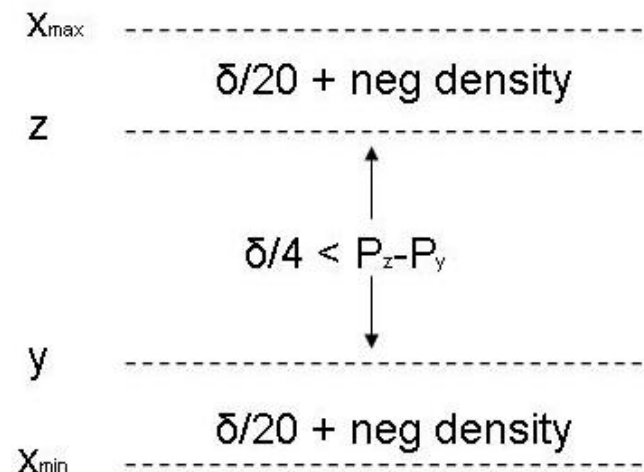
- Claim:** given $\Pr_{x,y \in X} [|P_{x_1} - P_{x_0}| > \frac{\delta}{4}] > \frac{\delta}{4}$, there exist two sets $Y, Z \subset \text{supp}(X)$ s.t.

$$\forall y \in Y, z \in Z : P_z - P_y \geq \delta/4 \quad (1)$$

$$\Pr_{x \in X} [x \in Z] \approx \Pr_{x \in X} [x \in Y] \approx \delta/20 \quad (2)$$

Where \approx means equal up to a negligible term.

- O.W.** $\Pr_{x,y} [|P_x - P_y| < \delta/4] \geq (1 - \delta/10)^2 \geq 1 - \delta/5$



A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Having $Y, Z \subset \text{supp}(X)$ s.t.

$$\forall y \in Y, z \in Z : P_z - P_y \geq \delta/4 \quad (1)$$

$$\Pr_{x \in X} [x \in Z] \approx \Pr_{x \in X} [x \in Y] \approx \delta/20 \quad (2)$$

- We now define our distribution $X' = X|Y \cup Z$.

- And our predicate $B(x) = \begin{cases} 1 & x \in Z \\ 0 & x \in Y \end{cases}$

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- $X' = X|Y \cup Z$ is still a w.s. distribution. Hence, for $x \in_R X'$ any poly S queries I_x on x with negligible probability.
- As long as S doesn't query x , it outputs $B(x)$ w.p. at most $1/2$.
- Overall, $\Pr[S^{I_x} = B(x)] \leq 1/2 + \text{neg}(n)$.
- On the other hand:

$$\Pr[A(\mathcal{H}(x, r)) = B(x)] \approx \frac{1}{2} [P_{x|x \in Z} + 1 - P_{x|x \in Y}] \geq 1/2 + \delta/8$$

- This contradicts the OS property.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?
Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Assume towards contradiction the existence of an adversary A and a poly p s.t. for any poly size family $\mathcal{L} = \{L_n\}$ there are infinitely many values n for which there exist $x, y \notin L_n$ s.t.:

$$\Pr_r[A(\mathcal{H}(x, r)) = 1] - \Pr_r[A(\mathcal{H}(y, r)) = 1] \geq 1/p(n)$$

- We will construct a distinguisher D and a w.s. distribution ensemble $\mathcal{X} = \{X_n\}$ s.t.:

$$\Pr_{x,r}[D(x, A(\mathcal{H}(x, r)) = 1)] - \Pr_{x,y,r}[D(x, A(\mathcal{H}(y, r)) = 1)] \geq \frac{\Omega(1)}{p(n)}$$

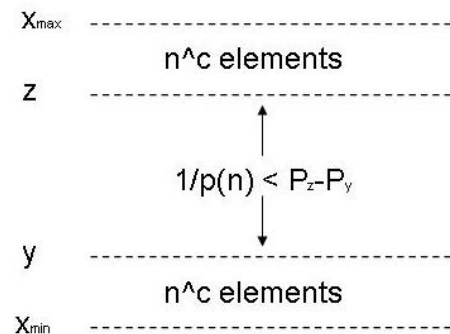
Where $x, y \in_R X_n$ and $r \in_R R$.

