The Power of Undirected Rewindings for Adaptive Security

Dennis Hofheinz Julia Kastner Karen Klein

ETH Zürich

Motivation

Selective Security

Adaptive Security

Corruptions

RoR-challenge

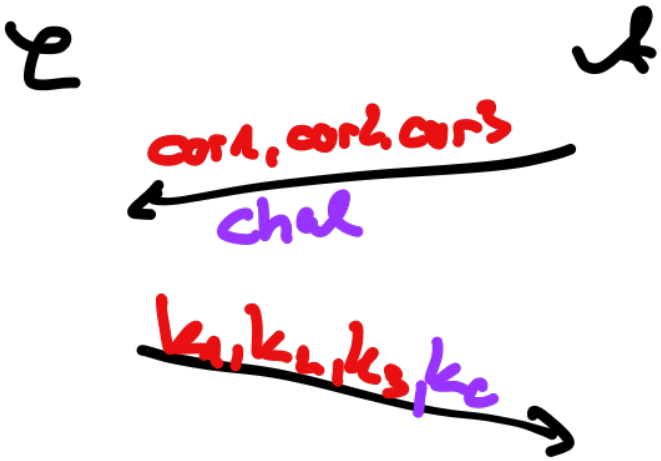
Motivation

Selective Security

Adaptive Security

Motivation

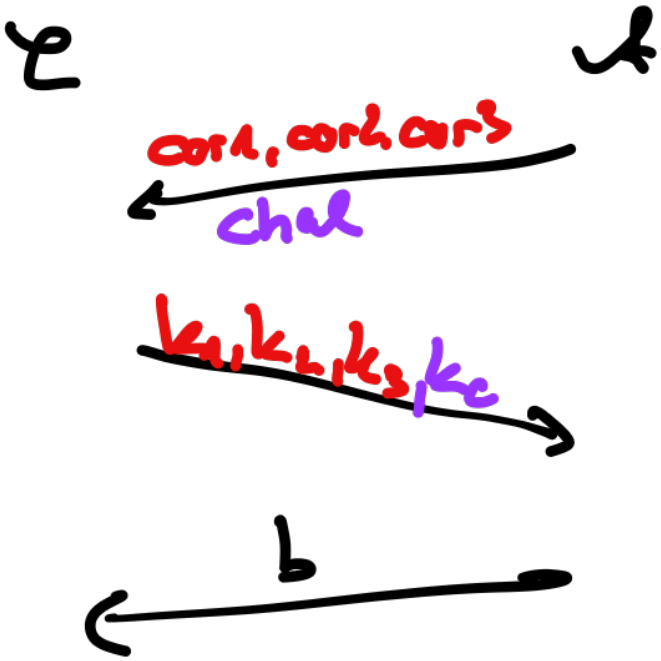
Selective Security



Adaptive Security

Motivation

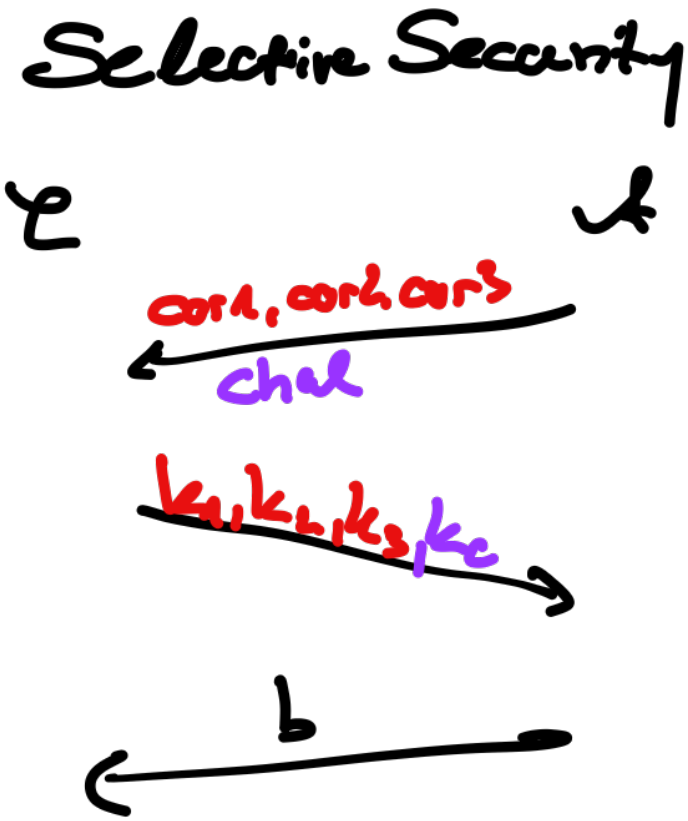
Selective Security



Adaptive Security

Motivation

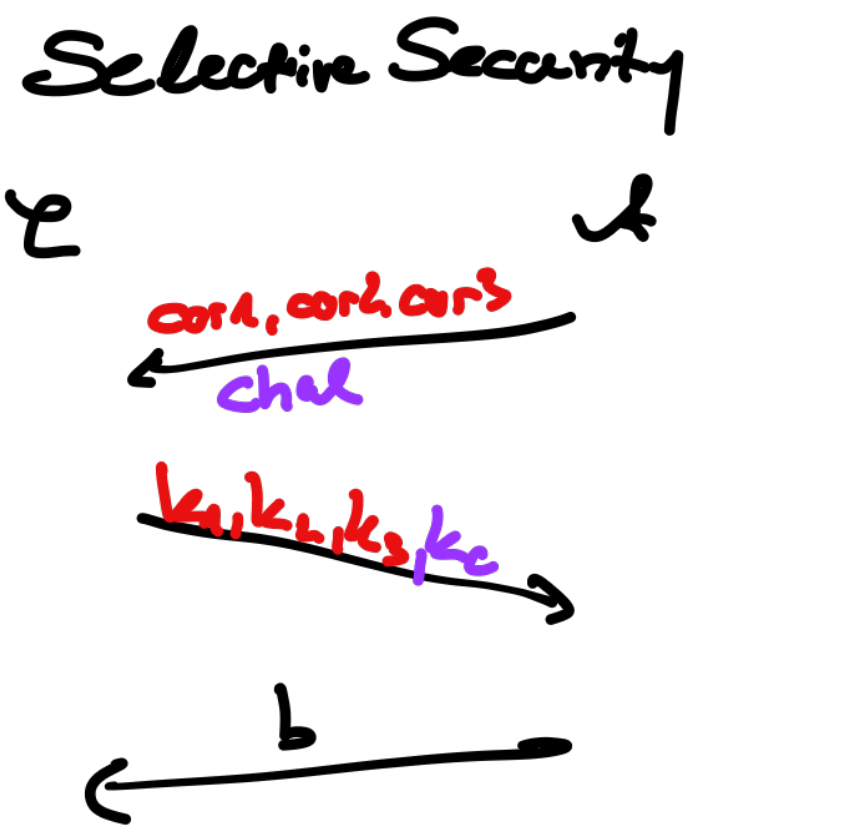
Selective Security



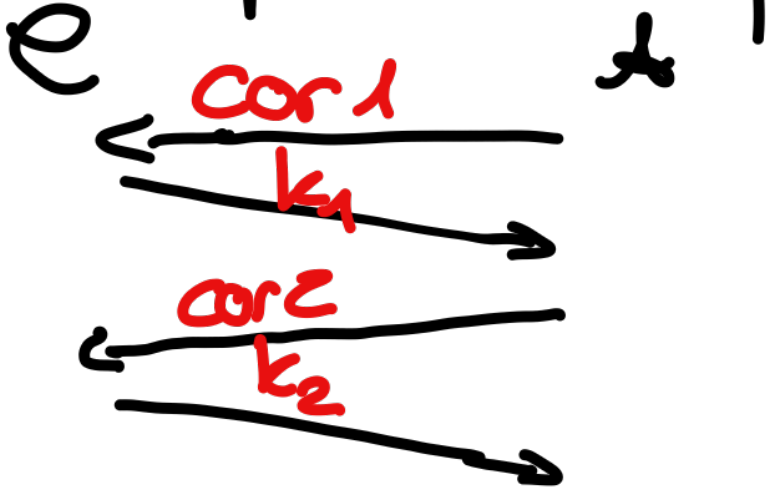
Adaptive Security

Motivation

Selective Security

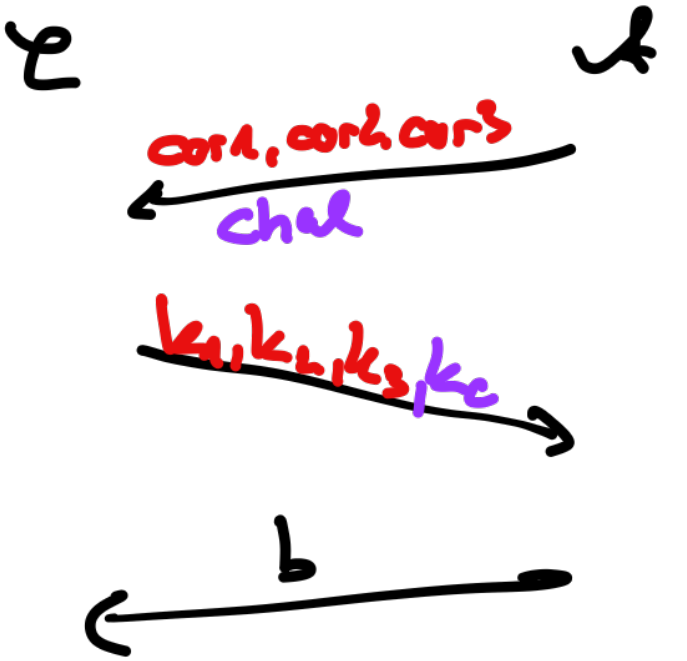


Adaptive Security

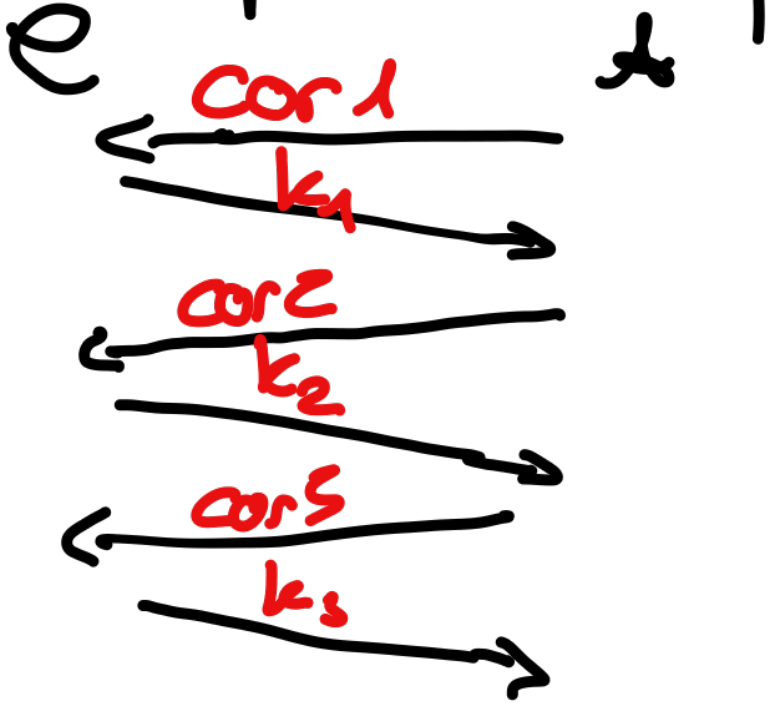


Motivation

Selective Security

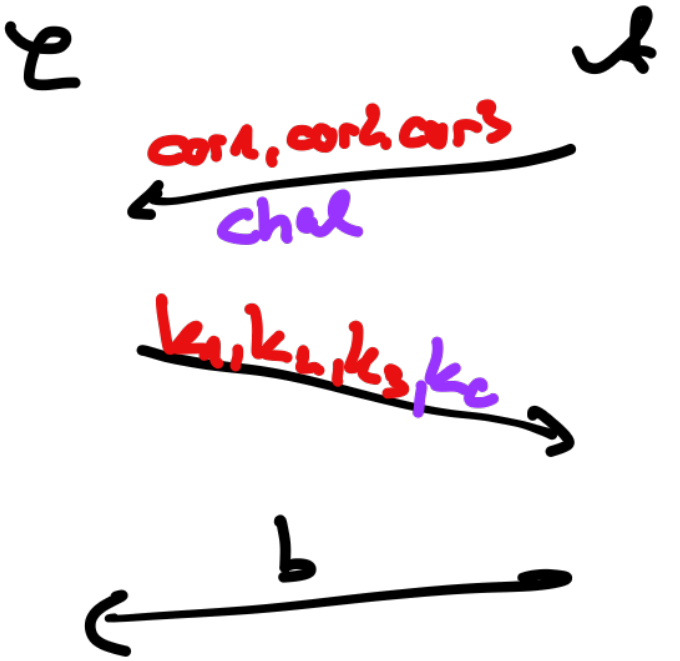


Adaptive Security

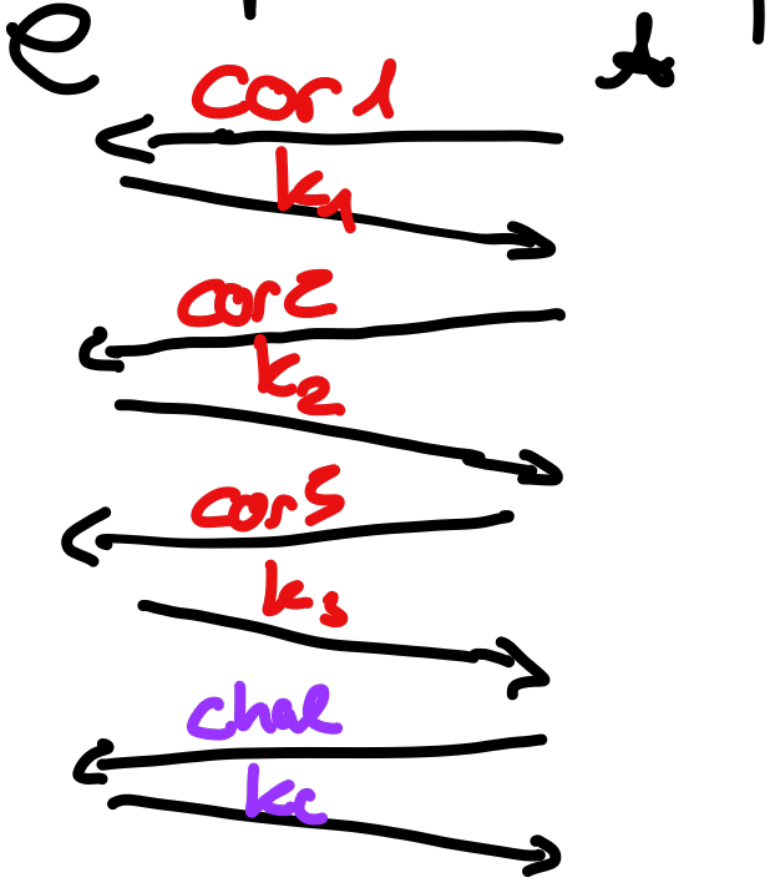


Motivation

Selective Security

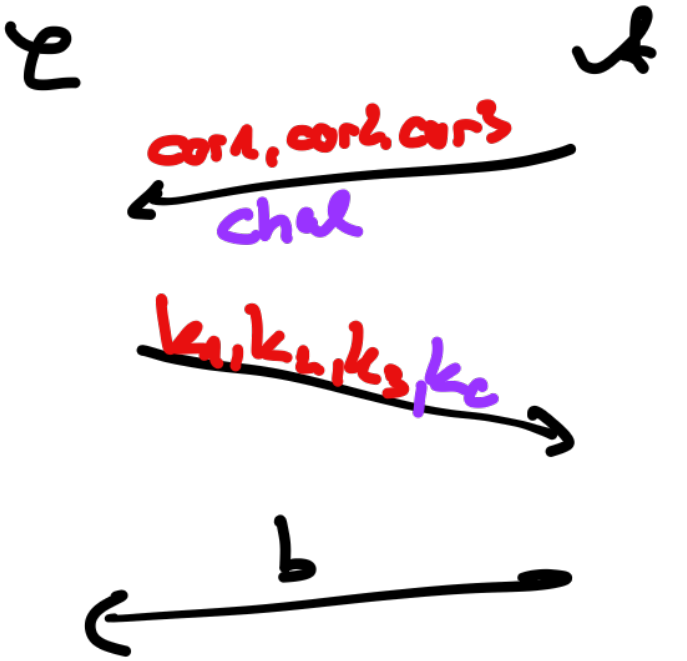


Adaptive Security

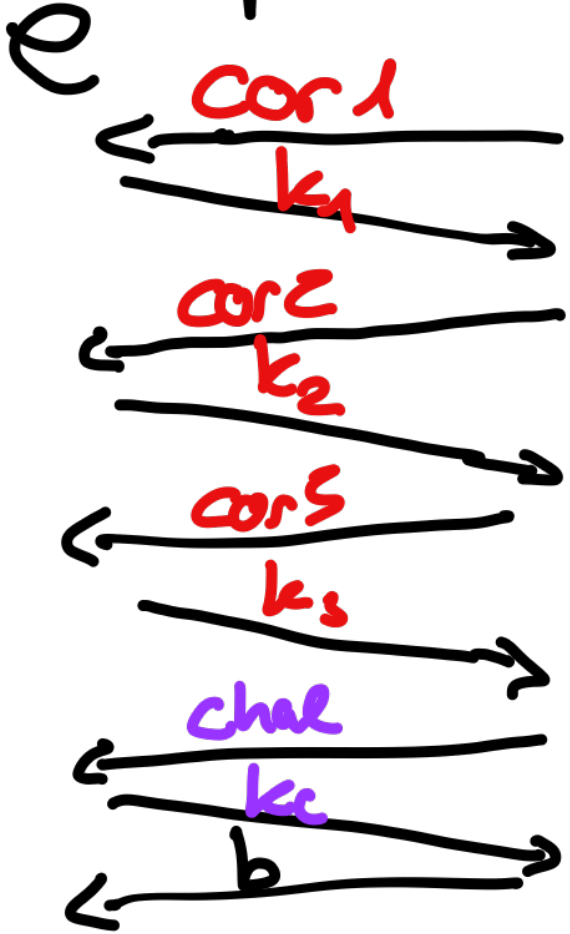


Motivation

Selective Security

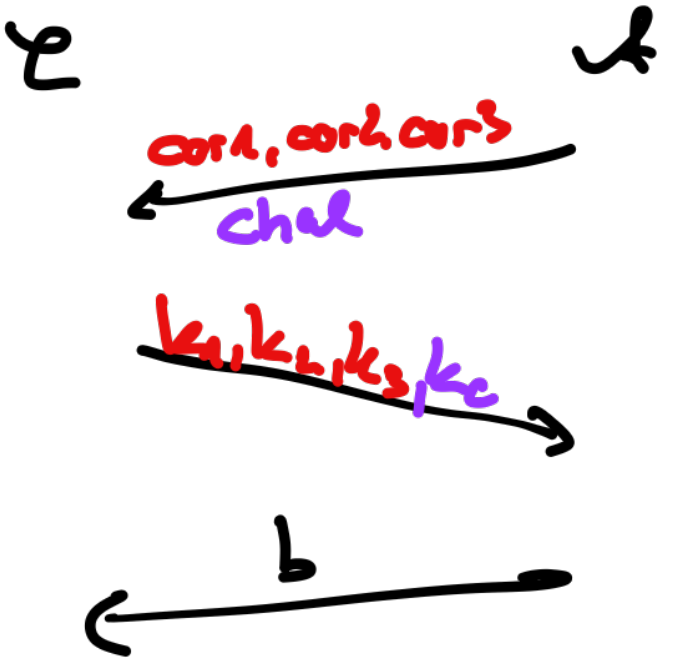


Adaptive Security

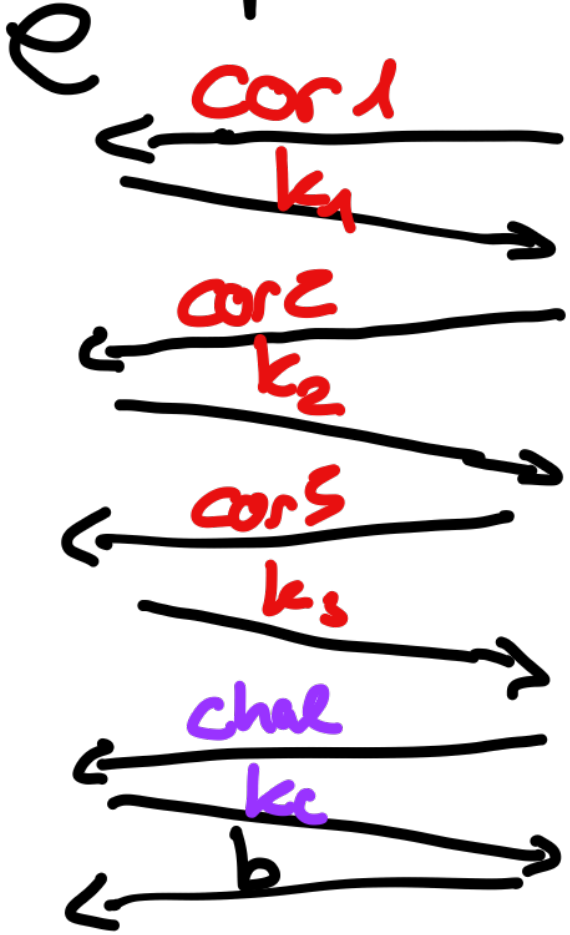


Motivation

Selective Security



Adaptive Security

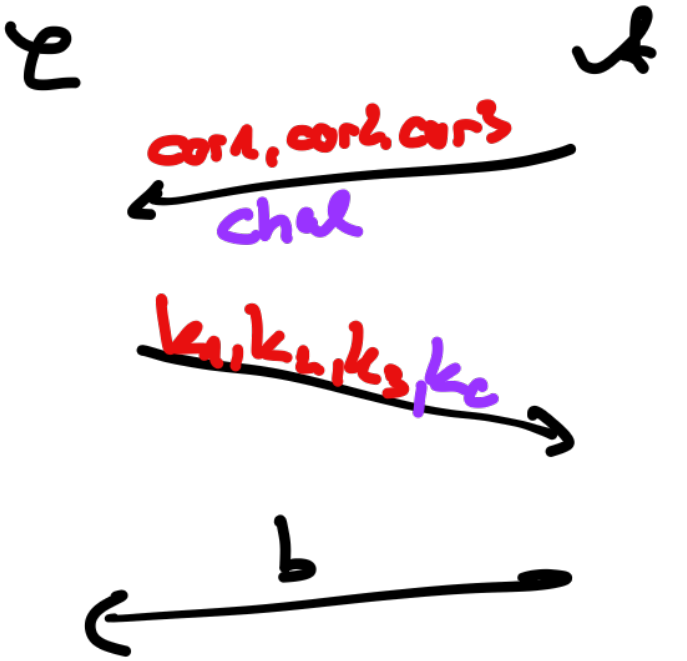


easier to prove

weaker notion

Motivation

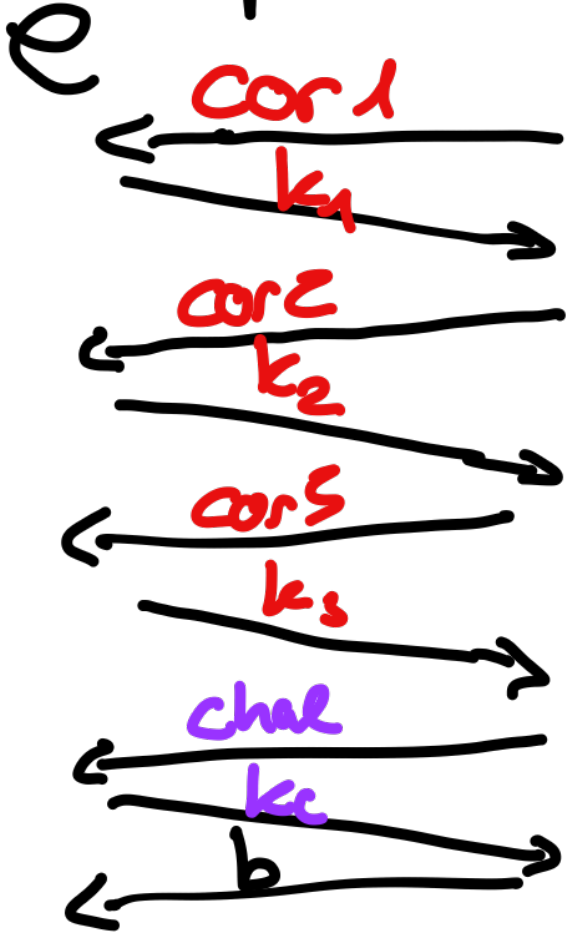
Selective Security



easier to prove

weaker notion

Adaptive Security

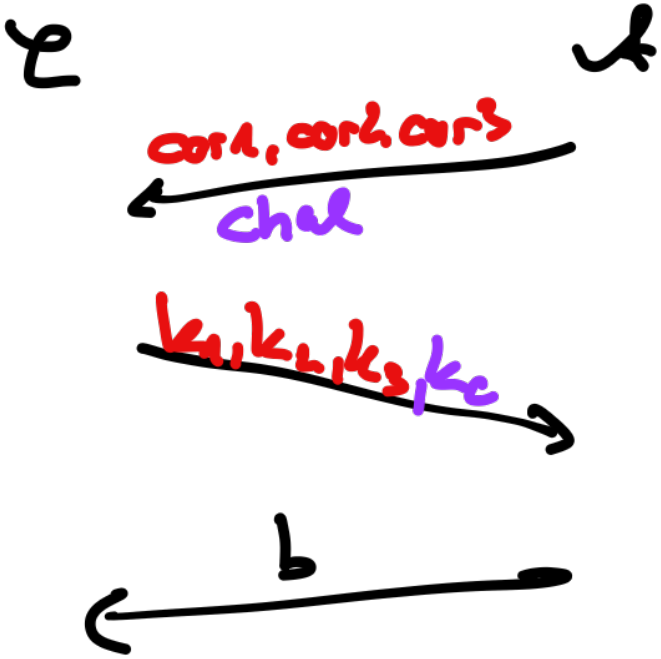


harder to prove

Stronger notion

Motivation

Selective Security

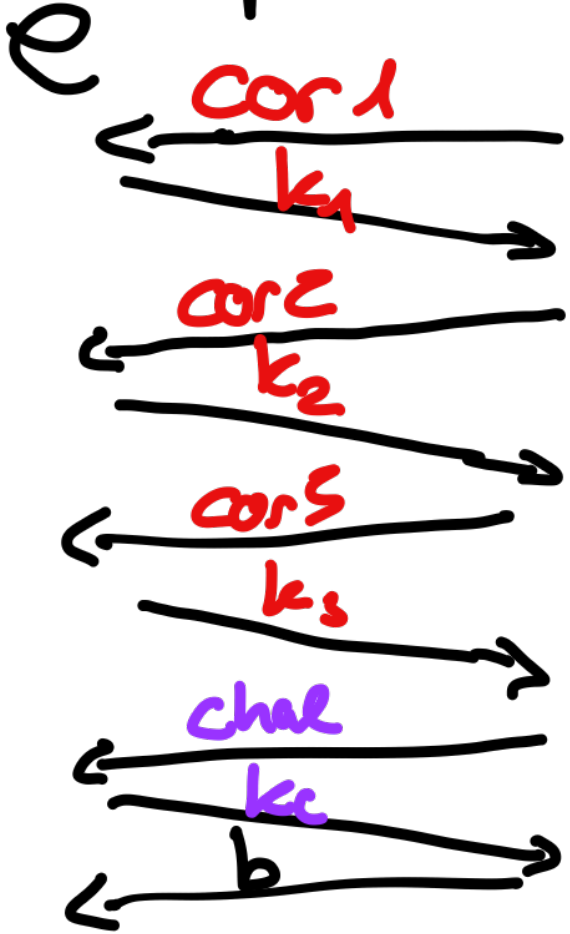


easier to prove

weaker notion

This talk

Adaptive Security



harder to prove

Stronger notion

PRFs

$$F_k : \{0,1\}^n \rightarrow \{0,1\}^m$$

PRFs

$$F_k : \{0,1\}^n \rightarrow \{0,1\}^m$$

Security:

$k \xleftarrow{\$} \mathcal{K}$

$$Pr[A^{R(\cdot)} = 1] - Pr[A^{F_k(\cdot)} = 1] \leq negl$$

Prefix-Constrained PRF

$$F_k : \{0,1\}^n \rightarrow \{0,1\}^m$$

Constrained keys k_x evaluate if input has prefix x

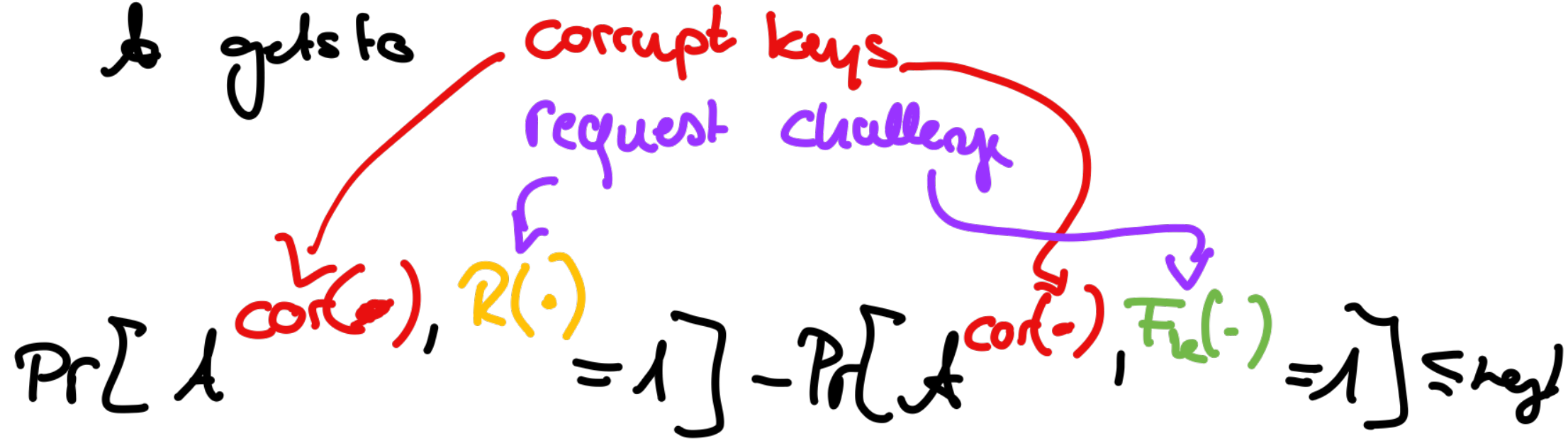
Prefix-Constrained PRF

$$F_k : \{0,1\}^n \to \{0,1\}^m$$

Constrained keys k_x — evaluate if input has prefix x

Security:

$\mathcal{A}$ gets to



Our contributions

- adaptive security of GGM PC-PRF
  based on security of PRG with polynomial loss
- adaptive security of LKH (Multicast Encryption)
  based on IND-CPA security of underlying encryption with polynomial loss

Main technique: undirected rewinding

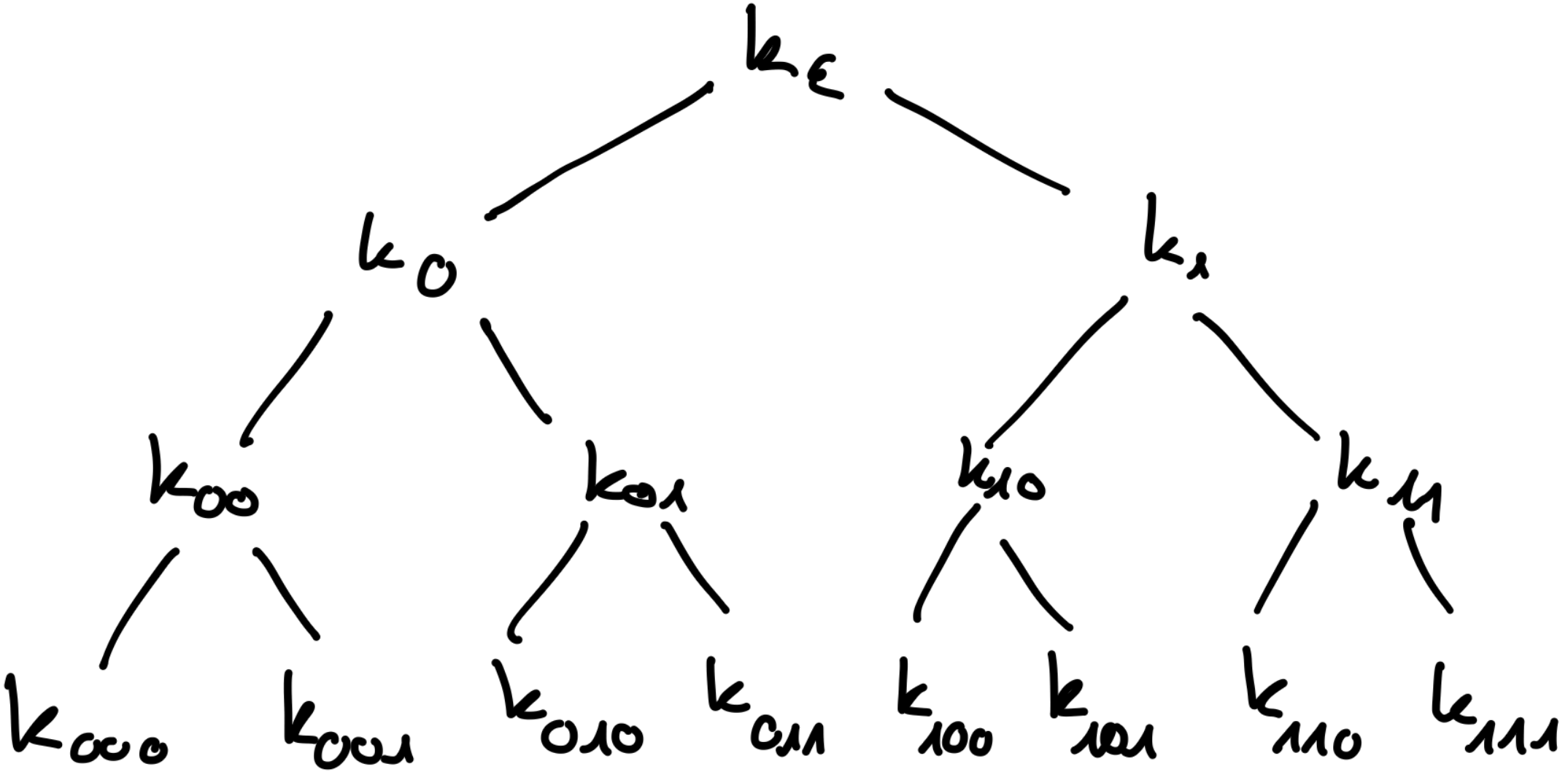
Our contributions

This talk

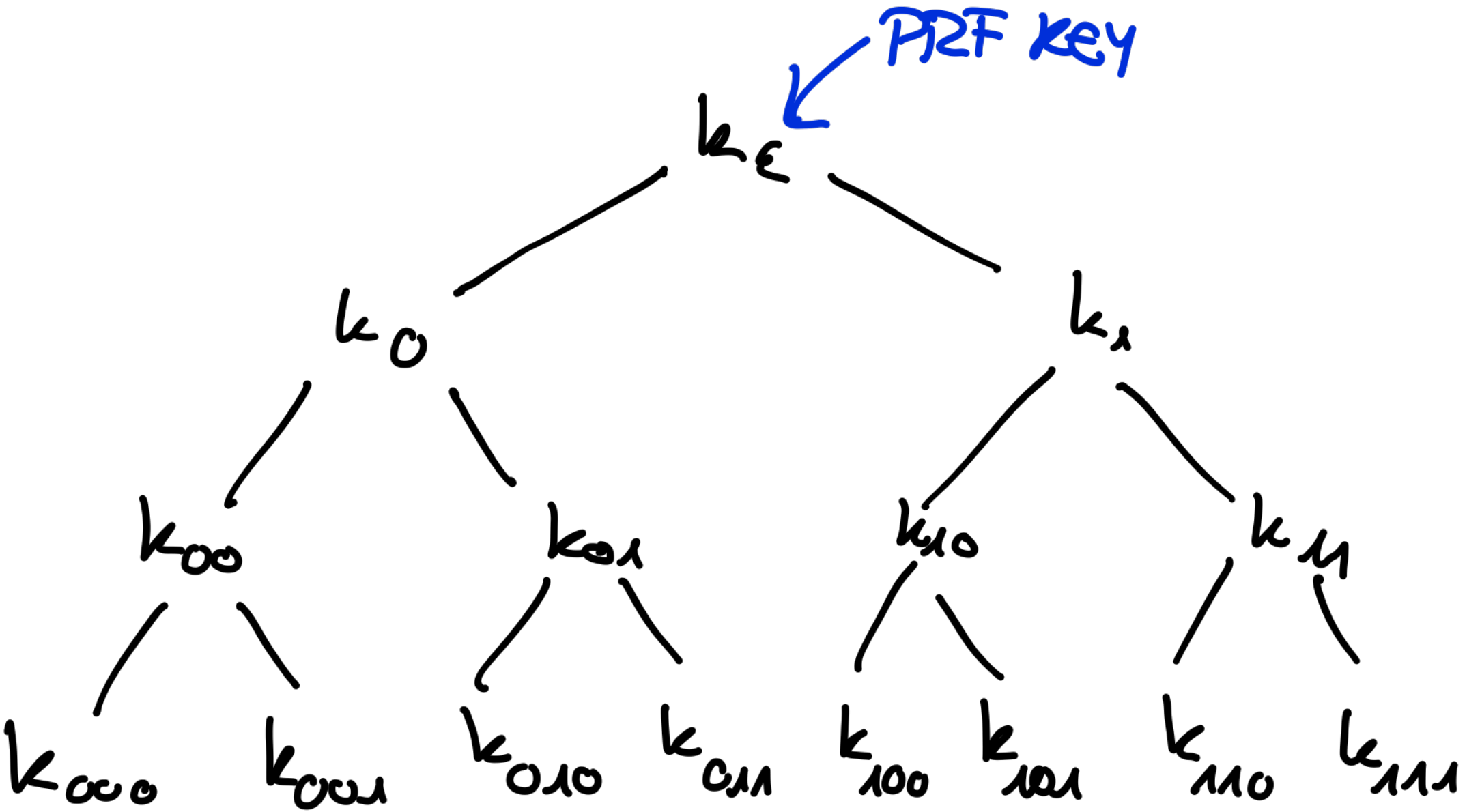
- adaptive security of GGM PC-PRF based on security of PRG with polynomial loss
- adaptive security of LKH (Multicast Encryption) based on IND-CPA security of underlying encryption with polynomial loss

Main technique: undirected rewinding

The GGM PRF

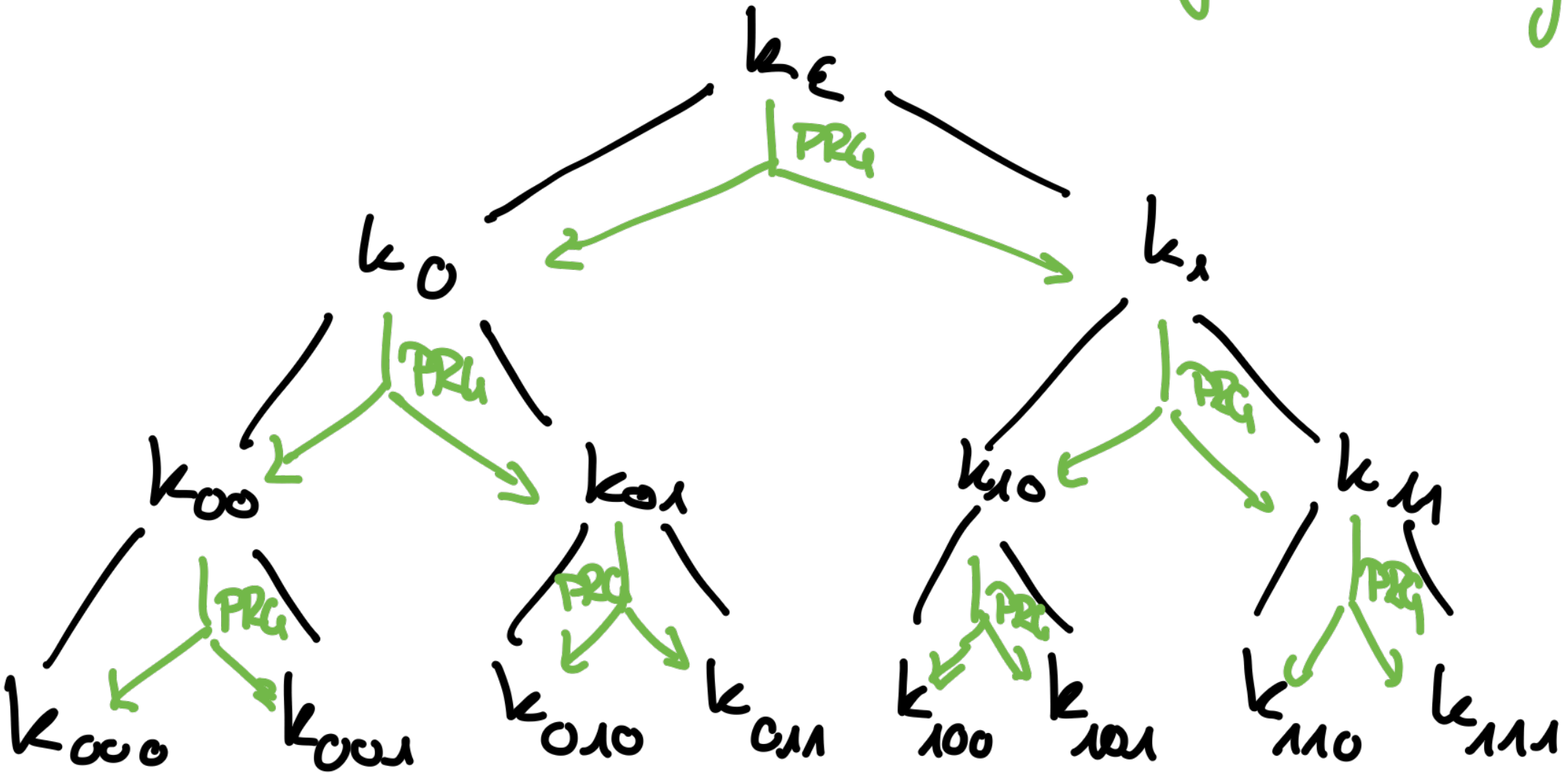

k_ε
k_0
k_1
k_{00}
k_{01}
k_{10}
k_{11}
k_{000}
k_{001}
k_{010}
k_{011}
k_{100}
k_{101}
k_{110}
k_{111}

The GGM PRF

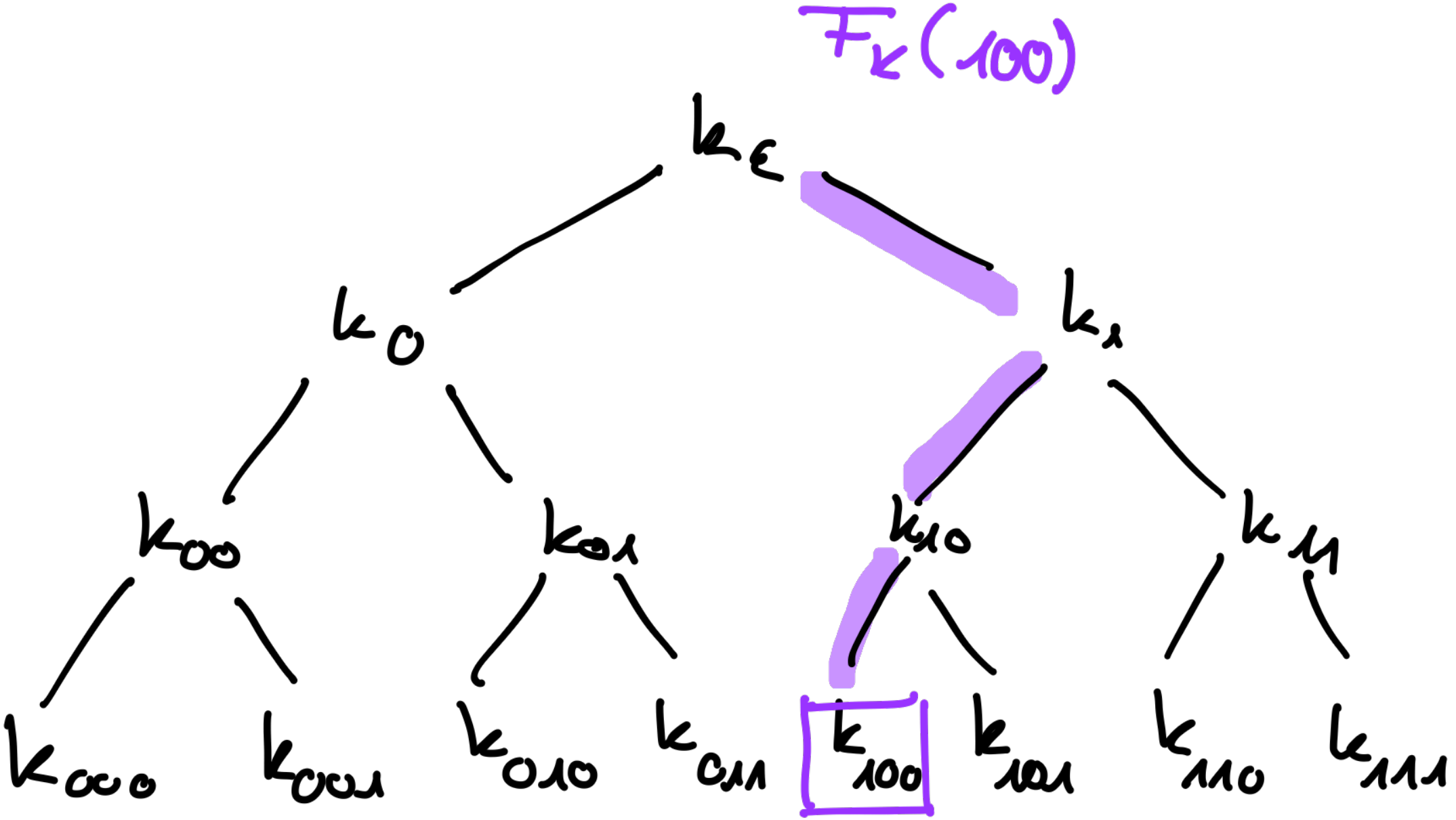

PRF key
k_ε
k_0
k_1
k_{00}
k_{01}
k_{10}
k_{11}
k_{000}
k_{001}
k_{010}
k_{011}
k_{100}
k_{101}
k_{110}
k_{111}

The GGM PRF

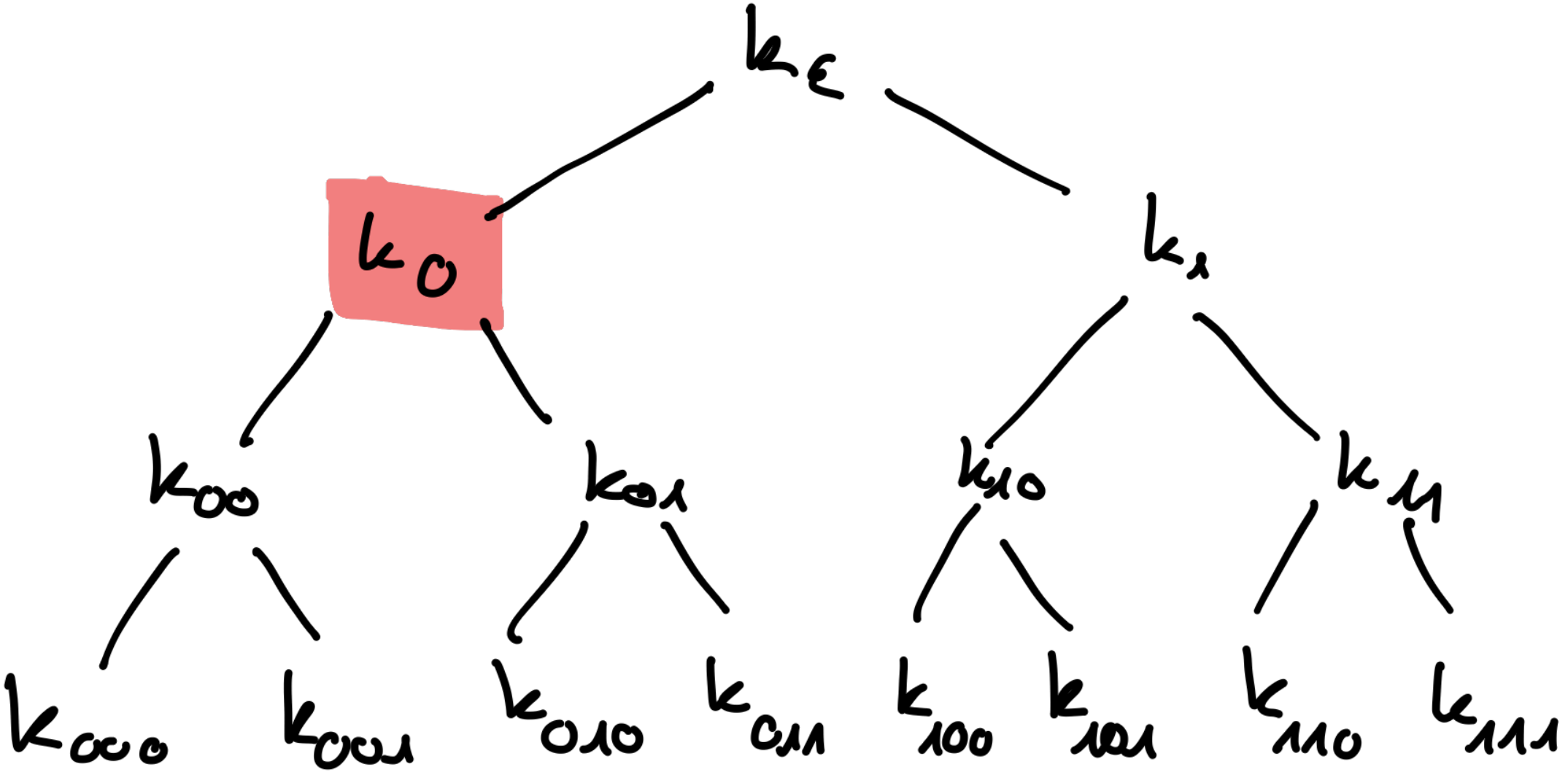
PRG: length-doubling



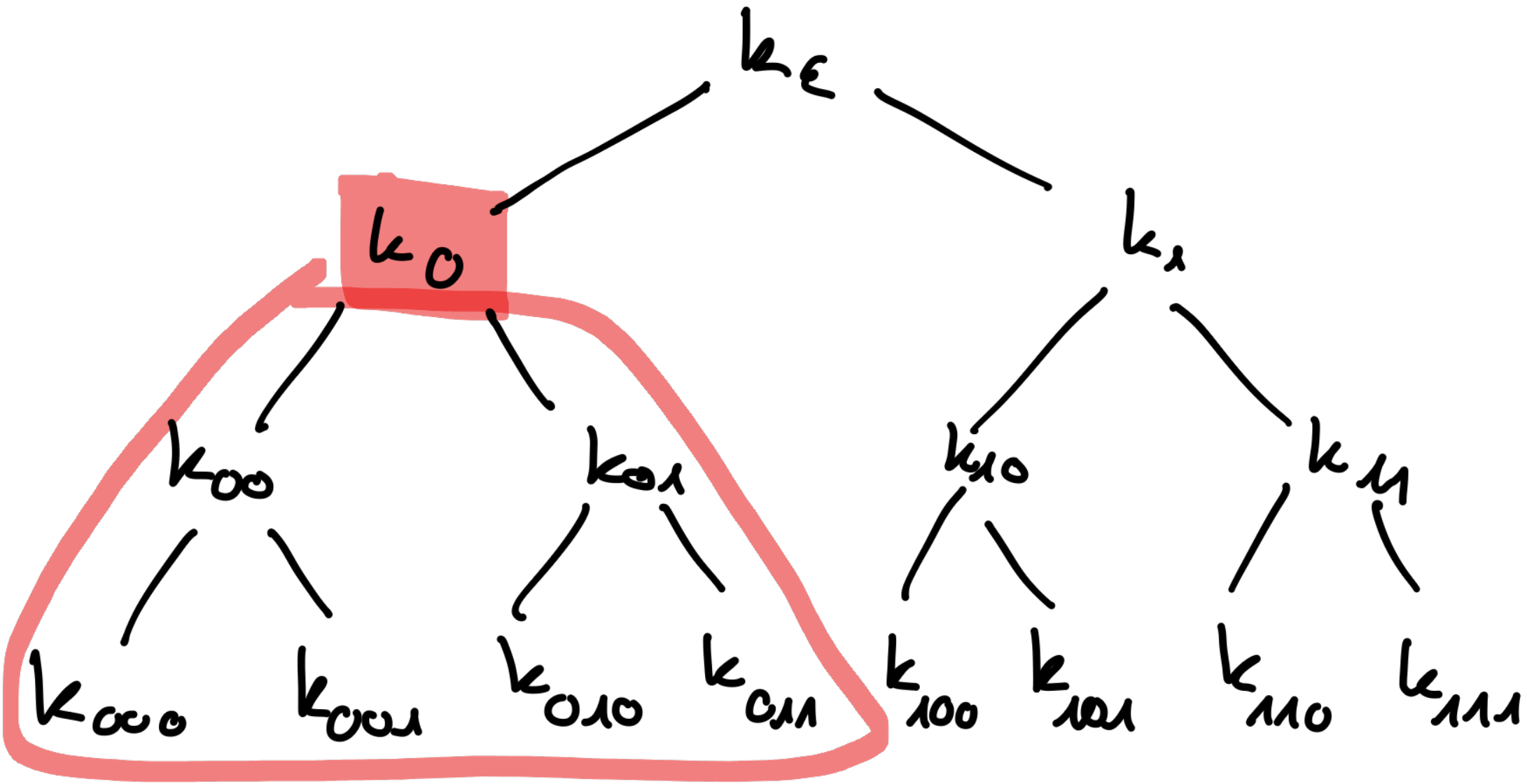
The GGM PRF


$F_k(100)$
k_ε
k_0
k_1
k_{00}
k_{01}
k_{10}
k_{11}
k_{000}
k_{001}
k_{010}
k_{011}
k_{100}
k_{101}
k_{110}
k_{111}

