Privately Puncturing PRFs from Lattices: Adaptive Security and Collusion Resistant Pseudorandomness

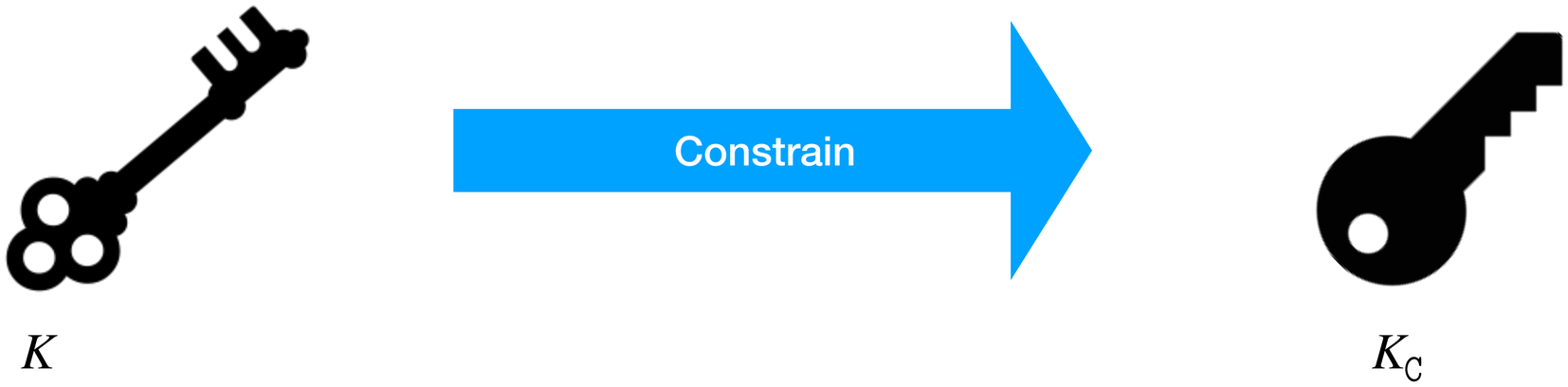
Rupeng Yang
University of Wollongong

Constrained Pseudorandom Function

K K_C

Correctness: if $C(x) = 1$, $F_K(x) = F_{K_C}(x)$

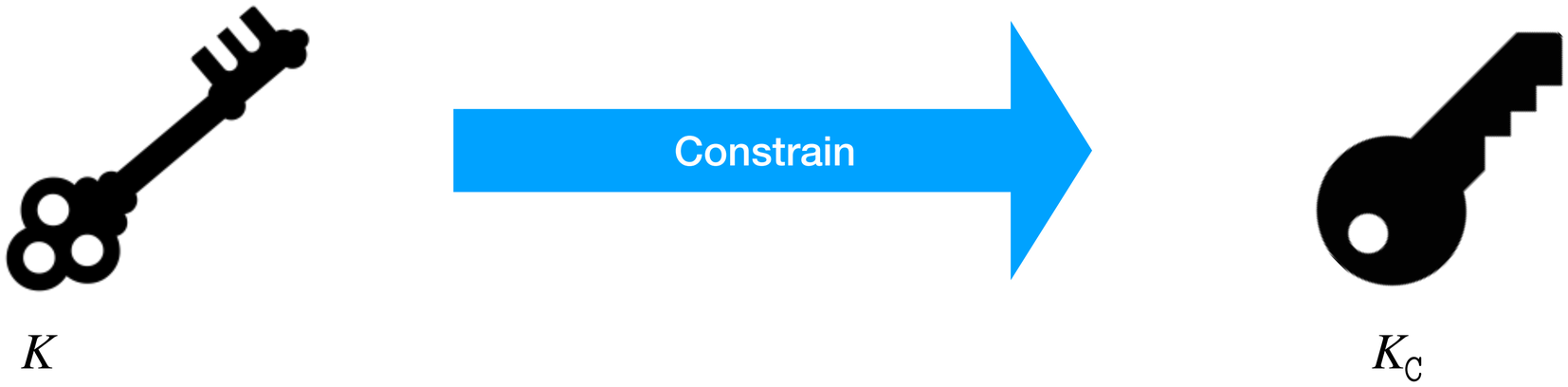
Constrained Pseudorandom Function



Correctness: if $\mathsf{C}(x) = 1$, $\mathsf{F}_K(x) = F_{K_C}(x)$

Pseudorandomness: if $\mathsf{C}(x) = 0$, $\mathsf{F}_K(x)$ **is hidden given** K_C

Constrained Pseudorandom Function



Correctness: if $\mathsf{C}(x) = 1$, $\mathsf{F}_K(x) = F_{K_{\mathsf{C}}}(x)$

Pseudorandomness: if $\mathsf{C}(x) = 0$, $\mathsf{F}_K(x)$ is hidden given K_{C}

Privacy: C is hidden given K_{C}

(Required by private constrained PRF)

Security of Constrained PRF

Pseudorandomness

$K \leftarrow \mathtt{KeyGen}(1^\lambda)$
$b \leftarrow \{0,1\}$

$x^*, \mathtt{C}$

$K_\mathtt{C} \leftarrow \mathtt{Constrain}(K, \mathtt{C})$
$y_0^* = \mathsf{F}_K(x^*)$
$y_1^* \leftarrow \mathcal{Y}$

$K_\mathtt{C}, y_b^*$

x

$y = \mathsf{F}_K(x)$

b'

The adversary wins if:

1. $b = b'$
2. $\mathtt{C}(x^*) = 0$
3. $x^* \neq x$ for all queried x

Security of Constrained PRF

(Sel,1-key)-Pseudorandomness

$K \leftarrow \mathtt{KeyGen}(1^\lambda)$
$b \leftarrow \{0,1\}$

$x^*, \mathtt{C}$

$K_\mathtt{C} \leftarrow \mathtt{Constrain}(K, \mathtt{C})$
$y_0^* = \mathsf{F}_K(x^*)$
$y_1^* \leftarrow \mathcal{Y}$

Key Query+Challenge Query

$K_\mathtt{C}, y_b^*$

x

$y = \mathsf{F}_K(x)$

Evaluation Queries

b'

The adversary wins if:
1. $b = b'$
2. $\mathtt{C}(x^*) = 0$
3. $x^* \neq x$ for all queried x

Selective Security: Queries are in some predefined order.
1-Key Security: Only 1 key query is allowed.

