Updatable Private Set Intersection Revisited: Extended Functionalities, Deletion, and Worst-Case Complexity

Saikrishna Badrinarayanan[1], Peihan Miao[2], Xinyi Shi[2],
Max Tromanhauser[3], Ruida Zeng[2]

[1]LinkedIn, [2]Brown University, [3]Cornell University

Asiacrypt 2024

Today's Talk

1. The Updatable Private Set Intersection Setting
2. Previous Results & Our Improvements
3. High-Level Construction Preview
4. Evaluation

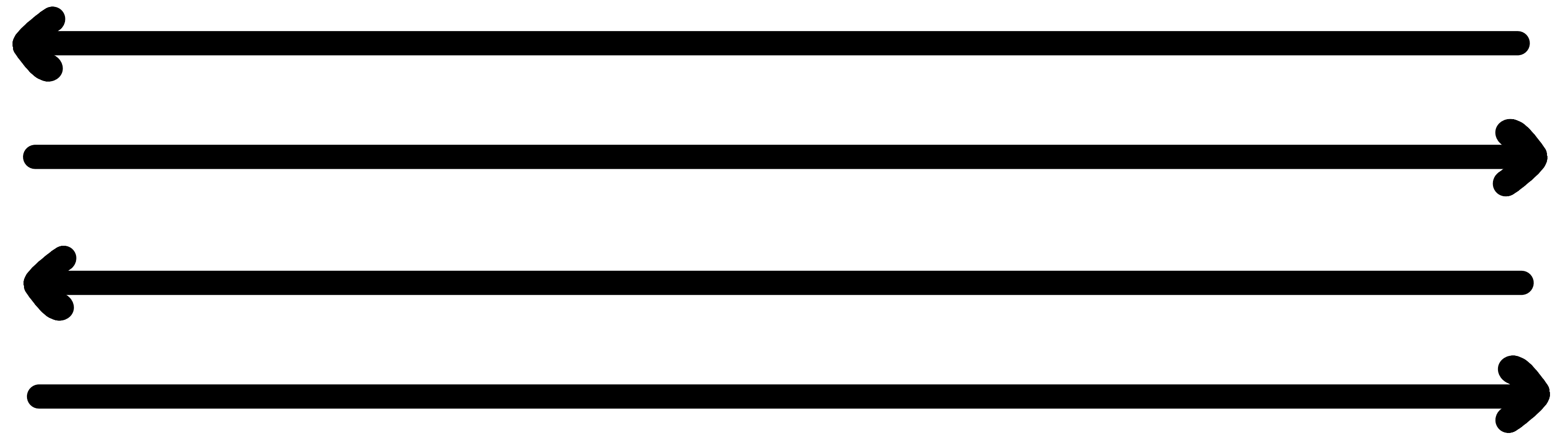
Private Set Intersection (PSI)

Alice

$X = \{x_1, x_2, \ldots, x_n\}$

Bob

$Y = \{y_1, y_2, \ldots, y_n\}$

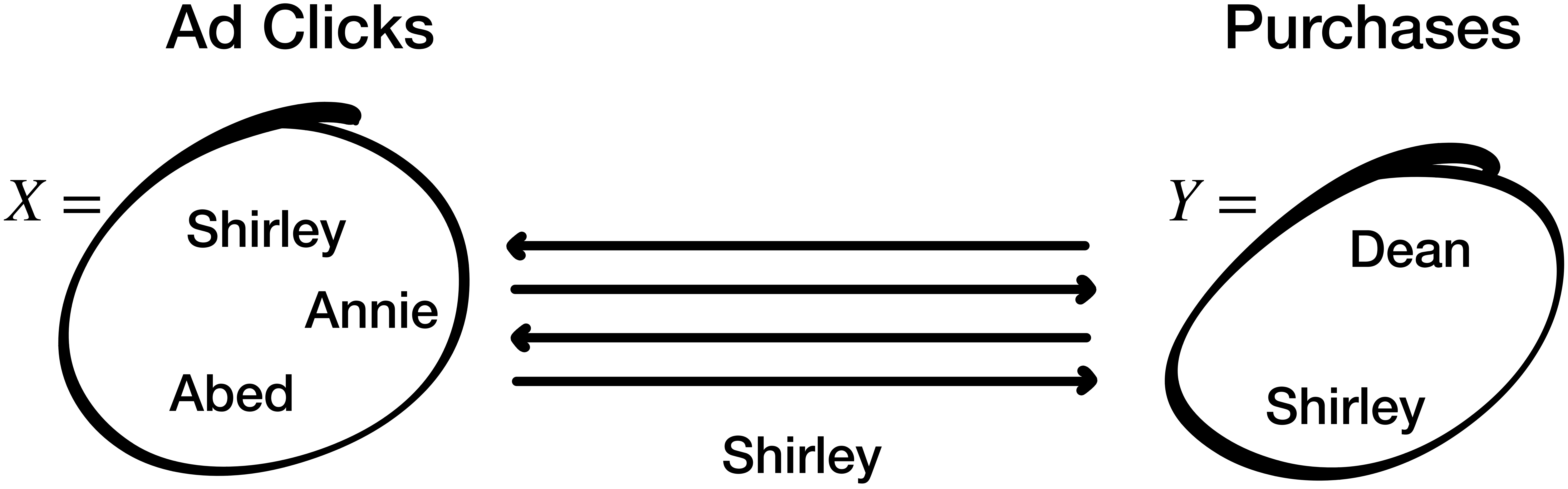


$X \cap Y$

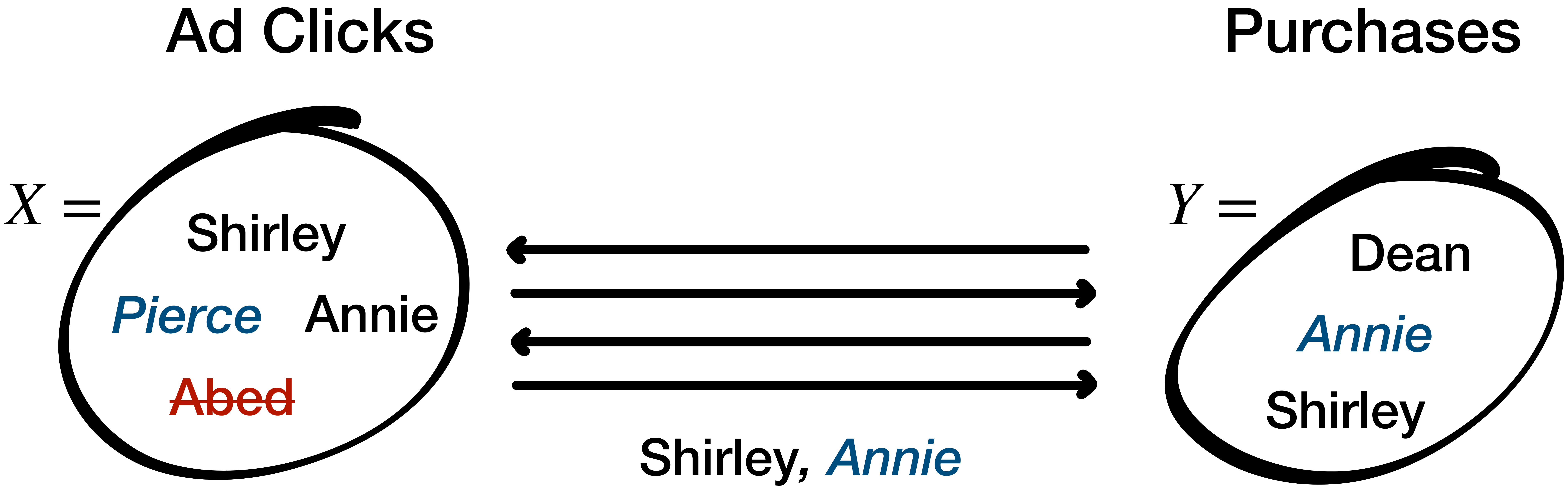
Very well studied…

[HFH99, KS05, DT10, DMRY11, JL10, PSZ14, KKRT16, PRTY19,IKN+20, CGS22, RR22, …]

Updatable Private Set Intersection (UPSI)



Updatable Private Set Intersection (UPSI)



