# DISTRIBUTED (CORRELATION) SAMPLERS

## HOW TO REMOVE A TRUSTED DEALER IN ONE ROUND

DAMIANO ABRAM

PETER SCHOLL

SOPHIA YAKOUBOV

AARHUS UNIVERSITY

# CONTRIBUTIONS

# CONTRIBUTIONS

## DISTRIBUTED SAMPLER

# CONTRIBUTIONS

DISTRIBUTED SAMPLER → one-round generation of any CRS

# CONTRIBUTIONS

DISTRIBUTED SAMPLER → one-round generation of any CRS

- definition

# CONTRIBUTIONS

DISTRIBUTED SAMPLER → one-round generation of any CRS

- definition
- first constructions

# CONTRIBUTIONS

DISTRIBUTED SAMPLER → one-round generation of any CRS

- definition
- first constructions

PUBLIC-KEY PCF

# CONTRIBUTIONS

DISTRIBUTED SAMPLER → one-round generation of any CRS

- definition
- first constructions

PSEUDORANDOM CORRELATION FUNCTION

PUBLIC-KEY PCF → one-round generation of correlated randomness with sublinear communication

# CONTRIBUTIONS

## DISTRIBUTED SAMPLER

- definition
- first constructions

→ one-round generation of any CRS

PSEUDORANDOM CORRELATION FUNCTION

## PUBLIC-KEY PCF

- introduced by [OSY21] (OT and VOLE)

→ one-round generation of correlated randomness with sublinear communication

# CONTRIBUTIONS

## DISTRIBUTED SAMPLER

- definition
- first constructions

→ one-round generation of any CRS

PSEUDORANDOM CORRELATION FUNCTION

## PUBLIC-KEY PCF

- introduced by [OSY21] (OT and VOLE)
- formalisation

→ one-round generation of correlated randomness with sublinear communication

# CONTRIBUTIONS

## DISTRIBUTED SAMPLER

- definition
- first constructions

→ one-round generation of any CRS

PSEUDORANDOM CORRELATION FUNCTION

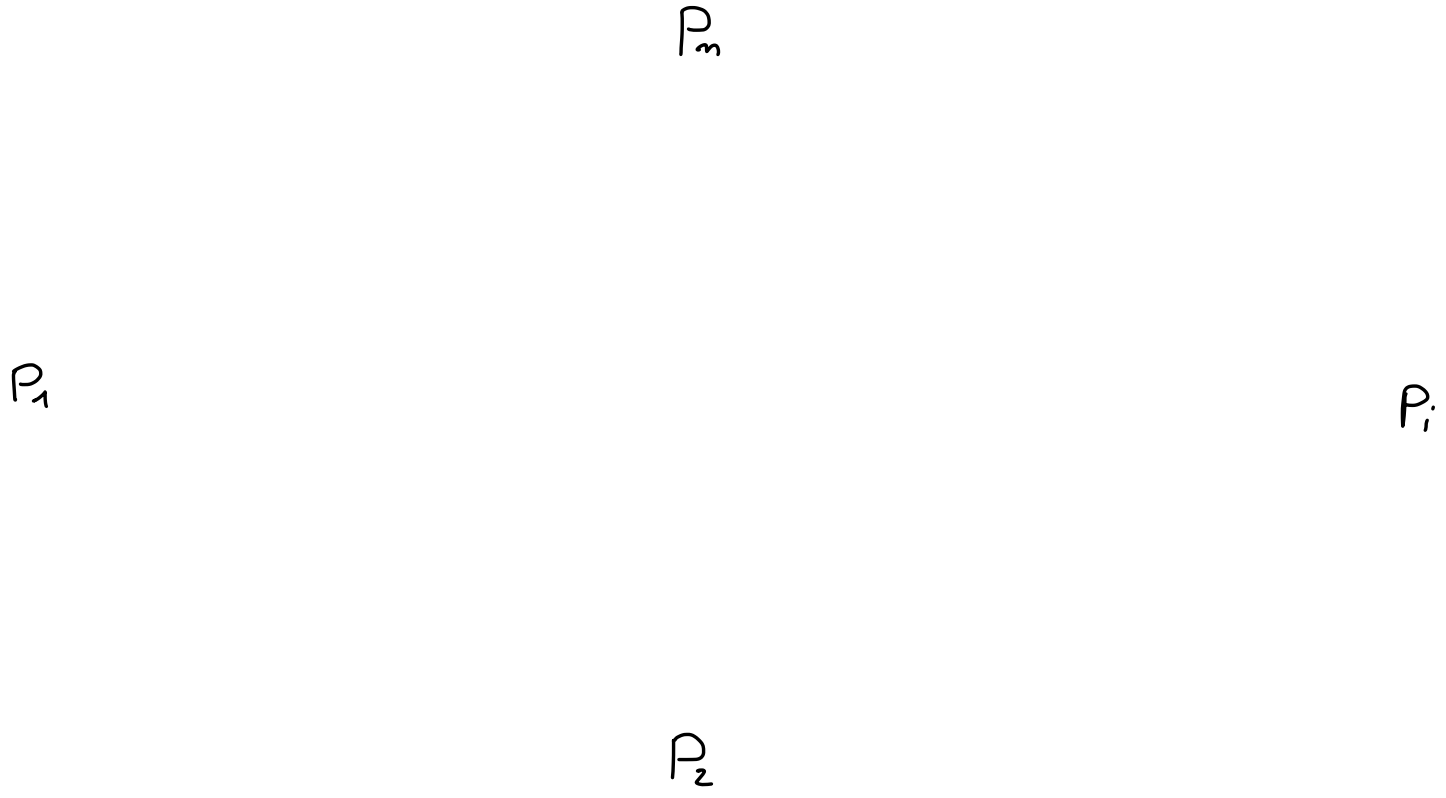
## PUBLIC-KEY PCF

- introduced by [OSY21] (OT and VOLE)
- formalisation
- first constructions for any correlation

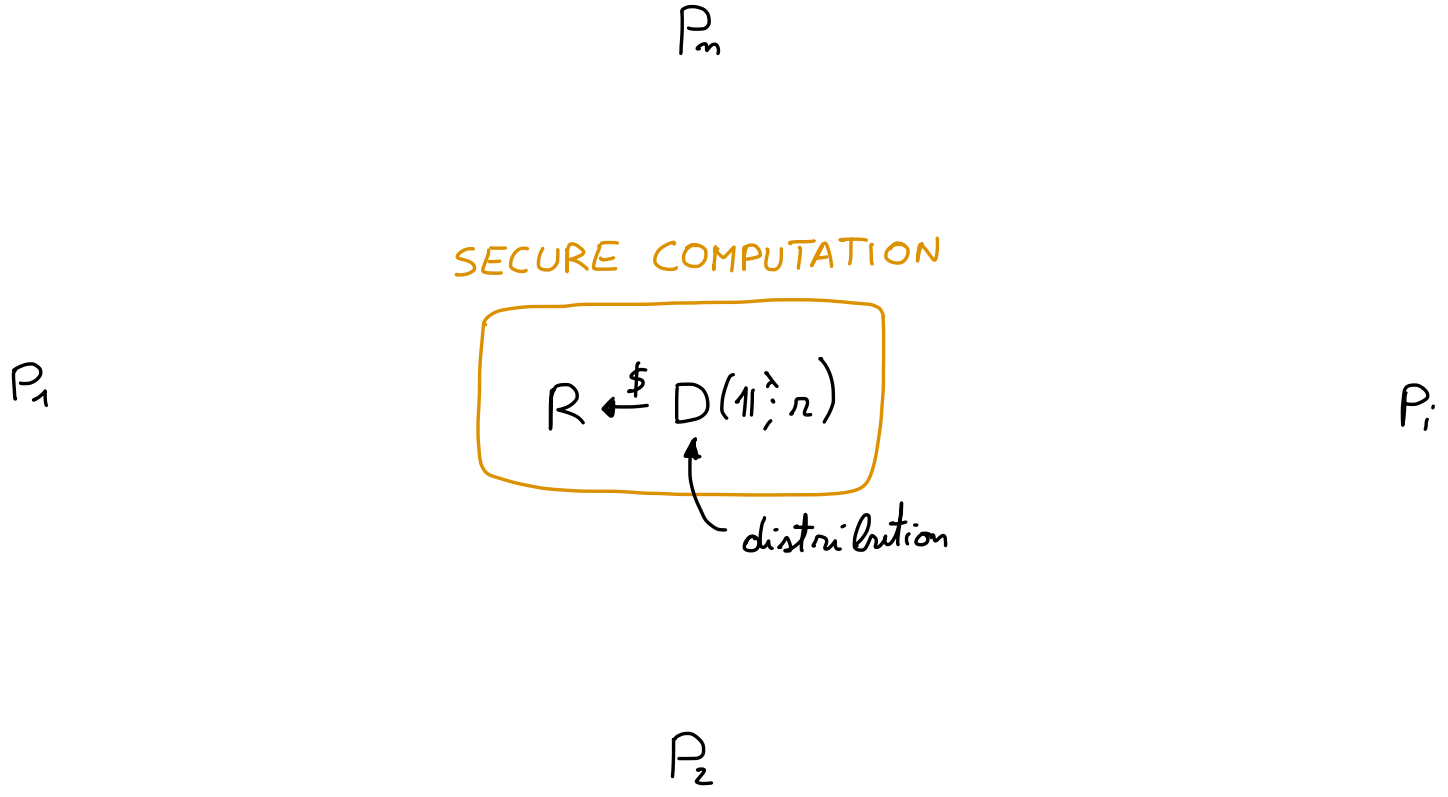
→ one-round generation of correlated randomness with sublinear communication

# DISTRIBUTED SAMPLERS

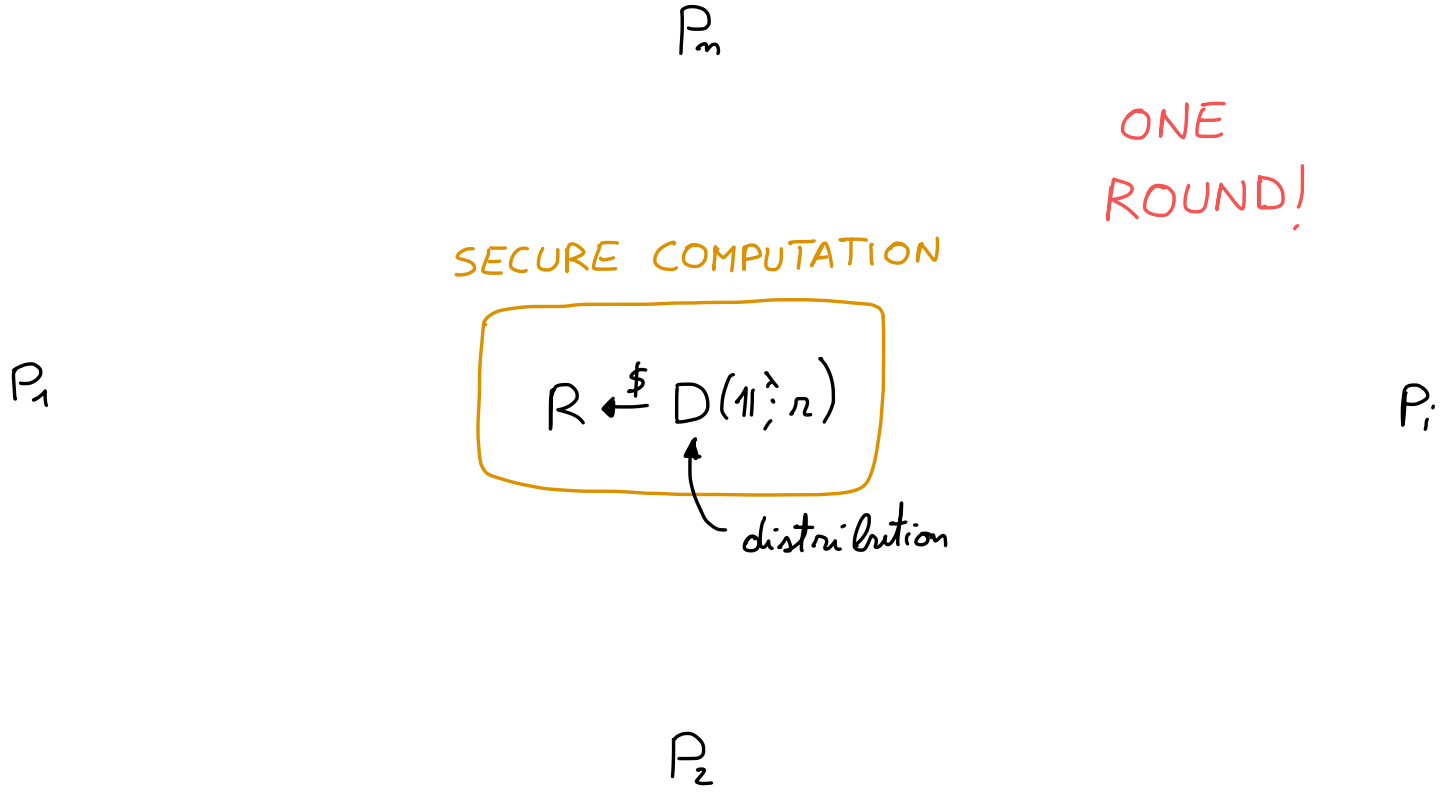
# DISTRIBUTED SAMPLERS



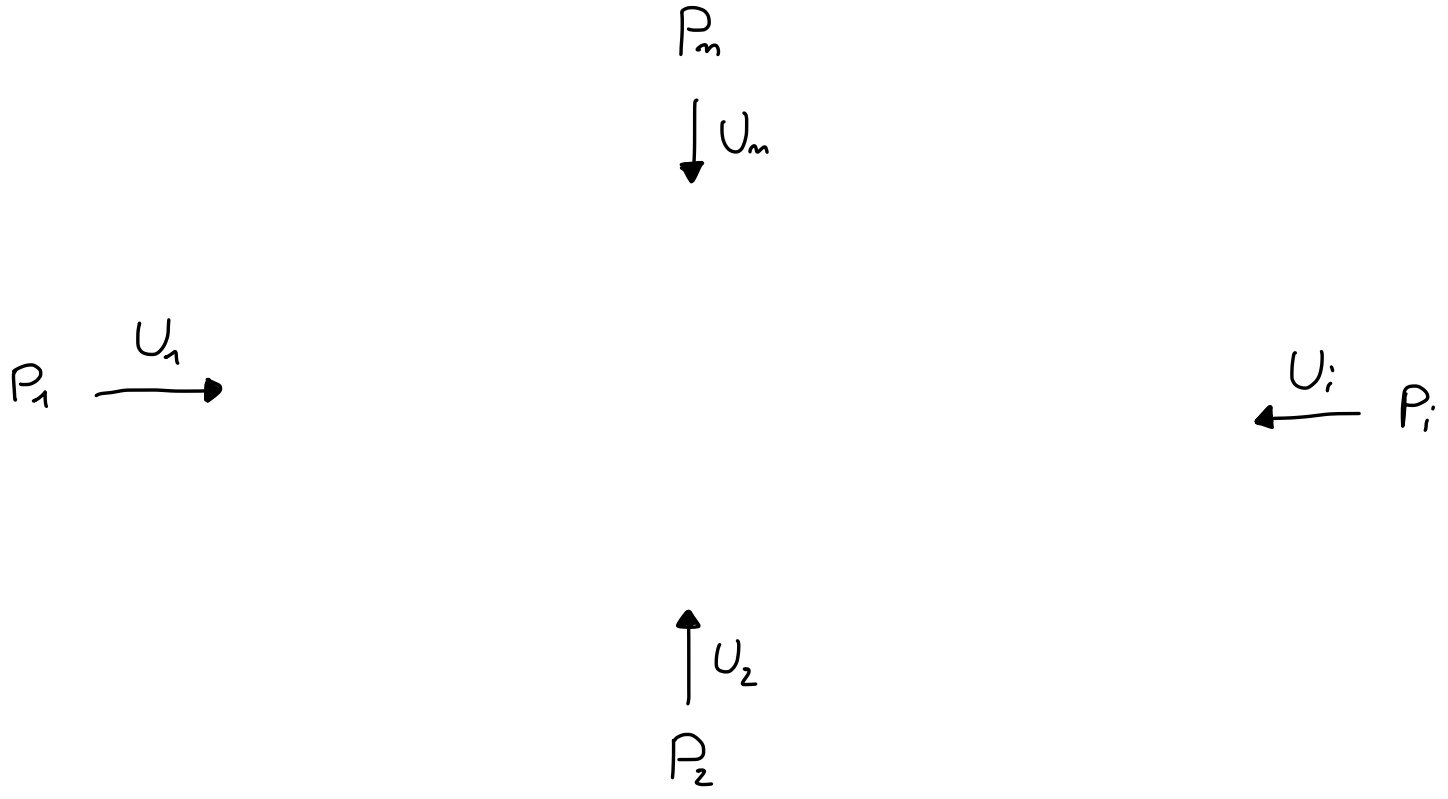
# DISTRIBUTED SAMPLERS



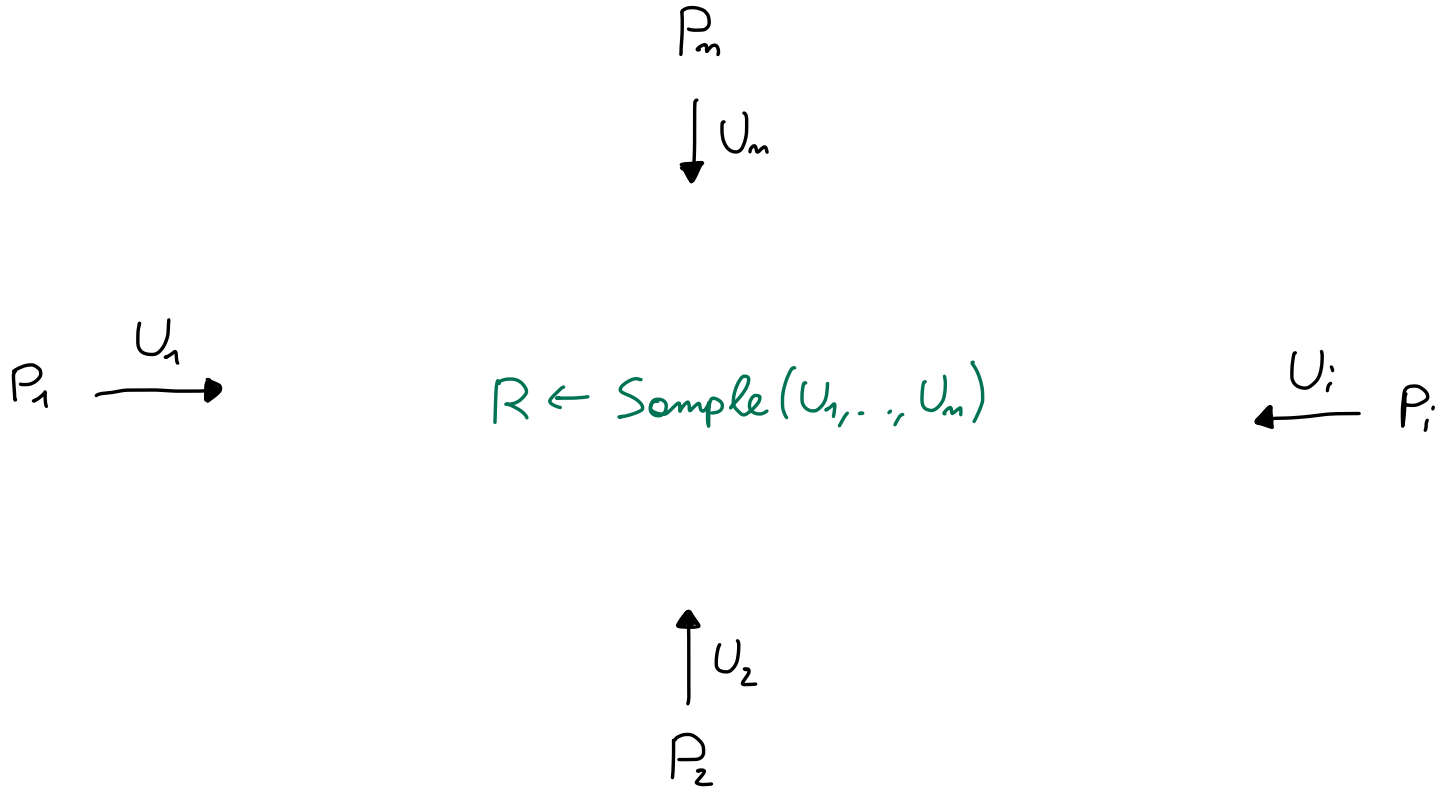
# DISTRIBUTED SAMPLERS



# DISTRIBUTED SAMPLERS



# DISTRIBUTED SAMPLERS



# SECURITY DEFINITION

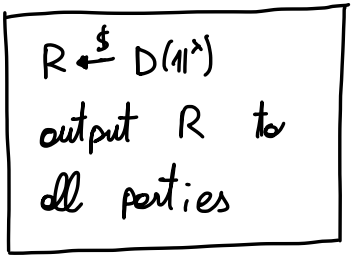
# SECURITY DEFINITION

NON - RUSHING
SEMI - MALICIOUS

# SECURITY DEFINITION

NON-RUSHING
SEMI-MALICIOUS

$\mathcal{F}_D$



# SECURITY DEFINITION

NON - RUSHING
SEMI - MALICIOUS

$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$
output $R$ to
all parties