Security of Constrained PRF

(Sel,1-key)-Pseudorandomness

$K \leftarrow \mathtt{KeyGen}(1^\lambda)$
$b \leftarrow \{0,1\}$

$x^*, \mathtt{C}$

$K_{\mathtt{C}} \leftarrow \mathtt{Constrain}(K, \mathtt{C})$
$y_0^* = \mathsf{F}_K(x^*)$
$y_1^* \leftarrow \mathcal{Y}$

$K_{\mathtt{C}}, y_b^*$

x

$y = \mathsf{F}_K(x)$

b'

The adversary wins if:
1. $b = b'$
2. $\mathtt{C}(x^*) = 0$
3. $x^* \neq x$ for all queried x

(Sel,1-key)-Privacy

$K \leftarrow \mathtt{KeyGen}(1^\lambda)$
$b \leftarrow \{0,1\}$

$\mathtt{C}_0^*, \mathtt{C}_1^*$

$K_{\mathtt{C}_b^*} \leftarrow \mathtt{Constrain}(K, \mathtt{C}_b^*)$

$K_{\mathtt{C}_b^*}$

x

$y = \mathsf{F}_K(x)$

b'

The adversary wins if:
1. $b = b'$
2. $\mathtt{C}_0^*(x) = \mathtt{C}_1^*(x)$ for all queried x

Adaptive Security

- Adaptive Security: The adversary can make queries in an arbitrary order.
- Constructions of adaptively secure constrained PRFs are available:
  - from obfuscation [HKW15,AMN+19,DKN+20];
  - for constraints that can be implemented by an inner-product predicate [DKN+20];
- Q1: Adaptive security from **standard lattice assumptions** for **beyond inner-product predicates**.

* Here, we do not consider constructions using complexity leveraging or in the random oracle model.

Collusion Resistance

- Collusion Resistance: The adversary can make more than 1 key queries.
- Constructions of collusion resistant constrained PRFs are available:
  - from obfuscation [BW13, BLW17, …];
  - for constraints that can be implemented by an inner-product predicate [BW13,KPTZ13,BGI14,BFP+15,DKN+20];
- Q2: Collusion Resistance from **standard lattice assumptions** for **beyond inner-product predicates**.

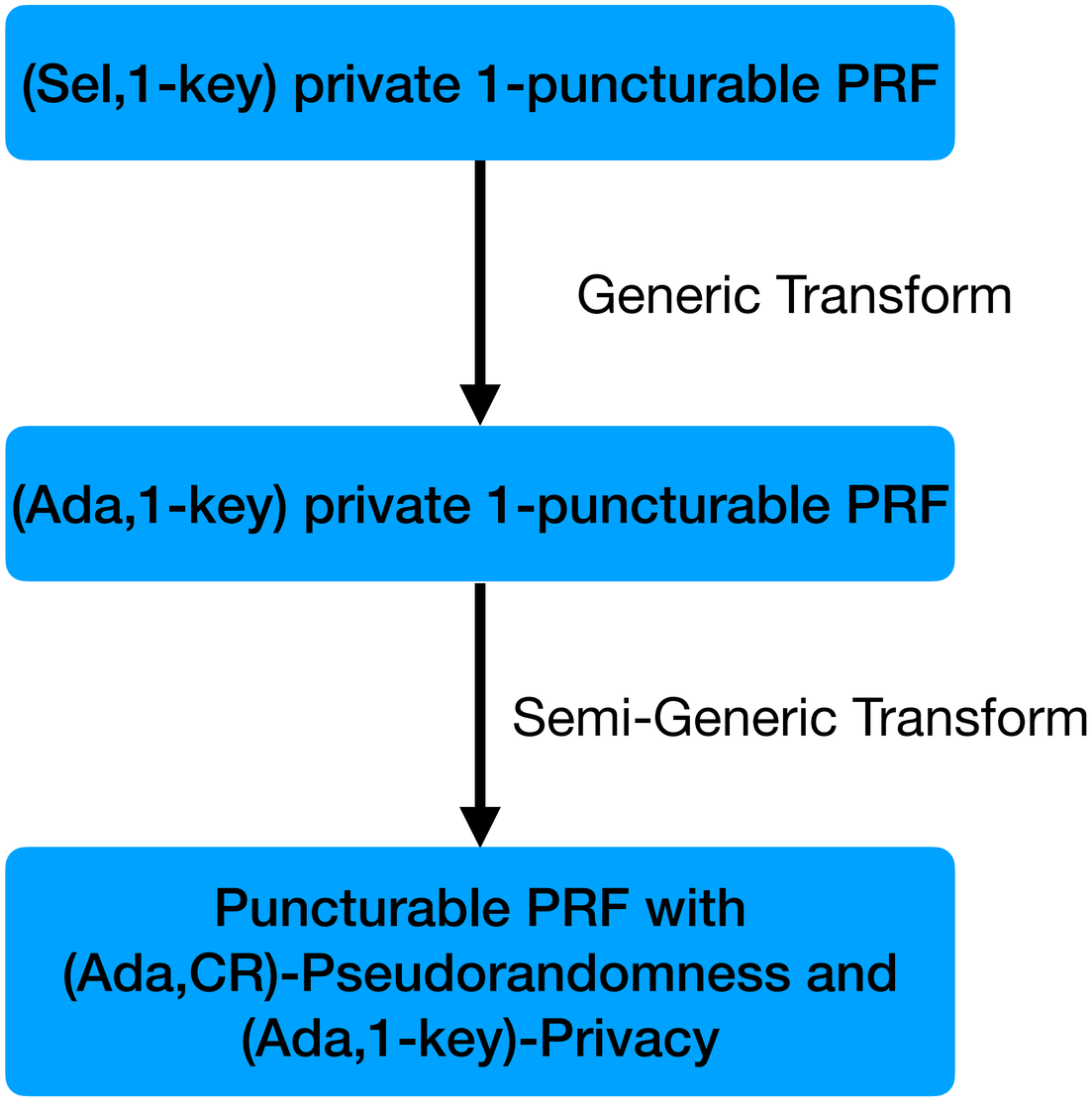
Our Results

- A private **puncturable** PRF from standard lattice assumptions that has
  - adaptive collusion resistant pseudorandomness
  - and adaptive 1-key privacy
- In a puncturable PRF, the constraint $\mathsf{C}_{\mathscr{P}}(x) = 1$ iff $x \notin \mathscr{P}$
  - 1-puncturable PRF: $|\mathscr{P}| = 1$
  - τ-puncturable PRF: $|\mathscr{P}| = \tau$

Our Results

- A private **puncturable** PRF from standard lattice assumptions that has
  - adaptive collusion resistant pseudorandomness
  - and adaptive 1-key privacy
- Why puncturable PRF?
    - The puncturing constraint cannot be implemented by the inner-product predicate [PTW20].
    - Puncturable PRFs are useful in applications like watermarking, searchable encryption, etc.

Our Approach



From Selective Security to Adaptive Security

- The construction needs a new primitive called explainable hash.
- An explainable hash H is an injective function with explainability:

- The experiments above may abort with a non-negligible probability if the queries from the adversary are not “good”.
- Explainable hash can be constructed from standard lattice assumptions.

