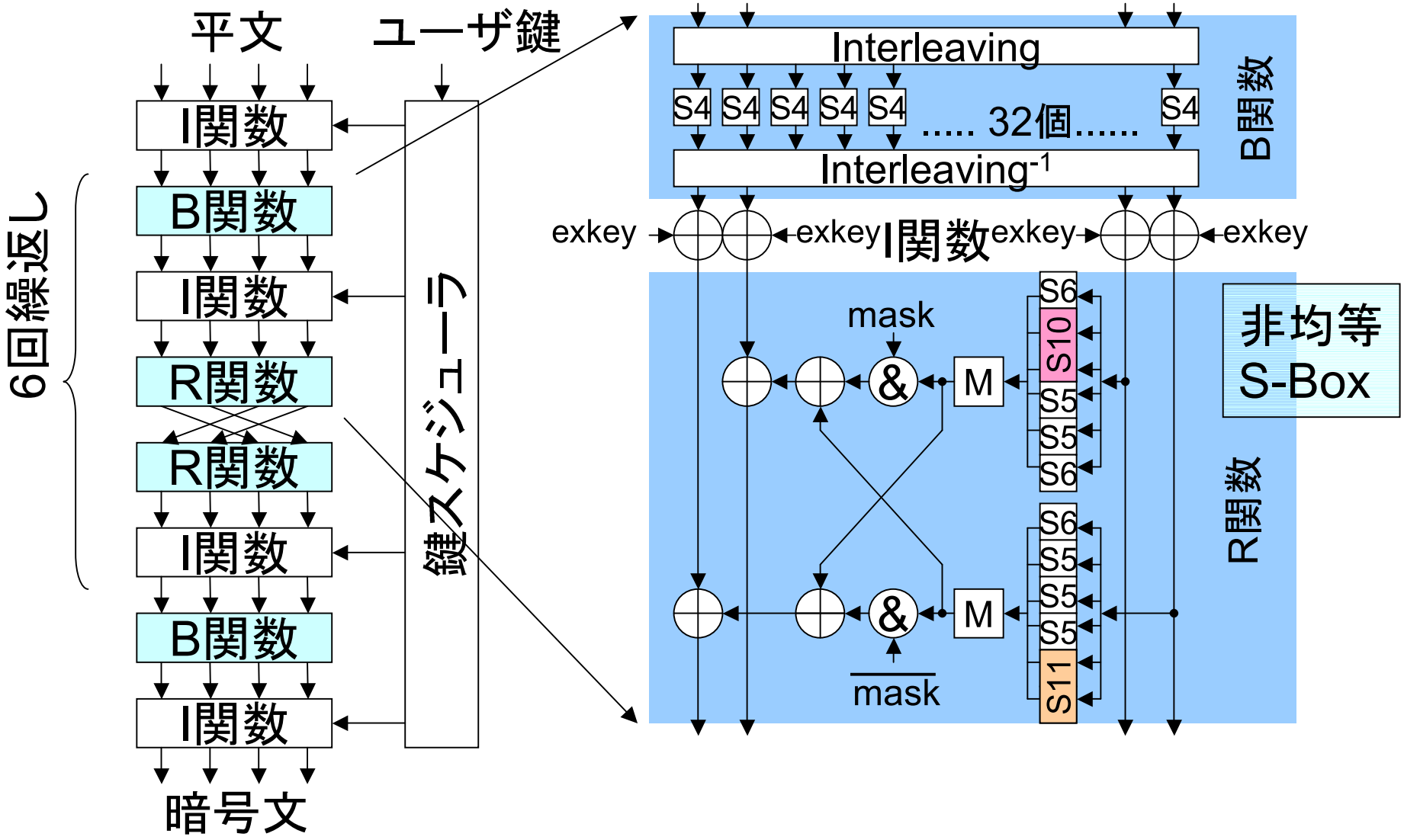
共通鍵ブロック暗号 SC2000の実装（III）

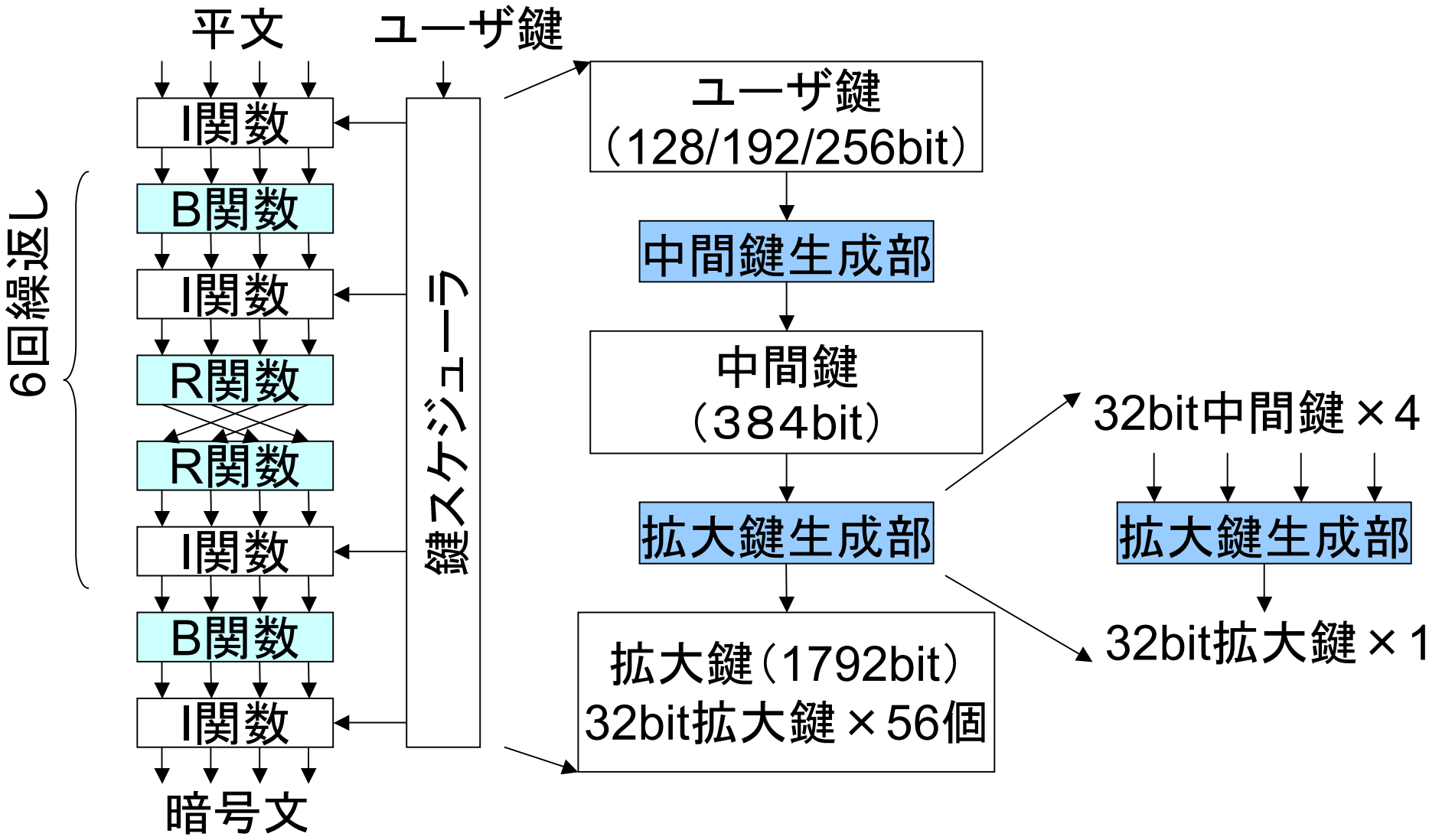
株式会社富士通研究所
武仲正彦，鳥居直哉
Helsinki University of Technology
Helger Lipmaa

