MisterTEA  

128-bit TEA Encryption Chip

Size of design: **496\mu m \times 498\mu m**

Transistor count: **13,098 transistors**

Transistor Density: **18.9 \mu m^2/\text{transistor}**

Clock Frequency: **83 MHz***

Data Rate: **100 Mbit/sec**

**Features:**

- 8-bit input/output ports
  - Reduce demand on I/O speed
  - Latch in directly to core registers
  - Eliminate need for input/output buffer

- 32-bit Carry Lookahead Adder (3.5ns)
  - Optimized critical path (18% perf. gain)
  - Fine-tuned custom gate design
  - Compact layout provides routability

- CPL logic for 3-Input XOR (0.3ns)
  - Very compact design
  - Offer both output and inverted output
  - Superb performance

- Delayed datapath clock signal
  - Make use the delay through clock buffer
  - Allow control path to run ahead
  - Hide control delays, improve performance

- Latches for Key and Delta
  - Compact size
  - Store 160 bits of data
  - Use 4.1% of chip area

**Description:**

The 128-bit TEA Encryption Chip is a high performance encryption chip that implements the Tiny Encryption Algorithm in hardware. It is designed using the HP.35um technology.

The chip takes a 128-bit key, goes through 32 fast iterations of a simple routine to scramble one 64-bit data-block at a time. It has a simple, yet flexible interface with support for easy integration on an asynchronous bus. Developed for securing multiple digital communication channels, it supports time-division multiple access architectures with zero task-switch overhead.

The 128-bit TEA Encryption Chip adds one more level of security to any digital communication channel completely transparent to the user.

* Due to computing resource limitations, only piecewise critical path and whole chip schematics are verified. All successful simulations confirmed the expected performance.
## Encryption Instruction

1) Assert RESET = 1 for at least 2ns
2) Set \{PROG, DinVALID\} = \{1,0\}
3) Wait for RDY4in be asserted
4) To program the key,  
   set \{PROG, KEYDELTA\} = \{0,1\}  
5) Send the low byte of key to dataIN  
6) De-assert PROG (PROG = 0)  
7) Send the rest of the key. (Big Endian order)  
8) Wait for RDY4in be asserted  
9) To program the delta,  
   set \{PROG, KEYDELTA\} = \{0,0\}  
10) Send the low byte of delta to dataIN  
11) De-assert PROG (PROG = 0)  
12) Send the rest of the delta  
13) Wait for RDY4in be asserted  
14) To encrypt, set \{PROG, KEYDELTA, PASS, ENCRY\} = \{1,0,0,1\}  
15) Send the high byte of data to dataIN  
16) Set DinVALID = 1  
17) Send the rest of the data (Little Endian)  
18) Wait for the DoutRDY assertion  
19) When DoutRDY is asserted, valid encrypted output will appear on dataOUT (Little Endian)

## Abstract

The Tiny Encryption Algorithm (TEA) is one of the fastest and most efficient cryptographic algorithms in existence. It encrypts 64 data bits at a time using a 128-bit key, and seems highly resistant to differential cryptanalysis.

Our chip employs the HP .35um technology and contains 13,098 transistors. The design incorporates static and complimentary pass-gate logic and implements components such as 32-bit logarithmic 2-bit carry look-ahead adder/subtractor, 128-bit latch array, and 64-bit registers with sub-nanosecond access time.

With a peak data rate reaching the order of 100Mbits/sec, this chip can be used to secure high-speed local area networks, such as 100-Mbit Ethernet. In addition, its compact size also enables it to be embedded into a wide range of wireless communication equipments.

Yue Chang  
Jike Chong  
Chirag Shah  
Chris verBurg