Karlsruhe Institute of Technology

KASTEL

A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels

Wasilij Beskorovajnov, **Roland Gröll**, Jörn Müller-Quade, Astrid Ottenhues, and **Rebecca Schwerdt** | PKC 2022

A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels

Introduction

A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels

All emojis designed by OpenMoji – the open-source emoji and icon project. License: CC BY-SA 4.0

Introduction

A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels

All emojis designed by OpenMoji – the open-source emoji and icon project. License: CC BY-SA 4.0

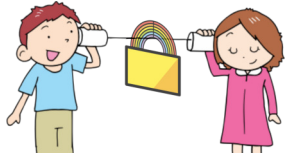
Introduction

A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels

All emojis designed by OpenMoji – the open-source emoji and icon project. License: CC BY-SA 4.0

Introduction

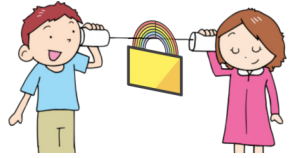
A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels



All emojis designed by OpenMoji – the open-source emoji and icon project. License: CC BY-SA 4.0

Introduction

A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels



All emojis designed by OpenMoji – the open-source emoji and icon project. License: CC BY-SA 4.0

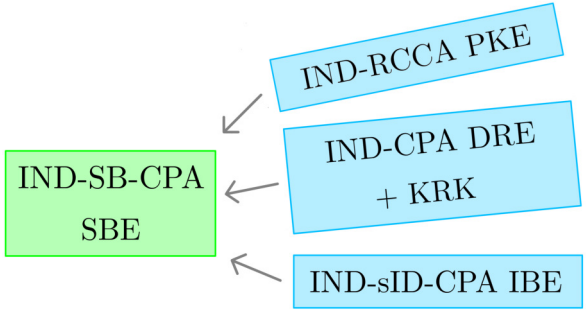
Overview

Overview

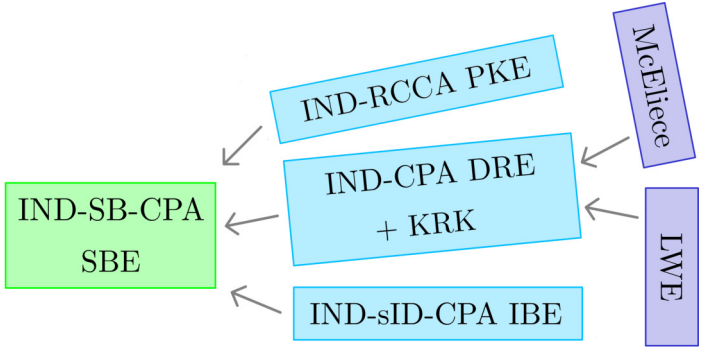
IND-SB-CPA

SBE

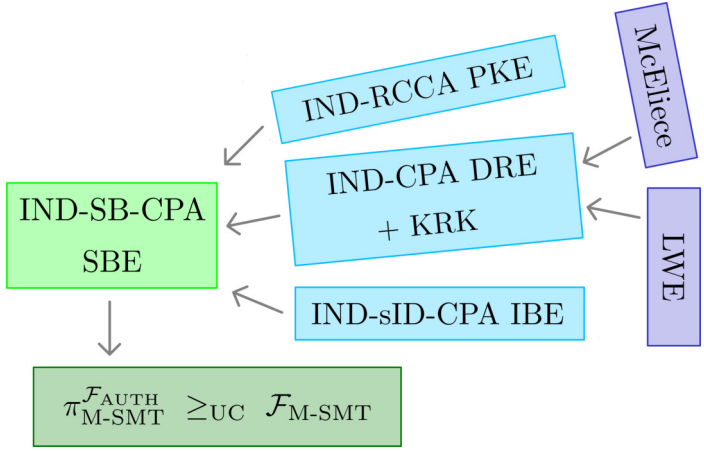
Overview



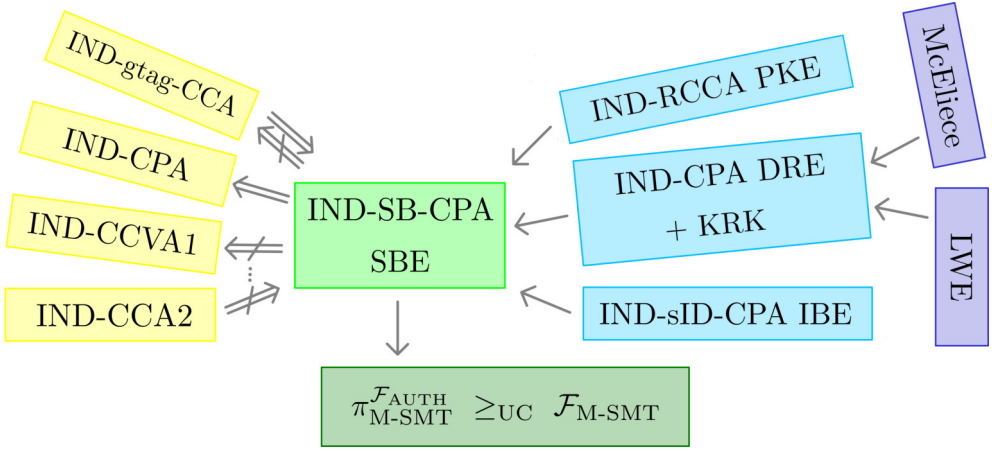
Overview


IND-RCCA PKE
McEliece
IND-CPA DRE
+ KRK
IND-SB-CPA
SBE
LWE
IND-sID-CPA IBE

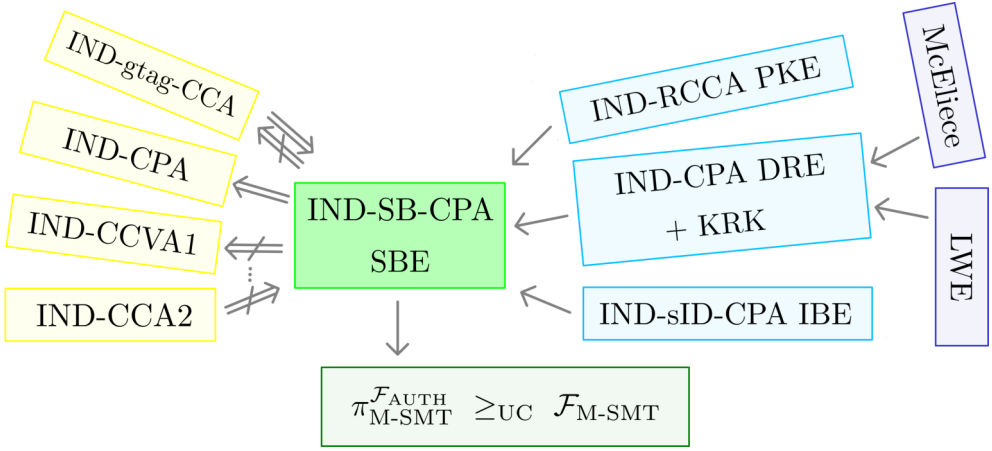
Overview


IND-RCCA PKE
McEliece
IND-CPA DRE
+ KRK
IND-SB-CPA
SBE
LWE
IND-sID-CPA IBE
$\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$

Overview


IND-gtag-CCA
IND-CPA
IND-CCVA1
IND-CCA2
IND-SB-CPA
SBE
IND-RCCA PKE
IND-CPA DRE
+ KRK
IND-sID-CPA IBE
McEliece
LWE
$\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$

SBE and IND-SB-CPA



Classic Public-key Encryption

$$\begin{aligned}
\mathsf{gen}: \quad & 1^\lambda \mapsto (sk, pk) && \text{(Key Generation)}\\
\mathsf{enc}: \quad & (pk, m) \mapsto c && \text{(Encryption)}\\
\mathsf{dec}: \quad & (sk, c) \mapsto m. && \text{(Decryption)}
\end{aligned}$$

$$m = \mathsf{dec}(sk, \mathsf{enc}(pk, m)) \qquad \text{(Correctness)}$$

Tag-based Encryption (TBE)

$$\begin{aligned}
\mathtt{gen}: \quad & 1^\lambda \mapsto (sk, pk) && \text{(Key Generation)}\\
\mathtt{enc}: \quad & (pk, \boldsymbol{t}, m) \mapsto c && \text{(Encryption)}\\
\mathtt{dec}: \quad & (sk, \boldsymbol{t}, c) \mapsto m. && \text{(Decryption)}
\end{aligned}$$

$$m = \mathtt{dec}(sk, \boldsymbol{t}, \mathtt{enc}(pk, \boldsymbol{t}, m)) \qquad \text{(Correctness)}$$

Sender-binding Encryption (SBE)

$$\mathtt{gen}: \quad 1^\lambda \mapsto (sk, pk) \qquad \text{(Key Generation)}$$

$$\mathtt{enc}: \quad (pk, \boldsymbol{S}, m) \mapsto c \qquad \text{(Encryption)}$$

$$\mathtt{dec}: \quad (sk, \boldsymbol{S}, c) \mapsto m. \qquad \text{(Decryption)}$$

$$m = \mathtt{dec}(sk, \boldsymbol{S}, \mathtt{enc}(pk, \boldsymbol{S}, m)) \qquad \text{(Correctness)}$$

IND-SB-CPA Security

$\mathcal{C}_{\text{hallenger}}$	$\mathcal{A}_{\text{dversary}}$	$\mathcal{O}_{\text{racle}}$

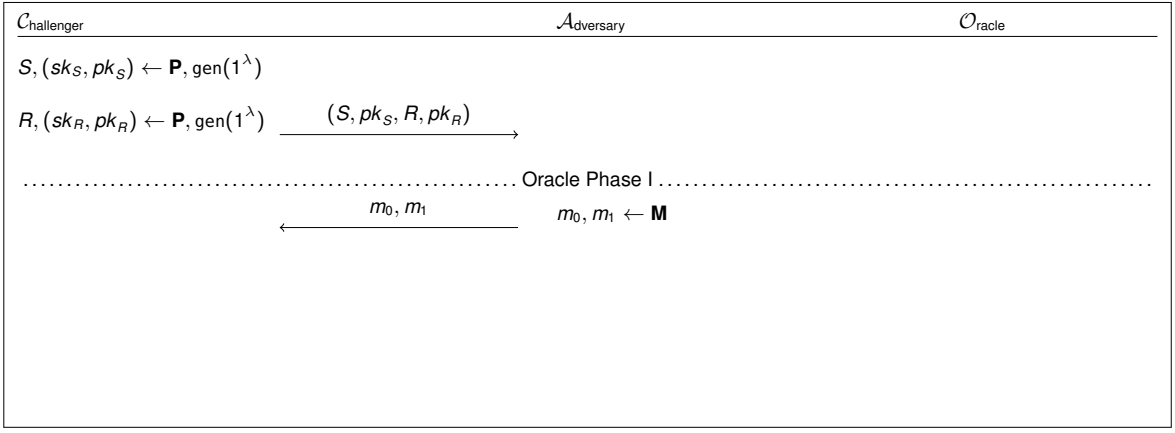
IND-SB-CPA Security

$\mathcal{C}_{\text{hallenger}}$	$\mathcal{A}_{\text{dversary}}$	$\mathcal{O}_{\text{racle}}$
$S, (sk_S, pk_S) \leftarrow \mathbf{P}, \text{gen}(1^\lambda)$		
$R, (sk_R, pk_R) \leftarrow \mathbf{P}, \text{gen}(1^\lambda)$	$\xrightarrow{(S, pk_S, R, pk_R)}$	

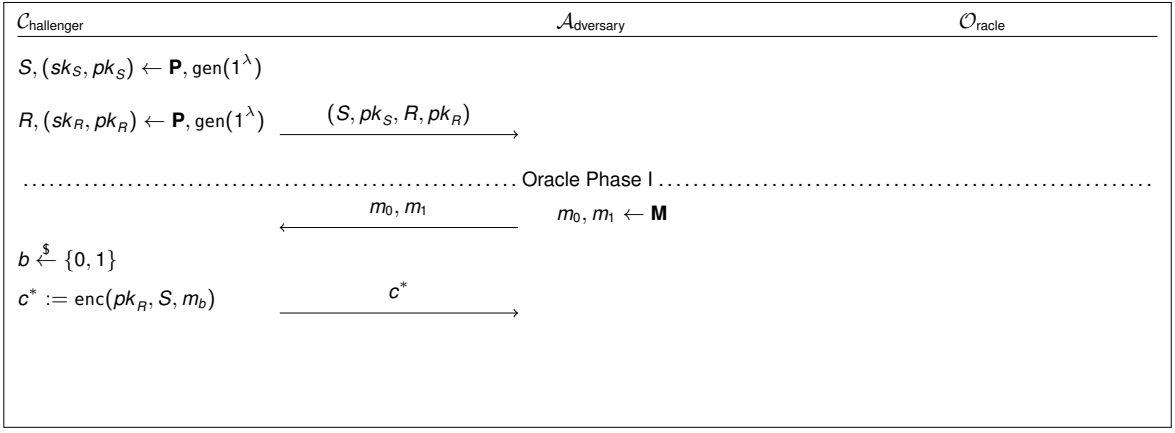
IND-SB-CPA Security

$\mathcal{C}_{\text{hallenger}}$		$\mathcal{A}_{\text{dversary}}$	$\mathcal{O}_{\text{racle}}$
$S, (sk_S, pk_S) \leftarrow \mathbf{P}, \text{gen}(1^\lambda)$			
$R, (sk_R, pk_R) \leftarrow \mathbf{P}, \text{gen}(1^\lambda)$	$\xrightarrow{(S, pk_S, R, pk_R)}$		
..... Oracle Phase I			

