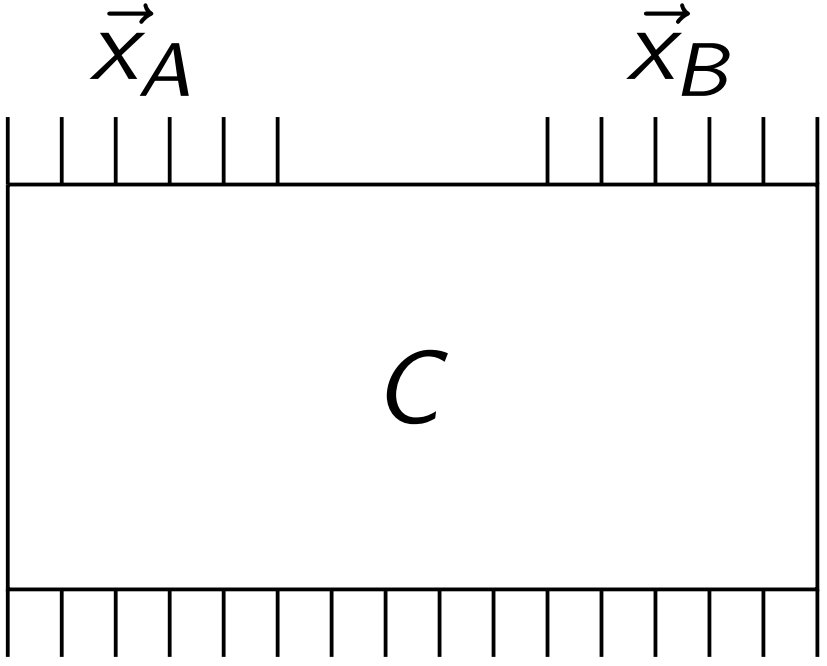
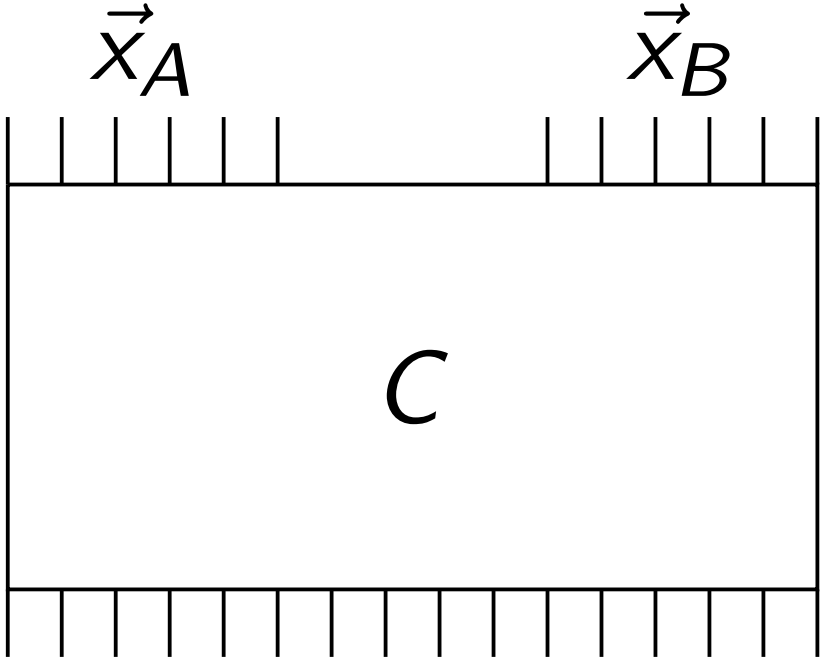
Breaking the Circuit-Size Barrier under Quasi-Polynomial LPN