Ad Clicks

$X =$

Shirley

Pierce Annie

~~Abed~~

Purchases

$Y =$

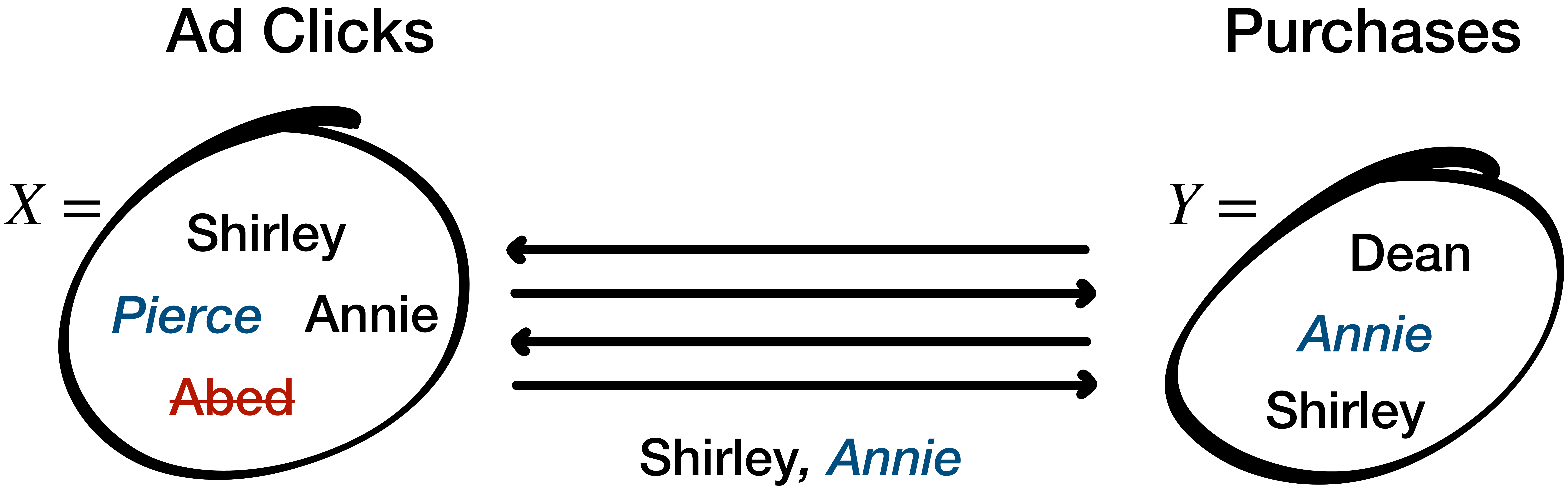
Dean

Annie

Shirley

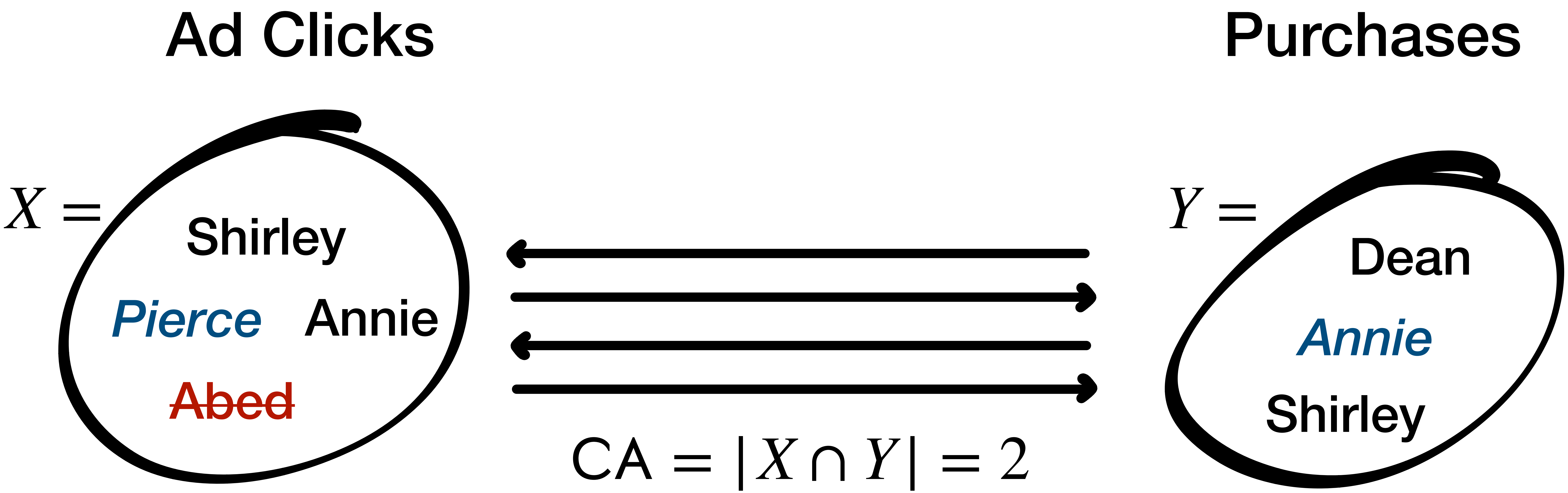
Shirley, *Annie*

Updatable Private Set Intersection (UPSI)



Communication and computation proportional to *update size*.

Updatable Private Set Intersection (UPSI)



Ad Clicks

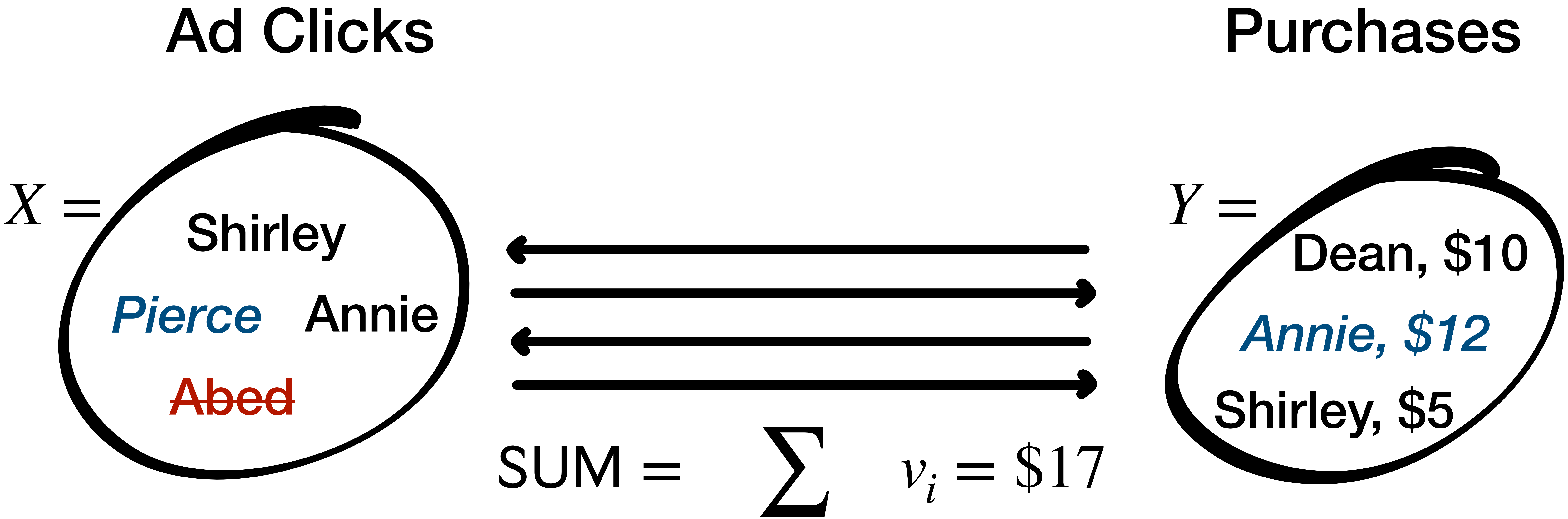
$X =$ Shirley Pierce Annie ~~Abed~~

Purchases

$Y =$ Dean Annie Shirley

$\mathrm{CA} = |X \cap Y| = 2$

Updatable Private Set Intersection (UPSI)



Ad Clicks

$X =$

Shirley

Pierce

Annie

~~Abed~~

Purchases

$Y =$

Dean, $10

Annie, $12

Shirley, $5

$$\text{SUM} = \sum_{i : x_i \in X \cap Y} v_i = \$17$$

Previous Work

Badrinarayanan et al. (PETS ’22) gave protocols for Updatable PSI in the following regimes (with semi-honest security)

Paper	Functionality	Output	Updates	Complexity
[BMX22]	PSI	Two-Sided	Addition Only	$O(n)$
		One-Sided		$O^*(n \log N)$
		Two-Sided	Weak Deletion	$O(nt)$

where N is the total size of the input sets, n is the size of the update, and O^* denotes amortized complexity.

Our Work

Paper	Functionality	Output	Updates	Complexity
[BMX22]	PSI	Two-Sided	Addition Only	$O(n)$
		One-Sided		$O^*(n \log N)$
		Two-Sided	Weak Deletion	$O(nt)$
Ours	PSI, PSI-CA, PSI-SUM	One-Sided	Addition Only	$O(n \log N)$
	Circuit PSI	Secret Shared		

Our Work

Paper	Functionality	Output	Updates	Complexity
[BMX22]	PSI	Two-Sided	Addition Only	$O(n)$
		One-Sided		$O^*(n \log N)$
		Two-Sided	Weak Deletion	$O(nt)$
Ours	PSI, PSI-CA, PSI-SUM	One-Sided	Addition Only	$O(n \log N)$
	Circuit PSI	Secret Shared		
	PSI, PSI-CA, PSI-SUM	One-Sided	Single Deletion	

Our Work

Paper	Functionality	Output	Updates	Complexity
[BMX22]	PSI	Two-Sided	Addition Only	$O(n)$
		One-Sided		$O^*(n \log N)$
		Two-Sided	Weak Deletion	$O(nt)$
Ours	PSI, PSI-CA, PSI-SUM	One-Sided	Addition Only	$O(n \log N)$
	Circuit PSI	Secret Shared		
	PSI, PSI-CA, PSI-SUM	One-Sided	Single Deletion	
	PSI, PSI-CA, PSI-SUM		Arbitrary Deletion	$O(n \log^2 N)$

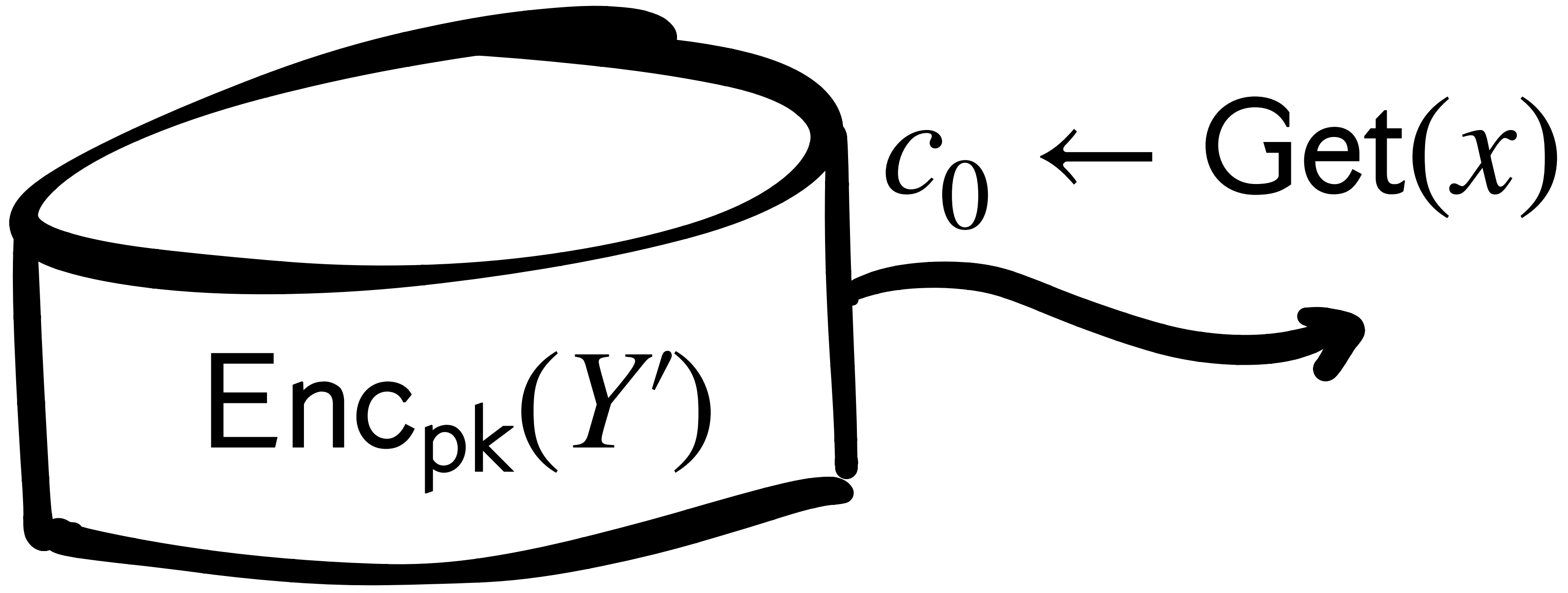
Construction Warm Up

Alice

(pk, sk$_a$), $x \in \mathbb{F}$

Bob

(pk, sk$_b$), $Y \in \mathbb{F}^N$



Enc$_{\mathsf{pk}}(Y')$

$c_0 \leftarrow$ Get(x)

(pk, sk$_a$, sk$_b$) for a 2-out-of-2 threshold, linearly homomorphic encryption scheme over $\mathbb{F}$

