Composition Does Not Imply Adaptive Security

Krzysztof Pietrzak
ETH Zürich

a 08/15 talk

Pseudorandom Functions

A PRF is a family of functions $\mathcal{F}$ indexed by $\mathbb{N}$. For $n \in \mathbb{N}$ the function $\mathsf{F} \in \mathcal{F}$

$$\mathsf{F} : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{Y}_n \qquad \text{notation : } \mathsf{F}_k(.) = \mathsf{F}(k, .)$$

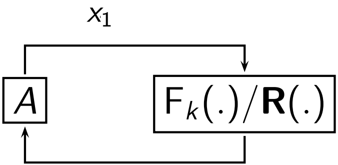
is such that for all efficient distinguishers A.

$$\left| \Pr[A^{\mathsf{F}_k(.)} \to 1] - \Pr[A^{\mathbf{R}} \to 1] \right| = \mathrm{negl}(n)$$

Here $\mathbf{R}$ is a uniform random function and $k \in_R \mathcal{K}_n$ is a random key.

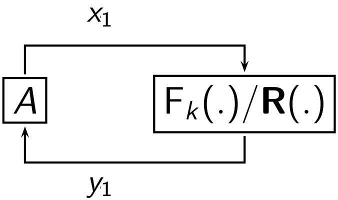
Adaptive vs. Non-Adaptive Distinguisher

Adaptive distinguisher A



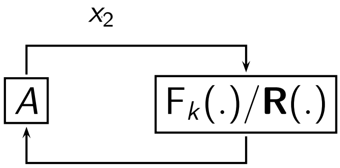
Adaptive vs. Non-Adaptive Distinguisher

Adaptive distinguisher A



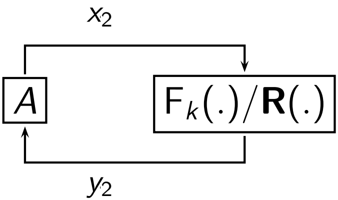
Adaptive vs. Non-Adaptive Distinguisher

Adaptive distinguisher A



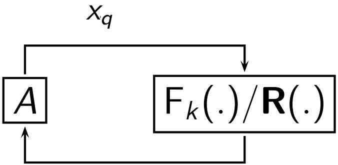
Adaptive vs. Non-Adaptive Distinguisher

Adaptive distinguisher A



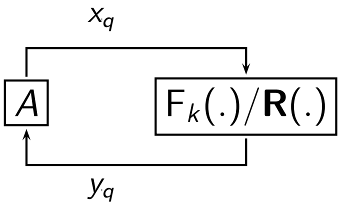
Adaptive vs. Non-Adaptive Distinguisher

Adaptive distinguisher A



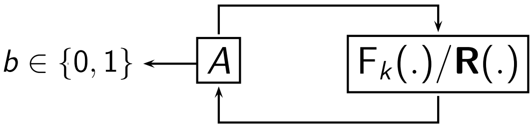
Adaptive vs. Non-Adaptive Distinguisher

Adaptive distinguisher A



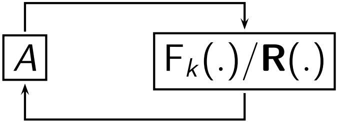
Adaptive vs. Non-Adaptive Distinguisher

Adaptive distinguisher A



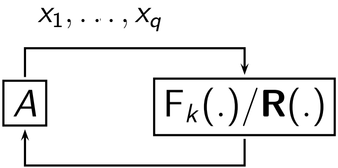
Adaptive vs. Non-Adaptive Distinguisher

Non-Adaptive distinguisher A



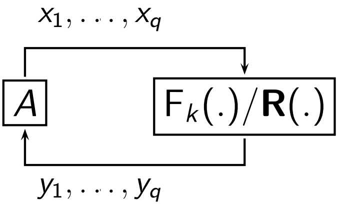
Adaptive vs. Non-Adaptive Distinguisher

Non-Adaptive distinguisher A



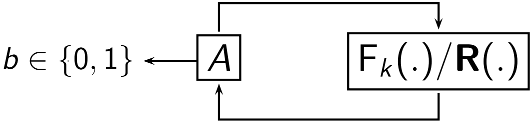
Adaptive vs. Non-Adaptive Distinguisher

Non-Adaptive distinguisher A



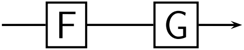
Adaptive vs. Non-Adaptive Distinguisher

Non-Adaptive distinguisher A



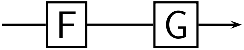
Composition of PRFs

Sequential composition: $(\mathsf{G} \circ \mathsf{F})(x) = \mathsf{G}(\mathsf{F}(x))$