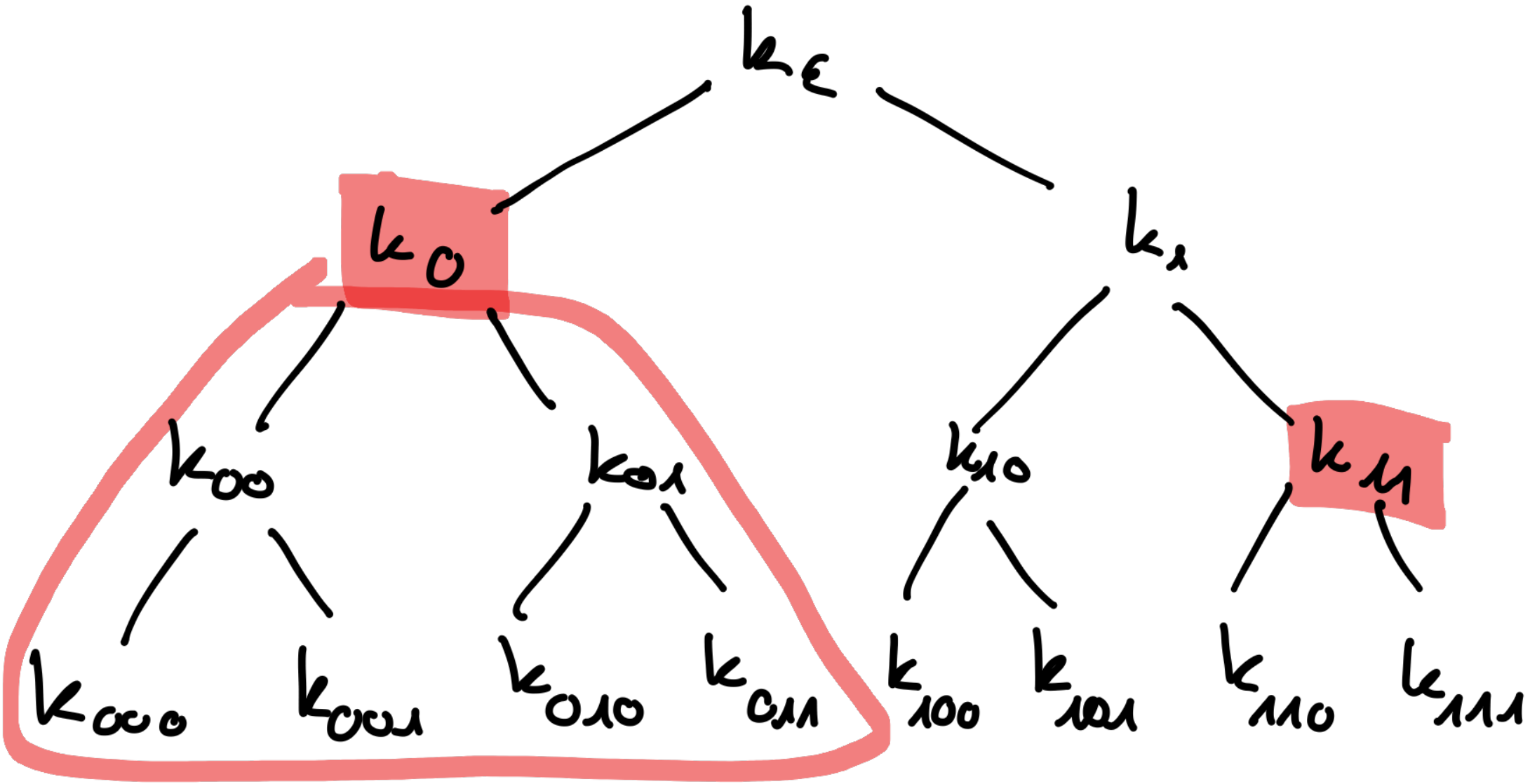
The GGM PRF as a PC-PRF



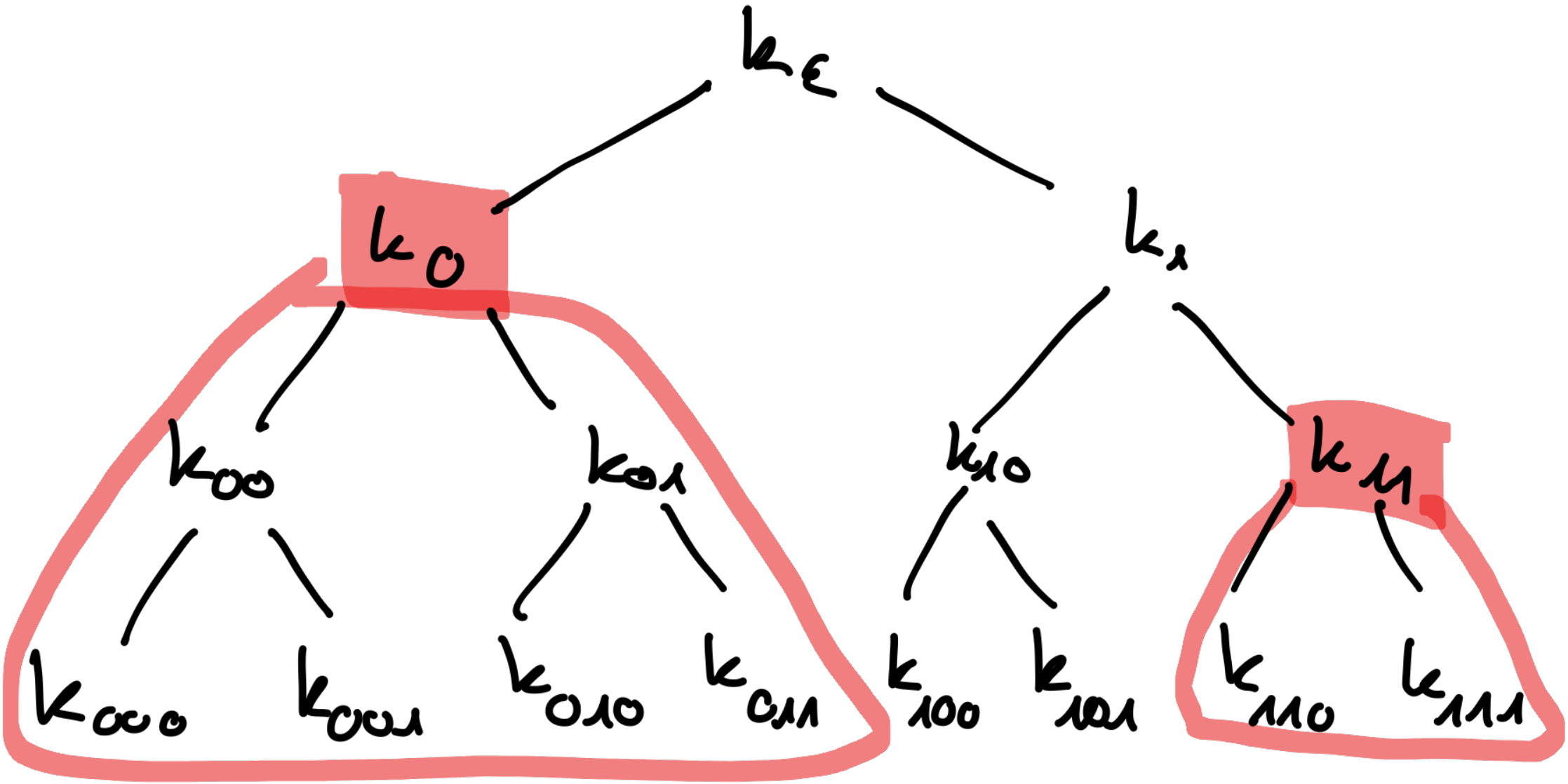
The GGM PRF as a PC-PRF



The GGM PRF as a PC-PRF



The GGM PRF as a PC-PRF



PRG Security

$PRG : \{0,1\}^n \rightarrow \{0,1\}^{2n}$

PRG Security

$$PRG : \{0,1\}^n \rightarrow \{0,1\}^{2n}$$

$$Pr[A^{chal}(1^\lambda) = 1] - Pr[A^{chal}(1^\lambda) = 1] \leq negl$$

PRG Security

$PRG : \{0,1\}^n \to \{0,1\}^{2n}$

output : $y \xleftarrow{\$} \{0,1\}^{2n}$

$$\Pr[A^{chal}(1^\lambda) = 1] - \Pr[A^{chal}(1^\lambda) = 1] \leq negl$$

PRG Security

$$PRG : \{0,1\}^n \to \{0,1\}^{2n}$$

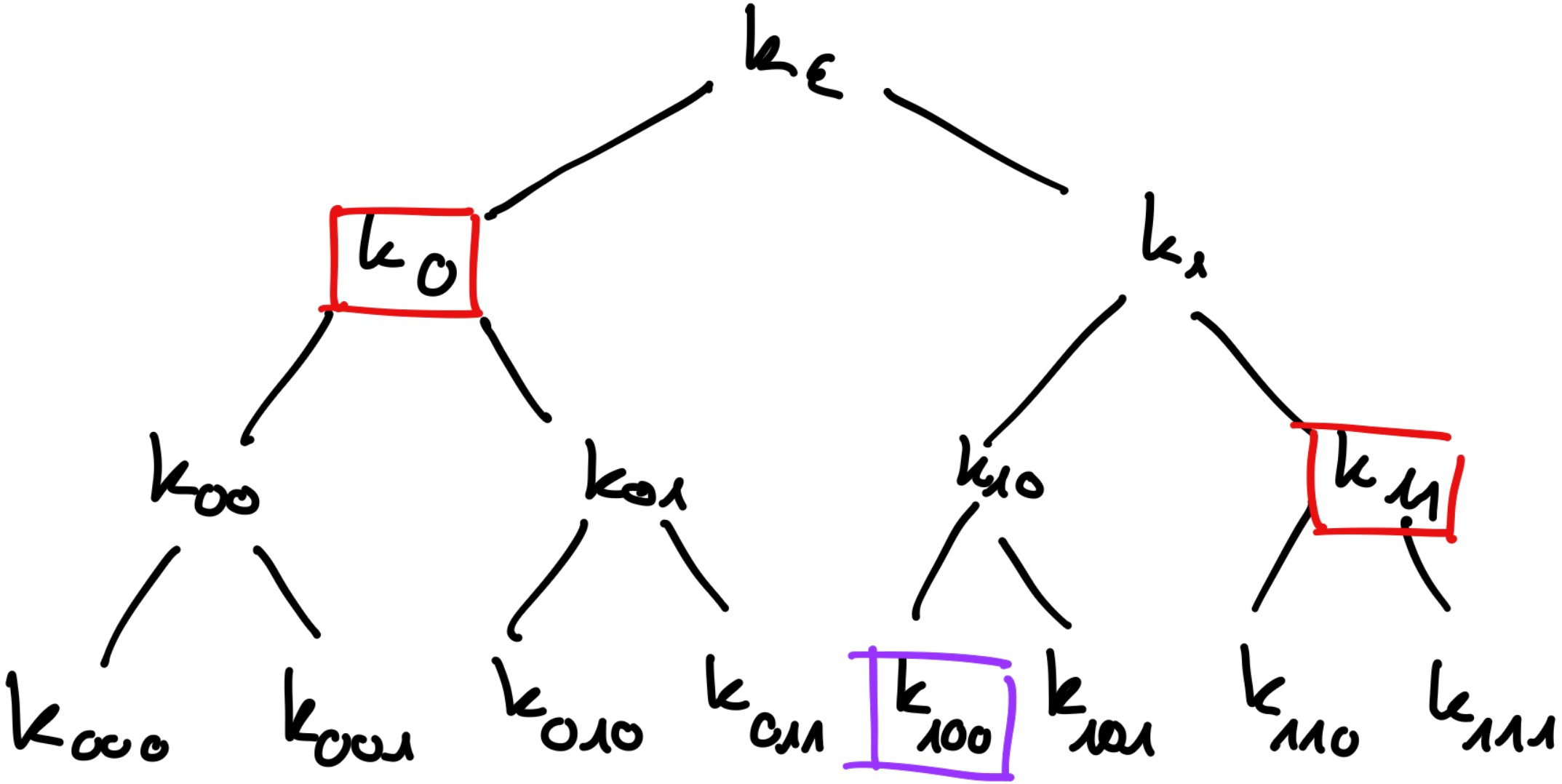
$s \xleftarrow{\$} \{0,1\}^n$

output: $y \xleftarrow{\$} \{0,1\}^{2n}$

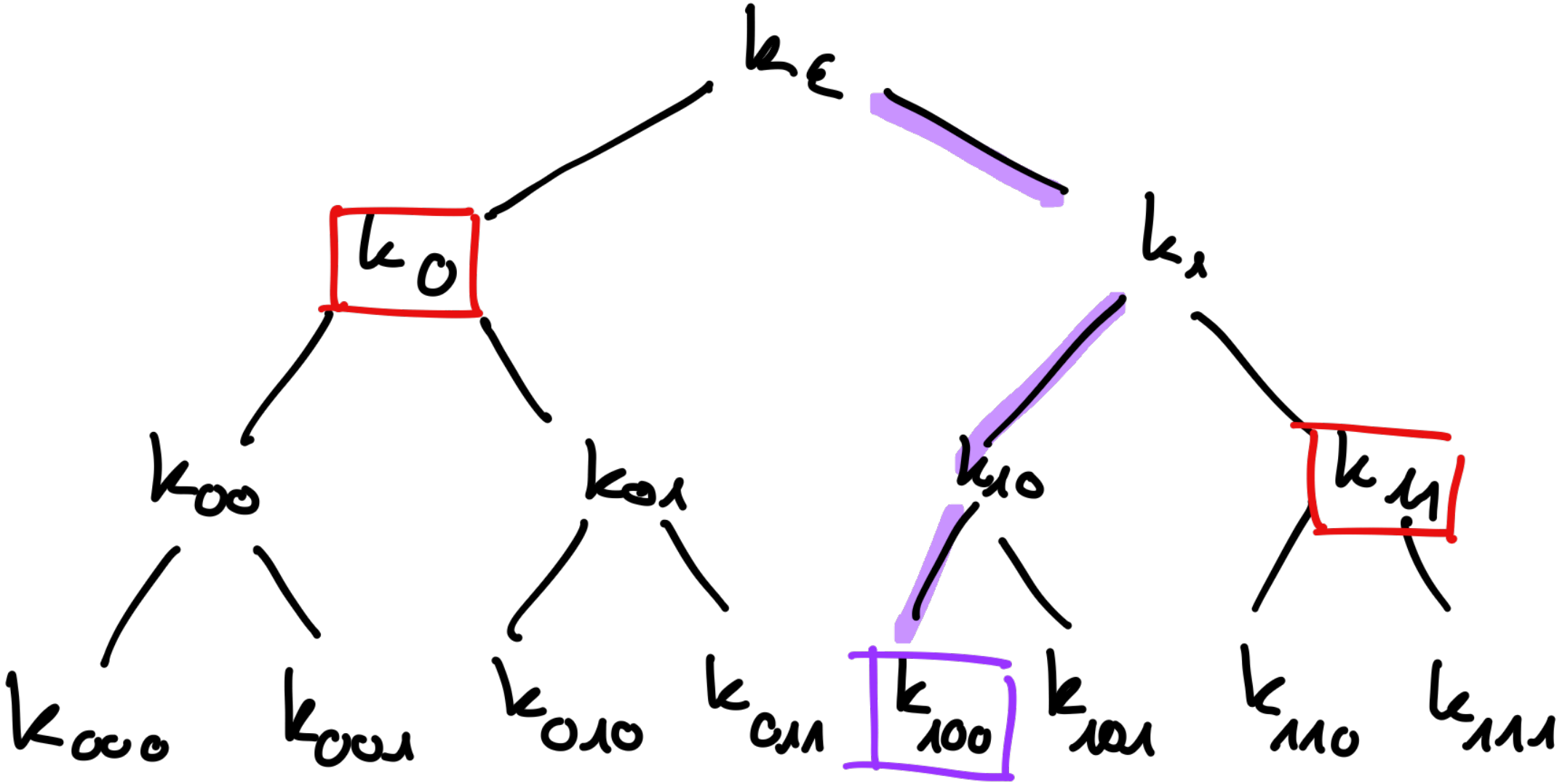
output: $y := PRG(s)$

$$\Pr[A^{chal}(1^\lambda) = 1] - \Pr[A^{chal}(1^\lambda) = 1] \leq negl(\lambda)$$

