

# **CRYPTO**MEMORY™

## **Marketing Presentation**

**Jean Pierre Benhammou**

**[jbenhammou@cs0.atmel.com](mailto:jbenhammou@cs0.atmel.com)**

# CryptoMemory™ Goal

➤ **Fill the void between:**

Plain serial EEPROM memory

- No security
- Low price

And Microprocessor

- High security
- Expensive

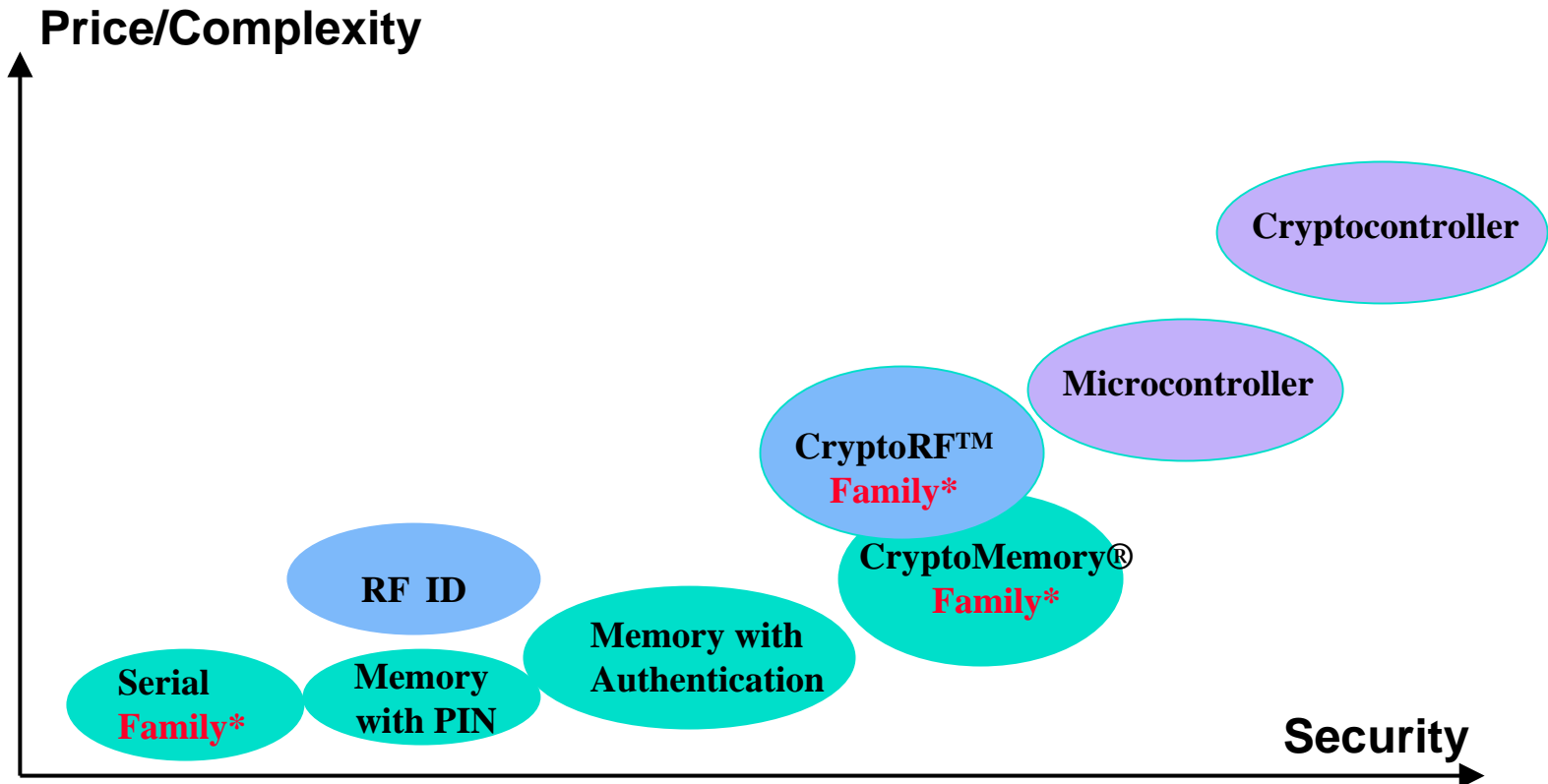
➤ **CryptoMemory is a Family of circuits**

