

QP Testing

Performance Test Results

Crypt ALARM



-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**

-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**

<u>File</u>	<u>Size (byte)</u>
• 10Mzeri.bin	• 10.485.760
• 100Mzeri.bin	• 104.857.600
• SaveAsPDF.exe	• 936.168
• ubuntu-10.10-desktop-i386.iso	• 726.827.008
• videoH264_1h.mp4	• 198.889.939
• videomp4.mp4	• 3.540.923.949
• Visual Basic Language Specification 10.0.docx	• 2.258.293
• FOndazione Italia Giappone.pdf	• 2.290.073

- **QP_Dyn (256 & 1152)**

- Buffer size 400 byte e 10.000 byte
- Versione per windows: utilizzata la libreria fornita da CA durante il primo incontro a Roma
- Versione per uBuntu: utilizzata libreria fornita da CA via email
- Parametri di input: utilizzati quelli forniti da CA

- **AES, TwoFish, RSA, Diffie-Hellman (DH), Curve Ellittiche**

- Utilizzata la libreria Crypto++ ver.5.6.1
- AES e TwoFish utilizzata la modalità OFB

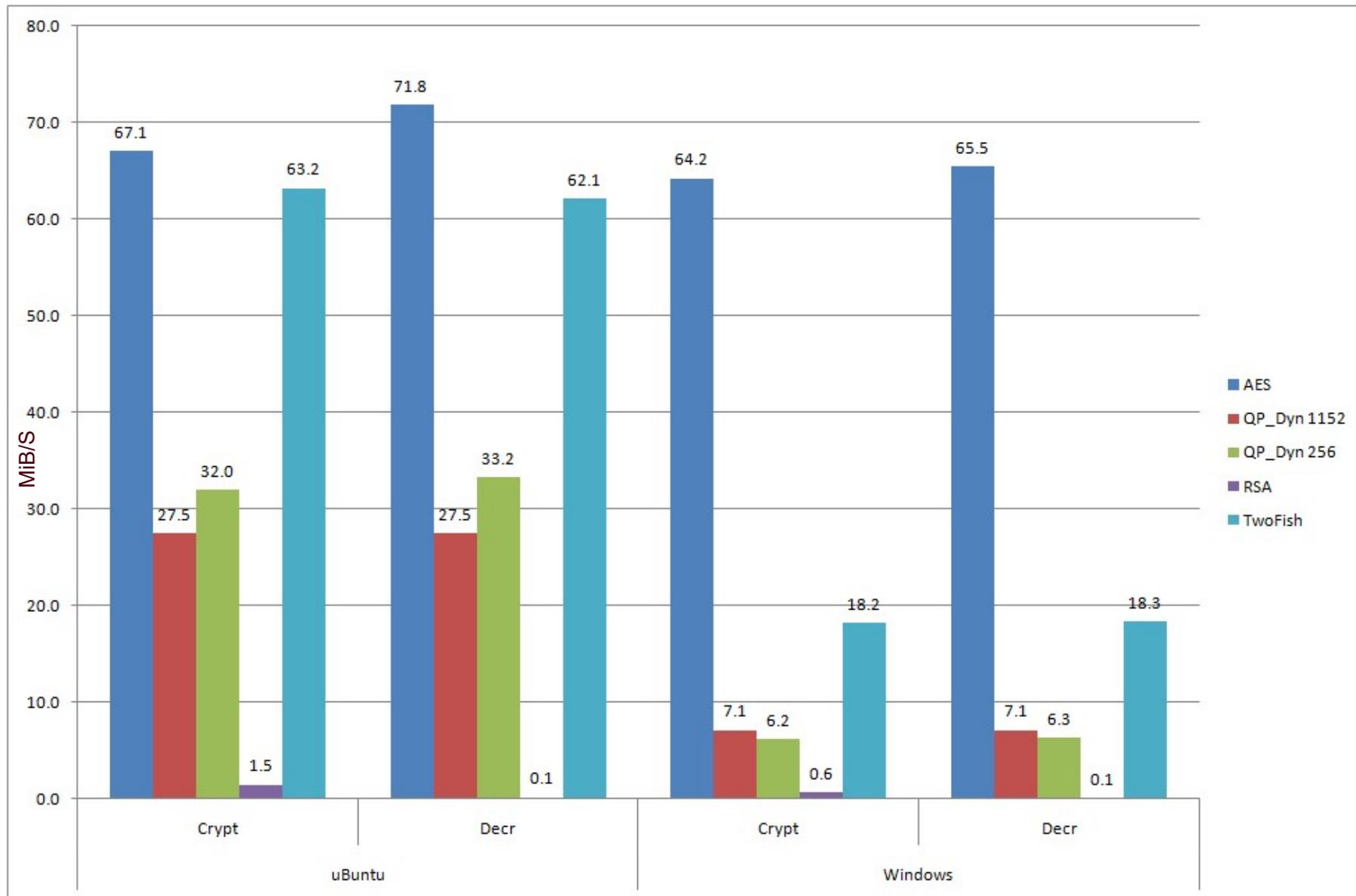
- **HW**

- HP 4530s
- Processore Core i5 2410M, 2.3GHz
- RAM 4GB 1.333 MHz
- HD 640 GB 5400 rpm

