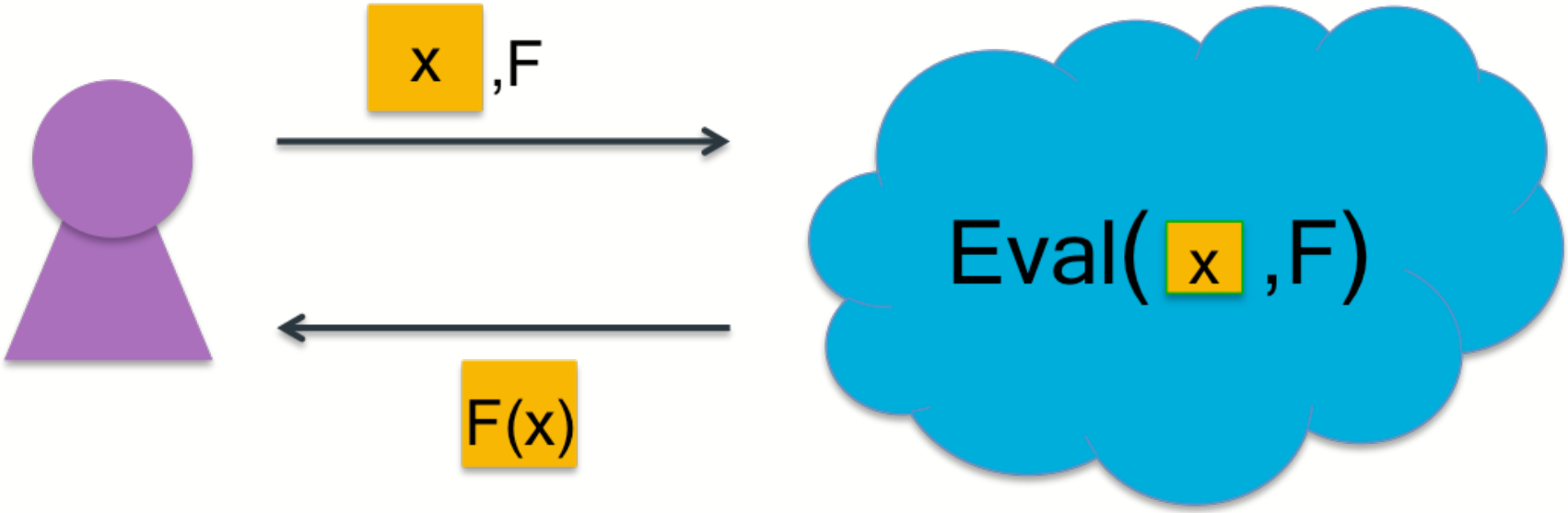
On the precision loss in approximate homomorphic encryption

Selected Areas in Cryptography (SAC)
Fredericton, New Brunswick | August 2023

Anamaria Costache, Benjamin R. Curtis, Erin Hales, Sean Murphy, Tabitha Ogilvie, Rachel Player

NTNU
ZAMA
ROYAL HOLLOWAY UNIVERSITY OF LONDON

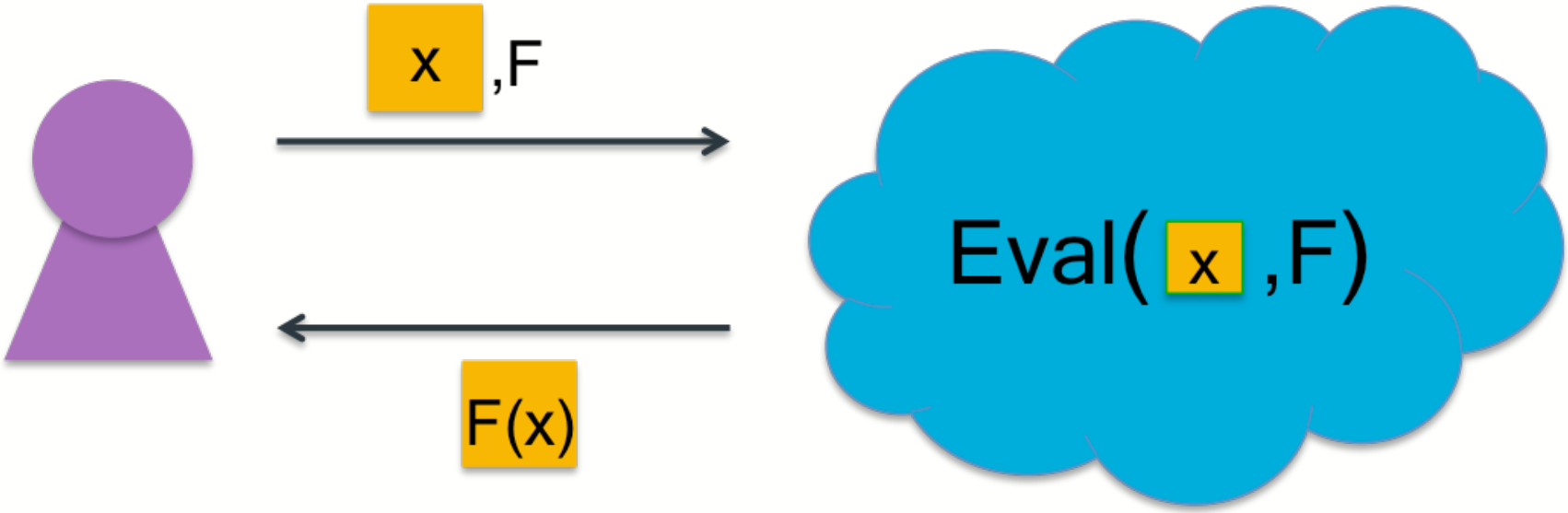
Homomorphic encryption (HE)



x Encryption of x

F(x) Encryption of F(x)

Homomorphic encryption (HE)



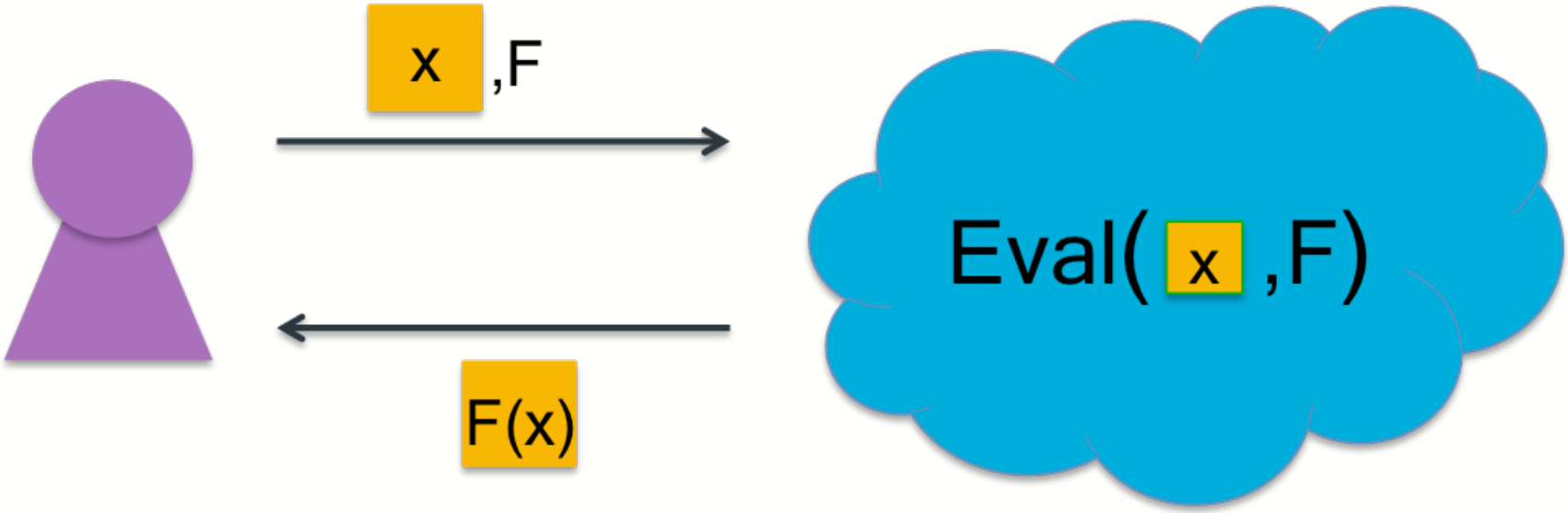
x Encryption of x

F(x) Encryption of F(x)

Somewhat homomorphic encryption:

- F is a polynomial of at most some fixed degree

Homomorphic encryption (HE)



x Encryption of x

F(x) Encryption of F(x)

Somewhat homomorphic encryption:

- F is a polynomial of at most some fixed degree

Approximate homomorphic encryption:

- Decrypted result is approximately equal to F(x)

What is noise and why is it important?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- All ciphertexts in HE schemes have inherent noise
- Noise grows during homomorphic operations
- If noise too large, decryption will fail
- Understanding noise growth is essential to choose good parameters
- Requiring large parameters is a major challenge in practical HE

The CKKS approximate HE scheme

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- For applications that can tolerate approximation, e.g. PPML
- Natively supports real or complex-valued messages
  - Encoding mechanism into polynomial plaintext space
- Widely implemented
- Extensively optimised, with RNS variants
- Similar to BGV/BFV schemes, but
  - Noise introduced in encoding and homomorphic operations
  - Need to track scale parameter Δ

J. H. Cheon, A. Kim, M. Kim, Y. Song. Homomorphic encryption for arithmetic of approximate numbers. Asiacrypt 2017.
J. H. Cheon, K. Han, A. Kim, M. Kim, Y. Song. A full RNS variant of approximate homomorphic encryption. SAC 2018.