IND-SB-CPA Security



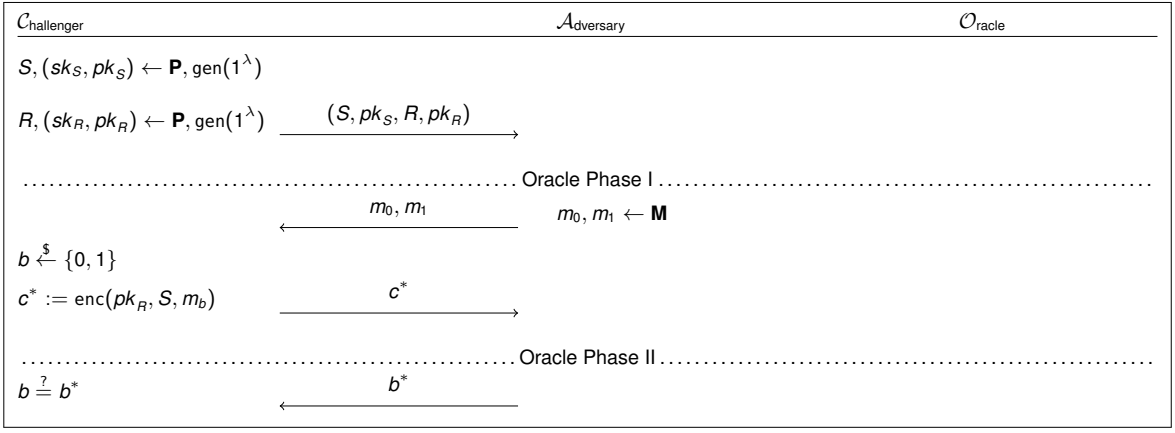
IND-SB-CPA Security



IND-SB-CPA Security

$\mathcal{C}_{\text{challenger}}$		$\mathcal{A}_{\text{dversary}}$	$\mathcal{O}_{\text{racle}}$
$S, (sk_S, pk_S) \leftarrow \mathbf{P}, \text{gen}(1^\lambda)$			
$R, (sk_R, pk_R) \leftarrow \mathbf{P}, \text{gen}(1^\lambda)$	$\xrightarrow{(S, pk_S, R, pk_R)}$		
.....		Oracle Phase I	
	$\xleftarrow{m_0, m_1}$	$m_0, m_1 \leftarrow \mathbf{M}$	
$b \xleftarrow{\$} \{0,1\}$			
$c^* := \text{enc}(pk_R, S, m_b)$	$\xrightarrow{c^*}$		
.....		Oracle Phase II	

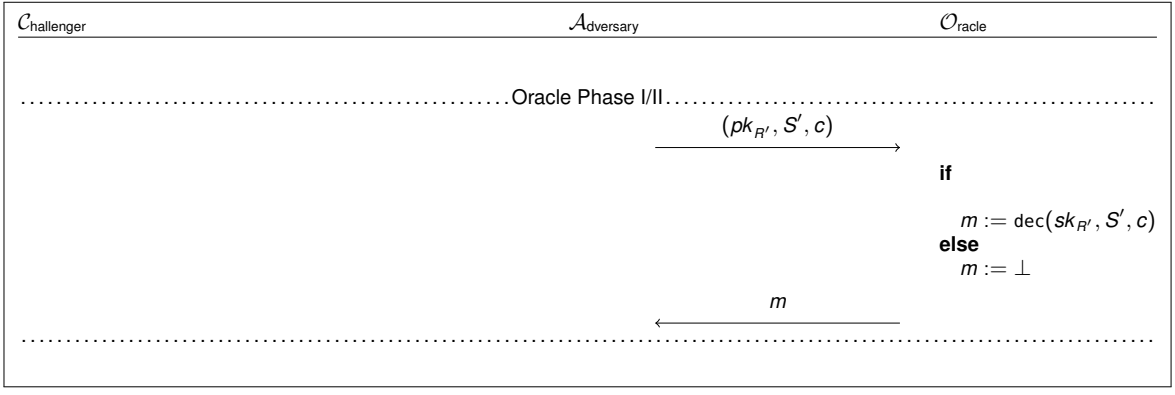
IND-SB-CPA Security



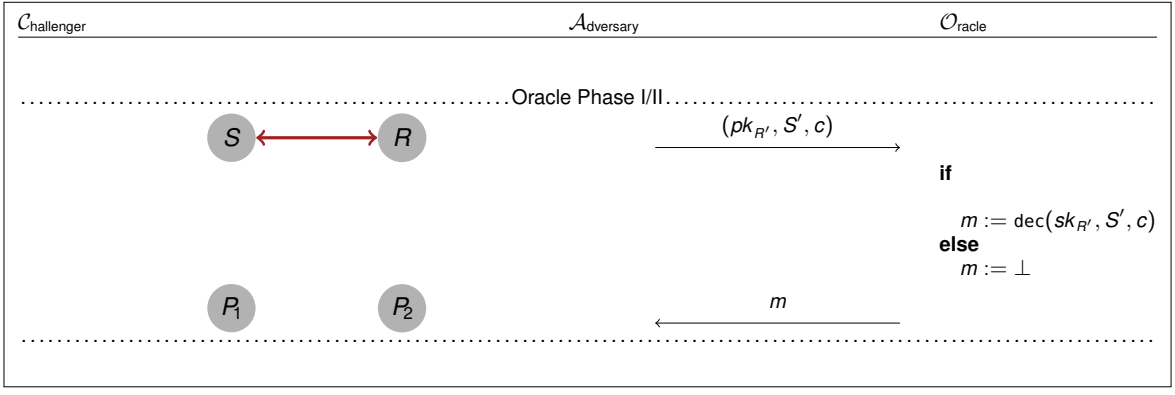
IND-SB-CPA Security: Oracle Phase I/II

$\mathcal{C}$hallenger	$\mathcal{A}$dversary	$\mathcal{O}$racle
	Oracle Phase I/II	