Sublinear 2-PC from LPN, the HSS Route

Geoffroy Couteau Pierre Meyer

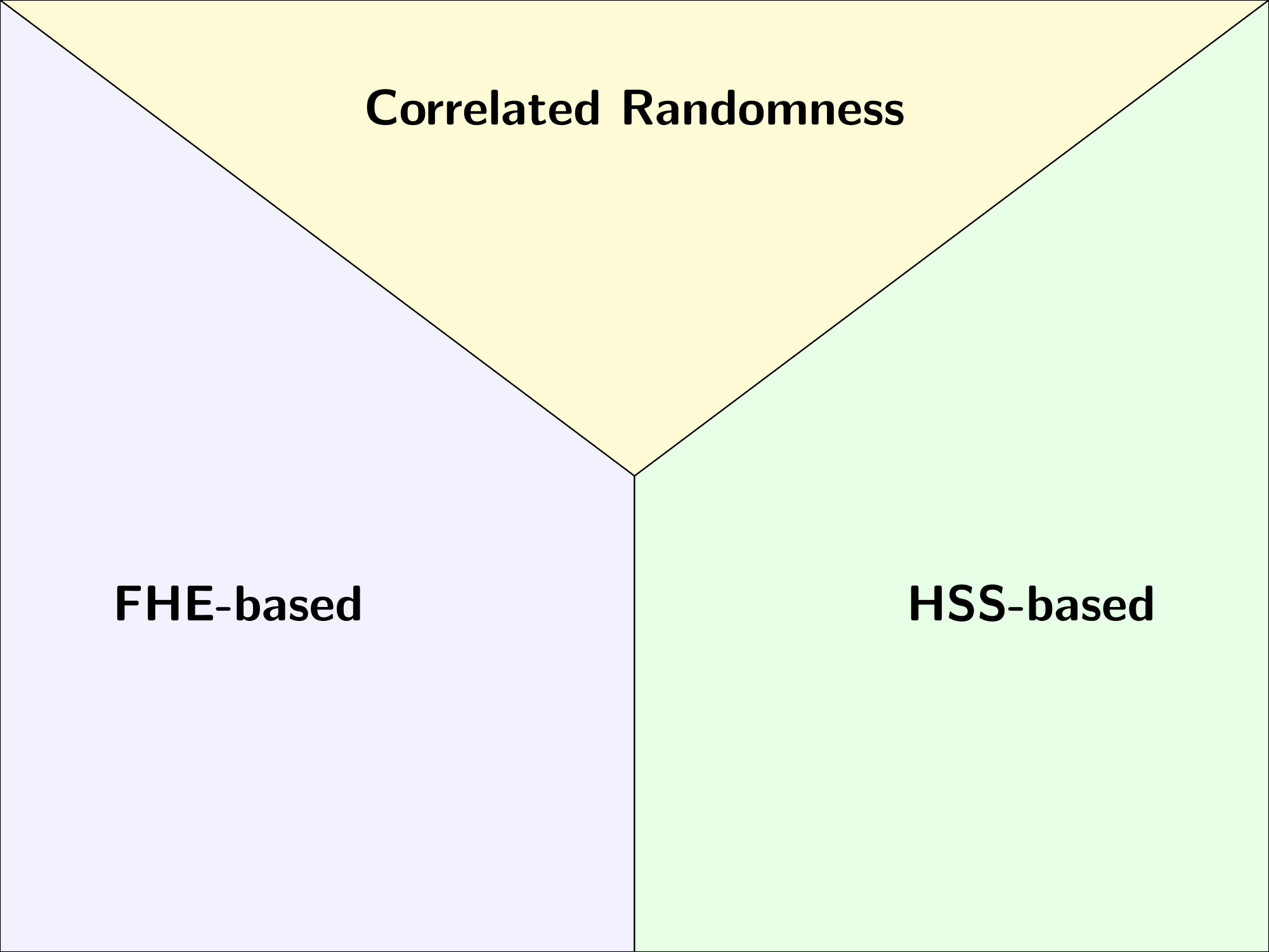
Eurocrypt 2021

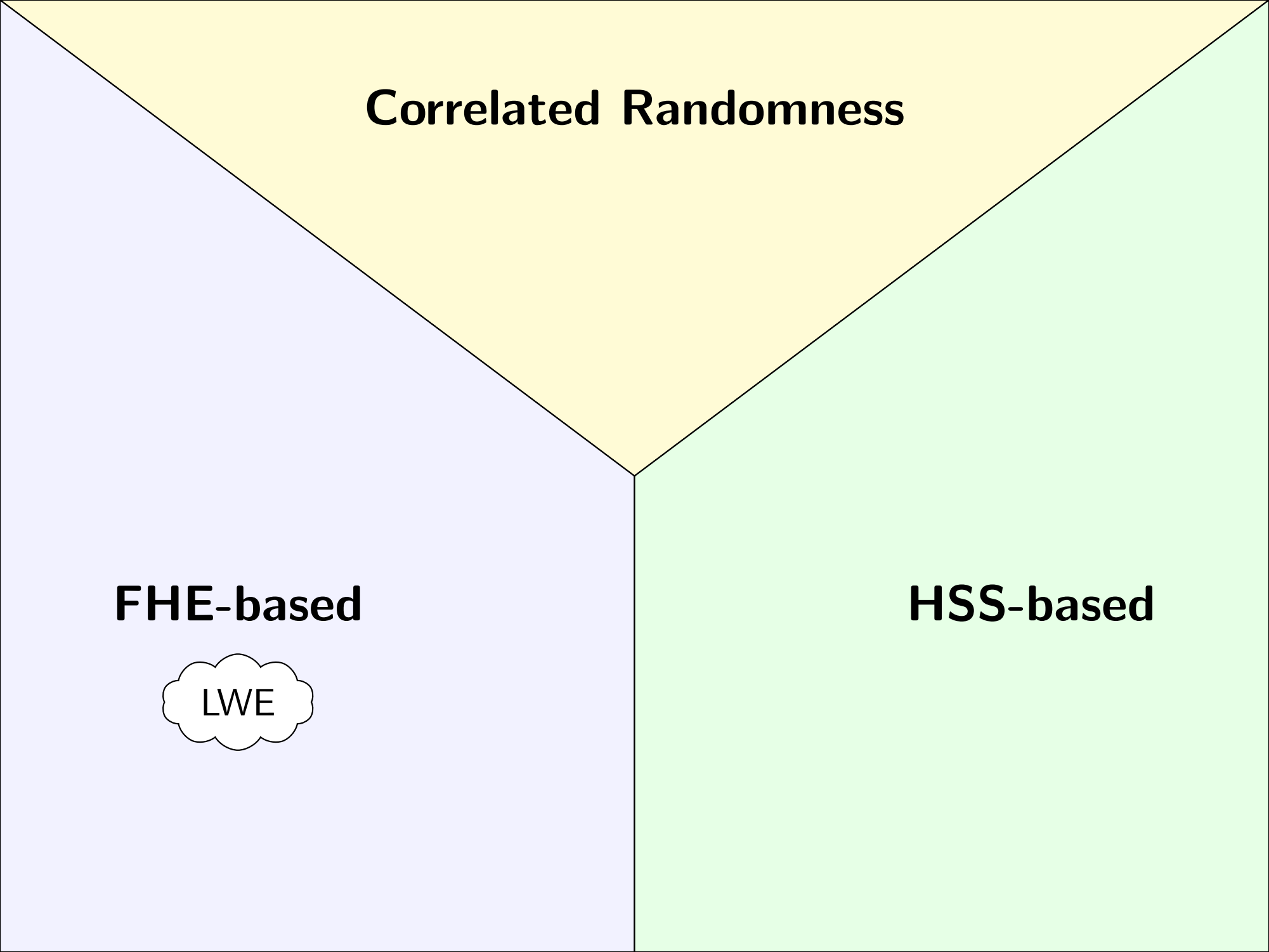

$\vec{x}_A$
$\vec{x}_B$
C

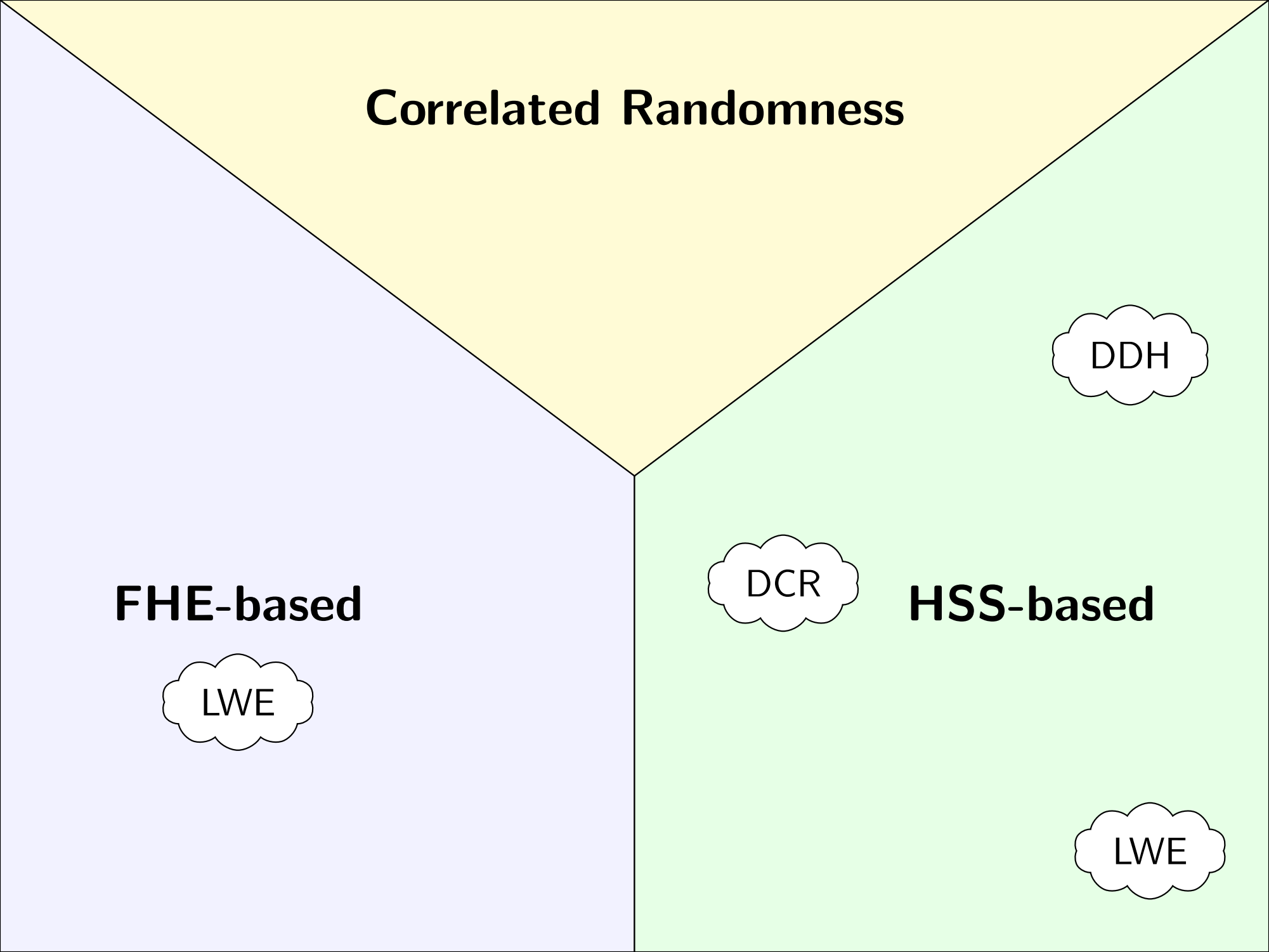


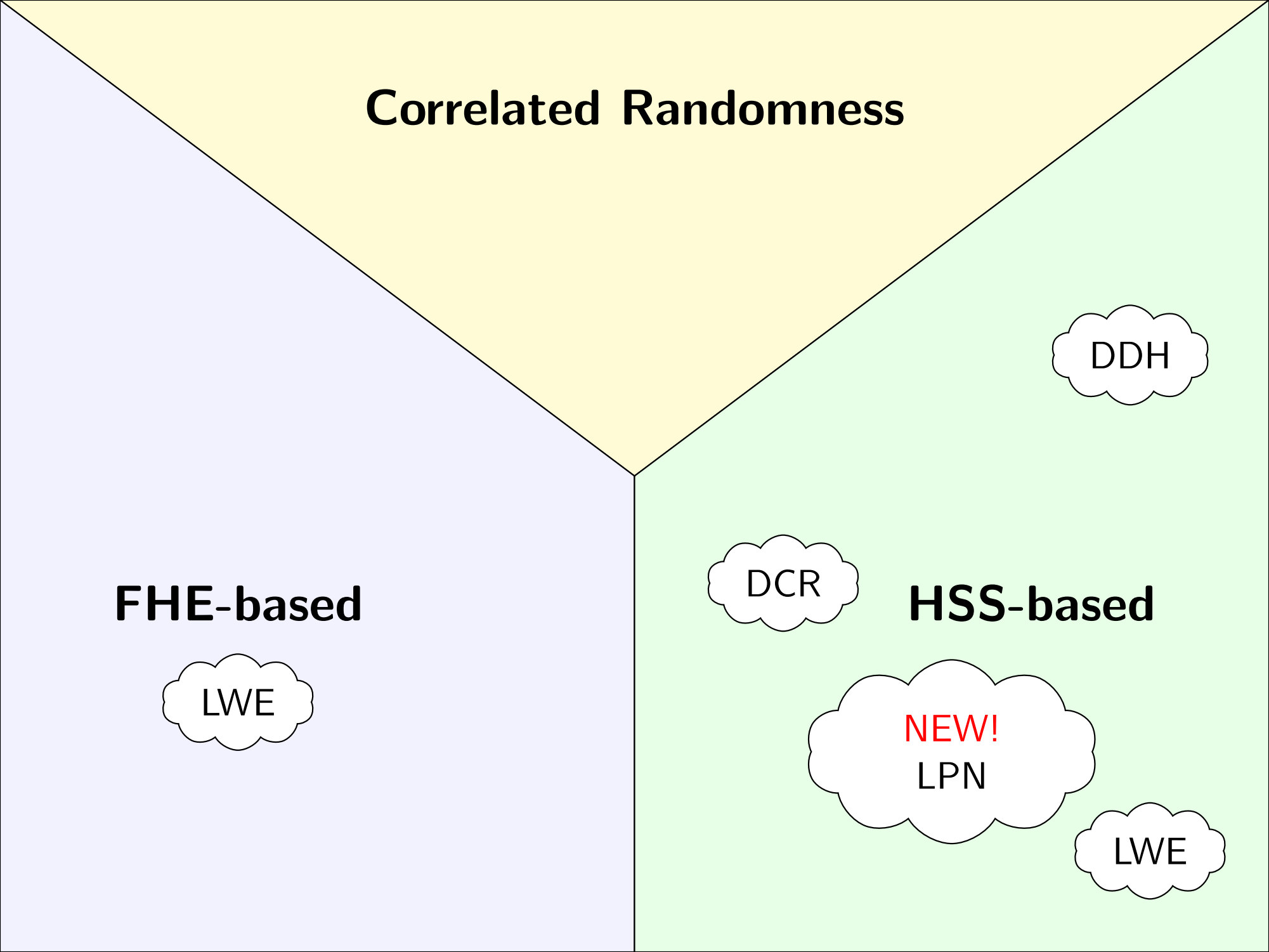
Communication $o(|C|)$

Computation $|C|^{\mathcal{O}(1)}$

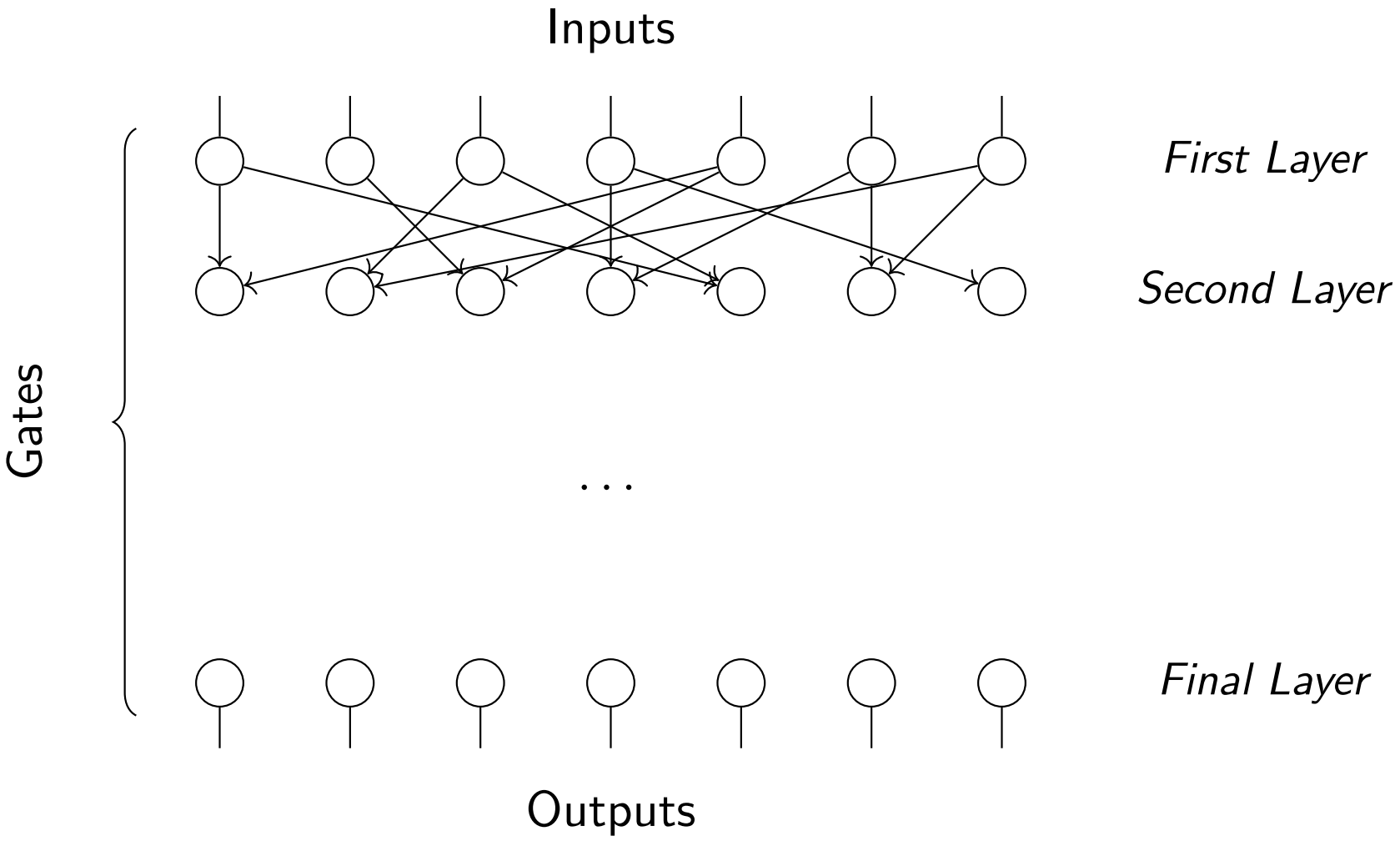

