

SHA-3 Round-3 ASIC

X. Guo, M. Srivastav, S. Huang, D. Ganta, M. Henry, L. Nazhandali, P. Schaumont
ECE Department, Virginia Tech

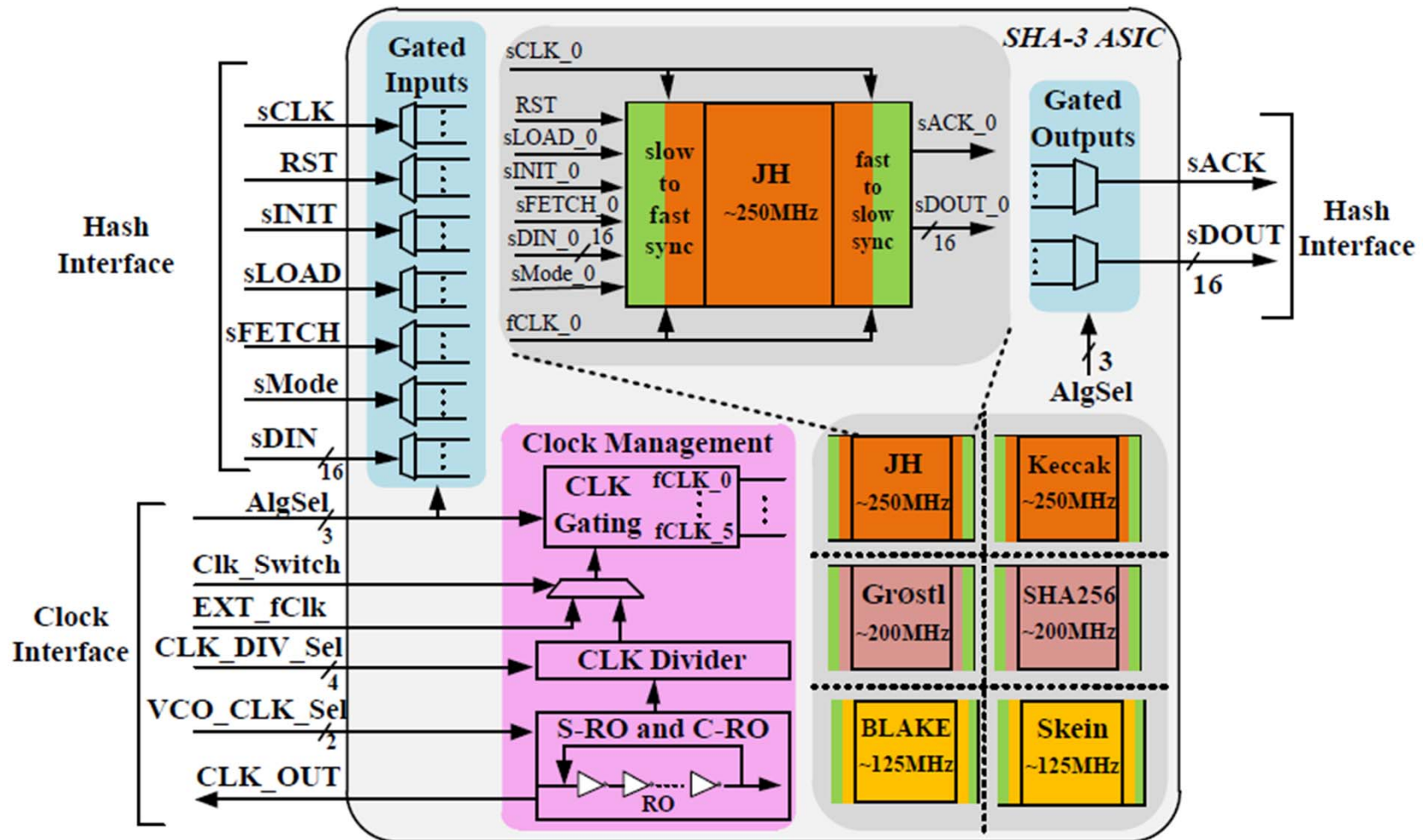


NIST

GMU, VT, UIC

Side-channel Attack
Standard Evaluation Board
SASEBO

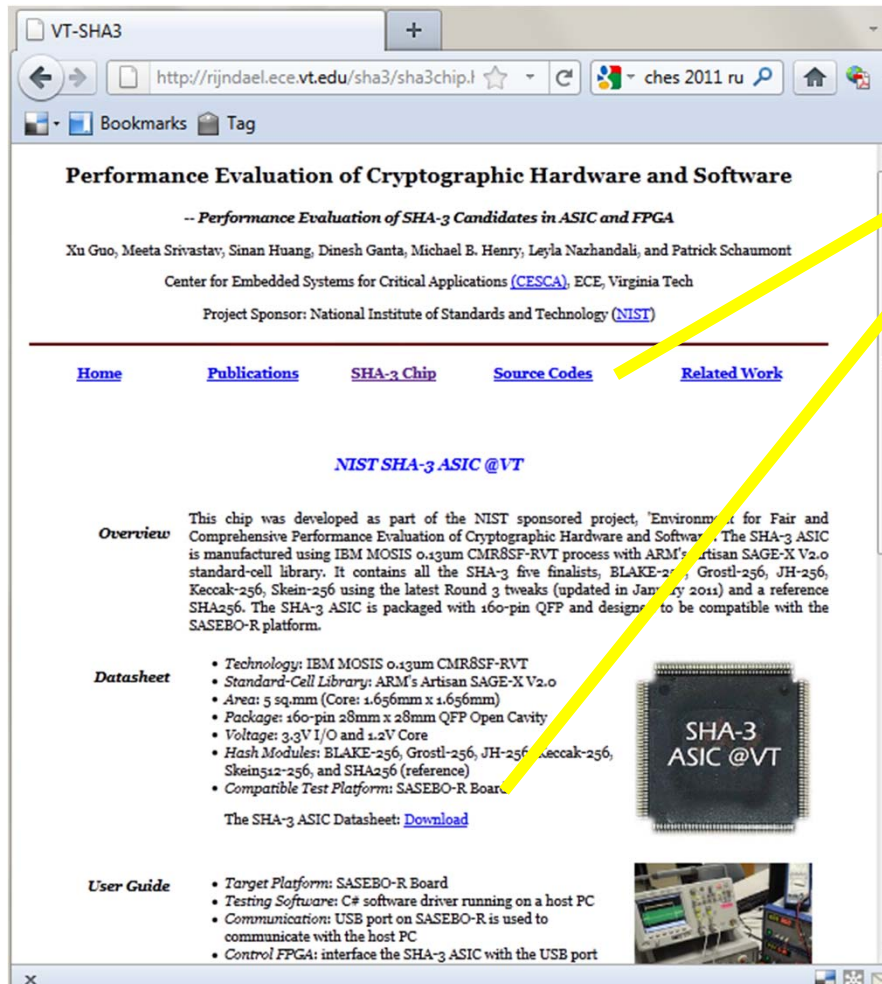
6 Good Neighbours



**130 nm CMOS stdcells (IBM CMR8SF-RVT)
with custom clock generator**

Chip is yours for free, if you ask!

Instructions at <http://rijndael.ece.vt.edu/sha3>
or send email to sha3vt@gmail.com



The screenshot shows a web browser window with the URL <http://rijndael.ece.vt.edu/sha3/sha3chip.html>. The page title is "Performance Evaluation of Cryptographic Hardware and Software". The authors listed are Xu Guo, Meeta Srivastav, Sinan Huang, Dinesh Ganta, Michael B. Henry, Leyla Nazhandali, and Patrick Schaumont. The project is sponsored by the National Institute of Standards and Technology (NIST). The page has a navigation menu with links for Home, Publications, SHA-3 Chip, Source Codes, and Related Work. The main content area is titled "NIST SHA-3 ASIC @VT" and includes an overview, a datasheet, and a user guide. The overview states that the chip was developed as part of the NIST sponsored project, "Environment for Fair and Comprehensive Performance Evaluation of Cryptographic Hardware and Software". The datasheet lists the technology as IBM MOSIS 0.13um CMR8SF-RVT, the standard-cell library as ARM's Artisan SAGE-X V2.0, the area as 5 sq.mm (Core: 1.656mm x 1.656mm), the package as 160-pin 28mm x 28mm QFP Open Cavity, the voltage as 3.3V I/O and 1.2V Core, the hash modules as BLAKE-256, Groestl-256, JH-256, Keccak-256, Skein512-256, and SHA256 (reference), and the compatible test platform as SASEBO-R Board. The user guide lists the target platform as SASEBO-R Board, the testing software as C# software driver running on a host PC, the communication as USB port on SASEBO-R is used to communicate with the host PC, and the control FPGA as interface the SHA-3 ASIC with the USB port. There are images of the SHA-3 ASIC chip and the SASEBO-R board.

- Datasheet
- User Guide (SASEBO-R)
- RTL Source (Round-2)