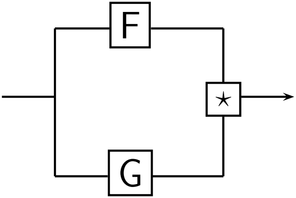


Composition of PRFs

Sequential composition: $(G \circ F)(x) = G(F(x))$



Parallel composition: $(F \star G)(x) = G(x) \star F(x)$.



Adaptive Security by Composition?

Question:

If $\mathcal{F}, \mathcal{G}$ are non-adaptively secure PRFs, is $\mathcal{G} \circ \mathcal{F}$ or $\mathcal{F} \star \mathcal{G}$ adaptively secure?

Adaptive Security by Composition?

Question:

If $\mathcal{F}, \mathcal{G}$ are non-adaptively secure PRFs, is $\mathcal{G} \circ \mathcal{F}$ or $\mathcal{F} \star \mathcal{G}$ adaptively secure?

- Yes, in the information theoretic setting [Maurer,P., TCC04].

Adaptive Security by Composition?

Question:

If $\mathcal{F}, \mathcal{G}$ are non-adaptively secure PRFs, is $\mathcal{G} \circ \mathcal{F}$ or $\mathcal{F} \star \mathcal{G}$ adaptively secure?

- Yes, in the information theoretic setting [Maurer,P., TCC04].
- If the answer is yes in the computational setting, then there is *no black-box proof* for it. [Myers, EC04].

Adaptive Security by Composition?

Question:

If $\mathcal{F}, \mathcal{G}$ are non-adaptively secure PRFs, is $\mathcal{G} \circ \mathcal{F}$ or $\mathcal{F} \star \mathcal{G}$ adaptively secure?

- Yes, in the information theoretic setting [Maurer,P., TCC04].
- If the answer is yes in the computational setting, then there is *no black-box proof* for it. [Myers, EC04].
- No, in the computational setting under DDH.

Distinguishing advantage

Let $\mathcal{A}(t, q)$ denote all distinguishers running in time t and making at most q oracle queries.

$$\mathbf{Adv}_{\mathbf{F}}(t, q) = \max_{A \in \mathcal{A}(t,q)} \left| \Pr[A^{\mathbf{F}(.)} \rightarrow 1] - \Pr[A^{\mathbf{R}(.)} \rightarrow 1] \right|$$

Distinguishing advantage

Let $\mathcal{A}(t, q)$ denote all distinguishers running in time t and making at most q oracle queries.

$$\mathbf{Adv}_{\mathbf{F}}(t, q) = \max_{A \in \mathcal{A}(t,q)} \left| \Pr[A^{\mathbf{F}(.)} \rightarrow 1] - \Pr[A^{\mathbf{R}(.)} \rightarrow 1] \right|$$

$\mathcal{F}$ is a PRF if for all $c > 0$, $\mathbf{F}(.) = \mathsf{F}_k(.)$ with $k \in_R \mathcal{K}_n$

$$\mathbf{Adv}_{\mathbf{F}}(n^c, n^c) = \mathrm{negl}(n)$$

Distinguishing advantage

Let $\mathcal{A}(t,q)$ denote all distinguishers running in time t and making at most q oracle queries.

$$\mathbf{Adv_F}(t,q) = \max_{A \in \mathcal{A}(t,q)} \left| \Pr[A^{\mathbf{F}(.)} \to 1] - \Pr[A^{\mathbf{R}(.)} \to 1] \right|$$

$\mathcal{F}$ is a PRF if for all $c > 0$, $\mathbf{F}(.) = \mathsf{F}_k(.)$ with $k \in_R \mathcal{K}_n$

$$\mathbf{Adv_F}(n^c, n^c) = \mathrm{negl}(n)$$

$\mathbf{Adv}_{\mathbf{F}}^{non-adaptive}(t,q)$ defined like $\mathbf{Adv_F}(t,q)$ but for non-adaptive distinguishers.