From Selective Security to Adaptive Security

$K \leftarrow \mathtt{KeyGen}(1^\lambda)$
$b \leftarrow \{0,1\}$

x^*

$K_{x^*} \leftarrow \mathtt{Constrain}(K, x^*)$
$y_0^* = \mathsf{F}_K(x^*)$
$y_1^* \leftarrow \mathcal{Y}$

K_{x^*}, y_b^*

x
$y = \mathsf{F}_K(x)$

b'

The adversary wins if:
1. $b = b'$
2. $x^* \neq x$ for all queried x

$K \leftarrow \mathtt{KeyGen}(1^\lambda)$
$b \leftarrow \{0,1\}$

x
$y = \mathsf{F}_K(x)$

x^*

$K_{x^*} \leftarrow \mathtt{Constrain}(K, x^*)$
$y_0^* = \mathsf{F}_K(x^*)$
$y_1^* \leftarrow \mathcal{Y}$

K_{x^*}, y_b^*

x
$y = \mathsf{F}_K(x)$

b'

The adversary wins if:
1. $b = b'$
2. $x^* \neq x$ for all queried x

From Selective Security to Adaptive Security

$K \leftarrow \mathtt{KeyGen}(1^\lambda)$
$b \leftarrow \{0,1\}$

x^*

$K_{x^*} \leftarrow \mathtt{Constrain}(K, x^*)$
$y_0^* = \mathsf{F}_K(x^*)$
$y_1^* \leftarrow \mathcal{Y}$

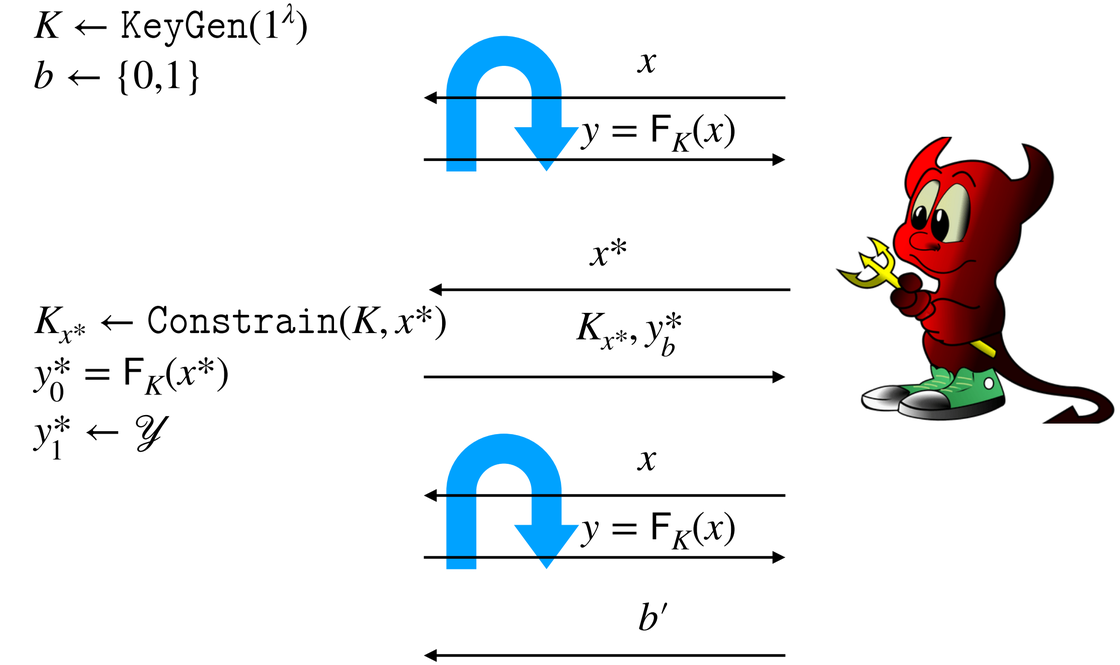
K_{x^*}, y_b^*

x
$y = \mathsf{F}_K(x)$

b'

The adversary wins if:
1. $b = b'$
2. $x^* \neq x$ for all queried x

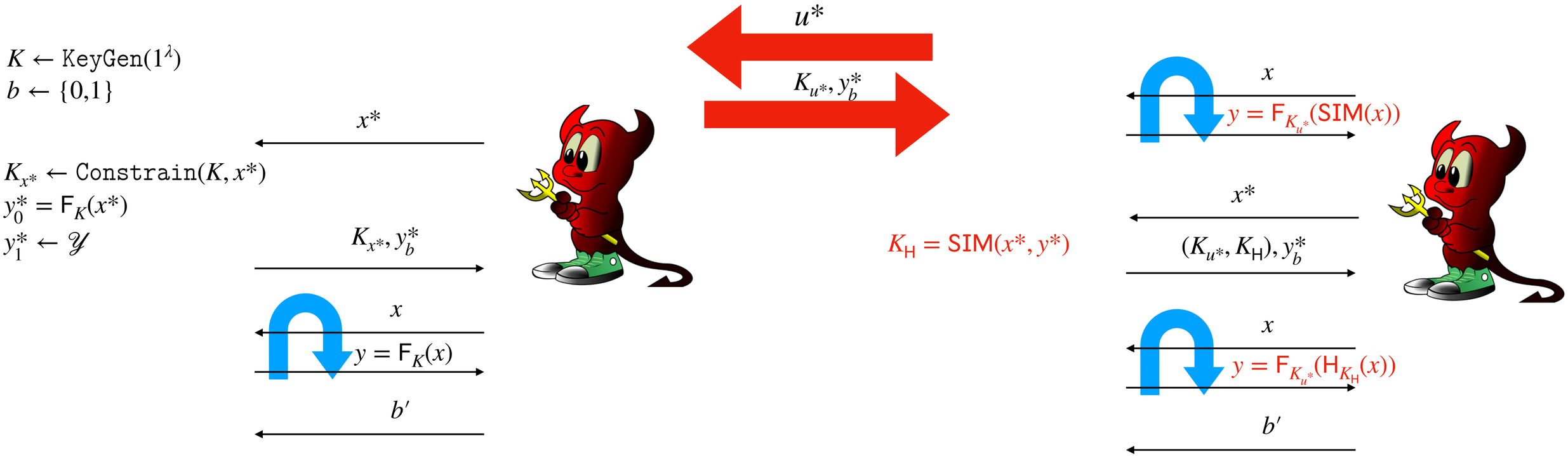
- F is a 1-puncturable PRF with selective 1-key pseudorandomness
- H is an explainable hash



The adversary wins if:
1. $b = b'$
2. $x^* \neq x$ for all queried x

- $K' = (K, K_{\mathsf{H}}) \qquad K'_x = (K_x, K_{\mathsf{H}})$
- $\mathsf{F}_{K'}(x) = \mathsf{F}_K(\mathsf{H}_{K_{\mathsf{H}}}(x))$

From Selective Security to Adaptive Security



The adversary wins if:

1. $b = b'$
2. $x^* \neq x$ for all queried x

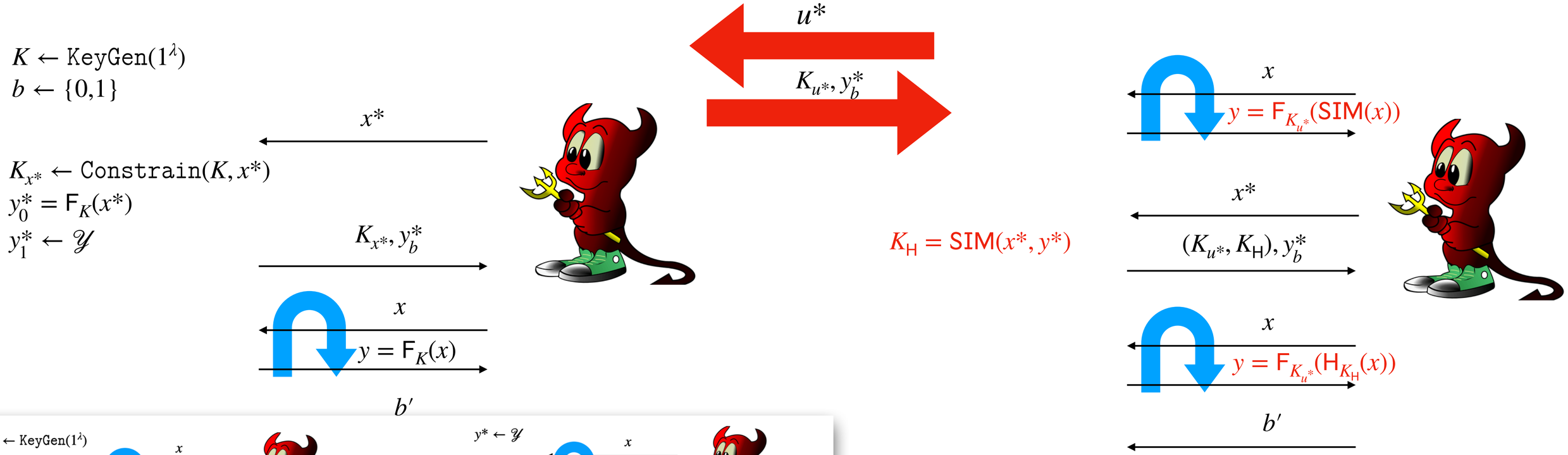
The adversary wins if:

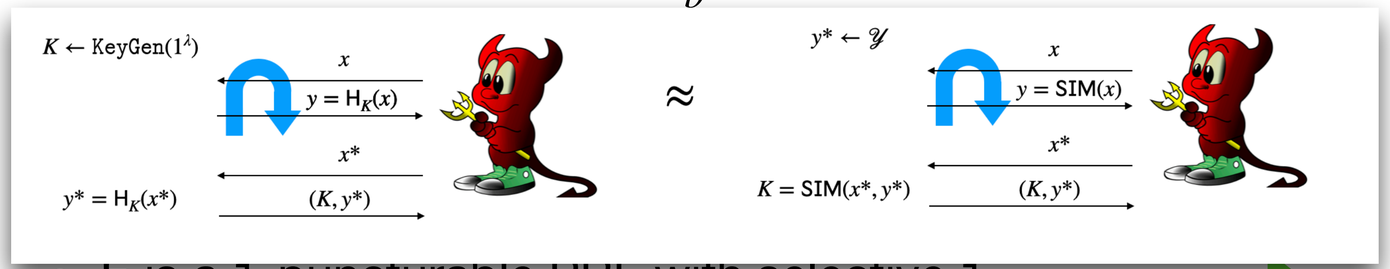
1. $b = b'$
2. $x^* \neq x$ for all queried x

- F is a 1-puncturable PRF with selective 1-key pseudorandomness
- H is an explainable hash

- $K' = (K, K_{\mathsf{H}}) \qquad K'_x = (K_x, K_{\mathsf{H}})$
- $\mathsf{F}_{K'}(x) = \mathsf{F}_K(\mathsf{H}_{K_{\mathsf{H}}}(x))$

From Selective Security to Adaptive Security





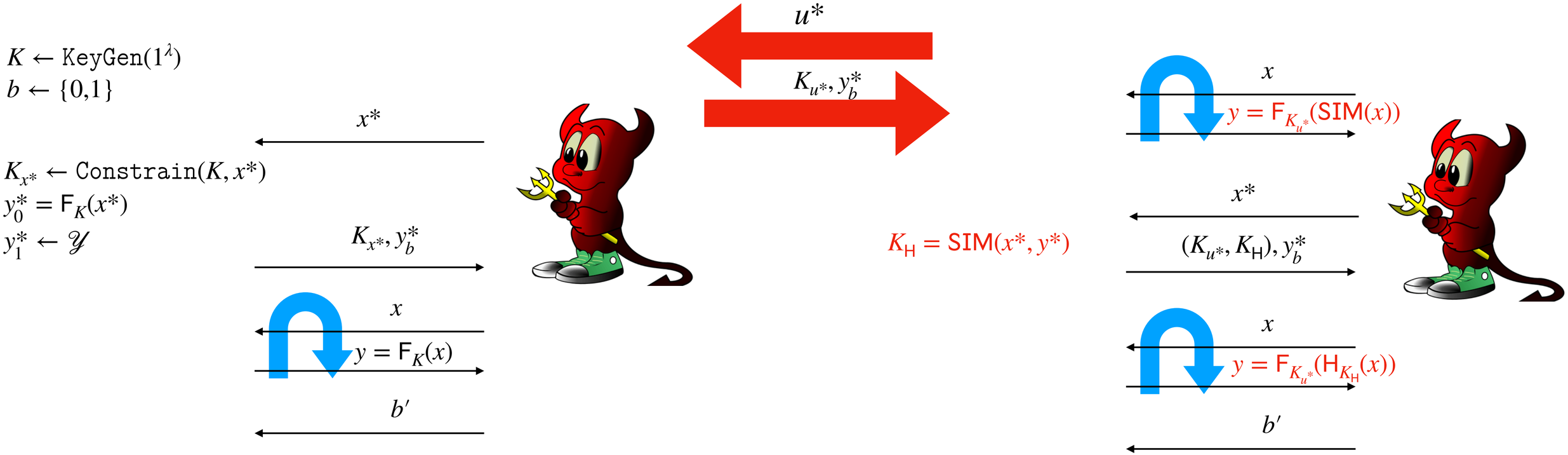
- F is a 1-puncturable PRF with selective 1-key pseudorandomness
- H is an explainable hash

The adversary wins if:

1. $b = b'$
2. $x^* \neq x$ for all queried x

- $K' = (K, K_{\mathsf{H}})$ $\quad K'_x = (K_x, K_{\mathsf{H}})$
- $\mathsf{F}_{K'}(x) = \mathsf{F}_K(\mathsf{H}_{K_{\mathsf{H}}}(x))$

From Selective Security to Adaptive Security



The adversary wins if:

1. $b = b'$
2. $x^* \neq x$ for all queried x

- F is a 1-puncturable PRF with selective 1-key pseudorandomness
- H is an explainable hash

The adversary wins if:

1. $b = b'$
2. $x^* \neq x$ for all queried x

- $K' = (K, K_\mathsf{H}) \qquad K'_x = (K_x, K_\mathsf{H})$
- $\mathsf{F}_{K'}(x) = \mathsf{F}_K(\mathsf{H}_{K_\mathsf{H}}(x))$

Adaptive privacy of the construction can be shown in a similar way.