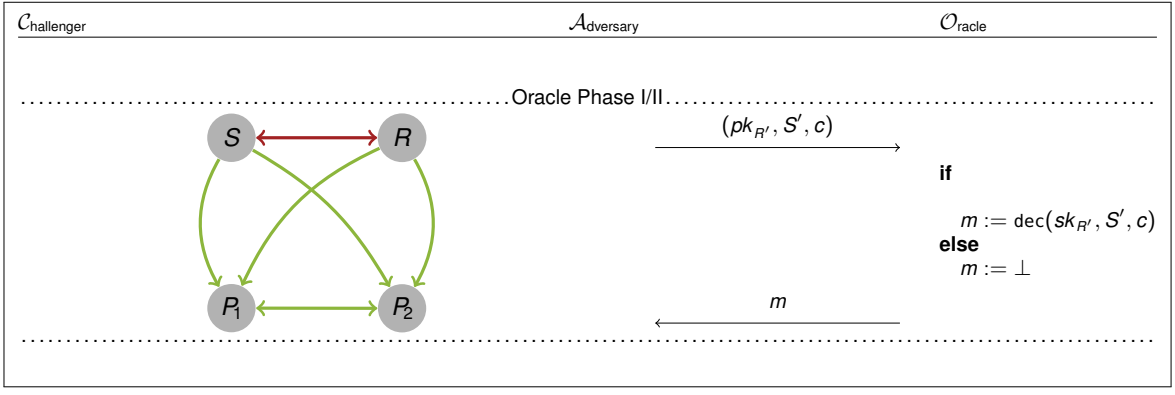
IND-SB-CPA Security: Oracle Phase I/II



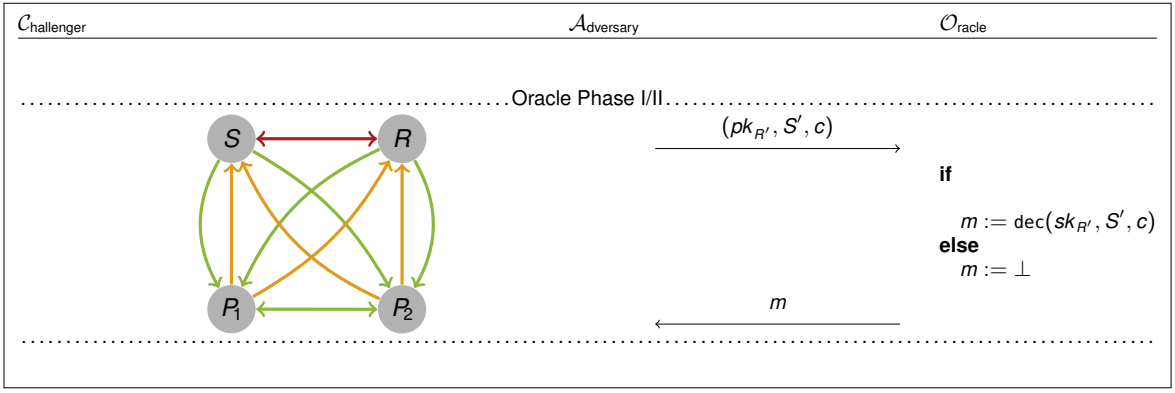
IND-SB-CPA Security: Oracle Phase I/II



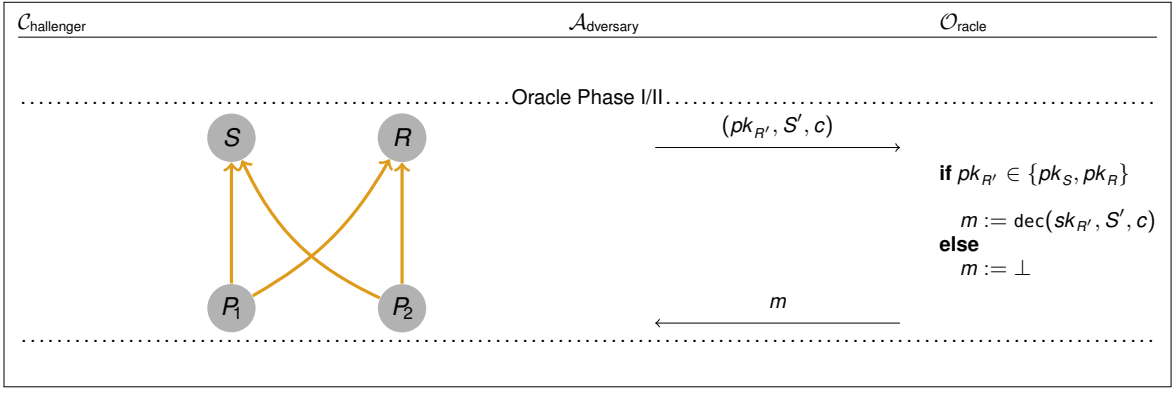
IND-SB-CPA Security: Oracle Phase I/II



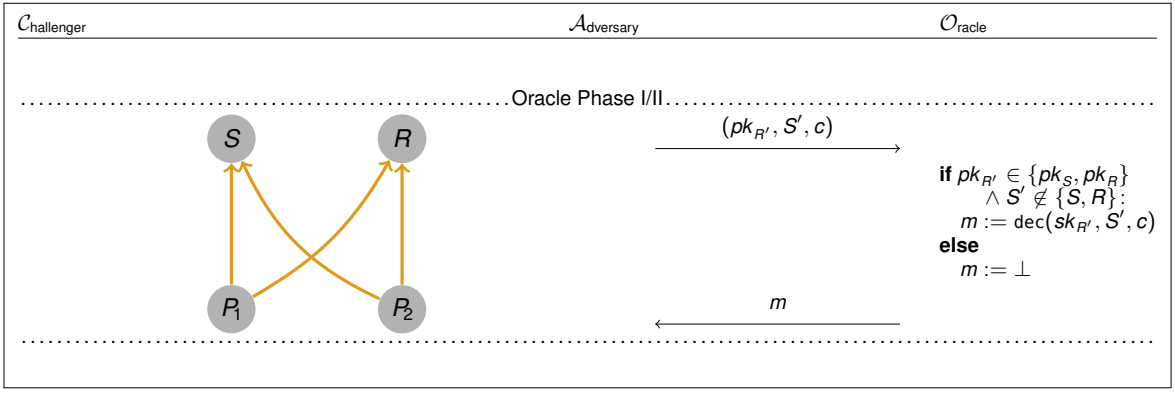
IND-SB-CPA Security: Oracle Phase I/II



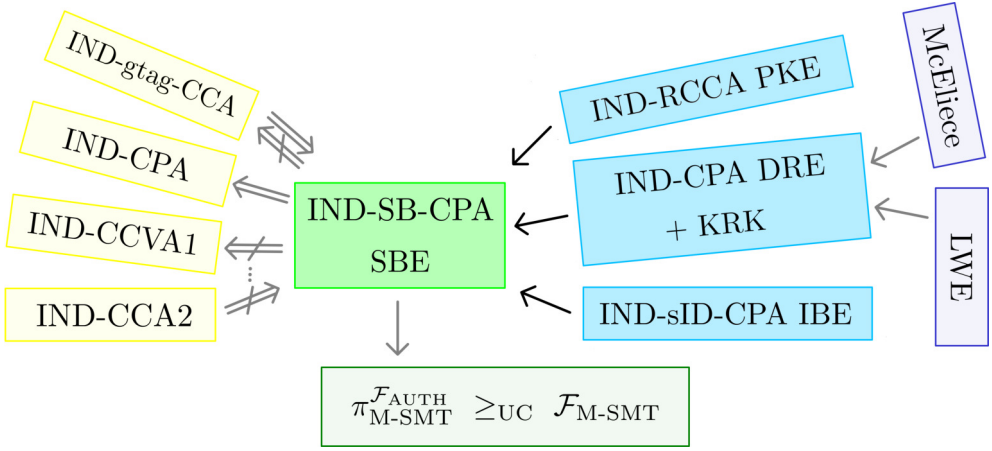
IND-SB-CPA Security: Oracle Phase I/II



IND-SB-CPA Security: Oracle Phase I/II



Generic Transformations



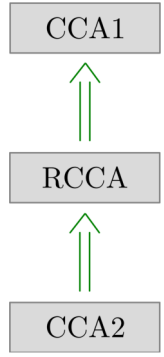
PKE $\rightsquigarrow$ SBE Transformation

$$(pk_R, S, m) \mapsto \mathsf{enc}(pk_R, m \| S) \qquad \text{(Construction)}$$

PKE $\rightsquigarrow$ SBE Transformation

$$(pk_R, S, m) \mapsto \mathsf{enc}(pk_R, m \| S)$$

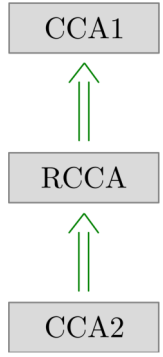
(Construction)



PKE $\rightsquigarrow$ SBE Transformation

$$(pk_R, S, m) \mapsto \mathrm{enc}(pk_R, m \| S) \qquad \text{(Construction)}$$

$$c \mapsto \begin{cases} \perp & , \mathrm{dec}(sk_R, c) \in \{m_0, m_1\} \\ \mathrm{dec}(sk_R, c) & , \text{otherwise.} \end{cases} \qquad \text{(Oracle Phase II)}$$



DRE Recap

DRE Recap

$$\begin{aligned}
\mathsf{gen}: &\quad 1^\lambda \mapsto (sk, pk) \\
\mathsf{enc}: &\quad (pk_1, pk_2, m) \mapsto c \\
\mathsf{dec}: &\quad (sk_i, pk_1, pk_2, c) \mapsto m
\end{aligned}$$

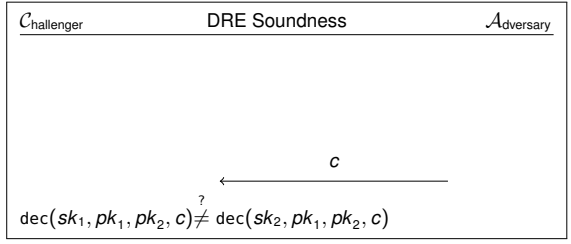
DRE Recap

$$\begin{aligned}
\mathsf{gen}: &\quad 1^\lambda \mapsto (sk, pk)\\
\mathsf{enc}: &\quad (pk_1, pk_2, m) \mapsto c\\
\mathsf{dec}: &\quad (sk_i, pk_1, pk_2, c) \mapsto m
\end{aligned}$$

$\mathcal{C}_{\text{hallenger}}$	DRE Soundness	$\mathcal{A}_{\text{dversary}}$

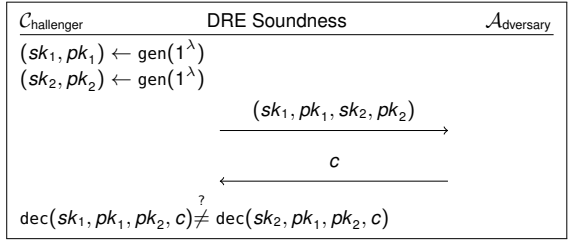
DRE Recap

$$\begin{aligned} \mathsf{gen}: \quad & 1^\lambda \mapsto (sk, pk) \\ \mathsf{enc}: \quad & (pk_1, pk_2, m) \mapsto c \\ \mathsf{dec}: \quad & (sk_i, pk_1, pk_2, c) \mapsto m \end{aligned}$$



DRE Recap

$$\begin{aligned} \mathsf{gen}: \quad & 1^\lambda \mapsto (sk, pk) \\ \mathsf{enc}: \quad & (pk_1, pk_2, m) \mapsto c \\ \mathsf{dec}: \quad & (sk_i, pk_1, pk_2, c) \mapsto m \end{aligned}$$



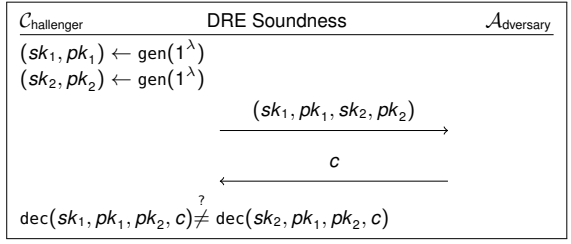
DRE Recap

$$\mathsf{gen}: \quad 1^\lambda \mapsto (sk, pk)$$

$$\mathsf{enc}: \quad (pk_1, pk_2, m) \mapsto c$$

$$\mathsf{dec}: \quad (sk_i, pk_1, pk_2, c) \mapsto m$$

$$\mathsf{f}_{\mathsf{Key}}: \quad (sk, pk) \mapsto \begin{cases} \text{true} \\ \text{false.} \end{cases}$$

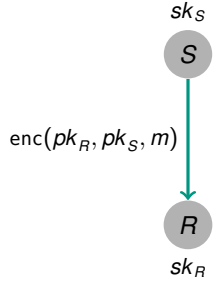


DRE $\rightsquigarrow$ SBE Transformation

DRE scheme $(\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$.

DRE $\rightsquigarrow$ SBE Transformation

DRE scheme $(\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$.



DRE $\rightsquigarrow$ SBE Transformation

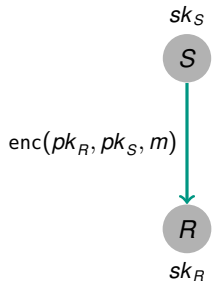
DRE scheme $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$.

SBE Construction Sketch

$\mathtt{Gen} \sim \mathtt{gen}$

$\mathtt{Enc}\colon \mathtt{enc}(pk_R, pk_S, m)$

$\mathtt{Dec}\colon \mathtt{dec}(sk_R, pk_R, pk_S, c)$



DRE $\rightsquigarrow$ SBE Transformation

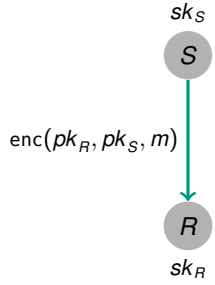
DRE scheme $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$.

SBE Construction Sketch

$\mathtt{Gen} \sim \mathtt{gen}$

$\mathtt{Enc}\colon \mathtt{enc}(pk_R, pk_S, m)$

$\mathtt{Dec}\colon \mathtt{dec}(sk_R, pk_R, pk_S, c)$



$\mathcal{F}_{\mathrm{KRK}}$

DRE $\rightsquigarrow$ SBE Transformation

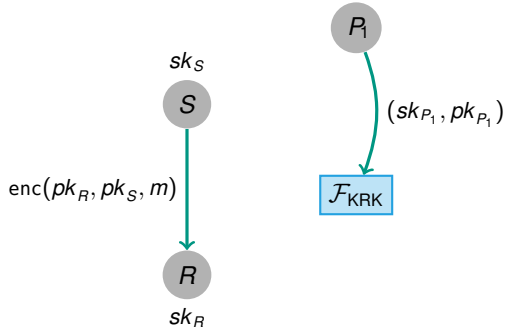
DRE scheme $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$.

SBE Construction Sketch

$\mathtt{Gen} \sim \mathtt{gen}$

$\mathtt{Enc}\colon \mathtt{enc}(pk_R, pk_S, m)$

$\mathtt{Dec}\colon \mathtt{dec}(sk_R, pk_R, pk_S, c)$



DRE $\rightsquigarrow$ SBE Transformation

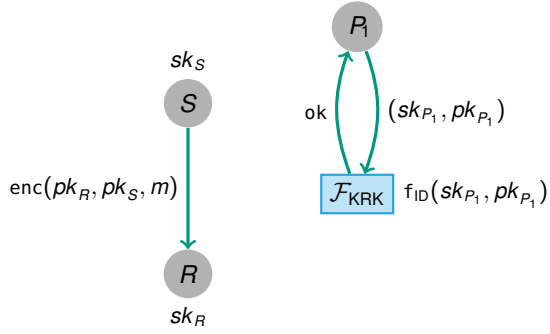
DRE scheme $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$.

SBE Construction Sketch

$\mathtt{Gen} \sim \mathtt{gen}$

$\mathtt{Enc}\colon \mathtt{enc}(pk_R, pk_S, m)$

$\mathtt{Dec}\colon \mathtt{dec}(sk_R, pk_R, pk_S, c)$



DRE $\rightsquigarrow$ SBE Transformation

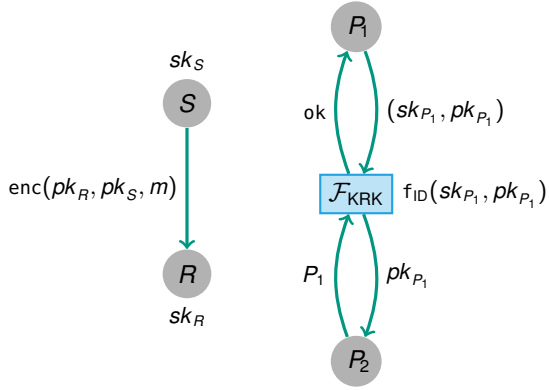
DRE scheme $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$.

SBE Construction Sketch

$\mathtt{Gen} \sim \mathtt{gen}$

$\mathtt{Enc}\colon \mathtt{enc}(pk_R, pk_S, m)$

$\mathtt{Dec}\colon \mathtt{dec}(sk_R, pk_R, pk_S, c)$

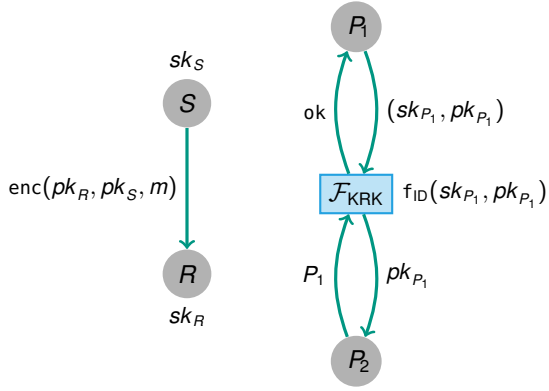


DRE $\rightsquigarrow$ SBE Transformation

DRE scheme $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$.

SBE Construction Sketch

$\mathtt{Gen} \sim \mathtt{gen}$	+ Register (sk, pk)
$\mathtt{Enc}\colon \mathtt{enc}(pk_R, pk_S, m)$	+ Retrieve pk_R
$\mathtt{Dec}\colon \mathtt{dec}(sk_R, pk_R, pk_S, c)$	+ Retrieve pk_S

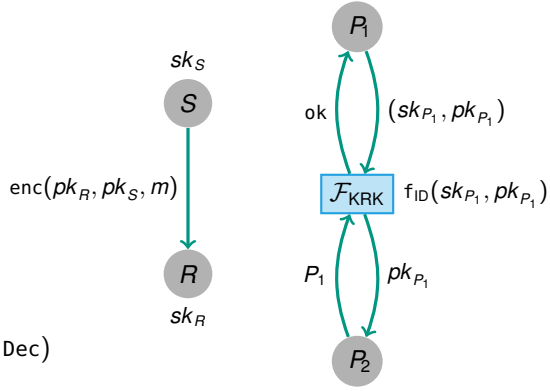


DRE $\rightsquigarrow$ SBE Transformation

DRE scheme $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$.