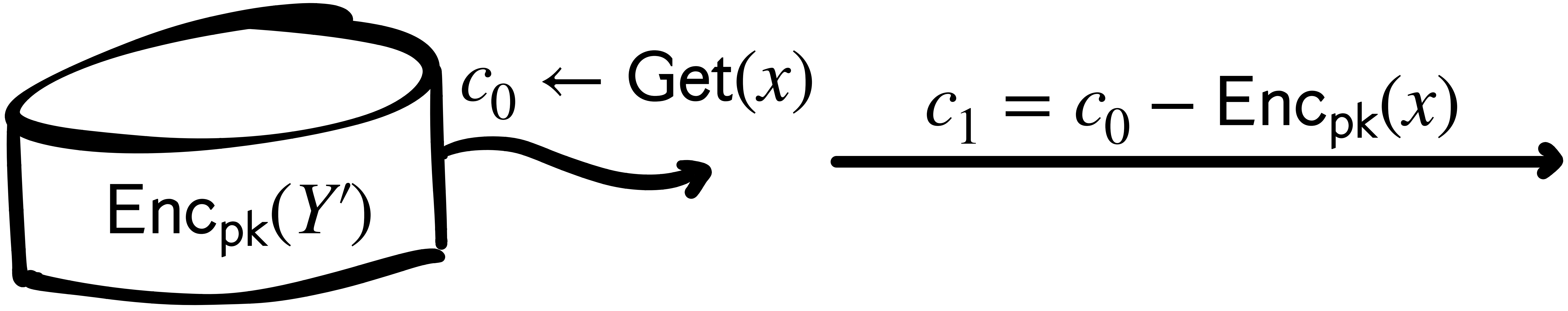
Construction Warm Up

Alice

$(\mathsf{pk}, \mathsf{sk}_a),\ x \in \mathbb{F}$

Bob

$(\mathsf{pk}, \mathsf{sk}_b),\ Y \in \mathbb{F}^N$



$\mathsf{Enc}_{\mathsf{pk}}(Y')$

$c_0 \leftarrow \mathsf{Get}(x)$

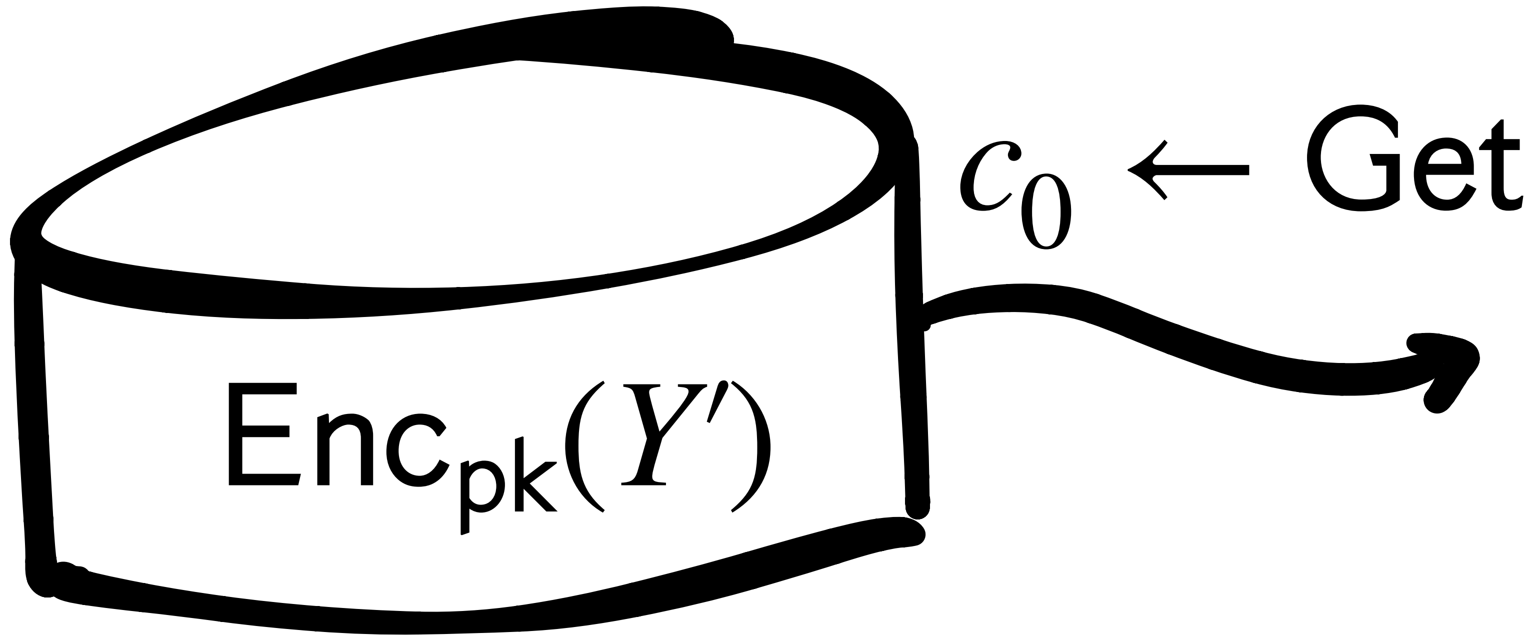
$c_1 = c_0 - \mathsf{Enc}_{\mathsf{pk}}(x)$

$(\mathsf{pk}, \mathsf{sk}_a, \mathsf{sk}_b)$ for a 2-out-of-2 threshold, linearly homomorphic encryption scheme over $\mathbb{F}$

Construction Warm Up

Alice

(pk, sk$_a$), $x \in \mathbb{F}$



Enc$_{\mathsf{pk}}(Y')$

$c_0 \leftarrow$ Get(x)

$$c_1 = c_0 - \mathsf{Enc}_{\mathsf{pk}}(x) \longrightarrow$$

Bob

(pk, sk$_b$), $Y \in \mathbb{F}^N$

$\alpha \xleftarrow{\$} \mathbb{F}^\times$

(pk, sk$_a$, sk$_b$) for a 2-out-of-2 threshold, linearly homomorphic encryption scheme over $\mathbb{F}$

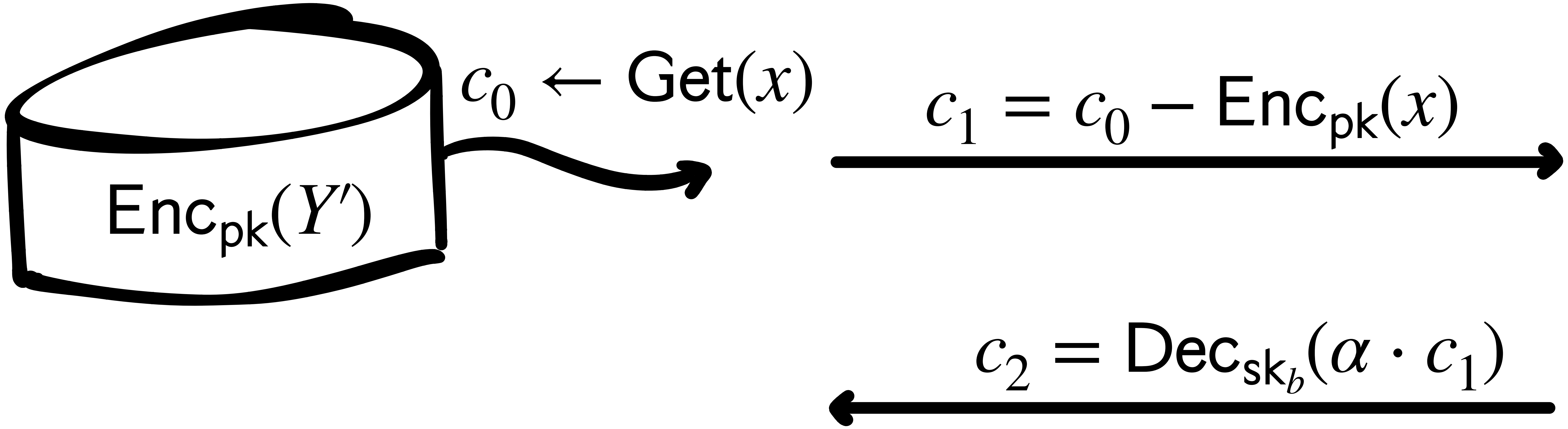
Construction Warm Up

Alice

$(\mathsf{pk}, \mathsf{sk}_a),\ x \in \mathbb{F}$

Bob

$(\mathsf{pk}, \mathsf{sk}_b),\ Y \in \mathbb{F}^N$



$\mathsf{Enc}_{\mathsf{pk}}(Y')$

$c_0 \leftarrow \mathsf{Get}(x)$

$c_1 = c_0 - \mathsf{Enc}_{\mathsf{pk}}(x)$

$\alpha \xleftarrow{\$} \mathbb{F}^{\times}$

$c_2 = \mathsf{Dec}_{\mathsf{sk}_b}(\alpha \cdot c_1)$

$(\mathsf{pk}, \mathsf{sk}_a, \mathsf{sk}_b)$ for a 2-out-of-2 threshold, linearly homomorphic encryption scheme over $\mathbb{F}$

