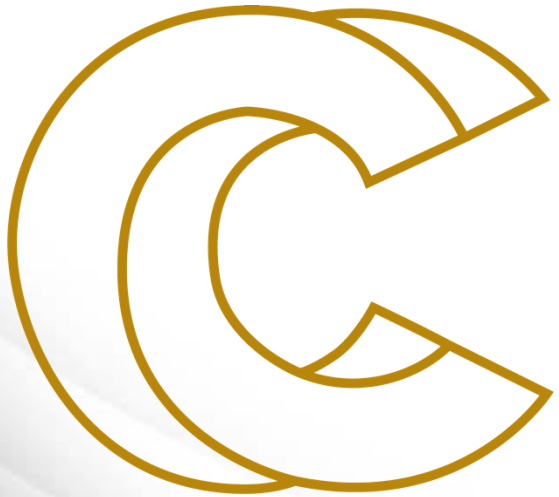

EURO^2

GPU Optimization of Advanced Encryption Standard

Cihangir Tezcan, PhD

Graduate School of Informatics, METU, Ankara

ncc@ulakbim.gov.tr

Lesson 6: Encryption Performance of AES on GPUs

EURO²

GPU Performance in the Literature

Gbps	Device	Architecture	Launch year	Reference
80.5	GTX 780	Kepler	2013	[1]
123.0	GTX 970	Maxwell	2014	[2]
207.3	GTX TITAN X	Maxwell	2015	[1]
214.0	GTX 1070	Pascal	2016	[2]
279.9	GTX 1080	Pascal	2016	[1]
310.0	RTX 2070	Turing	2018	[2]
605.9	Tesla P100	Pascal	2016	[3]

Lesson 6: Encryption Performance of AES on GPUs

EURO²

GPU Performance in the Literature

Gbps	Device	Architecture	Launch year	Reference
80.5	GTX 780	Kepler	2013	[1]
102.4	*I7-980X*	*Gulftown*	2010	[4]
123.0	GTX 970	Maxwell	2014	[2]
207.3	GTX TITAN X	Maxwell	2015	[1]
214.0	GTX 1070	Pascal	2016	[2]
279.9	GTX 1080	Pascal	2016	[1]
310.0	RTX 2070	Turing	2018	[2]
605.9	Tesla P100	Pascal	2016	[3]

Lesson 6: Encryption Performance of AES on GPUs

Gbps	Device	Architecture	Launch year	Reference
80.5	GTX 780	Kepler	2013	[1]
90.6	*I7-6700K*	*Skylake*	2013	[5]
102.4	*I7-980X*	*Gulftown*	2010	[4]
123.0	GTX 970	Maxwell	2014	[2]
134.7	*I7-10700F*	*Comet Lake*	2020	[5]
207.3	GTX TITAN X	Maxwell	2015	[1]
214.0	GTX 1070	Pascal	2016	[2]
279.9	GTX 1080	Pascal	2016	[1]
310.0	RTX 2070	Turing	2018	[2]
605.9	Tesla P100	Pascal	2016	[3]

Lesson 6: Encryption Performance of AES on GPUs

Encryption and Key Search Performance of AES on GPUs

- Codes are also available at https://www.github.com/cihangirtezcan/CUDA_AES
- Academic publication [5] is available at

[5] *Cihangir Tezcan. Optimization of advanced encryption standard on graphics processing units. IEEE Access, 9:67315–67326, 2021.*

Lesson 6: Encryption Performance of AES on GPUs

EURO²

GPU Specs

GPU	Cores	Clock Rate	CC	Architecture
MX 250	384	1582 MHz	6.1	Pascal
GTX 860M	640	1020 MHz	5.0	Maxwell
GTX 970	1664	1253 MHz	5.2	Maxwell
RTX 2070 Super	2560	1770 MHz	7.5	Turing

Lesson 6: Encryption Performance of AES on GPUs

EURO²

Our Encryption Results for AES in CTR Mode

GPU	AES-128	AES-192	AES-256
MX 250	102.7 Gbps	72.3 Gbps	60.0 Gbps
GTX 860M	95.9 Gbps	77.1 Gbps	65.3 Gbps
GTX 970	312.2 Gbps	254.8 Gbps	214.7 Gbps
RTX 2070 Super	878.6 Gbps	718.3 Gbps	606.9 Gbps

