

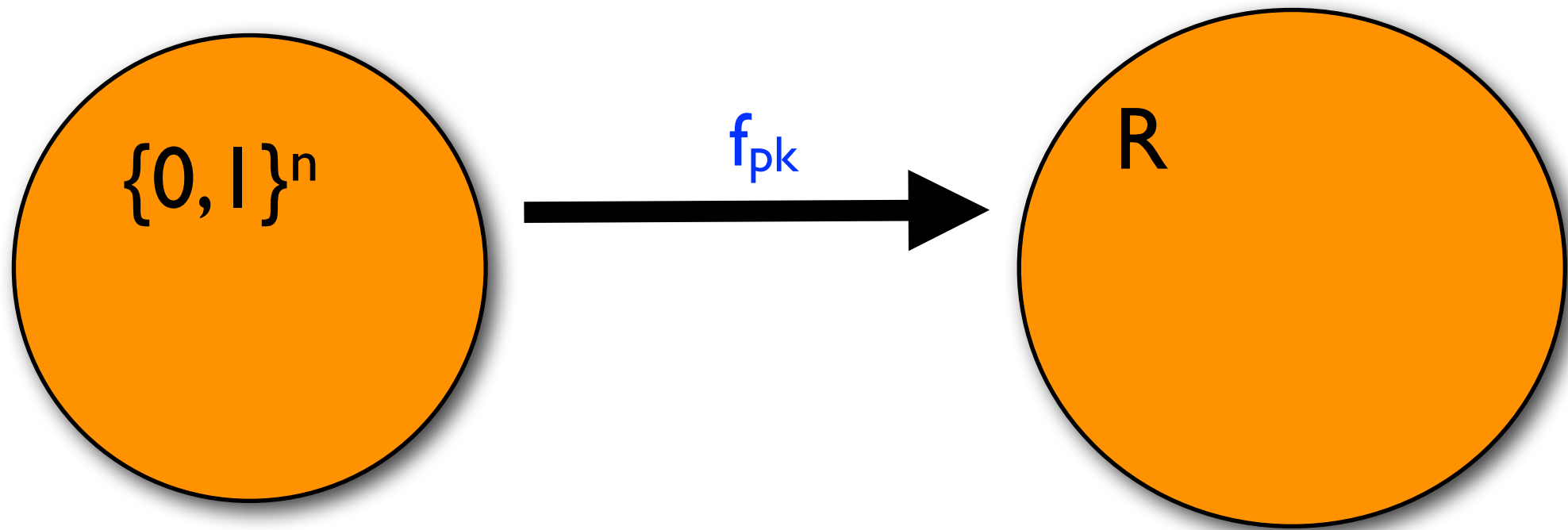


LOSSY

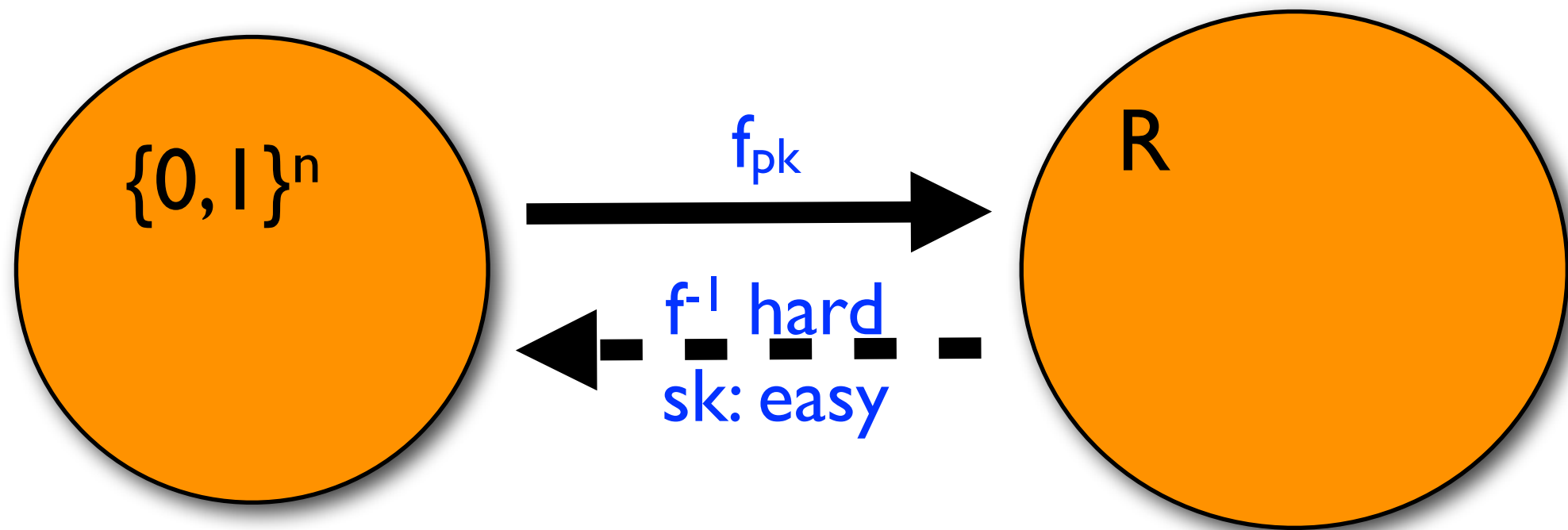
Identity-based (Lossy) Trapdoor Functions and Applications

Mihir Bellare, Eike Kiltz, Chris Peikert, Brent Waters

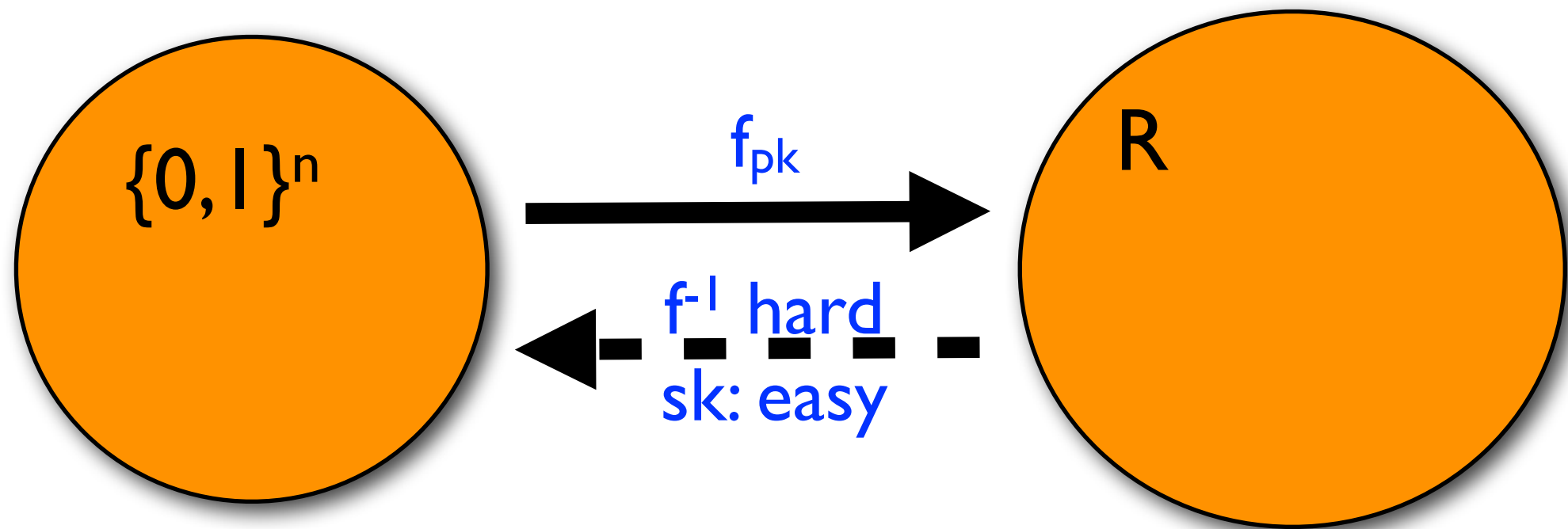
Injective trapdoor function



Injective trapdoor function



Injective trapdoor function



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

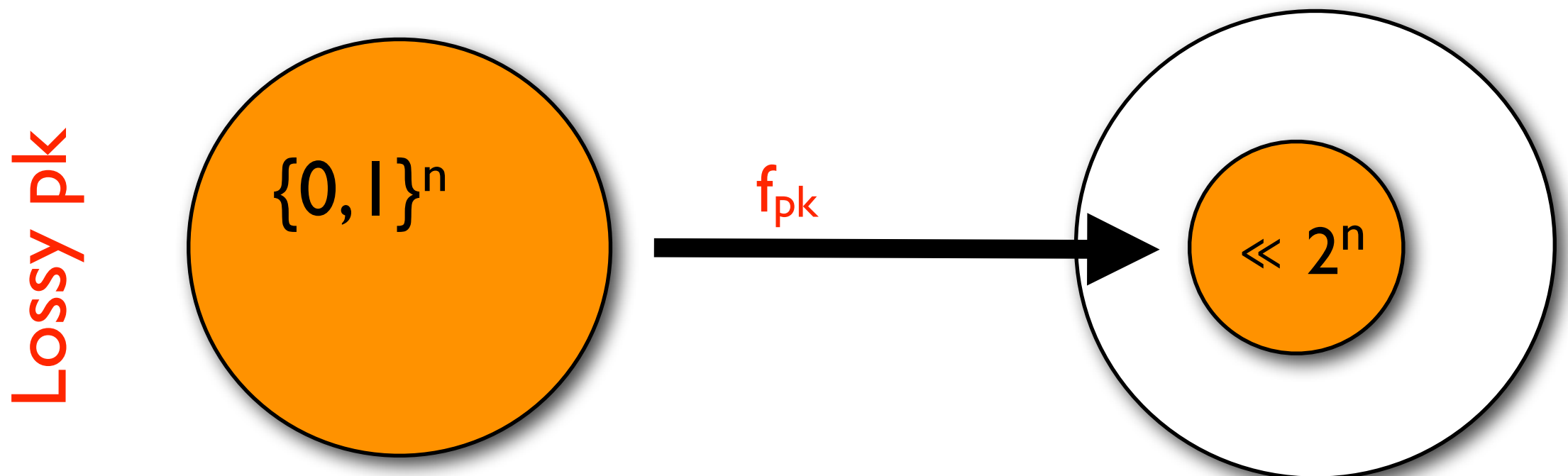
Security notions

Security notions

- One-wayness: $\text{Gen} \rightarrow (\text{pk}, \text{sk})$
 $\text{pk}, f_{\text{pk}}(x) \rightarrow x$ hard (random x)

