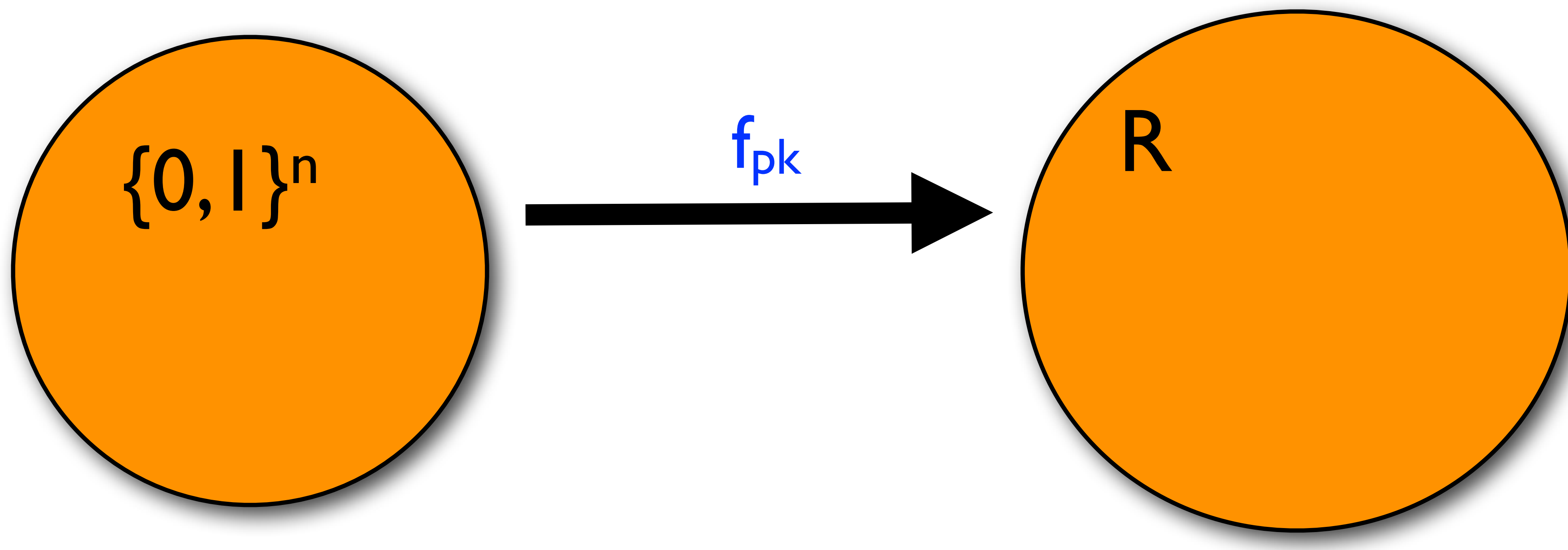
Identity-based (Lossy) Trapdoor Functions

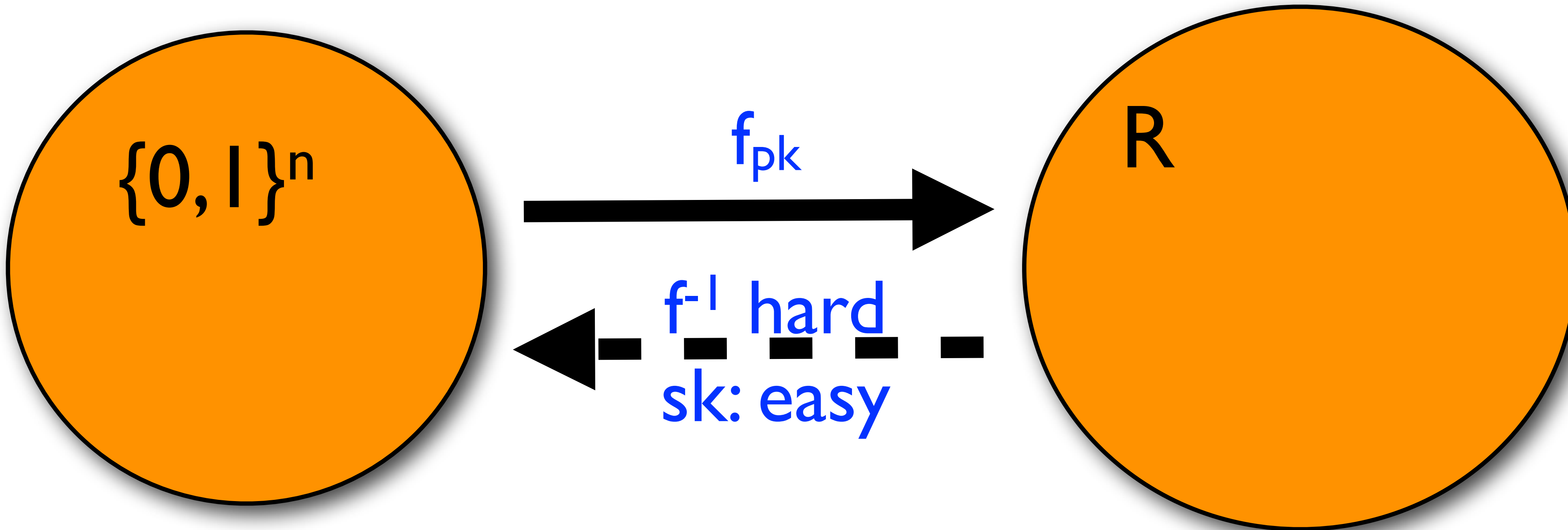
and Applications

Mihir Bellare, Eike Kiltz, Chris Peikert, Brent Waters

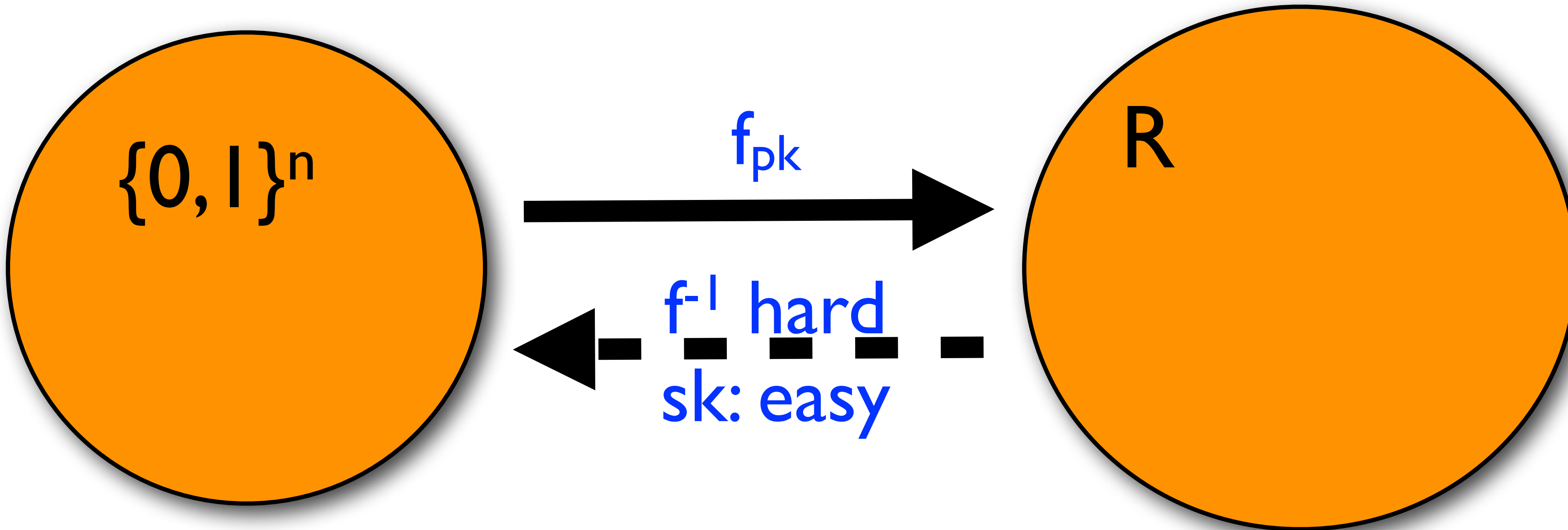
Injective trapdoor function



Injective trapdoor function



Injective trapdoor function



- Example: RSA [RSA 78]
- TDF: most fundamental crypto primitive
- History: 6 years before encryption [GM 84]