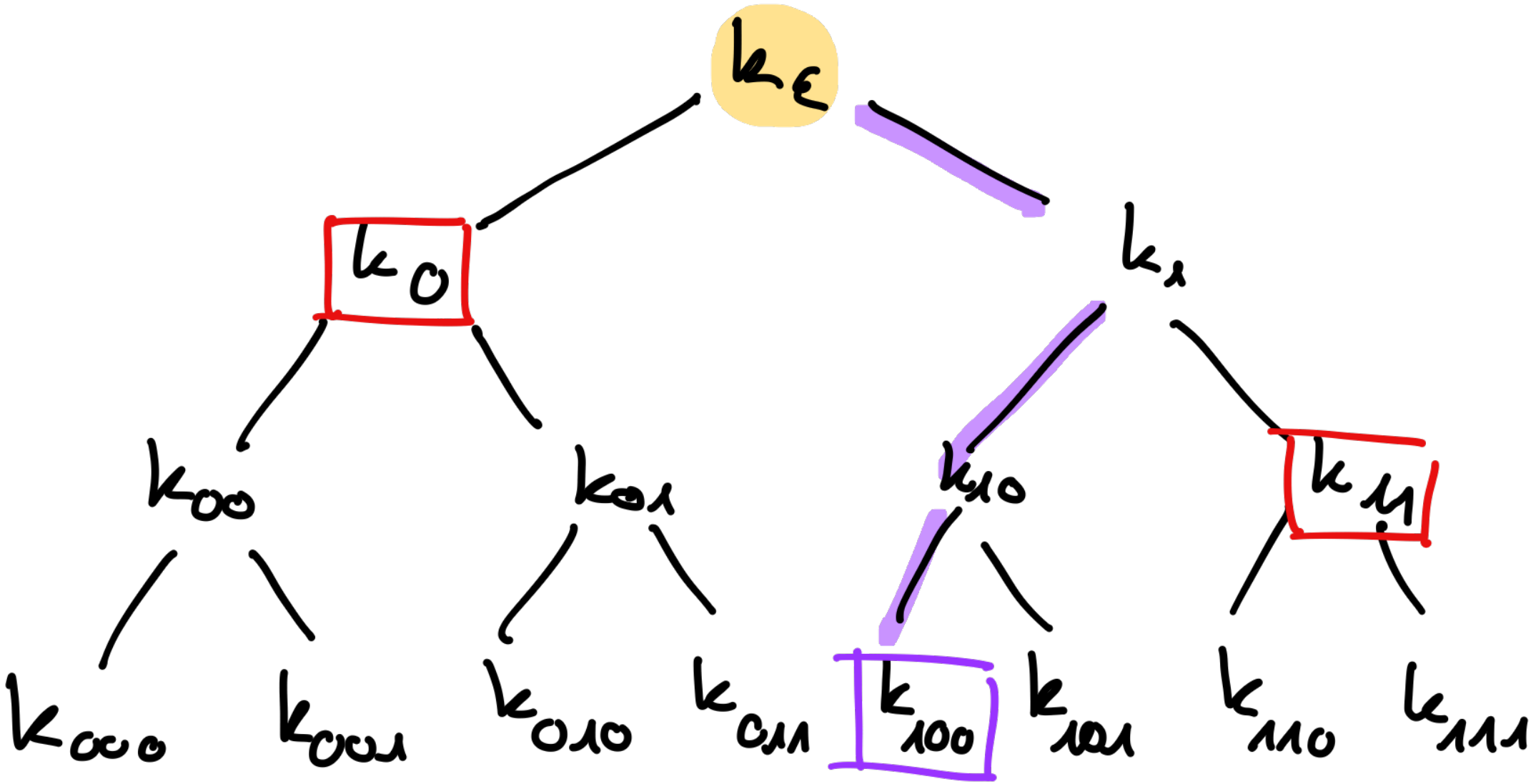
Selective Security



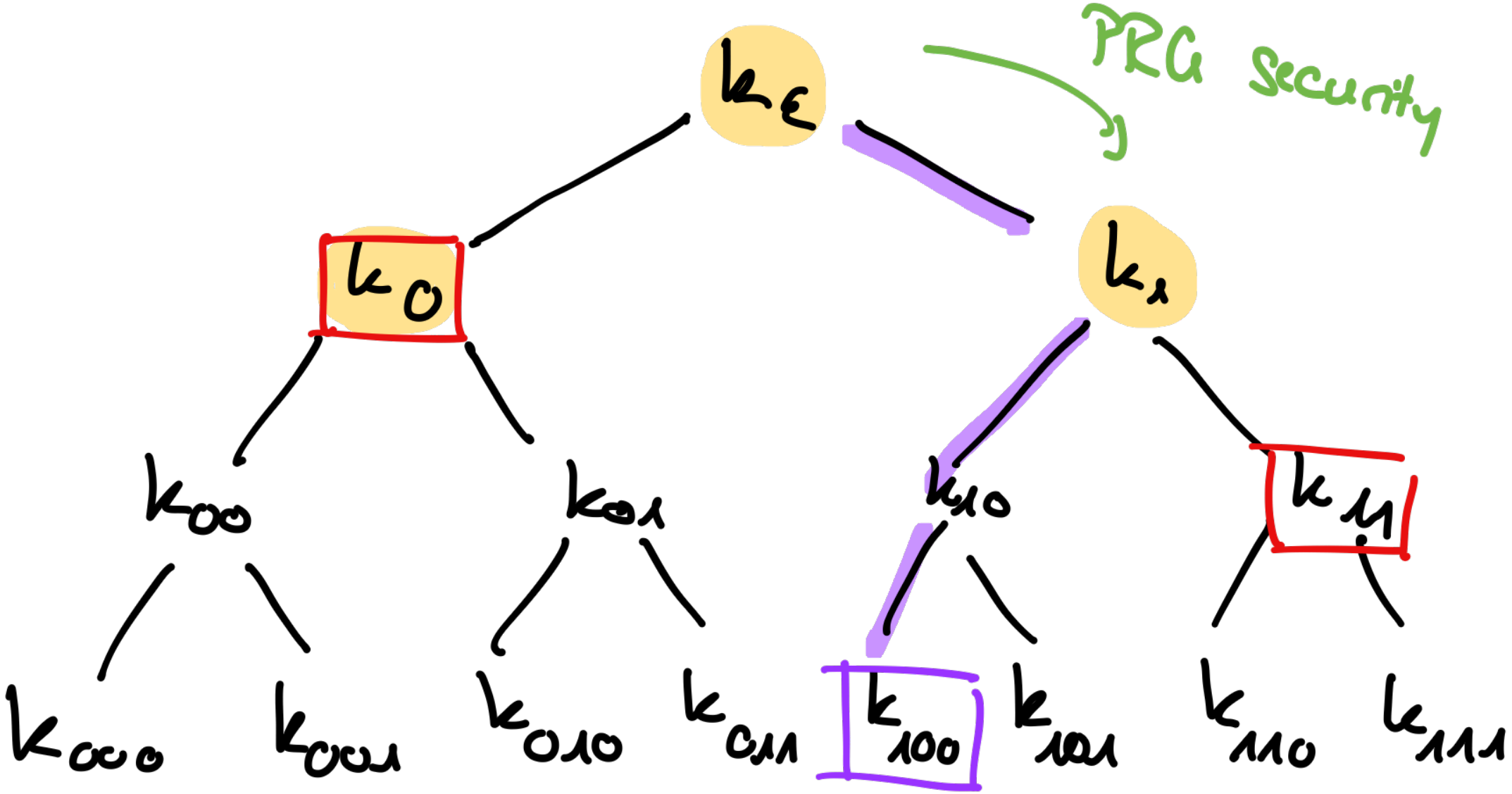
Selective Security



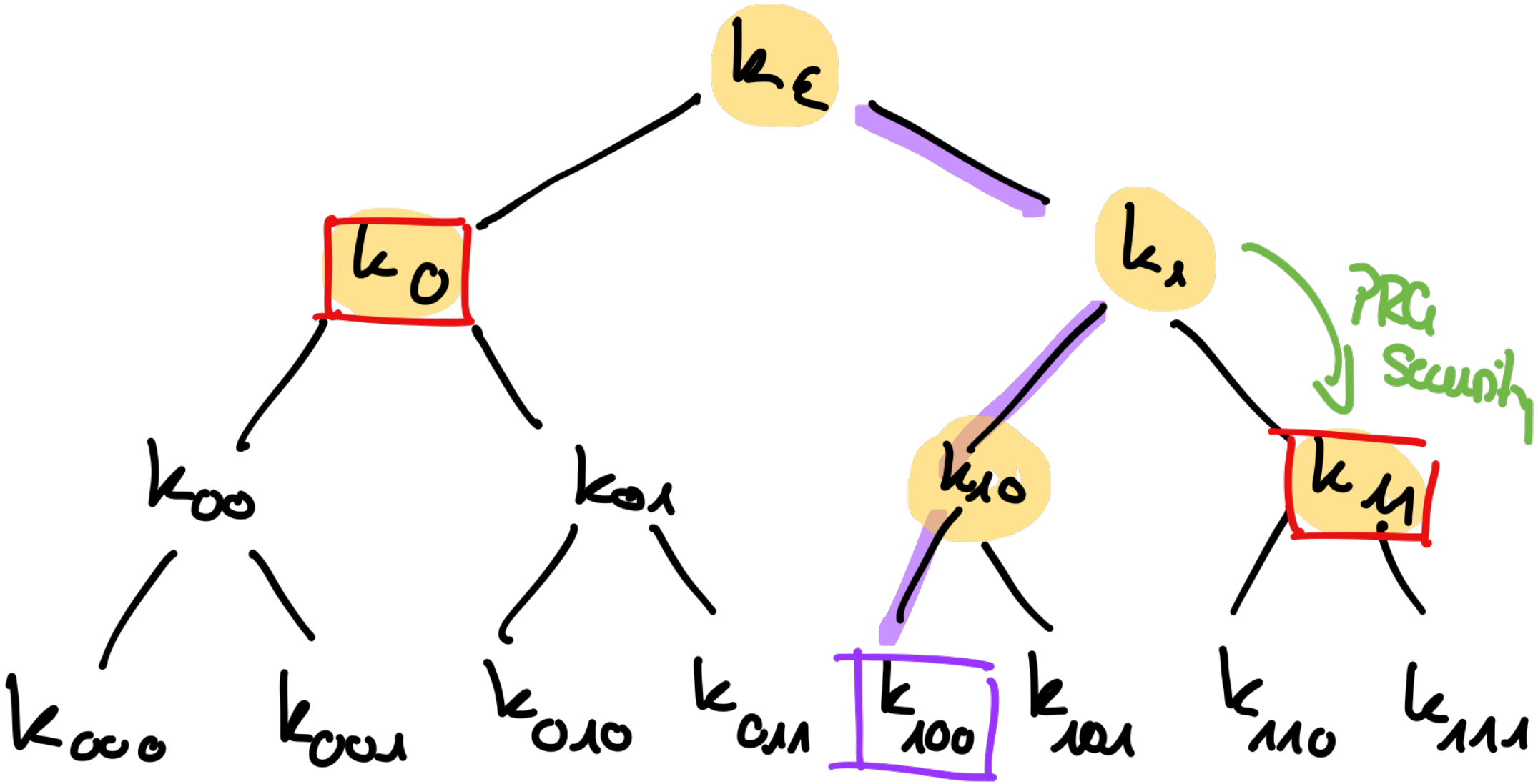
Selective Security



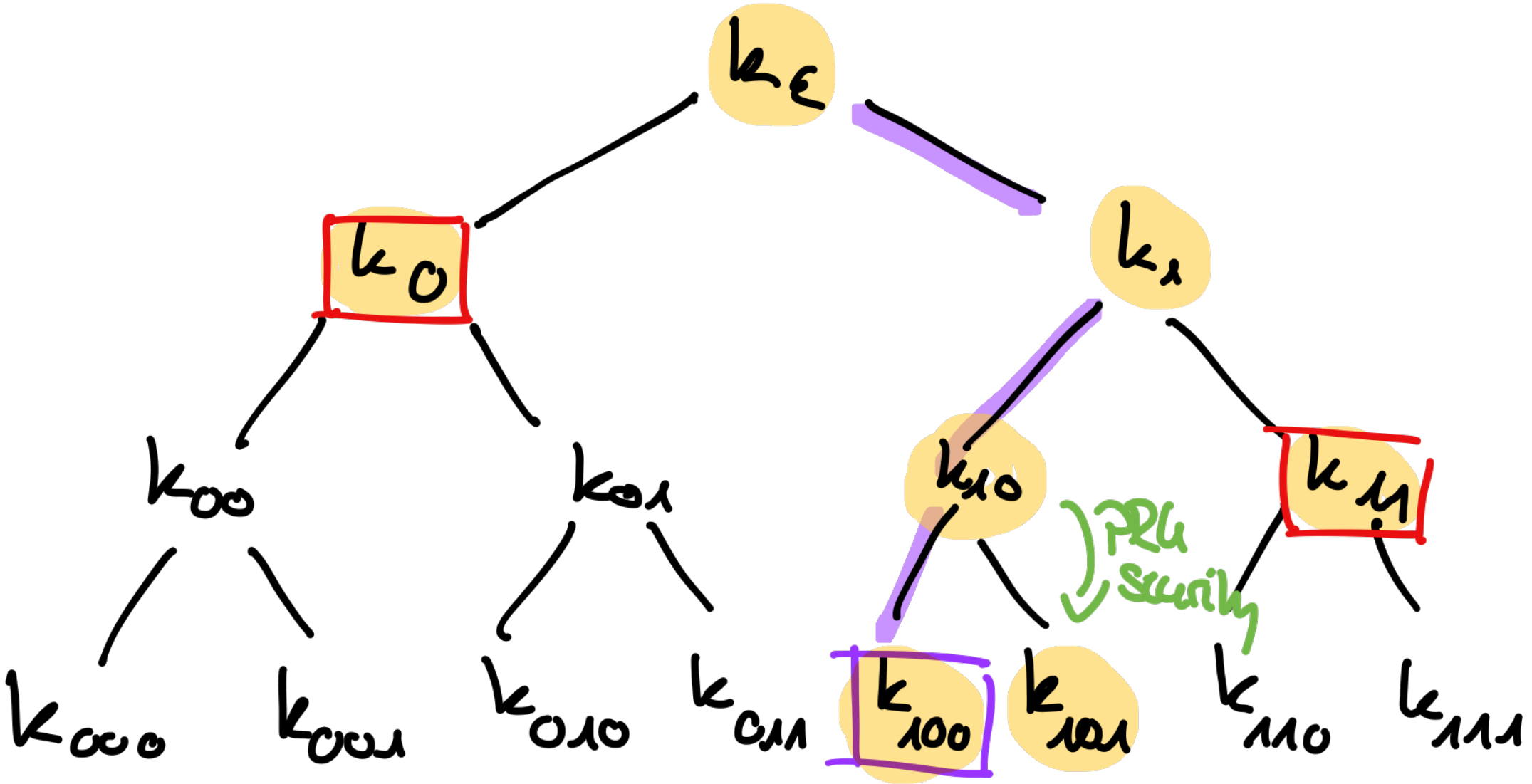
Selective Security



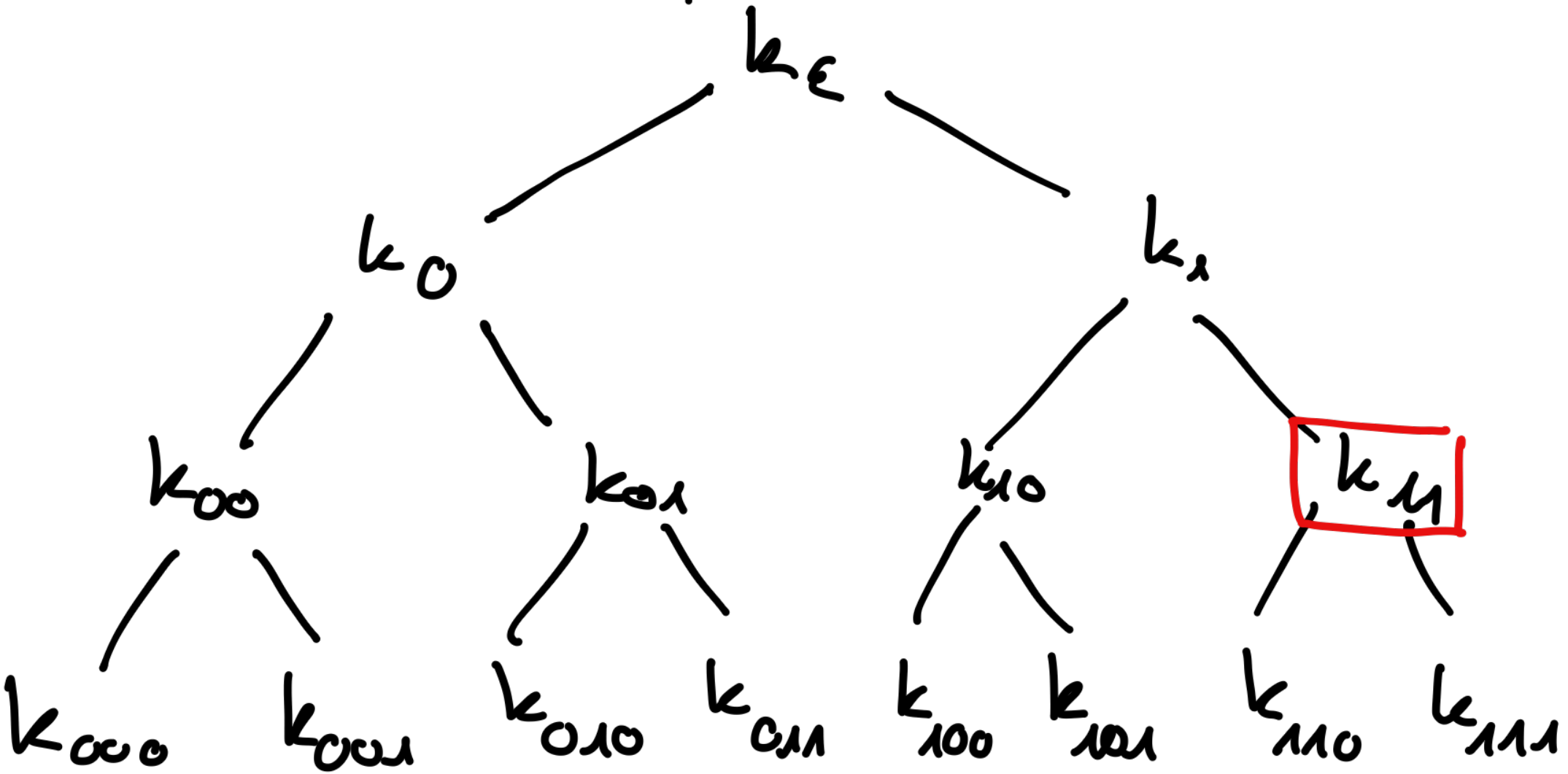
Selective Security



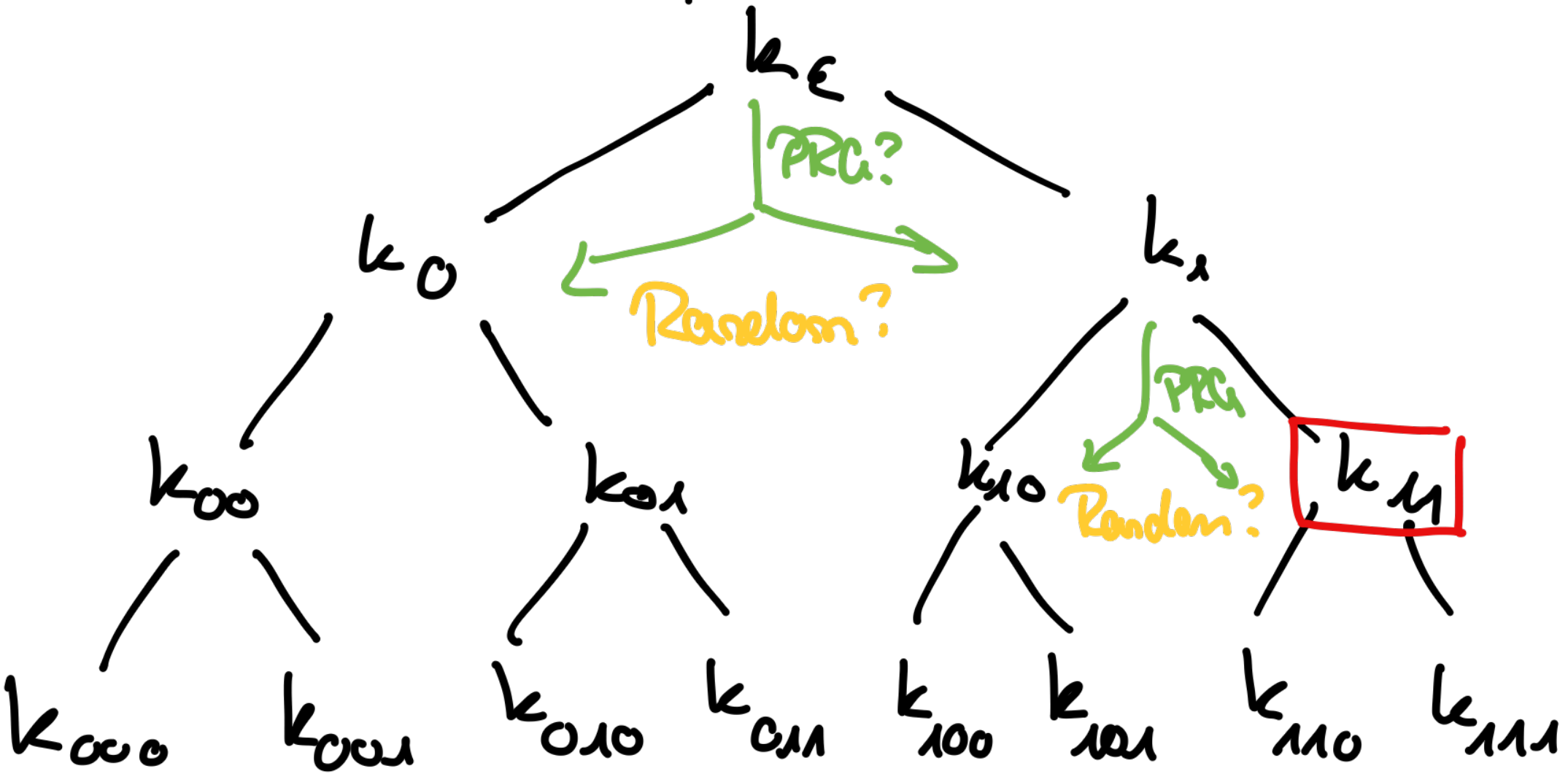
Selective Security



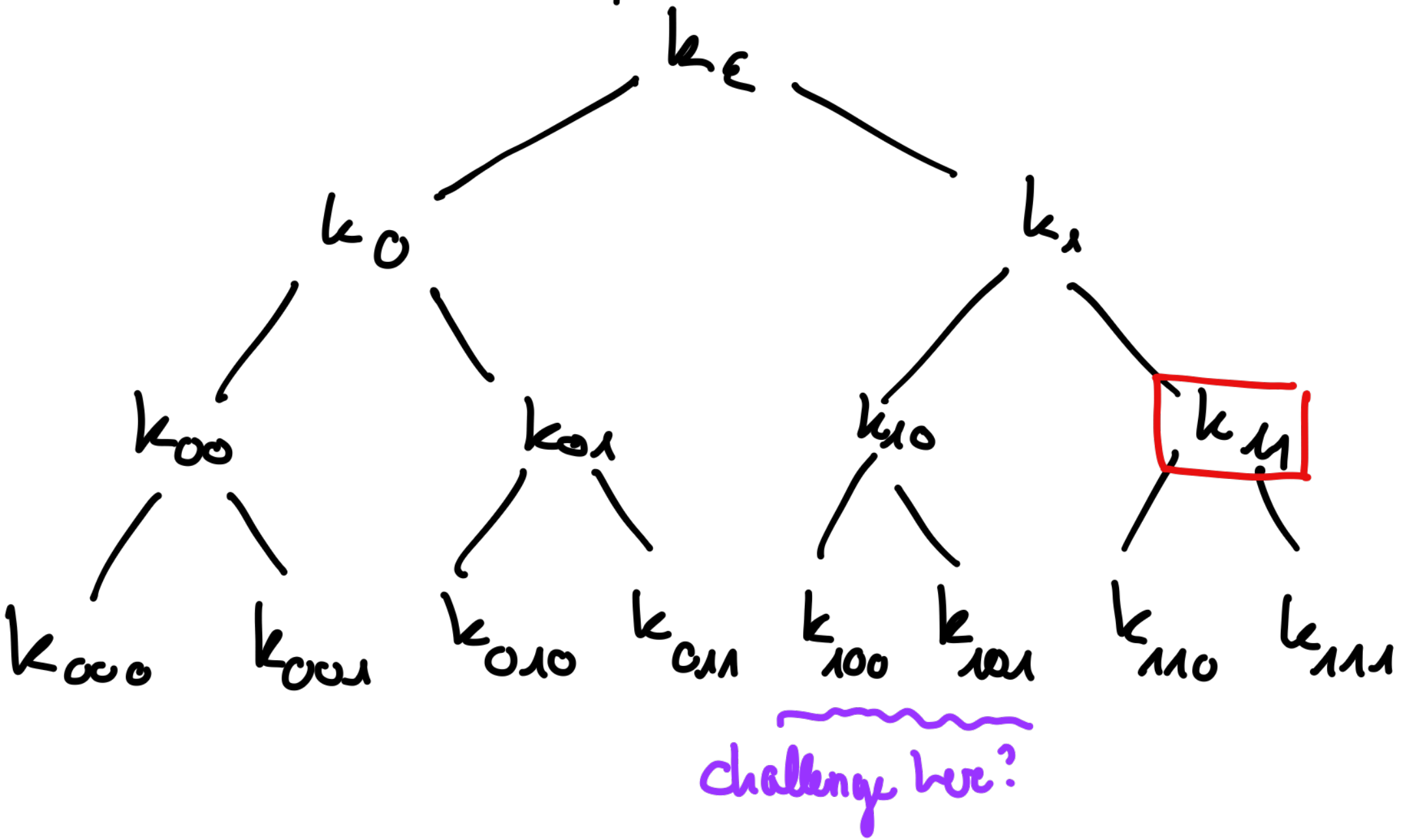
Adaptive Security - Challenges



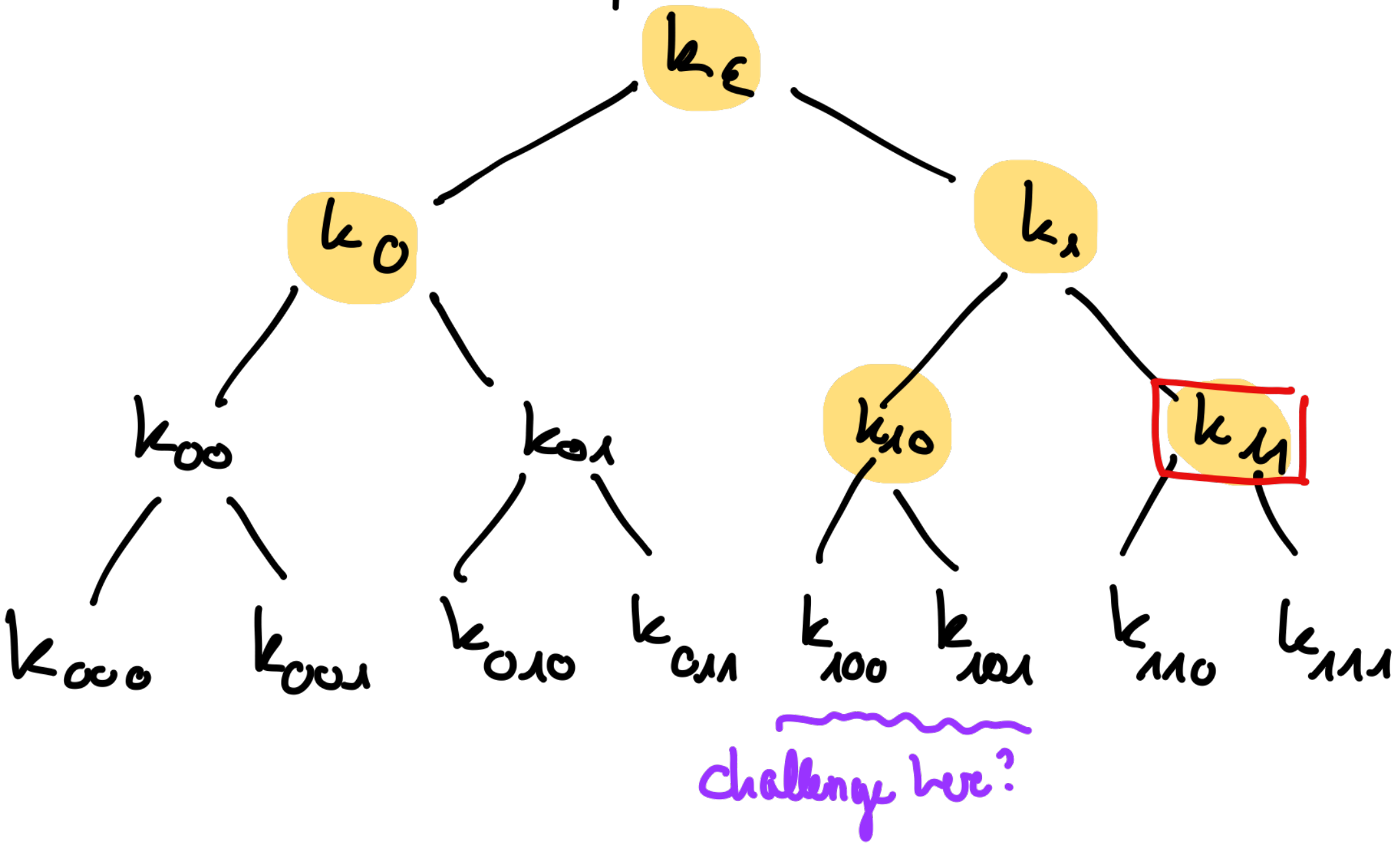
Adaptive Security - Challenges



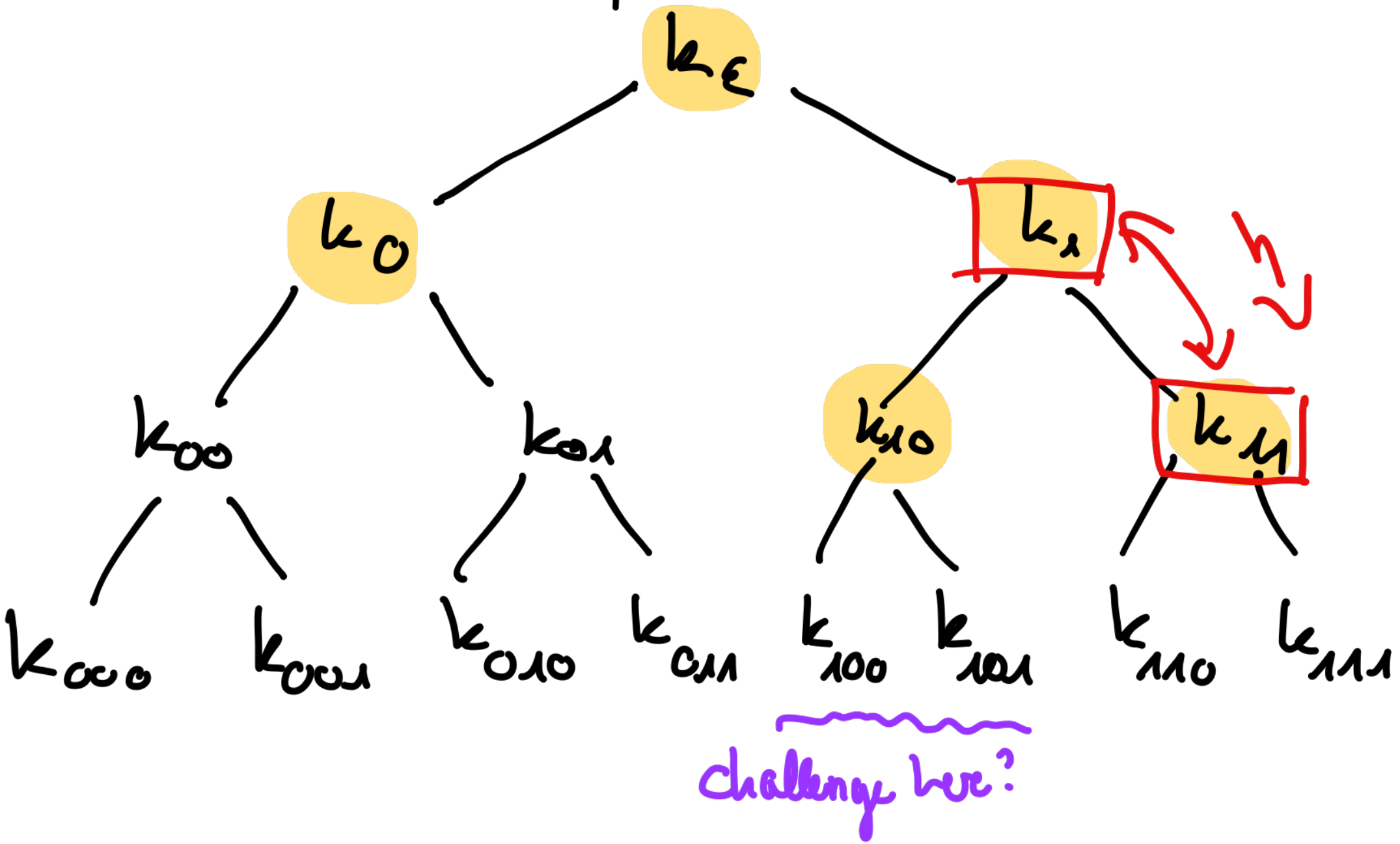
Adaptive Security - Challenges



Adaptive Security - Challenges



Adaptive Security - Challenges



Impossibility Result [KKPW21]

Any straight-line reduction proving adaptive security for the GGM PC-PRF based on the security of the underlying PRG loses a superpolynomial factor in the input size n.

Impossibility Result [KKPW21]

Any straight-line reduction (rewinding!) proving adaptive security for the GGM PC-PRF based on the security of the underlying PRG loses a superpolynomial factor in the input size n.

