



Sidense Corp.

The Future of Memory IP... NOW!

Embedded Non-Volatile Memories in Security Applications

CMOS Emerging Technologies, Banff, July 06

Xerxes Wania

www.sidense.com

NOTE: The information contained in these slides is confidential and proprietary to Sidense Corp. (the Company). These slides have been prepared solely for the information of selected individuals and is provided upon the understanding that any person accepting them will not, without the prior written permission of the Company, utilize the information contained in these Slides for any purpose other than gaining a further understanding of the Company's operations. No portion of these slides may be reproduced or distributed. Acceptance of these slides by an individual shall constitute an agreement not to use the information contained in these slides for any purpose other than evaluating the Company's business, not to make the information contained available to any other person.

Agenda

- What does Sidense do?
- Traditional Embedded Non-Volatile Memories
- Sidense's Antifuse
- How secure is Sidense's Antifuse
- Features
- Types of Security applications
- Conclusion

What does Sidense do?

- We design **Non-Volatile Memories (NVM)** as an **alternative to** embedded and discrete **FLASH, EEPROM, PROM and ROM**
- Our products are **targeted to the** fast growing, **consumer electronic (CE)** market
- Our patent pending **technology is the smallest, fastest, and one of the most secure NVM solutions on the market**
- Our business model is to **sell Intellectual Property (IP) licenses** to companies developing **System-on-chips (SoCs)**

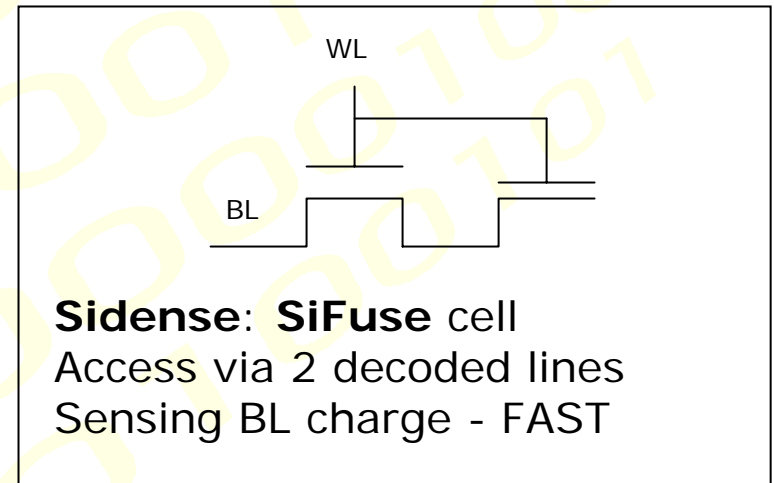
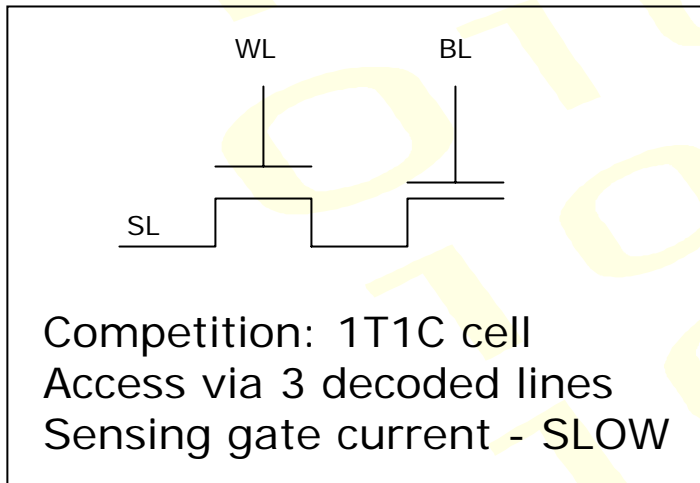
Traditional Embedded Non-Volatile Memories