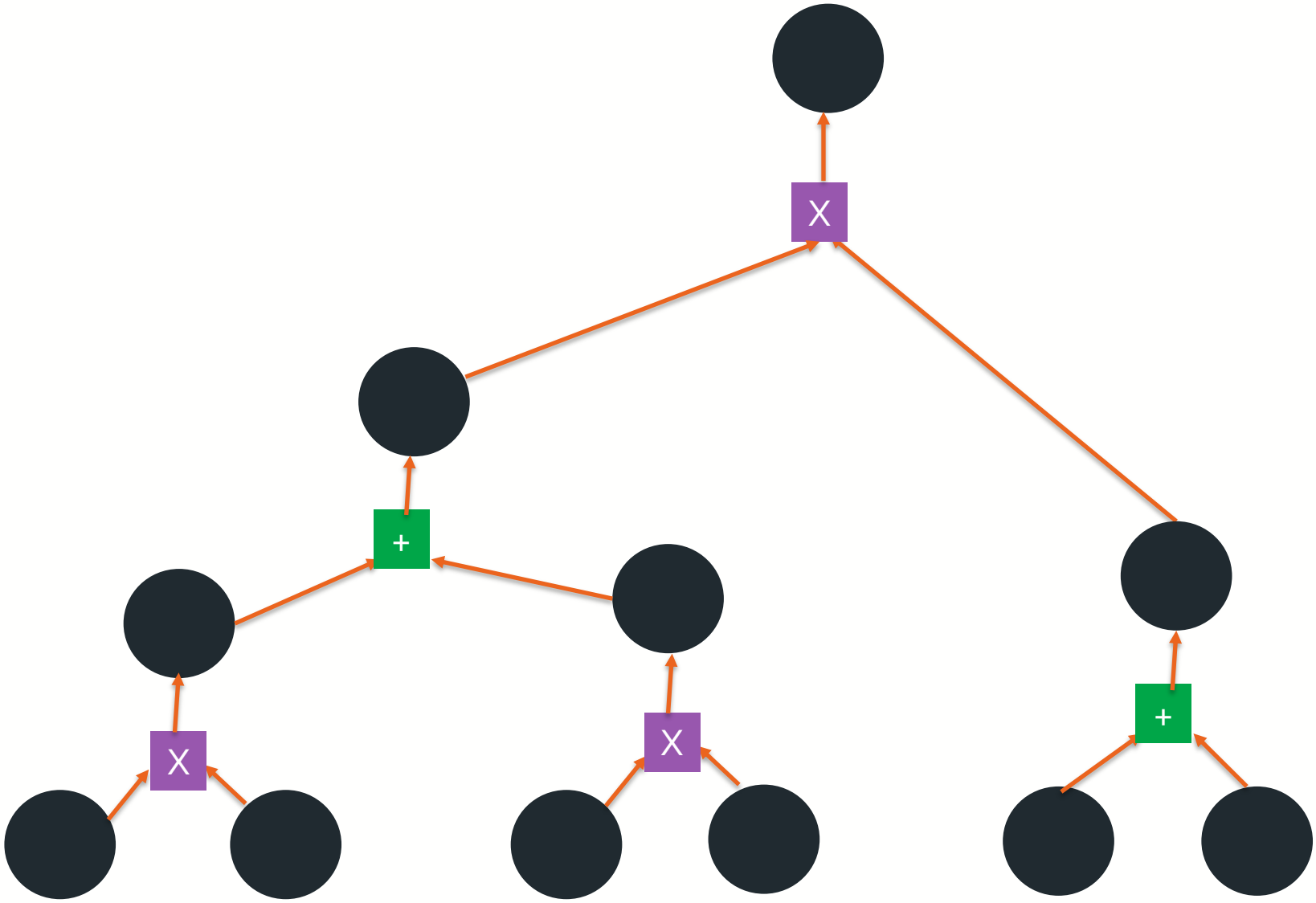
Contributions of this work

ROYAL HOLLOWAY UNIVERSITY OF LONDON

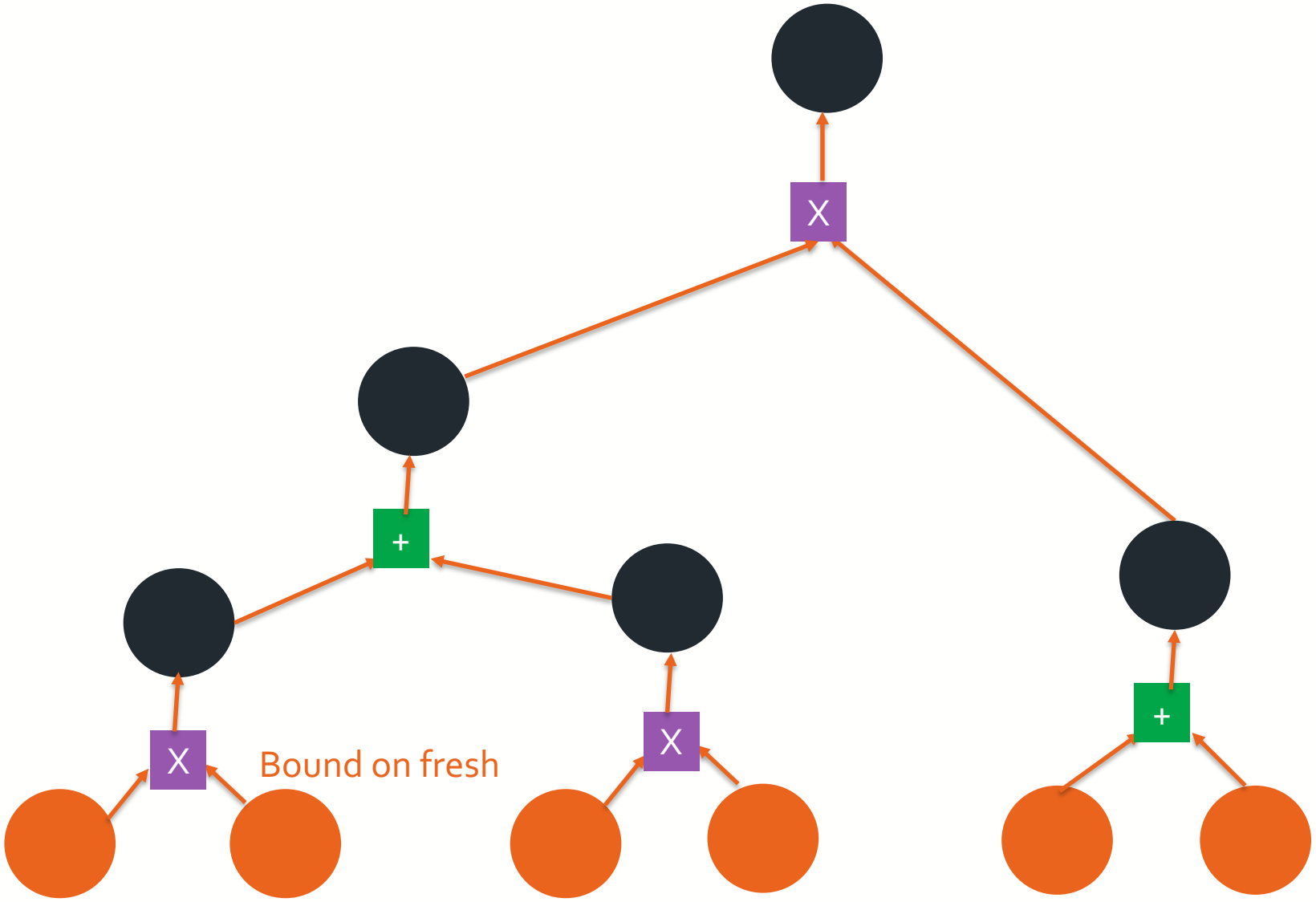
- **New tighter bound on precision loss from encoding**
  - Proof that bound is best possible
- **First average-case noise analysis for CKKS**
  - For Textbook CKKS and RNS-CKKS
- **Evaluation compared to prior worst-case noise analyses and observed noise in implementations**
  - For HEAAN v1.0 and FullRNS-HEAAN

HEAAN v1.0: https://github.com/snucrypto/HEAAN/releases/tag/1.0
FullRNS-HEAAN: https://github.com/KyoohyungHan/FullRNS-HEAAN

