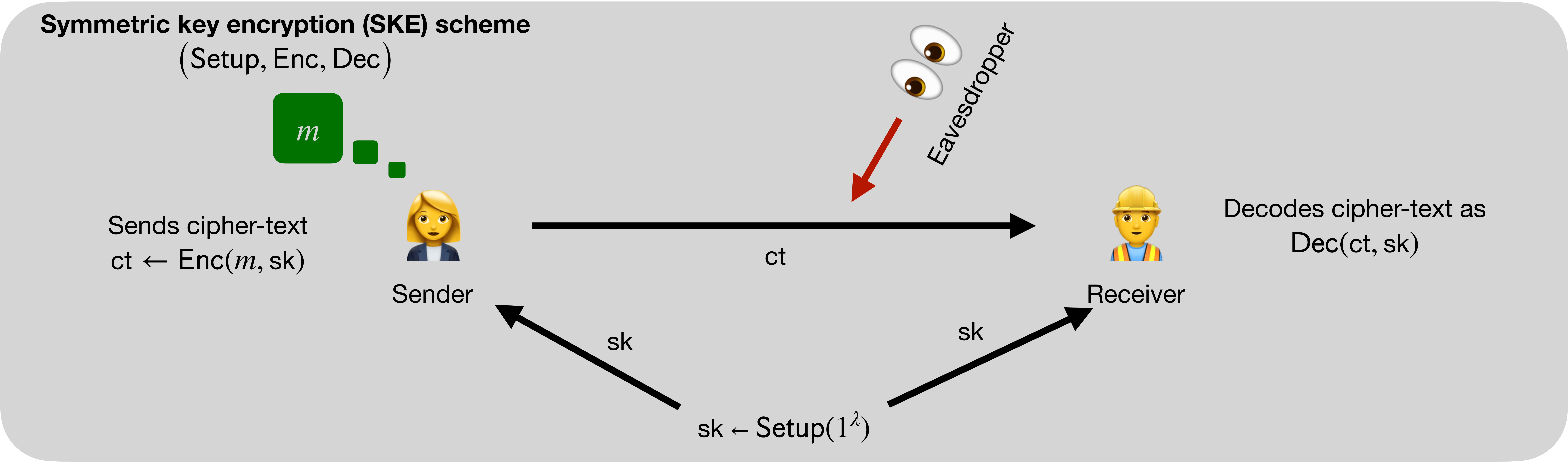
Leakage-Resilient Incompressible Cryptography: Constructions and Barriers

Kaartik Bhushan[1]   Rishab Goyal[2]   Venkata Koppula[3]

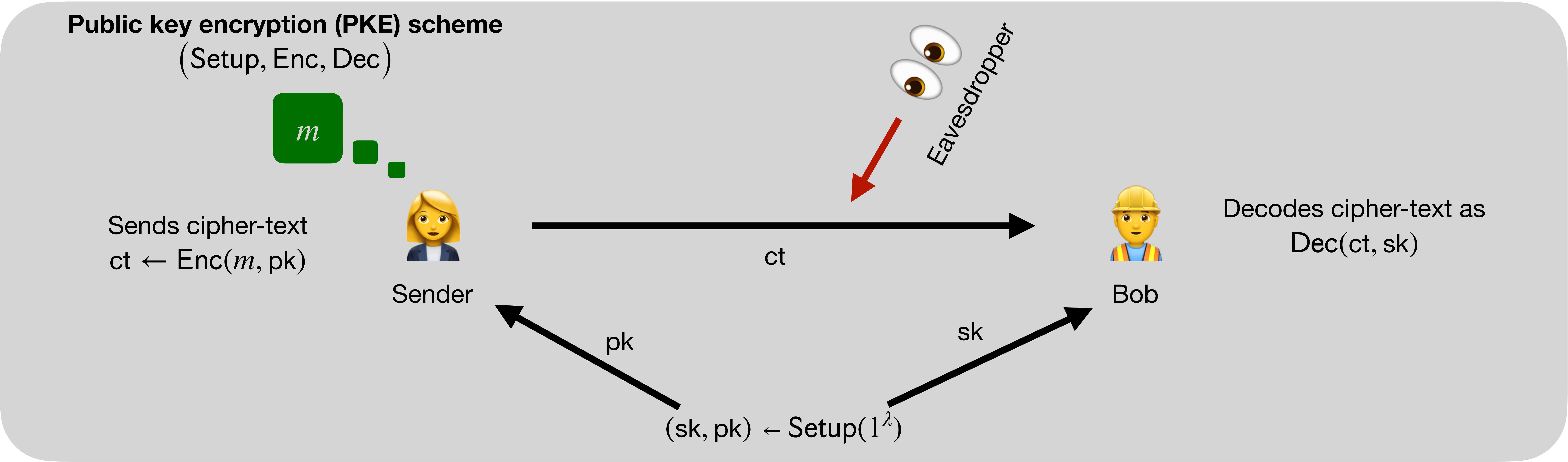
Varun Narayanan[4]   Manoj Prabhakaran[1]   Mahesh Sreekumar Rajasree[3]

1. Indian Institute of Technology, Bombay
2. University of Wisconsin-Madison
3. Indian Institute of Technology, Delhi
4. University of California, Los Angeles



