Enocoro-128v2:
A Hardware Oriented Stream Cipher

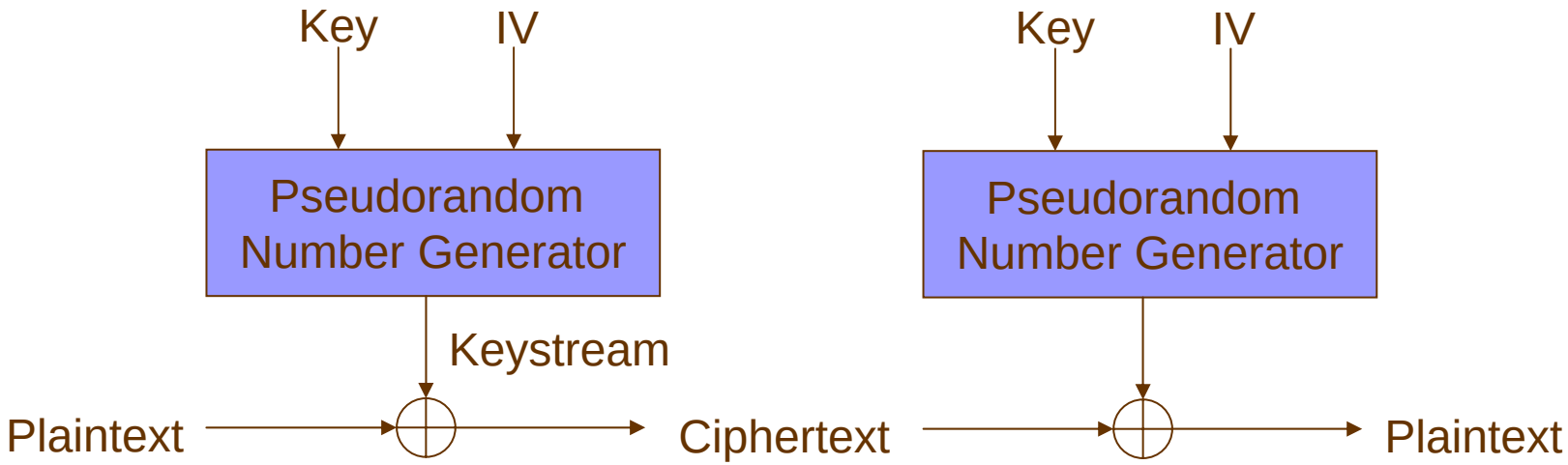
Systems Development Laboratory,
Hitachi, Ltd.

Outline

- A stream cipher
- Specification of *Enocoro*-128v2
- Security and performance results
- Summary

