MN63Y2008介绍

Double Dragon

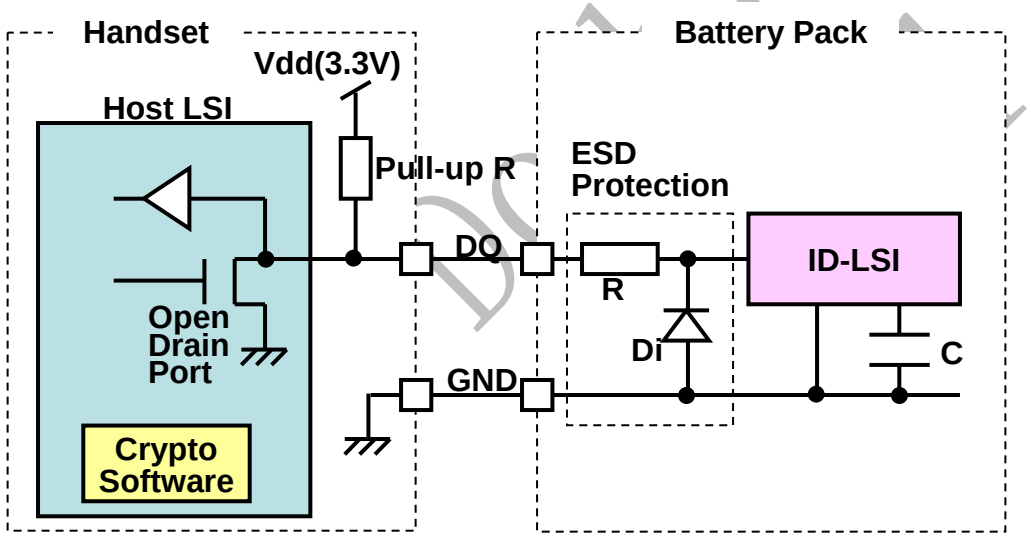
- 使用NTRU 公钥算法进行授权管理
- 非易失性铁电存储器
- WLCSP 晶片级封装
- 单线通信接口(界面)，无需单独供电
- 算法具有良好的保密性，在HOST端不需要保存和IC中相同的私钥。
- 算法具有强度高、速度快的特点。

ID-LSI MN63Y2008 with Public Key Crypto

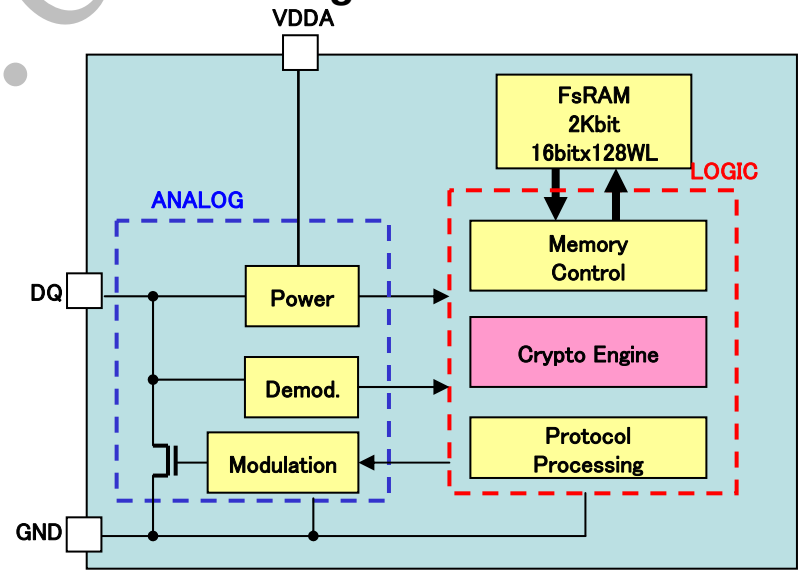
◆ Enhanced Security Level using Public Key Cryptography Authentication

- **Provide Safety and Reassurance with:**
  - ➢Authentication Using Public (Asymmetric) Key Cryptography of NTRU
  - ➢Tamper Resistance Non-Volatile FeRAM
- **Contribute for Small Set with:**
  - ➢Small Package: WLCSP (1.14x1.26mm)
  - ➢Single Wire I/F
  - ➢Minimal number of external components（only one C/R/Di）
- **2K bits FeRAM with lock data function:**
  - ➢System Area: 1424bits
  - ➢General Purpose Area: 624bits