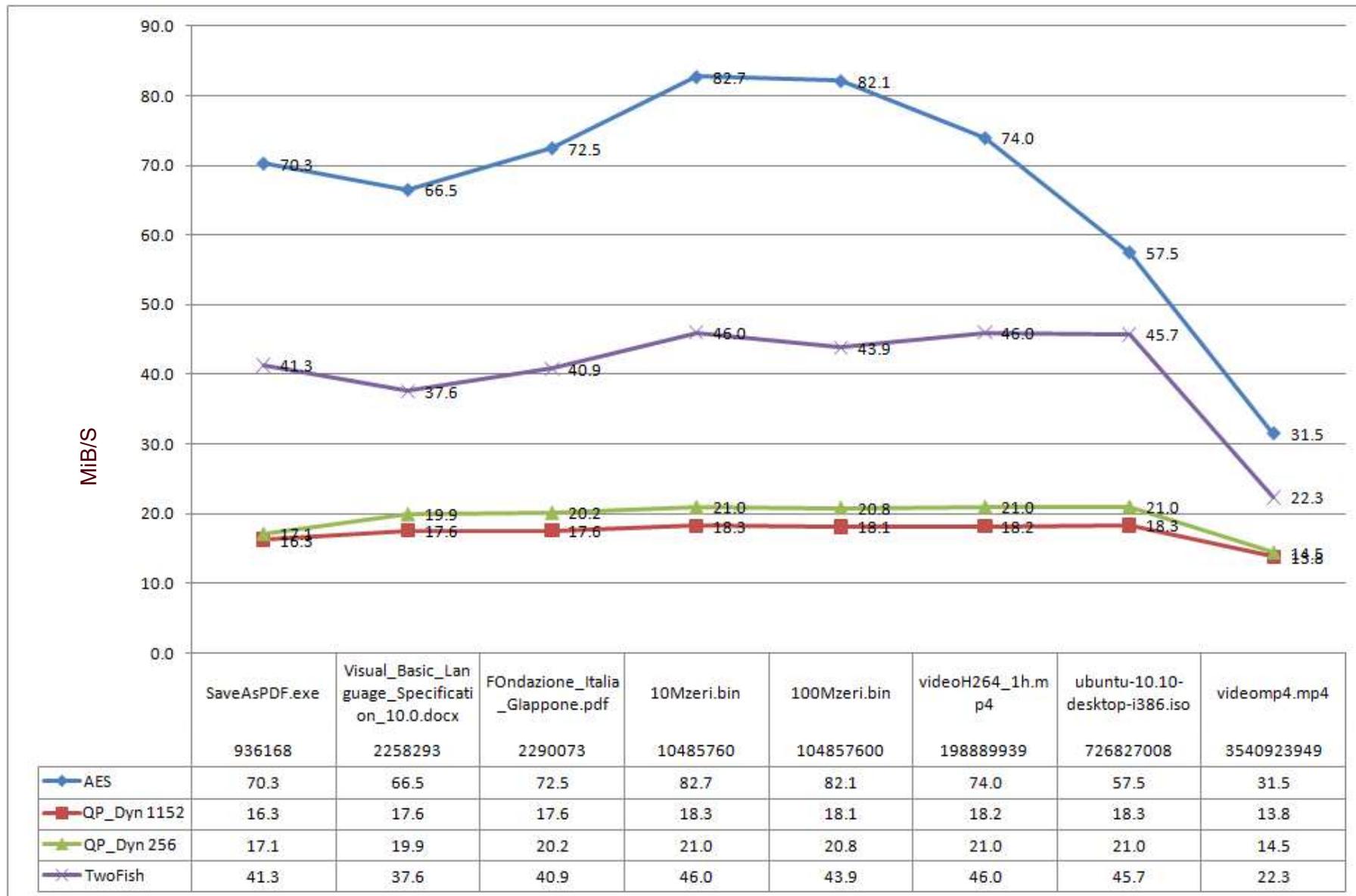
- **OS**

- Windows 7 32 bit
- uBuntu v.10.04

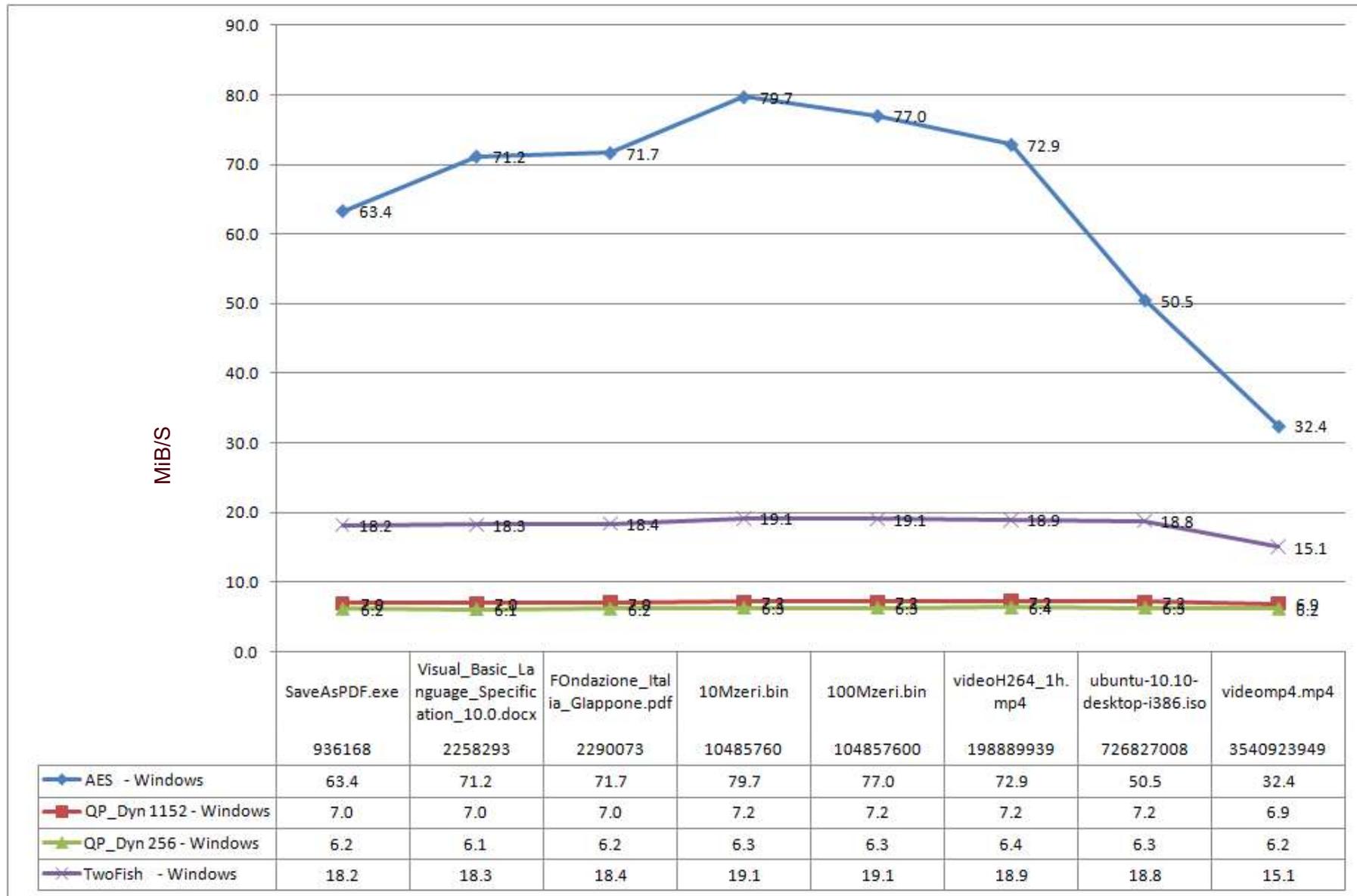
-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**



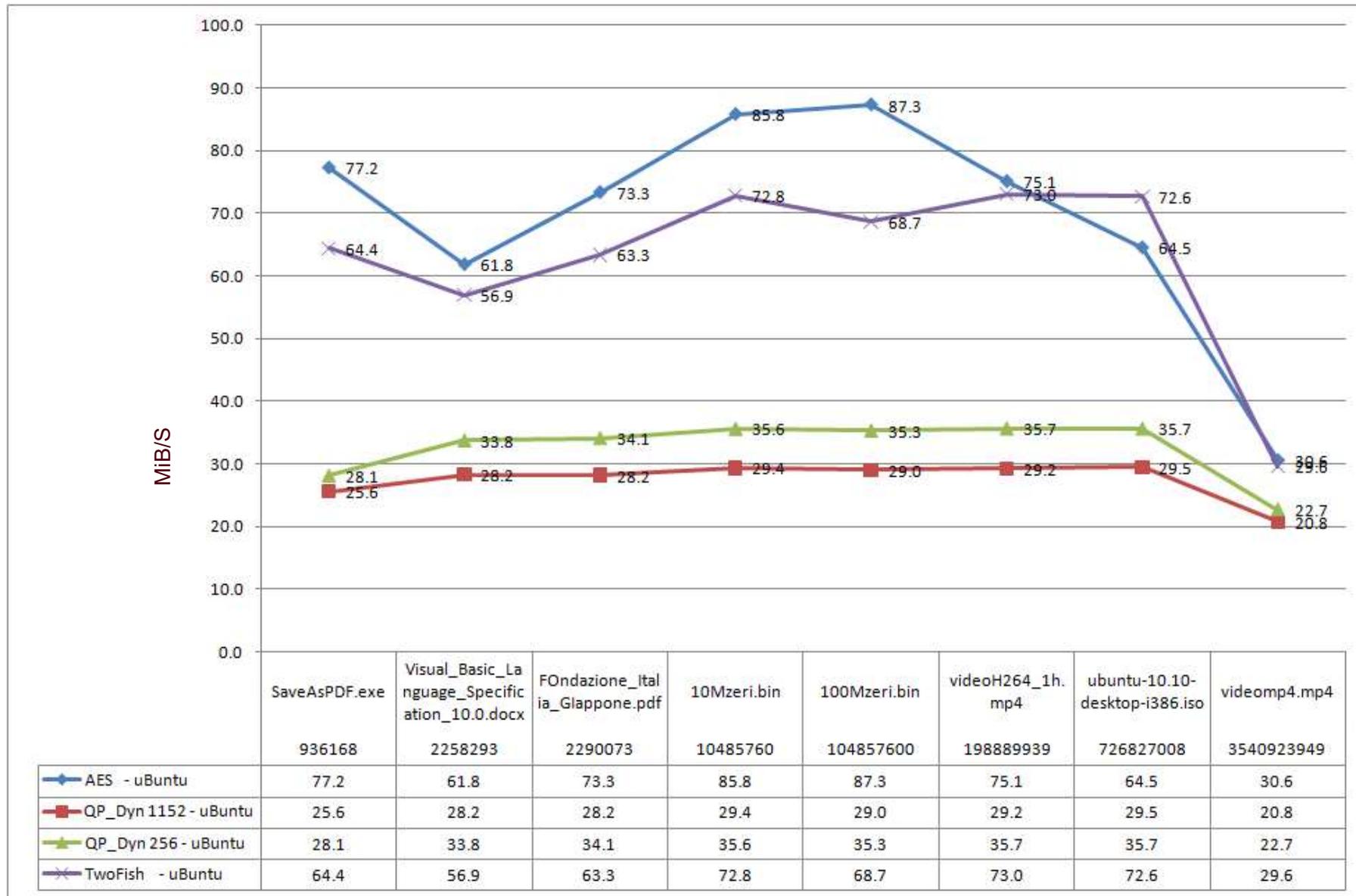
Al variare della del file



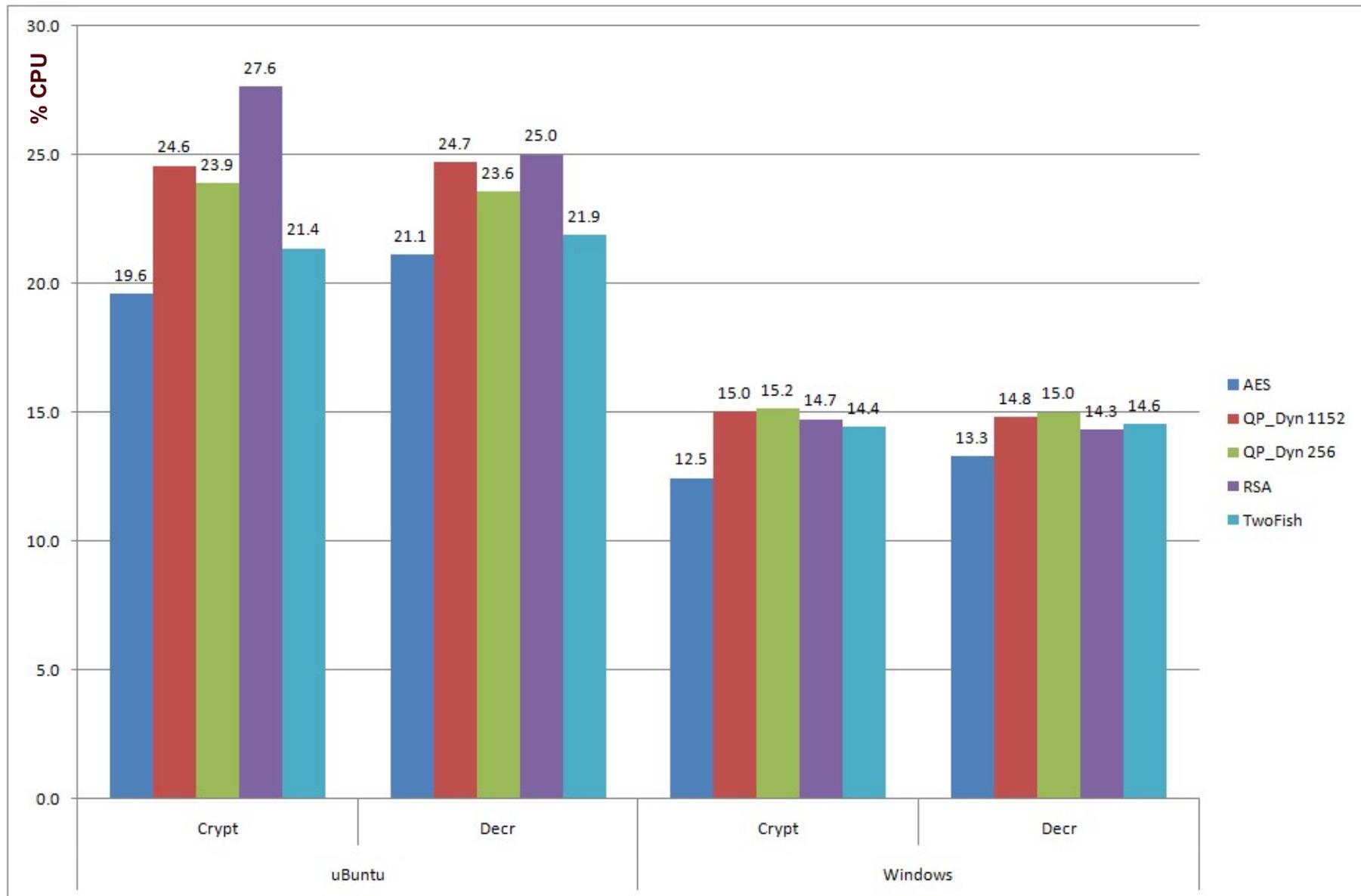
Al variare del file (OS: Windows)



