Benchmarking of Round 3 CAESAR Candidates in Hardware:

Appendix – New Implementations of AES-OTR, CLOC, & SILC

Ekawat Homsirikamol,
Farnoud Farahmand,
William Diehl,
and Kris Gaj
George Mason University
USA

http://cryptography.gmu.edu
https://cryptography.gmu.edu/athena

Background

- On **October 6, 2017**, Kazuhiko Minematsu submitted the **refined hardware implementations of AES-OTR** to the crypto-competitions@googlegroups.com
- These new implementations were based on **novel unrolled hardware architectures of aes128otrpv3 and aes128otrcv3** defined in the AES-OTR specification v3.5
- On **November 11, 2017**, the **corresponding optimized results** were added to the ATHENa database of results at
  https://cryptography.gmu.edu/athenadb/fpga_auth_cipher/rankings_view
  https://cryptography.gmu.edu/athenadb/fpga_auth_cipher/table_view

Background (cont.)

- On **November 11, 2017**, the following additional results were added to the ATHENa database of results at

  https://cryptography.gmu.edu/athenadb/fpga_auth_cipher/rankings_view
  https://cryptography.gmu.edu/athenadb/fpga_auth_cipher/table_view

  Virtex 6 and Virtex 7 results for
  - **present80n6t4silcv3**
  - **led80n6t4silcv3**
  - **twine80n6t4clocv3**

Contents & Convention

- In the following slides, we describe the **influence of the new results on ranking of Round 3 CAESAR Candidates compared to the GMU Report from August 28, 2017**

- For each page of the report influenced by the new submission, we provide the original version, as of August 28, 2017, marked

ORIGINAL

and the revised version, based on the status of the ATHENa database as of November 11, 2017, marked

REVISED

Architectures

ORIGINAL

- Majority of algorithms have designs based on

  Basic Iterative Architecture (One Round per Clock Cycle)

Exceptions:

ACORN (NTU):	8bit & 32bit lightweight
AEGIS (NTU):	Folded /8v
AES-OTR (NEC):	Unrolled x2
COLM (CINVESTAV-IPN):	Quasi-pipelined
Deoxys-I (NTU):	4-stream pipelined
Deoxys-I (GMU):	Basic iterative with speculative pre-computation
JAMBU-SIMON:	Unrolled x4

Architectures

REVISED

- Majority of algorithms have designs based on

  Basic Iterative Architecture (One Round per Clock Cycle)

Exceptions:

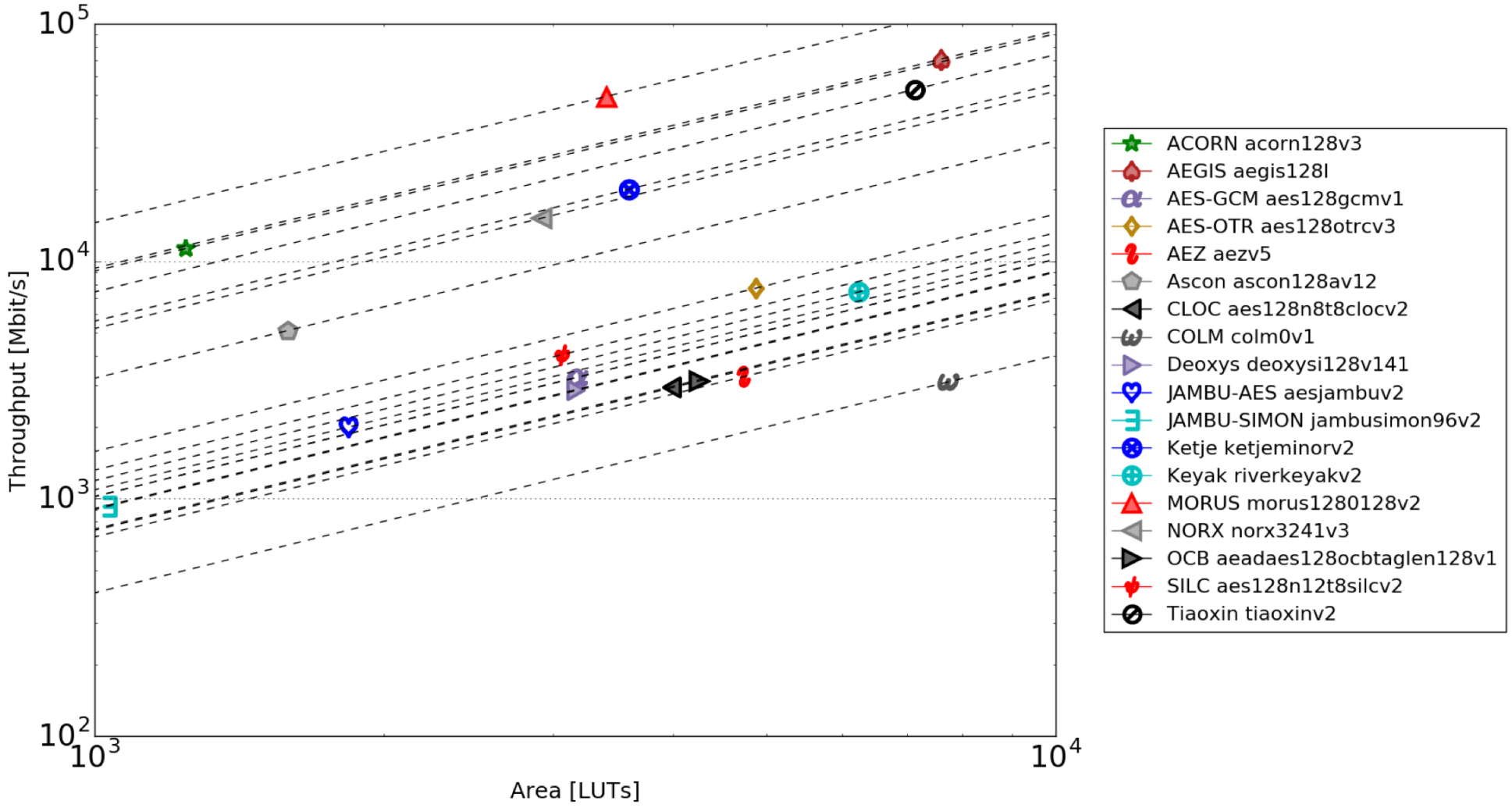
ACORN (NTU):	8bit & 32bit lightweight
AEGIS (NTU):	Folded /8v
AES-OTR (NEC):	**Unrolled x2, x4, x6 (Dual, Quad, Hexa)**
COLM (CINVESTAV-IPN):	Quasi-pipelined
Deoxys-I (NTU):	4-stream pipelined
Deoxys-I (GMU):	Basic iterative with speculative pre-computation
JAMBU-SIMON:	Unrolled x4

All Use Cases

Virtex-6

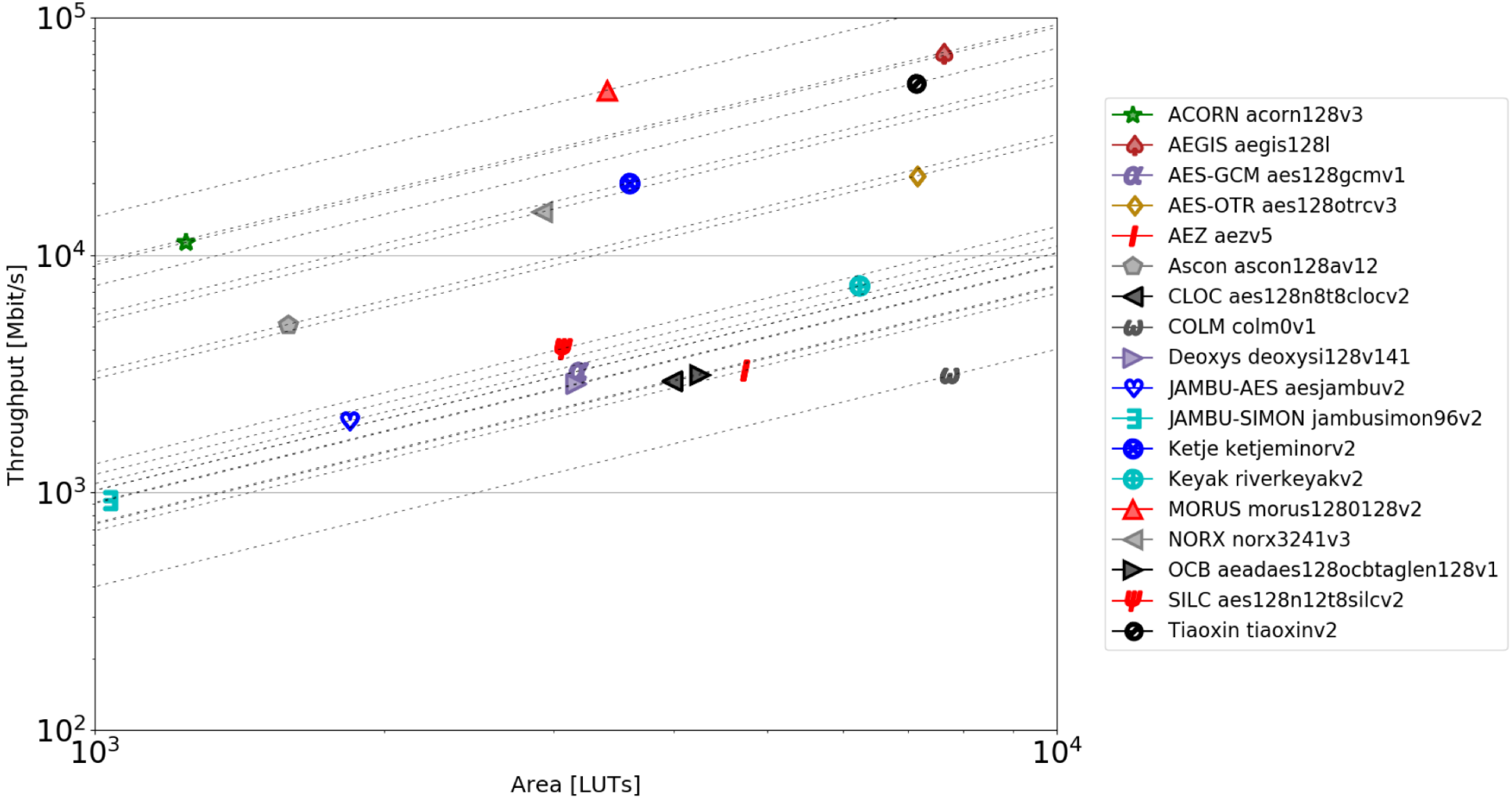
Results for Virtex-6 – Throughput vs. Area Logarithmic Scale

ORIGINAL

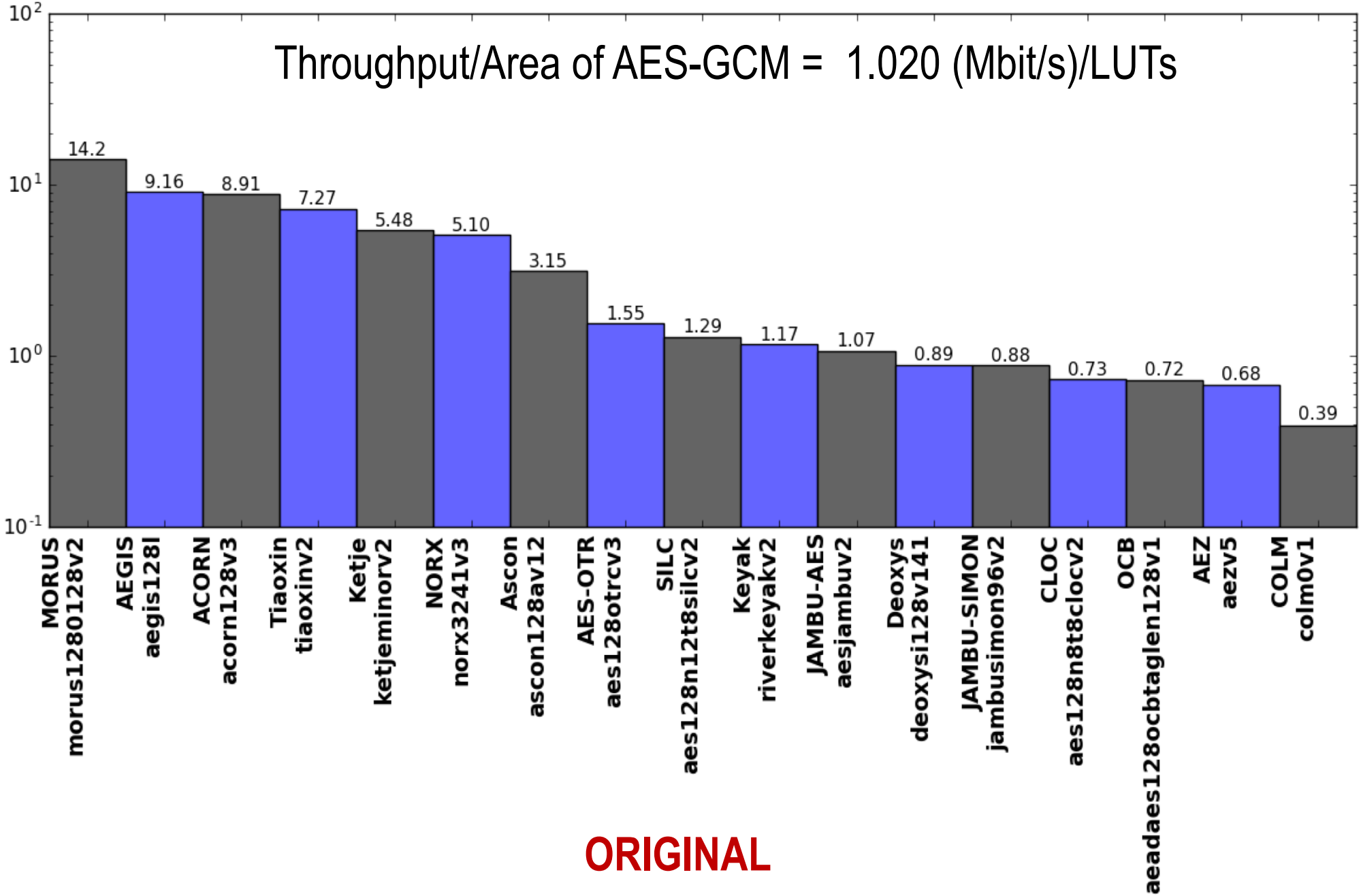


Results for Virtex-6 – Throughput vs. Area Logarithmic Scale

REVISED

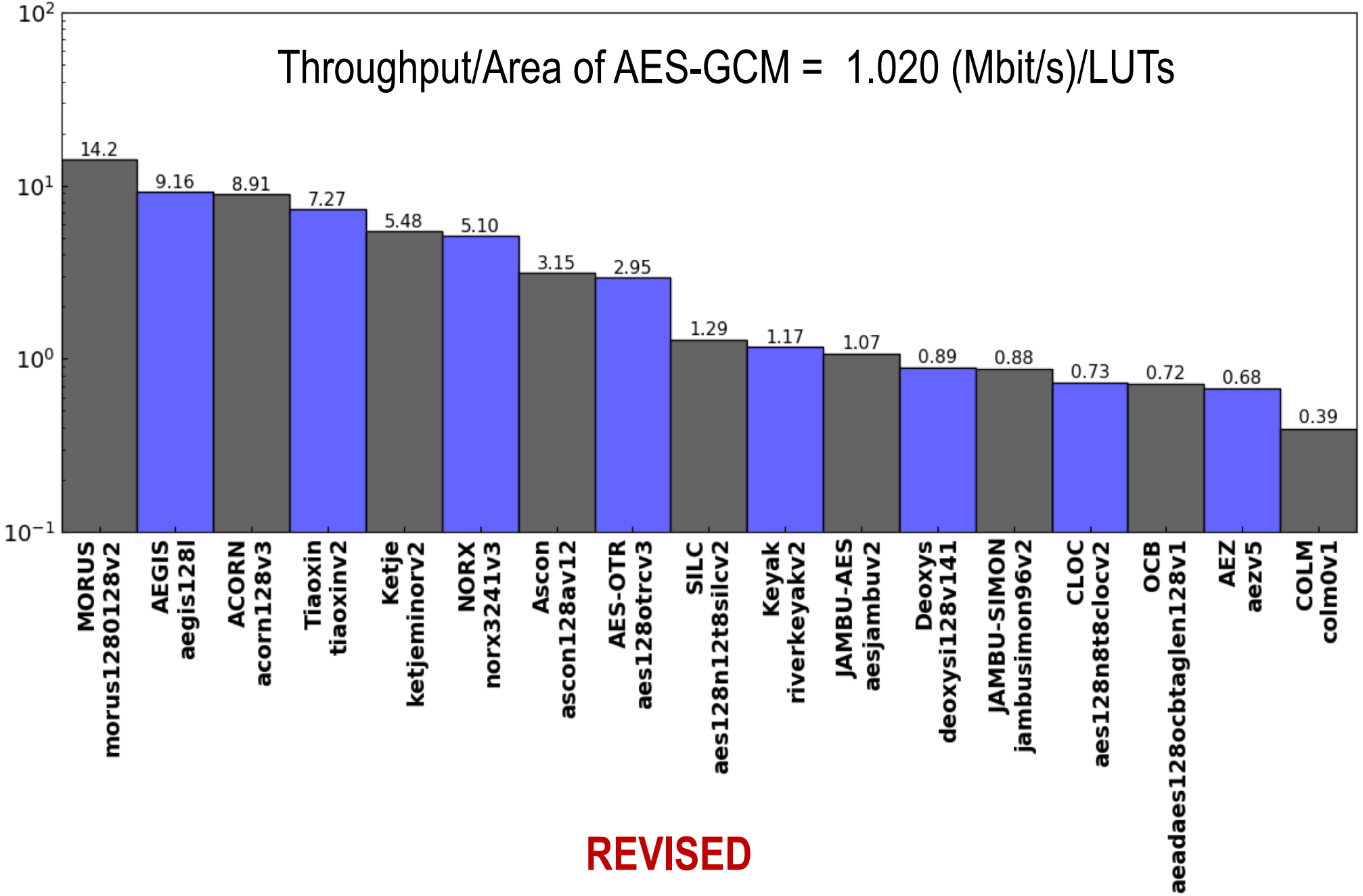


Relative Throughput/Area in Virtex-6 vs. AES-GCM



ORIGINAL

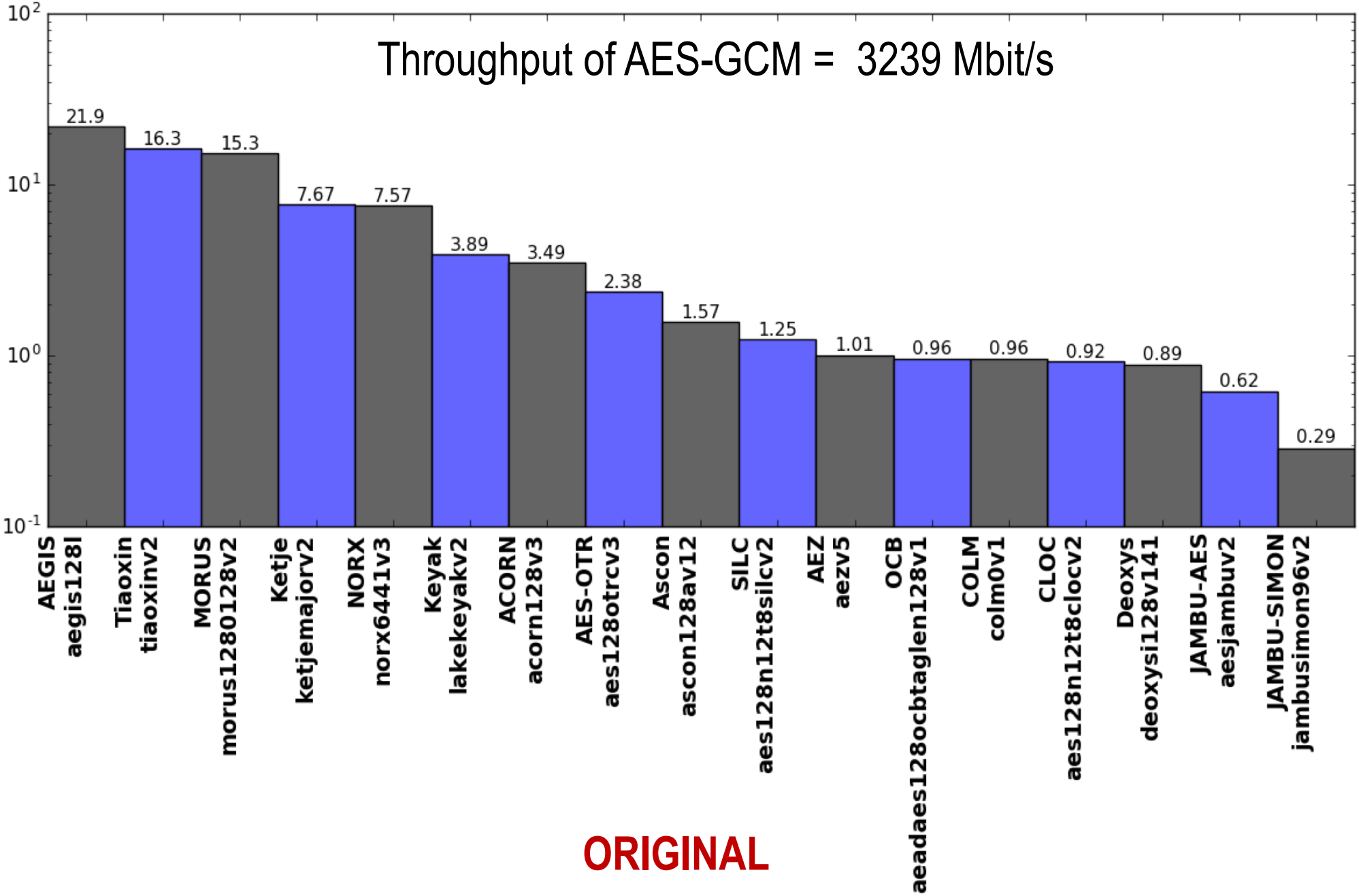
Relative Throughput/Area in Virtex-6 vs. AES-GCM



REVISED

Relative Throughput in Virtex-6

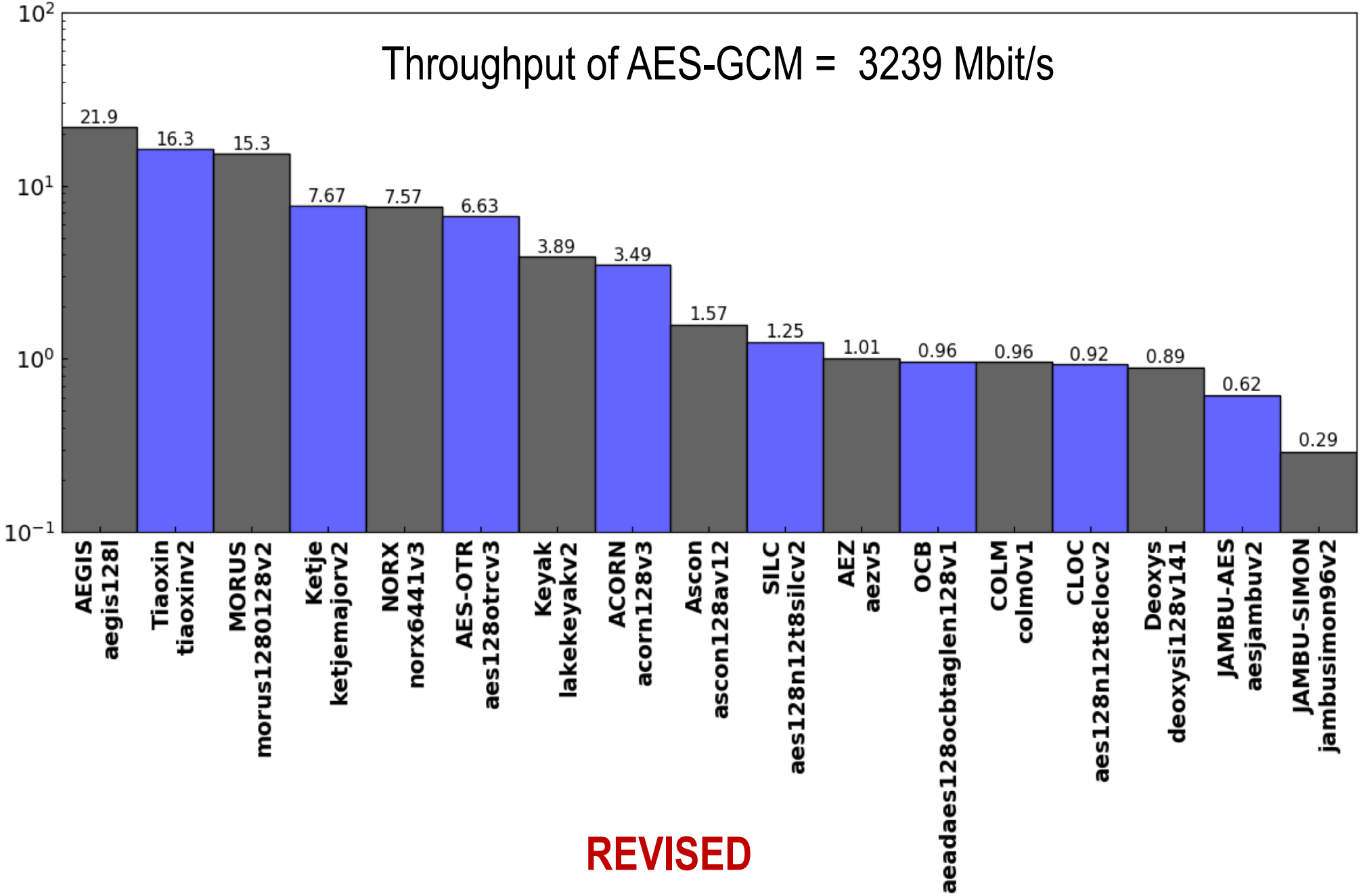
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

Relative Throughput in Virtex-6

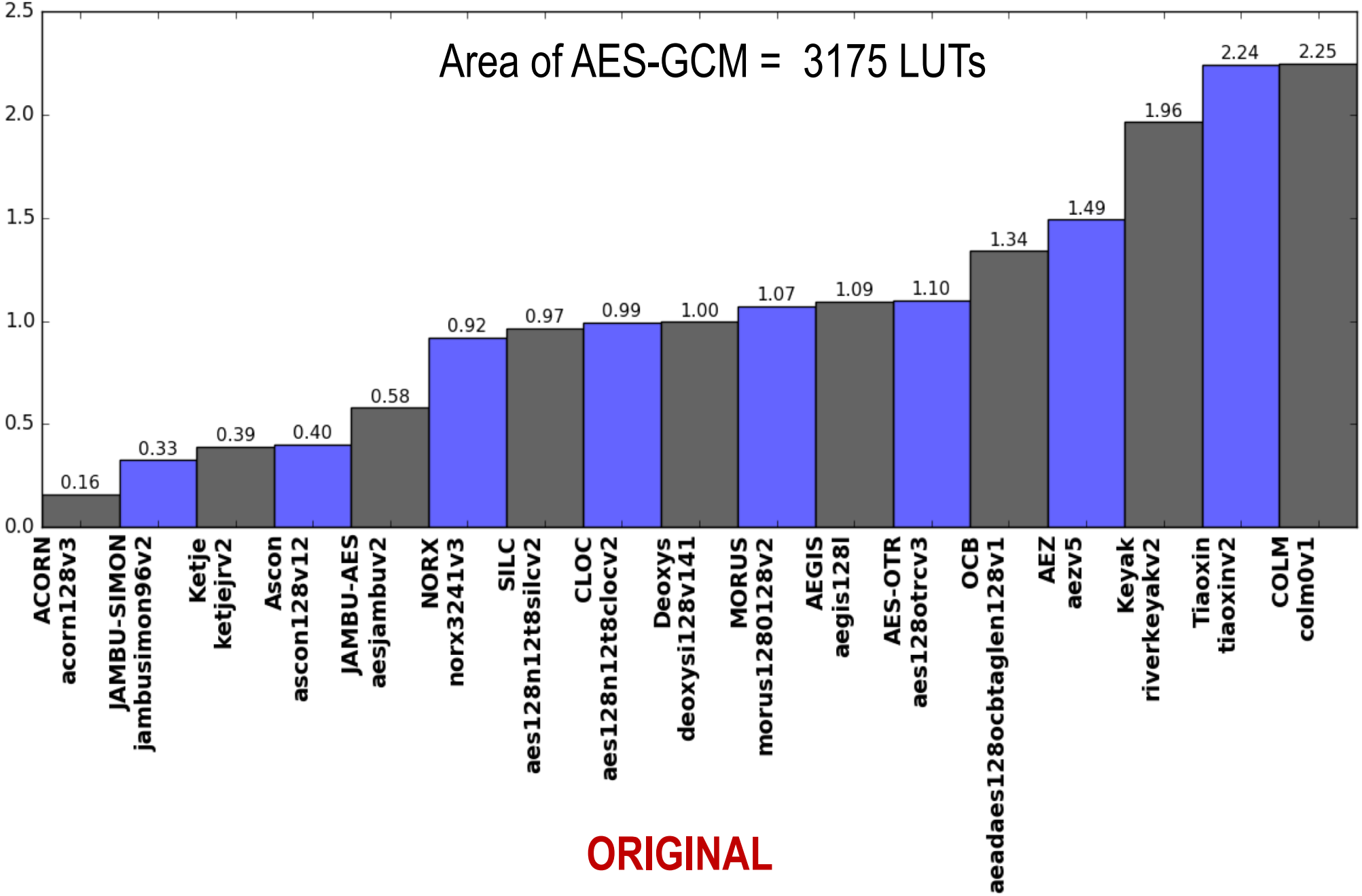
Ratio of a given Cipher Throughput/Throughput of AES-GCM