Security notions

Security notions

- One-wayness: Gen $\to$ (pk, sk)

  pk, $f_{pk}(x) \to x$ hard (random x)

Security notions

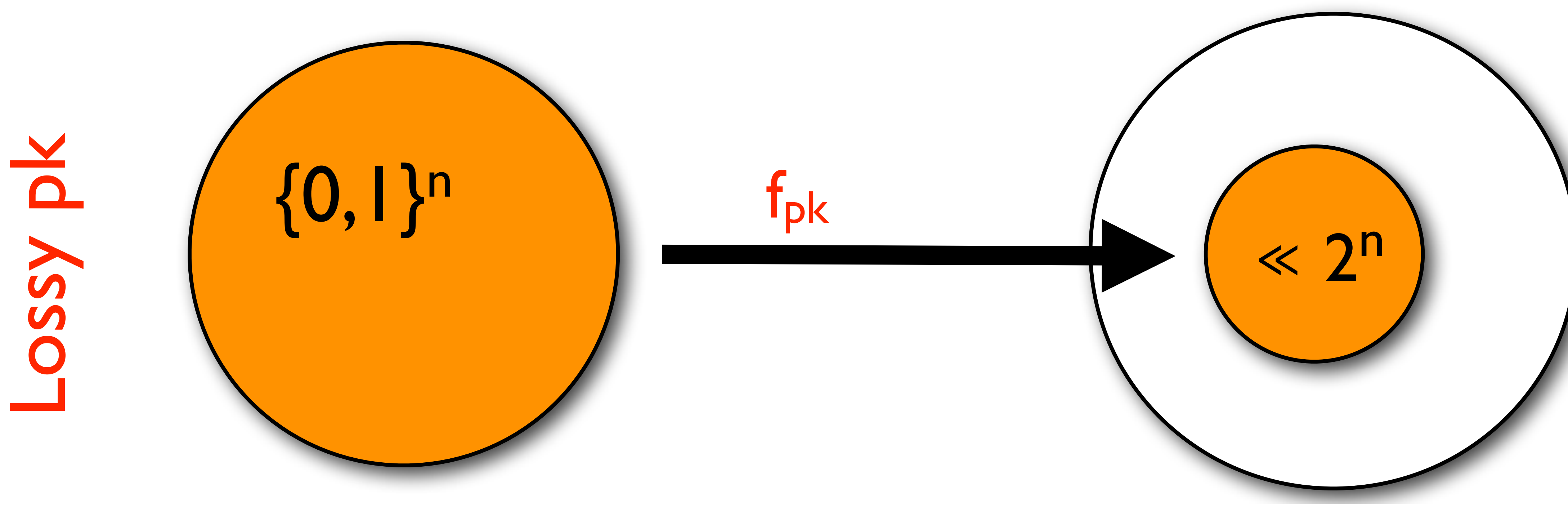
- One-wayness: Gen → (pk, sk)

  pk, $f_{pk}(x)$ → x hard (random x)

- Lossiness [PW08]: exists Gen' → "fake" pk:

  1. pk $\approx_c$ pk

  2. Range(f_{pk}) $\ll 2^n$



Lossy trapdoor functions

Lossy trapdoor functions

- Basic primitives:
  One-way TDFs, CR hashing

Lossy trapdoor functions

- Basic primitives:
  One-way TDFs, CR hashing
- Advanced encryption:
  CCA security, selective opening security, deterministic PKE, hedged PKE

Lossy trapdoor functions

- Basic primitives:
  One-way TDFs, CR hashing
- Advanced encryption:
  CCA security, selective opening security, deterministic PKE, hedged PKE
- Constructions:
  DDH, QR, Paillier, LWE, Phi-Hiding, ...

Our paper

Trapdoor functions in ID-based framework

1. Definitions
2. Applications
3. Constructions
   - From bilinear maps
   - From lattices

ID-based encryption (IBE)

- Gen $\to$ (pk,sk)
- Enc(pk,ID,m) $\to$ c for ID$\in\{0,1\}^n$
- Extract(sk,ID) $\to$ trapdoor sk_{ID}
- Dec(sk_{ID},ID,c) = m

ID-based encryption (IBE)

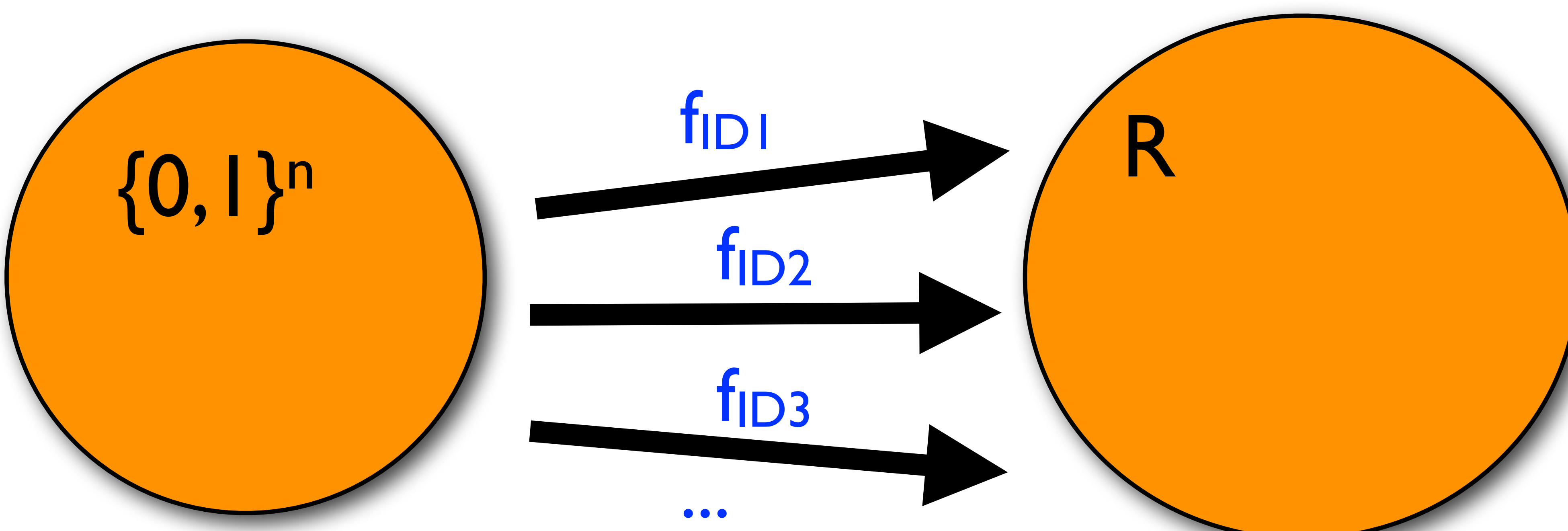
- Gen $\rightarrow$ (pk,sk)
- Enc(pk,ID,m) $\rightarrow$ c for $ID \in \{0,1\}^n$
- Extract(sk,ID) $\rightarrow$ trapdoor sk_{ID}
- Dec(sk_{ID},ID,c) = m

History:

- IBE [S84, BF03]
- ID-based signatures, ...