A stream cipher

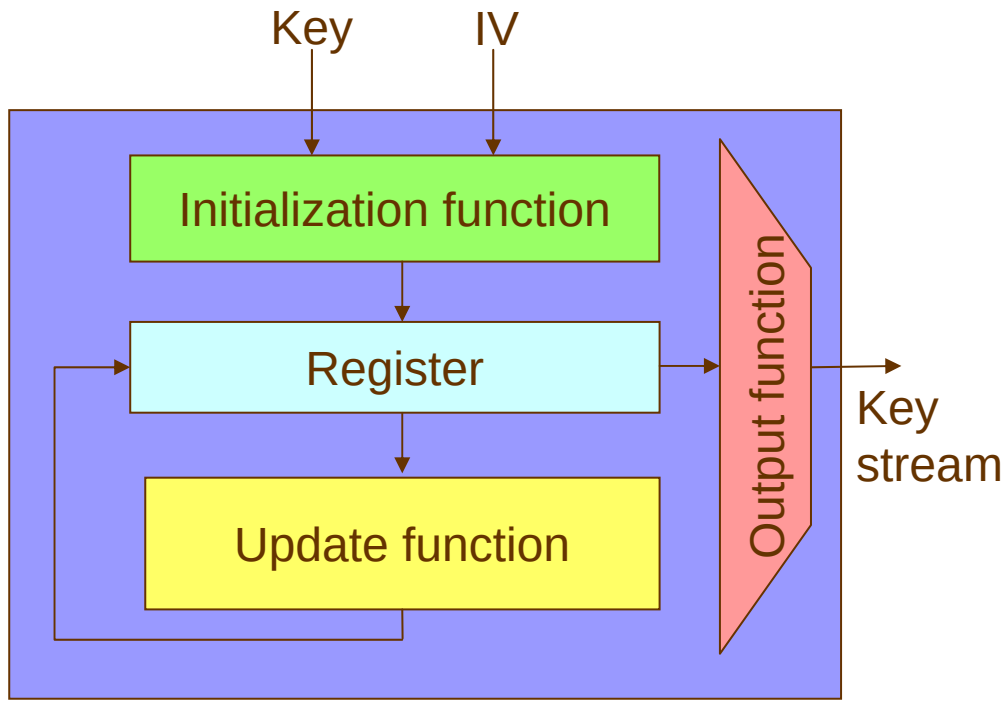
What is a stream cipher



- Originated at Vernam cipher
  - Encryption and decryption are done by XORing a plaintext and a keystream
  - A keystream is generated by a deterministic algorithm called a pseudorandom number generator (PRNG)
  - The security depends on that of a PRNG

Pseudorandom number generator

- Deterministic cryptographic algorithm s.t.
  - Input: a short string
    - Secret: Key
    - Public: Initial vector (IV)
  - Output
    - Long bit string
    - Good randomness properties
    - Hard to recover a key



Security requirements

- The security of stream cipher depends on the underlying PRNG
- Hardness to recover a secret key
  - A PRNG should not leak any information about the key
  - Two kinds of attackers
    - One uses non-randomness property of the outputs
    - One uses “initialization weaknesses”
- Good randomness properties
  - A kind of randomness testing
  - Not necessary to recover a secret key

Time-meory-data trade off

- Generic attack on stream ciphers
  - Proposed by Babbage and Golić independently
    - Consisiting of *pre-computation* phase and *on-line* phase
  - Provides a trade-off between
    - Memory (required to store the result of pre-computations),
    - Time (required to run the attack on line),
    - Data (given data encrypted by a key).
  - Significant suggestion
    - If the size of the secret internal state is smaller than a double of the key length, the stream cipher cannot achieve sufficient security.