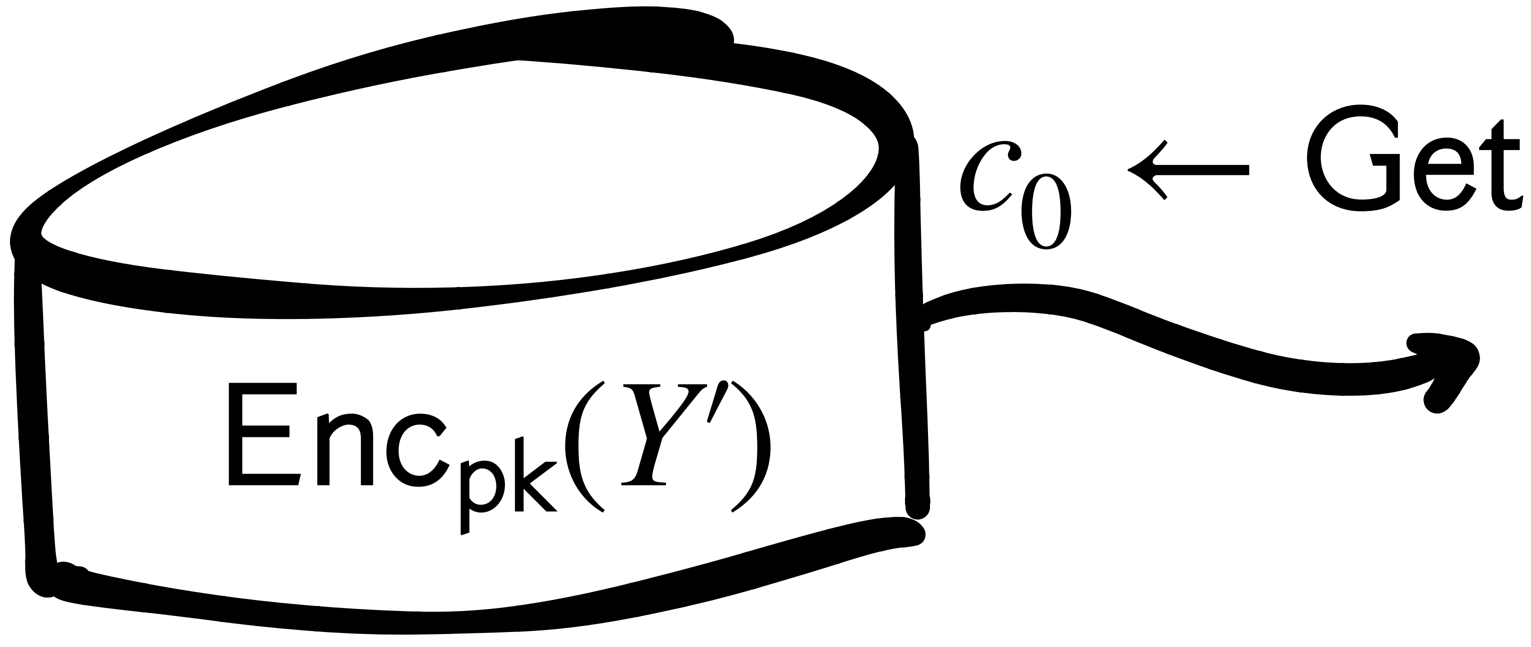
Construction Warm Up

Alice

$(\mathsf{pk}, \mathsf{sk}_a),\ x \in \mathbb{F}$

Bob

$(\mathsf{pk}, \mathsf{sk}_b),\ Y \in \mathbb{F}^N$



$\mathsf{Enc}_{\mathsf{pk}}(Y')$

$c_0 \leftarrow \mathsf{Get}(x)$

$$c_1 = c_0 - \mathsf{Enc}_{\mathsf{pk}}(x) \longrightarrow$$

$\alpha \xleftarrow{\$} \mathbb{F}^{\times}$

$$\longleftarrow c_2 = \mathsf{Dec}_{\mathsf{sk}_b}(\alpha \cdot c_1)$$

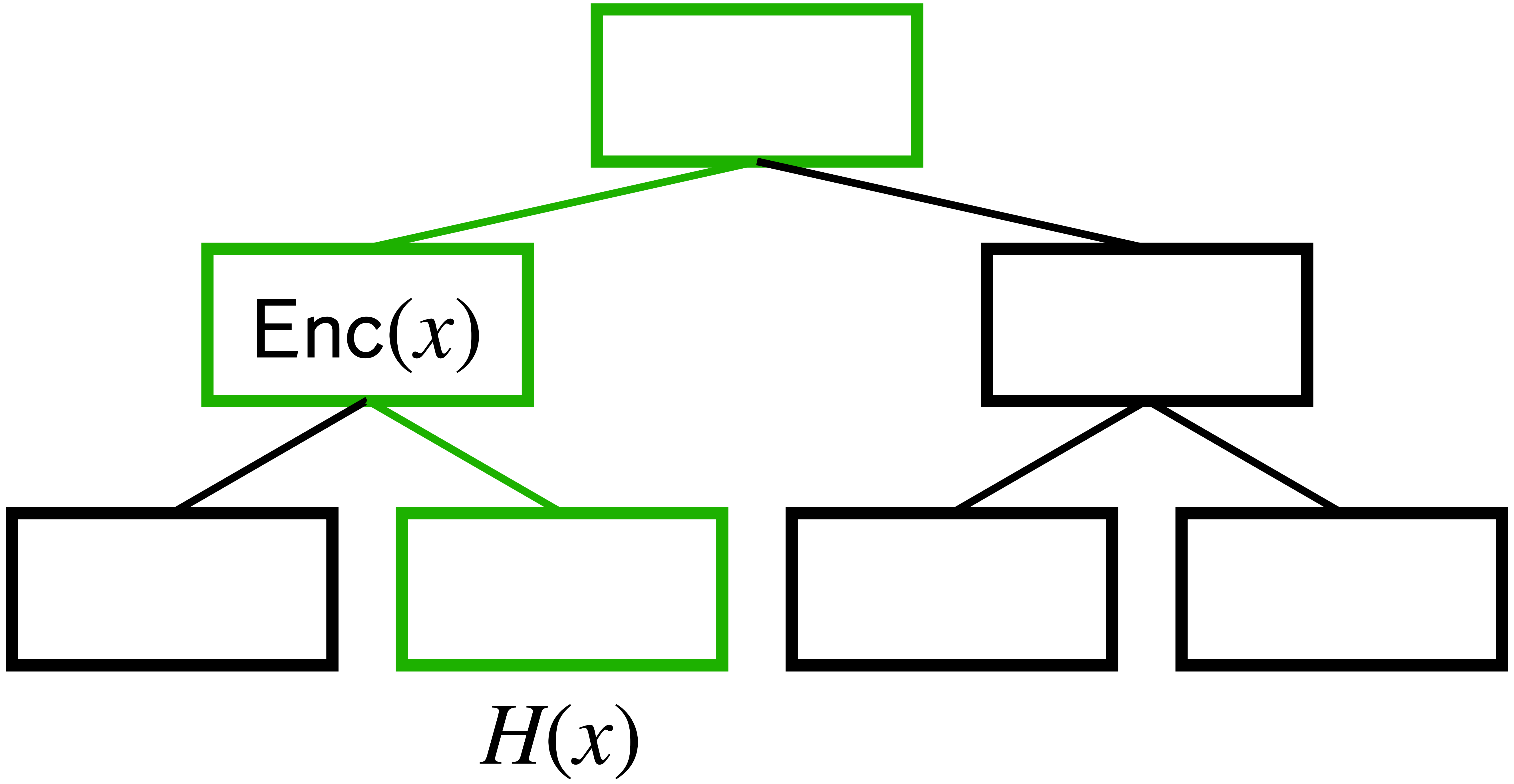
$\mathsf{Dec}_{\mathsf{sk}_a}(c_2) = \alpha(y - x)$

Output $\mathsf{Dec}_{\mathsf{sk}_a}(c_2) = 0$

$(\mathsf{pk}, \mathsf{sk}_a, \mathsf{sk}_b)$ for a 2-out-of-2 threshold, linearly homomorphic encryption scheme over $\mathbb{F}$

Encrypted Database

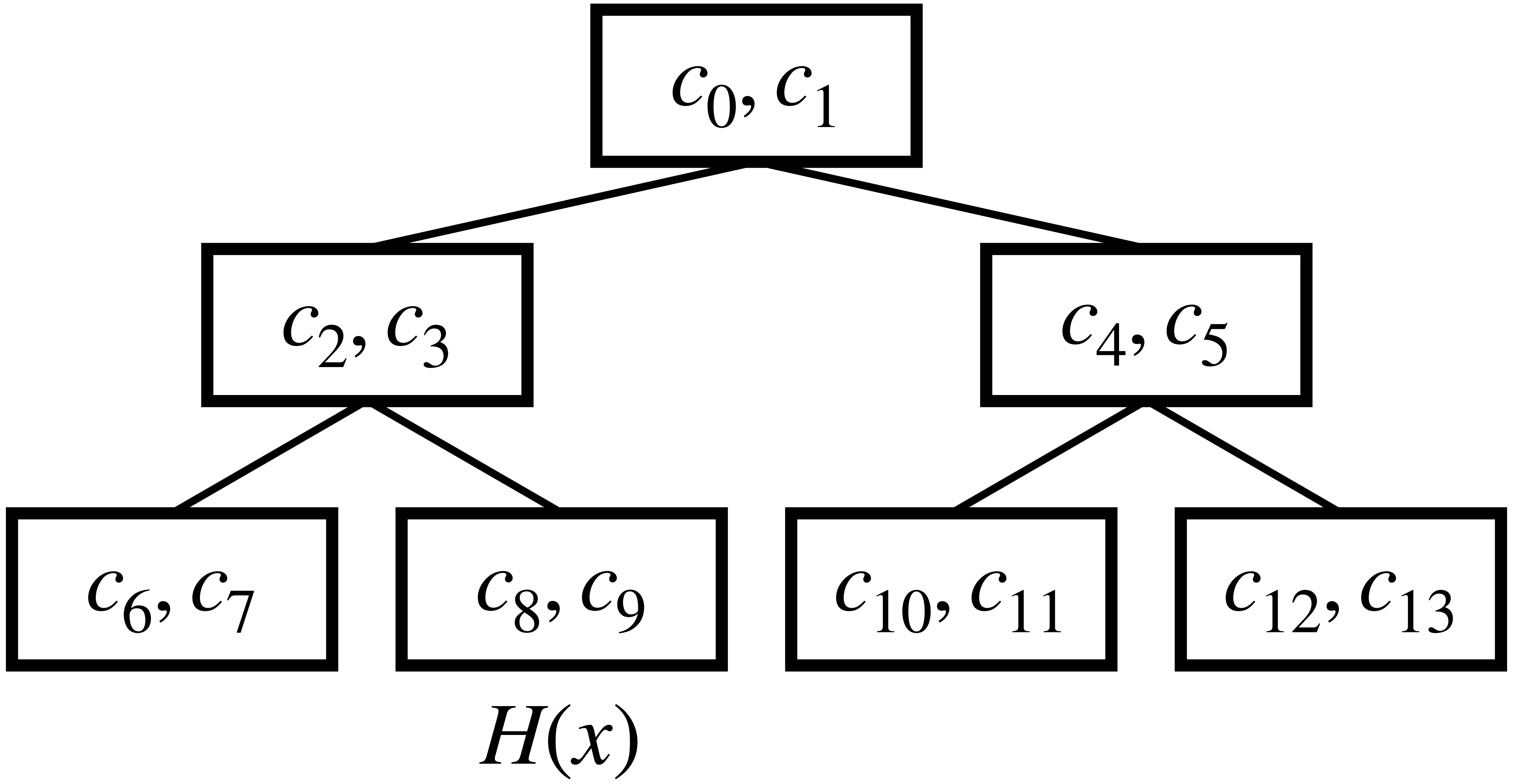
Modified from Path ORAM [SvS+13]



Keep the invariant that x will always appear either in the stash or in the root to leaf path to $H(x)$ for some public hash function.

Encrypted Database: Get

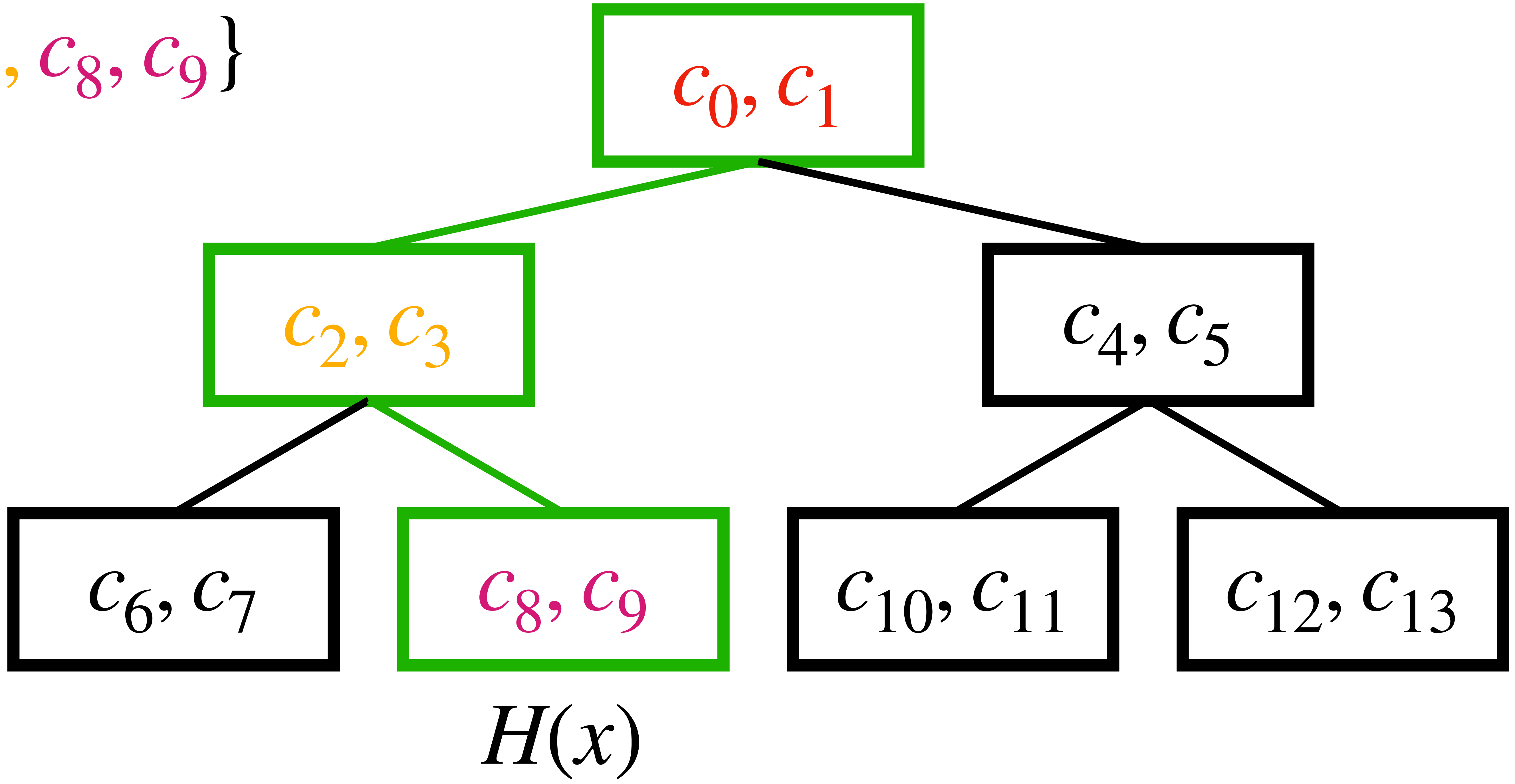
Want to Get(x)