From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF

$\mathscr{K}$

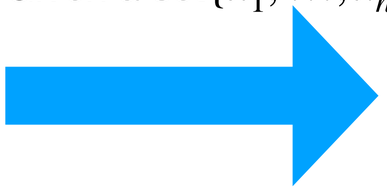
PRF Key: $\mathscr{K}$

$\mathscr{F}_{\mathscr{K}}(x) = \mathsf{F}_{\mathscr{K}}(x)$

From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF

$\mathcal{K}$

Given a set $\{x_1, \ldots, x_n\}$



$K^{(x_1)}$

$K^{(x_2)}$

PRF Key: $\mathcal{K}$

$\mathcal{F}_{\mathcal{K}}(x) = \mathsf{F}_{\mathcal{K}}(x)$

$K^{(x_n)}$

For i from 1 to n:

$K^{(x_i)} = \mathsf{G}_s(x_i)$, where G is a PRF and s is the key.

$$K^{(0)} = \mathcal{K} - \sum_{i=1}^{n} K^{(x_i)}$$

$K^{(0)}$

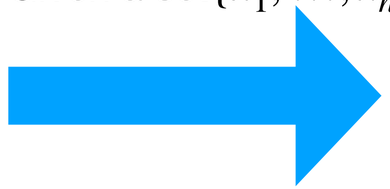
From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF

$\mathscr{K}$

PRF Key: $\mathscr{K}$

$\mathscr{F}_{\mathscr{K}}(x) = \mathsf{F}_{\mathscr{K}}(x)$

Given a set $\{x_1, \ldots, x_n\}$



$K^{(x_1)}$

$K^{(x_2)}$

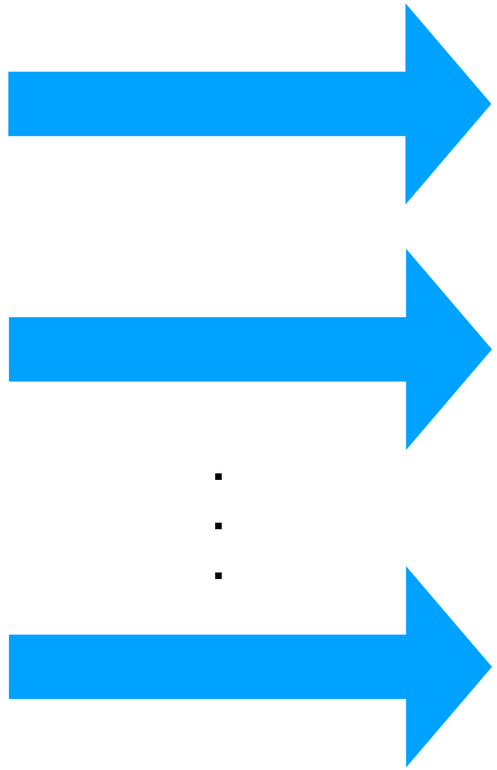
$K^{(x_n)}$

$K^{(0)}$

For i from 1 to n:

$K^{(x_i)} = \mathsf{G}_s(x_i)$, where G is a PRF and s is the key.

$$K^{(0)} = \mathscr{K} - \sum_{i=1}^{n} K^{(x_i)}$$



$K_{x_1}^{(x_1)}$

$K_{x_2}^{(x_2)}$

$K_{x_n}^{(x_n)}$

Constrained Key $\mathscr{K}_{\{x_1,\ldots,x_n\}} = (K^{(0)}, K_{x_1}^{(x_1)}, K_{x_2}^{(x_2)}, \ldots, K_{x_n}^{(x_n)})$

$$\mathscr{F}_{\mathscr{K}_{x_1,\ldots,x_n}}(x) = \mathsf{F}_{K^{(0)}}(x) + \sum_{i=1}^{n} \mathsf{F}_{K_{x_i}^{(x_i)}}(x)$$

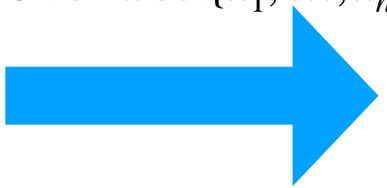
From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF

$\mathcal{K}$

PRF Key: $\mathcal{K}$

$\mathcal{F}_{\mathcal{K}}(x) = \mathsf{F}_{\mathcal{K}}(x)$

Given a set $\{x_1, \ldots, x_n\}$



$K^{(x_1)}$

$K^{(x_2)}$

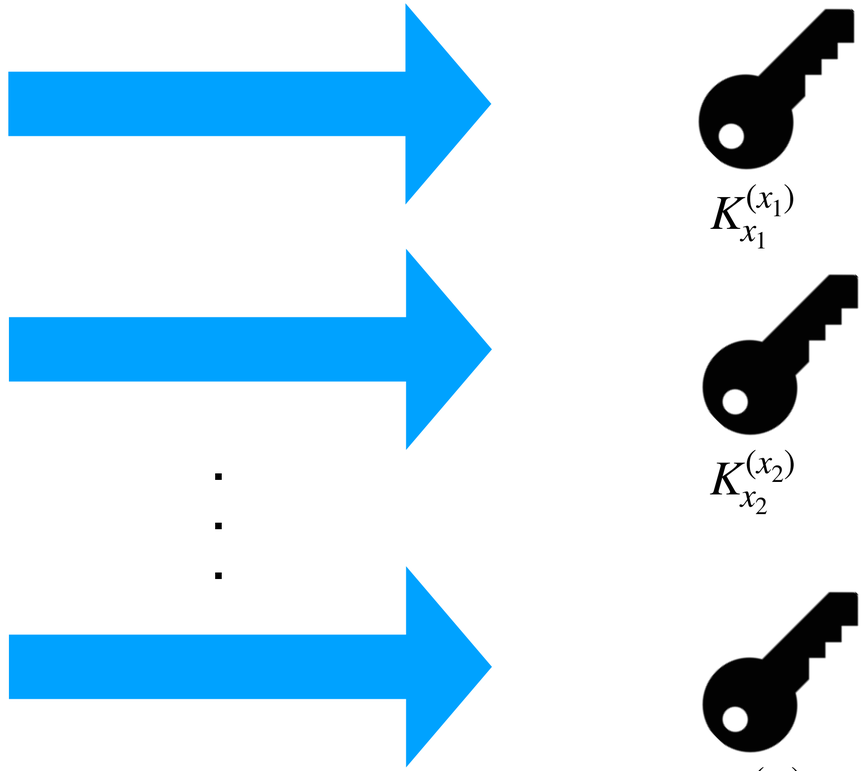
$K^{(x_n)}$

$K^{(0)}$

For i from 1 to n:

$K^{(x_i)} = \mathsf{G}_s(x_i)$, where G is a PRF and s is the key.