The Information Theoretic Setting

Theorem (Maurer,P.04)

If $\mathbf{Adv}_{\mathbf{E}}^{non-adaptive}(\infty, q) \leq \epsilon$ *and* $\mathbf{Adv}_{\mathbf{F}}^{non-adaptive}(\infty, q) \leq \epsilon$
then

The Information Theoretic Setting

Theorem (Maurer,P.04)

If $\mathbf{Adv}_{\mathbf{E}}^{non-adaptive}(\infty, q) \leq \epsilon$ *and* $\mathbf{Adv}_{\mathbf{F}}^{non-adaptive}(\infty, q) \leq \epsilon$ *then*

$$\mathbf{Adv}_{\mathbf{F} \circ \mathbf{E}}(\infty, q) \leq 2\epsilon(1 + \ln \epsilon^{-1})$$

The Information Theoretic Setting

Theorem (Maurer,P.04)

If $\mathbf{Adv}_{\mathbf{E}}^{non-adaptive}(\infty, q) \leq \epsilon$ *and* $\mathbf{Adv}_{\mathbf{F}}^{non-adaptive}(\infty, q) \leq \epsilon$ *then*

$$\mathbf{Adv}_{\mathbf{F} \circ \mathbf{E}}(\infty, q) \leq 2\epsilon(1 + \ln \epsilon^{-1})$$

$$\mathbf{Adv}_{\mathbf{E} \star \mathbf{F}}(\infty, q) \leq 2\epsilon(1 + \ln \epsilon^{-1})$$

The Computational Setting

There exist non-adaptively secure PRFs $\mathcal{F}$ and $\mathcal{G}$ where $\mathcal{G} \circ \mathcal{F}$ $(\mathcal{F} \star \mathcal{G})$ are not adaptively secure.

The Computational Setting

There exist non-adaptively secure PRFs $\mathcal{F}$ and $\mathcal{G}$ where $\mathcal{G} \circ \mathcal{F}$ ($\mathcal{F} \star \mathcal{G}$) are not adaptively secure.

The non-adaptive security of $\mathcal{F}$ and $\mathcal{G}$ is proven under the decisional Diffie-Hellman (DDH) assumption:

The Computational Setting

There exist non-adaptively secure PRFs $\mathcal{F}$ and $\mathcal{G}$ where $\mathcal{G} \circ \mathcal{F}$ ($\mathcal{F} \star \mathcal{G}$) are not adaptively secure.

The non-adaptive security of $\mathcal{F}$ and $\mathcal{G}$ is proven under the decisional Diffie-Hellman (DDH) assumption:

Let $\mathcal{H} = \mathcal{H}(n)$ be a prime order cyclic group and g a generator of $\mathcal{H}$. Then for random a, b, c the distributions

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

are indistinguishable.

El-Gamal Encryption

Public: group $\mathcal{H}$ of prime order P and generator g of $\mathcal{H}$.

Secret key is a random $x \in \mathbb{Z}_P$, public key is g^x. Encryption of $m \in \mathcal{H}$ with randomness $r \in \mathbb{Z}_P$:

$$\mathrm{Enc}_{g^x}(m, r) = (mg^{xr}, g^r)$$

Decryption of $(a, b) \in \mathcal{H}^2$:

$$\mathrm{Dec}_x(a, b) = a/b^x$$

El-Gamal Encryption

Public: group $\mathcal{H}$ of prime order P and generator g of $\mathcal{H}$.