- A motivating example (CANETTI 97)
- Any Suggestions?
- So what do we need?
- Obfuscation of Point Functions
- Formally Defining Security
- Defining Security cont'
- Alternative Definition
- Alternative Definition cont'
- Alternative Definitions cont'
- Yet Another Definition
- Which One Do You Prefer?
- The (r, r^x) Construction
- The (r, r^x) Construction cont'
- The (r, r^x) Construction cont'
- Proof
- Proof - First Step
- Proof - First Step cont'
- Proof - First Step cont'
- Proof - Distinguishing

- For a fixed $c \in \mathbb{N}$ and security parameter n define a set of n^c elements, $L_n^{(c)} = Z_n^{(c)} \cup Y_n^{(c)}$ as follows.
- $Z_n^{(c)}$ is the set of $\lceil \frac{n^c}{2} \rceil$ elements z with maximal P_z .
- $Y_n^{(c)}$ is the set of $\lfloor \frac{n^c}{2} \rfloor$ elements y with minimal P_y .
- Note that by our assumption for any fixed c there are infinitely many n 's s.t.:

$$\forall z \in Z_n^{(c)}, y \in Y_n^{(c)} : P_z - P_y > 1/p(n)$$

O.W. $\{L_n^{(c)}\}$ is a poly family covering all bad values.



A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- **Fact 1:** for any fixed c there are infinitely many n s.t.:

$$\forall z \in Z_n^{(c)}, y \in Y_n^{(c)} : P_z - P_y > 1/p(n) \quad (1)$$

- For any n let c_n be the maximal c s.t. (1) holds with respect to n and $L_n^{(c)}$ (note that for a fixed n at some point n^c covers the entire domain).
- We define $\mathcal{X} = \{X_n\}$ as follows³:

- If $c_n > \max_{i < n} c_i$ then $X_n = U(L_n^{(c_n)})$.

- O.W. it is U on an arbitrary set of size $n \binom{\max_{i < n} c_i}{i < n}$.

³The first condition assures "growth" and the second "monotonicity".

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- \mathcal{X} is a well spread distribution ensemble.
- Indeed, fact (1) and the construction of \mathcal{X} imply that for any c and all sufficiently large n : $|X_n| > n^c$ (the first "if" is satisfied infinit. many times).
- Moreover, for infinitely many n 's $X_n = Y_n \cup Z_n$, where $|Z_n| \approx |Y_n|$ and:

$$\forall z \in Z_n, y \in Y_n : P_z - P_y > 1/p(n)$$

- We can now construct D s.t.:

$$\Pr_{x,r}[D(x, A(\mathcal{H}(x, r)) = 1] - \Pr_{x,y,r}[D(x, A(\mathcal{H}(y, r)) = 1] \geq \frac{\Omega(1)}{p(n)}$$

Where $x, y \in_R X_n$ and $r \in_R R$.

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Upon input x , $b = A(\mathcal{H}(?, r))$, D first estimates P_x using $np^2(n)$ samples and decides whether $P_x > med(X_n)$ (the median is given as advice).
- If $P_x > med$ output b otherwise o.p. $1 - b$.
Informally, 1 represents "same x " answer.
- When P_x is large A is likely to output 1. If b is consistent we o.p. 1 o.w. we guess it's "not the same x " and o.p. 0.
- To conclude the proof condition on the distinguisher deciding correctly its relation to the median (by the properties of our distribution, one can use Chernoff to check that it decides wrongly is negligible).

A Note About Auxiliary Inputs

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- The definitions we've covered so far do not deal with scenarios in which the adversary knows some a-priori information regarding the input and is not allowed to learn any extra information.
- Trying to incorporate aux info, it looks like each definition has its own subtleties.
- Consider the DI definition. We will define Strong DI.
- **SDI**: For any binary poly adversary A , any w.s. distribution ensemble $\{X_n\}$ and any function z :

$$x, A(z(x), \mathcal{H}(x, r)) \approx_c x, A(z(x), \mathcal{H}(y, r))$$

Where $r \in_R R_n$ and $x, y \in_R X_n$ (independently).

A Note About Auxiliary Inputs

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- **SDI**: For any binary poly adversary A , any w.s. distribution ensemble $\{X_n\}$ and any function z :

$$x, A(z(x), \mathcal{H}(x, r)) \approx_c x, A(z(x), \mathcal{H}(y, r))$$

- Makes sense?