Security notions

- **One-wayness:** $\text{Gen} \rightarrow (\text{pk}, \text{sk})$
 $\text{pk}, f_{\text{pk}}(x) \rightarrow x$ hard (random x)
- **Lossiness [PW08]:** exists $\text{Gen}' \rightarrow$ “fake” pk :
 1. $\text{pk} \approx_c \text{pk}$
 2. $\text{Range}(f_{\text{pk}}) \ll 2^n$



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

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, ...

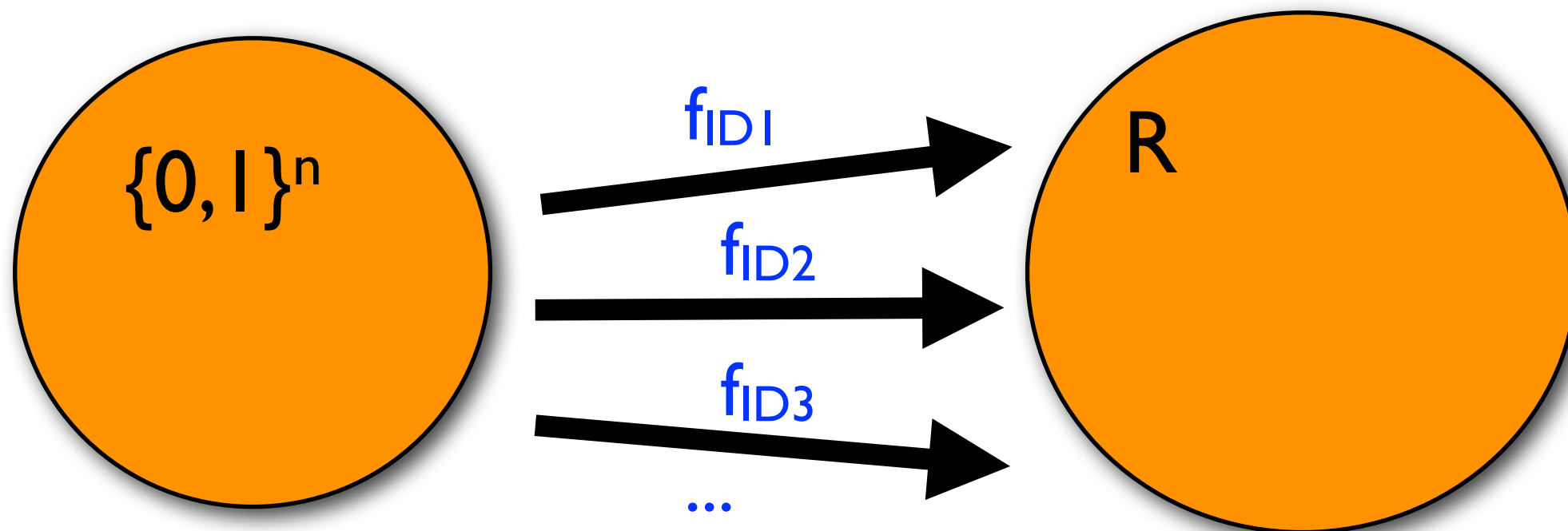
ID-based trapdoor functions

- **Gen** \rightarrow (pk,sk)

- **Eval**(pk, ID, \cdot) = $f_{ID} : \{0,1\}^n \rightarrow R$ for $ID \in \{0,1\}^n$

- **Extract**(sk, ID) \rightarrow trapdoor sk_{ID}

- **Invert**(sk_{ID} , \cdot) = $f_{ID}^{-1}(\cdot)$



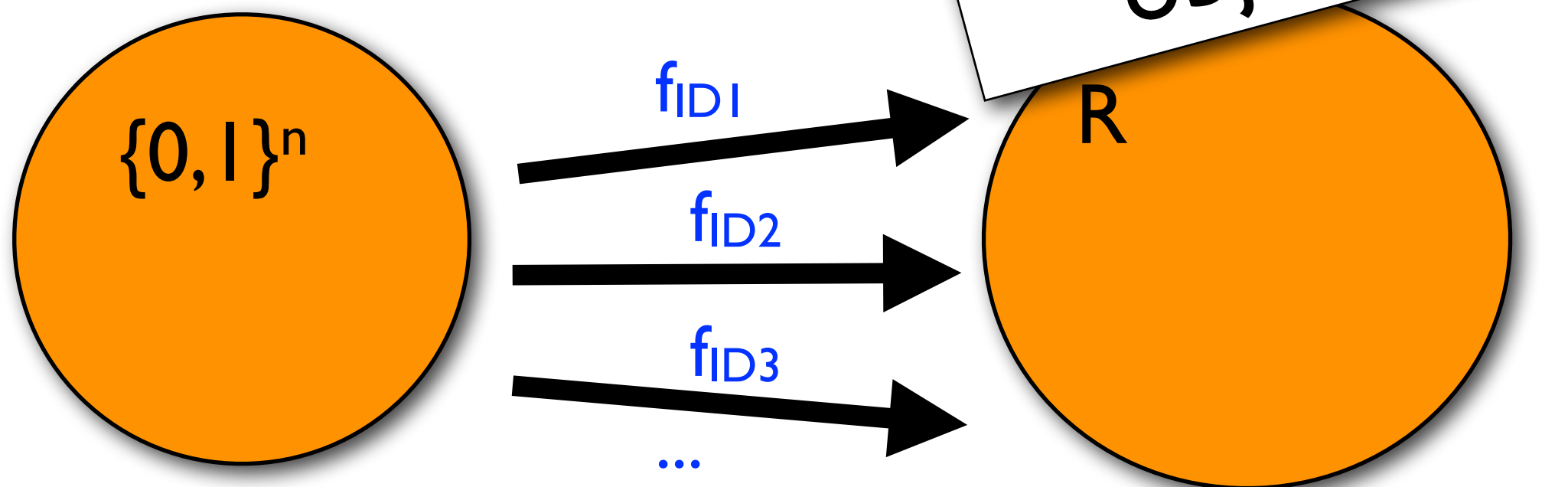
ID-based trapdoor functions

- **Gen** \rightarrow (pk,sk)

- **Eval**(pk, ID, \cdot) = $f_{ID} : \{0,1\}^n \rightarrow R$ for $ID \in \{0,1\}^n$