Correlated Randomness
FHE-based
HSS-based

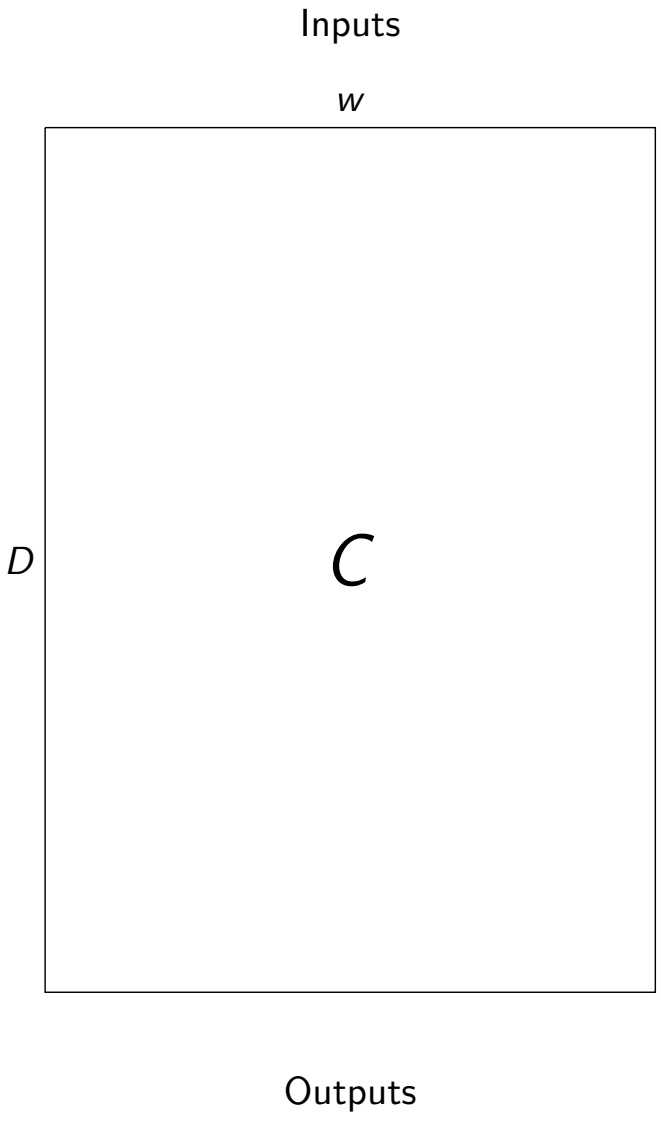

Correlated Randomness
FHE-based
LWE
HSS-based

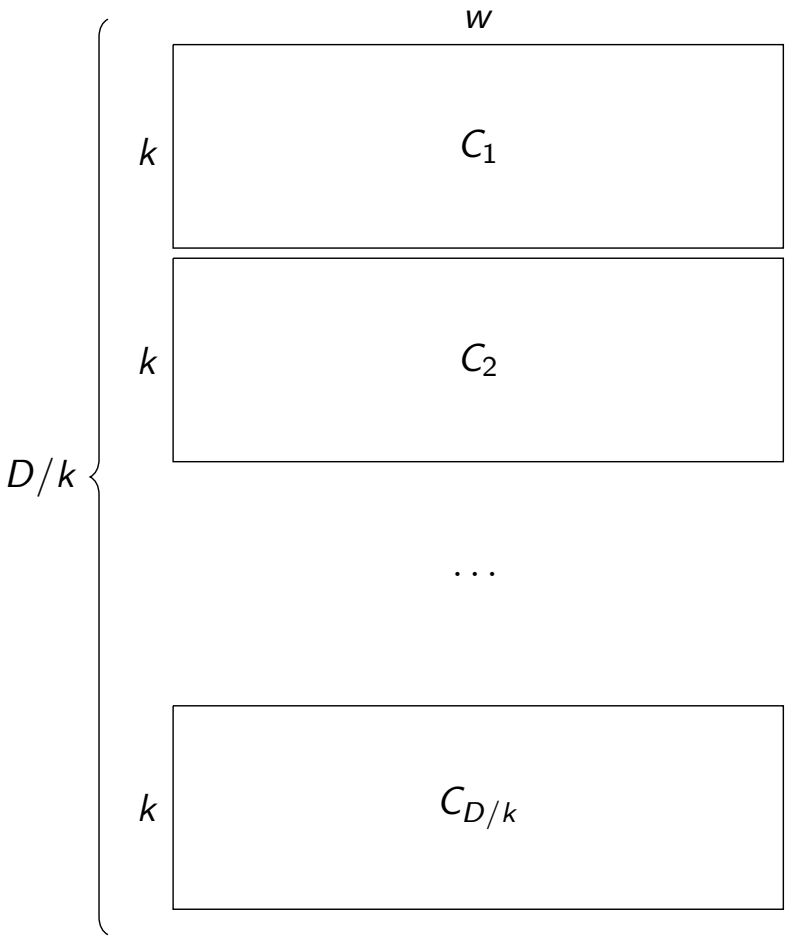

Correlated Randomness
DDH
DCR
FHE-based
HSS-based
LWE
LWE

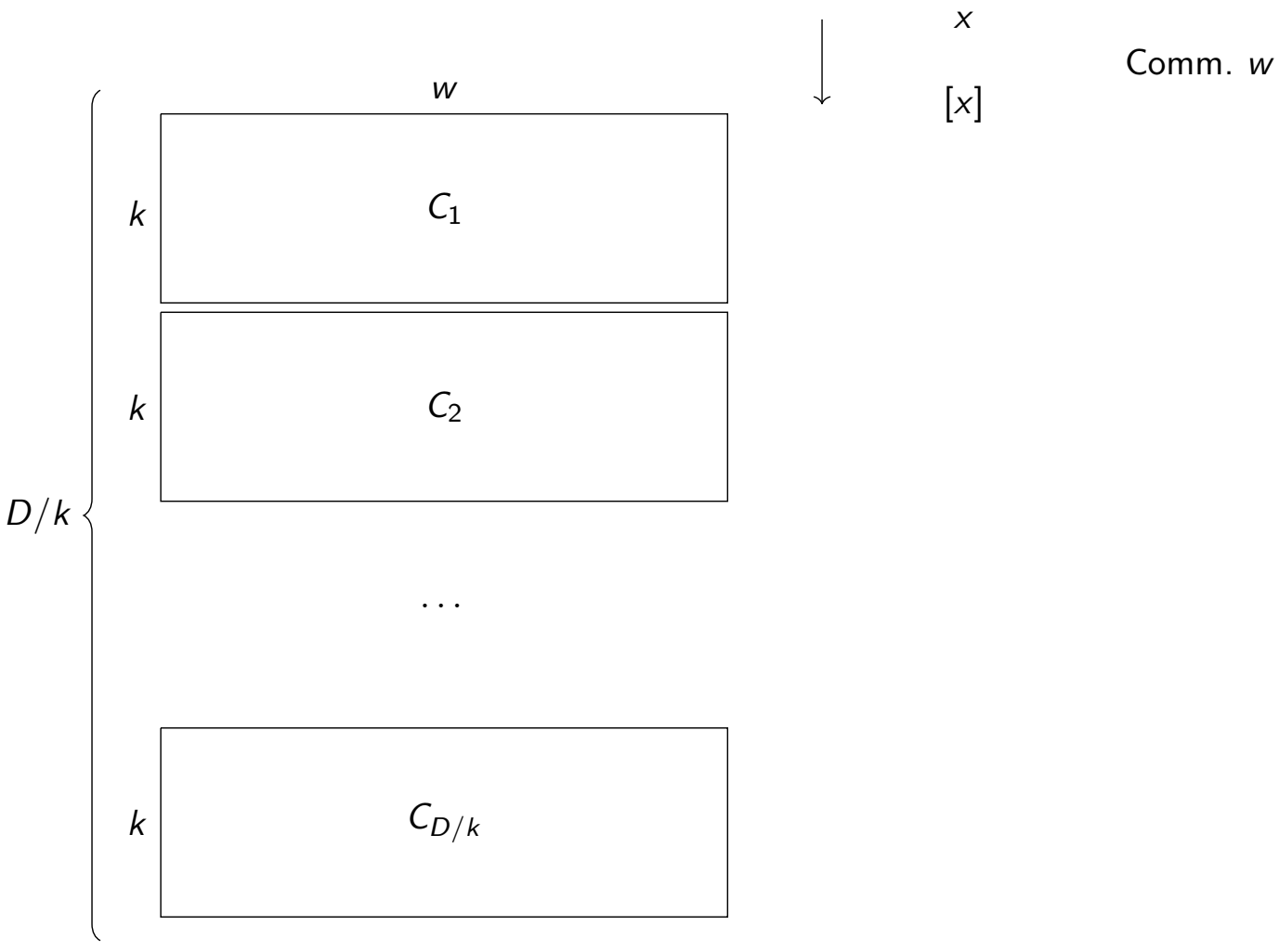

Correlated Randomness
DDH
DCR
FHE-based
HSS-based
LWE
NEW!
LPN
LWE

