SHA-3 Round-3 ASIC

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

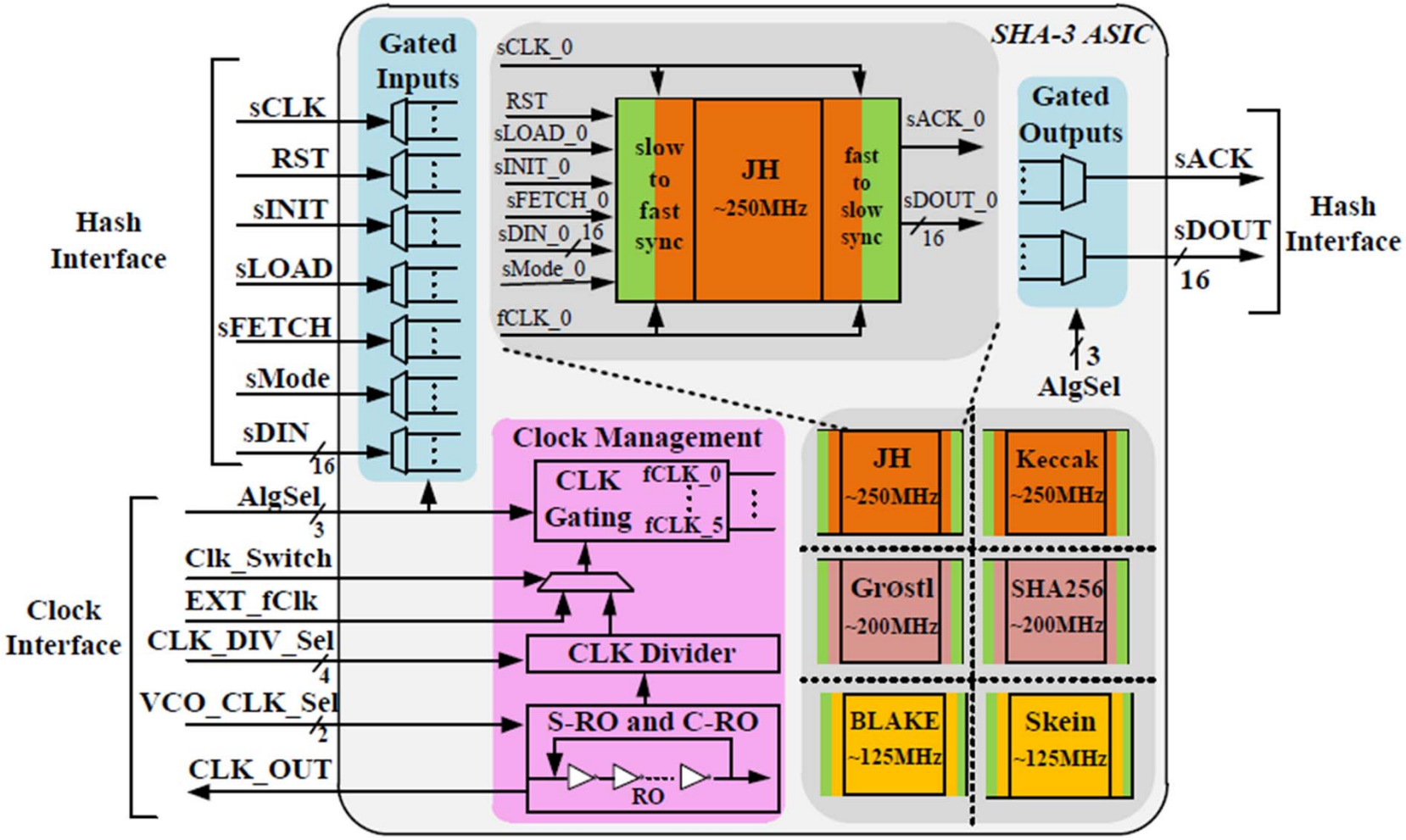
NIST

GMU, VT, UIC

Side-channel Attack Standard Evaluation BOard

SASEBO

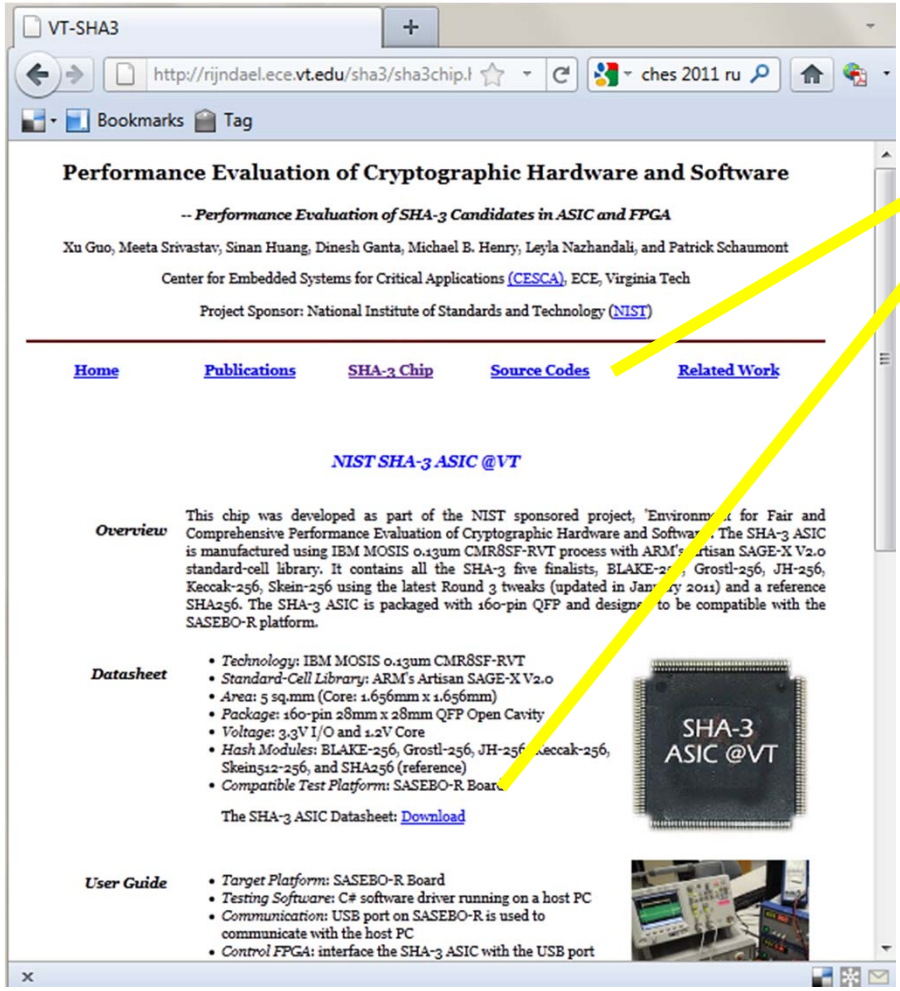
6 Good Neighbours



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



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