- **Extract**(sk, ID) \rightarrow trapdoor sk_{ID}

- **Invert**(sk_{ID} , \cdot) = $f_{ID}^{-1}(\cdot)$

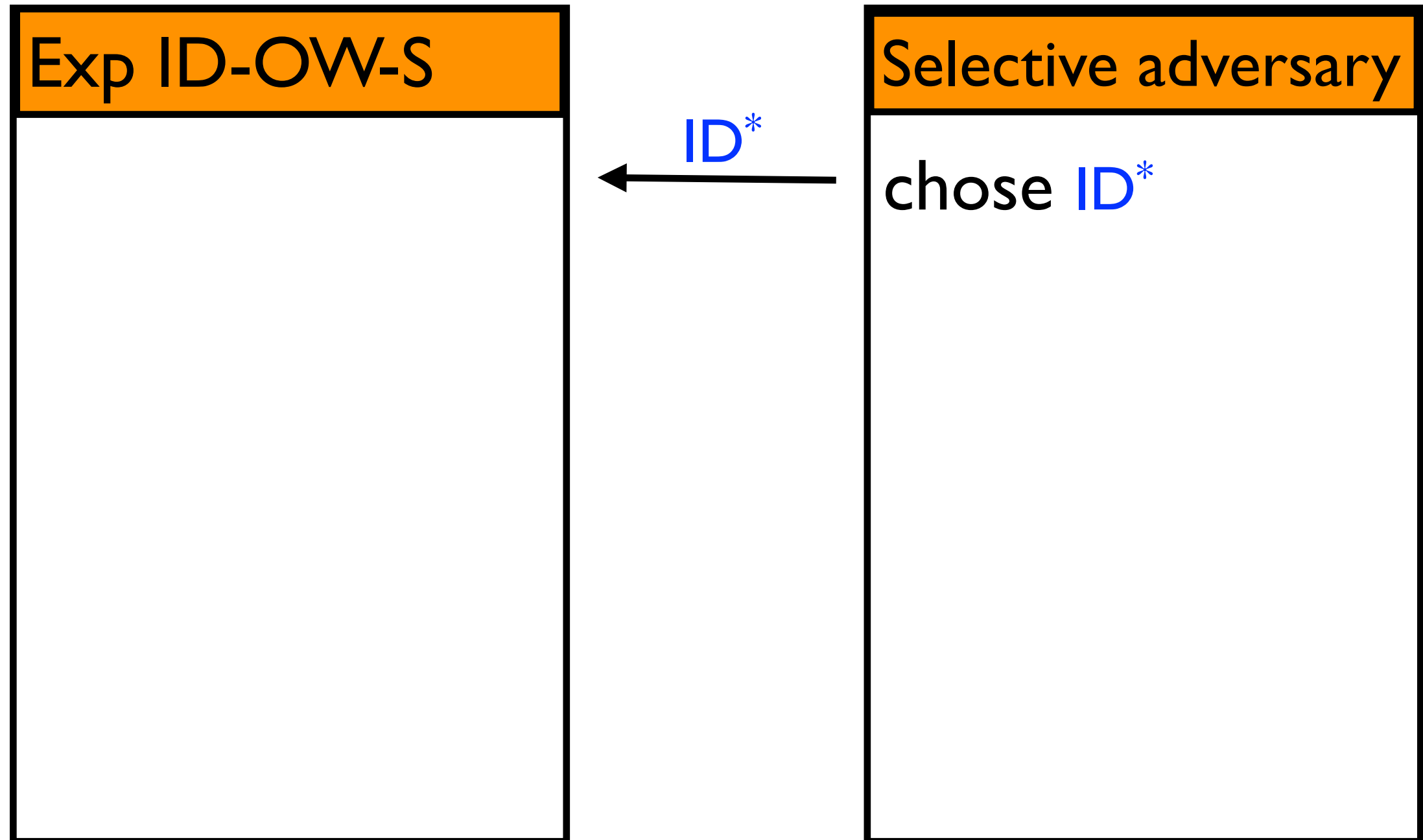


Security?

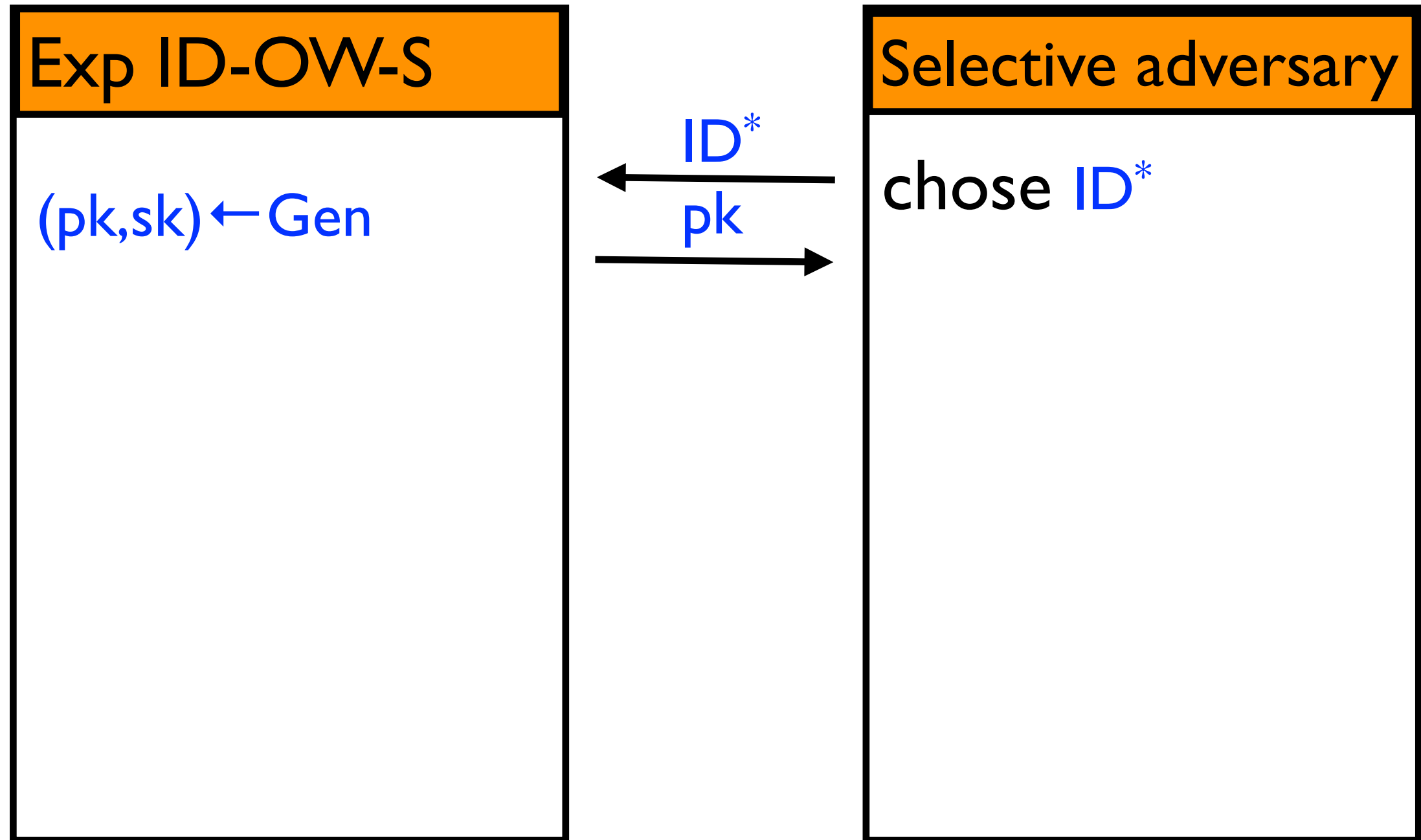
Intuition: $f_{ID^*}(\cdot)$ “secure” even given sk_{ID} for $ID \neq ID^*$