ACTIVE

# SECURITY DEFINITION

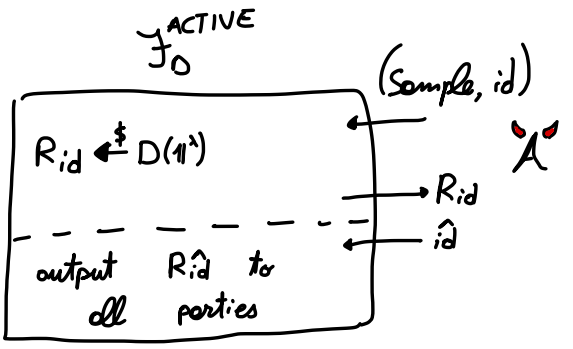
## NON-RUSHING SEMI-MALICIOUS

$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

## ACTIVE



# DISTRIBUTED SAMPLERS

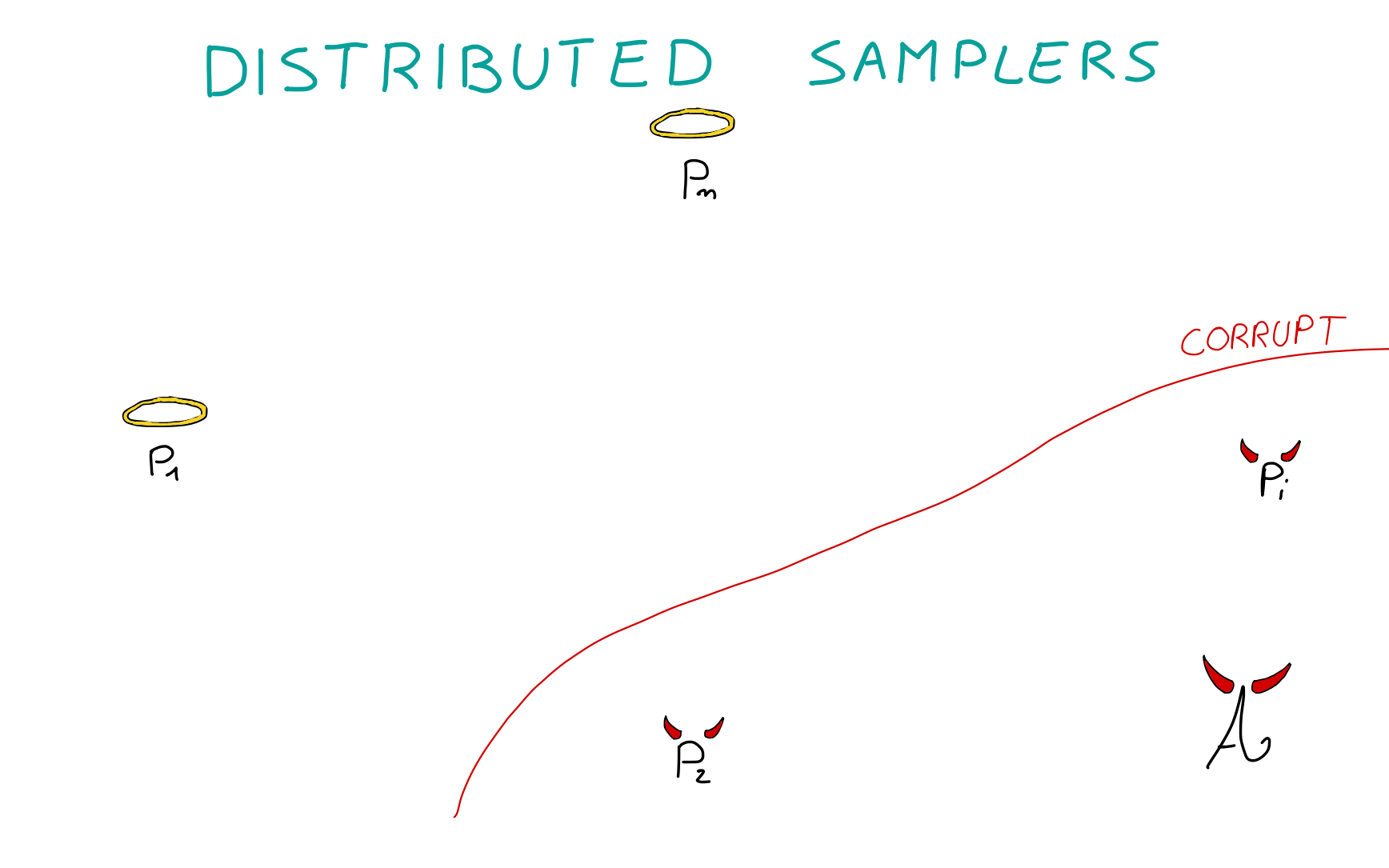
$P_m$

$P_1$

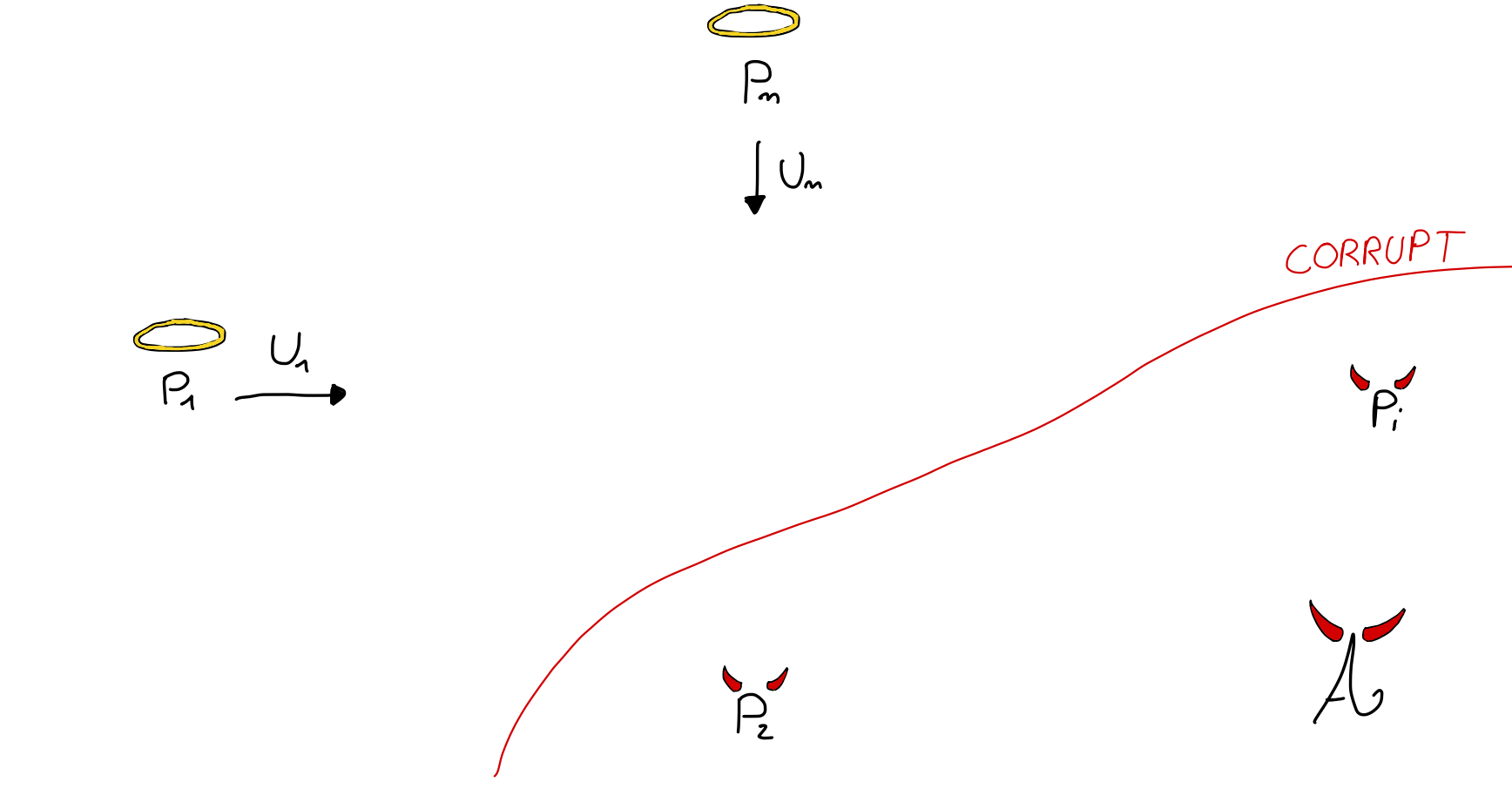
$P_i$

$P_2$

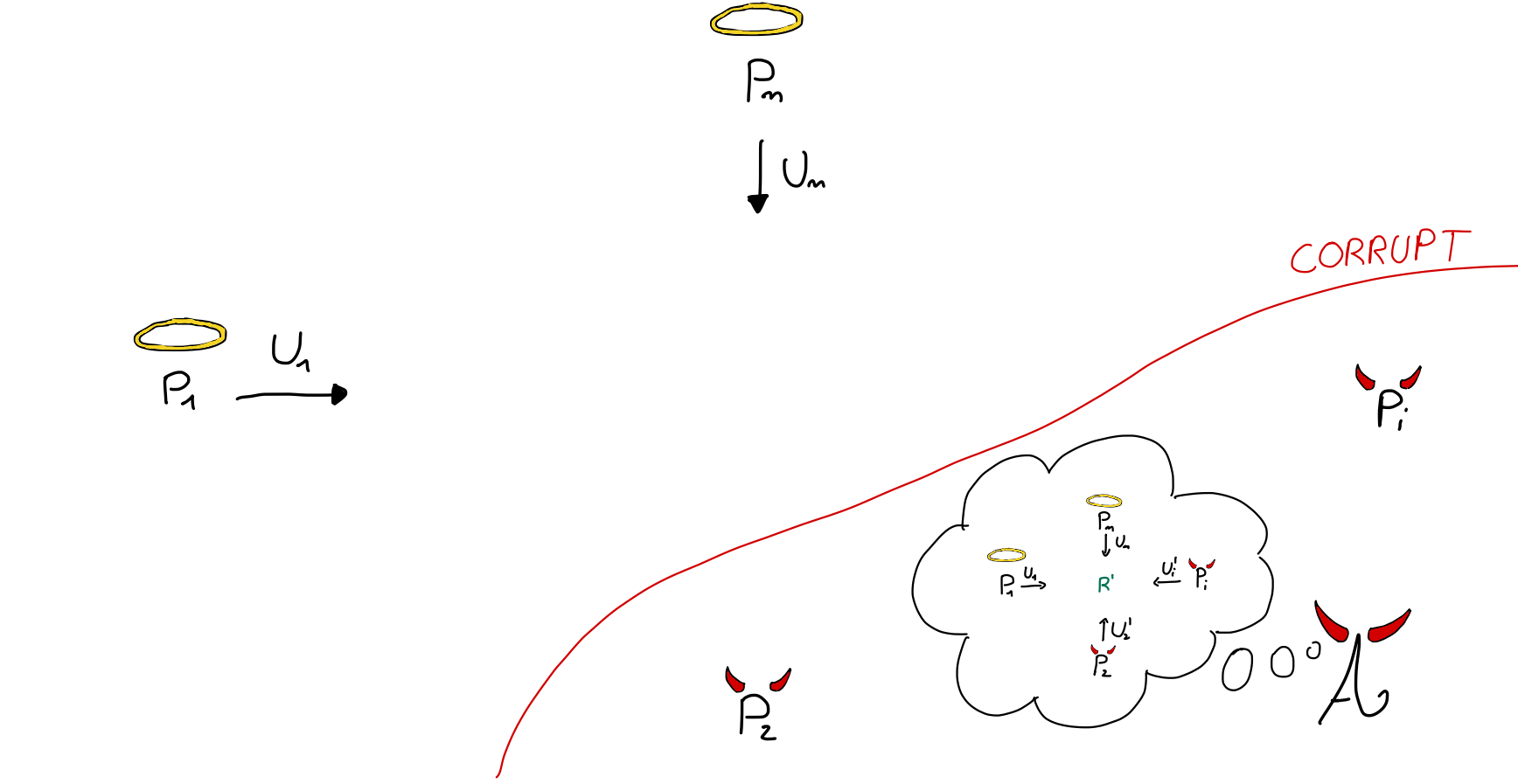
# DISTRIBUTED SAMPLERS



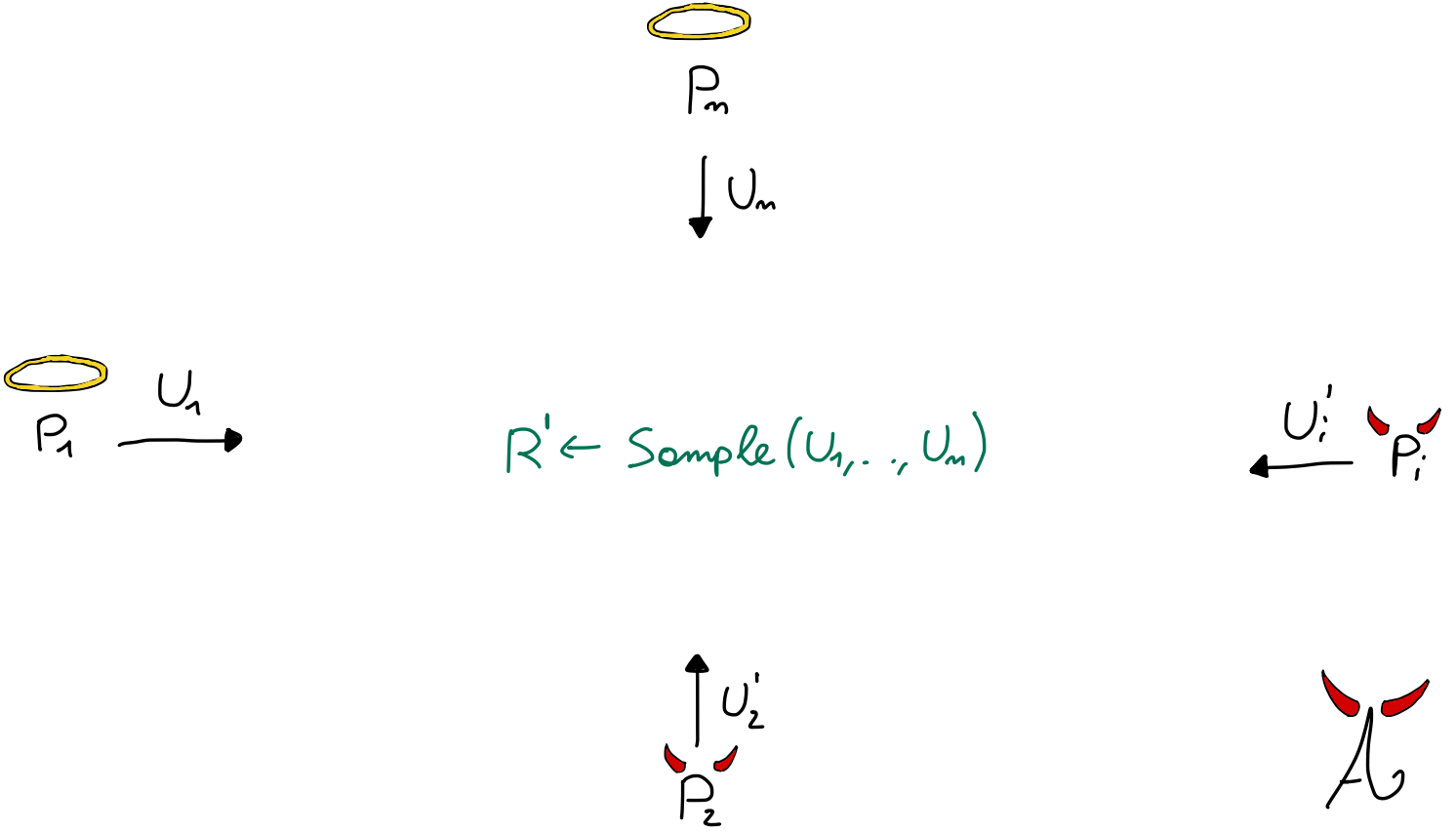
# DISTRIBUTED SAMPLERS



# DISTRIBUTED SAMPLERS



# DISTRIBUTED SAMPLERS



# OUR RESULTS

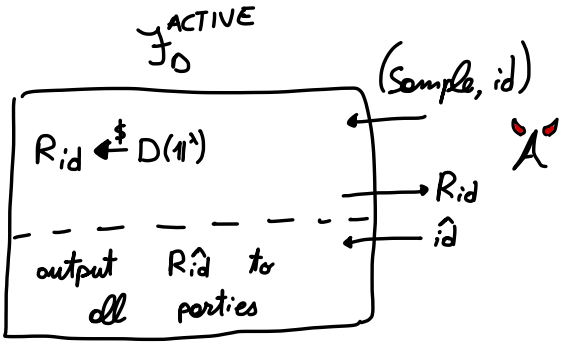
## NON-RUSHING SEMI-MALICIOUS

$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

## ACTIVE



# OUR RESULTS

## NON-RUSHING SEMI-MALICIOUS

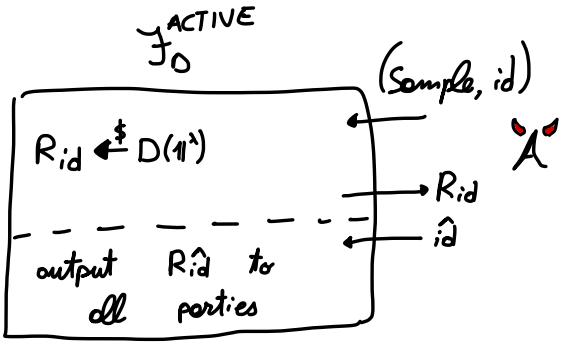
$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

- any distribution $D$

## ACTIVE



# OUR RESULTS

## NON-RUSHING SEMI-MALICIOUS

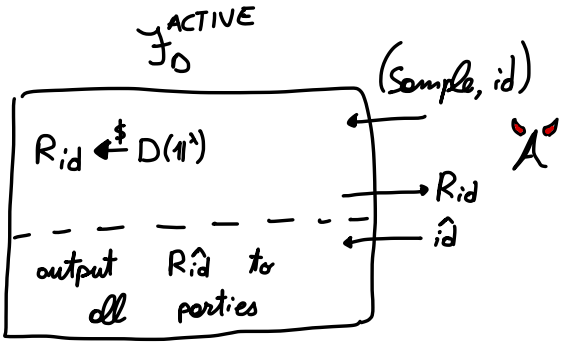
$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

- any distribution $D$
- in the PLAIN MODEL

## ACTIVE



# OUR RESULTS

## NON-RUSHING SEMI-MALICIOUS

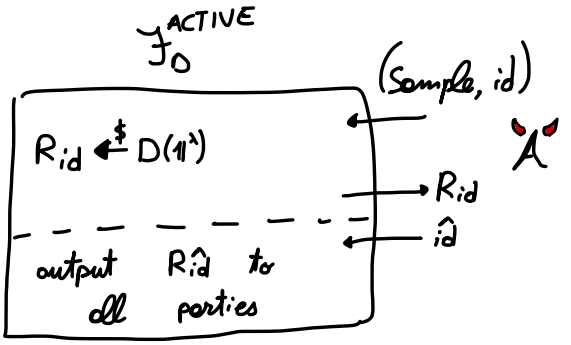
$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

- any distribution $D$
- in the PLAIN MODEL
- from polynomial $iO$ and polynomial multi-key FHE

## ACTIVE



# OUR RESULTS

## NON-RUSHING SEMI-MALICIOUS

$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

- any distribution $D$
- in the PLAIN MODEL
- from polynomial iO and polynomial multi-key FHE

## ACTIVE

$\mathcal{F}_D^{ACTIVE}$

$R_{id} \xleftarrow{\$} D(1^\lambda)$

output $R_{\hat{id}}$ to all parties

(sample, id)

$R_{id}$

$\hat{id}$

- any distribution $D$

# OUR RESULTS

## NON-RUSHING SEMI-MALICIOUS

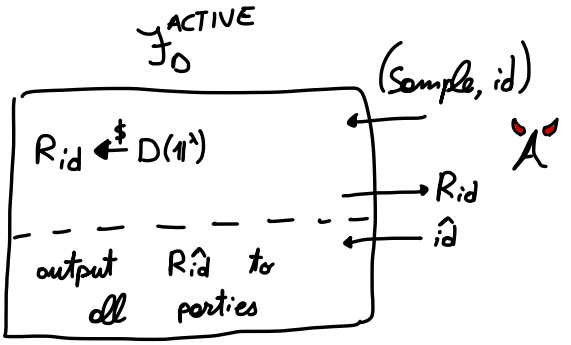
$f_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

- any distribution $D$
- in the PLAIN MODEL
- from polynomial $i\mathcal{O}$ and polynomial multi-key FHE

## ACTIVE




- any distribution $D$
- in the RANDOM ORACLE MODEL

# OUR RESULTS

## NON-RUSHING SEMI-MALICIOUS

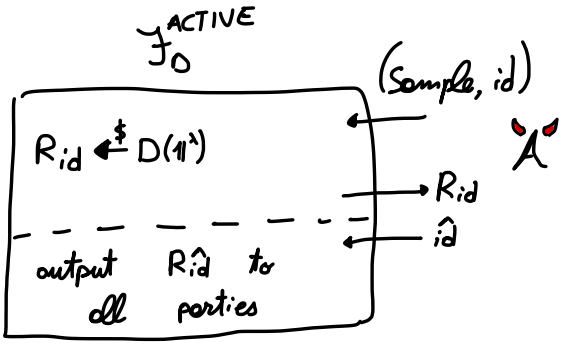
$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

- any distribution $D$
- in the PLAIN MODEL
- from polynomial $i\mathcal{O}$ and polynomial multi-key FHE

## ACTIVE




- any distribution $D$
- in the RANDOM ORACLE MODEL
- from polynomial $i\mathcal{O}$
  polynomial multi-key FHE
  polynomial NIZK

# SEMI-MALICIOUS CONSTRUCTION

# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$

$P_1$

$P_i$

$P_2$

# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$

$P_1$ $R \leftarrow D$ $P_i$

$P_2$

# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$ $r_m$

$P_1$

$r_1$

$R \leftarrow D(1^\lambda; r_1 \oplus \ldots \oplus r_m)$

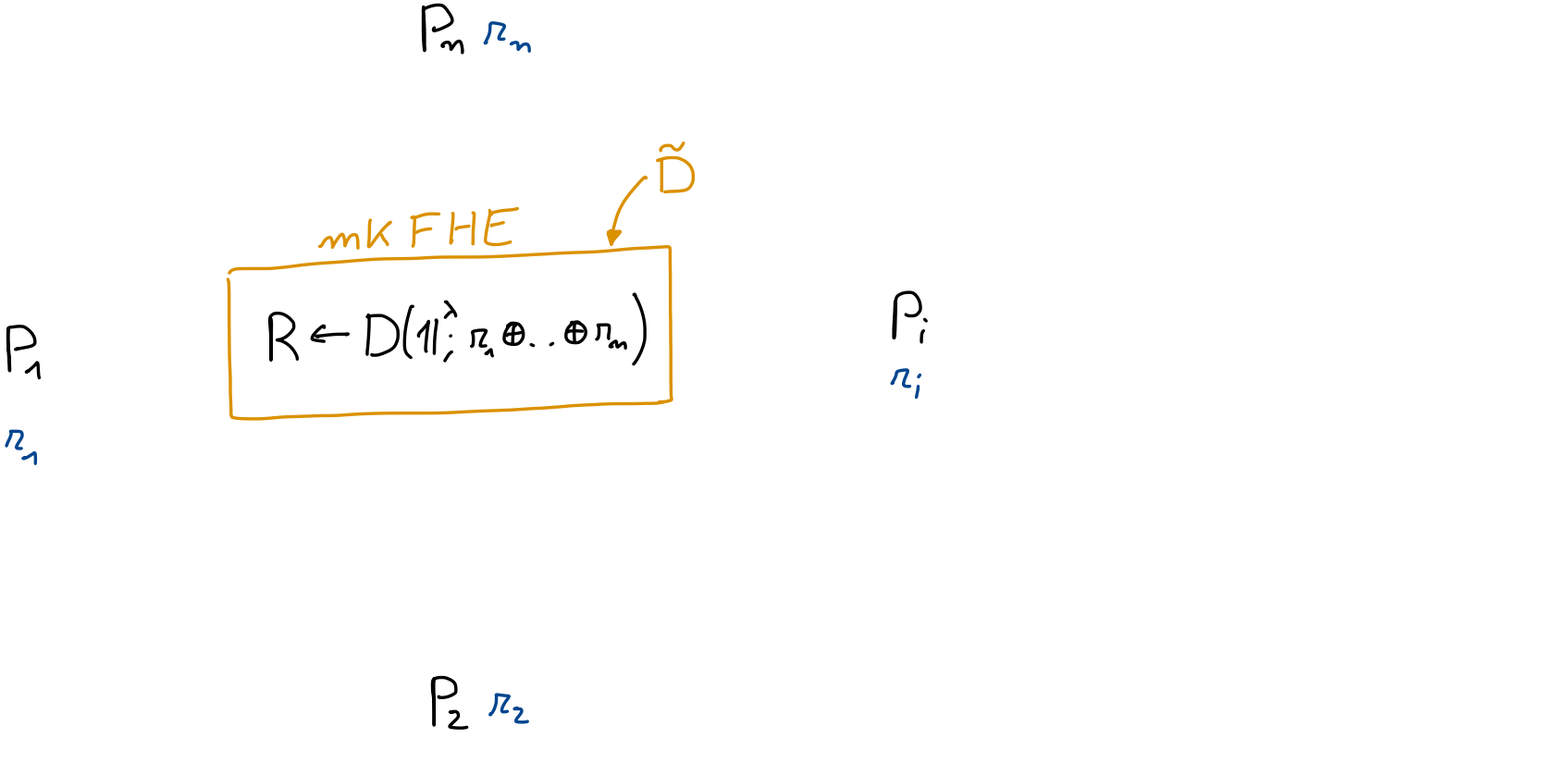
$P_i$

$r_i$

$P_2$ $r_2$

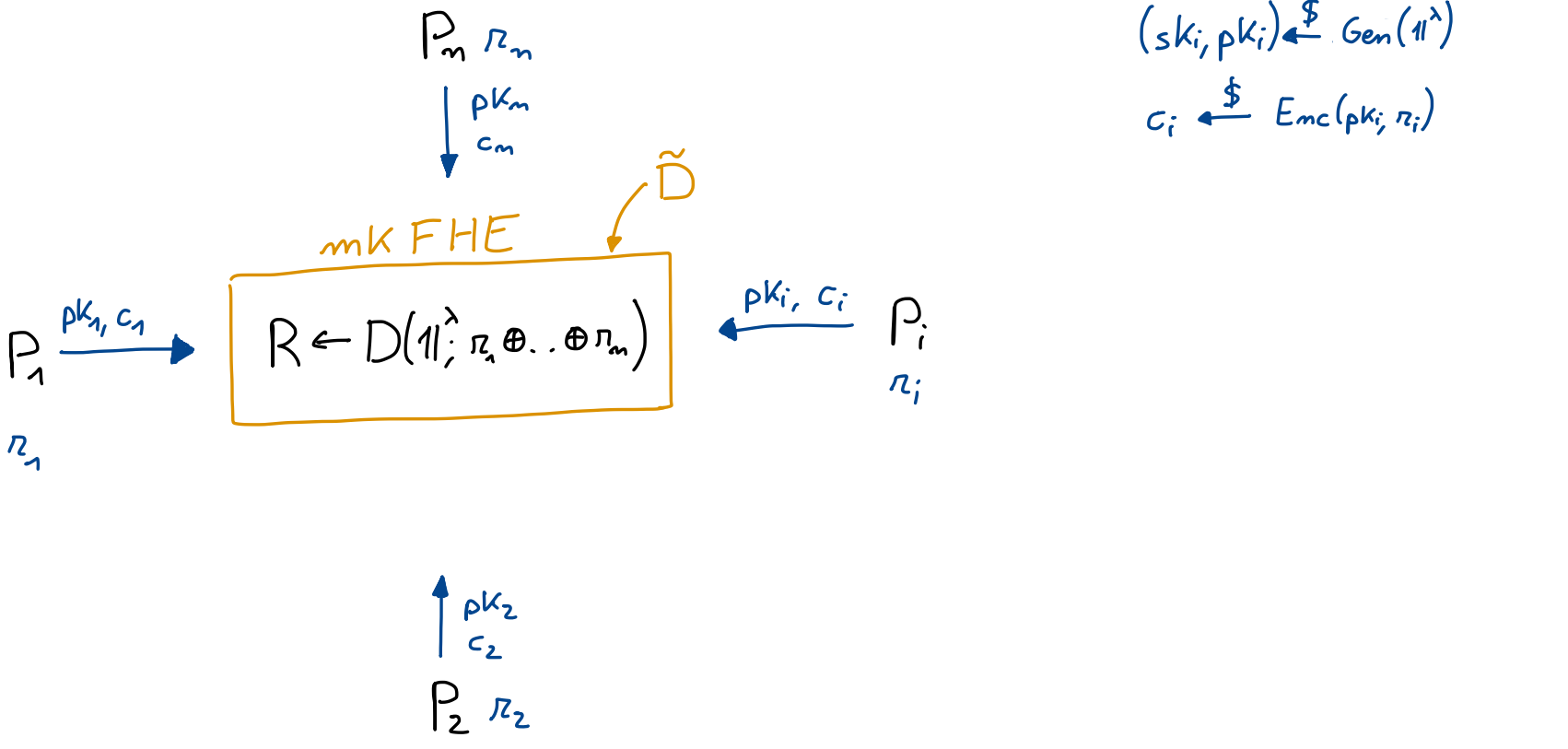
# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