Contents

SC2000のデータスクランブル部



SC2000の鍵スケジュール部



実践ソフトウェア

IA-32上の

従来の実装結果（ソフトウェア）

Processor	Language	Strategy	Encrypt（cycles）
Pentium III (Katmai)	C + inline Asm	(6,10,10,6)	383
		(11,10,11)	525
Athlon (K7)	C + inline Asm	(6,10,10,6)	392
		(11,10,11)	318
UltraSPARC-2	C	(6,10,10,6)	274
Alpha 21264	C	(11,10,11)	238

SC2000はIA-32上で速度が出ない?

IA-32上で高速化実装を！

非均等S-Boxの結合方法

	Look-up	Size	
S6 S5 S5 S5 S5 S6	6回	1KB	
S6 S10 S10 S6	4回	8.5KB	PentiumIIIの 1st-cacheに 入るサイズ
S11 S10 S11	3回	20KB	Athlonの 1st-cacheに 入るサイズ
提案方式 S16 S16	2回	512KB	PentiumIIIの 2nd-cacheに 入るサイズ

実装・評価環境（ソフトウェア）

- プロセッサ

  Pentium III-M 1.2GHz（Tualation-512）
  Mem：128MB OS：Linux 2.4.18

  Athlon 1.4GHz（Thunderbird）
  Mem：512MB OS：Linux 2.4.17

- コンパイラ（C言語実装）

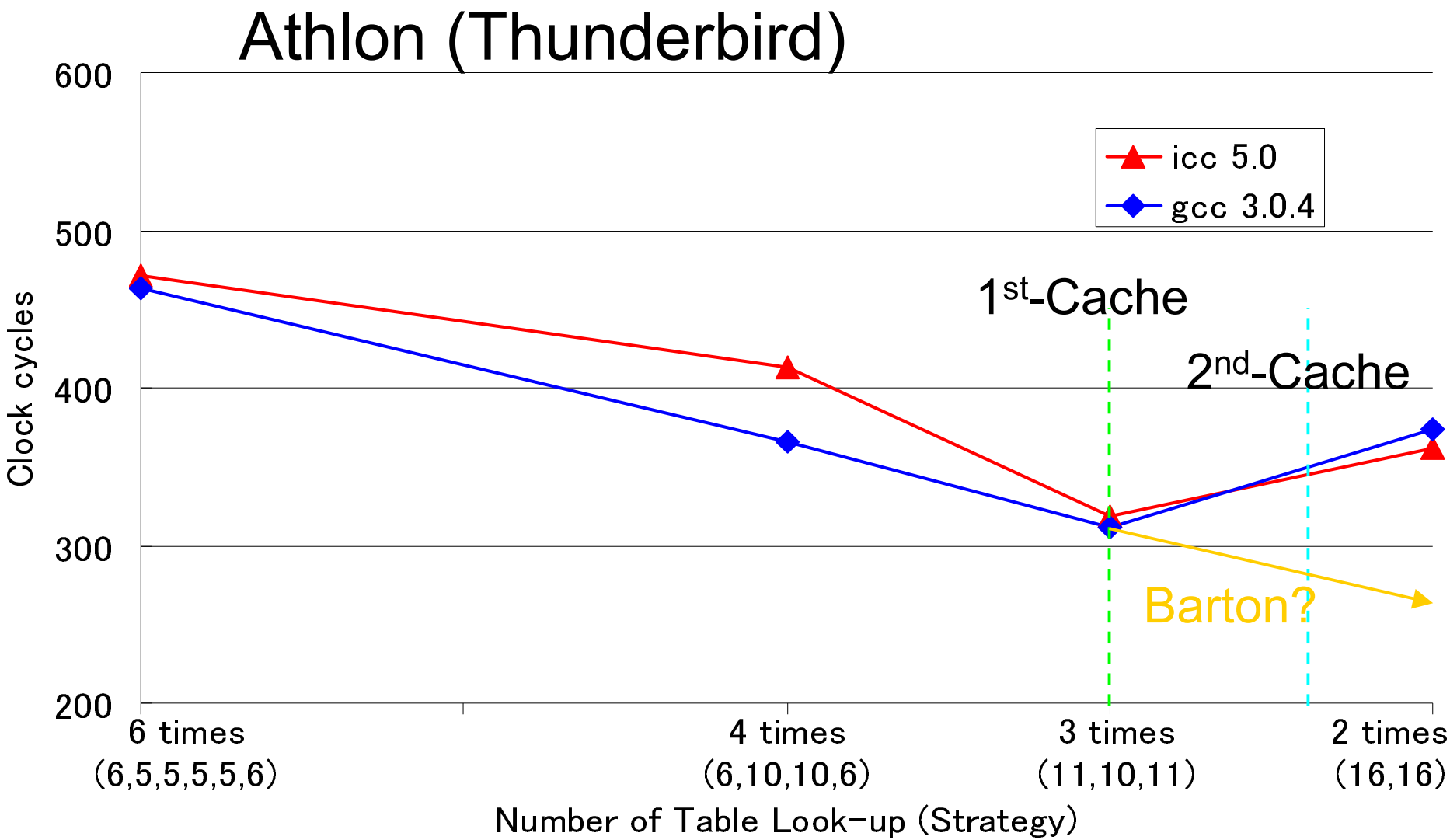
  Intel C Compiler Version 5.0（icc 5.0）