Impossibility Result [KKPW21]

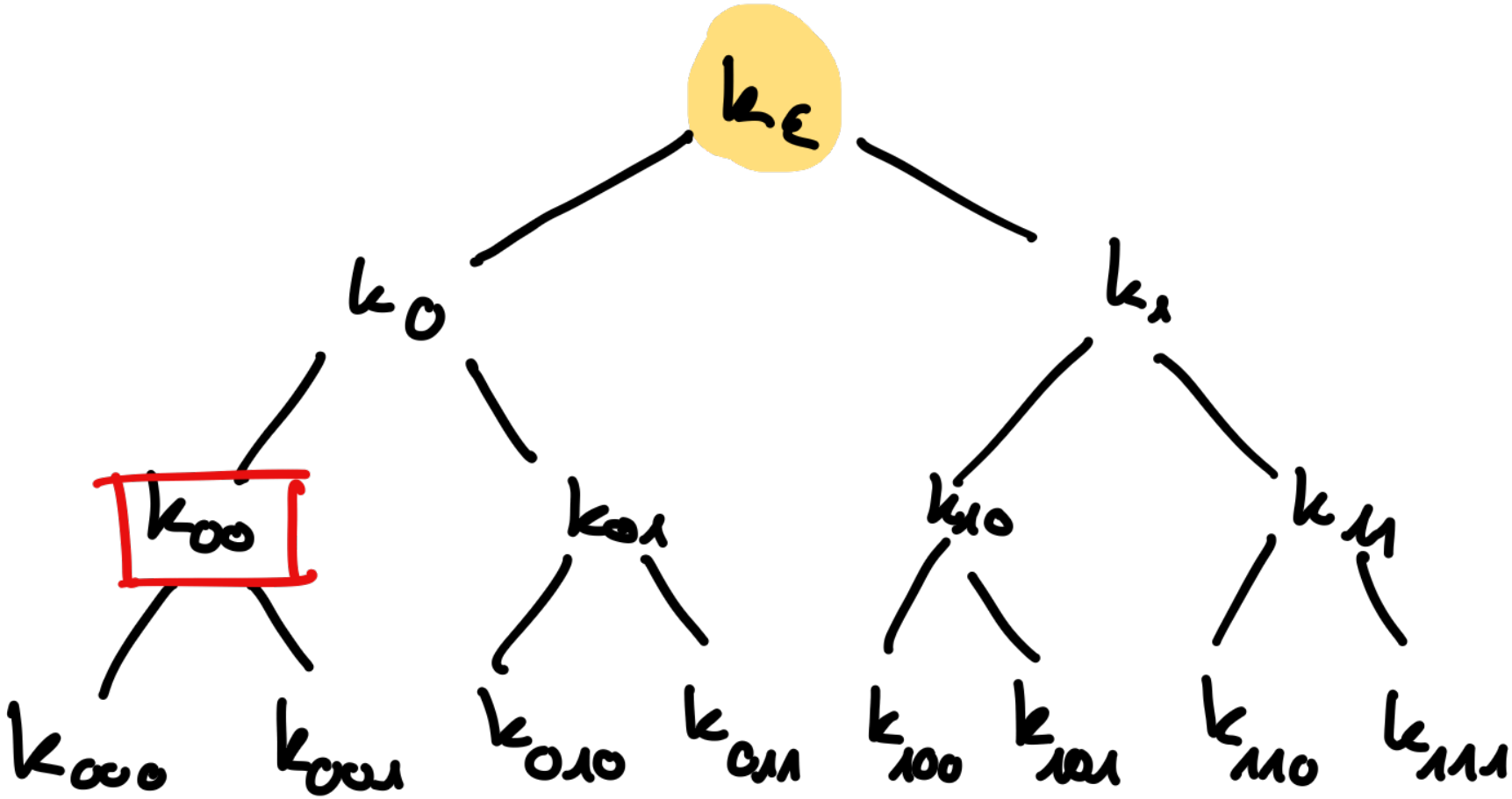
Any straight-line reduction (rewinding!) proving adaptive security for the GGM PC-PRF based on the security of the underlying PRG loses a ~~super-polynomial~~ factor in the input size n.

polynomial

Adversarial views

- Corruptions
- honest PRG
- random values

Corrupt k_{00}

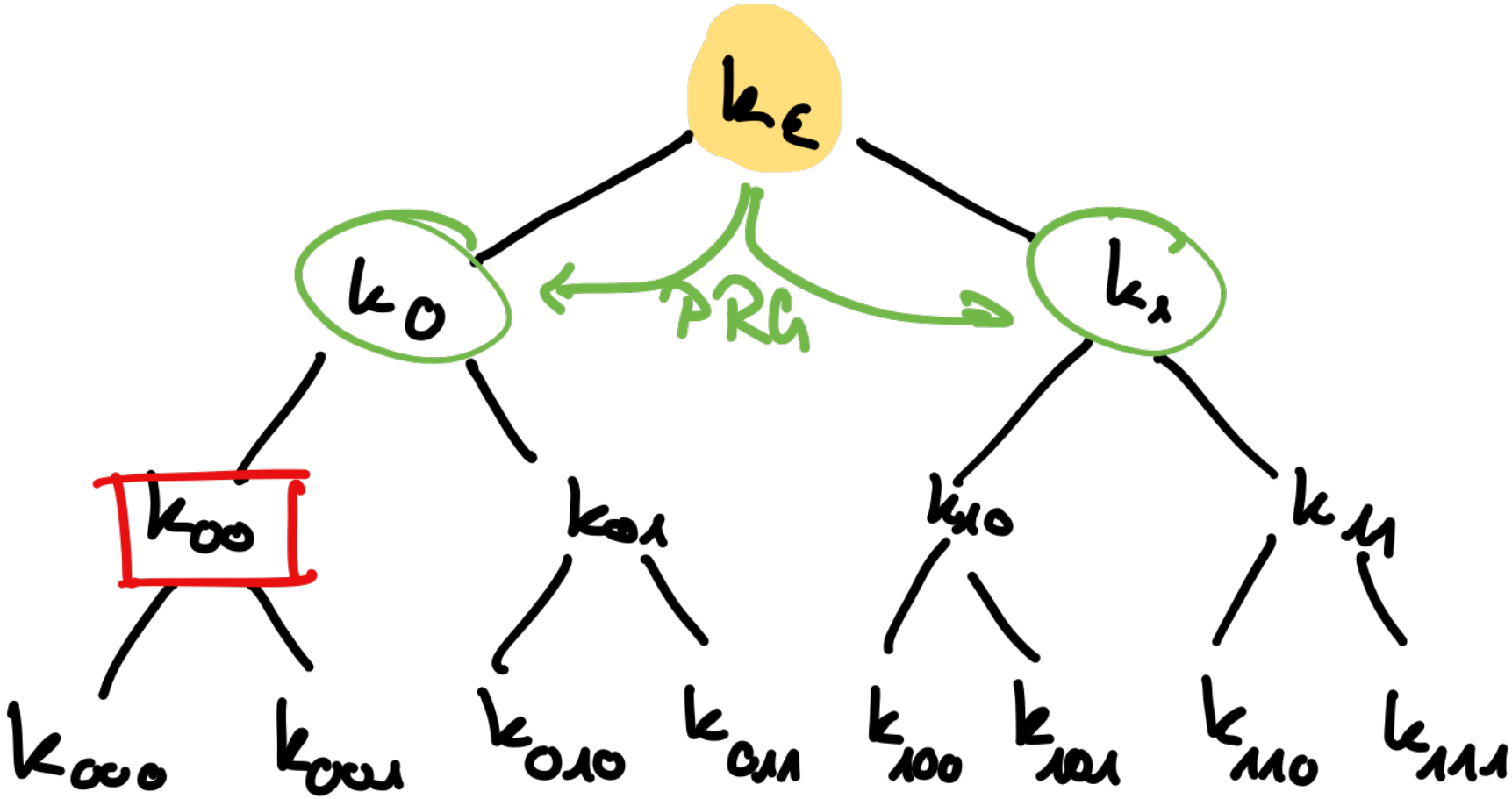


Adversarial views

- Corruptions
- honest PRG
- random values

Corrupt k_{00}

PRG ε



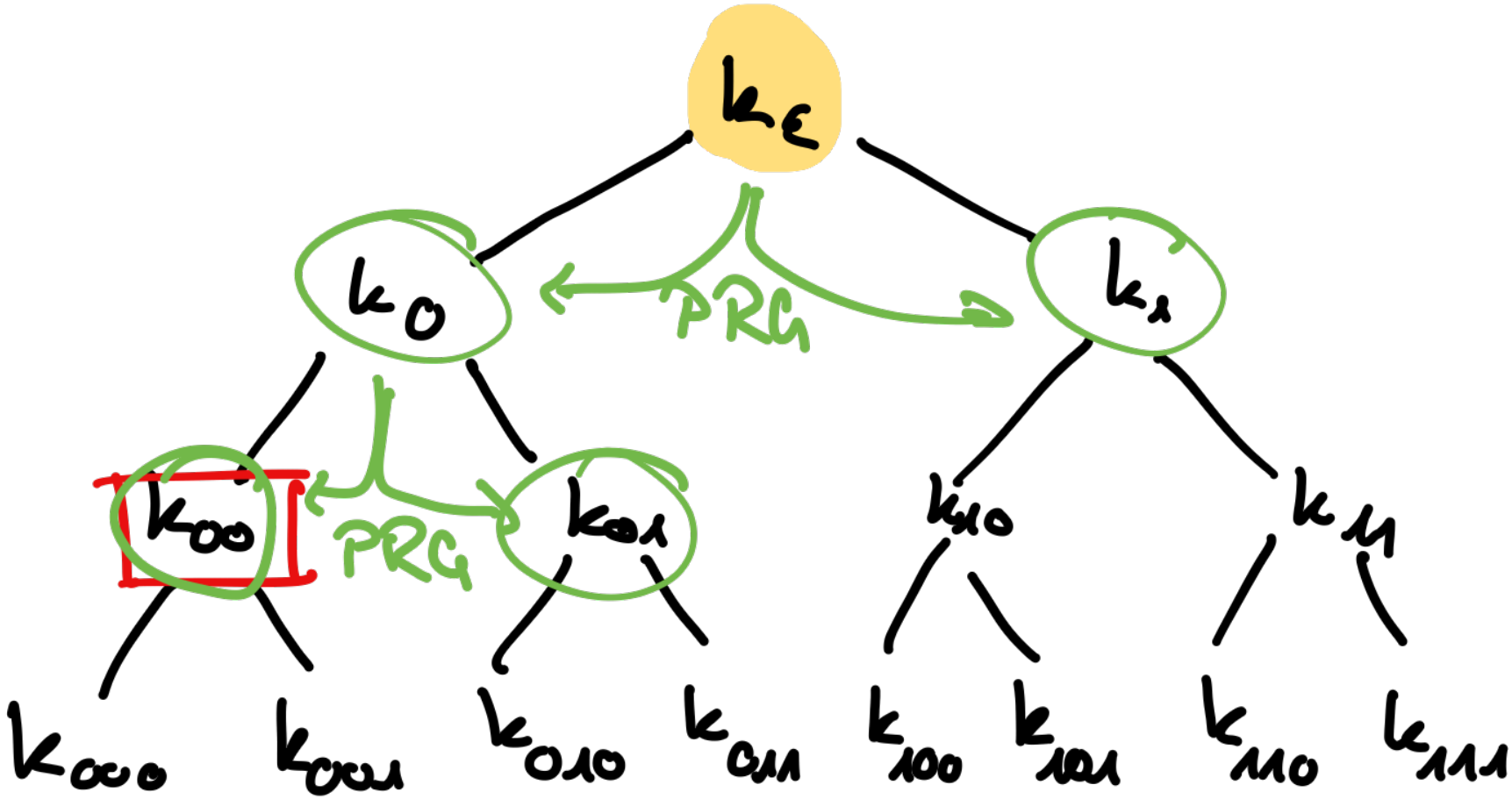
Adversarial views

- Corruptions
- honest PRG
- random values

Corrupt k_{00}

PRG ε

PRG 0



Adversarial views

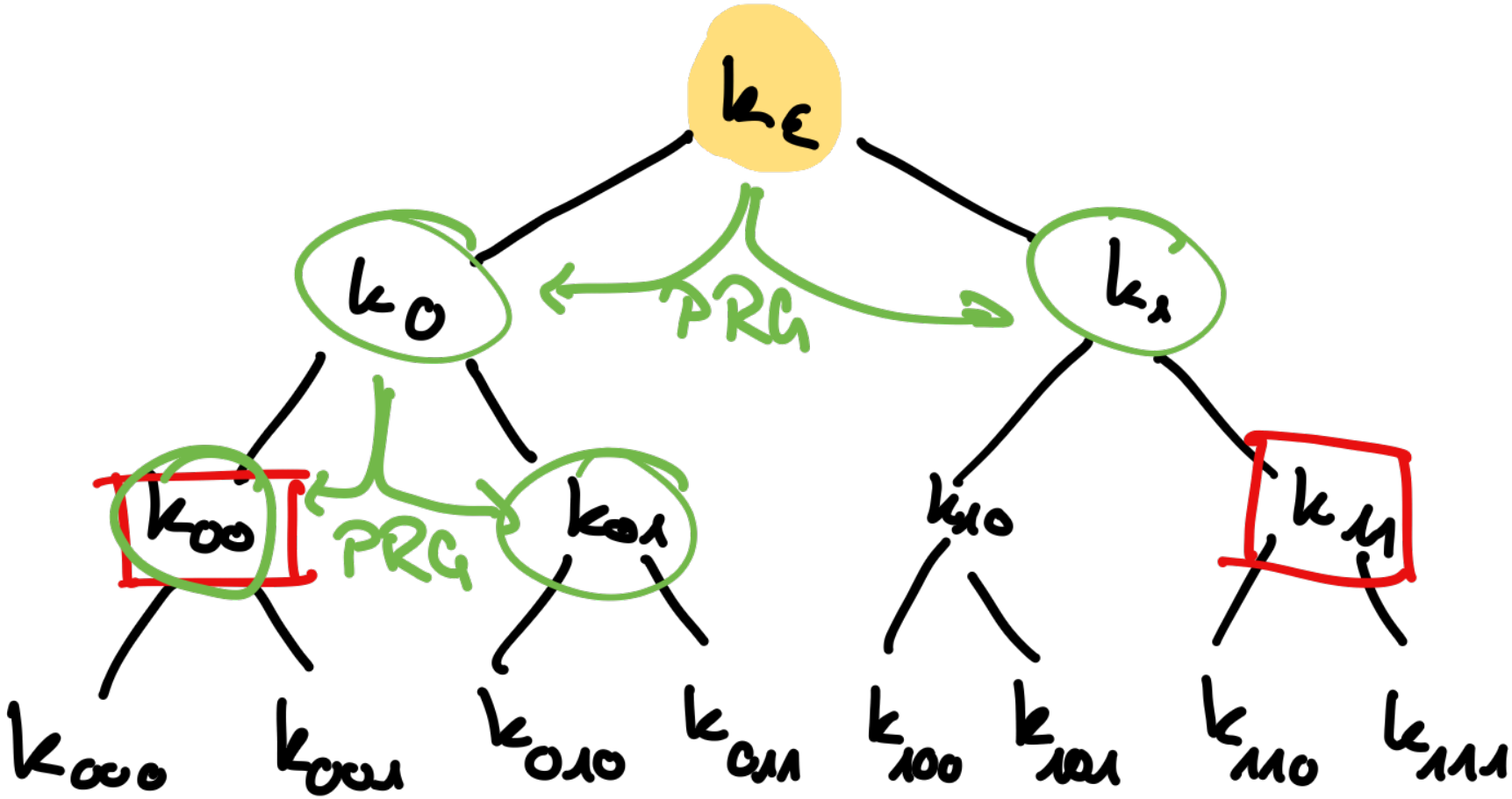
- Corruptions
- honest PRG
- random values

