Funksionet e rastësishme

Qëllimet dhe objektivat

- Formalizimi i vlerësimit të sigurisë të përdorimeve të natyrshme të blok-shifruesve
- Prezantimi i funksioneve pseudo të rastësishme dhe shqyrtimi i vetivë themelore të tyre
- Shfrytëzimi i funksioneve pseudo të rastësishme si modele për blok shifrues, duke mundësuar kështu analizën e sigurisë së protokoleve të mbështetura mbi blok shifruesit

Përmbajtja

Rikujtim

- Studiuam sigurinë e një blok shifruesi kundër kthimit të çelësit.
- Por, pamë se siguria kundër kthimit të çelësit nuk është e mjaftueshme për të siguruar se përdorimet e natyrshme të një blok shifruesi janë të sigurta.
- Dëshirojmë t'i përgjigjemi pyetjes:

  Ç'është një blok shifrues i mirë?

  ku „i mirë“ do të thotë se përdorimet e natyrshme të blok shifruesit janë të sigurta.
- Do të mund të përpiqeshim ta përkufizojmë „i mirë“ me anë të një liste kushtesh të nevjshme:
  - Kthimi i çelësit është i vështirë
  - Kthimi i M nga $C = E_K(M)$ është i vështirë
  - ...
- Por një gjë e tillë as nuk është domosdoshmërisht korrekte as tërheqëse.

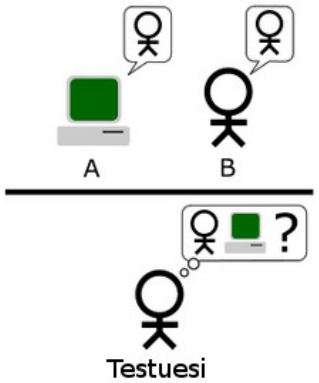
Testi Turing i inteligjencës

- Pyetja: Ç'do të thotë për një program (kompjuter) të jetë „inteligjent“ në kuptim të një njeriu?
- Përgjegjjet e mundshme:
  - Mund të jetë i lumtur
  - Mund të njohë imazhe
  - Mund të shumëzojë
    - Por vetëm numra të vegjël!
  - ...
- Qartazi, asnjë listë e tillë nuk është përgjegjje e kënaqshme e pyetjes.

Testi Turing i inteligjencës (Vazhdim)

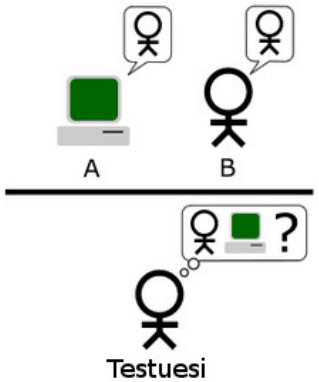
- Pyetja: Ç'do të thotë për një program (kompjuter) të jetë „inteligjent“ në kuptim të një njeriu?
- Përgjegjja e Turing-ut: Një program (kompjuter) është inteligjent në qoftë se sjellja e tij hyrje/dalje është e padallueshme nga ajo e një njeriu.

Testi Turing i inteligjencës (Vazhdim)



- Prapa murit:
  - Dhoma A: Programi P
  - Dhoma B: Një njeri

Testi Turing i inteligjencës (Vazhdim)



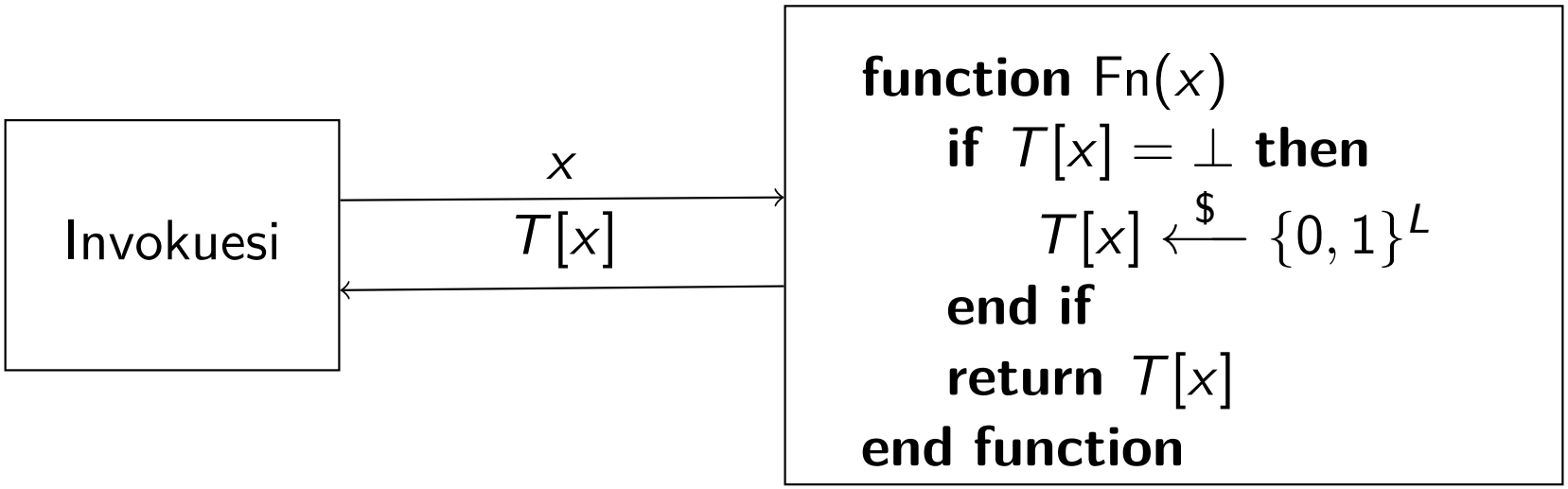
- Loja:
  - Fut testuesin në dhomën A dhe le të ketë interaksion me objektin pas murit
  - Fut testuesin në dhomën B dhe le të ketë interaksion me objektin pas murit
  - Tani pyet testuesin: Në cilën dhomë është cili?
- Masa e „inteligjencës“ së P është përmasa për të cilën testuesi gabon.

Reale kundrejt ideale

Nocioni	Objekti real	Objekti ideal
Inteligjenca	Program	Njeri
FPR	Blok shifrues	Funksion i rastësishëm

Funksionet e rastësishme

- Një funksion i rastësishëm me dalje L-bitëshe implementohet me kutinë vijuese Fn, ku T është ka vlerat iniciale $\perp$:



Funksionet e rastësishme (Vazhdim)

- Loja $\text{Rand}^{A}_{\{0,1\}^L}$

  function Fn(x)
  if $T[x] = \perp$ **then**
  $T[x] \xleftarrow{\$} \{0,1\}^L$
  end if
  return $T[x]$
  end function

  - Kundërshtari A
    - Bën pyetësorë nga Fn
    - Më në fund ndalon me ndonjë dalje

- Shënojmë me

$$\Pr\left[\text{Rand}^{A}_{\{0,1\}^L} = d\right]$$

probabilitetin që A jep d në dalje.