REVISED

Relative Area (#LUTs) in Virtex-6

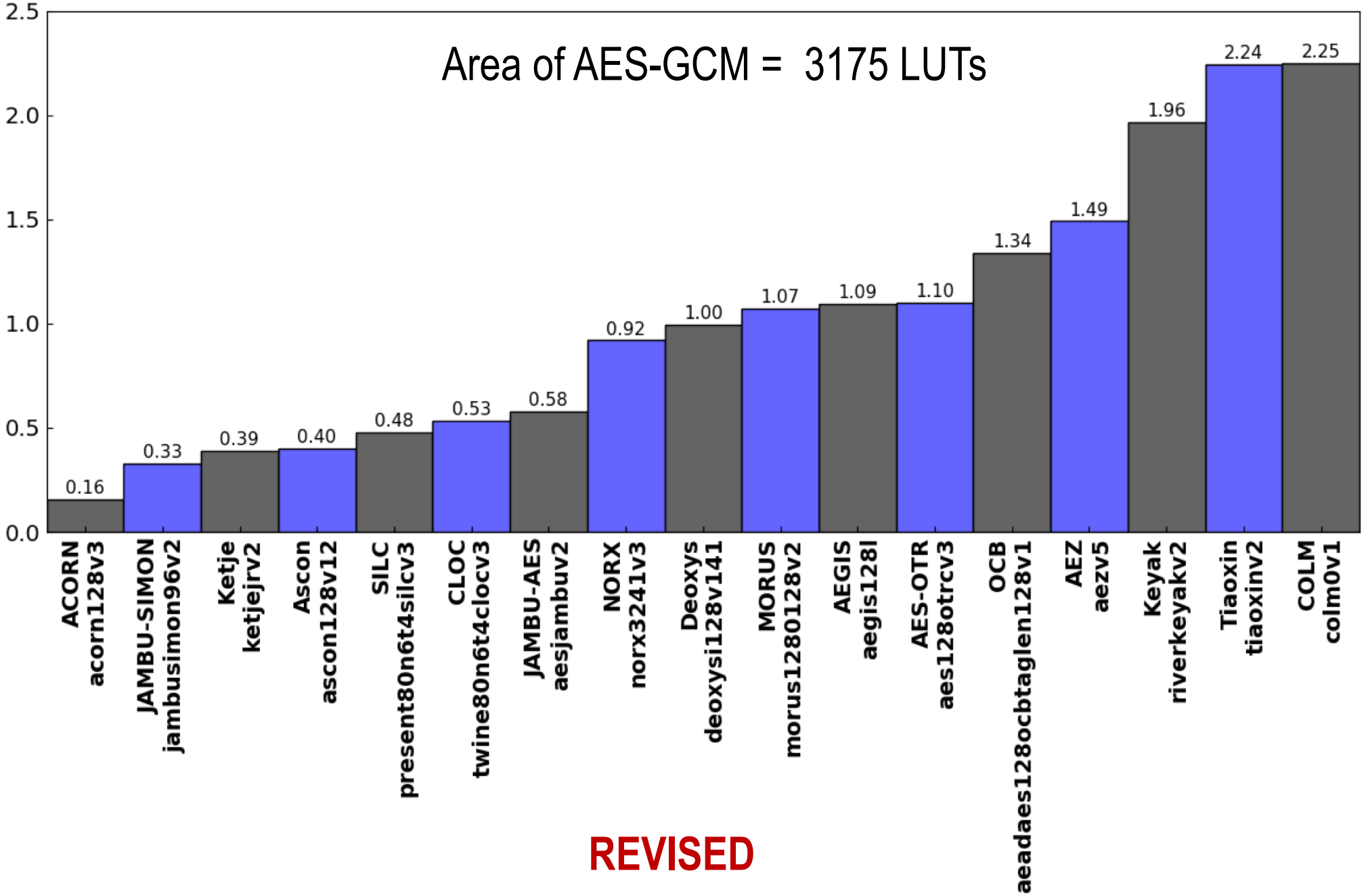
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#LUTs) in Virtex-6

Ratio of a given Cipher Area/Area of AES-GCM

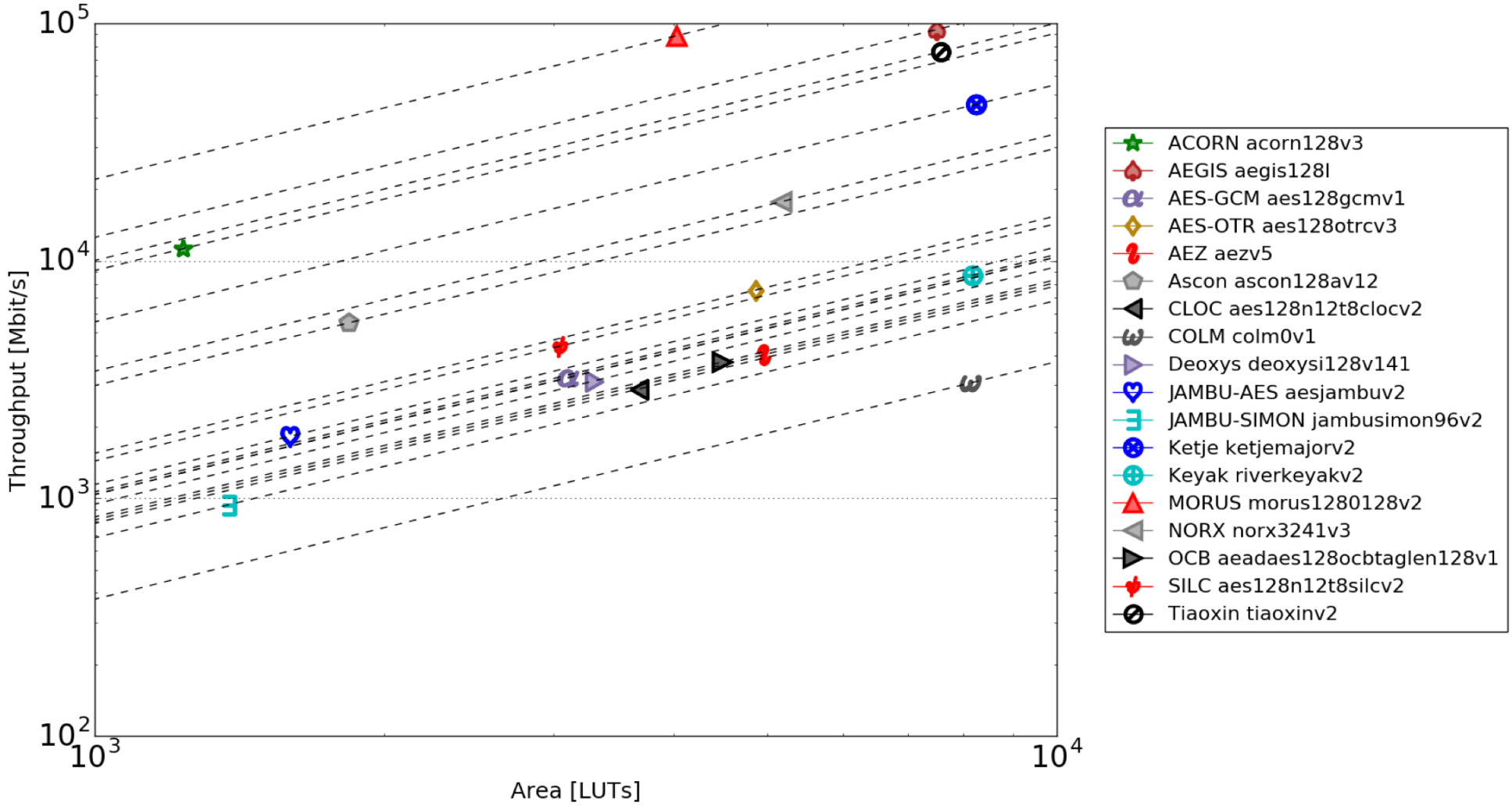


REVISED

Virtex-7

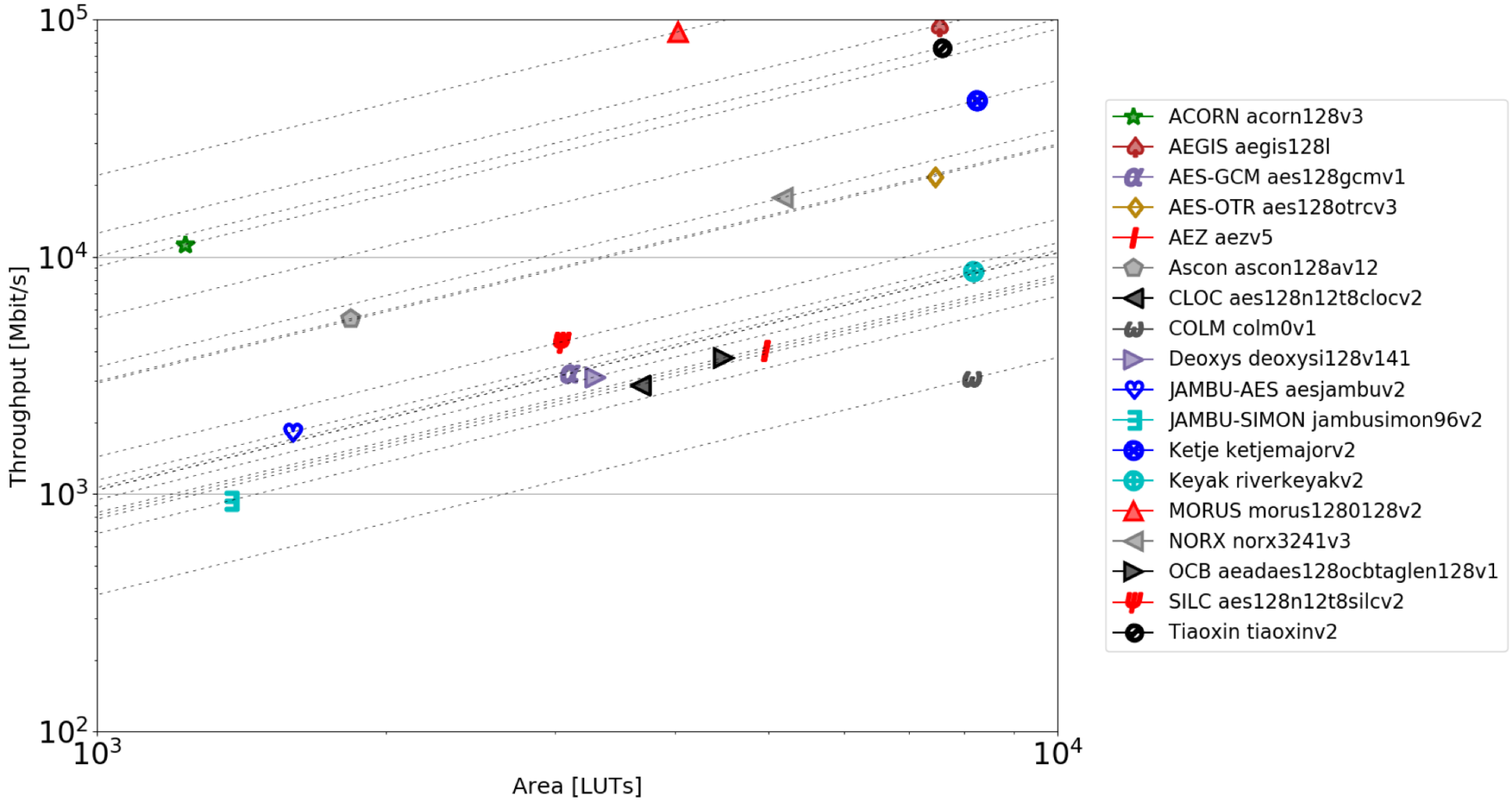
Results for Virtex-7 – Throughput vs. Area Logarithmic Scale

ORIGINAL

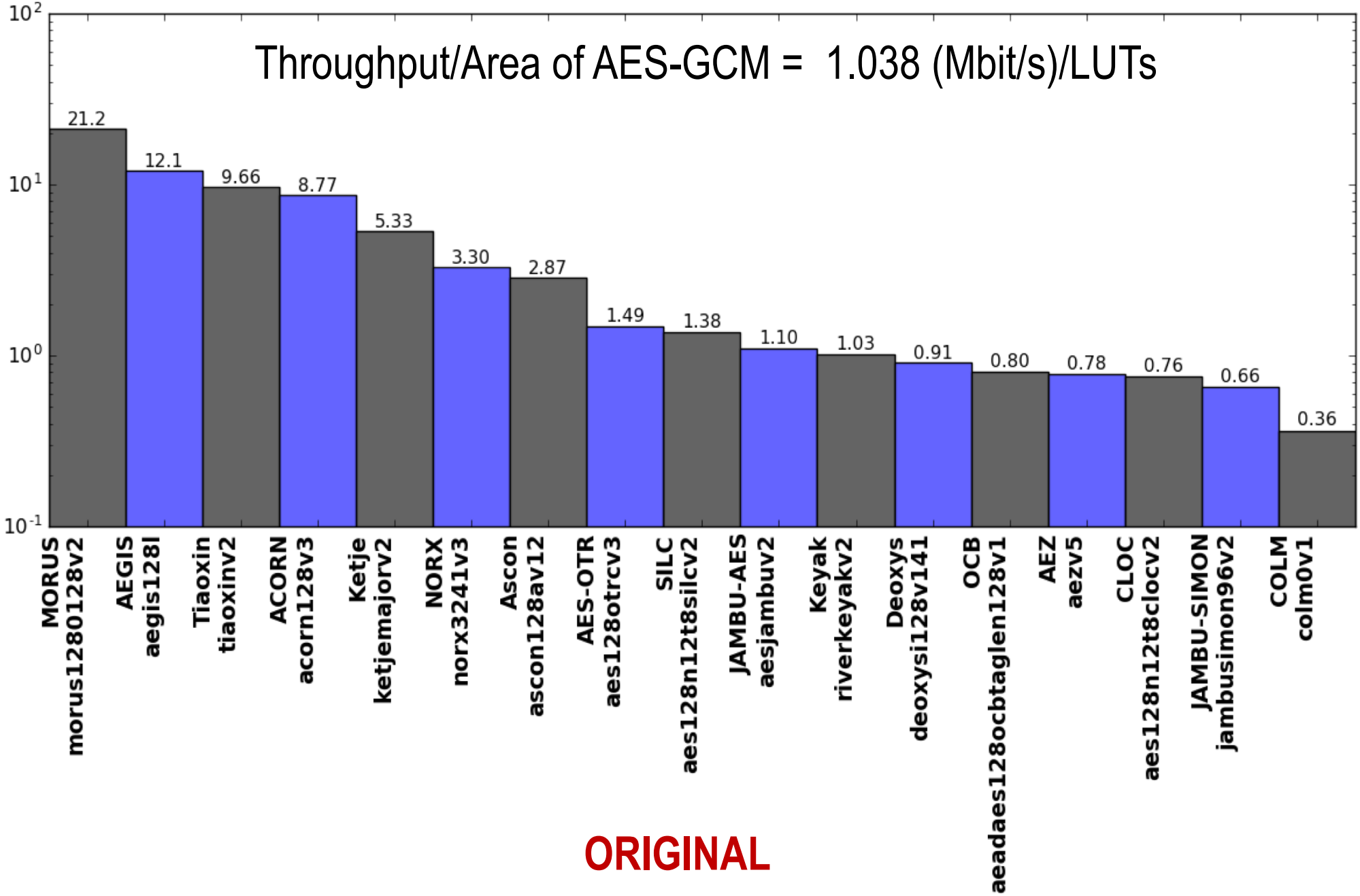


Results for Virtex-7 – Throughput vs. Area Logarithmic Scale

REVISED

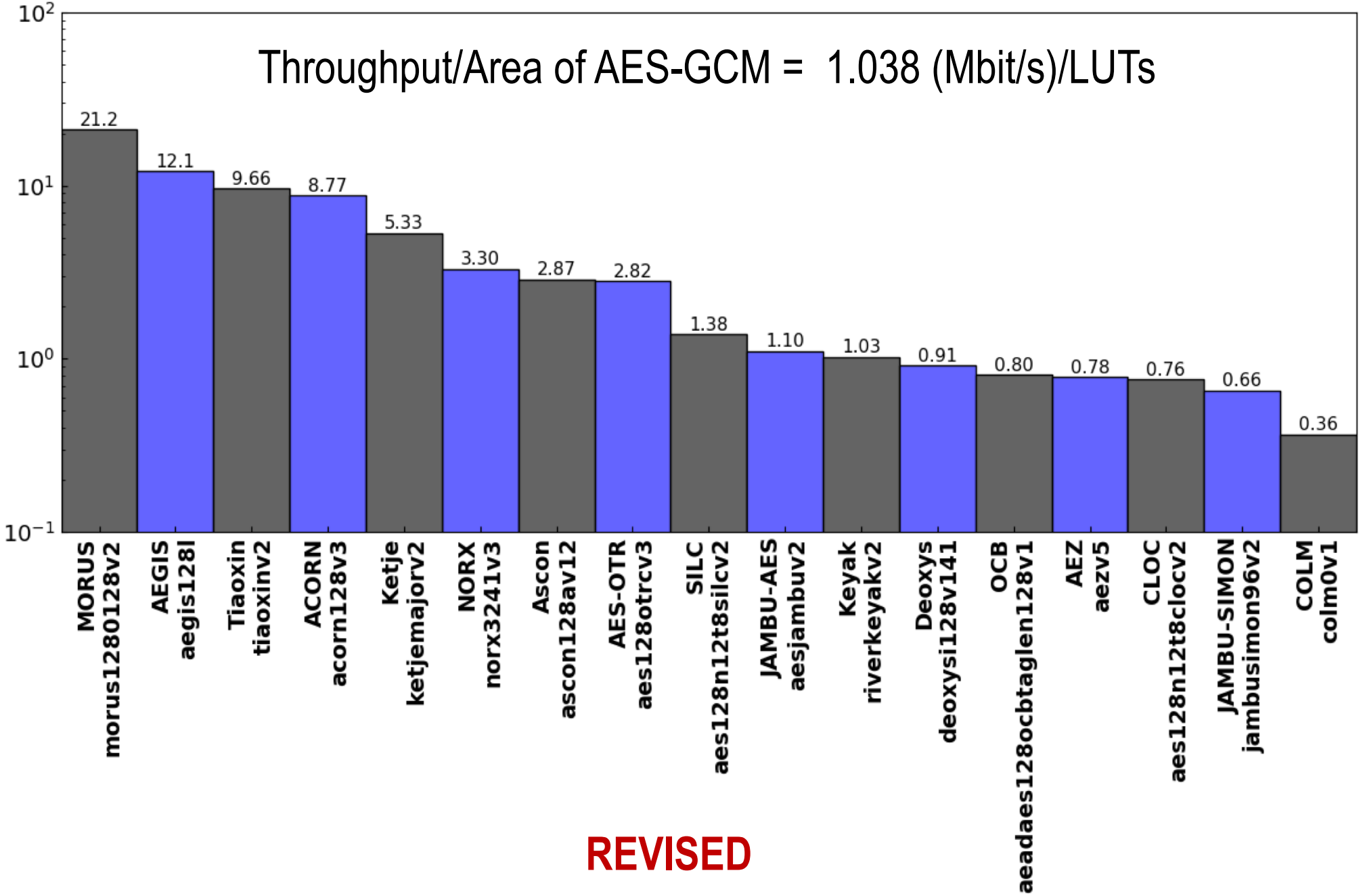


Relative Throughput/Area in Virtex-7 vs. AES-GCM



ORIGINAL

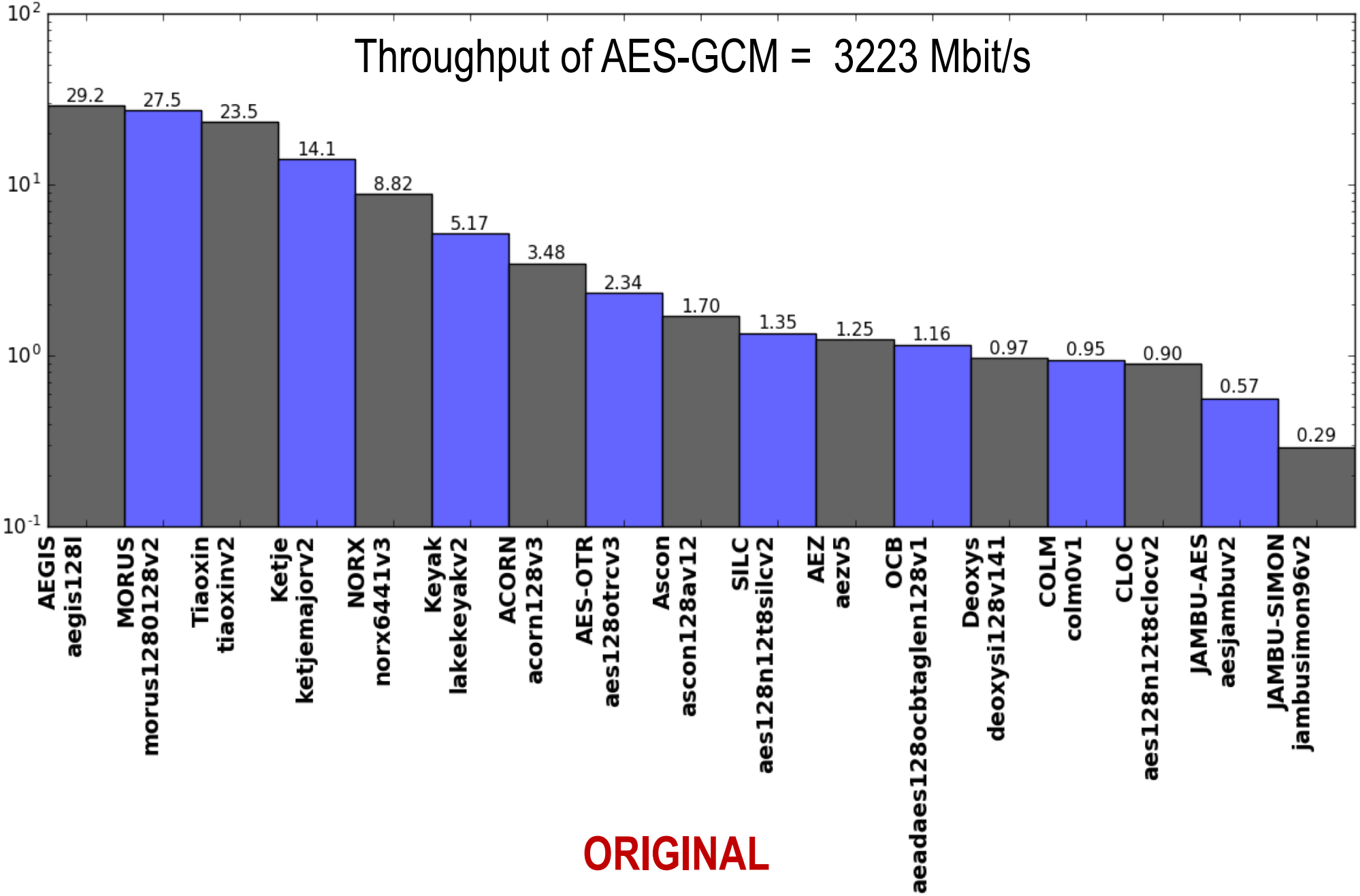
Relative Throughput/Area in Virtex-7 vs. AES-GCM



REVISED

Relative Throughput in Virtex-7

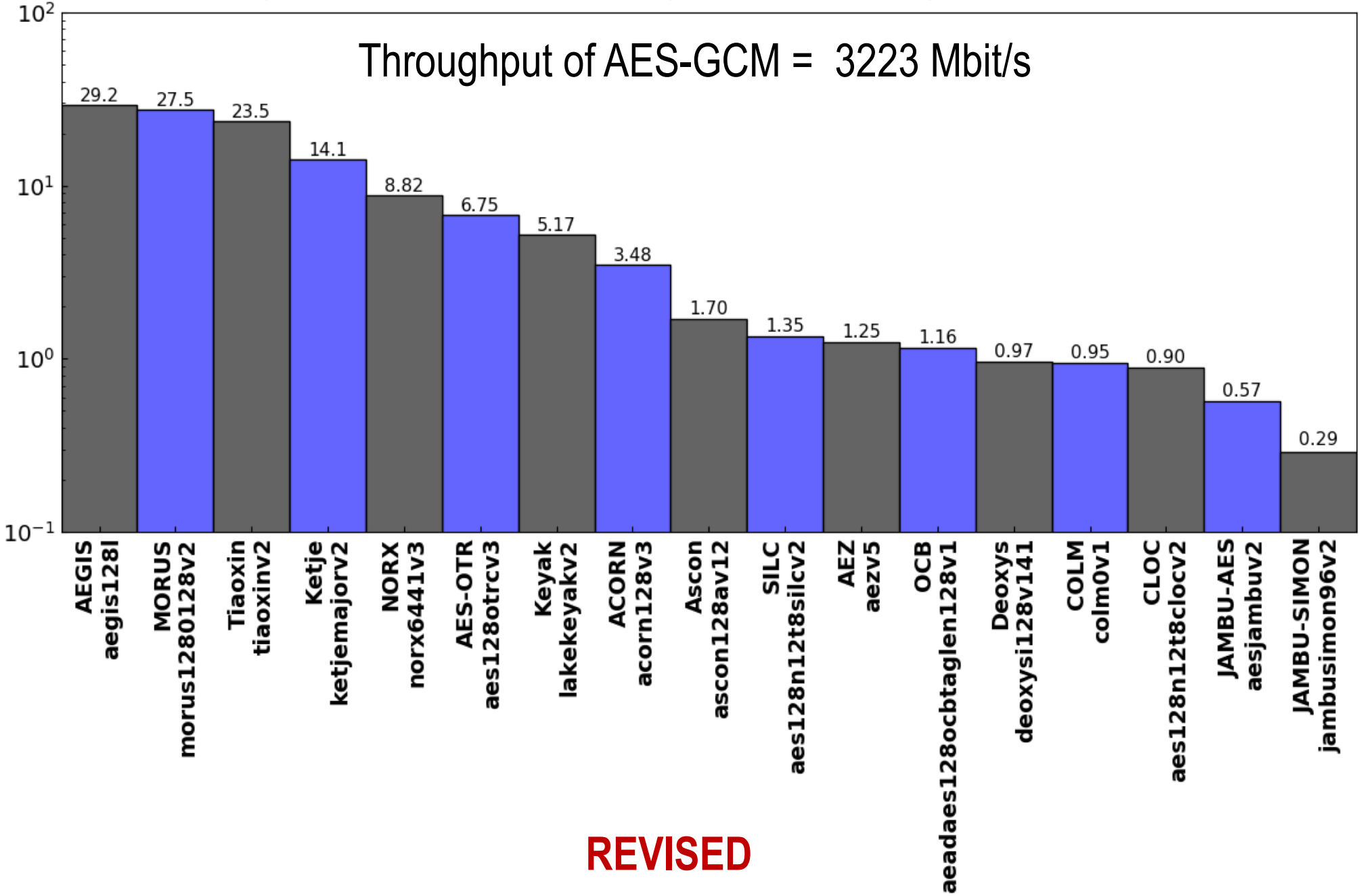
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

Relative Throughput in Virtex-7

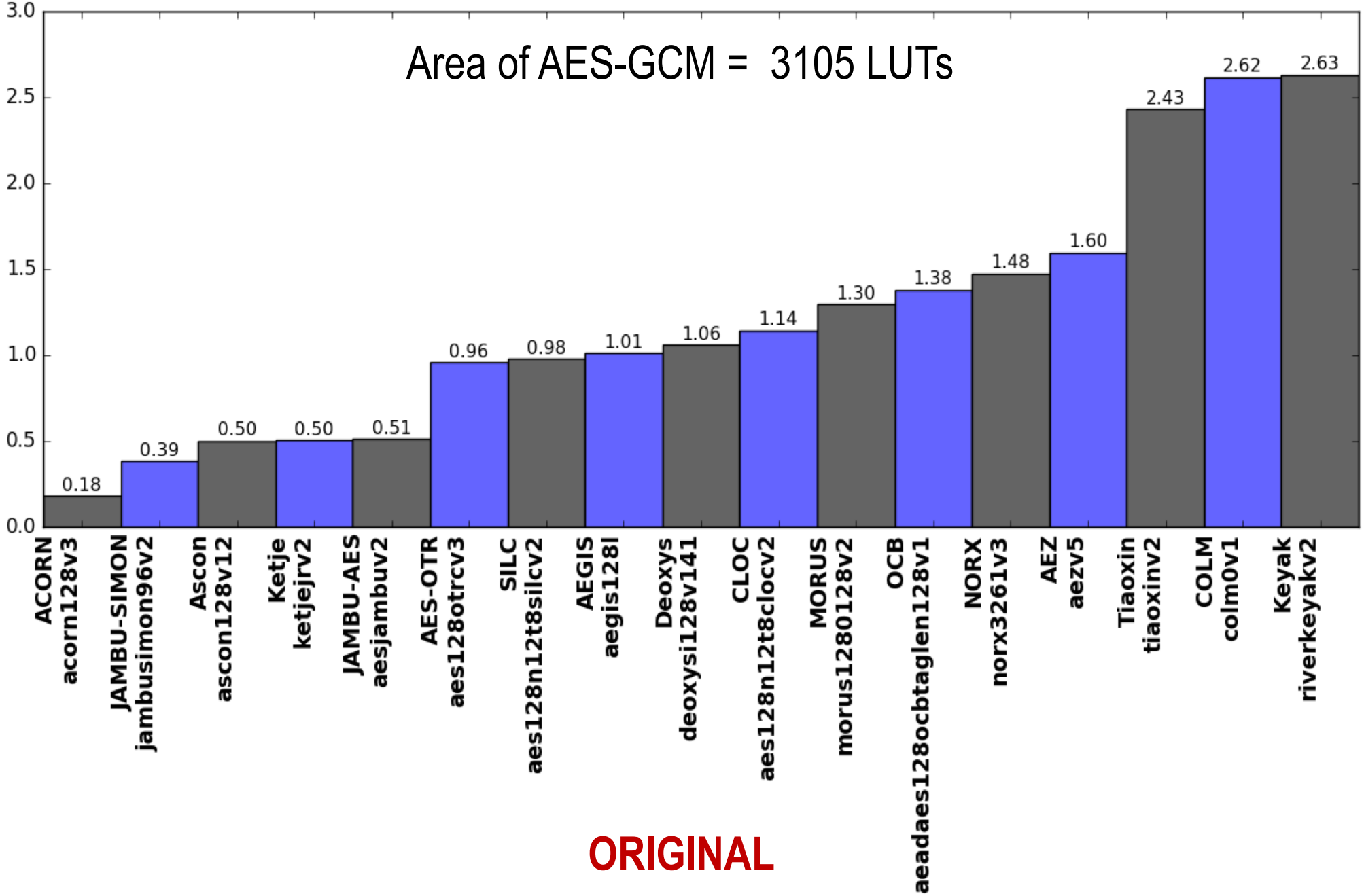
Ratio of a given Cipher Throughput/Throughput of AES-GCM



REVISED

Relative Area (#LUTs) in Virtex-7

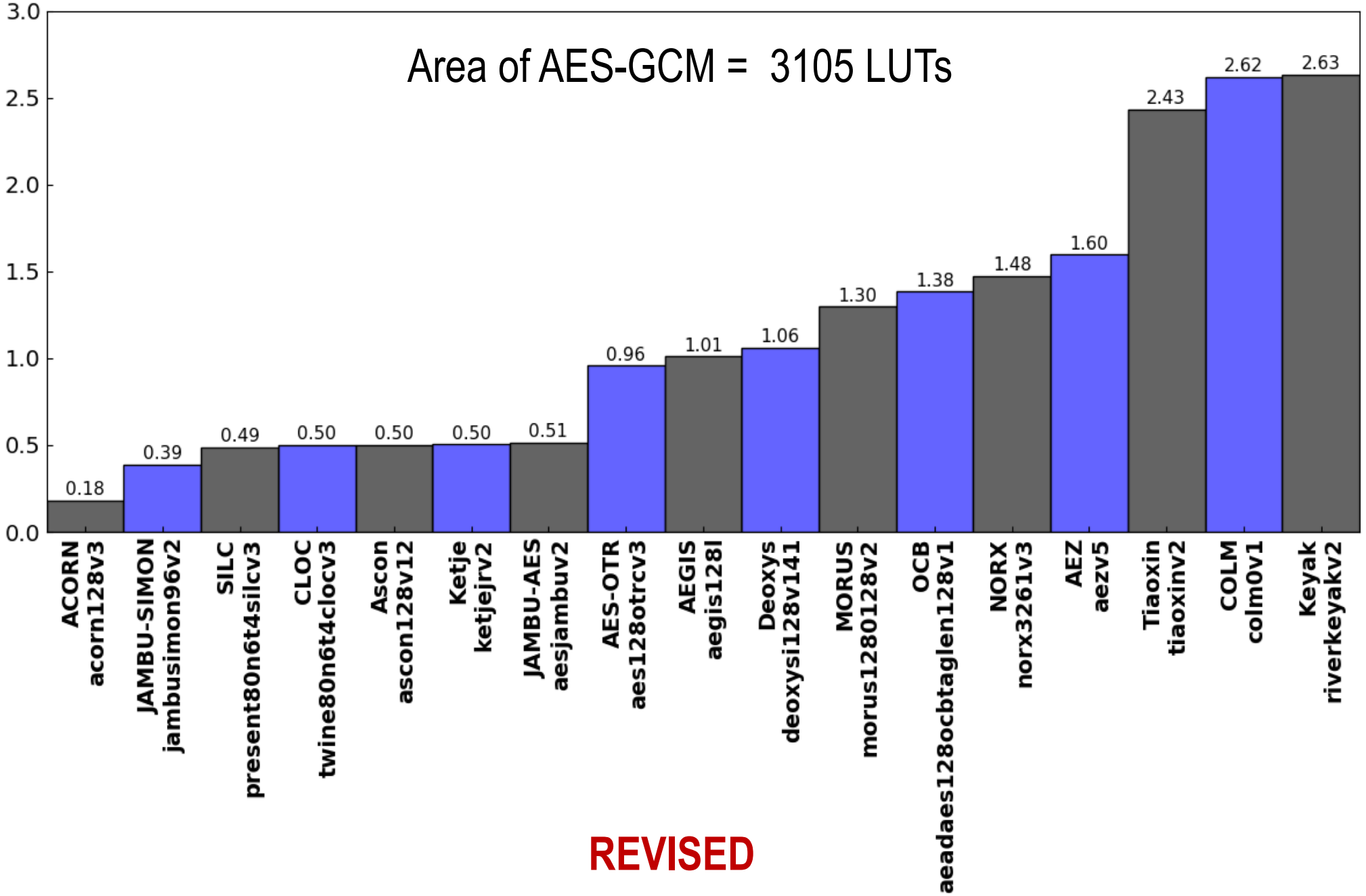
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#LUTs) in Virtex-7

