Introducing the PIC24F “GB2” MCU Family: eXtreme Low Power with Hardware Crypto Engine

Alexis Alcott, Product Marketing Manager, MCU16 Division
June 24, 2014
Announcing at Sensors Expo

- **PIC24F “GB2” MCUs for Protecting Data in Embedded Applications**
  - Hardware crypto engine (Industry-standard AES, DES, 3DES)
  - Random Number Generator (RNG)
  - One-Time-Programmable (OTP) Key Storage

- **eXtreme Low Power Extends Battery Life**
  - 18 nA Sleep, 180 µA/MHz Run
  - Enabling Integrity of Data without Sacrificing Power Consumption

- **Connection to USB or Wireless Protocols**
  - Integrated USB 2.0 Device, Host, OTG
  - Easy Connection to Certified Modules for Wi-Fi®, ZigBee®, Sub-GHz, Bluetooth® LE

- **Ideal for IoT Sensor Nodes, Access Control Systems, Door Locks**
Example Applications

- **Industrial**
  - Security door locks
  - Access control systems
  - Security cameras
  - POS terminals
  - Smartcard readers
  - Heat/Gas meters
  - IoT sensor nodes

- **Computer**
  - PC peripherals
  - Printers
  - Portable accessories

- **Medical/Fitness**
  - Pedometers
  - Wearable fitness
  - Handheld devices
Integrated Crypto Engine

- **Hardware Crypto Engine**
  - Industry Standards for AES, DES, 3DES
  - Encryption, Decryption & Authentication
  - Secure Data Transfer & Storage

- **Random Number Generator**
  - Supporting True-Random and Pseudo-Random Numbers
  - Reach a Higher Level of Data Security
  - Reduces Possibility of Hacking

- **Secure Key Storage for Additional Protection**
  - 512 bits OTP Key Storage
  - Once Written, Keys cannot be Read or Overwritten by Software
  - Stores up to 4 AES Keys or 8 DES Keys

- **Advantages of Hardware Crypto over Software Implementation**
  - Less Software Overhead Frees Up CPU Bandwidth & Memory
  - Operate at a Lower CPU Frequency to Save Power
  - Another Example of Microchip’s Core Independent Peripherals
PIC24 “GB2” Block Diagram

**PIC24F 16 MIPS**
- 16-bit ALU
- 16x16 Register
- 17x17 MPY
- JTAG & EMU
- Barrel Shifter
- Address Generation

**MEMORY BUS**
- 64-128 KB Flash
- 8 KB RAM
- 6 Channel DMA

**PERIPHERAL BUS**
- 28-pin: SSOP, SOIC, SPDIP, QFN
- 44-pin: TQFP, QFN

**PERIPHERAL BUS (PPS)**
- Hardware Crypto Engine - AES, DES, 3DES
- 512 bits OTP Key Storage
- Random Number Generator
- USB 2.0
- I²C™ - 2
- SPI w/DMA / I²S - 3
- UART - ISO 7816 Compatible w/LIN - 4
- Input Compare - 6
- Output Compare - 6
- 16-bit Timers - 5
- Charge Time Meas. Unit (CTMU)
- 10/12-bit ADC, 12 Channels
- Comparators - 3
- Deep Sleep Interrupt
- Deep Sleep WDT & BOR
- VBAT, RTCC
- Deep Sleep XLP
Application Example: Electronic Door Lock

- **Encryption for Security**
  - Uses Crypto, RNG & Key Storage
  - User data is encrypted
  - Secure key storage

- **eXtreme Low Power**
  - Low power extends battery life
  - Vbat with RTCC for battery backup

- **Access Options**
  - Enter code manually via keypad
  - Magnetic keycard
  - Wirelessly via Smartphone
## Flexible Development Tools

<table>
<thead>
<tr>
<th>Main Development Board</th>
<th>Explorer 16 Board</th>
<th>DM240002</th>
<th>$129.99</th>
</tr>
</thead>
</table>

### Processor Plug-In Modules

<table>
<thead>
<tr>
<th>Module Type</th>
<th>Model</th>
<th>Part Number</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC24FJ128GB204 Plug-In Module (USB)</td>
<td></td>
<td>MA240036</td>
<td>$25.00</td>
</tr>
<tr>
<td>PIC24FJ128GA204 Plug-In Module (Non-USB)</td>
<td></td>
<td>MA240037</td>
<td>$25.00</td>
</tr>
</tbody>
</table>

### PICtail™ Plus Daughter Cards

<table>
<thead>
<tr>
<th>Card Type</th>
<th>Model</th>
<th>Part Number</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB PICtail Plus Daughter Board</td>
<td></td>
<td>AC164131</td>
<td>$60.00</td>
</tr>
<tr>
<td>Smart Card/SIM Card PICtail Daughter Board</td>
<td></td>
<td>AC164141</td>
<td>$29.99</td>
</tr>
</tbody>
</table>

### Wireless Daughter Cards

<table>
<thead>
<tr>
<th>Card Type</th>
<th>Model</th>
<th>Part Number</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>RN4020 Bluetooth® LE PICtail/PICtail Plus</td>
<td></td>
<td>RN-4020-PICtail</td>
<td>$49.00</td>
</tr>
<tr>
<td>Wi-Fi® PICtail</td>
<td></td>
<td>RN-171-PICtail</td>
<td>$39.95</td>
</tr>
<tr>
<td>802.15.4/ZigBee® MRF24J40MA PICtail Plus</td>
<td></td>
<td>AC164134-1</td>
<td>$24.99</td>
</tr>
<tr>
<td>Sub-GHz MRF89XAM8A PICtail Plus</td>
<td></td>
<td>AC164138-1</td>
<td>$39.99</td>
</tr>
</tbody>
</table>
PIC24F “GB2” MCU Family: Low Power with Crypto Engine