Specification of *Enocoro*-128v2

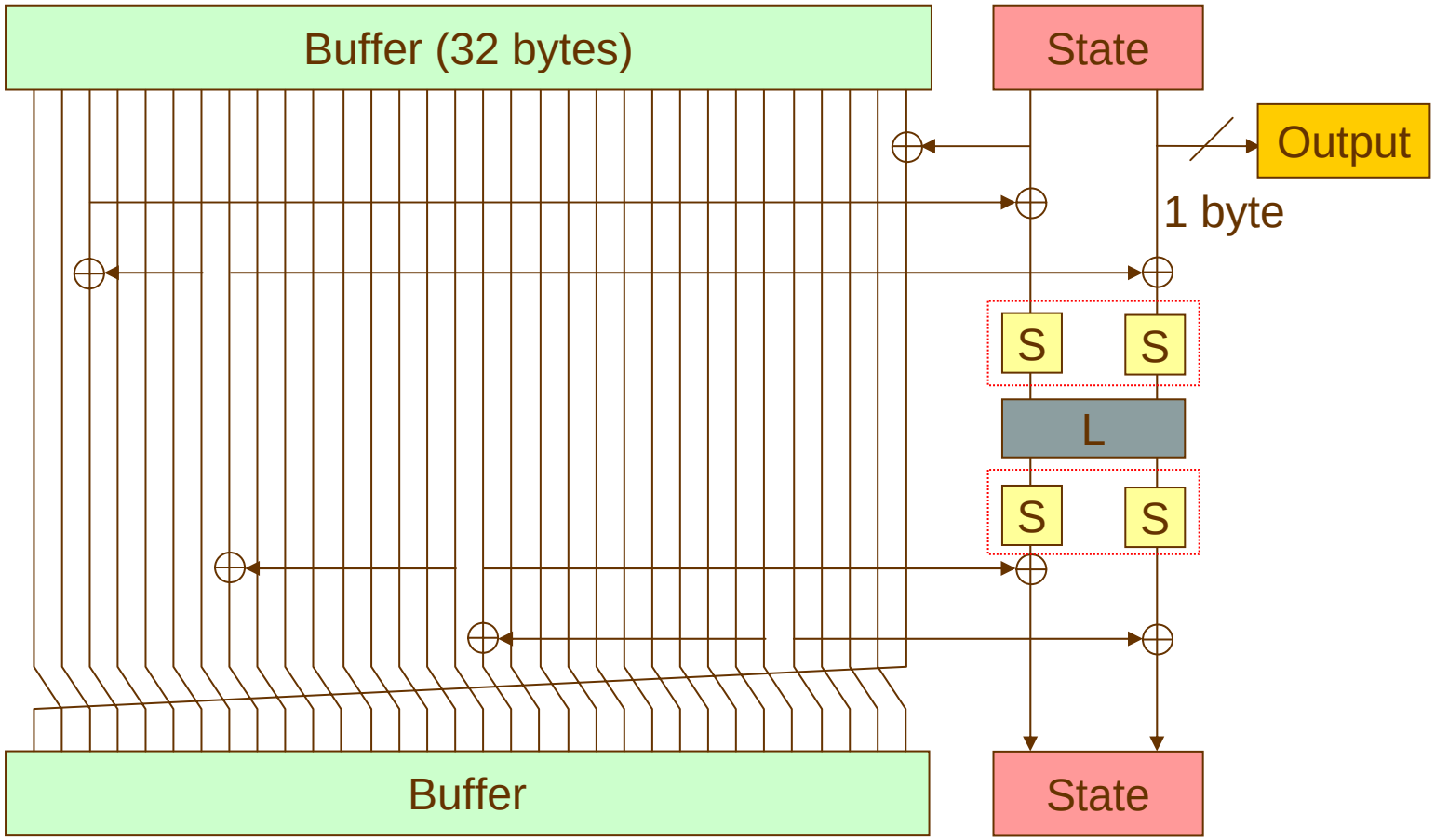
Motivation and design strategy

- eSTREAM Profile-2
  - Hardware oriented light-weight ciphers
  - All selected algorithms are based on bit-wise operations
- Byte-wise design
  - Successful in the design of MUGI
    - Good performances even in software implementations
    - Easy to evaluate the security because many techniques for block ciphers are available