Ratio of a given Cipher Area/Area of AES-GCM

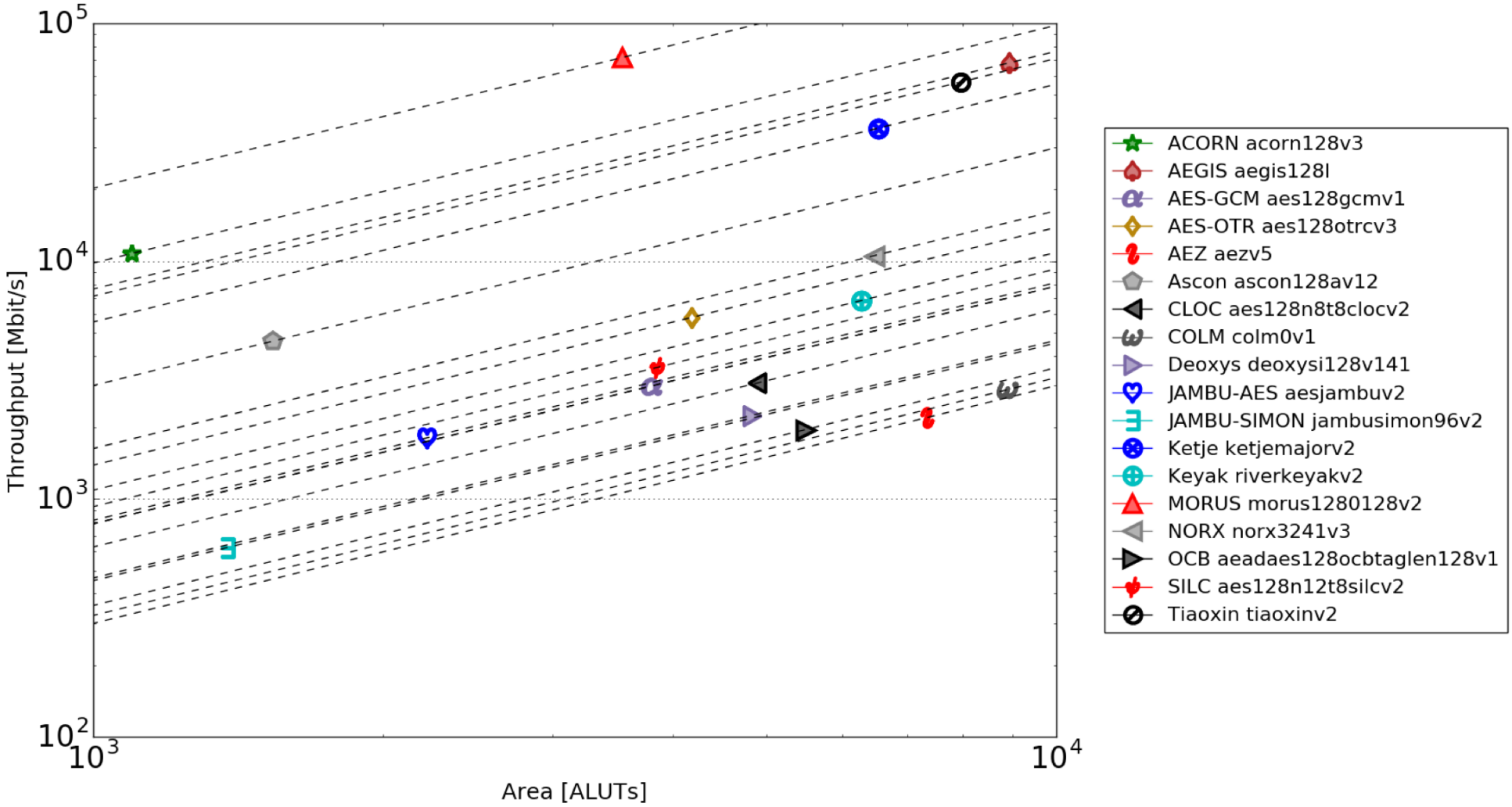


REVISED

Stratix IV

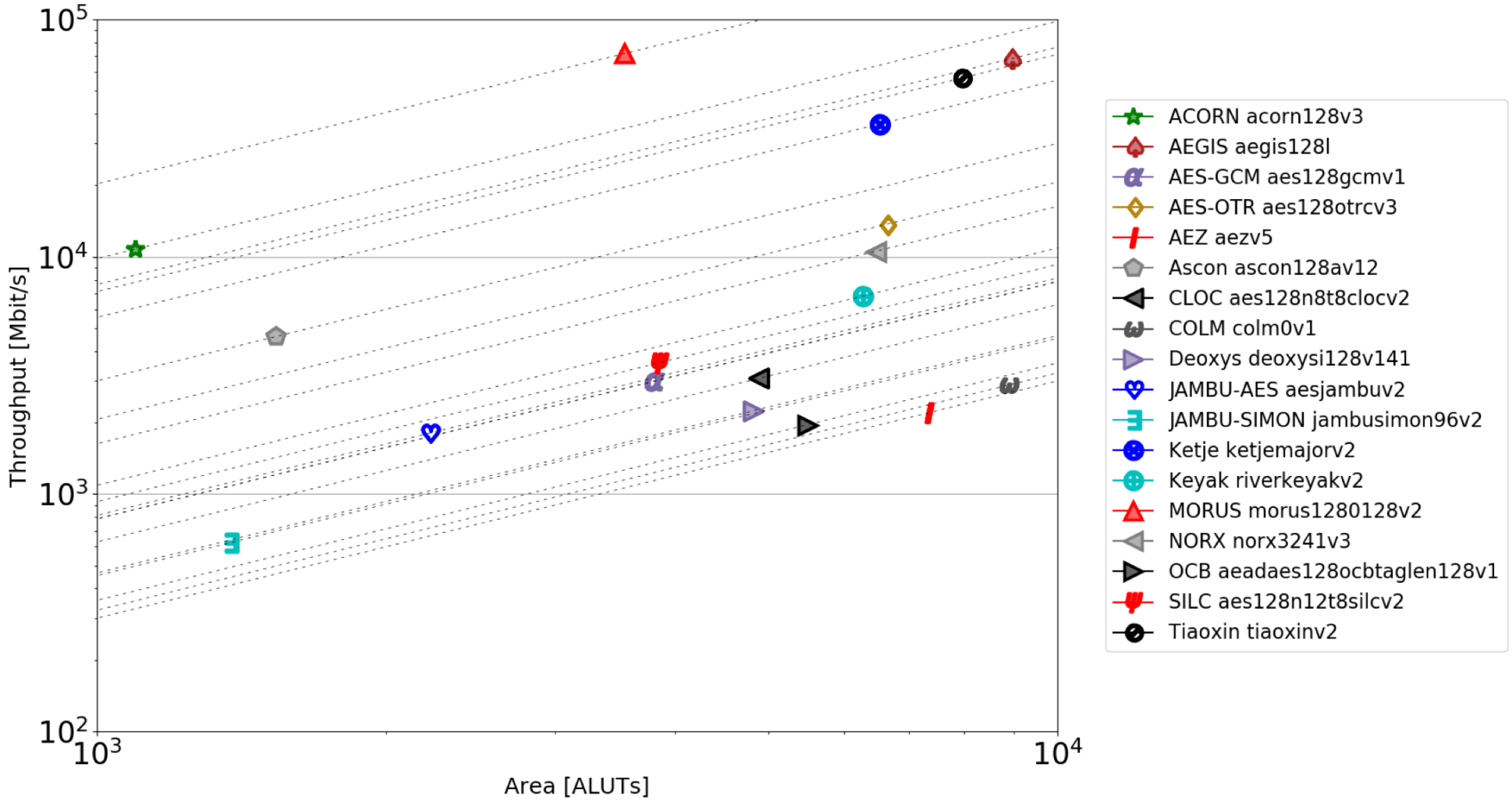
Results for Stratix IV – Throughput vs. Area Logarithmic Scale

ORIGINAL

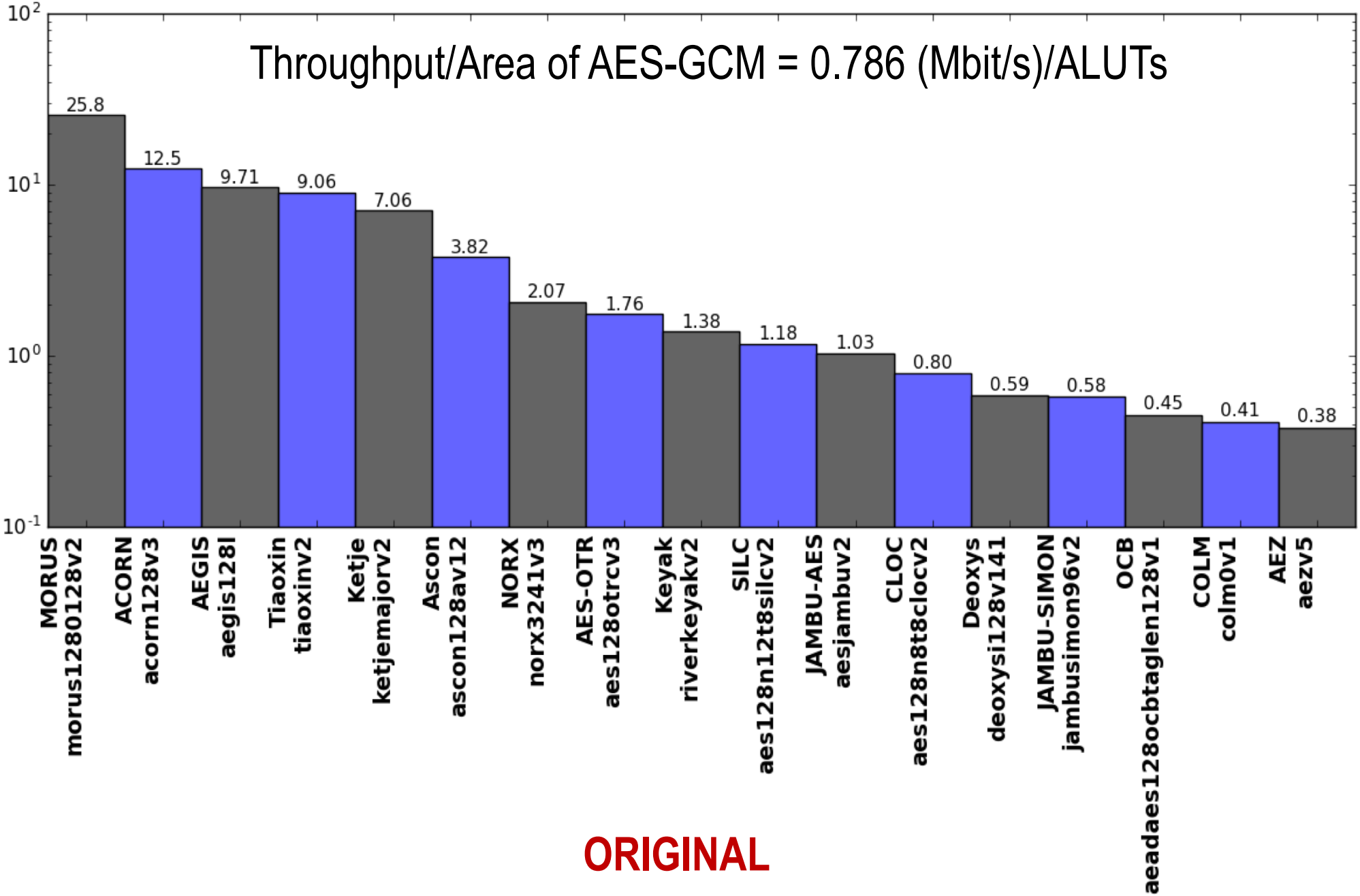


Results for Stratix IV – Throughput vs. Area Logarithmic Scale

REVISED

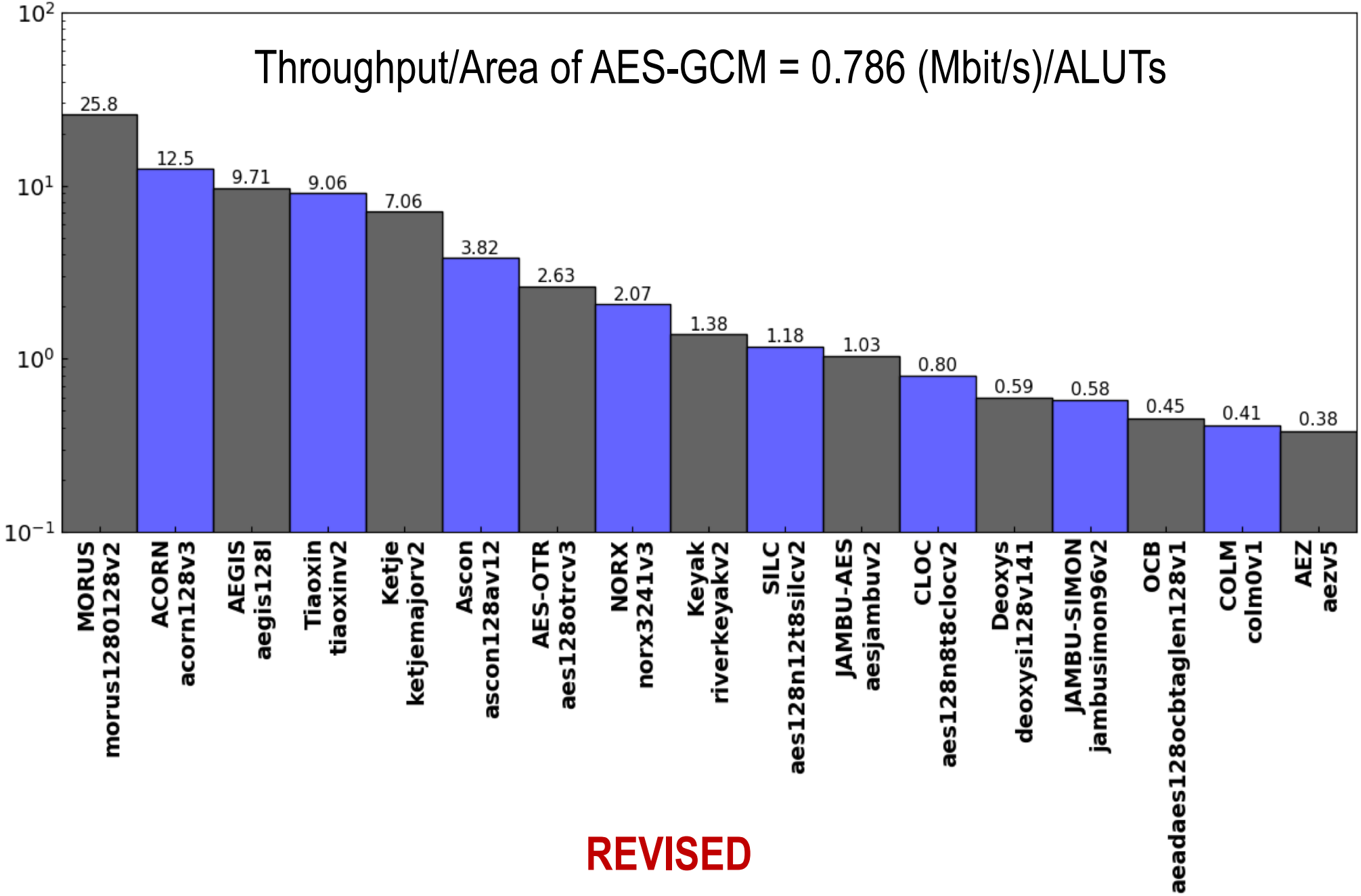


Relative Throughput/Area in Stratix IV vs. AES-GCM



ORIGINAL

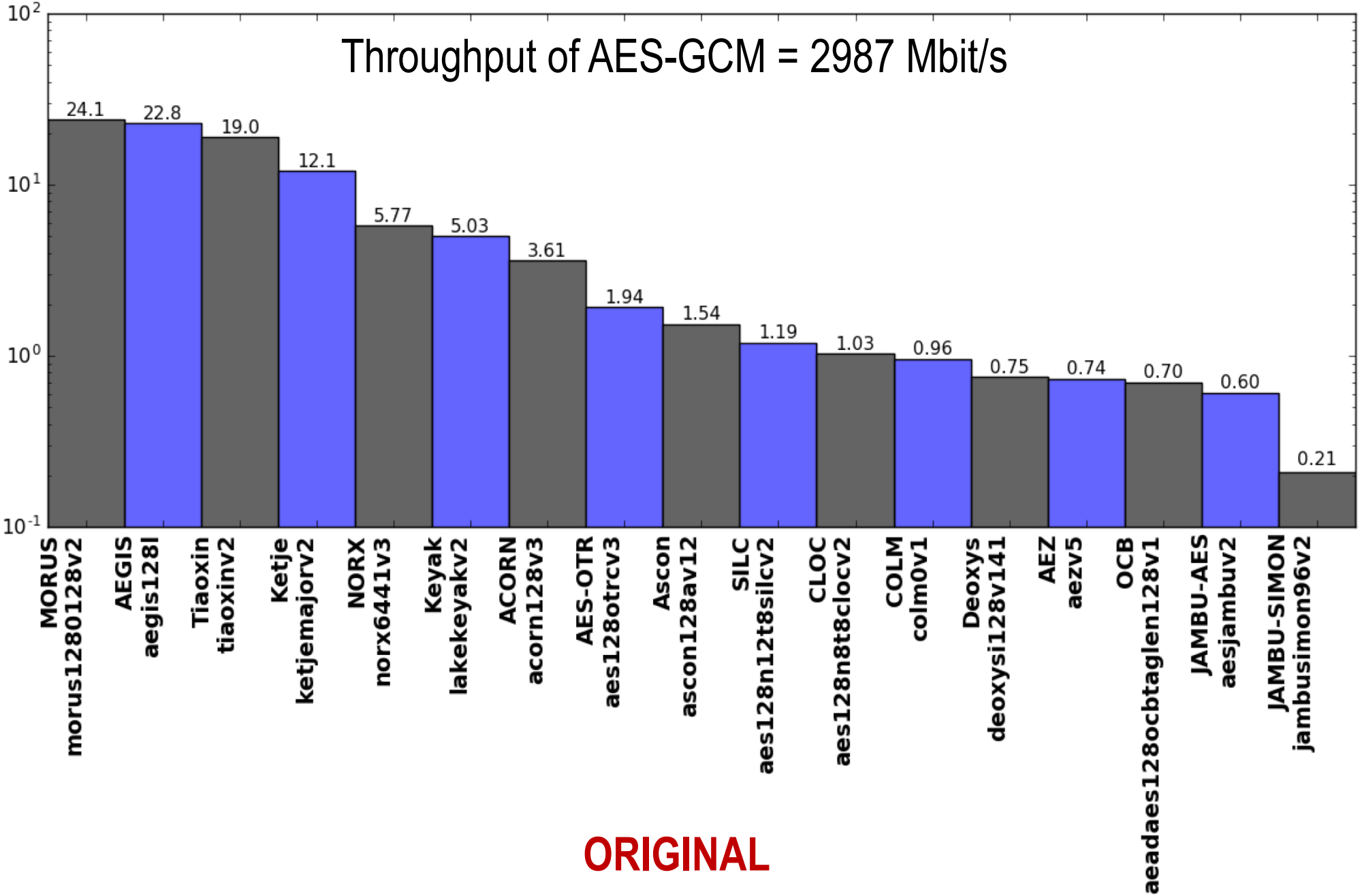
Relative Throughput/Area in Stratix IV vs. AES-GCM



REVISED

Relative Throughput in Stratix IV

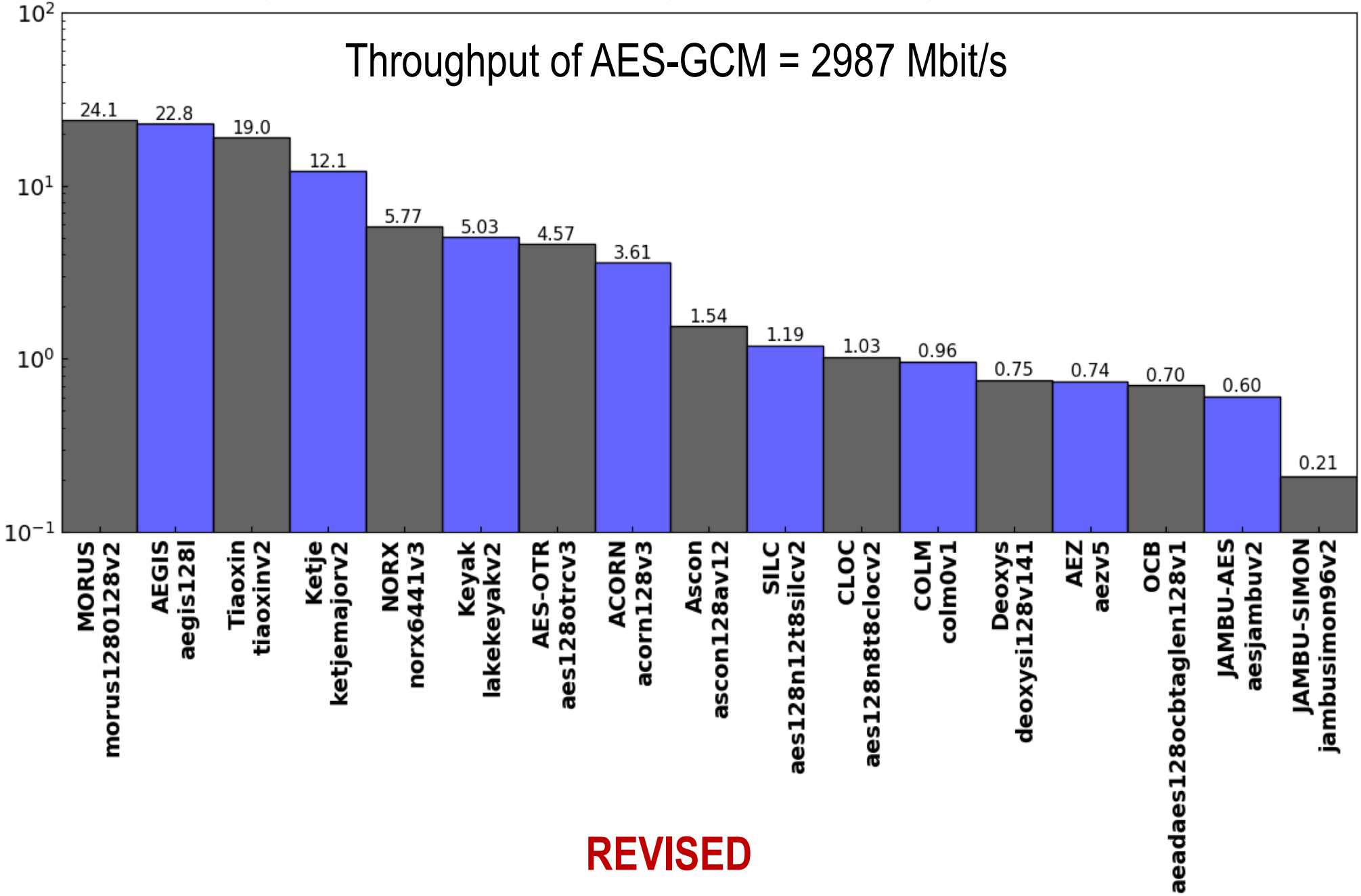
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

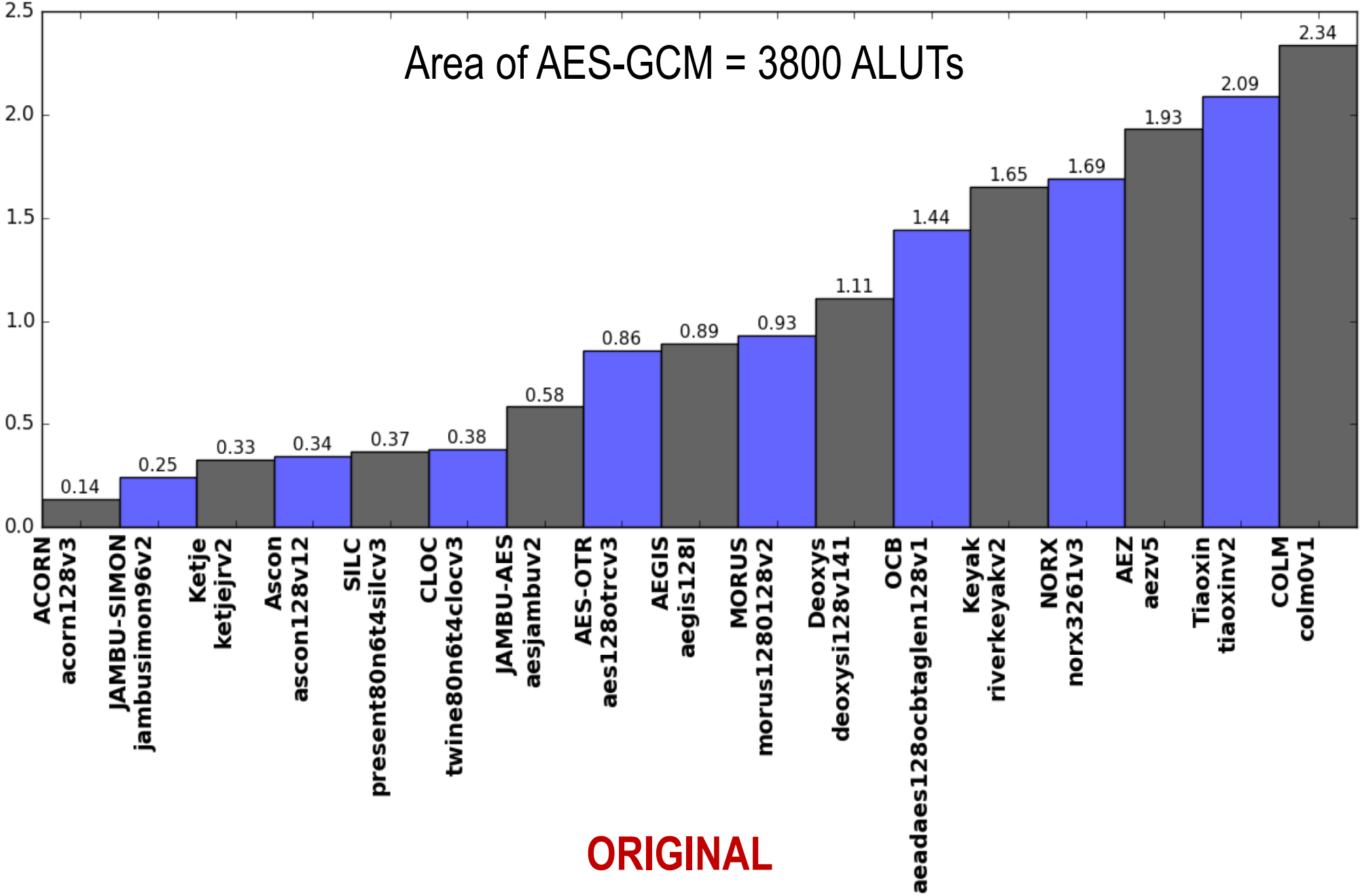
Relative Throughput in Stratix IV

Ratio of a given Cipher Throughput/Throughput of AES-GCM



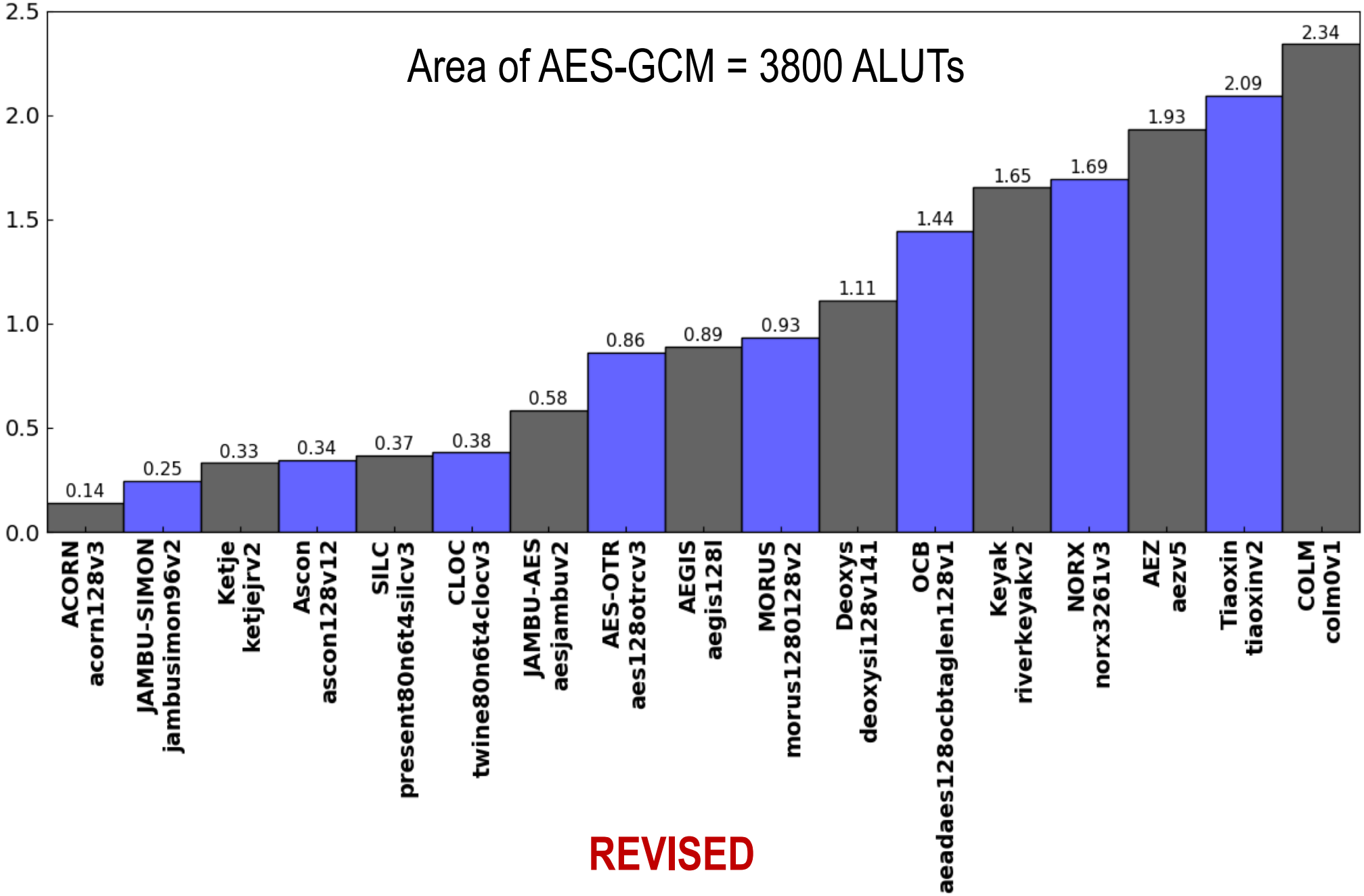
REVISED

Relative Area (#ALUTs) in Stratix IV
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#ALUTs) in Stratix IV
Ratio of a given Cipher Area/Area of AES-GCM