$$K^{(0)} = \mathcal{K} - \sum_{i=1}^{n} K^{(x_i)}$$



$K^{(x_1)}_{x_1}$

$K^{(x_2)}_{x_2}$

$K^{(x_n)}_{x_n}$

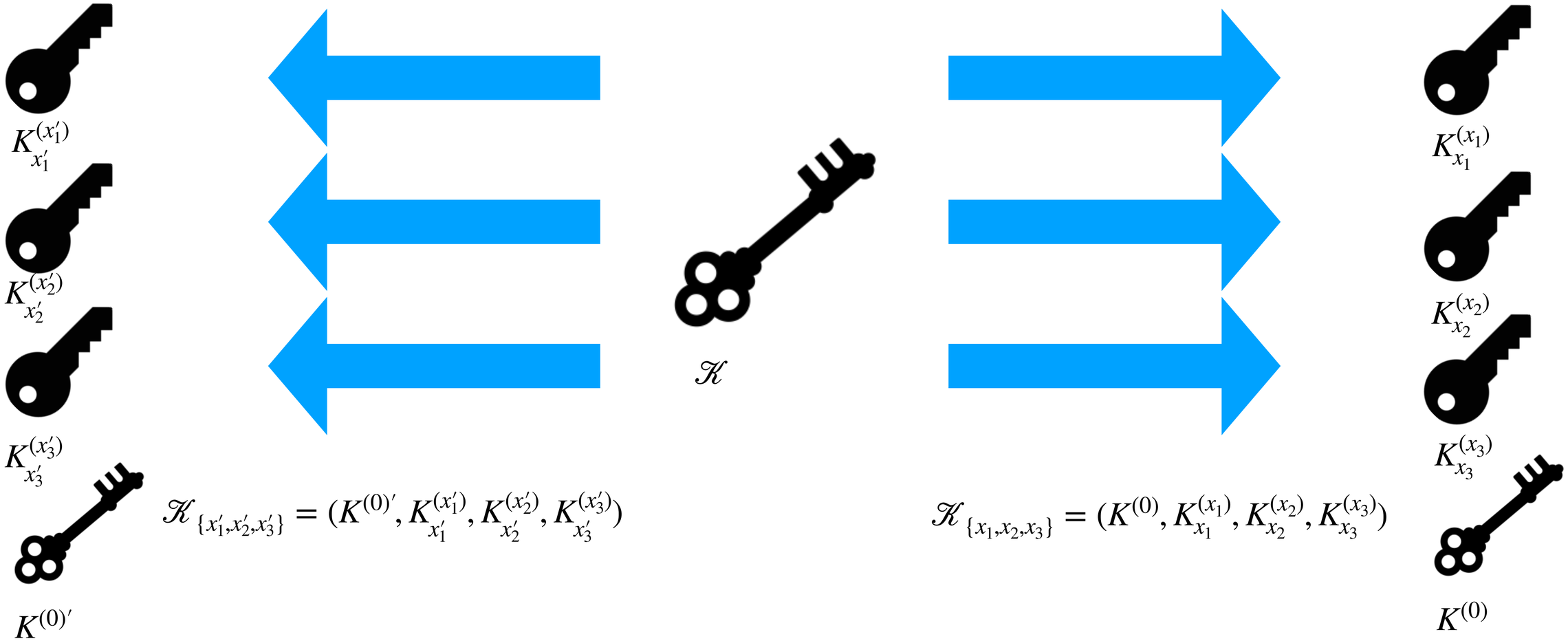
Constrained Key $\mathcal{K}_{\{x_1,\ldots,x_n\}} = (K^{(0)}, K^{(x_1)}_{x_1}, K^{(x_2)}_{x_2}, \ldots, K^{(x_n)}_{x_n})$

$$\mathcal{F}_{\mathcal{K}_{x_1,\ldots,x_n}}(x) = \mathsf{F}_{K^{(0)}}(x) + \sum_{i=1}^{n} \mathsf{F}_{K^{(x_i)}_{x_i}}(x)$$

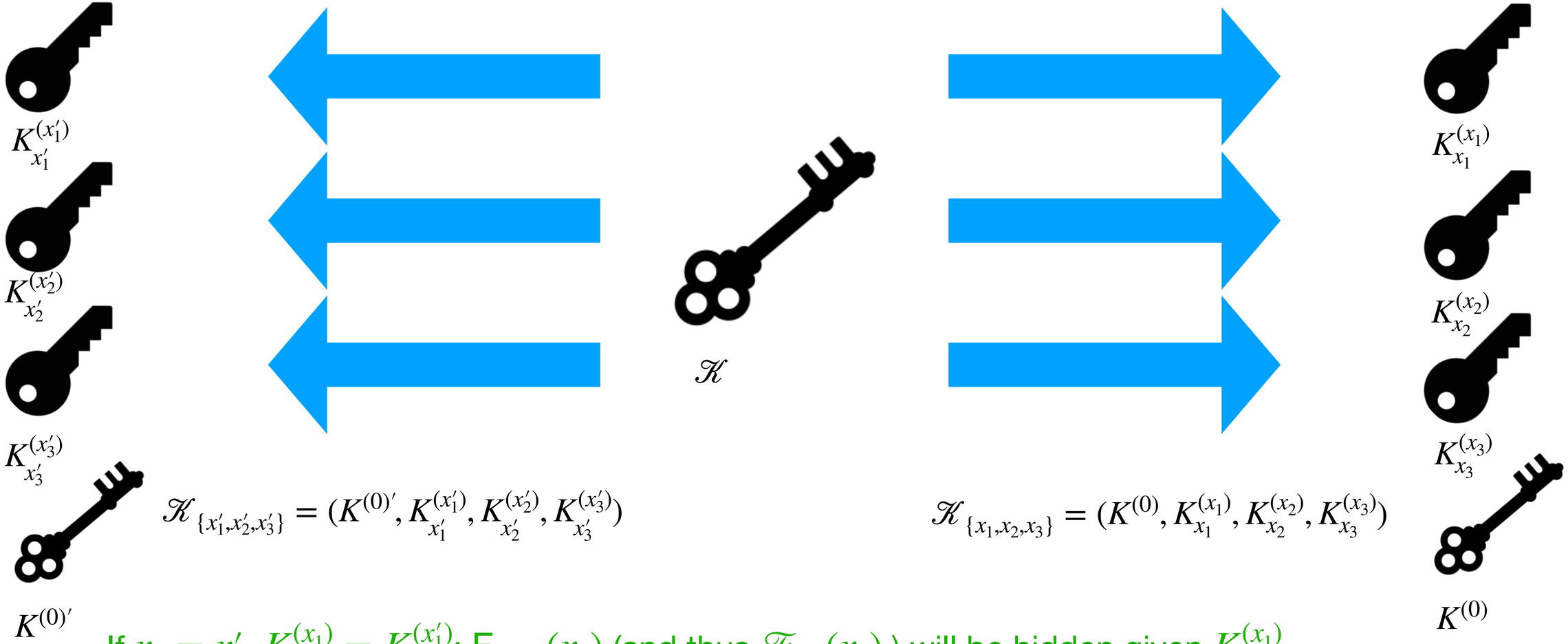
Correctness holds if F **is key-homomorphic, i.e.,**