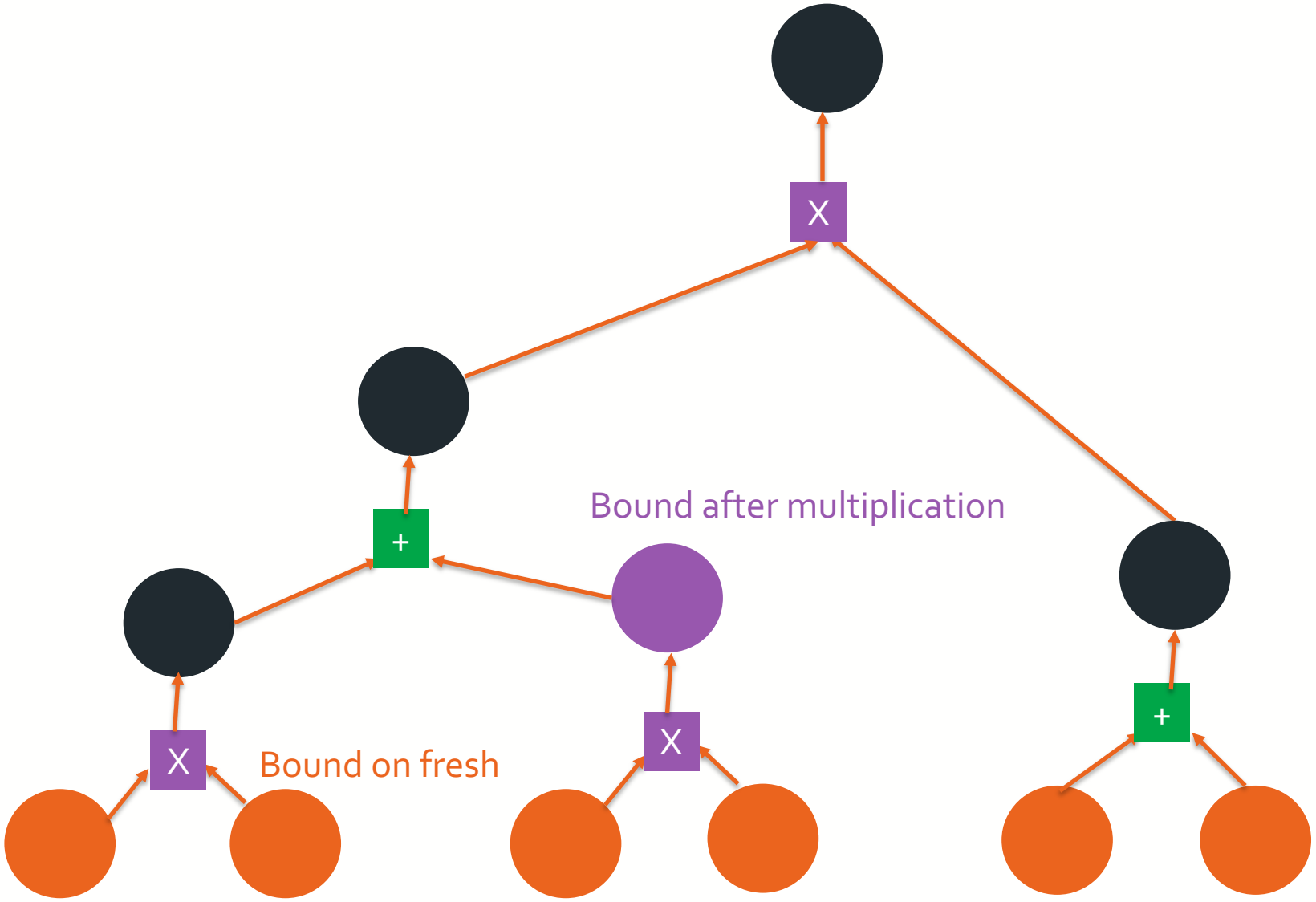
Worst-case approach for noise analysis



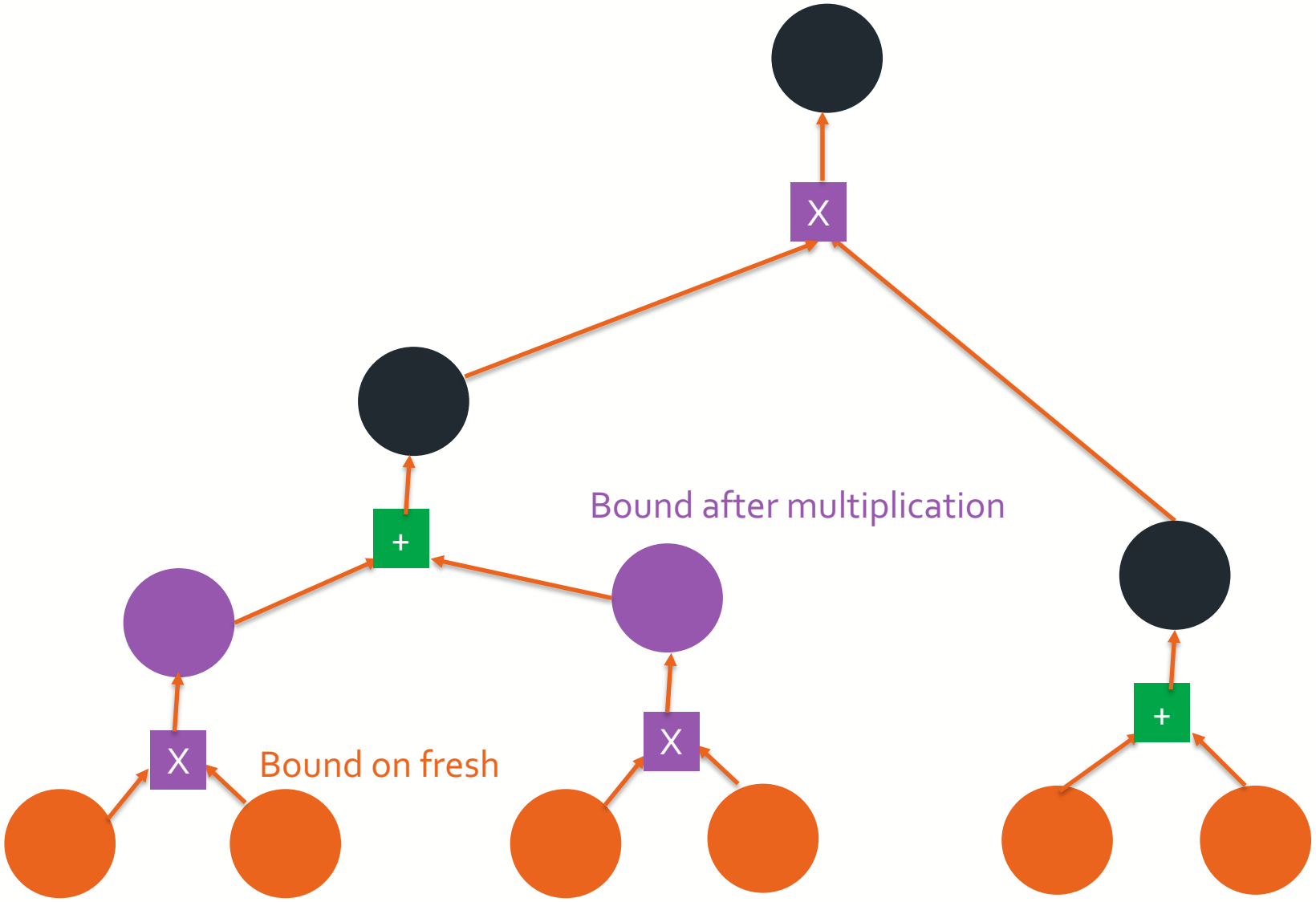
Worst-case approach for noise analysis



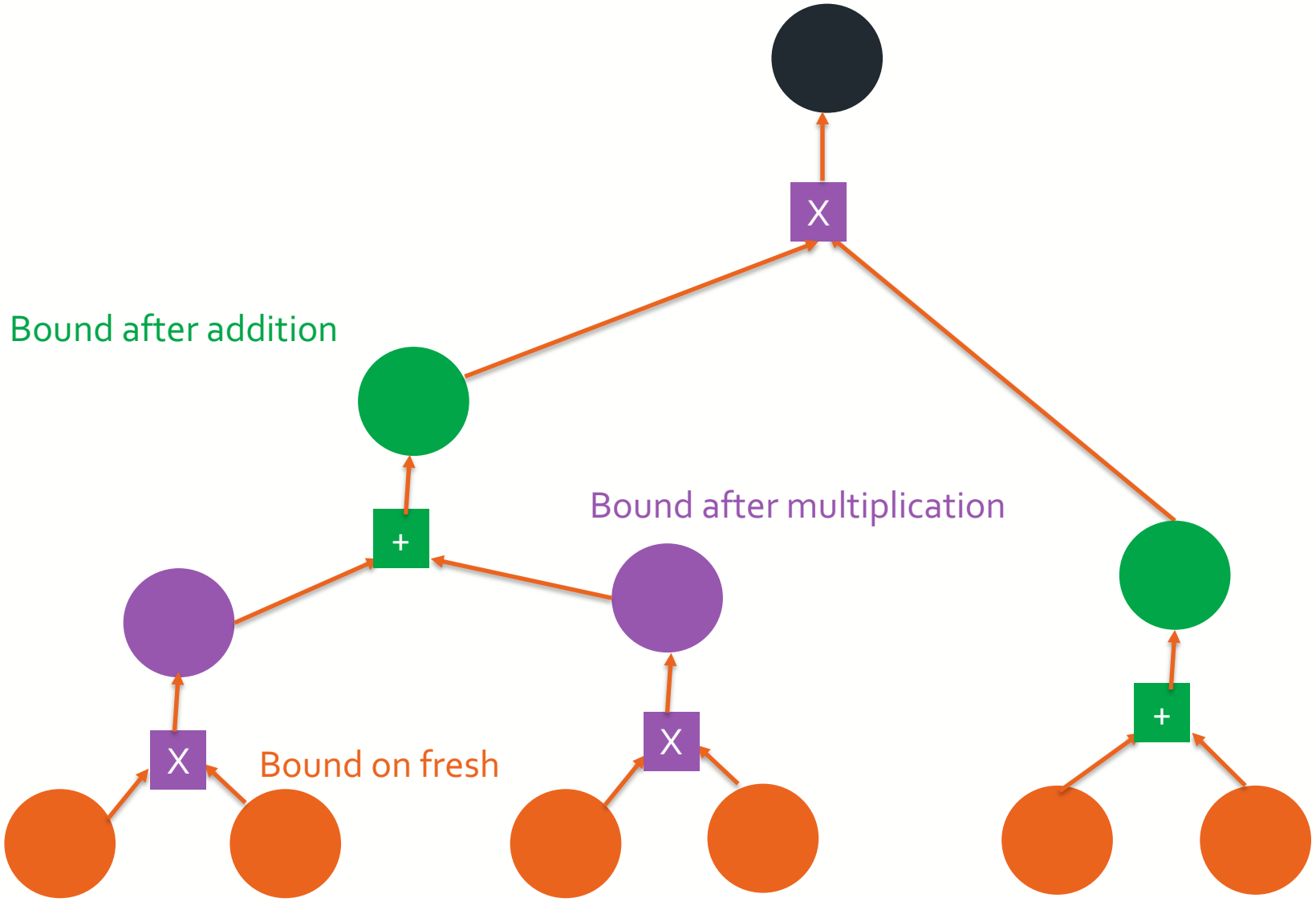
Worst-case approach for noise analysis