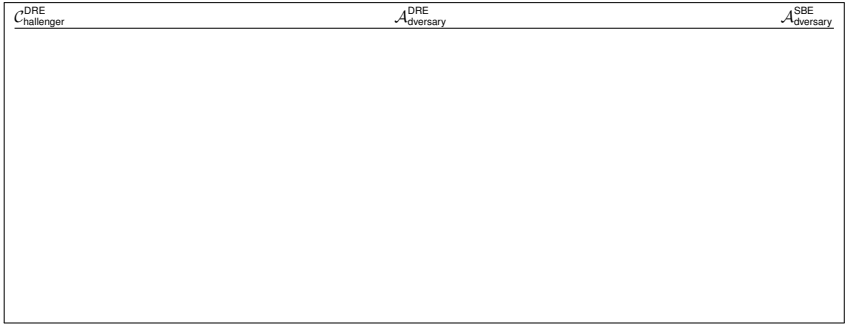
SBE Construction Sketch

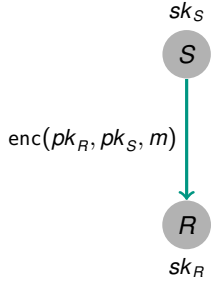
$\mathtt{Gen} \sim \mathtt{gen}$	+ Register (sk, pk)
$\mathtt{Enc}\colon \mathtt{enc}(pk_R, pk_S, m)$	+ Retrieve pk_R
$\mathtt{Dec}\colon \mathtt{dec}(sk_R, pk_R, pk_S, c)$	+ Retrieve pk_S



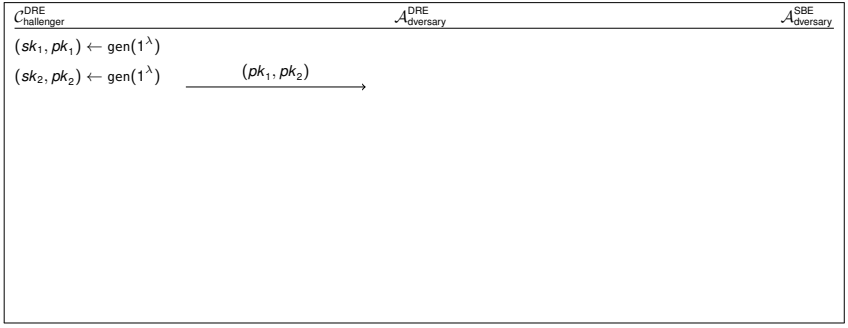
IND-CPA $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec}) + \mathcal{F}_{\mathrm{KRK}}^{\mathrm{f_{ID}}} \rightsquigarrow$ IND-SB-CPA $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$

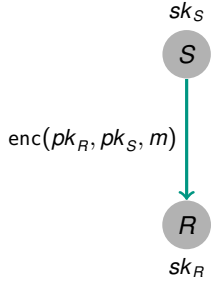
DRE $\rightsquigarrow$ SBE Transformation: Proofsketch



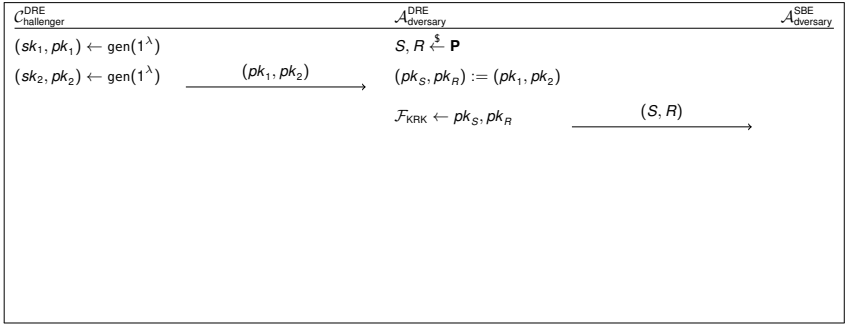


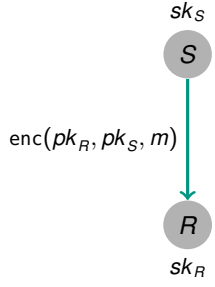
DRE $\rightsquigarrow$ SBE Transformation: Proofsketch



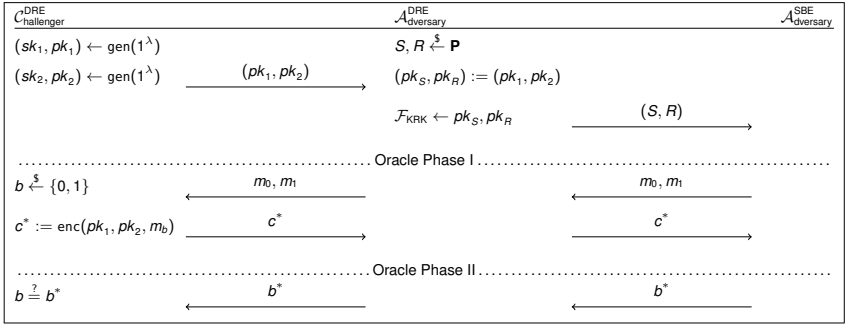


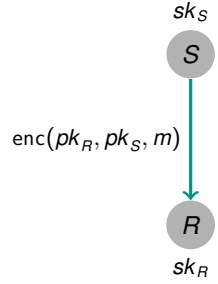
DRE $\rightsquigarrow$ SBE Transformation: Proofsketch



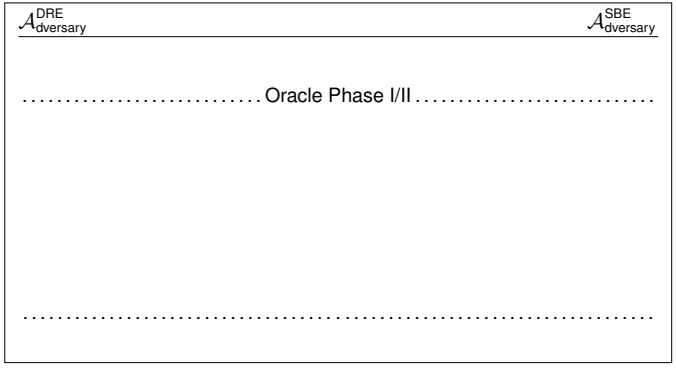


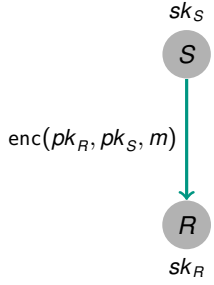
DRE $\rightsquigarrow$ SBE Transformation: Proofsketch



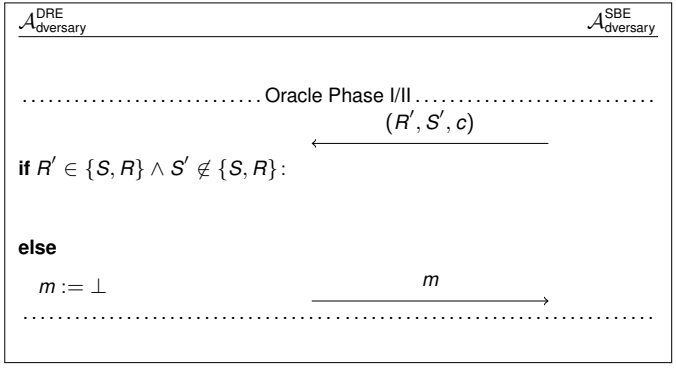


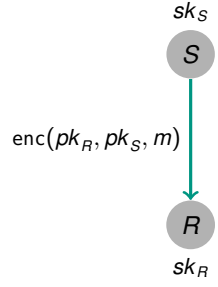
DRE $\rightsquigarrow$ SBE Transformation: Proofsketch



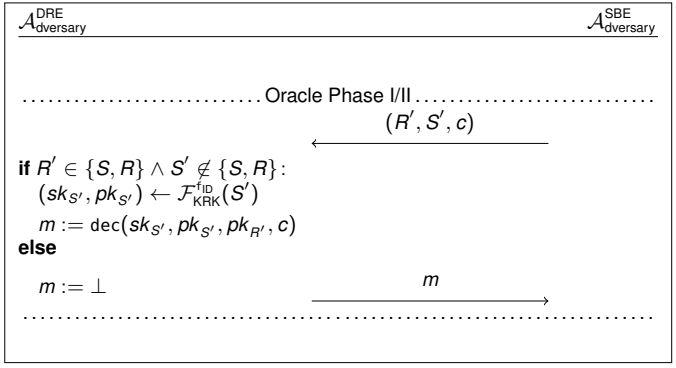


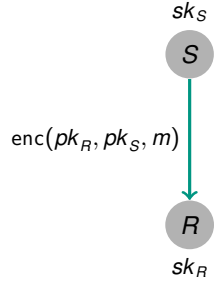
DRE $\rightsquigarrow$ SBE Transformation: Proofsketch



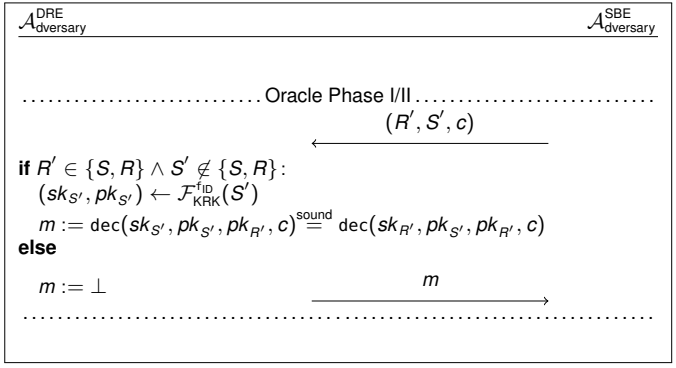


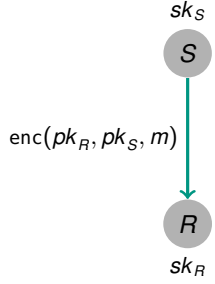
DRE $\rightsquigarrow$ SBE Transformation: Proofsketch



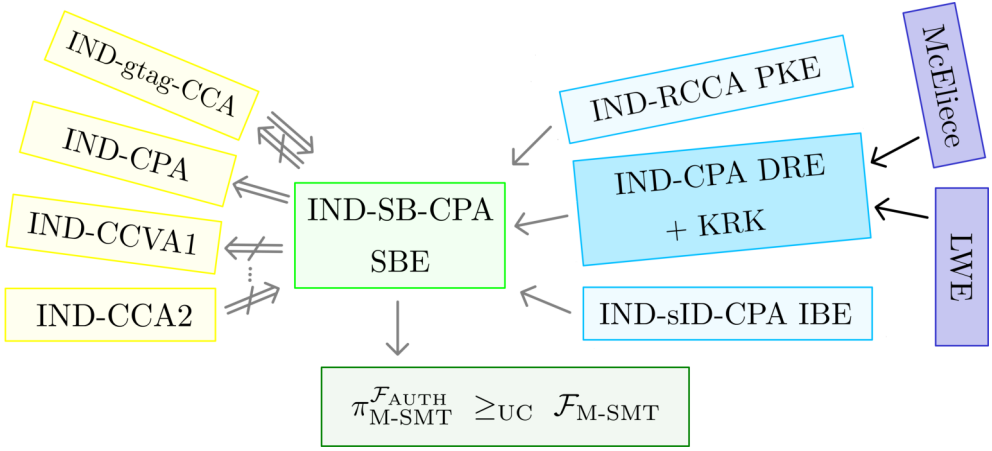


DRE $\rightsquigarrow$ SBE Transformation: Proofsketch





Efficient Constructions



Idea

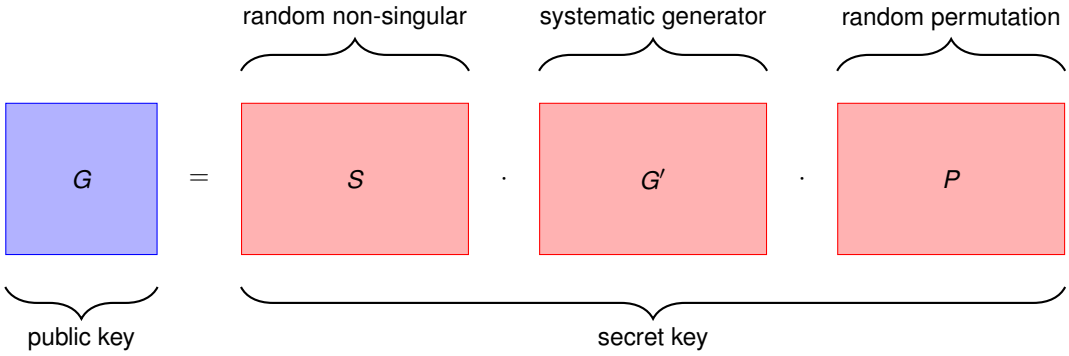
- Encode the message via a publicly known Goppa code generator
- McEliece encrypt a random vector to both sender and receiver
- Use this random vector to get an error vector to mask the encoded message
- Close to a contruction from Kiltz et al.