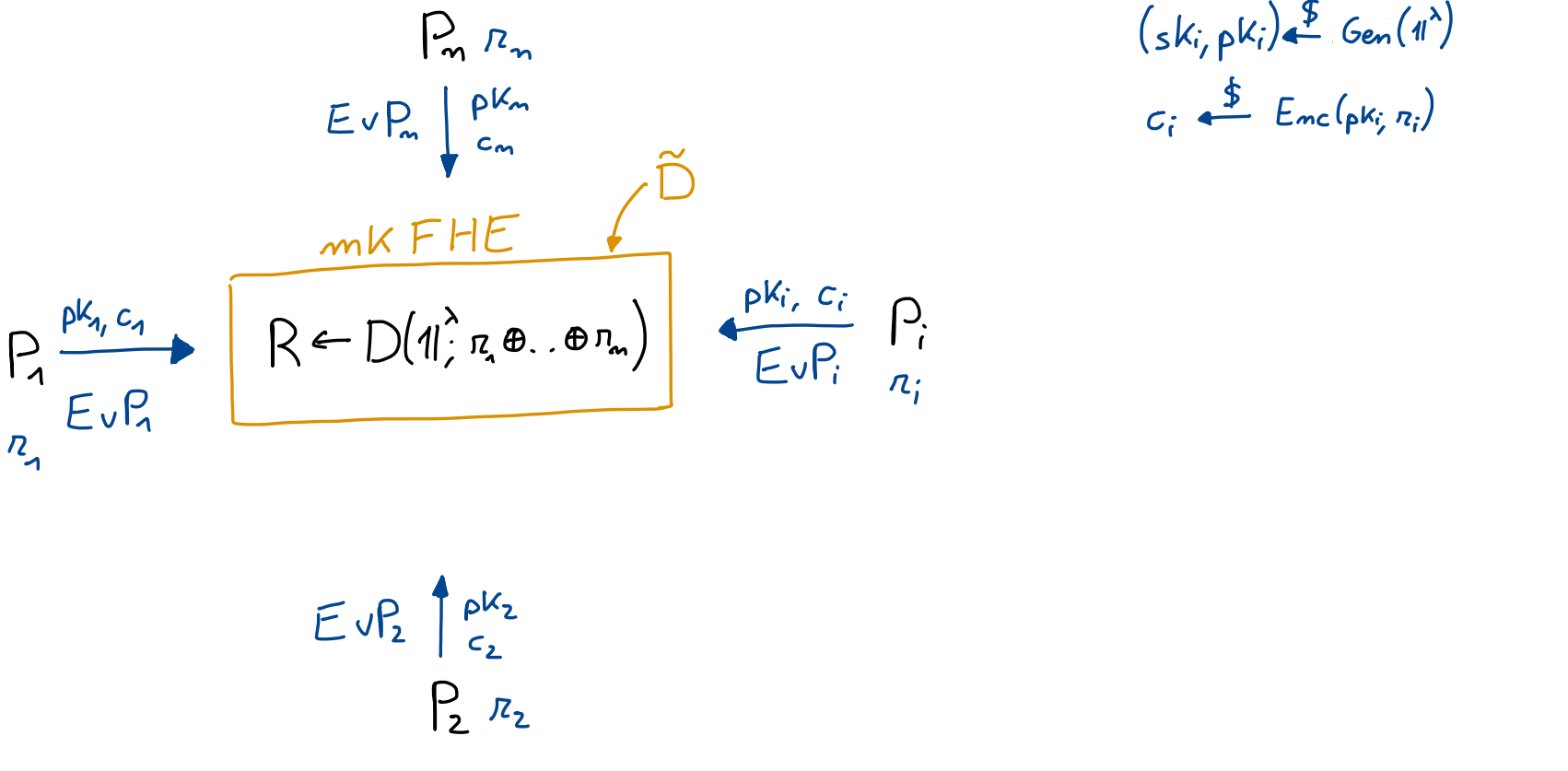
# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



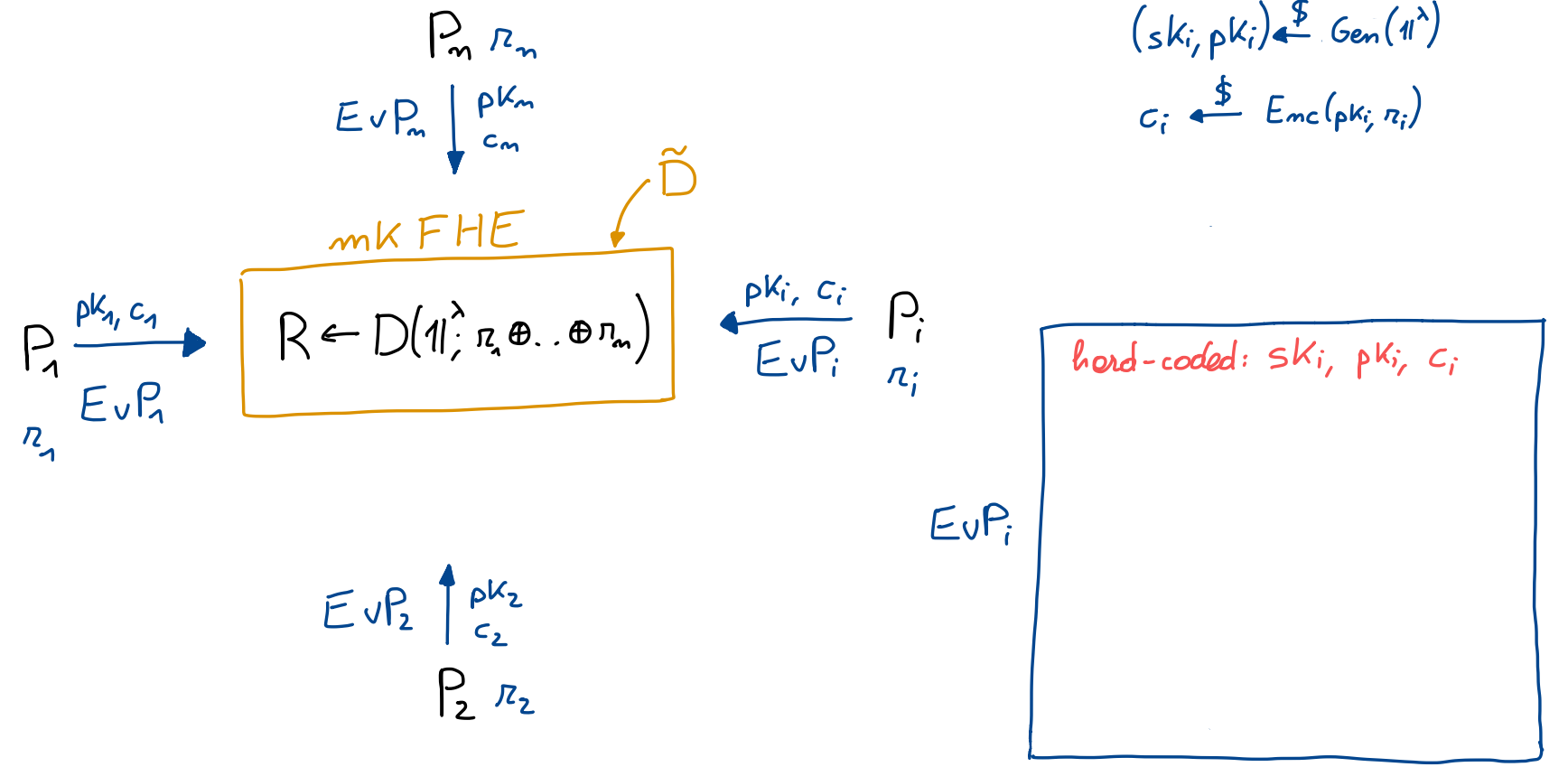
# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



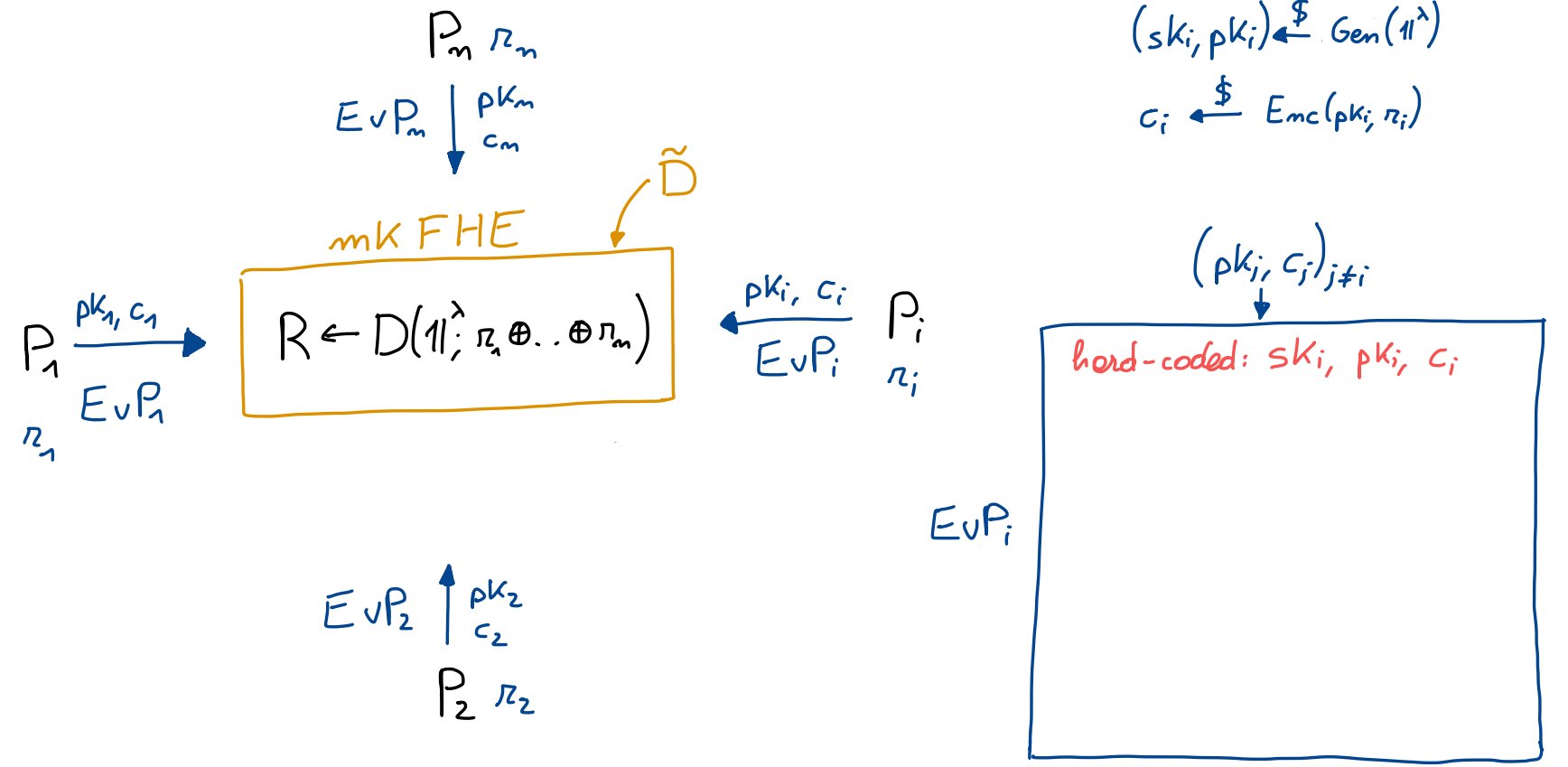
# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



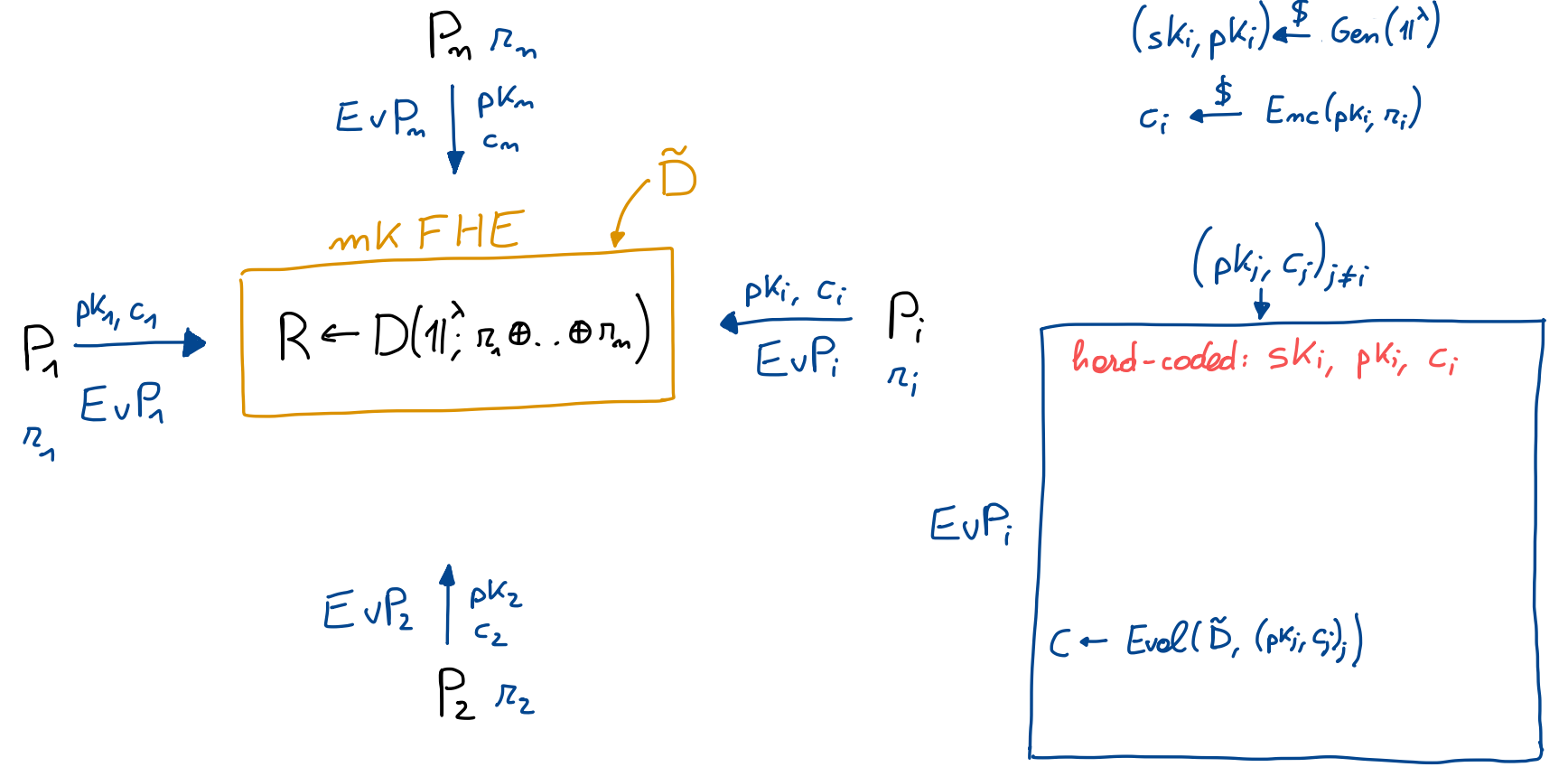
# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



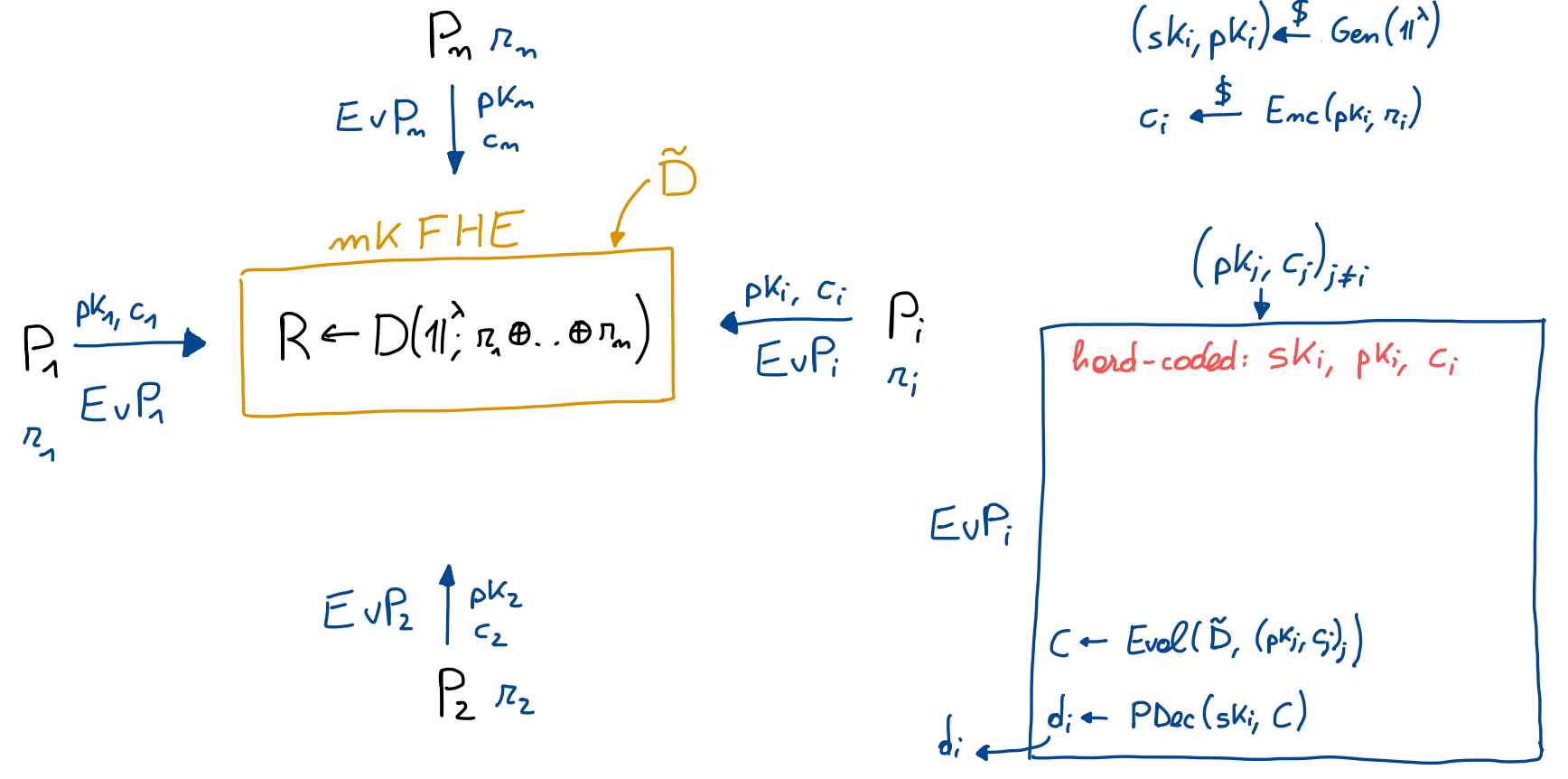
# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



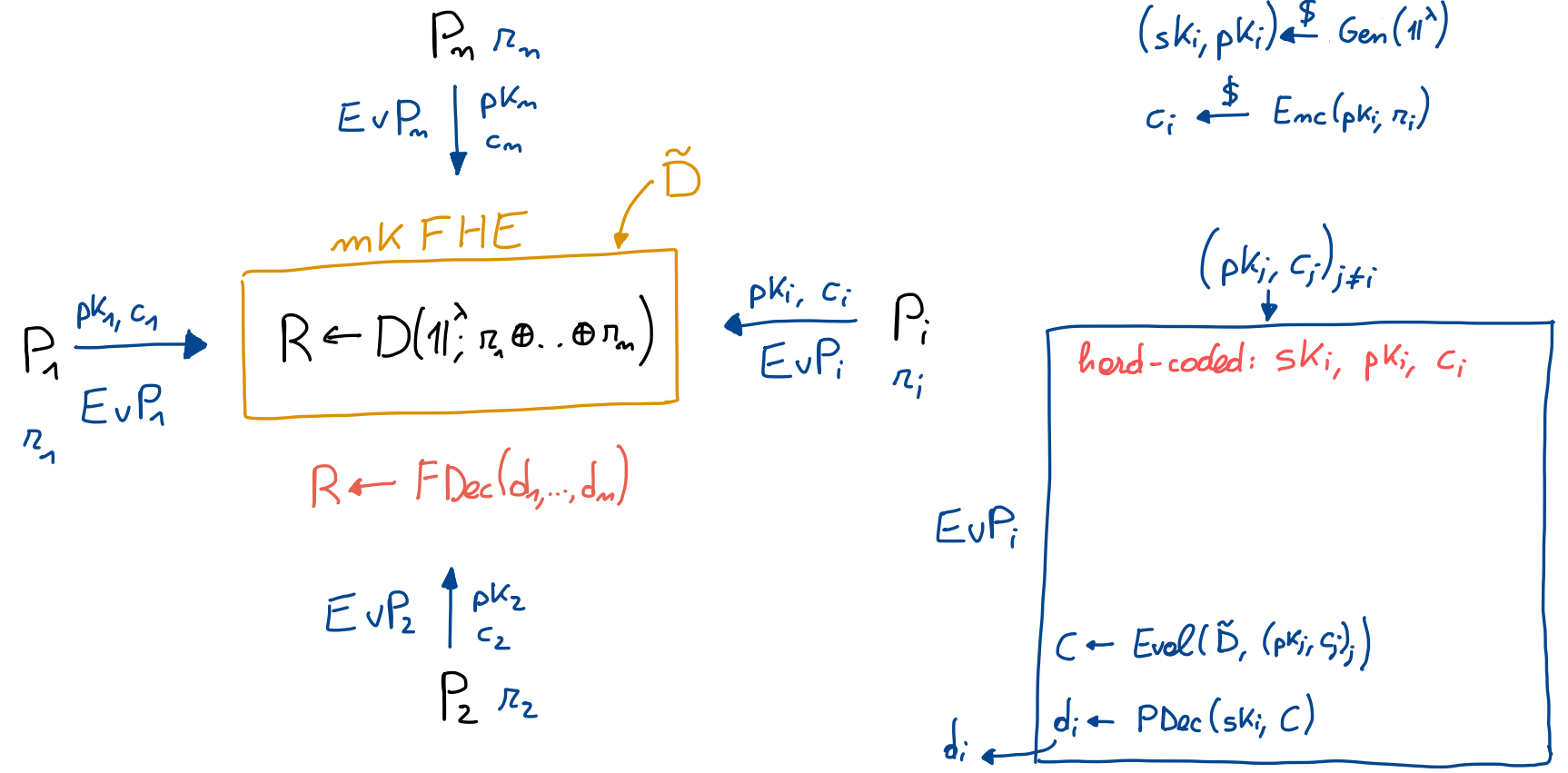
# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT



# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$ $\pi_m$

PROBLEMS

$\pi := \pi_1 \oplus \dots \oplus \pi_m$

$P_1$

$\pi_1$

$P_2$ $\pi_2$

$(sk_i, pk_i) \xleftarrow{\$} Gen(1^\lambda)$

$c_i \xleftarrow{\$} Enc(pk_i, \pi_i)$

$(pk_j, c_j)_{j \neq i}$

$P_i$

$\pi_i$

hard-coded: $sk_i$, $pk_i$, $c_i$

$EvP_i$

$C \leftarrow Eval(\tilde{D}, (pk_j, c_j)_j)$

$d_i \leftarrow PDec(sk_i, C)$

$d_i$

# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$ $r_m$

PROBLEMS

$r := r_1 \oplus \dots \oplus r_m$

$P_1$

$r_1$

$P_2$ $r_2$

$(sk_i, pk_i) \xleftarrow{\$} Gen(1^\lambda)$

$c_i \xleftarrow{\$} Enc(pk_i, r_i)$

$c_1' \xleftarrow{\$} Enc(pk_1, r_1 \oplus e)$

$(pk_j, c_j)_{j \neq i}$

$P_i$

$r_i$

$EvP_i$

hard-coded: $sk_i$, $pk_i$, $c_i$

$C \leftarrow Eval(\tilde{D}, (pk_j, c_j)_j)$

$d_i \leftarrow PDec(sk_i, C)$

$d_i$

# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$ $r_m$

**PROBLEMS**

$r := r_1 \oplus \dots \oplus r_m$

1) $\forall e$ $R_e := D(1^\lambda; r \oplus e)$ is leaked.

$P_1$

$r_1$

$P_2$ $r_2$

$(sk_i, pk_i) \xleftarrow{\$} Gen(1^\lambda)$

$c_i \xleftarrow{\$} Enc(pk_i, r_i)$

$c_1' \xleftarrow{\$} Enc(pk_1, r_1 \oplus e)$

$(pk_j, c_j)_{j \neq i}$

$P_i$

$r_i$

$EvP_i$

hard-coded: $sk_i$, $pk_i$, $c_i$

$C \leftarrow Eval(\tilde{D}, (pk_j, c_j)_j)$

$d_i \leftarrow PDec(sk_i, C)$

$d_i$

# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$ $r_m$

**PROBLEMS**

$r := r_1 \oplus \dots \oplus r_m$

1) $\forall e$ $R_e := D(1^\lambda; r \oplus e)$ is leaked.

$P_1$ $r_1$

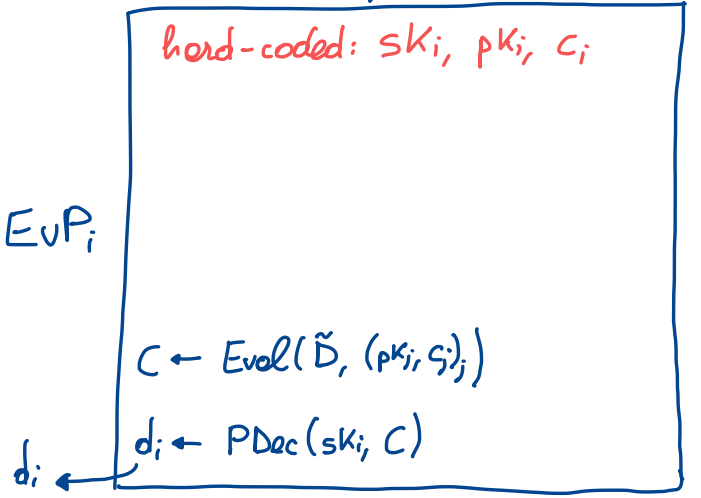
$P_2$ $r_2$

$P_i$ $r_i$

$(sk_i, pk_i) \xleftarrow{\$} Gen(1^\lambda)$

$c_i \xleftarrow{\$} Enc(pk_i, r_i)$

$(pk_j, c_j)_{j \neq i}$



# SEMI-MALICIOUS CONSTRUCTION

## 1st ATTEMPT

$P_m$ $\pi_m$

**PROBLEMS**

$\pi := \pi_1 \oplus \dots \oplus \pi_m$

1) $\forall e$ $R_e := D(1^\lambda; \pi \oplus e)$ is leaked.

