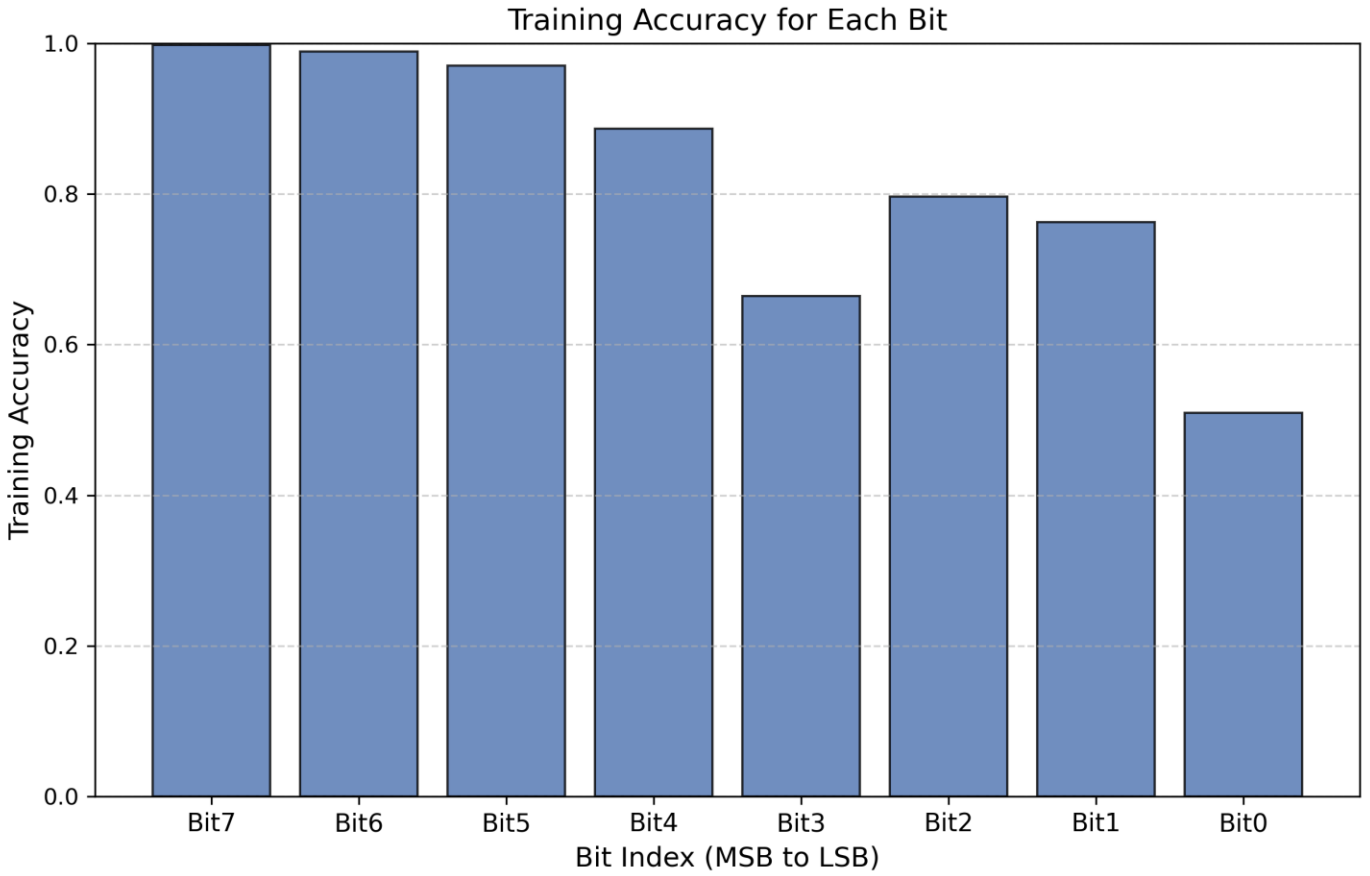
PSCA Characterization using CNN

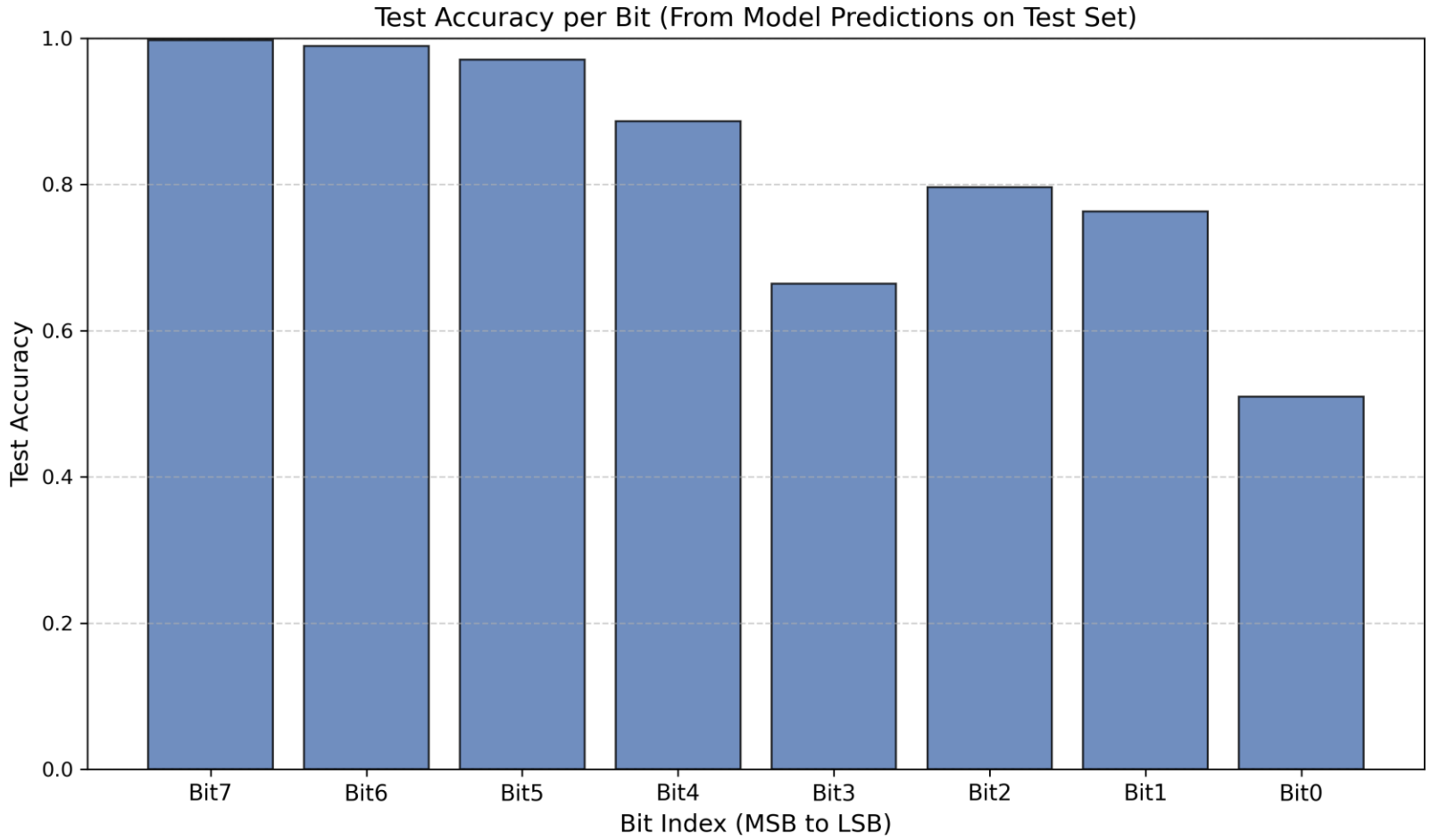
Security Characterization

- 1V Supply Single-ended SAR using switch capacitor scheme.
- Unsecure SAR – 8-bit with split-cap DAC SAR
- Secure SAR – Flash-SAR hybrid (2+6=8-bit)
- Data collection includes a long ramp with multiple conversions per LSB.
- The current trace on VREF should be saved from transient simulation.

