'Security Refresh': Protecting Phase-Change Memory

A hardware mechanism to avoid information leak and protect memory against malicious wear-out

Inventors at Georgia Tech have developed a hardware mechanism called “Security Refresh” which protects memory against malicious attacks by constantly migrating the physical location of data inside the PCM. Using a logical function for address translation, the mechanism shuffles physical memory locations inside the memory chip. This effectively extends the lifetime of the memory chip by evenly wearing out memory blocks across the entire memory space. Additionally, the technology protects against malicious attacks by obscuring the actual data location.

Summary Bullets

- **Longer memory lifespan —** Lifetime is extended by creating even wear-out
- **Versatile —** Not limited to PCM, can be applied to any future memory technology that suffers from limited write endurance
- **Secure —** Protects against attacks by masking actual data location

Solution Advantages

- **Longer memory lifespan —** Lifetime is extended by creating even wear-out
- **Versatile —** Not limited to PCM, can be applied to any future memory technology that suffers from limited write endurance
- **Secure —** Protects against attacks by masking actual data location

Potential Commercial Applications

- Memory chips

Background and More Information

Given the short lifespan and scaling issue in flash memories and dynamic random access memories (DRAM), alternative memory technologies are desired to continue to expanding processing and memory capabilities. Phase-change memories (PCMs) have shown the most promise, however PCM faces serious challenges of reliability and usability. A PCM device can be rendered useless in a matter of minutes because it has a faster

access speed than flash memory and a shorter endurance than DRAM.

Inventors

- Hsien-Hsin Lee
  Associate Professor — Georgia Tech School of Electrical and Computer Engineering
- Dong Woo
  Graduate Student — Georgia Tech School of Electrical and Computer Engineering
- Nak Seong
  Graduate Student — Georgia Tech School of Electrical and Computer Engineering

IP Status

: US8806171B2

Publications

, -

Images

Visit the Technology here:
'Security Refresh': Protecting Phase-Change Memory