$\mathsf{F}_{K_1}(x) + \mathsf{F}_{K_2}(x) = \mathsf{F}_{K_1+K_2}(x)$

From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF



From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF

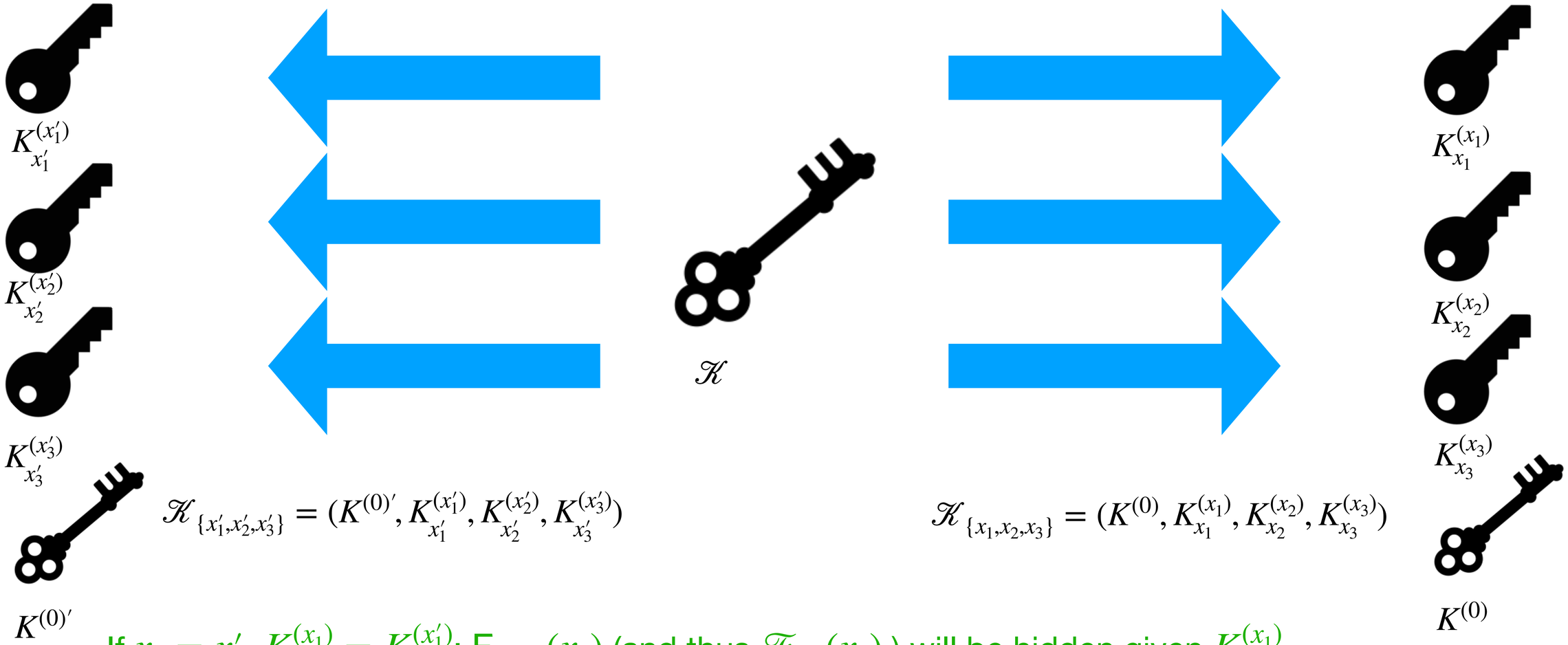


$\mathscr{K}_{\{x'_1,x'_2,x'_3\}} = (K^{(0)'}, K^{(x'_1)}_{x'_1}, K^{(x'_2)}_{x'_2}, K^{(x'_3)}_{x'_3})$

$\mathscr{K}_{\{x_1,x_2,x_3\}} = (K^{(0)}, K^{(x_1)}_{x_1}, K^{(x_2)}_{x_2}, K^{(x_3)}_{x_3})$

If $x_1 = x'_1$, $K^{(x_1)}_{x_1} = K^{(x'_1)}_{x'_1}$: $\mathsf{F}_{K^{(x_1)}}(x_1)$ (and thus $\mathscr{F}_{\mathscr{K}}(x_1)$) will be hidden given $K^{(x_1)}_{x_1}$.

From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF



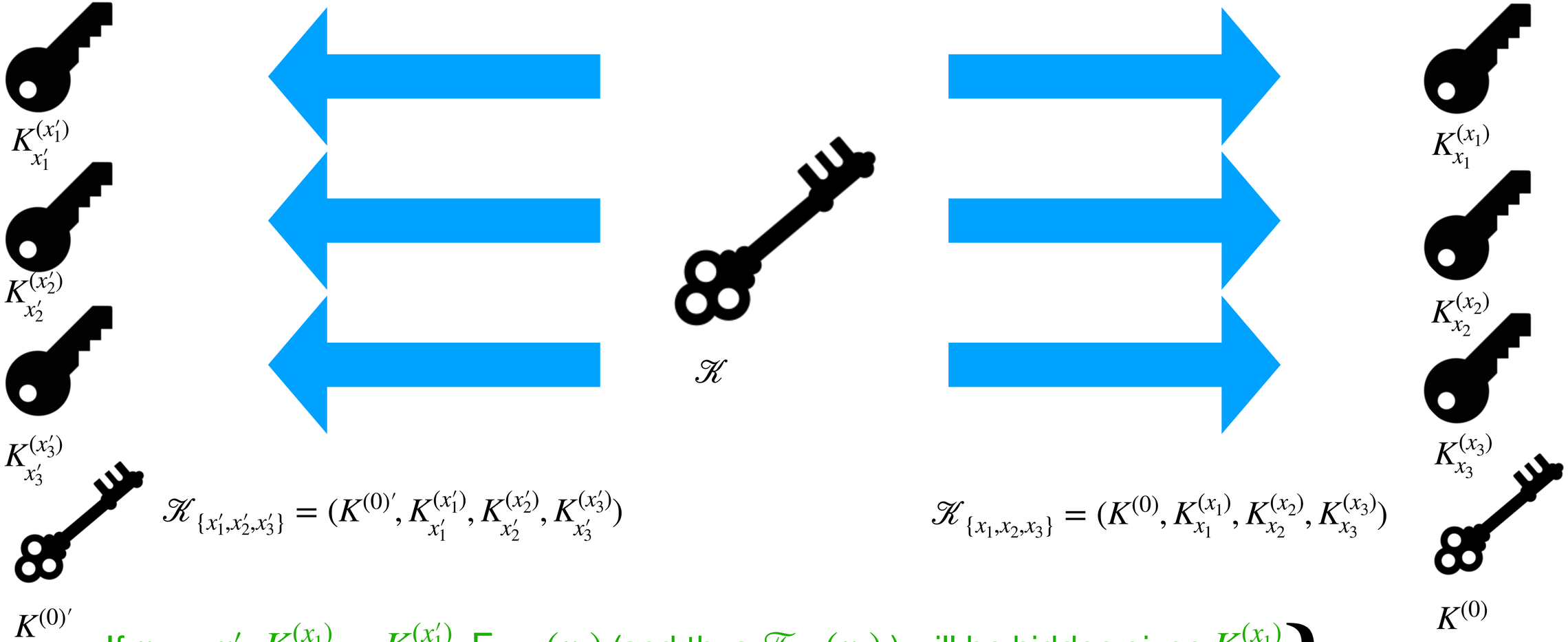
$\mathscr{K}_{\{x'_1,x'_2,x'_3\}} = (K^{(0)'}, K^{(x'_1)}_{x'_1}, K^{(x'_2)}_{x'_2}, K^{(x'_3)}_{x'_3})$

$\mathscr{K}_{\{x_1,x_2,x_3\}} = (K^{(0)}, K^{(x_1)}_{x_1}, K^{(x_2)}_{x_2}, K^{(x_3)}_{x_3})$

If $x_1 = x'_1$, $K^{(x_1)}_{x_1} = K^{(x'_1)}_{x'_1}$: $\mathsf{F}_{K^{(x_1)}}(x_1)$ (and thus $\mathscr{F}_{\mathscr{K}}(x_1)$) will be hidden given $K^{(x_1)}_{x_1}$.