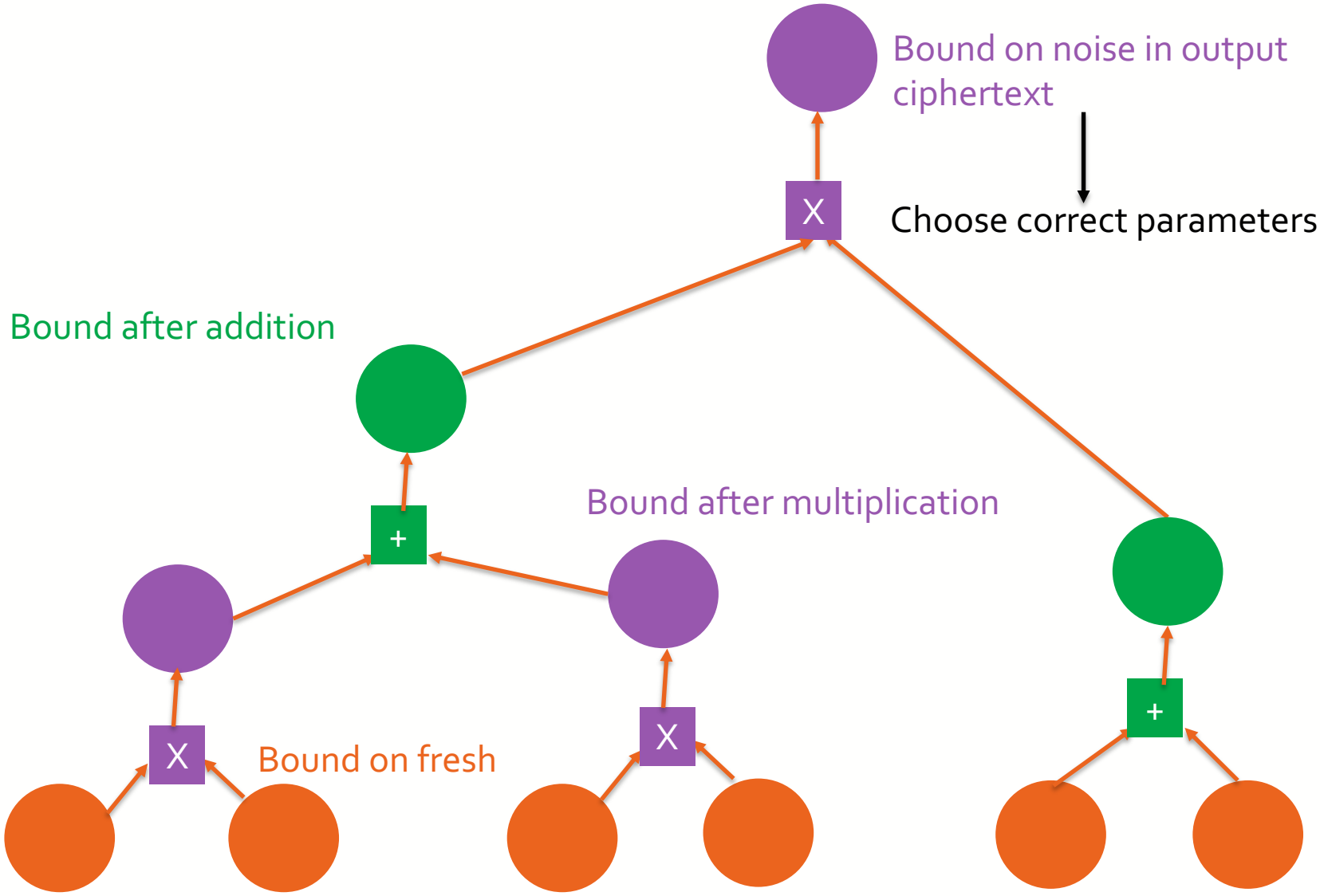
Worst-case approach for noise analysis



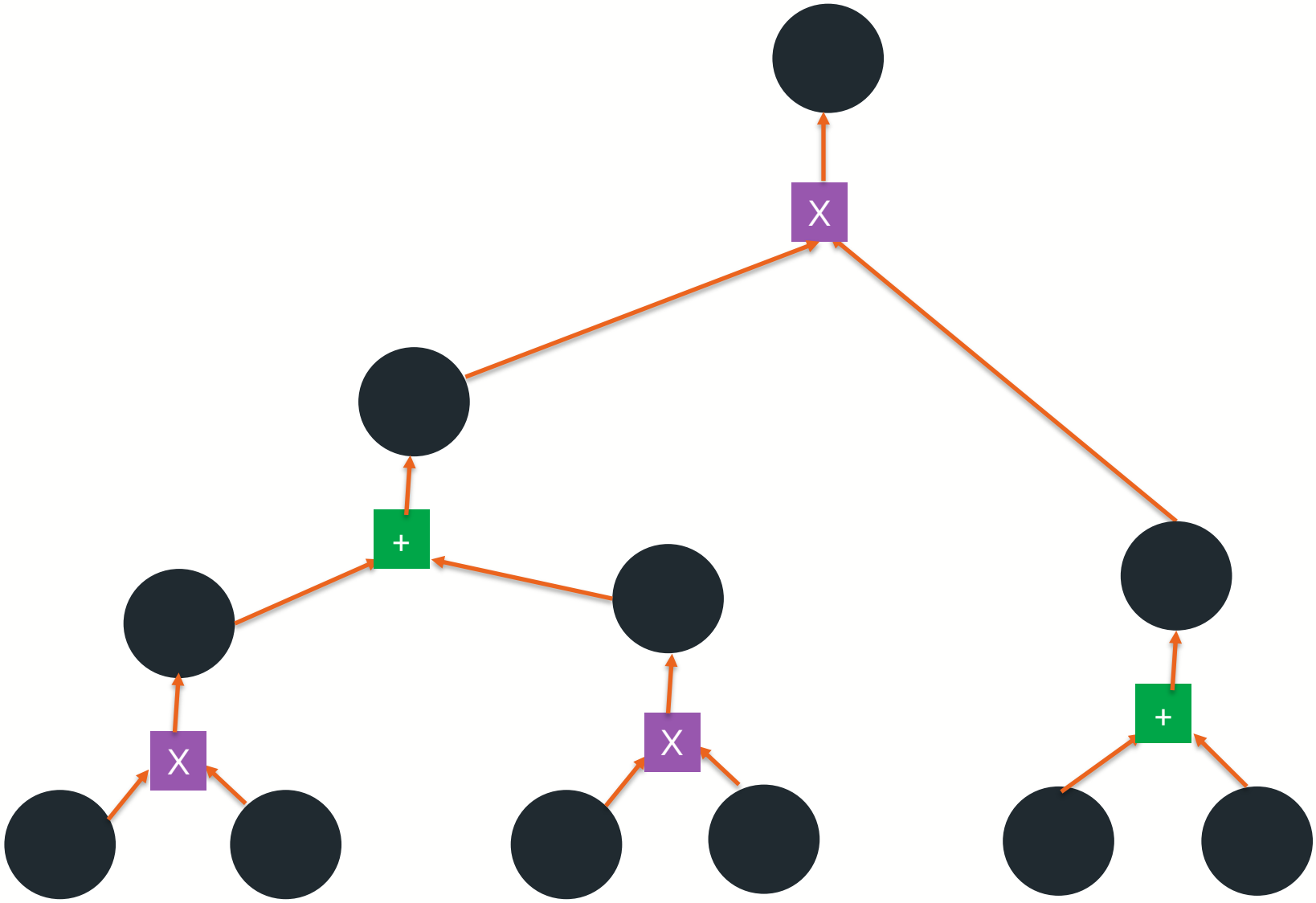
Worst-case approach for noise analysis



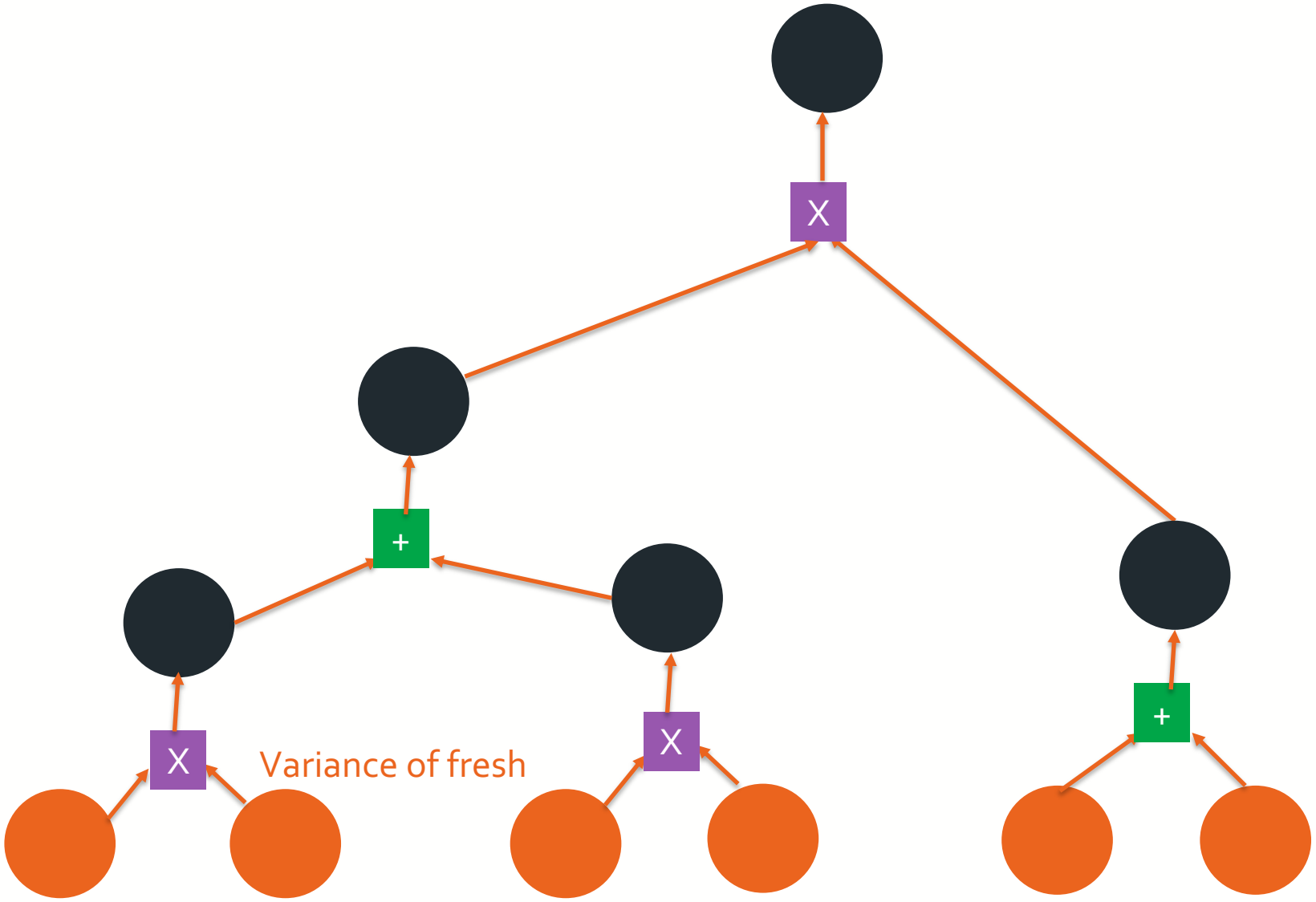
Worst-case approach for noise analysis