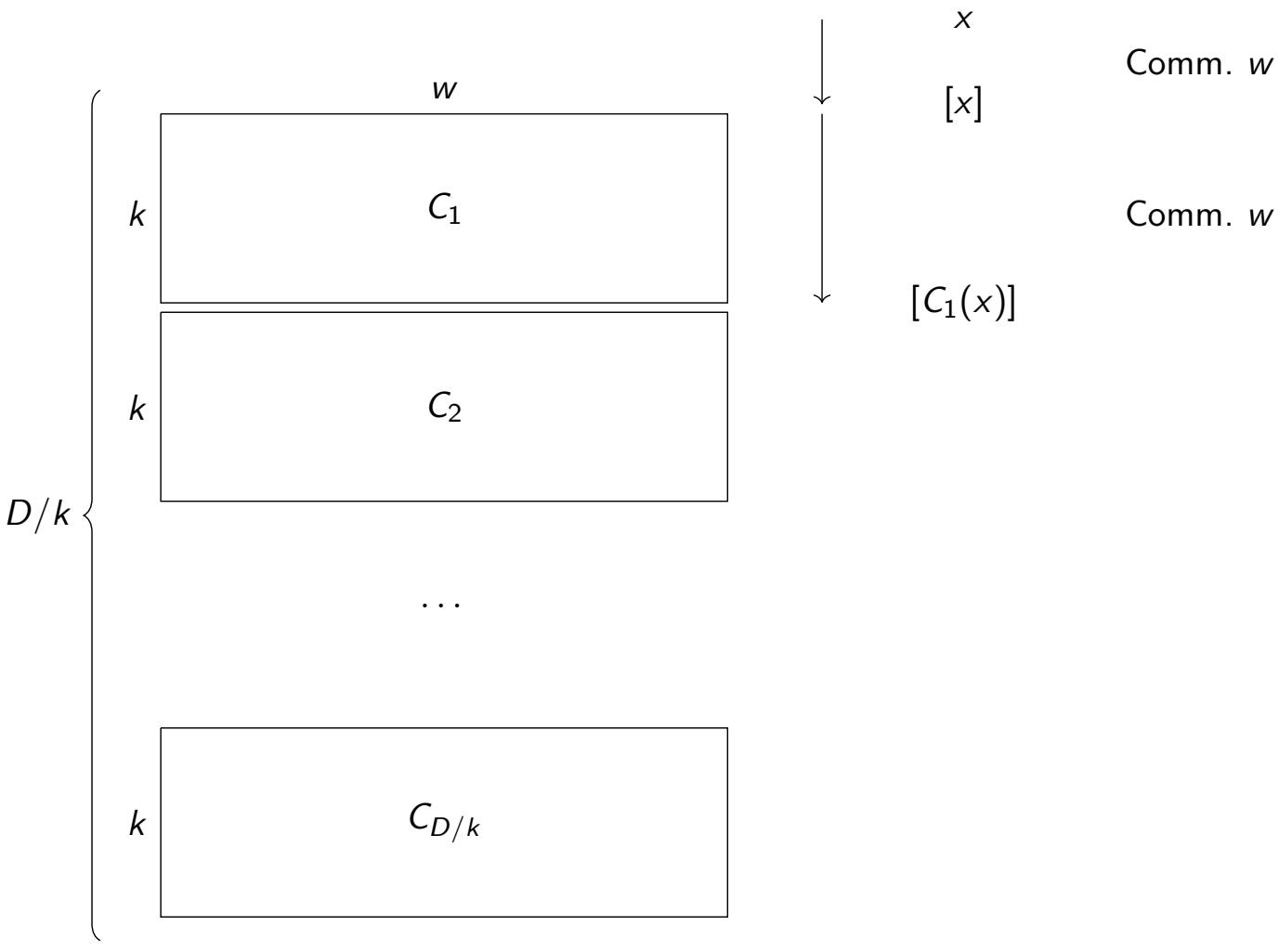
HSS-Based Sublinear 2-PC

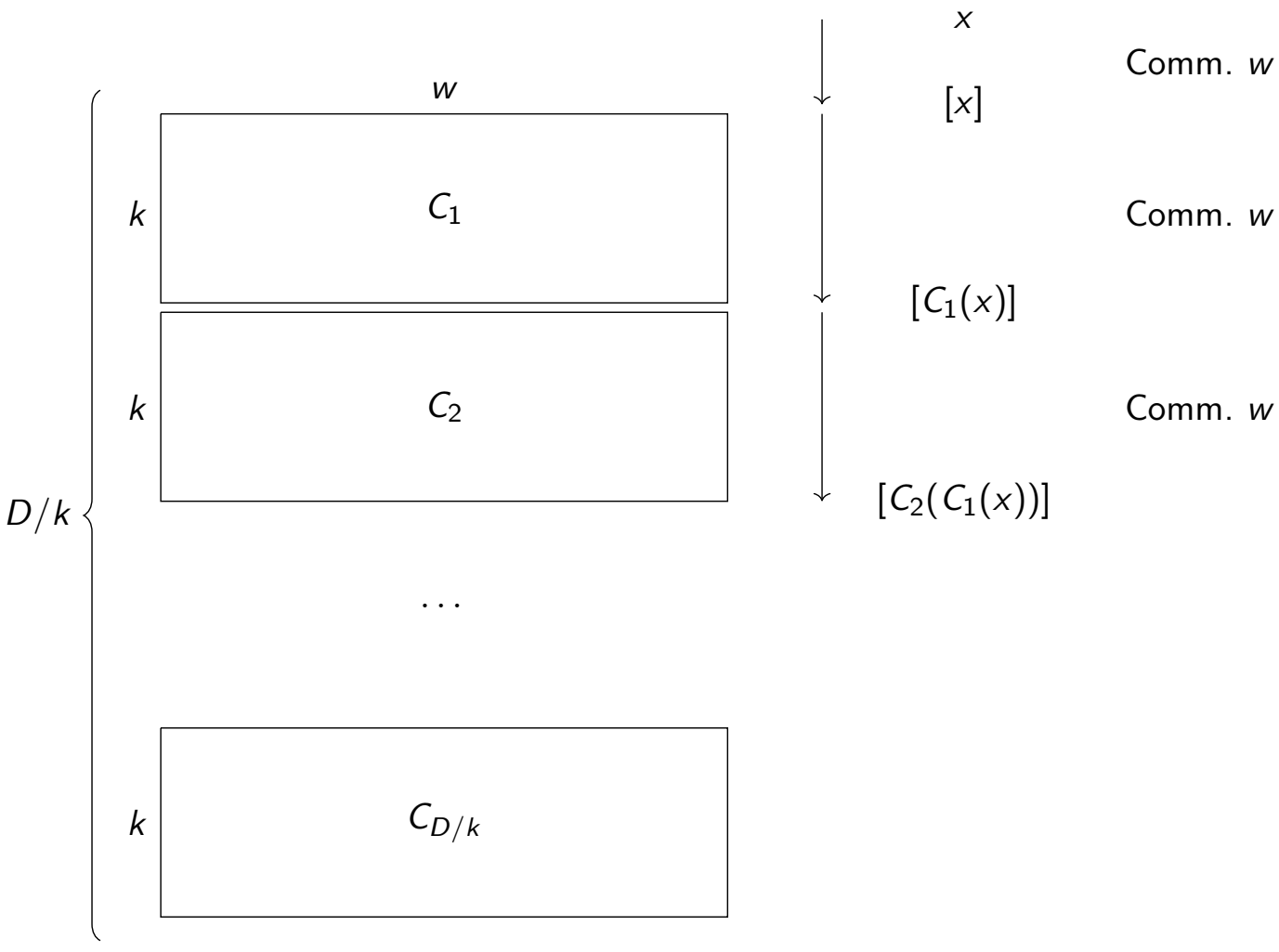

Inputs
First Layer
Second Layer
Gates
...
Final Layer
Outputs

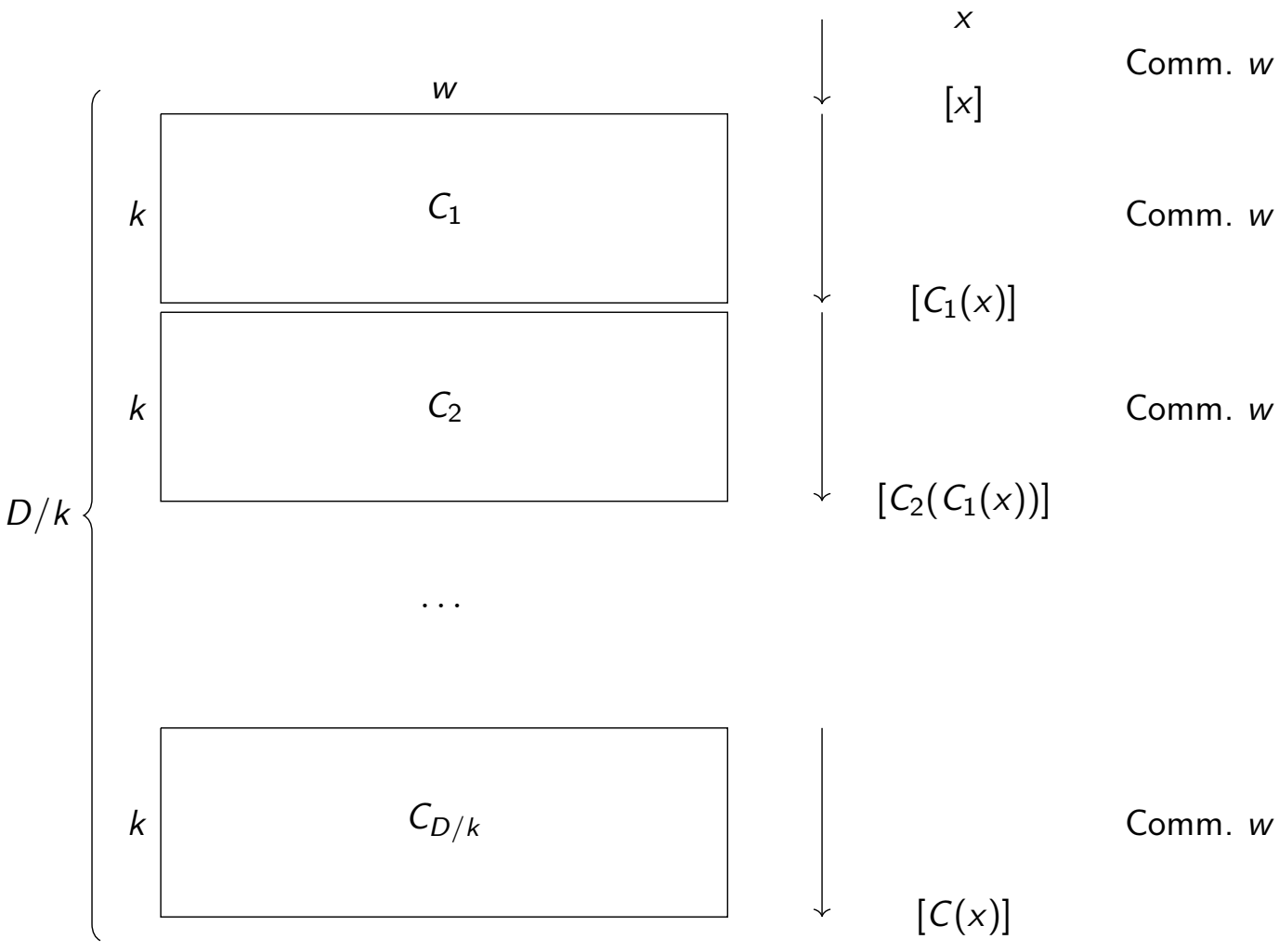

Inputs
w
D
C
Outputs

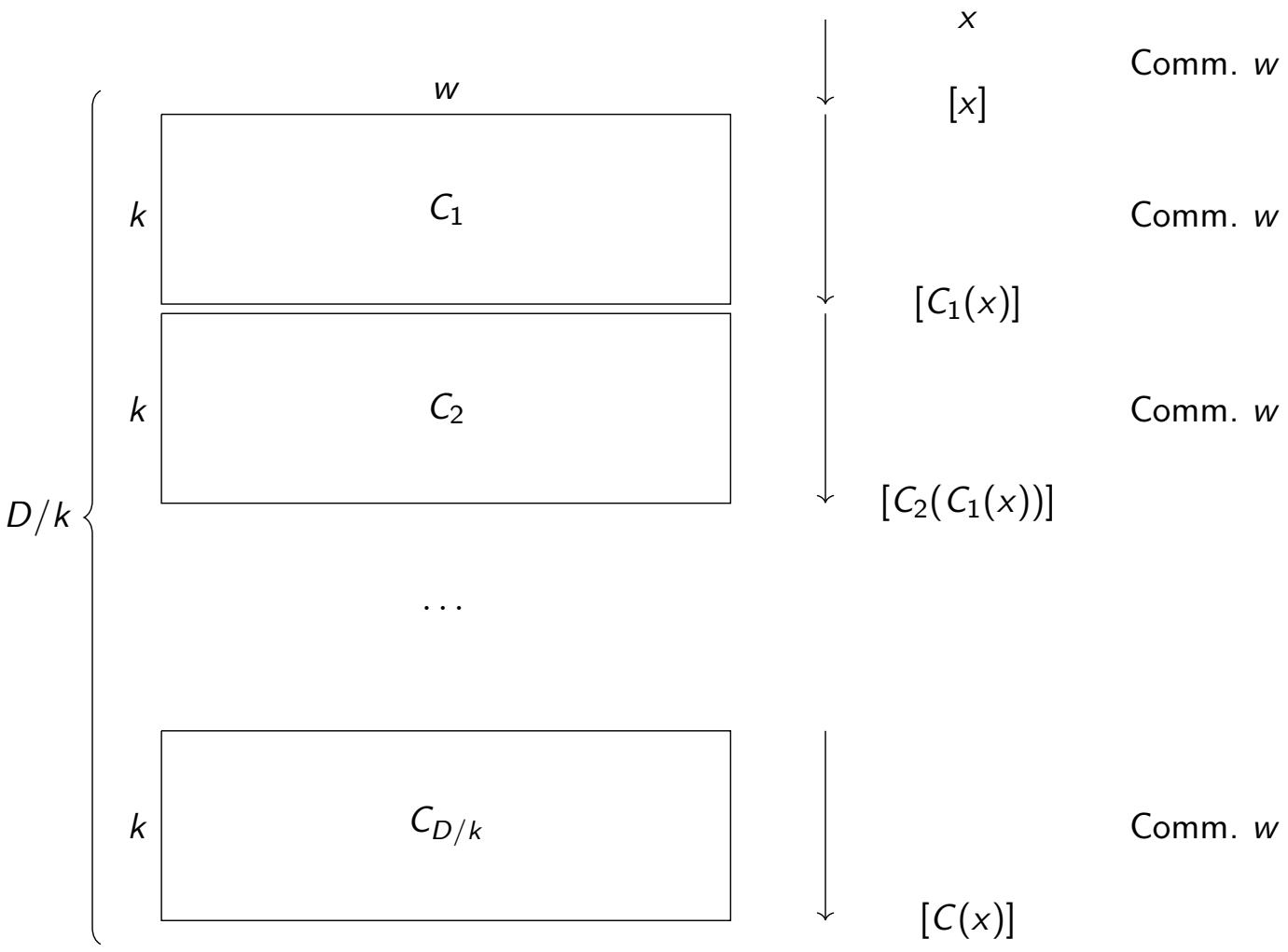

w
k
C_1
k
C_2
D/k
...
k
$C_{D/k}$


x
Comm. w
[x]
w
k
C_1
k
C_2
D/k
...
k
$C_{D/k}$


x
Comm. w
w
