MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Indistinguishability of sums and products). *Let $\mathcal{X}_0$ and $\mathcal{X}_1$ be (t_1, ε_1)-indistinguishable and let $\mathcal{Y}_0$ and $\mathcal{Y}_1$ be (t_2, ε_2)-indistinguishable. Estimate the computational distance between the following games*

```
$\mathcal{G}_0$
    $x \leftarrow \mathcal{X}_0$
    $y \leftarrow \mathcal{Y}_0$
    $u = x + y$
    $v = x \cdot y$
    return $\mathsf{Adv}(u, v)$
```

```
$\mathcal{G}_0$
    $x \leftarrow \mathcal{X}_1$
    $y \leftarrow \mathcal{Y}_1$
    $u = x + y$
    $v = x \cdot y$
    return $\mathsf{Adv}(u, v)$
```

Highlight all hidden assumptions. Do you get different results when you known that Adv *ignores the second argument. Formalise this and explain why the resulting bound is different.*

Solution.