Linear Codes

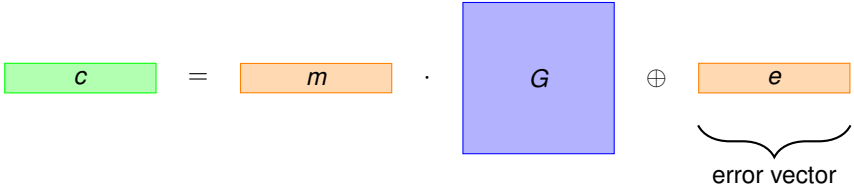
Linear Codes

- Hard to decode in general
- But: There are classes of codes that are easy to decode (given a generator in systematic form) – (irreducible, binary) Goppa Codes
- Random Goppa codes are indistinguishable from random linear codes
- Can be used to correct errors

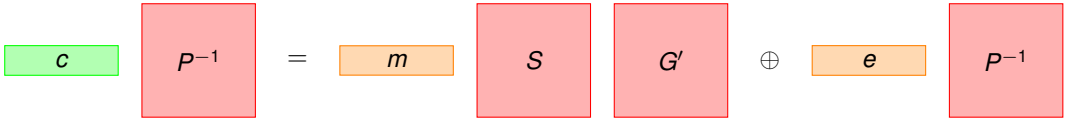
McEliece


random non-singular
systematic generator
random permutation
G
=
S
·
G′
·
P
public key
secret key

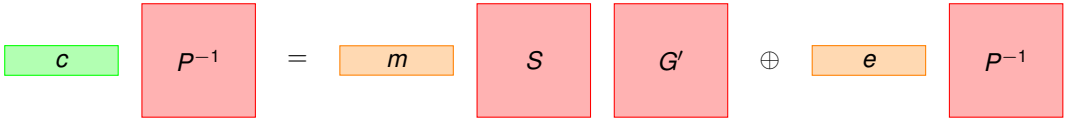
McEliece



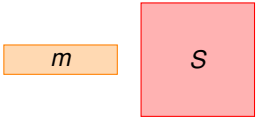
McEliece



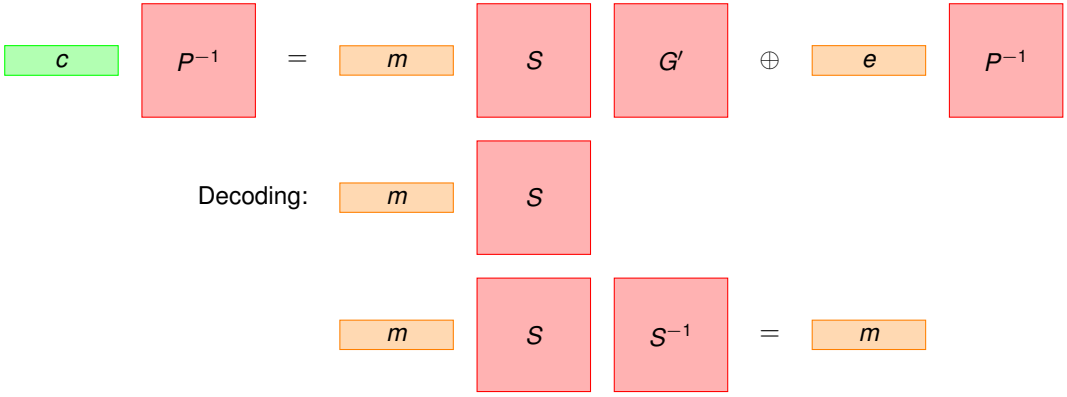
McEliece



Decoding:



McEliece



Preliminiaries

- $\mathcal{G}_{n,t}$ – family of irreducible binary Goppa-codes of length n, which can correct up to t errors with a code dimension l.
- Let $\theta = \frac{t}{n} + \epsilon$ be the Bernoulli parameter of the error for some $\epsilon > 0$.
- Let $G_2 \in \{0,1\}^{l \times n}$ be the publicly known generator matrix of a code from $\mathcal{G}_{n,t}$, where *Correct* is the according error-correcting algorithm.
- Let $M = \{0,1\}^l$ be the message space.

Key Generation

- Sample random matrix $C \in \{0,1\}^{l \times n}$
- Generate a McEliece Keypair: $G, (S, G', P)$

$\hookrightarrow$ Return $pk = (G, C, t)$ and $sk = (S, G', P)$

Encryption

- Parse pk_R as (G_R, C_R, t) and pk_S as (G_S, C_S, t)
- Sample $s \xleftarrow{\$} \{0,1\}^l$
- Use McEliece encryption to get $c_S \leftarrow enc_S(s)$ and $c_R \leftarrow enc_R(s)$
- $e \leftarrow \mathcal{B}_\theta$
- $c' = s \cdot C_S \oplus e \oplus m \cdot G_2$

$\hookrightarrow$ Return $c = (c_R, c_S, c')$.

Decryption

- Parse c as (c_R, c_S, c') and sk_R as (S_R, G'_R, P_R)
- Decrypt c_R using McEliece to get s
- Compute $c'_S = s \cdot G_S$
- Set the verification bit b as follows
  - Set $b = 1$ if the hamming weight of $c'_S \oplus c_S$ is smaller than t.
  - Set $b = 0$ otherwise.

$\hookrightarrow$ If $b = 0$ return $\perp$, otherwise:

- Compute $c' = s \cdot C_S$
- Correct the error from $m = \mathit{Correct}(c \oplus c')$, where $c \oplus c' = (m \cdot G_2 \oplus e)$.

$\hookrightarrow$ Return m.

Comparisons

Construction	Public Key	Ciphertext
Kiltz et al.	$(A, B_0, B_1, C) \in (\mathbb{Z}_2^{m \times n'})^3 \times \mathbb{Z}_2^{l' \times n'}$	$(c, c_0, c_1, c_2) \in (\mathbb{Z}_2^m)^3 \times \mathbb{Z}_2^{l'}$
Yu et al.	$(A, B_0, B_1, C) \in \mathbb{Z}_2^{\bar{n} \times \bar{n}} \times (\mathbb{Z}_2^{q \times \bar{n}})^2 \times \mathbb{Z}_2^{\bar{l} \times \bar{n}}$	$(c, c_0, c_1, c_2) \in (\mathbb{Z}_2^{\bar{n}}) \times (\mathbb{Z}_2^q)^2 \times \mathbb{Z}_2^{\bar{l}}$
This Work	$(G, C) \in \mathbb{Z}_2^{l \times n} \times \mathbb{Z}_2^{l \times n}$	$(c_R, c_S, c') \in (\mathbb{Z}_2^n)^3$

Comparisons

Construction	Public Key	Estimation Source
Kiltz et al.	77 megabyte	Is Public-Key Encryption Based on LPN Practical
Yu et al.	2.5 megabyte	On Solving LPN using BKW and Variants
This Work	505 kilobyte	Attacking and Defending the McEliece Cryptosystem

Estimated sizes for 80 bits of security

Security assumptions

Definition (Indistinguishability Assumption for Goppa Codes)

A random irreducible Goppa code is indistuingishable from a random linear code.

Definition (LPN Distinguishing Problem (LPNDP))

Let:

- s be a random binary string of length l
- $\mathcal{B}_\theta$ be a Bernoulli distribution with parameter $\theta \in (0, \frac{1}{2})$

Let $\mathcal{Q}_{s,\theta}$ be the following distribution:

$$\{(a, \langle s, a\rangle \oplus e) | a \xleftarrow{\$} \{0,1\}^l, e \leftarrow \mathcal{B}_\theta\}$$

It is hard to distuingish between $\mathcal{Q}_{s,\theta}$ and a uniformly random distribution.

IND-CPA security

Game 1

$c^* = (s \cdot G_S \oplus e_S, \quad s \cdot G_R \oplus e_R, \quad s \cdot C_S \oplus e \oplus m_b \cdot G_2)$

IND-CPA security

Game 1

$c^* = (s \cdot G_S \oplus e_S, \quad s \cdot G_R \oplus e_R, \quad s \cdot C_S \oplus e \oplus m_b \cdot G_2)$

Game 2 + 3

$c^* = (s \cdot U_S \oplus e_S, \quad s \cdot U_R \oplus e_R, \quad s \cdot C_S \oplus e \oplus m_b \cdot G_2)$

IND-CPA security

Game 1

$c^* = (s \cdot G_S \oplus e_S, \quad s \cdot G_R \oplus e_R, \quad s \cdot C_S \oplus e \oplus m_b \cdot G_2)$

Game 2 + 3

$c^* = (s \cdot U_S \oplus e_S, \quad s \cdot U_R \oplus e_R, \quad s \cdot C_S \oplus e \oplus m_b \cdot G_2)$

Game 4

$c^* = (u_1, \quad u_2, \quad u_3 \oplus m_b \cdot G_2)$

DRE soundness

- Assume $\mathsf{dec}(pk_S, sk_R, c) = \perp$ and $\mathsf{dec}(pk_R, sk_S, c) = m$

DRE soundness

- Assume $\mathtt{dec}(pk_S, sk_R, c) = \perp$ and $\mathtt{dec}(pk_R, sk_S, c) = m$
- $c = (c_R, c_S, c')$ and $pk_R = (G_R, C_R)$ and $pk_S = (G_S, C_S)$

DRE soundness

- Assume $\mathsf{dec}(pk_S, sk_R, c) = \perp$ and $\mathsf{dec}(pk_R, sk_S, c) = m$
- $c = (c_R, c_S, c')$ and $pk_R = (G_R, C_R)$ and $pk_S = (G_S, C_S)$
-

$$c_R = s' \cdot G_R \oplus e_R$$
$$c_S = s \cdot G_S \oplus e_S$$

DRE soundness

- Assume $\mathtt{dec}(pk_S, sk_R, c) = \perp$ and $\mathtt{dec}(pk_R, sk_S, c) = m$
- $c = (c_R, c_S, c')$ and $pk_R = (G_R, C_R)$ and $pk_S = (G_S, C_S)$
-

$$c_R = s' \cdot G_R \oplus e_R$$
$$c_S = s \cdot G_S \oplus e_S$$

- $\mathtt{dec}(pk_S, sk_R, c) = \perp$ means the verification has failed

DRE soundness

- Assume $\mathtt{dec}(pk_S, sk_R, c) = \perp$ and $\mathtt{dec}(pk_R, sk_S, c) = m$
- $c = (c_R, c_S, c')$ and $pk_R = (G_R, C_R)$ and $pk_S = (G_S, C_S)$
-

$$c_R = s' \cdot G_R \oplus e_R$$
$$c_S = s \cdot G_S \oplus e_S$$

- $\mathtt{dec}(pk_S, sk_R, c) = \perp$ means the verification has failed
- Hamming distance between $s' \cdot G_S$ and c_S has to be $\geq t$

DRE soundness

- Assume $\mathtt{dec}(pk_S, sk_R, c) = \perp$ and $\mathtt{dec}(pk_R, sk_S, c) = m$
- $c = (c_R, c_S, c')$ and $pk_R = (G_R, C_R)$ and $pk_S = (G_S, C_S)$
-

$$c_R = s' \cdot G_R \oplus e_R$$
$$c_S = s \cdot G_S \oplus e_S$$

- $\mathtt{dec}(pk_S, sk_R, c) = \perp$ means the verification has failed
- Hamming distance between $s' \cdot G_S$ and c_S has to be $\geq t$
- $wgt(s'G_S \oplus sG_S \oplus e_S) \geq t$

DRE soundness

- Assume $\mathtt{dec}(pk_S, sk_R, c) = \perp$ and $\mathtt{dec}(pk_R, sk_S, c) = m$
- $c = (c_R, c_S, c')$ and $pk_R = (G_R, C_R)$ and $pk_S = (G_S, C_S)$
-

$$c_R = s' \cdot G_R \oplus e_R$$
$$c_S = s \cdot G_S \oplus e_S$$

- $\mathtt{dec}(pk_S, sk_R, c) = \perp$ means the verification has failed
- Hamming distance between $s' \cdot G_S$ and c_S has to be $\geq t$
- $wgt(s'G_S \oplus sG_S \oplus e_S) \geq t$
- So $s' \neq s$ due to e_S being guaranteed to have the hamming weight $wgt(e_S) < t$

DRE soundness

- However, from $\mathtt{dec}(pk_R, sk_S, c) = m$ it follows that

$$wgt(sG_R \oplus s'G_R \oplus e_R) < t$$

DRE soundness

- However, from $\mathtt{dec}(pk_R, sk_S, c) = m$ it follows that

$$wgt(sG_R \oplus s'G_R \oplus e_R) < t$$

- sG_R and $s'G_R$ are codewords for $s \neq s'$
- Hamming distance $d(sG_R, s'G_R) \geq 2t + 1$