A Note About Auxiliary Inputs

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- **SDI**: For any binary poly adversary A , any w.s. distribution ensemble $\{X_n\}$ and any function z :

$$x, A(z(x), \mathcal{H}(x, r)) \approx_c x, A(z(x), \mathcal{H}(y, r))$$

- Makes sense? not really. It might be that $z(x) = x$. We will restrict $z(x)$ to uninvertible functions, i.e. $z(x)$ does not allow efficiently extracting x^4 .
- Considering the simulation based def. this issue seems to resolve itself (S will also get $z(x)$).
- It can be shown that under a very strong DDH variant, the r, r^x construction satisfies SDI (is this secure with respect to the OS def.) .

Simple Applications

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- BR suggested the following encryption scheme and showed it is semantically secure in the RO model (assuming the existence of TDP).
- Given a TDP $\mathcal{F} = F_n$, the public key is $f \in_R F_n$ and the private key is f^{-1} (the trapdoor).
- To encrypt m choose a random s and output $f(s), R(s) \oplus m$. Decryption is straight forward.
- Instead of using a RO use a perfect OW hash with public randomness (like r, r^x).
- To encrypt m choose random s, r and output $f(s), r, \mathcal{H}(s, r) \oplus m$.
- Security requires something weaker than SDI: $A(z(x), \mathcal{H}(x, r)) \approx_c A(z(x), \mathcal{H}(y, r))$ rather than $x, A(z(x), \mathcal{H}(x, r)) \approx_c x, A(z(x), \mathcal{H}(y, r))$

More Simple Applications

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Another application is "content concealing" signatures.
- Say you want to sign m in a way that the signature reveals no information about m (to someone who doesn't have m).
- Instead of signing m sign $c = \mathcal{H}(m, r)$ (and give both c and the signature).

Another Construction (WEE 05)

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Based on another (strong!) assumption.
- **Assumption:** There exists an eff. comp. permutation family $\{\pi_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$ s.t. for any poly family of circuits $\{A_n\}$ there is a poly q s.t.:

$$\Pr_{x \in U_n} [A_n(\pi(x)) = x] \leq q(n)/2^n$$

- Leaving the essential eff. comp. requirement aside, one can use a probabilistic argument to show the existence of strong such strong *OWP*.
- They do show that if public coin point obfs. exist, then there also exist *OWP* (but in a weaker sense)

The Construction

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?
Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition
Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition
Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- We construct:

$$\mathcal{H} : \underbrace{\{0, 1\}^n}_{\text{domain}} \times \underbrace{\{0, 1\}^{3n^2}}_{\text{randomness}} \rightarrow \{0, 1\}^{3n^2+3n}$$

- Given a permutation $\pi : \{0, 1\}^n \rightarrow \{0, 1\}^n$:

$$\mathcal{H}(x, r_1, \dots, r_{3n}) = r_1, \dots, r_{3n}, \langle x, r_1 \rangle, \langle \pi_x, r_2 \rangle \dots \langle \pi_x^{3n-1}, r_{3n} \rangle$$

- Where π_x denotes $\pi(x)$ and $\langle \cdot, \cdot \rangle$ is scalar product over \mathbb{Z}_2 .

The Construction cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

$$\mathcal{H}(x, r_1, \dots, r_{3n}) = r_1, \dots, r_{3n}, \langle x, r_1 \rangle, \langle \pi_x, r_2 \rangle \dots \langle \pi_x^{3n-1}, r_{3n} \rangle$$

- **Def 1:** π is a (Q, T) – *OWP* if any circuit of size at most $Q(n)$ inverts π on at most $T(n)$ values.
- **Def 2:** A point obfuscator, \mathcal{O} , is (k, m, ϵ) – *VBB* if for any circuit A of size at most m there is a circuit S of size at most k s.t. for any $x \in \{0, 1\}^n$:

$$\Pr[A(\mathcal{O}_x) = 1] - \Pr[S^{I_x} = 1] \leq \epsilon$$

*The parameters T, Q, k, m should be thought of as poly's.

- **Claim:** If π is a $(m \cdot \text{poly}(n, \frac{1}{\epsilon}), \epsilon k / 16n)$ – *OWP* Then \mathcal{H} can be used to construct a $(k \cdot \text{poly}(n), m, \epsilon)$ – *VBB* point obfuscator.