The remaining parts of the constrained keys can be generated given $\mathscr{K} - K^{(x_1)}$, which will not leak information about $K^{(x_1)}$ if the PRF keys are uniform.

From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF



$\mathscr{K}_{\{x_1',x_2',x_3'\}} = (K^{(0)'}, K^{(x_1')}_{x_1'}, K^{(x_2')}_{x_2'}, K^{(x_3')}_{x_3'})$

$\mathscr{K}_{\{x_1,x_2,x_3\}} = (K^{(0)}, K^{(x_1)}_{x_1}, K^{(x_2)}_{x_2}, K^{(x_3)}_{x_3})$

If $x_1 = x_1'$, $K^{(x_1)}_{x_1} = K^{(x_1')}_{x_1'}$: $\mathsf{F}_{K^{(x_1)}}(x_1)$ (and thus $\mathscr{F}_{\mathscr{K}}(x_1)$) will be hidden given $K^{(x_1)}_{x_1}$.

The remaining parts of the constrained keys can be generated given $\mathscr{K} - K^{(x_1)}$, which will not leak information about $K^{(x_1)}$ if the PRF keys are uniform.

} **Collusion Resistant Pseudorandomness follows!**

From 1-key 1-Puncturable PRF to Collusion Resistant Puncturable PRF

$\mathcal{K}$

PRF Key: $\mathcal{K}$

$\mathcal{F}_{\mathcal{K}}(x) = \mathsf{F}_{\mathcal{K}}(x)$

Given a set $\{x_1, \ldots, x_n\}$

$K^{(x_1)}$

$K^{(x_2)}$

$K^{(x_n)}$

$K^{(0)}$

For i from 1 to n:

$K^{(x_i)} = \mathsf{G}_s(x_i)$, where G is a PRF and s is the key.

$$K^{(0)} = \mathcal{K} - \sum_{i=1}^{n} K^{(x_i)}$$

$K_{x_1}^{(x_1)}$

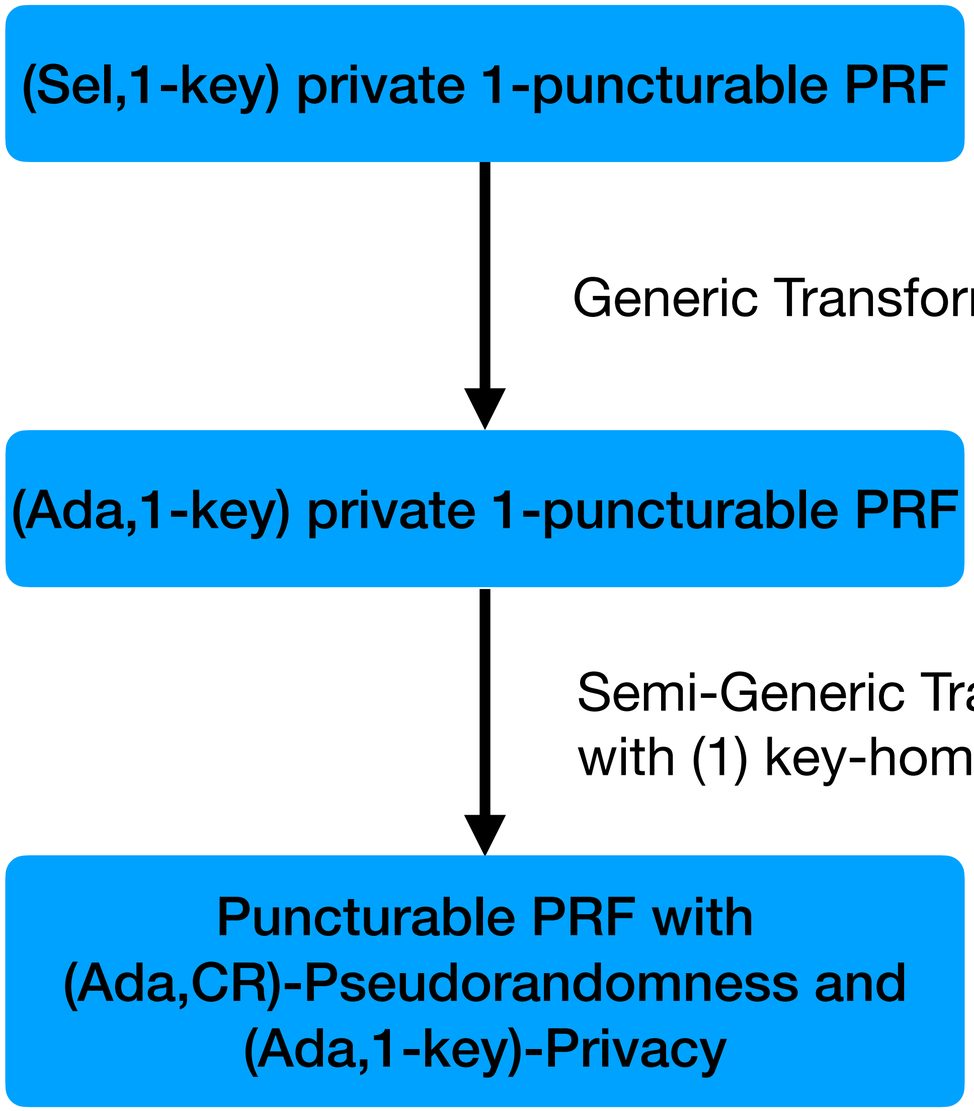
$K_{x_2}^{(x_2)}$

$K_{x_n}^{(x_n)}$

Constrained Key $\mathcal{K}_{\{x_1,\ldots,x_n\}} = (K^{(0)}, K_{x_1}^{(x_1)}, K_{x_2}^{(x_2)}, \ldots, K_{x_n}^{(x_n)})$

The construction does not have collusion resistant privacy, but it can keep the 1-key privacy.

Putting it All Together



Putting it All Together

Puncturable PRF from [PS20] with
(1) almost key-homomorphism
(2) almost uniform keys

(Sel,1-key) private 1-puncturable PRF

Generic Transform

Puncturable PRF with
(1) almost key-homomorphism
(2) almost uniform keys
(3) adaptive security

(Ada,1-key) private 1-puncturable PRF

Semi-Generic Transform from puncturable PRFs with (1) key-homomorphism and (2) uniform keys.

Puncturable PRF with
(1) adaptive security
(2) collusion resistant PR
(3) 1-key privacy

Puncturable PRF with (Ada,CR)-Pseudorandomness and (Ada,1-key)-Privacy

Conclusion

- A private **puncturable** PRF from standard lattice assumptions that has
  - adaptive collusion resistant pseudorandomness
  - and adaptive 1-key privacy
- Open Problems
  - How to construct Private Puncturable PRF with collusion resistant privacy
  - How to construct adaptively secure and/or collusion resistant (private) contained PRFs for general constraints.

Conclusion

- A private **puncturable** PRF from standard lattice assumptions that has
  - adaptive collusion resistant pseudorandomness
  - and adaptive 1-key privacy
- Open Problems
  - How to construct Private Puncturable PRF with collusion resistant privacy
  - How to construct adaptively secure and/or collusion resistant (private) contained PRFs for general constraints.

Thanks for your Attention!