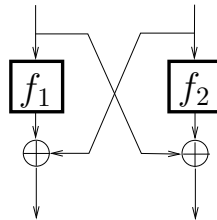


**Ülesanne.** Olgu  $f_1: \{0, 1\}^n \rightarrow \{0, 1\}^n$  ja  $f_2: \{0, 1\}^n \rightarrow \{0, 1\}^n$  juhuslikud funktsioonid. Näita, et konstruktsioon (vt. ka joonis)

$$F^{f_1 f_2}(x_1, x_2) = (f_1(x_1) \oplus x_2, f_2(x_2) \oplus x_1)$$

ei sobi pseudujuhuslikuks funktsiooniks.



**Lahendus 1: Uue väärtuse arvutamine olemasolevate põhjal.** Eristav vastane võib küsida väljundid sisenditele  $(a, 0)$  ja  $(0, b)$ , millest ta saab teada väärtused  $f_1(a)$  ja  $f_2(b)$ . Sellest aga saab välja arvutada (ja kontrollida!) sisendile  $(a, b)$  vastava väljundi  $(b \oplus f_1(a), a \oplus f_2(b))$ . Juhusliku funktsiooni korral õnnestuks selline kontroll vaid tõenäosusega  $2^{-n}$ .

**Lahendus 2: Seoste leidmine väärtuste vahel.** Eristav vastane võib küsida väljundid sisenditele  $(a_1, b)$  ja  $(a_2, b)$ . Olgu need väljundid vastavalt  $(y_1, z_1)$  ja  $(y_2, z_2)$ . Toodud konstruktsiooni korral peab kehtima samasus  $a_1 \oplus a_2 = z_1 \oplus z_2$ , mis juhusliku funktsiooni korral kehtib vaid tõenäosusega  $2^{-n}$ .

**Lahendus 3: Vähene tundlikkus sisendi väikese muudatuse suhtes.** Eristav vastane valib mingi sisendi  $(a, b)$  ja muudab seejärel  $a$  ühtainsat bitti. Toodud konstruktsiooni korral muutub siis vaid üksainus teise väljundkomponendi  $a \oplus f_2(b)$  bitt. Mis tahes valitud biti korral on juhuslikul funktsioonil selline omadus vaid tõenäosusega  $2^{-n}$ .