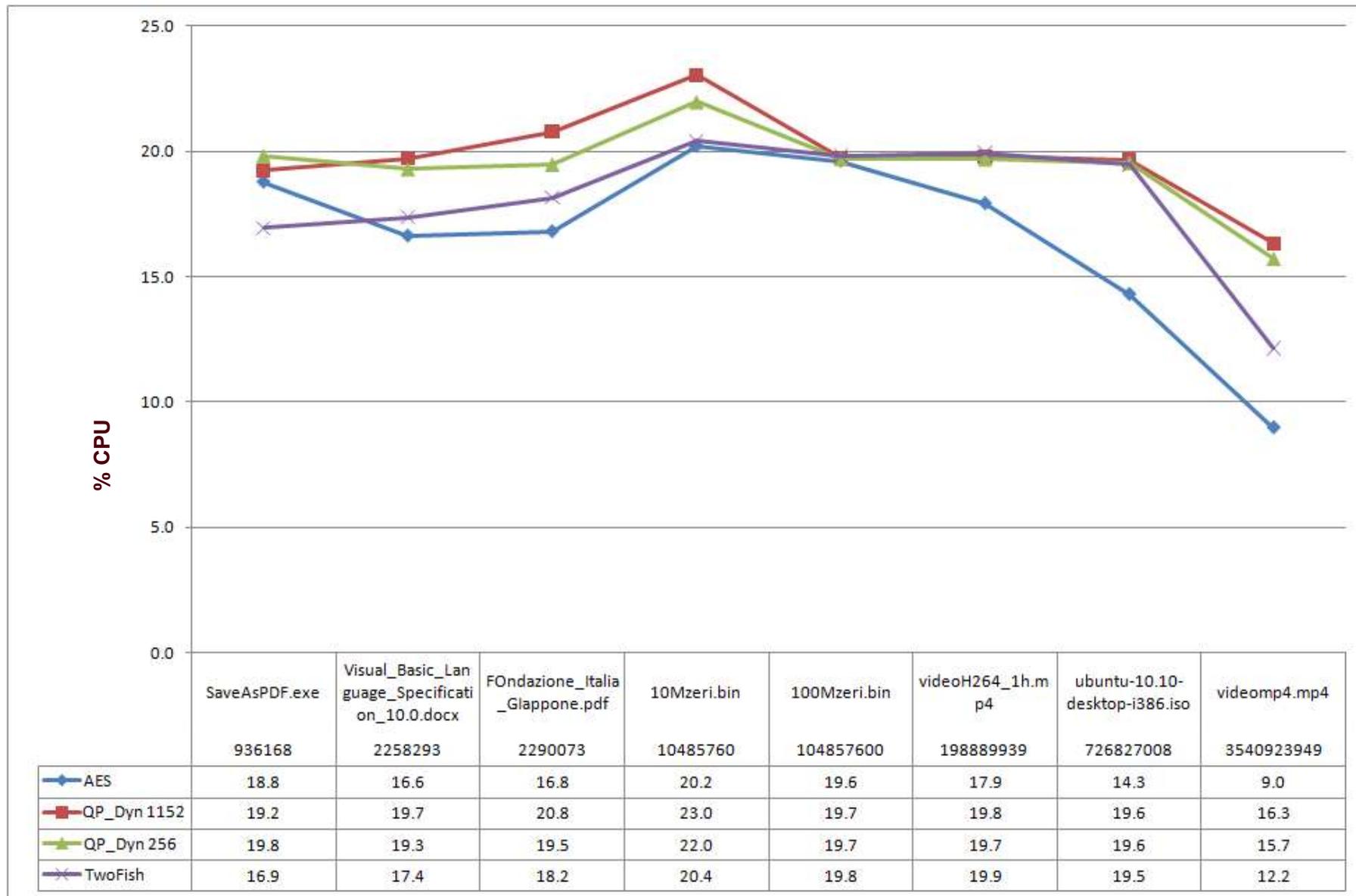
Al variare del file (OS: uBuntu)



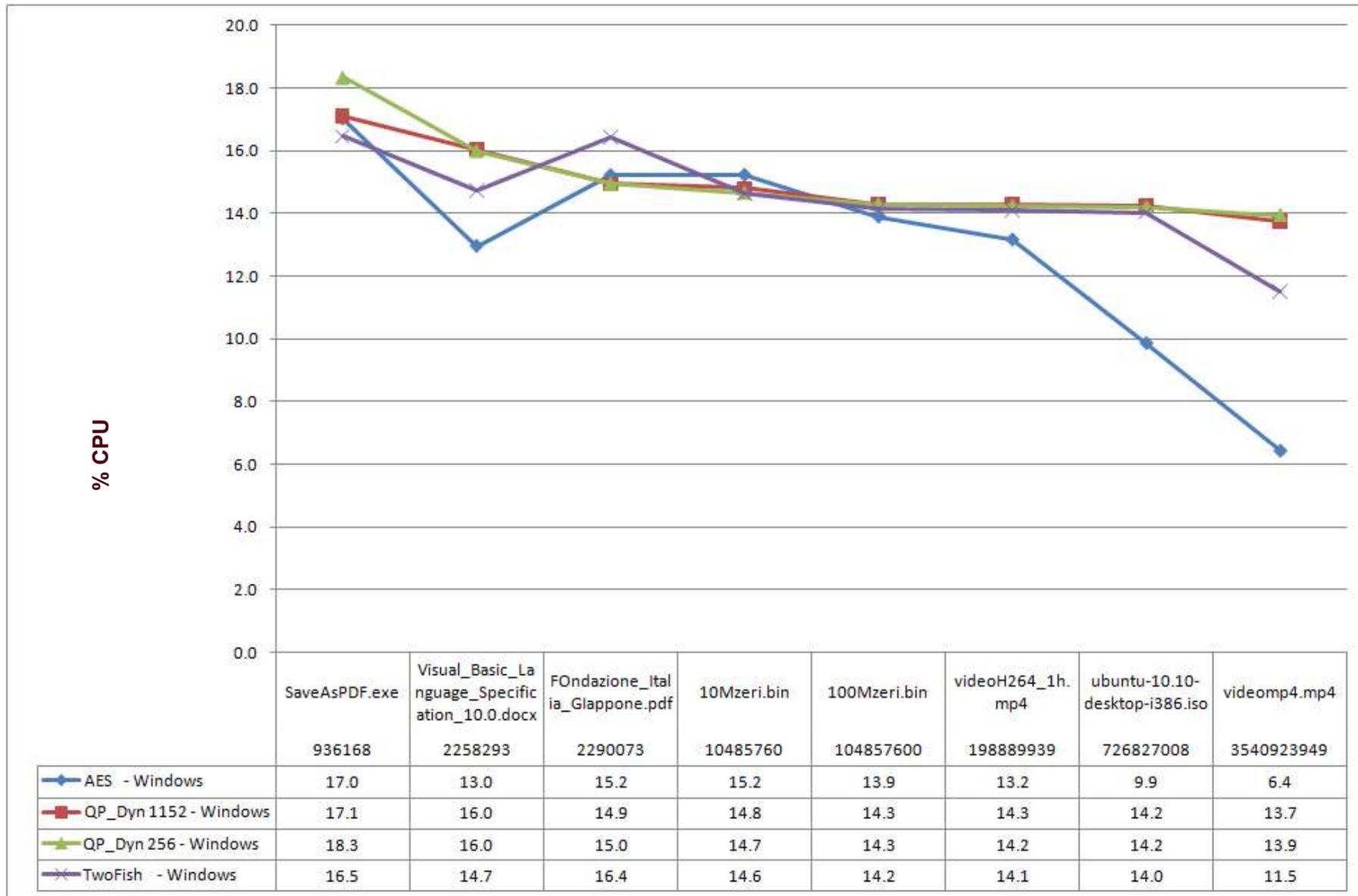
-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**



