Incompressible Functional Encryption

Mahesh Sreekumar Rajasree
CISPA Helmholtz

European Research Council
Established by the European Commission

Joint work with Rishab Goyal (UW-Madison), Venkata Koppula (IITD) and Aman Verma (IITD)

Functional Encryption (FE) [Sahai-Waters05…]

Functional Encryption (FE)[Sahai-Waters05…]

mpk

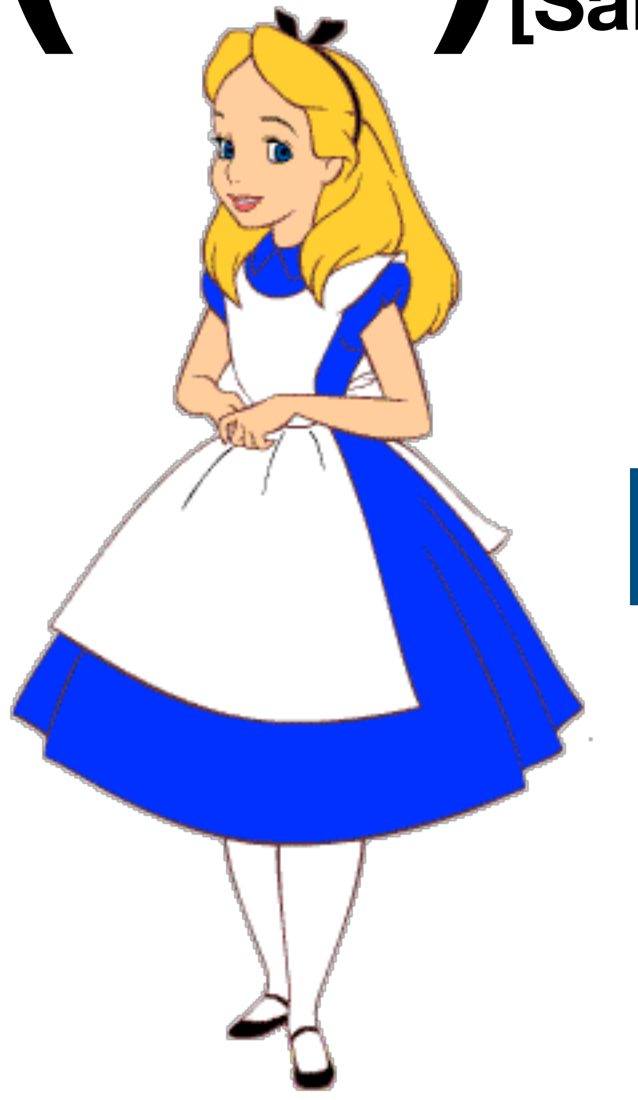
Functional Encryption (FE)[Sahai-Waters05…]

msk

mpk

Functional Encryption (FE)[Sahai-Waters05…]

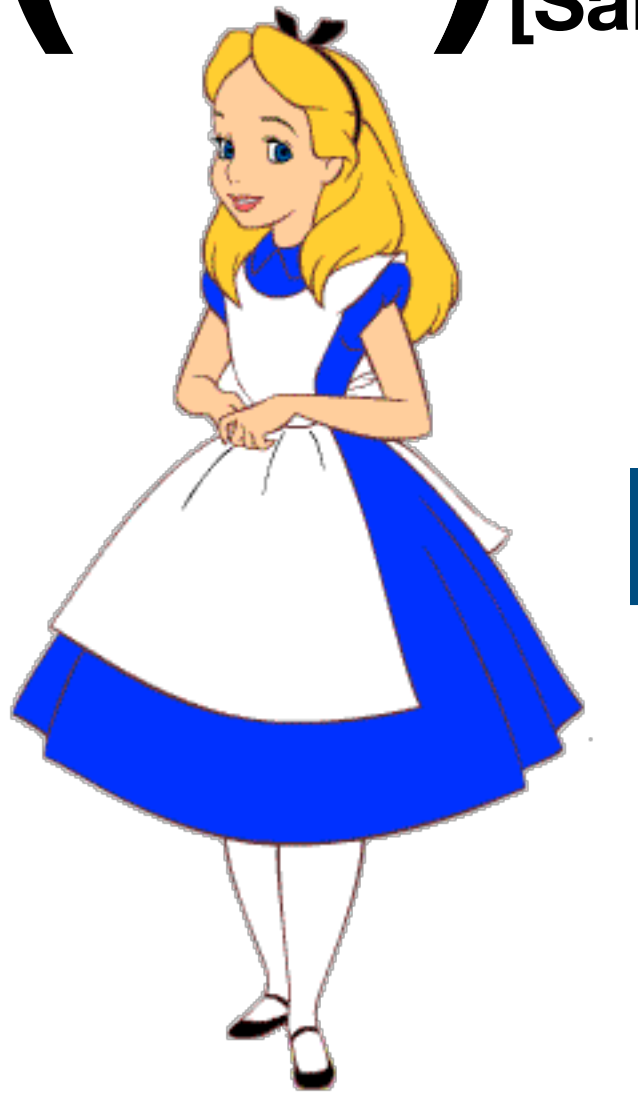
msk



mpk

Functional Encryption (FE)[Sahai-Waters05…]

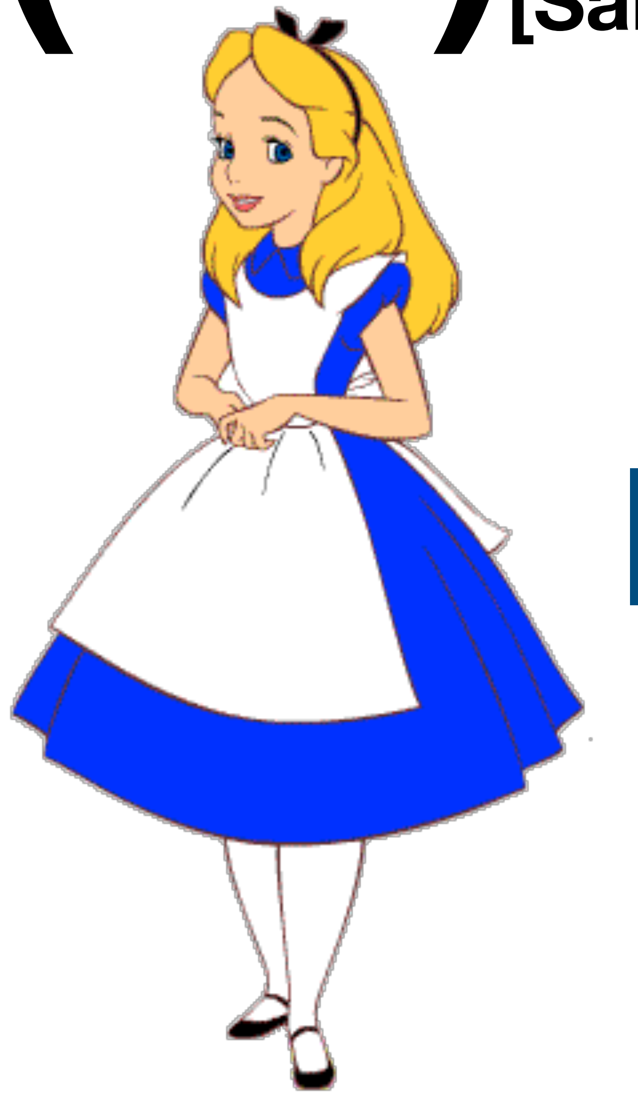
$\boxed{msk}$



$\boxed{mpk}, m$

Functional Encryption (FE) [Sahai-Waters05…]

msk



mpk, m

Functional Encryption (FE)[Sahai-Waters05…]

$\boxed{msk}$

$\boxed{mpk}, m$

Functional Encryption (FE) [Sahai-Waters05…]

msk

mpk, m

$ct = Enc(mpk, m)$

Functional Encryption (FE) [Sahai-Waters05…]

msk

mpk, m

$ct = Enc(mpk, m)$

Learns only $f(m)$

Functional Encryption (FE) [Sahai-Waters05...]