Funksionet e rastësishme (Vazhdim)

- Loja $\text{Rand}^A_{\{0,1\}^3}$

  function $\text{Fn}(x)$
  if $T[x] = \perp$ **then**
  $T[x] \xleftarrow{\$} \{0,1\}^3$
  end if
  return $T[x]$
  end function

  - Kundërshtari A:

    $y \leftarrow \text{Fn}(01)$
    return $(y = 000)$

$$\Pr\left[\text{Rand}^A_{\{0,1\}^3} = \top\right] = 2^{-3}$$

Funksionet e rastësishme (Vazhdim)

- Loja $\text{Rand}^{A}_{\{0,1\}^3}$

  function $\text{Fn}(x)$
  if $T[x] = \perp$ **then**
  $T[x] \xleftarrow{\$} \{0,1\}^3$
  end if
  return $T[x]$
  end function

  - Kundërshtari A

    $y_1 \leftarrow \text{Fn}(00)$
    $y_2 \leftarrow \text{Fn}(11)$
    return $(y_1 = 010 \wedge y_2 = 011)$

$$\Pr\left[\text{Rand}^{A}_{\{0,1\}^3} = \top\right] = 2^{-6}$$

Funksionet e rastësishme (Vazhdim)

- Loja $\text{Rand}^{A}_{\{0,1\}^3}$

  function $\text{Fn}(x)$
  if $T[x] = \perp$ **then**
  $T[x] \xleftarrow{\$} \{0,1\}^3$
  end if
  return $T[x]$
  end function

  - Kundërshtari A

    $y_1 \leftarrow \text{Fn}(00)$
    $y_2 \leftarrow \text{Fn}(11)$
    return $(y_1 \oplus y_2 = 101)$

$$\Pr\left[\text{Rand}^{A}_{\{0,1\}^3} = \top\right] = 2^{-3}$$

Familje funksionesh

- Një familje funksionesh

$$F : \text{Keys}(F) \times \text{Dom}(F) \to \text{Range}(F)$$

është një pasqyrim me dy ndryshore. Për $K \in \text{Keys}(F)$ vejmë

$$F_K : \text{Dom}(F) \to \text{Range}(F)$$

të përkufizuar me

$$(\forall x \in \text{Dom}(F))F_K(x) = F(K, x)$$

- Shembuj:
  - DES: $\text{Keys}(F) = \{0,1\}^{56}$, $\text{Dom}(F) = \text{Range}(F) = \{0,1\}^{64}$
  - AES: $\text{Keys}(F) = \text{Dom}(F) = \text{Range}(F) = \{0,1\}^{128}$
  - Çdo blok shifrues: $\text{Dom}(F) = \text{Range}(F)$ dhe çdo F_K është një permutacion.

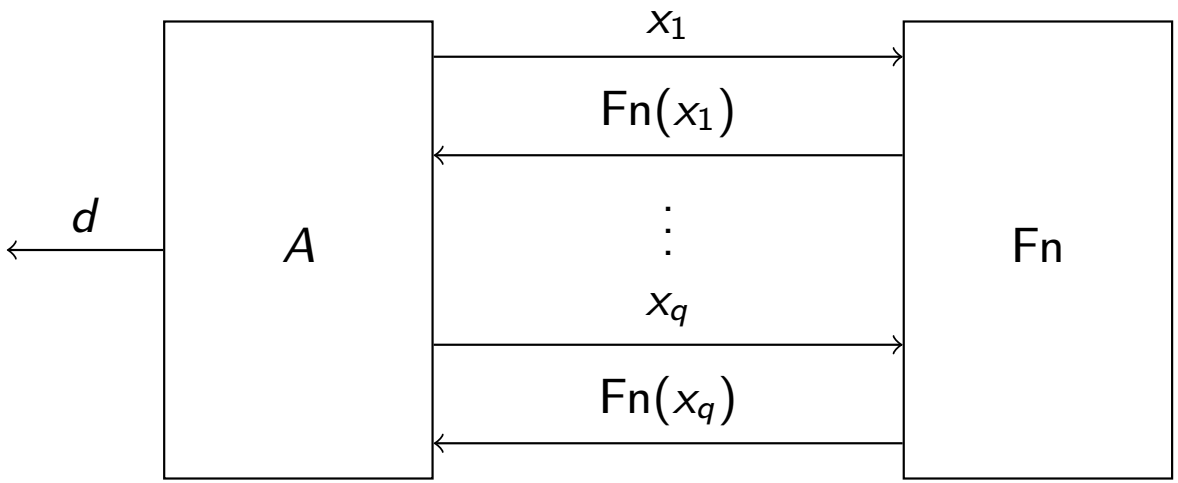
Reale kundrejt ideale (Vazhdim)

Nocioni	Objekti real	Objekti ideal
FPR	Familje funksionesh (p.sh. një blok shifrues)	Funksion i rastësishëm

- F është FPR në qoftë se sjellja hyrje/dalje e F_K i duket testuesit sikur sjellja hyrje/dalje e një funksioni të rastësishëm.
- Testuesi nuk e ka çelësin K.

FPR-kundërshtarët

- Le të jetë $F : \text{Keys}(F) \times \text{Dom}(F) \to \text{Range}(F)$ një familje funksionesh.
- Një fpr-kundërshtar (testuesi ynë) ka një orakul Fn për një funksion prej $\text{Dom}(F)$ te $\text{Range}(F)$. Ai mund të
  - Bëjë një orakul pyetësor x sipas dëshirës dhe të marrë $\text{Fn}(x)$ në kthim
  - Bëjë këtë shumë herë
  - Ndalojë më në fund dhe të japë në dalje një bit d.



Përsëritja e pyetësorëve

- Një funksion i rastësishën duhet të jetë konsistent, d.m.th. pasi të ketë kthyer njëherë y si përgjegjje të x, duhet të kthejë përsëri y në qoftë se merr sërish një pyetësor me të njëjtin x.
  - Kjo është arsyeja për „if“ në algoritmin e lojës $\text{Rand}_{\text{Range}(F)}$:

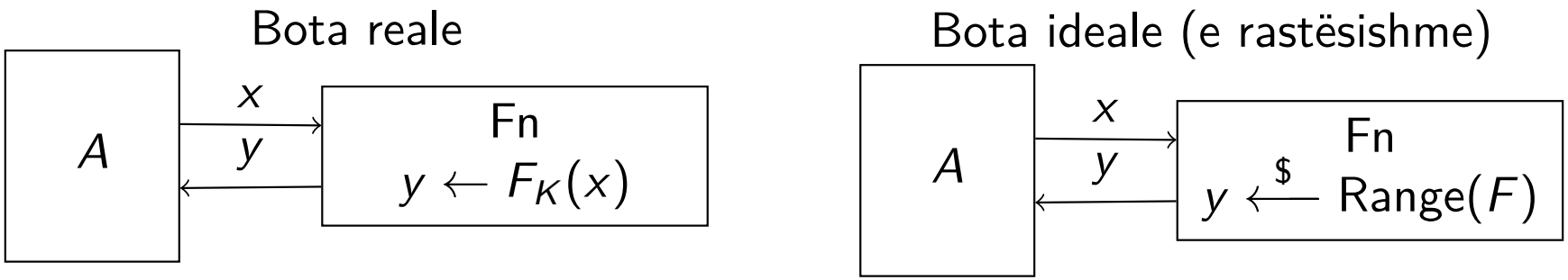
function Fn(x)
  if $T[x] = \perp$ **then**
    $T[x] \xleftarrow{\$} \text{Range}(F)$
  end if
  return $T[x]$
end function

- Prej këtu e tutje dakordojmë një rregull:
  - Një fpr-kundërshtar nuk lejohet të përsërisë një orakul pyetësor
  - Tani loja jonë $\text{Rand}_{\text{Range}(F)}$ është:

function Fn(x)
  $T[x] \xleftarrow{\$} \text{Range}(F)$
  return $T[x]$
end function

FPR-kundërshtarët (Vazhdim)

- Le të jetë $F : \text{Keys}(F) \times \text{Dom}(F) \to \text{Range}(F)$ një familje funksionesh.