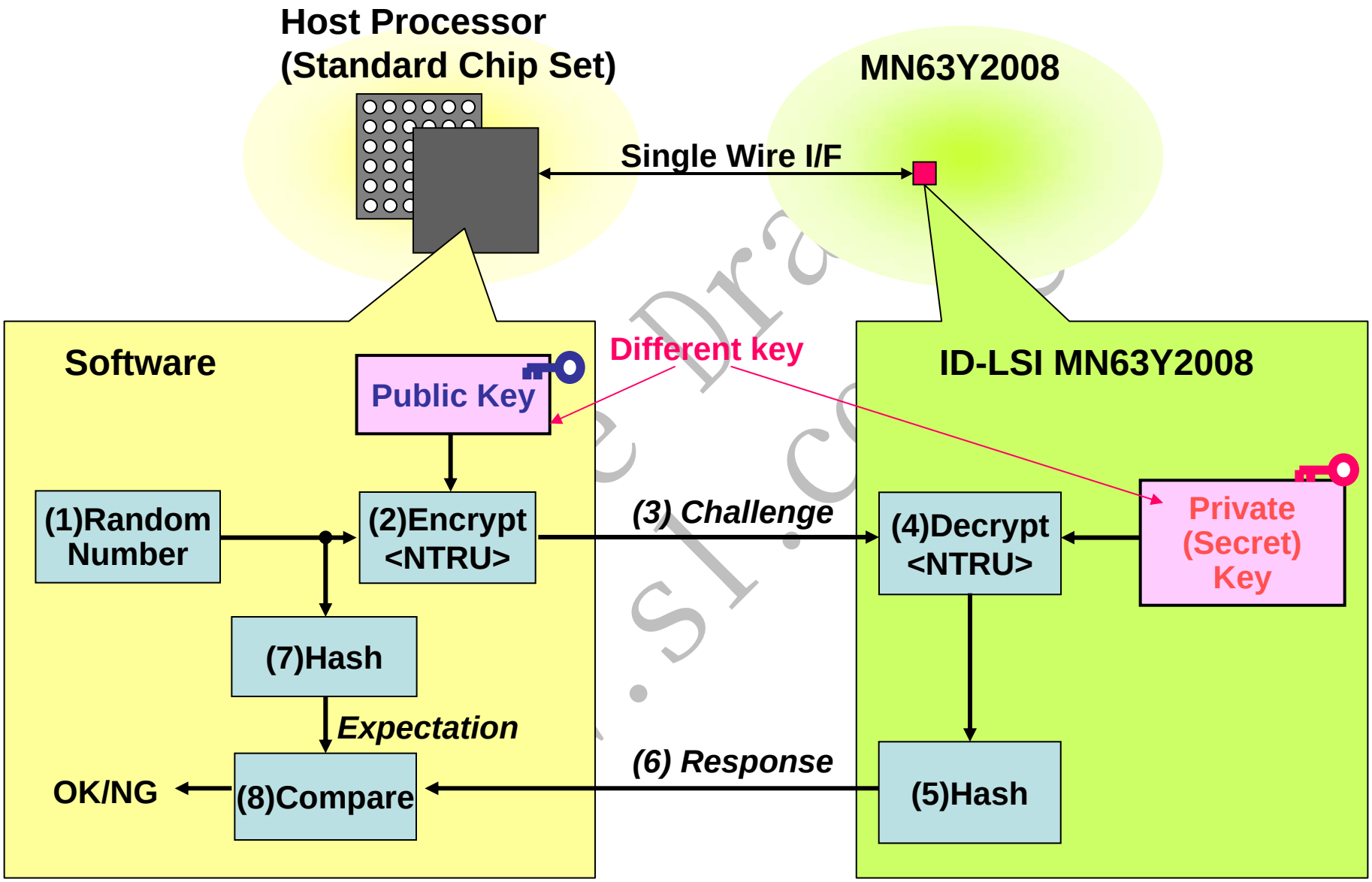
■ Application Circuit



■ Block Diagram



MN63Y2008 Authentication Scheme (Public Key)



◆Host processor cannot work without ID-LSI

Panasonic FeRAM

Shipped more than 400 million Smart Card LSIs & RFID solutions based on FeRAM
- Printer cartridge tag (first commercial product in 2000)
- ID card
- Drivers license card
- Transportation card

◆What is FeRAM?

