



## Company Press Release

### For More Information Contact:

Hemi Bhatnagar  
(480) 231 2074  
Tallika Corp.  
marketing@tallika.com

### ***Tallika announces immediate availability of High Speed Security Cores***

---

Mesa, AZ., July 21, 2005 – Tallika Corporation, an Intellectual Property and Design Services Company, today announced immediate availability of multi-gigabit security cores for Encryption and Hash engines. The Company also disclosed that its solutions have been proven on FPGA platforms and have been licensed to a large semiconductor vendor for integration into a high-end ASSP product for imminent tapeout in 0.13u technology.

“Tallika is committed to providing leading edge, complete IP solutions to enable its Customers to get to Market faster,” said Hemi Bhatnagar, President, CEO of Tallika Corporation. “This is our first set of products in the security space and today’s introduction enables us to leverage our core expertise in this space. Tallika’s founding team has had a long and very successful track record of pioneering work in providing cutting edge solutions for Information Security. With this product introduction, Tallika is well positioned for enabling its Customers to cost effectively integrate security functions into their products. Coupled with our design services and other high speed interface IP offerings, these products enable us to leverage our system level expertise in Security space and offer a compelling one stop security solution which can address the needs of a broad array of applications. We are pleased to work with our Customers towards such a rapid ramp to getting our product silicon proven. This is a vote of confidence from the industry in Tallika team’s expertise in the security space.”

### **Key Features:**

#### **TDES/DES:**

- Fully compliant with NIST FIPS PUB 46-3, CBC/ECB modes in NIST PUB 81
- 56-bit DES and 168-bit Triple-DES implementations

- Supports both encryption and decryption
- Provides ability to pre-load Initialization Vector (IV)
- Single channel provides 4 Gbps throughput for DES and 1.33 Gbps throughput for TDES in @250 MHz in 0.13u
- Suitable for insertion in pipelined designs
- Provides ability to pass cleartext and upto 16 bits of control information through the DES pipeline
- No dead cycles for key loading or mode switching
- Suitable for Electronic Codebook (ECB), Cipher Block Chaining (CBC), CFB and OFB implementations

### **AES:**

- Key Sizes supported are AES 128, AES 192, AES 256.
- CBC mode of operation.
- Supports XCBC Counter Mode
- 64-bit Input/Output data path
- Pipelined 64-bit output data path
- Supports loading and unloading data while data is being ciphered concurrently.
- Provides ability to pre-load Initialization Vector (IV)
- No dead cycles for key loading or mode switching
- Works at 250 MHz in 0.13u technology

### **Hashing Engine:**

- Supports both HMAC MD5 and SHA1 algorithms per RFC 2104.
- Provides 64-bit input datapath.
- Provides two 64-byte message buffers virtually eliminating the idle time for the core engine.
- SHA1 algorithm is implemented with datapath that works on two 32 bit data at a time thereby doubling the throughput.
- Supports 64-bit interface for register reads and writes. This interface is used to write idigest (HMAC computed over ipad) and odigest (HMAC computed over opad) data as well as to read the final message digest data.
- Has extra buffer so that next packet's idigest and odigest information can be loaded ahead before HMAC operation has finished on the current packet there by saving loading time and improving throughput.
- Works at 250 MHz in 0.13u technology

### **Deliverables:**

- Block level testbench which has been used to ensure compliance with NIST vector sets for the algorithms
- Available as fully functional and synthesizable Verilog soft-core
- User guide

---

## **About Tallika Corporation**

Tallika Corporation is a leading provider of Silicon Intellectual Property and Professional Services for consumer, networking, computing, and storage markets. Tallika's IP Portfolio includes PCI Express End-Point Controller and DDR I/II Controllers. Tallika's design services include turn-key Specification to GDSII – Specification, RTL, Verification, and RTL-to-GDSII – for digital and mixed-signal designs.

For more information on Tallika's Products and Services, please visit <http://www.tallika.com>