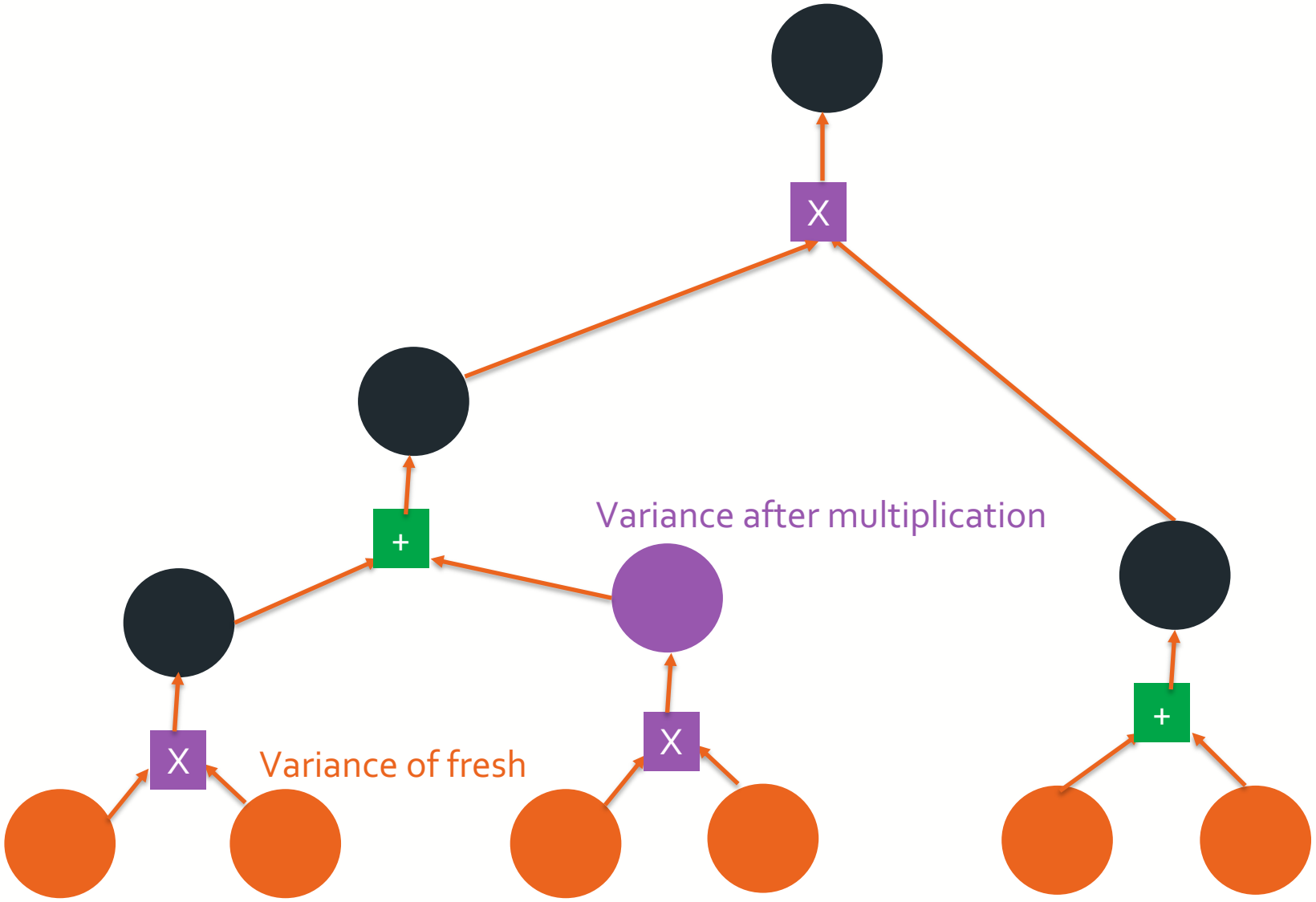
Average-case approach for noise analysis



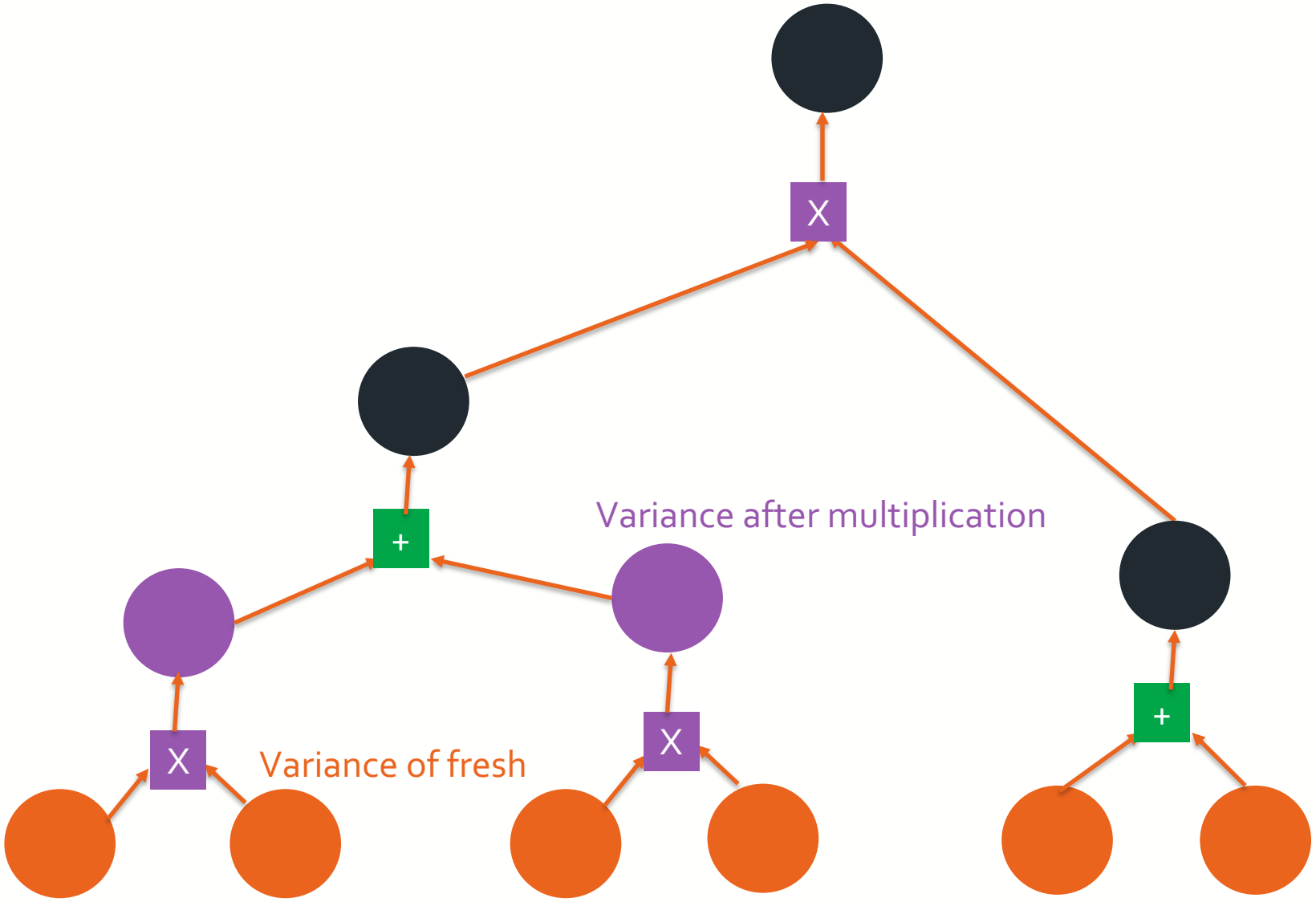
Average-case approach for noise analysis



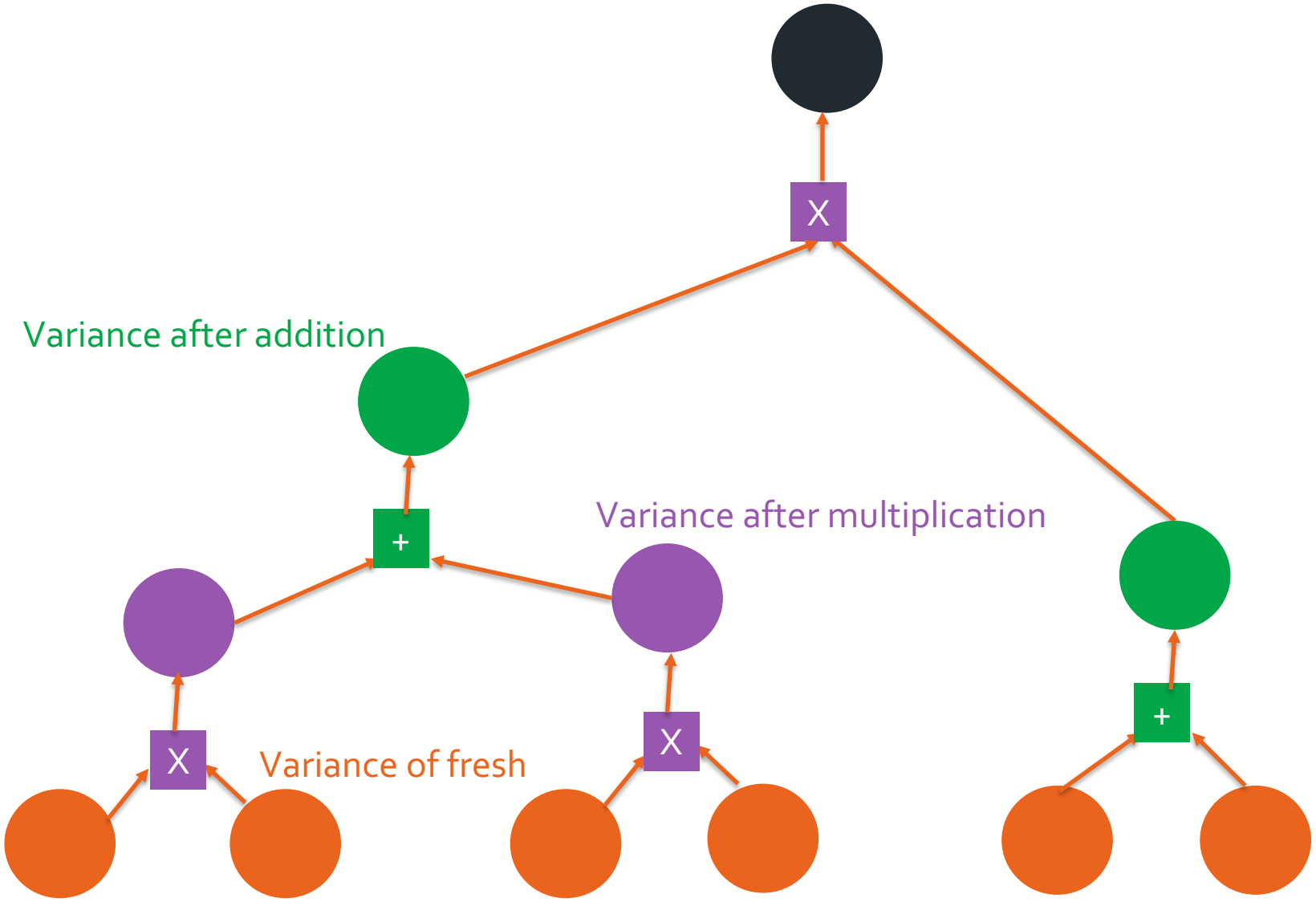
Average-case approach for noise analysis