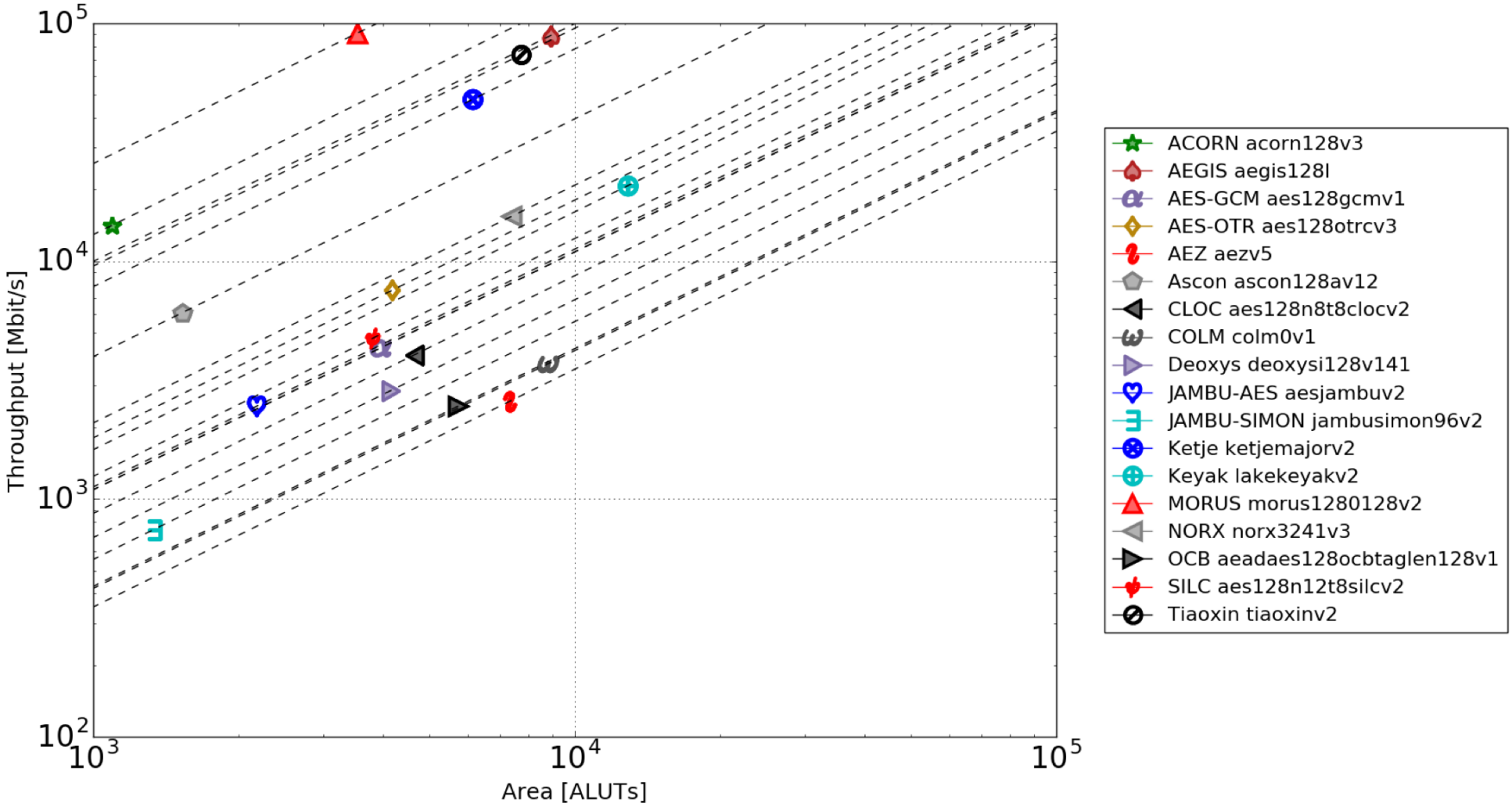


REVISED

Stratix V

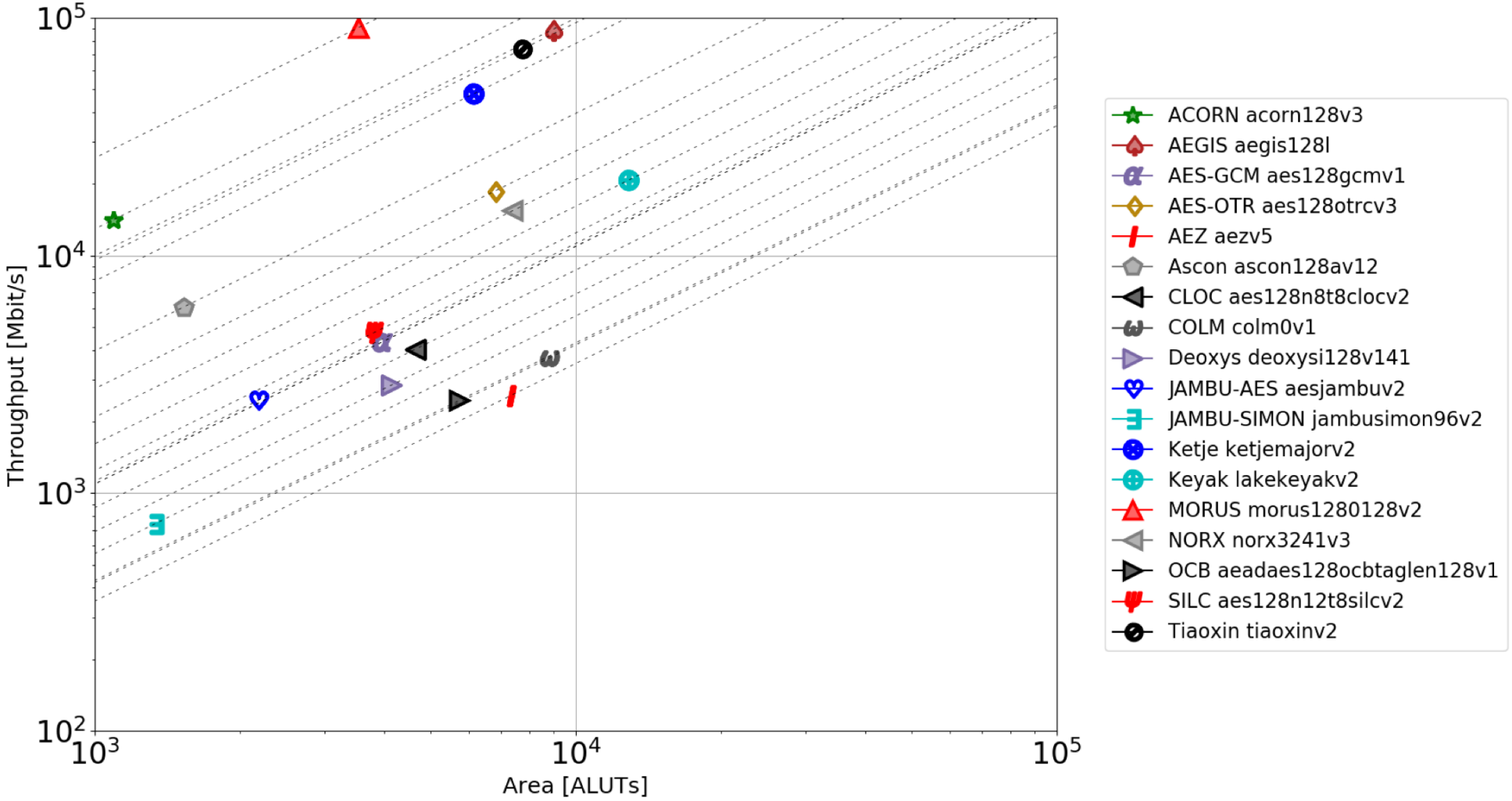
Results for Stratix V – Throughput vs. Area Logarithmic Scale

ORIGINAL

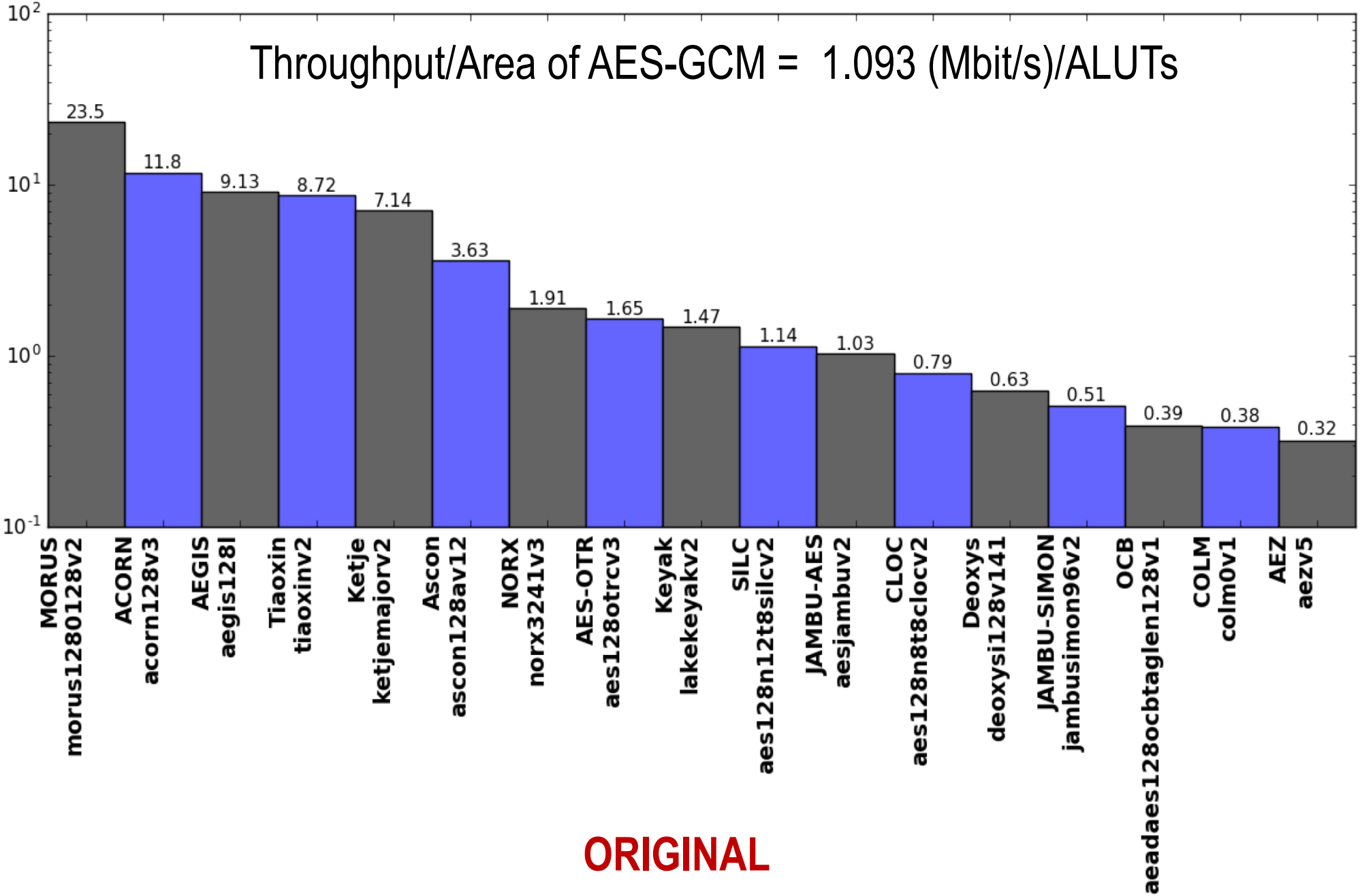


Results for Stratix V – Throughput vs. Area Logarithmic Scale

REVISED

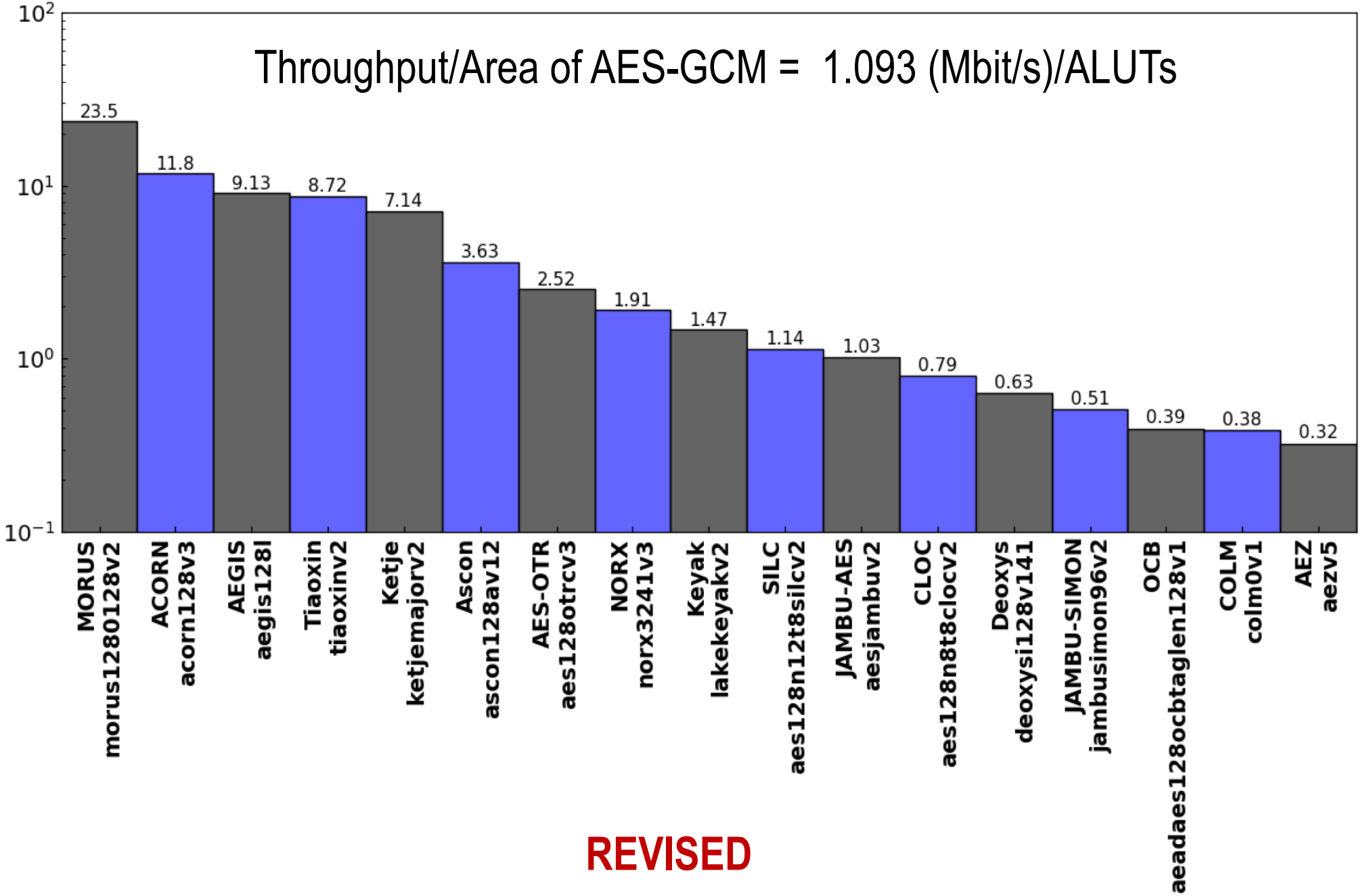


Relative Throughput/Area in Stratix V vs. AES-GCM



ORIGINAL

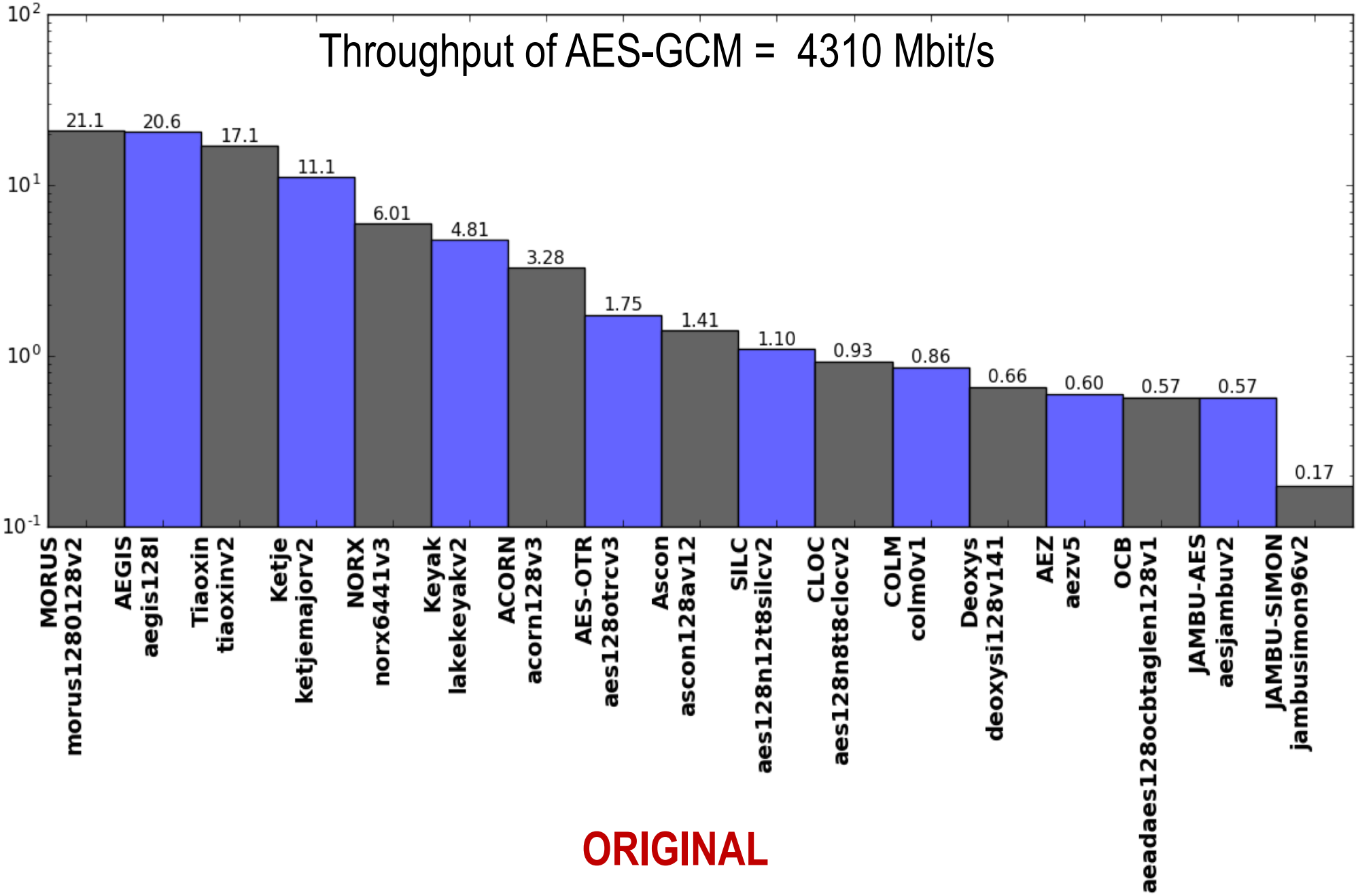
Relative Throughput/Area in Stratix V vs. AES-GCM



REVISED

Relative Throughput in Stratix V

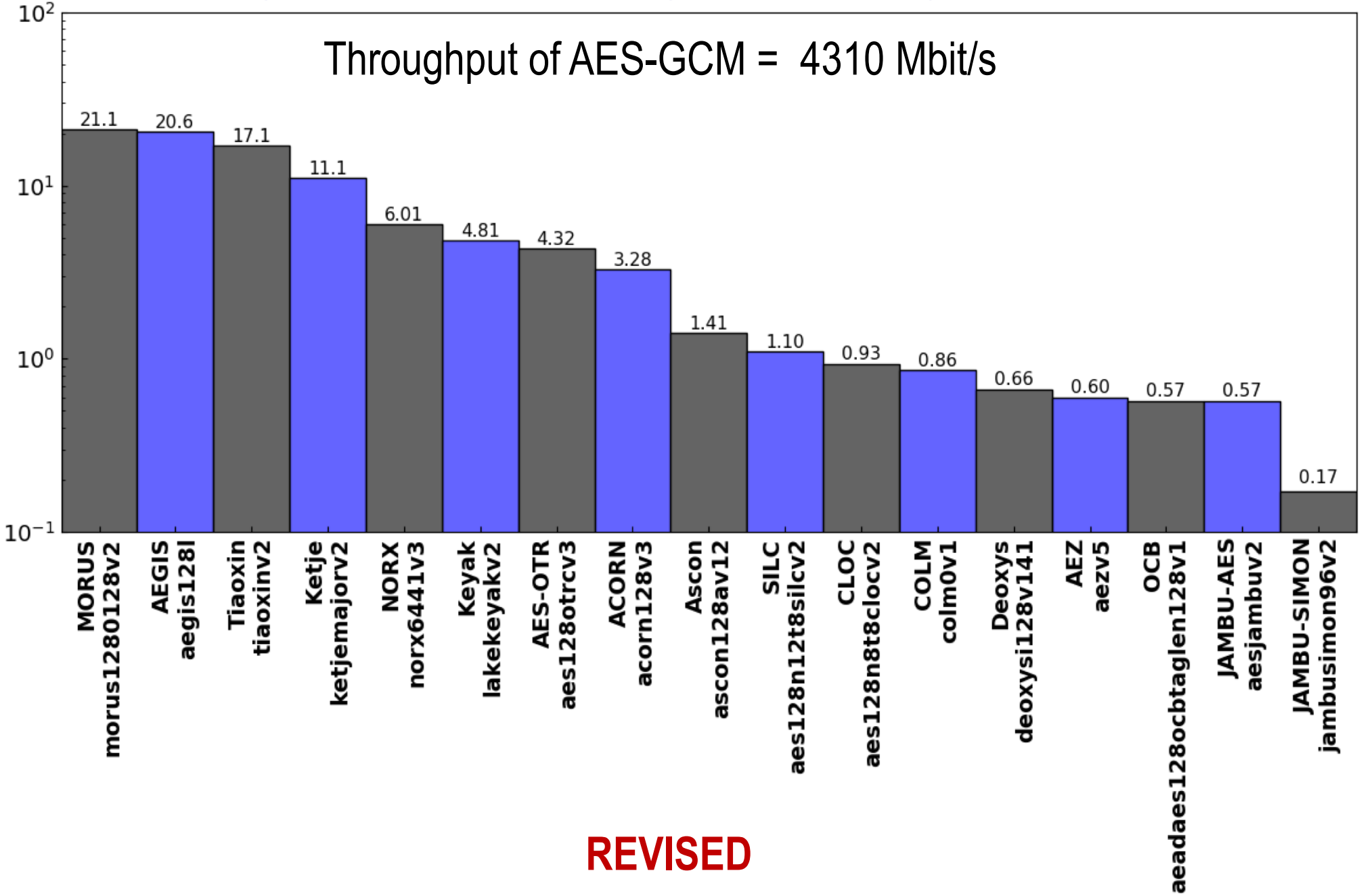
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

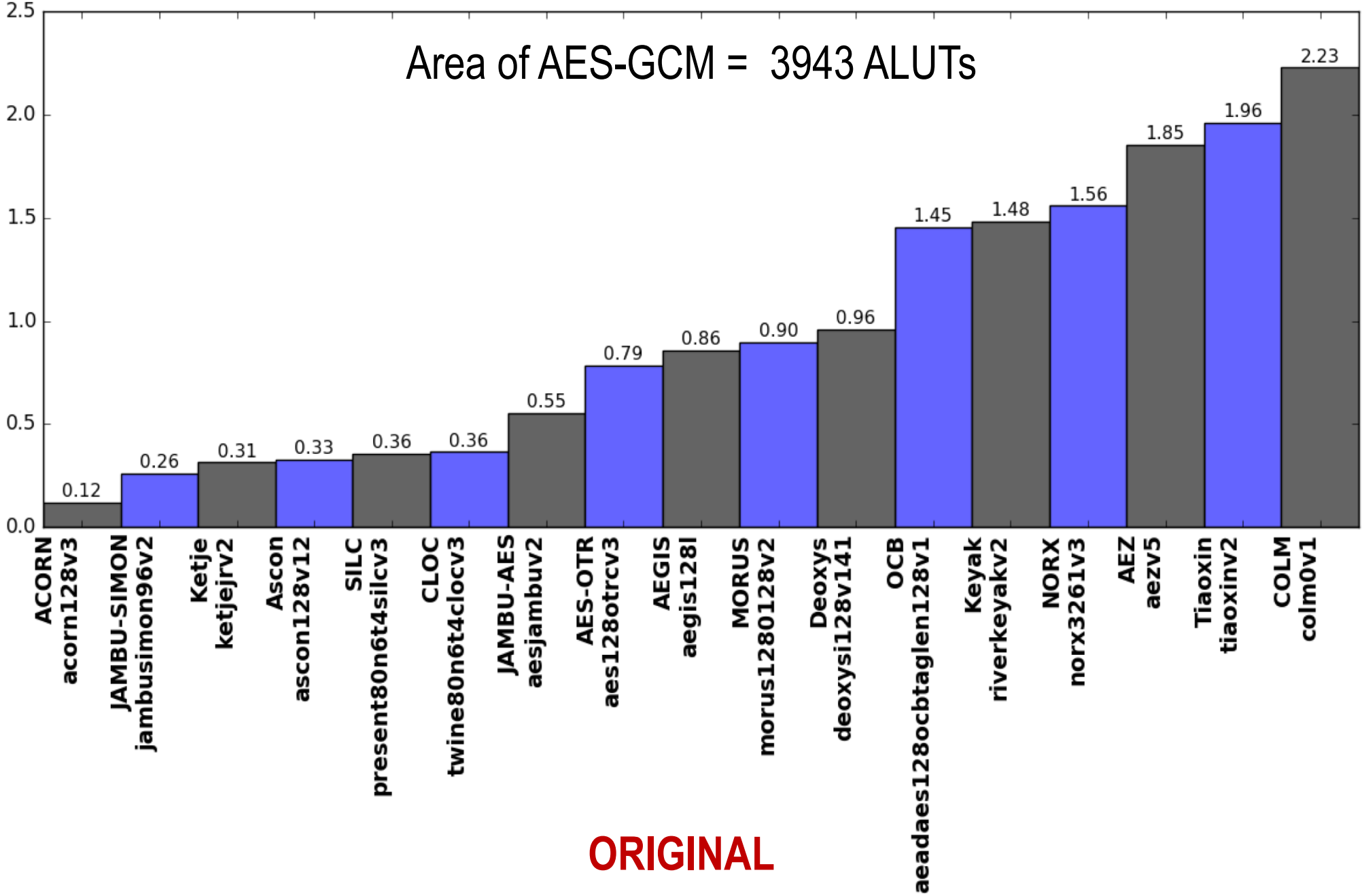
Relative Throughput in Stratix V

Ratio of a given Cipher Throughput/Throughput of AES-GCM



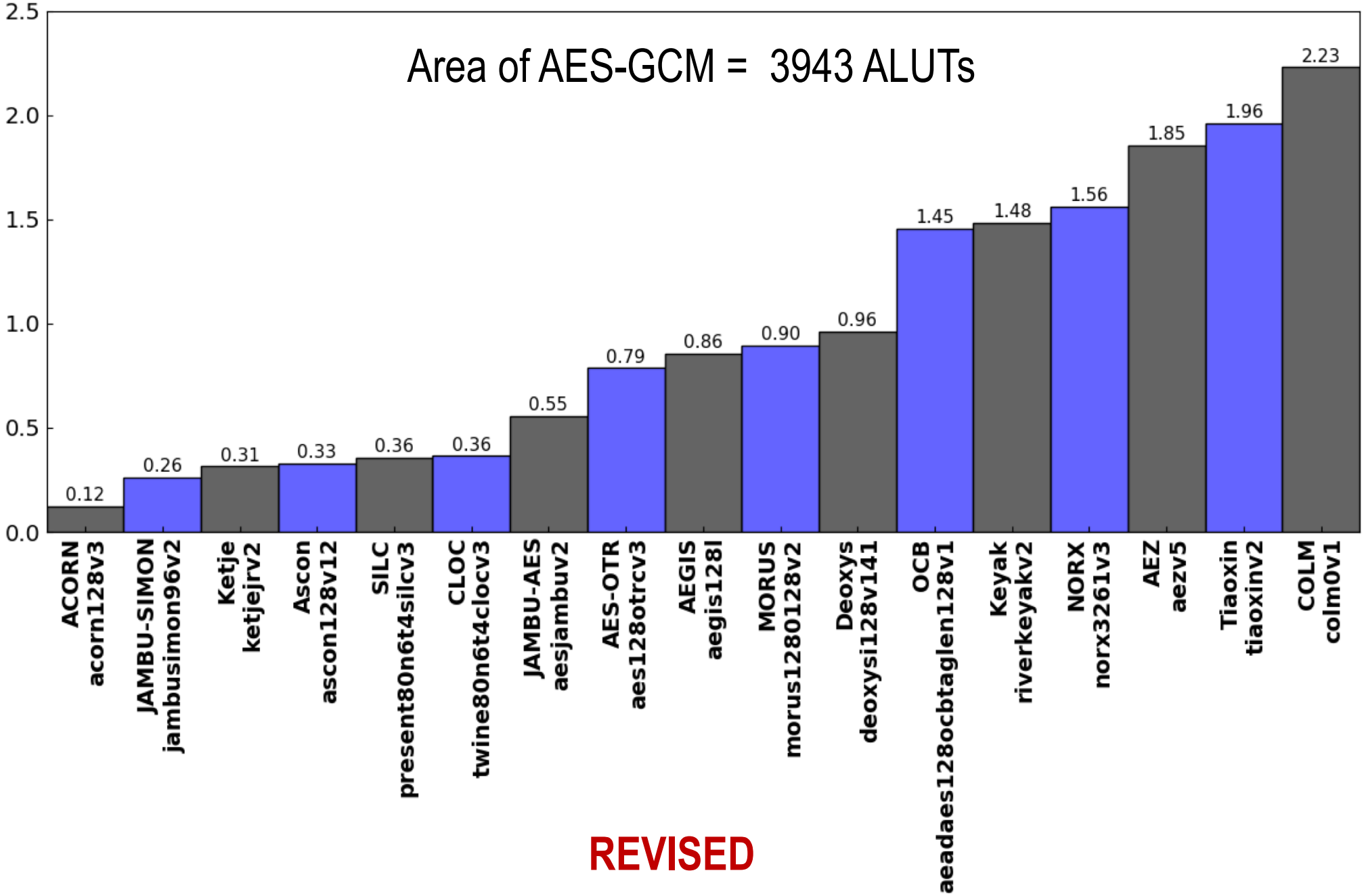
REVISED

Relative Area (#ALUTs) in Stratix V
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#ALUTs) in Stratix V
Ratio of a given Cipher Area/Area of AES-GCM