Correctness. Receiver correctly decrypts the message

Security. Eavesdropper cannot learn m from cipher-text

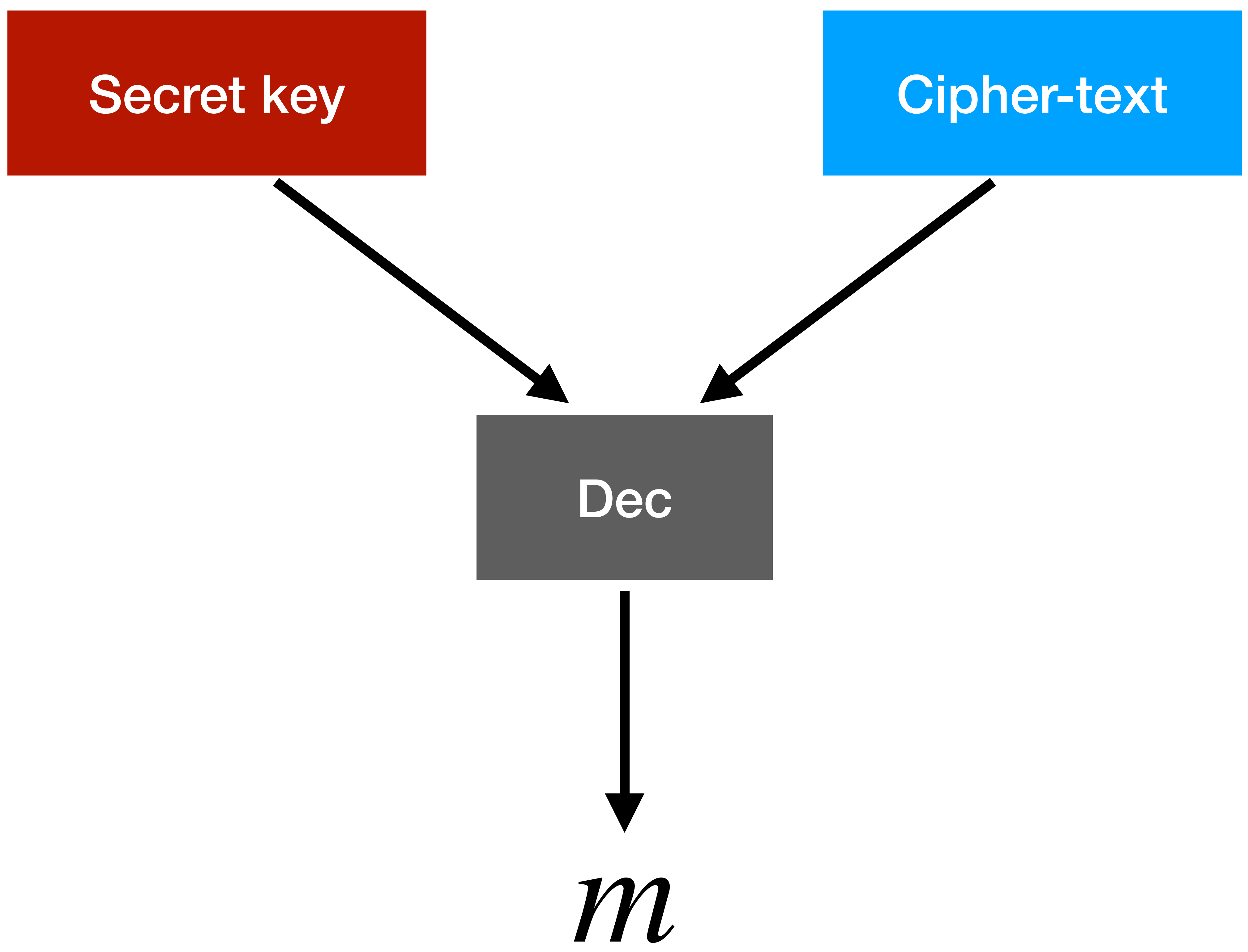


Correctness. Receiver correctly decrypts the message

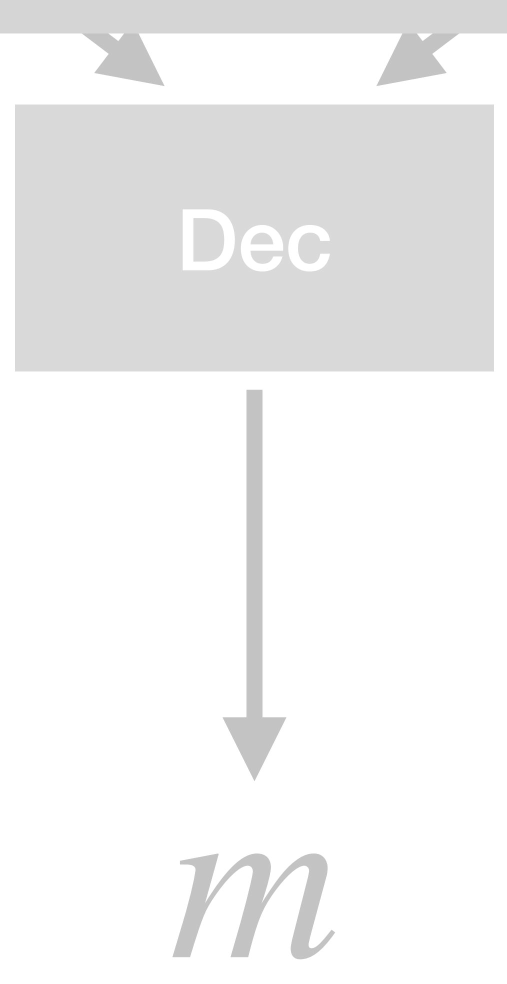
Security. Eavesdropper cannot learn m from cipher-text and public key