ID-based trapdoor functions

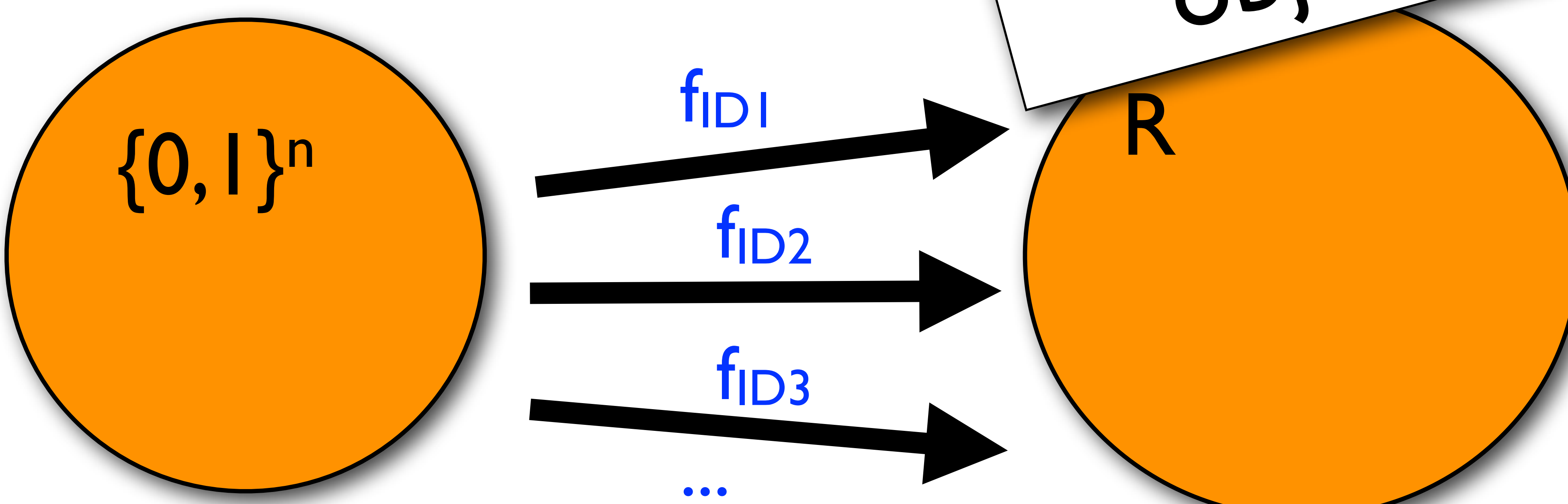
- Gen → (pk,sk)
- Eval(pk,ID,·) = $f_{ID} : \{0,1\}^n \rightarrow R$ for $ID \in \{0,1\}^n$
- Extract(sk,ID) → trapdoor sk_{ID}
- Invert(sk_{ID},·) = $f_{ID}^{-1}(\cdot)$



ID-based trapdoor functions

- Gen → (pk,sk)
- $\boxed{\textbf{Eval}(pk, ID, \cdot) = f_{ID} : \{0,1\}^n \to R \text{ for } ID \in \{0,1\}^n}$
- Extract(sk,ID) → trapdoor sk_{ID}
- Invert(sk_{ID}, ·) = $f_{ID}^{-1}(\cdot)$

Natural object!



Security?

Intuition: $f_{ID^*}(.)$ “secure” even given sk_{ID} for $ID \neq ID^*$

secure	Selective	Adaptive
one-way	ID-OW-S	ID-OW-A
lossy	ID-LS-S	ID-LS-A

One-wayness

Exp ID-OW-S

Selective adversary

chose ID^*

$\xleftarrow{\mathrm{ID}^*}$

One-wayness

Exp ID-OW-S		Selective adversary
	$\xleftarrow{ID^*}$	chose ID^*
$(pk,sk) \leftarrow Gen$	$\xrightarrow{pk}$	