$\boxed{msk}$

$\boxed{mpk}, m$

$ct = Enc(mpk, m)$

Learns only $f(m)$

Functional Encryption (FE)[Sahai-Waters05…]

$\boxed{msk}$

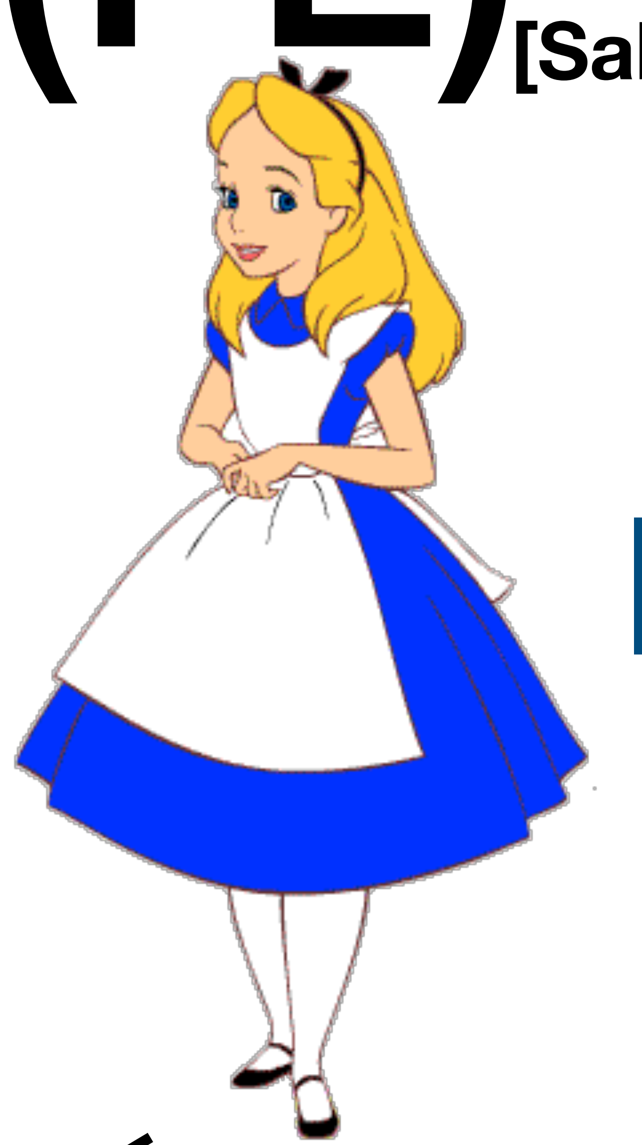
$\boxed{mpk}, m$

$ct = Enc(mpk, m)$

Learns only $f(m)$

Functional Encryption (FE) [Sahai-Waters05…]

msk



mpk, m

sk_f

$ct = Enc(mpk, m)$

Learns only $f(m)$

Functional Encryption (FE) [Sahai-Waters05…]

msk

- *Hides* everything but $f(m)$

mpk, m

sk_f

$ct = Enc(mpk, m)$

Learns only $f(m)$

Functional Encryption (FE)[Sahai-Waters05…]

msk

- *Hides* everything but $f(m)$
- *Without* outsourcing to Bob

mpk, m

sk_f

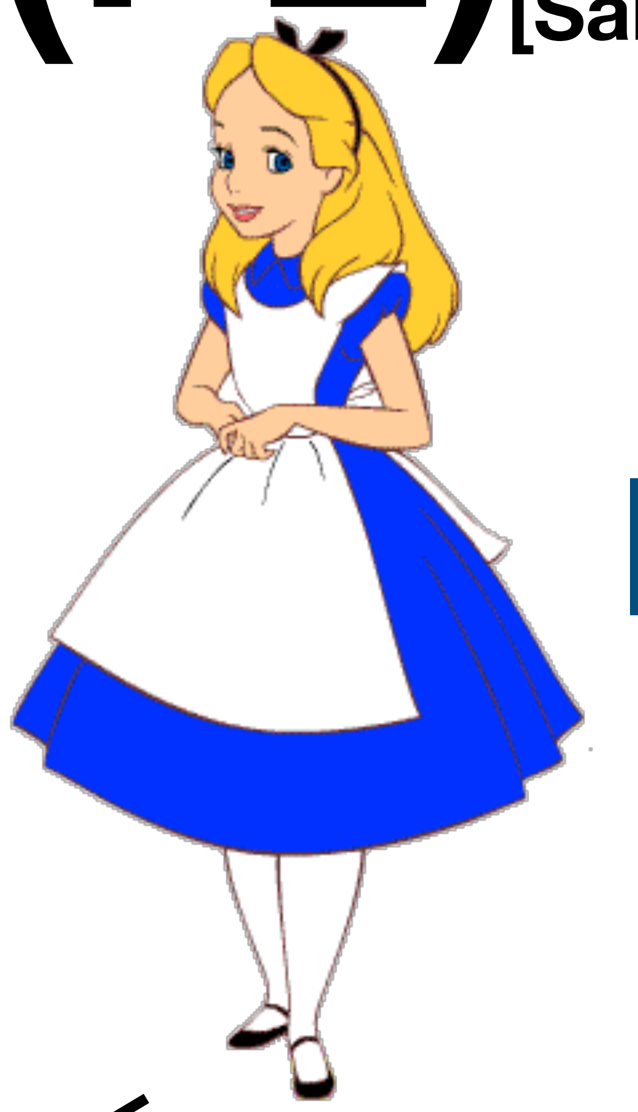
$ct = Enc(mpk, m)$

Learns only $f(m)$

Functional Encryption (FE) [Sahai-Waters05…]

msk

- *Hides* everything but $f(m)$
- *Without* outsourcing to Bob
- Even when Bob is *offline*



mpk, m

sk_f

$ct = Enc(mpk, m)$

Learns only $f(m)$

FE Syntax

FE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

FE Syntax

$Setup(\lambda) \to$ master public key $\boxed{mpk}$, master secret key $\boxed{msk}$

$Enc(\boxed{mpk}, m) \to$ Ciphertext $\boxed{ct}$

FE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk, master secret key msk

$Enc(mpk, m) \rightarrow$ Ciphertext ct

$KeyGen(msk, f) \rightarrow$ Secret key sk_f

FE Syntax

$Setup(\lambda) \rightarrow$ master public key $\boxed{mpk}$, master secret key $\boxed{msk}$

$Enc(\boxed{mpk}, m) \rightarrow$ Ciphertext $\boxed{ct}$

$KeyGen(\boxed{msk}, f) \rightarrow$ Secret key $\boxed{sk_f}$

$Dec(\boxed{sk_f}, \boxed{ct}) \rightarrow f(m)$

FE Security

FE Security

Adversary

FE Security

$Enc(mpk, \mathbf{m_0})$

$sk_{f_1}, \ldots, sk_{f_q}$

Adversary

FE Security

$Enc(mpk, \mathbf{m_0})$
$sk_{f_1}, \ldots, sk_{f_q}$

Adversary

$Enc(mpk, \mathbf{m_1})$
$sk_{f_1}, \ldots, sk_{f_q}$

FE Security

$Enc(mpk, \mathbf{m_0})$
$sk_{f_1}, \ldots, sk_{f_q}$

Adversary

$Enc(mpk, \mathbf{m_1})$
$sk_{f_1}, \ldots, sk_{f_q}$

Indistinguishable whenever $f_i(m_0) = f_i(m_1)$ **for all** i

FE Security: Limitations

FE Security: Limitations

- Master secret key must remain completely hidden from adversary.

FE Security: Limitations

- Master secret key must remain completely hidden from adversary.
  - Can generate any secret key!!!

FE Security: Limitations

- Master secret key must remain completely hidden from adversary.
  - Can generate any secret key!!!
- Wins if adversary obtains even a single **distinguishing key** (sk_f such that $f(m_0) \neq f(m_1)$).

FE Security: Limitations

- Master secret key must remain completely hidden from adversary.
  - Can generate any secret key!!!
- Wins if adversary obtains even a single **distinguishing key** (sk_f such that $f(m_0) \neq f(m_1)$).
  - Unrealistic to expect that **every secret key** can be securely stored.

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has entire ciphertext and entire secret key due to correctness.

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has entire ciphertext and entire secret key due to correctness.

- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model.

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has entire ciphertext and entire secret key due to correctness.

- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model.

    - Make ciphertext large so that long-term storage is expensive.

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has entire ciphertext and entire secret key due to correctness.
- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model.
  - Make ciphertext large so that long-term storage is expensive.
  - Adversary gets a challenge ciphertext ct^* for m_0, m_1 and then it has to compress/reduce its storage which contains ct^*.

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has entire ciphertext and entire secret key due to correctness.
- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model.
  - Make ciphertext large so that long-term storage is expensive.
  - Adversary gets a challenge ciphertext ct^* for m_0, m_1 and then it has to compress/reduce its storage which contains ct^*.
  - After which it receives sk, but still should not be able to distinguish.

Prior works

Prior works

	Primitives

Prior works

	Primitives
Dziembowski'06	Introduced and constructed the first Incompressible SKE.

Prior works

	Primitives
Dziembowski'06	Introduced and constructed the first Incompressible SKE.
Guan-Wichs-Zhandry'22	Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).

Prior works

	Primitives
Dziembowski'06	Introduced and constructed the first Incompressible SKE.
Guan-Wichs-Zhandry'22	Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).
Branco-Döttling-Dujmovic'23	Constructed CCA-Incompressible PKE (rate-1) from standard assumptions.

Prior works

	Primitives
Dziembowski'06	Introduced and constructed the first Incompressible SKE.
Guan-Wichs-Zhandry'22	Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).
Branco-Döttling-Dujmovic'23	Constructed CCA-Incompressible PKE (rate-1) from standard assumptions.
Guan-Wichs-Zhandry'23	Extended the notion to Multi-user Incompressible PKE setting.

This work

This work

- Our goal — generalize incompressibility to Functional encryption.

This work

- Our goal — generalize incompressibility to Functional encryption.
  - Defined 3 levels of security notion.

This work

- Our goal — generalize incompressibility to Functional encryption.
  - Defined 3 levels of security notion.
  - Adversary can be provided either msk or multiple distinguishing keys or only a single distinguishing key.

This work

- Our goal — generalize incompressibility to Functional encryption.
  - Defined 3 levels of security notion.
  - Adversary can be provided either msk or multiple distinguishing keys or only a single distinguishing key.
- Presented multiple incompressible FE schemes with (optimal) efficiency parameters.

This work

- Our goal — generalize incompressibility to Functional encryption.
  - Defined 3 levels of security notion.
  - Adversary can be provided either msk or multiple distinguishing keys or only a single distinguishing key.
- Presented multiple incompressible FE schemes with (optimal) efficiency parameters.
- Incompressible ABE from standard assumptions.

Incompressible FE Security

Incompressible FE Security

Incompressible FE Security

Challenger

Adversary 1

Incompressible FE Security

Challenger

Adversary 1

$$(msk, mpk) \leftarrow Setup()$$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{mpk}$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{mpk}$

$\xleftarrow{f}$

$\xrightarrow{KeyGen(msk, f)}$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$

mpk

f

$KeyGen(msk, f)$

m_0, m_1

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{\quad mpk \quad}$

$\xleftarrow{\quad f \quad}$ $\xrightarrow{\quad KeyGen(msk, f) \quad}$

$\xleftarrow{\quad m_0, m_1 \quad}$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{mpk}$

$\xleftarrow{f}$ $\xrightarrow{KeyGen(msk, f)}$

$\xleftarrow{m_0, m_1}$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$ $\xrightarrow{c}$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{\quad mpk \quad}$

$\xleftarrow{\quad f \quad}$ $\xrightarrow{\quad KeyGen(msk, f) \quad}$

$\xleftarrow{\quad m_0, m_1 \quad}$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$ $\xrightarrow{\quad c \quad}$

$\xleftarrow{\quad f \quad}$ $\xrightarrow{\quad KeyGen(msk, f) \quad}$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{\quad mpk \quad}$

$\xleftarrow{\quad f \quad}$ $\xrightarrow{\quad KeyGen(msk, f) \quad}$

$\xleftarrow{\quad m_0, m_1 \quad}$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$ $\xrightarrow{\quad c \quad}$

$\xleftarrow{\quad f \quad}$ $\xrightarrow{\quad KeyGen(msk, f) \quad}$

$\xleftarrow{\quad state \quad}$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{\quad mpk \quad}$

$\xleftarrow{\quad f \quad}$ $\xrightarrow{\quad KeyGen(msk, f) \quad}$

$\xleftarrow{\quad m_0, m_1 \quad}$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$ $\xrightarrow{\quad c \quad}$

$\xleftarrow{\quad f \quad}$ $\xrightarrow{\quad KeyGen(msk, f) \quad}$

$\xleftarrow{\quad state \quad}$

$|state| \leq S$

Incompressible FE Security

Challenger

Adversary 1

Adversary 2

$(msk, mpk) \leftarrow Setup()$ $\quad mpk \rightarrow$

f $\leftarrow$ / $\rightarrow$ $KeyGen(msk, f)$

$\leftarrow m_0, m_1$

$b \leftarrow \{0,1\}$

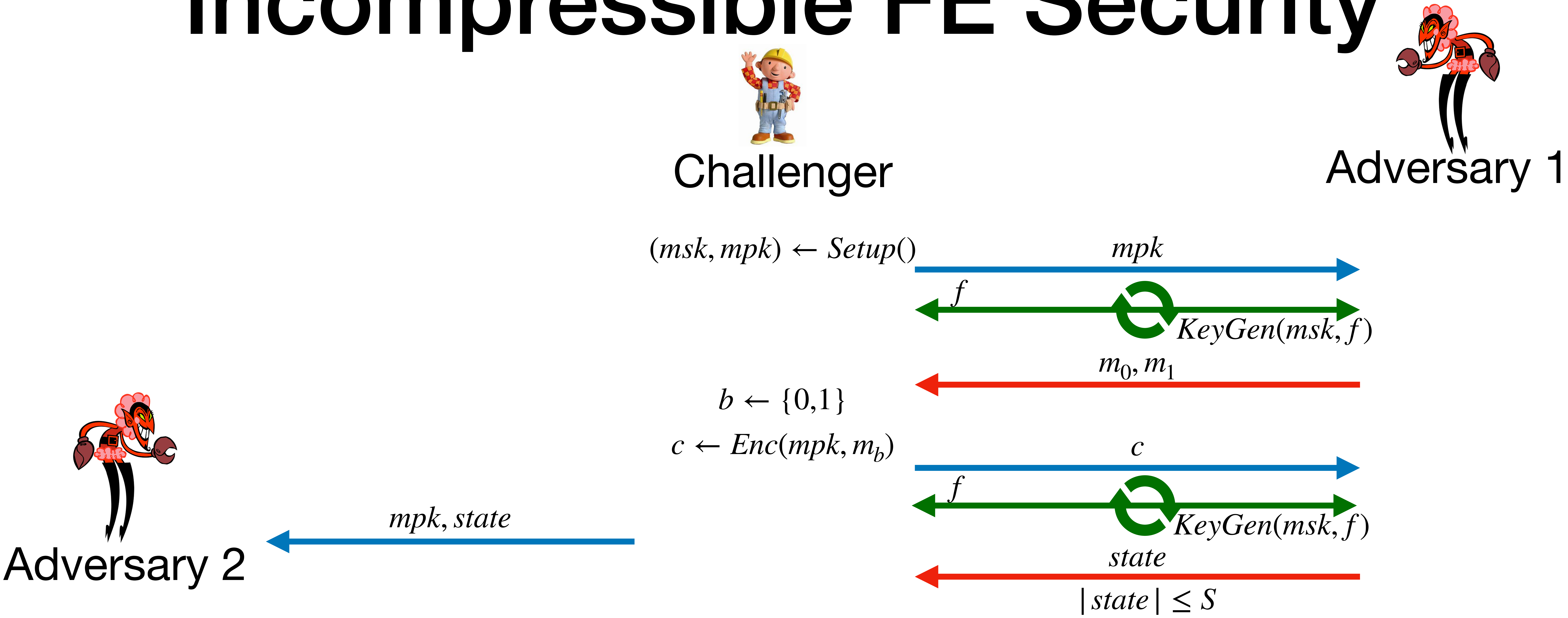
$c \leftarrow Enc(mpk, m_b)$ $\quad c \rightarrow$

f $\leftarrow$ / $\rightarrow$ $KeyGen(msk, f)$

$\leftarrow state$

$|state| \leq S$

Incompressible FE Security



Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\quad$ mpk

f $\quad$ $KeyGen(msk, f)$

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$ $\quad$ c

f $\quad$ $KeyGen(msk, f)$

$state$

$|state| \leq S$

Adversary 2

$mpk, state$

$distinguishing\ f$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$

mpk

f

$KeyGen(msk, f)$

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$

c

f

$KeyGen(msk, f)$

$state$

$|state| \leq S$

Adversary 2

$mpk, state$

distinguishing f

sk_f

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$ $\xrightarrow{mpk}$

$\xleftarrow{f}$ $\xrightarrow{}$ $KeyGen(msk, f)$

$\xleftarrow{m_0, m_1}$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$ $\xrightarrow{c}$