Sketch of Proof

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

$$\mathcal{H}(x, r_1, \dots, r_{3n}) = r_1, \dots, r_{3n}, \langle x, r_1 \rangle, \langle \pi_x, r_2 \rangle \dots \langle \pi_x^{3n-1}, r_{3n} \rangle$$

- The obfus. of x includes $\mathcal{H}(x, R)$. On input y it checks whether $\mathcal{H}(y, R) = \mathcal{H}(x, R)$ (R is public).
- The functionality here is approximate rather than accurate. That is $\Pr_R[\exists y \neq x : \mathcal{H}(x, R) = \mathcal{H}(y, R)] = \frac{1}{2^n}$.
- Indeed, $\Pr[\forall j \in [3n] : \langle \pi_x^{j-1}, r_j \rangle = \langle \pi_y^{j-1}, r_j \rangle] = 1/2^{3n}$ and union bound over all pairs x, y yields the above.

Sketch of Proof cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

$$\mathcal{H}(x, r_1, \dots, r_{3n}) = r_1, \dots, r_{3n}, \langle x, r_1 \rangle, \langle \pi_x, r_2 \rangle \dots \langle \pi_x^{3n-1}, r_{3n} \rangle$$

- For an adversary, A , of size m . We define:

$$L_n = \{x : |\Pr_R[A(\mathcal{H}(x, R)) = 1] - \Pr[A(U_{3n^2+3n}) = 1]| \geq \epsilon\}$$

- L_n is the set of "bad values" (resembles the OI def.).
- In case $|L_n| \leq k$, we can easily simulate A with a $k \cdot \text{poly}(n)$ circuit, S , achieving ϵ -accuracy (S^{I_x} would first check if $x \in L_n$).
- **Claim:** if $|L_n| > k$ we can use A to construct an adversary of size $m \cdot \text{poly}(n, \frac{1}{\epsilon})$ which inverts π on more than $k/16n$ inputs.

Sketch of Proof cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- Assume WLOG that for all $x \in L_n$:

$$\Pr_R[A(\mathcal{H}(x, R) = 1)] - \Pr[A(U_{3n^2+3n}) = 1] \geq \epsilon$$

- Then: $\Pr_{x \in L_n, R}[A(\mathcal{H}(x, R) = 1)] - \Pr[A(U_{3n^2+3n}) = 1] \geq \epsilon$

- Given rand. bits $\{b_i\}$ consider the following hybrids:

$$\begin{array}{ccccccc}
 r_1 & \dots & r_{3n} & \langle x, r_1 \rangle & \langle \pi_x, r_2 \rangle & \dots & \langle \pi_x^{3n-1}, r_{3n} \rangle \\
 r_1 & \dots & r_{3n} & b_1 & \langle \pi_x, r_2 \rangle & \dots & \langle \pi_x^{3n-1}, r_{3n} \rangle \\
 \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\
 r_1 & \dots & r_{3n} & b_1 & b_2 & \dots & b_{3n}
 \end{array}$$

- By an hybrid argument there is a $j \in [3n - 1]$ and a predictor P (uses A) that on input

$$r_1, \dots, sr_{3n}, \langle \pi_x^j, r_{j+1} \rangle, \dots, \langle \pi_x^{3n-1}, r_{3n} \rangle$$

Sketch of Proof cont'

A motivating example
(CANETTI 97)

Any Suggestions?

So what do we need?

Obfuscation of Point
Functions

Formally Defining
Security

Defining Security cont'

Alternative Definition

Alternative Definition
cont'

Alternative Definitions
cont'

Yet Another Definition

Which One Do You
Prefer?

The (r, r^x)
Construction

The (r, r^x)
Construction cont'

The (r, r^x)
Construction cont'

Proof

Proof - First Step

Proof - First Step cont'

Proof - First Step cont'

Proof - Distinguishing

- By an hybrid argument there is a $j \in [3n - 1]$ and a predictor P (uses A) that on input $r_1, \dots, r_{3n}, \langle \pi_x^j, r_{j+1} \rangle, \dots, \langle \pi_x^{3n-1}, r_{3n} \rangle$ predicts $\langle \pi_x^{j-1}, r_j \rangle$ w.p. $1/2 + \epsilon/3n$ (the prob. is over $\{r_i\}, x \in L$ and $\{b_i\}$ which P will toss on its own).
- One can fix all coins but r_j to get a deterministic P' which satisfies:
$$\Pr_{x \in L', r_j} [P'(\pi_x^j, r_j) = \langle \pi_x^{j-1}, r_j \rangle] \geq \frac{1}{2} + \frac{\epsilon}{3n}$$
Note that given π_x^j it can compute π_x^t for any $t > j$.
- Having this one can pull a GL stunt to invert π on $\Omega(\epsilon/n)$ fraction of the k elements in $\pi^{j-1}(L)$.