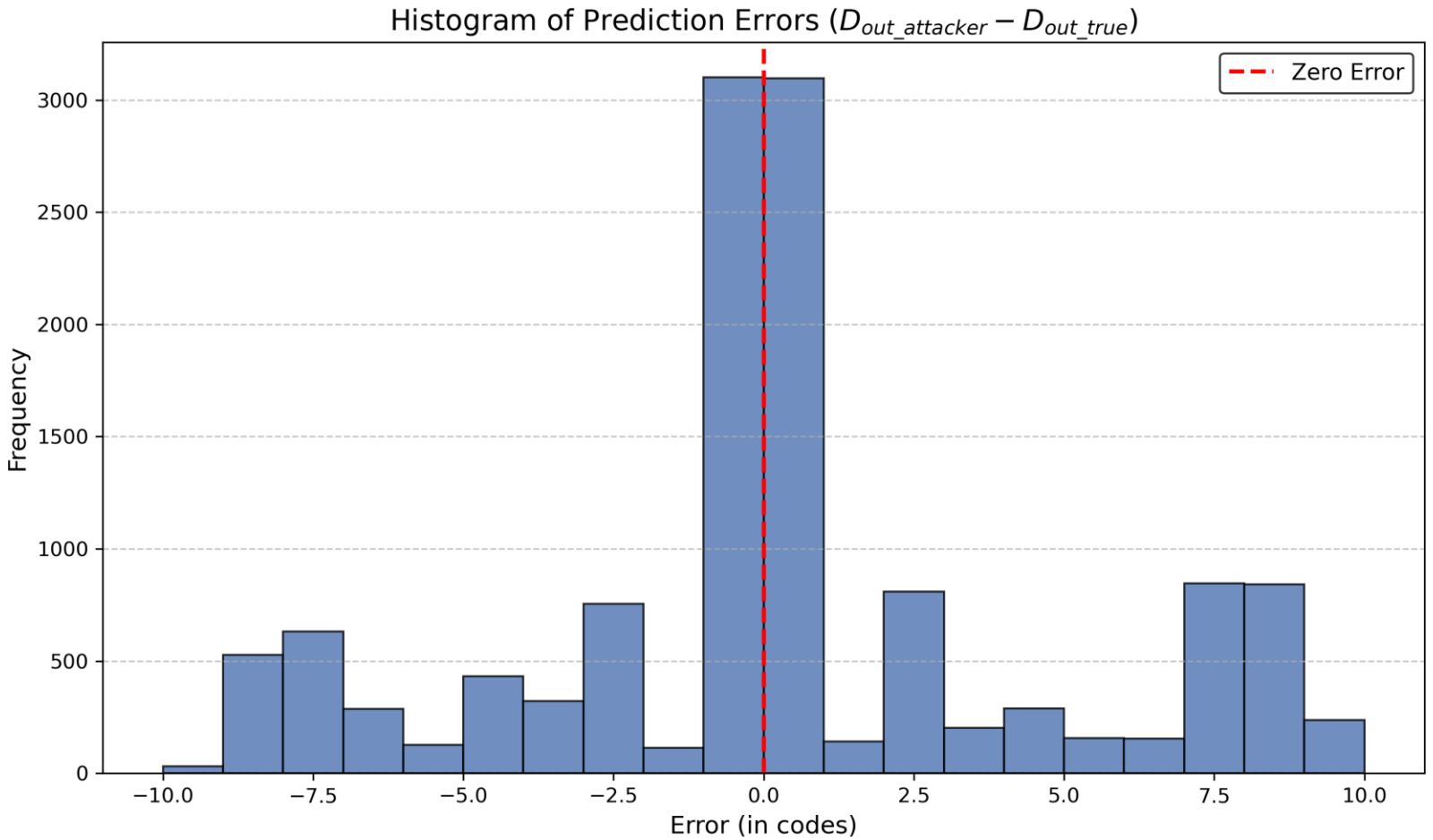
Training accuracy



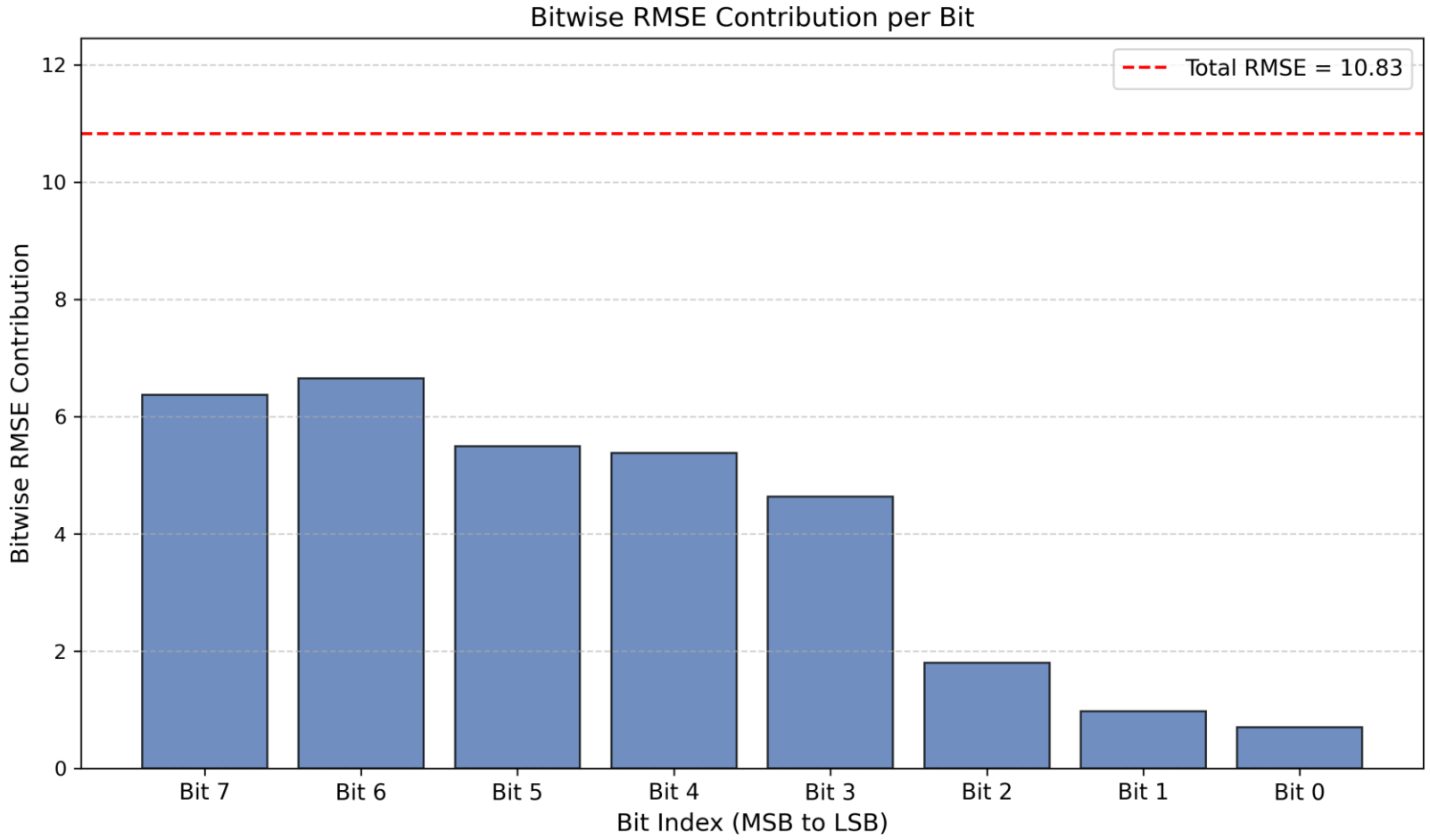
Test Accuracy



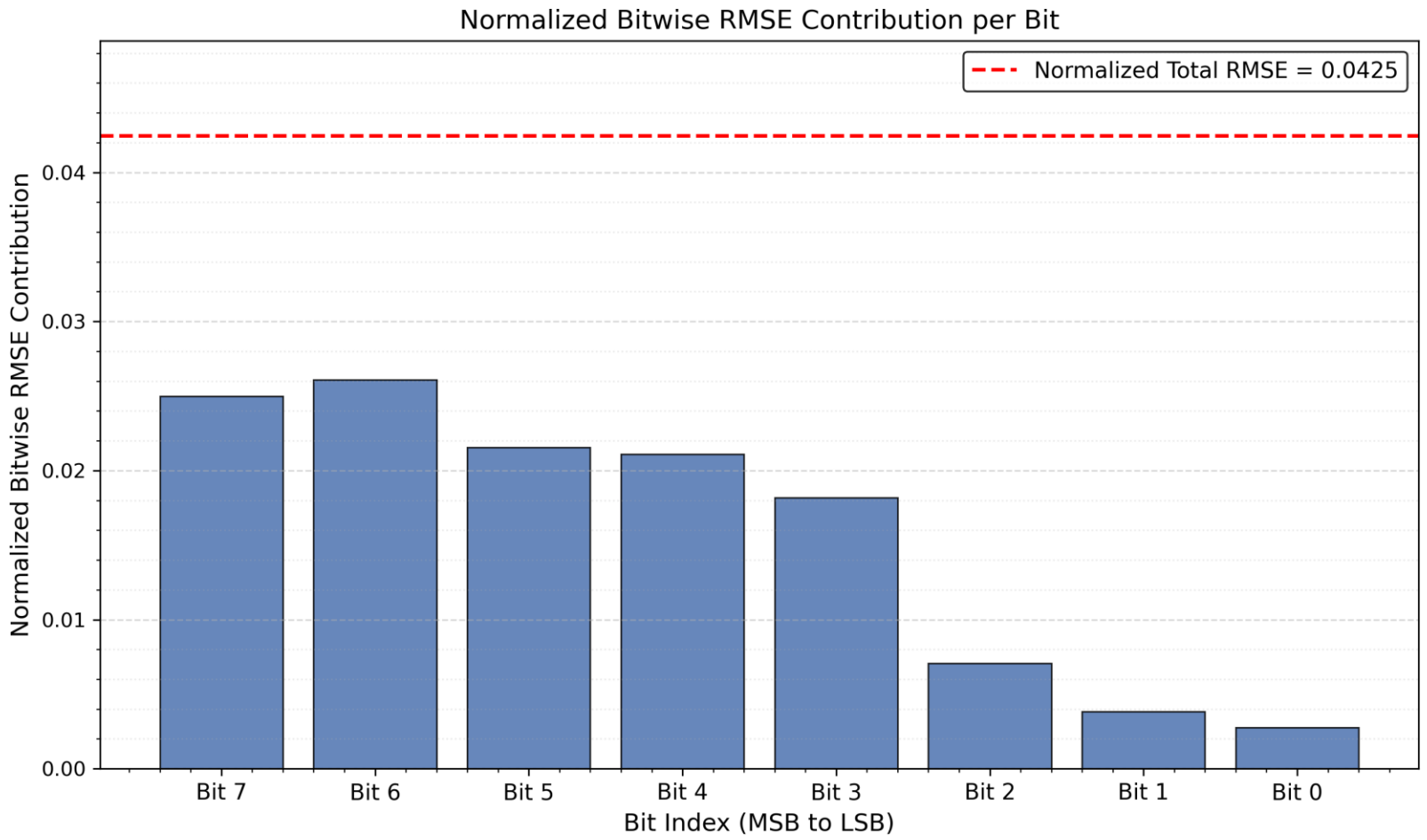
$Dout_{attacker} - Dout_{true}$



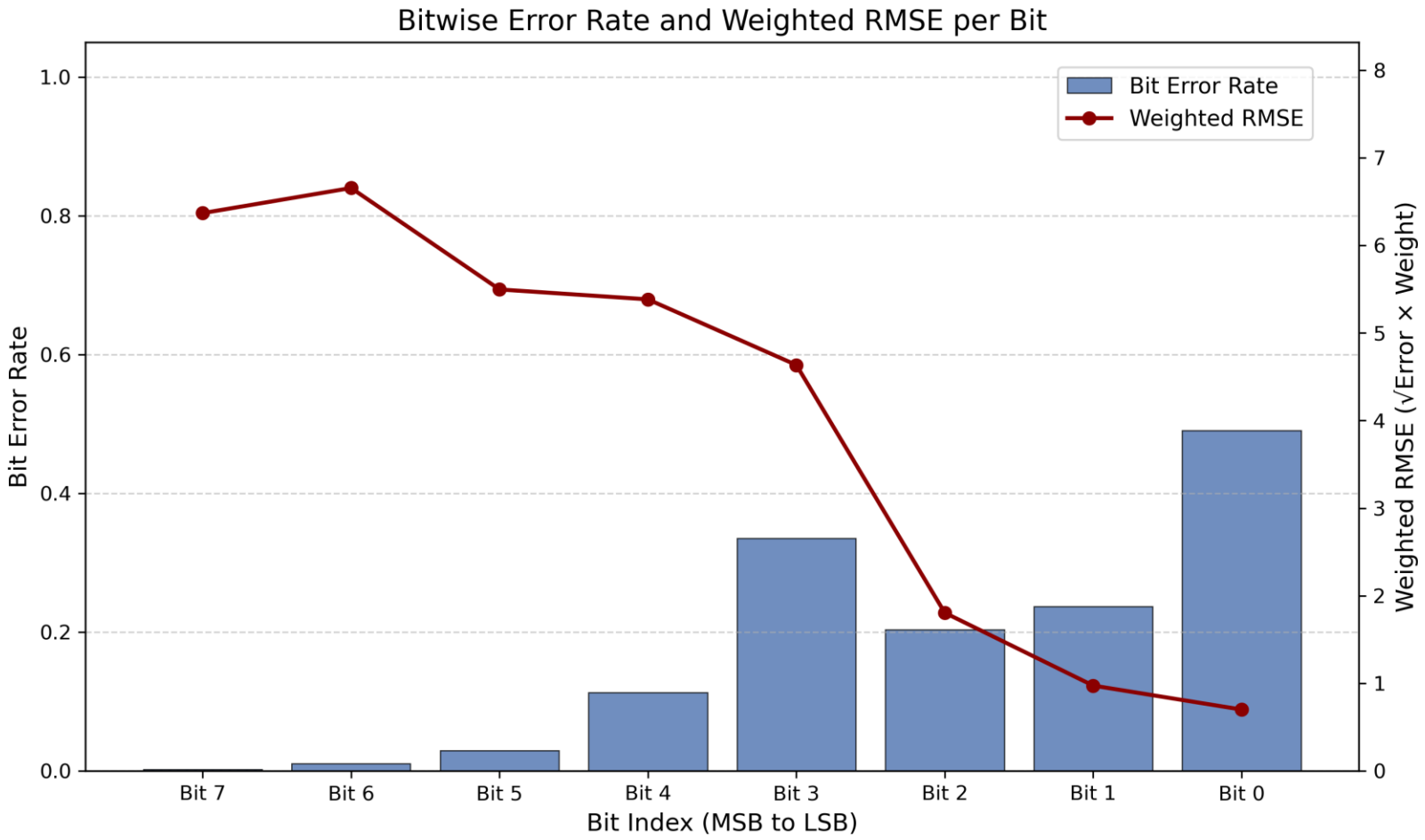
Bitwise RMSE contribution



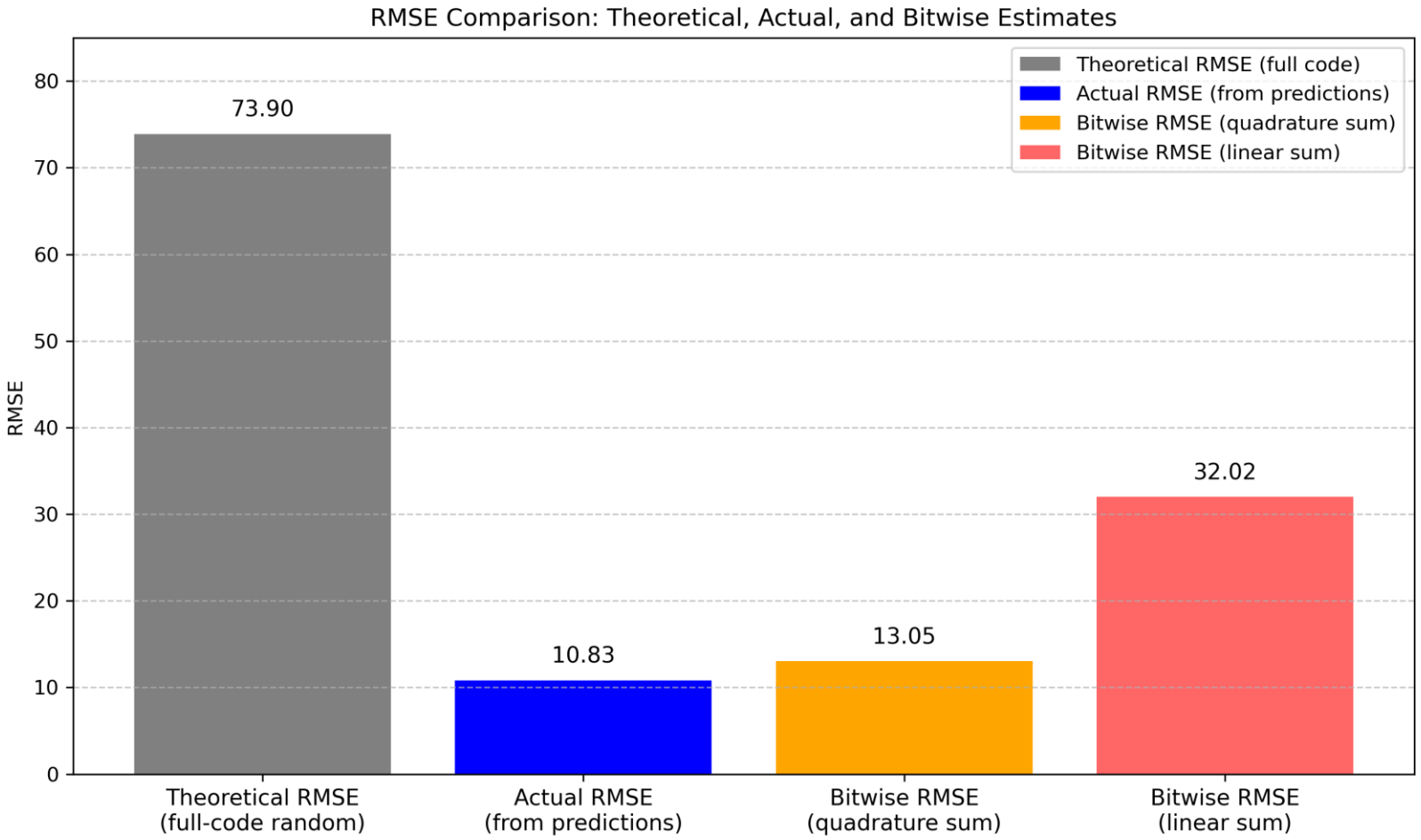
Normalized RMSE