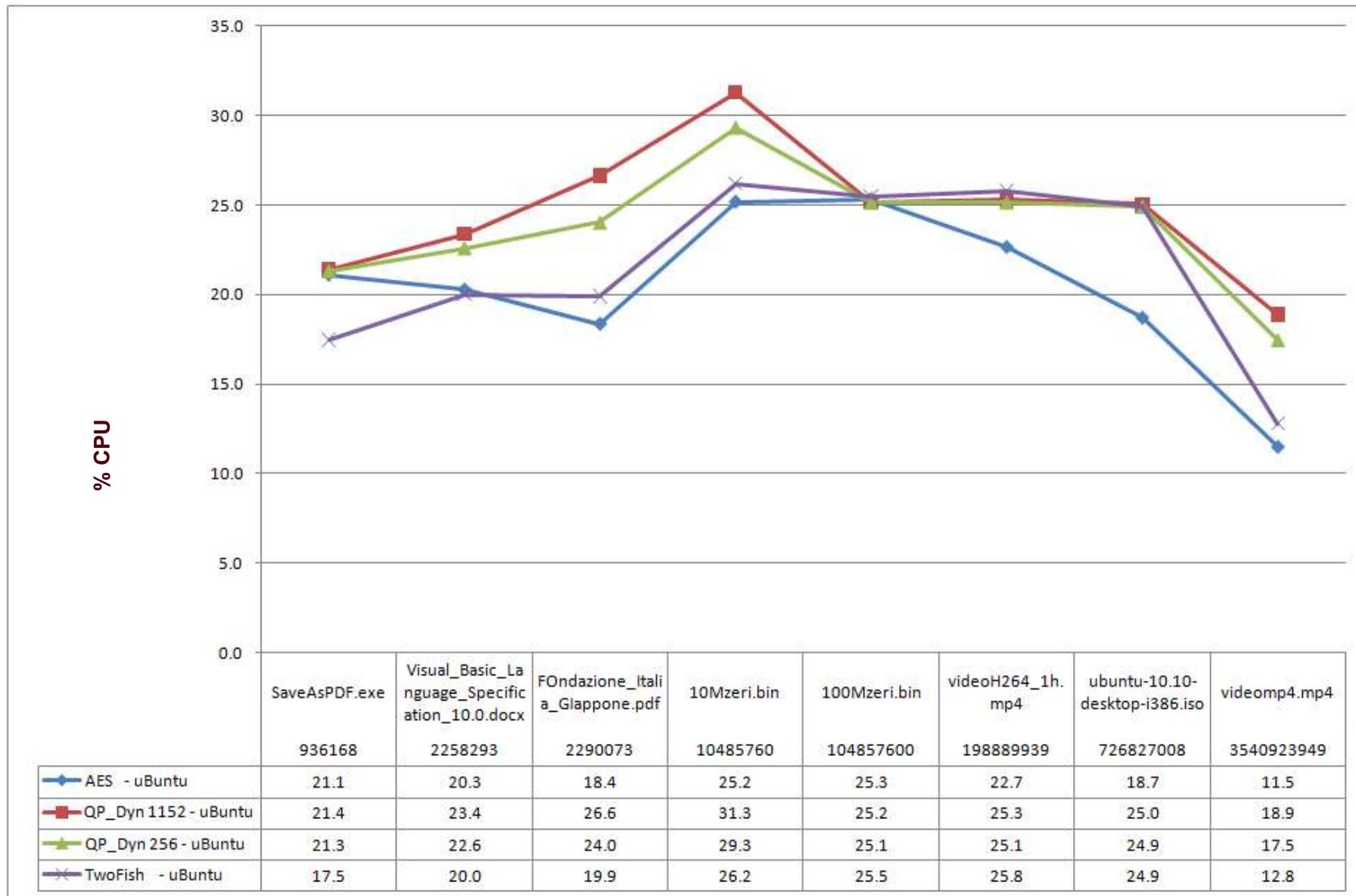
Al variare del del file



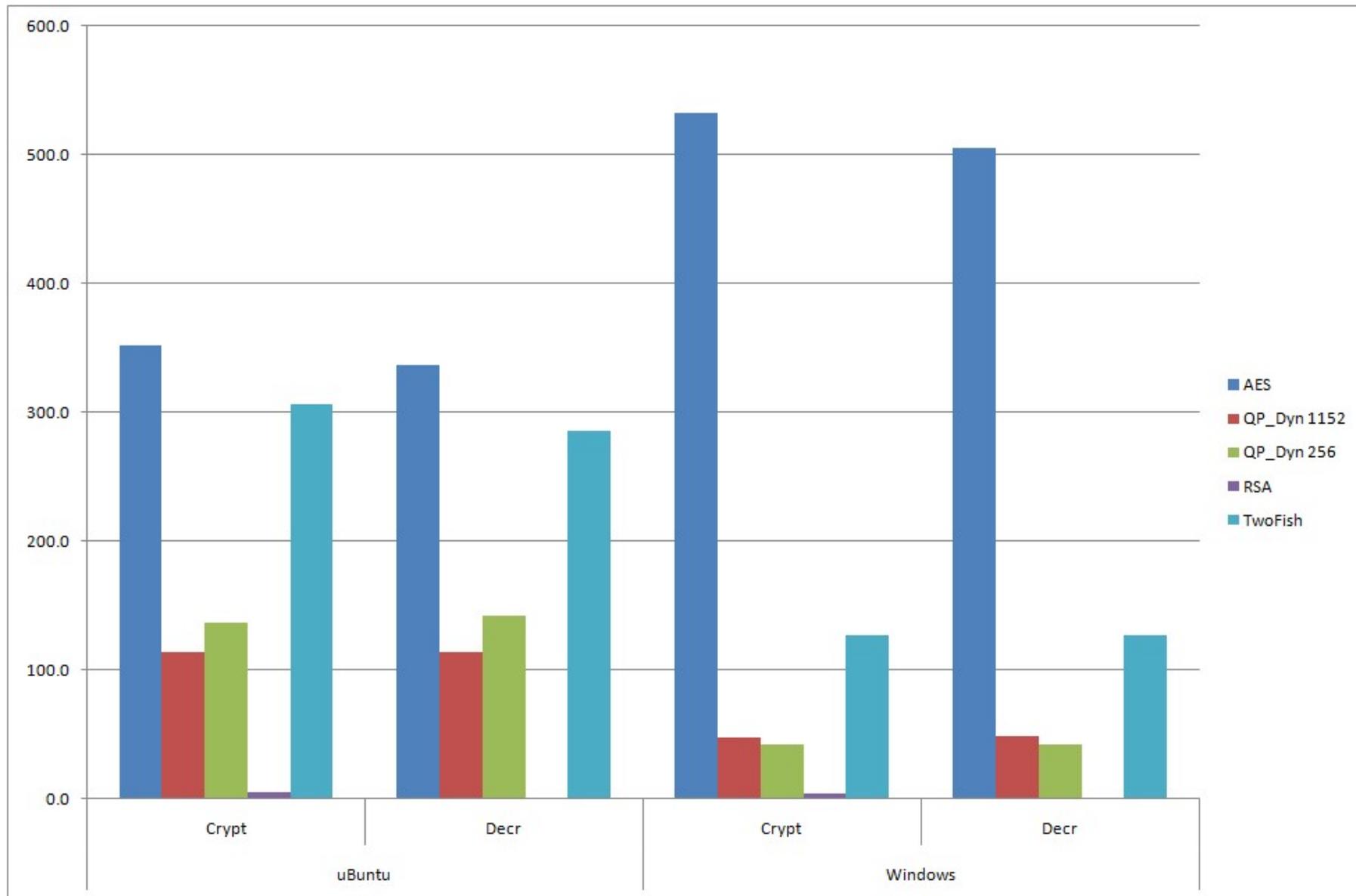
Al variare del file (OS: Windows)



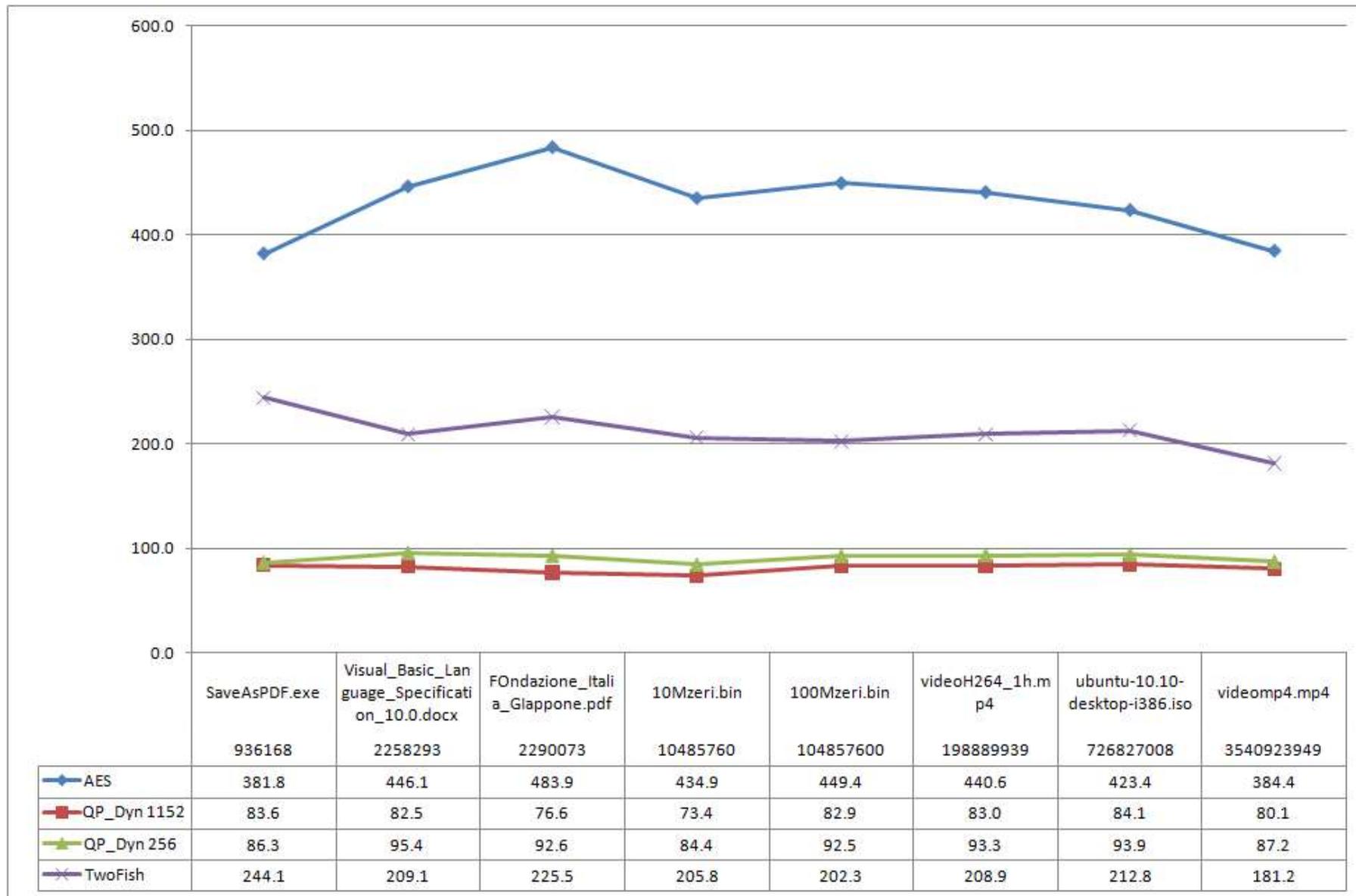
Al variare del file (OS: uBuntu)



