Adaptive Security of Compositions

Patrick Pletscher
pat@student.ethz.ch

ETH Zurich

June 30, 2005

Topic of this semester thesis

Question

Given are *non-adaptively* secure pseudo-random functions, is the composition of such functions guaranteed to be secure against *adaptive* adversaries?

Topic of this semester thesis

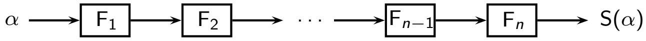
Question

Given are *non-adaptively* secure pseudo-random functions, is the composition of such functions guaranteed to be secure against *adaptive* adversaries?

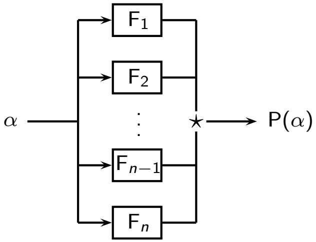
Things to notice

- Non-adaptive vs. adaptive.
- We work in the computational setting.
- Everything must be efficiently computable.

Composition: sequential and parallel



$$S := F_1 \triangleright F_2 \triangleright \ldots \triangleright F_{n-1} \triangleright F_n$$



$$P := F_1 \star \ldots \star F_n$$

Figure: Sequential and Parallel composition of *n* functions

Overview

1. What is known - before and after
2. Sequential composition
   - Function for the sequential counterexample
   - Adaptive Distinguishability of the Sequential Composition
   - Non-Adaptive Indistinguishability of F
3. Parallel composition

What is known - before and after

Known results

- True in the information theoretic setting [MP04].
- Counterexamples for sequential and parallel composition. But only for the composition of two functions [Pie05].
- Open problem: Can we generalize this counterexample for arbitrary many functions?

What is known - before and after

Known results

- True in the information theoretic setting [MP04].
- Counterexamples for sequential and parallel composition. But only for the composition of two functions [Pie05].
- Open problem: Can we generalize this counterexample for arbitrary many functions?

Results of semester thesis

- We found a counterexample for the sequential composition of arbitrary many functions.
- Function is rather simple.
- Parallel composition remains an open problem.

Sequential composition - The big picture

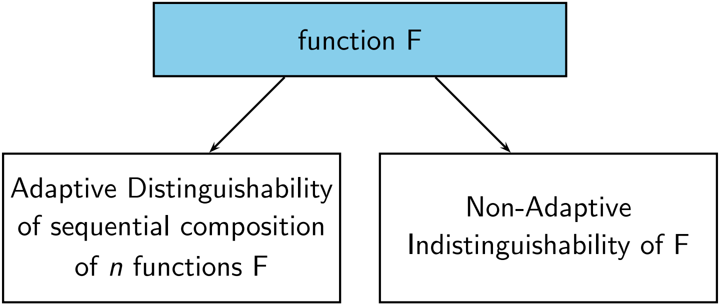


Figure: Proof sketch for "composition does not imply adaptive security"

Function for sequential counterexample (1/2)

Some intuition

- Counterexamples of [Pie05] based on Decisional Diffie-Hellman (DDH) problem, let's try to use DDH as well for the generalization.
- 2 adaptive queries might be sufficient.
- Use effect of cancelling out. As we work in the exponent, consider using the multiplicative inverse.

$$g^{xx^{-1}} = g$$

Function for sequential counterexample (2/2)

Function F

Output computed as:

$$\mathsf{F}(s, t, u, v) \rightarrow (s^{xr_1}, t^{r_1}, u^{x^{-1}r_2}, v^{r_2})$$

Explanations

- $x \in \mathbb{Z}_p^*$ secret key and x^{-1} its multiplicative inverse, i.e. $xx^{-1} \equiv 1 \mod p$. Where p is the prime order of the group.
- $k_\mathsf{F} \in \mathcal{K}_\mathsf{R}$ to generate pseudo-random values.

$$(r_1, r_2) \leftarrow \mathsf{R}_{k_\mathsf{F}}(s, t, u, v)$$

- Domain and range of F: $\mathcal{G}_\mathsf{S} := \mathcal{G} - \{1\}$.

Sequential composition - The big picture

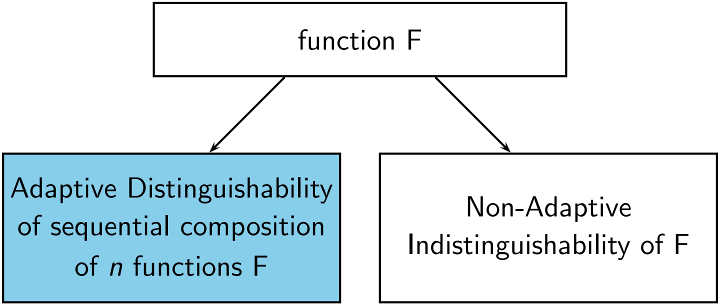


Figure: Proof sketch for "composition does not imply adaptive security"