2) removing $sk_i$ from $EvP_i$ requires exponentially many hybrids.

$P_1$ $\pi_1$

$P_2$ $\pi_2$

$P_i$ $\pi_i$

$(sk_i, pk_i) \xleftarrow{\$} Gen(1^\lambda)$

$c_i \xleftarrow{\$} Enc(pk_i, \pi_i)$

$(pk_j, c_j)_{j \neq i}$

$EvP_i$

hard-coded: $sk_i$, $pk_i$, $c_i$

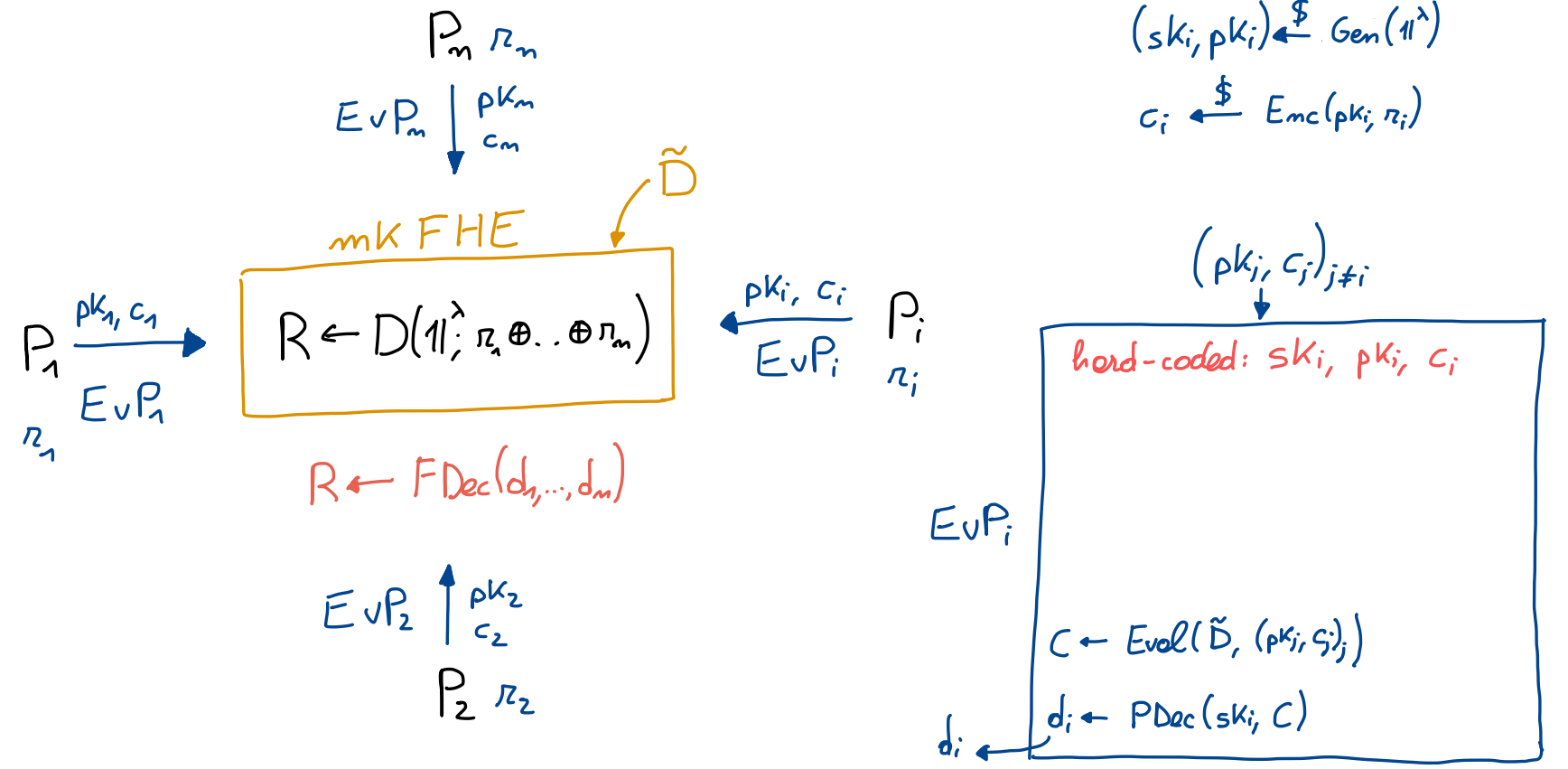
$C \leftarrow Eval(\tilde{D}, (pk_j, c_j)_j)$