Memory based on atomic level switching

- •High speed writable
- •Low power
- •Much write cycle
- •Unnecessary high voltage to write
- •Tamper resistance
- •Pb free

◆FeRAM vs. EEPROM

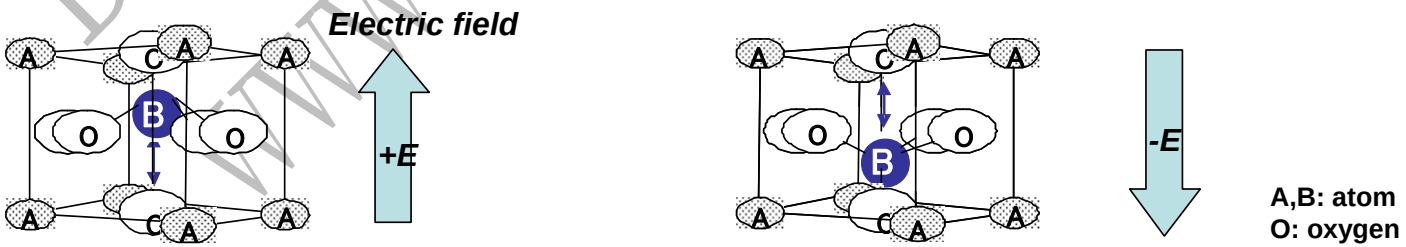
	FeRAM	EEPROM
Write speed	~ μ sec.	~ m sec.
Power Consumption (ratio)	1	5～10
Write cycles	>10e8	10e4～10e5

◆Basic Operating Principle of FeRAM

1）An external electric field causes the polarization of Atom B. The polarization has two stable states.

2）The polarization state of Atom B is retained even if the external eclectic field is removed.

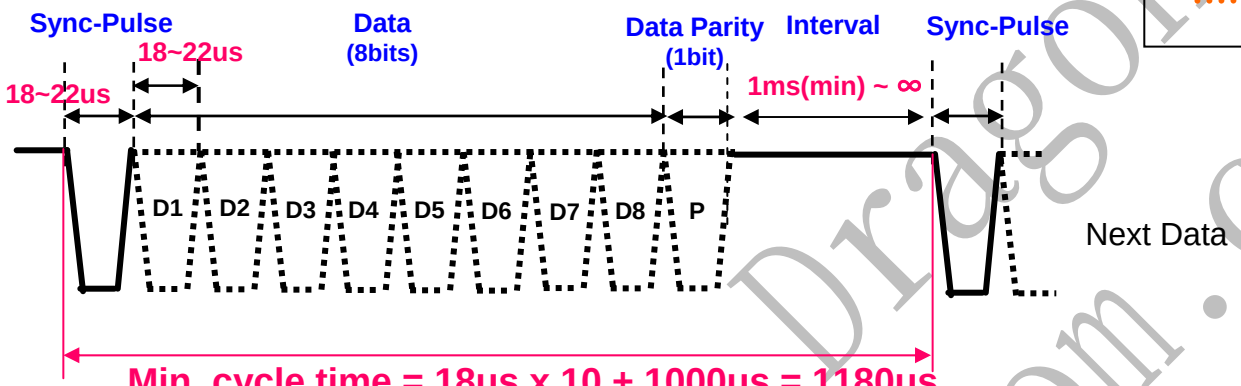
Ferroelectric Crystal Structure



1. Communication bit rate

Waveform of uplink data

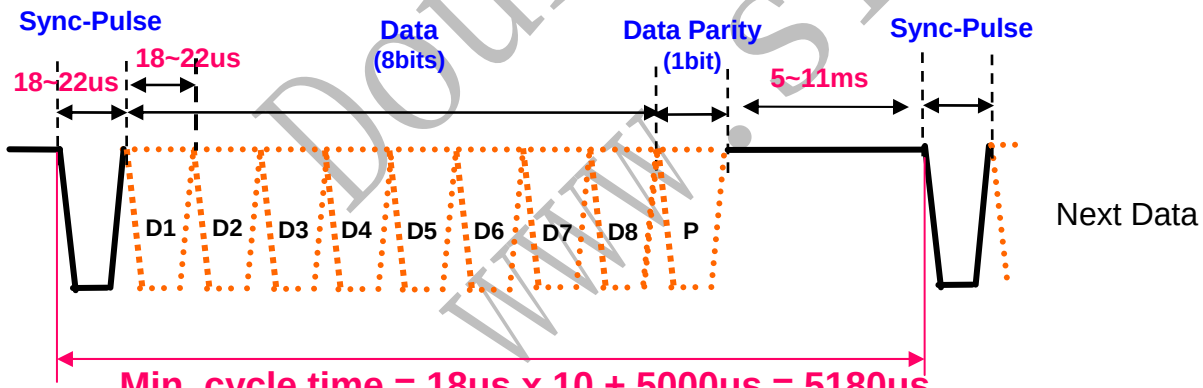
Host LSI Sends 1 byte data to ID LSI after sync-pulse.