Corrupt k_{00}

PRG ε

PRG 0

corrupt k_{11}



Adversarial views

- Corruptions
- honest PRG
- random values

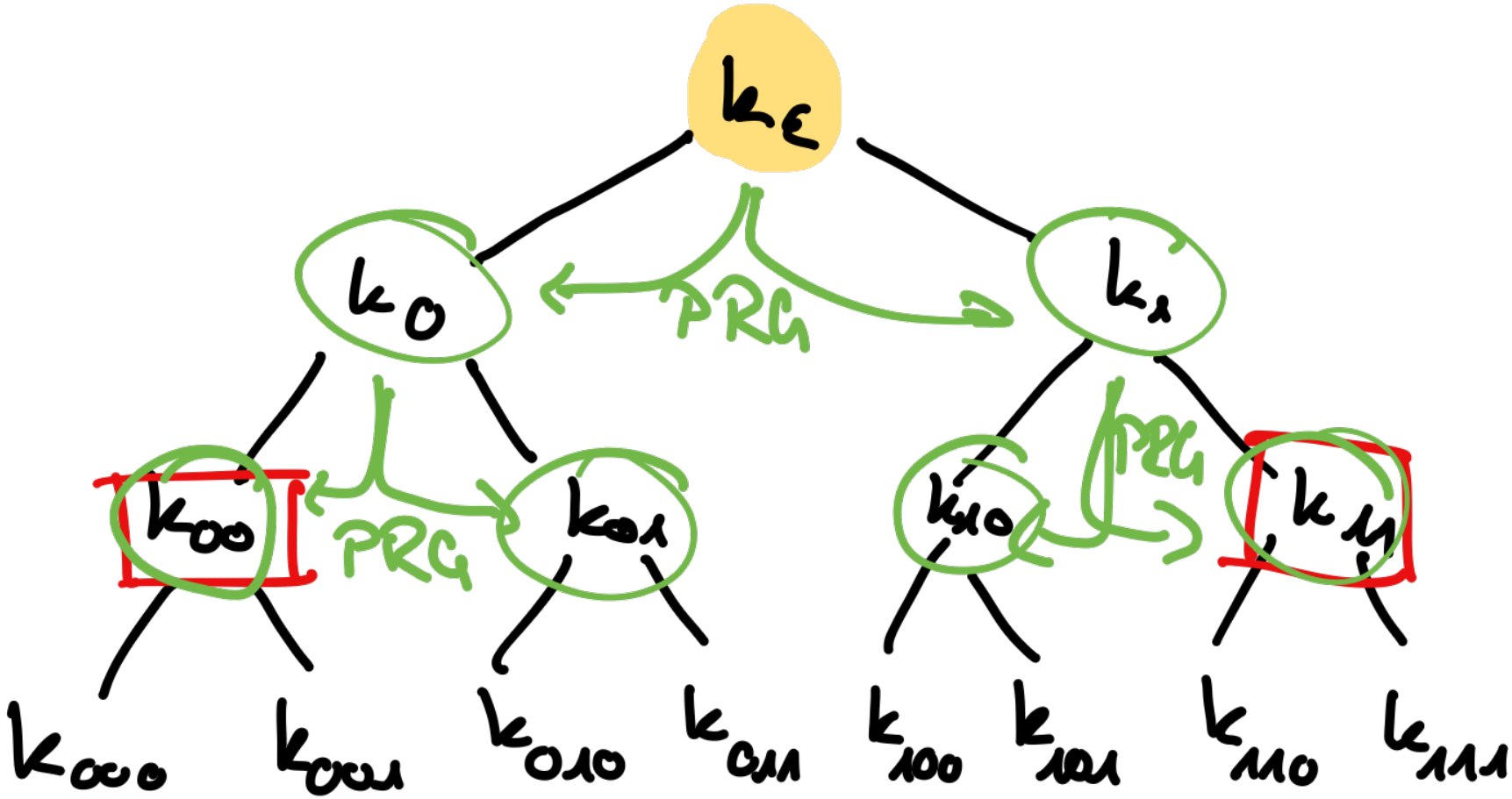
Corrupt k_{00}

PRG ε

PRG 0

Corrupt k_{11}

PRG 1



Adversarial views

- Corruptions
- honest PRG
- random values

Corrupt k_{00}

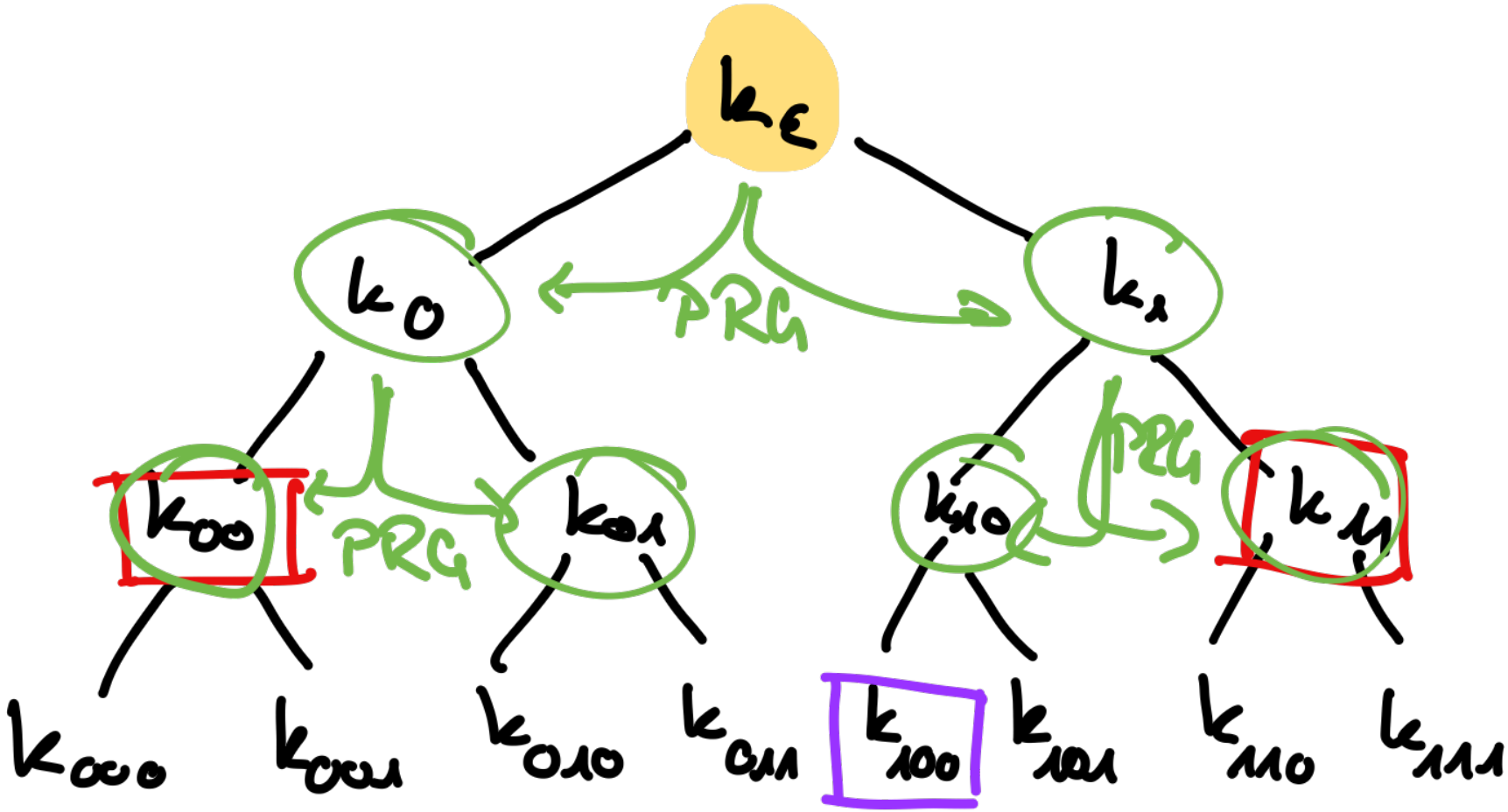
PRG ε

PRG 0

Corrupt k_{11}

PRG 1

challenge 100



Adversarial views

- Corruptions
- honest PRG
- random values

Corrupt k_{00}

PRG ε

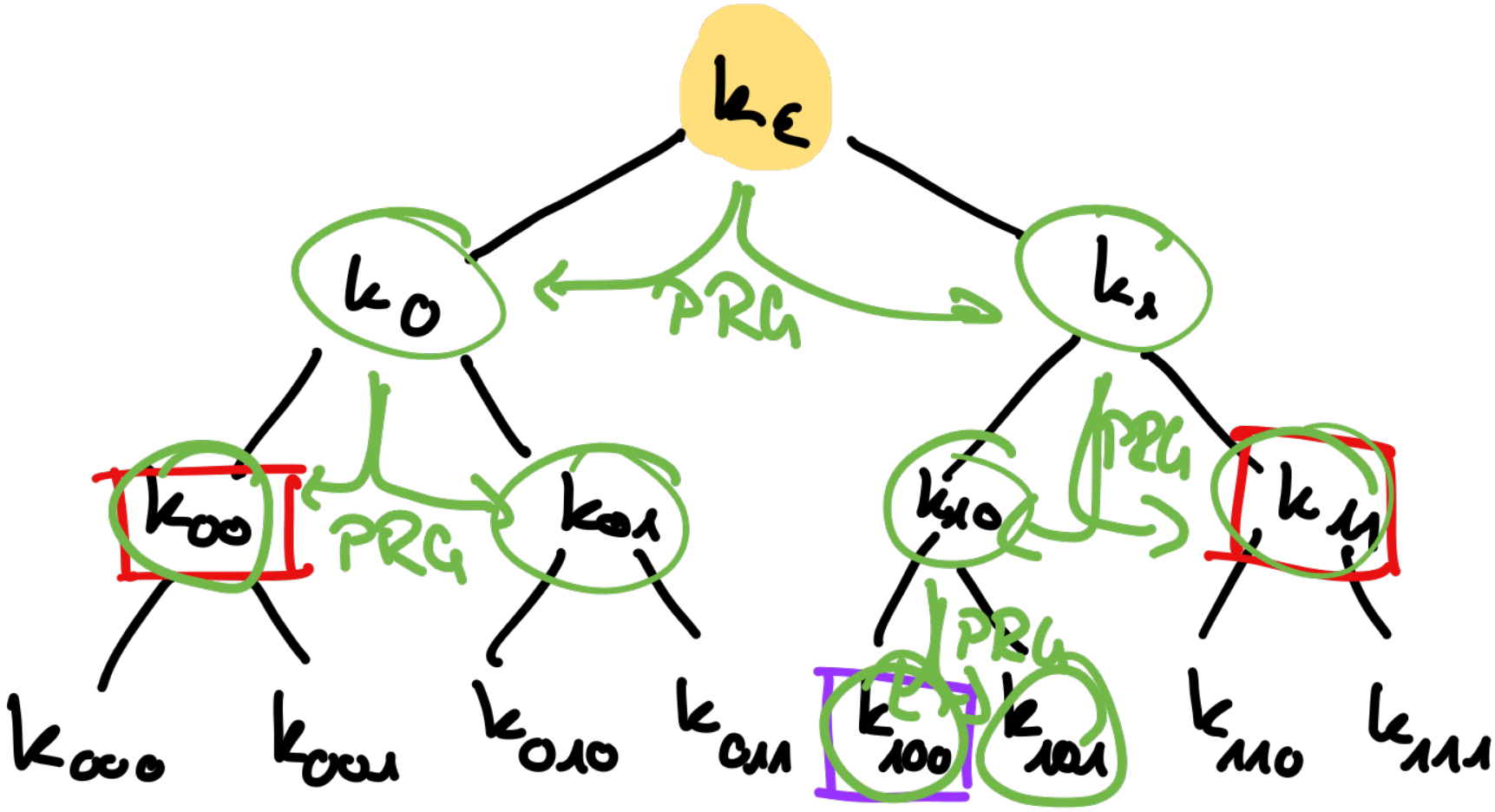
PRG 0

Corrupt k_{11}

PRG 1

Challenge 100

PRG 10



Adversarial views

- corruptions
- honest PRG
- random value
- ← rewinding index

Corrupt k_{00} ←

PRG ε

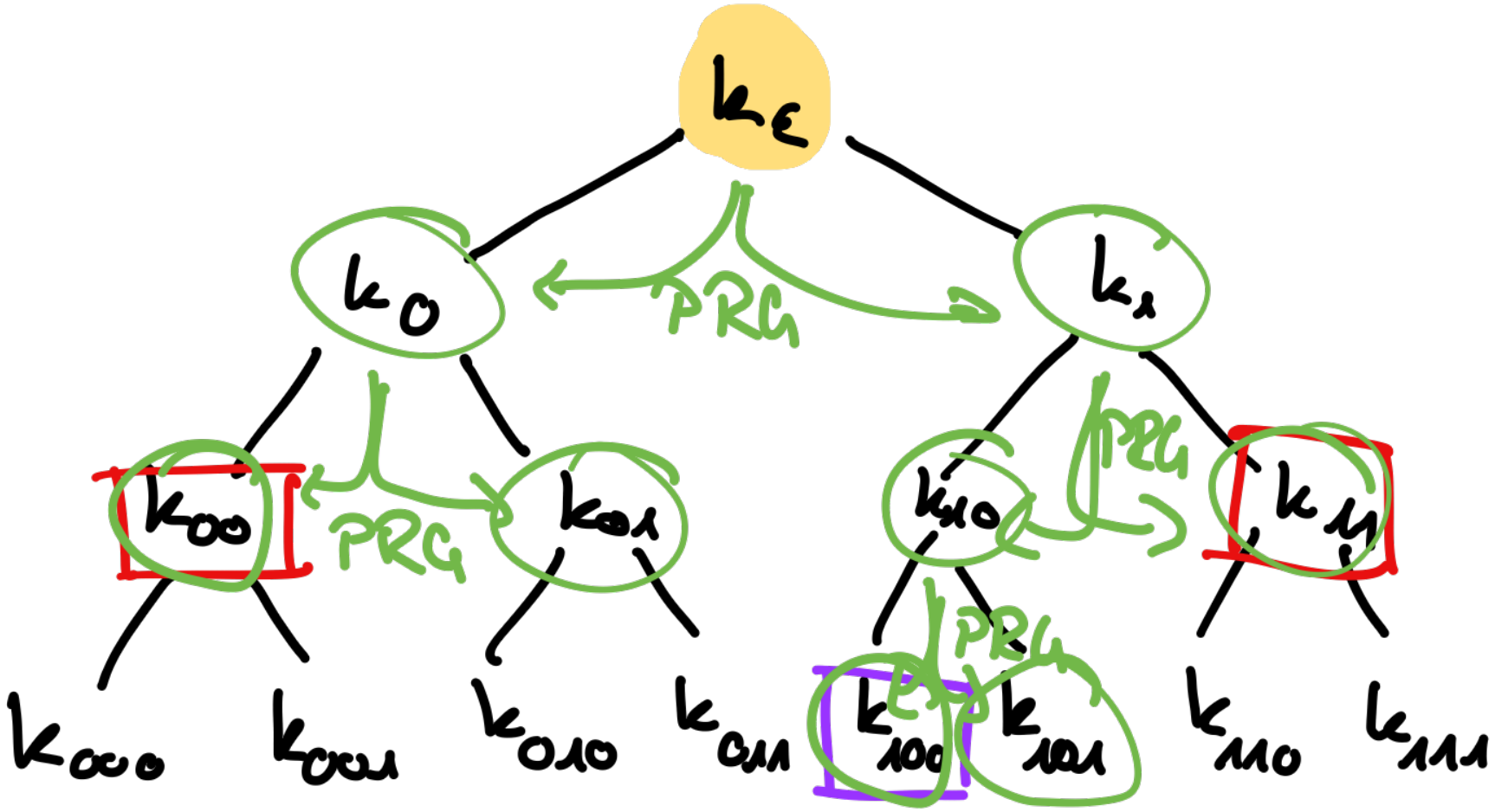
PRG 0

corrupt k_{11}

PRG 1

challenge 100

PRG 10



Adversarial views

- corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

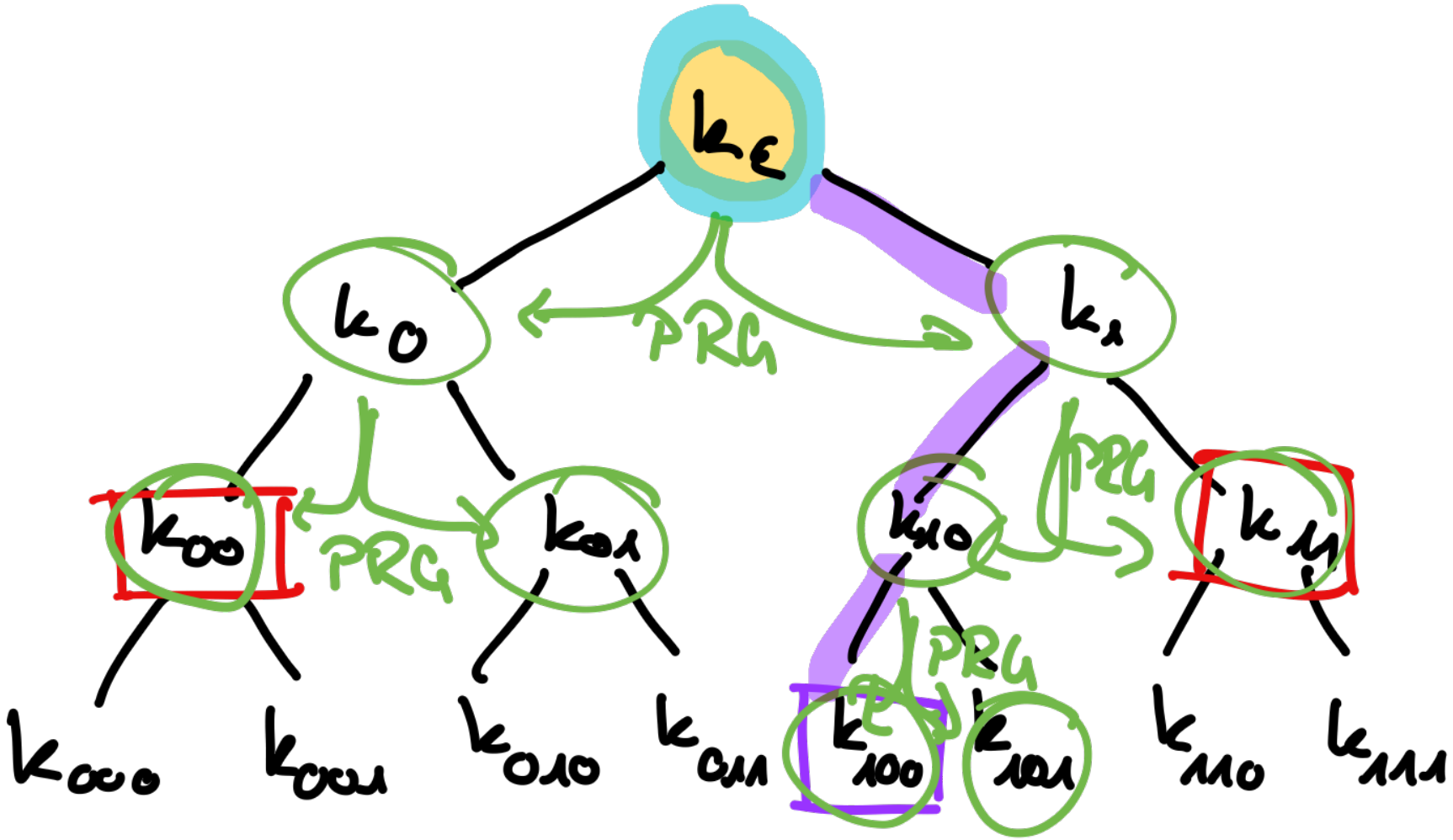
PRG 0

Corrupt k_{11}

PRG 1

challenge 100

PRG 10

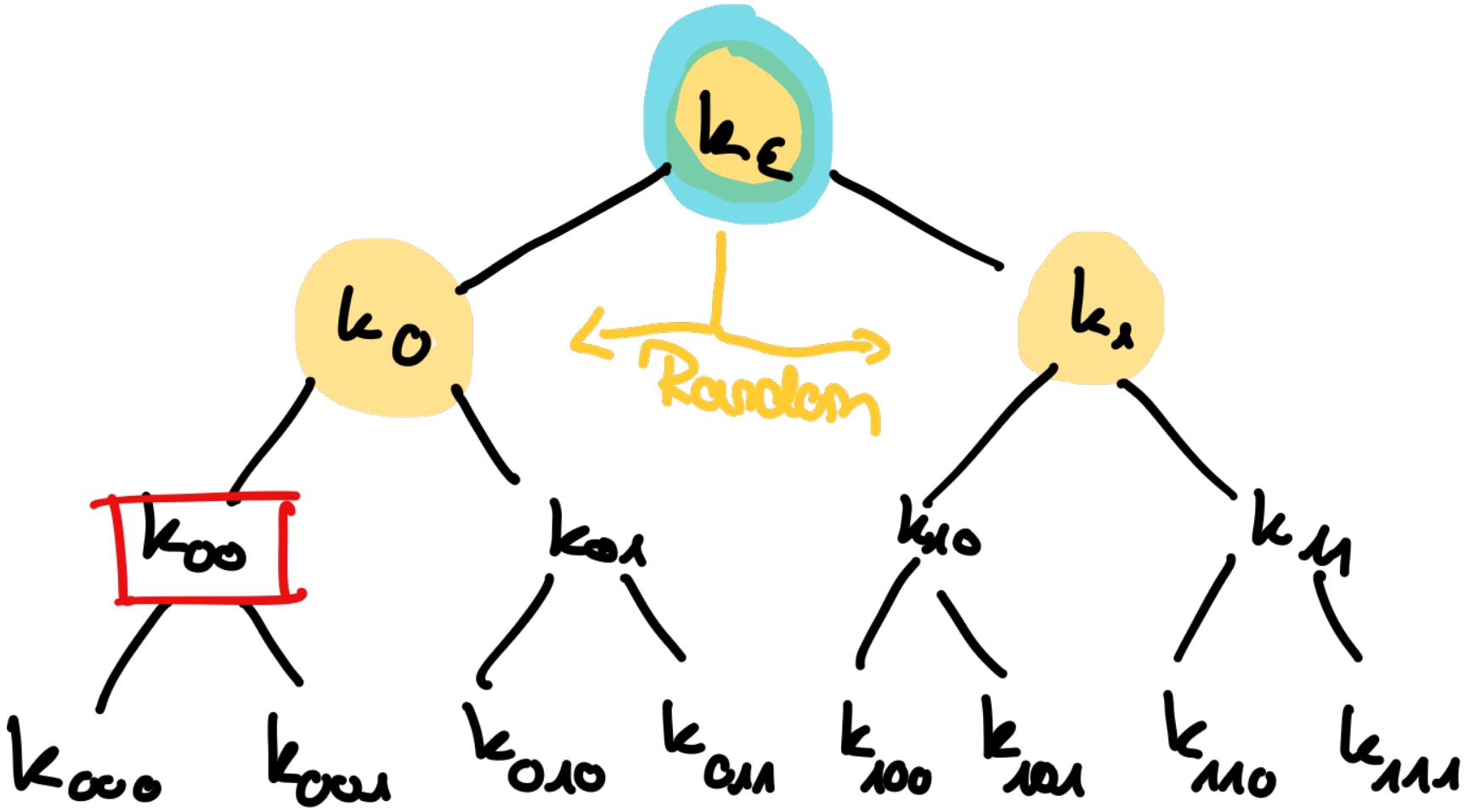


Adversarial views

Corrupt k_{00}

PRG ε

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index



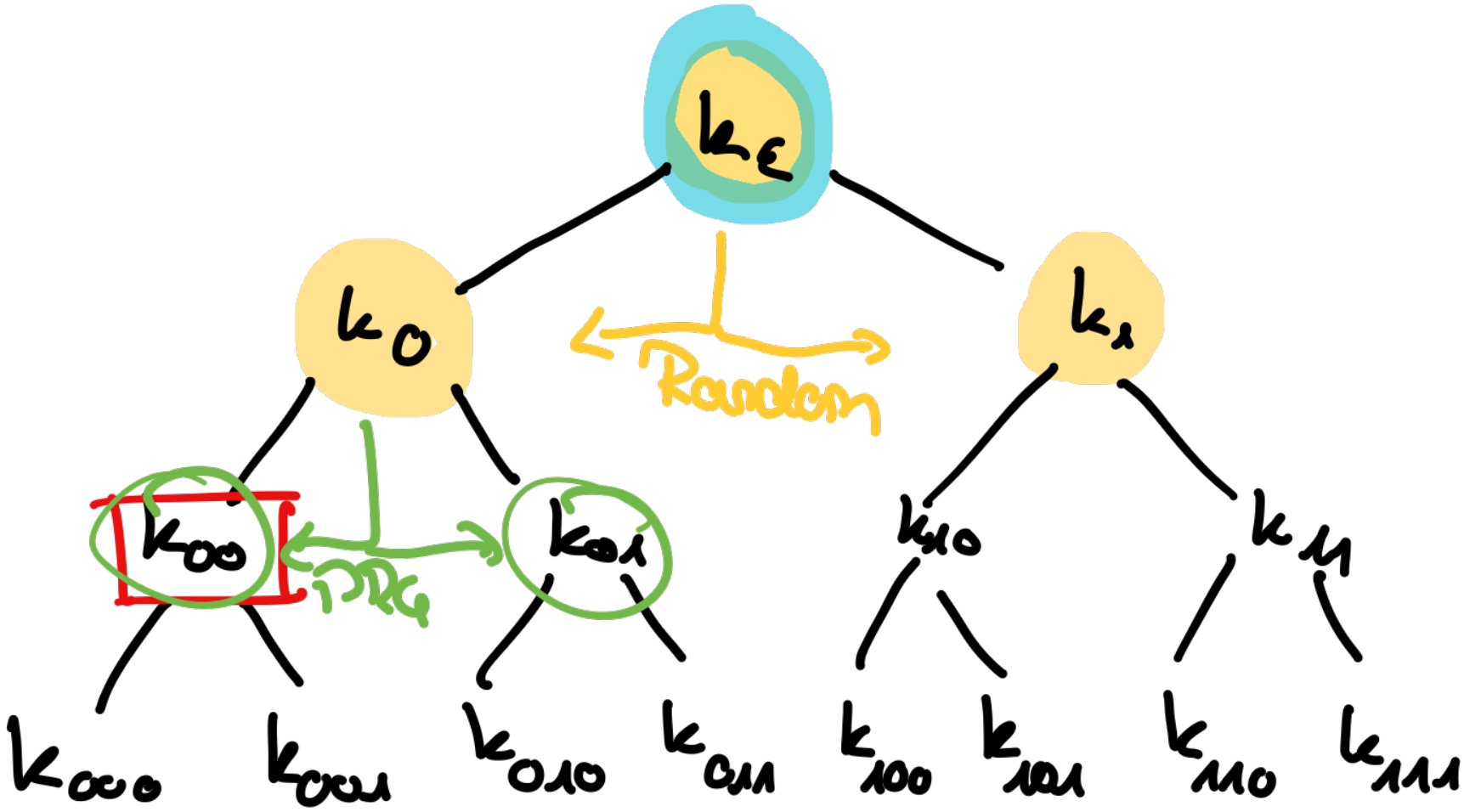
Adversarial views

Corrupt k_{00}

PRG ε

PRG 0

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index



Adversarial views

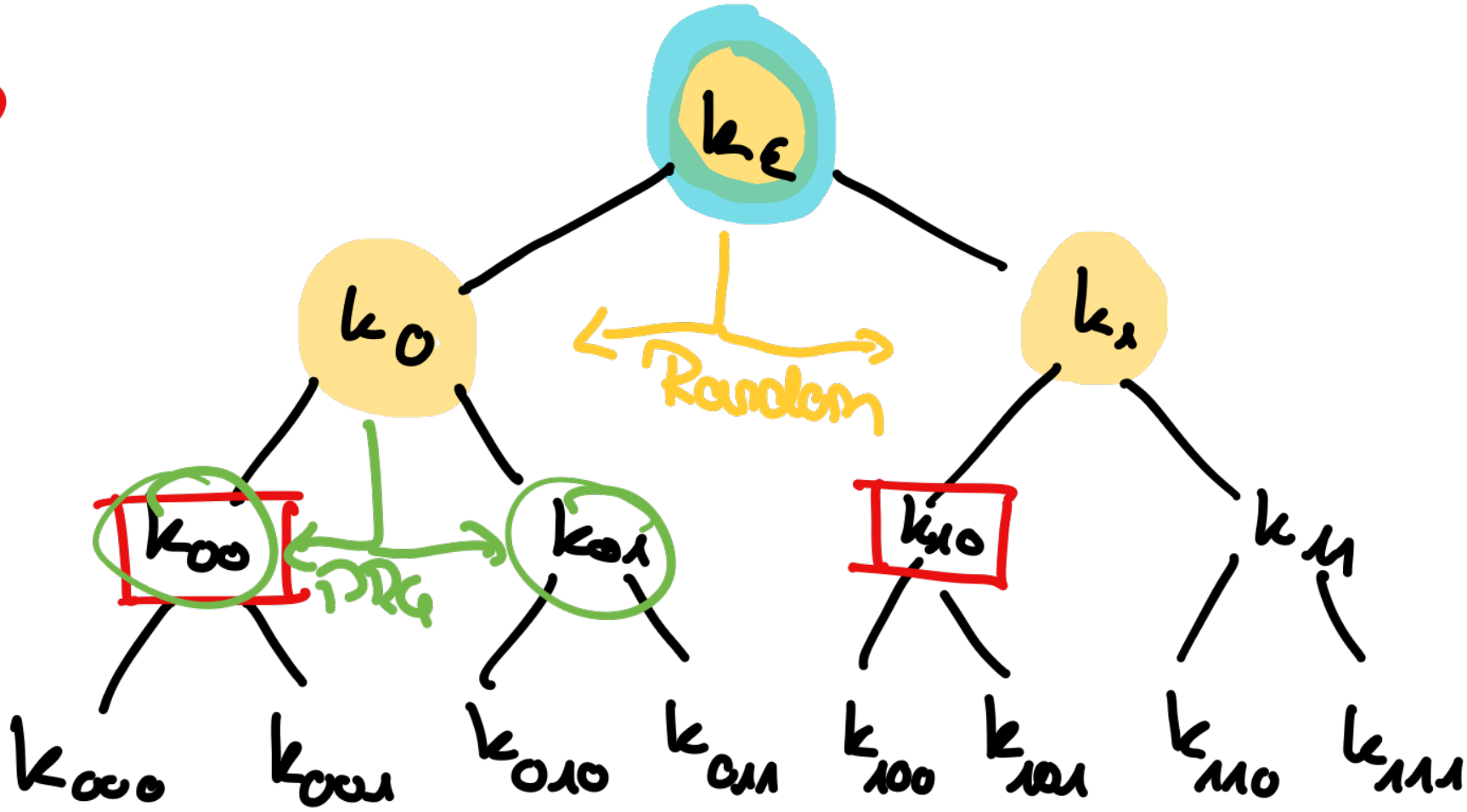
- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε ←