Adaptive Distinguishability (1/2)

Abbreviation

j'th randomness generated in the i'th query:

$$r_{\mathsf{S}}^{(i,j)} := r_{\mathsf{F}_1}^{(i,j)} \cdot \ldots \cdot r_{\mathsf{F}_n}^{(i,j)}$$

Adaptive Distinguishability (1/2)

Abbreviation

j'th randomness generated in the i'th query:

$$r_{\mathsf{S}}^{(i,j)} := r_{\mathsf{F}_1}^{(i,j)} \cdot \ldots \cdot r_{\mathsf{F}_n}^{(i,j)}$$

First Query

Use (g, g, g, g) as first query, we will get:

$$(g^{x_1 \cdot \ldots \cdot x_n \cdot r_{\mathsf{S}}^{(1,1)}}, g^{r_{\mathsf{S}}^{(1,1)}}, g^{x_1^{-1} \cdot \ldots \cdot x_n^{-1} \cdot r_{\mathsf{S}}^{(1,2)}}, g^{r_{\mathsf{S}}^{(1,2)}})$$

Adaptive Distinguishability (1/2)

Abbreviation

j'th randomness generated in the i'th query:

$$r_{\mathsf{S}}^{(i,j)} := r_{\mathsf{F}_1}^{(i,j)} \cdot \ldots \cdot r_{\mathsf{F}_n}^{(i,j)}$$

First Query

Use (g, g, g, g) as first query, we will get:

$$(g^{x_1 \cdot \ldots \cdot x_n \cdot r_{\mathsf{S}}^{(1,1)}}, g^{r_{\mathsf{S}}^{(1,1)}}, g^{x_1^{-1} \cdot \ldots \cdot x_n^{-1} \cdot r_{\mathsf{S}}^{(1,2)}}, g^{r_{\mathsf{S}}^{(1,2)}})$$

Interchange arguments

Interchange first two output arguments by third and forth:

$$(g^{x_1^{-1} \cdot \ldots \cdot x_n^{-1} \cdot r_{\mathsf{S}}^{(1,2)}}, g^{r_{\mathsf{S}}^{(1,2)}}, g^{x_1 \cdot \ldots \cdot x_n \cdot r_{\mathsf{S}}^{(1,1)}}, g^{r_{\mathsf{S}}^{(1,1)}})$$

Adaptive Distinguishability (2/2)

Input of second query

Use output on previous slide as second input:

$$(g^{x_1^{-1}\cdot\ldots\cdot x_n^{-1}\cdot r_{\mathsf{S}}^{(1,2)}}, g^{r_{\mathsf{S}}^{(1,2)}}, g^{x_1\cdot\ldots\cdot x_n\cdot r_{\mathsf{S}}^{(1,1)}}, g^{r_{\mathsf{S}}^{(1,1)}})$$

Adaptive Distinguishability (2/2)

Input of second query

Use output on previous slide as second input:

$$(g^{x_1^{-1}\cdot\ldots\cdot x_n^{-1}\cdot r_S^{(1,2)}}, g^{r_S^{(1,2)}}, g^{x_1\cdot\ldots\cdot x_n\cdot r_S^{(1,1)}}, g^{r_S^{(1,1)}})$$

Output of second query

The secret keys of all functions will cancel out, so we get

$$(g^{r_S^{(1,2)} r_S^{(2,1)}}, g^{r_S^{(1,2)} r_S^{(2,1)}}, g^{r_S^{(1,1)} r_S^{(2,2)}}, g^{r_S^{(1,1)} r_S^{(2,2)}}).$$

which is of course not pseudo-random.

Sequential composition - The big picture

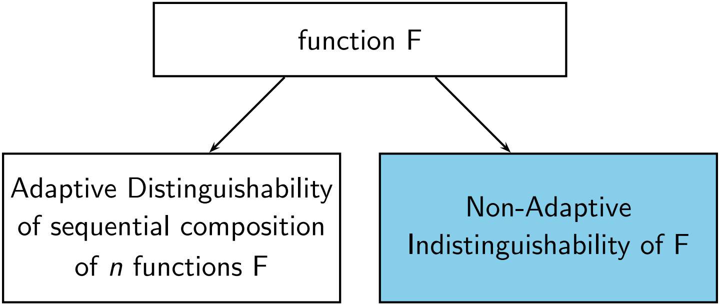


Figure: Proof sketch for "composition does not imply adaptive security"

Non-Adaptive Indistinguishability - Overview

Where we are ...

- **What we have seen:** The sequential composition of n functions F can be distinguished by an adaptive adversary from random in 2 queries.
- **What's left:** Is F really non-adaptively indistinguishable from random?

Non-Adaptive Indistinguishability - Overview

Where we are ...