[x]
k
C1
Comm. w
[C1(x)]
k
C2
D/k
...
k
CD/k


x
Comm. w
w
[x]
k
C_1
Comm. w
$[C_1(x)]$
k
C_2
Comm. w
D/k
$[C_2(C_1(x))]$
...
k
$C_{D/k}$


x
Comm. w
w
[x]
k
C_1
Comm. w
$[C_1(x)]$
k
C_2
Comm. w
$[C_2(C_1(x))]$
D/k
...
k
$C_{D/k}$
Comm. w
$[C(x)]$

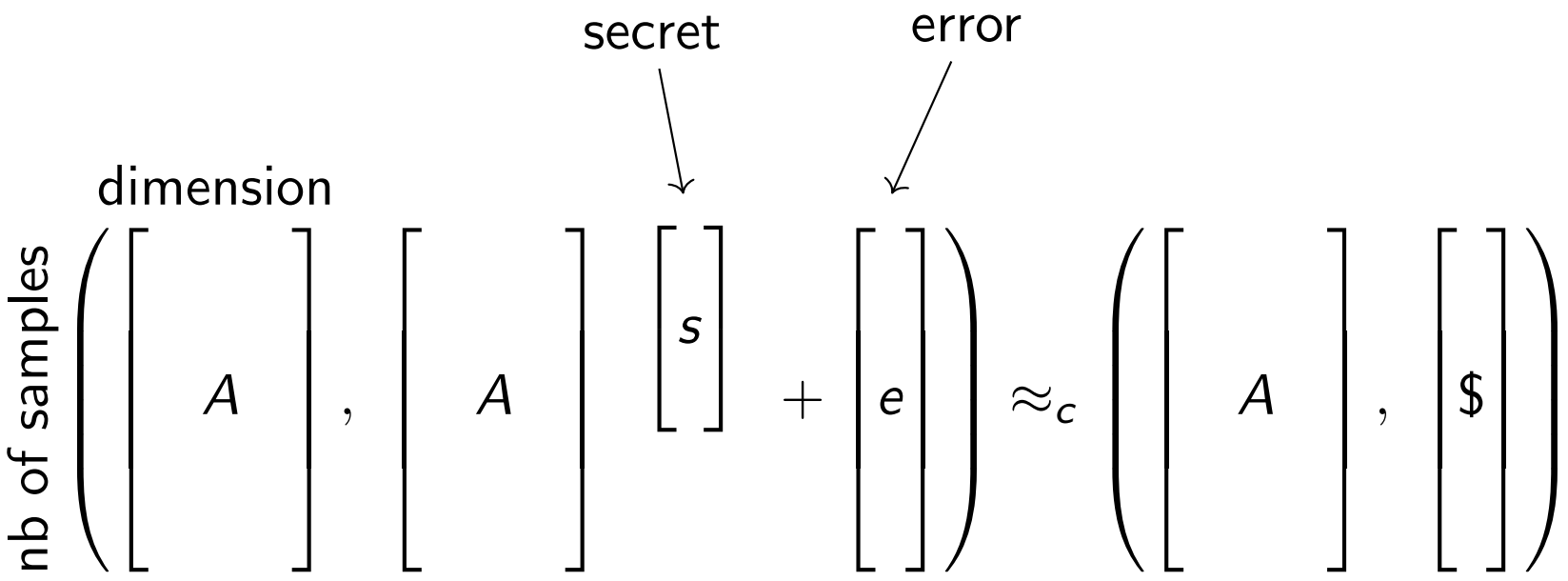


Total: $\frac{D}{k} \cdot w = |C|/k$

What is the flavour of LPN assumption?