- **Poly and metal Fuses**
 - Programmed mostly at wafer level, not in field
 - Very large programming currents
 - Limited memory size < 1-2k bits
 - Large area, no routing over the fuses
 - Easy to reverse engineer, recognizable 0's and 1's, no security
 - Poor reliability – potential fuse re-grow problems
- **Embedded EEPROM/EPROM/Flash**
 - Older process nodes, large geometries, high programming voltages
 - Additional mask and process steps – expensive \$\$
 - Specialized process, poor second sourcing
 - Roadmaps limited to 0.18/0.13 geometries
- **Floating gate NVM in CMOS Logic**
 - Large bit size – low bit count
 - Restricted to geometries 0.13um larger, require >70A gate oxide
 - Low retention at high temperature, gate leakage issues
 - Limited operating temperature range, reliability issues
- **MASK ROM**
 - Inflexible programming – long turn around time
 - Initially low cost but mask changes very expensive \$\$

Need NVM solutions in 90nm, 65nm, 45nm Process Nodes

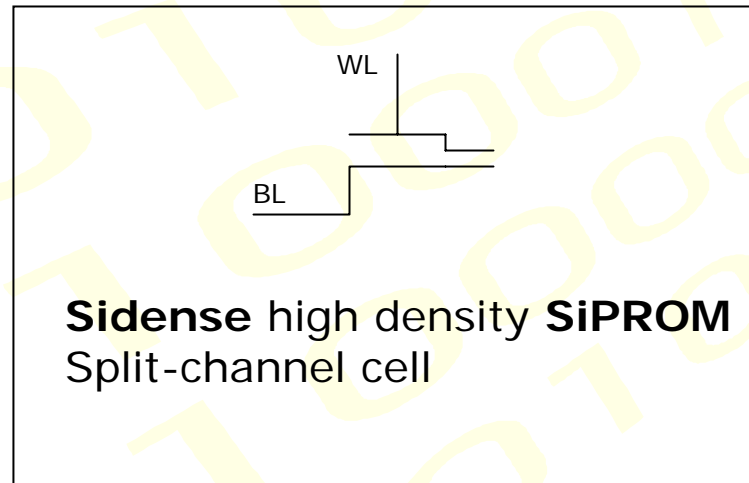
Sidense Antifuse Memory

Sidense's SiFUSE is based on classical gate oxide antifuse principle



Sidense High Density Cell

Sidense SiPROM arrays are based on high density Split-Channel cell



Features - Sidense Antifuse

- **Field Programmable**
 - *On wafer, in package or in field via JTAG, I2C or other interfaces*
- **High density**
 - *Approximately 1Mbit/mm² density using 1T cell/bit*
- **Very Fast**
 - *Read Speeds of < 10ns*
- **Flexible in large volume production**
 - *Mask ROM option through a single mask change*
 - *Any partition of PROM can be replaced by Mask ROM*
- **Scalable technology**
 - *0.18um, 0.13um, 90nm, 65nm...*
- **Portable across different Foundries**
 - *Standard Logic CMOS process, no additional masks or process steps*
- **Multiple Time Programming**
 - *emulated MTP (eMTP)*
- **Wide I/O bus**
 - *8bits to 512bits per macro*

How secure is Sidense's Antifuse?

- No known procedures to reverse engineer the state of the Sidense antifuse
 - Looks similar in programmed and un-programmed state under an optical or electron microscope
 - Voltage contrast method un-usable as multiple cells share common gate polysilicon
- Once programmed, the bits cannot be erased or altered (OTP)
- Sidense engaged with leading technology and reverse engineering experts to confirm security of our antifuse technology

Sidense OTP – Security Features

- Built-in comparator allows to verify 128 or 256-bit code in a single clock cycle without data being ever transferred outside the macro
- Programming operation can be locked at the memory macro level, cannot be unlocked through microsurgery
- Differential sensing assures no noise signature during read operation
- Attempt to change or temper with the NVM would get detected using proprietary sensing techniques
- Long data word, special circuitry and layout techniques prevent any electrical or mechanical attack

Low Density Applications

- Small memory sizes: 128bits to 64Kbits
 - Chip/secure/RF ID
 - Unique identification in every chip
 - Can be used as multi-time programmable cell as well
 - Memory repair
 - Replace laser or electrical fuses to repair memory
 - Option select
 - I/O and option selection replaces mask programming
 - Analog trimming and adjustments
 - Adjust and trim capacitors, resistors and voltage references
 - Encryption Key Storage
 - HDCP, DRM, etc.
 - Most secure

Unique Identification – FLASH/ASICs

OTP Fraud Protection Register - 256bits

128-bits ASIC Programmed	128-bits OEM Programmed
-------------------------------------	------------------------------------