  Gnu C Compiler Version 3.0.4（gcc 3.0.4）

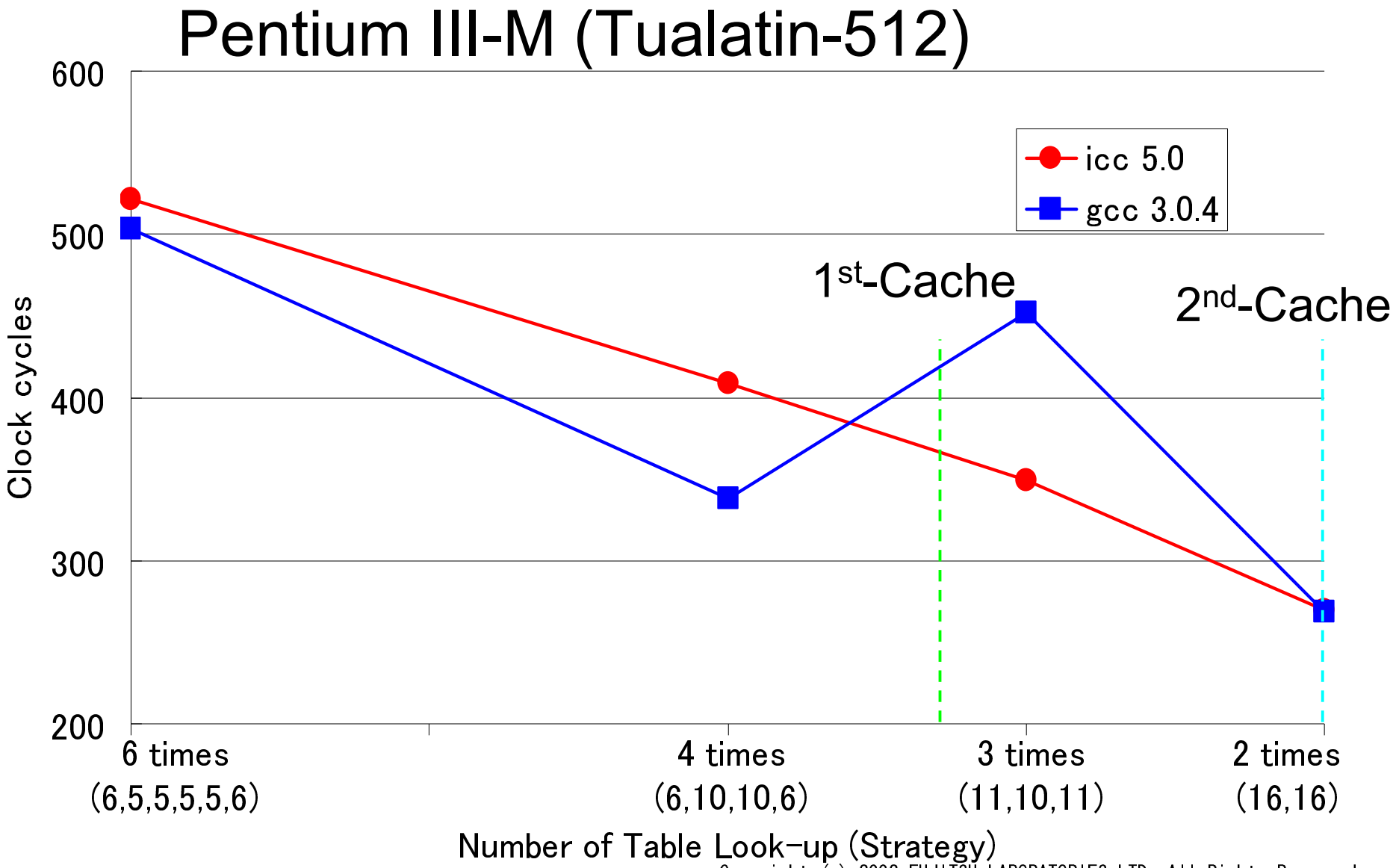
- S-Boxの結合方法

  (6,5,5,5,5,6), (6,10,10,6), (11,10,11), (16,16)

実装結果（ソフトウェア1）



実装結果（ソフトウェア2）



他暗号との性能比較

Cipher	Compiler (Language)	Encrypt（cycles）	Decrypt（cycles）
AES	icc 5.0	430	435
	gcc 3.0.4	346	371
	assembly	226	226
RC6	icc 5.0	257	289
	gcc 3.0.4	234	265
	assembly	222	222
SC2000	icc 5.0	270	278
	gcc 3.0.4	269	376