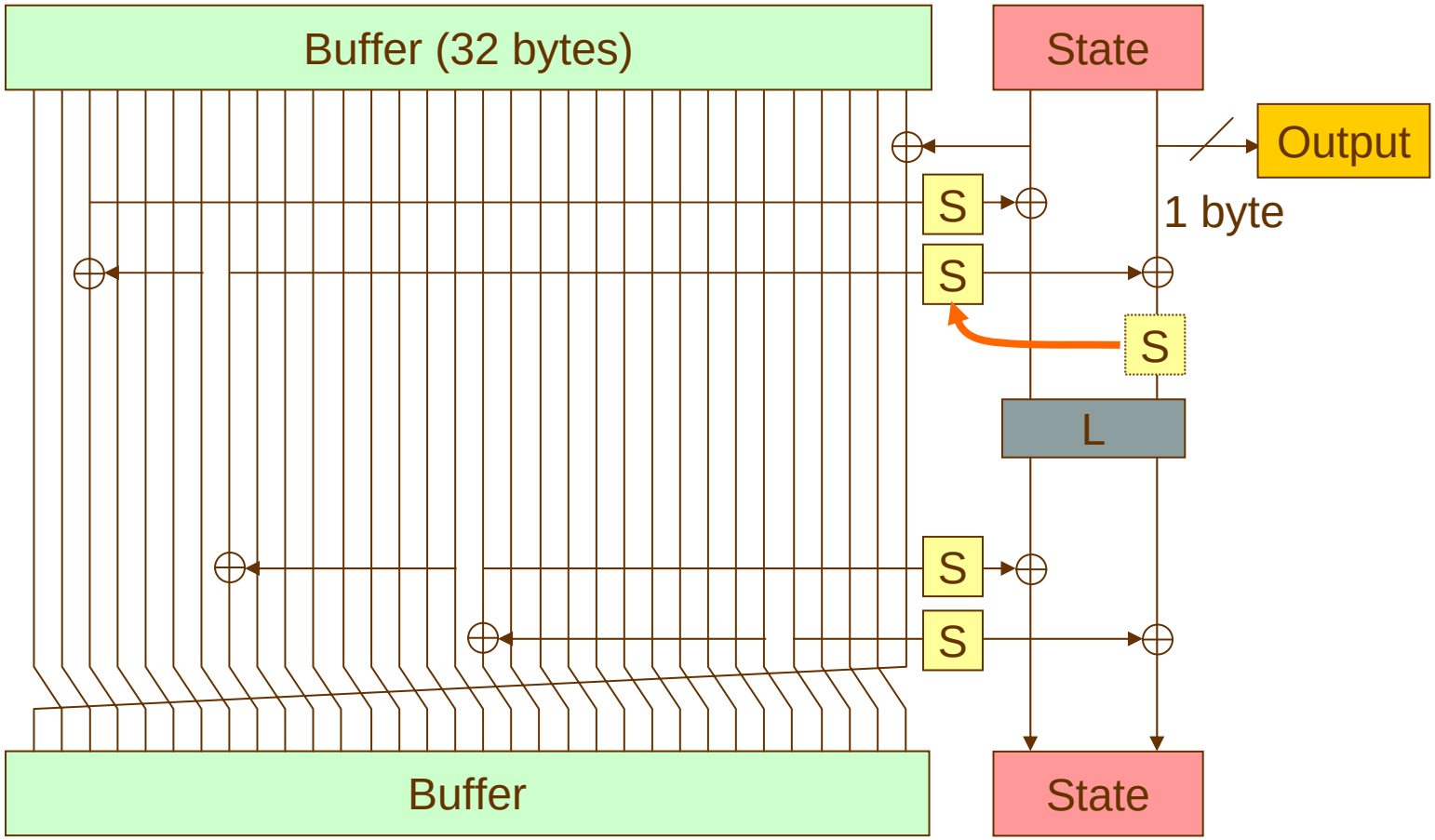
Enocoro-128v2: The feature

- Interface
  - Key length: 128 bits
  - IV length: 64 bits
  - Output
    - 1 byte per a round
    - Up to 2^{64} bytes for each key and IV
- Structure
  - 272 bits internal state
    - Much smaller than MUGI and Panama (in MULTI-S01)
  - byte-wise operations

