Embedded Microprocessor Family KROLIK, version KMX

Architecture update of embedded microprocessor family KROLIK is represented by new cores KMX32 and KMX8 (32 and 8 bit cores respectively), based on KM211 proprietary RISC architecture and intended for use in low-power, low gate-count, secure and highly stable applications in low performance class of processors. Improved architecture with additional instructions and new GCC compiler version produce 20-25% better performance and energy efficiency, with a minimal increase in gatecount and even lower power consumption per megahertz.

Application Domains

- General Purpose microcontrollers.
- Embedded Control.
- Smart-cards.
- Bank Cards.
- SIM Cards.
- E-passport or other ID.
- Contactless tags.
- Embedded Security modules.
- Access Control, Transportation.
- Automotive.
- Real-time signal control (freeRTOS, etc…).
- Portable Devices.
- Ultra-Low Power applications.

Embedded microprocessor family KROLIK is specifically designed for efficiency of C-code, providing a secure and yet a cost-effective solution. Microprocessors are developed with requirements of operating in unstable voltage supply and clock signal, other sources of instability. Architecture and instruction set are well optimized for C-language, resulting in outstanding code density with minimal core size and power consumption.

Client-friendly

- Flexible ISA, expandable by client request.
- Highly Configurable RTL.
- SDK Eclipse 3.7 (Indigo) and GCC 4.7.2 (available at www.km211.com/en/downloads)
- Ported OS: freeRTOS and other

Flexible proprietary instruction set and in-house tools and RTL give KM211 the ability to make fast and easy estimations of architecture changes to meet client needs. Processor configurability helps achieve best area/power results and avoid redundant functionality. A single page configuration file needs to be edited to create a new core version. Due to a specific Verilog-RTL description style no re-synthesis errors are generated with any target library, either FPGA or ASIC.

Architecture

- RISC, Harvard.
- 3-stage pipeline.
- No jump prediction faults.
- Most instructions execute in 1 clock period.
- Data and instructions memory up to 4GB.
- C-optimized architecture.

KROLIK architecture achieves outstanding results in compiled code density and performance, due to overhead-free mix of 16/32 bit instructions (90% of instructions are 16 bit).

Cost Sensitive Approach

- Small core size.
- High Code Density.
- Flexible licensing.
- Implementations:
  - ASIC,
  - FPGA.

KROLIK cores are supplied as Verilog RTL or hard IP. The clearly commented code and highly configurable RTL enable engineers to customize the processor to achieve specific application goals.

Implementation examples

Below table presents synthesis results for maximal address space core configuration with register file.

		KMX8	KMX32	Units
General characteristics	Performance efficiency, Dhrystone		2.1	DMIPS/MHz
	Performance efficiency, Coremark		2.1	Coremark/MHz
	Operands size	8	32	bits
	Code size (generated from C sources as a percentage of ARM Thumb-2)		97	%
90 nm, area optimized	Area (utilization 70%)	0.026	0.09	mm^2
	Gatecount	10	33	K gates
	Dynamic consumption	12	28	uW/MHz
	Static leakage	1.25	2.8	uA
90 nm, performance optimized	Work frequency, not less than	100	100	MHz
	Area (utilization 70%)	0.035	0.12	mm^2
	Gatecount	13	36	K gates
	Dynamic consumption		40	uW/MHz
	Static leakage		5	uA
180 nm, area optimized	Area (utilization 70%)	0.178	0.53	mm^2
	Dynamic consumption		192	uW/MHz
	Static leakage		15	uA
180 nm, performance optimized	Work frequency, not less than	50	50	MHz
	Area (utilization 70%)	0.266	0.94	mm^2
	Dynamic consumption		296	uW/MHz
	Static leakage		33	uA
Altera Cyclone EP4CE115	Gatecount of FPGA Altera Logic Elements	3000	3500	LE

Note. TSMC 90 nm LP, JSC MIKRON 180 nm CMOSF8 (for KMX8) and JSC MIKRON HCMOS8D (for KMX32) processes were used

Fast and Responsive

- Over 100MHz @90nm.
- Fast Context Switching.
- Small Interrupt Latency of 1-3 Clocks.
- Single cycle multiply 8x8/16x16/optional 32x32.
- Extensible with Co-processors:
  - Multiply/Accumulate (MAC),
  - Crypto,
  - Video,
  - Other.

Stable

- Operational in:
  - wide temperature range,
  - wide supply voltages range,
  - in a noisy conditions.
- Correctly defends from hacking attempts.
- Stable results at RTL synthesis in different libraries.

The cores are efficiently fast, in terms of power vs. performance trade-off. Cores enable real time applications by means of fast context-switching through virtual register file approach in operands-addressing, fast interrupt reaction; arithmetic instructions can access entire memory without need of load/store instructions. Optional acceleration blocks to meet client needs are available. A number of peripheral blocks available: Timers, PWM, CRC, FLASH Memory Controllers, LCD, GPIO and other.

The core was specifically designed to be stable, not only it is designed to avoid error of re-synthesis and busses instability, from fault or untrusted execution. Sophisticated clock tree keeps the core functionality in conditions of clock instability.

Protected

- Two execution modes with different resources access rights (KMX32 only).
- Restricted memory access and firmware protection.
- Per-client Instruction Set Remap.
- IC protection for bank and ID cards.

The core was specifically designed to protect its internal data, code and hardware structures. Core security rights features are the major differentiation from competitor MCU's. System (kernel) and user modes of execution with different resources access rights and memory protection ensure the confidentiality of code and data, which gives additional protection against hacking. Lock bits protect system and user memory area from dump through a debugger interface. Per-client instruction set remapping is an additional protection of executable code.

Data encryption options

- EC-DSA (160-2048).
- RSA (512-4096).
- AES (128/256).
- DES/3DES.
- GOST 28147-89.
- GOST 34.10.
- GOST 34.11.

Data encoding hardware IP from KM211 portfolio enables any security features. It supports both international and local standards and dramatically increases system performance by solving similar problems.

Suites Smart Cards Requirements

- ISO14443A contactless interface.
- ISO7816 contact smartcard interface.
- Power scheme optimized for RF-powered IC's.

Additional features for RF-field powered smart cards development are present. IC based on this MCU core can achieve very good results in power consumption and security characteristics. Power dissipation issues are proven to fulfil the requirements of RF-powered designs.

Tools Support and Debugging

- Windows-Linux Eclipse 3.7 (Indigo) based SDK:
  - C compiler GNU GCC 4.7.2;
  - Debugger GDB,
    - tracer,
    - profiler;
  - Instruction Set Simulator (ISS);
  - Cycle Accurate Simulator (CAS);
  - External models with LUA;
  - JTAG;
  - FPGA prototyping board;
  - Verilog Testbench for verification and new projects.

The SDK is based on Eclipse environment and always improving GCC compiler. Reconfiguration of SDK for new memory sizes and peripheral blocks is supported, peripheral block connection is done through LUA scripts. The debug interface features are optional and do not go against chip protection issues and have a number of configuration bits to block debug access.

Contacts

Headquarters and R&D

Design Center KM211, Ltd.

Zelenograd, proezd 4806, dom 5, stroenie 23
Moscow, 124498, Russia

email: info@km211.com

tel: +7(499) 940 0356

fax: +7(499) 940 0357

web site: www.km211.com

US Representative

email: alexey.makhalov@km211.ru

tel: +1 425 9987756

KM211 is a member of Special Economic Zone "Zelenograd" (www.oez-zel.com**)**