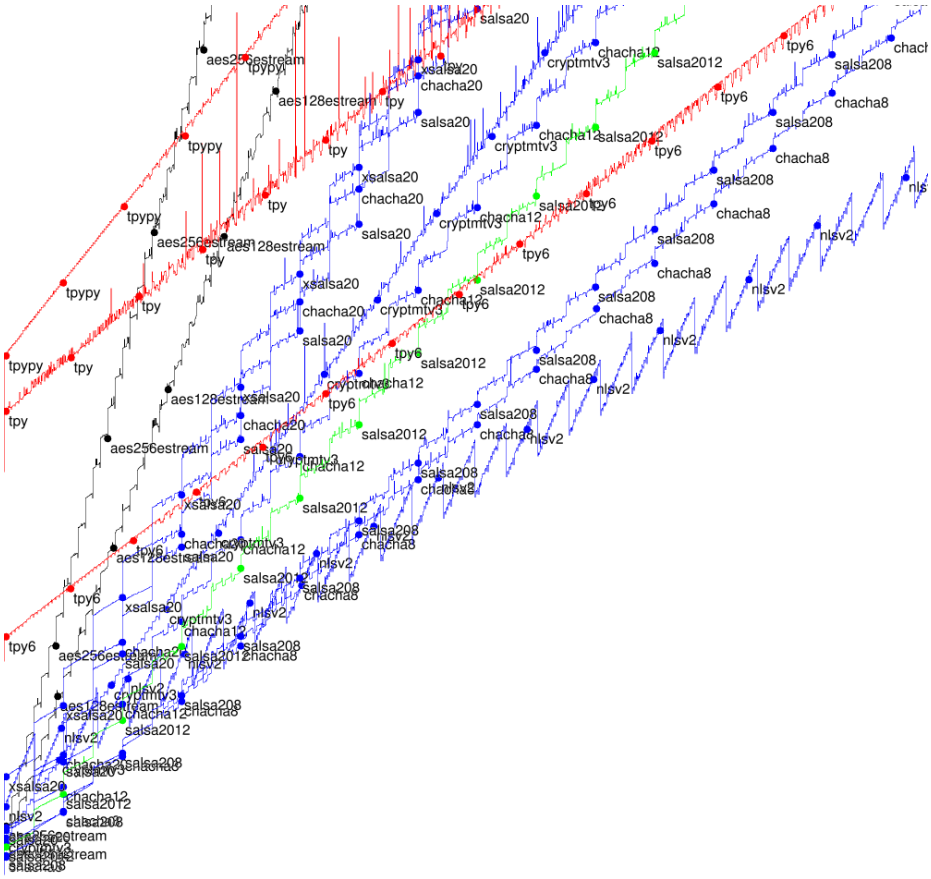
Software speed of stream ciphers

Daniel J. Bernstein[1] and Tanja Lange[2]

[1] Department of Computer Science
University of Illinois at Chicago, Chicago, IL 60607–7045, USA
djb@cr.yp.to
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
tanja@hyperelliptic.org

When eSTREAM came to an end in 2008, did stream-cipher benchmarking also come to an end? No! Here's a graph of stream-cipher performance on a computer named `h1mx515`, a freshly purchased pocket-size Sharp Netwalker:



This computer has a Freescale i.MX515 CPU released in 2009. The core of this CPU is an ARM Cortex A8, the same ARMv7-A core used in the Apple A4

(iPad, iPhone 4). The horizontal axis on the graph is message length, from 0 bytes to 2000 bytes; the vertical axis is time, from 0 cycles to 20000 cycles; the bottom-left-to-top-right diagonal is 10 cycles/byte.

This graph can be found on the web pages of the eBASC project run by ECRYPT's VAMPIRE lab, along with 131 graphs for other machines with a wide variety of CPUs. ABIs include amd64, armeabi, cellspu, ia64, mips32, mips64, mipso32, ppc32, ppc64, sparcv9, and x86; if a machine supports two ABIs then it is graphed separately for each ABI. Each graph is clickable for higher resolution, and is accompanied by several tables showing median cycle counts and quartile cycle counts for various message lengths. Implementors can click on machine names to see comparisons of the performance of different implementations of the same cipher (rather than just the best implementation, the one whose performance is graphed), and to see compiler errors and test errors for non-functional implementations.

For more information:

- `bench.cr.yp.to`: eBACS (ECRYPT Benchmarking of Cryptographic Systems), an umbrella project covering eBATS (public-key systems), eBASH (hash functions), and eBASC.
- `bench.cr.yp.to/ebasc.html`: eBASC (ECRYPT Benchmarking of Stream Ciphers), this project.
- `bench.cr.yp.to/primitives-stream.html`: List of stream ciphers measured, and list of implementations measured. At the moment there are 178 implementations of 28 stream ciphers in 16 families: AES, ChaCha, CryptMT v3, Dragon, HC-128/256, LEX v2, NLS v2, OCELOT, Panama, Rabbit, Salsa20, SNOW 2.0, Sosemanuk, TPy, Trivium, and XSalsa20.
- `bench.cr.yp.to/computers.html`: List of machines.
- `bench.cr.yp.to/results-stream.html`: Latest measurements, indexed by machine.
- `bench.cr.yp.to/supercop.html`: How to add your own machine.
- `bench.cr.yp.to/call-stream.html`: How to add your own stream-cipher software.