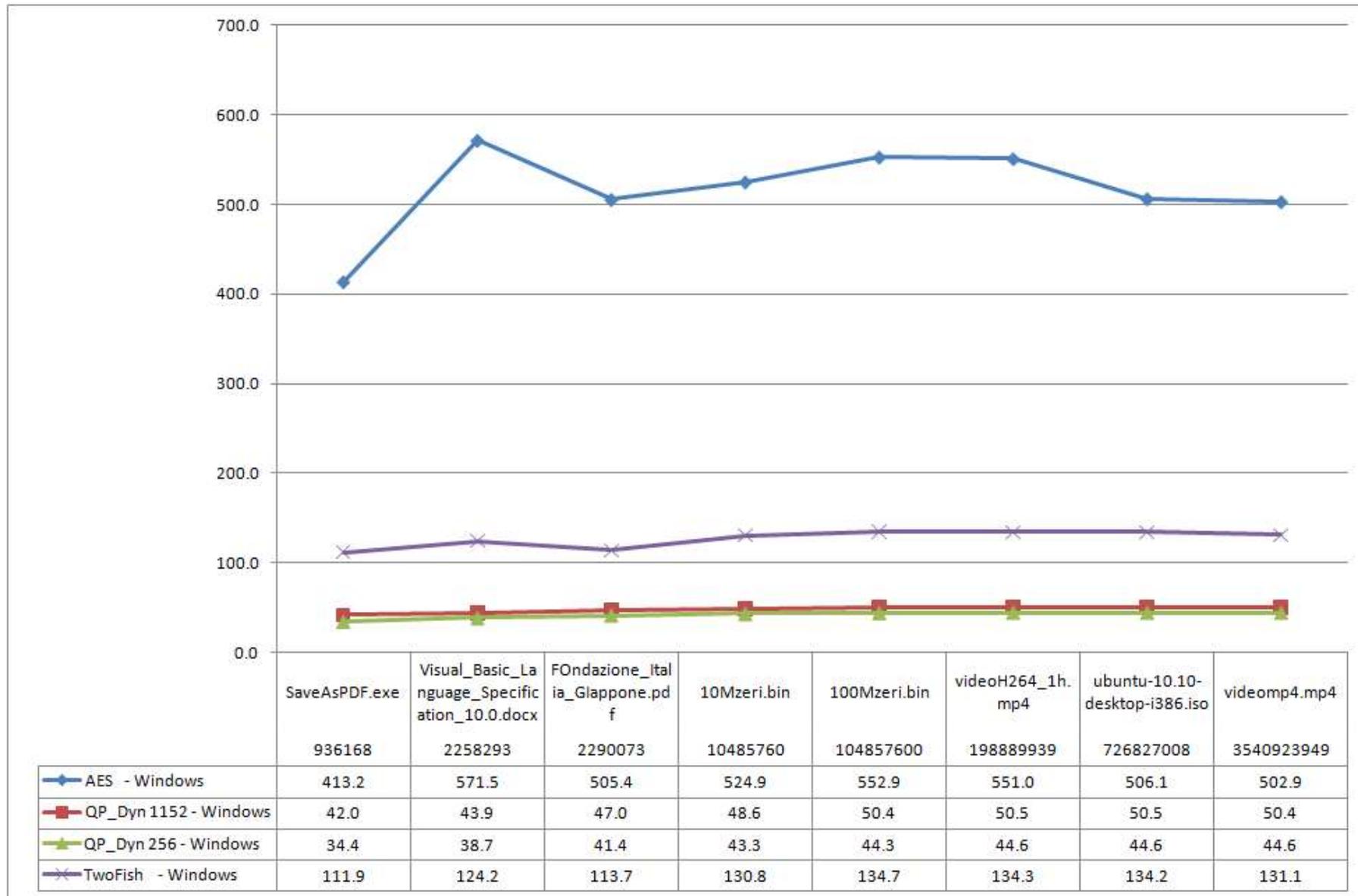
-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**



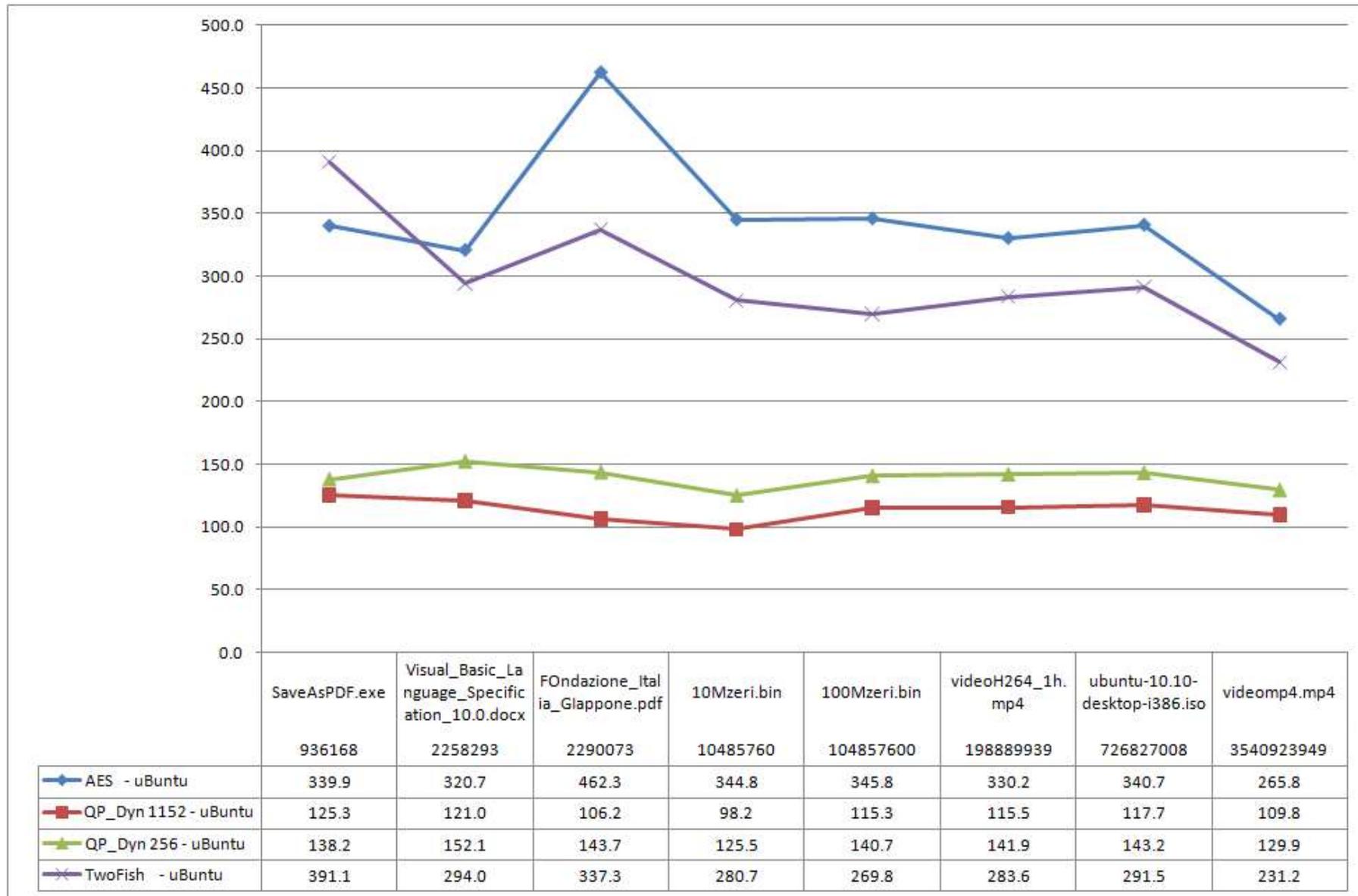
Al variare del del file



Al variare del file (OS: Windows)