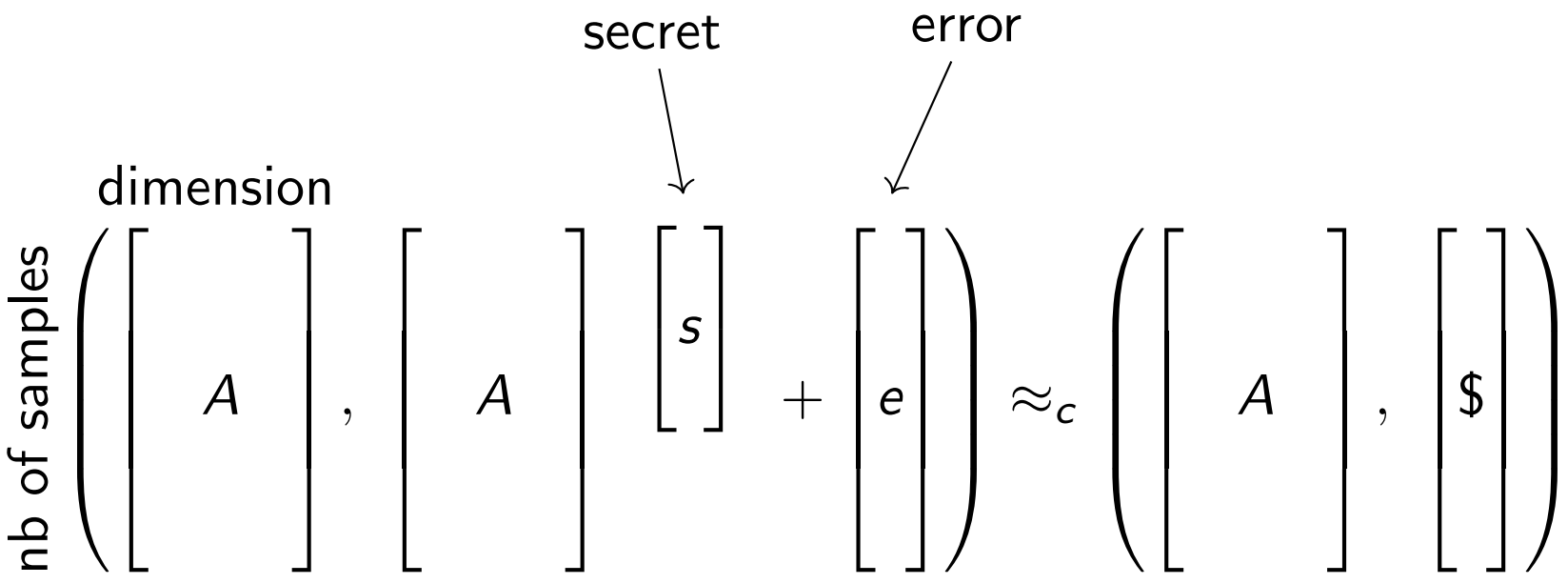
Quasi-Poly Learning Parity with Noise (LPN)

(Operations are over $\mathbb{F}_q$)



Quasi-Poly Learning Parity with Noise (LPN)

(Operations are over $\mathbb{F}_q$)

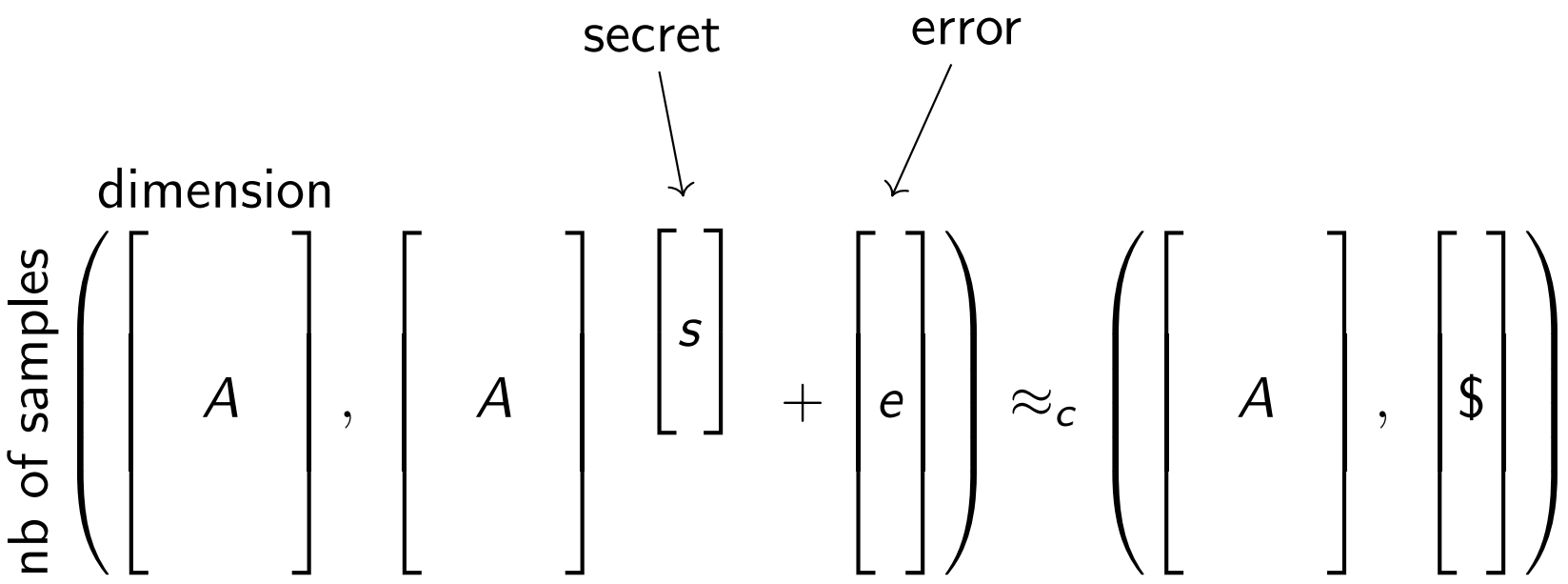


Noise Rate:

$$r = \frac{\mathsf{HW}(e)}{\text{nb of samples}}$$

Quasi-Poly Learning Parity with Noise (LPN)

(Operations are over $\mathbb{F}_q$)

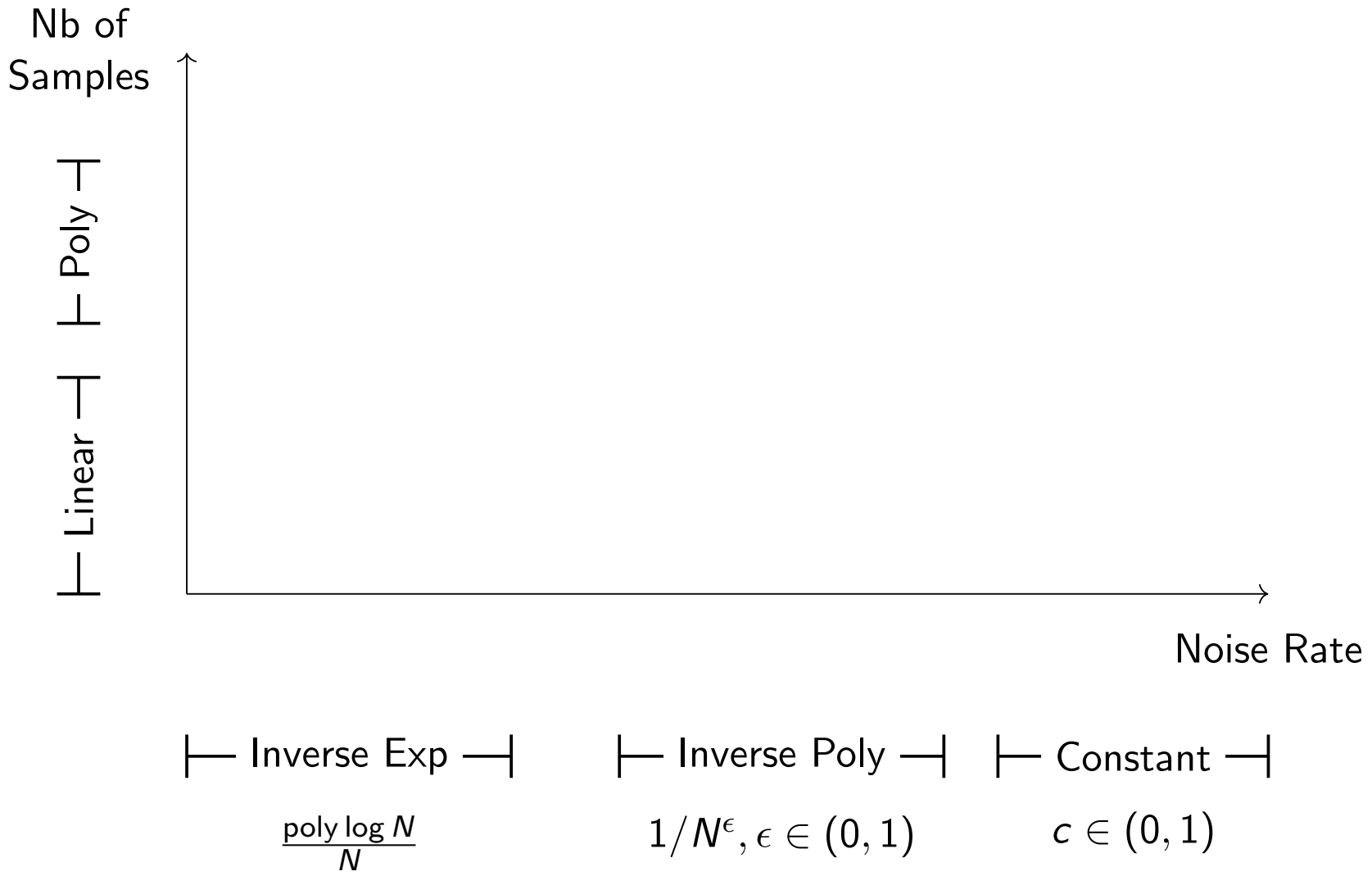


Noise Rate:

$$r = \frac{\mathsf{HW}(e)}{\text{nb of samples}}$$

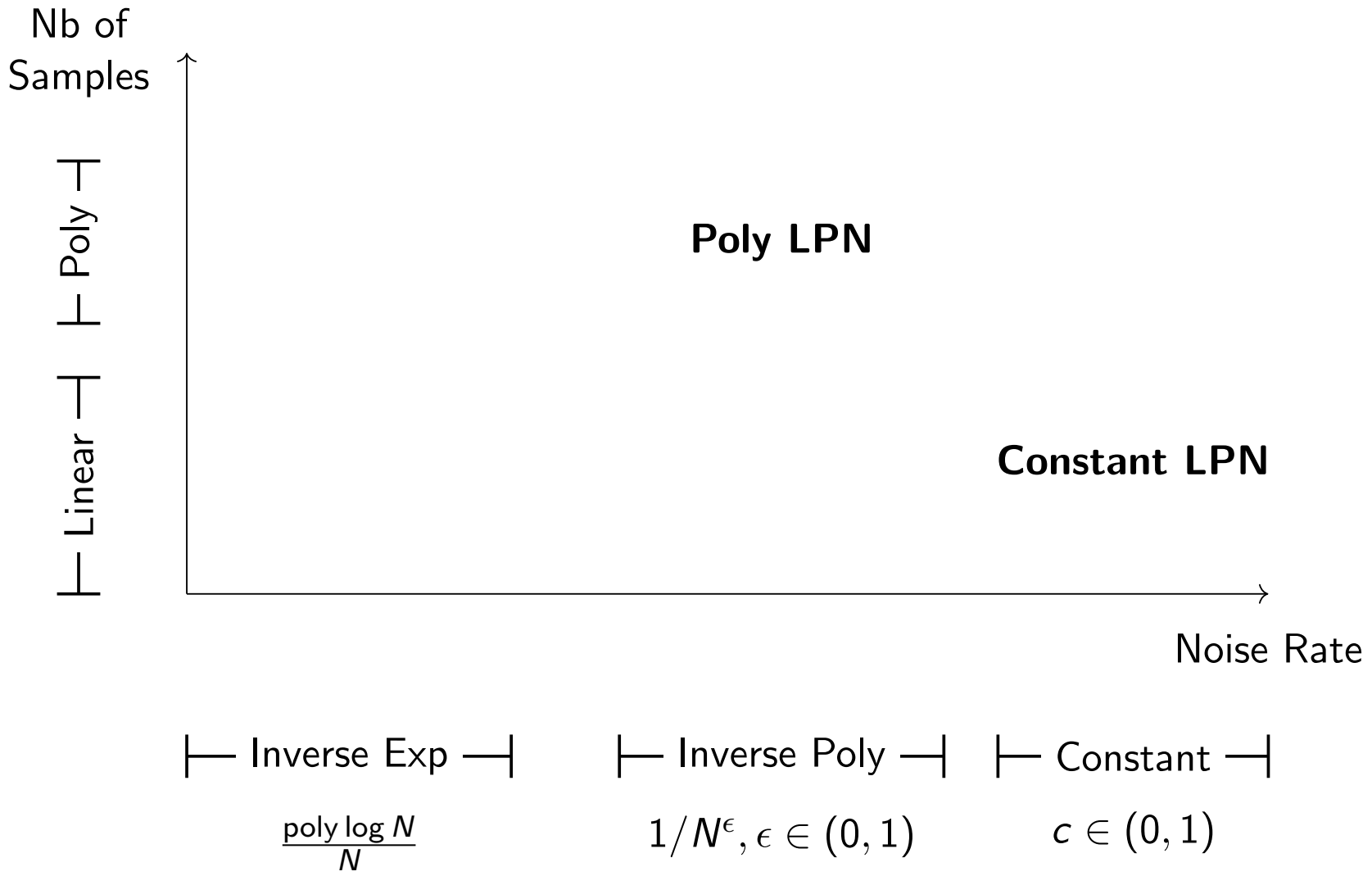
Adv. Runtime:	$\lambda^{2\log\lambda}$
Dimension:	$N = \lambda^{\log\lambda}$
Nb of Samples:	$2N$
Noise Rate:	λ/N

Inspired from Benny Applebaum's amazing talk at CISPA Summer School 2021
https://cispa.de/video/2021/summer-school/01_BennyApplebaum_cut.mp4



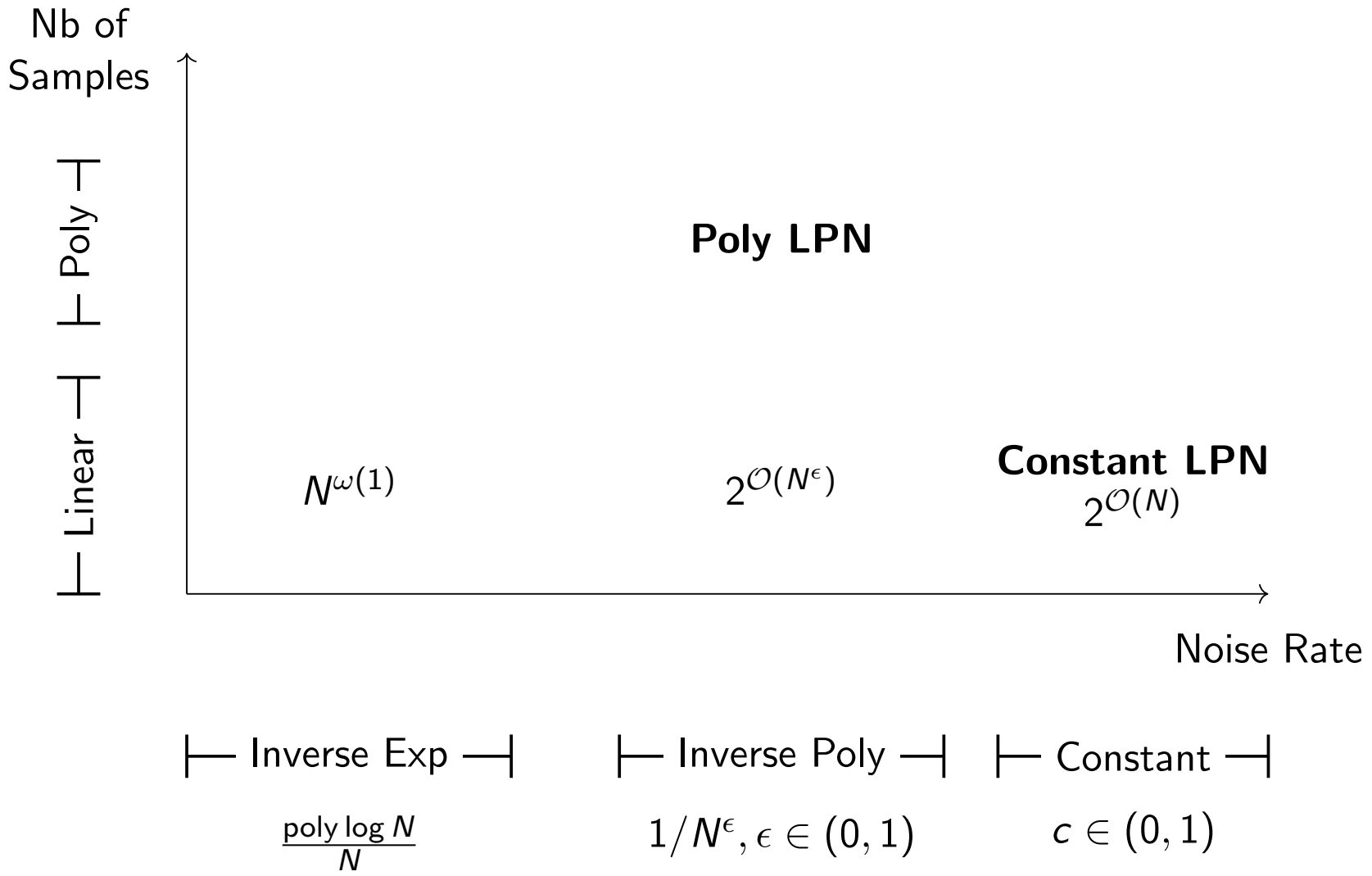
N: Dimension

Inspired from Benny Applebaum's amazing talk at CISPA Summer School 2021
https://cispa.de/video/2021/summer-school/01_BennyApplebaum_cut.mp4