$d_i \leftarrow PDec(sk_i, C)$

$d_i$

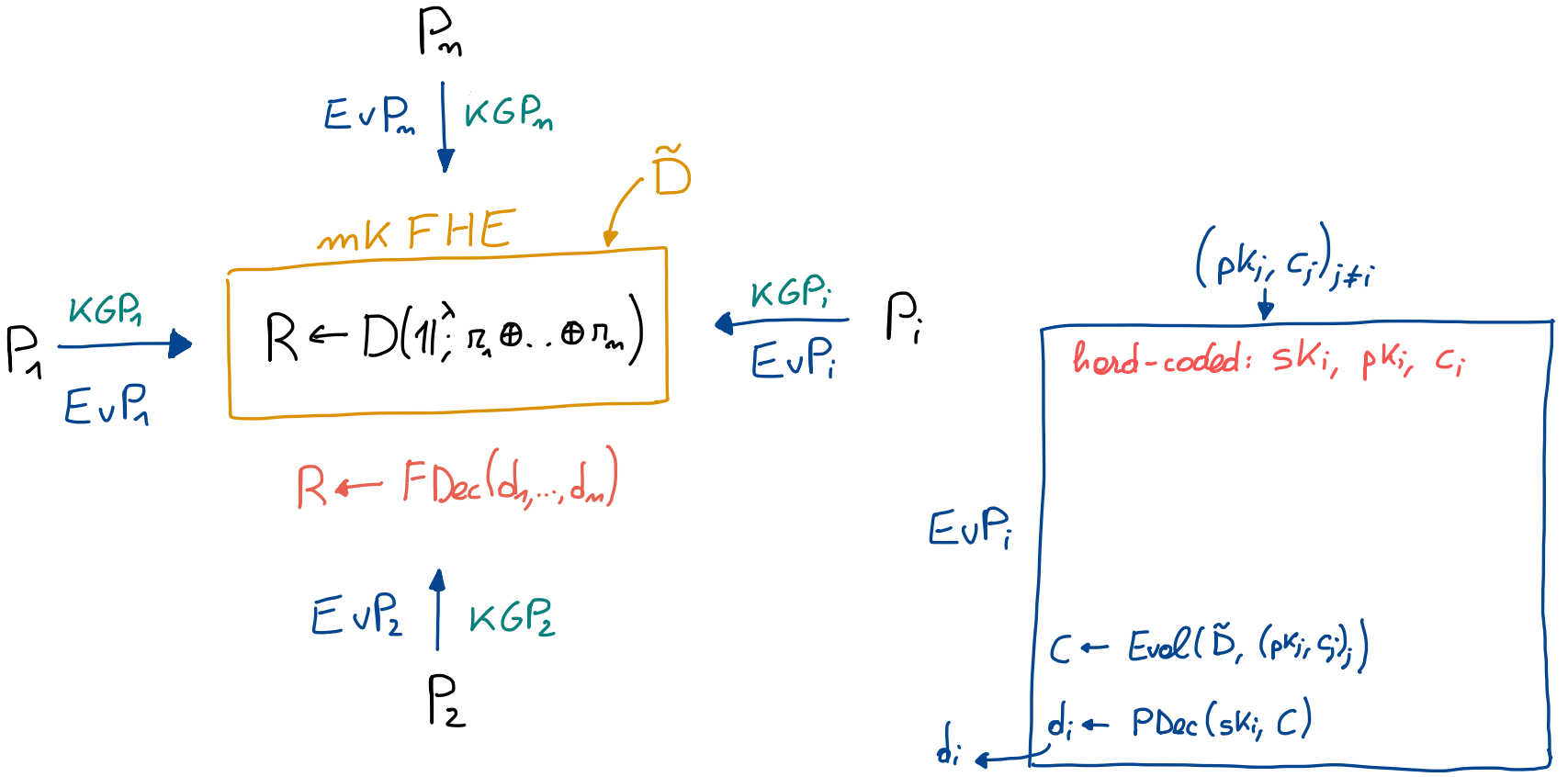
# SEMI-MALICIOUS CONSTRUCTION

## 2nd ATTEMPT



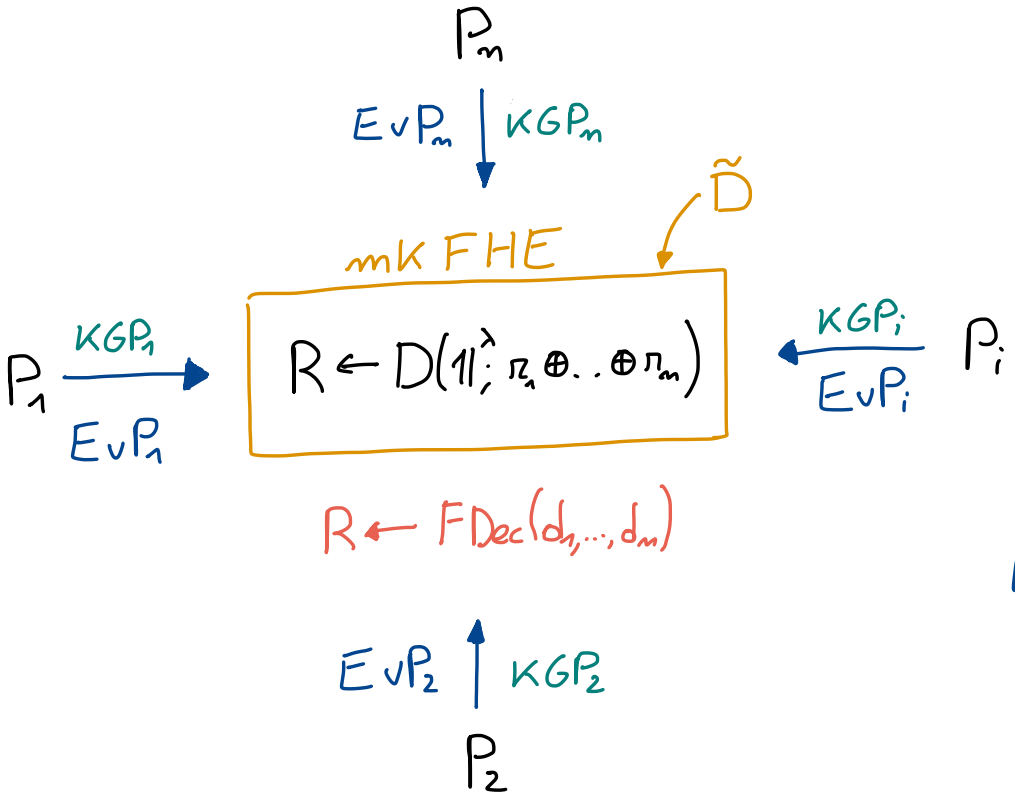
# SEMI-MALICIOUS CONSTRUCTION

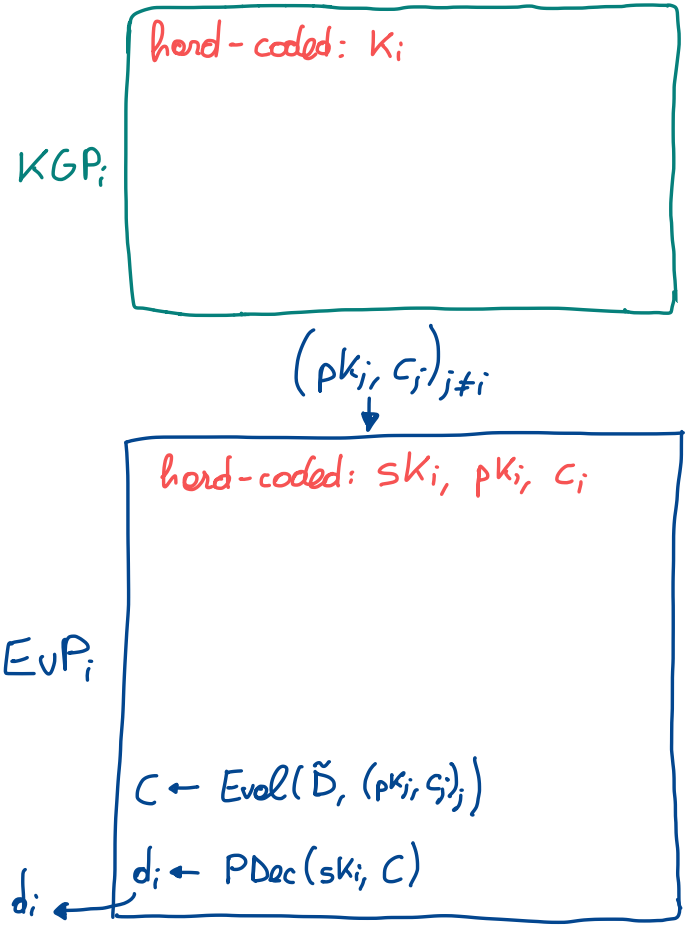
## 2nd ATTEMPT



# SEMI-MALICIOUS CONSTRUCTION

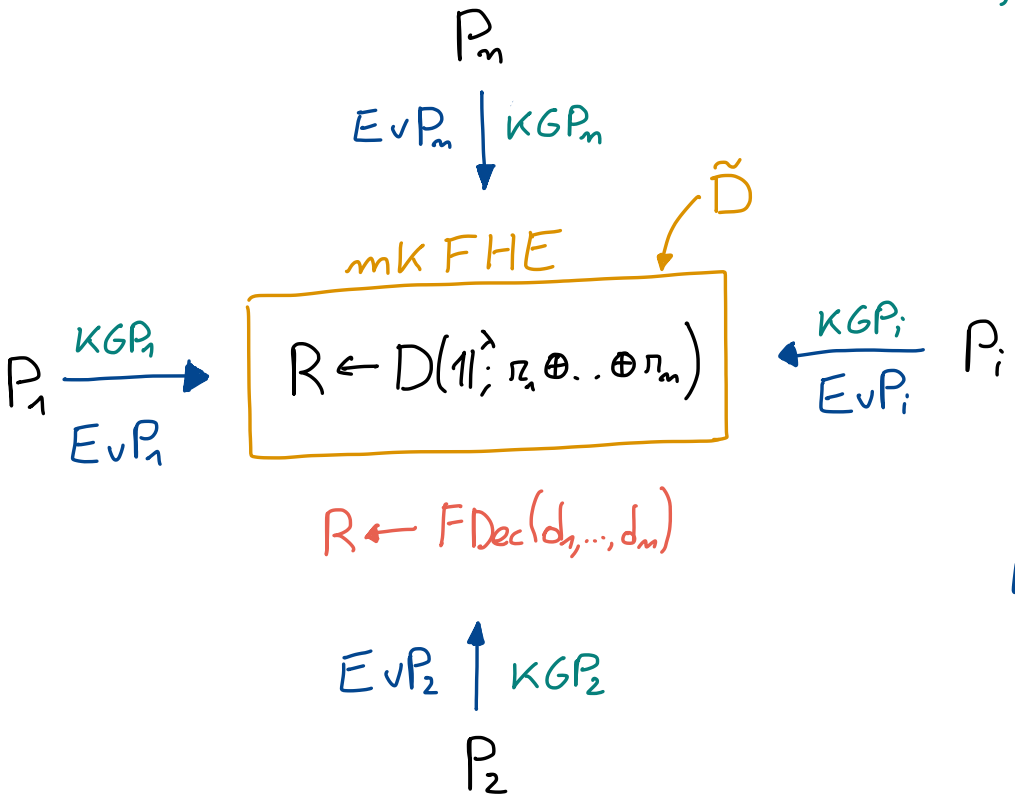
## 2nd ATTEMPT

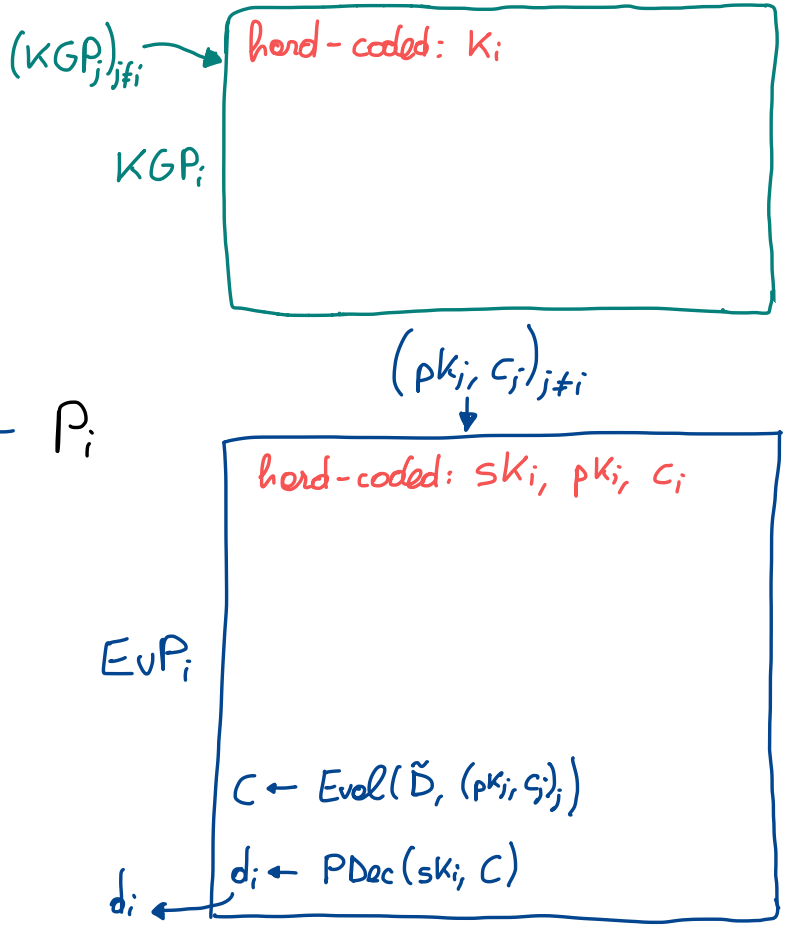


# SEMI-MALICIOUS CONSTRUCTION

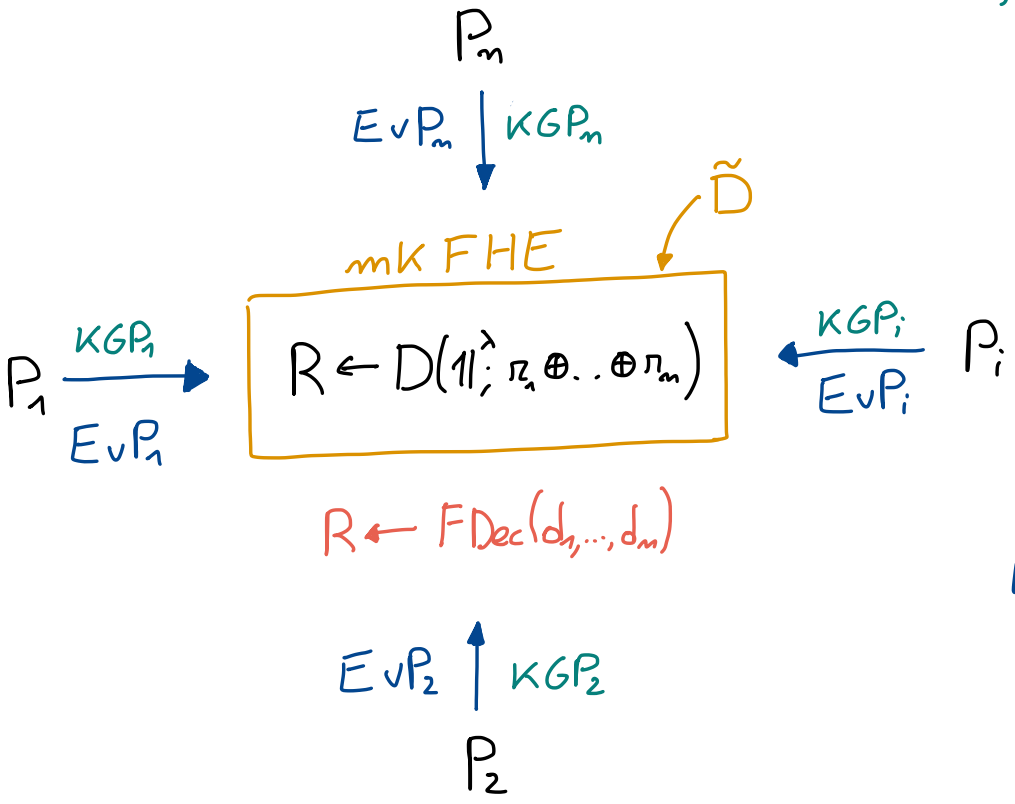
## 2nd ATTEMPT

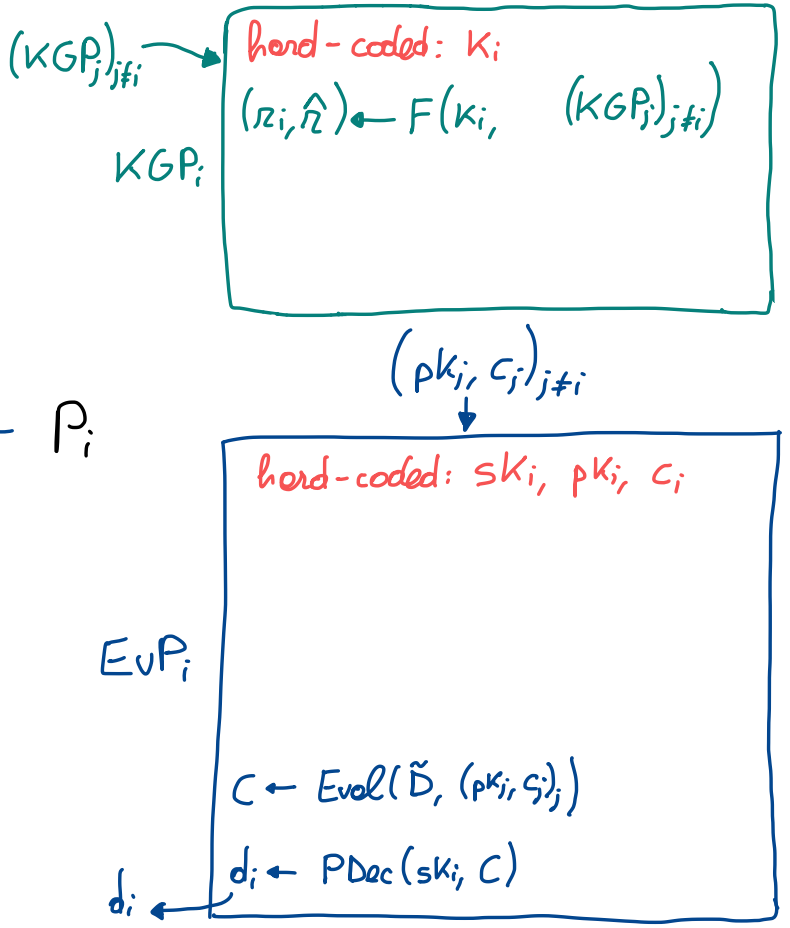


# SEMI-MALICIOUS CONSTRUCTION

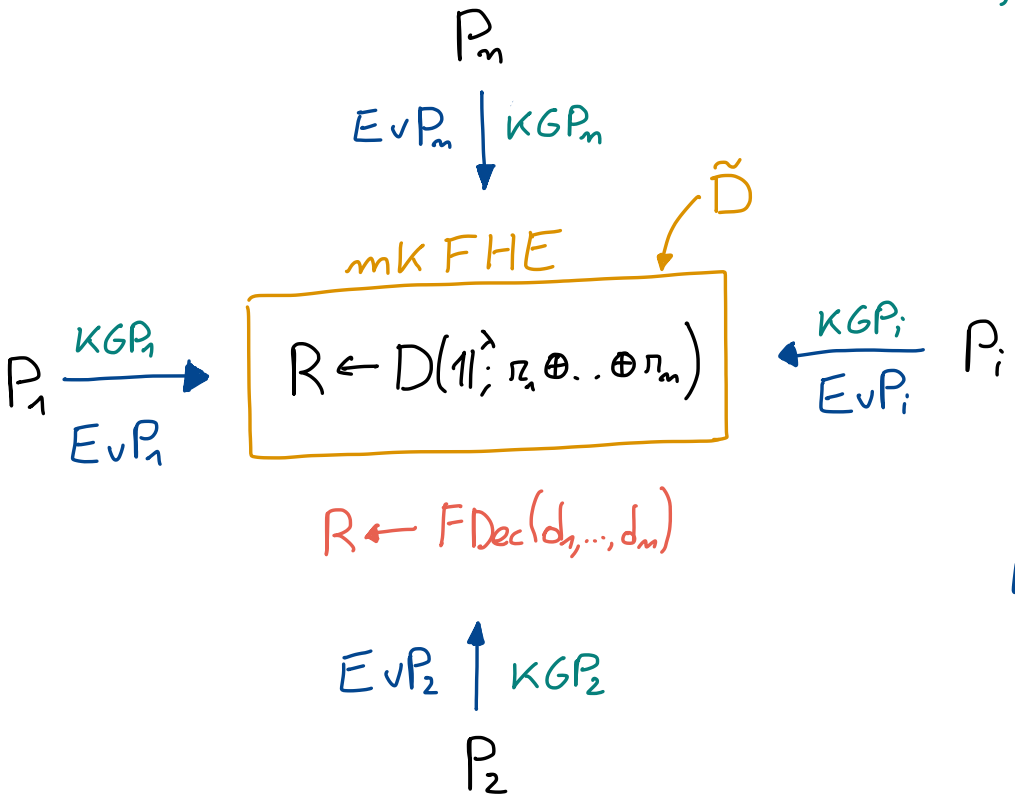
## 2nd ATTEMPT

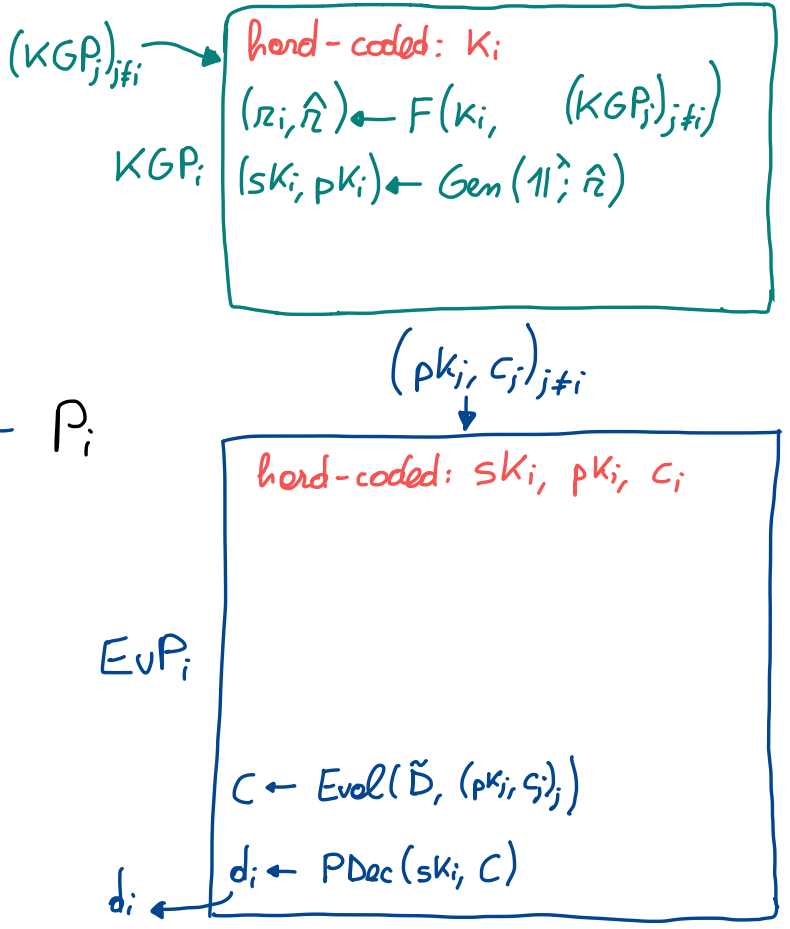


# SEMI-MALICIOUS CONSTRUCTION

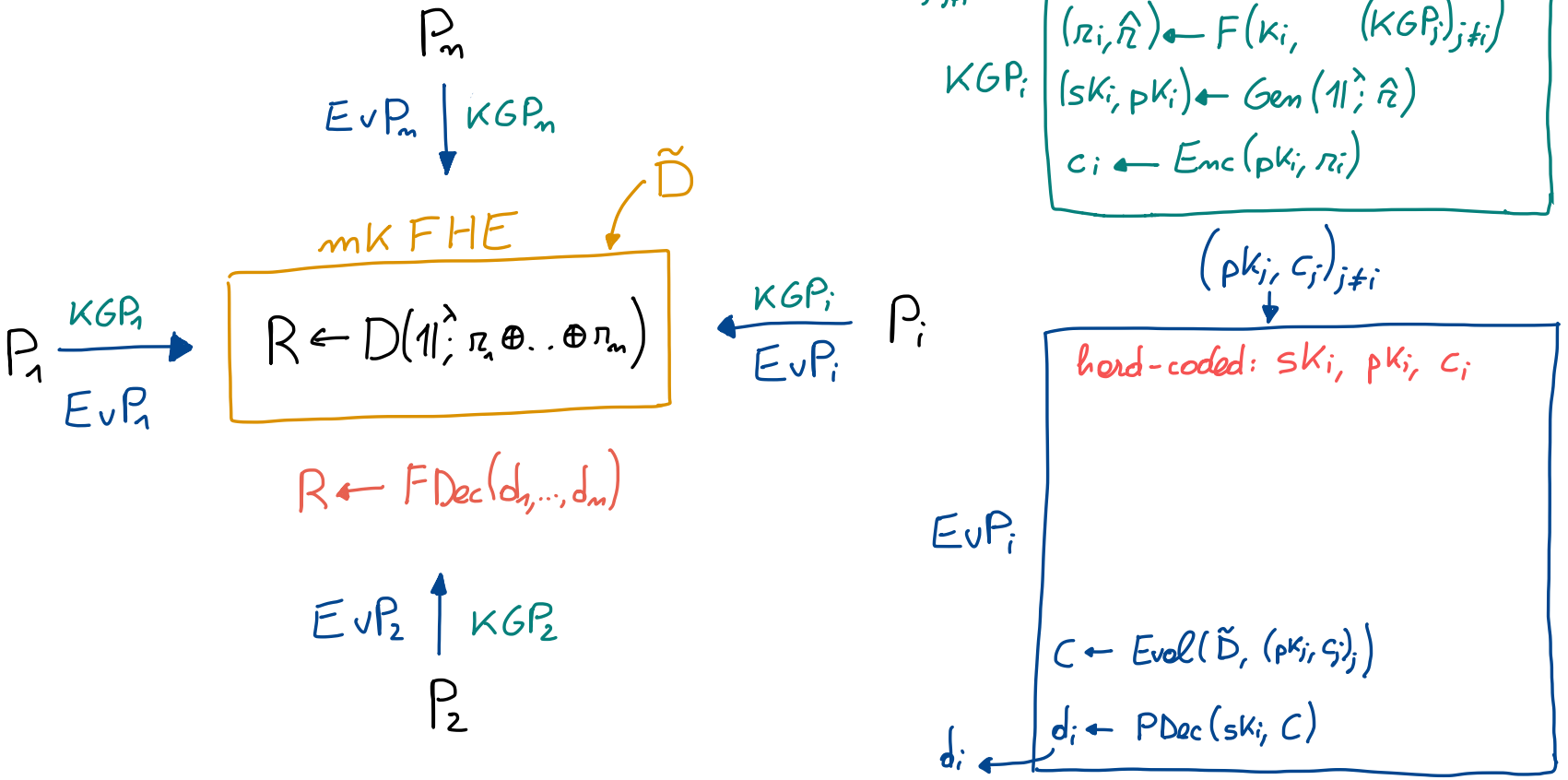
## 2nd ATTEMPT



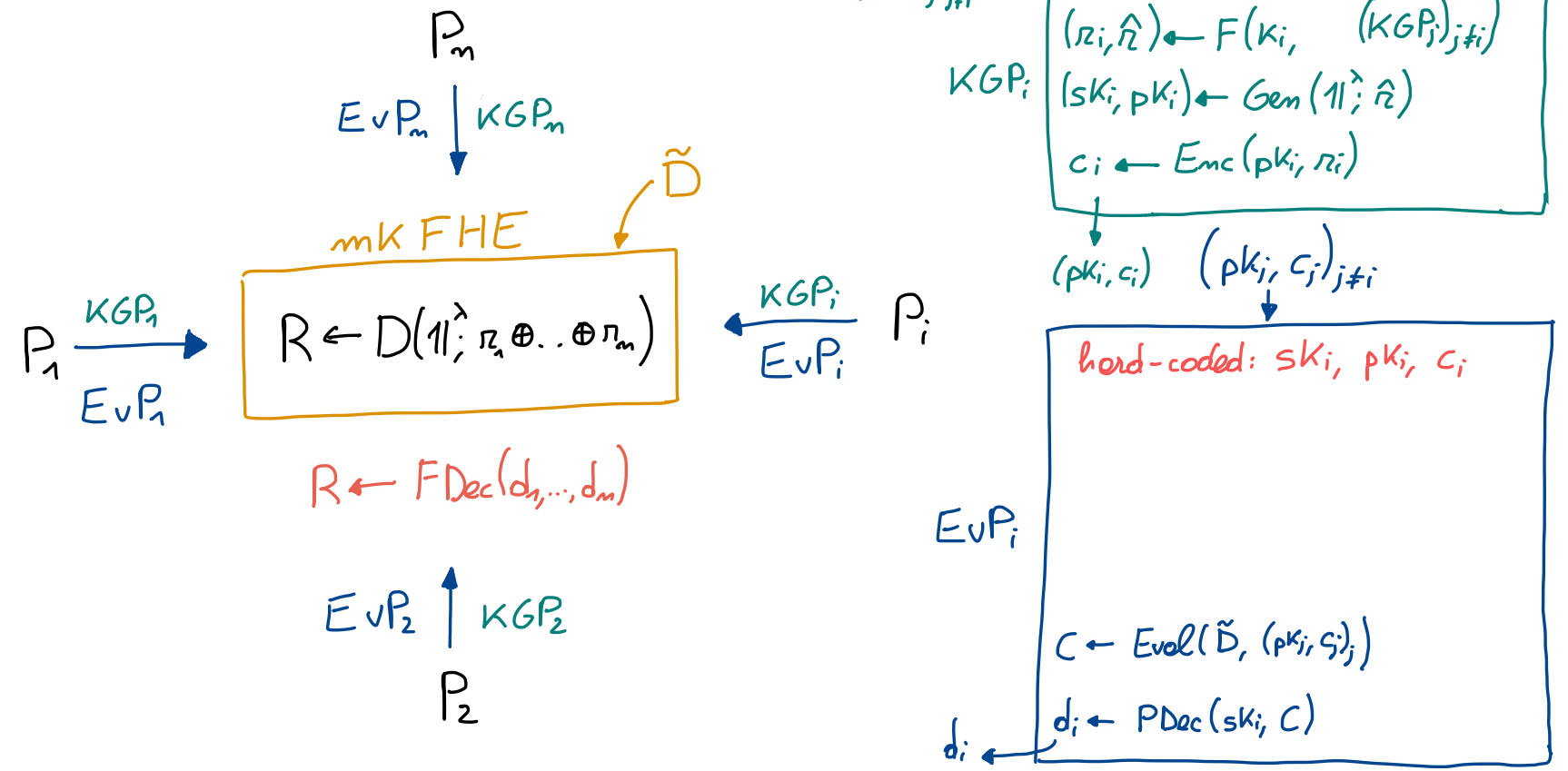
# SEMI-MALICIOUS CONSTRUCTION

## 2nd ATTEMPT



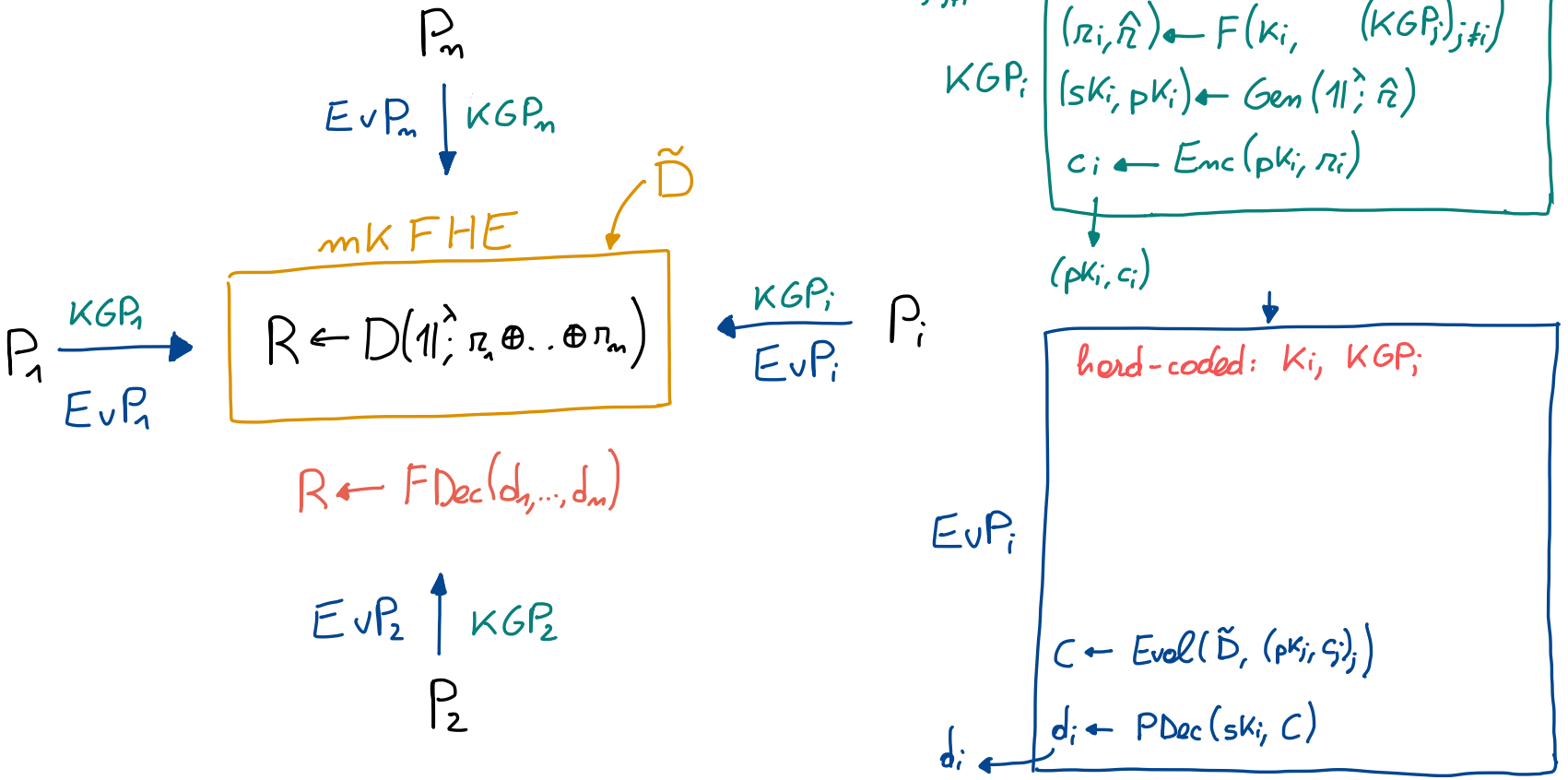
# SEMI-MALICIOUS CONSTRUCTION

2nd ATTEMPT



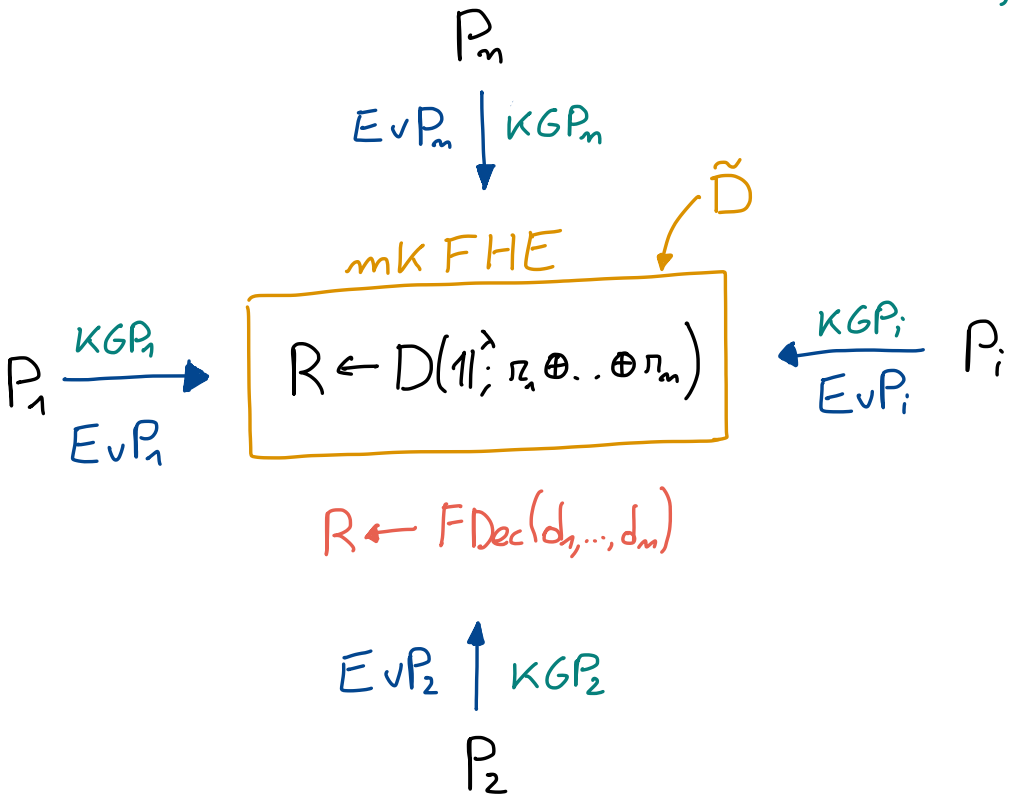
# SEMI-MALICIOUS CONSTRUCTION

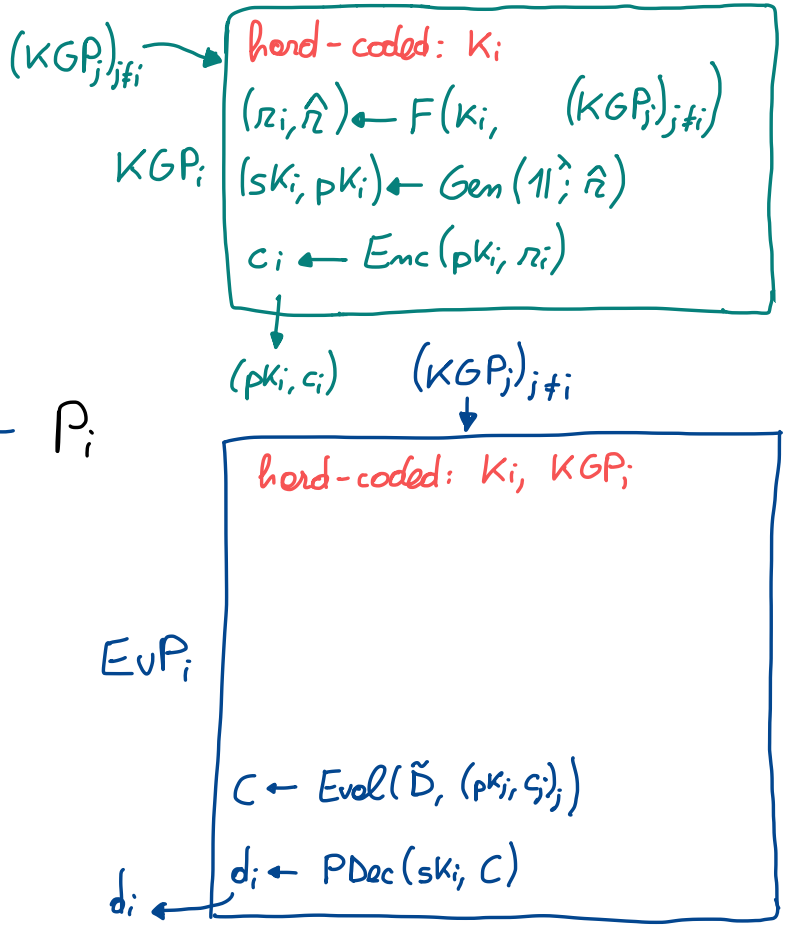
## 2nd ATTEMPT



# SEMI-MALICIOUS CONSTRUCTION

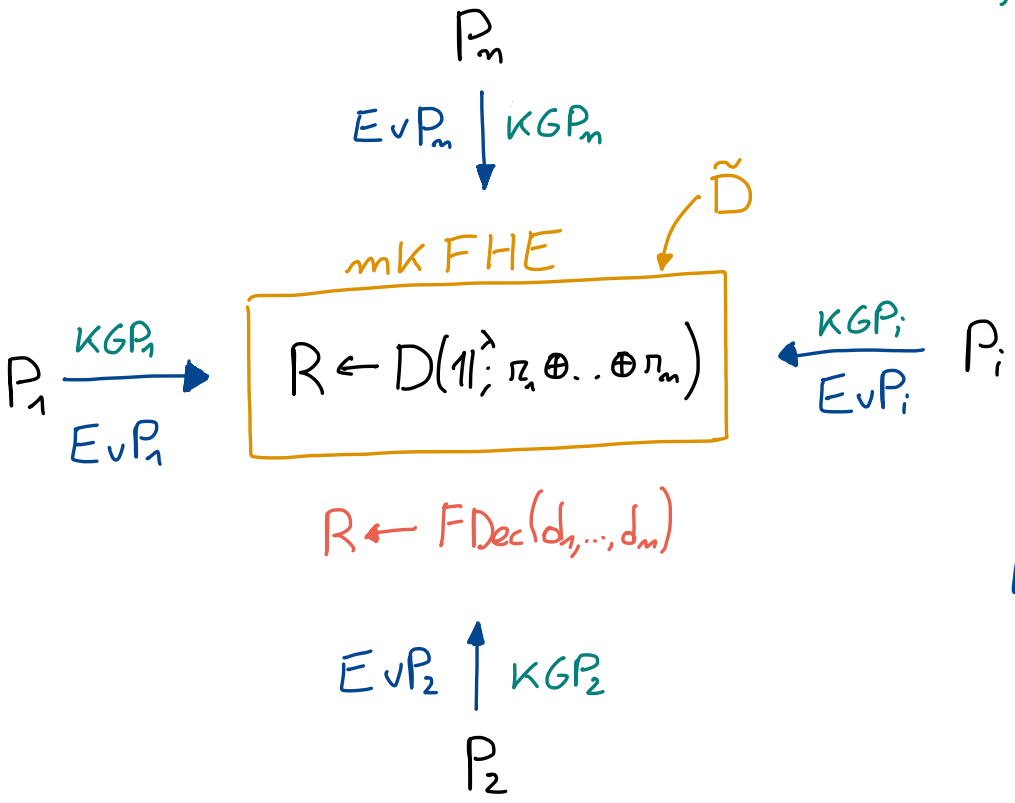
## 2nd ATTEMPT

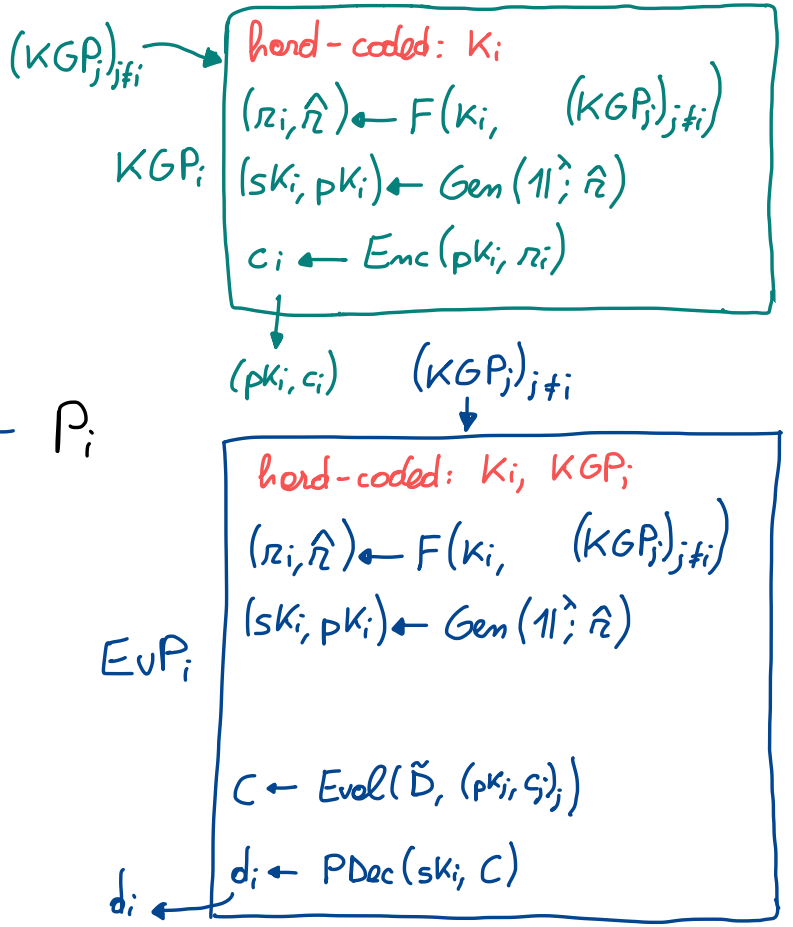


# SEMI-MALICIOUS CONSTRUCTION

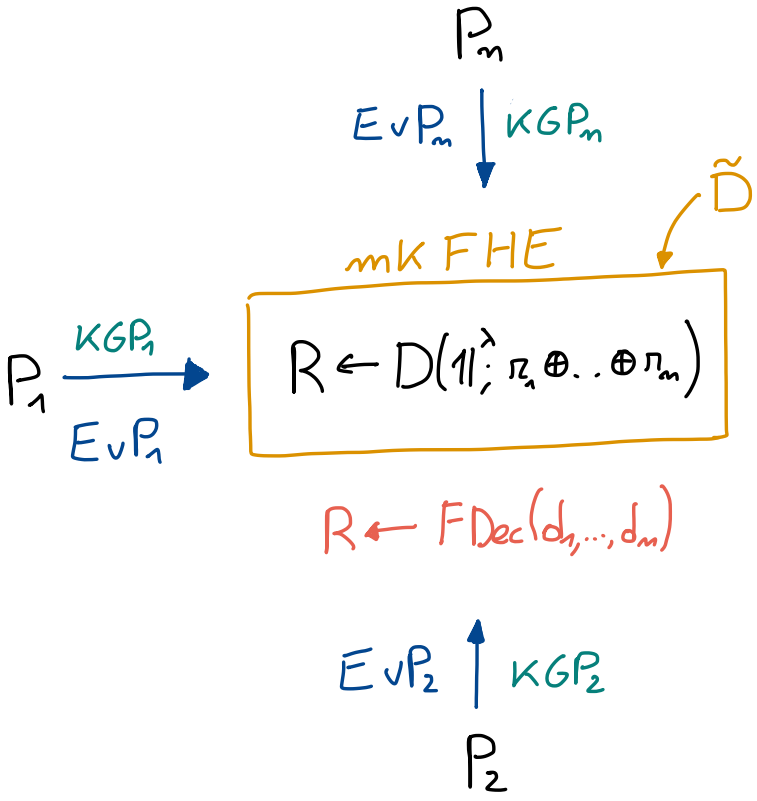
## 2nd ATTEMPT

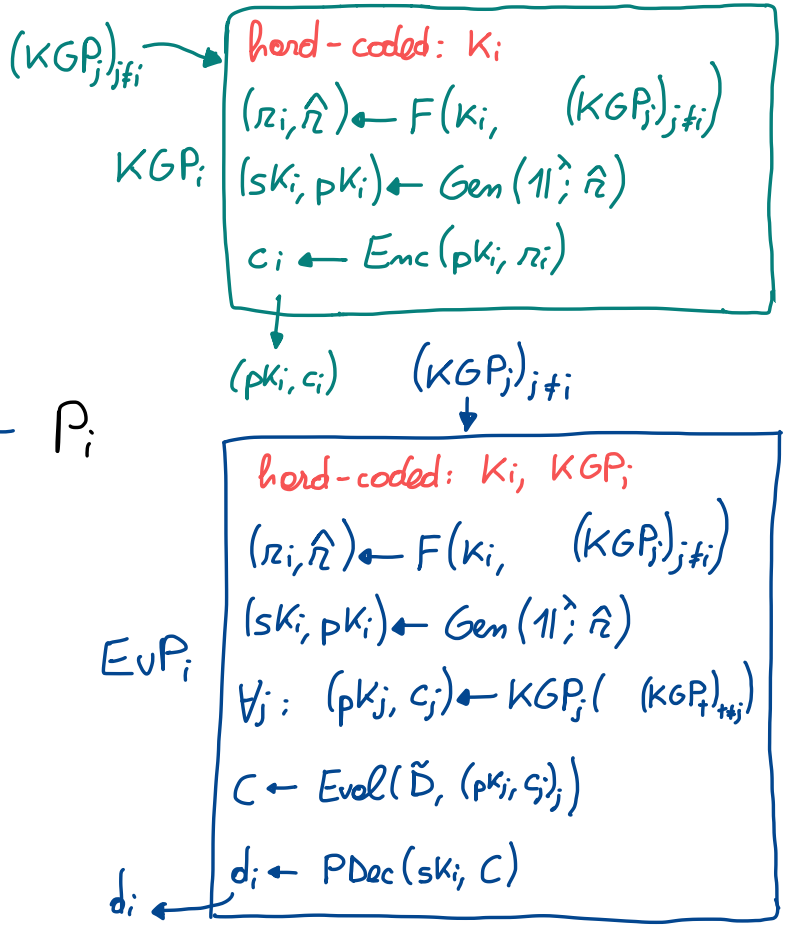


# SEMI-MALICIOUS CONSTRUCTION

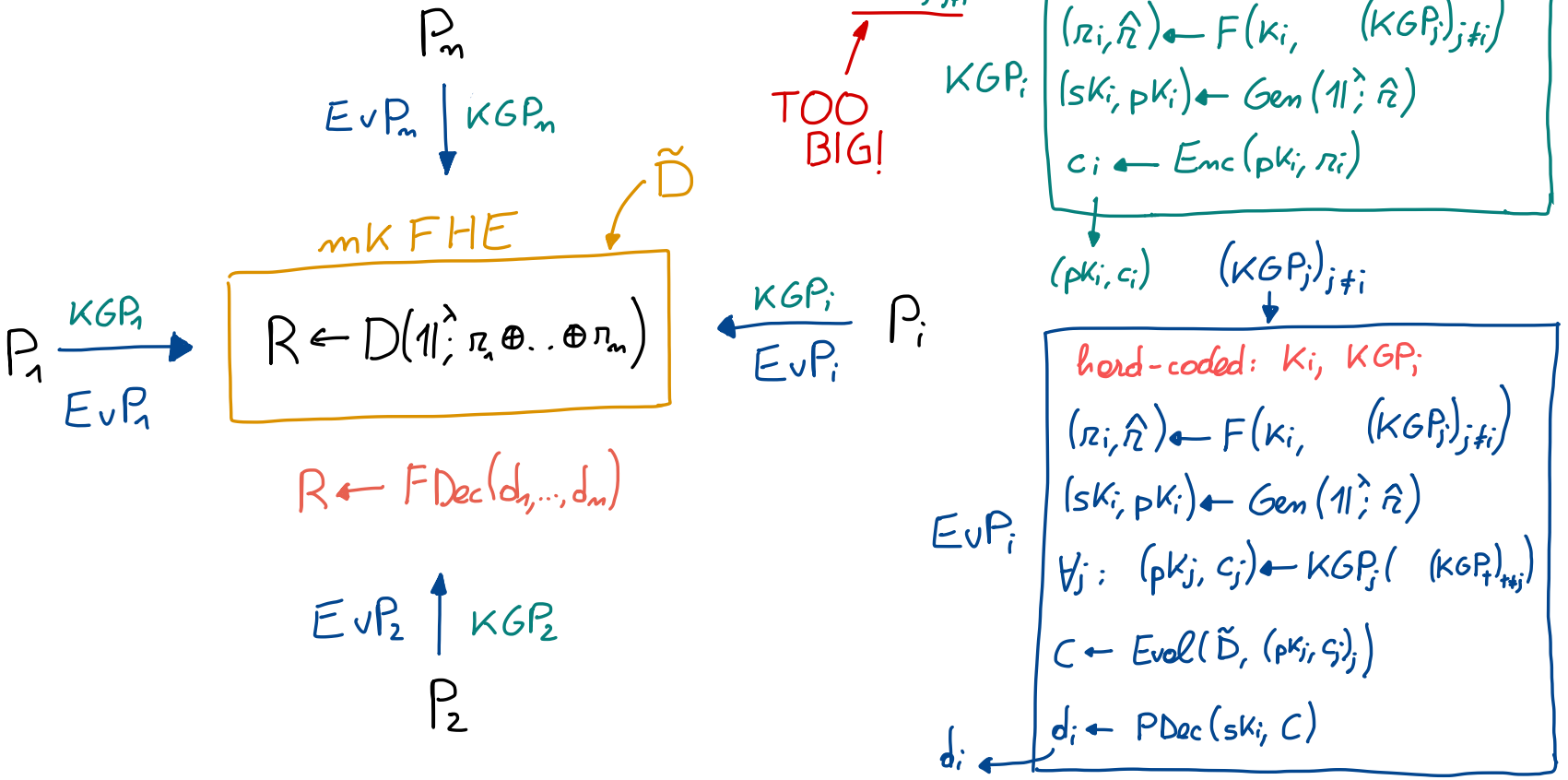