Encrypted Database: Get

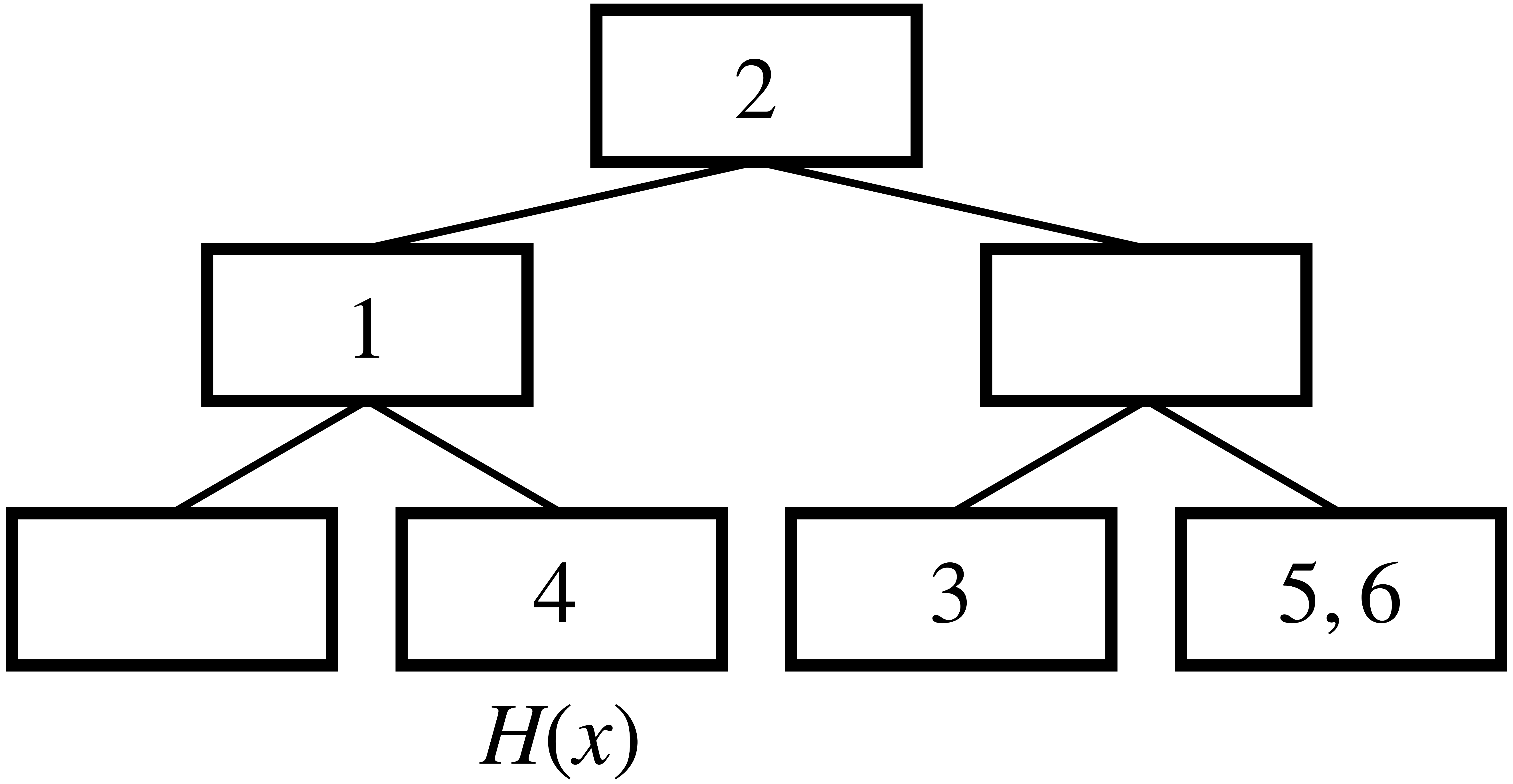
Want to Get(x)