Secret key is a random $x \in \mathbb{Z}_P$, public key is g^x. Encryption of $m \in \mathcal{H}$ with randomness $r \in \mathbb{Z}_P$:

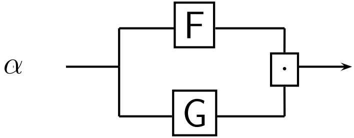
$$\mathrm{Enc}_{g^x}(m, r) = (mg^{xr}, g^r)$$

Decryption of $(a, b) \in \mathcal{H}^2$:

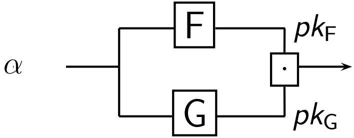
$$\mathrm{Dec}_x(a, b) = a/b^x$$

$$\mathrm{Dec}_x(mg^{xr}, g^r) = mg^{xr}/g^{rx} = m$$

Intuition for the Parallel Counterexample

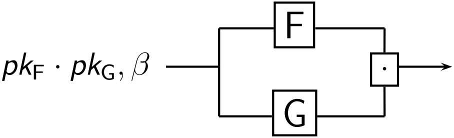


Intuition for the Parallel Counterexample



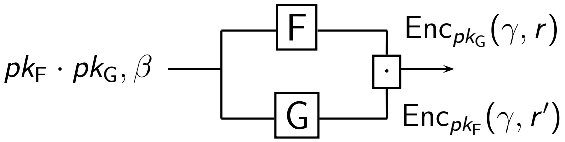
1. $\alpha \rightarrow pk_F \cdot pk_G$

Intuition for the Parallel Counterexample



1. $\alpha \to pk_F \cdot pk_G$

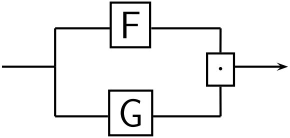
Intuition for the Parallel Counterexample



1. $\alpha \longrightarrow pk_F \cdot pk_G$
2. $pk_F \cdot pk_G, \beta \longrightarrow \mathrm{Enc}_{pk_G}(\gamma, r) \cdot \mathrm{Enc}_{pk_F}(\gamma, r')$

Intuition for the Parallel Counterexample

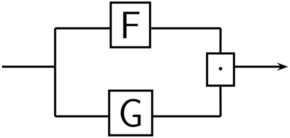
$pk_F \cdot pk_G, \mathsf{Enc}_{pk_G}(\gamma, r) \cdot \mathsf{Enc}_{pk_F}(\gamma; r')$



1. $\alpha \longrightarrow pk_F \cdot pk_G$
2. $pk_F \cdot pk_G, \beta \longrightarrow \mathsf{Enc}_{pk_G}(\gamma, r) \cdot \mathsf{Enc}_{pk_F}(\gamma, r')$

Intuition for the Parallel Counterexample

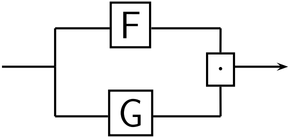
$pk_\mathsf{F} \cdot pk_\mathsf{G}, \mathsf{Enc}_{pk_\mathsf{G}}(\gamma, r) \cdot \mathsf{Enc}_{pk_\mathsf{F}}(\gamma; r')$



1. $\alpha \longrightarrow pk_\mathsf{F} \cdot pk_\mathsf{G}$
2. $pk_\mathsf{F} \cdot pk_\mathsf{G}, \beta \longrightarrow \mathsf{Enc}_{pk_\mathsf{G}}(\gamma, r) \cdot \mathsf{Enc}_{pk_\mathsf{F}}(\gamma, r')$

Intuition for the Parallel Counterexample

$pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma; r')$

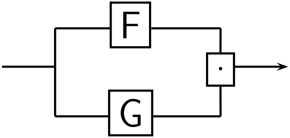


1. $\alpha \longrightarrow pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}$
2. $pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta \longrightarrow \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')$

F checks

Intuition for the Parallel Counterexample

$pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma; r')$



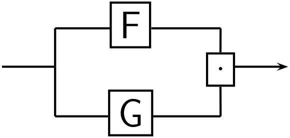
1. $\alpha \longrightarrow pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}$
2. $pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta \longrightarrow \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')$

F checks

$$\underline{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')}$$

Intuition for the Parallel Counterexample

$pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma; r')$



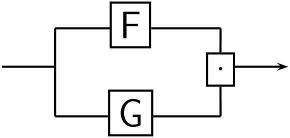
1. $\alpha \longrightarrow pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}$
2. $pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta \longrightarrow \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')$