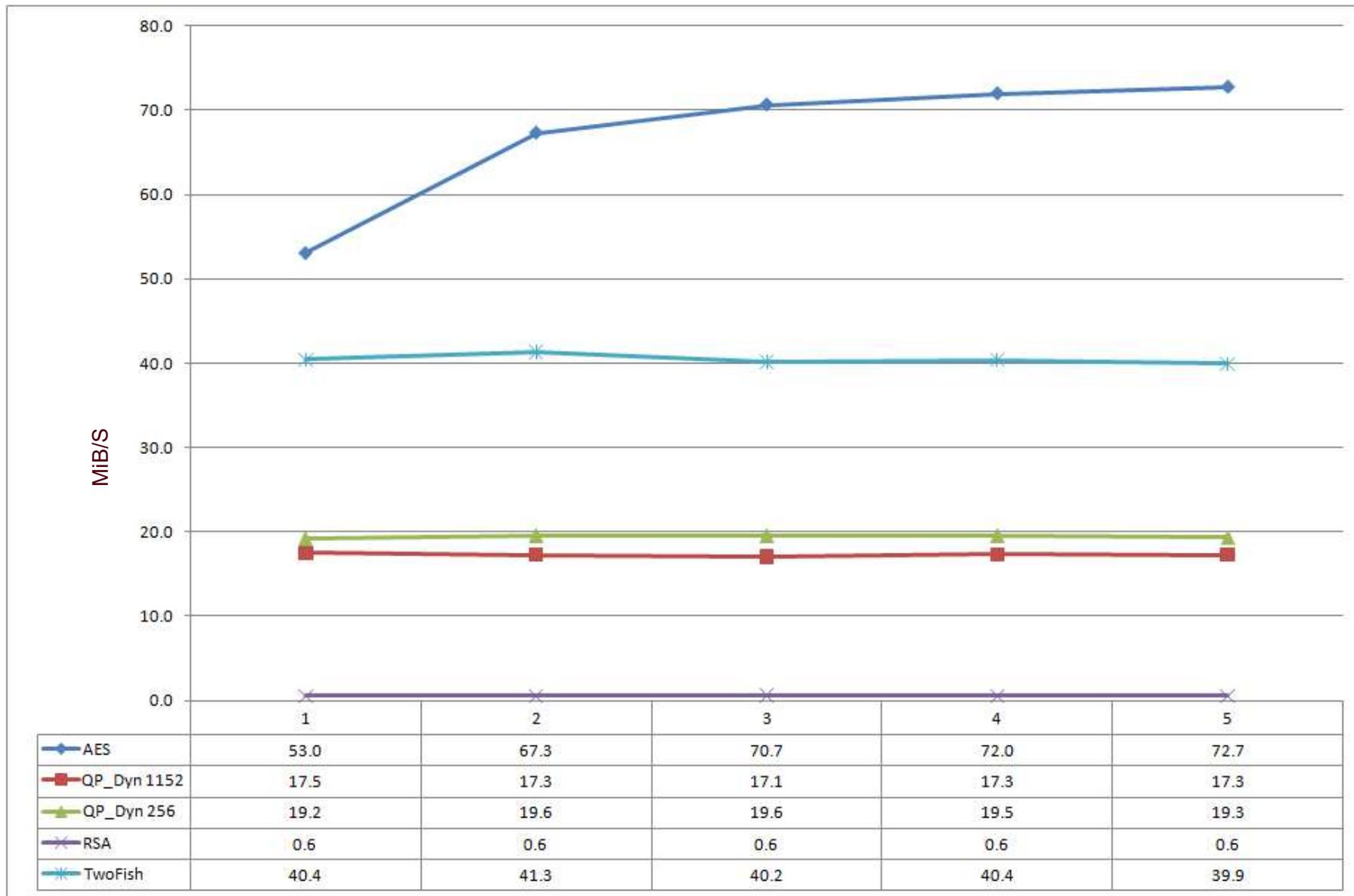


Al variare del file (OS: uBuntu)

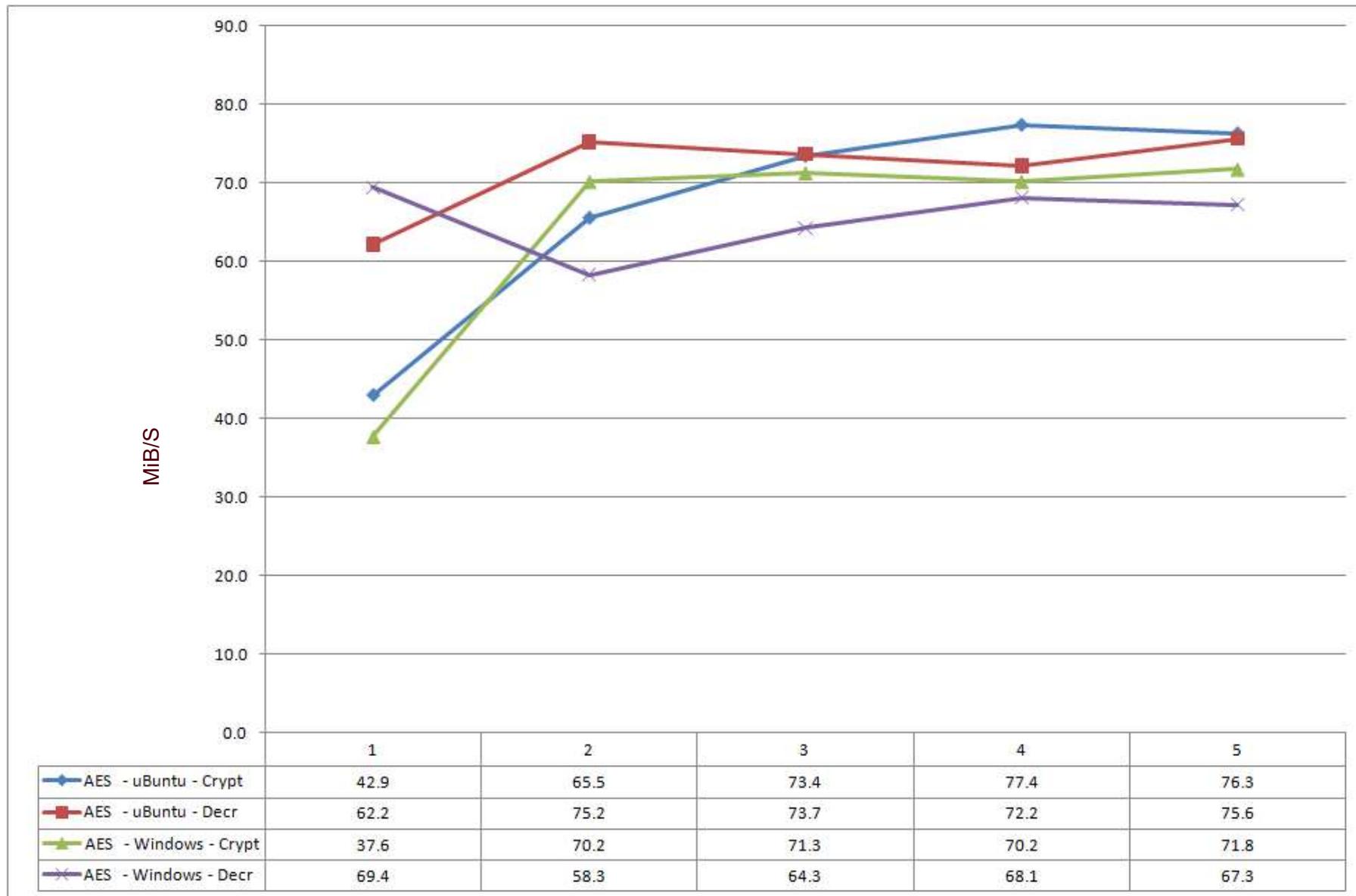


-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**

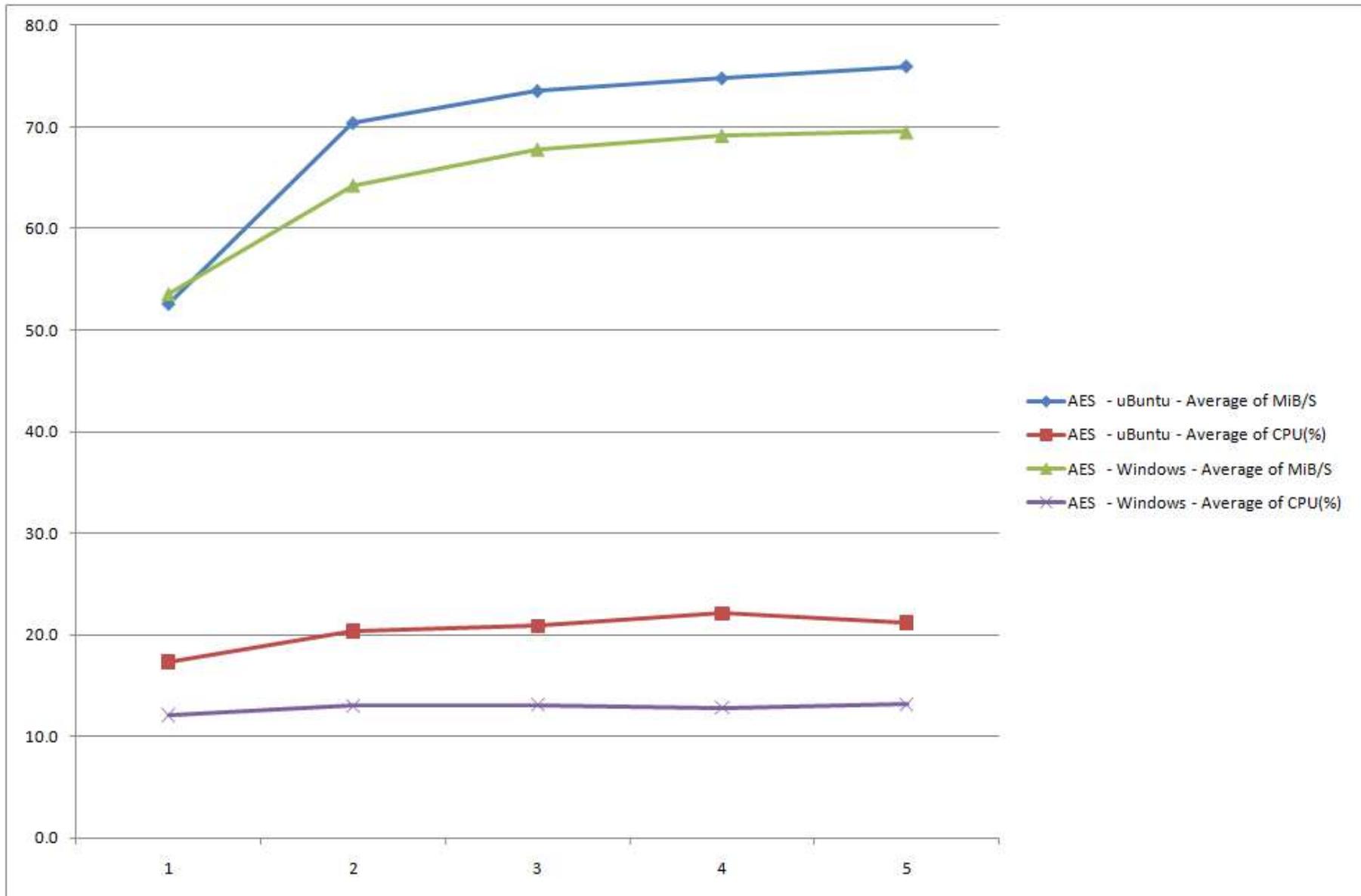
Punto di attenzione: 1° Esecuzione di AES