Secret key

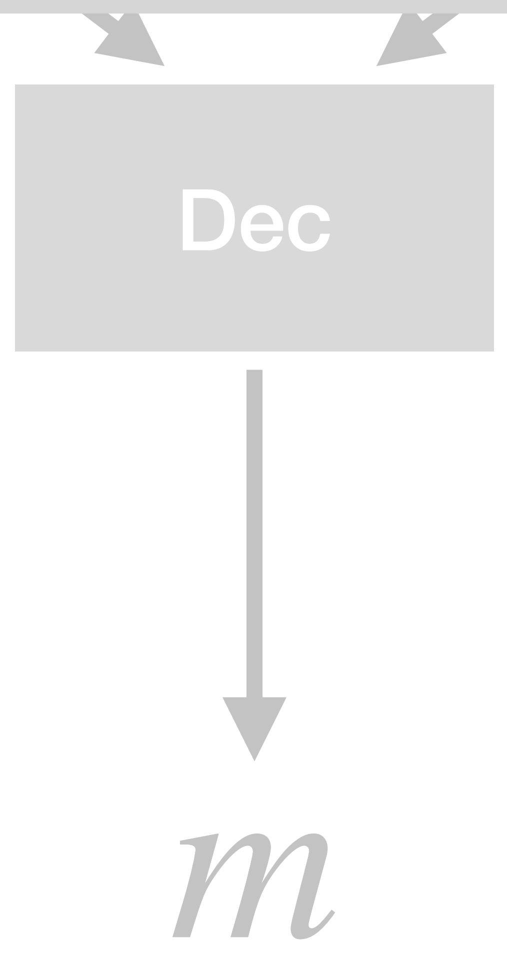
Cipher-text


Secret key
Cipher-text
Dec
m

Can we ensure security when everything is not compromised



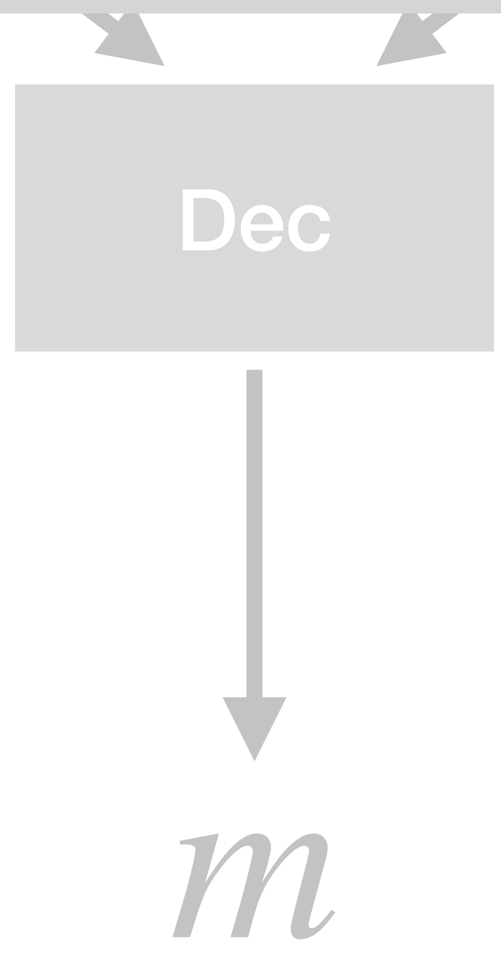
Can we ensure security when everything is not compromised



<u>Case 1</u>

Cipher-text: fully leaked
Secret key: partially leaked

Can we ensure security when everything is not compromised



Case 1

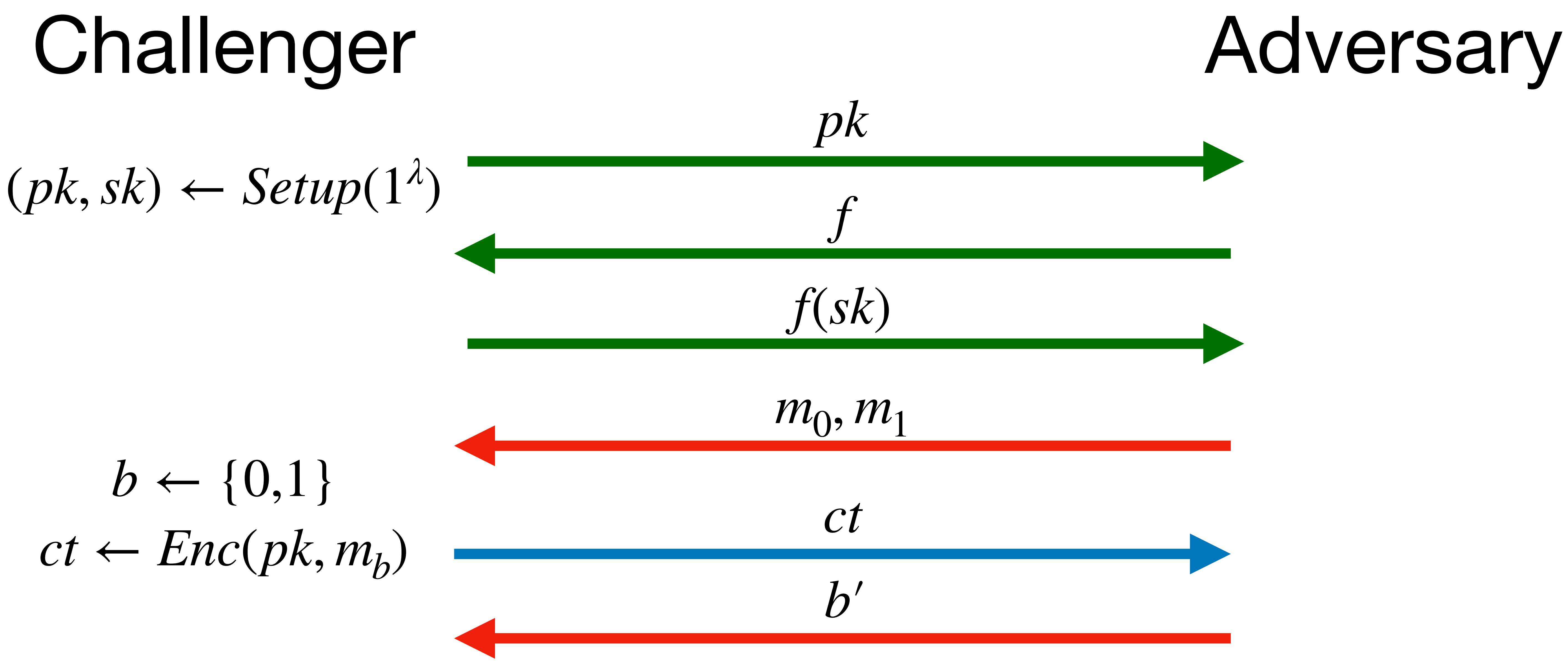
Cipher-text: fully leaked
Secret key: partially leaked