より詳しい結果はISC2002(9/30-10/2 Brazil Sao Paulo)をご参照ください

熱帯ドキュメンタリー概要

従来の実装結果（ハードウェア）

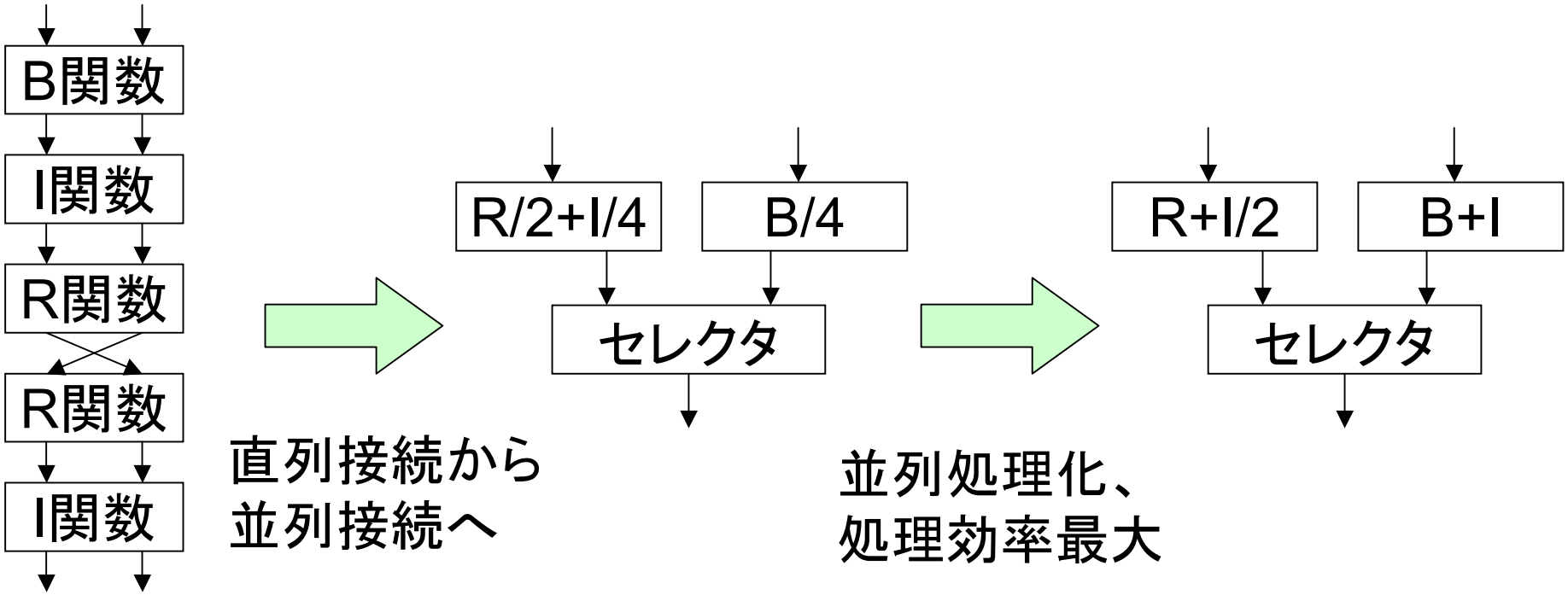
発表	テクノロジ	構成	回路規模（KGate）	処理速度（Mbps）
SCIS2001	0.25 μm	大規模（unroll）	226	1290
		中規模（loop）	63	964
		小規模（loop）	33	264
SCIS2002	0.18 μm	小規模（loop）	8.9	200

SC2000は高速処理に向かない?