**Four new devices 32K to 256Kbits**

Full family from 1K to 256Kbits available now

All devices in the family share the same secure algorithm and features

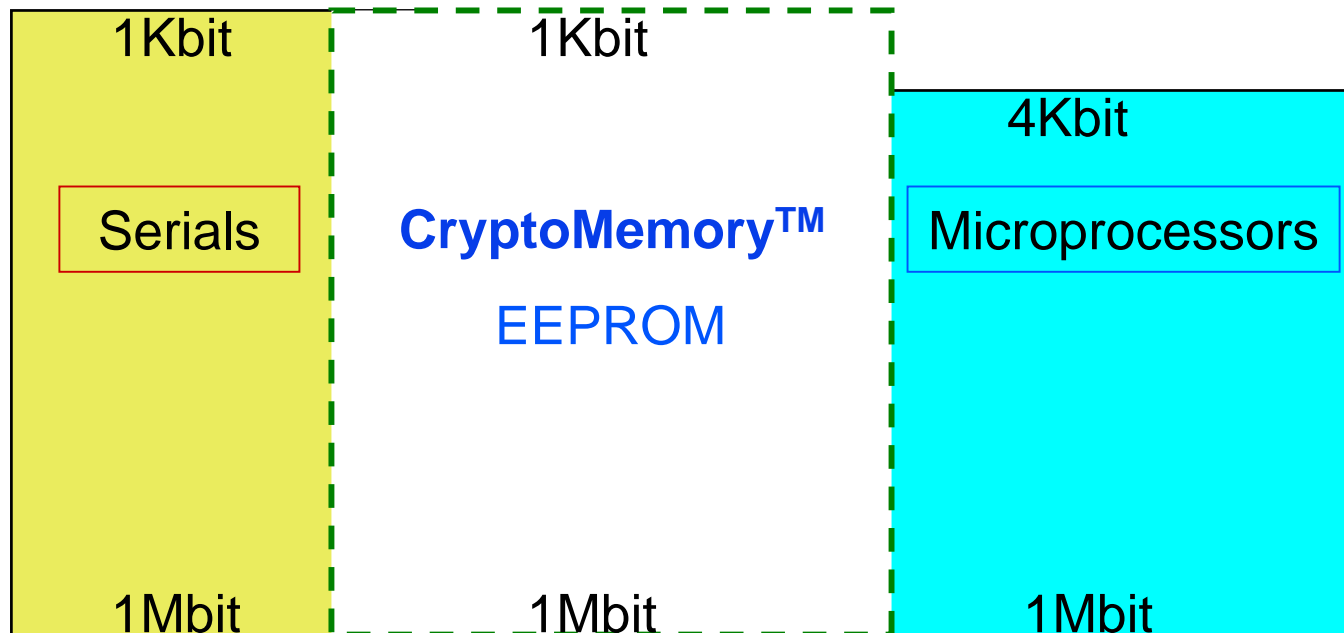
# Components for Security



- \*A family is defined as a group of products with the following in common:
1. Products have different user memory densities and
  2. The end user does not need to modify the application software when needing additional user memory.

# CryptoMemory™ Business

## Filling the Gap Between Serials and Microprocessors



# CryptoMemory™

## Family Portrait

Device Type	Memory Density	Number of Zones
AT88SC0104C	1Kbit (1/8Kbyte)	4
AT88SC0204C	2Kbit (1/4Kbyte)	4
AT88SC0404C	4Kbit (1/2Kbyte)	4
AT88SC0808C	8Kbit (1Kbyte)	8
AT88SC1616C	16Kbit (2Kbytes)	16
AT88SC3216C	32Kbit (4Kbytes)	16
AT88SC6416C	64Kbit (8Kbytes)	16
AT88SC12816C	128Kbit (16Kbytes)	16
AT88SC25616C	256Kbit (32Kbytes)	16

**Density is Customer “Usable” Memory**

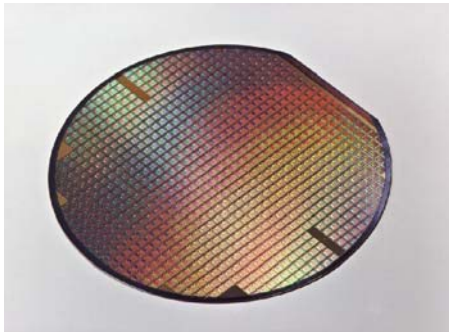
# **CryptoMemory™**

## **Wafer and Module Main Features**

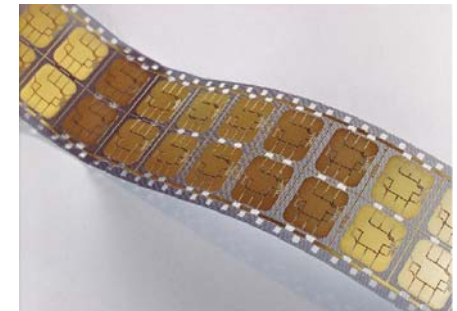
- **Symmetric Dynamic Mutual Authentication: 64 bit keys**
- **R & W Passwords with attempts counters**
- **Encrypted Passwords**
- **R & W Encrypted Checksum**
- **Stream Encryption**
- **Write Lock Mode**
- **Anti Tearing**
- **Dual protocol: T=0, 2-wire (1.5MHz clock rate)**
- **Device/Host speed rate negotiation (32 to 256Kbit devices)**
- **ATR: ISO 7816-3, EMV and PC/SC Compatible**
- **No operating system required on chip**
- **Operating Voltage: 2.7 to 5.5 Volts**

# CryptoMemory™

## Smart Card Applications



- ID Card
- Driving License
- Health Care Card
- Insurance Card
- Campus/College
- Access control
- Energy Meters
- Transaction records
- Multi-Applications



# CryptoMemory™

## Family Effect on an Application

### Example: Driving License

A country (USA, China, India...) with many states and different requirements: Cards from different states can be read by any reader from any state. Basic data will be at the same location. Security features/Algorithms are the same for all memory densities. The last two bytes of the ATR give the memory density to the application.