$\xleftarrow{f}$ $\xrightarrow{}$ $KeyGen(msk, f)$

$\xleftarrow{state}$

$|\, state \,| \leq S$

Adversary 2

$\xleftarrow{mpk, state}$

$\xrightarrow{distinguishing\ f}$

$\xleftarrow{sk_f}$

$\xrightarrow{b' \in \{0,1\}}$

Incompressible FE Security

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$

mpk

f

$KeyGen(msk, f)$

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$

c

f

$KeyGen(msk, f)$

$state$

$|state| \leq S$

Adversary 2

$mpk, state$

$distinguishing\ f$

sk_f

$b' \in \{0,1\}$

Adversaries win if $b = b'$

Incompressible FE Security (Regular)

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$

mpk

f

$KeyGen(msk, f)$

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$

c

f

$KeyGen(msk, f)$

$state$

$|state| \leq S$

Adversary 2

$mpk, state$

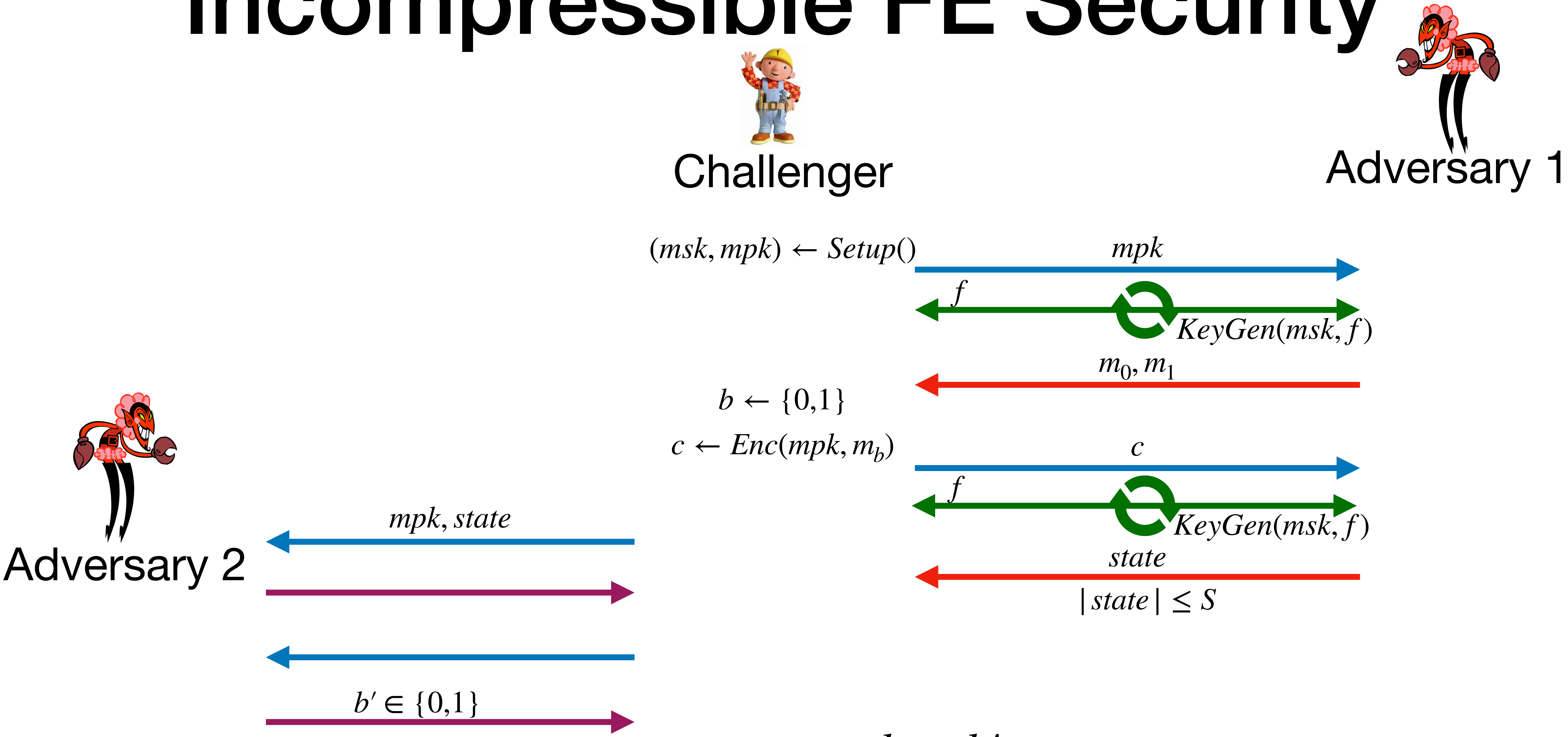
$distinguishing\ f$

sk_f

$b' \in \{0,1\}$

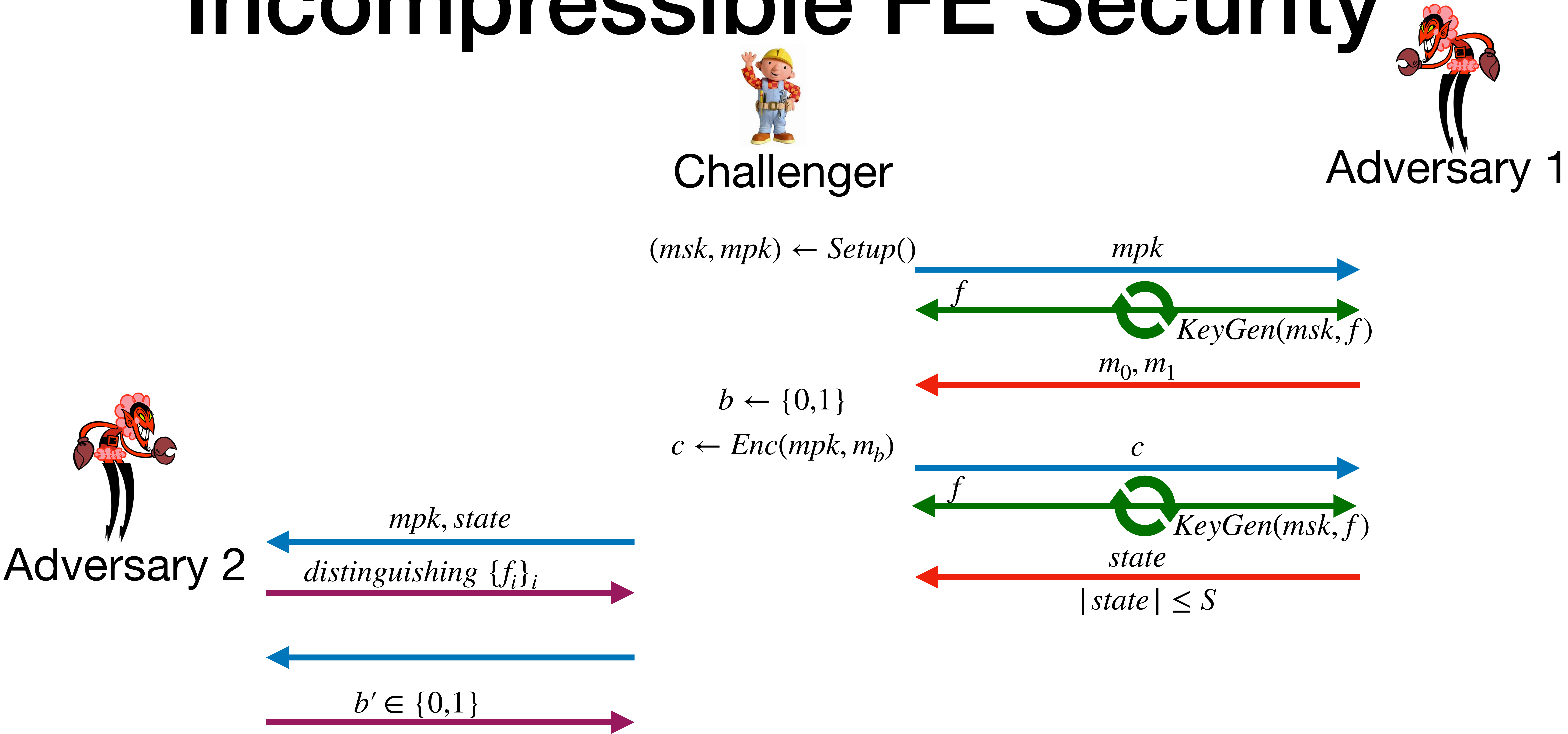
Adversaries win if $b = b'$

Incompressible FE Security



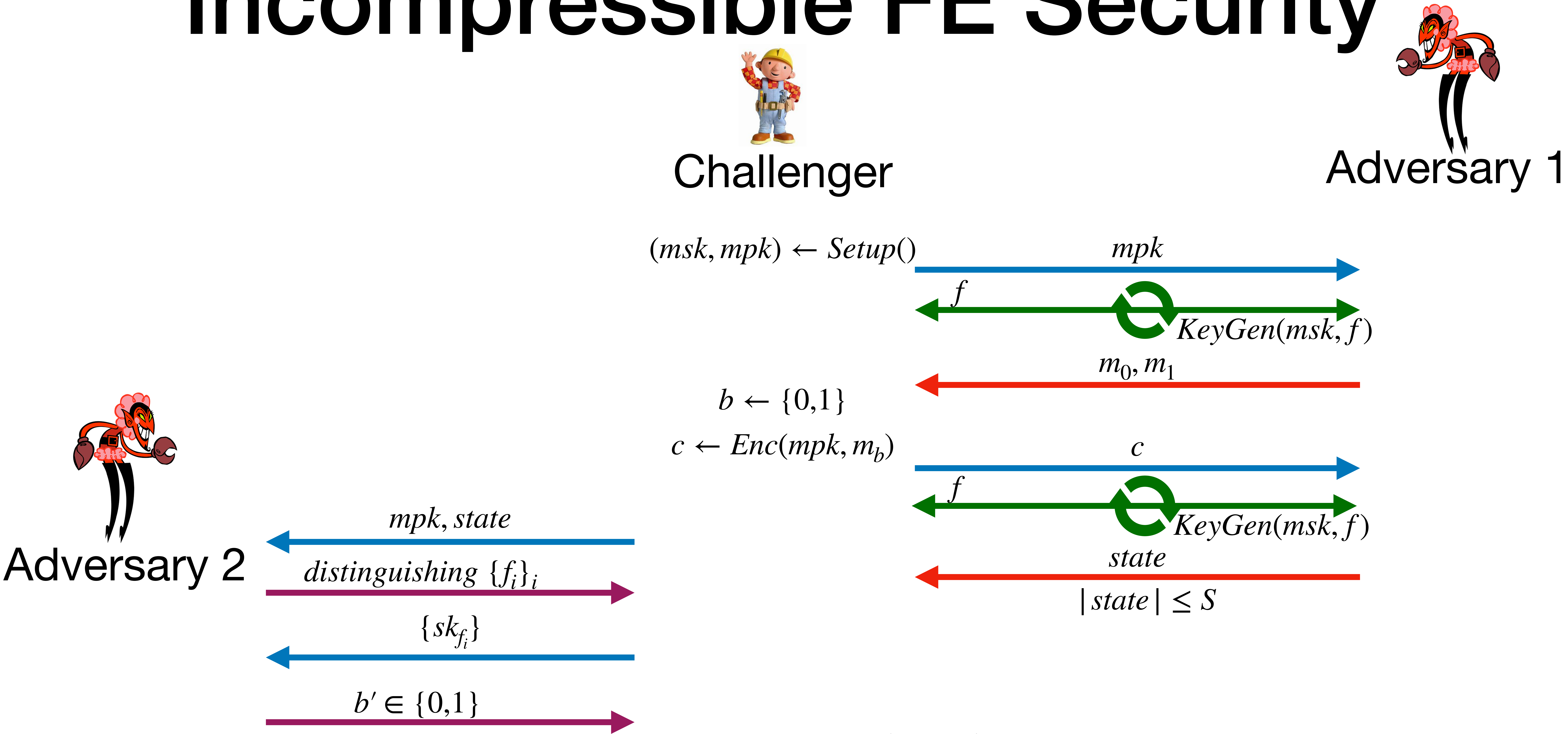
Adversaries win if $b = b'$

Incompressible FE Security



Adversaries win if $b = b'$

Incompressible FE Security



Adversaries win if $b = b'$

Incompressible FE Security
(Semi-Strong)