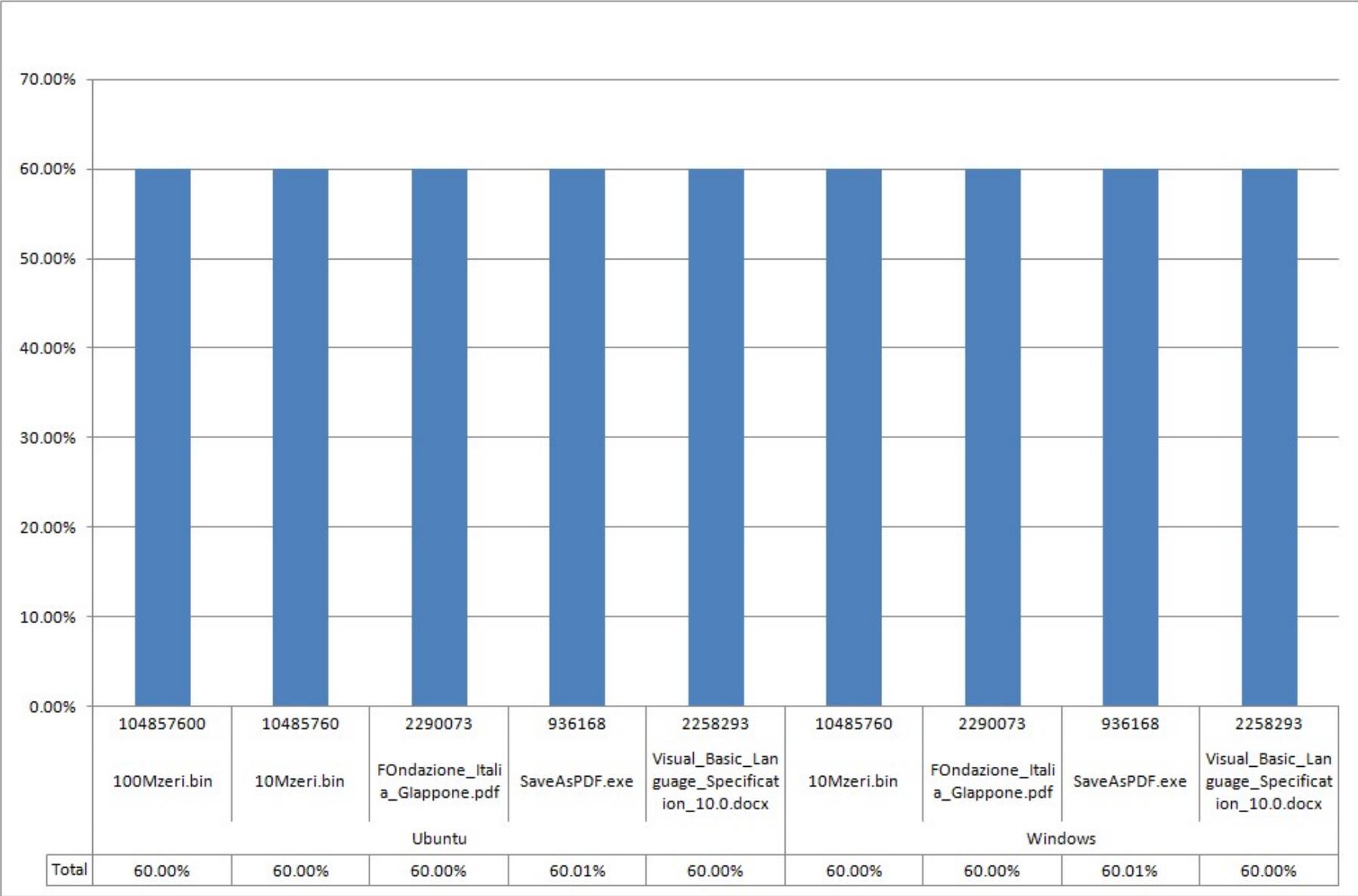
Punto di attenzione: 1° Esecuzione di AES



Punto di attenzione: 1° Esecuzione di AES

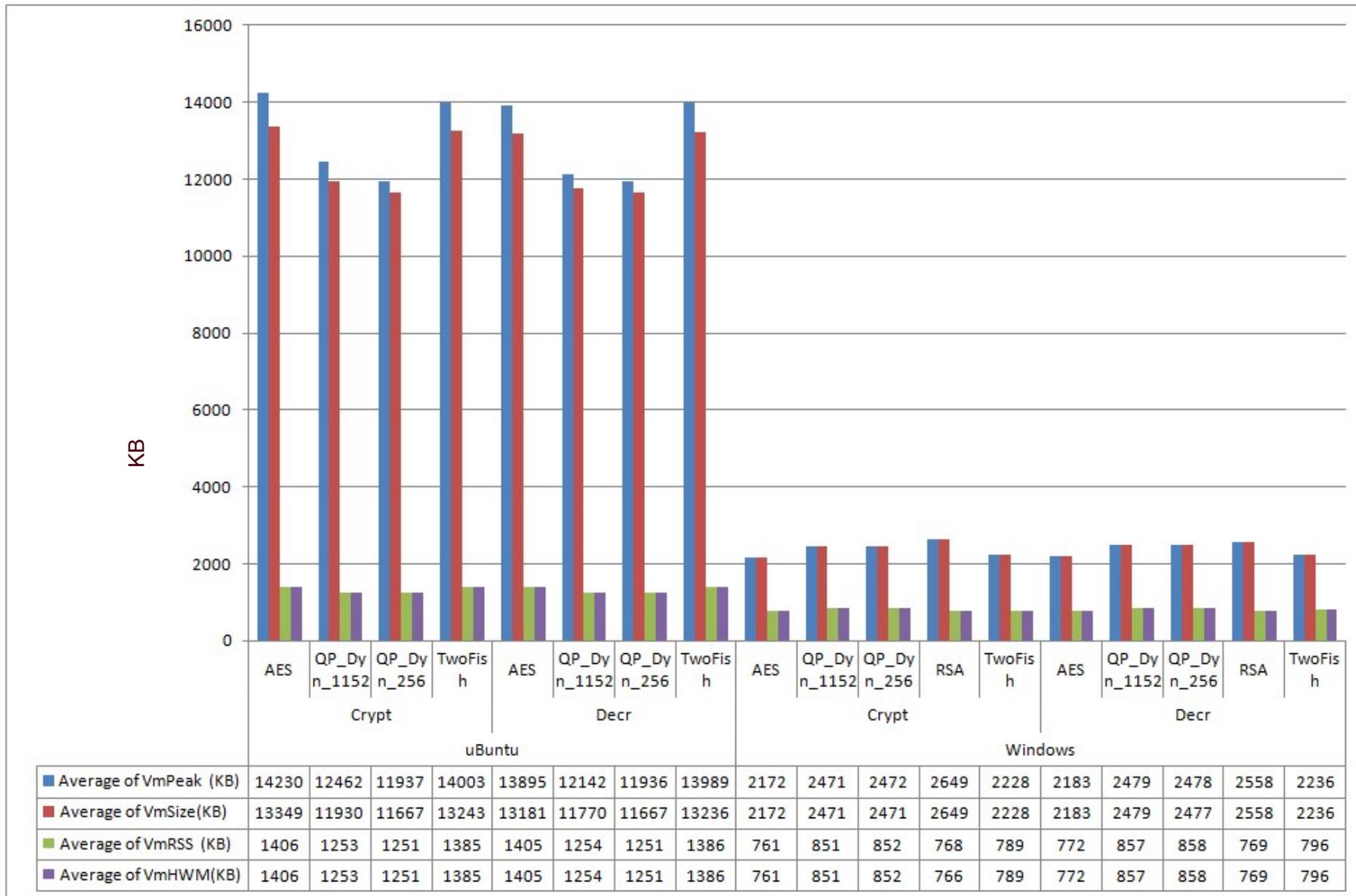


-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**



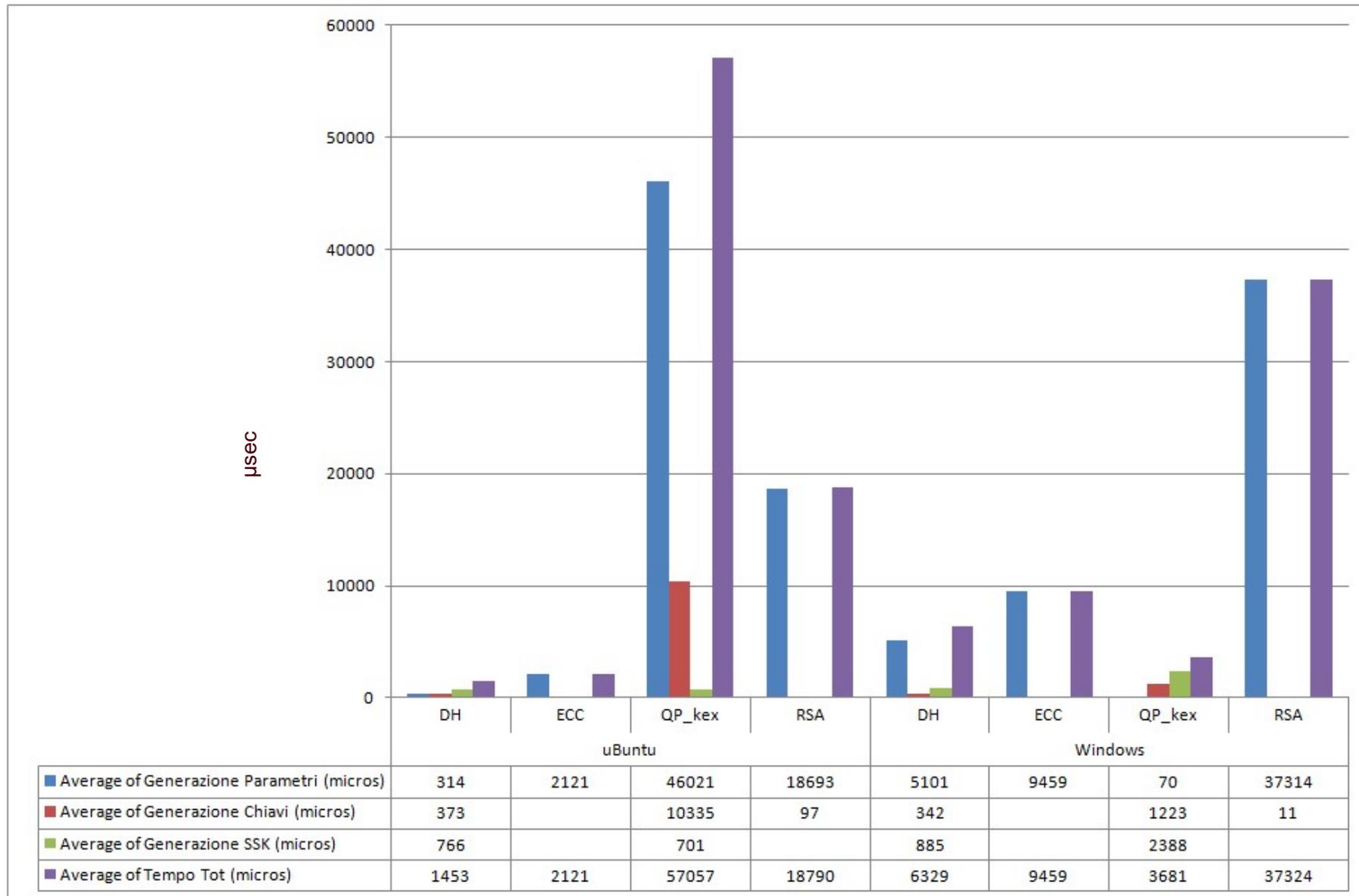
-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**