- **What we have seen:** The sequential composition of n functions F can be distinguished by an adaptive adversary from random in 2 queries.
- **What's left:** Is F really non-adaptively indistinguishable from random?

We will show ...

$$\mathbf{Adv}_{\mathrm{F}}^{non-adaptive}(q,t) \leq \mathbf{Adv}_{\mathrm{R}}(q,t') + q\mathbf{Adv}_{DDH}(t')$$

where $t' = t + poly(\log p, q)$.

Reformulating our problem (1/2)

- Now: only one query, later on: hybrid argument.
- First three exponents are random:

$$a := xr_1, \ b := r_1, \ c := x^{-1}r_2$$

the forth exponent can be expressed by the others, namely

$$acb^{-1} = \underbrace{xr_1}_{a}\underbrace{x^{-1}r_2}_{c}\underbrace{r_1^{-1}}_{b^{-1}} = r_2$$

so we can see the function as

$$\mathsf{F}(s, t, u, v) \to (s^a, t^b, u^c, v^{acb^{-1}})$$

for random a, b, c.

Reformulating our problem (2/2)

- Reformulated function

$$F(s, t, u, v) \to (s^a, t^b, u^c, v^{acb^{-1}})$$

- Equivalent to

$$F(g^{z_1}, g^{z_2}, g^{z_3}, g^{z_4}) \to (g^{z_1 a}, g^{z_2 b}, g^{z_3 c}, g^{z_4 acb^{-1}})$$

  for some values z_1, z_2, z_3, z_4.
- Assume adversary knows the discrete logarithms of his inputs. So he can exponentiate with the inverses of the z_i's to compute roots.
- Without loss of generality adversary has to distinguish

$$(g^a, g^b, g^c, g^{acb^{-1}})$$

  for random a, b, c from random.

At least as hard as DDH

Distinguisher for our problem is given

Assume we are given a distinguisher A which is able to distinguish

$$(g^a, g^b, g^c, g^{acb^{-1}}) \quad \text{from} \quad (g^a, g^b, g^c, g^d)$$

for random a, b, c, d.

At least as hard as DDH

Distinguisher for our problem is given

Assume we are given a distinguisher A which is able to distinguish

$$(g^a, g^b, g^c, g^{acb^{-1}}) \quad \text{from} \quad (g^a, g^b, g^c, g^d)$$

for random a, b, c, d.

Decide DDH with the help of A: $g^c \stackrel{?}{=} g^{ab}$

1. On input $(\alpha, \beta, \gamma) = (g^a, g^b, g^c)$ compute random value r and its inverse r^{-1}.
2. Use A with input $(\alpha, g^r, \beta, \gamma^{r^{-1}})$.

If $c = ab$, we have an input to A of the form $(g^a, g^r, g^b, g^{abr^{-1}})$, otherwise if c is random, the input to A, is as well random.

Putting it all together

Hybrid argument

On previous slide: our problem $\geq DDH$. Adversary is able to ask q queries. Does this enhance his advantage?
Yes, but only by the factor q (use Hybrid argument).

Putting it all together

Hybrid argument

On previous slide: our problem $\geq DDH$. Adversary is able to ask q queries. Does this enhance his advantage?
Yes, but only by the factor q (use Hybrid argument).

We use a pseudo-random function

We don't use a truly random function. $\mathbf{Adv}_{\mathrm{R}}(q, t')$ accounts for this inaccuracy.

Putting it all together

Hybrid argument

On previous slide: our problem $\geq DDH$. Adversary is able to ask q queries. Does this enhance his advantage?
Yes, but only by the factor q (use Hybrid argument).

We use a pseudo-random function

We don't use a truly random function. $\mathbf{Adv}_{\mathrm{R}}(q, t')$ accounts for this inaccuracy.

Everything together

$$\mathbf{Adv}_{\mathrm{F}}^{non-adaptive}(q, t) \leq \mathbf{Adv}_{\mathrm{R}}(q, t') + q\mathbf{Adv}_{DDH}(t')$$

Parallel composition

Seems to be somewhat harder . . .

- We couldn't reuse the counterexample for the sequential composition.
- The idea of [Pie05], seems as well not to generalize.
- Use another hardness assumption than DDH??
- Comments are of course highly appreciated . . .

Parallel composition

Seems to be somewhat harder ...

- We couldn't reuse the counterexample for the sequential composition.
- The idea of [Pie05], seems as well not to generalize.
- Use another hardness assumption than DDH??
- Comments are of course highly appreciated ...

Any questions?

Ueli Maurer and Krzysztof Pietrzak.
Composition of random systems: When two weak make one strong.
In *Theory of Cryptograpy — TCC '04*, volume 2951 of *Lecture Notes in Computer Science*, pages 410–427, 2004.

Krzysztof Pietrzak.
Composition does not imply adaptive security.
In *Advances in Cryptology — CRYPTO '05 (to appear)*, Lecture Notes in Computer Science, 2005.