Dalja d e A	Domethënia e dëshiruar: Mendoj se jam në
1	Botën reale
0	Botën ideale (të rastësishme)

- Sa më vështirë të jetë për A që ta qëllojë se në cilën botë ndodhet, aq FPR „më i mirë“ është F.

Lojërat

- Le të jetë $F : \text{Keys}(F) \times \text{Dom}(F) \to \text{Range}(F)$ një familje funksionesh.

Loja Real_F

$K \xleftarrow{\$} \text{Keys}(F)$
function $\text{Fn}(x)$
  return $F_K(x)$
end function

Loja $\text{Rand}_{\text{Range}(F)}$

function $\text{Fn}(x)$
  $T[x] \xleftarrow{\$} \text{Range}(F)$
  return $T[x]$
end function

- F dhe A u shoqërohen probabilitetet

$$\Pr\left[\text{Real}_F^A = 1\right] \quad \text{dhe} \quad \Pr\left[\text{Rand}_{\text{Range}(F)}^A = 1\right]$$

  që A jep 1 në dalje në secilën botë.

- *Përparsia* e A është

$$\text{Adv}_F^{prf}(A) = \Pr\left[\text{Real}_F^A = 1\right] - \Pr\left[\text{Rand}_{\text{Range}(F)}^A = 1\right].$$

Shembull

- Le të jetë $F : \{0,1\}^k \times \{0,1\}^{128} \to \{0,1\}^{128}$ i përkufizuar me

$$F_K(x) = x.$$

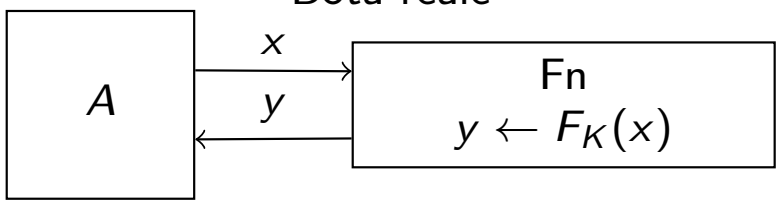
- FPR-kundërshtari A le të jetë i përkufizuar me

function A ▷ FPR-kundërshtari
  if $\text{Fn}(0^{128}) = 0^{128}$ **then return** 1
  else return 0
  end if
end function

Loja Real_F

$K \xleftarrow{\$} \{0,1\}^k$
function $\text{Fn}(x)$
  return $F_K(x)$
end function

Bota reale



- Atëherë,

$$\Pr\left[\text{Real}_F^A = 1\right] = 1,$$

sepse vlera e kthyer nga Fn do të jetë $\text{Fn}(0^{128}) = F_K(0^{128}) = 0^{128}$, kështu që A gjithmonë do të kthejë 1.

Shembull (Vazhdim)

- Le të jetë $F : \{0,1\}^k \times \{0,1\}^{128} \to \{0,1\}^{128}$ i përkufizuar me

$$F_K(x) = x.$$

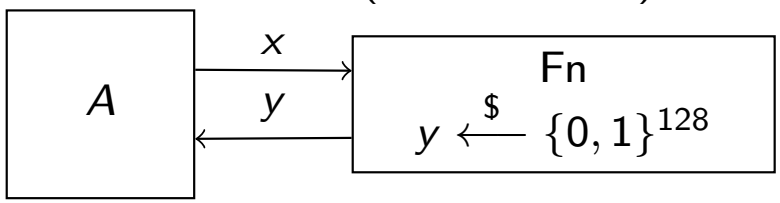
- FPR-kundërshtari A le të jetë i përkufizuar me

function A ▷ FPR-kundërshtari
  if $\text{Fn}(0^{128}) = 0^{128}$ **then return** 1
  else return 0
  end if
end function

Loja $\text{Rand}_{\{0,1\}^{128}}$

function $\text{Fn}(x)$
  $T[x] \xleftarrow{\$} \{0,1\}^{128}$
  return $T[x]$
end function

Bota ideale (e rastësishme)



- Atëherë,

$$\Pr\left[\text{Rand}^A_{\text{Range}(F)} = 1\right] = \Pr\left[\text{Fn}(0^{128}) = 0^{128}\right] = 2^{-128},$$

sepse $\text{Fn}(0^{128})$ është një string 128-bitësh i rastësishëm.

Shembull: Llogaritja e përparsisë

- Le të jetë $F : \{0,1\}^k \times \{0,1\}^{128} \to \{0,1\}^{128}$ i përkufizuar me

$$F_K(x) = x.$$

- FPR-kundërshtari A le të jetë i përkufizuar me

function A ▷ FPR-kundërshtari
  if $\mathrm{Fn}(0^{128}) = 0^{128}$ **then return** 1
  else return 0
  end if
end function

- Atëherë,

$$\mathrm{Adv}_F^{prf}(A) = \Pr\left[\mathrm{Real}_F^A = 1\right] - \Pr\left[\mathrm{Rand}_{\mathrm{Range}(F)}^A = 1\right] = 1 - 2^{-128}.$$

Masa e suksesit

- Le të jetë $F : \text{Keys}(F) \times \text{Dom}(F) \to \text{Range}(F)$ një familje funksionesh dhe A një fpr-kundërshtar. Atëherë,

$$\text{Adv}_F^{prf}(A) = \Pr\left[\text{Real}_F^A = 1\right] - \Pr\left[\text{Rand}_{\text{Range}(F)}^A = 1\right]$$

  është numër ndërmjet -1 dhe 1.
- Një përparsi e madhe (afër 1) do të thotë
  - A është duke shkuar mirë
  - F nuk është i sigurtë
- Një përparsi e vogël (afër 0 ose ≤ 0) do të thotë
  - A është duke shkuar keq
  - F i reziston sulmeve të ngritura nga A

Siguria e FPR

- Përparësia e kundërshtarit varet nga
  - strategjia e tij
  - resurset: koha (kompleksiteti) t dhe numri q i orakul pyetësorëve
- Siguria: F është një FPR (i sigurt) në qoftë se $\mathrm{Adv}_F^{prf}(A)$ është i vogël për çdo A që shfrytëzon sasi „praktike“ resursesh.
  - Shembull: Siguri 80-bitëshe mund të ketë domethënien se për çdo $n = 1, \ldots, 80$ kemi

$$\mathrm{Adv}_F^{prf}(A) \leq 2^{-n}$$

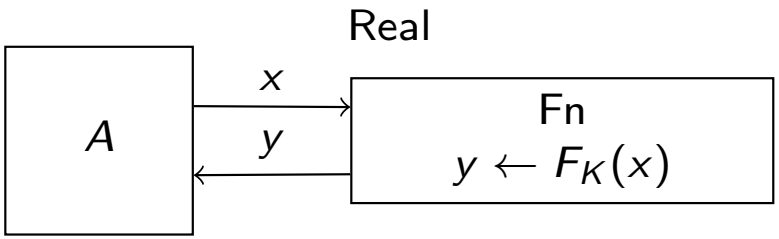
    për çfarëdo A me kohë dhe numër orakul pyetësorësh të shumtën 2^{80-n}.
- Pasiguria: F është i pasigurt (jo një FPR) në qoftë se ekziston A që shfrytëzon „pak“ resurse i cili arrin përparsi „të lartë“.