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

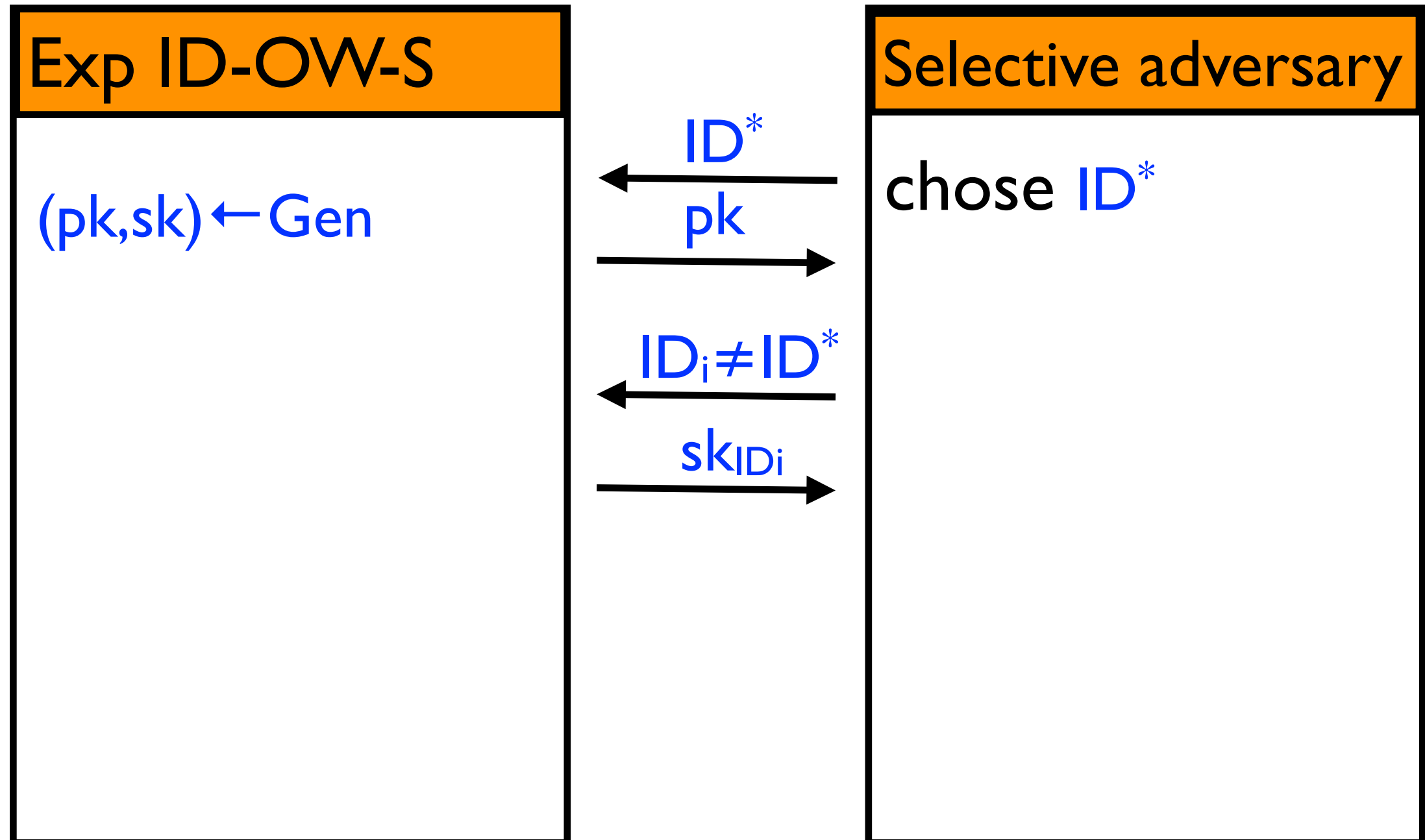
One-wayness



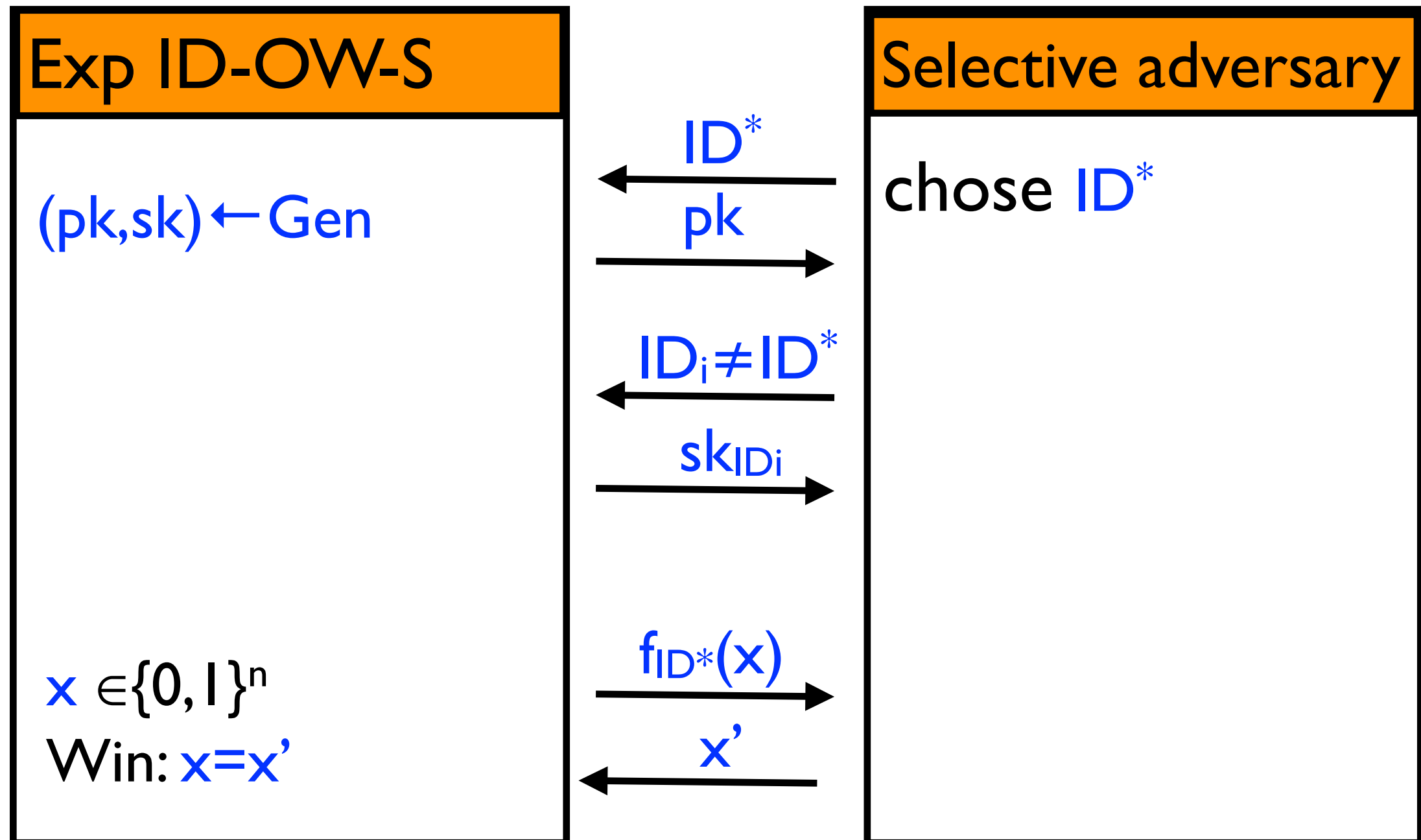
One-wayness



One-wayness