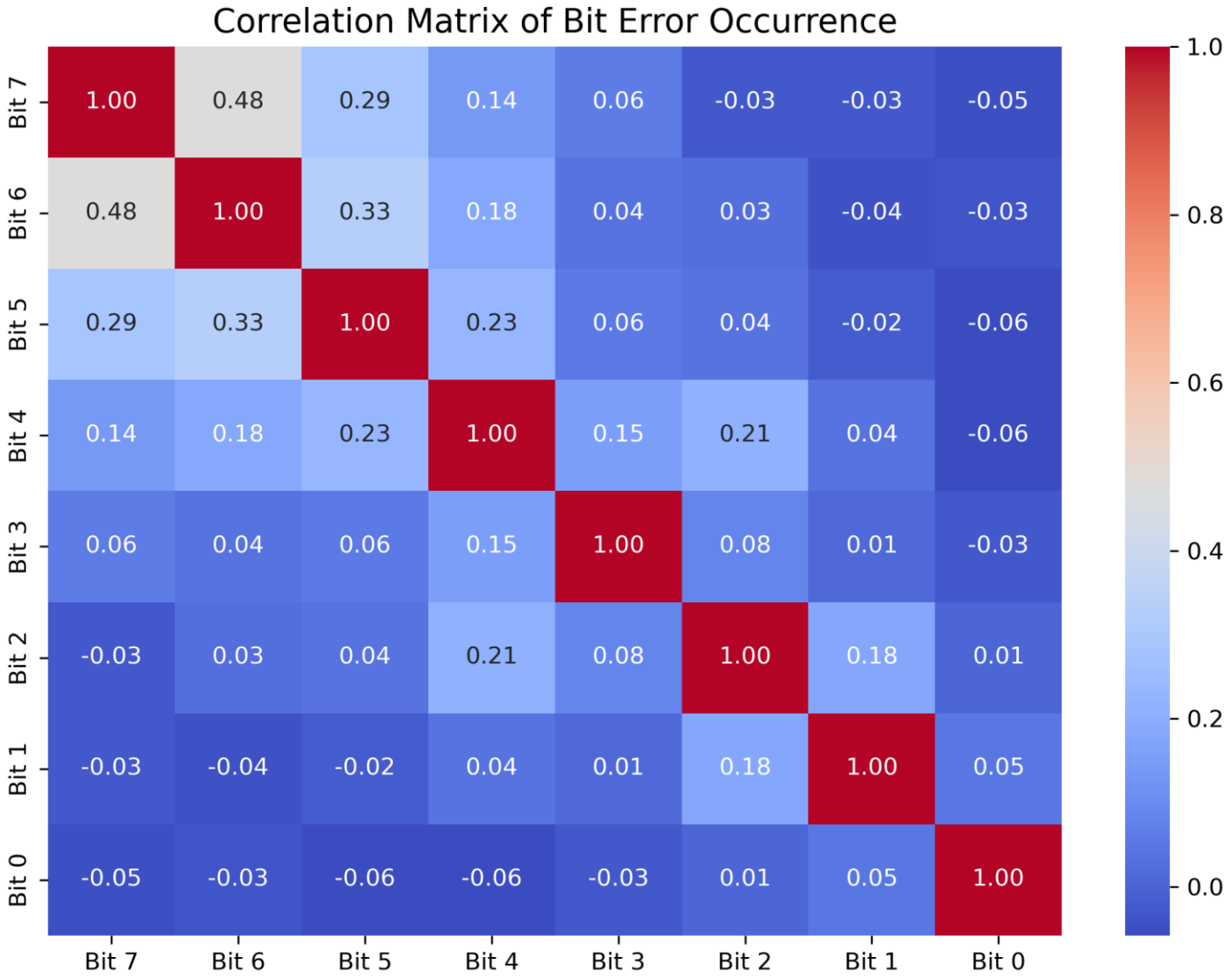
Bitwise Error rate and per-bit RMSE



RMSE Comparison

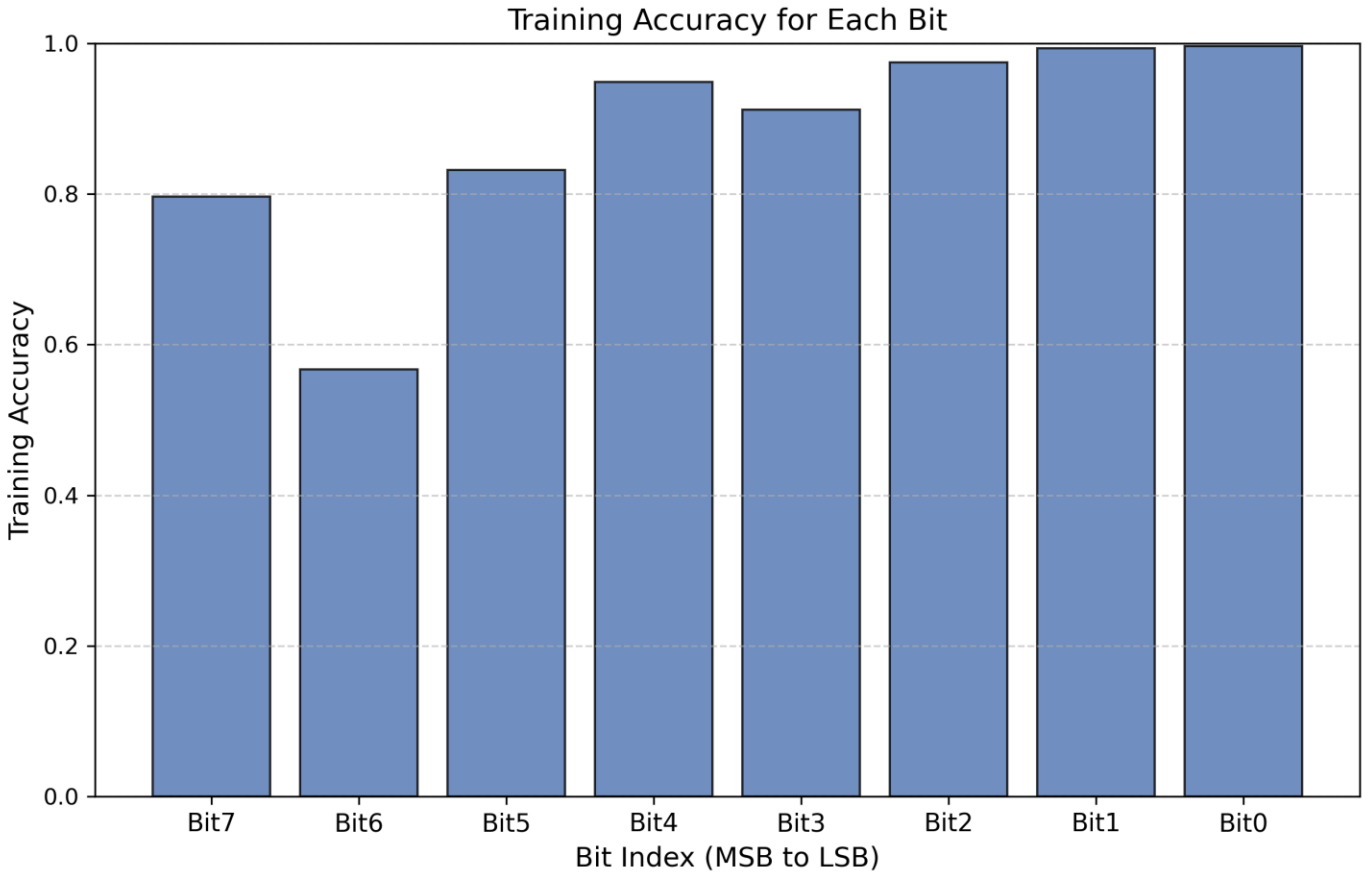


Heatmap

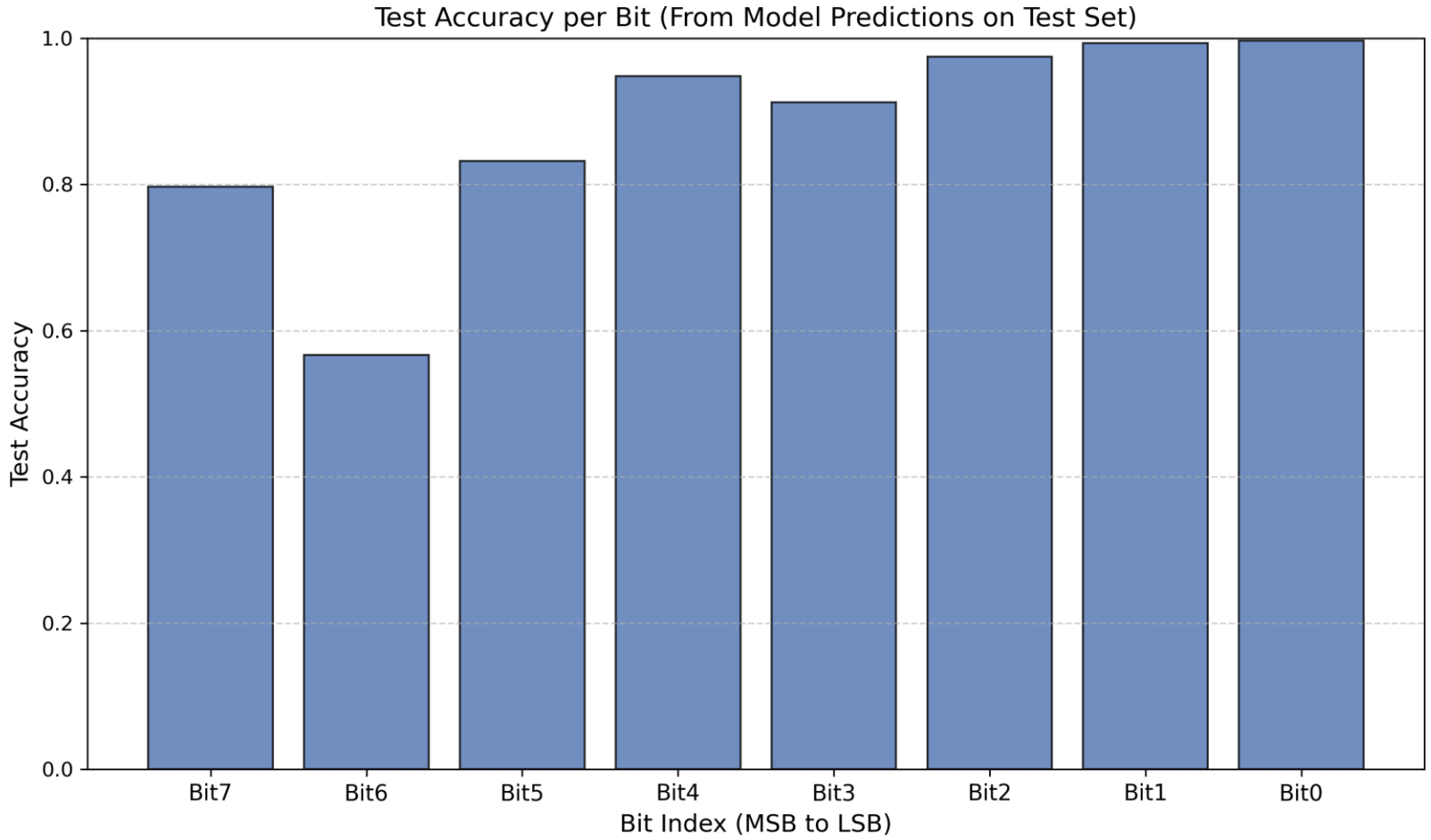

Correlation Matrix of Bit Error Occurrence
Bit 7
Bit 6
Bit 5
Bit 4
Bit 3
Bit 2
Bit 1
Bit 0
1.00 0.48 0.29 0.14 0.06 -0.03 -0.03 -0.05
0.48 1.00 0.33 0.18 0.04 0.03 -0.04 -0.03
0.29 0.33 1.00 0.23 0.06 0.04 -0.02 -0.06
0.14 0.18 0.23 1.00 0.15 0.21 0.04 -0.06
0.06 0.04 0.06 0.15 1.00 0.08 0.01 -0.03
-0.03 0.03 0.04 0.21 0.08 1.00 0.18 0.01
-0.03 -0.04 -0.02 0.04 0.01 0.18 1.00 0.05
-0.05 -0.03 -0.06 -0.06 -0.03 0.01 0.05 1.00
1.0
0.8
0.6
0.4
0.2
0.0