Case 2

Cipher-text: partially leaked
Secret key: fully leaked

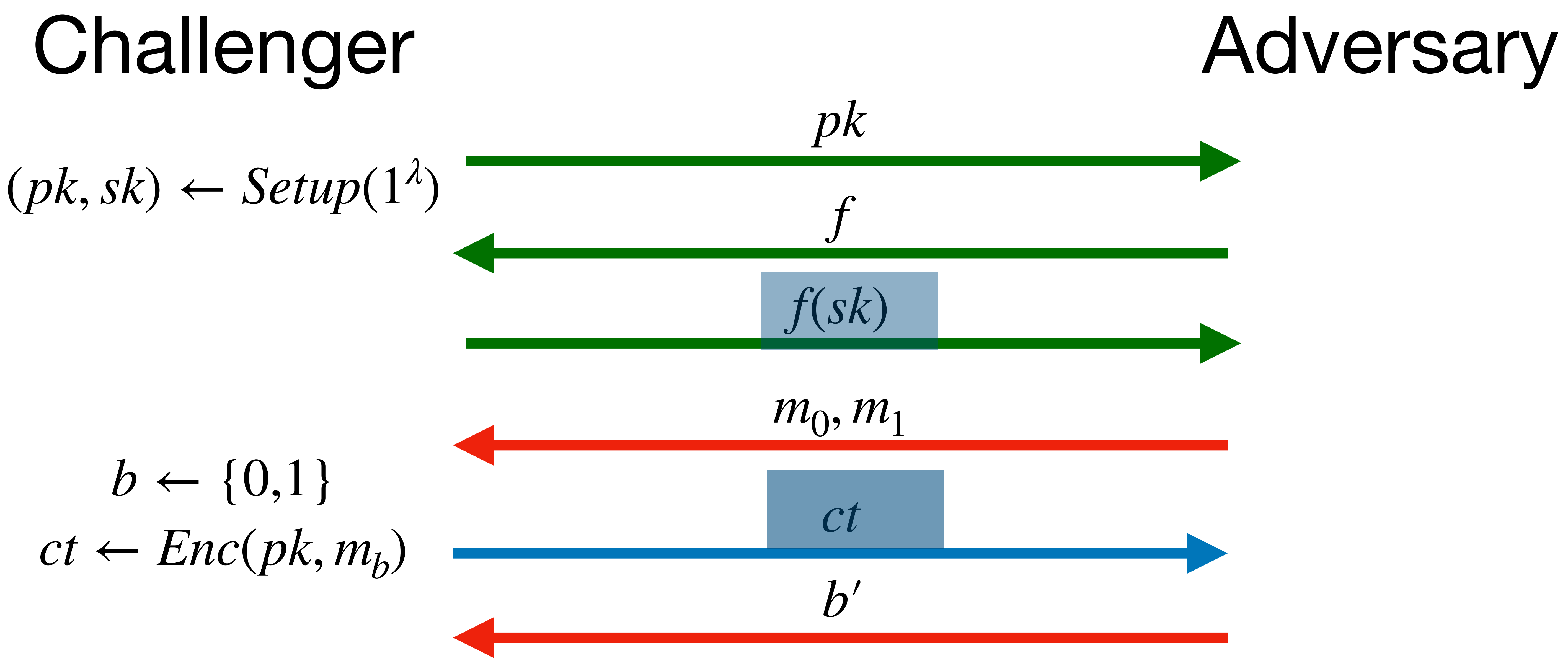
Leakage Resilient Encryption

Secure even if whole cipher text and part of secret key are leaked



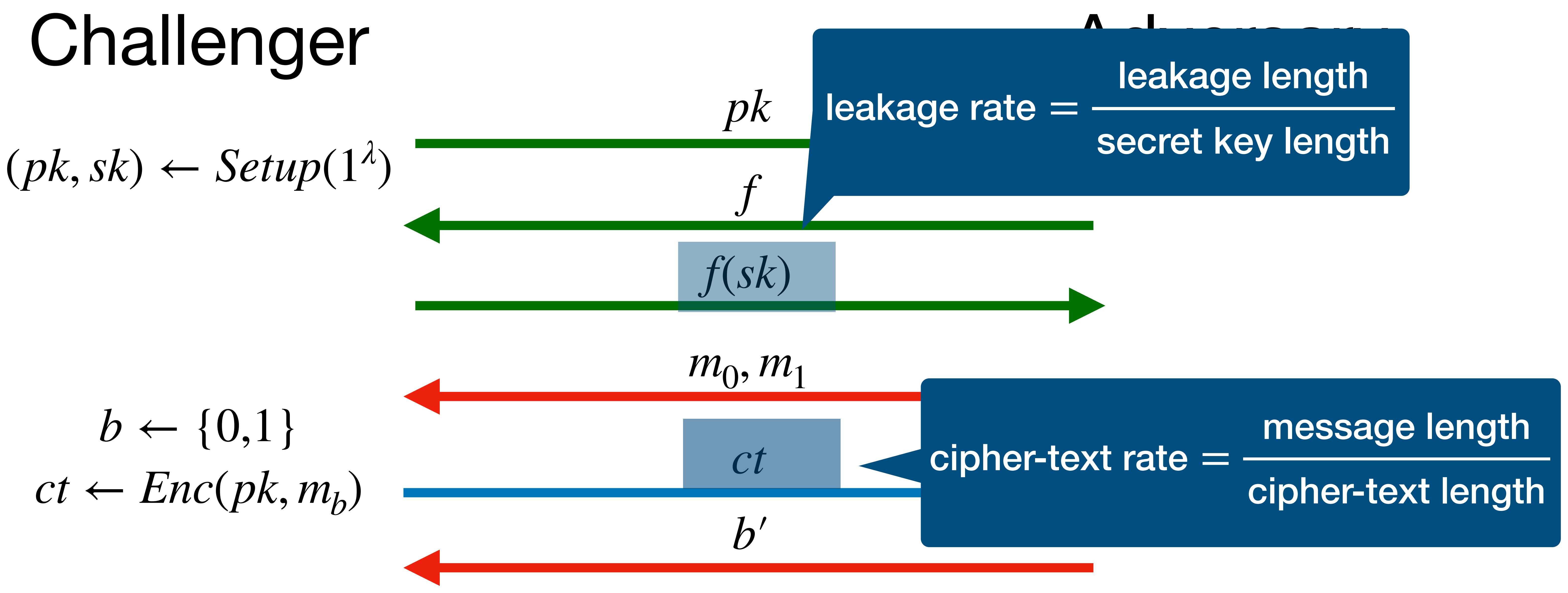
Leakage Resilient Encryption

Secure even if whole cipher text and part of secret key are leaked



Leakage Resilient Encryption

Secure even if whole cipher text and part of secret key are leaked