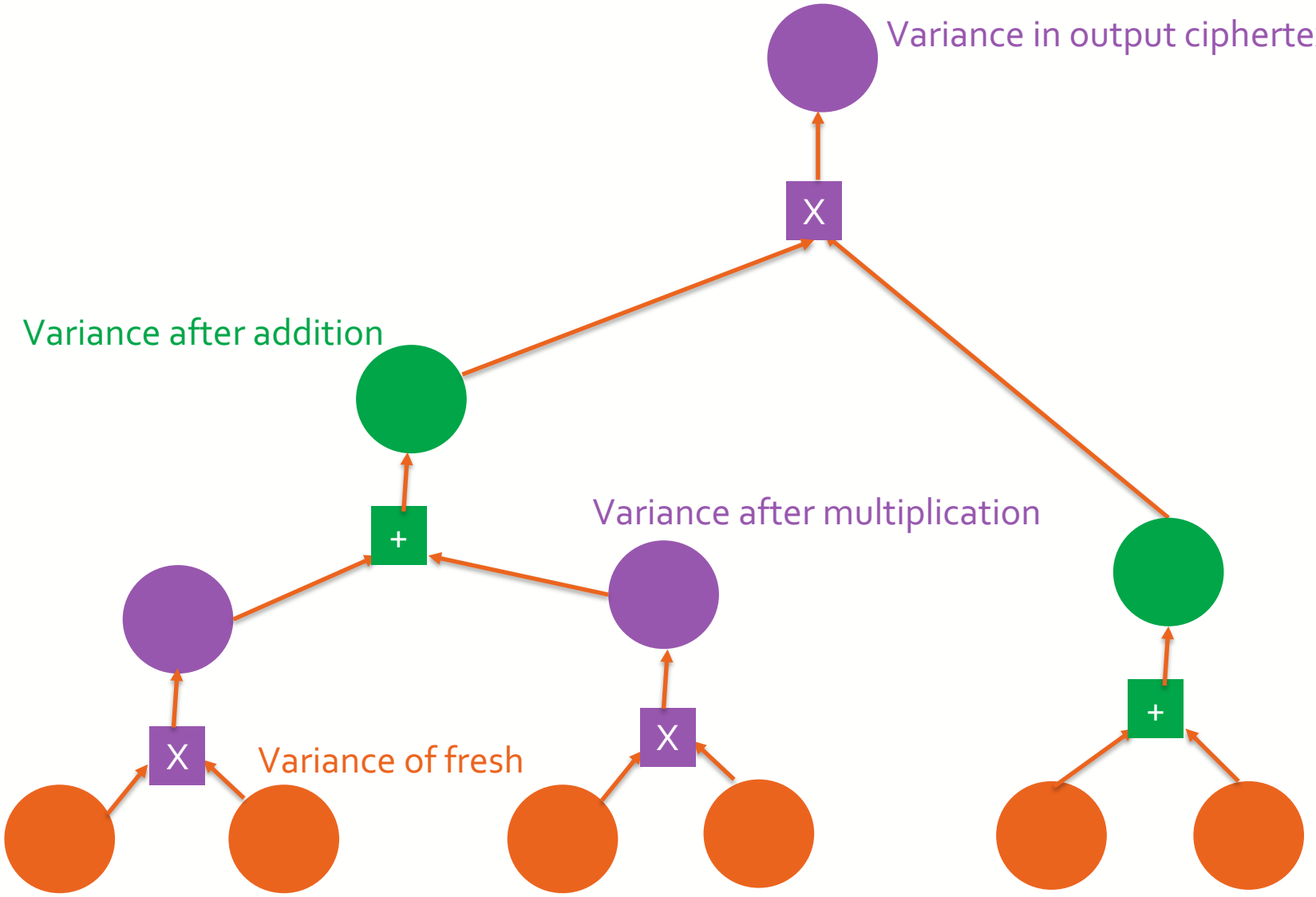
Average-case approach for noise analysis



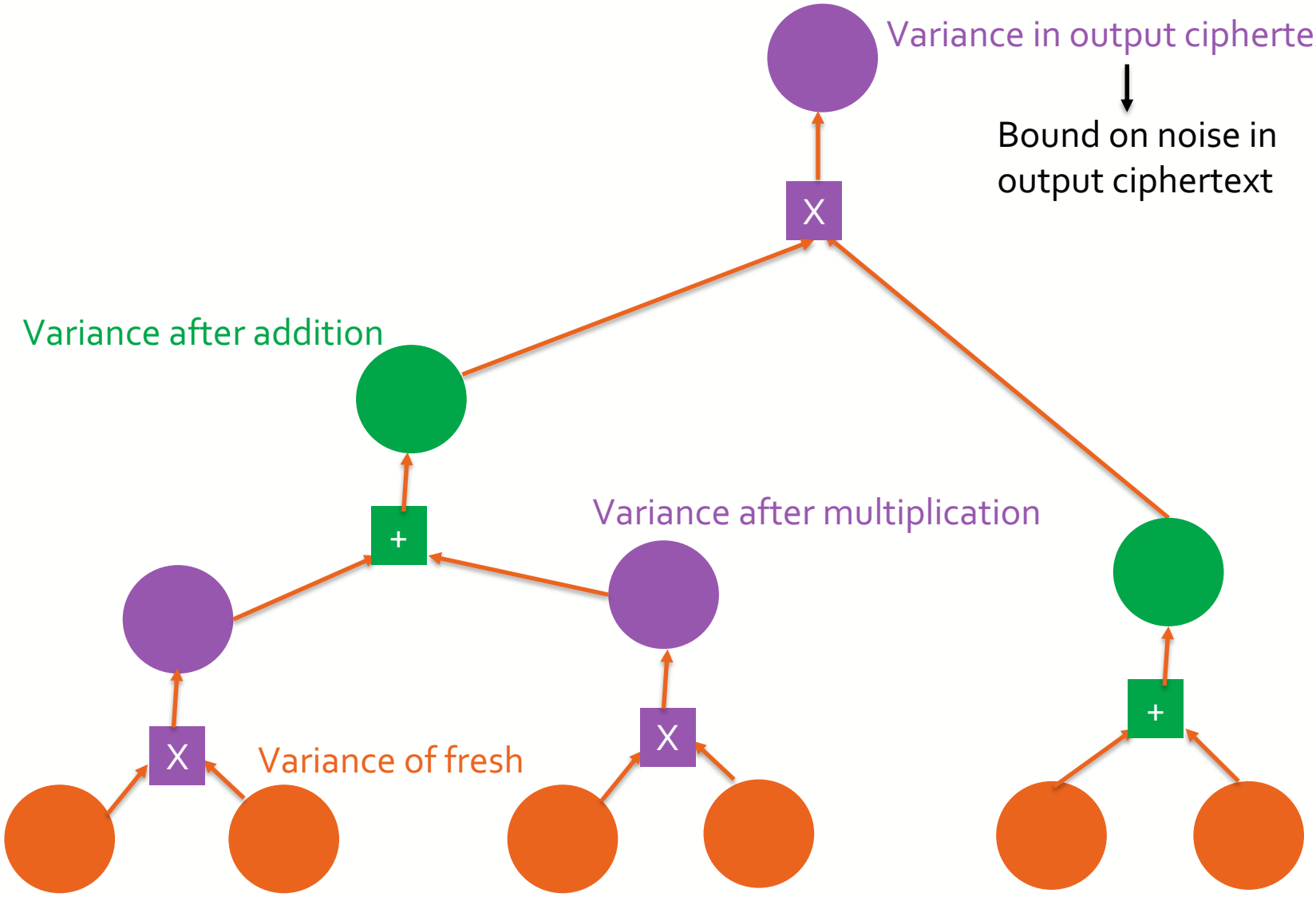
Average-case approach for noise analysis



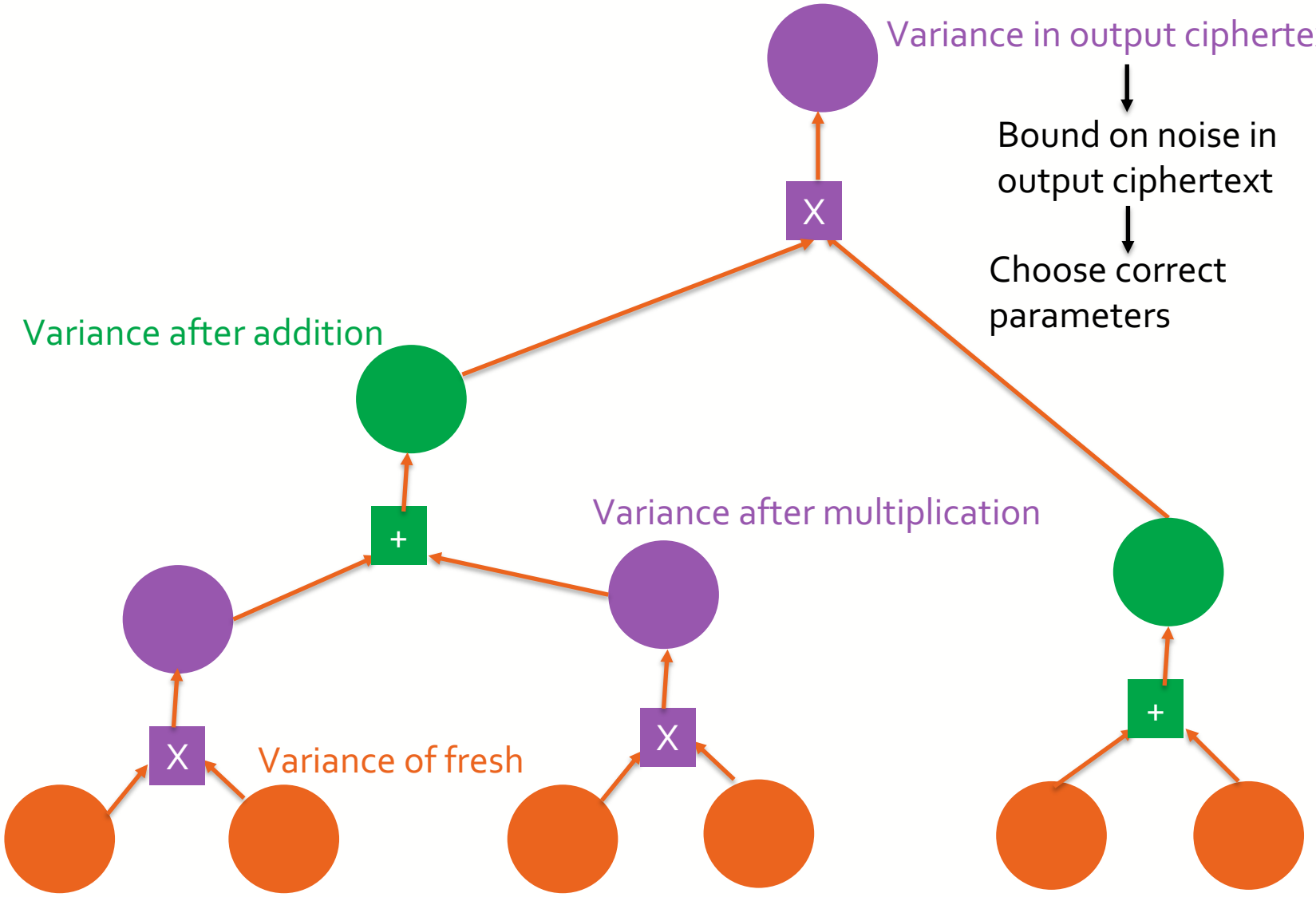
Average-case approach for noise analysis