Secure ADC with security Module

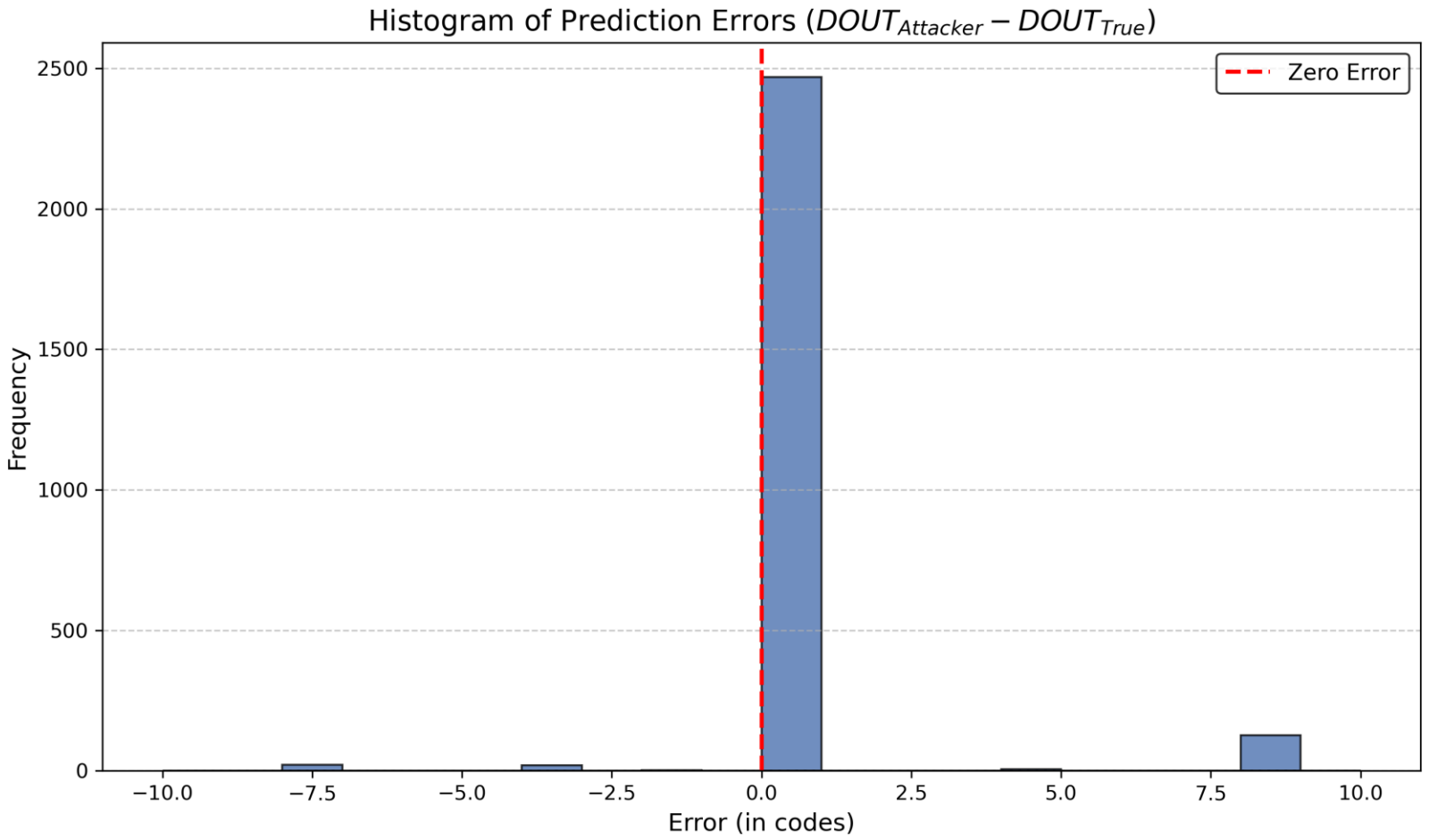
Training accuracy



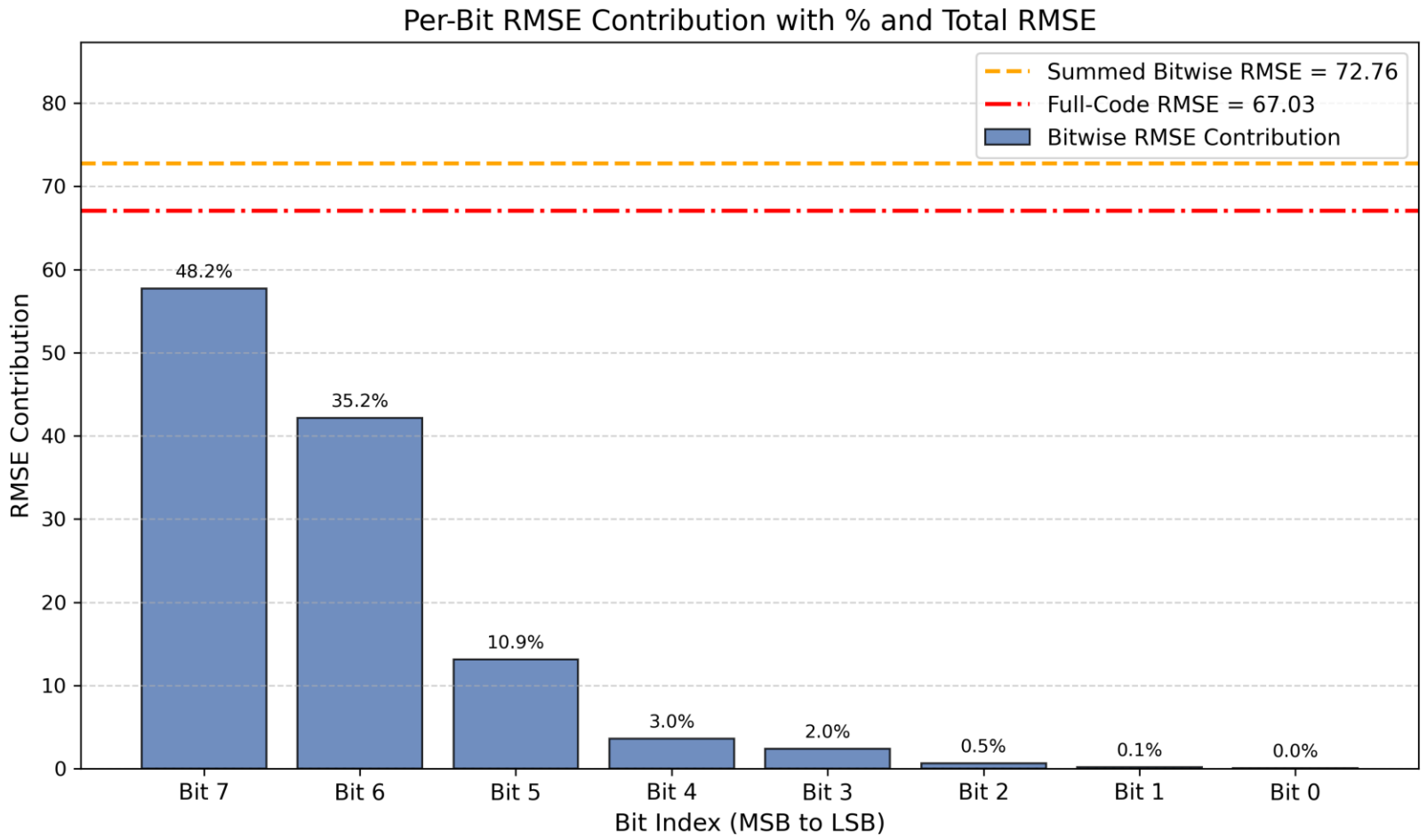
Test Accuracy



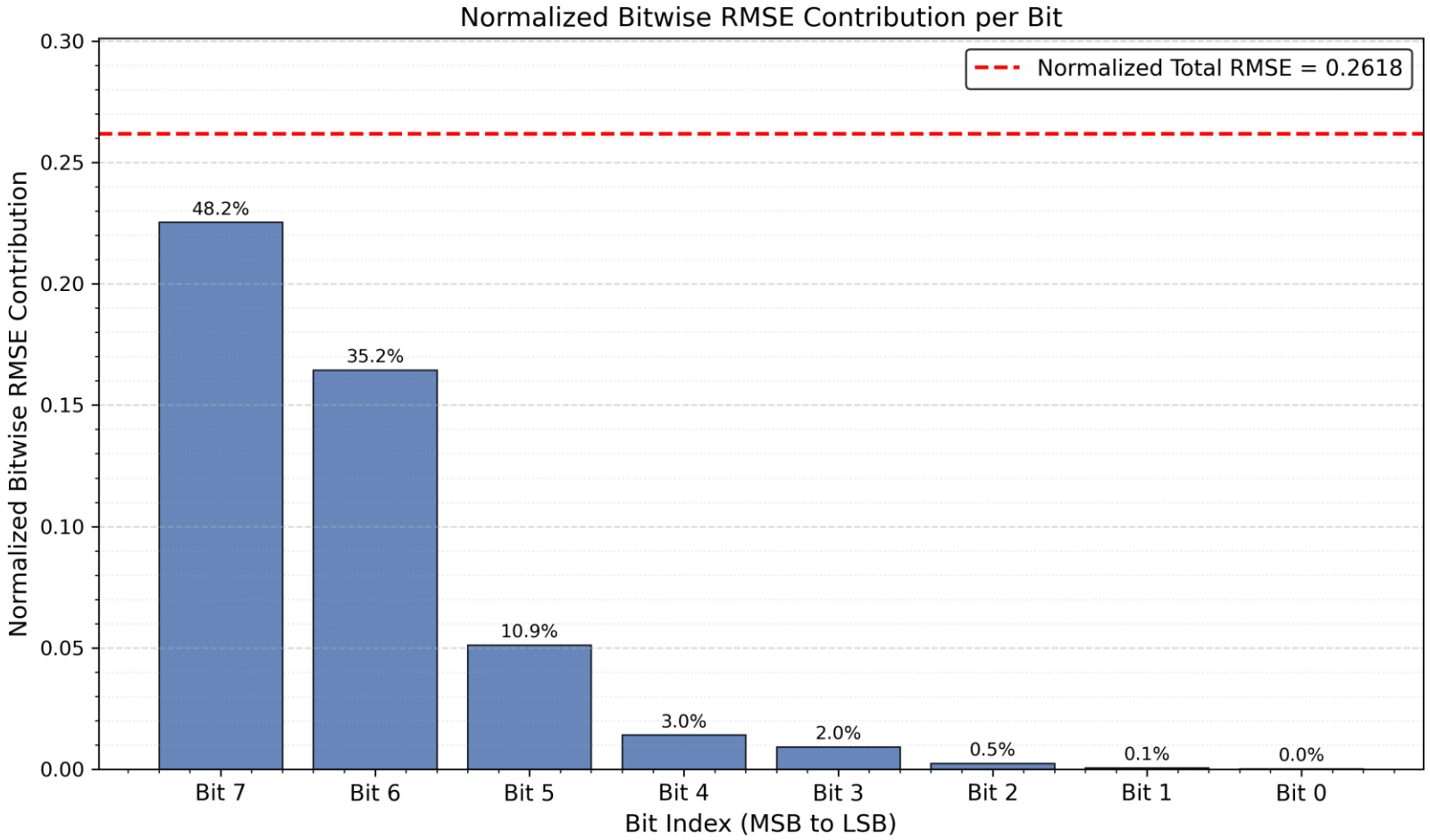
$Dout_{attacker} - Dout_{true}$



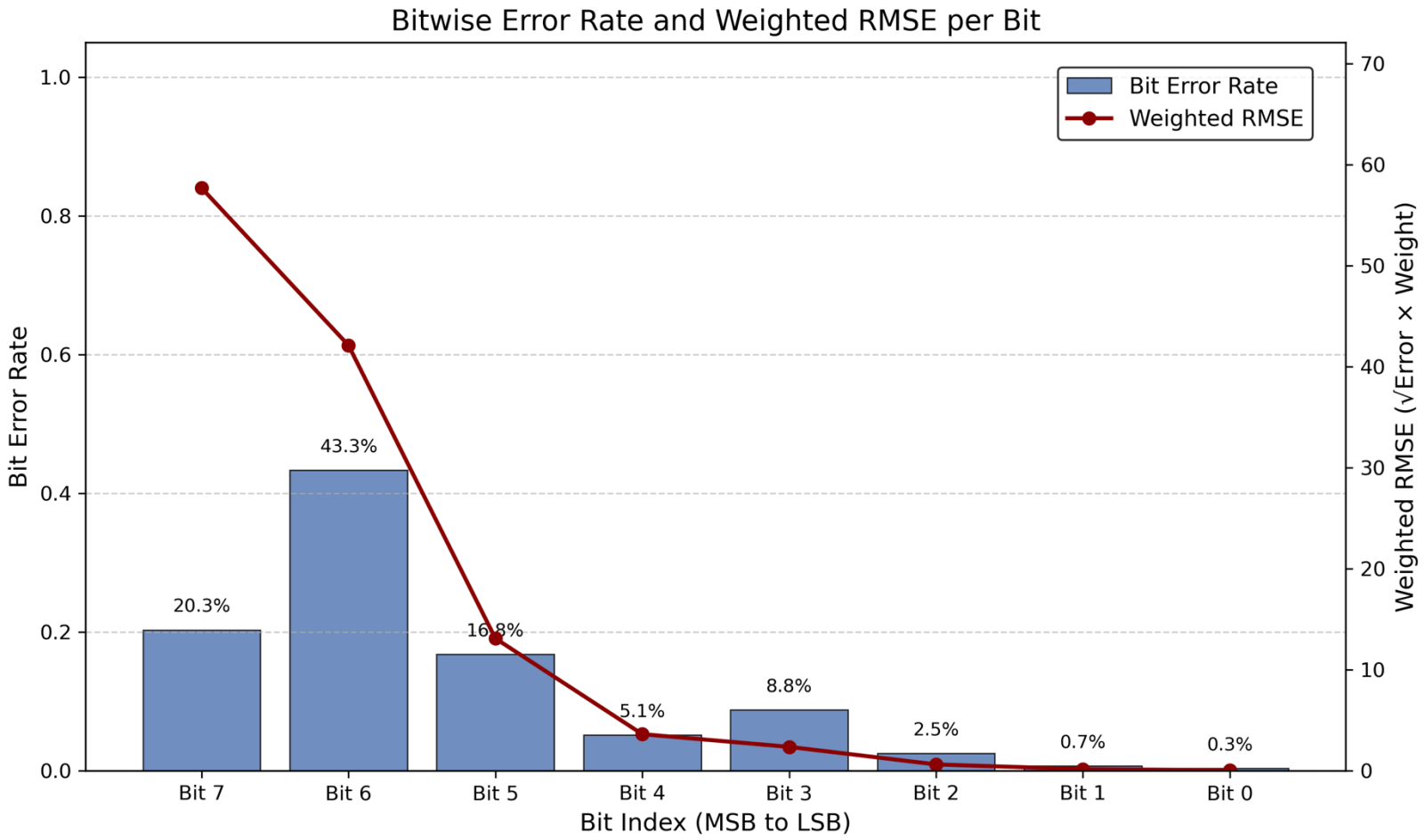
Bitwise RMSE contribution



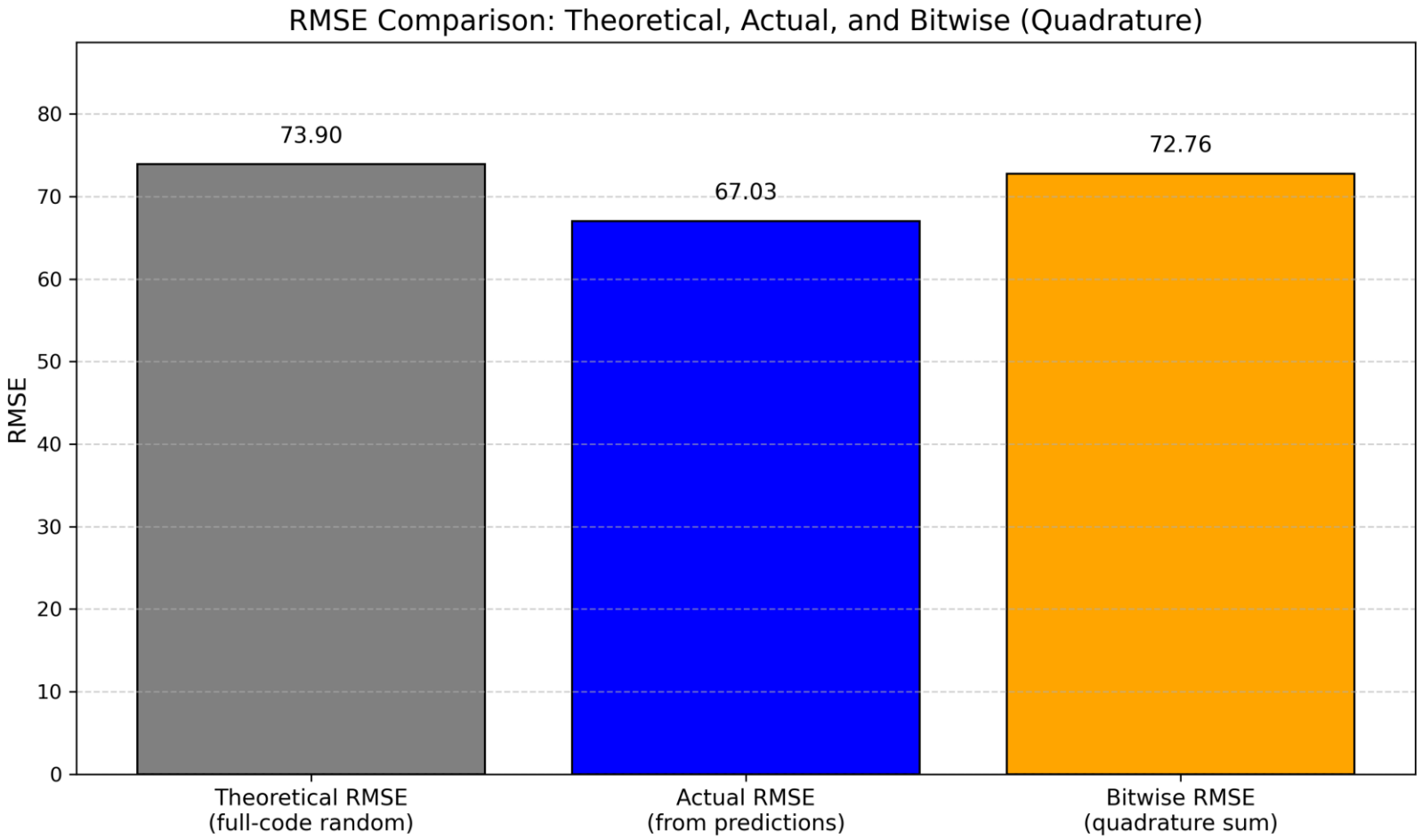