$\rightarrow \{c_0, c_1, c_2, c_3, c_8, c_9\}$



Encrypted Database: Update

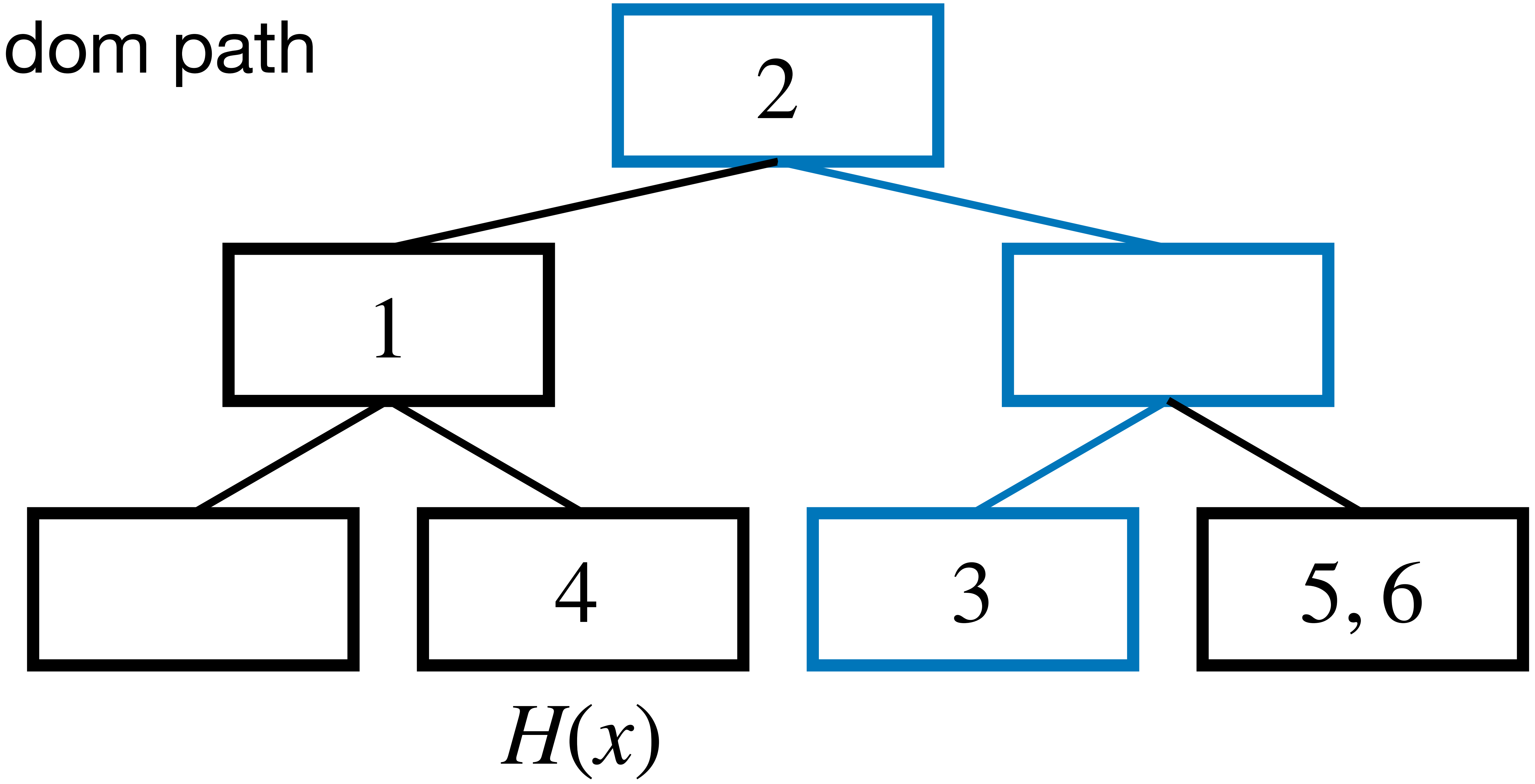
Want to update with x



Encrypted Database: Update

Want to update with x

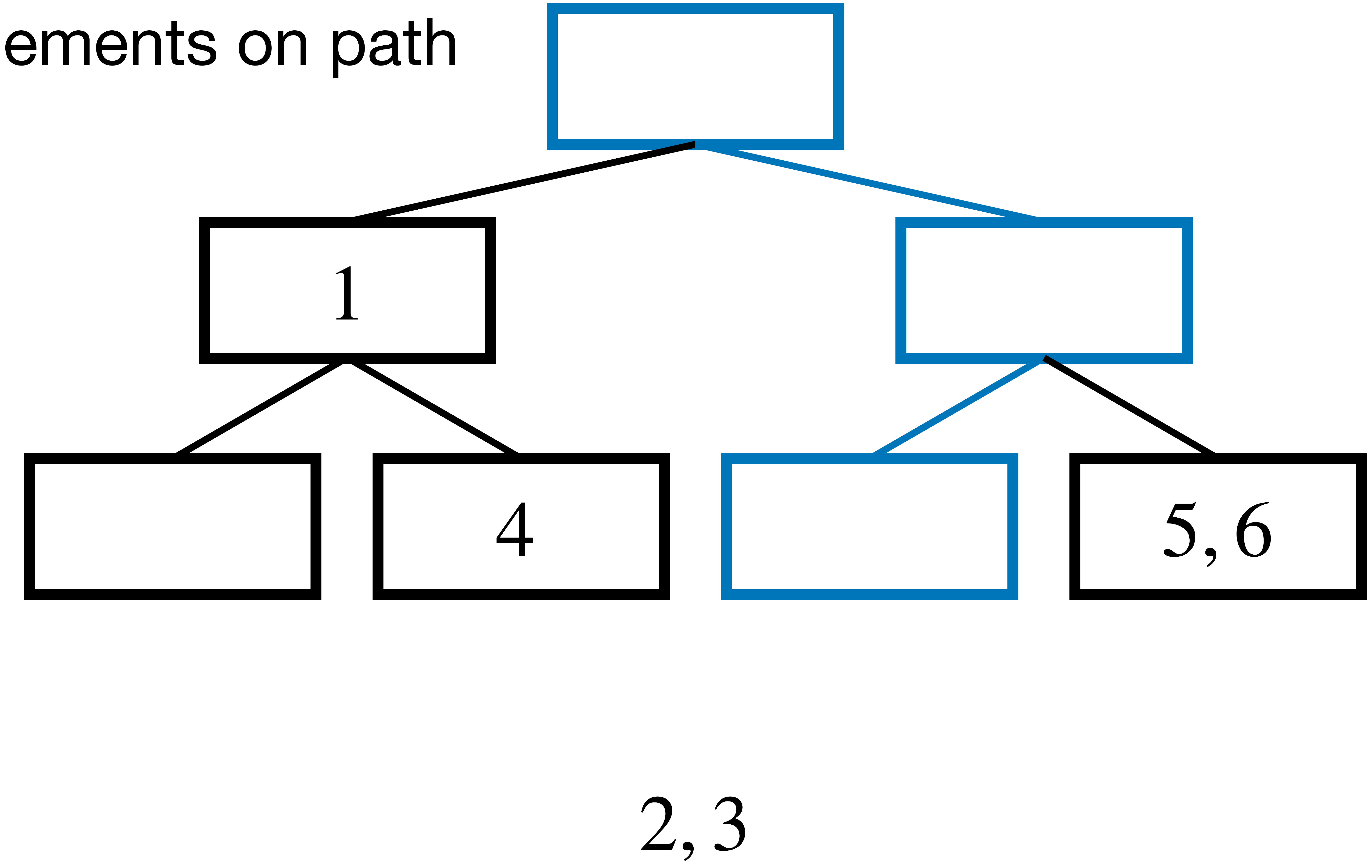
(1) Choose a random path



Encrypted Database: Update

Want to update with x

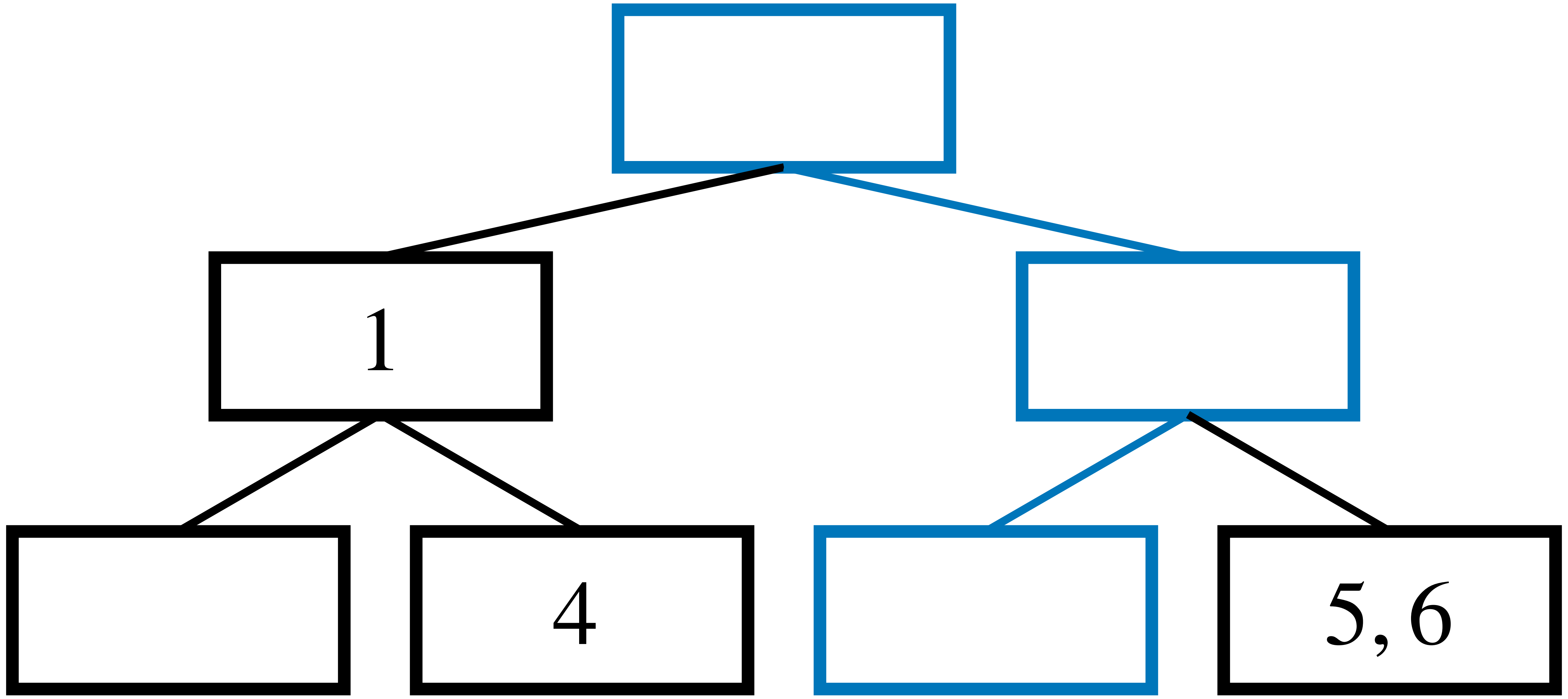
(2) Remove all elements on path



Encrypted Database: Update

Want to update with x

(3) Add x to pool

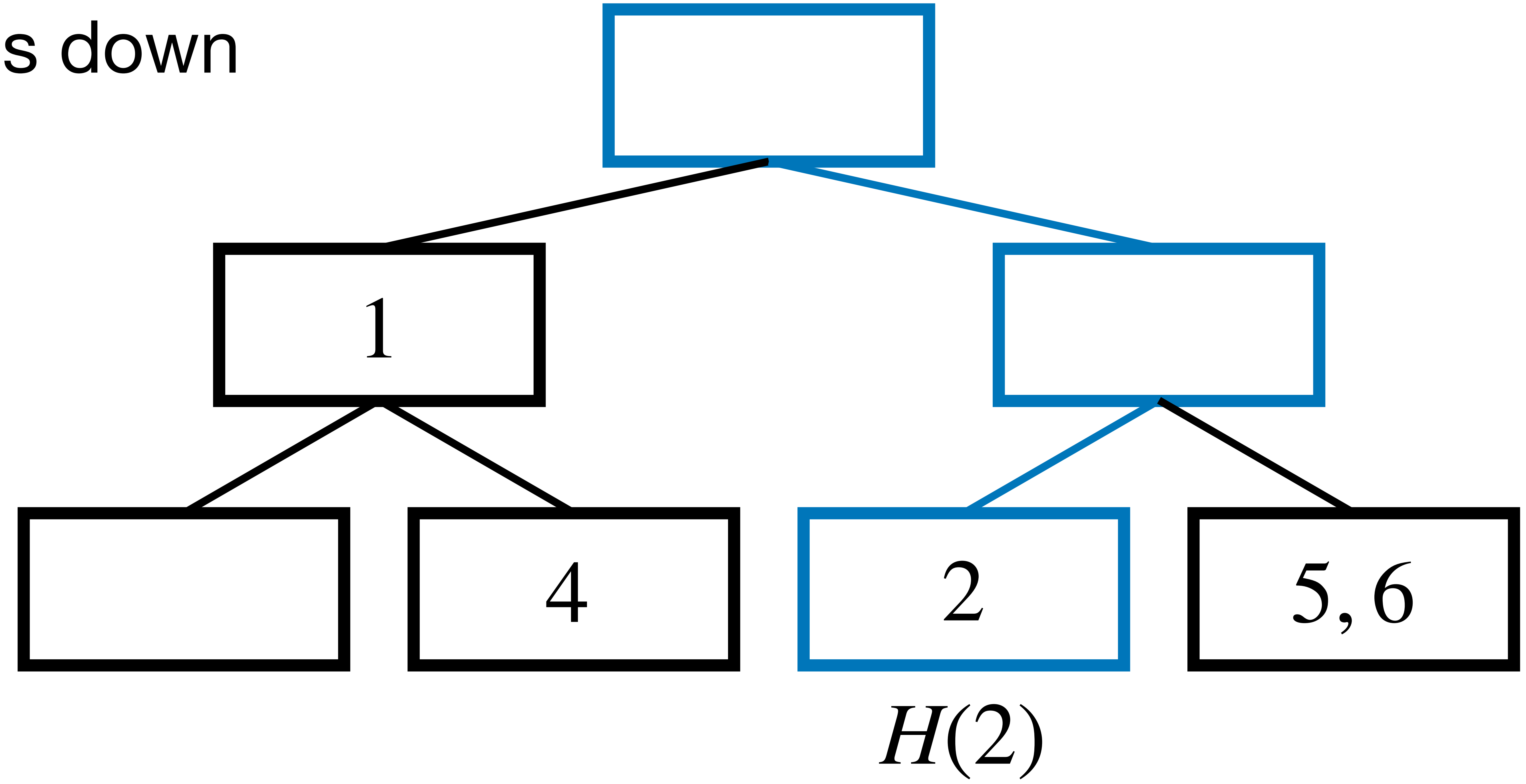


$2, 3, x$