F checks

$$\frac{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')}{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \longleftarrow \mathsf{F}(pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta)}$$

Intuition for the Parallel Counterexample

$pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma; r')$



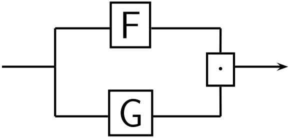
1. $\alpha \rightarrow pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}$
2. $pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta \rightarrow \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')$

F checks

$$\frac{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')}{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \leftarrow \mathsf{F}(pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta)} = \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')$$

Intuition for the Parallel Counterexample

$$pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma; r')$$



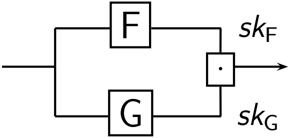
1. $\alpha \longrightarrow pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}$
2. $pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta \longrightarrow \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')$

F checks

$$\mathsf{Dec}_{sk_{\mathsf{F}}}\left(\frac{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')}{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \leftarrow \mathsf{F}(pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta)} = \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')\right) \stackrel{?}{=} \gamma$$

Intuition for the Parallel Counterexample

$$pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma; r')$$



1. $\alpha \rightarrow pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}$
2. $pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta \rightarrow \mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')$

F checks

$$\mathsf{Dec}_{sk_{\mathsf{F}}}\left(\frac{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \cdot \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')}{\mathsf{Enc}_{pk_{\mathsf{G}}}(\gamma, r) \leftarrow \mathsf{F}(pk_{\mathsf{F}} \cdot pk_{\mathsf{G}}, \beta)} = \mathsf{Enc}_{pk_{\mathsf{F}}}(\gamma, r')\right) \stackrel{?}{=} \gamma$$

Definition of the PRFs

Group $\mathcal{H}$ of prime order P, $\langle g \rangle = \mathcal{H}$.
A PRF $\mathsf{R} : \mathcal{K}_R \times \mathcal{H}^3 \to \mathbb{Z}_P^3$.

$\mathsf{F} : \mathcal{K} \times \mathcal{H}^3 \to \mathcal{H}^3$ where $\mathcal{K} = \mathbb{Z}_P \times \mathcal{K}_R$.

$F(\{x, k_F\}, u, v, w)$ is computed as:

$\mathsf{F}(\{x, k_\mathsf{F}\}, u, v, w)$ is computed as:

$$(r_1, r_2, r_3) \leftarrow \mathsf{R}_{k_\mathsf{F}}(u, v, w)$$

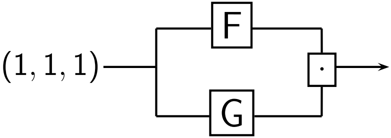
$F(\{x, k_F\}, u, v, w)$ is computed as:

$$(r_1, r_2, r_3) \leftarrow R_{k_F}(u, v, w)$$

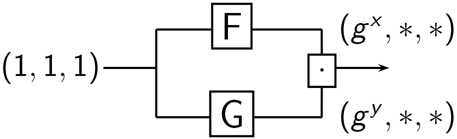
$$\begin{array}{rcl}
F(1,1,1) & \rightarrow & (g^x, g^{r_2}, g^{r_3}) \\
F(u \neq 1, 1, 1) & \rightarrow & ((u/g^x)^{r_1}, g^{r_1}, g^{r_3}) \\
F(u \neq 1, v \neq 1, w \neq 1) & \rightarrow & (a, b, c) \quad \text{where} \\
& & (d, e, f) \leftarrow F(u, 1, 1) \\
& & \text{if } (v/d) = (w/e)^x \text{ then} \\
& & \quad (a, b, c) = (x, 1, 1) \\
& & \text{otherwise } (a, b, c) = (g^{r_1}, g^{r_2}, g^{r_3}) \\
F(\text{ all other cases }) & \rightarrow & (g^{r_1}, g^{r_2}, g^{r_3})
\end{array}$$