Normalized bitwise RMSE



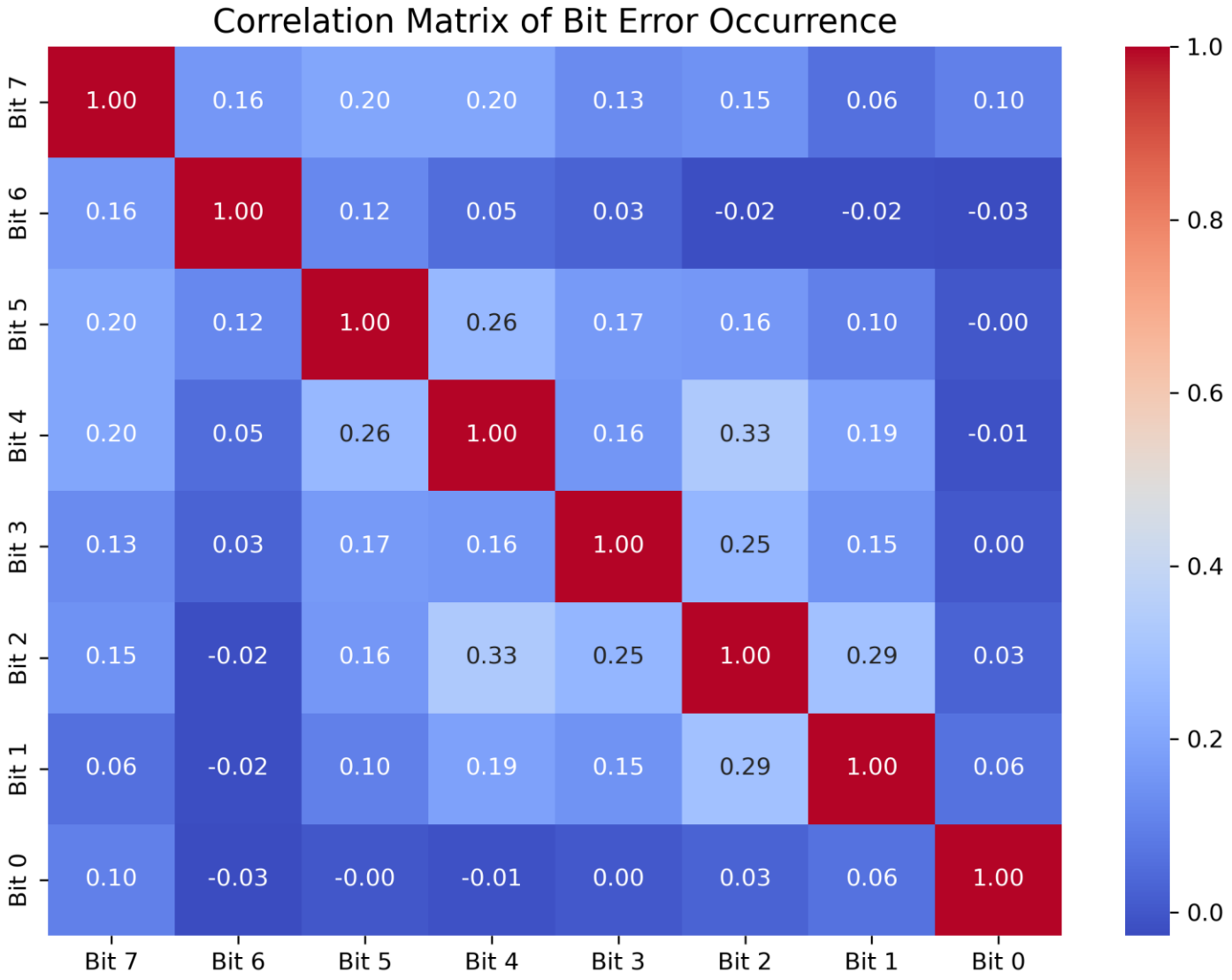
Bitwise Error rate and per-bit RMSE



RMSE Comparison

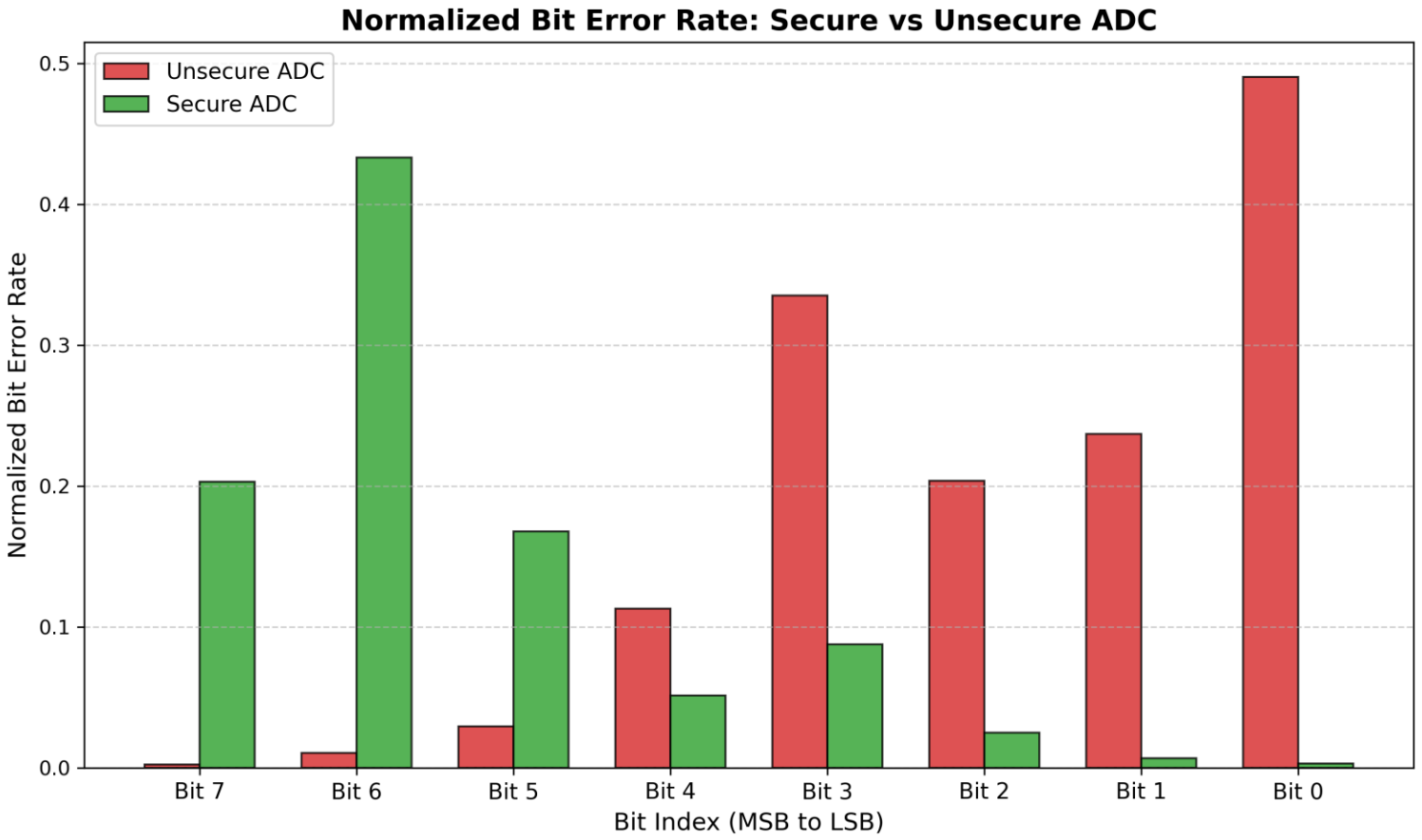


Heatmap

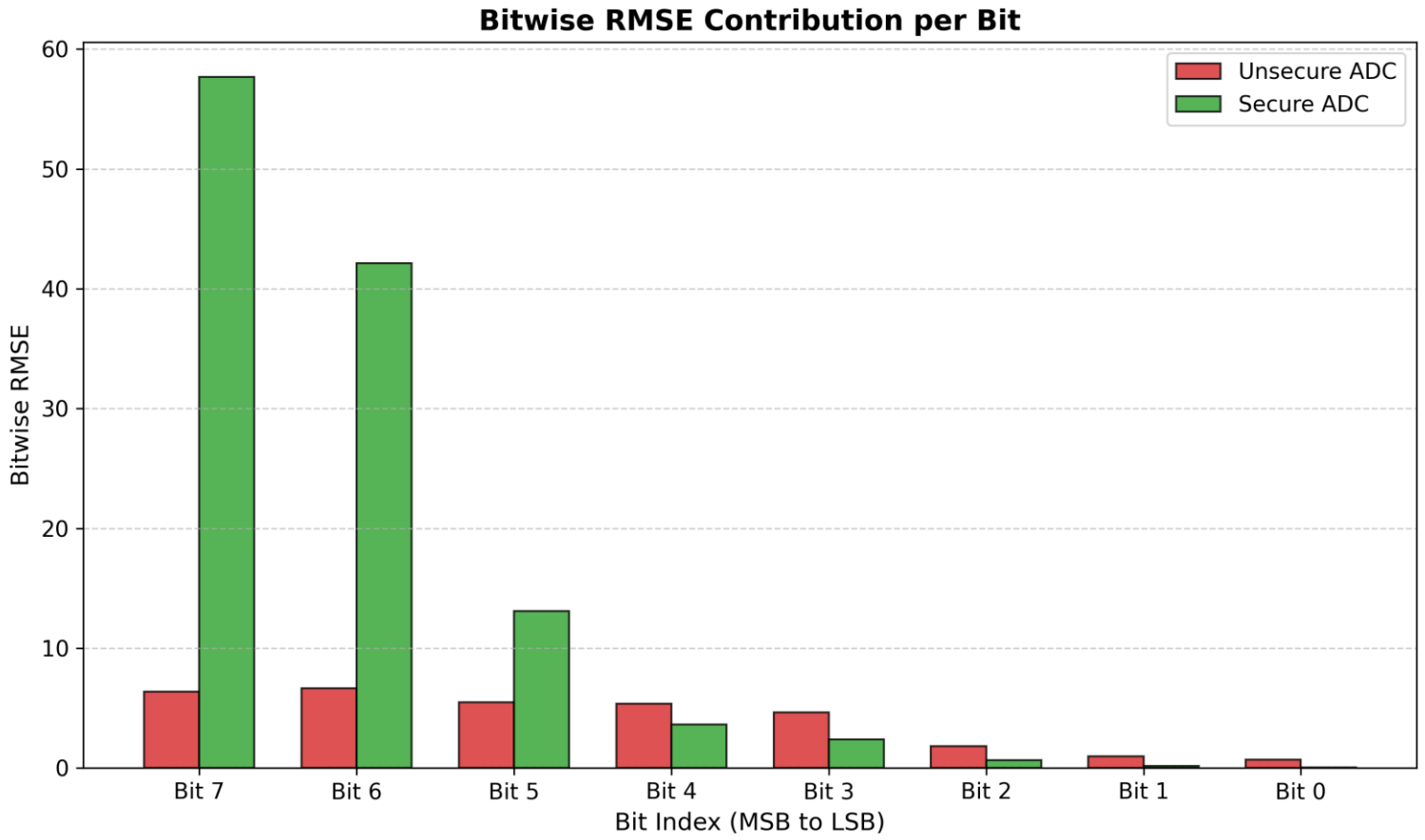

Correlation Matrix of Bit Error Occurrence
Bit 7
Bit 6
Bit 5
Bit 4
Bit 3
Bit 2
Bit 1
Bit 0
1.00 0.16 0.20 0.20 0.13 0.15 0.06 0.10
0.16 1.00 0.12 0.05 0.03 -0.02 -0.02 -0.03
0.20 0.12 1.00 0.26 0.17 0.16 0.10 -0.00
0.20 0.05 0.26 1.00 0.16 0.33 0.19 -0.01
0.13 0.03 0.17 0.16 1.00 0.25 0.15 0.00
0.15 -0.02 0.16 0.33 0.25 1.00 0.29 0.03
0.06 -0.02 0.10 0.19 0.15 0.29 1.00 0.06
0.10 -0.03 -0.00 -0.01 0.00 0.03 0.06 1.00
1.0
0.8
0.6
0.4
0.2
0.0