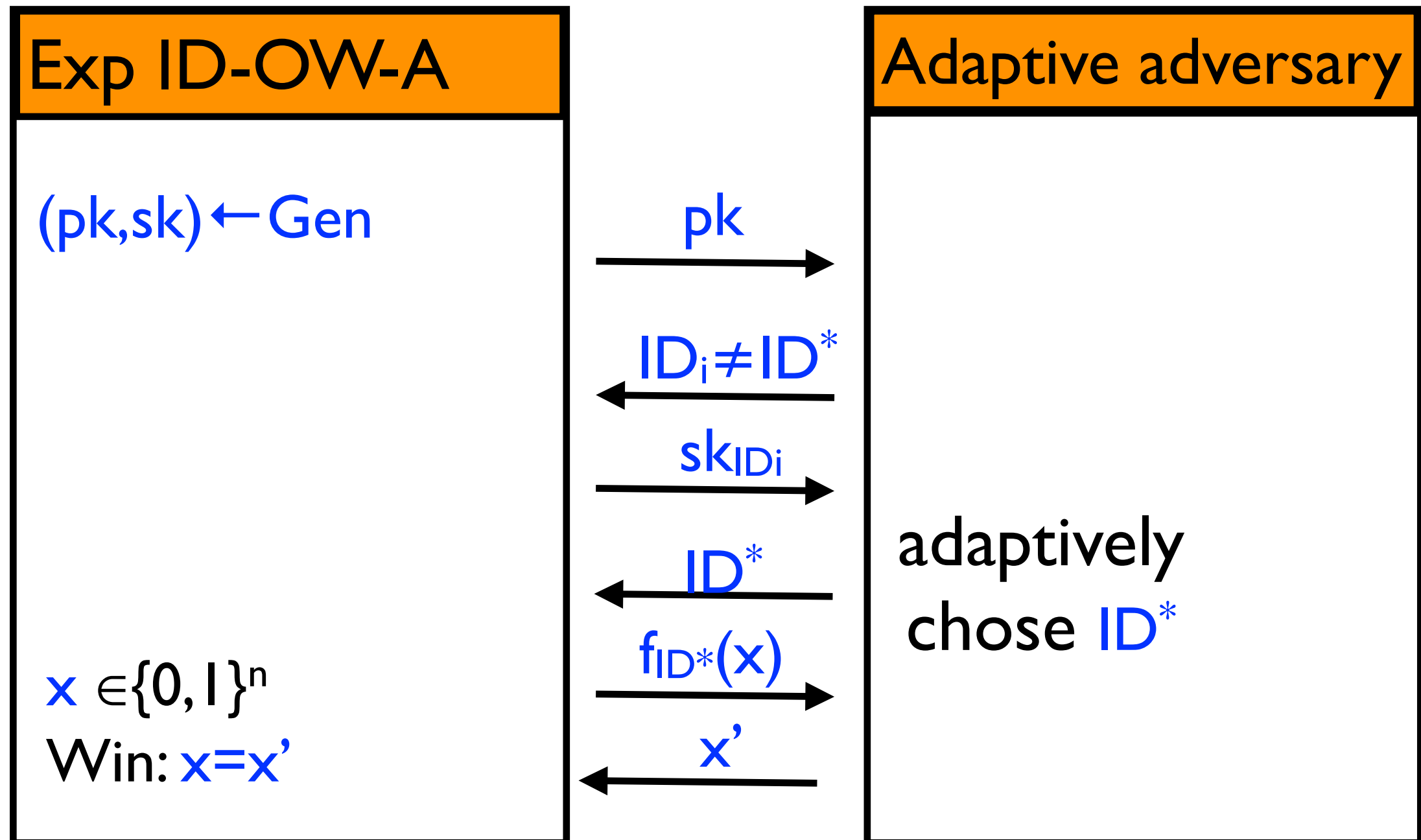


One-wayness



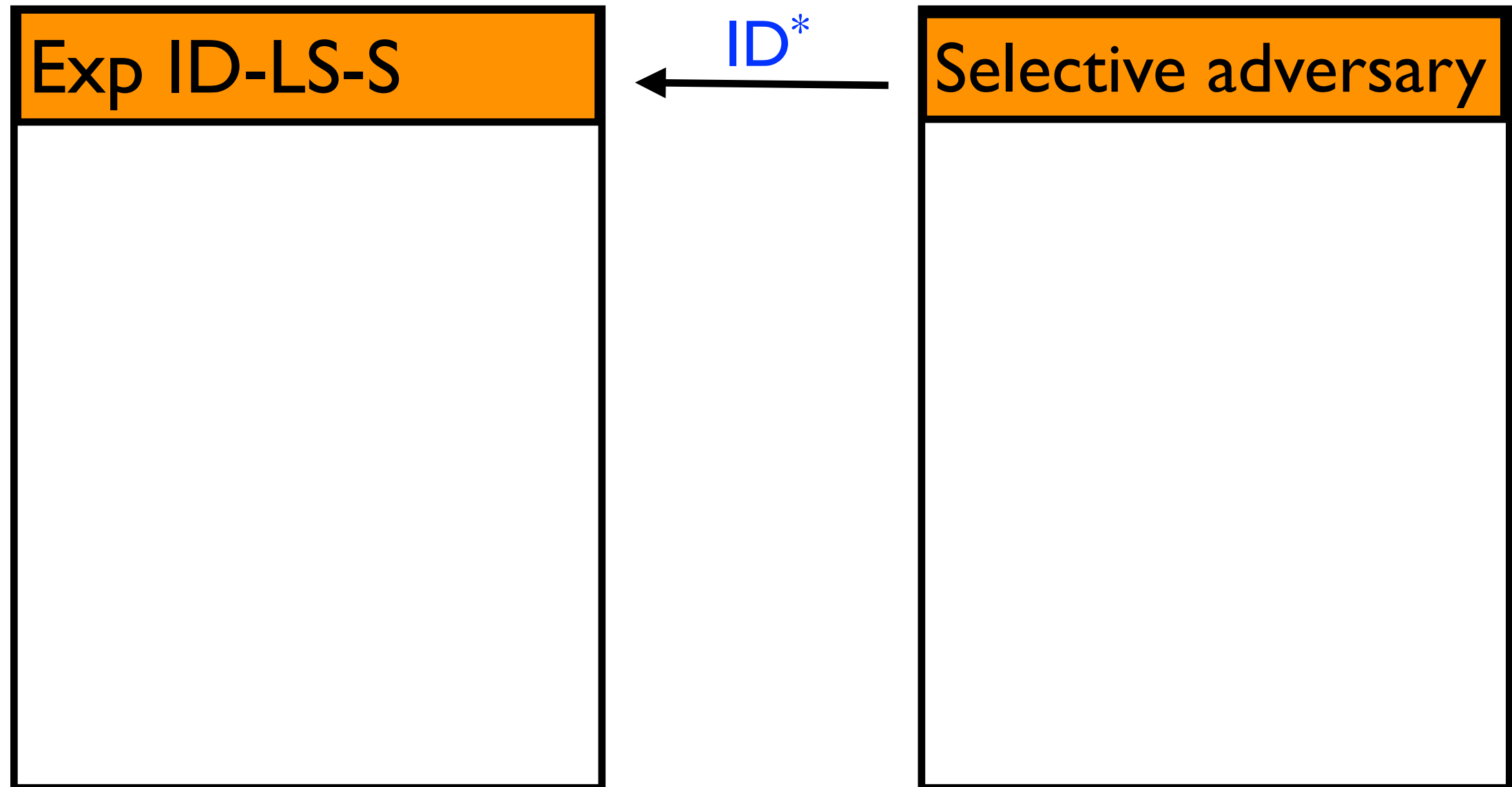
Def: One-way $\Leftrightarrow \Pr[\text{Adversary wins}] = \text{negl}$