128 bits – ASIC manufacturer

- Unique ID – OTP so write once only
- Programmed after packaging

128 bits – OEM Customer

- Tracking and fraud protection
- Match the memory, CPU, or ASIC component with other system components preventing device substitution
- Programmed after system is built

OTP Fraud Protection Register/Password – eMTP for consumer

128-bits ASIC Programmed	128-bits X20 User Programmed
-------------------------------------	---

High Density Applications

- Large memory sizes, 64 Kbits to Mega Bytes:
 - Boot and processor code storage
 - Secure boot
 - DSP and controller code storage
 - Embedded programmable logic
 - Embedded PLD type applications
 - Configurable Logic
 - Structured ASICs
 - Field programmability added to Mask programmable logic
 - Embedded OTP data storage
 - Games
 - Consumer Electronic products
 - PLDs and FPGAs
 - OTP type PLDs
 - Security features in FPGAs

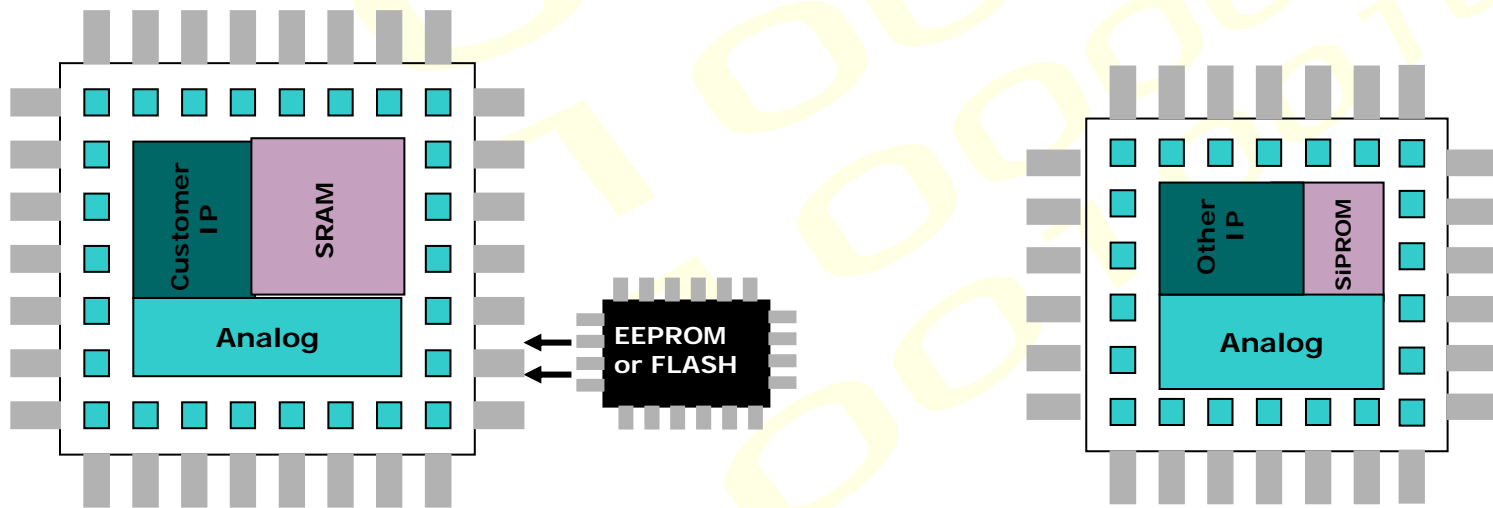
Secure Boot - External Flash/EEPROM replacement

○ Current Solution

- Typical 2 chip solution
- External EEPROM or FLASH + Large SRAM
- Load firmware from EEPROM/FLASH to internal SRAM

○ Sidense Solution

- One chip solution with Embedded SiPROM
- **Save \$** in testing, package and die size
- Low pin count
- **Lower power**
- **Secure**
- No boot-up time - Instant on



Overview

- Limited number of NVM solutions on the market for the advanced process technology nodes
- Antifuse OTP gains acceptance as the best NVM solution for security applications
- Sidense offers the highest density and the most secure OTP and MTP solutions for encryption applications
- Sidense is working with Elliptic Semiconductor, and Certicom on security applications