Challenger

Adversary 1

$(msk, mpk) \leftarrow Setup()$

mpk

f

$KeyGen(msk, f)$

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$

c

f

$KeyGen(msk, f)$

$state$

$|state| \leq S$

Adversary 2

$mpk, state$

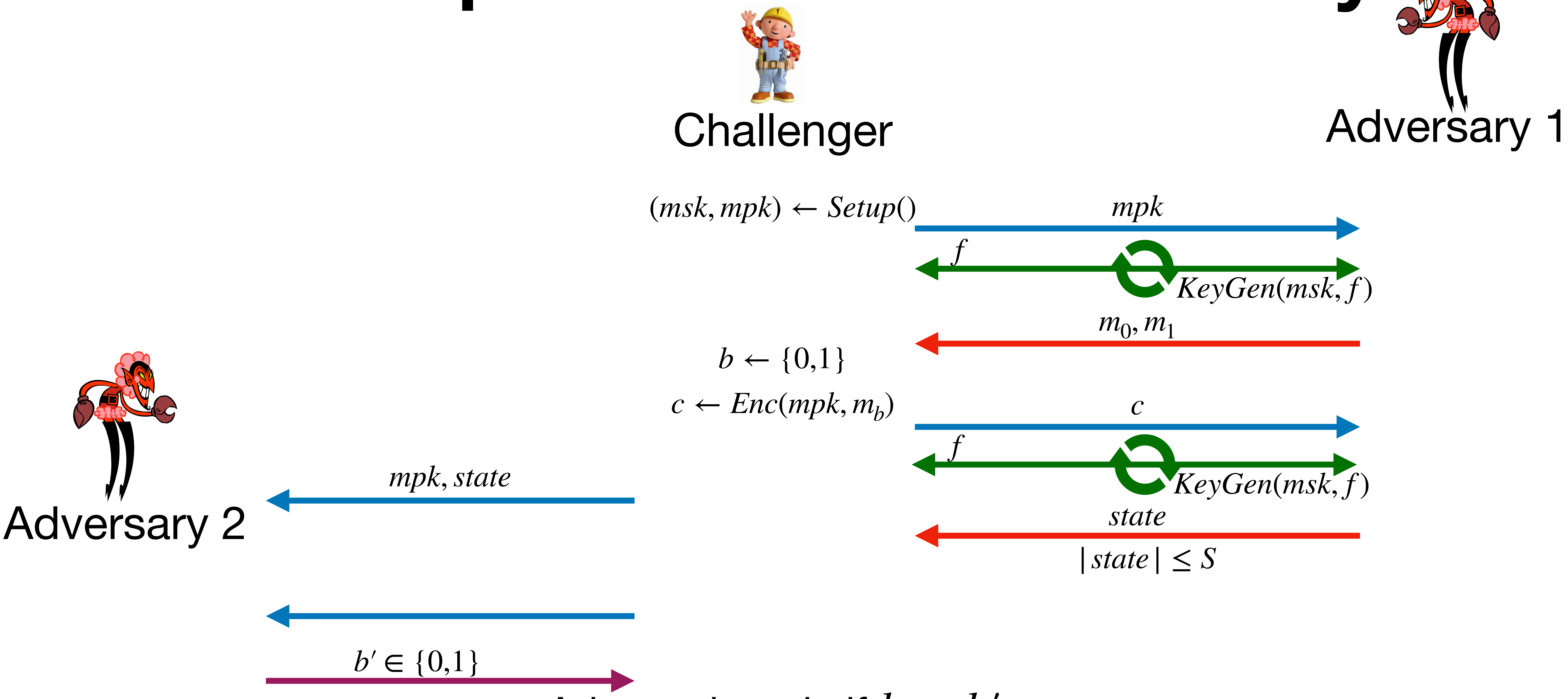
$distinguishing\ \{f_i\}_i$

$\{sk_{f_i}\}$

$b' \in \{0,1\}$

Adversaries win if $b = b'$

Incompressible FE Security



Adversaries win if $b = b'$

Incompressible FE Security

Challenger

Adversary 1

Adversary 2

$(msk, mpk) \leftarrow Setup()$

mpk

f

$KeyGen(msk, f)$

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$

c

f

$KeyGen(msk, f)$

$state$

$|state| \leq S$

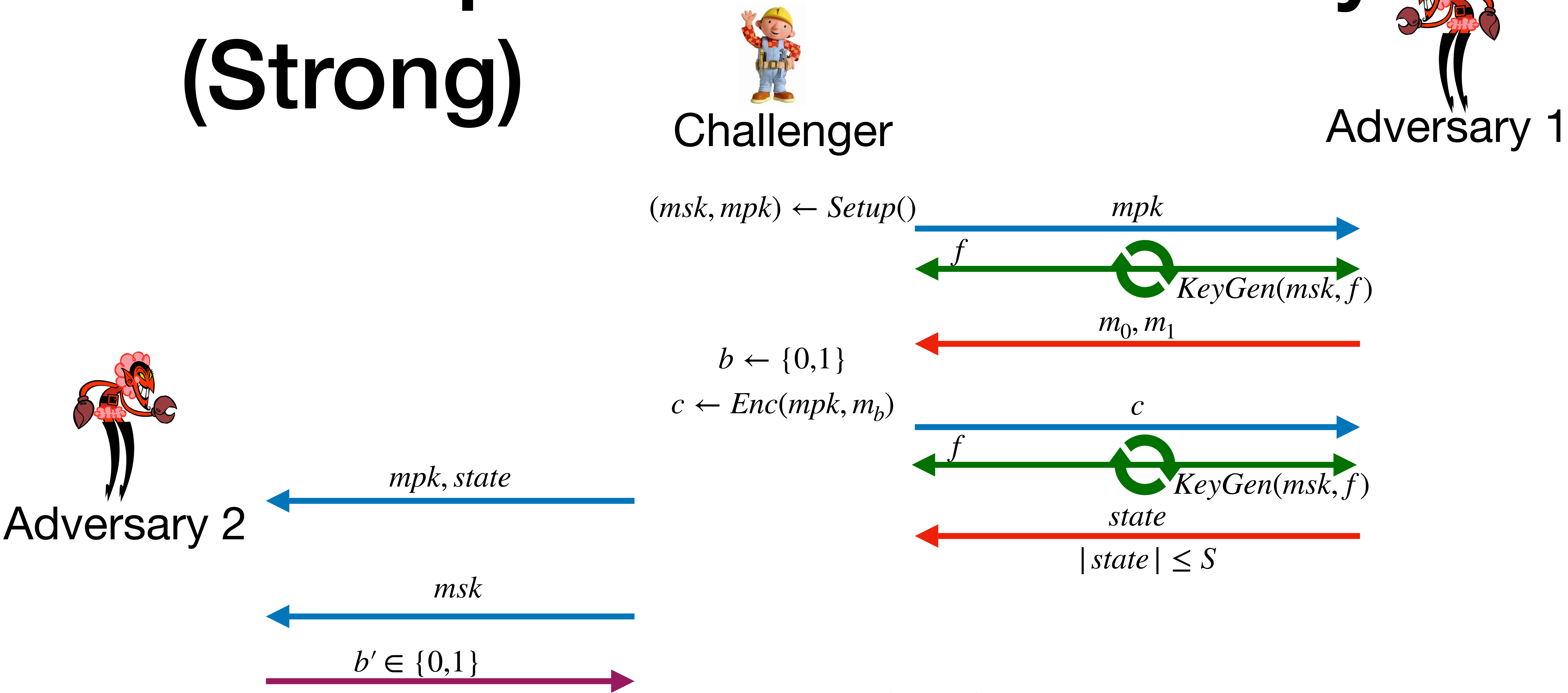
$mpk, state$

msk

$b' \in \{0,1\}$

Adversaries win if $b = b'$

Incompressible FE Security (Strong)



Adversaries win if $b = b'$

Our Results

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions
Semi-Strong Incomp FE	1/2	Short	No	FE

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions
Semi-Strong Incomp FE	1/2	Short	No	FE
Semi-Strong Incomp FE	1/4	Short	Yes	FE

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions
Semi-Strong Incomp FE	1/2	Short	No	FE
Semi-Strong Incomp FE	1/4	Short	Yes	FE
Semi-Strong Incomp FE	1	Large	No	FE

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions
Semi-Strong Incomp FE	1/2	Short	No	FE
Semi-Strong Incomp FE	1/4	Short	Yes	FE
Semi-Strong Incomp FE	1	Large	No	FE
Regular Incomp FE	1	Short*	No	FE

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions
Semi-Strong Incomp FE	1/2	Short	No	FE
Semi-Strong Incomp FE	1/4	Short	Yes	FE
Semi-Strong Incomp FE	1	Large	No	FE
Regular Incomp FE	1	Short*	No	FE

* = functions with one bit output

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions
Semi-Strong Incomp FE	1/2	Short	No	FE
Semi-Strong Incomp FE	1/4	Short	Yes	FE
Semi-Strong Incomp FE	1	Large	No	FE
Regular Incomp FE	1	Short*	No	FE
Regular Incomp ABE	1/2	Short	Yes	subexp LWE

* = functions with one bit output

Our Results

Primitive	Rate (|m| / |ct|)	Secret-key size	Adaptive	Assumptions
Semi-Strong Incomp FE	1/2	Short	No	FE
Semi-Strong Incomp FE	1/4	Short	Yes	FE
Semi-Strong Incomp FE	1	Large	No	FE
Regular Incomp FE	1	Short*	No	FE
Regular Incomp ABE	1/2	Short	Yes	subexp LWE

OPTIMAL [BGKNPR'24]

* = functions with one bit output

Rate-1/2 Incomp FE with Large Keys

Rate-1/2 Incomp FE with Large Keys

1. **Regular FE scheme**

Rate-1/2 Incomp FE with Large Keys

1. **Regular FE scheme**
2. **Regular SKE scheme**

Rate-1/2 Incomp FE with Large Keys

1. **Regular FE scheme**
2. **Regular SKE scheme**
3. **Incompressible PKE scheme**

Rate-1/2 Incomp FE with Large Keys

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow$

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = ($

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\boxed{FE.MPK} \;,$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ \boxed{FE.MPK}\ ,\ \boxed{IncPKE.PK}\ )$$

$$MSK = ($$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\boxed{FE.MPK} , \boxed{IncPKE.PK})$$

$$MSK = (\boxed{FE.MSK} ,$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\boxed{FE.MPK} , \boxed{IncPKE.PK})$$

$$MSK = (\boxed{FE.MSK} , \boxed{IncPKE.SK})$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ \boxed{FE.MPK}\ ,\ \boxed{IncPKE.PK}\ )$$

$$MSK = (\ \boxed{FE.MSK}\ ,\ \boxed{IncPKE.SK}\ )$$

$$Enc(m) \rightarrow$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \to MPK = (\boxed{FE.MPK} , \boxed{IncPKE.PK})$$

$$MSK = (\boxed{FE.MSK} , \boxed{IncPKE.SK})$$

$$Enc(m) \to \qquad \boxed{IncPKE.Enc(\mathbf{0})}$$

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = ($ $\boxed{FE.MPK}$, $\boxed{IncPKE.PK}$ $)$