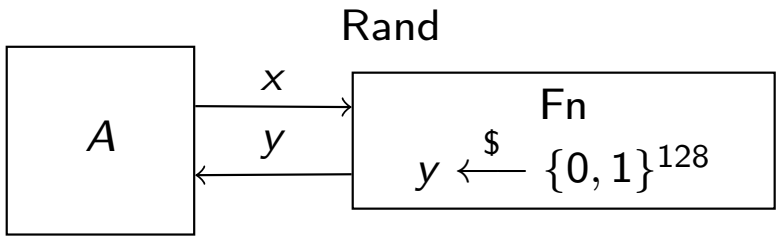
Shembull 1

- Përkufizojmë $F : \{0,1\}^k \times \{0,1\}^{128} \to \{0,1\}^{128}$ me

$$F_K(x) = x.$$

- A është F një FPR i sigurt?





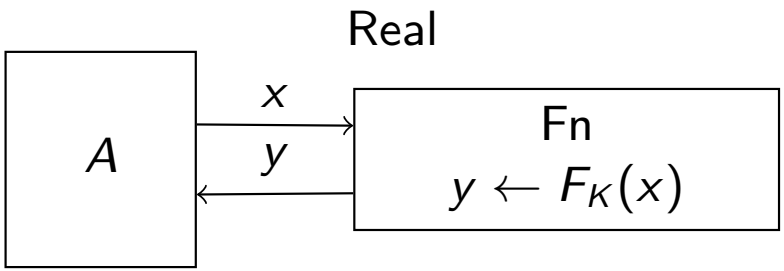
- A mund ta disenjojmë A ashtu që

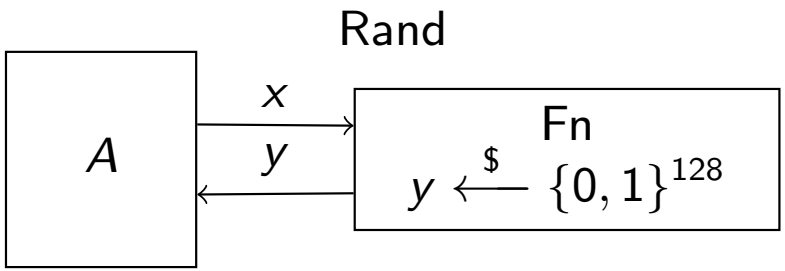
$$\mathrm{Adv}_F^{prf}(A) = \Pr\left[\mathrm{Real}_F^A = 1\right] - \Pr\left[\mathrm{Rand}_{\mathrm{Range}(F)}^A = 1\right]$$

të jetë afër 1?

- Dobësitë e F që mund të eksploatohen: $F_K(0^{128}) = 0^{128}$ për çdo K. Mund të përcaktojmë se në cilën botë ndodhemi duke testuar se a është $\mathrm{Fn}(0^{128}) = 0^{128}$.

Shembull 1: Kundërshtari





- $F_K(x) = x$
- Kundërshtari A:

function A
  if $\mathrm{Fn}(0^{128}) = 0^{128}$ **then return** 1
  else return 0
  end if
end function

▷ FPR-kundërshtari

Shembull 1: Analiza

- $F_K(x) = x$
- Kundërshtari A:

  function A ▷ FPR-kundërshtari
  if $\text{Fn}(0^{128}) = 0^{128}$ **then return** 1
  else return 0
  end if
  end function

- Tanimë analizuam rastin dhe pamë se

$$\Pr\left[\text{Real}_F^A = 1\right] = 1, \quad \Pr\left[\text{Rand}_{\text{Range}(F)}^A = 1\right] = 2^{-128}.$$

- Atëherë,

$$\text{Adv}_F^{prf}(A) = \Pr\left[\text{Real}_F^A = 1\right] - \Pr\left[\text{Rand}_{\text{Range}(F)}^A = 1\right] = 1 - 2^{-128},$$

  që d.m.th. se A është efikas.

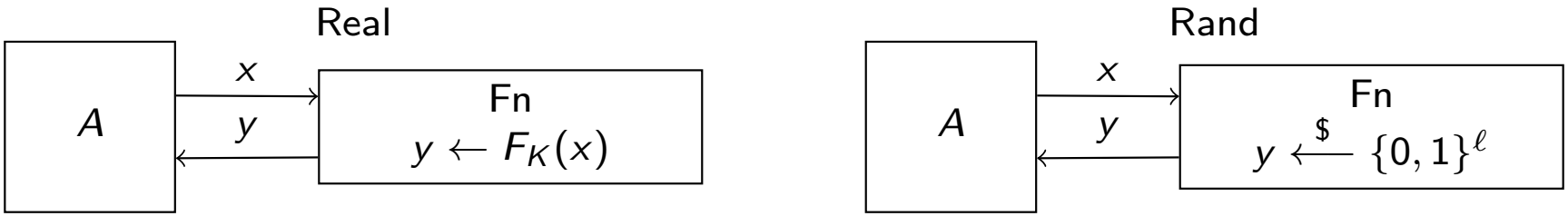
- Konkludimi: F nuk është një FPR is sigurt.

Shembull 2

- Përkufizojmë $F : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ me

$$F_K(x) = K \oplus x.$$

- A është F një FPR i sigurt?



- A mund ta disenjojmë A ashtu që

$$\mathrm{Adv}^{prf}_F(A) = \Pr\left[\mathrm{Real}^A_F = 1\right] - \Pr\left[\mathrm{Rand}^A_{\mathrm{Range}(F)} = 1\right]$$

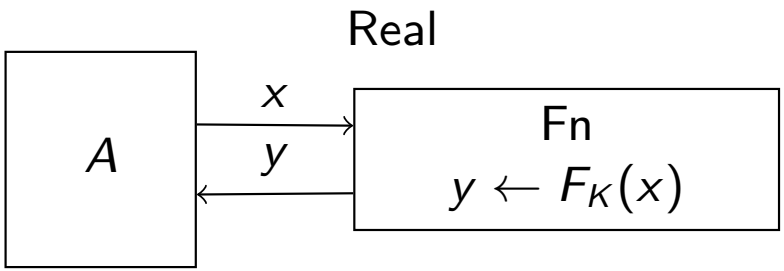
  të jetë afër 1?
- Dobësitë e F që mund të eksploatohen:

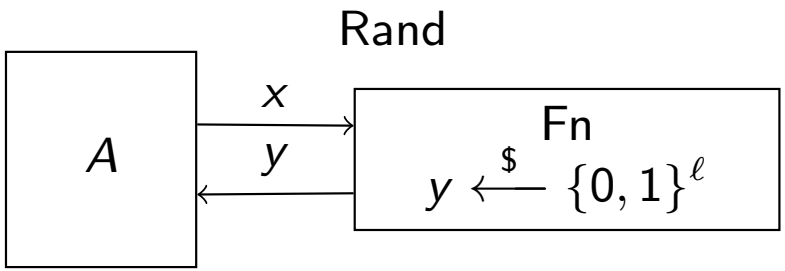
$$F_K(0^\ell) \oplus F_K(1^\ell) = (K \oplus 0^\ell) \oplus (K \oplus 1^\ell) = 1^\ell$$

  për çdo K. Mund të përcaktojmë se në cilën botë ndodhemi duke testuar se a është

$$\mathrm{Fn}(0^\ell) \oplus \mathrm{Fn}(1^\ell) = 1^\ell.$$

Shembull 2: Kundërshtari





- $F_K(x) = K \oplus x$
- Kundërshtari A:

function A
  if $\mathrm{Fn}(0^\ell) \oplus \mathrm{Fn}(1^\ell) = 1^\ell$ **then return** 1
  else return 0
  end if
end function

▷ FPR-kundërshtari

Shembull 2: Analiza e botës reale

- Le të jetë $F : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ i përkufizuar me

$$F_K(x) = K \oplus x.$$

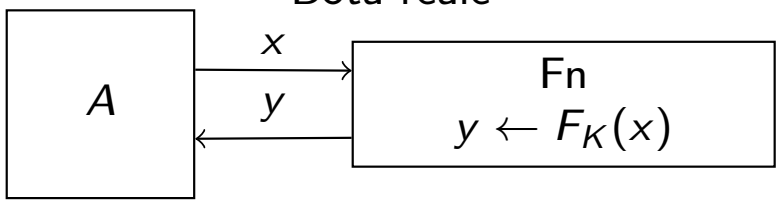
- FPR-kundërshtari A:

function A ▷ FPR-kundërshtari
  if $\mathrm{Fn}(0^\ell) \oplus \mathrm{Fn}(1^\ell) = 1^\ell$ **then return** 1
  else return 0
  end if
end function

Loja Real_F

$K \xleftarrow{\$} \{0,1\}^\ell$
function $\mathrm{Fn}(x)$
  return $F_K(x)$
end function

Bota reale



- Atëherë,

$$\Pr\left[\mathrm{Real}_F^A = 1\right] = 1,$$

sepse

$$\mathrm{Fn}(0^\ell) \oplus \mathrm{Fn}(1^\ell) = F_K(0^\ell) \oplus F_K(1^\ell) = (K \oplus 0^\ell) \oplus (K \oplus 1^\ell) = 1^\ell$$

Shembull 2: Analiza e botës ideale

- Le të jetë $F : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ i përkufizuar me

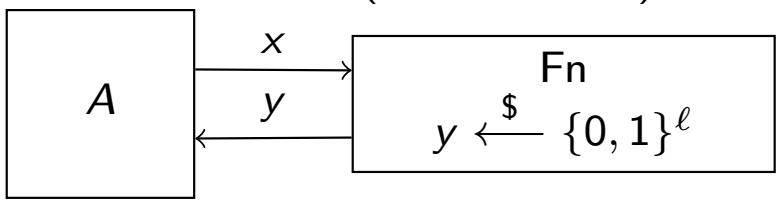
$$F_K(x) = K \oplus x.$$

- FPR-kundërshtari A:

function A ▷ FPR-kundërshtari
  if $\text{Fn}(0^\ell) \oplus \text{Fn}(1^\ell) = 1^\ell$ **then return** 1
  else return 0
  end if
end function

Loja $\text{Rand}_{\{0,1\}^\ell}$
function $\text{Fn}(x)$
  $T[x] \xleftarrow{\$} \{0,1\}^\ell$
  return $T[x]$
end function

Bota ideale (e rastësishme)



- Atëherë,

$$\Pr\left[\text{Rand}^A_{\{0,1\}^\ell} = 1\right] = \Pr\left[\text{Fn}(1^\ell) \oplus \text{Fn}(0^\ell) = 1^\ell\right] = 2^{-\ell},$$

sepse $\text{Fn}(0^\ell)$, $\text{Fn}(1^\ell)$ janë stringje të rastësishme 128-bitëshe.

Shembull 2: Konkludimi

- Le të jetë $F : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ i përkufizuar me

$$F_K(x) = K \oplus x.$$

- FPR-kundërshtari A:

function A ▷ FPR-kundërshtari
  if $\mathrm{Fn}(0^\ell) \oplus \mathrm{Fn}(1^\ell) = 1^\ell$ **then return** 1
  else return 0
  end if
end function

- Atëherë,

$$\mathrm{Adv}^{prf}_F(A) = \Pr\left[\mathrm{Real}^A_F = 1\right] - \Pr\left[\mathrm{Rand}^A_{\{0,1\}^\ell} = 1\right] = 1 - 2^{-\ell}.$$

- Konkludimi: F nuk është FPR i sigurt
  - A është efikas.

Problemi i ditëlindjes

- q njerëz $1, \ldots, q$ me ditëlindjet

$$y_1, \ldots, y_q \in \{1, \ldots, 365\}.$$

- Supozojmë se ditëlindja e secilit person është një ditë e rastësishme e vitit.
- Le të jetë

$$\begin{aligned} C(365, q) &= \Pr[\text{2 ose më tepër persona kanë të njëjtën ditëlindje}] \\ &= \Pr[y_1, \ldots, y_q \quad \text{nuk janë të gjithë të ndryshëm}]. \end{aligned}$$

- Sa është vlera e $C(365, q)$?
- Sa duhet të jetë e madhe q para se $C(365, q)$ të jetë së paku $\frac{1}{2}$?
- Intuicioni naiv:
  - $C(365, q) \approx \frac{q}{365}$
  - q duhet të jetë rreth 183
- Realiteti:
  - $C(365, q) \approx \frac{q^2}{2 \cdot 365}$
  - q duhet të jetë vetëm rreth 23

Vlera probabilitetesh ndeshjeje ditëlindjesh

- $C(365, q)$ është probabiliteti se ndonjë dy njerëz kanë të njëjtën ditëlindje në një dhomë me q njerëz me ditëlindje të rastësishme.

q	$C(365, q)$
15	0.253
18	0.347
20	0.411
21	0.444
23	0.507
25	0.569
27	0.627
30	0.706
35	0.814
40	0.891
50	0.970

Problemi i ditëlindjes (Vazhdim)

- Zgjedh $y_1, \ldots, y_q \xleftarrow{\$} \{1, \ldots, N\}$ dhe le të jetë

$$C(N, q) = \Pr[y_1, \ldots, y_q \quad \textbf{jo} \text{ të gjithë të ndryshëm}].$$

- Problemi i ditëlindjes: $N = 365$
- Fakt: $C(N, q) \approx \frac{q^2}{2N}$

Formula mbi ndeshjet e ditëlindjeve

- Le të jetë $y_1, \ldots, y_q \xleftarrow{\$} \{1, \ldots, N\}$. Atëherë,

$$\begin{aligned} 1 - C(N, q) &= \Pr[y_1, \ldots, y_q \quad \text{të gjithë të ndryshëm}] \\ &= 1 \cdot \frac{N-1}{N} \cdot \frac{N-2}{N} \cdots \frac{N-(q-1)}{N} \\ &= \prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right). \end{aligned}$$

- Prandaj

$$C(N, q) = 1 - \prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right).$$