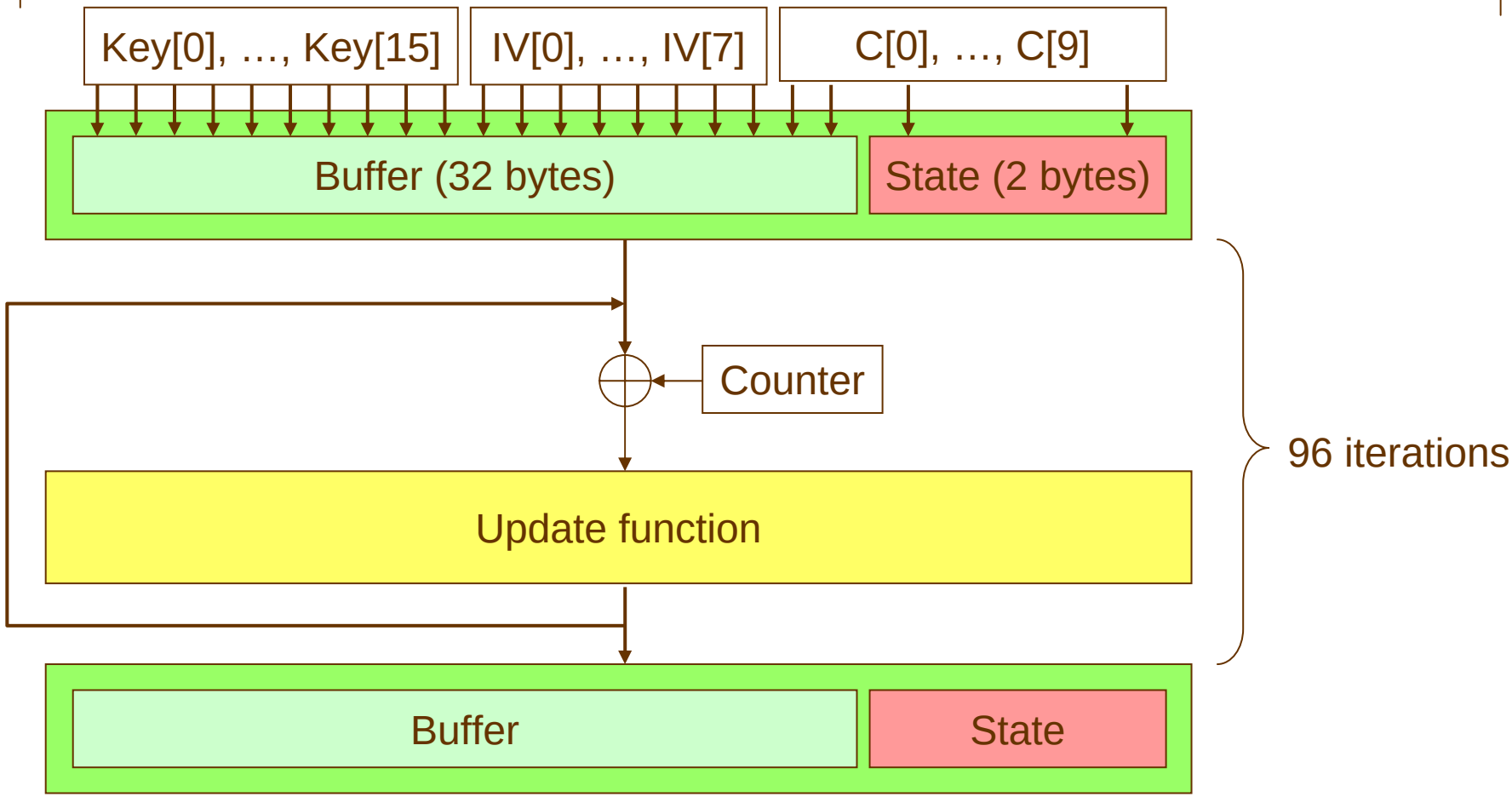
Update function: basic idea



Update function: parallelization



Initialization



Components

- 8-bit Sbox S_8 (non-linear permutation)
  - Consisting of 4 4-bit Sboxes S_4 and a 2x2 matrix over GF(2^4)
  - Substituion-Permutation-Substitution structure
  - MDP=$2^{-4.678}$, MLP=2^{-4}, Alg. deg.=6
- Linear transformation *L*
  - A 2x2 matrix over GF(2^8)
  - Branch num.=3

Security and performances

Current security status

Optimized exhaustive search of the secret internal state	Exhaustive key search	2^{128}
	Time-Memory-Data trade off	2^{136}
	Guess and Determine attack	2^{144}
Distinguishing attacks	Linear distinguishing attack	$\geq 2^{144}$
Initialization weakness	Differential attack	$\geq 2^{140.3}$
	Linear attack	$\geq 2^{177.8}$

- No attack faster than exhaustive key search has been found.

Hardware performance

Algorithm	Max. clock freq. (MHz)	Throughput (Mbps)	Area (K gate)	Process (μm)
Grain-128	925.9	926	1.9	0.13
	581.4	4,651	2.5	
Mickey 2.0	413.2	413	5.0	
Enocoro-128v2	**440.0**	**3,520**	**4.1**	**0.09**
MUGI	51.1	1,600	22.7	0.18
	186.2	11,900	46.0	0.18
AES	131.2	311	5.4	0.11
	80.0	10	3.4	0.35

The results except for Enocoro-128v2 refer to
T.Good and M.Benaissa, ``Hardware performance of eStream phase-III stream cipher candidates,'' in SASC 2008 Proceedings, February 13-14, 2008.

Software performance

Algorithm	Throughput (cycles/byte)	Initialization (cycles)
Grain-128	31.2	1137.5
Mickey-128 2.0	1231.4	56592.1
Enocoro-128v2	**46.3**	**4869.5**
AES-CTR	17.8	469.6
SNOW 2.0	5.0	1086.0

The results except for Enocoro-128v2 refer to http://www.ecrypt.eu.org/stream/phase3perf/2007a/pentium-4-a/ (revision 206).

Summary

- A new stream cipher *Enocoro*-128v2
  - Based on byte-wise operations
  - Good secuirty status
  - Still comparably small in ASIC design
  - Moderate performance in software implementation