Application Features	Kbit	Device
Basic ID Card	2K	AT88SC0204C
ID Card + Finger Print	4K	AT88SC0404C
ID Card + Finger Print + Picture	8K	AT88SC0808C
ID Card + Finger Print + Picture + Driving Violations	16K	AT88SC1616C
ID Card + Finger Print + Picture + Driving Violations + Health Data	64K	AT88SC6416C

# CryptoMemory™

## Answer To Reset

- 64 bit ATR including historical bytes or memory density bytes (T1, T2)
- ATR is generated in **asynchronous mode only**
- Asynchronous ISO 7816-3, EMV and PC/SC compliant

TS	T0	TA(1)	TB(1)	TD(1)	TD(2)	T1	T2
\$3B	\$B2	\$11	\$00	\$10	\$80	\$01	\$28

- The last 2 bytes indicate a 128Kbit device

# CryptoMemory™

## Competition Analysis: CryptoMemory™ vs. Microprocessors

User  
Memory  
Density

Microprocessors  
(Competition)

CryptoMemory™

Microprocessors  
(Atmel)

		Atmel 256 Kbit AT88SC25616C	Atmel 32 Kbit (32KB Flash) AT90SC3232
	ST 128 Kbit (16KB ROM) ST16SF4F	Atmel 128 Kbit AT88SC12816C	Atmel 128 Kbit (48KB ROM) AT05SC4816R
	ST 64 Kbit (16KB ROM) ST16SF48	Atmel 64 Kbit AT88SC6416C	Atmel 64 Kbit (24KB ROM) AT05SC2408R
	ST 32 Kbit (16KB ROM) ST16SF44	Atmel 32 Kbit AT88SC3216C	Atmel 32 Kbit (16KB ROM) AT05SC1604R

**Need a Microprocessor with a minimum of 16KBytes of ROM to emulate CryptoMemory™**

# CryptoMemory™

## Application Cycle Time & Cost

- How long from concept to market production?

Design cycle time using a ROM Microprocessor (with ROM redesign)

**32 to 52 Weeks**

Design cycle time using a CryptoMemory™ (no firmware development)

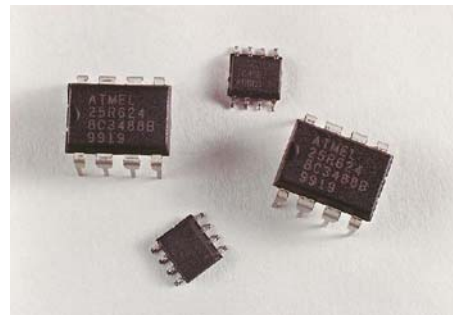
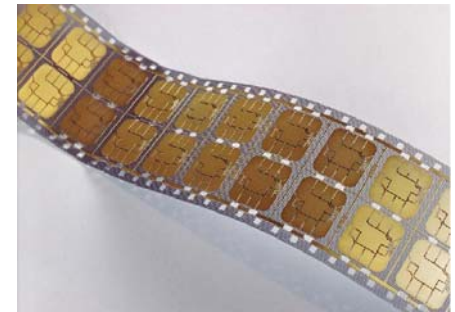
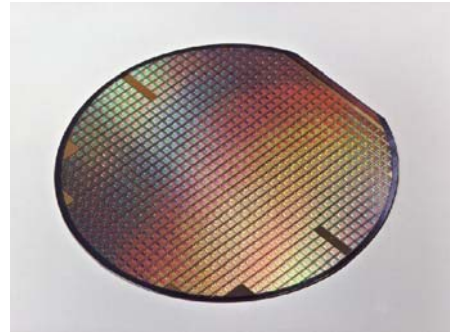
**6 to 8 Weeks**

- An application using CryptoMemory™ is 30% to 50% cheaper than using a ROM Microprocessor

# CryptoMemory™ Packaging

**CryptoMemory™ circuits can be delivered in:**

- **Wafer form, thinned to 180 microns**
- **Smart card module form**
- **Plastic package for PC board assembly: SOIC, PDIP, LAP**



# CryptoMemory™ Demo Kits

- **Device Demo Kit: Hands on the device**

**AT88SC25616C-EK**

- **Device Development Kit: How to write an application, includes crypto function F2**

**AT88SC25616C-DK**