Average-case approach for noise analysis



Average-case approach for noise analysis



Prior work: TFHE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- TFHE is a HE scheme with an average-case noise analysis
- Noise is heuristically modelled as subgaussian
- Heuristic was experimentally verified for gate bootstrapping
- Every TFHE operation can be achieved by gate bootstrapping on a linear combination of ciphertexts
- By linearity, all noises can be modelled in this way

Can the same approach work for CKKS?

I. Chillotti, N. Gama, M. Georgieva, M. Izabachène. TFHE: fast fully homomorphic encryption over the torus. J. of Cryptology, 2019.

An average-case approach for CKKS?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- CKKS mult noise is the product of two input noises
- The product of two Gaussians is not Gaussian
- This suggests an average-case approach may be tricky

An average-case approach for CKKS?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- CKKS mult noise is the product of two input noises
- The product of two Gaussians is not Gaussian
- This suggests an average-case approach may be tricky

A Central Limit Approach

- Coefficient of v_{mult} is a sum of n terms of the form $v_{1,i} \cdot v_{2,j}$
- Suggests that Central Limit Theorem may be applicable!

CLT approach for CKKS

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Suppose $v_1 \sim \mathcal{N}(\boldsymbol{\mu_1}, \rho_1^2 I_N)$ and $v_2 \sim \mathcal{N}(\boldsymbol{\mu_2}, \rho_2^2 I_N)$
- What is the distribution of $V = v_1\, v_2$?

CLT approach for CKKS

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Suppose $v_1 \sim \mathcal{N}(\boldsymbol{\mu_1}, \rho_1^2 I_N)$ and $v_2 \sim \mathcal{N}(\boldsymbol{\mu_2}, \rho_2^2 I_N)$
- What is the distribution of $V = v_1\, v_2$?

Theorem

- V has mean $\boldsymbol{\mu} = \boldsymbol{\mu_1}\boldsymbol{\mu_2}$ and covariance $\rho^2 I_N + S$
  - $\rho^2 = N\rho_1^2\, \rho_2^2 + \rho_1^2 \|\boldsymbol{\mu_2}\|_2^2 + \rho_1^2 \|\boldsymbol{\mu_1}\|_2^2$
  - S is an off-diagonal matrix
- Moreover, we can approximate $V_i \sim \mathcal{N}(\mu_i, \rho^2)$

CLT approach for CKKS

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Theorem

- V has mean $\boldsymbol{\mu} = \boldsymbol{\mu_1}\boldsymbol{\mu_2}$ and covariance $\rho^2 I_N + S$
  - $\rho^2 = N\rho_1^2\,\rho_2^2 + \rho_1^2\|\boldsymbol{\mu_2}\|_2^2 + \rho_1^2\|\boldsymbol{\mu_1}\|_2^2$
  - S is an off-diagonal matrix
- Moreover, we can approximate $V_i \sim \mathcal{N}(\mu_i, \rho^2)$

CLT approach for CKKS

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Theorem

- V has mean $\boldsymbol{\mu} = \boldsymbol{\mu_1}\boldsymbol{\mu_2}$ and covariance $\rho^2 I_N + S$
  - $\rho^2 = N\rho_1^2\,\rho_2^2 + \rho_1^2\|\boldsymbol{\mu_2}\|_2^2 + \rho_1^2\|\boldsymbol{\mu_1}\|_2^2$
  - S is an off-diagonal matrix
- Moreover, we can approximate $V_i \sim \mathcal{N}(\mu_i, \rho^2)$

Heuristic: We can approximate $V \sim \mathcal{N}(\boldsymbol{\mu},\ \rho^2\, I_N + S)$

CLT approach for CKKS

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Theorem

- V has mean $\boldsymbol{\mu} = \boldsymbol{\mu_1}\boldsymbol{\mu_2}$ and covariance $\rho^2 I_N + S$
  - $\rho^2 = N\rho_1^2\,\rho_2^2 + \rho_1^2\|\boldsymbol{\mu_2}\|_2^2 + \rho_1^2\|\boldsymbol{\mu_1}\|_2^2$
  - S is an off-diagonal matrix
- Moreover, we can approximate $V_i \sim \mathcal{N}(\mu_i, \rho^2)$

Heuristic: We can approximate $V \sim \mathcal{N}(\boldsymbol{\mu},\ \rho^2\, I_N + S)$

Assumption: S is negligible, so $V \sim \mathcal{N}(\boldsymbol{\mu},\ \rho^2\, I_N)$

Experiments: Textbook CKKS, HEAAN v1.0

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	Average	Maximum	CLT	WCR	CE	P-CE	gap
Ring Addition noise.								
13	109	4.58	5.52	4.32	4.82	10.87	12.77	-1.20
14	219	4.63	5.39	4.35	4.85	11.40	13.27	-1.04
15	443	4.68	5.49	4.37	4.87	11.92	13.77	-1.12
Ring Multiplication noise.								
13	109	5.18	6.19	5.67	19.32	12.61	14.32	-0.52
14	219	5.21	6.04	5.70	20.35	13.13	14.82	-0.34
15	443	5.27	6.09	5.72	21.37	13.66	15.32	-0.37
Real Addition error.								
13	109	-25.37	-23.42	-29.70	-22.83	-29.13	-27.22	-6.28
14	219	-24.41	-22.55	-29.18	-21.80	-28.60	-26.72	-6.63
15	443	-23.35	-21.32	-28.65	-20.78	-28.08	-26.22	-7.33
Real Multiplication error.								
13	109	-25.07	-23.00	-28.35	-8.33	-27.39	-25.68	-5.35
14	219	-24.03	-21.77	-27.83	-6.30	-26.87	-25.18	-6.06
15	443	-23.03	-20.98	-27.30	-4.28	-26.34	-24.68	-6.32

Comparison of noise analysis approaches with observed noise in HEAAN v1.0.

Experiments: Textbook CKKS, HEAAN v1.0

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	Average	Maximum	CLT	WCR	CE	P-CE	gap
Ring Addition noise.								
13	109	4.58	5.52	4.32	4.82	10.87	12.77	-1.20
14	219	4.63	5.39	4.35	4.85	11.40	13.27	-1.04
15	443	4.68	5.49	4.37	4.87	11.92	13.77	-1.12
Ring Multiplication noise.								
13	109	5.18	6.19	5.67	19.32	12.61	14.32	-0.52
14	219	5.21	6.04	5.70	20.35	13.13	14.82	-0.34
15	443	5.27	6.09	5.72	21.37	13.66	15.32	-0.37
Real Addition error.								
13	109	-25.37	-23.42	-29.70	-22.83	-29.13	-27.22	-6.28
14	219	-24.41	-22.55	-29.18	-21.80	-28.60	-26.72	-6.63
15	443	-23.35	-21.32	-28.65	-20.78	-28.08	-26.22	-7.33
Real Multiplication error.								
13	109	-25.07	-23.00	-28.35	-8.33	-27.39	-25.68	-5.35
14	219	-24.03	-21.77	-27.83	-6.30	-26.87	-25.18	-6.06
15	443	-23.03	-20.98	-27.30	-4.28	-26.34	-24.68	-6.32

Comparison of noise analysis approaches with observed noise in HEAAN v1.0.

Experiments: Textbook CKKS, HEAAN v1.0

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	Average	Maximum	CLT	WCR	CE	P-CE	gap
Ring Addition noise.								
13	109	4.58	5.52	4.32	4.82	10.87	12.77	-1.20
14	219	4.63	5.39	4.35	4.85	11.40	13.27	-1.04
15	443	4.68	5.49	4.37	4.87	11.92	13.77	-1.12
Ring Multiplication noise.								
13	109	5.18	6.19	5.67	19.32	12.61	14.32	-0.52
14	219	5.21	6.04	5.70	20.35	13.13	14.82	-0.34
15	443	5.27	6.09	5.72	21.37	13.66	15.32	-0.37
Real Addition error.								
Real Multiplication error.								
13	109	-25.07	-23.00	-28.35	-8.33	-27.39	-25.68	-5.35
14	219	-24.03	-21.77	-27.83	-6.30	-26.87	-25.18	-6.06
15	443	-23.03	-20.98	-27.30	-4.28	-26.34	-24.68	-6.32

CLT approach can more closely model noise growth than prior worst-case approach

Comparison of noise analysis approaches with observed noise in HEAAN v1.0.