## 2nd ATTEMPT



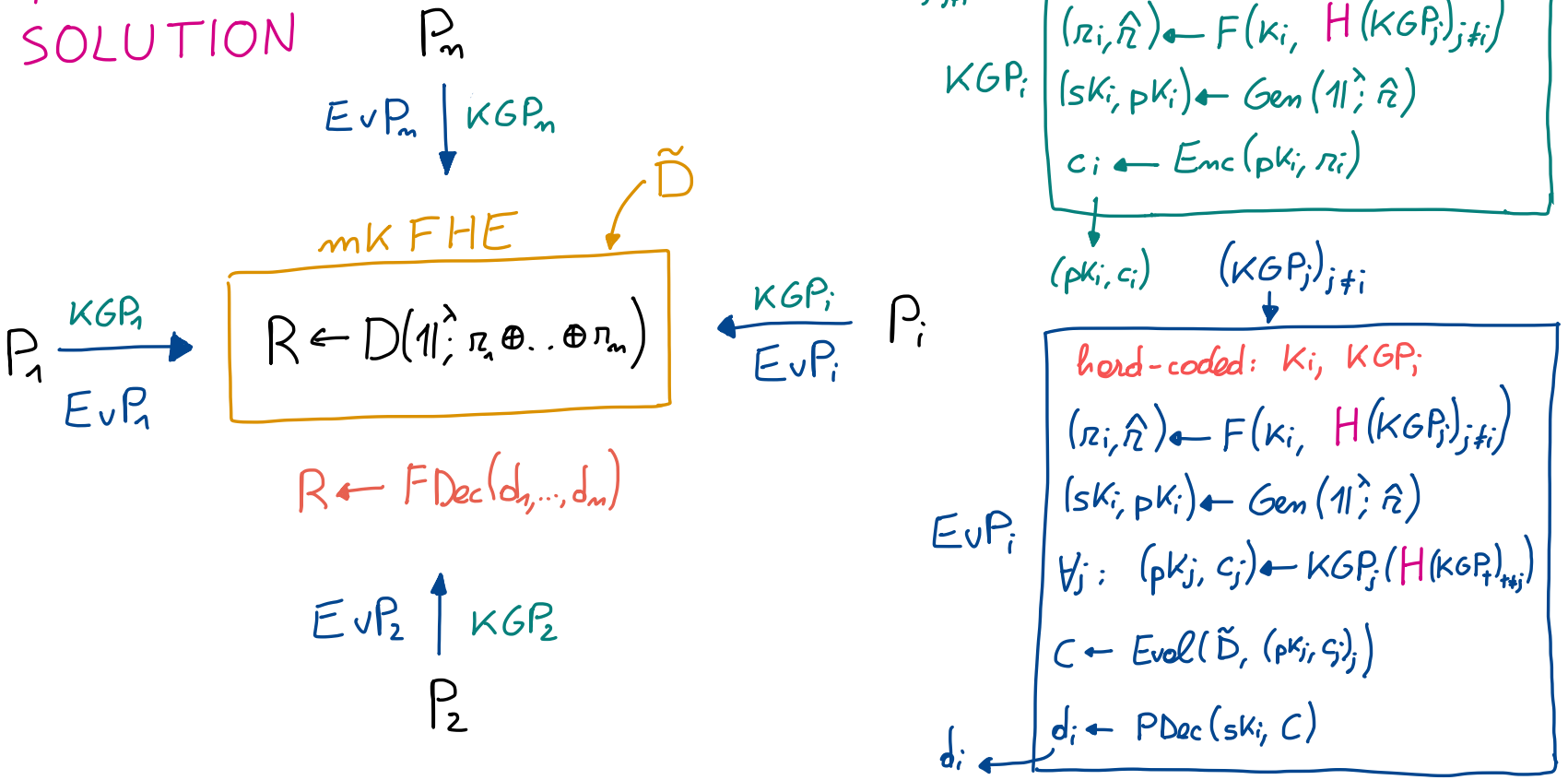
# SEMI-MALICIOUS CONSTRUCTION

## 2nd ATTEMPT



# SEMI-MALICIOUS CONSTRUCTION

## FINAL SOLUTION



# DISTRIBUTED SAMPLERS

## NON-RUSHING SEMI-MALICIOUS ✓

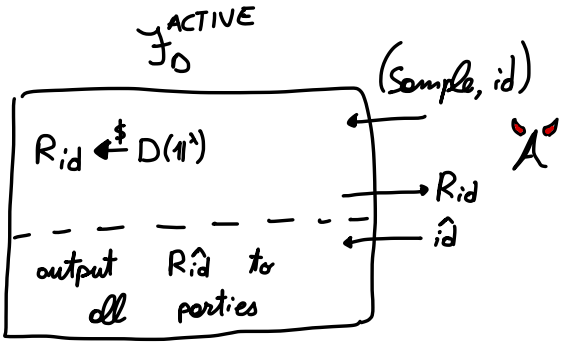
$\mathcal{F}_D$

$R \xleftarrow{\$} D(1^\lambda)$

output $R$ to all parties

- any distribution $D$
- in the PLAIN MODEL
- from polynomial $i\mathcal{O}$ and polynomial multi-key FHE

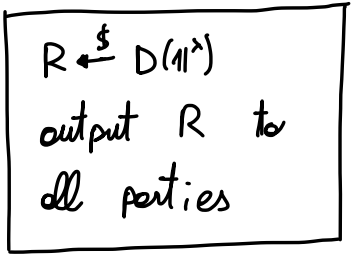
## ACTIVE




- any distribution $D$
- in the RANDOM ORACLE MODEL
- from polynomial $i\mathcal{O}$
  polynomial multi-key FHE
  polynomial NIZK

# DISTRIBUTED SAMPLERS

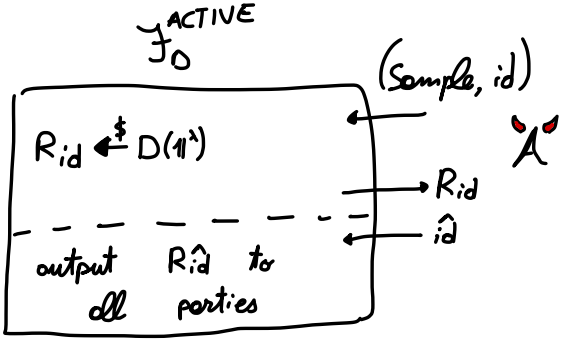
NON-RUSHING
SEMI-MALICIOUS ✓




ANTI-RUSHER COMPILER

using delayed backdoor programming [HJK+16]

ACTIVE



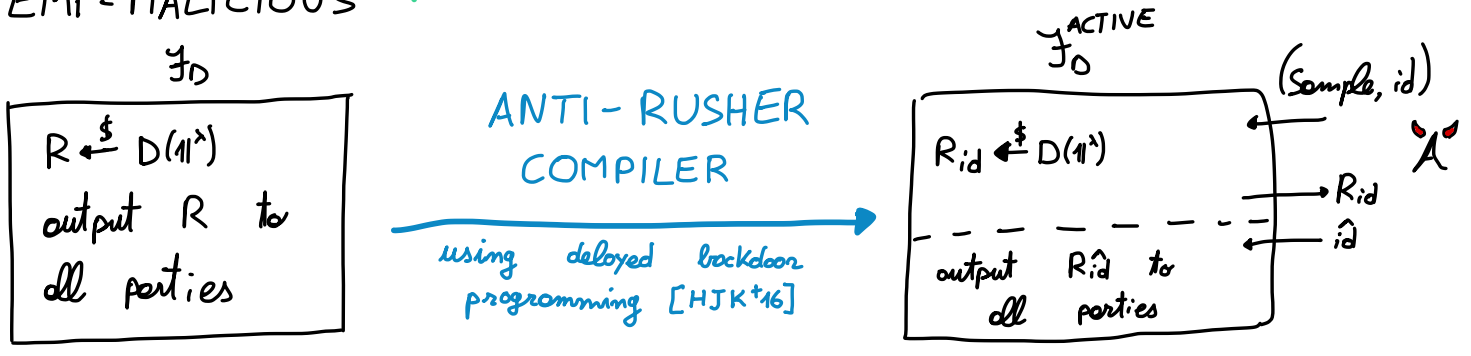

- any distribution D
- in the PLAIN MODEL
- from polynomial iO and polynomial multi-key FHE

- any distribution D
- in the RANDOM ORACLE MODEL
- from polynomial iO
  polynomial multi-key FHE
  polynomial NIZK

# DISTRIBUTED SAMPLERS

NON-RUSHING
SEMI-MALICIOUS ✓

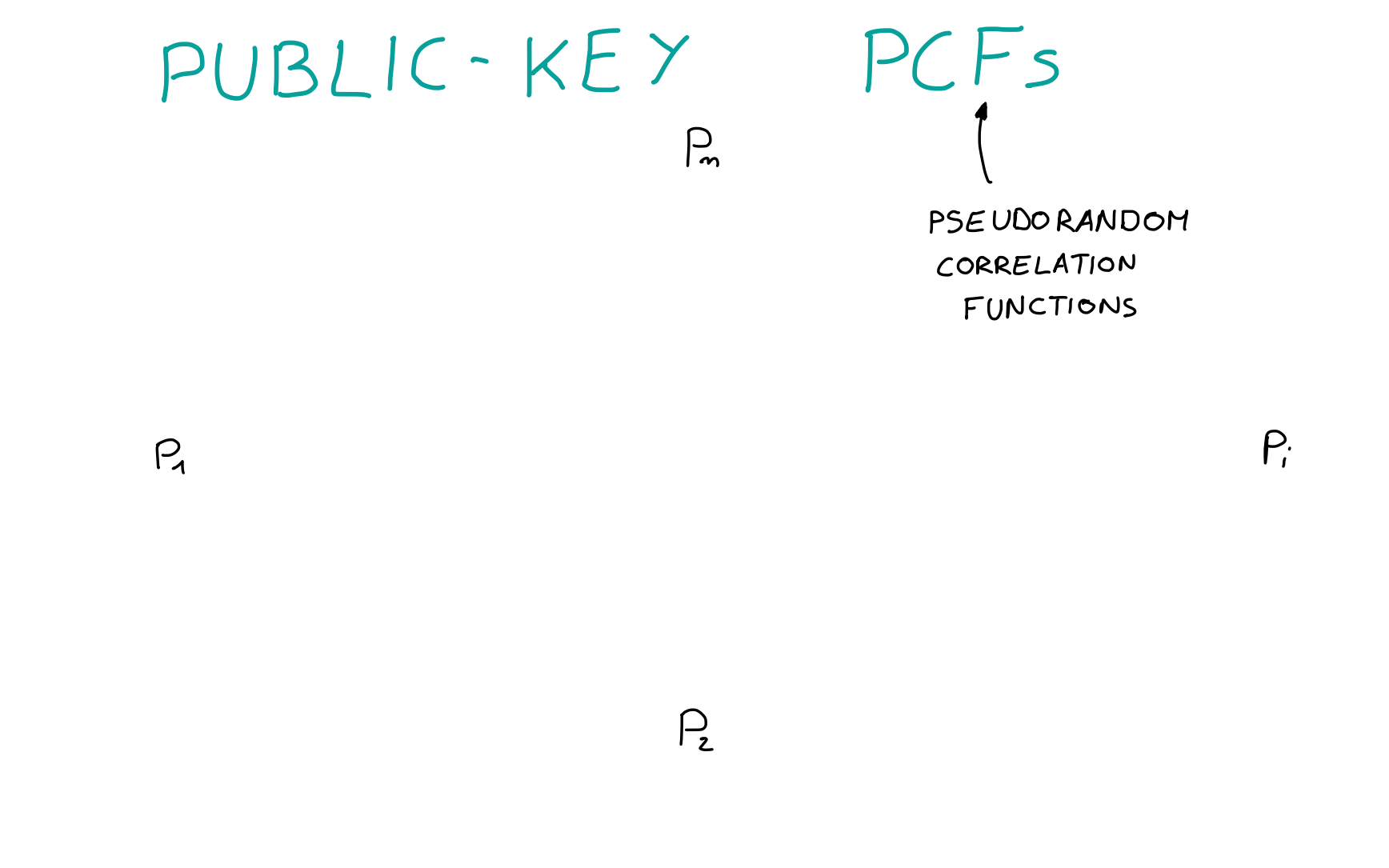
ACTIVE ✓




- any distribution D
- in the PLAIN MODEL
- from polynomial iO and polynomial multi-key FHE

- any distribution D
- in the RANDOM ORACLE MODEL
- from polynomial iO
  polynomial multi-key FHE
  polynomial NIZK