PRG 0

Corrupt k_{10}



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

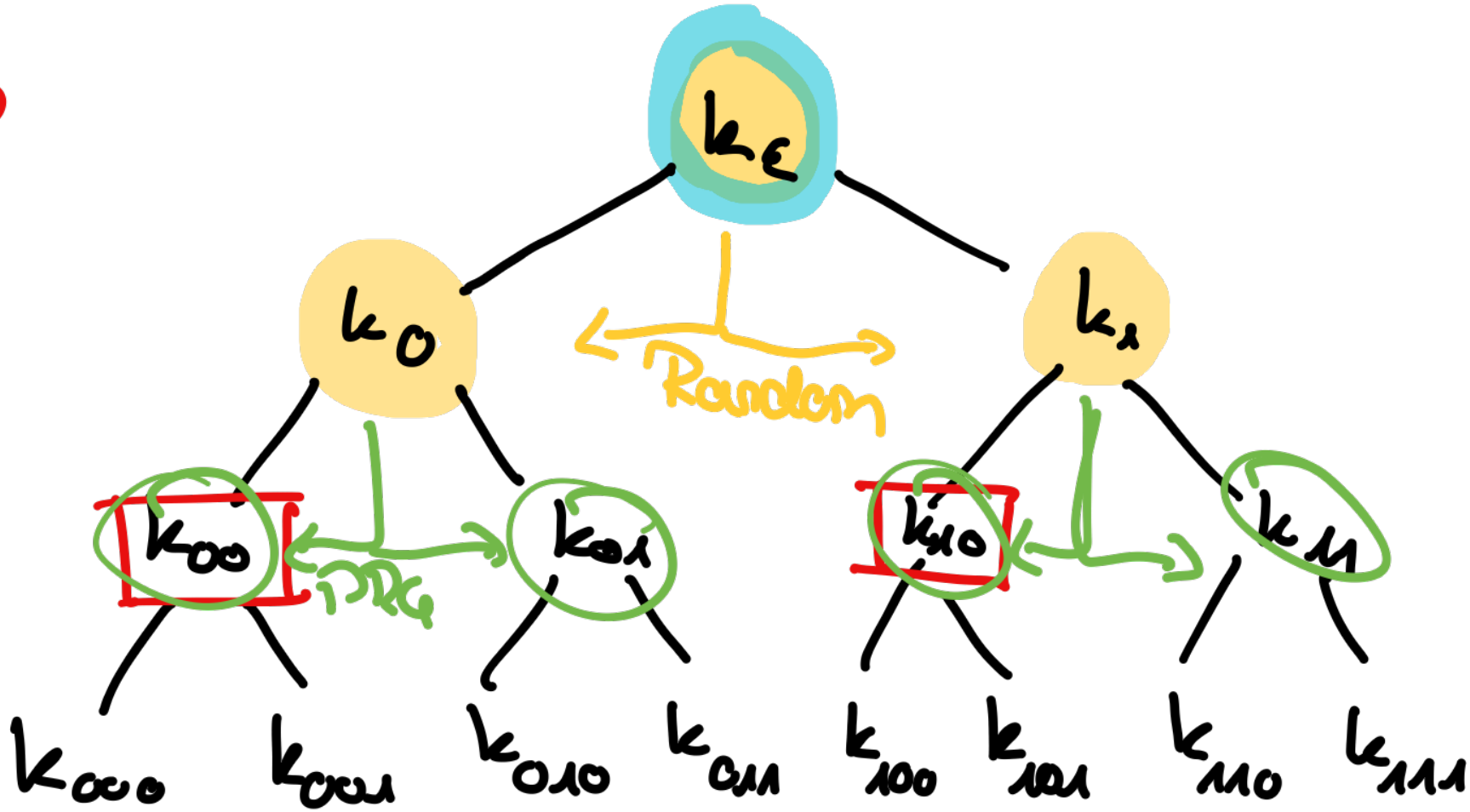
Corrupt k_{00}

PRG ε ←

PRG 0

Corrupt k_{10}

PRG 1



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

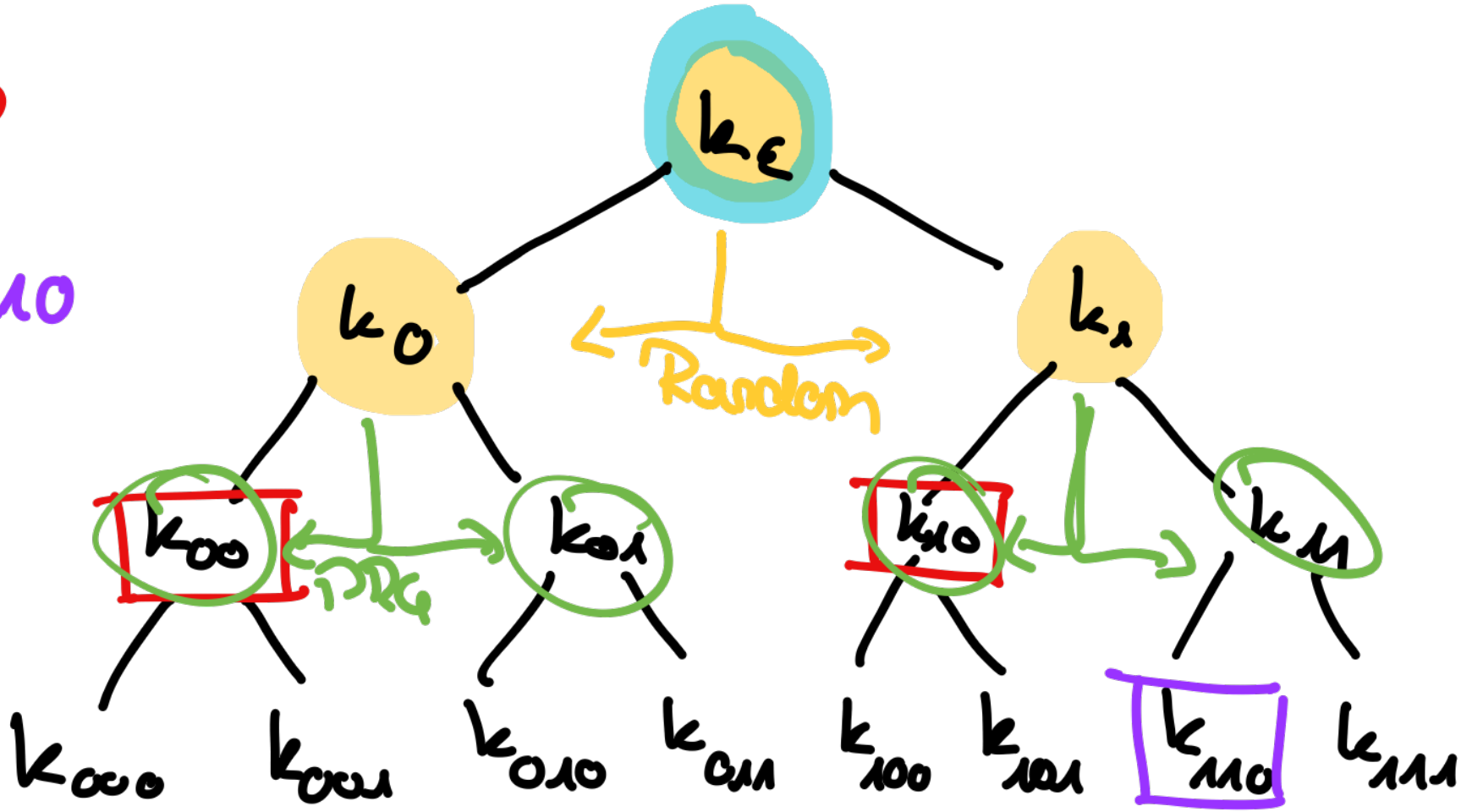
PRG ε ←

PRG 0

Corrupt k_{10}

PRG 1

challenge k_{110}



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

PRG 0

Corrupt k_{10}

PRG 1

challenge k_{110}

PRG 11

Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

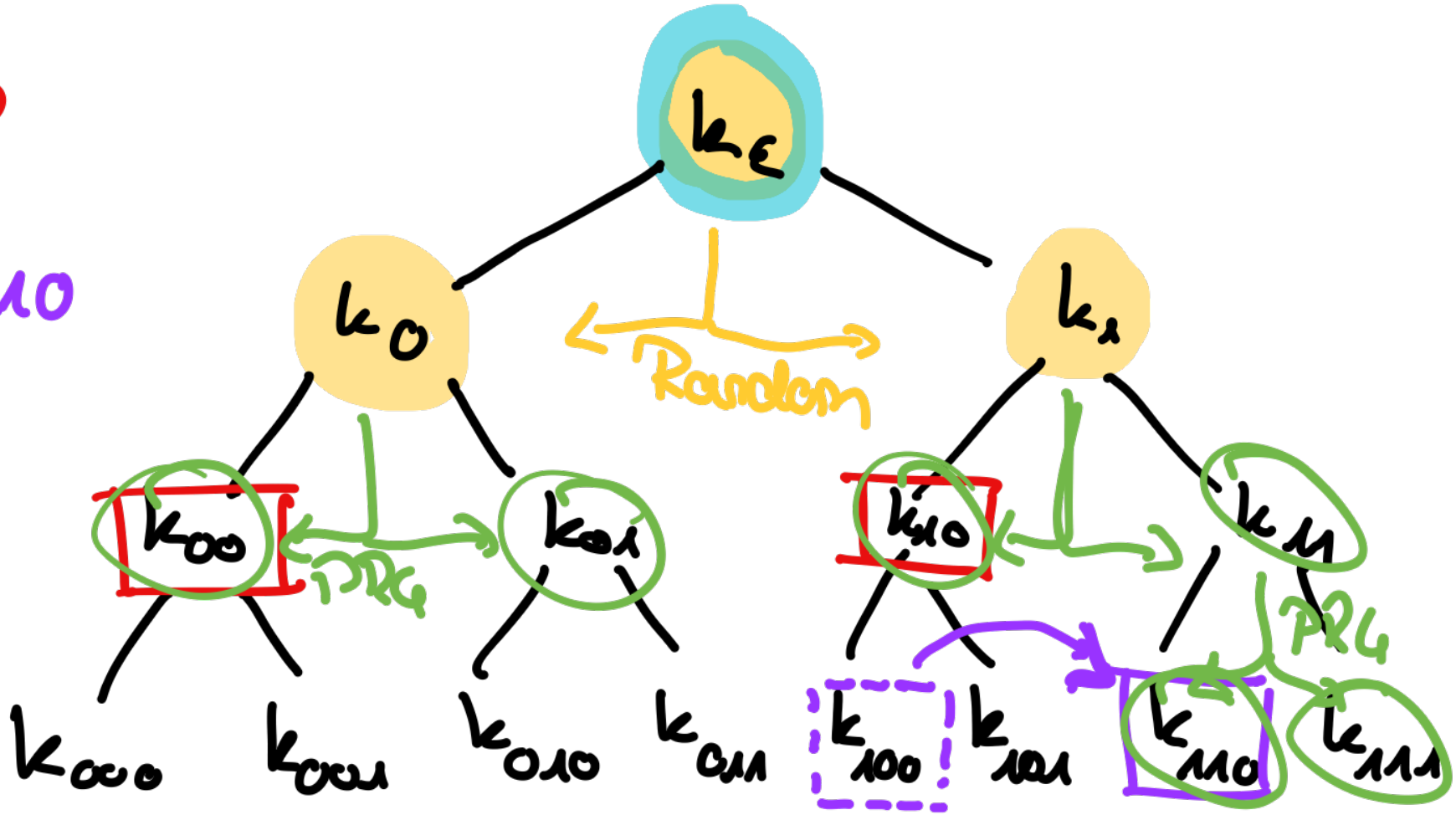
PRG 0

Corrupt k_{10}

PRG 1

challenge k_{110}

PRG 11



Adversarial views

- corruption's
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

PRG 0

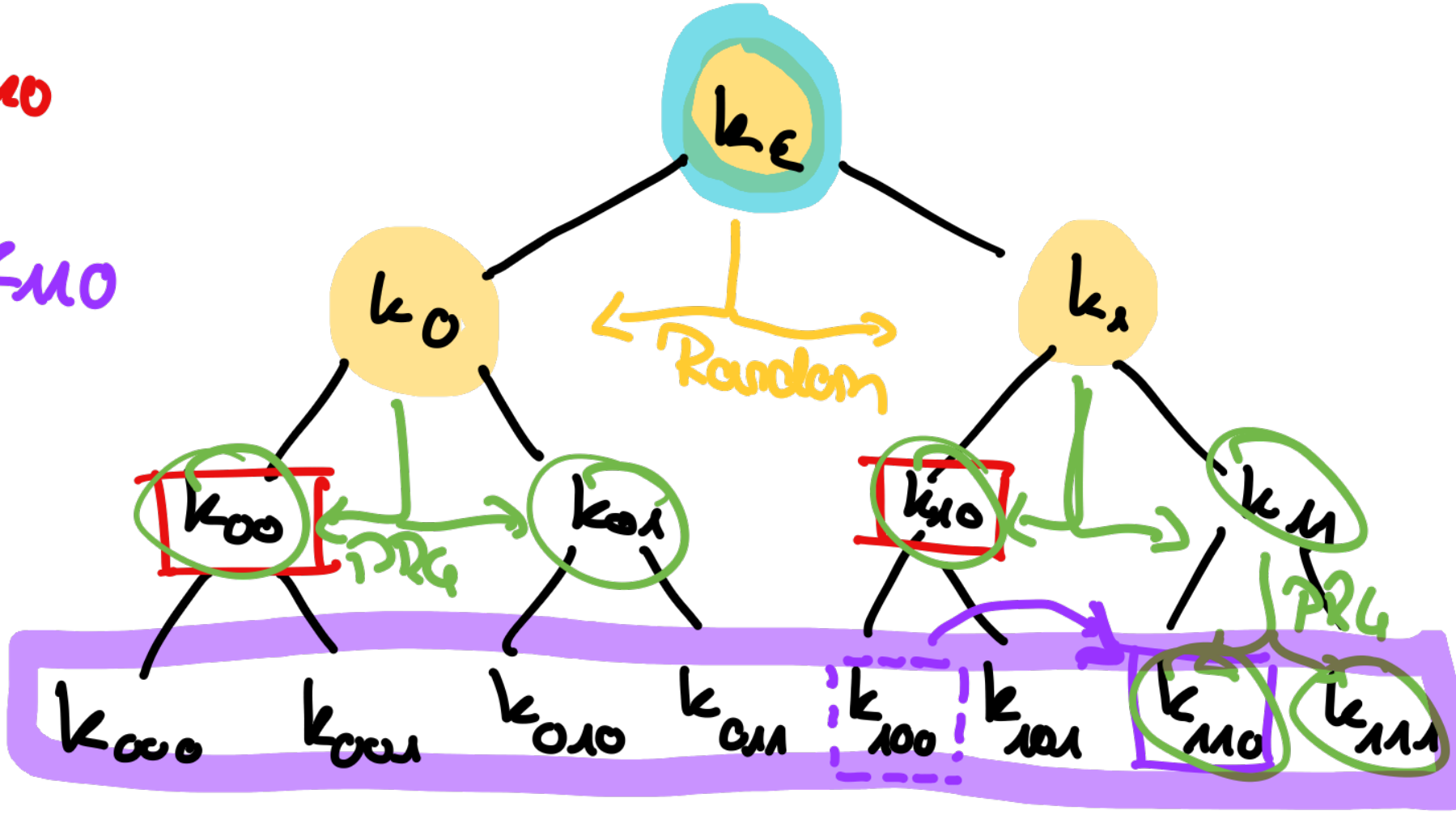
Corrupt k_{10}

PRG 1

challenge k_{110}

PRG 11

exponential



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

PRG 0

Corrupt k_{10}

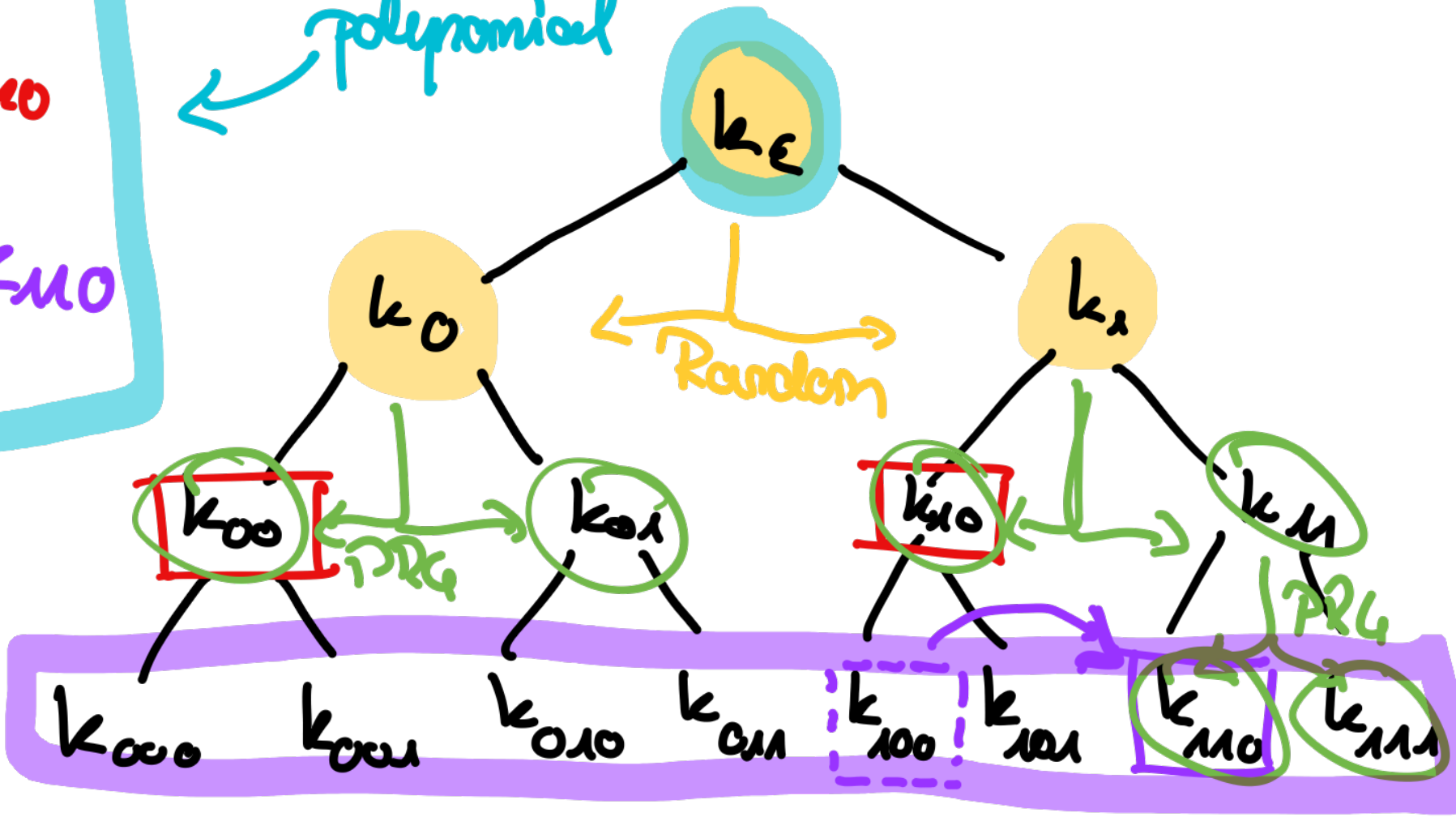
PRG 1

challenge k_{110}

PRG 11

polynomial

exponential



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

PRG 0

Corrupt k_{10}

PRG 1

challenge k_{110}

PRG 11

Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

PRG 0

Corrupt k_{10}

PRG 1

challenge k_{110}

PRG 11

Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

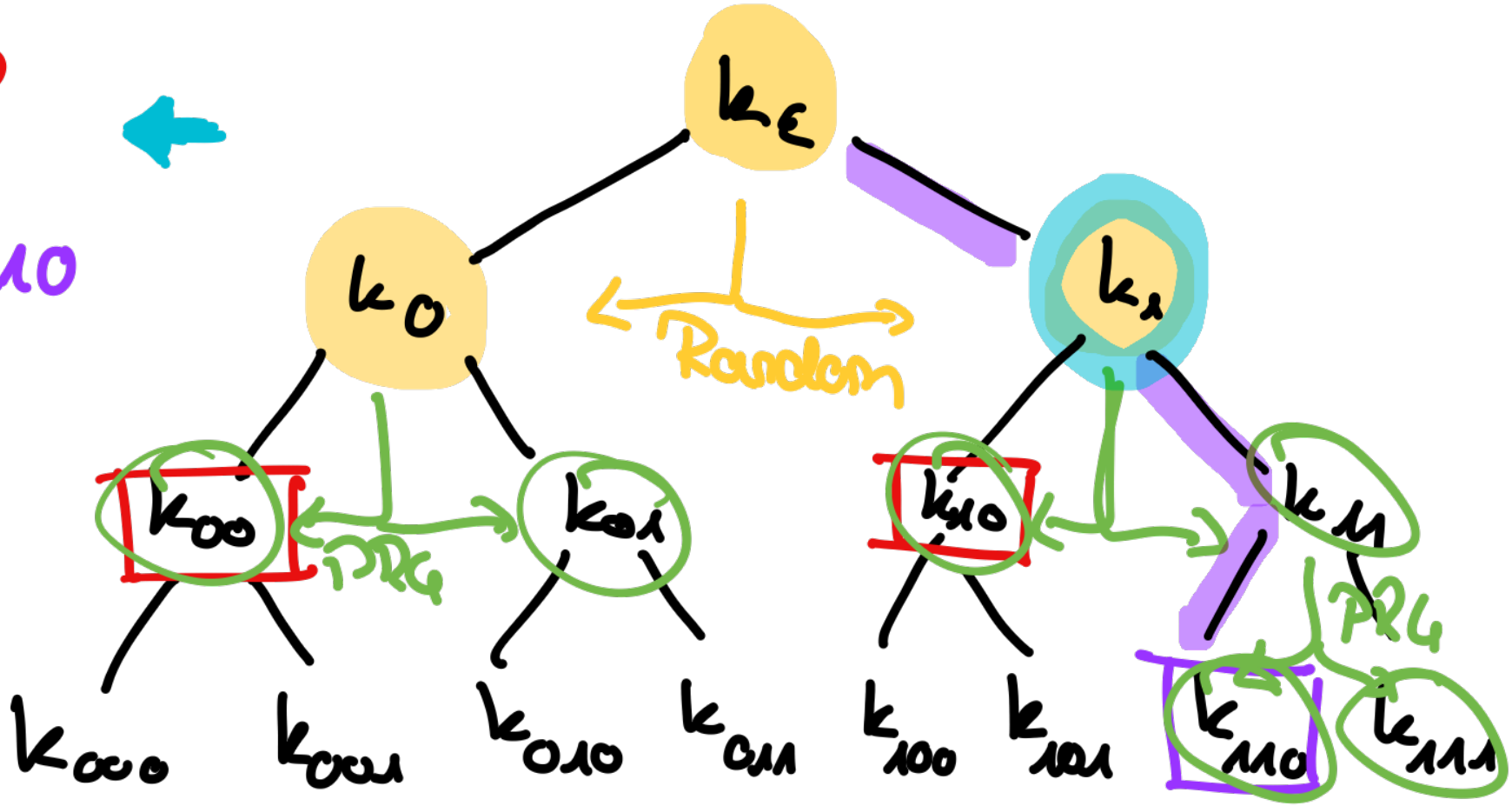
PRG 0

Corrupt k_{10}

PRG 1

challenge k_{110}

PRG 11



Adversarial views

- corruptions
- honest PRG
- random values
- rewinding index
- relevant index

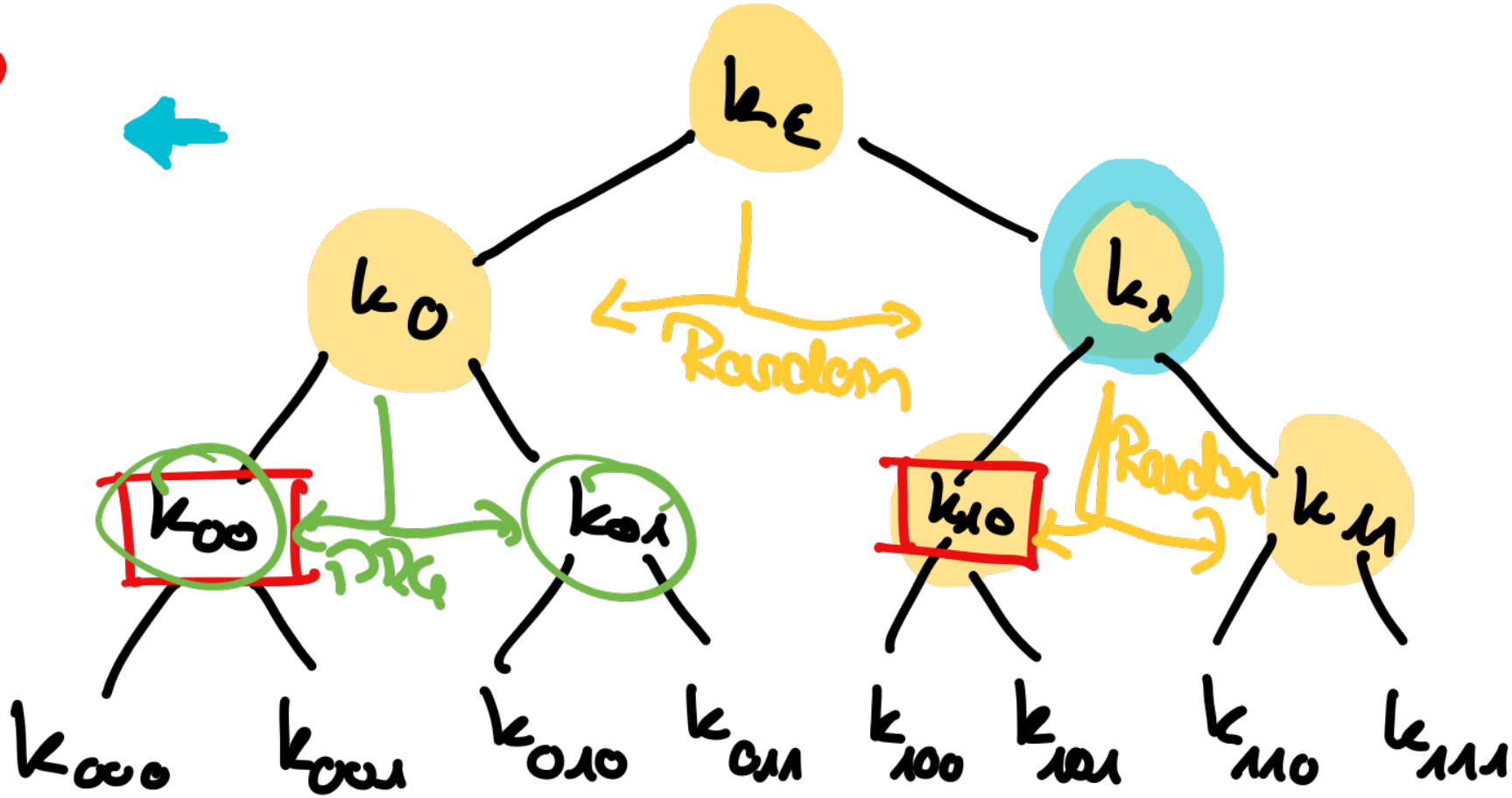
Corrupt k_{00}

PRG ε

PRG 0

Corrupt k_{10}

PRG 1



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

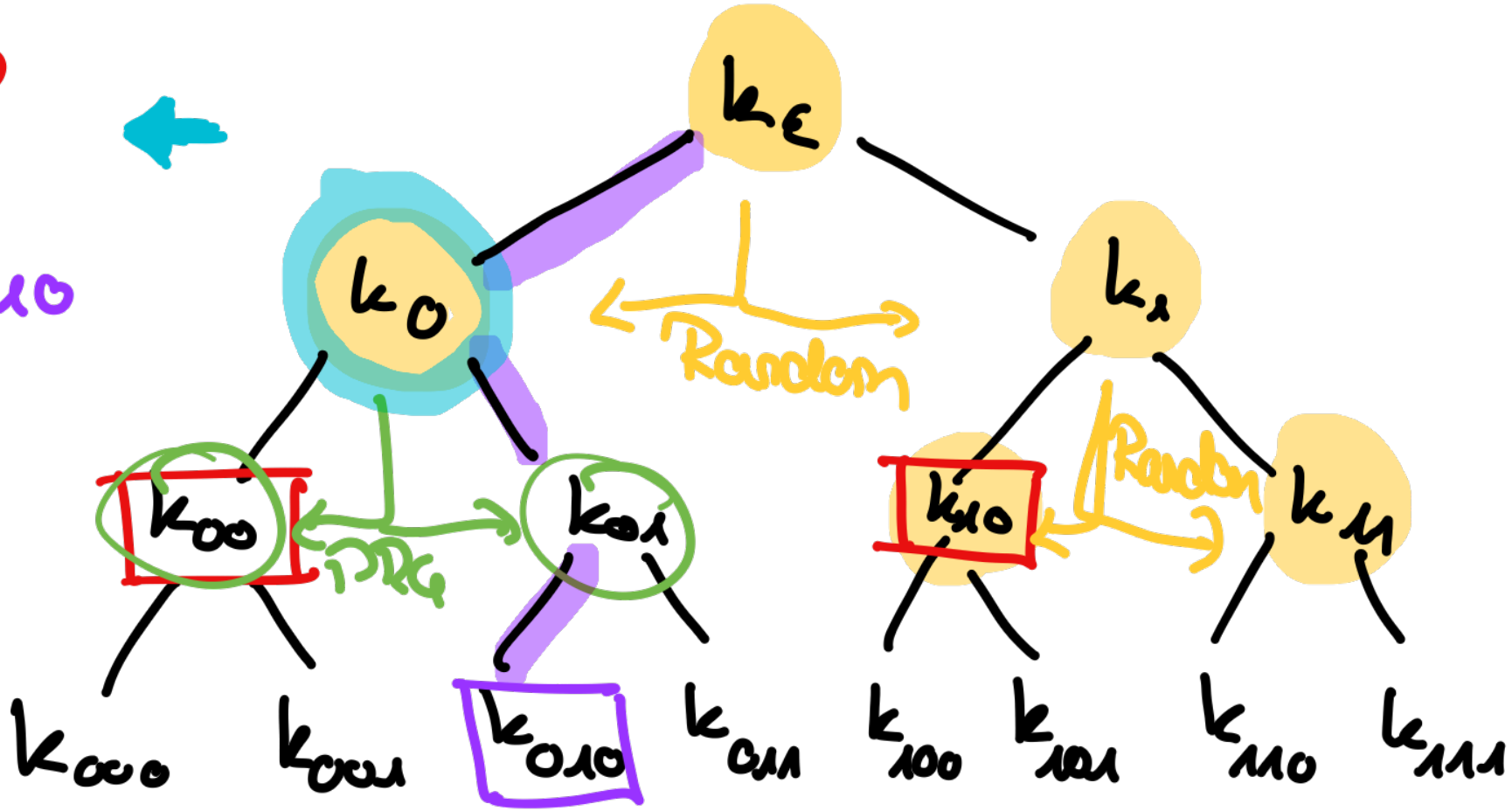
PRG ε

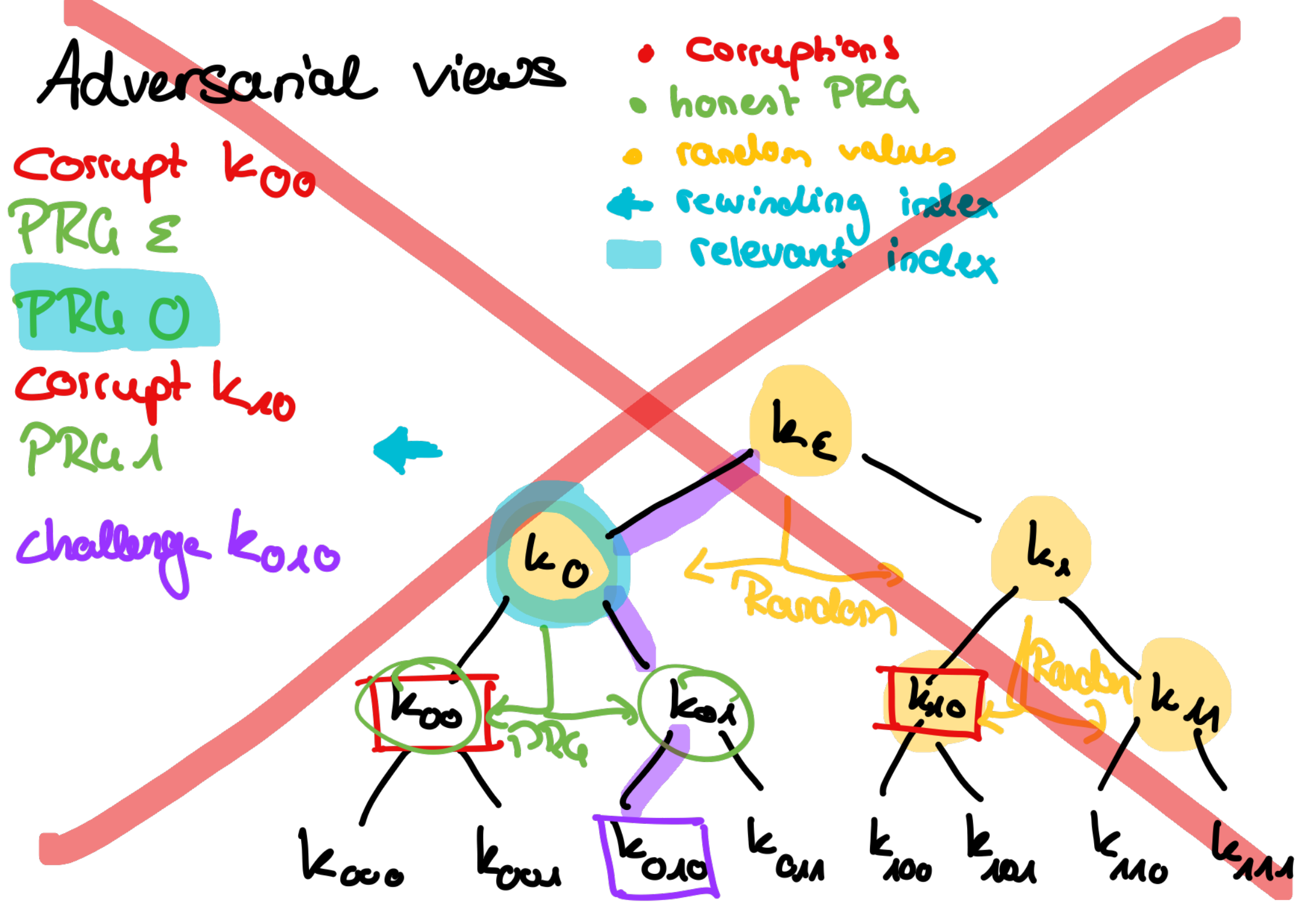
PRG 0

Corrupt k_{10}

PRG 1

challenge k_{010}




Adversarial views
Corruptions
honest PRG
random values
rewinding index
relevant index
Corrupt k_{00}
PRG ε
PRG 0
Corrupt k_{10}
PRG 1
Challenge k_{010}
k_ε
k_0
k_1
Random
k_{00}
k_{01}
PRG
k_{10}
Random
k_{11}
k_{000}
k_{001}
k_{010}
k_{011}
k_{100}
k_{101}
k_{110}
k_{111}

Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

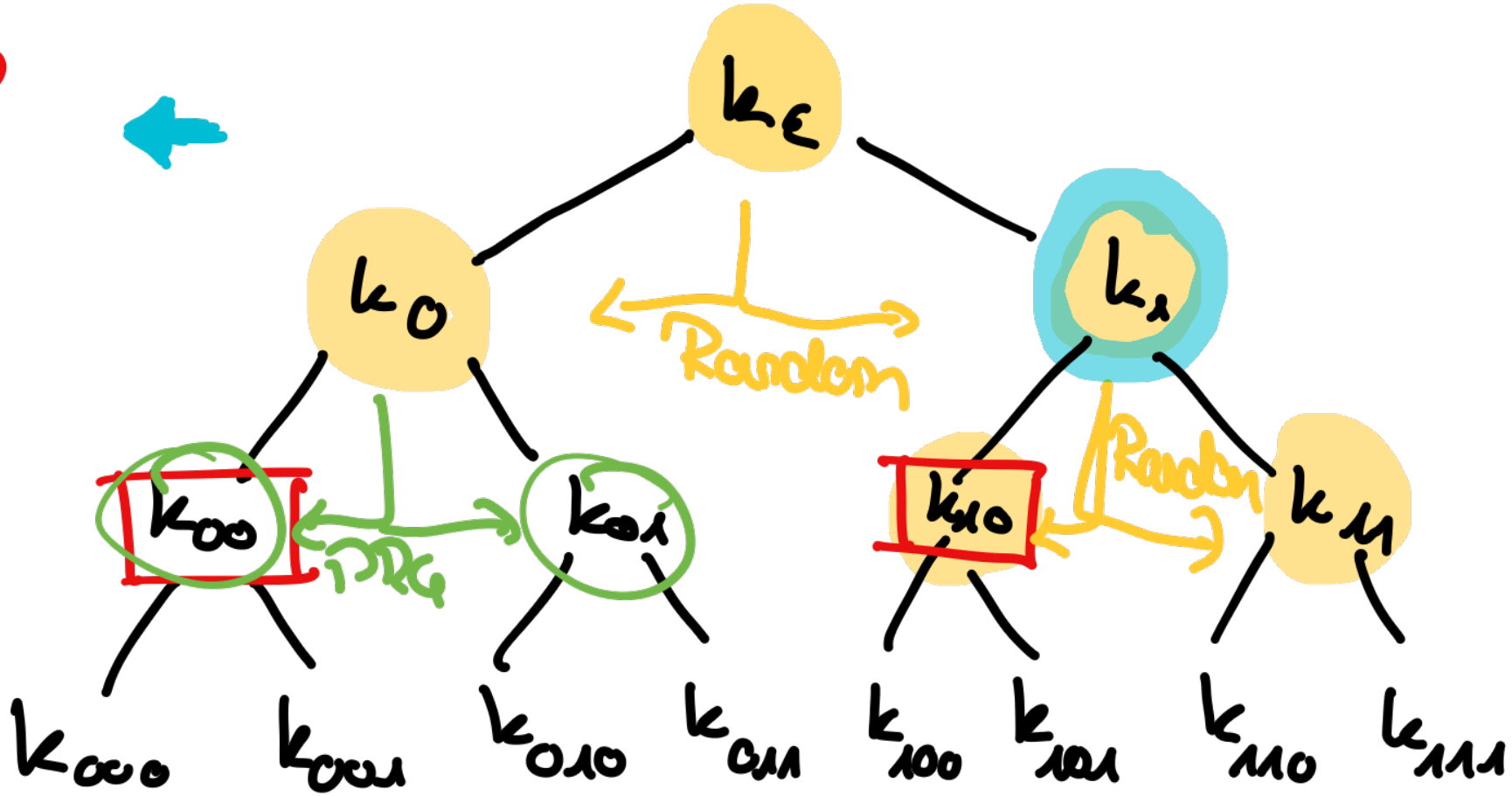
Corrupt k_{00}

PRG ε

PRG 0

Corrupt k_{10}

PRG 1



Adversarial views

- corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

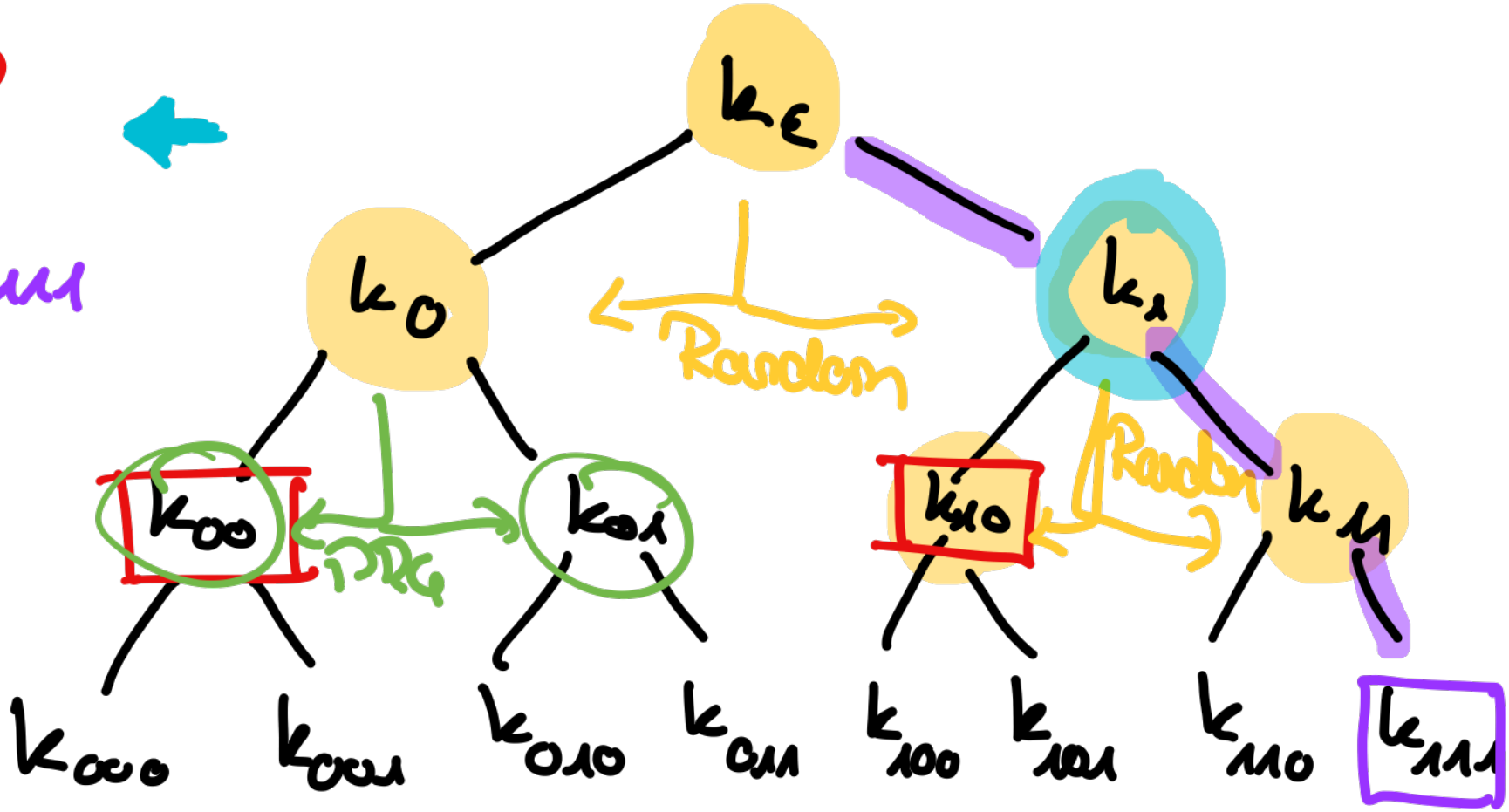
PRG ε

PRG 0

Corrupt k_{10}

PRG 1

challenge k_{111}



Adversarial views

- corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

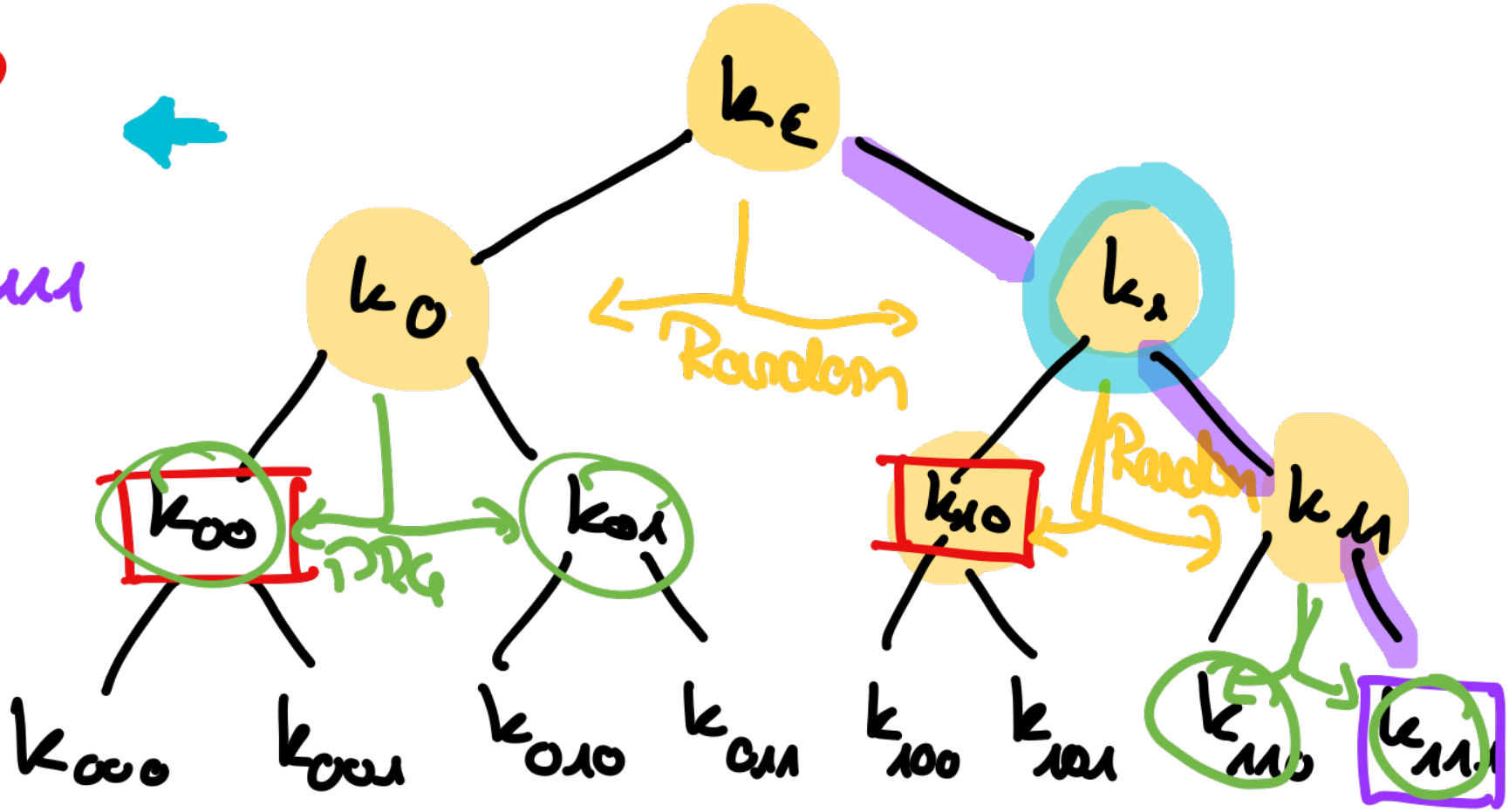
PRG 0

Corrupt k_{10}

PRG 1

Challenge k_{11}

PRG 11



Adversarial views

- corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

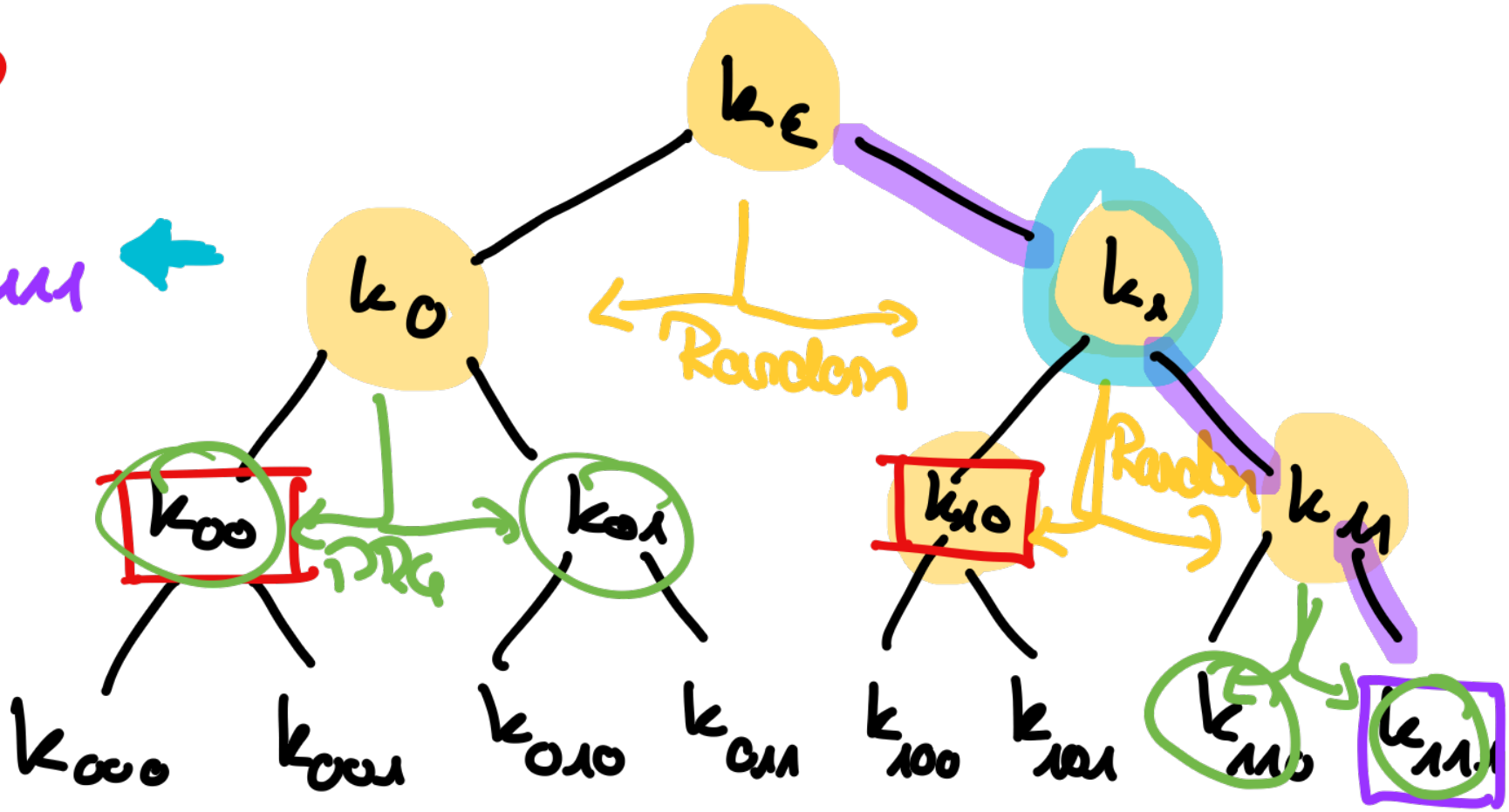
PRG 0

Corrupt k_{10}

PRG 1

challenge k_{11} ←

PRG 11



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

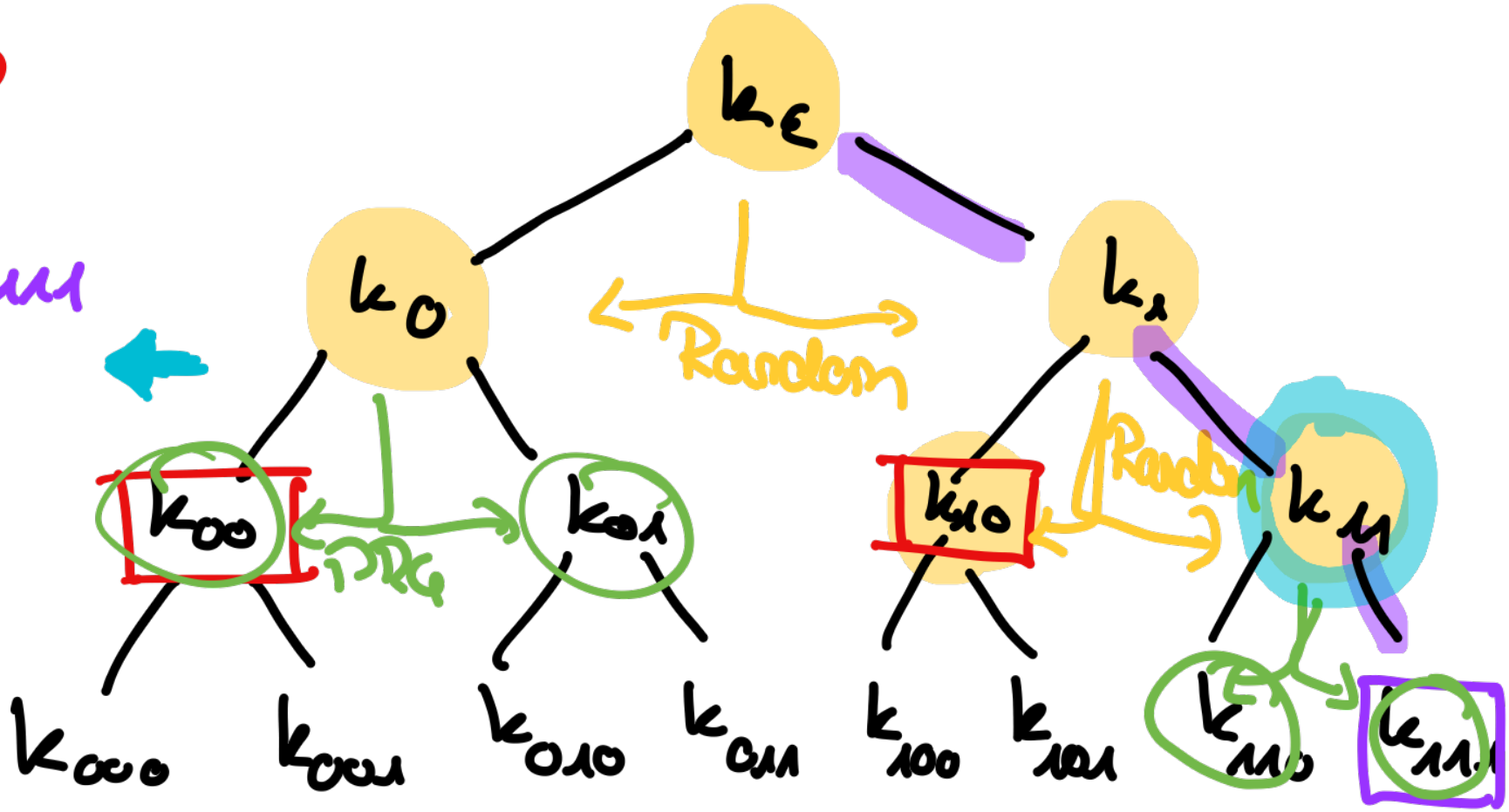
PRG 0

Corrupt k_{10}

PRG 1

challenge k_{11}

PRG 11



Adversarial views

- Corruptions
- honest PRG
- random values
- rewinding index
- relevant index

Corrupt k_{00}

PRG ε

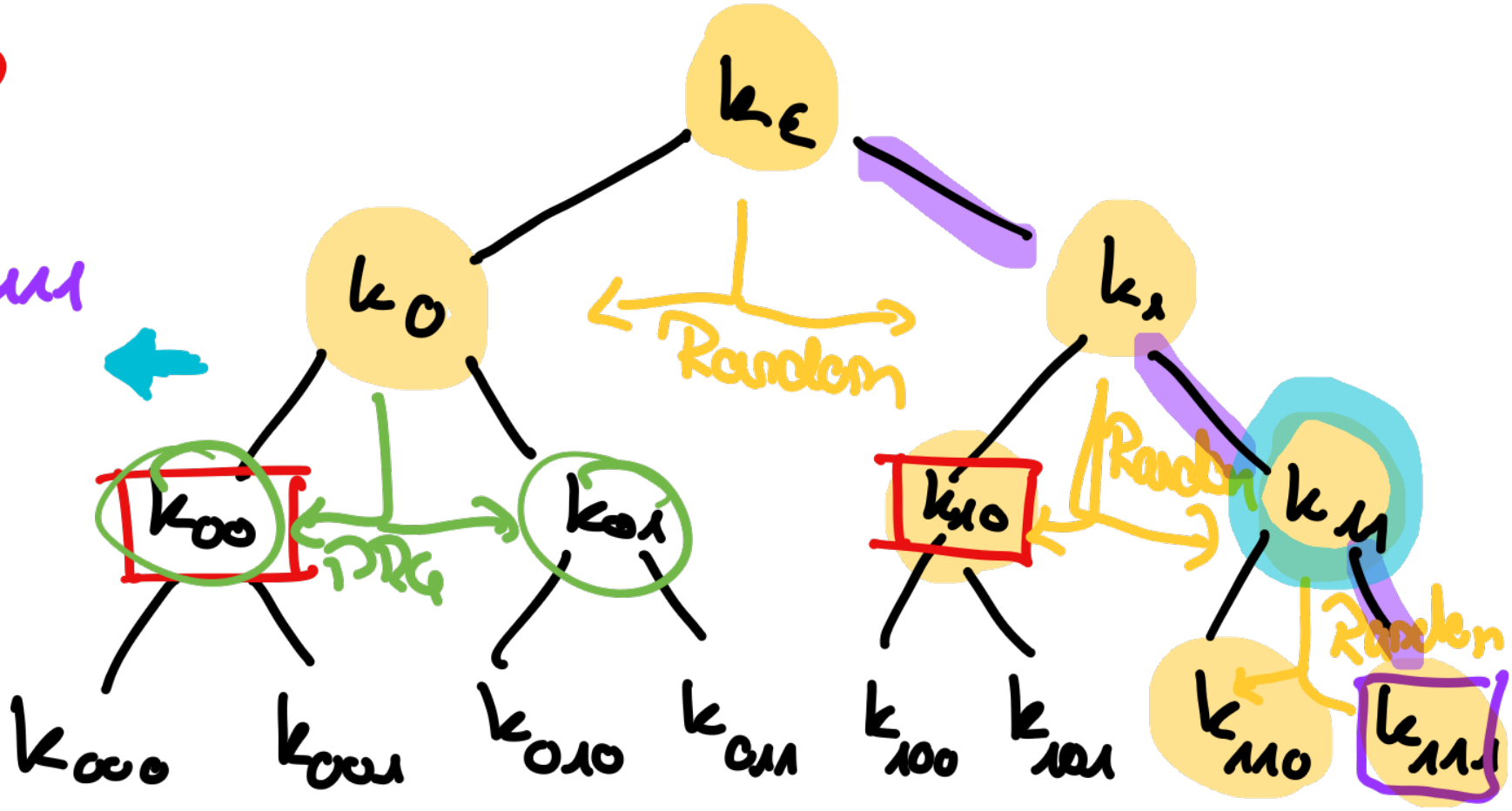
PRG 0

Corrupt k_{10}

PRG 1

challenge k_{11}

PRG 11



Conclusion

- undirected rewinding
- PC-PRF security of GGM TKF with poly loss from PRG
- Security of LKH (Multicast Encryption) with poly loss from IND-CPA

Conclusion

- undirected rewinding
- PC-PRF security of GGM TRF with poly loss from PRG
- security of LKH (Multicast Encryption) with poly loss from IND-CPA

Open Questions

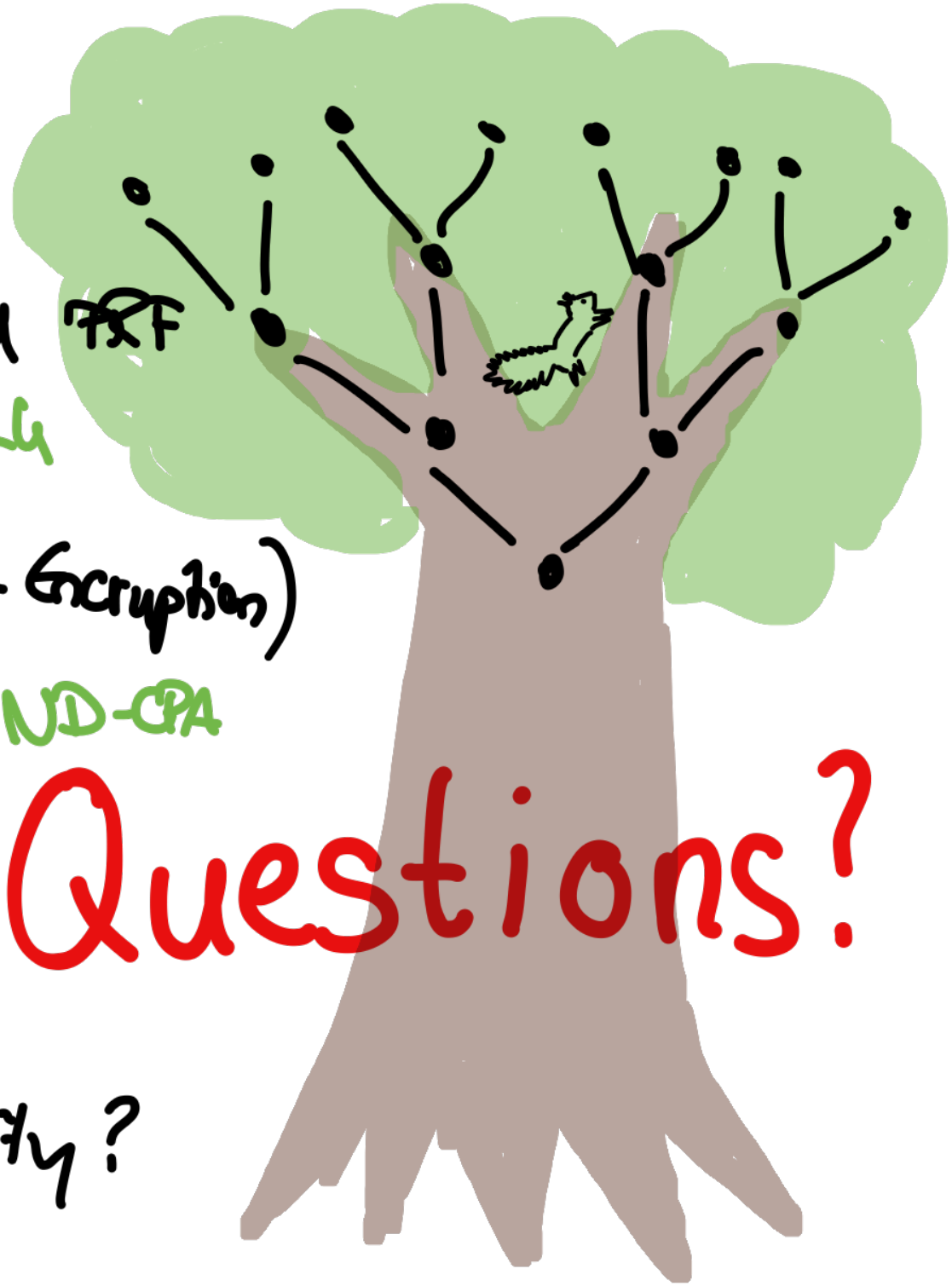
- Other Applications?
- Generic Applicability?

Conclusion

- undirected rewinding
- PC-PRF security of GGM with poly loss from PRG
- security of LKH (Multicast Encryption) with poly loss from IND-CPA

Open Questions

- Other Applications?
- Generic Applicability?



Questions?