- Embedded Applications in the Internet-Connected World
  Demand Secure Data & Long Battery Life

- PIC24F “GB2” for Secure Data Transfer & Storage
  - Hardware Crypto Engine
  - Random Number Generator & Secure Key Storage

- PIC24F “GB2” for eXtreme Low Power
  - Longer battery life for portable applications

- PIC24F “GB2” for Easy Connections
  - Integrated USB
  - Easy interface to certified Wi-Fi® or Bluetooth® LE modules

www.microchip.com/PIC24FJ128GB204
Additional Materials

Note: The Microchip name and logo, and PIC are registered trademarks of Microchip Technology Inc. in the U.S.A., and other countries. PICtail is a trademark of Microchip Technology Inc. in the U.S.A., and other countries. All other trademarks mentioned herein are property of their respective companies.
## Availability & Pricing

<table>
<thead>
<tr>
<th>Part #</th>
<th>USB</th>
<th>Flash</th>
<th>Pins</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC24FJ128GB204</td>
<td>Yes</td>
<td>128 KB</td>
<td>44</td>
<td>TQFP, QFN</td>
</tr>
<tr>
<td>PIC24FJ128GB202</td>
<td>Yes</td>
<td>128 KB</td>
<td>28</td>
<td>SOIC, SSOP, QFN, SPDIP</td>
</tr>
<tr>
<td>PIC24FJ64GB204</td>
<td>Yes</td>
<td>64 KB</td>
<td>44</td>
<td>TQFP, QFN</td>
</tr>
<tr>
<td>PIC24FJ64GB202</td>
<td>Yes</td>
<td>64 KB</td>
<td>28</td>
<td>SOIC, SSOP, QFN, SPDIP</td>
</tr>
<tr>
<td>PIC24FJ128GA204</td>
<td>No</td>
<td>128 KB</td>
<td>44</td>
<td>TQFP, QFN</td>
</tr>
<tr>
<td>PIC24FJ128GA202</td>
<td>No</td>
<td>128 KB</td>
<td>28</td>
<td>SOIC, SSOP, QFN, SPDIP</td>
</tr>
<tr>
<td>PIC24FJ64GA204</td>
<td>No</td>
<td>64 KB</td>
<td>44</td>
<td>TQFP, QFN</td>
</tr>
<tr>
<td>PIC24FJ64GA202</td>
<td>No</td>
<td>64 KB</td>
<td>28</td>
<td>SOIC, SSOP, QFN, SPDIP</td>
</tr>
</tbody>
</table>

**Prices start at $1.30 in volume.**

**All products available now for sampling & volume.**

**Tape & Reel options available.**
Support for All AES/DES Modes

- We support all of the modes within AES, DES, 3DES

**DES Encryption/Decryption**
- Half-duplex operation
- Selectable between DES or Triple DES (3DES)
- 56-bit Key with support for 2-key or 3-key E-D-E/D-E-D Triple DES
- 64-bit Block Size
- ECB, CBC, CFB, OFB and CTR modes

**AES Encryption/Decryption**
- Half-duplex operation
- 128-bit, 192-bit or 256-bit Key
- 128-bit Block Size
- ECB, CBC, CFB, OFB and CTR modes
Crypto Modes

- **ECB – Electronic codebook**
  - The simplest of the encryption modes is the electronic codebook (ECB) mode. The message is divided into blocks, and each block is encrypted separately.

- **CBC – Cipher-block chaining**
  - IBM invented the cipher-block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

- **CFB – Cipher feedback**
  - The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher. Operation is very similar; in particular, CFB decryption is almost identical to CBC encryption performed in reverse.

- **OFB – Output feedback**
  - The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.

- **CTR – Counter**
  - Like OFB, counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular. CTR mode has similar characteristics to OFB, but also allows a random access property during decryption. CTR mode (CM) is also known as integer counter mode (ICM) and segmented integer counter (SIC) mode.

- **Modes of operation** are nowadays defined by a number of national and internationally recognized standards bodies. Notable standards organizations include NIST, ISO (with ISO/IEC 10116), the IEC, the IEEE, the national ANSI, and the IETF.

Key Storage/Management

- **Software Keys**
  - Keys stored in Flash or SRAM
  - Keys are accessible by software

- **Keys with 512-bit OTP Storage**
  - Keys are never exposed to software
  - No key erase or modification
  - Software only indicates which OTP key should be used

- **Encrypted Software Keys**
  - Encrypted keys are stored in the Flash or SRAM
  - OTP Key is dedicated as Key Encryption Key (KEK)
  - Software is never exposed to unencrypted keys (programmatically secure)

- **Randomly Generated Keys**
  - Keys are generated randomly by the hardware
  - Software is never exposed to keys (programmatically secure)
  - Can direct hardware to encrypt keys for transmission
Key Storage - OTP

- Stores up to 512 bits OTP
  - 4 keys for AES (128 bit key)
  - 2 keys for AES (256 bit key)
  - 8 keys for DES (64 bit key)
- OTP – One Time Programmable
  - Fuse based
  - Cannot be read or overwritten after locked