$\alpha = (1,1,1), \beta = (1,1)$ and $\gamma = 1$

The Parallel Counterexample

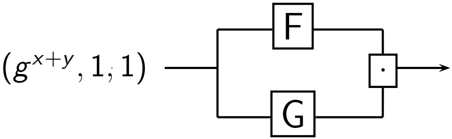


The Parallel Counterexample



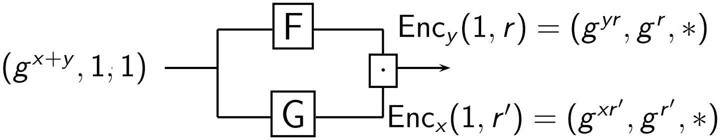
1. $(1, 1, 1) \longrightarrow (g^{x+y}, *, *)$

The Parallel Counterexample



1. $(1, 1, 1) \rightarrow (g^{x+y}, *, *)$

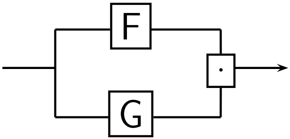
The Parallel Counterexample



1. $(1, 1, 1) \to (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \to (g^{xr'+yr}, g^{r+r'}, *)$

The Parallel Counterexample

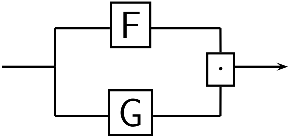
$$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$$



1. $(1, 1, 1) \longrightarrow (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \longrightarrow (g^{xr'+yr}, g^{r+r'}, *)$

The Parallel Counterexample

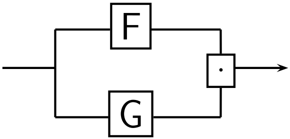
$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$



1. $(1, 1, 1) \longrightarrow (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \longrightarrow (g^{xr'+yr}, g^{r+r'}, *)$

The Parallel Counterexample

$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$

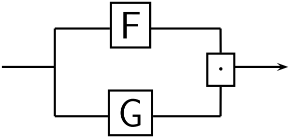


1. $(1, 1, 1) \longrightarrow (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \longrightarrow (g^{xr'+yr}, g^{r+r'}, *)$

F checks

The Parallel Counterexample

$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$



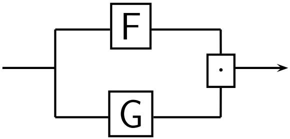
1. $(1,1,1) \longrightarrow (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \longrightarrow (g^{xr'+yr}, g^{r+r'}, *)$

F checks

$$\frac{(g^{xr'+yr}, g^{r+r'})}{}$$

The Parallel Counterexample

$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$



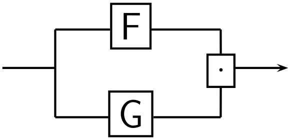
1. $(1, 1, 1) \rightarrow (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \rightarrow (g^{xr'+yr}, g^{r+r'}, *)$

F checks

$$\frac{(g^{xr'+yr}, g^{r+r'})}{(g^{yr}, g^{r}) \leftarrow \mathsf{F}(g^{x+y}, 1, 1)}$$

The Parallel Counterexample

$$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$$



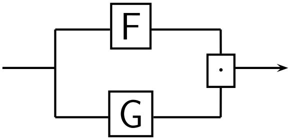
1. $(1, 1, 1) \longrightarrow (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \longrightarrow (g^{xr'+yr}, g^{r+r'}, *)$

F checks

$$\frac{(g^{xr'+yr}, g^{r+r'})}{(g^{yr}, g^{r}) \leftarrow \mathsf{F}(g^{x+y}, 1, 1)} = (g^{xr'}, g^{r'})$$

The Parallel Counterexample

$$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$$



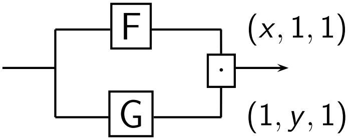
1. $(1,1,1) \to (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \to (g^{xr'+yr}, g^{r+r'}, *)$

F checks

$$\mathsf{Dec}_x\left(\frac{(g^{xr'+yr}, g^{r+r'})}{(g^{yr}, g^{r}) \leftarrow \mathsf{F}(g^{x+y}, 1, 1)} = (g^{xr'}, g^{r'})\right) \stackrel{?}{=} 1$$