# PUBLIC-KEY PCFs



# PUBLIC-KEY PCFs

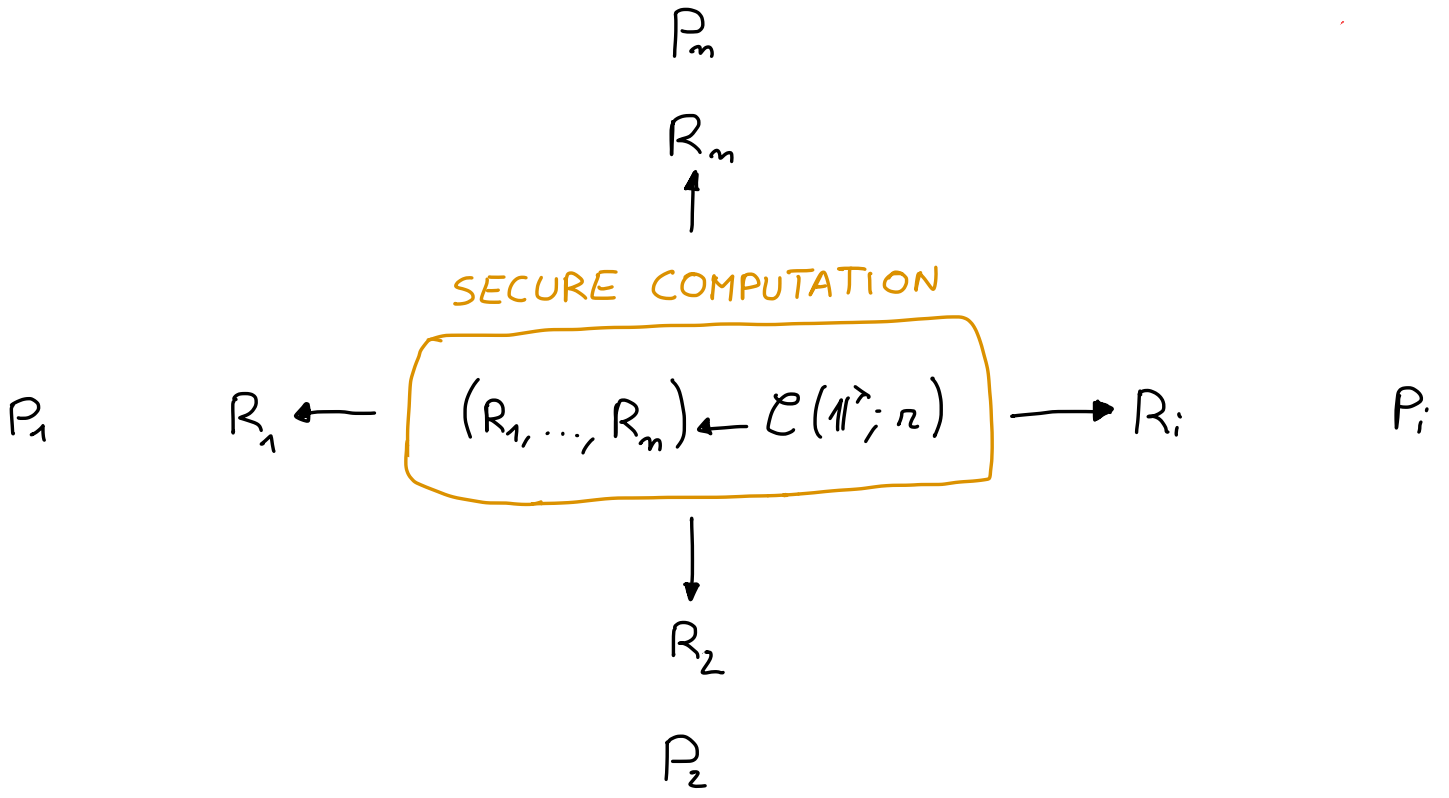
$P_m$

PSEUDORANDOM CORRELATION FUNCTIONS

$P_1$ $(R_1, \ldots, R_n) \leftarrow \mathcal{C}(1^\lambda; r)$ $P_i$

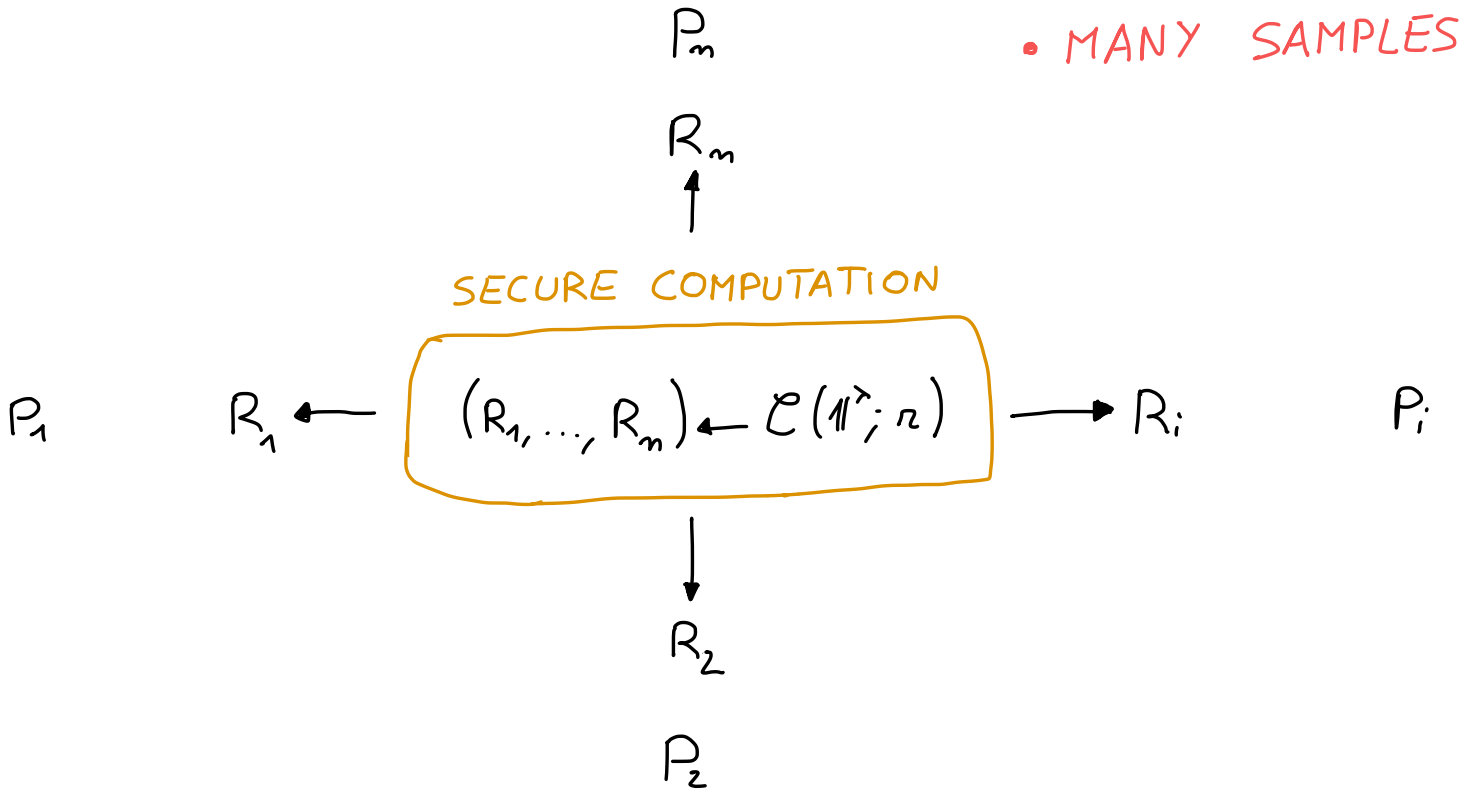
$P_2$

# PUBLIC-KEY PCFs



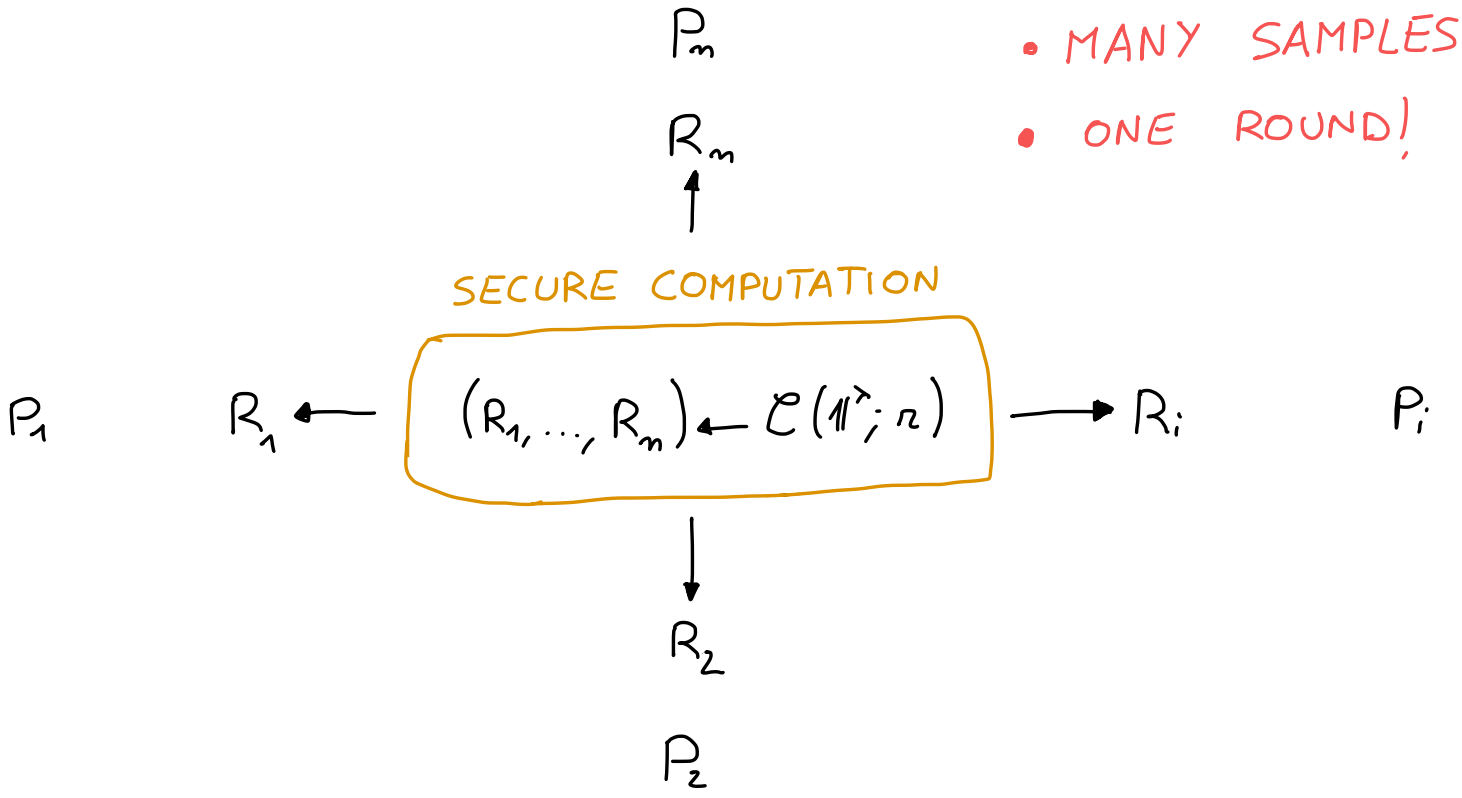
# PUBLIC-KEY PCFs

- MANY SAMPLES!



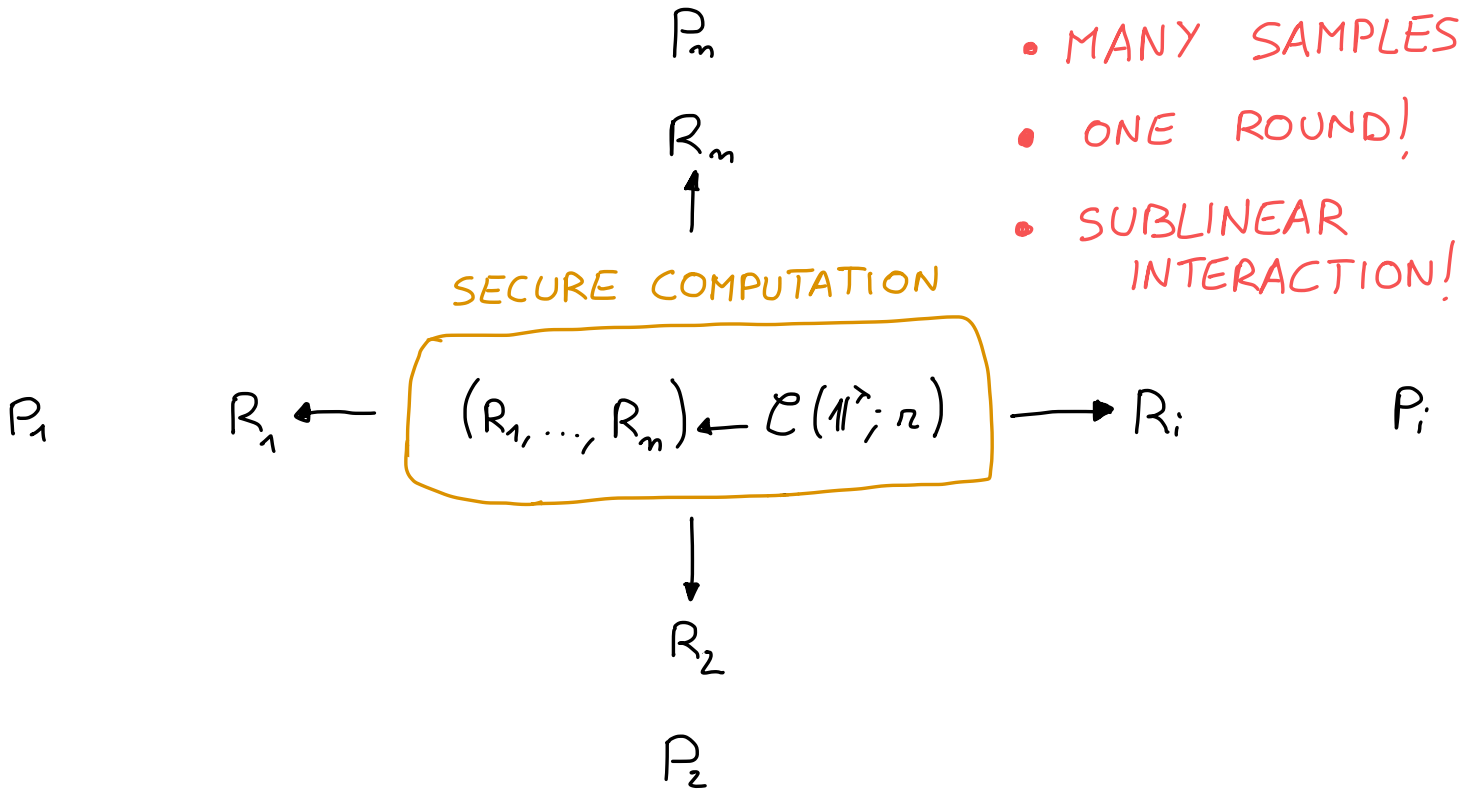
# PUBLIC-KEY PCFs

- MANY SAMPLES!
- ONE ROUND!



# PUBLIC-KEY PCFs

- MANY SAMPLES!
- ONE ROUND!
- SUBLINEAR INTERACTION!