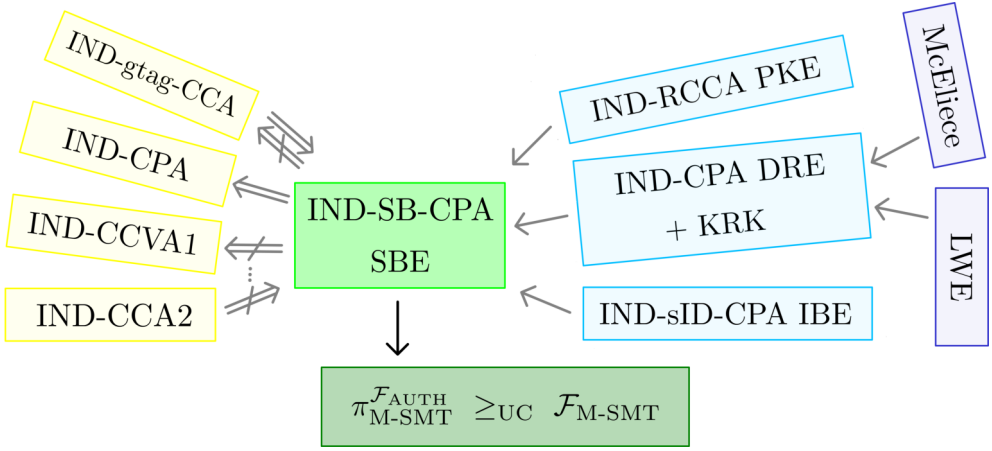
DRE soundness

- However, from $\mathtt{dec}(pk_R, sk_S, c) = m$ it follows that

$$wgt(sG_R \oplus s'G_R \oplus e_R) < t$$

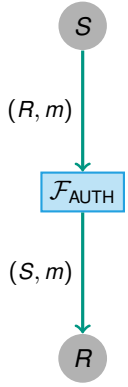
- sG_R and $s'G_R$ are codewords for $s \neq s'$
- Hamming distance $d(sG_R, s'G_R) \geq 2t + 1$
- But this contradicts with $wgt(sG_R \oplus s'G_R \oplus e_R) < t$ as $wgt(e_R) < t$

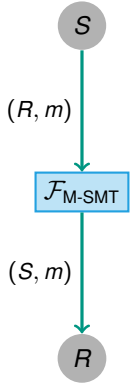
Realizing $\mathcal{F}_{\text{M-SMT}}$



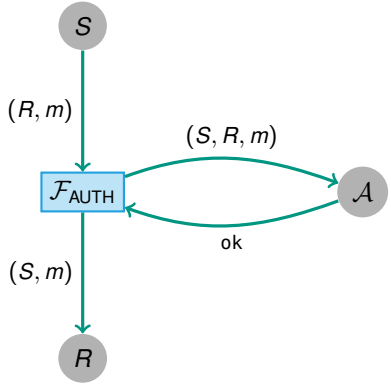
Ideal Functionalities

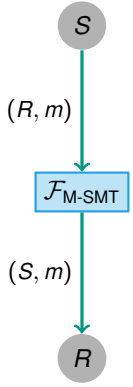
Ideal Functionalities



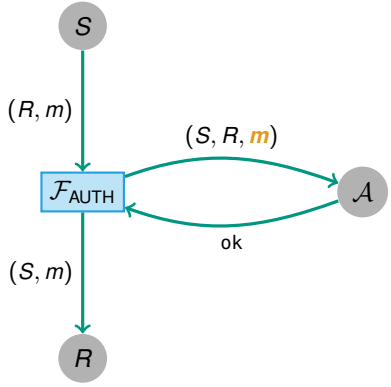


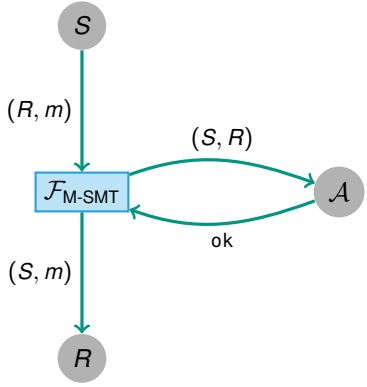
Ideal Functionalities



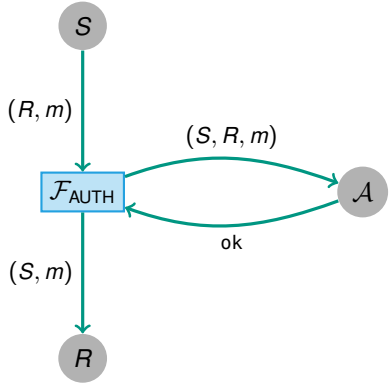


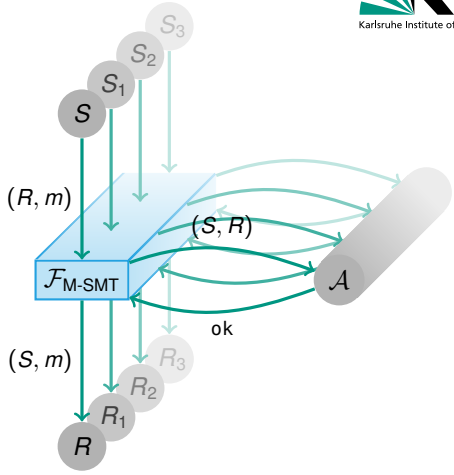
Ideal Functionalities





Ideal Functionalities

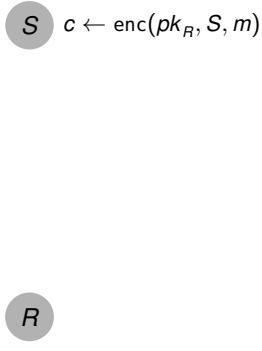




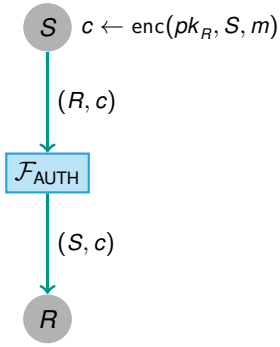
Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$

Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$

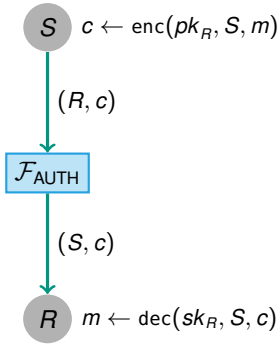
Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$



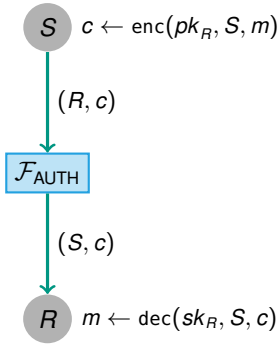
Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$

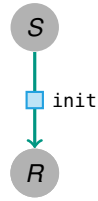


Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$

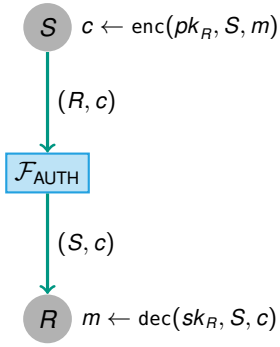


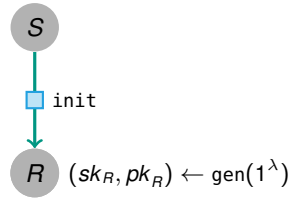
Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$



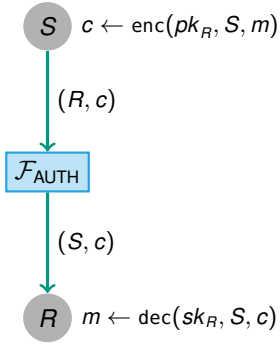


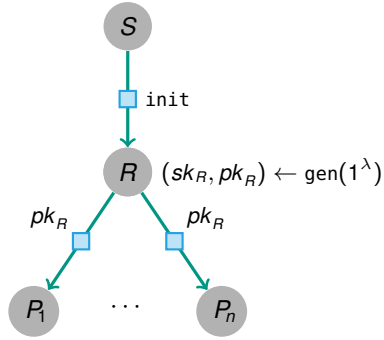
Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$





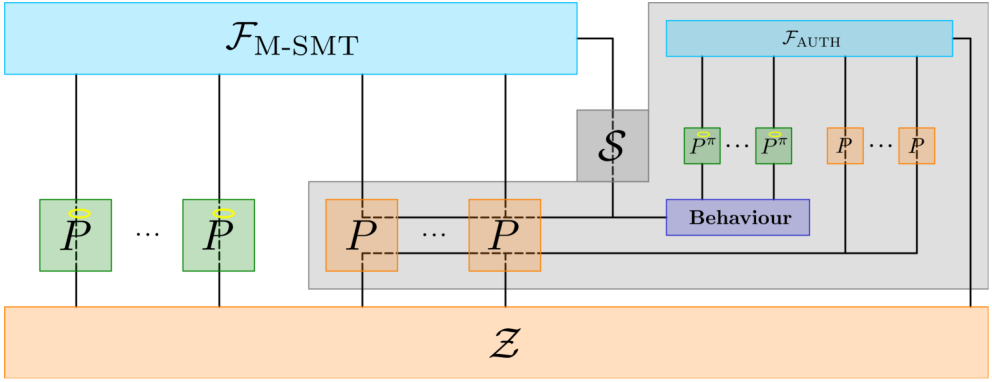
Protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$



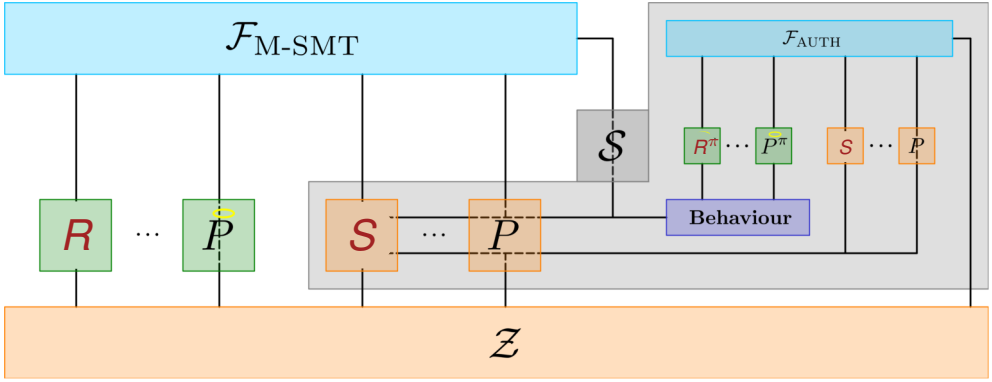


Simulator $\mathcal{S}_{\text{M-SMT}}$

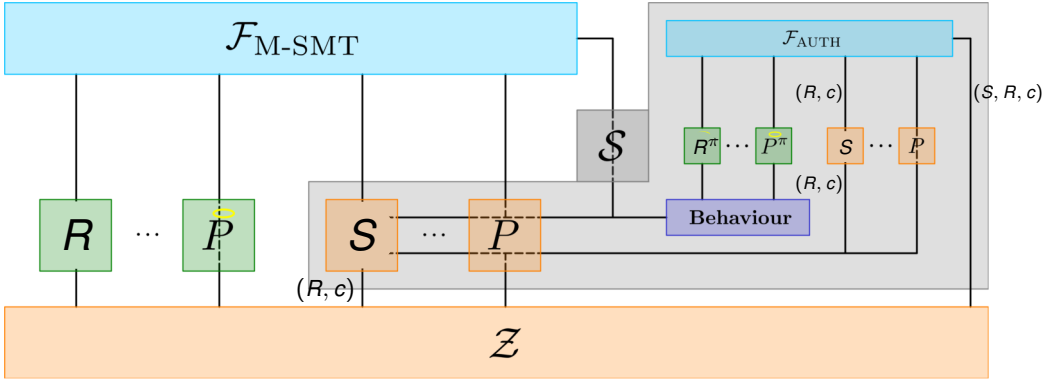
Simulator $\mathcal{S}_{\text{M-SMT}}$



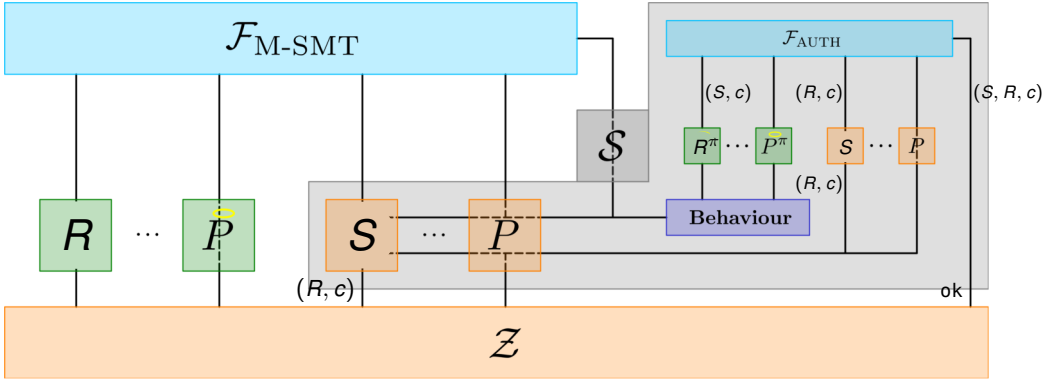
Simulator $\mathcal{S}_{\text{M-SMT}}$: Corrupted $\rightarrow$ Honest