Kufijtë e probabilitetit të ndeshjes së ditëlindjeve

- Le të jetë

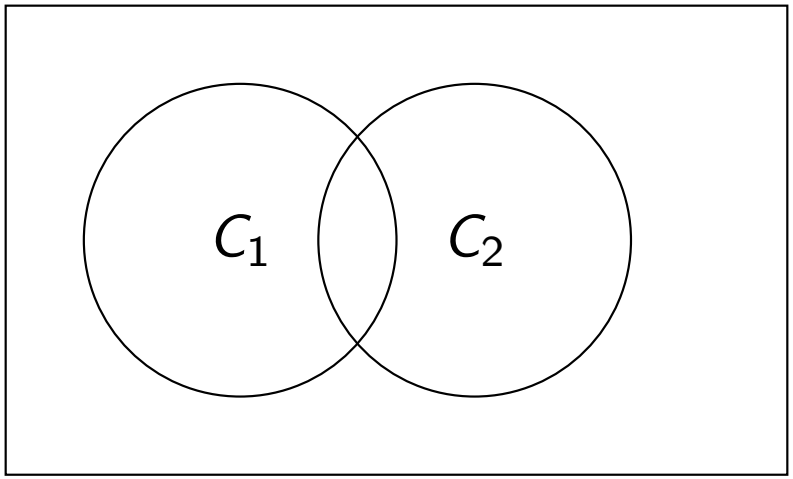
$$C(N,q) = \Pr[y_1, \ldots, y_q \quad \textbf{jo} \text{ të gjithë të ndryshëm}].$$

- Fakt:

$$0.3 \cdot \frac{q(q-1)}{N} \leq C(N,q) \leq 0.5 \cdot \frac{q(q-1)}{N},$$

ku kufiri i poshtëm vlen për $1 \leq q \leq \sqrt{2N}$.

Kufiri i probabilitetit të unionit



$$\begin{aligned}\Pr[C_1 \vee C_2] &= \Pr[C_1] + \Pr[C_2] - \Pr[C_1 \wedge C_2] \\ &\leq \Pr[C_1] + \Pr[C_2]\end{aligned}$$

- Në rastin e përgjithshëm

$$\Pr[C_1 \vee C_2 \vee \cdots \vee C_q] \leq \Pr[C_1] + \Pr[C_2] + \cdots + \Pr[C_q]$$

Pohime ndihmëse

- Shuma aritmetike

$$0 + 1 + 2 + \cdots + (q-1) = \frac{q(q-1)}{2}$$

Kufijtë e probabilitetit... (Vazhdim)

- Le të jetë

$$C(N,q) = \Pr[y_1, \ldots, y_q \quad \textbf{jo} \text{ të gjithë të ndryshëm}].$$

- Atëherë,

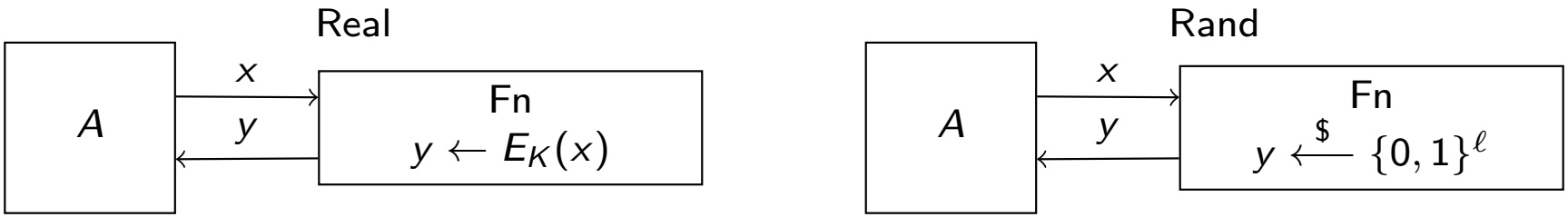
$$C(N,q) \leq 0.5 \cdot \frac{q(q-1)}{N}.$$

- Vërtetimi i kufirit të sipërm: Le të jetë C_i ngjarja $y_i \in \{y_1, \ldots, y_{i-1}\}$. Atëherë,

$$\begin{aligned} C(N,q) &= \Pr[C_1 \vee C_2 \vee \cdots \vee C_q] \\ &\leq \Pr[C_1] + \Pr[C_2] + \cdots + \Pr[C_q] \\ &= \frac{0}{N} + \frac{1}{N} + \cdots + \frac{q-1}{N} \\ &= \frac{q(q-1)}{2N}. \end{aligned}$$

Blok shifruesit si FPR

- Le të jetë $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ një blok shifrues.



- A mund ta disenjojmë A ashtu që

$$\mathrm{Adv}_F^{prf}(A) = \Pr\left[\mathrm{Real}_F^A = 1\right] - \Pr\left[\mathrm{Rand}_{\mathrm{Range}(F)}^A = 1\right]$$

të jetë afër 1?

Sulmi i ditëlindjes mbi blok shifrues

- Le të jetë
$$E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$$
një blok shifrues.
- Kundërshtari A

  Le të jenë $x_1, \ldots, x_q \in \{0,1\}^\ell$ të ndryshme
  for $i = 1, \ldots, q$ **do**
    $y_i \leftarrow \mathrm{Fn}(x_i)$
  end for
  if $y_1, \ldots, y_q$ janë të ndryshme **then**
    return 1
  else return 0
  end if

Analiza e botës reale

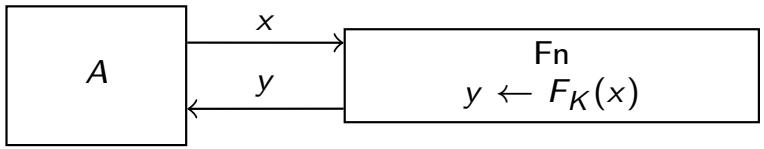
- Le të jetë
$$E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$$
një blok shifrues.
- Kundërshtari A

  Le të jenë $x_1, \ldots, x_q \in \{0,1\}^\ell$ të ndryshme
  for $i = 1, \ldots, q$ **do**
  $y_i \leftarrow \mathrm{Fn}(x_i)$
  end for
  if $y_1, \ldots, y_q$ janë të ndryshme **then**
  return 1
  else return 0
  end if

Loja Real_E

$K \xleftarrow{\$} \{0,1\}^k$
function $\mathrm{Fn}(x)$
return $E_K(x)$
end function

Bota reale



- Atëherë,
$$\Pr\left[\mathrm{Real}_F^A = 1\right] = 1,$$
sepse $y_1, \ldots, y_q$ do të jenë të ndryshme meqë E_K është permutacion.

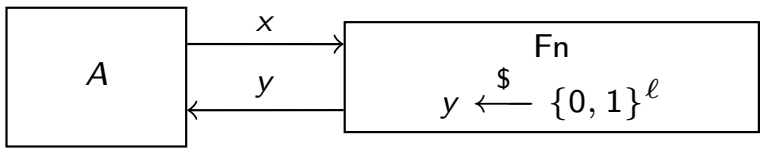
Analiza e botës ideale

- Le të jetë
$$E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$$
një blok shifrues.
- Kundërshtari A

  Le të jenë $x_1, \ldots, x_q \in \{0,1\}^\ell$ të ndryshme
  for $i = 1, \ldots, q$ **do**
    $y_i \leftarrow \mathrm{Fn}(x_i)$
  end for
  if $y_1, \ldots, y_q$ janë të ndryshme **then**
    return 1
  else return 0
  end if

Loja $\mathrm{Rand}_{\{0,1\}^\ell}$
function Fn(x)
  $T[x] \xleftarrow{\$} \{0,1\}^\ell$
  return $T[x]$
end function

Bota ideale (e rastësishme)



- Atëherë,
$$\Pr\left[\mathrm{Rand}^A_{\{0,1\}^\ell} = 1\right] = \Pr\left[y_1, \ldots, y_q \quad \text{janë të ndryshme}\right] = 1 - C(2^\ell, q),$$
sepse $y_1, \ldots, y_q$ janë janë zgjedhur në mënyrë të rastësishme nga $\{0,1\}^\ell$.