Secure vs Unsecure ADC Performance

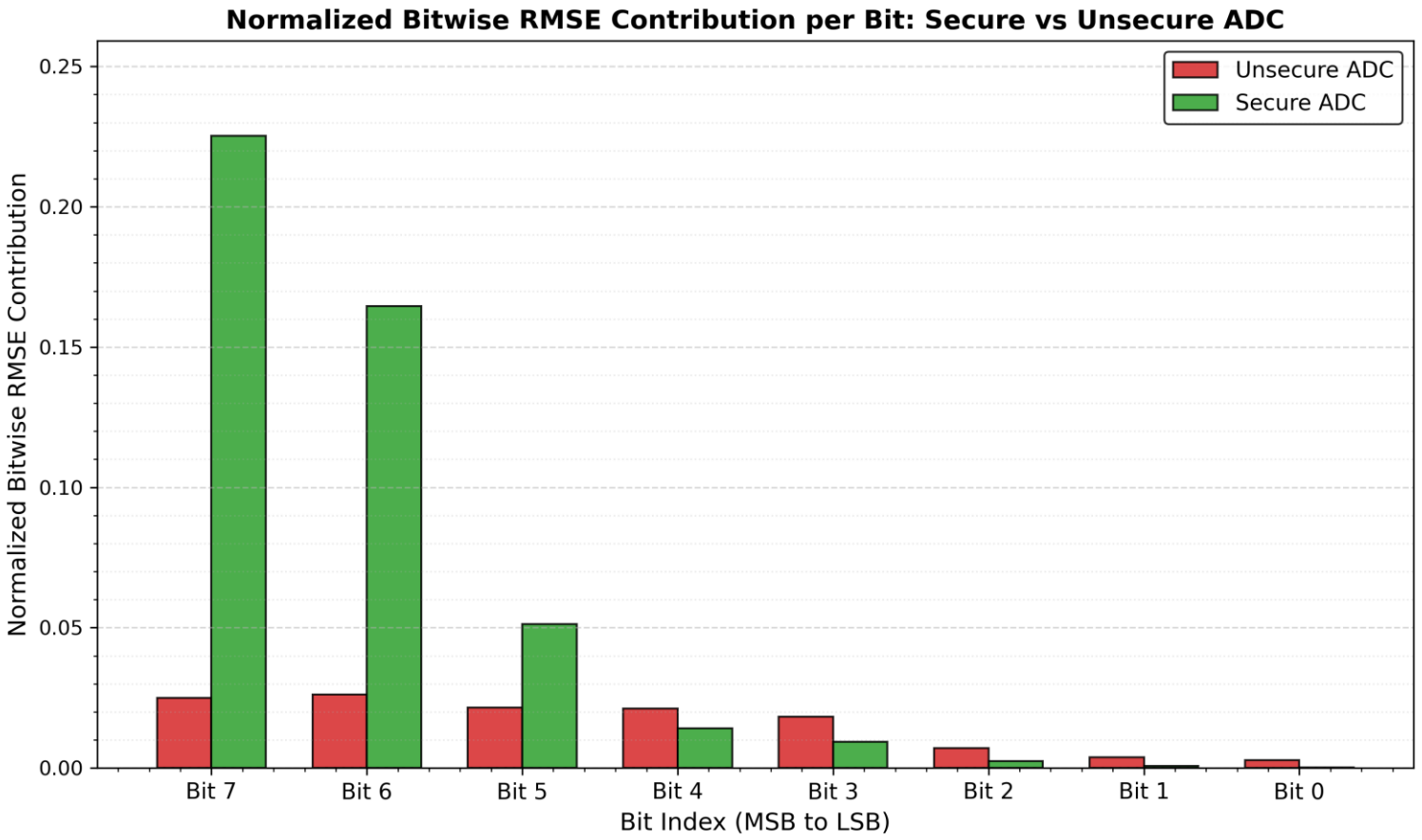
Normalized Bit Error Rate



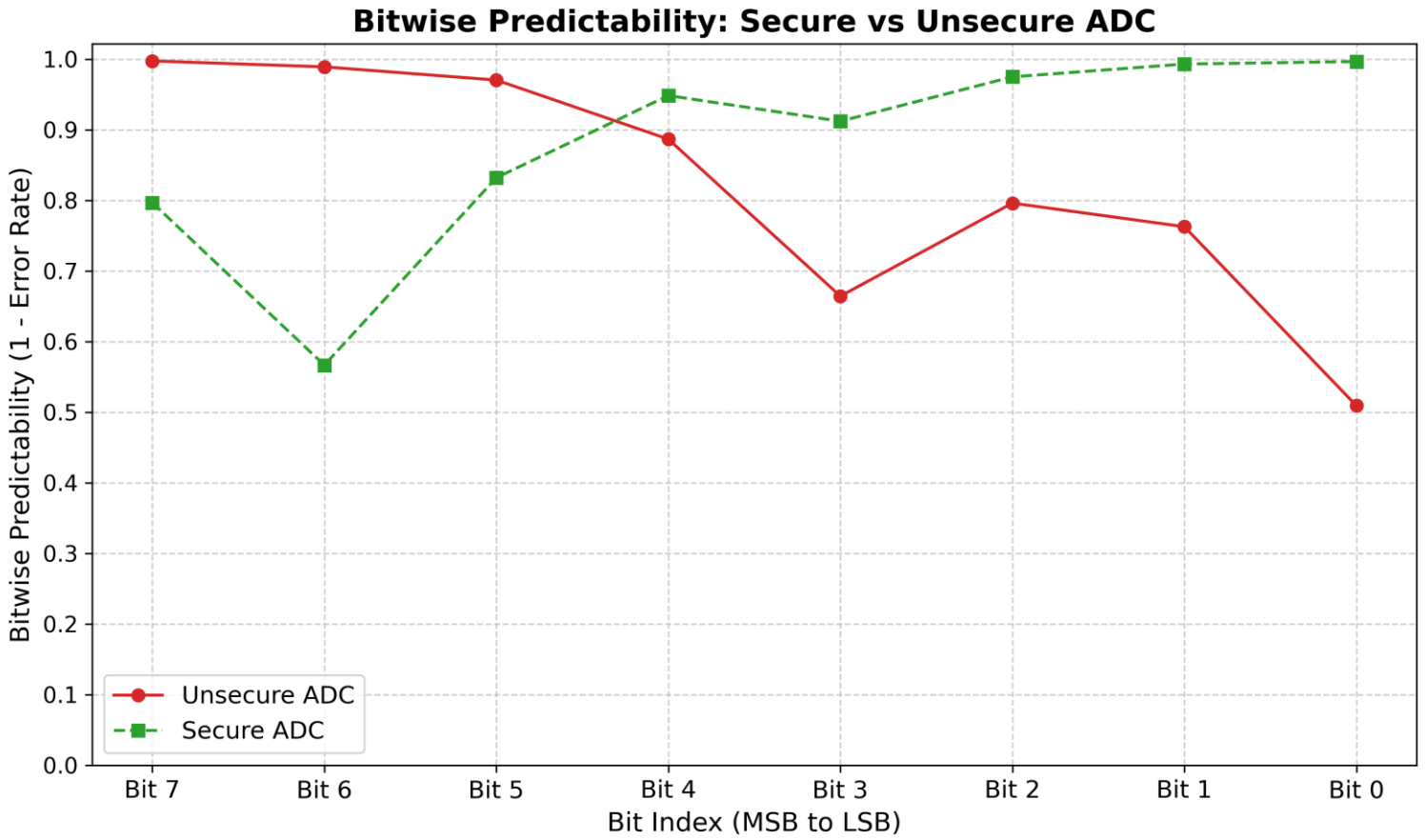
Bitwise RMSE Contribution



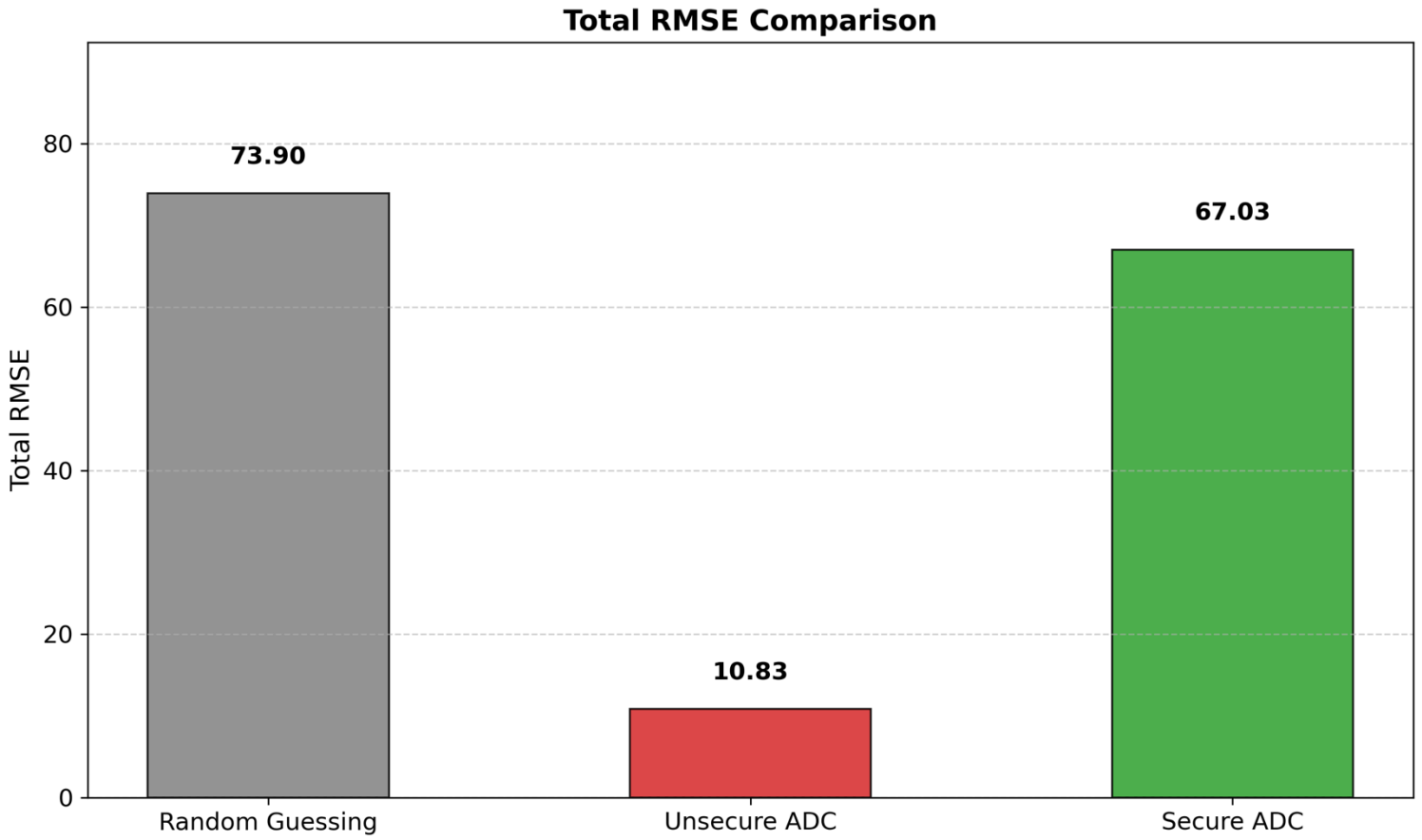
Normalized Bitwise RMSE contribution



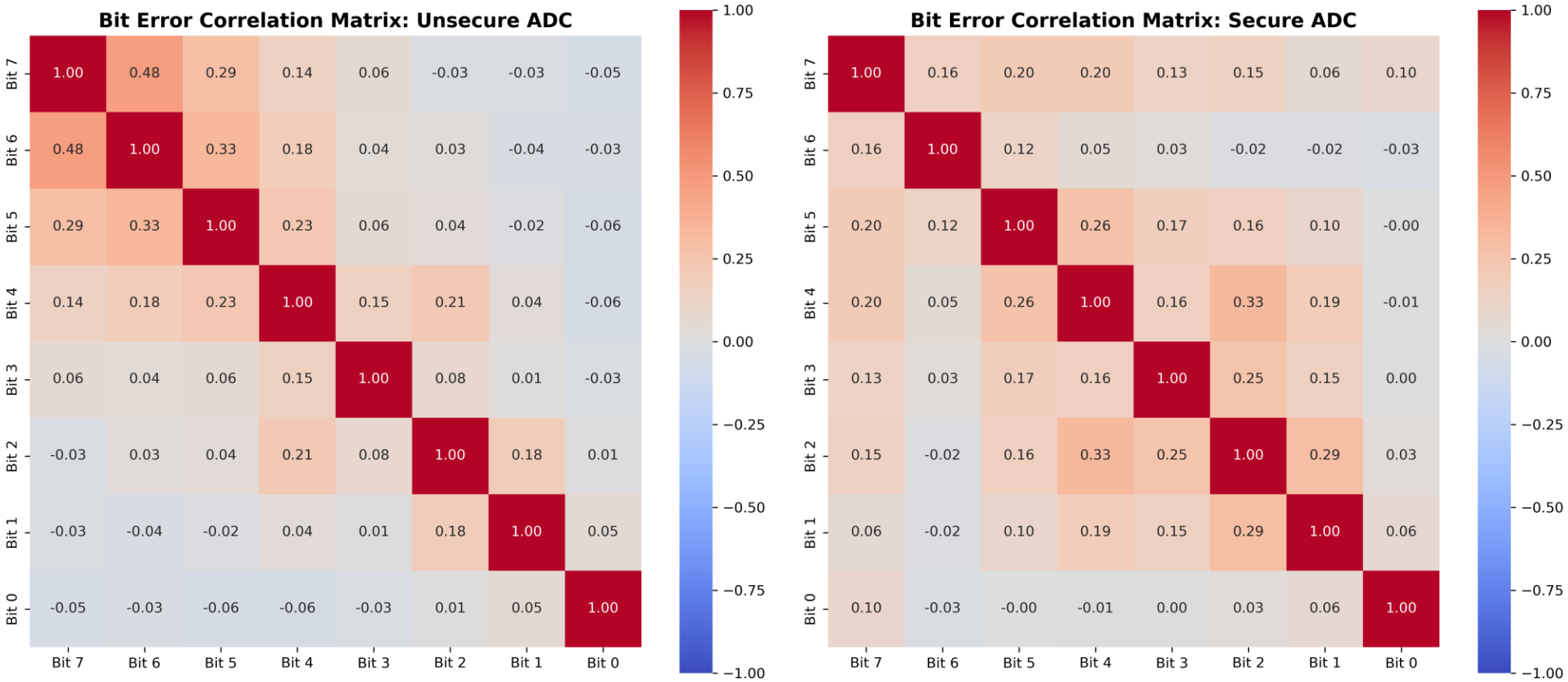
Bitwise Predictability



Total RMSE Comparison



Heatmap Comparison



Comments

- The comparison demonstrates enhanced security through the use of a secure module.
- Flash-SAR bits are harder to predict via a CNN attack.
- The result is normalized to an 8-bit value to compare with ADCs that have different resolutions.

Comparison with other work

Publication	This Work		TCAS-II '20 [35]		JSSC '21 [68]		HOST '24 [34]		CICC '22 [33]		VLSI '22 [32]		CICC '23 [31]	
Process (nm)	65[a]		180		65		65[a]		65		65		65	
Supply (V)	1		N/A[b]		1.2		1		1.2		1.2		1.2	
Resolution (bits)	8		10		12		8		8		12		12	
Topology	Single-Ended		Single-Ended		Differential		Differential		Differential		Differential		Differential	
Protected	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Power (µW)	308.4	536.2	63.5	65.0	83.2	158.5	145.0	150.7	43.4	50.2	539.8	539.8	722.0	698.0
Sample Rate (MS/s)	1.00	1.25	1.07	1.00	1.25	1.25	20.00	20.00	3.33	2.00	25.00	25.00	45.00	40.00
Area (mm^2)	0.061	0.095	0.070	0.075	0.340	0.500	0.015	0.017	0.064	0.073	0.072	0.072	0.075	0.075
ENOB (bit)	5.57	6.87	8.80	8.70	11.20[c]	11.20[c]	7.86	7.80	7.20	7.70	10.90	10.90	10.90[c]	10.80[c]
FoM_W (fJ/c.-s.)	6492	3667	130.80	151.50	27.90	54.30	31.00	33.80	88.60	120.70	11.30	11.30	8.50	9.80
SFDR (dB)	17.30	17.20	64.50	64.30	86.00	89.60	N/A[b]	N/A[b]	53.70	54.60	86.60	86.60	80.50	80.20
Leakage RMSE (LSBs)	10.83/ 256	67.03/ 256	-[e]	-[e]	117.74/ 4096	384.04/ 4096	24.50/ 256	103.00/ 256	0.70/ 256	58.00/ 256	14.21/ 4096	1625.39/ 4096	52.76/ 4096	1985.25/ 4096
Normalized RMSE	0.0415	0.2618	-[e]	-[e]	0.02870	0.0938	0.09500	0.4200	0.0027	0.2266	0.0035	0.3968	0.0129	0.4847
Random Bits (Mb/s)	NA	0	NA	1	NA	0	NA	200	NA	360	NA	275	NA	4080

[a]Simulation only

[b]Value not disclosed

[c]Calculated from FoM_W, Power, and Sample Rate

[d]Reported an unprotected leakage ENOB of 4.60 bits and a protected leakage ENOB of 0.8

[e]RMSE not reported