Encrypted Database: Update

Want to update with x

(4) Push elements down

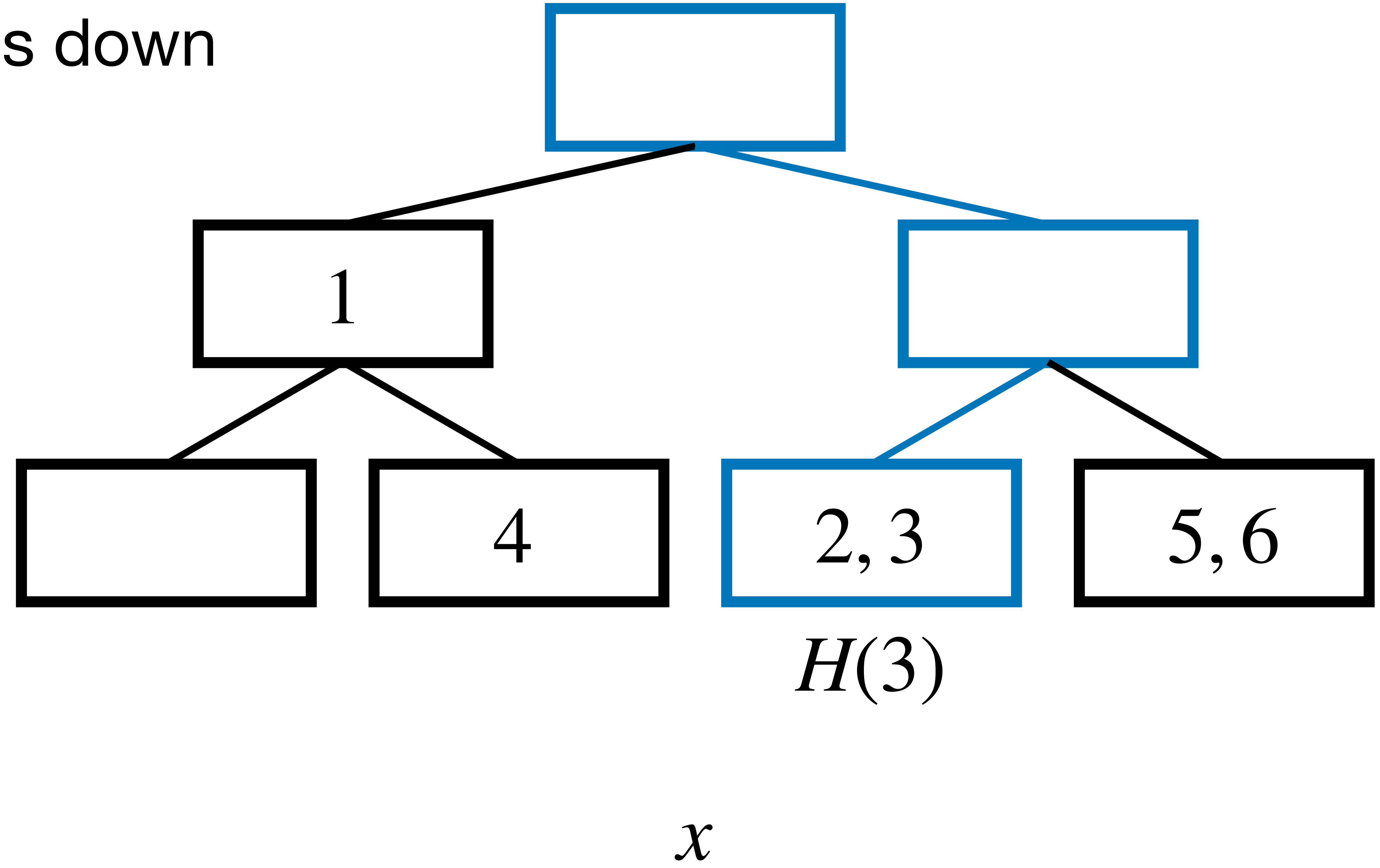


$2, x$

Encrypted Database: Update

Want to update with x

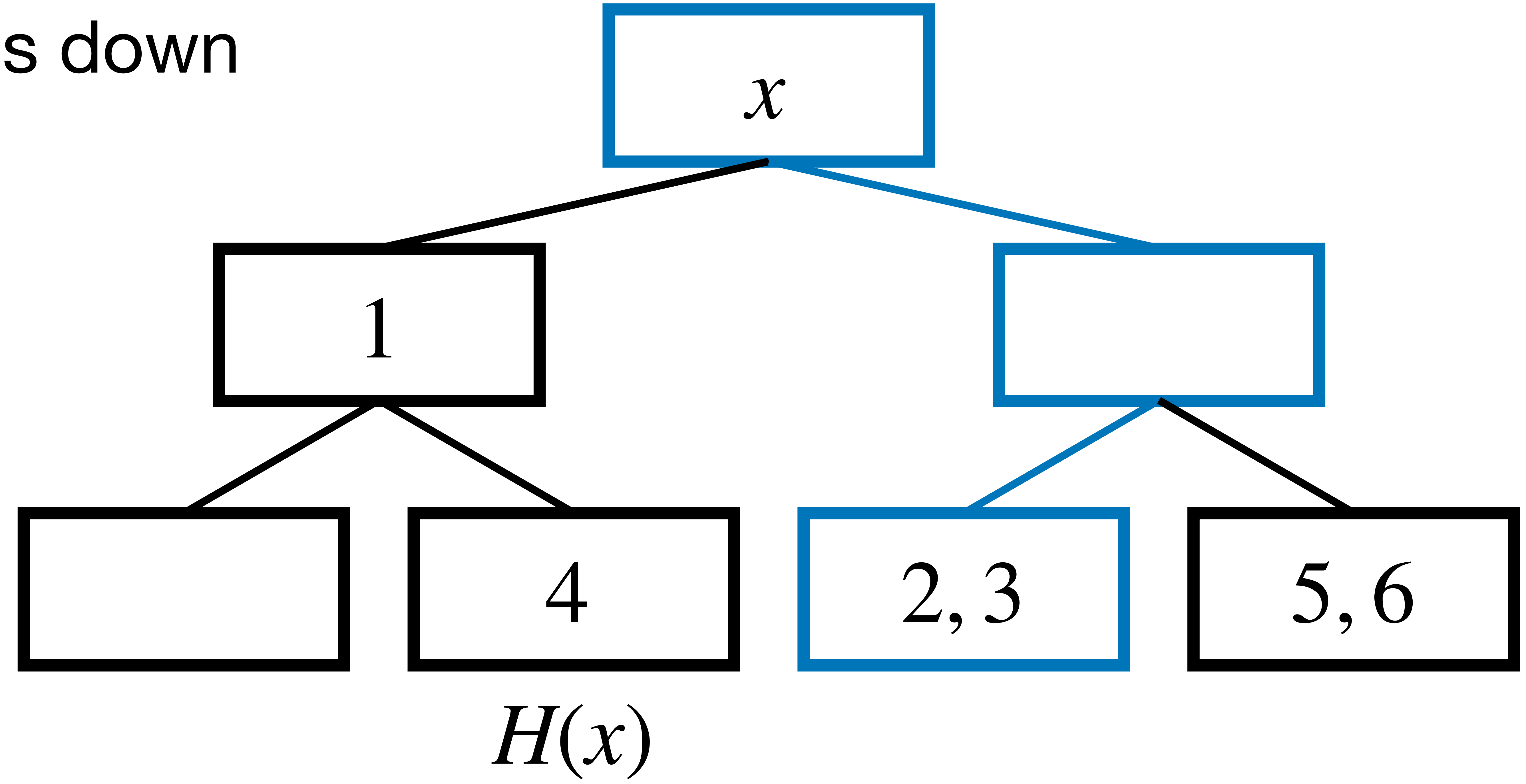
(4) Push elements down



Encrypted Database: Update

Want to update with x

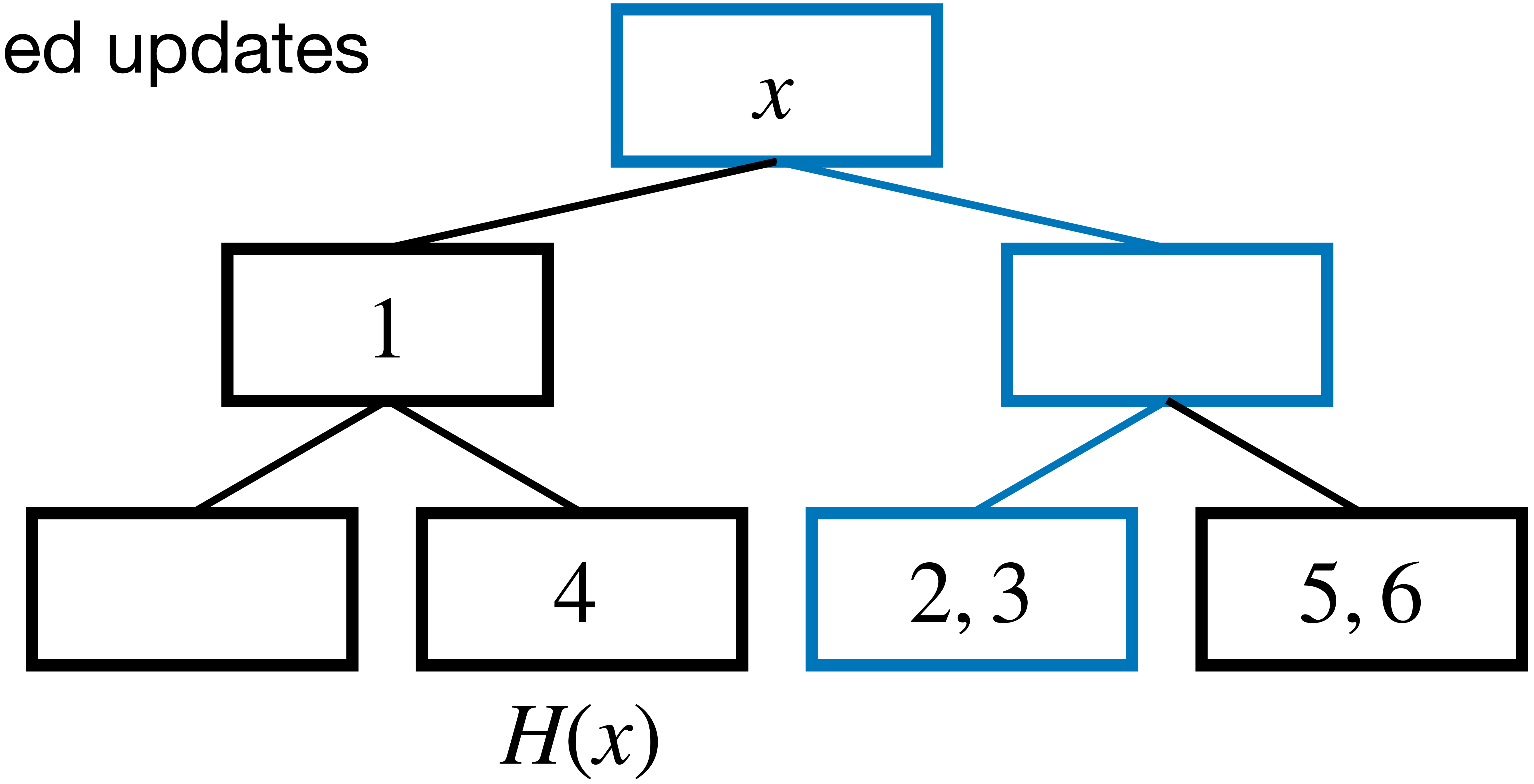
(4) Push elements down



Encrypted Database: Update

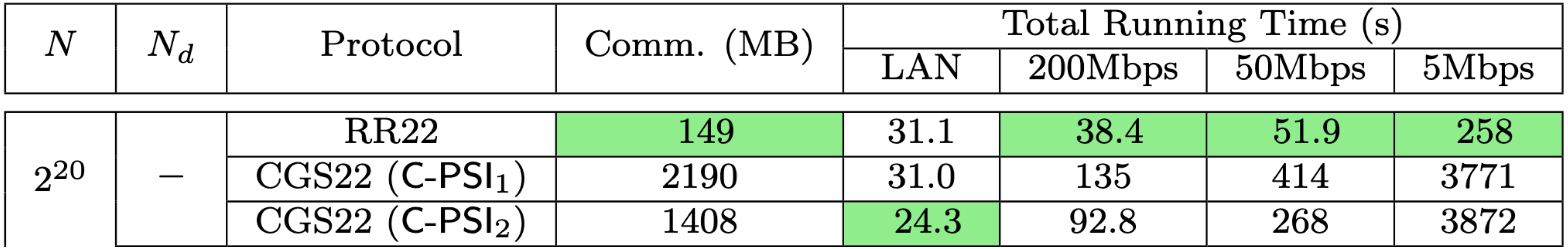
Want to update with x

(5) Send encrypted updates



Enc($\{x, 0\}, \{0, 0\}, \{2, 3\}$)