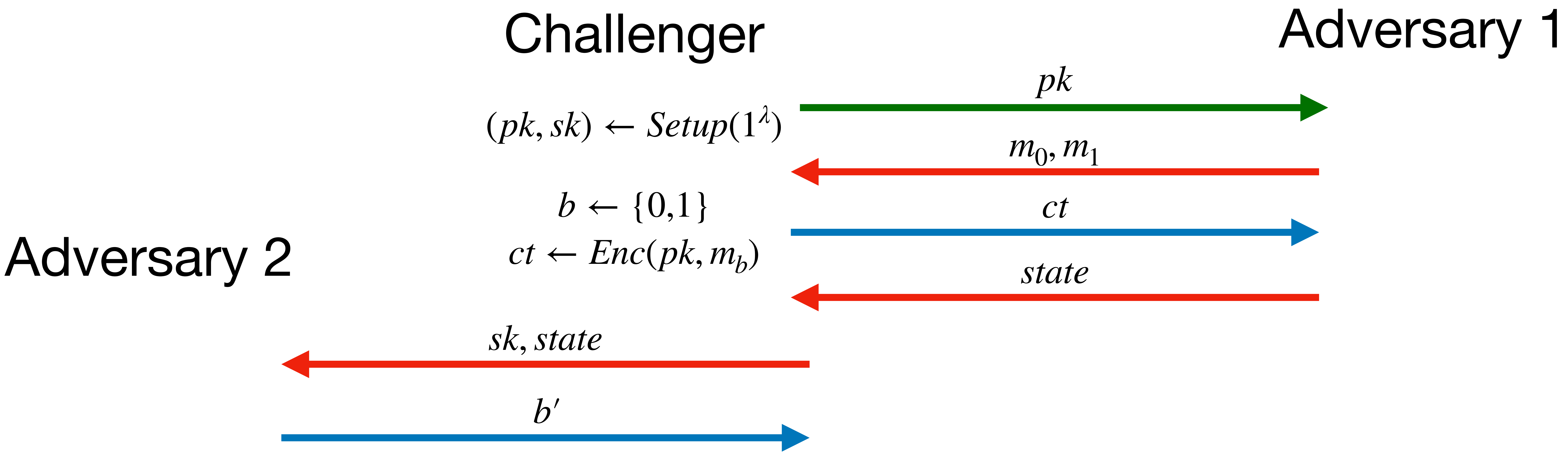
Leakage Resilient Encryption

Secure even if whole secret key and a *compression* of cipher-text are leaked

- [Canetti et al. 00] and [Dodis et al. 01] gave construction where a few bits of sk are leaked.
- [Dziembowski06], [Di Crescenzo et al.06], [Akavia et al.09], etc. considered arbitrary function f.
- Other works include [Dodis et al.09], [Brakerski et al.10], [Dodis et al.10], [Faonio et al.15] and many more