One-wayness

Exp ID-OW-S

$(pk, sk) \leftarrow Gen$

Selective adversary

chose ID^*

ID^* ←

pk →

$ID_i \neq ID^*$ ←

sk_{ID_i} →

One-wayness

Exp ID-OW-S

$(pk, sk) \leftarrow Gen$

$x \in \{0,1\}^n$

Win: $x = x'$

Selective adversary

chose ID^*

$\xleftarrow{ID^*}$

$\xrightarrow{pk}$

$\xleftarrow{ID_i \neq ID^*}$

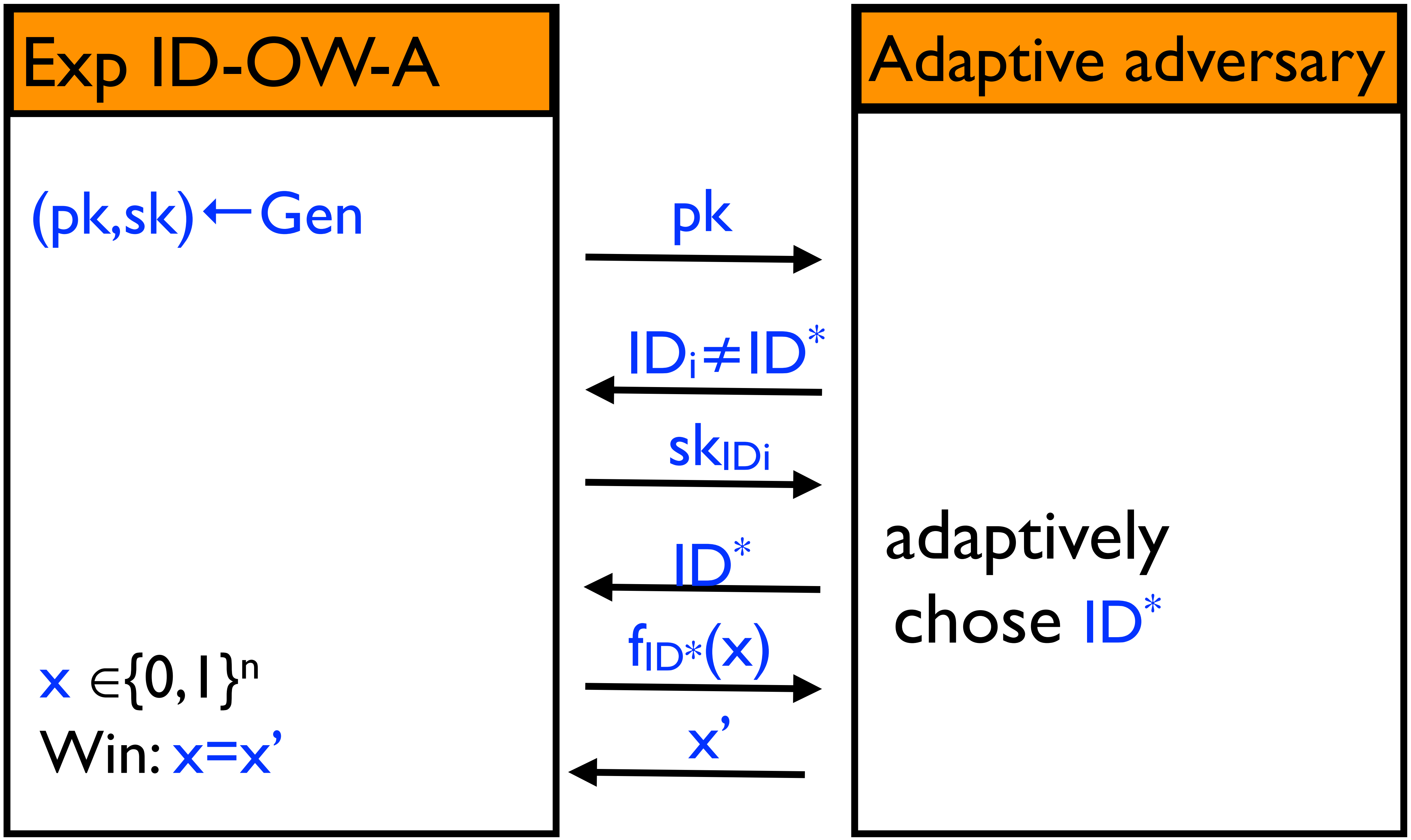
$\xrightarrow{sk_{IDi}}$

$\xrightarrow{f_{ID^*}(x)}$

$\xleftarrow{x'}$

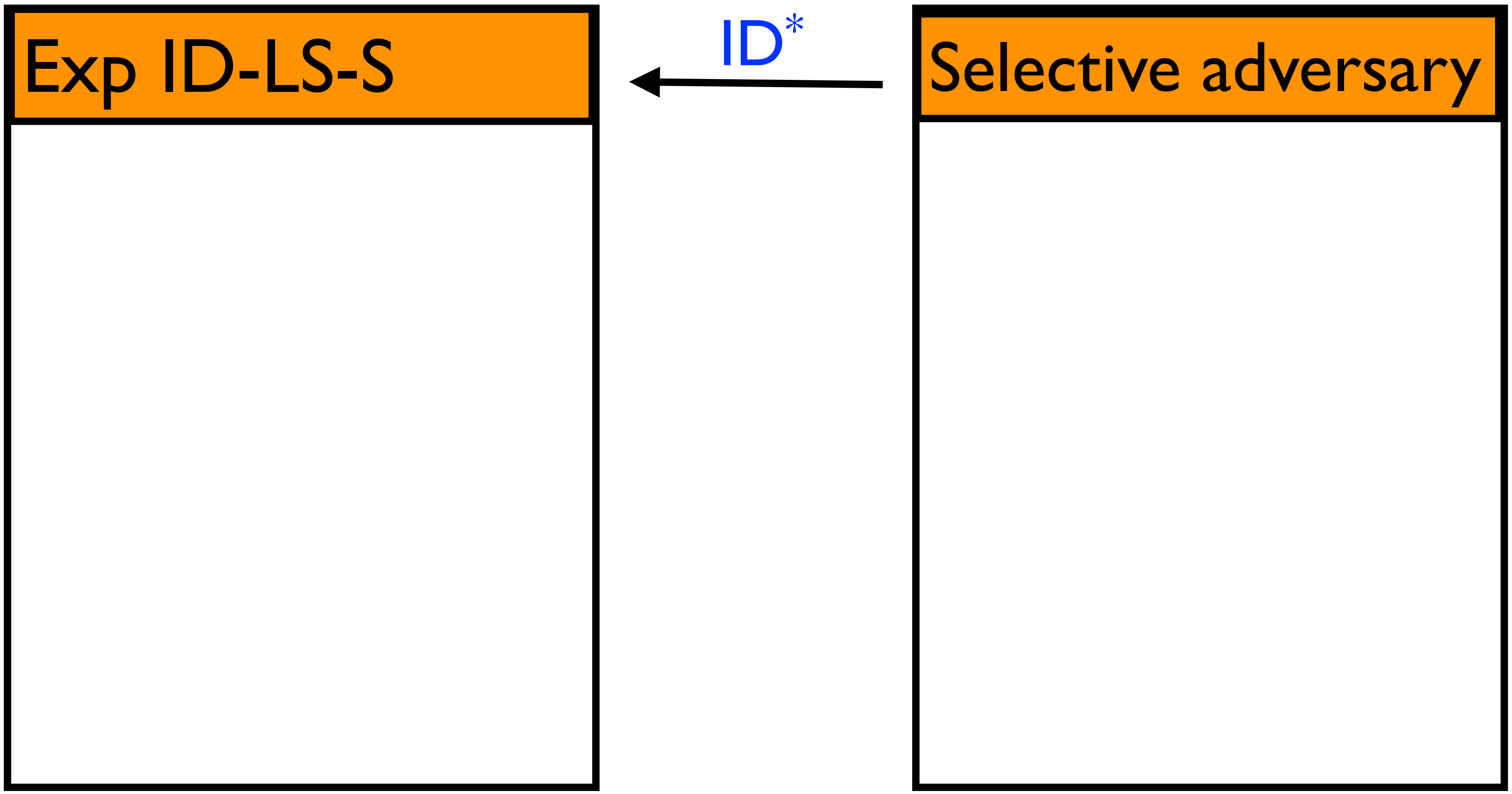
Def: One-way $\Leftrightarrow$ Pr[Adversay wins] = negl

One-wayness



Def: One-way ⇔ Pr[Adversay wins] = negl

Selective lossiness



Selective lossiness

Exp ID-LS-S

(pk,sk)←Gen

vs.

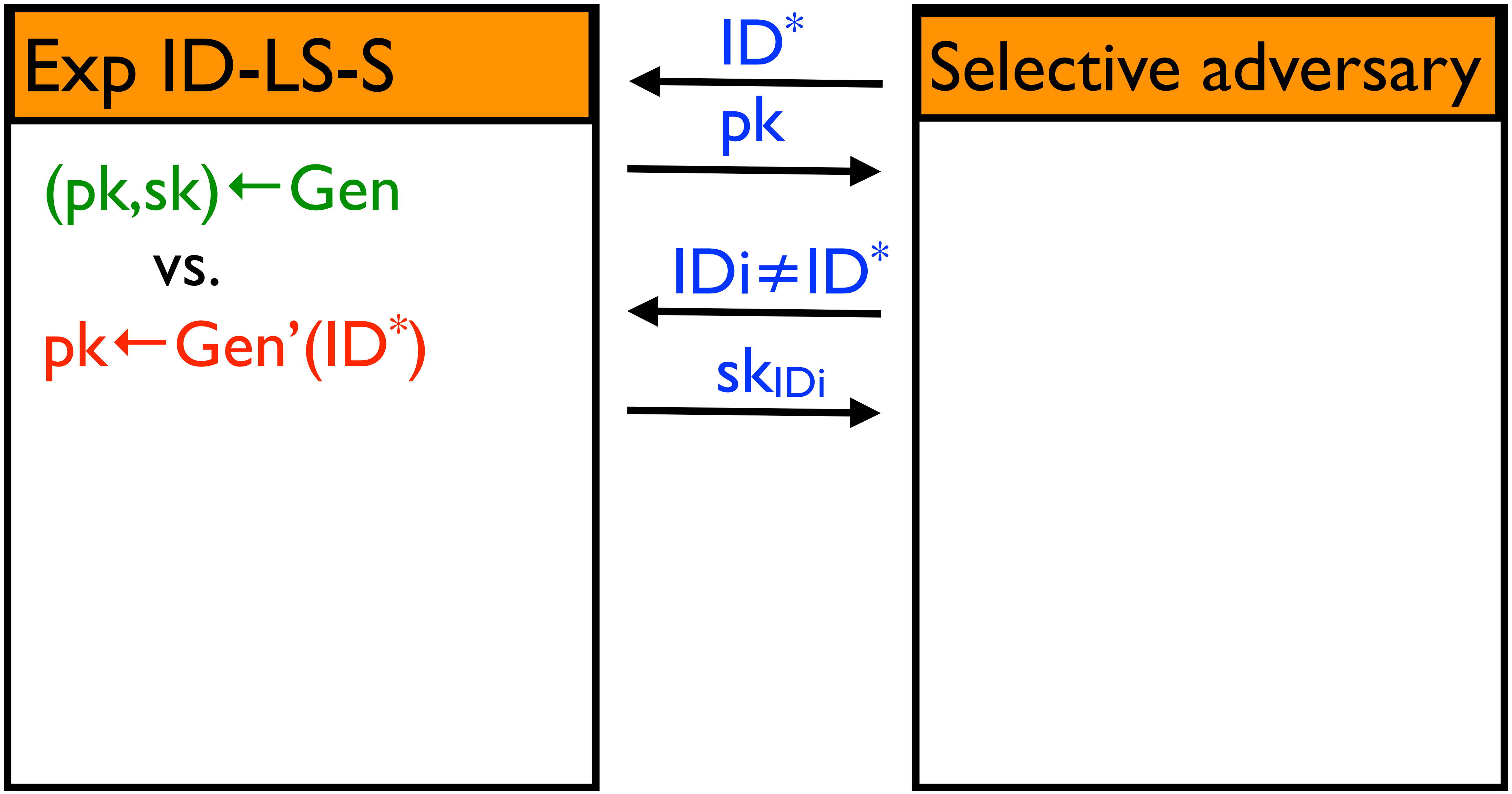
pk←Gen'(ID*)