Experiments: Textbook CKKS, HEAAN v1.0

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	Average	Maximum	CLT	WCR	CE	P-CE	gap
Ring Addition noise.								
13	109	4.58	5.52	4.32	4.82	10.87	12.77	-1.20
14	219	4.63	5.39	4.35	4.85	11.40	13.27	-1.04
15	443	4.68	5.49	4.37	4.87	11.92	13.77	-1.12
Ring Multiplication noise.								
13	109	5.18	6.19	5.67	19.32	12.61	14.32	-0.52
14	219	5.21	6.04	5.70	20.35	13.13	14.82	-0.34
15	443	5.27	6.09	5.72	21.37	13.66	15.32	-0.37
Real Addition error.								
13	109	-25.37	-23.42	-29.70	-22.83	-29.13	-27.22	-6.28
14	219	-24.41	-22.55	-29.18	-21.80	-28.60	-26.72	-6.63
15	443	-23.35	-21.32	-28.65	-20.78	-28.08	-26.22	-7.33
Real Multiplication error.								
13	109	-25.07	-23.00	-28.35	-8.33	-27.39	-25.68	-5.35
14	219	-24.03	-21.77	-27.83	-6.30	-26.87	-25.18	-6.06
15	443	-23.03	-20.98	-27.30	-4.28	-26.34	-24.68	-6.32

Comparison of noise analysis approaches with observed noise in HEAAN v1.0.

Experiments: Textbook CKKS, HEAAN v1.0

ROYAL HOLLOWAY UNIVERSITY OF LONDON

CLT approach can underestimate observed noise

$\log(N)$	$\log(q)$	Average	Maximum	CLT	WCR	CE	P-CE	gap
Ring Addition noise.								
						0.87	12.77	-1.20
						1.40	13.27	-1.04
						1.92	13.77	-1.12
Ring Multiplication noise.								
13	109	5.18	6.19	5.67	19.32	12.61	14.32	-0.52
14	219	5.21	6.04	5.70	20.35	13.13	14.82	-0.34
15	443	5.27	6.09	5.72	21.37	13.66	15.32	-0.37
Real Addition error.								
13	109	-25.37	-23.42	-29.70	-22.83	-29.13	-27.22	-6.28
14	219	-24.41	-22.55	-29.18	-21.80	-28.60	-26.72	-6.63
15	443	-23.35	-21.32	-28.65	-20.78	-28.08	-26.22	-7.33
Real Multiplication error.								
13	109	-25.07	-23.00	-28.35	-8.33	-27.39	-25.68	-5.35
14	219	-24.03	-21.77	-27.83	-6.30	-26.87	-25.18	-6.06
15	443	-23.03	-20.98	-27.30	-4.28	-26.34	-24.68	-6.32

Comparison of noise analysis approaches with observed noise in HEAAN v1.0.

Experiments: RNS-CKKS, FullRNS-HEAAN

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	L	k	Average	Maximum	CLT	CE	P-CE	gap
Real Addition error.									
12	100	2	3	-24.38	-24.21	-24.25	-23.63	-18.89	-0.04
13	100	2	3	-23.16	-22.93	-23.23	-22.61	-17.89	-0.30
14	220	5	6	-22.07	-21.75	-22.21	-21.59	-16.89	-0.46
15	420	10	11	-21.00	-20.74	-21.19	-20.57	-15.89	-0.45
Real Multiplication error.									
12	100	2	3	-21.86	-21.80	-22.96	-21.62	-17.39	-1.16
13	100	2	3	-21.70	-21.41	-21.94	-20.61	-16.39	-0.53
14	220	5	6	-17.79	-17.67	-20.92	-19.59	-15.39	-3.25
15	420	10	11	-16.77	-16.73	-19.90	-18.57	-14.39	-3.17

Comparison of noise analysis approaches with observed noise in FullRNS-HEAAN.

Experiments: RNS-CKKS, FullRNS-HEAAN

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	L	k	Average	Maximum	CLT	CE	P-CE	gap
Real Addition error.									
12	100	2	3	-24.38	-24.21	-24.25	-23.63	-18.89	-0.04
13	100	2	3	-23.16	-22.93	-23.23	-22.61	-17.89	-0.30
14	220	5	6	-22.07	-21.75	-22.21	-21.59	-16.89	-0.46
15	420	10	11	-21.00	-20.74	-21.19	-20.57	-15.89	-0.45
Real Multiplication error.									
12	100	2	3	-21.86	-21.80	-22.96	-21.62	-17.39	-1.16
13	100	2	3	-21.70	-21.41	-21.94	-20.61	-16.39	-0.53
14	220	5	6	-17.79	-17.67	-20.92	-19.59	-15.39	-3.25
15	420	10	11	-16.77	-16.73	-19.90	-18.57	-14.39	-3.17

Comparison of noise analysis approaches with observed noise in FullRNS-HEAAN.

Experiments: RNS-CKKS, FullRNS-HEAAN

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	L	k	Average	Maximum	CLT	CE	P-CE	gap
Real Addition error.									
12	100	2	3	-24.38	-24.21	-24.25	-23.63	-18.89	-0.04
							-22.61	-17.89	-0.30
							-21.59	-16.89	-0.46
							-20.57	-15.89	-0.45
Real Multiplication error.									
12	100	2	3	-21.86	-21.80	-22.96	-21.62	-17.39	-1.16
13	100	2	3	-21.70	-21.41	-21.94	-20.61	-16.39	-0.53
14	220	5	6	-17.79	-17.67	-20.92	-19.59	-15.39	-3.25
15	420	10	11	-16.77	-16.73	-19.90	-18.57	-14.39	-3.17

Again, CLT approach can underestimate observed noise

Comparison of noise analysis approaches with observed noise in FullRNS-HEAAN.

Experiments: RNS-CKKS, FullRNS-HEAAN

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	L	k	Average	Maximum	CLT	CE	P-CE	gap
Real Addition error.									
12	100	2	3	-24.38	-24.21	-24.25	-23.63	-18.89	-0.04
13	100	2	3	-23.16	-22.93	-23.23	-22.61	-17.89	-0.30
14	220	5	6	-22.07	-21.75	-22.21	-21.59	-16.89	-0.46
15	420	10	11	-21.00	-20.74	-21.19	-20.57	-15.89	-0.45
Real Multiplication error.									
12	100	2	3	-21.86	-21.80	-22.96	-21.62	-17.39	-1.16
13	100	2	3	-21.70	-21.41	-21.94	-20.61	-16.39	-0.53
14	220	5	6	-17.79	-17.67	-20.92	-19.59	-15.39	-3.25
15	420	10	11	-16.77	-16.73	-19.90	-18.57	-14.39	-3.17

Comparison of noise analysis approaches with observed noise in FullRNS-HEAAN.

Experiments: RNS-CKKS, FullRNS-HEAAN

ROYAL HOLLOWAY UNIVERSITY OF LONDON

$\log(N)$	$\log(q)$	L	k	Average	Maximum	CLT	CE	P-CE	gap
Real Addition error.									
12	100	2	3	-24.38	-24.21	-24.25	-23.63	-18.89	-0.04
							.61	-17.89	-0.30
							.59	-16.89	-0.46
							.57	-15.89	-0.45
Real Multiplication error.									
12	100	2	3	-21.86	-21.80	-22.96	-21.62	-17.39	-1.16
13	100	2	3	-21.70	-21.41	-21.94	-20.61	-16.39	-0.53
14	220	5	6	-17.79	-17.67	-20.92	-19.59	-15.39	-3.25
15	420	10	11	-16.77	-16.73	-19.90	-18.57	-14.39	-3.17

Jump in real data not captured in any of the noise analyses

Comparison of noise analysis approaches with observed noise in FullRNS-HEAAN.

Results

ROYAL HOLLOWAY UNIVERSITY OF LONDON

+ve: Our average-case approach

- Can more closely model noise growth
- Could refine starting point for manual parameter selection

Results

ROYAL HOLLOWAY UNIVERSITY OF LONDON

+ve: Our average-case approach

- Can more closely model noise growth
- Could refine starting point for manual parameter selection

-ve: Our average-case approach

- Often underestimates practical noise
- May not reflect all implementation choices
- Requires heuristic assumptions that limit applicability

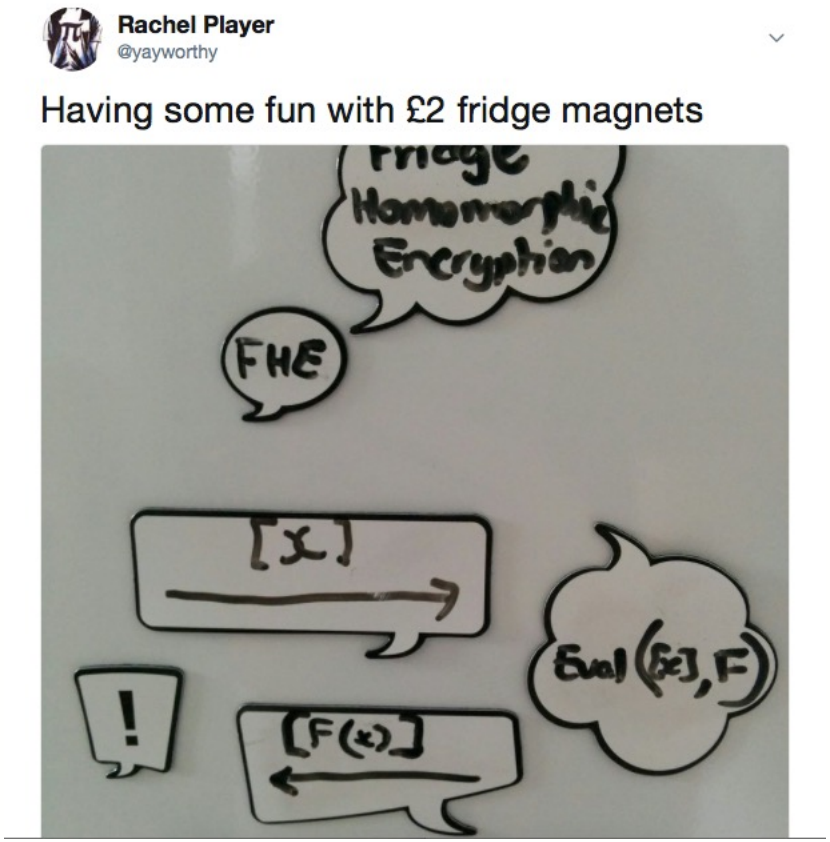
Future work

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Refine average-case analysis to avoid heuristics
- Tailor noise analyses to specific implementations
  - Shown to be effective for BGV as in HElib
- Incorporate noise analyses into compiler toolchains

A. Costache, L. Nürnberger, R. Player. Optimisations and tradeoffs for HElib. CT-RSA 2023.

Thank you & questions!



rachel.player@rhul.ac.uk

Preprint:

- eprint.iacr.org/2022/162

Code:

- github.com/bencrts/CKKS_noise