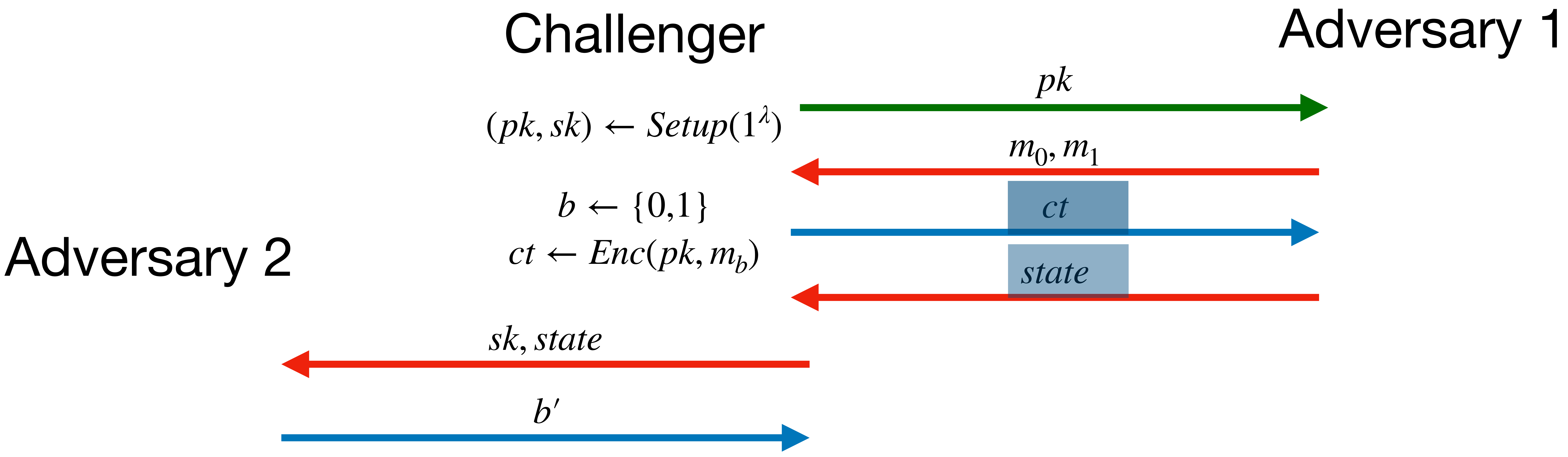
Incompressible Encryption Schemes

Secure even if whole secret key and a *compression* of cipher-text are leaked



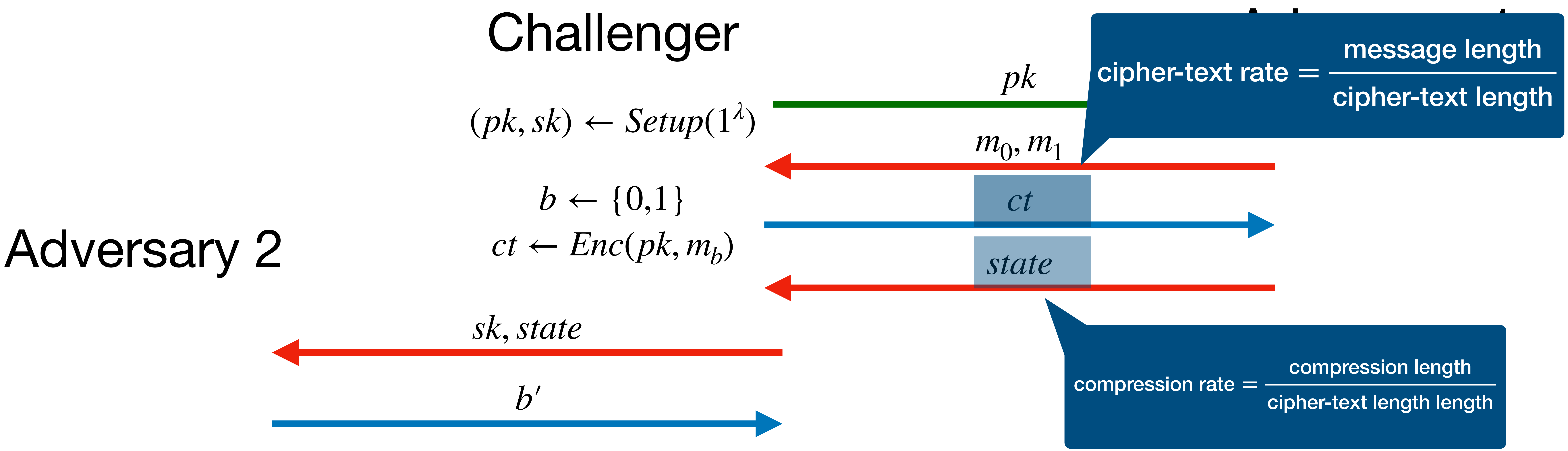
Incompressible Encryption Schemes

Secure even if whole secret key and a *compression* of cipher-text are leaked



Incompressible Encryption Schemes

Secure even if whole secret key and a *compression* of cipher-text are leaked



Incompressible Encryption Schemes

Secure even if whole secret key and a *compression* of cipher-text are leaked

- [Dzi06] gave the first construction under standard assumptions
- [BDD22] gave a rate-1 public key construction using incompressible encoding
- [GKRV24] showed more extensions

Can we achieve security under more types of joint leakages?

Can we achieve security under more types of joint leakages?

More combinations are possible!

Our Model

Leakage-Resilient Incompressible Encryption

Cipher-text is compressed together with some leakage of the secret key. Ensure secure when entire secret key is later revealed

LR-Incompressible Encryption Security Game

LR-Incompressible Encryption Security Game

LR-Incompressible Encryption Security Game

LR-Incompressible Encryption Security Game

Objectives

1. Obtain lower bounds for these rates
2. Design schemes that match the lower bounds

Goal 1: Study Lower Bounds

Conjecture [GWZ22]**.** Security of an *incompressible PKE* scheme with optimal rates cannot be secure when secret key is smaller than message length

Conjecture [GWZ22]**.** Security of an *incompressible PKE* scheme with optimal rates cannot be secure when secret key is smaller than message length

Conjecture'. Security of an *LRI PKE* scheme with optimal rates cannot be proved by black-box reduction from a secure cryptographic game

Conjecture [GWZ22]**.** Security of an *incompressible PKE* scheme with optimal rates cannot be secure when secret key is smaller than message length

Conjecture'. Security of an *LRI PKE* scheme with optimal rates cannot be proved by black-box reduction from a secure cryptographic game

Main Result

These schemes cannot be proved secure by black box reduction from secure cryptographic games

Theorem. Security of an *incompressible PKE* scheme with optimal rates cannot be proved by black-box reduction from a secure cryptographic game when secret key is smaller than message length