$\xleftarrow{\text{ID}^*}$

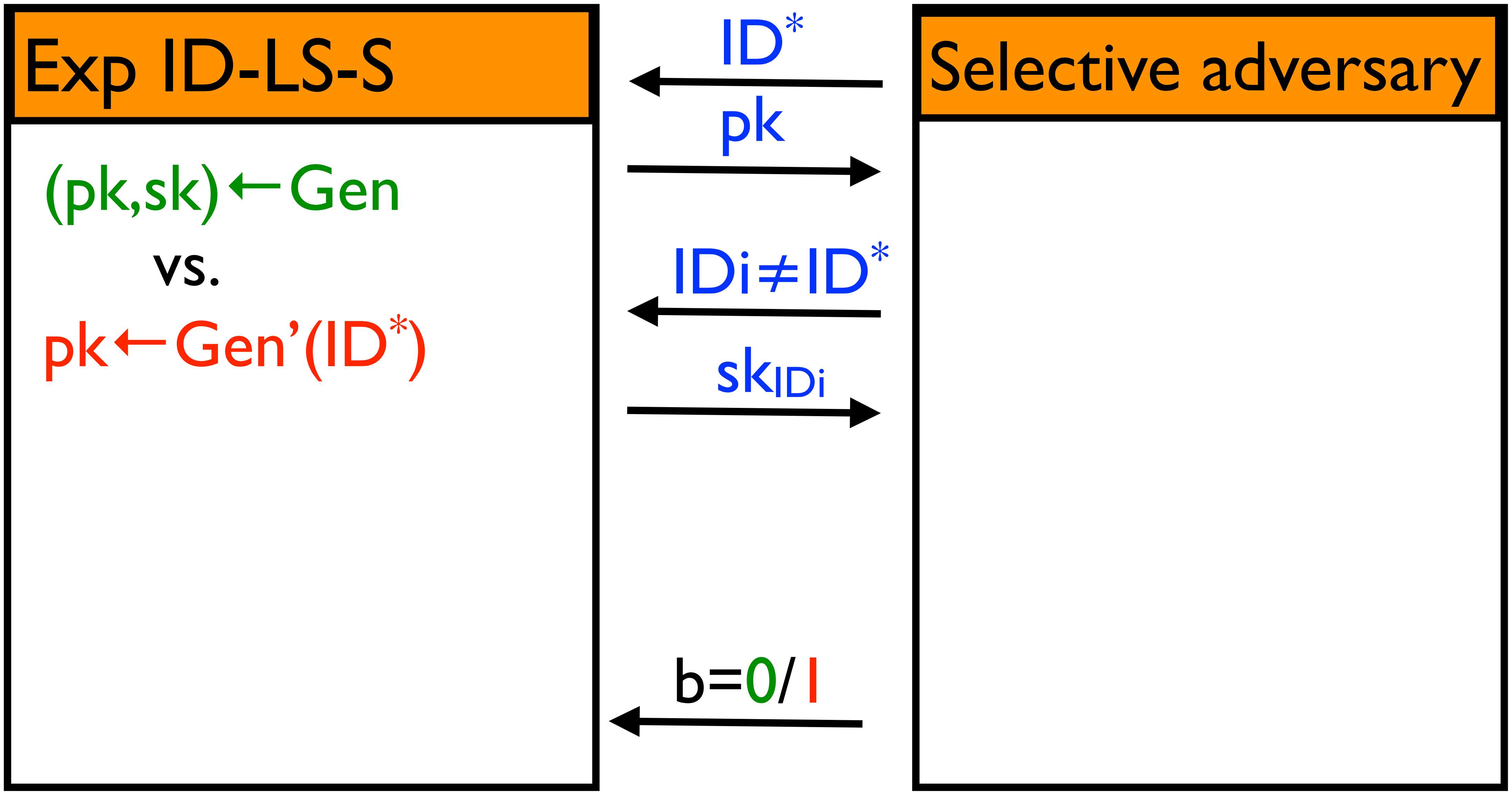
$\xrightarrow{\text{pk}}$

Selective adversary

Selective lossiness

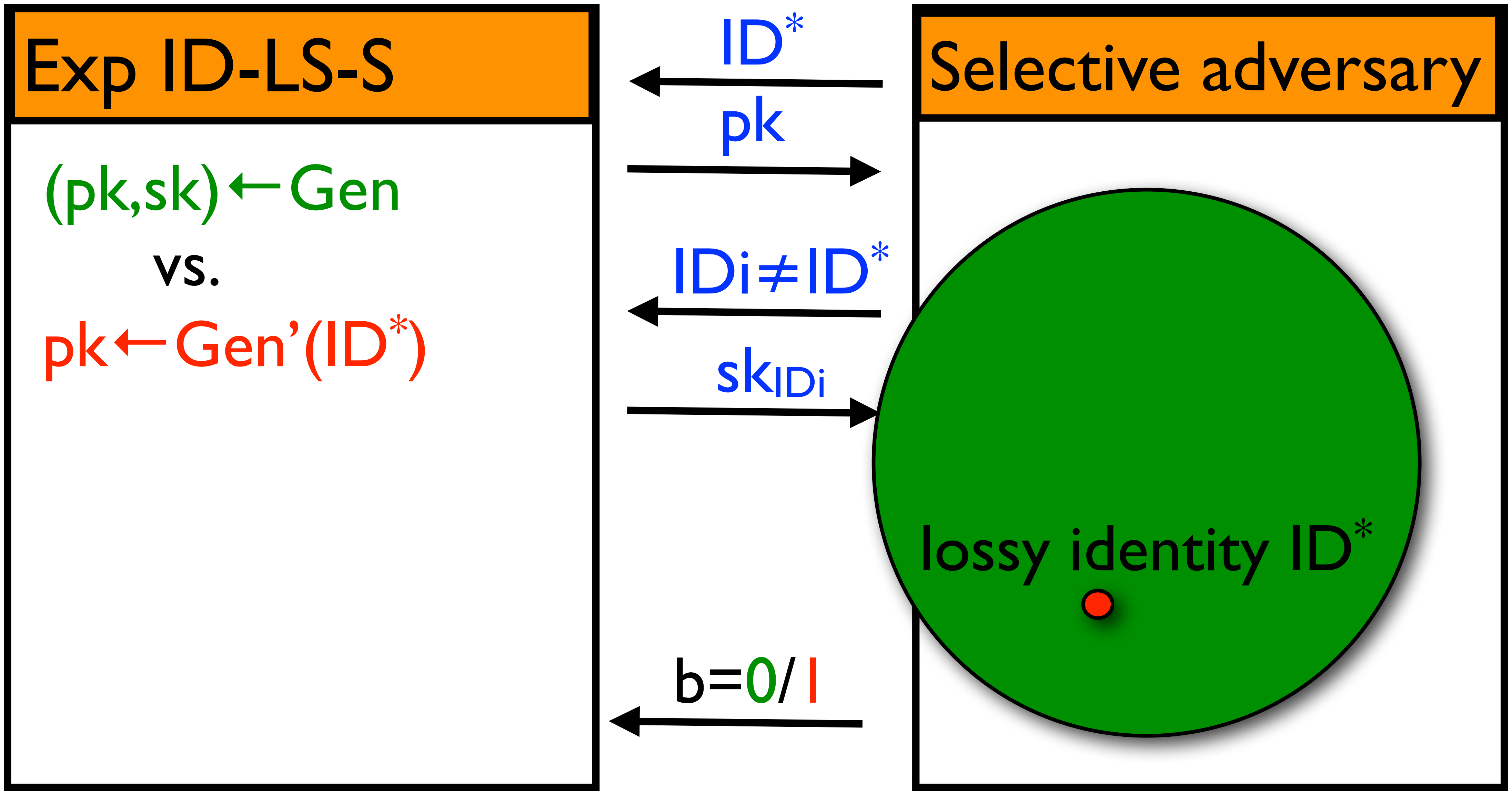


Selective lossiness



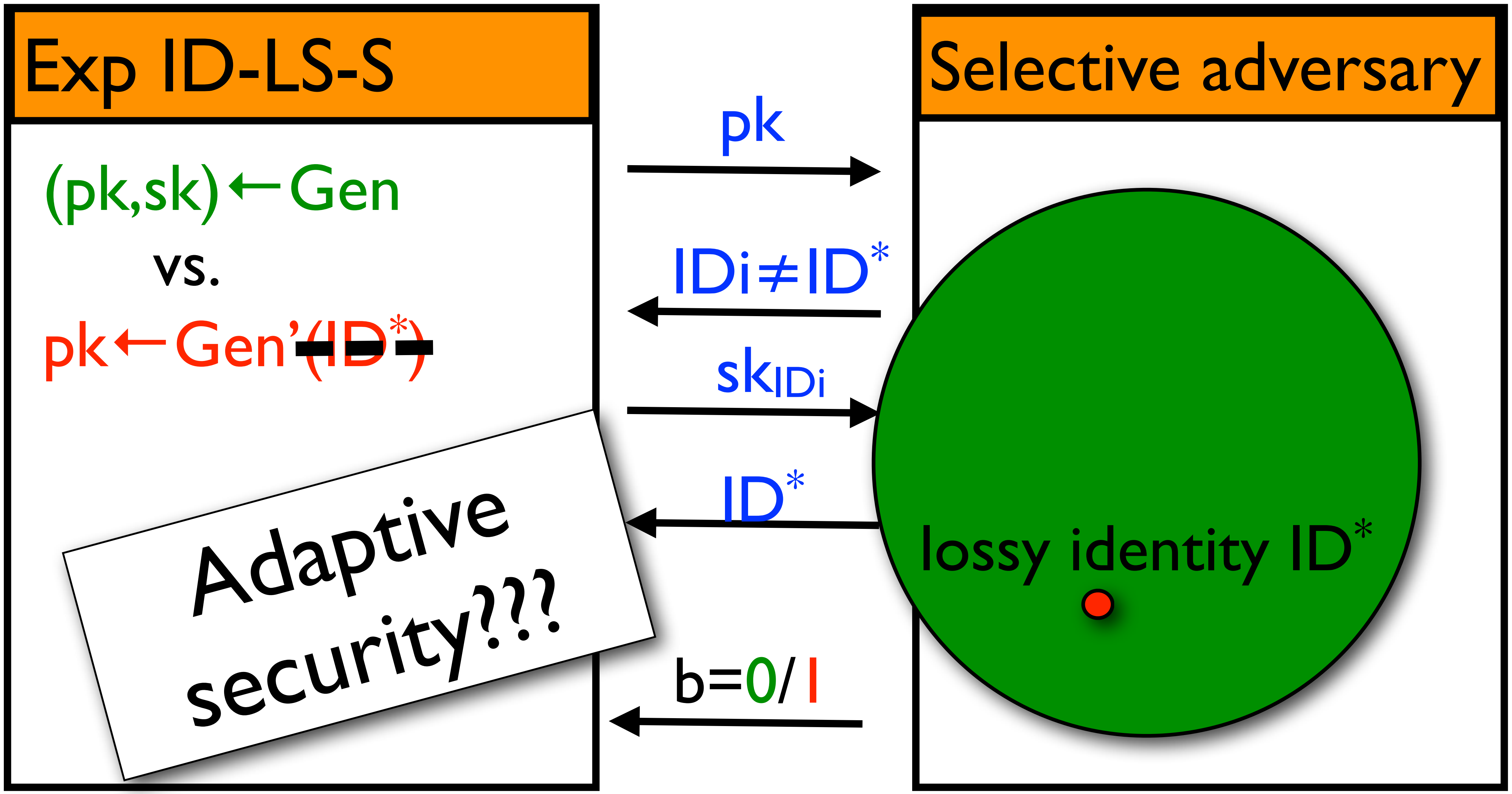