The Parallel Counterexample

$$(g^{x+y}, g^{xr'+yr}, g^{r+r'})$$



1. $(1,1,1) \longrightarrow (g^{x+y}, *, *)$
2. $(g^{x+y}, 1, 1) \longrightarrow (g^{xr'+yr}, g^{r+r'}, *)$

F checks

$$\mathrm{Dec}_x\left(\frac{(g^{xr'+yr}, g^{r+r'})}{(g^{yr}, g^{r}) \leftarrow \mathrm{F}(g^{x+y}, 1, 1)} = (g^{xr'}, g^{r'})\right) \stackrel{?}{=} 1$$

Non adaptive security

$$\mathbf{Adv}_{\mathsf{F}}^{non-adaptive}(t, q) =$$

Non adaptive security

$\mathbf{Adv}_{\mathsf{F}}^{non-adaptive}(t, q) =$

$\mathsf{F}(\{x, k_{\mathsf{F}}\}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathsf{R}_{k_{\mathsf{F}}}(u, v, w)$$

Non adaptive security

$$\mathbf{Adv}_{\mathsf{F}}^{non-adaptive}(t, q) = \mathbf{Adv}_{\mathsf{R}}(t, q)$$

$\mathsf{F}(\{x \quad\}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathbf{R}(u, v, w)$$

Non adaptive security

$$\mathbf{Adv}_{\mathsf{F}}^{non-adaptive}(t, q) = \mathbf{Adv}_{\mathsf{R}}(t, q)$$

$\mathsf{F}(\{x \quad \}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathbf{R}(u, v, w)$$

$$\begin{aligned}
\mathsf{F}(1,1,1) &\rightarrow (g^x, g^{r_2}, g^{r_3}) \\
\mathsf{F}(u \neq 1, 1, 1) &\rightarrow ((u/g^x)^{r_1}, g^{r_1}, g^{r_3}) \\
\mathsf{F}(u \neq 1, v \neq 1, w \neq 1) &\rightarrow (a, b, c) \quad \text{where} \\
& \quad (d, e, f) \leftarrow \mathsf{F}(u, 1, 1) \\
& \quad \boxed{\text{if } (v/d) = (w/e)^x \text{ then}} \\
& \quad\quad (a, b, c) = (x, 1, 1) \\
& \quad \text{otherwise } (a, b, c) = (g^{r_1}, g^{r_2}, g^{r_3}) \\
\mathsf{F}(\text{ all other cases }) &\rightarrow (g^{r_1}, g^{r_2}, g^{r_3})
\end{aligned}$$

Non adaptive security

$$\mathbf{Adv}_{\mathsf{F}}^{non-adaptive}(t,q) = \mathbf{Adv}_{\mathsf{R}}(t,q)$$

$\mathsf{F}(\{x \quad \}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathbf{R}(u, v, w)$$

$$
\begin{aligned}
\mathsf{F}(1,1,1) &\rightarrow (g^x, g^{r_2}, g^{r_3}) \\
\mathsf{F}(u \neq 1, 1, 1) &\rightarrow ((u/g^x)^{r_1}, g^{r_1}, g^{r_3}) \\
\mathsf{F}(u \neq 1, v \neq 1, w \neq 1) &\rightarrow (a, b, c) \quad \text{where} \\
& \quad\; (d, e, f) \leftarrow \mathsf{F}(u, 1, 1) \\
\Pr[\text{if evaluates true}] \leq 2/P & \quad\; \boxed{\text{if } (v/d) = (w/e)^x \text{ then}} \\
& \qquad (a, b, c) = (x, 1, 1) \\
& \quad\; \text{otherwise } (a, b, c) = (g^{r_1}, g^{r_2}, g^{r_3}) \\
\mathsf{F}(\text{ all other cases }) &\rightarrow (g^{r_1}, g^{r_2}, g^{r_3})
\end{aligned}
$$

Non adaptive security

$$\mathbf{Adv}_{\mathrm{F}}^{non-adaptive}(t,q) = \mathbf{Adv}_{\mathrm{R}}(t,q) + q \cdot 2/P$$