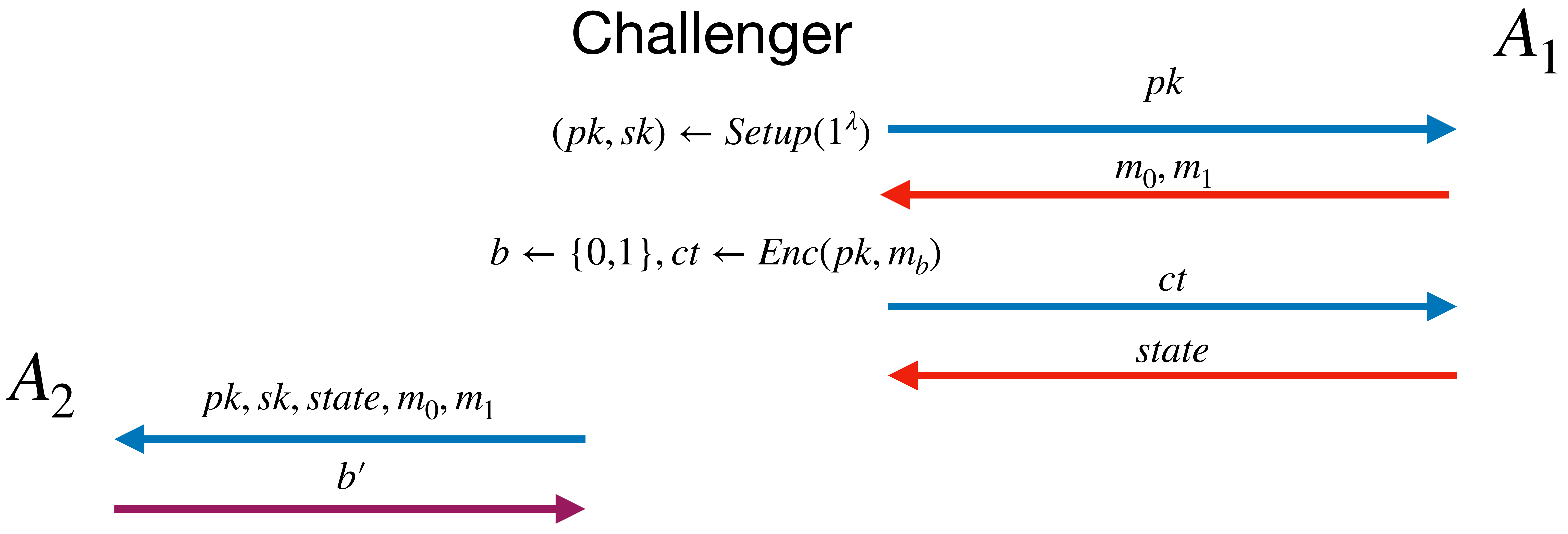
Proof. Using **Simulatable Attack** [GW11, Wichs13]

Theorem. Security of an *incompressible PKE* scheme with optimal rates cannot be proved by black-box reduction from a secure cryptographic game when secret key is smaller than message length

Proof. Using **Simulatable Attack** [GW11, Wichs13]

Simulatable attack for a cryptographic primitive $\mathscr{H}$

- **An inefficient attack A that breaks $\mathscr{H}$**
- **Comes with an efficient Sim that effectively emulates interaction with A**
- **Suppose R is a black box reduction from a secure cryptographic game $\mathscr{G}$ to $\mathscr{H}$**
- R^A **breaks** $\mathscr{G} \implies R^{\mathsf{Sim}}$ **breaks** $\mathscr{G}$
- **Contradicts security of $\mathscr{G}$ since R^{Sim} is efficient**



Simulatable attack for LRI PKE

- A_1 choses (m_0, m_1) as hash of pk; computes compression $state$ as hash of ct
- A_2 guesses b by brute force search to find a ct' that hashes to $state$ and decodes to m_b
- A_2 fails only if there is a ct'' that hashes to $state$ and decodes to m_{1-b}; extremely unlikely

Simulatable attack for LRI PKE

- A_1 choses (m_0, m_1) as hash of pk; computes compression $state$ as hash of ct
- A_2 guesses b by brute force search to find a ct' that hashes to $state$ and decodes to m_b
- A_2 fails only if there is a ct'' that hashes to $state$ and decodes to m_{1-b}; extremely unlikely

Simulating the attack

- Simulate A_1's hashes as random outputs to every fresh input, and storing them in a list
- Simulate A_2's brute force search by simply looking through list

Attack

1. Random functions g, h are hardcoded in A_1,A_2
2. $(m_0, m_1) = A_1(pk) = g(pk)$
3. $state = A_1(ct) = h(ct)$
4. $A_2(state, sk, pk, m_0, m_1)$:
   - $M = \{m : \exists ct', h(ct') = state, IncPKE.Dec(ct', sk) = m\}$
   - Output the unique b' such that $m_{b'} = IncPKE(ct', sk)$

Simulator

1. Sim emulates g, h by keeping databases Q_g, Q_h
2. Sim responds to requests:
   1. $A_1(pk)$: return (m_0, m_1) associated with pk in Q_g; on fail, return random (m_0, m_1) and add $((m_0, m_1), pk)$ to Q_g
   2. $A_1(ct)$: return $state$ associated with ct in Q_h; on fail, return random $state$ and add $(state, ct)$ to Q_h
   3. $A_2(state, sk, pk, m_0, m_1)$:
      - check (m_0', m_1') and ct' associated with pk and $state$
      - Output the unique b' such that $m_{b'} = IncPKE(ct', sk)$

- [Wichs13] and prior works built simulatable attacks for Hashes and Functions
- The correctness constraint makes proving simulatability challenging

Goal 2: Obtain Upper Bounds

Theorem. There exists a LRI SKE scheme with compression and cipher-text rate $1/2$ and leakage rate $1 - o(1)$ with unconditional security

Theorem. There exists a LRI SKE scheme with compression and cipher-text rate $1/2$ and leakage rate $1 - o(1)$ with unconditional security

Improves upon previous simple incSKE scheme with compression and cipher-text rate $1/3$

Theorem. There exists a LRI SKE scheme with compression and cipher-text rate $1/2$ and leakage rate $1 - o(1)$ with unconditional security

Improves upon previous simple incSKE scheme with compression and cipher-text rate $1/3$

Theorem. There exists a LRI PKE scheme with compression and cipher-text rate $1/2$ and leakage rate $1 - o(1)$