One-wayness

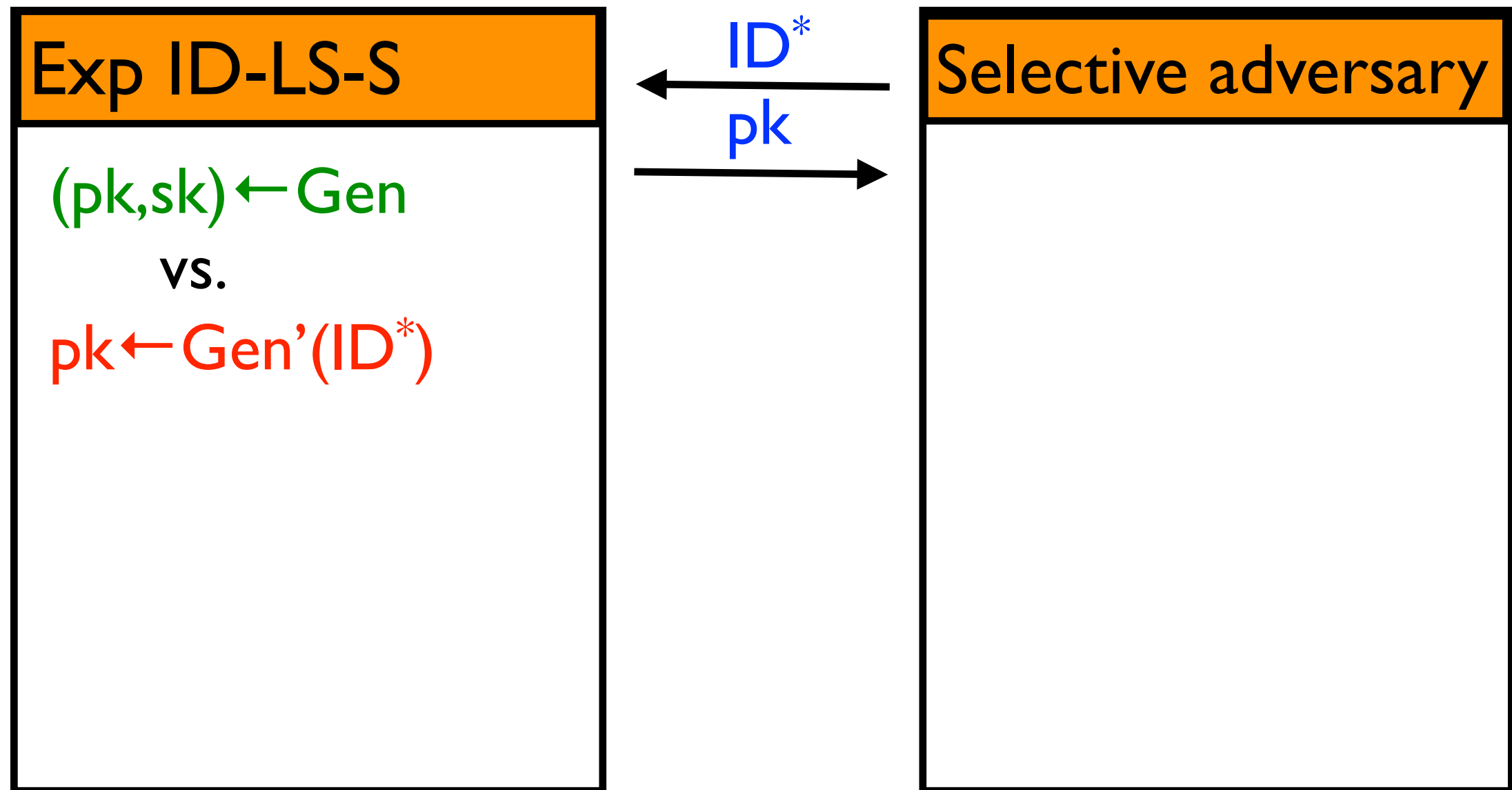


Def: One-way $\Leftrightarrow \Pr[\text{Adversary wins}] = \text{negl}$

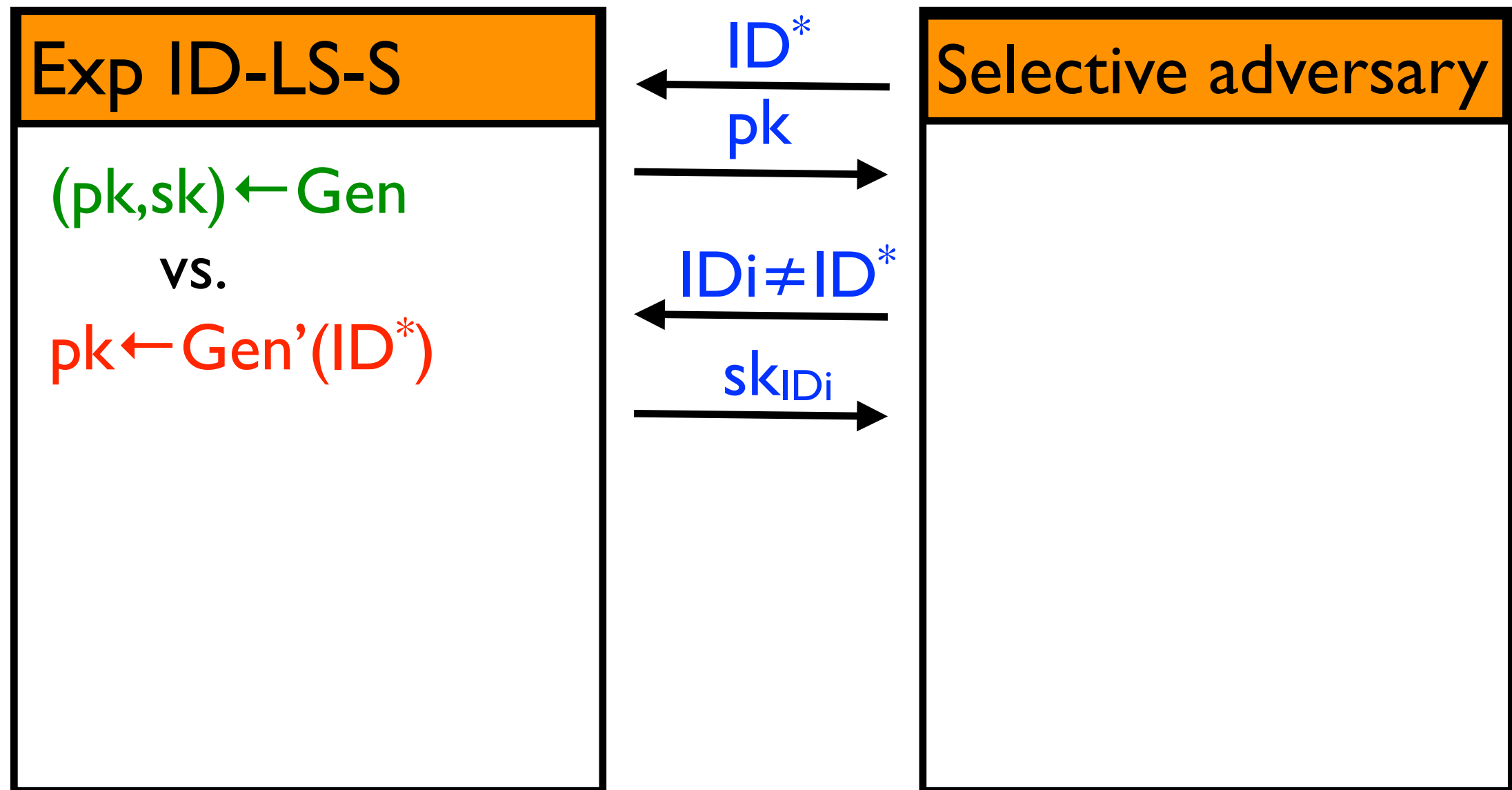
Selective lossiness



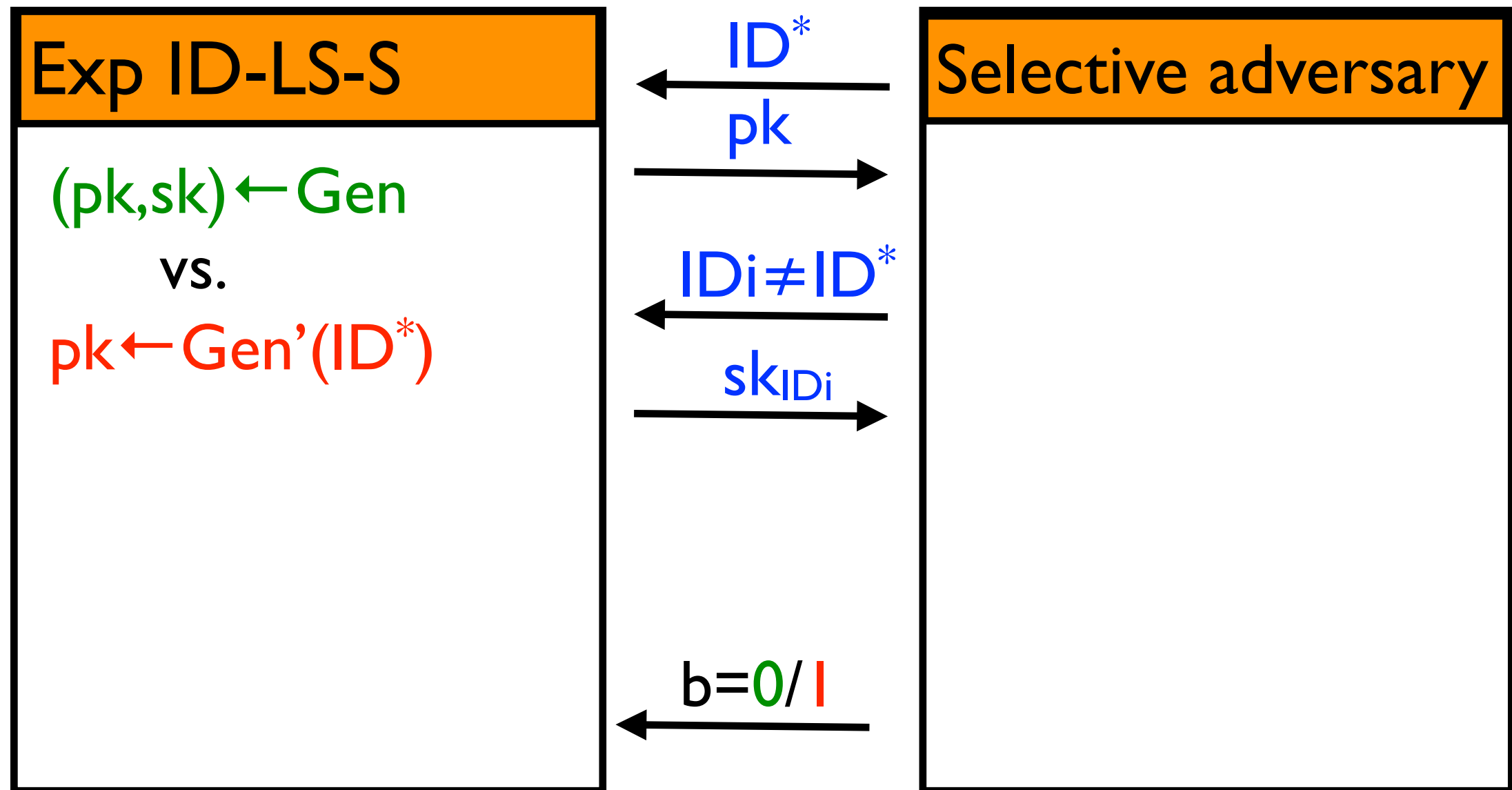
Selective lossiness



Selective lossiness

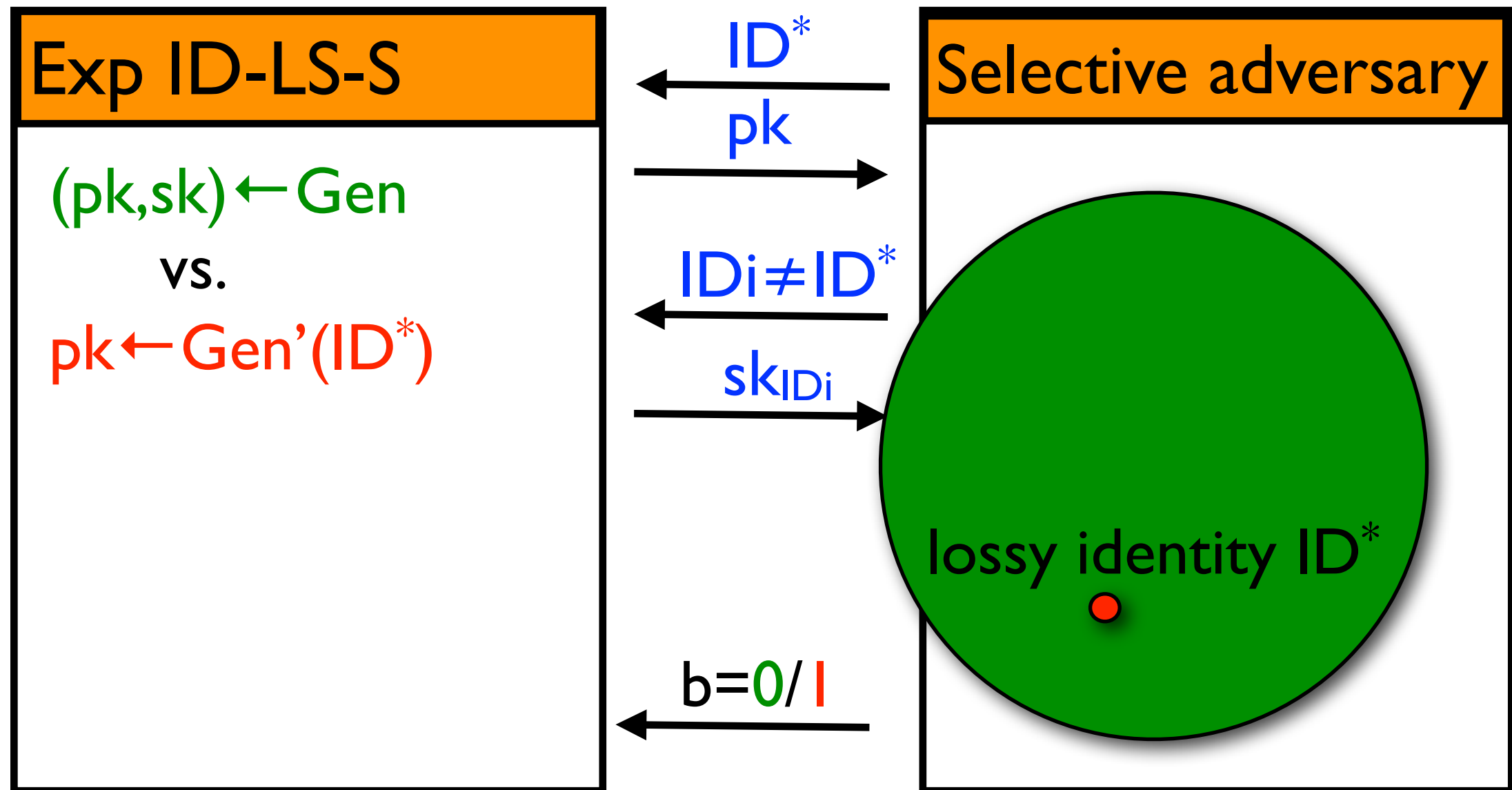


Selective lossiness