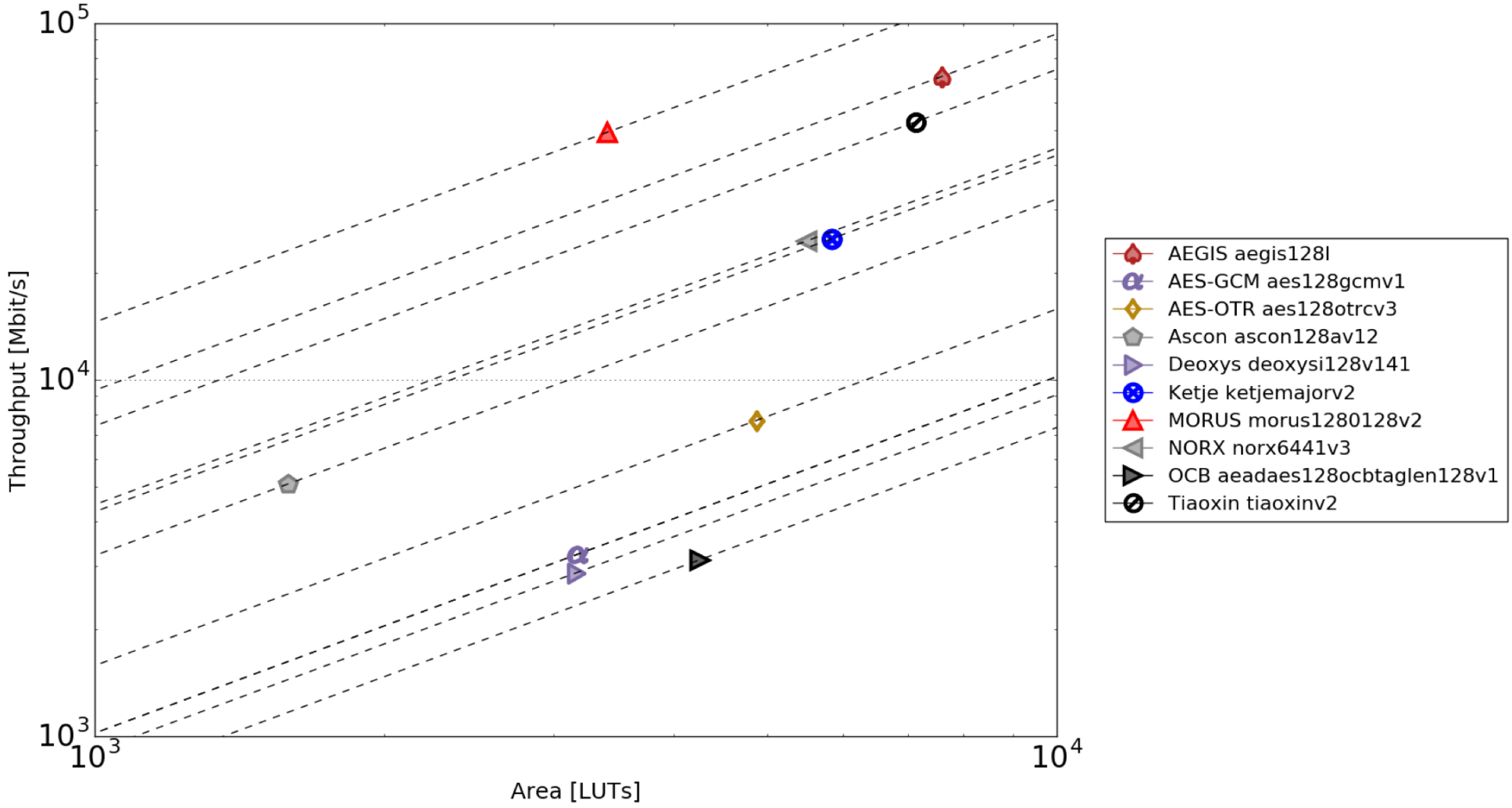
REVISED

Use Case 2

Virtex-6

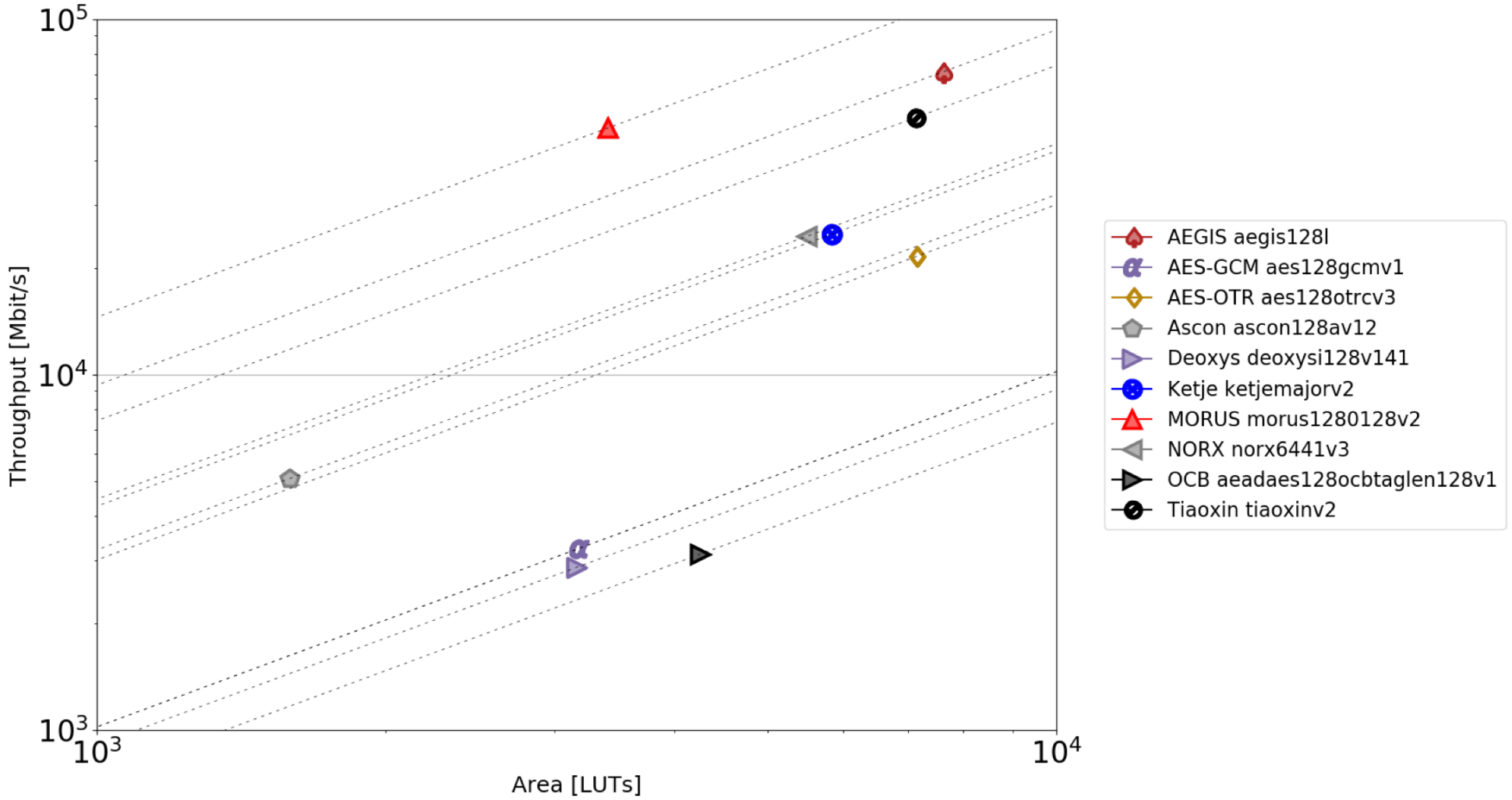
Results for Virtex-6 – Throughput vs. Area Logarithmic Scale

ORIGINAL

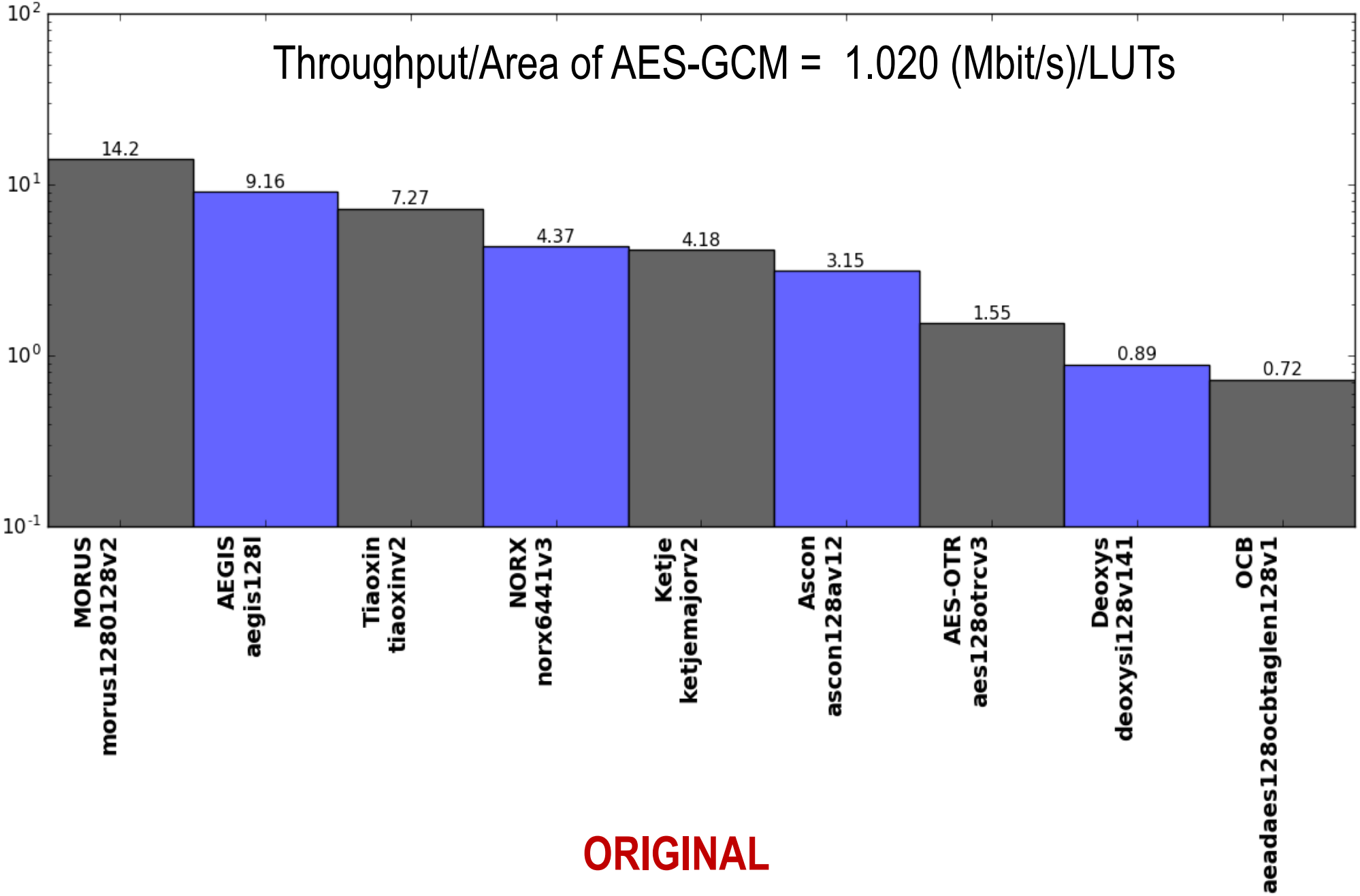


Results for Virtex-6 – Throughput vs. Area Logarithmic Scale

REVISED

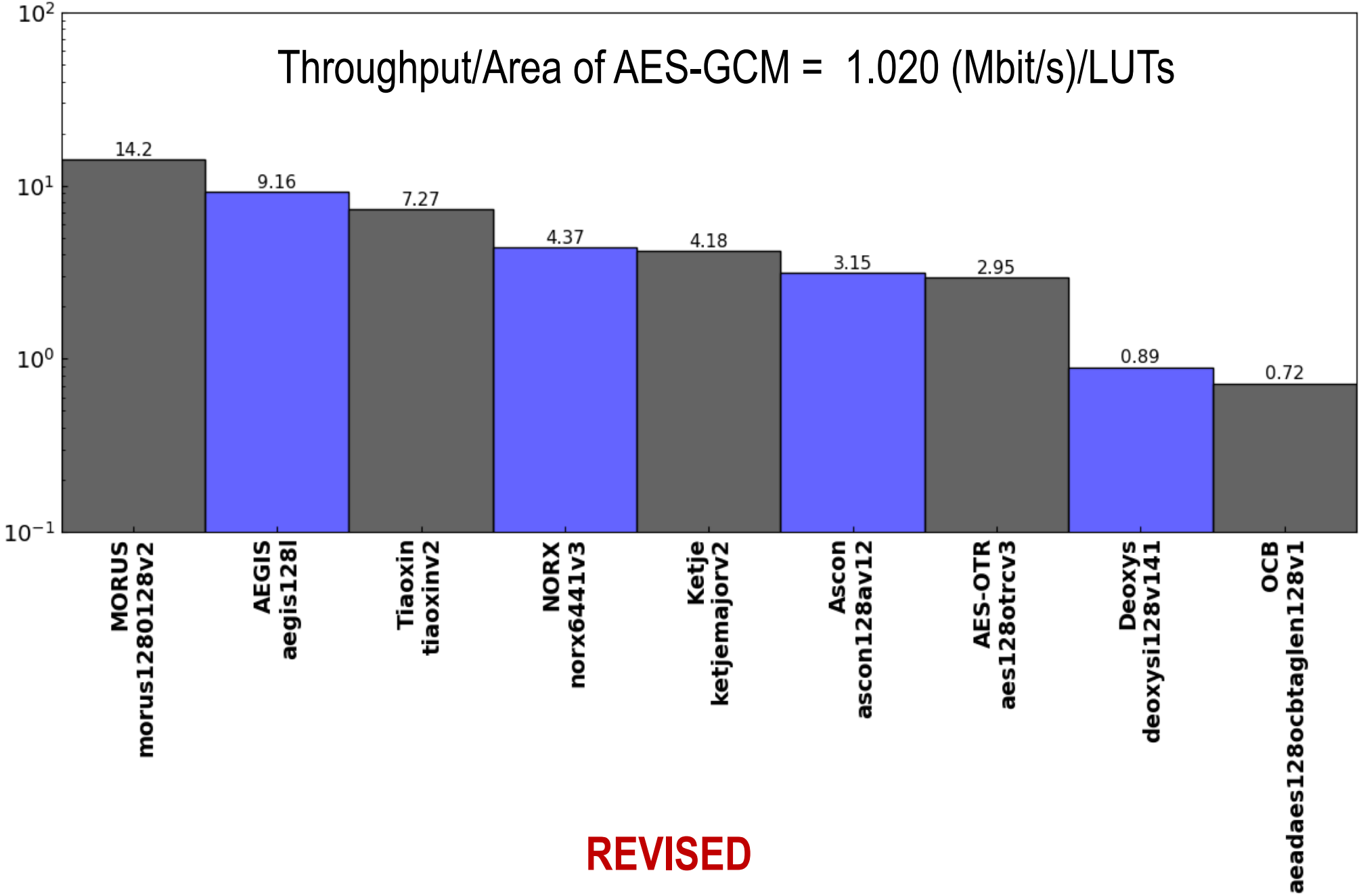


Relative Throughput/Area in Virtex-6 vs. AES-GCM



ORIGINAL

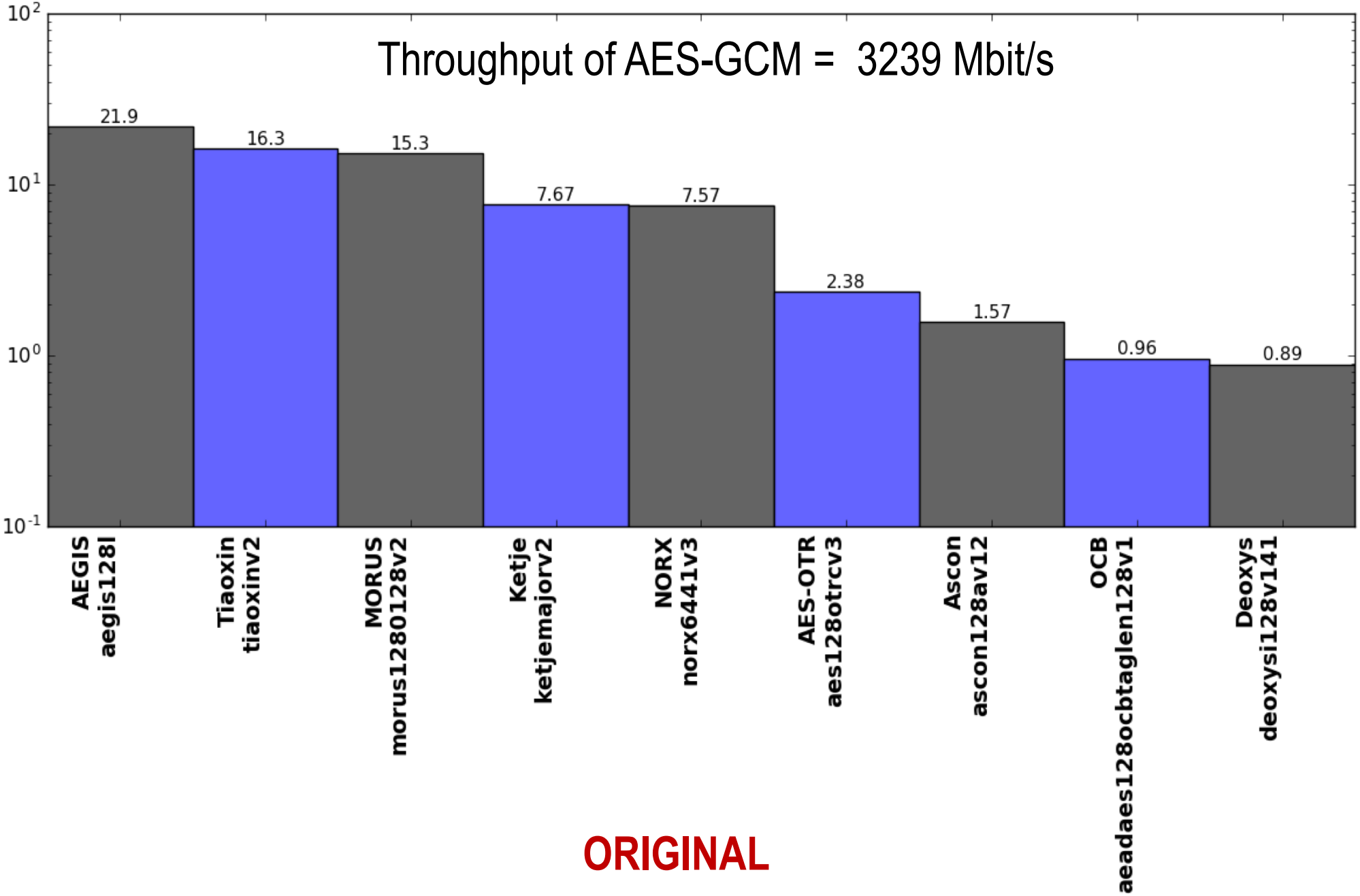
Relative Throughput/Area in Virtex-6 vs. AES-GCM



REVISED

Relative Throughput in Virtex-6

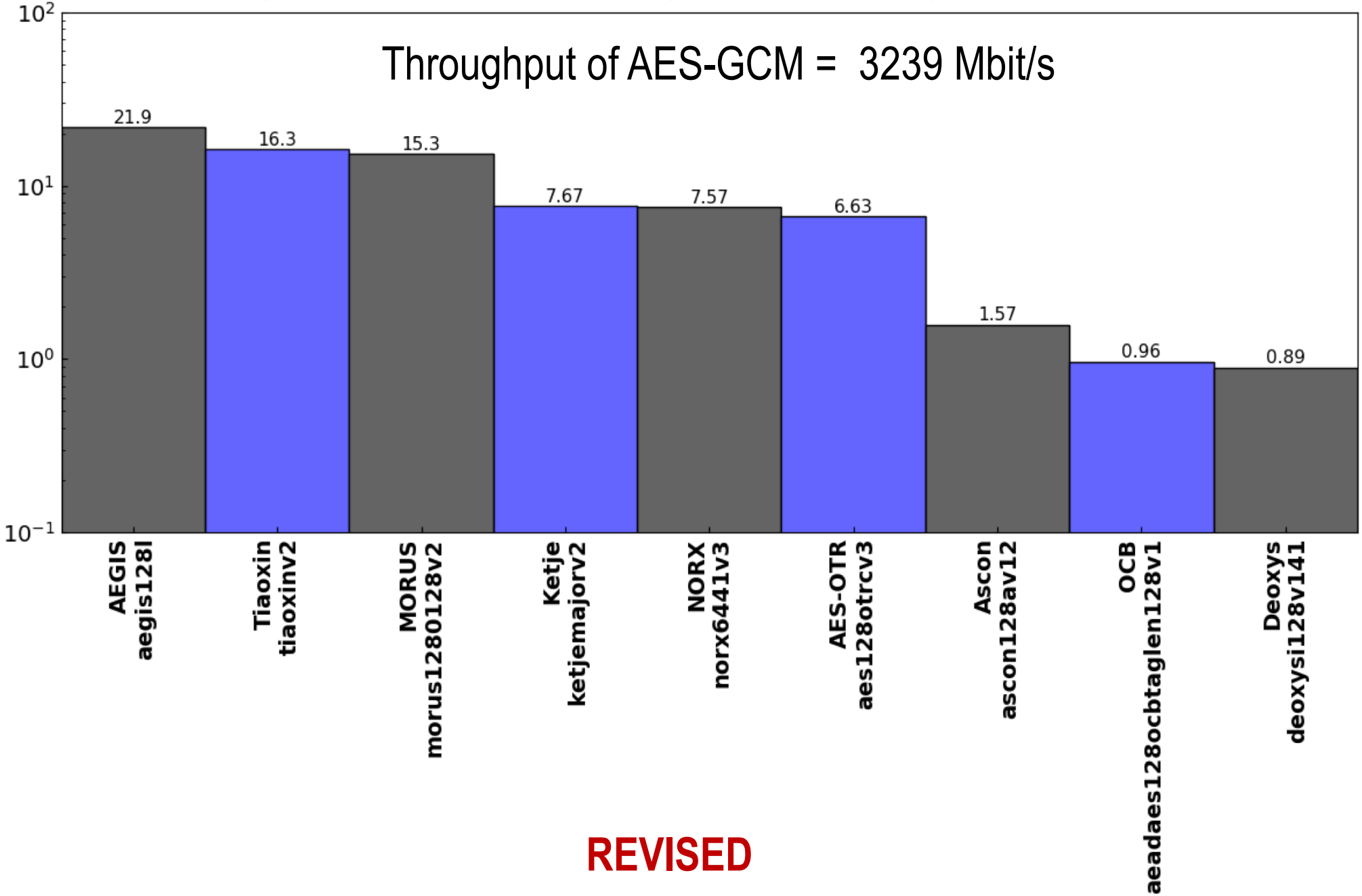
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

Relative Throughput in Virtex-6

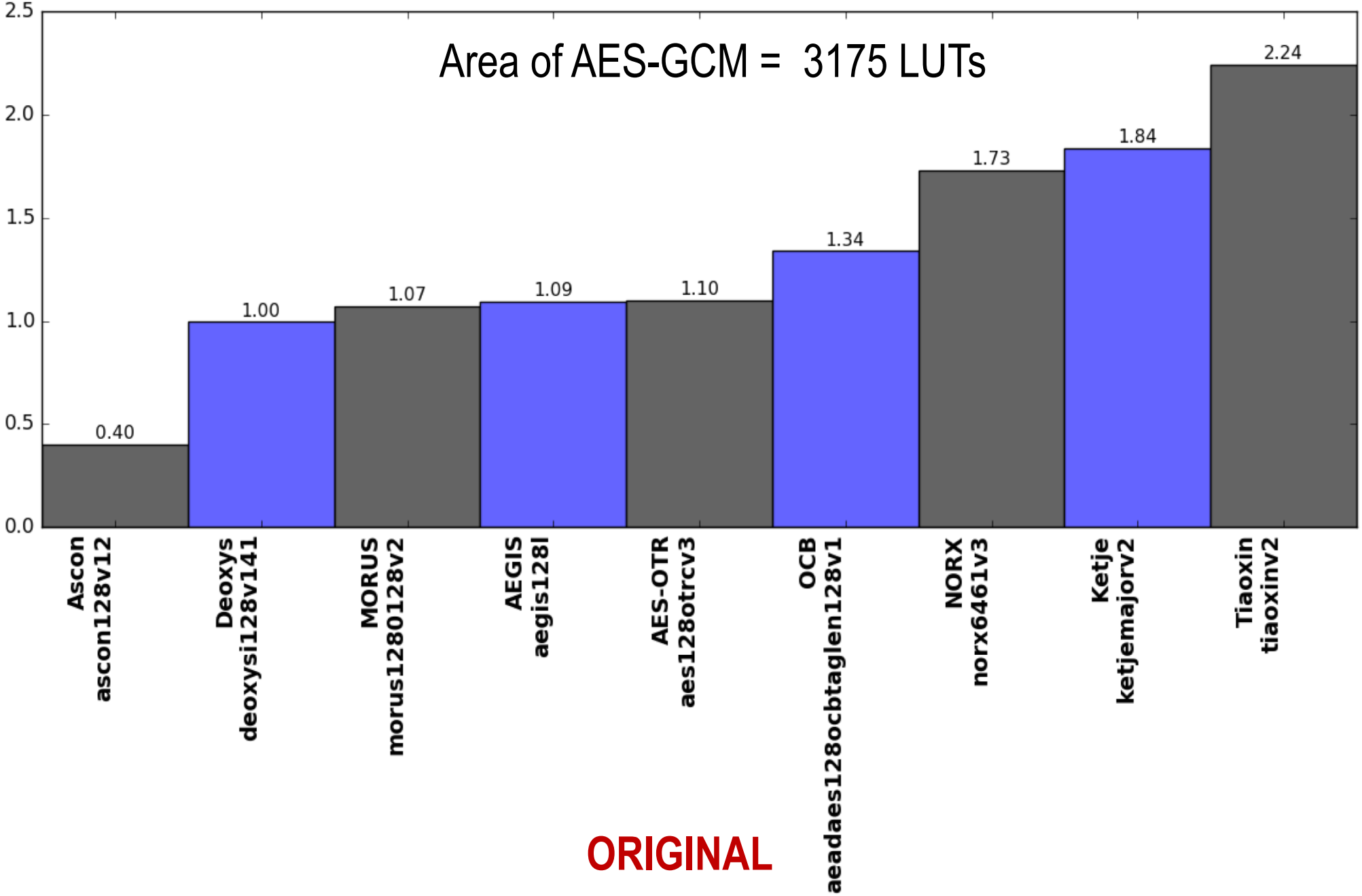
Ratio of a given Cipher Throughput/Throughput of AES-GCM



REVISED

Relative Area (#LUTs) in Virtex-6

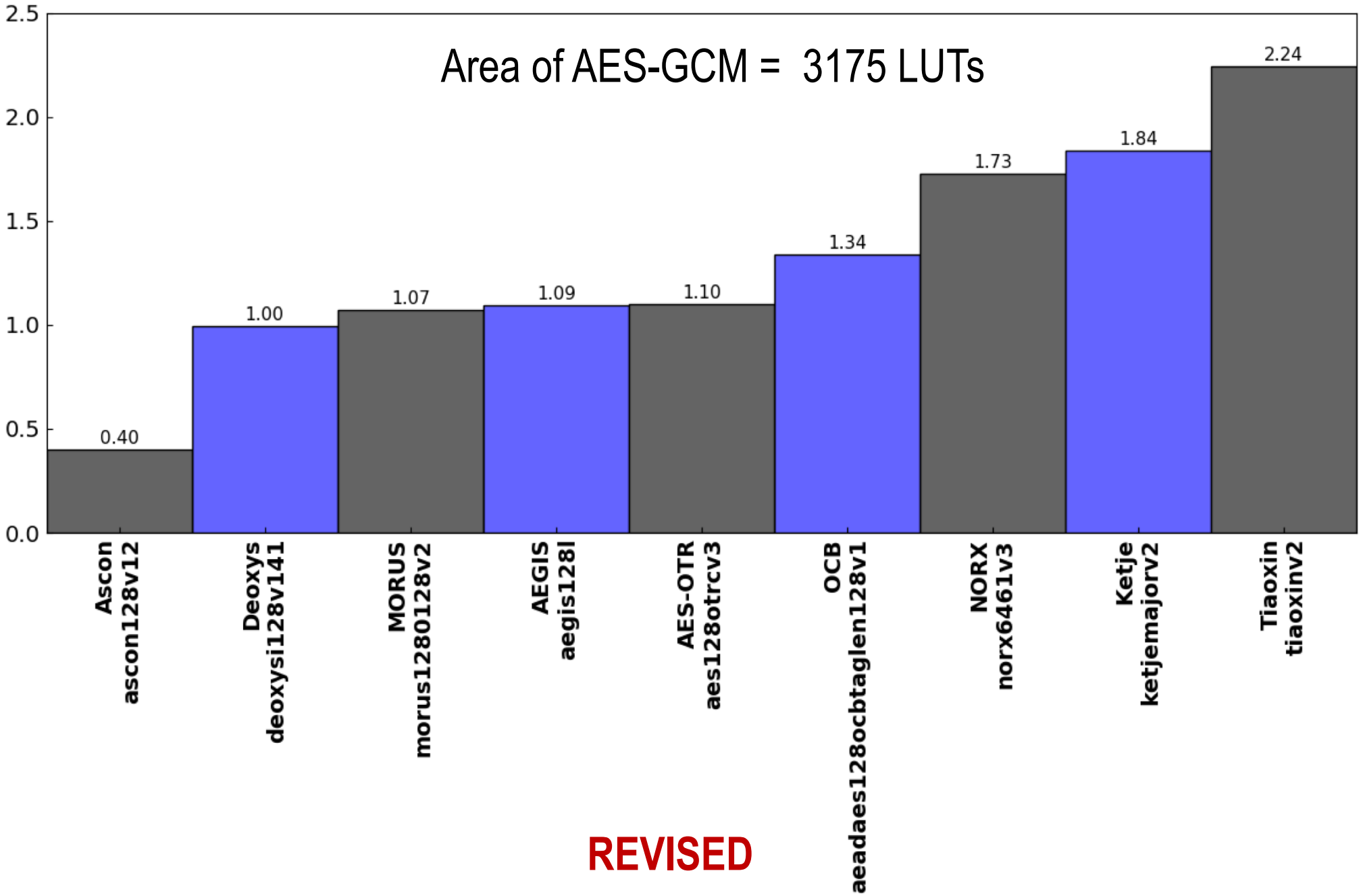
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#LUTs) in Virtex-6