Test di Performance: Memoria

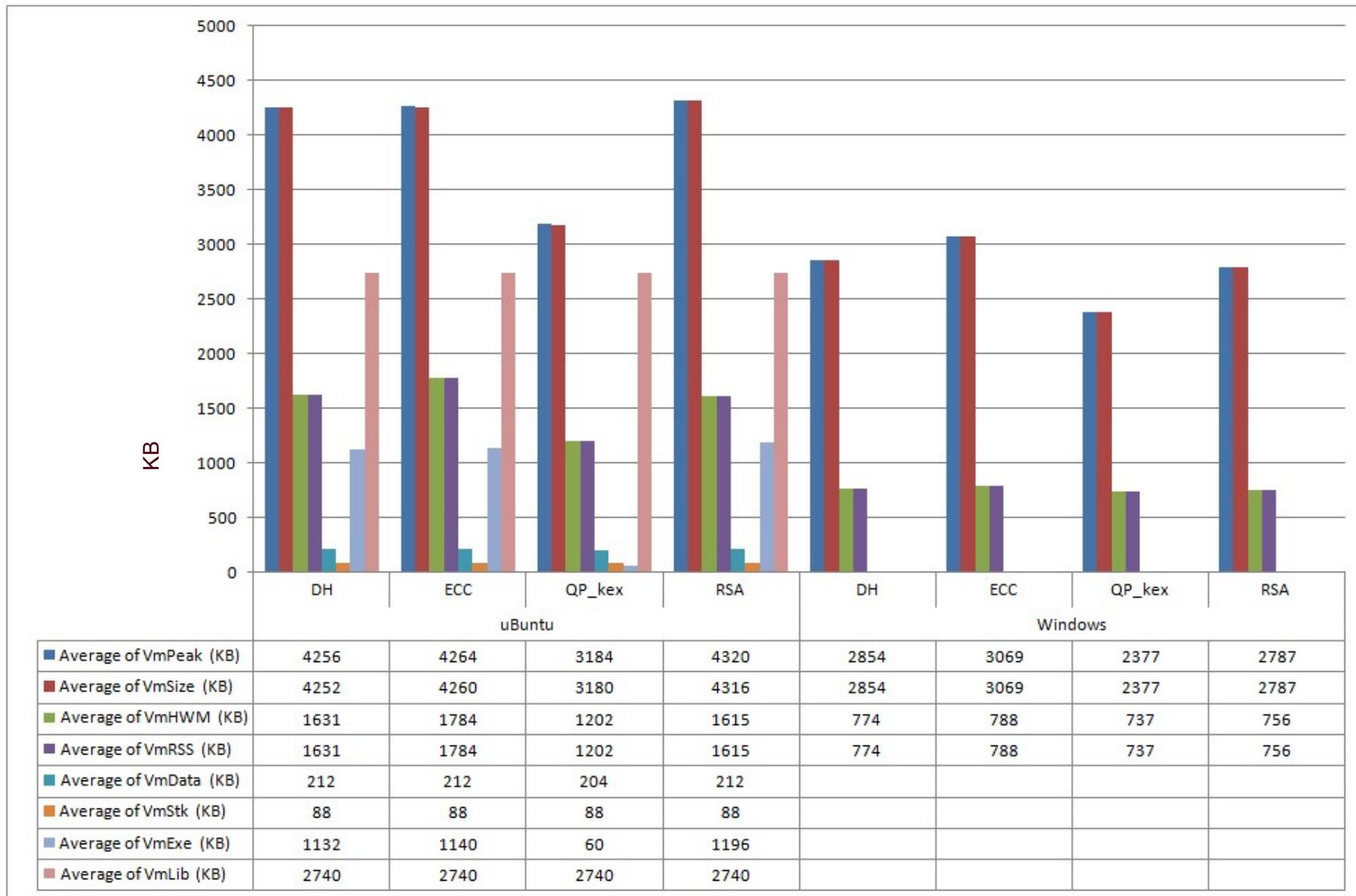


-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**

Test di Performance: Velocità

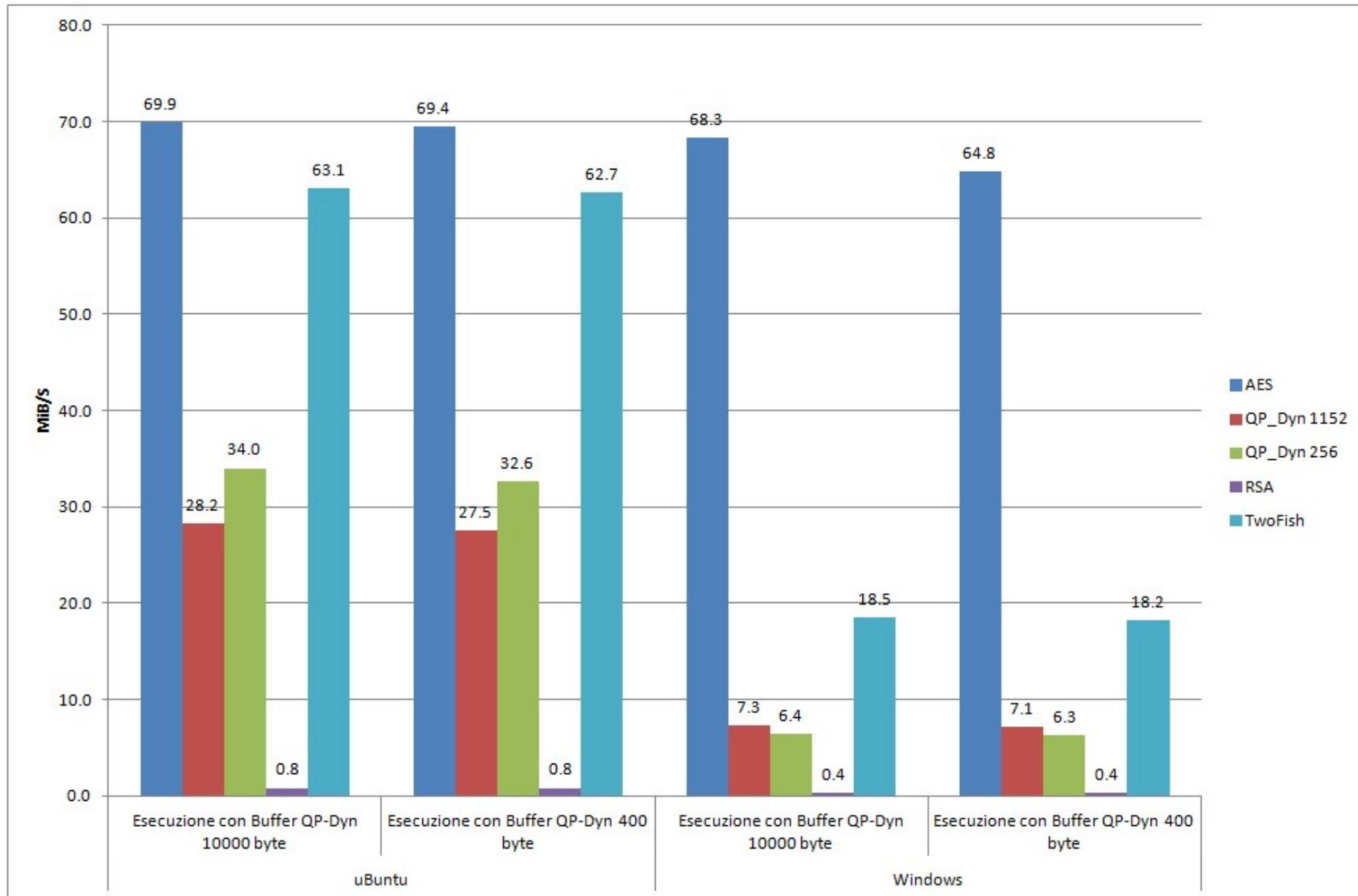


Test di Performance: Memoria



-
- **Test Environment**
 - **Test di performance: Velocità (QP-Dyn)**
 - **Test di performance: % CPU (QP-Dyn)**
 - **Test di performance: Velocità “Normalizzata” (QP-Dyn)**
 - **Punto di attenzione: 1° Esecuzione di AES**
 - **Test di performance: Ridondanza (QP-Dyn)**
 - **Test di performance: Memoria (QP-Dyn)**
 - **Test di performance (QP-Kex)**
 - **Approfondimento: Impatto del buffer size sulla velocità**

Approfondimento: Impatto del buffer size sulla velocità



Michele Pernice

email: m.pernice@reply.it

Desk: +39 0112912315

Mobile: +39 3357661822

Emanuel Cerro

email: e.cerro@reply.it

Desk: +39 0112912213