Evaluations

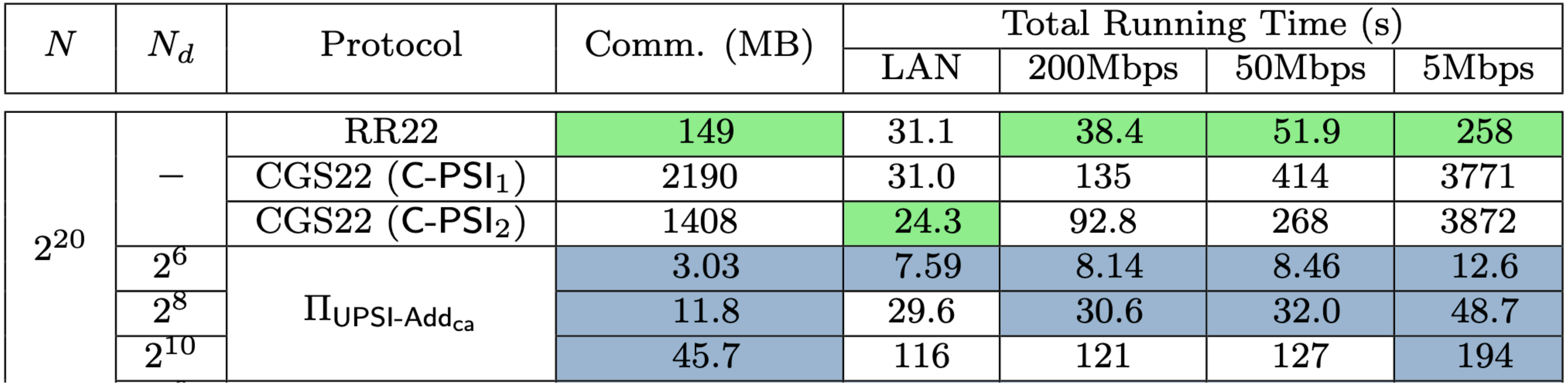


N	N_d	Protocol	Comm. (MB)	Total Running Time (s)			
				LAN	200Mbps	50Mbps	5Mbps
2^{20}	$-$	RR22	149	31.1	38.4	51.9	258
		CGS22 (C-PSI$_1$)	2190	31.0	135	414	3771
		CGS22 (C-PSI$_2$)	1408	24.3	92.8	268	3872

Communication cost and running time comparing **addition only** UPSI to standard **PSI**

[RR22] Blazing Fast PSI from Improved OKVS and Subfield VOLE (CCS ’22)
[CGS22] Circuit-PSI with Linear Complexity via Relaxed Batch OPPRF (PETs ’22)

Evaluations

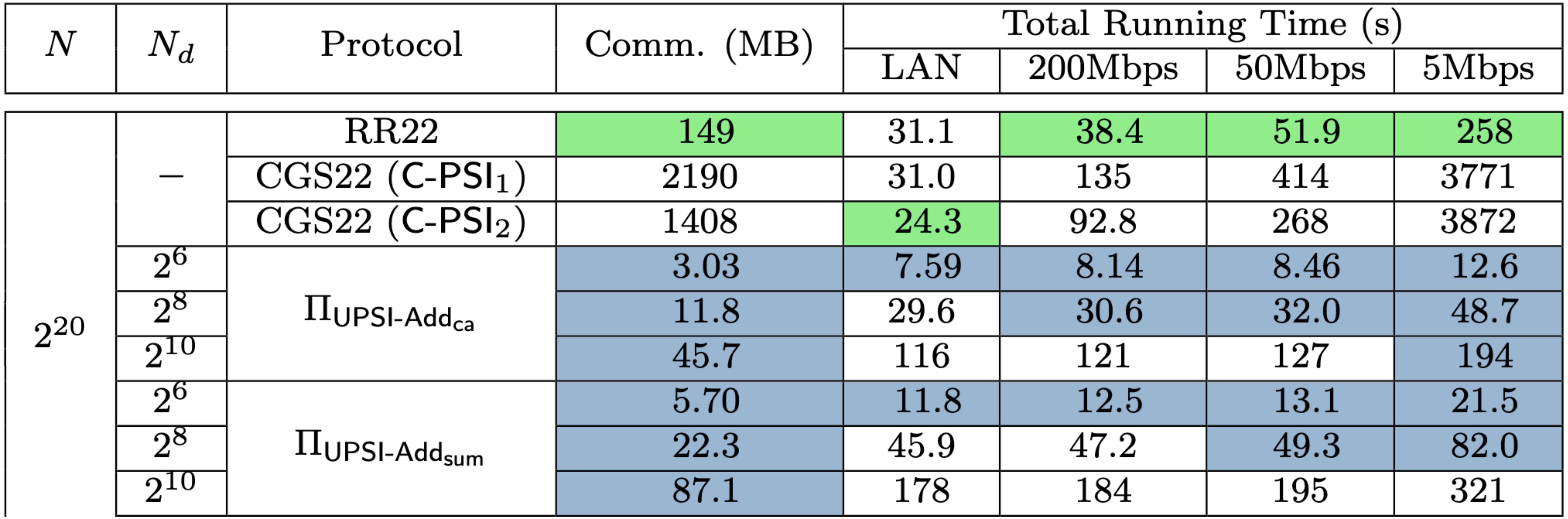


N	N_d	Protocol	Comm. (MB)	Total Running Time (s)			
				LAN	200Mbps	50Mbps	5Mbps
2^{20}	–	RR22	149	31.1	38.4	51.9	258
		CGS22 ($\mathsf{C\text{-}PSI}_1$)	2190	31.0	135	414	3771
		CGS22 ($\mathsf{C\text{-}PSI}_2$)	1408	24.3	92.8	268	3872
	2^6	$\Pi_{\mathsf{UPSI\text{-}Add}_{\mathsf{ca}}}$	3.03	7.59	8.14	8.46	12.6
	2^8		11.8	29.6	30.6	32.0	48.7
	2^{10}		45.7	116	121	127	194

Communication cost and running time comparing **addition only** UPSI to standard **PSI**

[RR22] Blazing Fast PSI from Improved OKVS and Subfield VOLE (CCS ’22)
[CGS22] Circuit-PSI with Linear Complexity via Relaxed Batch OPPRF (PETs ’22)

Evaluations

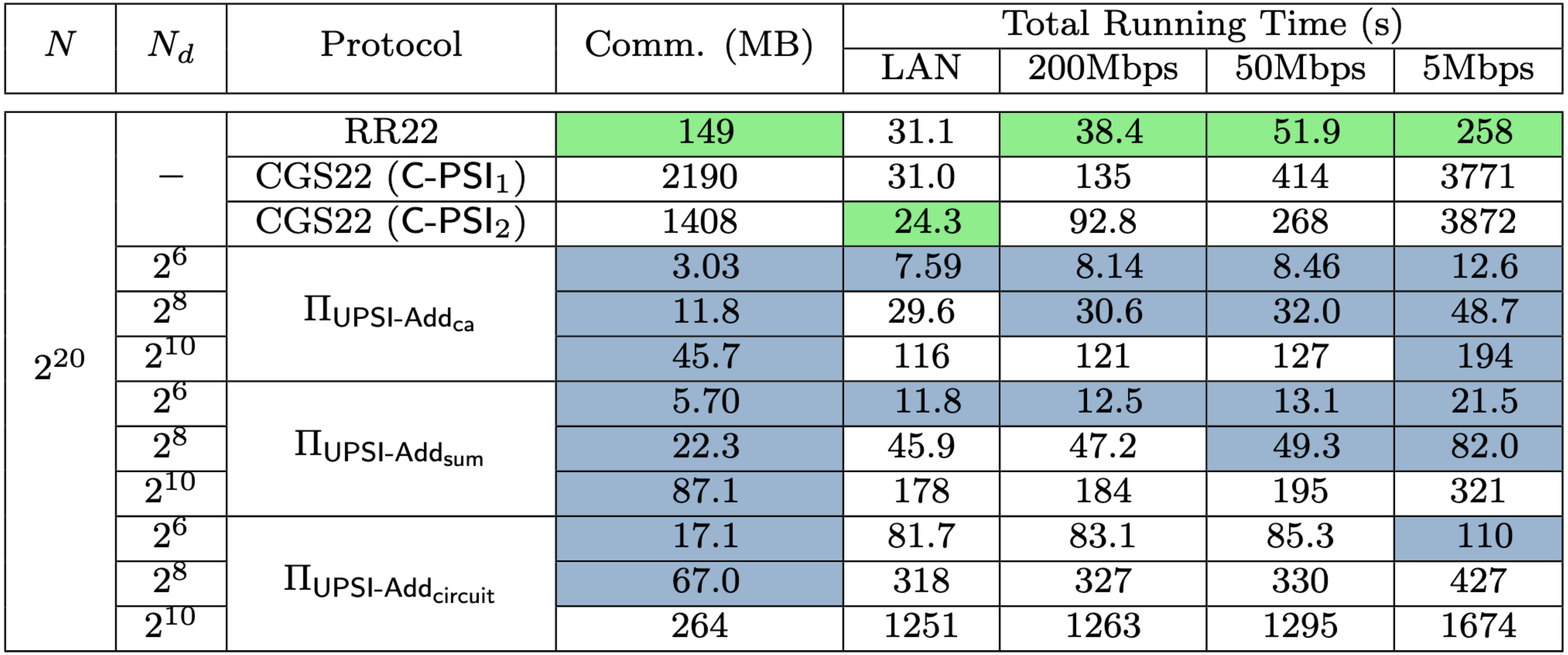


N	N_d	Protocol	Comm. (MB)	Total Running Time (s)			
				LAN	200Mbps	50Mbps	5Mbps
2^{20}	–	RR22	149	31.1	38.4	51.9	258
		CGS22 (C-PSI$_1$)	2190	31.0	135	414	3771
		CGS22 (C-PSI$_2$)	1408	24.3	92.8	268	3872
	2^6	$\Pi_{\text{UPSI-Add}_{\text{ca}}}$	3.03	7.59	8.14	8.46	12.6
	2^8		11.8	29.6	30.6	32.0	48.7
	2^{10}		45.7	116	121	127	194
	2^6	$\Pi_{\text{UPSI-Add}_{\text{sum}}}$	5.70	11.8	12.5	13.1	21.5
	2^8		22.3	45.9	47.2	49.3	82.0
	2^{10}		87.1	178	184	195	321

Communication cost and running time comparing **addition only** UPSI to standard **PSI**

[RR22] Blazing Fast PSI from Improved OKVS and Subfield VOLE (CCS ’22)
[CGS22] Circuit-PSI with Linear Complexity via Relaxed Batch OPPRF (PETs ’22)

Evaluations



N	N_d	Protocol	Comm. (MB)	Total Running Time (s)			
				LAN	200Mbps	50Mbps	5Mbps
2^{20}	–	RR22	149	31.1	38.4	51.9	258
		CGS22 (C-PSI$_1$)	2190	31.0	135	414	3771
		CGS22 (C-PSI$_2$)	1408	24.3	92.8	268	3872
	2^6	$\Pi_{\text{UPSI-Add}_{\text{ca}}}$	3.03	7.59	8.14	8.46	12.6
	2^8		11.8	29.6	30.6	32.0	48.7
	2^{10}		45.7	116	121	127	194
	2^6	$\Pi_{\text{UPSI-Add}_{\text{sum}}}$	5.70	11.8	12.5	13.1	21.5
	2^8		22.3	45.9	47.2	49.3	82.0
	2^{10}		87.1	178	184	195	321
	2^6	$\Pi_{\text{UPSI-Add}_{\text{circuit}}}$	17.1	81.7	83.1	85.3	110
	2^8		67.0	318	327	330	427
	2^{10}		264	1251	1263	1295	1674

Communication cost and running time comparing **addition only** UPSI to standard **PSI**

[RR22] Blazing Fast PSI from Improved OKVS and Subfield VOLE (CCS ’22)
[CGS22] Circuit-PSI with Linear Complexity via Relaxed Batch OPPRF (PETs ’22)

Thank you