<u>Def:</u> Lossy $\Leftrightarrow$ $\Pr[A(pk)=1] - \Pr[A(pk)=1 \wedge \mathrm{Range}(f_{ID^*}) \ll 2^n] = \mathrm{negl}$

Selective lossiness



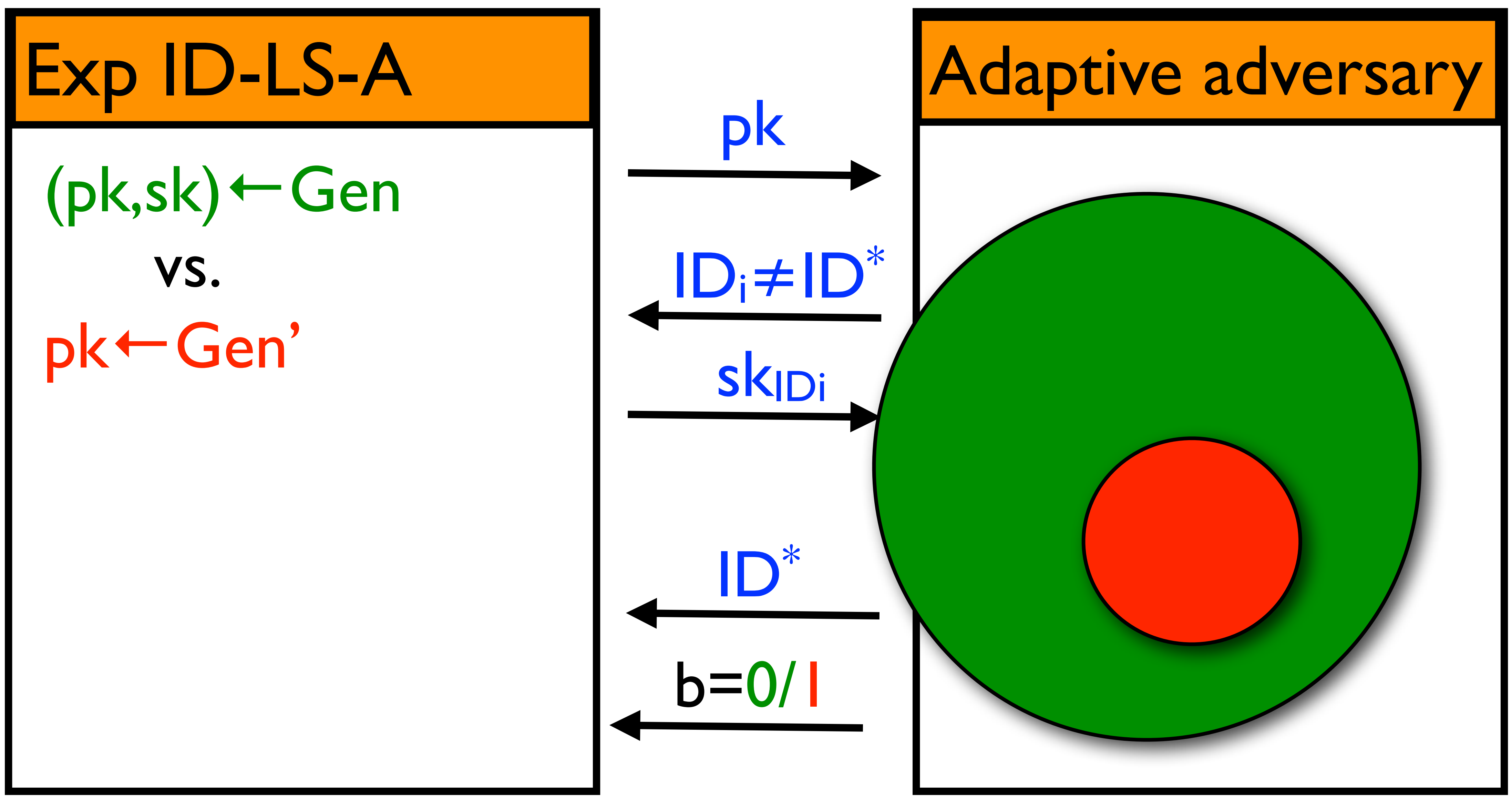
<u>Def:</u> Lossy $\Leftrightarrow$ $\Pr[A(pk)=1] - \Pr[A(pk)=1 \wedge \mathrm{Range}(f_{ID^*}) \ll 2^n] = \mathrm{negl}$