# PUBLIC-KEY PCFs

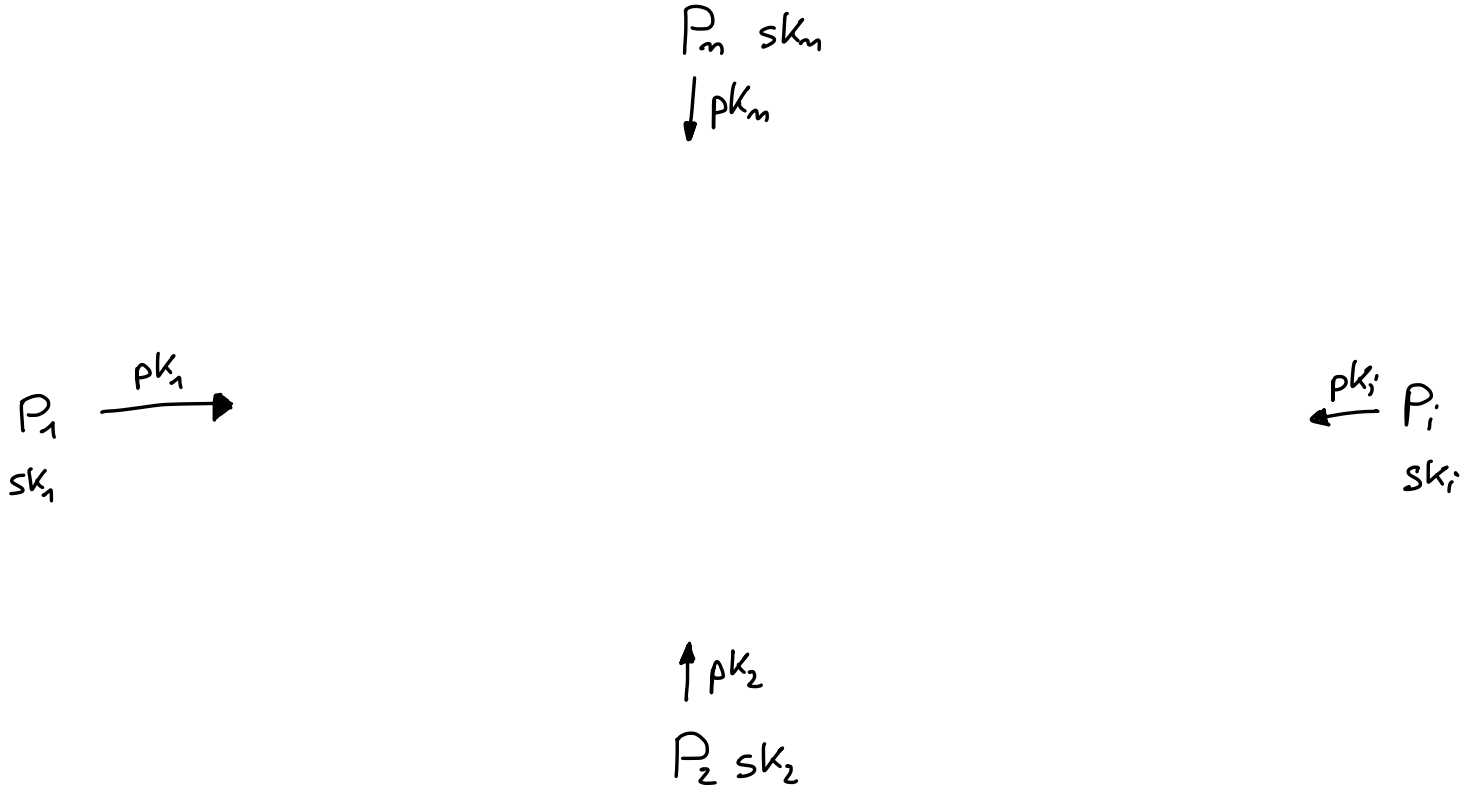
$P_m$

$P_1$

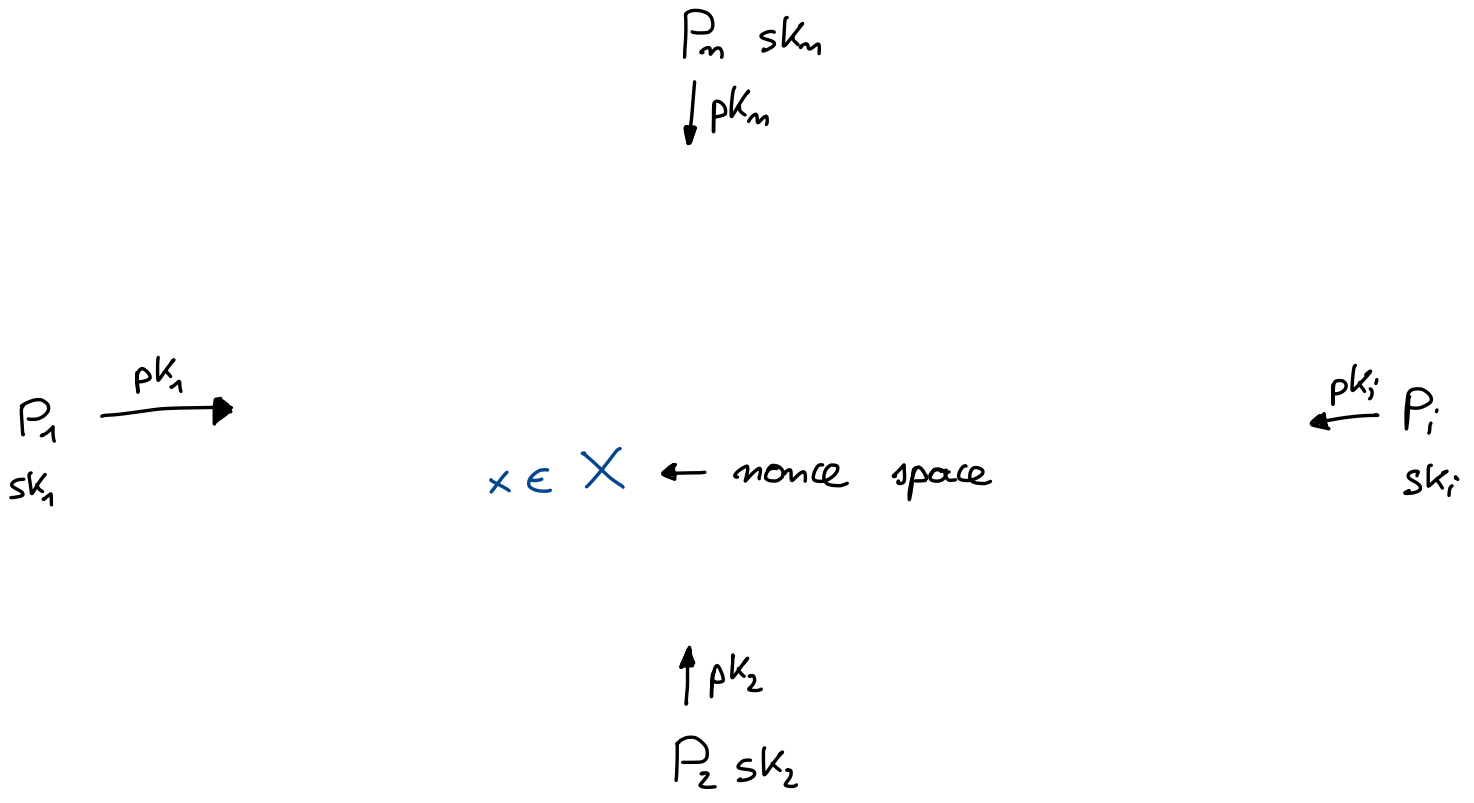
$P_i$

$P_2$

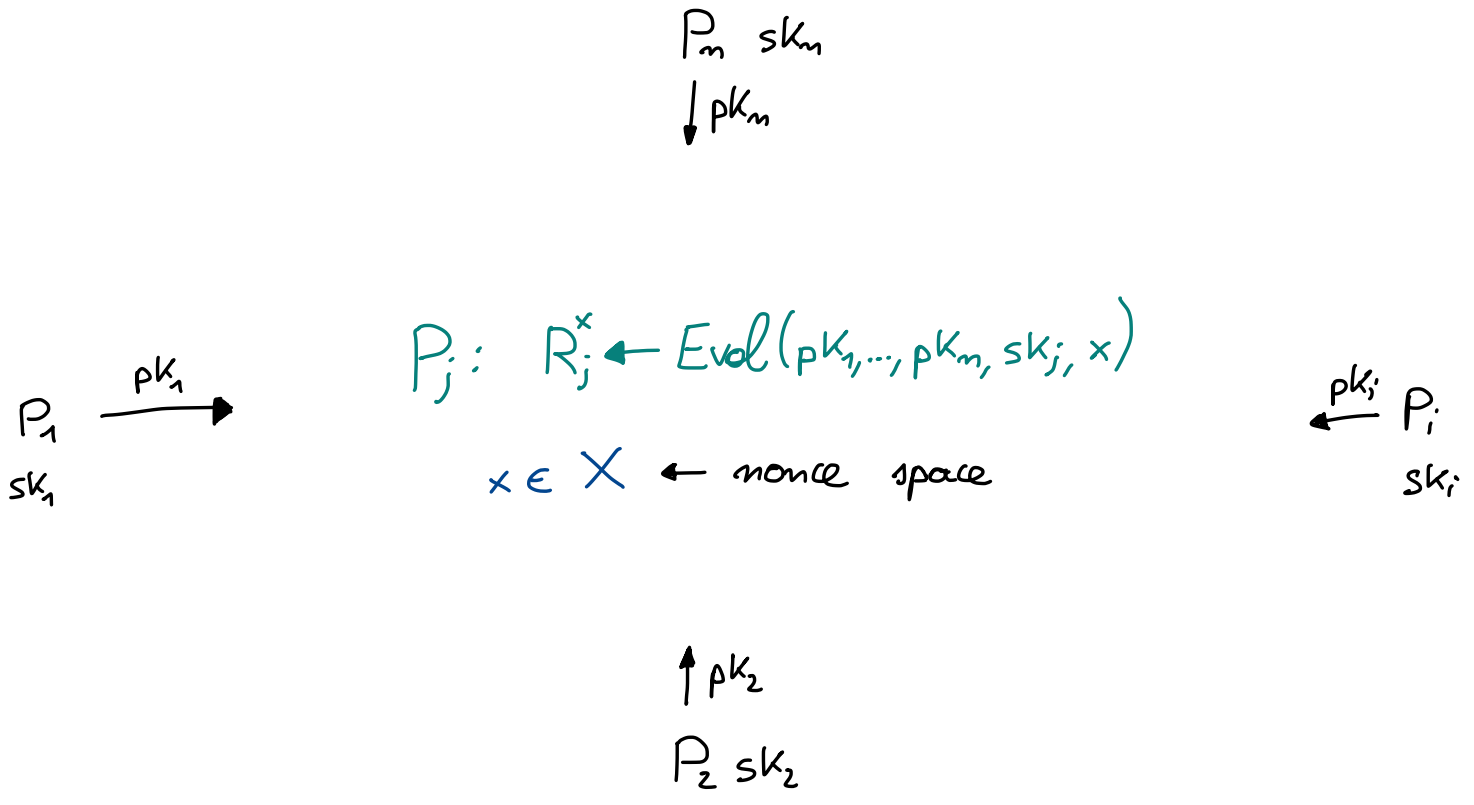
# PUBLIC-KEY PCFs



# PUBLIC-KEY PCFs



# PUBLIC-KEY PCFs



# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS

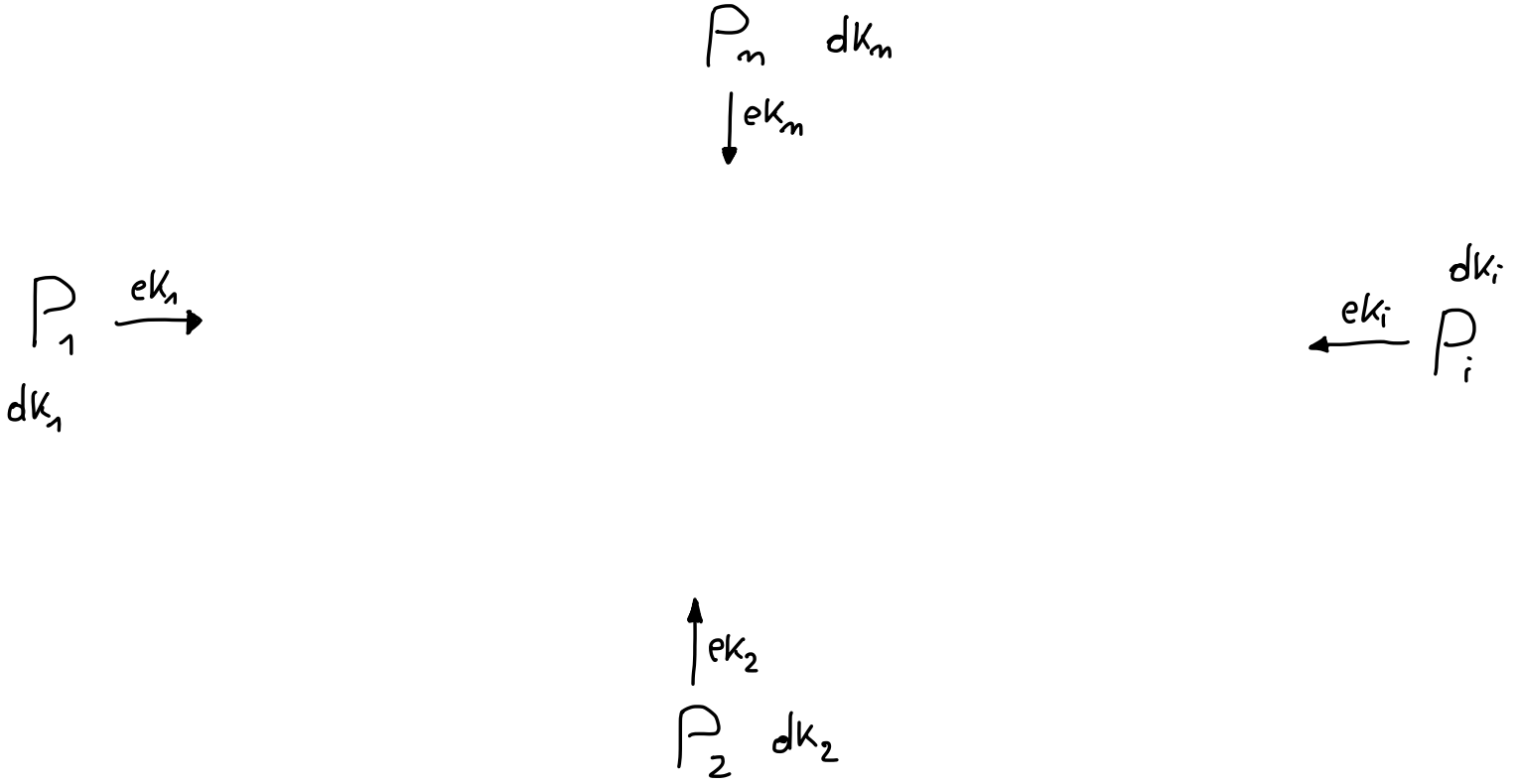
$P_n$

$P_1$

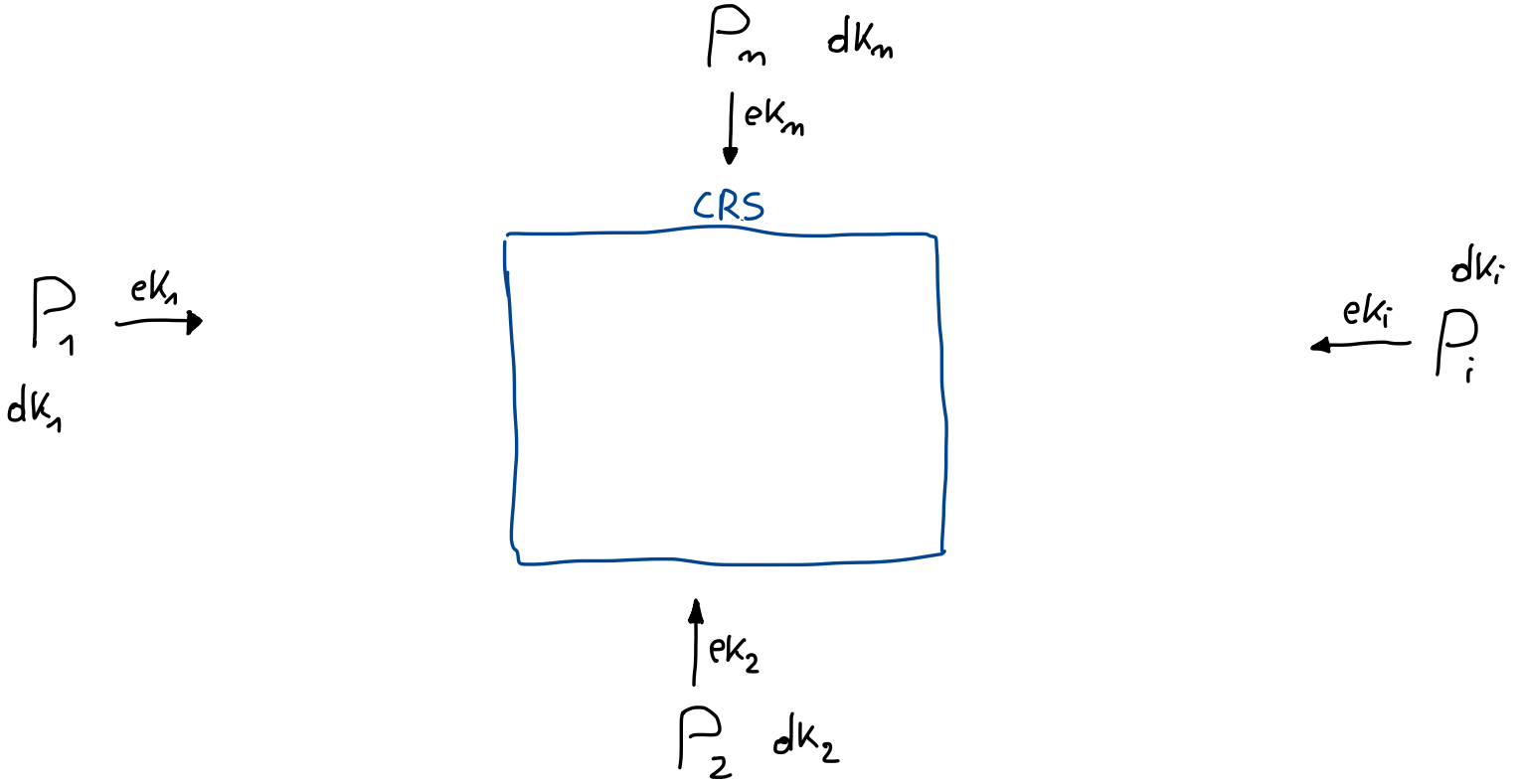
$P_i$

$P_2$

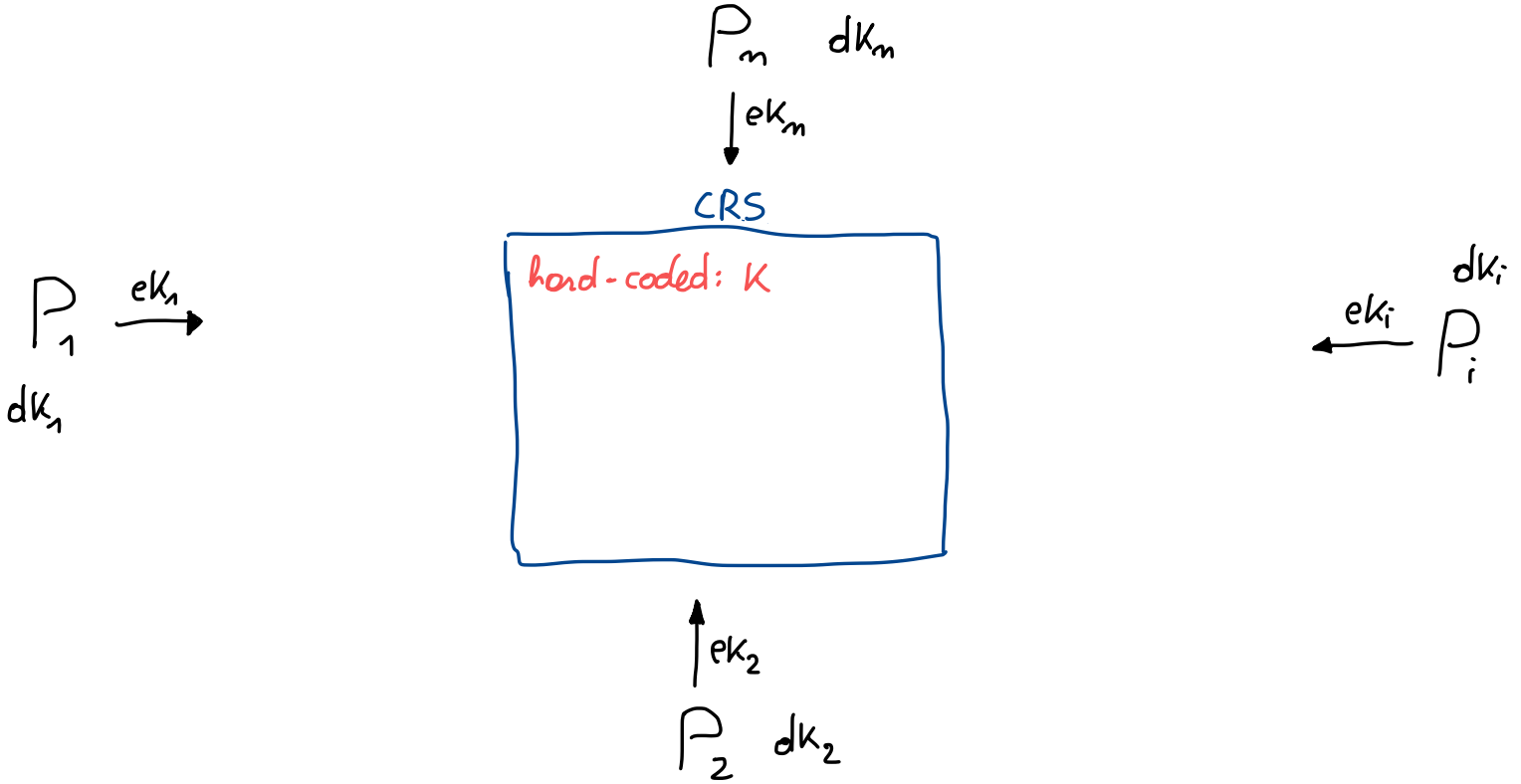
# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



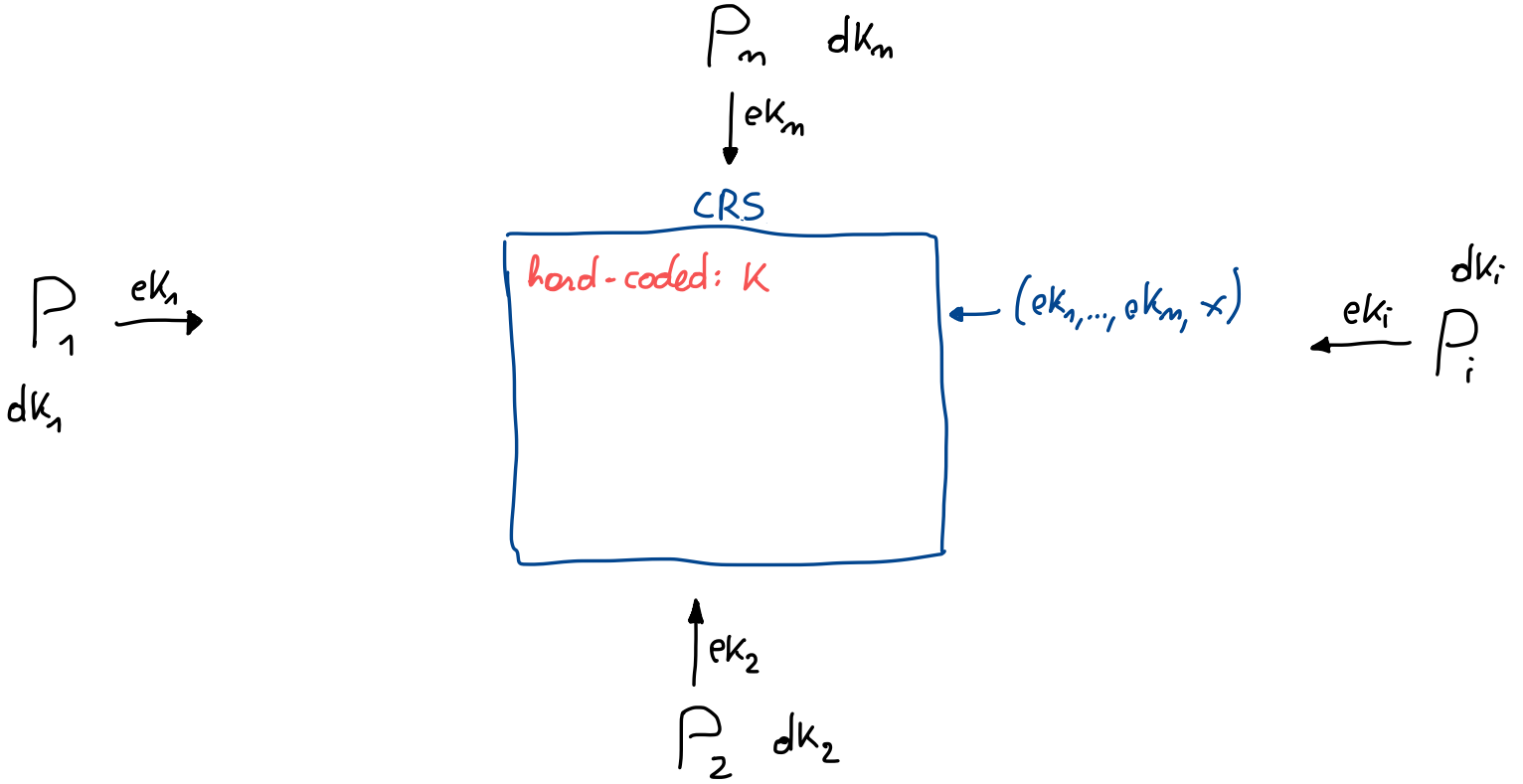
# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



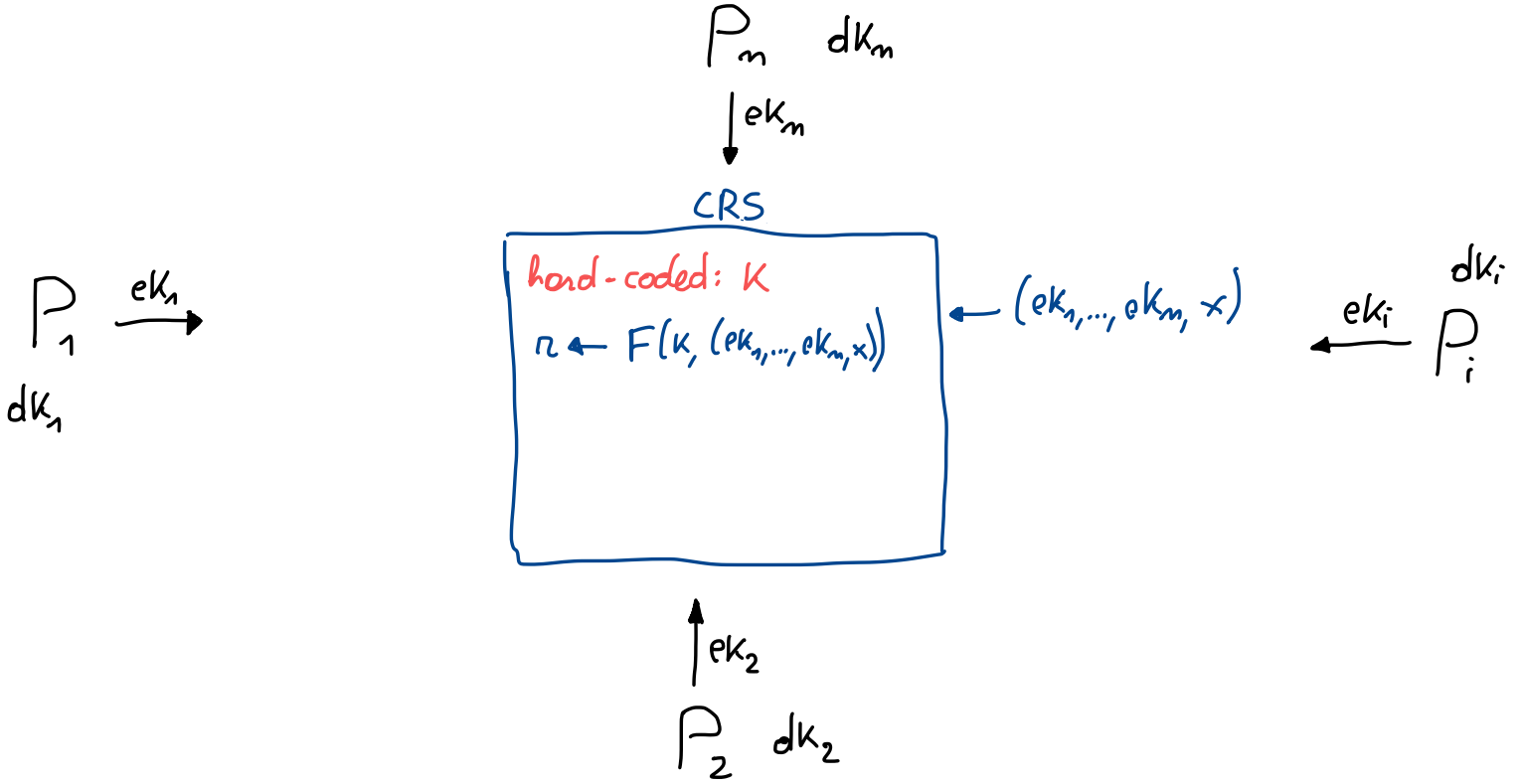
# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



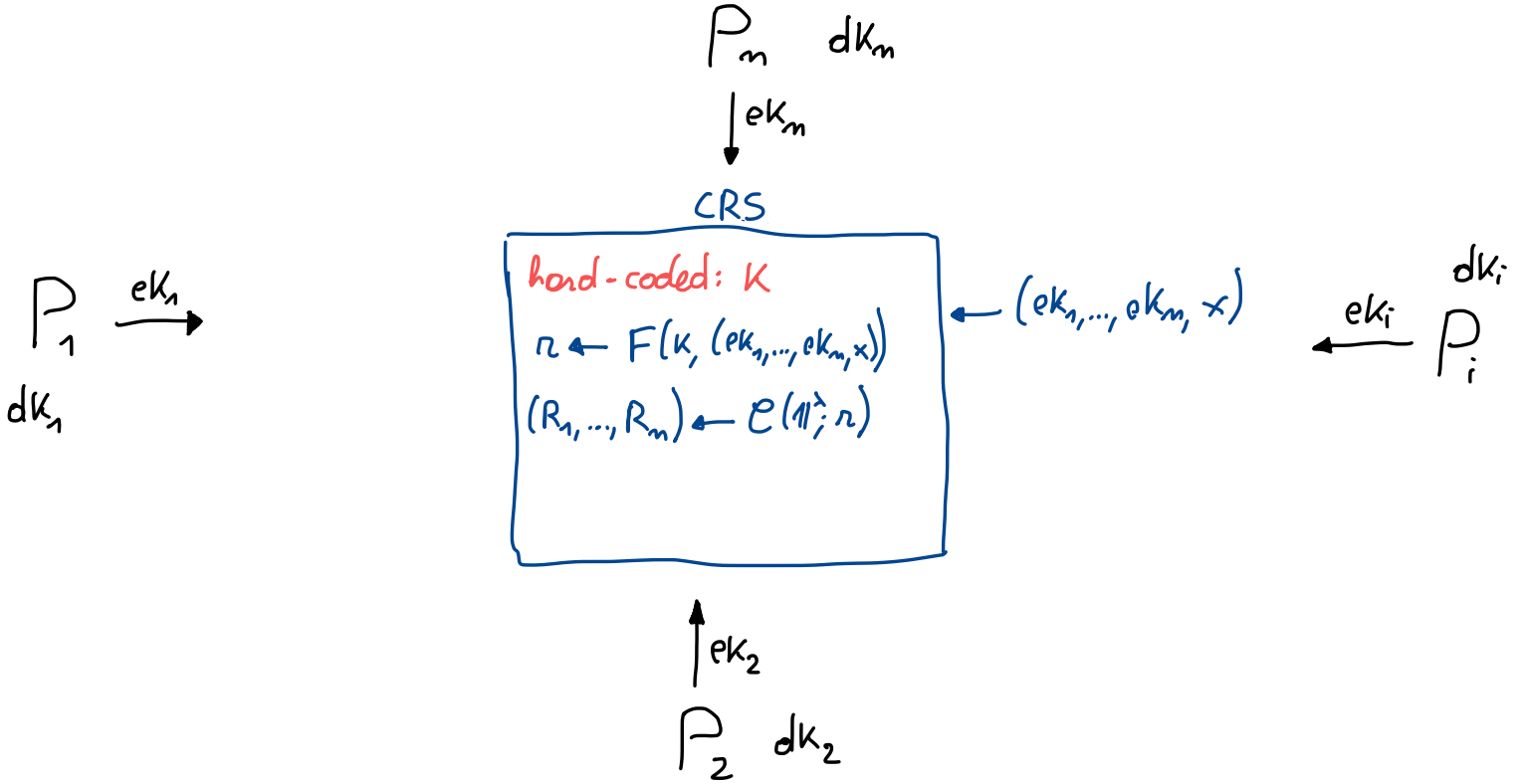
# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



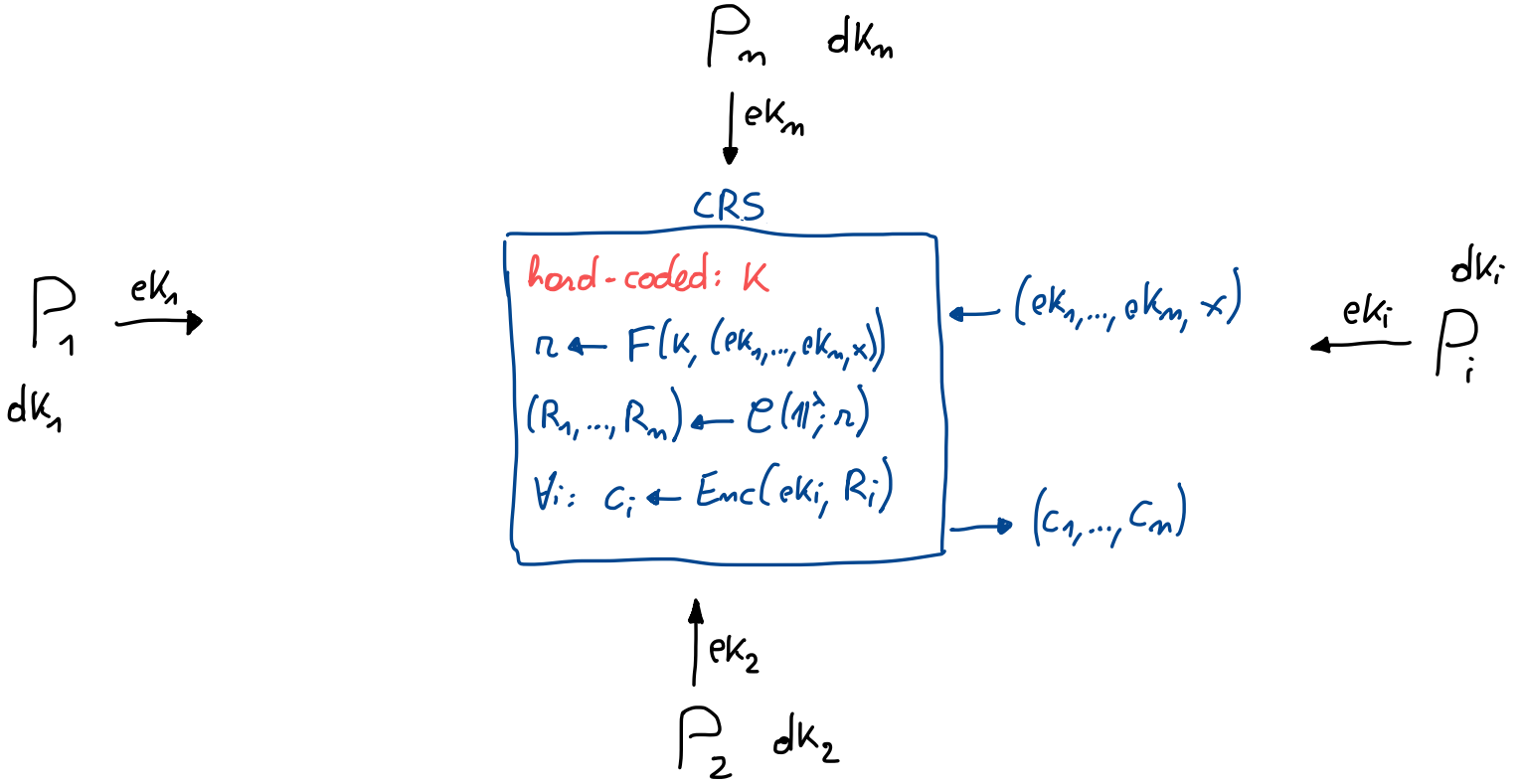
# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



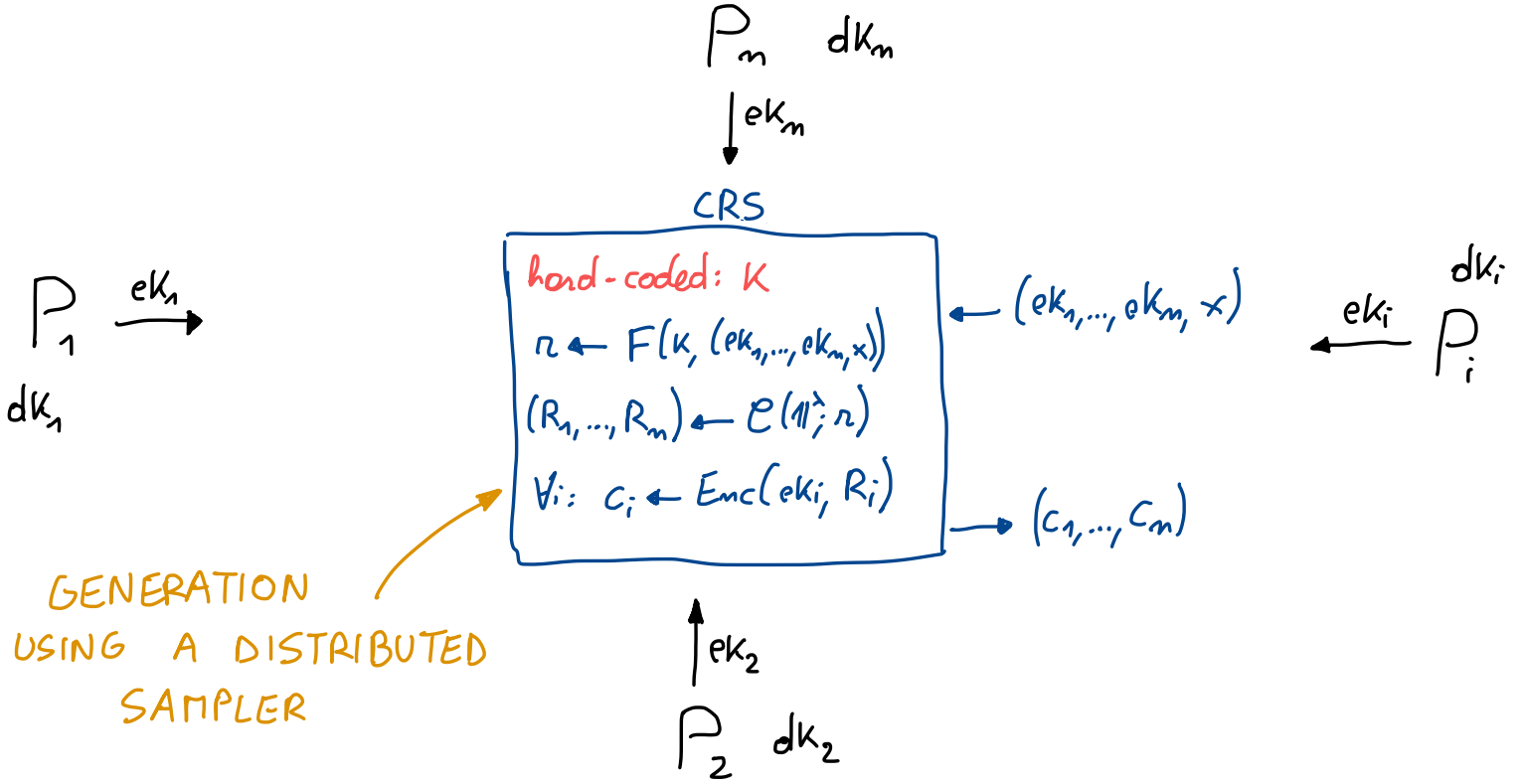
# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



# PUBLIC-KEY PCFs FROM DISTRIBUTED SAMPLERS



# SUMMARY OF RESULTS

## DISTRIBUTED SAMPLERS

### NON-RUSHING SEMI-MALICIOUS

- any distribution
- plain model
- poly iO, poly mKFHE

### ACTIVE

- any distribution
- random oracle
- poly iO, poly mKFHE, poly NIZK

## PUBLIC-KEY PCFs

any correlation

NON-RUSHING
SEMI-MALICIOUS
↓
plain model +
polynomial primitives

ACTIVE
↙ ↘
random oracle + polynomial primitives

URS model + subexponential primitives