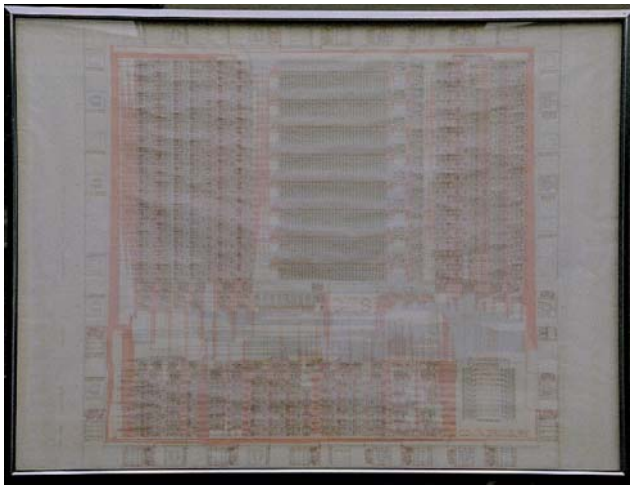
Blender

Colin Bradbury, MBA, Ph.D.

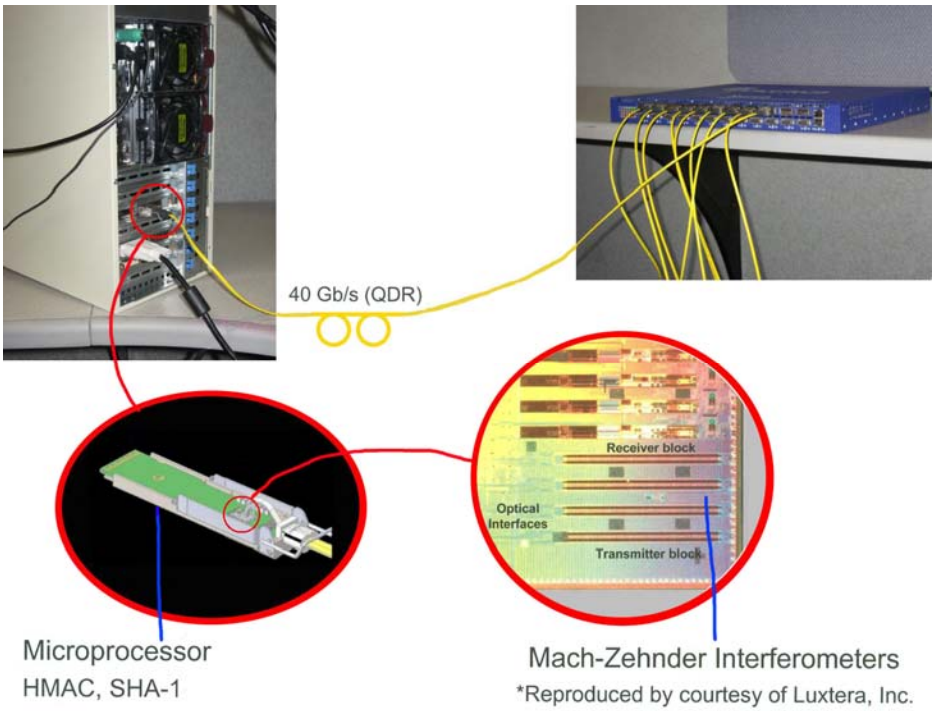
My Name In Silicon:

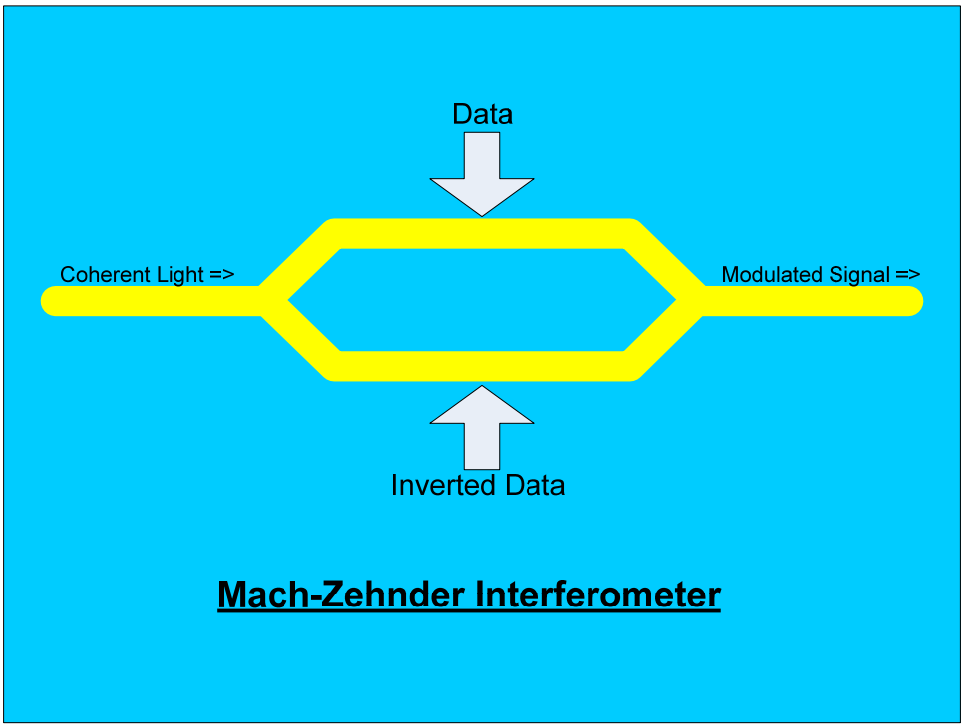


The first single-chip DES implementation, 1984

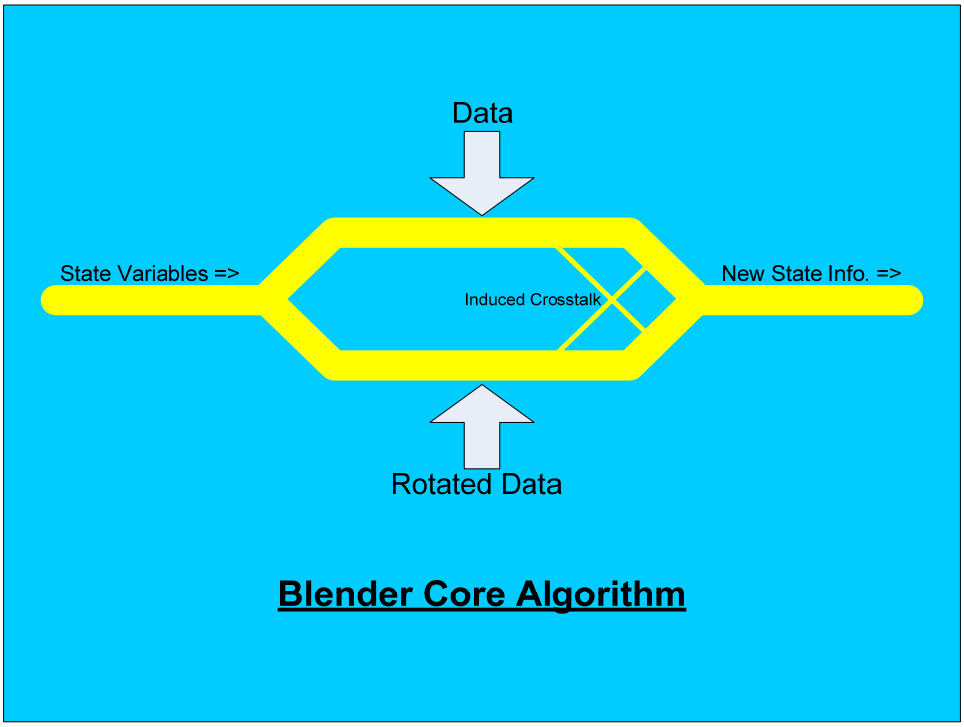
Hashing too slow?
Try our new Blender Accelerator:

- 10 Gigabits/second processing rate (PCIe x8)
- 8 Gigabits/second using PCI-X 133 (illustrated)
- Anything less is a price/performance tradeoff





Mach-Zehnder Interferometer



Blender Core Algorithm

Features:

- Core algorithm based on well-understood real-world physics
- Discrete Integral result
- Fast – just 5 gate-delays per round
- Designed explicitly for 8-bit processors
- Extendable to larger word sizes
- SHA-2 paternity

Benefits:

- Drop-in replacement for SHA-2 & SHA-1
- Portable to most micro-processors
- Extendable to arbitrary security levels
- Highly resistant to the extraction of secret keys from MAC systems
- Ideal for embedded systems