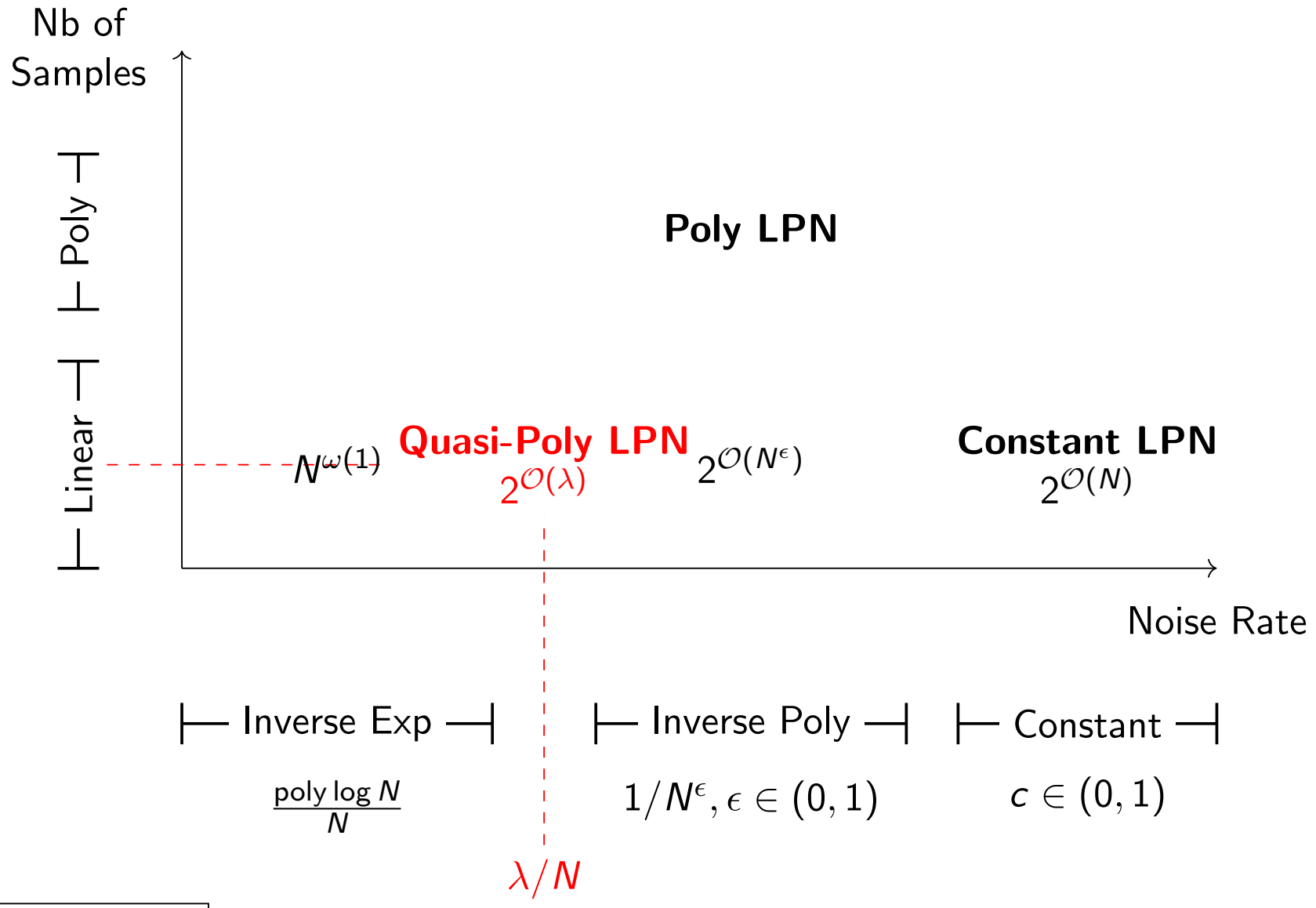
N: Dimension

Inspired from Benny Applebaum's amazing talk at CISPA Summer School 2021
https://cispa.de/video/2021/summer-school/01_BennyApplebaum_cut.mp4



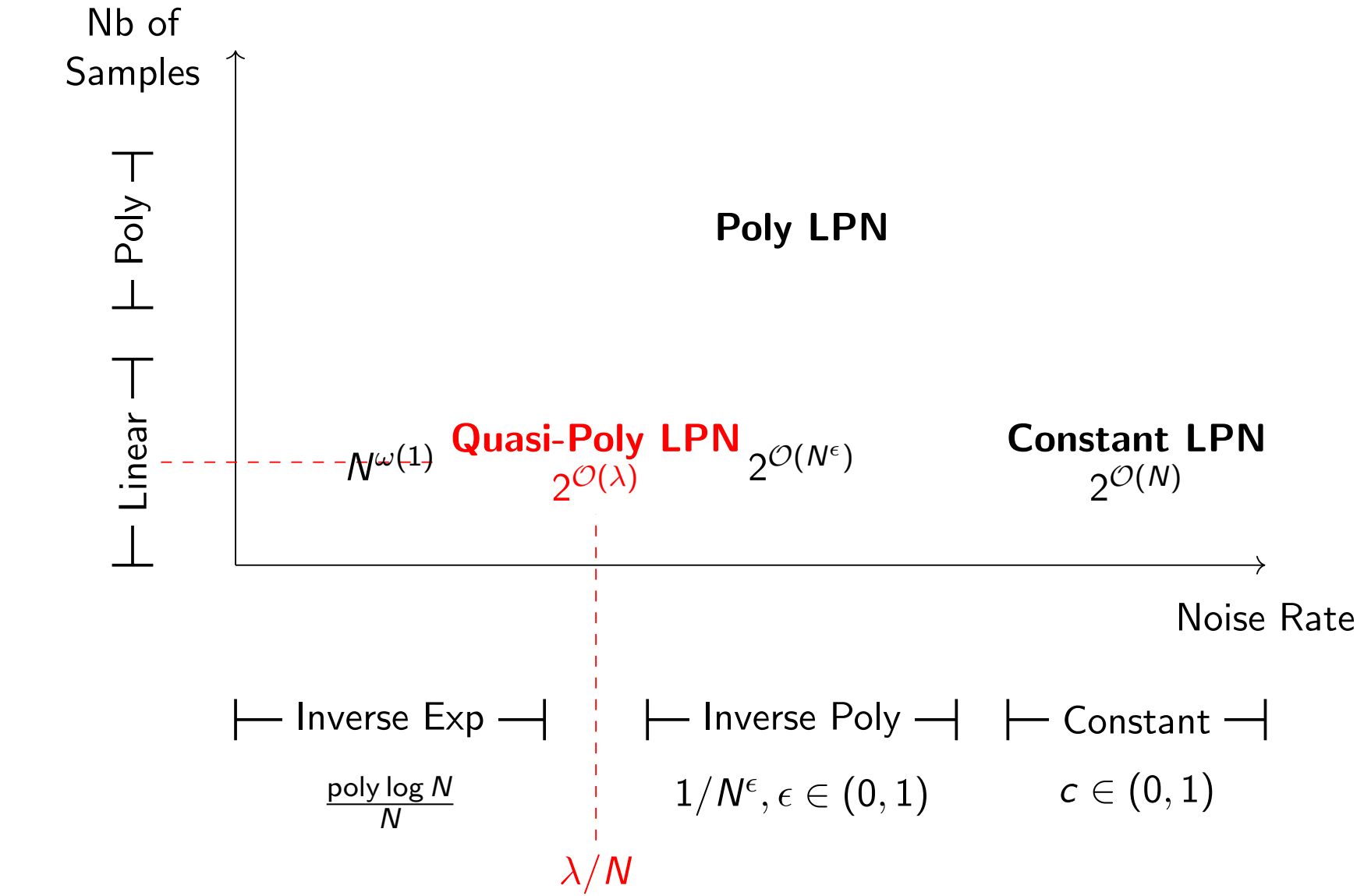
N: Dimension

Inspired from Benny Applebaum's amazing talk at CISPA Summer School 2021
https://cispa.de/video/2021/summer-school/01_BennyApplebaum_cut.mp4



N: Dimension

Inspired from Benny Applebaum's amazing talk at CISPA Summer School 2021
https://cispa.de/video/2021/summer-school/01_BennyApplebaum_cut.mp4



N: Dimension

We only require security against $2^{\log^2 \lambda}$:)

A Tutorial On Naming a Paper for Optimal Metrics

Breaking the Circuit-Size Barrier for Secure Computation under Quasi-Polynomial LPN

Couteau, M. (Eurocrypt'21)

Breaking the Circuit-Size Barrier for Secure Computation under Quasi-Polynomial LPN

Couteau, M. (Eurocrypt'21)

Breaking the Circuit-Size Barrier for Secure Computation under DDH

Boyle, Gilboa, Ishai (Best Paper Crypto'16)

Breaking the Circuit-Size Barrier for Secure Computation under Quasi-Polynomial LPN

Couteau, M. (Eurocrypt'21)

Breaking the Circuit-Size Barrier for Secure Computation under DDH

Boyle, Gilboa, Ishai (Best Paper Crypto'16)

$$\text{Normalised Citation Count} = \frac{\text{Number of Citations}}{\text{Age of Paper}}$$

Breaking the Circuit-Size Barrier for Secure Computation under Quasi-Polynomial LPN

Couteau, M. (Eurocrypt'21)

Breaking the Circuit-Size Barrier for Secure Computation under DDH

Boyle, Gilboa, Ishai (Best Paper Crypto'16)

$$\text{Normalised Citation Count} = \frac{\text{Number of Citations}}{\text{Age of Paper}}$$

TopNotch › Crypto Papers › Normalized Top-100 Ranking

Normalized Top-100 Crypto Papers

This webpage is an attempt to assemble a ranking of top-cited papers from the area of cryptography. The ranking has been created based on citations of papers published at top cryptography conferences. More details are available here.

Absolute citations are not necessarily a good indicator for the impact of a paper, as the number of citations usually grows with the age of a paper. The following list shows an alternative ranking, where the citations are normalized by the age of each paper.

93 cites??

Top 100 papers normalized by age ⌄

1 Geoffroy Couteau and Pierre Meyer:
Breaking the Circuit Size Barrier for Secure Computation Under Quasi-Polynomial LPN.
Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2021
93 cites at Google Scholar | 3691% above average of year | Last visited: Sep-2021 | Paper: DOI

2 Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam D. Smith:
Calibrating Noise to Sensitivity in Private Data Analysis.
Theory of Cryptography Conference (TCC), 2006
5248 cites at Google Scholar | 3144% above average of year | Last visited: Sep-2021 | Paper: DOI

3 Paul C. Kocher, Joshua Jaffe, and Benjamin Jun:
Differential Power Analysis.
International Cryptology Conference (CRYPTO), 1999
9271 cites at Google Scholar | 3040% above average of year | Last visited: Sep-2021 | Paper: DOI

3694%
over avg. . . ?

Source: `https://www.sec.cs.tu-bs.de/~konrieck/topnotch/crypto_ntop100.html`

Thank you!

ia.cr/2021/943