$MSK = ($ $\boxed{FE.MSK}$, $\boxed{IncPKE.SK}$ $)$

$Enc(m) \rightarrow FE.Enc($ $\boxed{IncPKE.Enc(\mathbf{0})}$

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = (\; FE.MPK \; , \; IncPKE.PK \;)$

$MSK = (\; FE.MSK \; , \; IncPKE.SK \;)$

$Enc(m) \rightarrow FE.Enc(\; m \; , \qquad IncPKE.Enc(\mathbf{0})$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$$

$$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$$

$$Enc(m) \rightarrow FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ \boxed{FE.MPK}\ ,\ \boxed{IncPKE.PK}\ )$$

$$MSK = (\ \boxed{FE.MSK}\ ,\ \boxed{IncPKE.SK}\ )$$

$$Enc(m) \rightarrow FE.Enc(\ \boxed{m}\ ,\ \boxed{0}\ ,\ \boxed{IncPKE.Enc(\mathbf{0})}\ ,\ \boxed{\perp}\ )$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$$

$$MSK = (\boxed{FE.MSK}, \boxed{IncPKE.SK})$$

$$Enc(m) \rightarrow FE.Enc(\boxed{m}, \boxed{0}, \boxed{IncPKE.Enc(\mathbf{0})}, \boxed{\perp})$$

$$KeyGen(f) \rightarrow$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$$

$$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$$

$$Enc(m) \rightarrow FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})\ ,\ \perp\ )$$

$$KeyGen(f) \rightarrow FE.KeyGen(\ \hat{f}_{SKE.CT}\ )$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$$

$$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$$

$$Enc(m) \rightarrow FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})\ ,\ \perp\ )$$

$$KeyGen(f) \rightarrow FE.KeyGen(\ \hat{f}_{SKE.CT}\ ) \longrightarrow SKE.Enc(\mathbf{0})$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ \boxed{FE.MPK}\ ,\ \boxed{IncPKE.PK}\ )$$

$$MSK = (\ \boxed{FE.MSK}\ ,\ \boxed{IncPKE.SK}\ )$$

$$Enc(m) \rightarrow FE.Enc(\ \boxed{m}\ ,\ \boxed{0}\ ,\ \boxed{IncPKE.Enc(\mathbf{0})}\ ,\ \boxed{\perp}\ )$$

$$KeyGen(f) \rightarrow FE.KeyGen(\ \boxed{\hat{f}_{SKE.CT}}\ ) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$$

$$\hat{f}_{SKE.CT}($$

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = (\boxed{FE.MPK} , \boxed{IncPKE.PK})$

$MSK = (\boxed{FE.MSK} , \boxed{IncPKE.SK})$

$Enc(m) \rightarrow FE.Enc(\boxed{m} , \boxed{0} , \boxed{IncPKE.Enc(\mathbf{0})} , \boxed{\perp})$

$KeyGen(f) \rightarrow FE.KeyGen(\boxed{\hat{f}_{SKE.CT}}) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$

$\hat{f}_{SKE.CT}(\boxed{m} ,$

Rate-1/2 Incomp FE with Large Keys

$$Setup \to MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$$

$$MSK = (\boxed{FE.MSK}, \boxed{IncPKE.SK})$$

$$Enc(m) \to FE.Enc(\boxed{m}, \boxed{0}, \boxed{IncPKE.Enc(\mathbf{0})}, \boxed{\perp})$$

$$KeyGen(f) \to FE.KeyGen(\boxed{\hat{f}_{SKE.CT}}) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$$

$$\hat{f}_{SKE.CT}(\boxed{m}, \boxed{b},$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \to MPK = (\ \boxed{FE.MPK}\ ,\ \boxed{IncPKE.PK}\ )$$

$$MSK = (\ \boxed{FE.MSK}\ ,\ \boxed{IncPKE.SK}\ )$$

$$Enc(m) \to FE.Enc(\ \boxed{m}\ ,\ \boxed{0}\ ,\ \boxed{IncPKE.Enc(\mathbf{0})}\ ,\ \boxed{\perp}\ )$$

$$KeyGen(f) \to FE.KeyGen(\ \boxed{\hat{f}_{SKE.CT}}\ ) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$$

$$\hat{f}_{SKE.CT}(\ \boxed{m}\ ,\ \boxed{b}\ ,\ \boxed{CT}\ ,$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$$

$$MSK = (\boxed{FE.MSK}, \boxed{IncPKE.SK})$$

$$Enc(m) \rightarrow FE.Enc(\boxed{m}, \boxed{0}, \boxed{IncPKE.Enc(\mathbf{0})}, \boxed{\perp})$$

$$KeyGen(f) \rightarrow FE.KeyGen(\boxed{\hat{f}_{SKE.CT}}) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$$

$$\hat{f}_{SKE.CT}(\boxed{m}, \boxed{b}, \boxed{CT}, \boxed{SKE.SK})$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$$

$$MSK = (\boxed{FE.MSK}, \boxed{IncPKE.SK})$$

$$Enc(m) \rightarrow FE.Enc(\boxed{m}, \boxed{0}, \boxed{IncPKE.Enc(\mathbf{0})}, \boxed{\perp})$$

$$KeyGen(f) \rightarrow FE.KeyGen(\boxed{\hat{f}_{SKE.CT}}) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$$

$$\hat{f}_{SKE.CT}(\boxed{m}, \boxed{b}, \boxed{CT}, \boxed{SKE.SK})$$

$$= \begin{cases} 1) \\ 2) \\ 3) \end{cases}$$

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$

$MSK = (\boxed{FE.MSK}, \boxed{IncPKE.SK})$

$Enc(m) \rightarrow FE.Enc(\boxed{m}, \boxed{0}, \boxed{IncPKE.Enc(\mathbf{0})}, \boxed{\perp})$

$KeyGen(f) \rightarrow FE.KeyGen(\boxed{\hat{f}_{SKE.CT}})$ $\boxed{SKE.Enc(\mathbf{0})}$

$\hat{f}_{SKE.CT}(\boxed{m}, \boxed{b}, \boxed{CT}, \boxed{SKE.SK})$

$$= \begin{cases} 1) & \boxed{f(m)} \\ 2) & \\ 3) & \end{cases}$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \to MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$$

$$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$$

$$Enc(m) \to FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})\ ,\ \perp\ )$$

$$KeyGen(f) \to FE.KeyGen(\ \hat{f}_{SKE.CT}\ ) \longrightarrow SKE.Enc(\mathbf{0})$$

$$\hat{f}_{SKE.CT}(\ m\ ,\ b\ ,\ CT\ ,\ SKE.SK\ )$$

$$= \begin{cases} 1) & f(m) \qquad \text{If } b = 0 \\ 2) & \\ 3) & \end{cases}$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\, FE.MPK \,,\, IncPKE.PK \,)$$

$$MSK = (\, FE.MSK \,,\, IncPKE.SK \,)$$

$$Enc(m) \rightarrow FE.Enc(\, m \,,\, 0 \,,\, IncPKE.Enc(\mathbf{0}) \,,\, \perp \,)$$

$$KeyGen(f) \rightarrow FE.KeyGen(\, \hat{f}_{SKE.CT} \,)$$

$$SKE.Enc(\mathbf{0})$$

$$\hat{f}_{SKE.CT}(\, m \,,\, b \,,\, CT \,,\, SKE.SK \,)$$

$$= \begin{cases} 1) & f(m) \\ 2) & \\ 3) & \end{cases}$$

If $b = 0$

Real Mode

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$

$MSK = (\boxed{FE.MSK}, \boxed{IncPKE.SK})$

$Enc(m) \rightarrow FE.Enc(\boxed{m}, \boxed{0}, \boxed{IncPKE.Enc(\mathbf{0})}, \boxed{\perp})$

$KeyGen(f) \rightarrow FE.KeyGen(\boxed{\hat{f}_{SKE.CT}}) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$