Sulmi i ditëlindjes mbi blok shifrues: Konkludimi

- Le të jetë
$$E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$$
një blok shifrues.
- Kundërshtari A

  Le të jenë $x_1, \ldots, x_q \in \{0,1\}^\ell$ të ndryshme
  for $i = 1, \ldots, q$ **do**
  $y_i \leftarrow \mathrm{Fn}(x_i)$
  end for
  if $y_1, \ldots, y_q$ janë të ndryshme **then**
  return 1
  else return 0
  end if

- Atëherë,
$$\begin{aligned}\mathrm{Adv}_F^{prf}(A) &= \Pr\left[\mathrm{Real}_F^A = 1\right] - \Pr\left[\mathrm{Rand}_{\{0,1\}^\ell}^A = 1\right] \\ &= 1 - (1 - C(2^\ell, q)) = C(2^\ell, q) \\ &\geq 0.3 \cdot \frac{q(q-1)}{2^\ell}.\end{aligned}$$
- Kështu,
$$q \approx 2^{\ell/2} \implies \mathrm{Adv}_F^{prf}(A) \approx 1.$$

Sulmi i ditëlindjes mbi blok shifrues: Konkludimi (Vazhdim)

- Konkludimi: Në qoftë se $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ është një blok shifrues, ekziston një sulm mbi të si FPR i cili ka sukses në rreth $2^{\ell/2}$ pyetësorë.

	ℓ	$2^{\ell/2}$	Statusi
DES, 2DES, 3DES3	64	2^{32}	Jo i sigurt
AES	128	2^{64}	I sigurt

KR-siguria kundrejt PRF-sigurisë

- Kemi shqyrtuar dy metrika të mundshme sigurie për një blok shifrues E:
  - *KR-siguria:* Duhet të jetë e vështirë të kthehet çelësi K nga shembuj hyrje/dalje të E_K
  - *PRF-siguria:* Duhet të jetë e vështirë të dallohet sjellja hyrje/dalje e E_K nga ajo e një funksioni të rastësishëm.
- Pyetje: A është e mundur që E të jetë:
  - PRF-i sigurt, por
  - **jo** KR-i sigurt?

KR-siguria kundrejt PRF-sigurisë (Vazhdim)

- Pyetje: A është e mundur që E të jetë PRF-i sigurt, por jo KR-i sigurt?
- Shumë e rëndësishme, sepse:
  - U pajtuam që KR-siguria është e nevojshme
  - Po pohojmë që PRF-siguria është e mjaftueshme

  për përdorim të sigurt të E.
- Fatmirësisht, përgjegjja e pyetjes së mësipërme është **jo**.
- Fakt: PRF-siguria implikon
  - KR-sigurinë
  - Shumë atribute tjera sigurie.

KR-siguria

- Le të jetë $F : \text{Keys}(F) \times \text{Dom}(F) \to \text{Range}(F)$ një familje funksionesh.
- Loja KR_F^A

  $K \xleftarrow{\$} \text{Keys}(F)$
  function $\text{Fn}(x)$
  return $F_K(x)$
  end function

- Kundërshtari A:

  Kërko një K'
  return $K = K'$

- Orakuli lejon sulm të mesazhit të zgjedhur.
- kr-përparësia e A përkufizohet me

$$\text{Adv}_F^{kr}(A) = \Pr\left[\text{KR}_F^A = 1\right]$$

- F është i sigurt kundër kthimit të çelësit në qoftë se $\text{Adv}_F^{kr}(A)$ është „e vogël“ për çdo A me resurse praktike.

Shembull 3

- Le të jetë $k = L\ell$ dhe le të jetë $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^L$ i përkufizuar me

$$F_K(x) = \begin{bmatrix} K[1,1] & K[1,2] & \dots & K[1,\ell] \\ K[2,1] & K[2,2] & \dots & K[2,\ell] \\ \vdots & & & \vdots \\ K[L,1] & K[L,2] & \dots & K[L,\ell] \end{bmatrix} \cdot \begin{bmatrix} x[1] \\ x[2] \\ \vdots \\ x[\ell] \end{bmatrix} = \begin{bmatrix} y[1] \\ y[2] \\ \vdots \\ y[L] \end{bmatrix}$$

- Këtu, bitët e matricës (dhe vektorëve) janë bitët e çelësit (dhe të bloqeve të mesazhit dhe të tekstit të shifruar).
- Aritmetika është sipas modulit 2.
- Pyetje: A është F i sigurt kundër kthimit të çelësit?
- Përgjegjja: Jo!

Shembull 3 (Vazhdim)

- Për $1 \leq j \leq \ell$ le të jetë

$$e_j = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

vektori i j-të unitar, me komponentën e j-të 1 dhe të gjitha komponentat tjera 0.

- Atëherë

$$F_K(e_j) = \begin{bmatrix} K[1,1] & K[1,2] & \dots & K[1,\ell] \\ K[2,1] & K[2,2] & \dots & K[2,\ell] \\ \vdots & & & \vdots \\ K[L,1] & K[L,2] & \dots & K[L,\ell] \end{bmatrix} \cdot \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} K[1,j] \\ K[2,j] \\ \vdots \\ K[L,j] \end{bmatrix}$$

.

KR-sulmi mbi Shembullin 3

- Kundërshtari A:

  $K \leftarrow \varepsilon$ ▷ ε është stringu bosh
  for $j = 1, \ldots, \ell$ **do**
  $y_j \leftarrow \mathrm{Fn}(e_j)$
  $K' \leftarrow K' || y_j$
  end for
  return K'

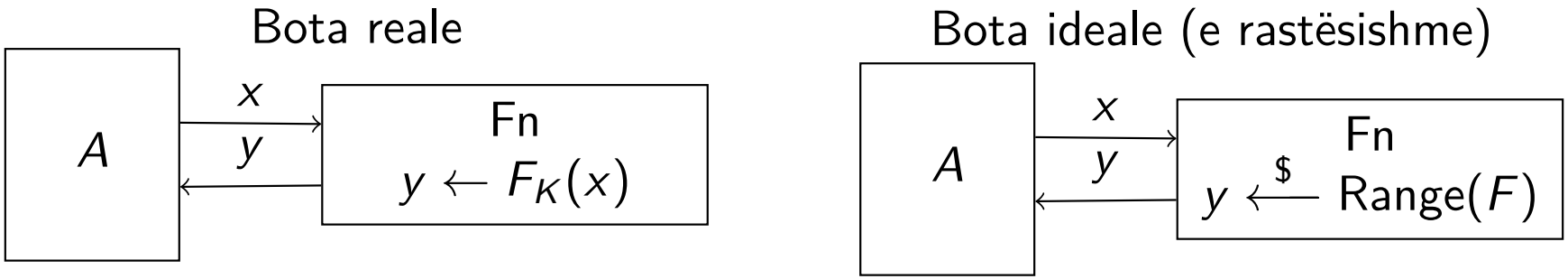
- Atëherë

$$\mathrm{Adv}^{kr}_F(A) = \Pr\left[\mathrm{KR}^A_F = 1\right] = 1$$

- Kompleksiteti kohor i A është $t = \mathrm{O}(\ell^2 L)$ meqë bën $q = \ell$ invokime orakulit të vet dhe çdo kompjutim i $\mathrm{Fn} = F_K$ ka kompleksitet $\mathrm{O}(L\ell)$ (si shumëzim i një matrice $L \times \ell$ me një vektor të gjatësisë ℓ).
- Prandaj, F është i pasigurt kundrejt kthimit të çelësit.