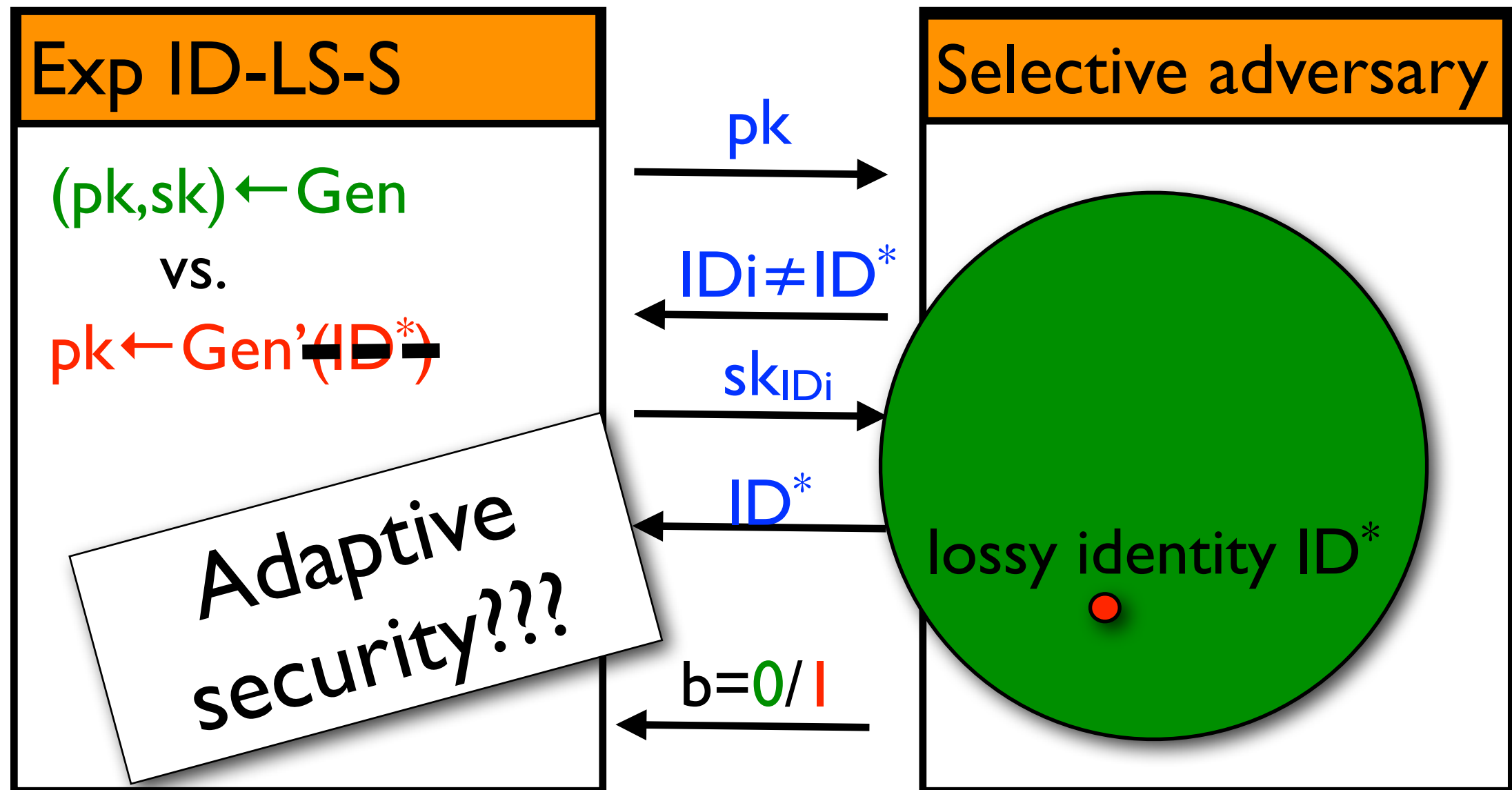
Def: Lossy $\Leftrightarrow \Pr[A(pk)=1] - \Pr[A(pk)=1 \wedge \text{Range}(f_{ID^*}) \ll 2^n] = \text{negl}$

Selective lossiness



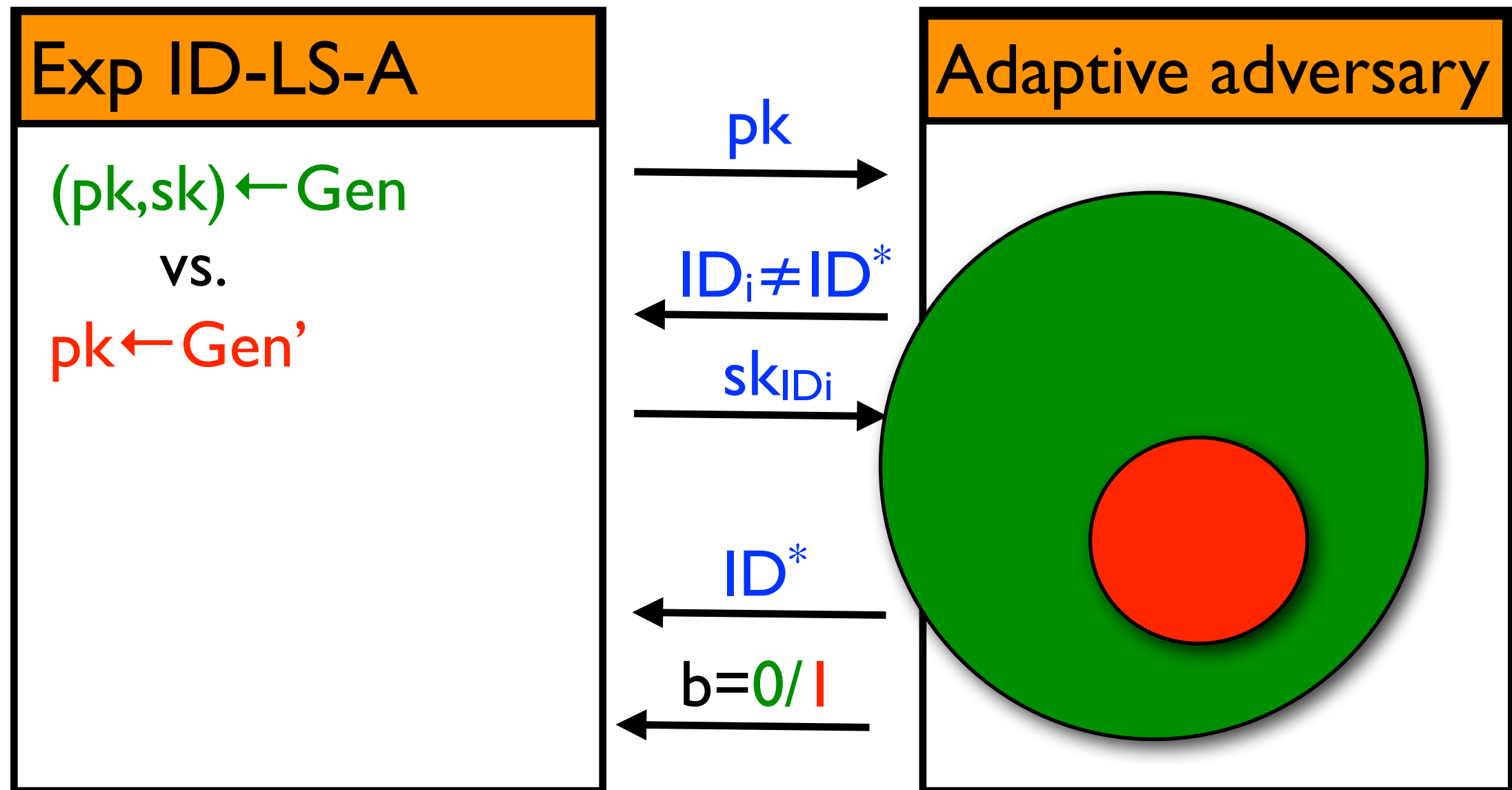
Def: Lossy $\Leftrightarrow \Pr[A(pk)=1] - \Pr[A(pk)=1 \wedge \text{Range}(f_{ID^*}) \ll 2^n] = \text{negl}$

