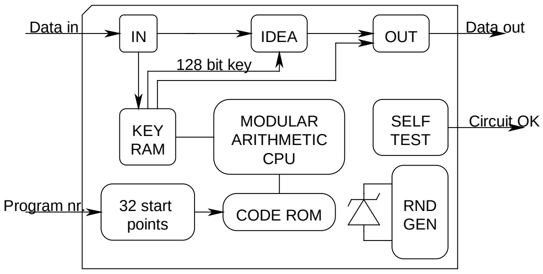
If you require



- FAST ENCRYPTION USING KNOWN ALGORITHM
- ADEQUATE KEY LENGTH
- KEY EXCHANGE IN THE SAME CIRCUIT
- SIMPLE EXTERNAL INTERFACE
- SELF TEST
- PROGRAMMABLE KEY EXCHANGE
- INTERNAL RANDOM NR. GENERATOR

Then we might have a product for you.

Introducing

IDEXP- IDEa and Discrete EXPonent processor

The circuit contains:

1) IDEA block transform with 128 bit key assuring that

- Your data is safe. The most popular algorithm - 3DES has effective keylength of 80 bits.

2) Programmable 96-bit modular arithmetics CPU giving the following benefits:

- The code rom is programmable and enables user to implement different key exchange algorithms. The CPU contains commands for modular multiply and exponent, so most of these algorithms can be implemented with just a few lines of code.
- Standard solutions are available, e.g. Diffie-Hellman and RSA. User can develop own code and test it in “test mode” of circuit.
- This CPU is also used for IDEA key inversion.
- The commands for bit field handling can be changed in microcode, what resides in the same code rom.

3) Shared ALU between CPU and IDEA transform

is achieved, because IDEA makes heavy use of modular calculations. Modular exponent on the other hand can be calculated with approximately 2*N modular multiplications.

Key exchange		IDEA transform
a^e mod N ≈ 2*dim(N) times: a*a mod N	↔	A*B mod F4

By sharing main ALU it is possible to save silicon area, what in return means shorter wires and higher yields or faster circuit and cheaper price.

4) Internal random number generator

based on the physical events ensures, that the generated keys are uniformly distributed and it is not possible to predict the key.

5) Self test

is used to determine the functionality of the circuit after turning the power on. Self-test uses state hashing of control structures and test program to check the circuit.

6) Simple external interface

The key exchange subroutines, however complicated are activated externally by entering the subprogram number. This number is translated into start address using table in beginning of code ROM.

SUPPORTING TOOLS

To aid in development of products based on the circuit the following tools are offered:

1) Circuit emulator/code debugger

The code debugger enables user to develop new code for key exchange algorithms. Debugger has the standard options of inserting breakpoints and inspecting/evaluating data registers. The debugger has built-in compiler. Using the compiler the user can write out the code in binary format and run it on the IDEXP circuit.
It is possible to add new commands to processor for bit-field handling used in key-exchange algorithms to generate/verify check fields. It is done by adding microcode. The debugger has the possibility to emulate the circuit's microcode.

2) Add-on card for testing the code on the real circuit.

If faster debugger response times are needed, then it is possible to link real device into debugger using PC card. The card contains code rom and programmable clock generator. When using circuit in test mode it is possible to execute commands from external ROM. This rom is kept up to date transparently by debugger, so all that user sees is faster debugger run time.

Prototyping results

The first version of circuit was prototyped using 1.0 µm CMOS 2 METAL layers technology. This circuit area is 104 mm^2. In this stage we used CLCC64 package, with 53 pins dedicated to IO signals. The circuit IO width is selectable from 16/8/1 bit. To achieve demanded IDEA encryption speed the IDEA IO is running in parallel with block cipher.
We received the circuits from prototyping at the beginning of summer 1997 and have since then ran several tests and improved debugger software. The circuit complied with the expectations. Here are the main parameters:

Supply voltage:	5.0	V
Clock speed:	25	MHz
Max moduli length	760	bits
a^x mod N time	0.1	sec
IDEA transform speed	20	Mbit/sec
Power Consumption	500	mW

We are now preparing for phase two, what includes redesign of datapath and switch to faster technology. We plan to use 2 ALUs in parallel and by that speed up modular calculations and IDEA transform. Destination is:

Supply voltage	3.0	V
Clock speed	66	MHz
Max moduli length	1520	bits
a^x mod N time	0.01	sec
IDEA transform speed	150	Mbit/sec

Estimated power consumption will be larger, but is too early at this stage to predict. We will include internal programmable clock multiplier, so users can run the circuit at slower speeds and conserve power.