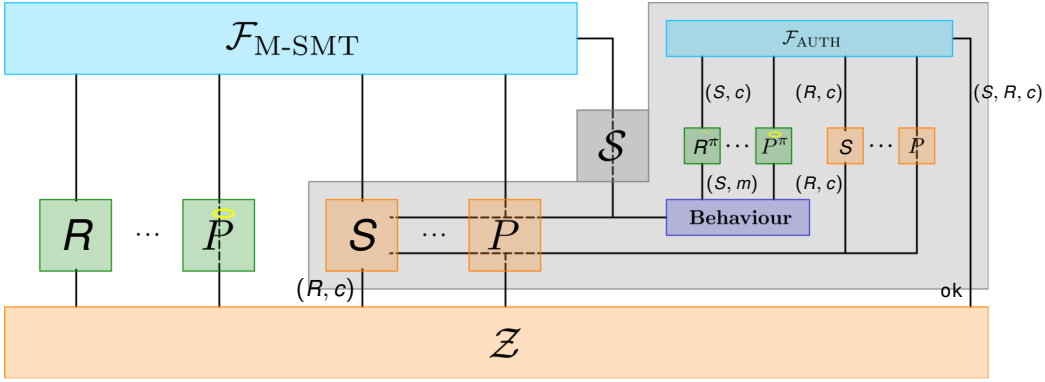
Simulator $\mathcal{S}_{\text{M-SMT}}$: Corrupted $\rightarrow$ Honest



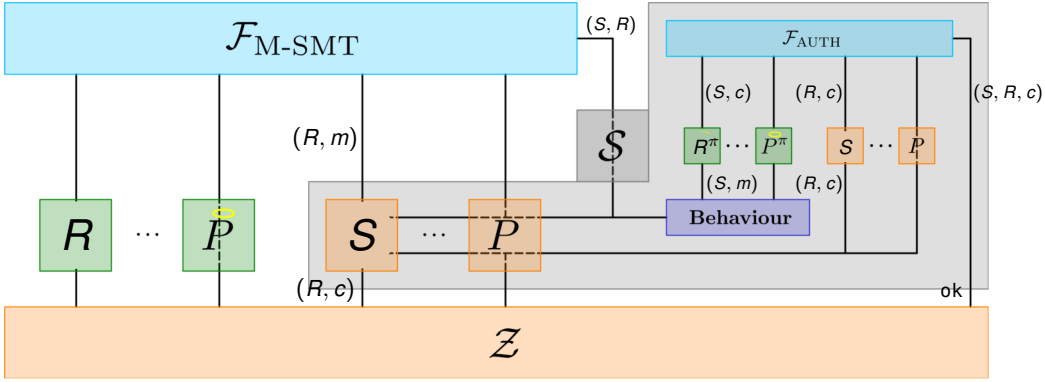
Simulator $\mathcal{S}_{\text{M-SMT}}$: Corrupted $\rightarrow$ Honest



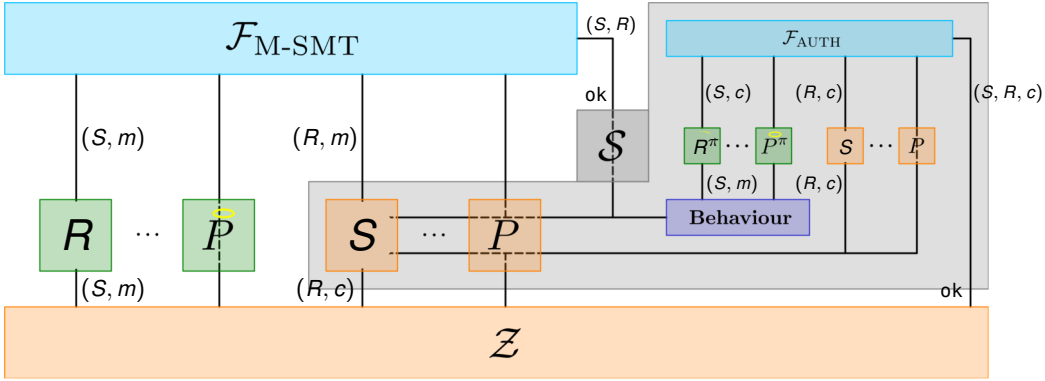
Simulator $\mathcal{S}_{\text{M-SMT}}$: Corrupted $\rightarrow$ Honest



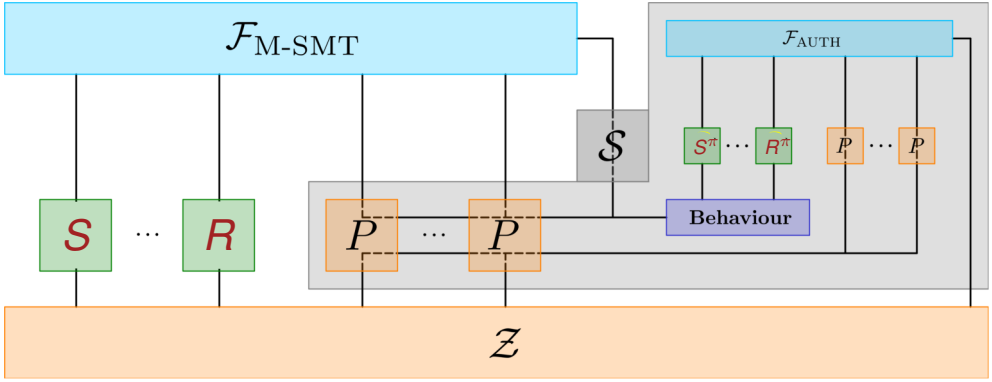
Simulator $\mathcal{S}_{\text{M-SMT}}$: Corrupted $\rightarrow$ Honest



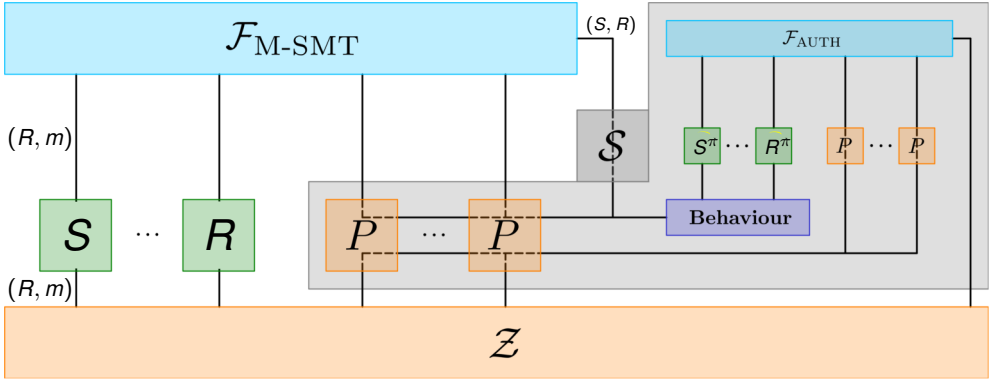
Simulator $\mathcal{S}_{\text{M-SMT}}$: Corrupted $\rightarrow$ Honest



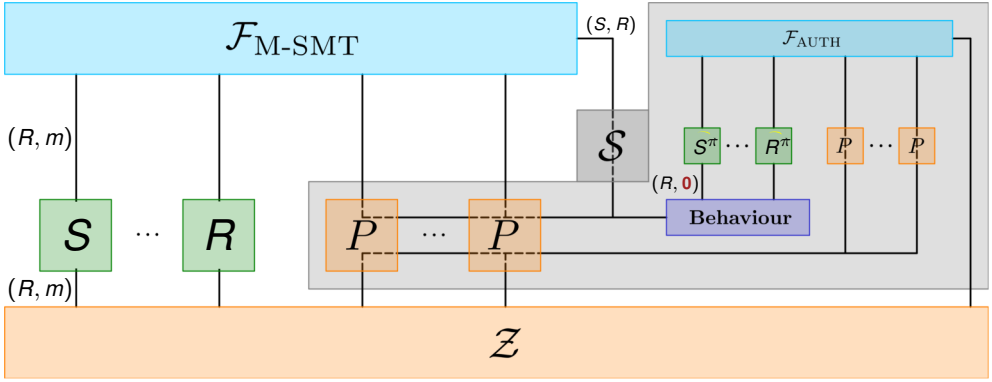
Simulator $\mathcal{S}_{\text{M-SMT}}$: Honest $\rightarrow$ Honest



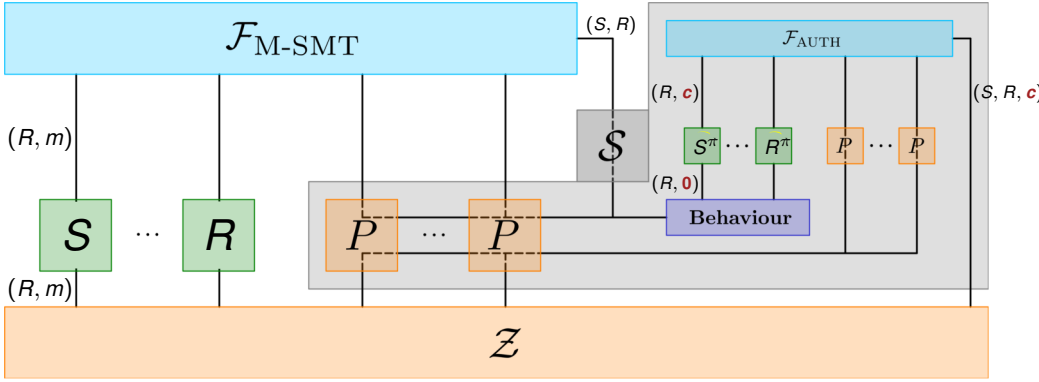
Simulator $\mathcal{S}_{\text{M-SMT}}$: Honest $\rightarrow$ Honest



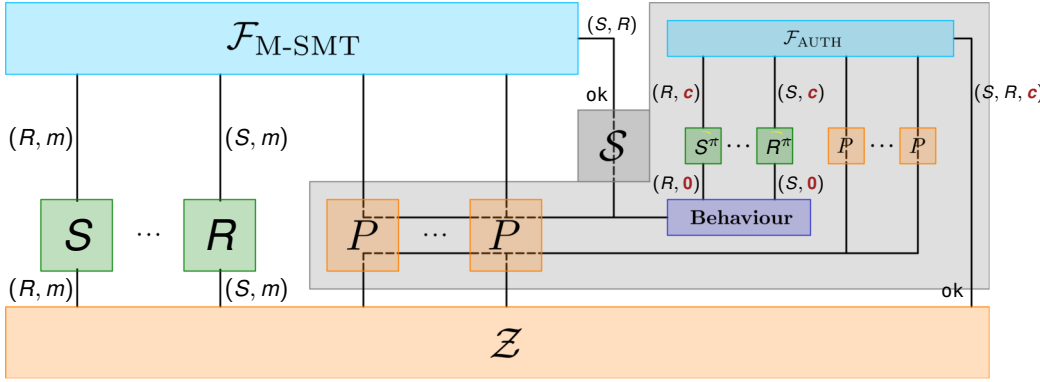
Simulator $\mathcal{S}_{\text{M-SMT}}$: Honest $\rightarrow$ Honest



Simulator $\mathcal{S}_{\text{M-SMT}}$: Honest $\rightarrow$ Honest



Simulator $\mathcal{S}_{\text{M-SMT}}$: Honest $\rightarrow$ Honest



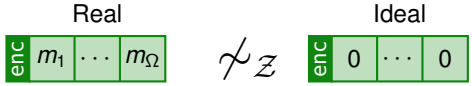
Proof Sketch

Proof Sketch: IND-SB-CPA $\rightsquigarrow \pi_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$