$\hat{f}_{SKE.CT}(\boxed{m}, \boxed{b}, \boxed{CT}, \boxed{SKE.SK})$

$$= \begin{cases} 1) & \boxed{f(m)} \\ 2) & \boxed{f(m)} \\ 3) & \end{cases}$$

If $b = 0$ $\longrightarrow$ Real Mode

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$$

$$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$$

$$Enc(m) \rightarrow FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})\ ,\ \perp\ )$$

$$KeyGen(f) \rightarrow FE.KeyGen(\ \hat{f}_{SKE.CT}\ )$$

$$SKE.Enc(\mathbf{0})$$

$$\hat{f}_{SKE.CT}(\ m\ ,\ b\ ,\ CT\ ,\ SKE.SK\ )$$

$$= \begin{cases} 1)\ f(m) & \text{If } b = 0 \\ 2)\ f(m) & \text{If } \hat{b} = 0 \\ 3) & \end{cases}$$

Real Mode

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = (\boxed{FE.MPK}, \boxed{IncPKE.PK})$

$MSK = (\boxed{FE.MSK}, \boxed{IncPKE.SK})$

$Enc(m) \rightarrow FE.Enc(\boxed{m}, \boxed{0}, \boxed{IncPKE.Enc(\mathbf{0})}, \boxed{\perp})$

$KeyGen(f) \rightarrow FE.KeyGen(\boxed{\hat{f}_{SKE.CT}}) \longrightarrow \boxed{SKE.Enc(\mathbf{0})}$

$\hat{f}_{SKE.CT}(\boxed{m}, \boxed{b}, \boxed{CT}, \boxed{SKE.SK})$

$$= \begin{cases} 1) & \boxed{f(m)} & \text{If } b = 0 \\ 2) & \boxed{f(m)} & \text{If } \hat{b} = 0 \\ 3) & & \end{cases}$$

Real Mode

$(\hat{b}, IncPKE.SK) = SKE.Dec(SKE.SK, SKE.CT)$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$$

$$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$$

$$Enc(m) \rightarrow FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})\ ,\ \perp\ )$$

$$KeyGen(f) \rightarrow FE.KeyGen(\ \hat{f}_{SKE.CT}\ )$$

$$SKE.Enc(\mathbf{0})$$

$$\hat{f}_{SKE.CT}(\ m\ ,\ b\ ,\ CT\ ,\ SKE.SK\ )$$

$$= \begin{cases} 1)\ f(m) \\ 2)\ f(m) \\ 3)\ f(IncPKE.Dec(IncPKE.SK, CT)) \end{cases}$$

If $b = 0$

If $\hat{b} = 0$

Real Mode

$$(\hat{b}, IncPKE.SK) = SKE.Dec(SKE.SK, SKE.CT)$$

Rate-1/2 Incomp FE with Large Keys

$$Setup \rightarrow MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$$

$$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$$

$$Enc(m) \rightarrow FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})\ ,\ \perp\ )$$

$$KeyGen(f) \rightarrow FE.KeyGen(\ \hat{f}_{SKE.CT}\ ) \longrightarrow SKE.Enc(\mathbf{0})$$

$$\hat{f}_{SKE.CT}(\ m\ ,\ b\ ,\ CT\ ,\ SKE.SK\ )$$

$$= \begin{cases} 1)\ f(m) & \text{If } b = 0 \\ 2)\ f(m) & \text{If } \hat{b} = 0 \\ 3)\ f(IncPKE.Dec(IncPKE.SK, CT)) & \end{cases}$$

Real Mode

$$(\hat{b}, IncPKE.SK) = SKE.Dec(SKE.SK, SKE.CT)$$

Distinguishing or not

Rate-1/2 Incomp FE with Large Keys

$Setup \rightarrow MPK = ($ $FE.MPK$, $IncPKE.PK$ $)$

$MSK = ($ $FE.MSK$, $IncPKE.SK$ $)$

$|ct| = |m| + 1 + |m| + poly(\lambda)$

$Enc(m) \rightarrow FE.Enc($ m , 0 , $IncPKE.Enc(\mathbf{0})$, $\perp$ $)$

$KeyGen(f) \rightarrow FE.KeyGen($ $\hat{f}_{SKE.CT}$ $)$ $\rightarrow$ $SKE.Enc(\mathbf{0})$

$\hat{f}_{SKE.CT}($ m , b , CT , $SKE.SK$ $)$

$$= \begin{cases} 1) & f(m) \\ 2) & f(m) \\ 3) & f(IncPKE.Dec(IncPKE.SK, CT)) \end{cases}$$

If $b = 0$ $\rightarrow$ Real Mode

If $\hat{b} = 0$ $\rightarrow$ Distinguishing or not

$(\hat{b}, IncPKE.SK) = SKE.Dec(SKE.SK, SKE.CT)$

Rate-1/2 Incomp FE with Large Keys

$Setup \to MPK = (\ FE.MPK\ ,\ IncPKE.PK\ )$

$MSK = (\ FE.MSK\ ,\ IncPKE.SK\ )$

$|ct| = |m| + 1 + |m| + poly(\lambda)$

$Enc(m) \to FE.Enc(\ m\ ,\ 0\ ,\ IncPKE.Enc(\mathbf{0})\ ,\ \perp\ )$

$KeyGen(f) \to FE.KeyGen(\ \hat{f}_{SKE.CT}\ )$

$SKE.Enc(\mathbf{0})$

$\hat{f}_{SKE.CT}(\ m\ ,\ b\ ,\ CT\ ,\ SKE.SK\ )$

$$= \begin{cases} 1)\ f(m) \\ 2)\ f(m) \\ 3)\ f(IncPKE.Dec(IncPKE.SK, CT)) \end{cases}$$

If $b = 0$

If $\hat{b} = 0$

Real Mode

$(\hat{b}, IncPKE.SK) = SKE.Dec(SKE.SK, SKE.CT)$

Distinguishing or not

Extending to better parameters

Extending to better parameters

- Using rate-1/2 incompressible PKE and another layer of SKE encryption, secret keys can be made short.

Extending to better parameters

- Using rate-1/2 incompressible PKE and another layer of SKE encryption, secret keys can be made short.

- Replacing incompressible PKE component with extractors gives rate-1 but large keys.

Extending to better parameters

- Using rate-1/2 incompressible PKE and another layer of SKE encryption, secret keys can be made short.
- Replacing incompressible PKE component with extractors gives rate-1 but large keys.
- Small keys can be achieved if the functions are Boolean.

Incompressible ABE

Incompressible ABE

- Assuming the (sub-exp) hardness of LWE problem, there exists incompressible ABE for predicate classes with circuit of depth D with
  $|mpk| = poly(\lambda), \quad |sk| = poly(\lambda) \cdot D,$
  $|ct| = poly(\lambda) \cdot (D + \log(|m|)) + m + S$

Incompressible ABE

- Assuming the (sub-exp) hardness of LWE problem, there exists incompressible ABE for predicate classes with circuit of depth D with
  $|mpk| = poly(\lambda), \quad |sk| = poly(\lambda) \cdot D,$
  $|ct| = poly(\lambda) \cdot (D + \log(|m|)) + m + S$

  - Uses two-level deferred encryption and this technique could find more applications in other contexts. Refer to the paper for more details.

Incompressible ABE

- Assuming the (sub-exp) hardness of LWE problem, there exists incompressible ABE for predicate classes with circuit of depth D with
  $|mpk| = poly(\lambda), \quad |sk| = poly(\lambda) \cdot D,$
  $|ct| = poly(\lambda) \cdot (D + \log(|m|)) + m + S$

  - Uses two-level deferred encryption and this technique could find more applications in other contexts. Refer to the paper for more details.

- From minimal assumption of ABE by extending ideas from Guan-Wichs-Zhandry'22.

Future Directions

Future Directions

1. Rate-1 Semi-Strong Incompressible FE with adaptive security.

Future Directions

1. Rate-1 Semi-Strong Incompressible FE with adaptive security.
2. Strong Incompressible FE with selective/adaptive security.

Future Directions

1. Rate-1 Semi-Strong Incompressible FE with adaptive security.
2. Strong Incompressible FE with selective/adaptive security.
3. Strong Incompressible ABE/IBE from standard assumptions.

Future Directions

1. Rate-1 Semi-Strong Incompressible FE with adaptive security.
2. Strong Incompressible FE with selective/adaptive security.
3. Strong Incompressible ABE/IBE from standard assumptions.
4. Using incompressible cryptography to build other primitives.

Thank You

https://eprint.iacr.org/2024/798.pdf