Pse PRF-siguria implikon KR-sigurinë?

- **Pohim:** KR-i **pa**sigurt $\implies$ PRF-i **pa**sigurt



- Në qoftë se më jepni një metodë B për të mposhtur KR-sigurinë, unë mund të disenjoj një metodë A për të mposhtur PRF-sigurinë.
- Çfarë bën A:
  - Përdor B për të gjetur K'
  - Teston se a është $Fn(x) = F_{K'}(x)$ për ndonjë x të ri
  - Në qoftë se është e vërtetë, vendos se është në botën reale.

Pse PRF-siguria implikon KR-sigurinë? (Vazhdim)

- Problemi: Për të funksionuar B (d.m.th. për të gjetur K'), duhet të ketë shembuj hyrje/dalje nën F_K.
- E zgjidhim ashtu që A i ofron orakulin e vet, d.m.th. i jep B shemmbuj hyrje/dalje nën Fn.
  - Kjo është korrekte në qoftë se A ndodhet në botën reale, por jo në qoftë se ndodhet në botën e rastësishme.
  - Mirëpo, mund të vërtetojmë se funksionon.

Në qoftë se F është FPR, atëherë është KR-i sigurt

- Është dhënë: $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^L$
- Është dhënë: Një FR-kundërshtar efikas B
- Konstrukto: Një PRF-kundërshtar efikas A të tillë që

$$\mathrm{Adv}_F^{kr}(B) \leq \mathrm{Adv}_F^{prf}(A) + \boxdot$$

- Si të konkludojmë se PRF-i sigurt $\implies$ KR-i sigurt?
- Rregulla e kontrapozicionit: F **jo** KR-i sigurt $\implies$ F **jo** PRF-i sigurt
  - Skema e vërtetimit:

$$\begin{aligned} F \textbf{ jo} \text{ KR-i sigurt} &\implies \mathrm{Adv}_F^{kr}(B) \text{ e madhe} \\ &\implies \mathrm{Adv}_F^{prf}(A) \text{ e madhe} \\ &\implies F \textbf{ jo} \text{ PRF-i sigurt} \end{aligned}$$

Vërtetimi me reduksion

- A do të ekzekutojë B si nënprogram
- Vetë A do t'u përgjigjet orakul pyetësorëve të B, duke i dhënë B përshtypjen se B është në botën e vet korrekte.

Në qoftë se F është FPR, atëherë KR-i sigurt (Vazhdim)

- Është dhënë: $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^L$
- Është dhënë: Një FR-kundërshtar efikas B
- Konstrukto: Një PRF-kundërshtar efikas A të tillë që

$$\mathrm{Adv}_F^{kr}(B) \leq \mathrm{Adv}_F^{prf}(A) + \boxdot$$

- Ideja:
  - A shfrytëzon B të gjejë çelësin K'
  - Teston se a është K' çelësi korrekt
- Problemet:
  - B ka nevojë për një F_K orakul, të cilin A e ka vetëm në botën reale
  - Çfarë në qoftë se A ndodhet në botën imagjinare?
- Si adresohen:
  - A i jep B orakulin e vet Fn
  - Teston duke shikuar se a pajtohet $F_{K'}$ me Fn në një pikë të re x.

Në qoftë se F është FPR, atëherë KR-i sigurt (Vazhdim)

- Është dhënë: $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^L$
- Është dhënë: Një FR-kundërshtar efikas B
- Konstrukto: Një PRF-kundërshtar efikas A të tillë që

$$\mathrm{Adv}^{kr}_F(B) \leq \mathrm{Adv}^{prf}_F(A) + \boxdot$$

- Kundërshtari A:

$i \leftarrow 0$
$K' \leftarrow \mathrm{KR}_{FSim}(B)$
$x \xleftarrow{\$} \{0,1\}^\ell - \{x_1, \ldots, x_i\}$
if $F_{K'}(x) = \mathrm{Fn}(x)$ **then**
    return 1
else return 0
end if

function $FSim(x)$
    $i \leftarrow i + 1$
    $x_i \leftarrow x$
    $y_i \leftarrow \mathrm{Fn}(x)$
    return y_i
end function

Analiza

- Kundërshtari A:

$i \leftarrow 0$
$K' \leftarrow \mathrm{KR}_{FSim}(B)$
$x \xleftarrow{\$} \{0,1\}^{\ell} - \{x_1, \ldots, x_i\}$
if $F_{K'}(x) = \mathrm{Fn}(x)$ **then**
  return 1
else return 0
end if

function $FSim(x)$
  $i \leftarrow i + 1$
  $x_i \leftarrow x$
  $y_i \leftarrow \mathrm{Fn}(x)$
  return y_i
end function

- Në qoftë se $\mathrm{Fn} = F_K$, atëherë $K' = K$ me probabilitet $\mathrm{Adv}^{kr}_F(B) = \Pr\left[\mathrm{KR}^B_F = 1\right]$, prandaj

$$\Pr\left[\mathrm{Real}^A_F = 1\right] \geq \mathrm{Adv}^{kr}_F(B).$$

- Në qoftë se Fn është funksion i rastësishëm, atëherë meqë $x \notin \{x_1, \ldots, x_i\}$

$$\Pr\left[\mathrm{Rand}^A_{\mathrm{Range}(F)} = 1\right] = 2^{-L}.$$

- Kështu,

$$\mathrm{Adv}^{prf}_F(A) = \Pr\left[\mathrm{Real}^A_F = 1\right] - \Pr\left[\mathrm{Rand}^A_{\mathrm{Range}(F)} = 1\right] \geq \mathrm{Adv}^{kr}_F(B) - 2^{-L}.$$

Në qoftë se F është FPR, atëherë KR-i sigurt (Vazhdim)

Teoremë

Le të jetë $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^L$ *një familje funksionesh dhe* B *një kr-kundërshtar që bën* q *orakul pyetësorë. Atëherë, ekziston një prf-kundërshtar* A *i cili bën* $q+1$ *orakul pyetësorë i tillë që*

$$\mathrm{Adv}^{kr}_F(B) \leq \mathrm{Adv}^{prf}_F(A) + 2^{-L}.$$

Kompleksiteti kohor i B *është ai i* A *plus* $\mathrm{O}(q\ell)$).

Rrjedhim

$$F \text{ është PRF-i sigurt} \implies F \text{ është KR-i sigurt.}$$

Supozime

- AES, DES janë blok shifrues të mirë në kuptim të të qenit PRF-të sigurtë në shkallë maksimale të mundur.
- **Deri më tani,** sulmi më i suksesshëm kundër tyre mbetet sulmi i ditëlindjes.