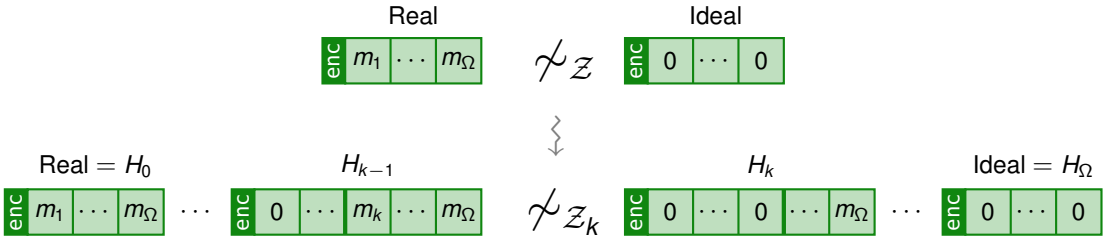
Proof Sketch: IND-SB-CPA $\rightsquigarrow \pi_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$

$$\pi_{\text{M-SMT}} \not\propto_{\mathcal{Z}} \mathcal{F}_{\text{M-SMT}}$$

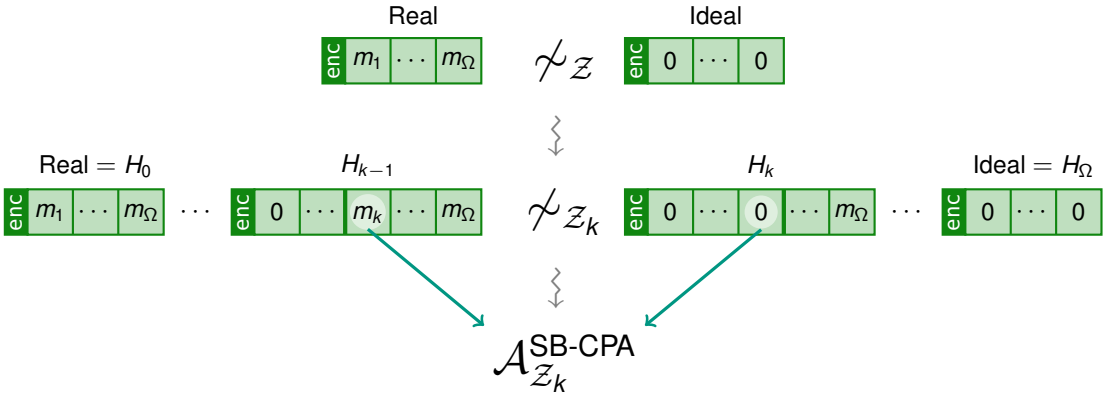
Proof Sketch: IND-SB-CPA $\rightsquigarrow \pi_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$



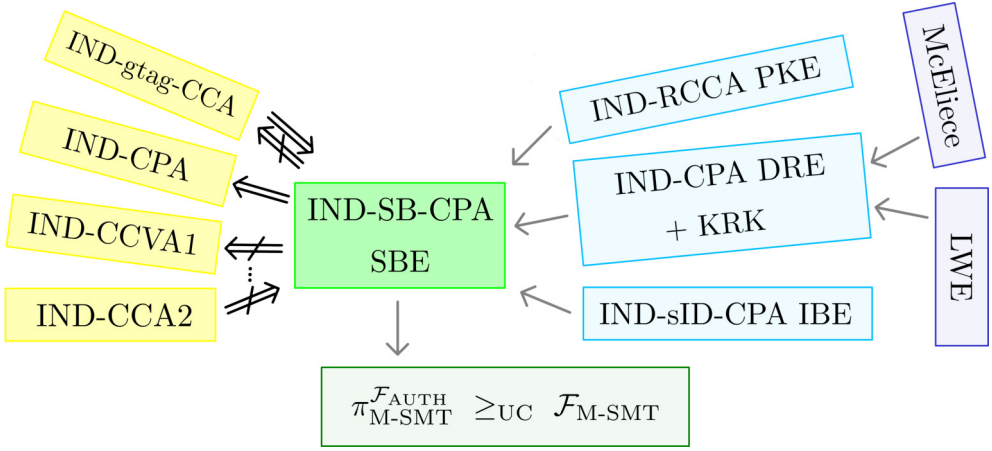
Proof Sketch: IND-SB-CPA $\rightsquigarrow \pi_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$



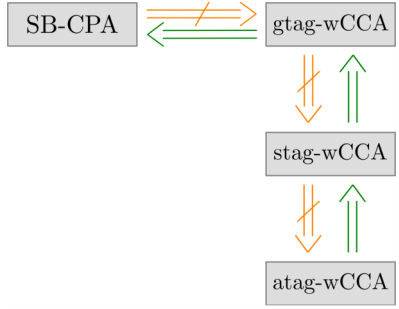
Proof Sketch: IND-SB-CPA $\rightsquigarrow \pi_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$



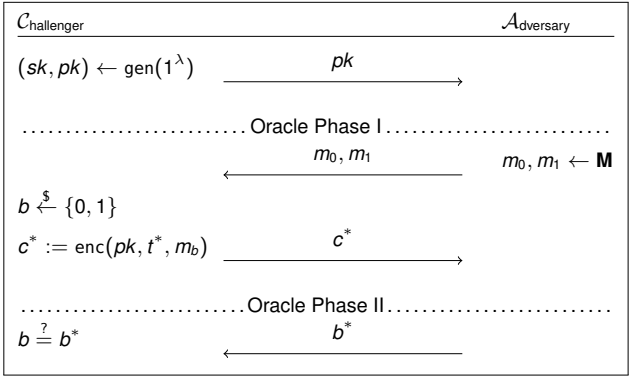
Theoretic Classification

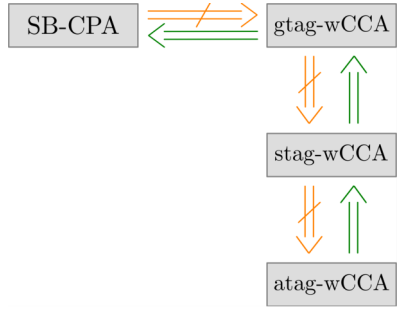


Relationship to TBE Notions

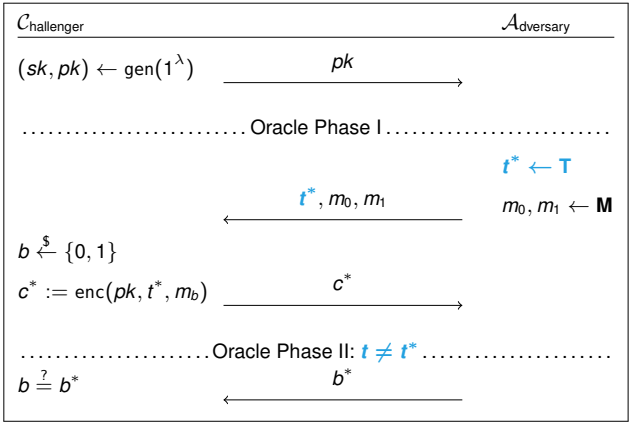


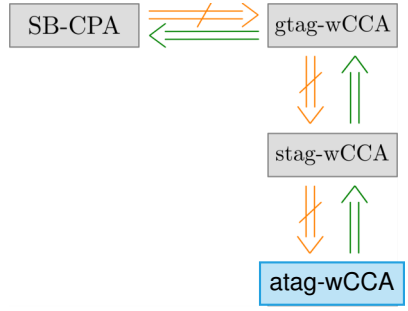
Relationship to TBE Notions



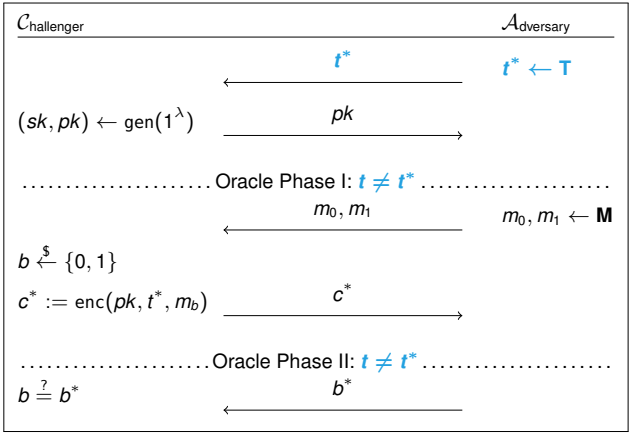


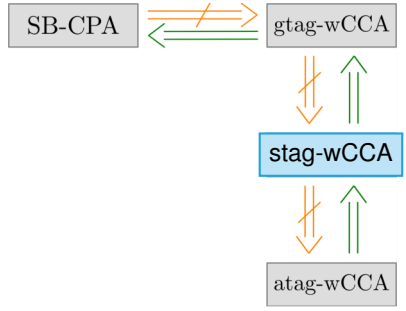
Relationship to TBE Notions



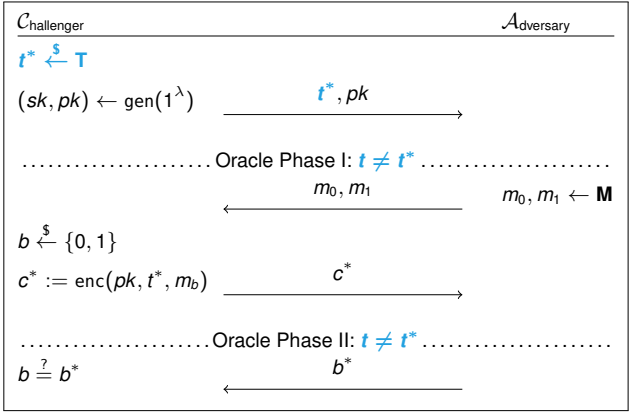


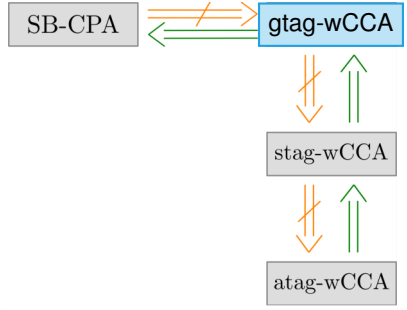
Relationship to TBE Notions



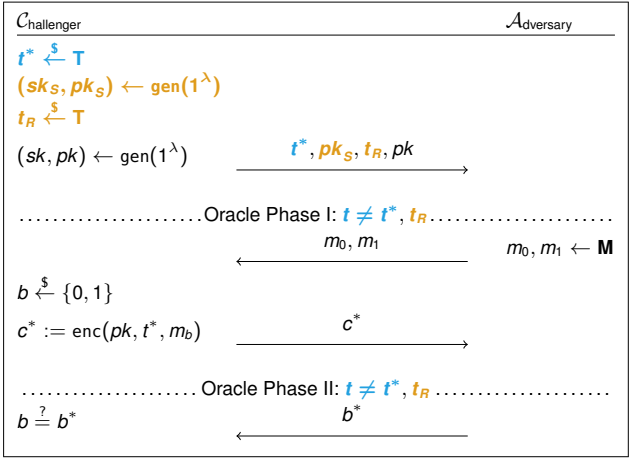


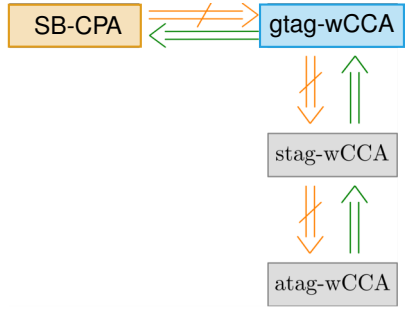
Relationship to TBE Notions



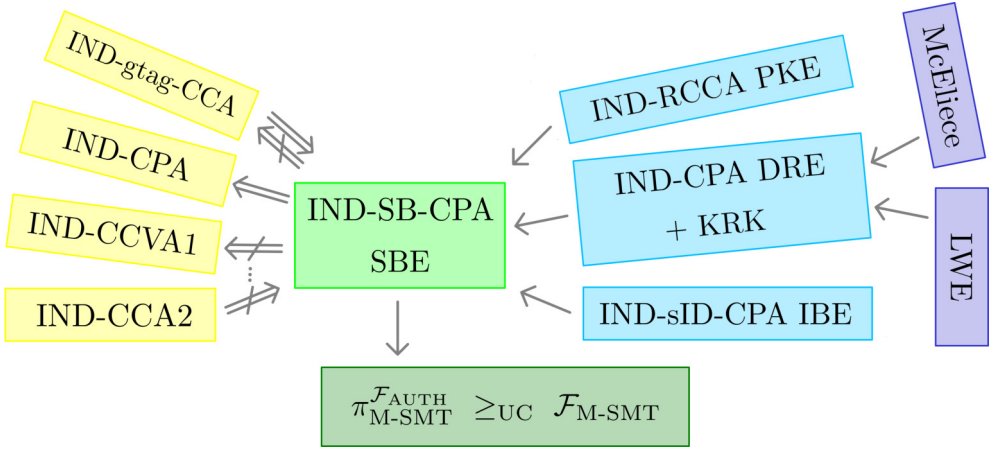


Relationship to TBE Notions





Conclusion


IND-gtag-CCA
IND-CPA
IND-CCVA1
IND-CCA2
IND-SB-CPA
SBE
IND-RCCA PKE
IND-CPA DRE
+ KRK
IND-sID-CPA IBE
McEliece
LWE
$\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}} \geq_{\text{UC}} \mathcal{F}_{\text{M-SMT}}$