Ratio of a given Cipher Area/Area of AES-GCM

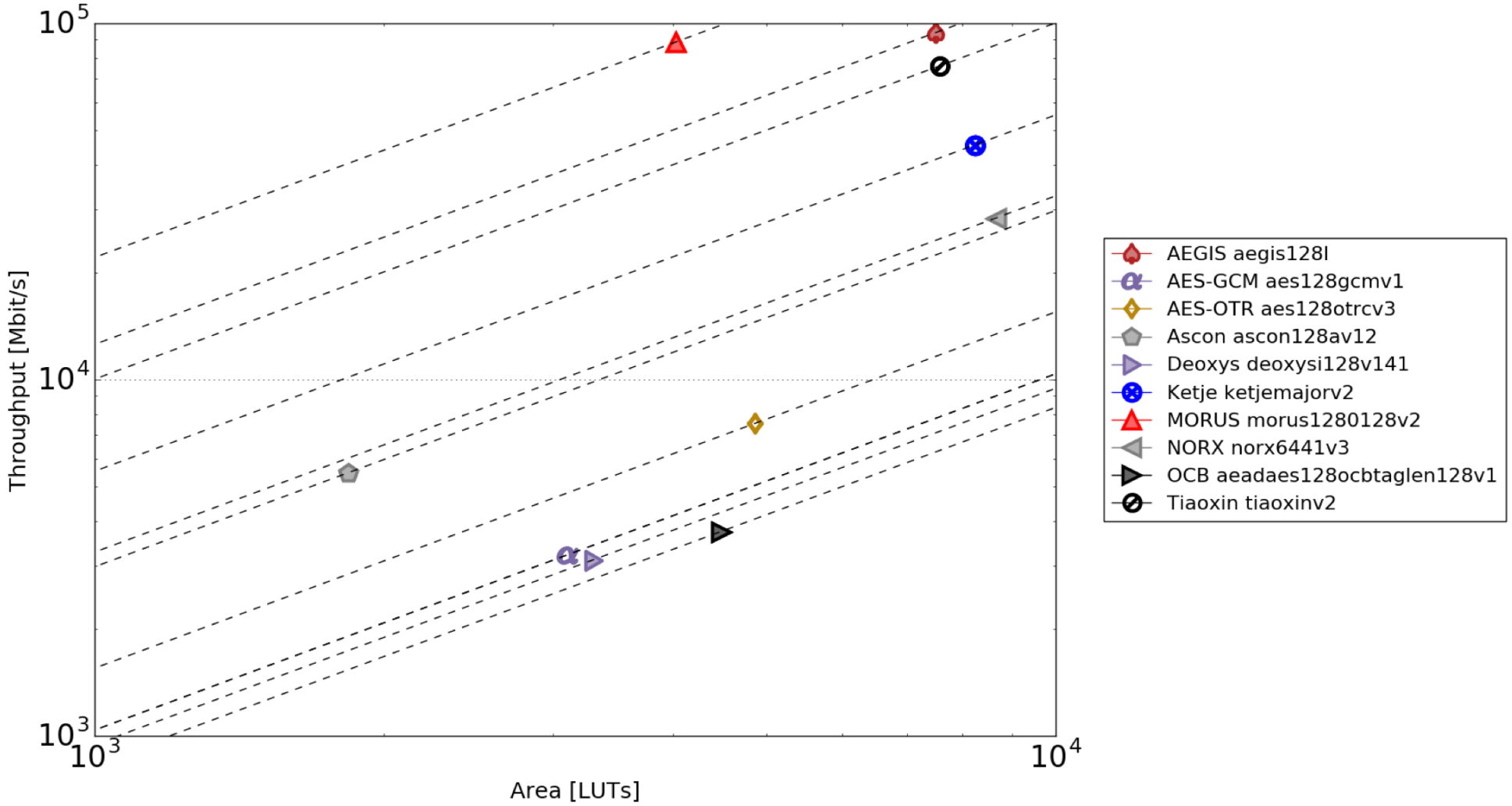


REVISED

Virtex-7

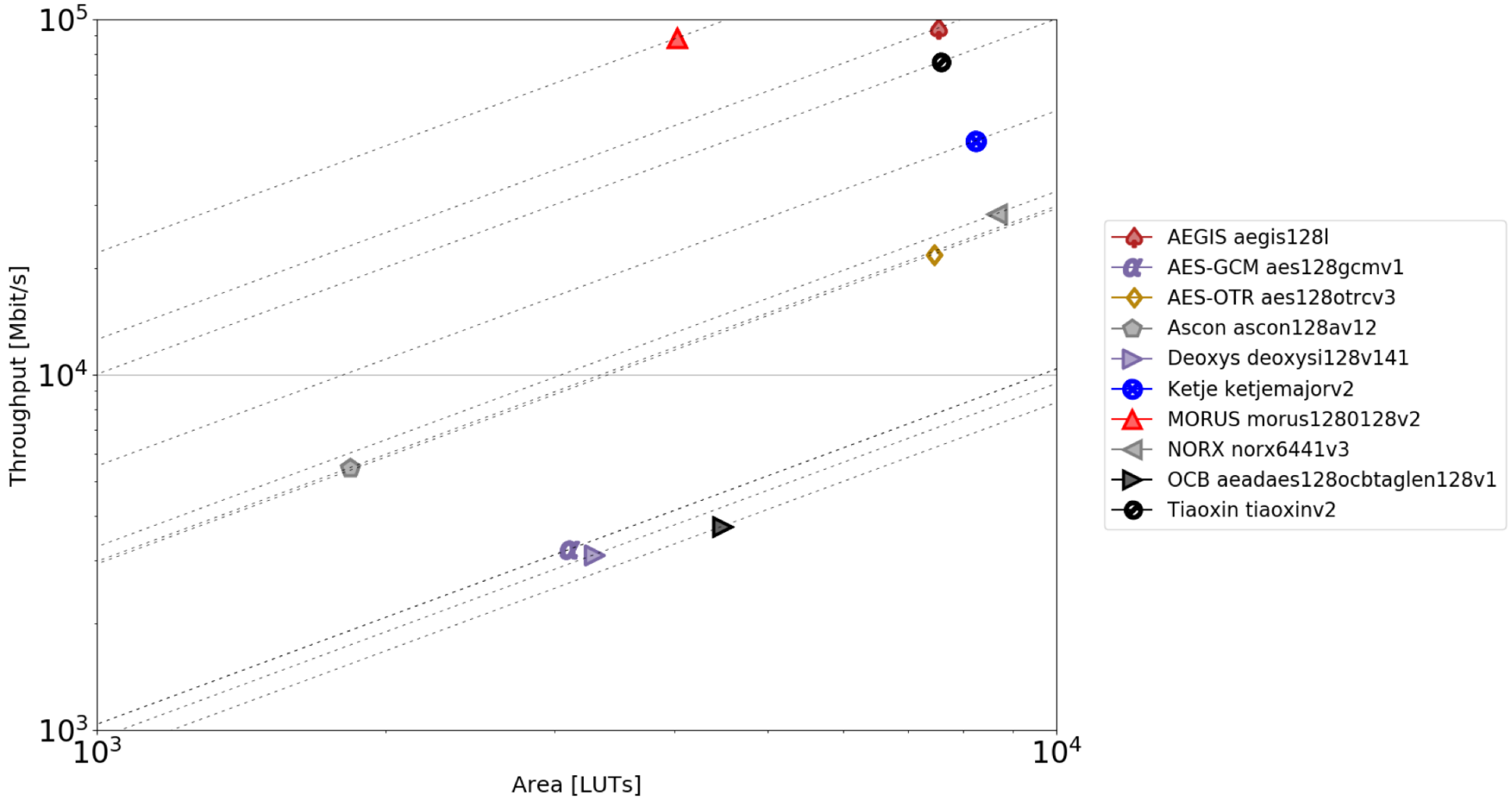
Results for Virtex-7 – Throughput vs. Area Logarithmic Scale

ORIGINAL

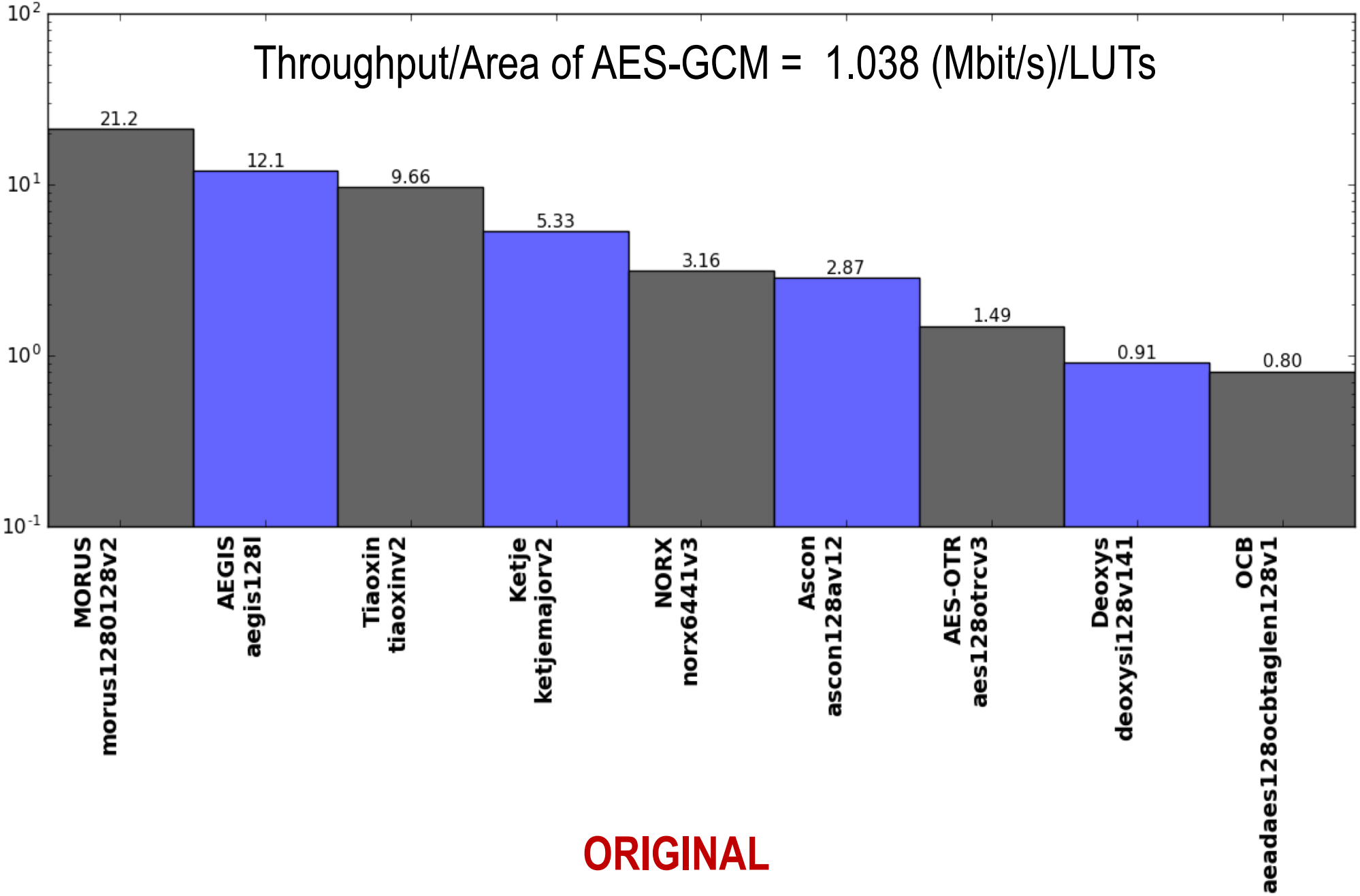


Results for Virtex-7 – Throughput vs. Area Logarithmic Scale

REVISED

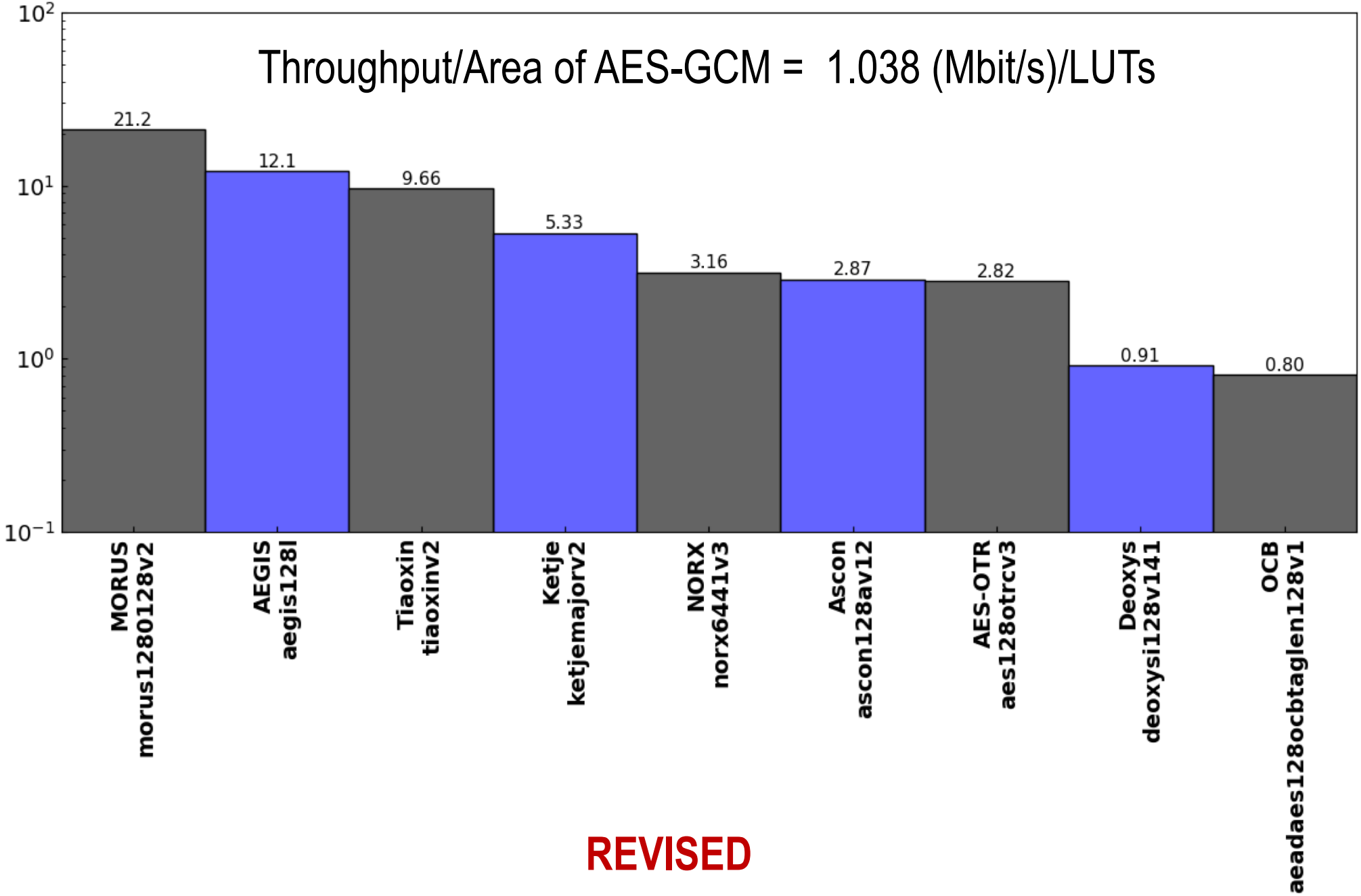


Relative Throughput/Area in Virtex-7 vs. AES-GCM



ORIGINAL

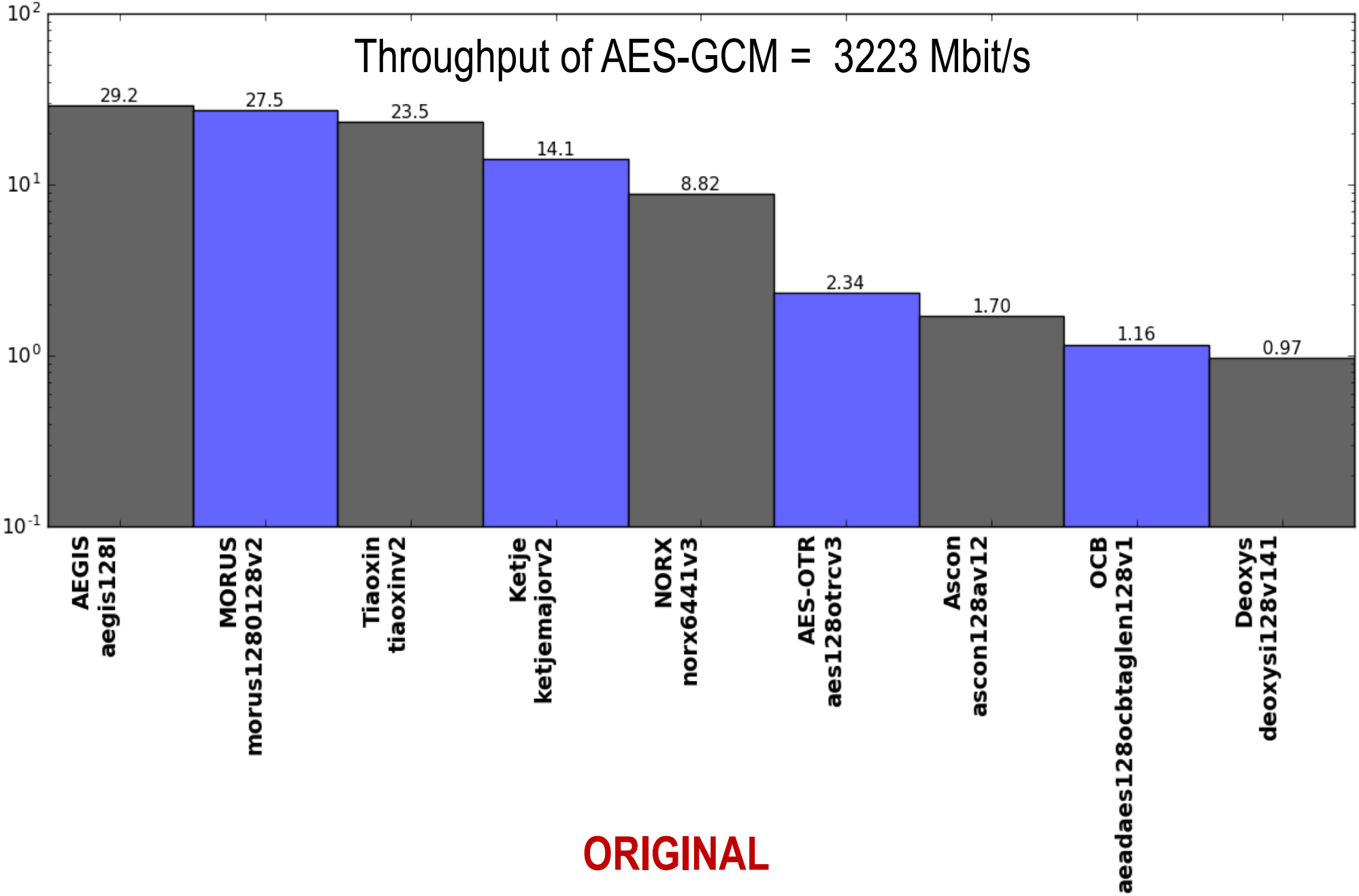
Relative Throughput/Area in Virtex-7 vs. AES-GCM



REVISED

Relative Throughput in Virtex-7

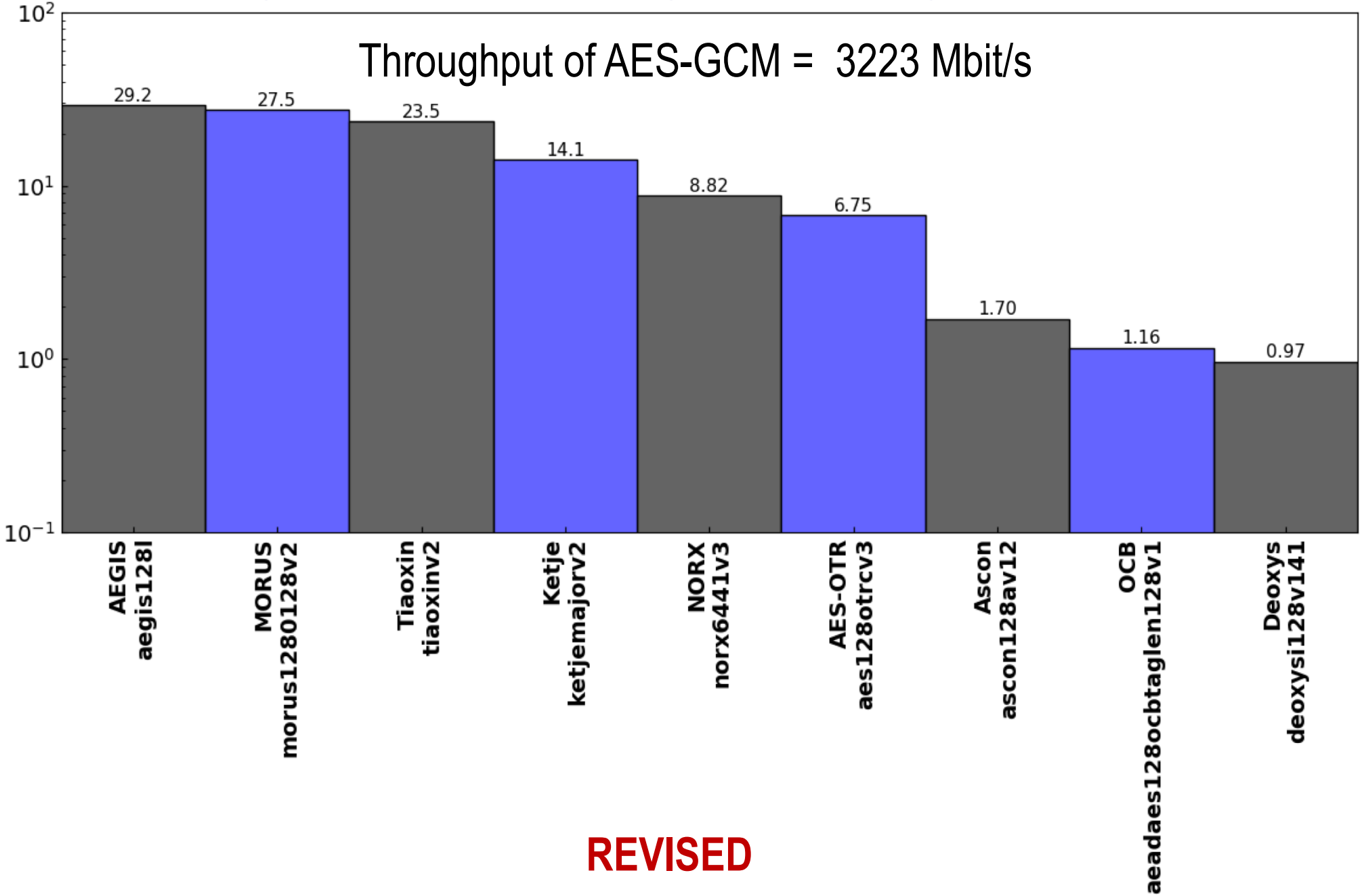
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

Relative Throughput in Virtex-7

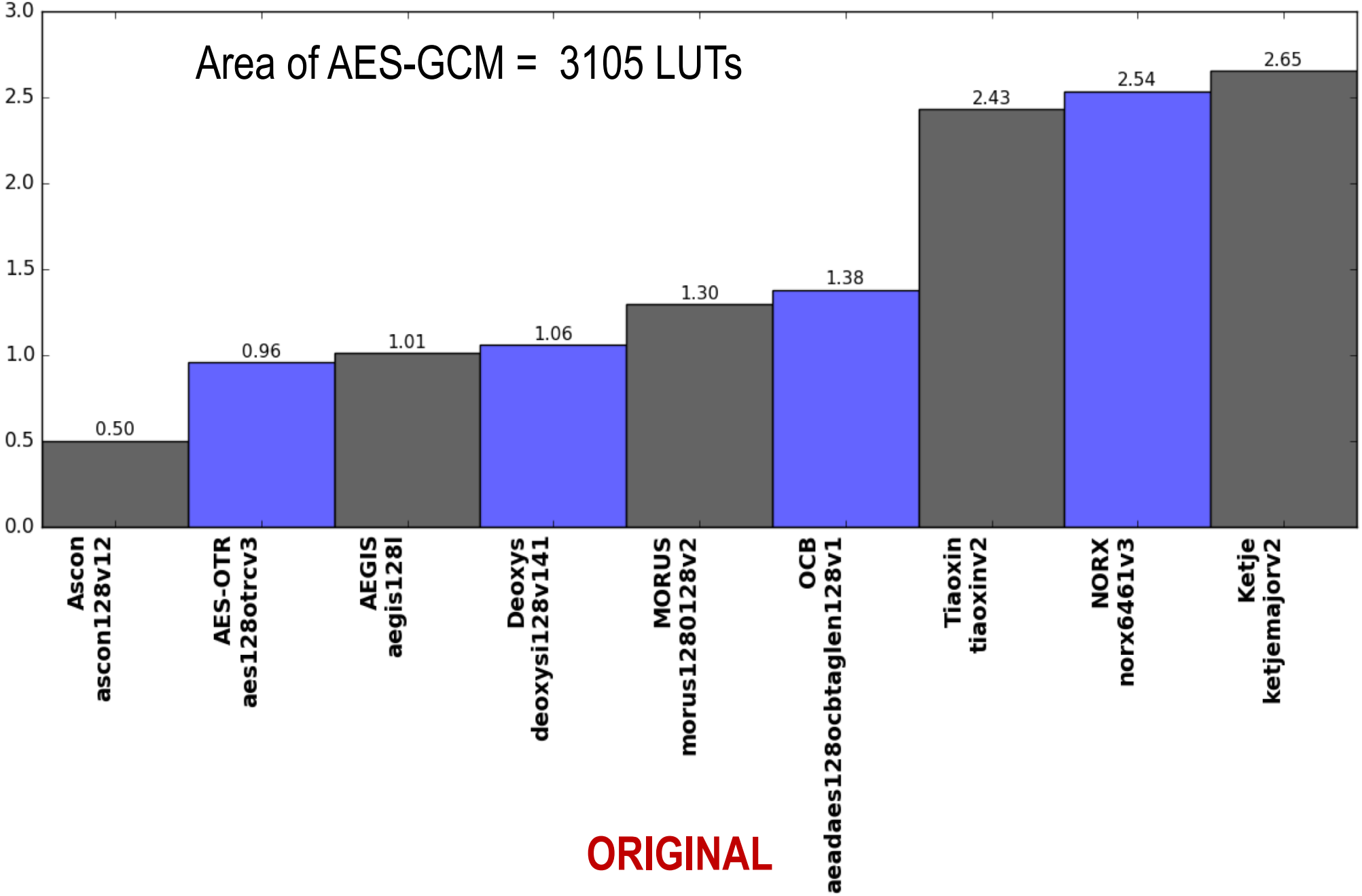
Ratio of a given Cipher Throughput/Throughput of AES-GCM



REVISED

Relative Area (#LUTs) in Virtex-7

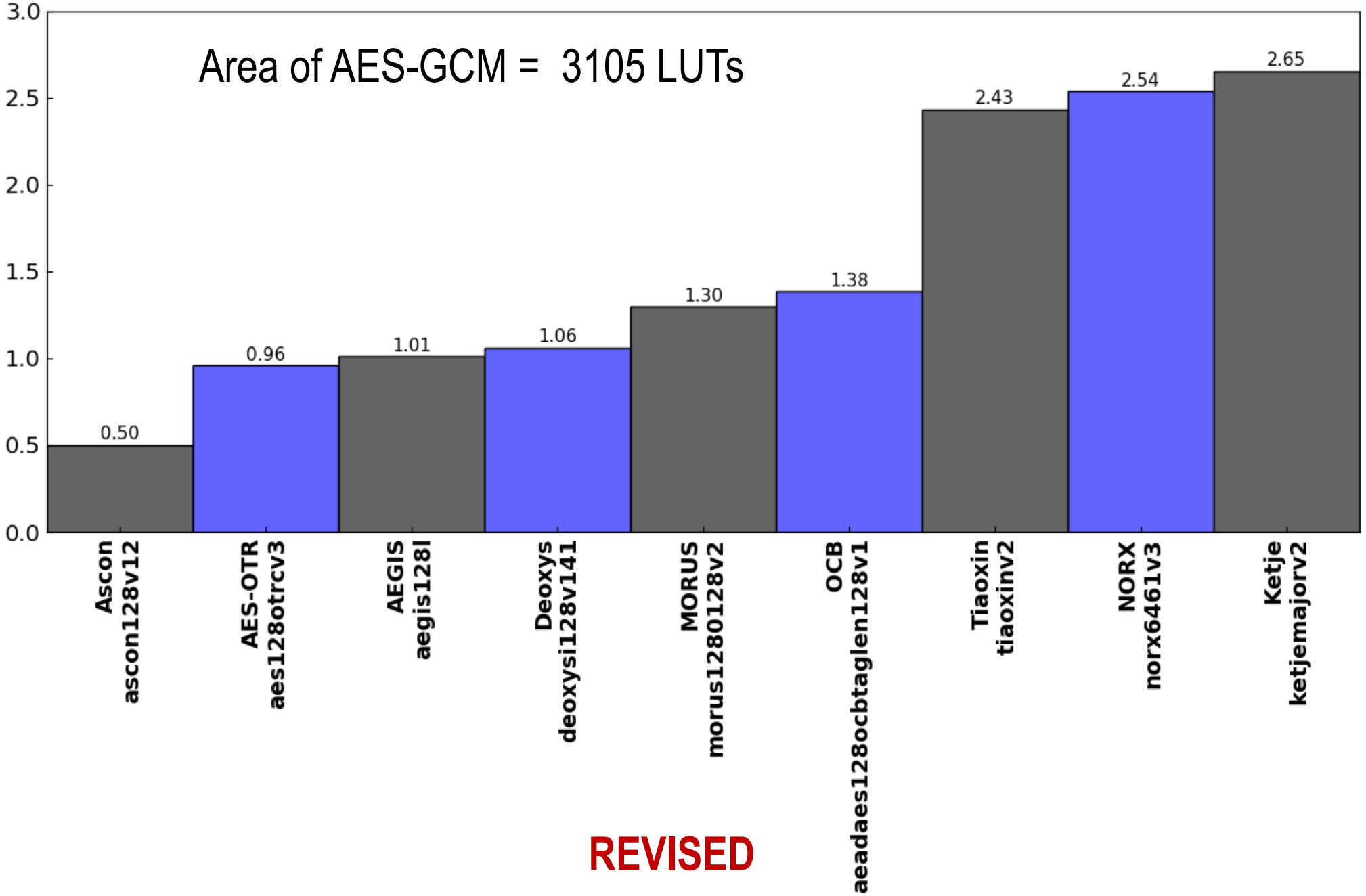
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#LUTs) in Virtex-7