Theorem. There exists a LRI SKE scheme with compression and cipher-text rate $1/2$ and leakage rate $1 - o(1)$ with unconditional security

- Transforms Incompressible SKE to LRI SKE
- Use a leakage resilient secret key in a Incompressible SKE scheme
- Instantiating with Inc SKE from [Dzi06] gives rate $1/3$
- We build an Inc SKE with rate $1/2$ using invertible extractors

LRI SKE + PKE -> LRI PKE

Public Key consists of 2n public keys $\{pk_{i,b}\}_{i \in [n], b \in \{0,2\}}$

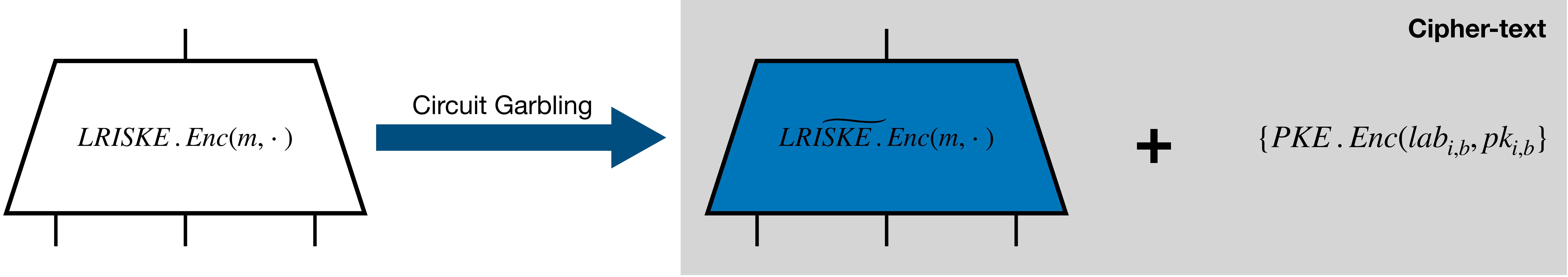
$lab_{1,0}, lab_{2,0}, \ldots, lab_{n,0}$

$lab_{1,1}, lab_{2,1}, \ldots, lab_{n,1}$

Deferred Encryption [GKW16, GKRV23]

LRI SKE + PKE -> LRI PKE

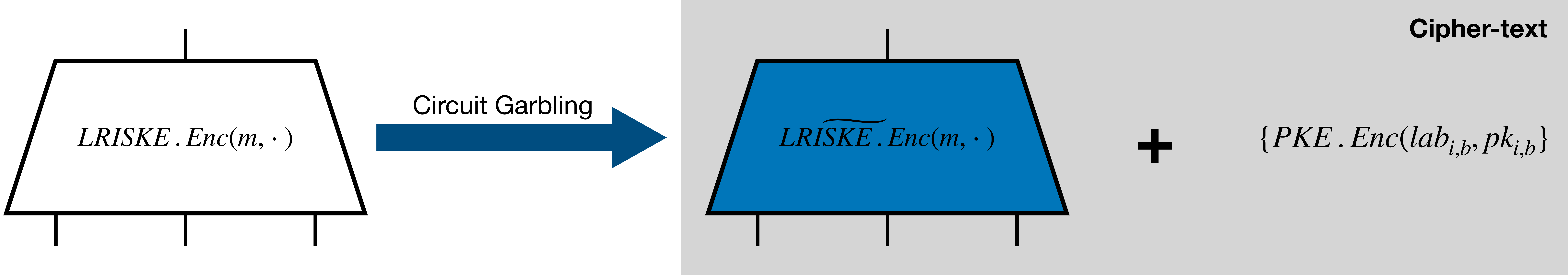
Public Key consists of 2n public keys $\{pk_{i,b}\}_{i\in[n],b\in\{0,1\}}$



Deferred Encryption [GKW16, GKRV23]

LRI SKE + PKE -> LRI PKE

Public Key consists of 2n public keys $\{pk_{i,b}\}_{i\in[n],b\in\{0,1\}}$



Secret Key consists of secret key s **for** $LRISKE$**, and n secret keys of PKE:** $\{sk_{i,s_i}\}_{i\in[n]}$

Decryption

- Recover $\{lab_{i,s_i}\}_{i\in[n]}$; use garbled circuit to compute $ct = LRISKE.Enc(m,s)$
- Recover the message as $m = LRISKE.Dec(ct,s)$

Deferred Encryption [GKW16, GKRV23]

Further Results

- Transformation from Incompressible SKE to LRI PKE using a leakage resilient non-committing key encapsulation mechanism.

- We define and construct LRI signatures as a generalization incompressible signatures as mentioned in [GWZ22].

Conclusion

	Cipher-text Rate	Compression Rate	Leakage Rate	Feasible?
IT.SKE	1/2	1/2	1-o(1)	This work
	1/3	1/2	0	[Dzi06]
PKE	1/2	1/2	1-o(1)	This work Assuming DDH,DCR
	1-o(1)	1-o(1)	0	[BDD22] using large secret key
PKE/SKE	1-o(1)	1-o(1)	1-o(1)	Barrier
	1-o(1)	1-o(1)	0	Barrier with message sized secret key

Leakage Resilient Incompressible (LRI) Encryption Schemes

Conclusion

	Cipher-text Rate	Compression Rate	Leakage Rate	Feasible?
IT.SKE	1/2	1/2	1-o(1)	This work
	1/3	1/2	0	[Dzi06]
PKE	1/2	1/2	1-o(1)	This work Assuming DDH,DCR
	1-o(1)	1-o(1)	0	[BDD22] using large secret key
PKE/SKE	1-o(1)	1-o(1)	1-o(1)	Barrier
	1-o(1)	1-o(1)	0	Barrier with message sized secret key

Leakage Resilient Incompressible (LRI) Encryption Schemes

Thank You!