Lesson 6: Encryption Performance of AES on GPUs

EURO²

Gbps	Device	Architecture	Launch year	Reference
80.5	GTX 780	Kepler	2013	[1]
90.6	*I7-6700K*	*Skylake*	2013	[5]
102.4	*I7-980X*	*Gulftown*	2010	[4]
123.0	GTX 970	Maxwell	2014	[2]
134.7	*I7-10700F*	*Comet Lake*	2020	[5]
207.3	GTX TITAN X	Maxwell	2015	[1]
214.0	GTX 1070	Pascal	2016	[2]
279.9	GTX 1080	Pascal	2016	[1]
310.0	RTX 2070	Turing	2018	[2]
315.2	GTX 970	Maxwell	2014	[5]
605.9	Tesla P100	Pascal	2016	[3]
878.6	RTX 2070 Super	Turing	2019	[5]

Lesson 6: Encryption Performance of AES on GPUs

EURO²

Gbps/W	Gbps	Device	Architecture	Launch year	Reference
0.322	80.5	GTX 780	Kepler	2013	[1]
0.788	102.4	i7-980X	Gulftown	2010	[4]
0.829	207.3	GTX TITAN X	Maxwell	2015	[1]
0.848	123	GTX 970	Maxwell	2014	[2]
0.996	90.6	i7-6700K	Skylake	2013	[5]
1.427	214	GTX 1070	Pascal	2016	[2]
1.555	279.9	GTX 1080	Pascal	2016	[1]
1.771	310	RTX 2070	Turing	2018	[2]
2.072	134.7	i7-10700F	Comet Lake	2020	[5]
2.174	315.2	GTX 970	Maxwell	2014	[5]
2.423	605.9	Tesla P100	Pascal	2016	[3]
4.087	878.6	RTX 2070 Super	Turing	2019	[5]

Lesson 6: Encryption Performance of AES on GPUs

EURO²

Speed Record of AES-CTR

- Very recently Lee et al. [6] achieved 1623 Gbps on an RTX 3080 using a bitsliced implementation
- Recall that we achieved 878.6 Gbps on an RTX 2070 Super

GPU	Cores	Clock Rate	CC	Architecture
RTX 2070 Super	2560	1770 MHz	7.5	Turing
RTX 3080	8704	1710 MHz	8.6	Ampere
RTX 4090	16384	2550 MHz	8.9	Ada Lovelace

- Our codes achieves 4215 Gbps on an RTX 4090

References

[1] A. A. Abdelrahman, M. M. Fouad, H. Dahshan, and A. M. Mousa. High performance CUDA AES implementation: A quantitative performance analysis approach. In 2017 Computing Conference, pages 1077-1085, 2017

[2] S. An and S. C. Seo. Highly efficient implementation of block ciphers on graphic processing units for massively large data. Applied Sciences, 10(11), 2020

[3] N. Nishikawa, H. Amano, and K. Iwai. Implementation of bitsliced AES encryption on CUDA-enabled GPU. In Network and System Security (NSS 2017), LNCS 10394, pages 273-287, 2017

[4] K. D. Akdemir, M. Dixon, W. K. Feghali, P. Fay, V. Gopal, J. Guilford, E. Ozturk, G. Wolrich, and R. Zohar. Breakthrough AES performance with INTEL AES new instructions. 2010

[5] C. Tezcan. Optimization of advanced encryption standard on graphics processing units. IEEE Access, 9:67315–67326, 2021

[6] W. -K. Lee, S. C. Seo, H. Seo, D. C. Kim and S. O. Hwang, "Speed Record of AES-CTR and AES-ECB Bit-Sliced Implementation on GPUs," in IEEE Embedded Systems Letters, vol. 16, no. 4, pp. 481-484, Dec. 2024

Thanks

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101101903. The JU receives support from the Digital Europe Programme and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Türkiye, Republic of North Macedonia, Iceland, Montenegro, Serbia