Selective lossiness

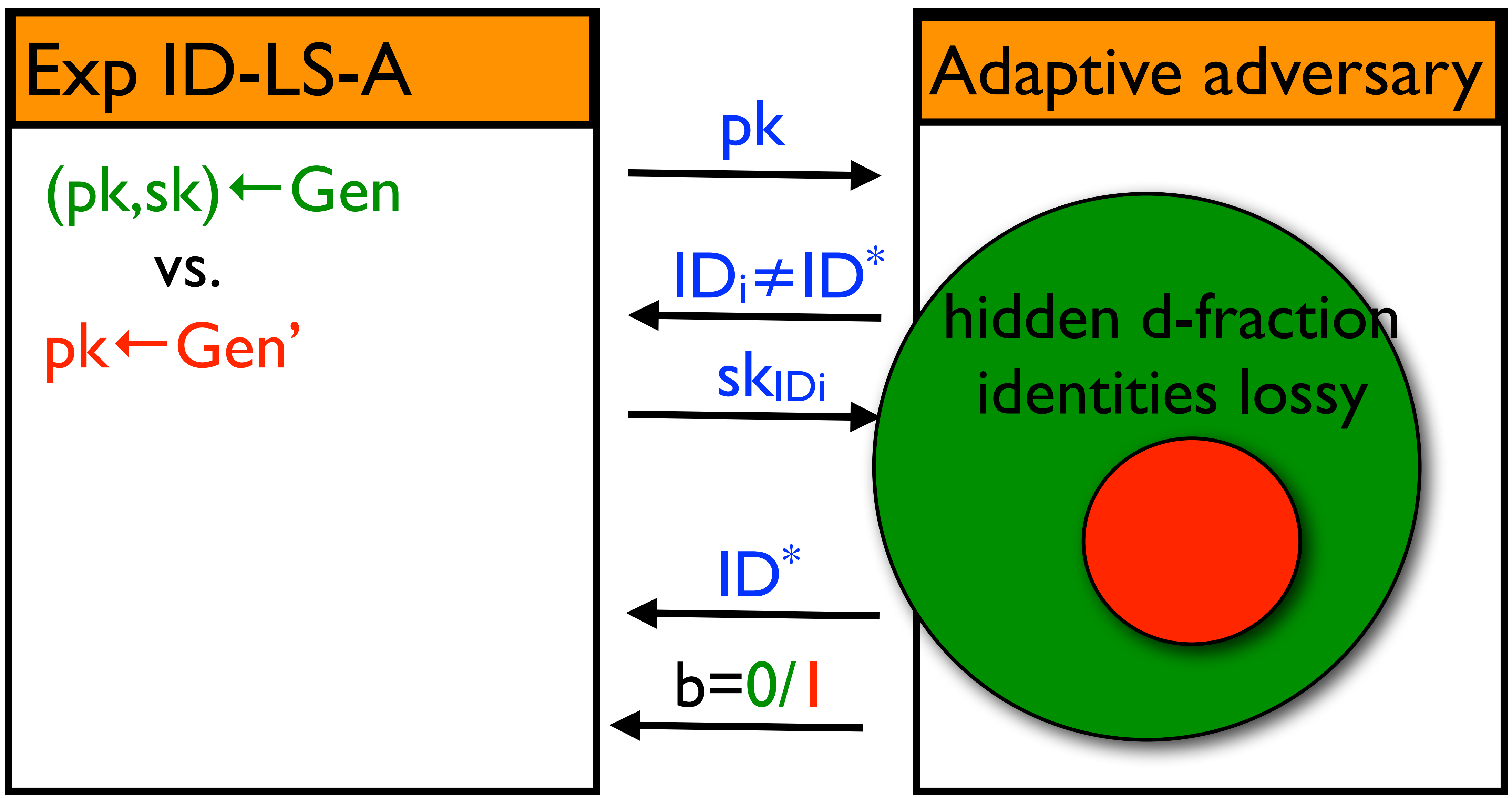


Def: Lossy $\Leftrightarrow$ $\Pr[A(pk)=1] - \Pr[A(pk)=1 \wedge \mathrm{Range}(f_{ID^*}) \ll 2^n] = \mathrm{negl}$

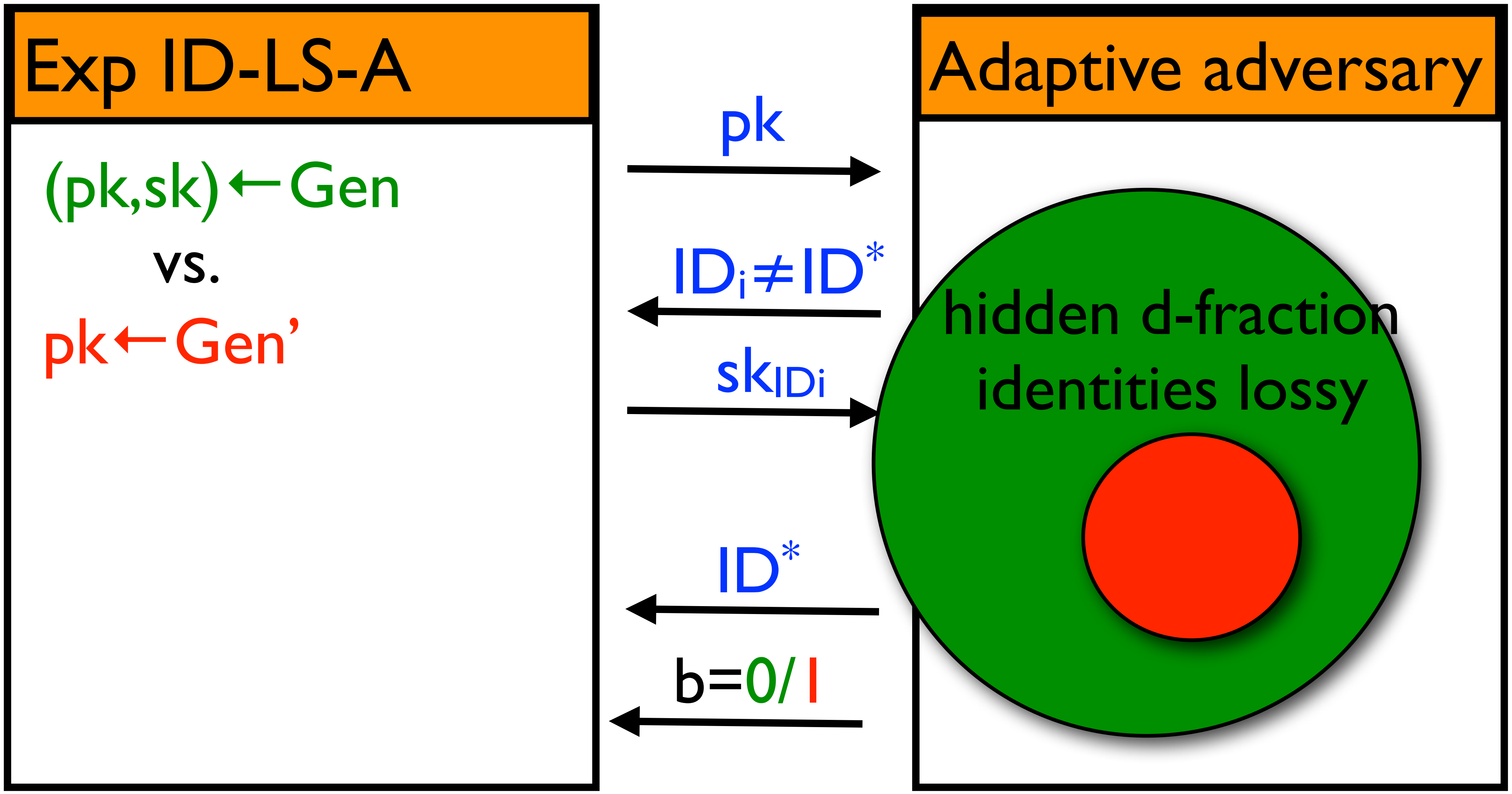
Adaptive lossiness



Adaptive lossiness



Adaptive lossiness



Def: d-lossy for scaling parameter $0<d<1$:

$d \Pr[A(pk)=1] - \Pr[A(pk)=1 \wedge \mathrm{Range}(f_{ID^*}) \ll 2^n] = \mathrm{negl}$

Implications

Implications

- Selective lossyness (ID-LS-S):
  - $\Rightarrow$ one-way (ID-OW-S)
  - $\Rightarrow$ deterministic
  - $\Rightarrow$ hedged IBE

Implications

- Selective lossyness (ID-LS-S):
  - $\Rightarrow$ one-way (ID-OW-S)
  - $\Rightarrow$ deterministic
  - $\Rightarrow$ hedged IBE
- Adaptive 1/poly-lossyness (ID-LS-A)
  - $\Rightarrow$ one-way (ID-OW-A)
  - $\Rightarrow$ IBE?

Construction

Construction

- Difficulty:

  IBE: $Enc_{ID}(.)$ probabilistic

  vs

  LTDF: $f_{ID}(.)$ deterministic

Construction

- Difficulty:

  IBE: $\mathrm{Enc}_{ID}(.)$ probabilistic

  vs

  LTDF: $f_{ID}(.)$ deterministic

- Random oracle model:

  $f_{ID}(x) := \mathrm{Enc}_{ID}(x; r{=}H(x))$

Construction

- Difficulty:
  IBE: $Enc_{ID}(.)$ probabilistic
  vs
  LTDF: $f_{ID}(.)$ deterministic
- Random oracle model:
  $f_{ID}(x) := Enc_{ID}(x; r=H(x))$
- Standard model?

Construction I: pairings

Construction I: pairings

- Idea: anonymous IBE scheme ("ciphertexts hide identity")

Construction I: pairings

- Idea: anonymous IBE scheme ("ciphertexts hide identity")
- Boyen-Waters 06?

Construction I: pairings

- Idea: anonymous IBE scheme ("ciphertexts hide identity")
- Boyen-Waters 06?
- New construction from linear assumption, more efficient!

Construction I: pairings

- Idea: anonymous IBE scheme ("ciphertexts hide identity")
- Boyen-Waters 06?
- New construction from linear assumption, more efficient!
- ID-LTDF: homomorphic properties of ciphertexts (inspired by [PW08])

ID-based TDF

Injective pk

Lossy pk

ID-based TDF

Injective pk

- Gen → (pk,sk), pk = matrix of IBE ciphertexts

Lossy pk

ID-based TDF

Injective pk

- Gen → (pk,sk), pk = matrix of IBE ciphertexts
- Evaluation $f_{ID}: \{0,1\}^n \rightarrow G^{2+2n}$
  - $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that $(C_1, C_2, C_3[i], C_4[i]) \in$ Enc(ID,x[i])

Lossy pk

ID-based TDF

Injective pk

- Gen → (pk,sk), pk = matrix of IBE ciphertexts
- Evaluation $f_{ID}: \{0,1\}^n \rightarrow G^{2+2n}$
  - $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that
    $(C_1, C_2, C_3[i], C_4[i]) \in$ Enc(ID,x[i])

Lossy pk

ID-based TDF

Injective pk

- Gen → (pk,sk), pk = matrix of IBE ciphertexts
- Evaluation $f_{ID}: \{0,1\}^n \to G^{2+2n}$
  - $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that $(C_1, C_2, C_3[i], C_4[i]) \in Enc(ID, x[i])$

Lossy pk

- Gen'(F) → (pk,sk) for controlling function $F: \{0,1\}^n \to Z_p$

ID-based TDF

Injective pk

- Gen → (pk,sk), pk = matrix of IBE ciphertexts
- Evaluation $f_{ID}: \{0,1\}^n \to G^{2+2n}$
  - $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that $(C_1, C_2, C_3[i], C_4[i]) \in Enc(ID, x[i])$

Lossy pk

- Gen'(F) → (pk,sk) for controlling function $F: \{0,1\}^n \to Z_p$
- $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that
  $(C_1, C_2, C_3[i], C_4[i]) \in Enc(ID, x[i])$: $F(ID) \neq 0$
  independent of x[i]: $F(ID) = 0$

ID-based TDF

Injective pk

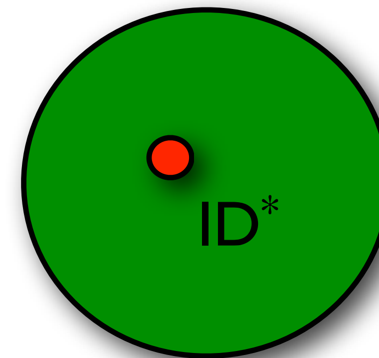
- Gen $\rightarrow$ (pk,sk), pk = matrix of IBE ciphertexts
- Evaluation f_{ID}: $\{0,1\}^n \rightarrow G^{2+2n}$
  - $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that
    $(C_1, C_2, C_3[i], C_4[i]) \in$ Enc(ID,x[i])

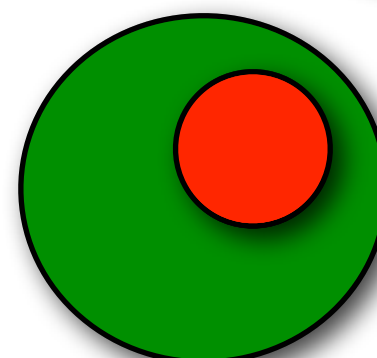
Lossy pk

- Gen'(F) $\rightarrow$ (pk,sk) for controlling function F: $\{0,1\}^n \rightarrow Z_p$
- $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that
  $(C_1, C_2, C_3[i], C_4[i]) \in$ Enc(ID,x[i]): $F(ID) \neq 0$
  independent of x[i]: $F(ID) = 0$
- Security: pk $\approx_c$ pk by anonymity of IBE (pk hides F)

ID-based TDF

- Selective lossiness: $F(ID) := ID - ID^*$
  - $f_{ID}(x)$ invertible if $F(ID) \neq 0$ iff $ID \neq ID^*$
  - $f_{ID^*}(x)$ loses information on x





- Full lossiness: $F(ID) = \sum ID_i F_i$

Lossy pk

- Gen'(F) → (pk,sk) for controlling function $F: \{0,1\}^n \rightarrow Z_p$
- $f_{ID}(x) = (C_1, C_2, \mathbf{C_3}, \mathbf{C_4})$ such that

  $(C_1, C_2, C_3[i], C_4[i]) \in$ Enc(ID,x[i]): $F(ID) \neq 0$

  independent of x[i]: $F(ID) = 0$
- Security: $pk \approx_c pk$ by anonymity of IBE (pk hides F)

Lattice construction

- LWE function

$$(x,e) \rightarrow Ax+e$$

  is lossy TDF (under LWE assumption)

- ID-based lossy TDF using delegation of lattice IBE [CHKP10, ABB10]

Summary

- ID-based trapdoor functions
- Security: oneway/lossy
- Applications
- Constructions
- Eprint 2011/479

Summary

- ID-based trapdoor functions
- Security: oneway/lossy
- Applications
- Constructions
- Eprint 2011/479

Thank you