Ratio of a given Cipher Area/Area of AES-GCM

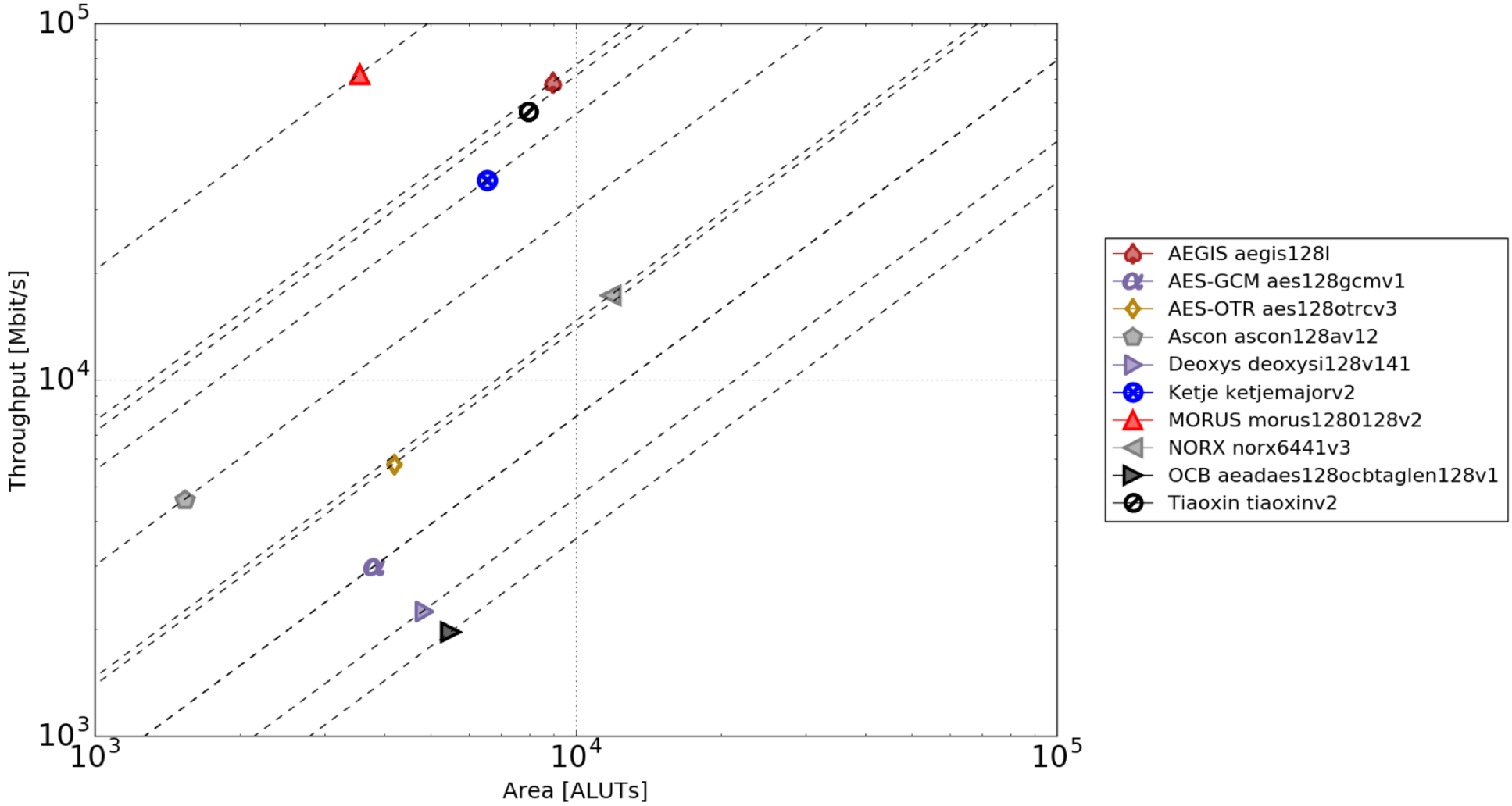


REVISED

Stratix IV

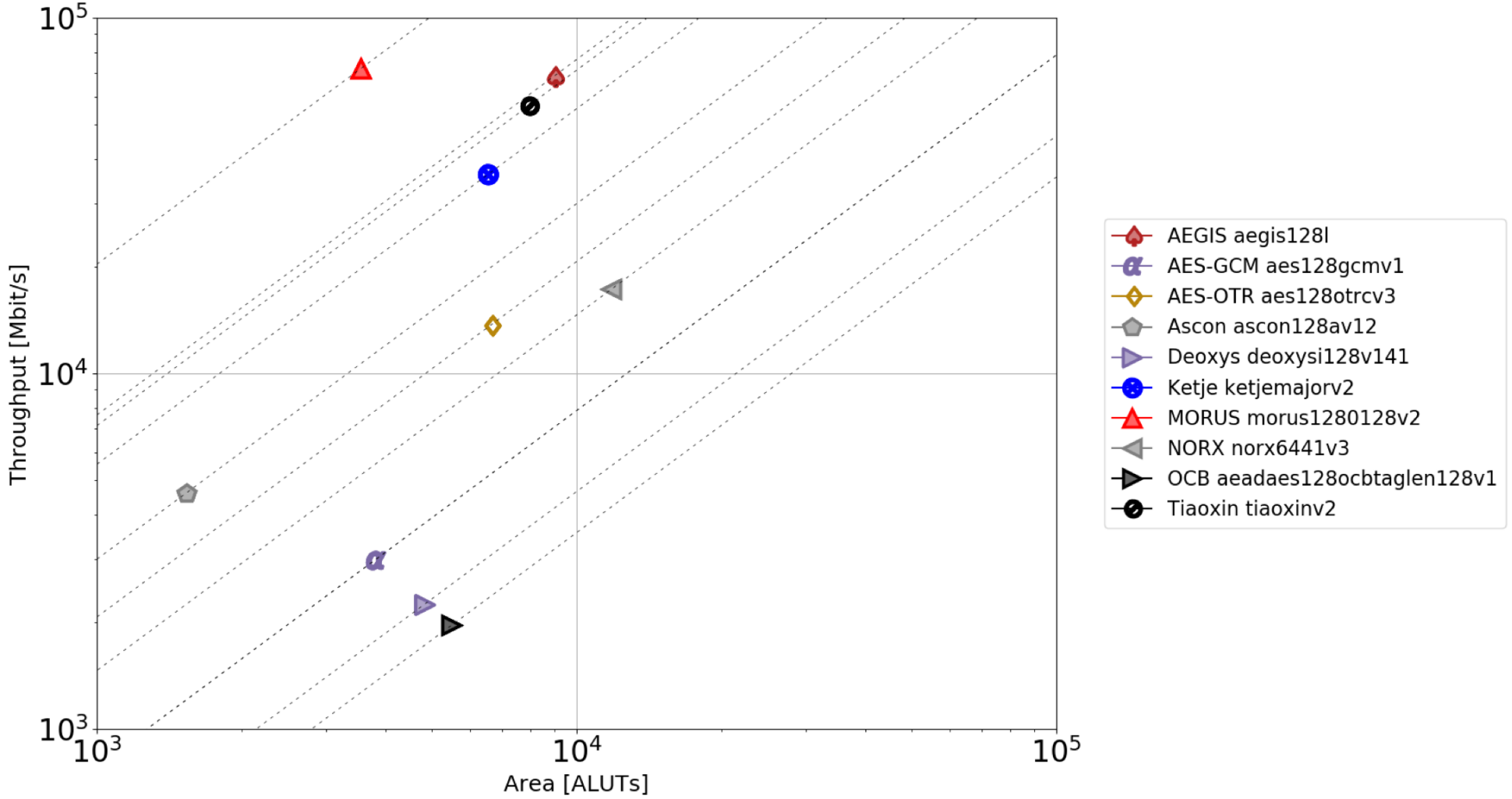
Results for Stratix IV – Throughput vs. Area Logarithmic Scale

ORIGINAL

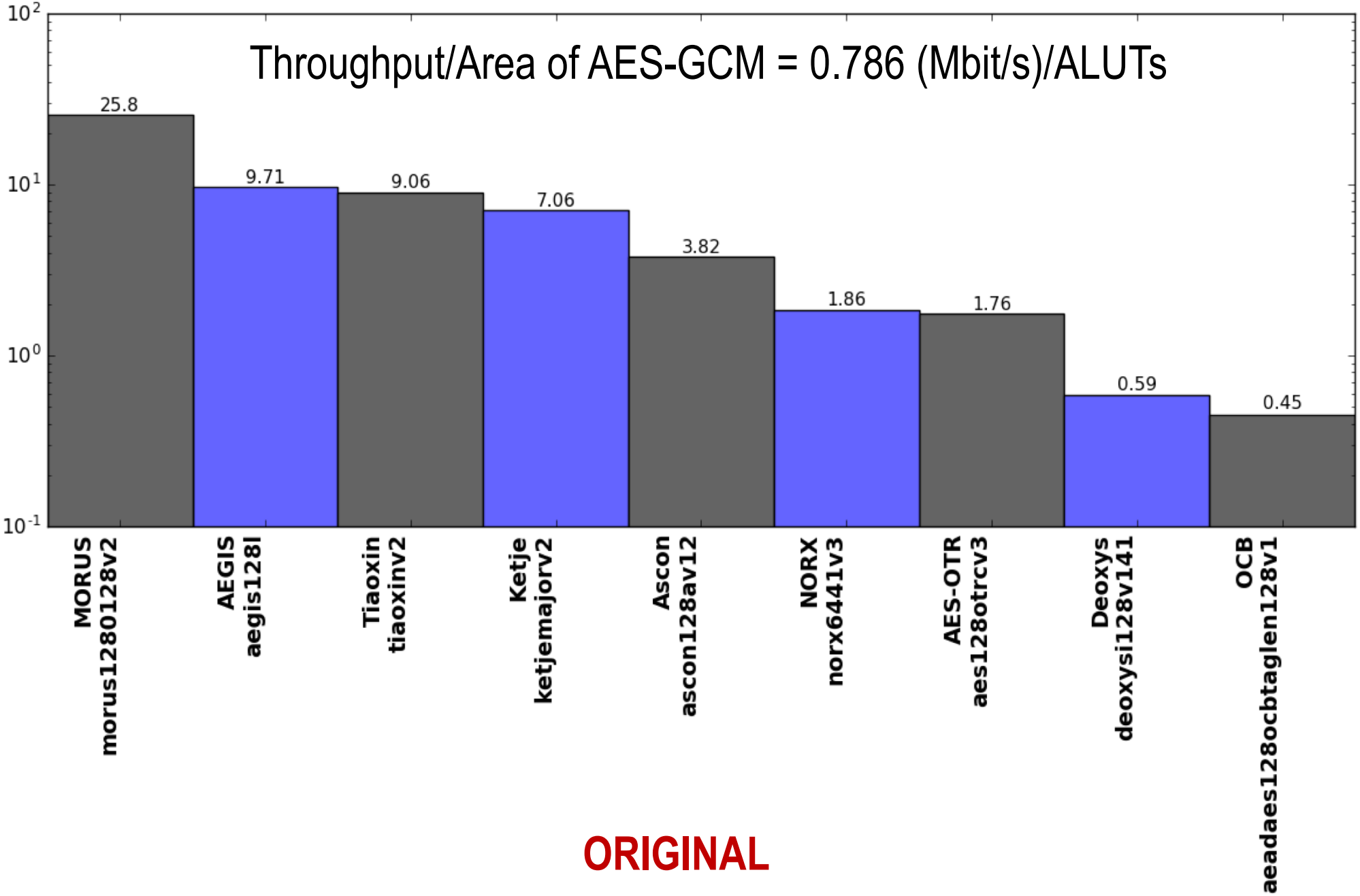


Results for Stratix IV – Throughput vs. Area Logarithmic Scale

REVISED

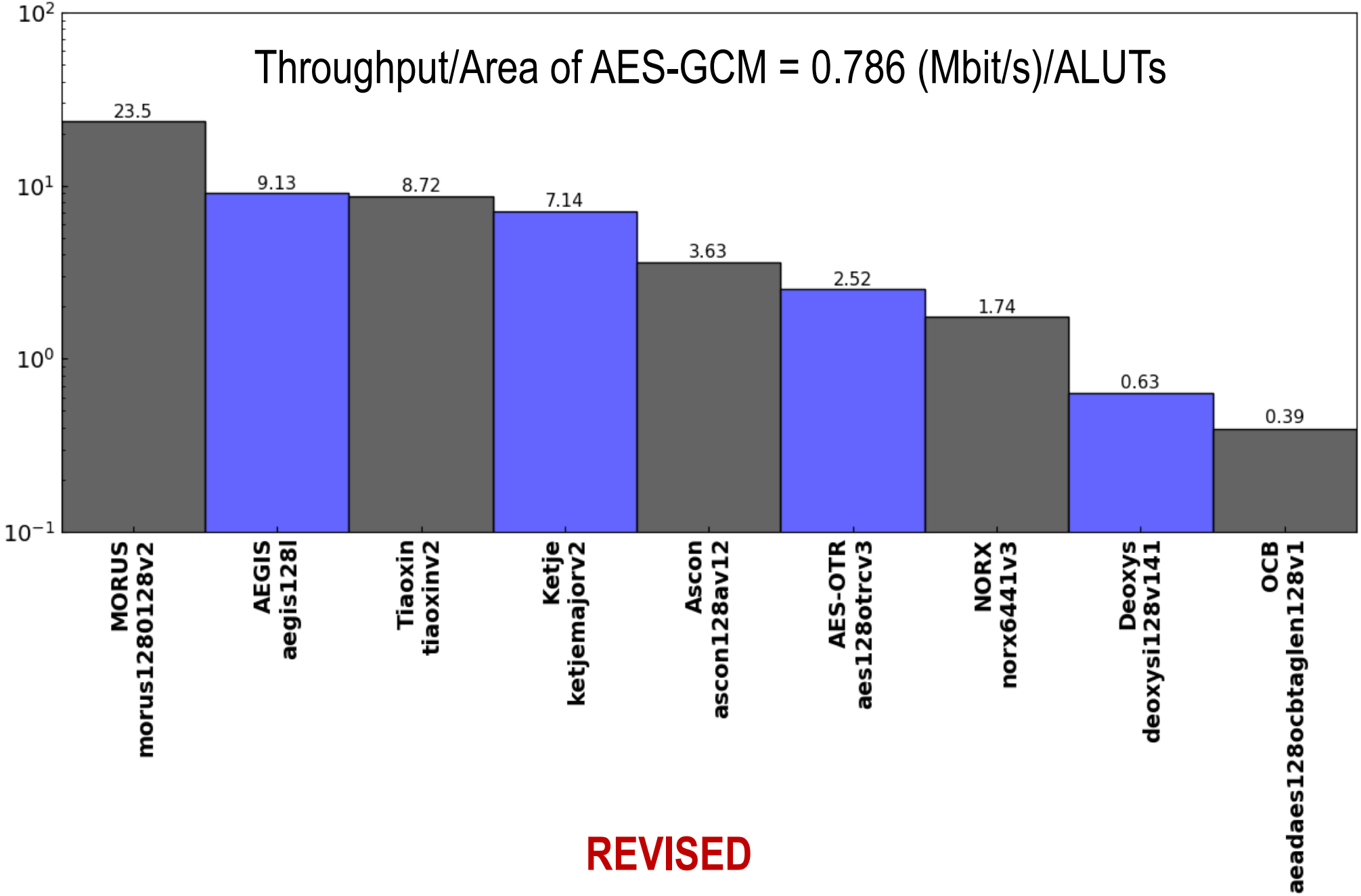


Relative Throughput/Area in Stratix IV vs. AES-GCM



ORIGINAL

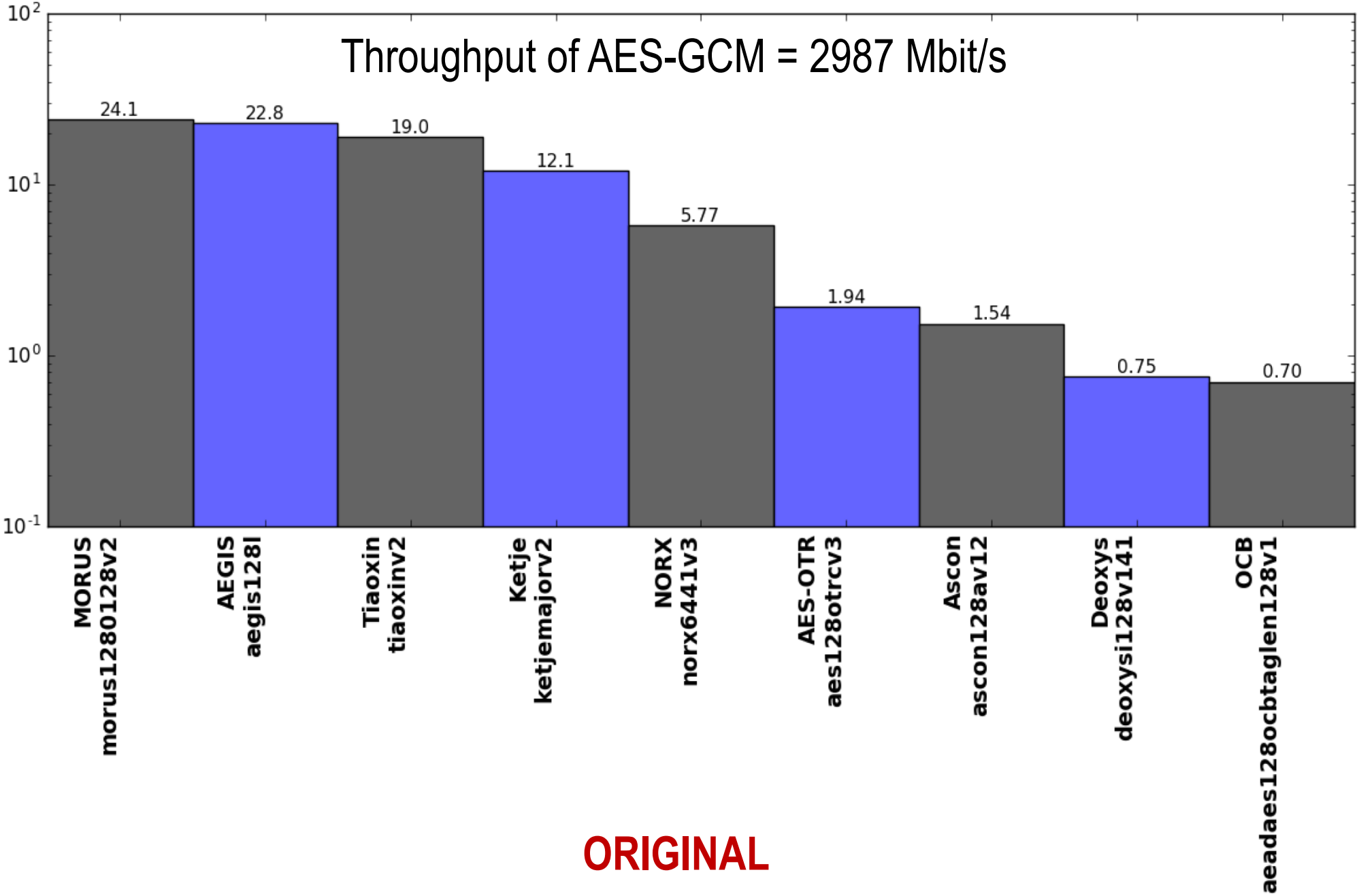
Relative Throughput/Area in Stratix IV vs. AES-GCM



REVISED

Relative Throughput in Stratix IV

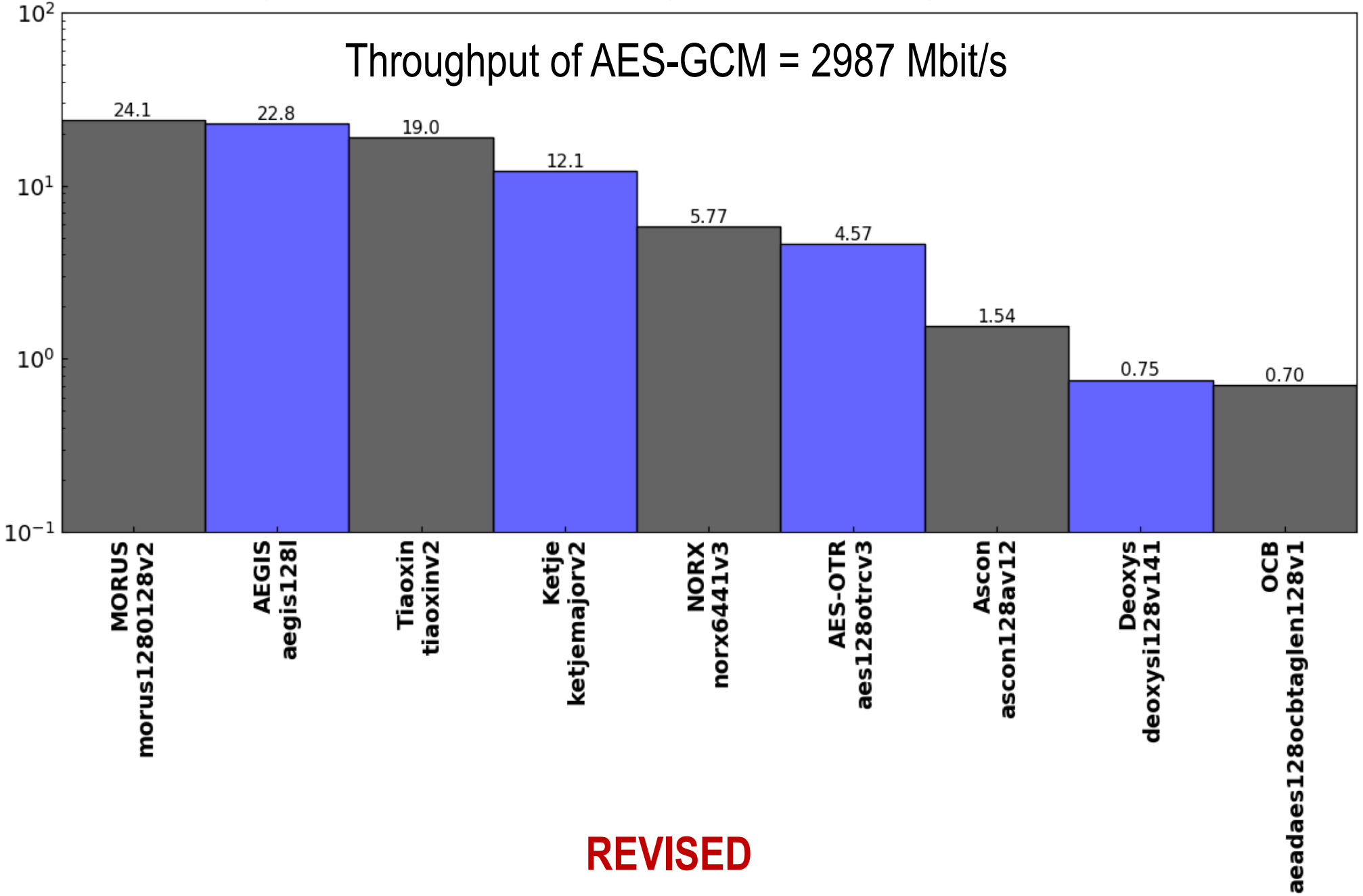
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

Relative Throughput in Stratix IV

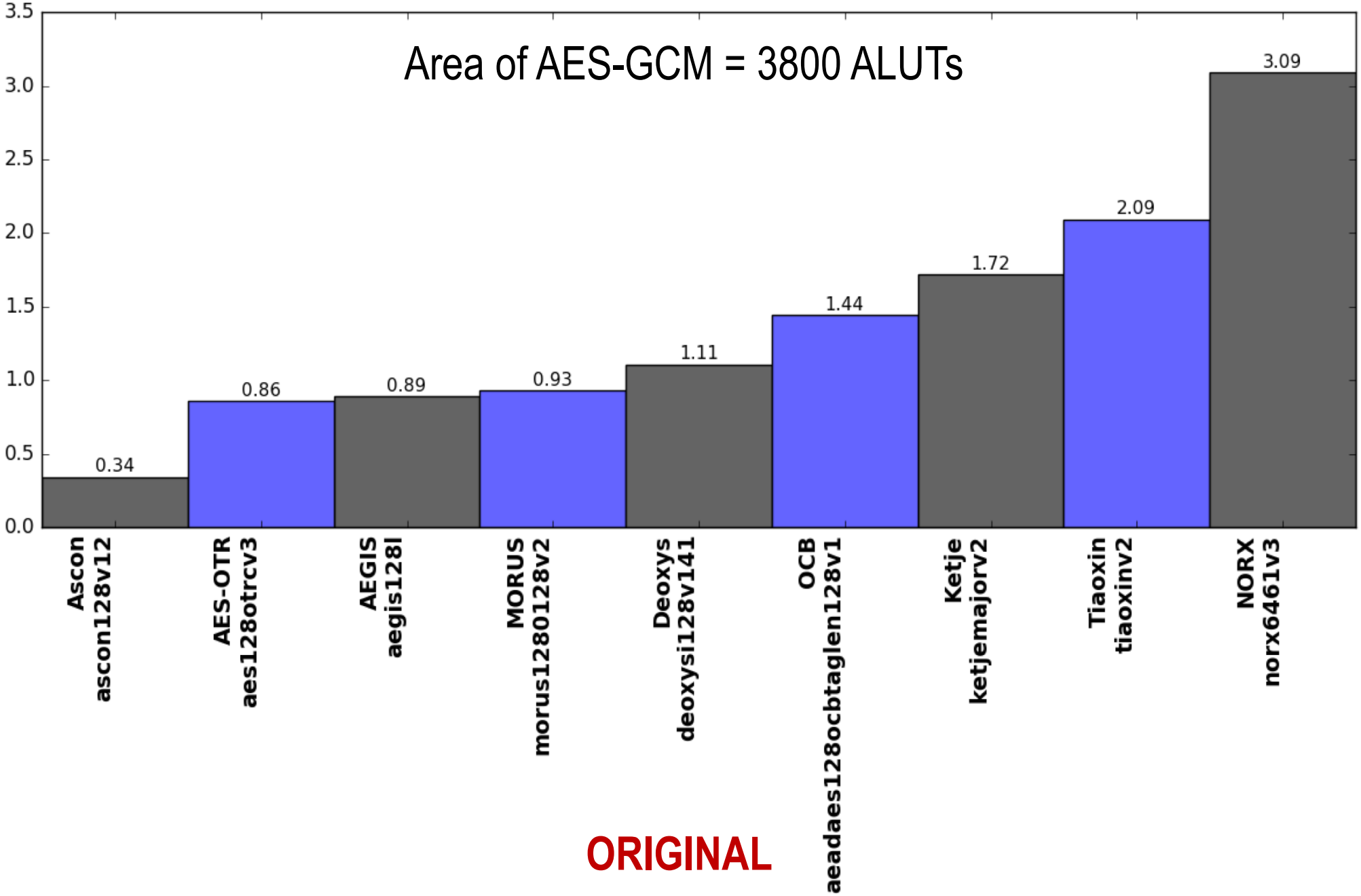
Ratio of a given Cipher Throughput/Throughput of AES-GCM



REVISED

Relative Area (#ALUTs) in Stratix IV

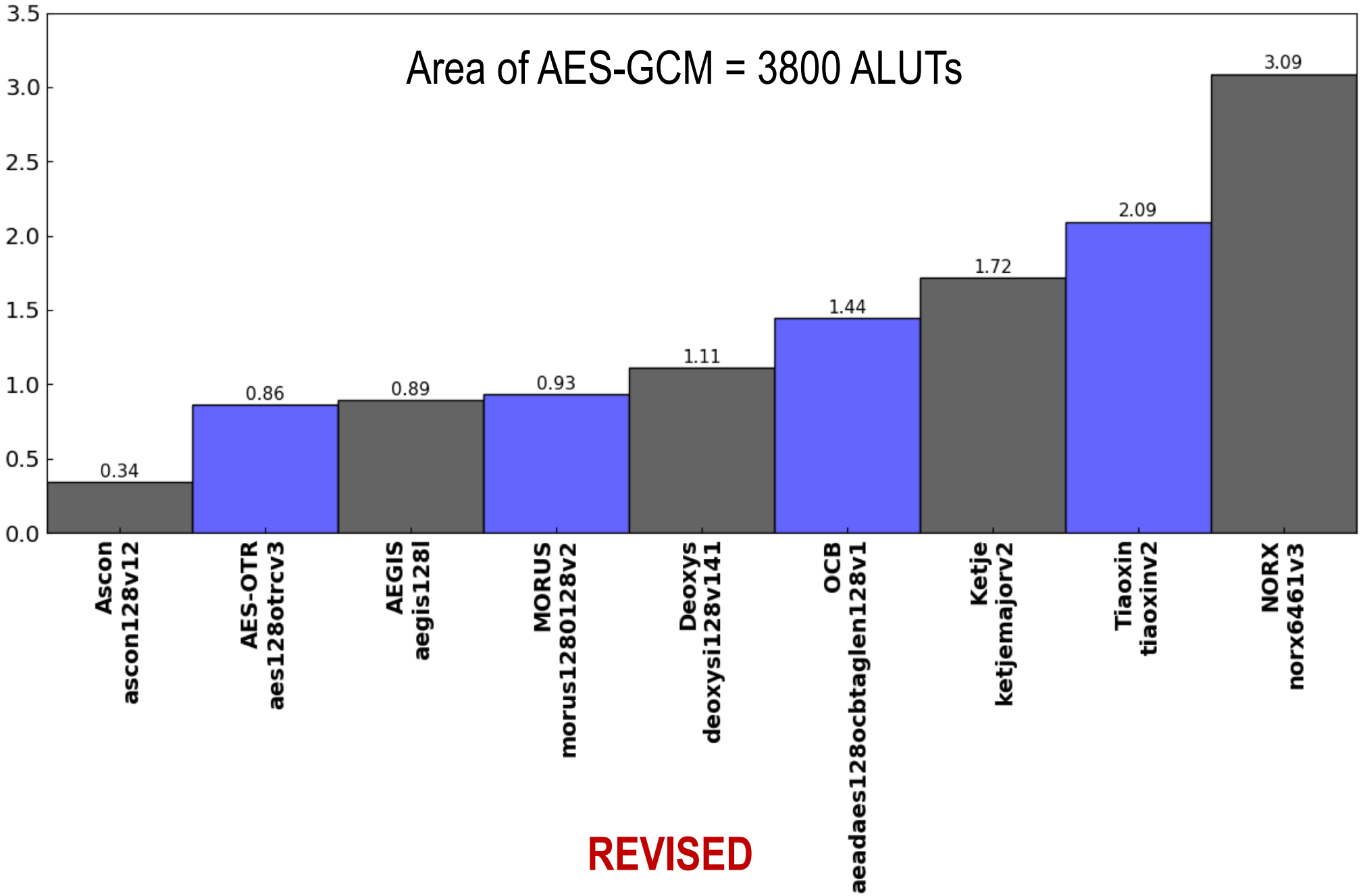
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#ALUTs) in Stratix IV