Selective lossiness

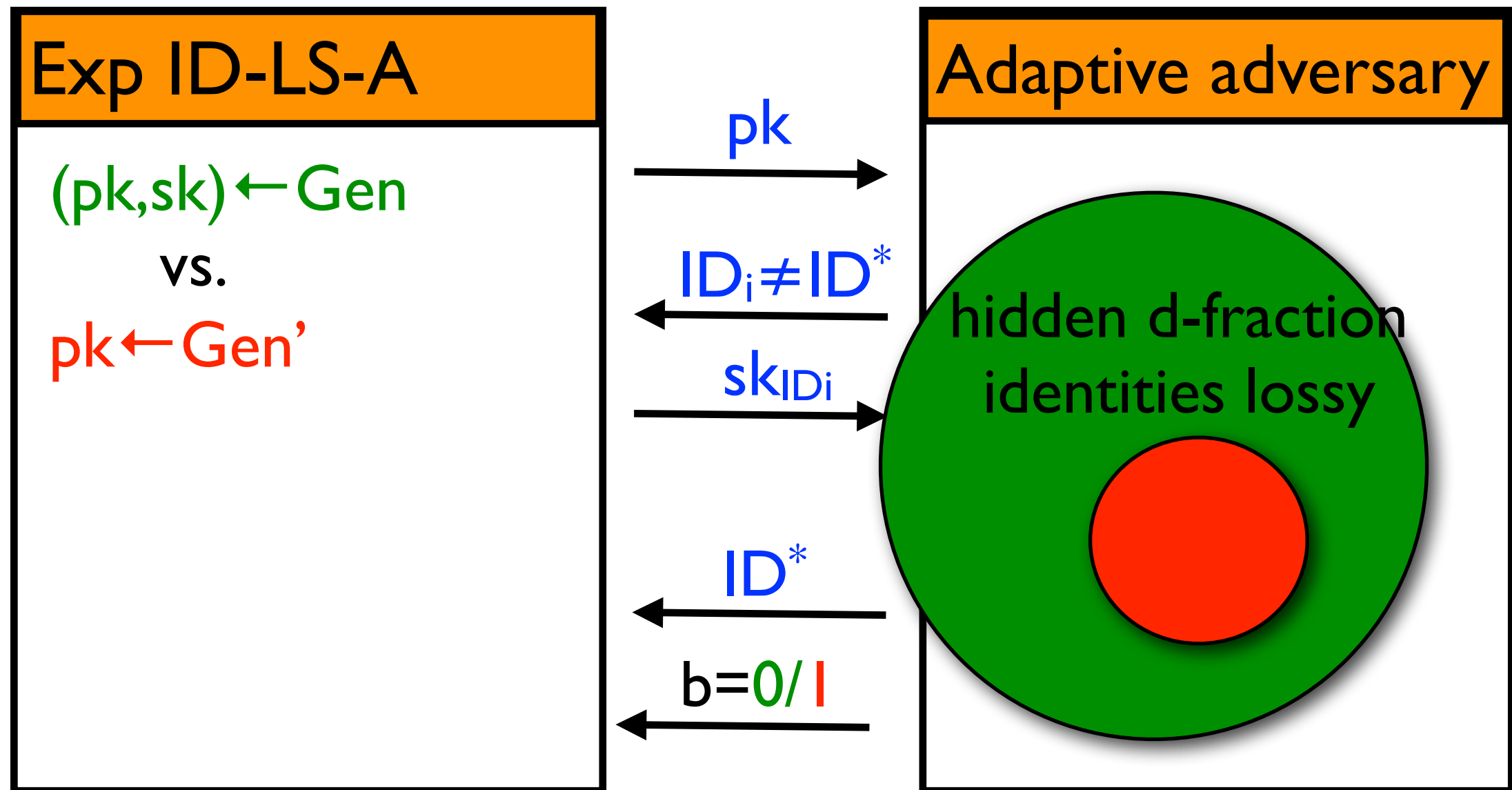


Def: Lossy $\Leftrightarrow \Pr[A(pk)=1] - \Pr[A(pk)=1 \wedge \text{Range}(f_{\text{ID}^*}) \ll 2^n] = \text{negl}$

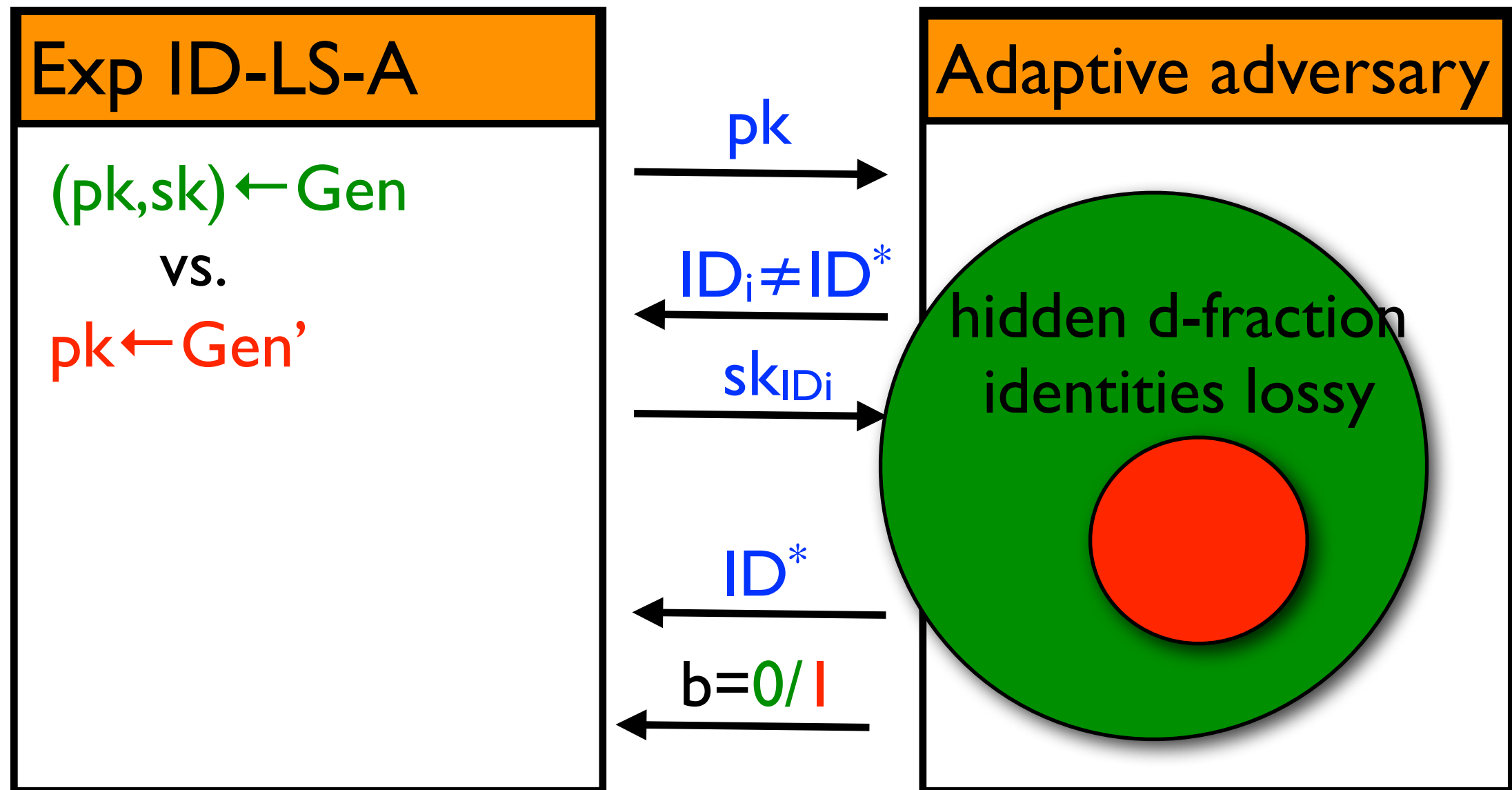
Adaptive lossiness



Adaptive lossiness



Adaptive lossiness



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

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

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 *l*/poly-lossyness (ID-LS-A)**
 - \Rightarrow one-way (ID-OW-A)
 - \Rightarrow IBE?

Construction

Construction

- Difficulty:
IBE: $\text{Enc}_{ID}(\cdot)$ probabilistic
vs
LTDF: $\text{f}_{ID}(\cdot)$ deterministic

Construction

- Difficulty:
IBE: $\text{Enc}_{\text{ID}}(\cdot)$ probabilistic
vs
LTDF: $f_{\text{ID}}(\cdot)$ deterministic
- Random oracle model:
 $f_{\text{ID}}(x) := \text{Enc}_{\text{ID}}(x; r=H(x))$

Construction

- Difficulty:
IBE: $\text{Enc}_{\text{ID}}(\cdot)$ probabilistic
vs
LTDF: $f_{\text{ID}}(\cdot)$ deterministic
- Random oracle model:
 $f_{\text{ID}}(x) := \text{Enc}_{\text{ID}}(x; r=H(x))$
- 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 \rightarrow (pk,sk), pk = matrix of IBE ciphertexts

Lossy pk

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
 $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(ID, x[i])$

Lossy pk

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
 $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(ID, x[i])$

Lossy pk

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
 $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(ID, x[i])$

Lossy pk

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

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
 $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(ID, x[i])$

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
 $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(ID, x[i]):$ $F(ID) \neq 0$
independent of $x[i]: F(ID) = 0$

ID-based TDF

Injective pk

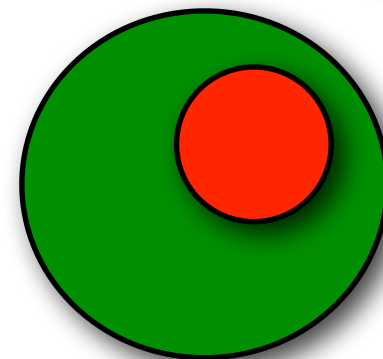
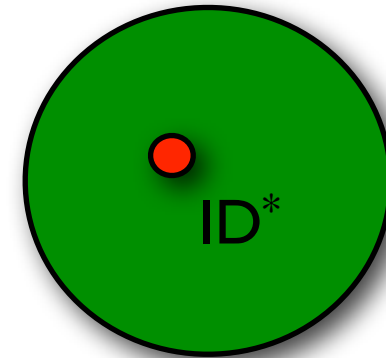
- Gen \rightarrow (pk, sk), pk = matrix of IBE ciphertexts
- Evaluation $f_{ID}: \{0, 1\}^n \rightarrow G^{2+2n}$
- $f_{ID}(x) = (C_1, C_2, \mathbf{C}_3, \mathbf{C}_4)$ such that
 $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(ID, x[i])$

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
 $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(ID, x[i]):$ $F(ID) \neq 0$
independent of $x[i]: F(ID) = 0$
- Security: $\text{pk} \approx_c \text{pk}$ by anonymity of IBE (pk hides F)

ID-based TDF

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



Lossy pk

- $\text{Gen}'(F) \rightarrow (\text{pk}, \text{sk})$ for controlling function $F: \{0, 1\}^n \rightarrow \mathbb{Z}_p$
- $f_{\text{ID}}(\mathbf{x}) = (C_1, C_2, \mathbf{C}_3, \mathbf{C}_4)$ such that
 - $(C_1, C_2, C_3[i], C_4[i]) \in \text{Enc}(\text{ID}, \mathbf{x}[i]): F(\text{ID}) \neq 0$
 - independent of $\mathbf{x}[i]: F(\text{ID}) = 0$
- Security: $\text{pk} \approx_c \text{pk}$ 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