$\mathrm{F}(\{x \quad\}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathbf{R}(u, v, w)$$

$$\begin{array}{rcl} \mathrm{F}(1,1,1) & \rightarrow & (g^x, g^{r_2}, g^{r_3}) \\ \mathrm{F}(u \neq 1, 1, 1) & \rightarrow & ((u/g^x)^{r_1}, g^{r_1}, g^{r_3}) \\ \mathrm{F}(u \neq 1, v \neq 1, w \neq 1) & \rightarrow & (a, b, c) \quad \text{where} \end{array}$$

$$(a, b, c) = (g^{r_1}, g^{r_2}, g^{r_3})$$

$$\mathrm{F}(\text{ all other cases }) \rightarrow (g^{r_1}, g^{r_2}, g^{r_3})$$

Non adaptive security

$$\mathbf{Adv}_{\mathsf{F}}^{non-adaptive}(t,q) = \mathbf{Adv}_{\mathsf{R}}(t,q) + q \cdot 2/P$$

$\mathsf{F}(\{x \quad\}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathbf{R}(u, v, w)$$

$$\begin{aligned} \mathsf{F}(1,1,1) &\rightarrow (g^x, g^{r_2}, g^{r_3}) \\ \mathsf{F}(u \neq 1,1,1) &\rightarrow ((u/g^x)^{r_1}, g^{r_1}, g^{r_3}) \end{aligned}$$

Non adaptive security

$$\mathbf{Adv}_{\mathrm{F}}^{non-adaptive}(t,q) = \mathbf{Adv}_{\mathrm{R}}(t,q) + q \cdot 2/P$$

$\mathrm{F}(\{x \quad \}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathbf{R}(u, v, w)$$

$$\begin{aligned} \mathrm{F}(1,1,1) &\rightarrow (g^x, g^{r_2}, g^{r_3}) \\ \mathrm{F}(u \neq 1,1,1) &\rightarrow ((u/g^x)^{r_1}, g^{r_1}, g^{r_3}) \end{aligned}$$

Which is equivalent to distinguish

$$(g^x, g^{a_1}, g^{xa_1}), \ldots, (g^x, g^{a_q}, g^{xa_q})$$

from

$$(g^x, g^{a_1}, g^{b_1}), \ldots, (g^x, g^{a_q}, g^{b_q})$$

Non adaptive security

$$\mathbf{Adv}_{\mathsf{F}}^{non-adaptive}(t,q) = \mathbf{Adv}_{\mathsf{R}}(t,q) + q \cdot 2/P + q \cdot \mathbf{Adv}_{DDH}(t)$$

$\mathsf{F}(\{x \quad\}, u, v, w)$ is defined as follows:

$$(r_1, r_2, r_3) \leftarrow \mathbf{R}(u, v, w)$$

$$\begin{array}{rcl} \mathsf{F}(1,1,1) & \rightarrow & (g^x, g^{r_2}, g^{r_3}) \\ \mathsf{F}(u \neq 1,1,1) & \rightarrow & ((u/g^x)^{r_1}, g^{r_1}, g^{r_3}) \end{array}$$

Which is equivalent to distinguish

$$(g^x, g^{a_1}, g^{xa_1}), \ldots, (g^x, g^{a_q}, g^{xa_q})$$

from

$$(g^x, g^{a_1}, g^{b_1}), \ldots, (g^x, g^{a_q}, g^{b_q})$$

Some Open Problems

- Counterexamples for more than two components? Patrick Pletscher gives counterexample for sequential composition with arbitrary many functions.

Some Open Problems

- Counterexamples for more than two components? Patrick Pletscher gives counterexample for sequential composition with arbitrary many functions.
- Counterexamples under weaker/other assumptions or even unconditionally? Probably no as counterexample for sequential composition implies key-agreement...

Some Open Problems

- Counterexamples for more than two components? Patrick Pletscher gives counterexample for sequential composition with arbitrary many functions.
- Counterexamples under weaker/other assumptions or even unconditionally? Probably no as counterexample for sequential composition implies key-agreement...
- Counterexample for sequential composition with pseudorandom *permutations*. This would show that cascading non-adaptively secure block-ciphers will not give adaptive security in general.