Min. cycle time = 18us x 10 + 1000us = 1180us
(Max. bit rate = 8bit / 1180us = 6.8kbps)

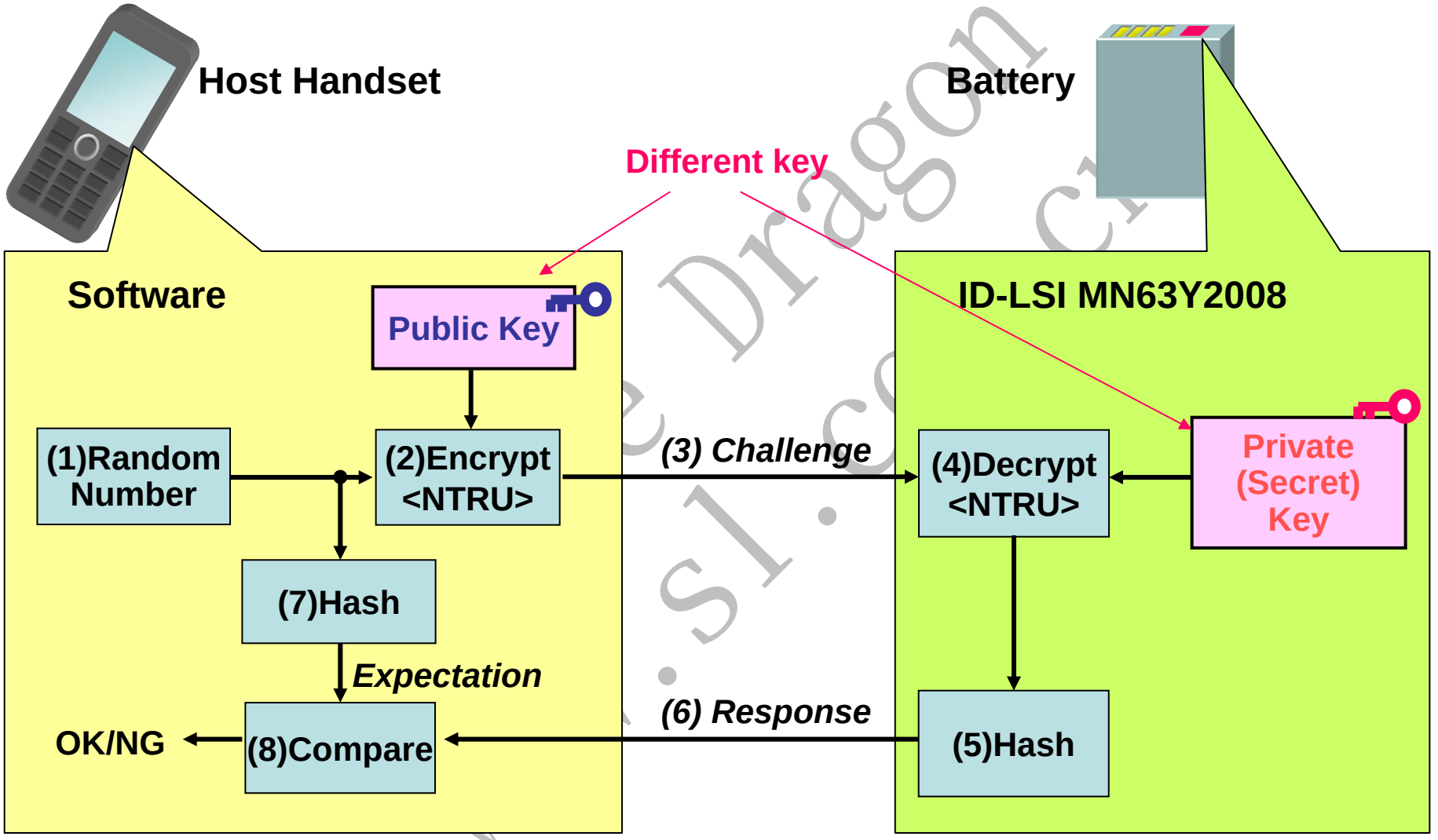
Waveform of downlink data

ID LSI returns 1 byte data to host after Host LSI sends sync-pulse.



Min. cycle time = 18us x 10 + 5000us = 5180us
(Max. bit rate = 8bit / 5180us = 1.5kbps)

MN63Y2008 Authentication Scheme (Public Key)



What is NTRU?

- One of Public (Asymmetric) key cryptosystem based on the shortest vector problem in a lattice
  - Faster & Smaller than RSA or ECC

	NTRU	ECC (Elliptic Curve Cryptosystem)	RSA
Key Length for NIST's Requirement of SP800-57 (Bits of security = 112bit: equivalent to 3-key triple DES)	<401 bit	224 bit	2048 bit
Processing Time for ID-LSI (RSA=1)	0.06	0.6	1
Standard	IEEE1363	ISO/IEC15946	ISO/IEC18033
Year of Proposal	1996	1985	1978

NIST: National Institute of Standards and Technology

For more information about NTRU:

http://en.wikipedia.org/wiki/NTRUEncrypt