Ratio of a given Cipher Area/Area of AES-GCM

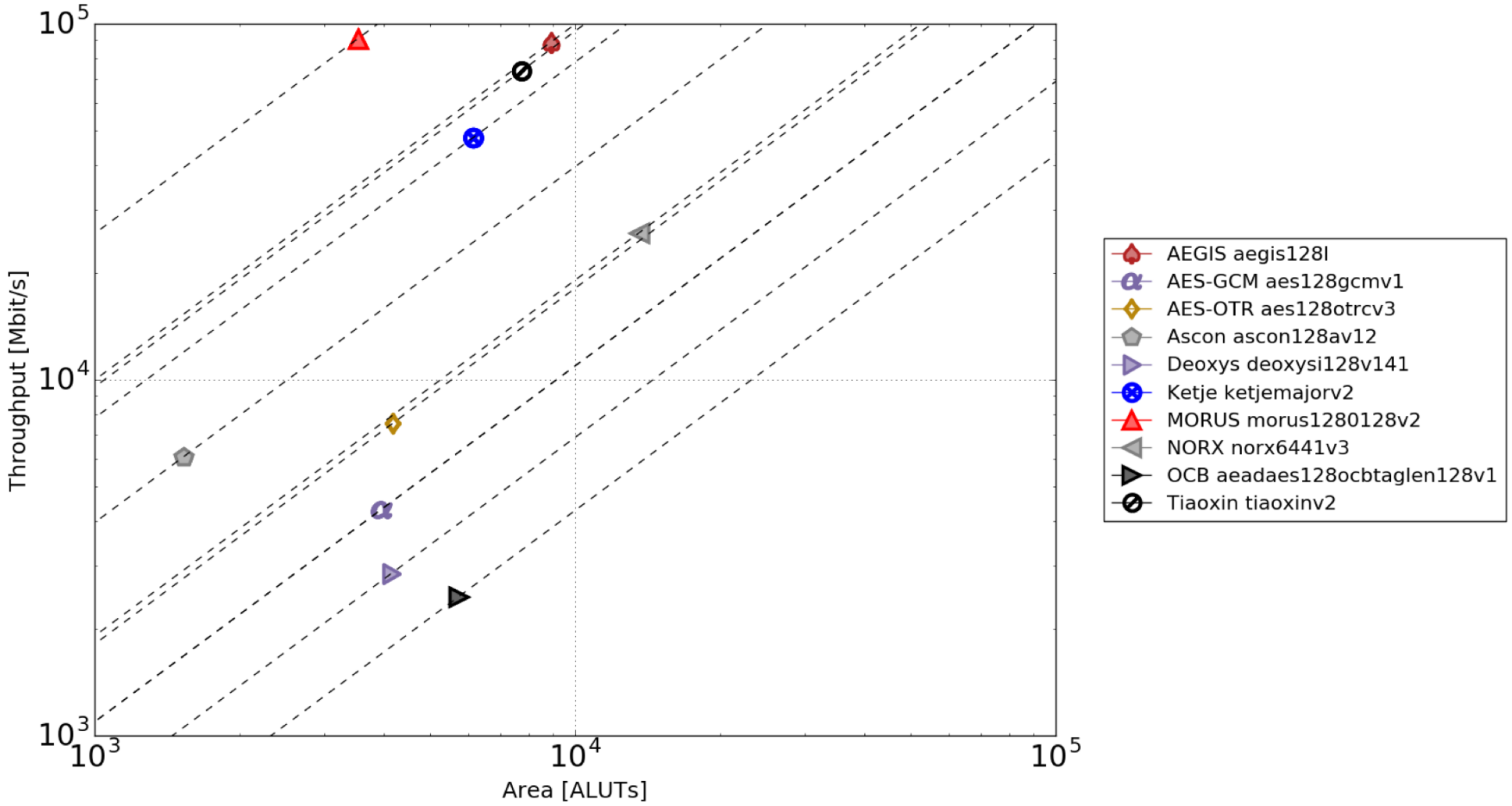


REVISED

Stratix V

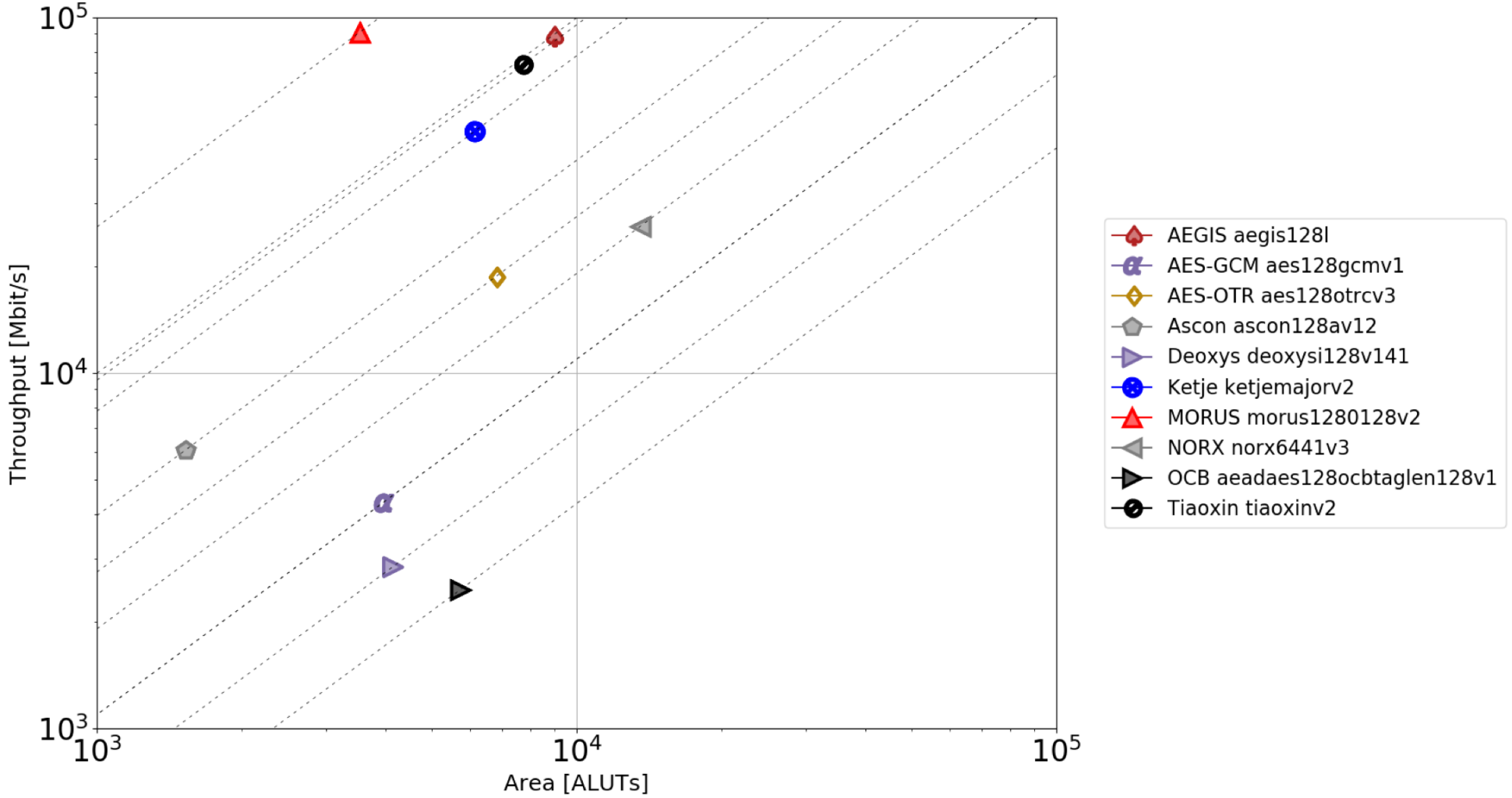
Results for Stratix V – Throughput vs. Area Logarithmic Scale

ORIGINAL

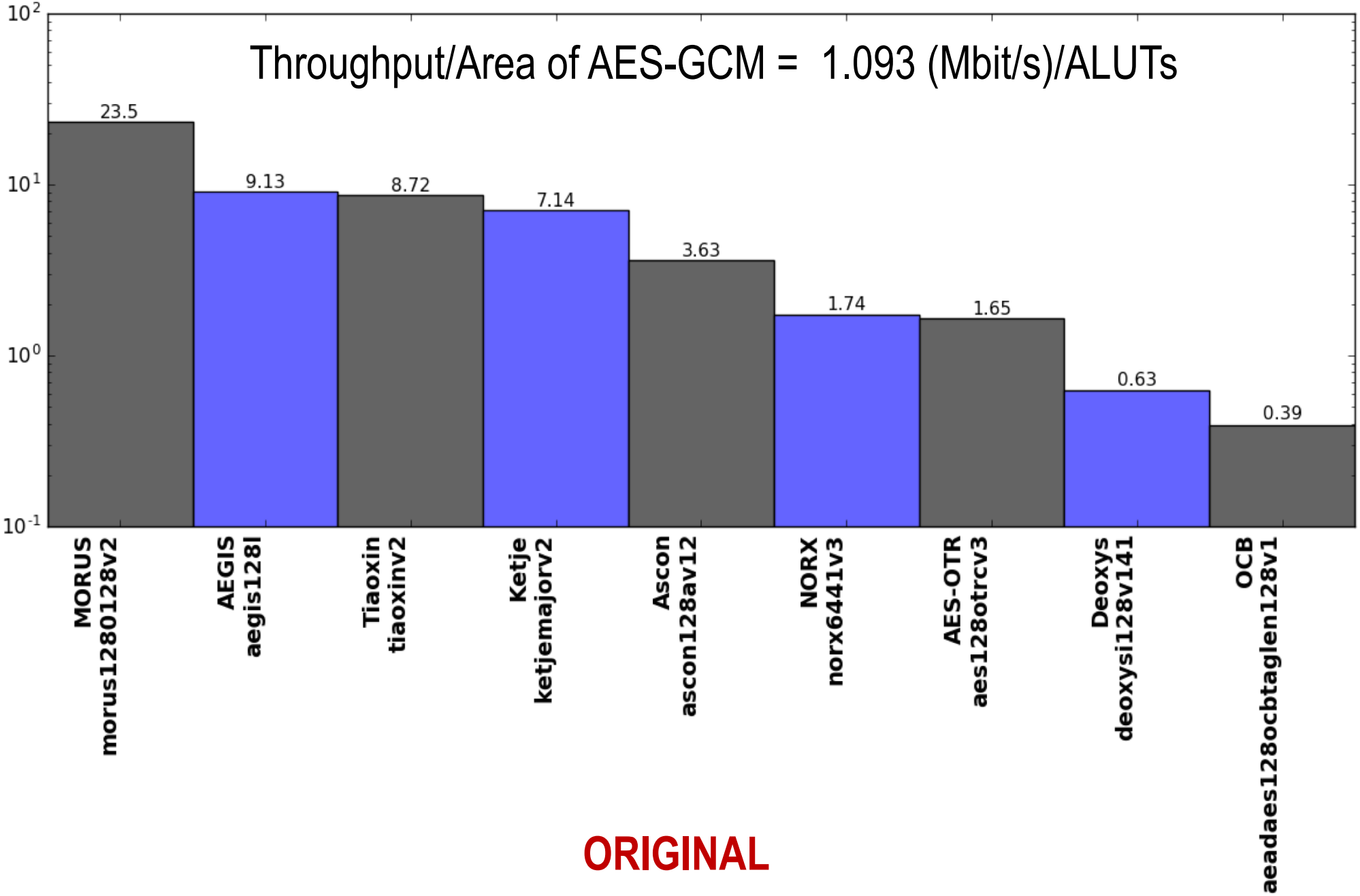


Results for Stratix V – Throughput vs. Area Logarithmic Scale

REVISED

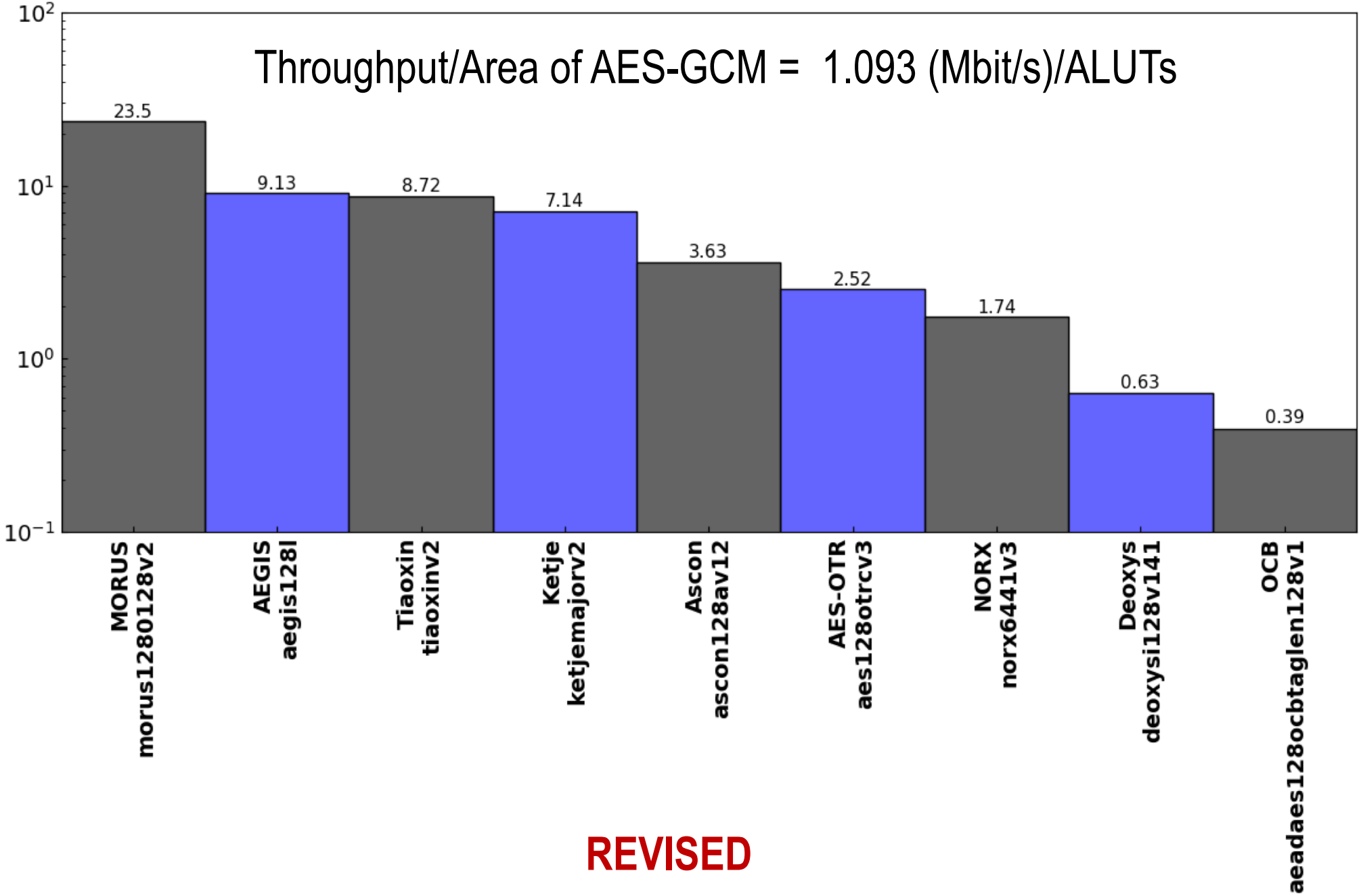


Relative Throughput/Area in Stratix V vs. AES-GCM



ORIGINAL

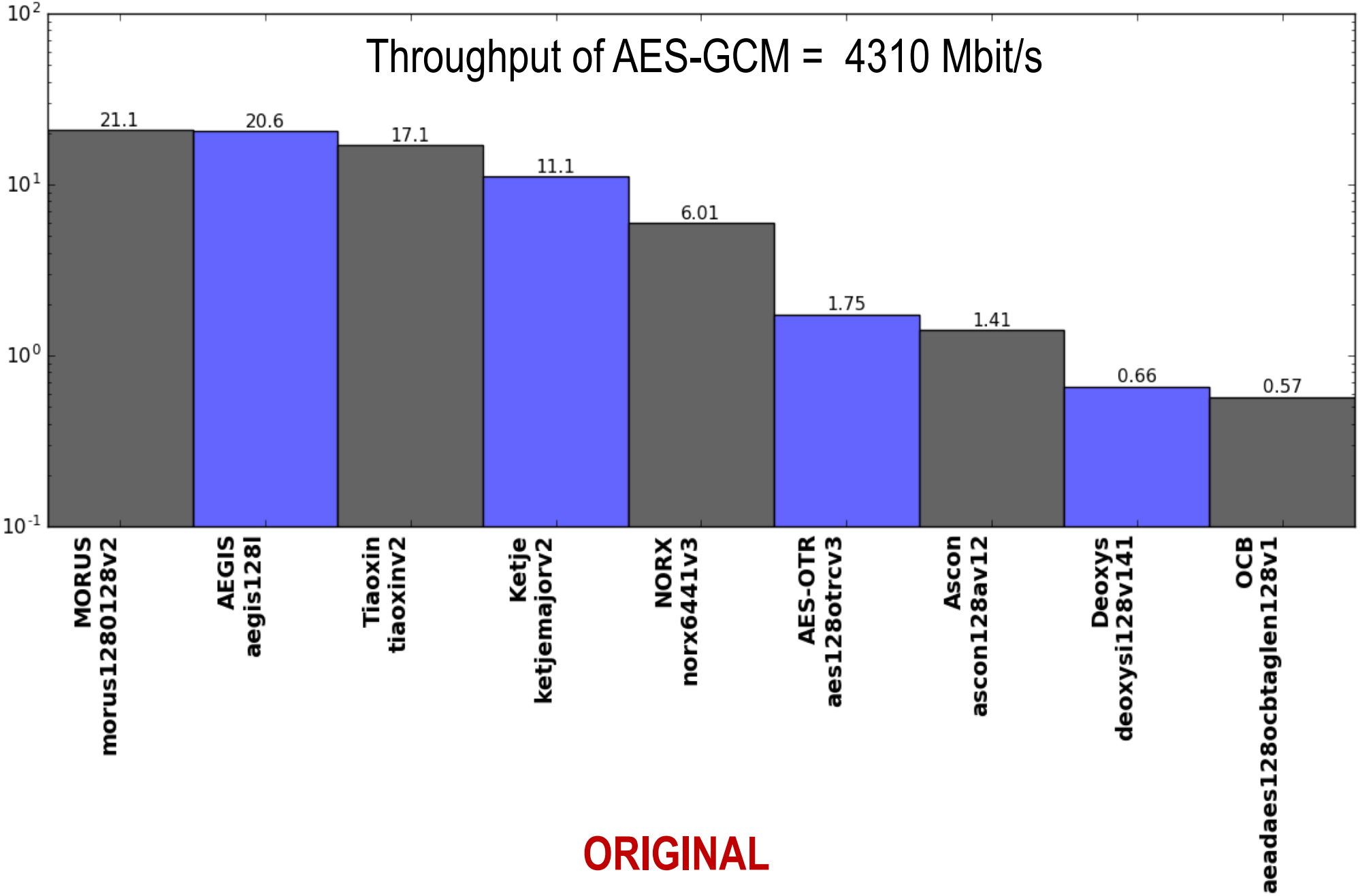
Relative Throughput/Area in Stratix V vs. AES-GCM



REVISED

Relative Throughput in Stratix V

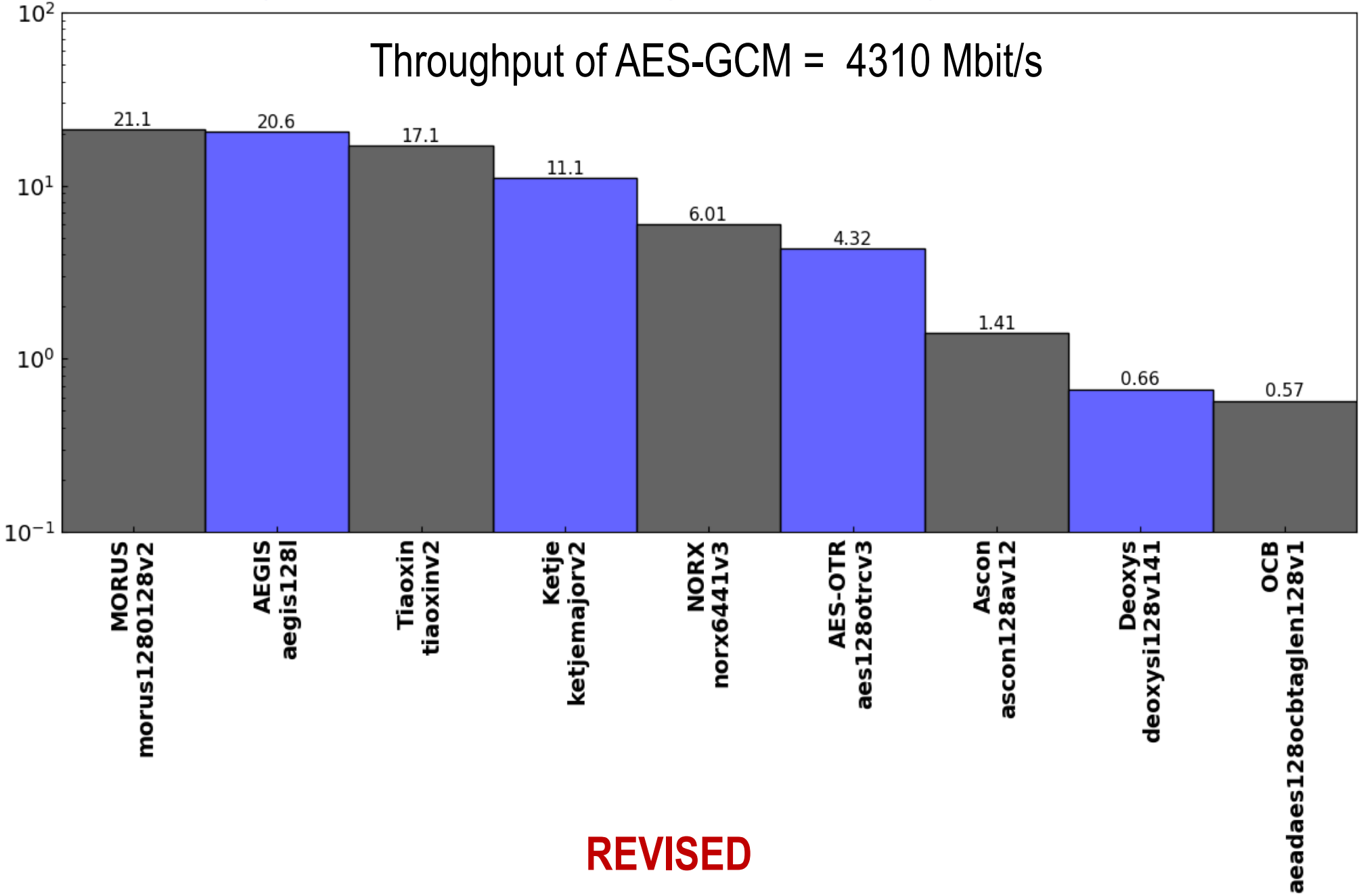
Ratio of a given Cipher Throughput/Throughput of AES-GCM



ORIGINAL

Relative Throughput in Stratix V

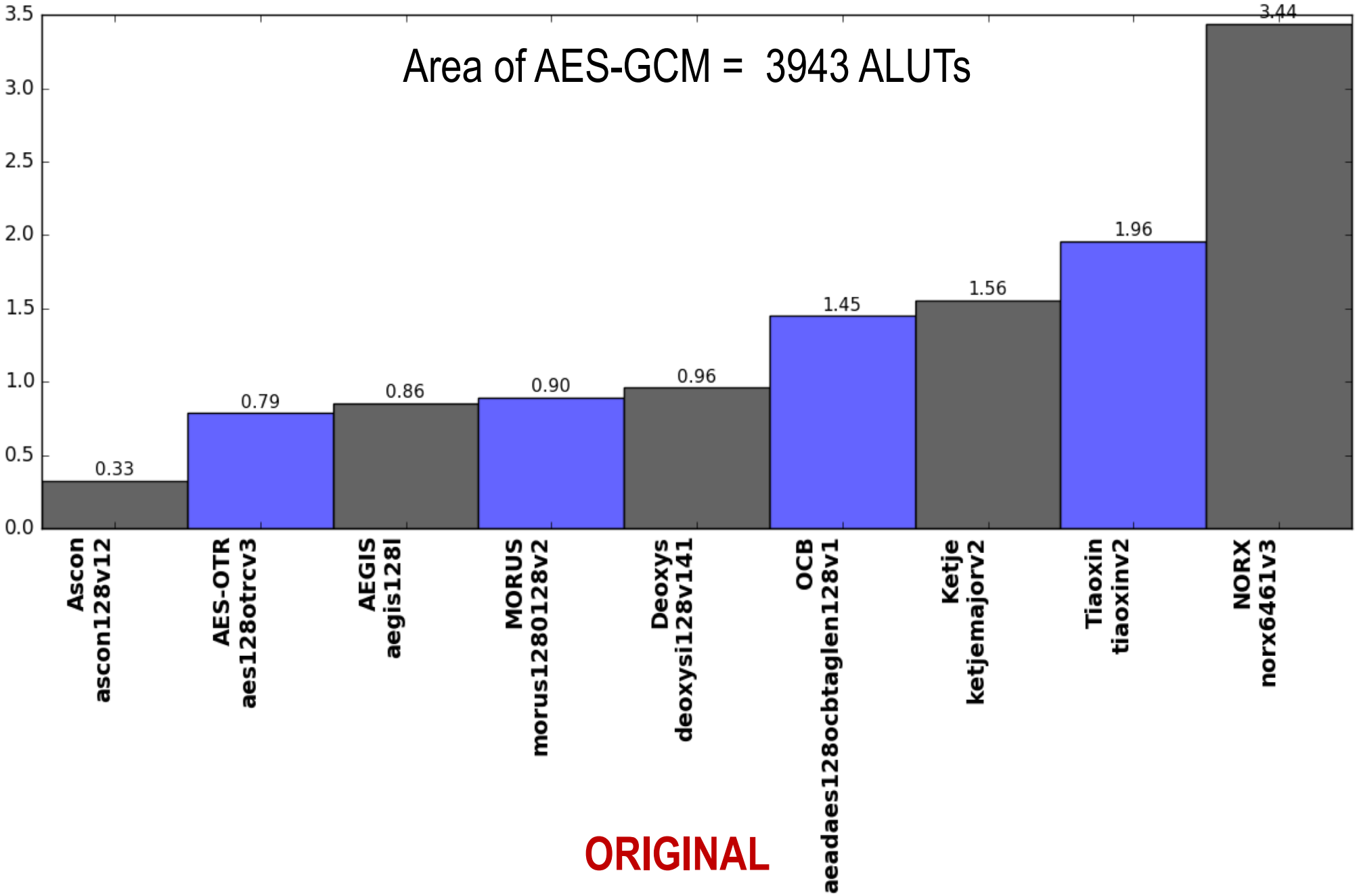
Ratio of a given Cipher Throughput/Throughput of AES-GCM



REVISED

Relative Area (#ALUTs) in Stratix V

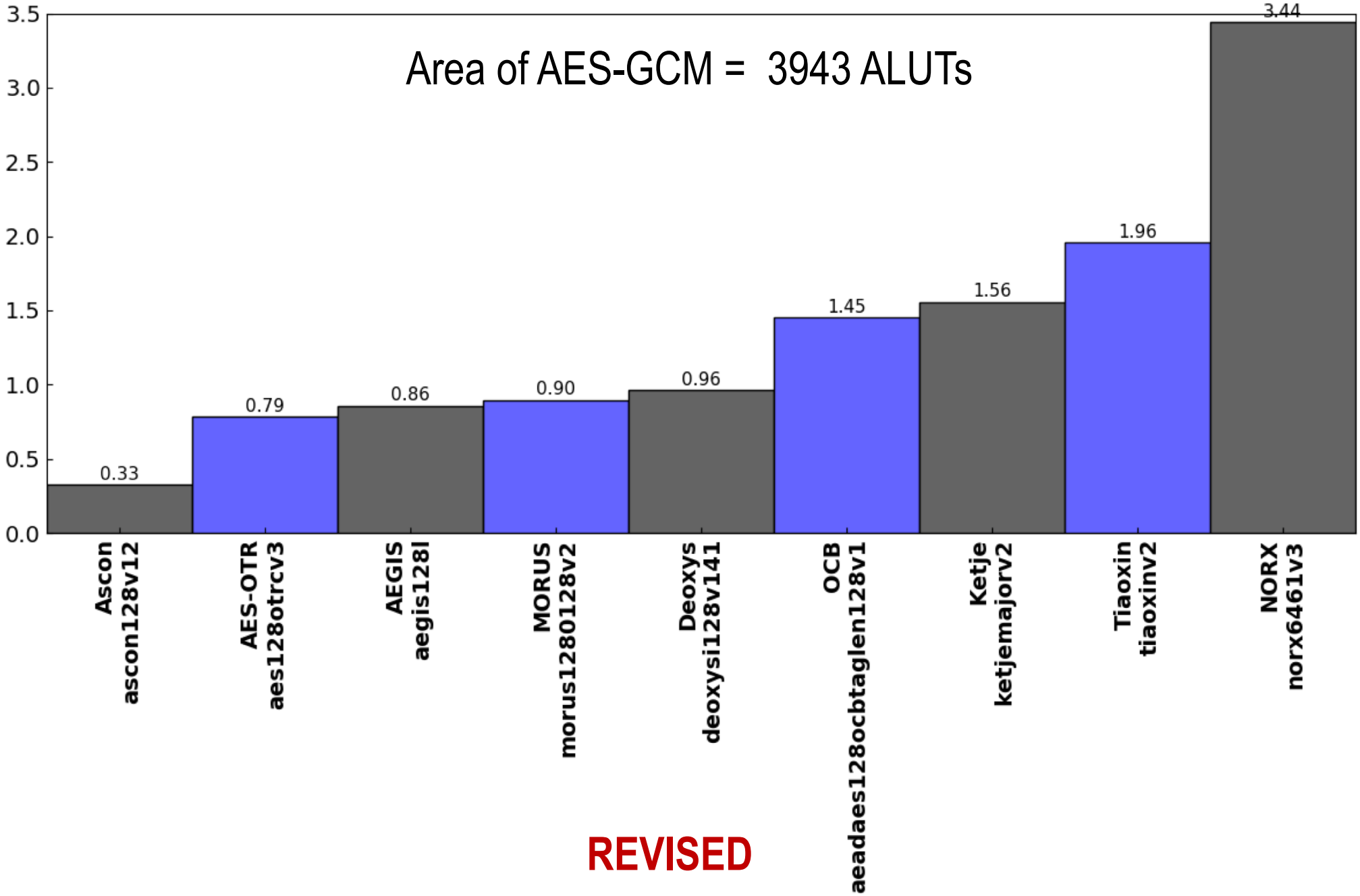
Ratio of a given Cipher Area/Area of AES-GCM



ORIGINAL

Relative Area (#ALUTs) in Stratix V

Ratio of a given Cipher Area/Area of AES-GCM



REVISED

Conclusions

- In terms of the Throughput/Area Ratio
  - In Virtex 6 and 7, position of AES-OTR did not change
  - In Stratix IV and V, revised AES-OTR outperformed NORX
- In terms of Throughput
  - In Virtex 6 and 7, revised AES-OTR outperformed ACORN and Keyak
  - In Stratix IV and V, revised AES-OTR outperformed ACORN

Conclusions (cont.)

- In terms of Area
  - In Virtex 6, SILC & CLOC outperformed NORX and AES-JAMBU
  - In Virtex 7
    SILC outperformed AES-OTR, JAMBU-AES, Ketje, and Ascon

    CLOC outperformed Deoxys, AEGIS, AES-OTR, JAMBU-AES, Ketje, and Ascon
- For candidates in Use Case 2, no changes in rankings occurred for either Throughput/Area, Throughput, or Area