↓

ハードウェアで高速化実装を！

提案構成概要（ハードウェア）

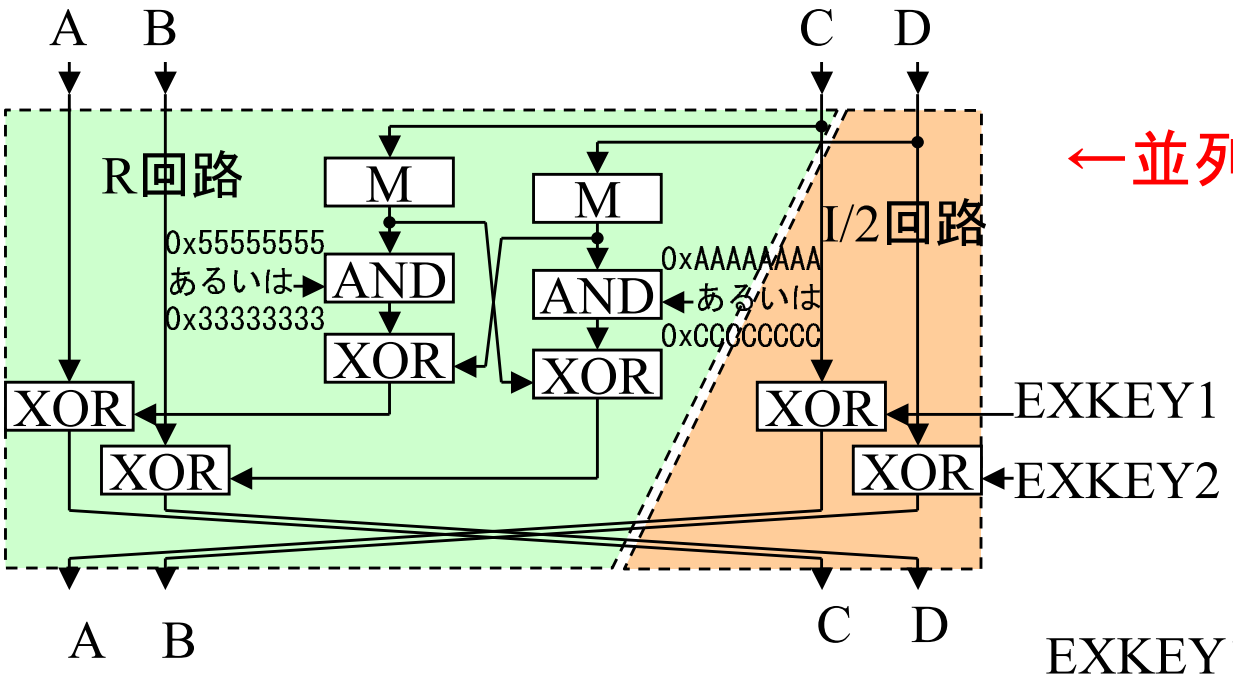


SCIS2001構成
CISC型

SCIS2002構成
RISC型

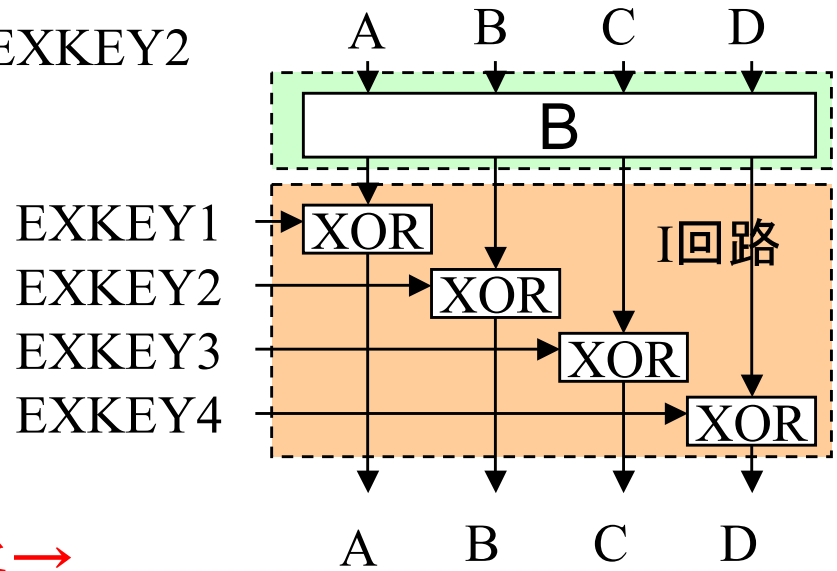
提案構成
RISC型

データスクランブル部の構成



←並列処理化

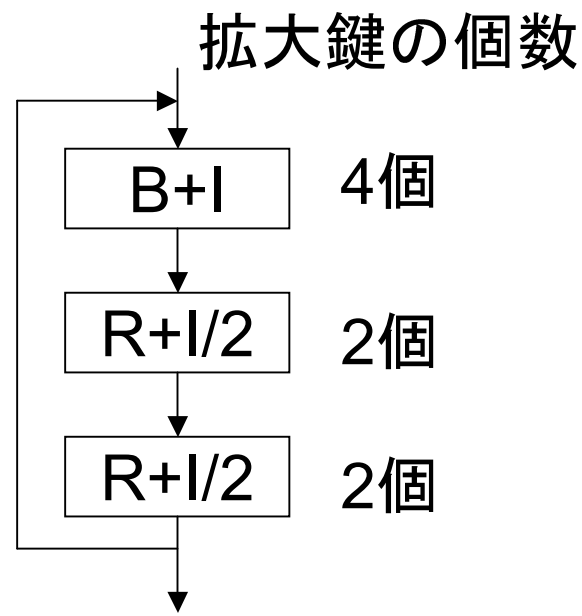
R+ I/2関数回路構成



サイクル当りの処理の効率化→

B+ I関数回路構成

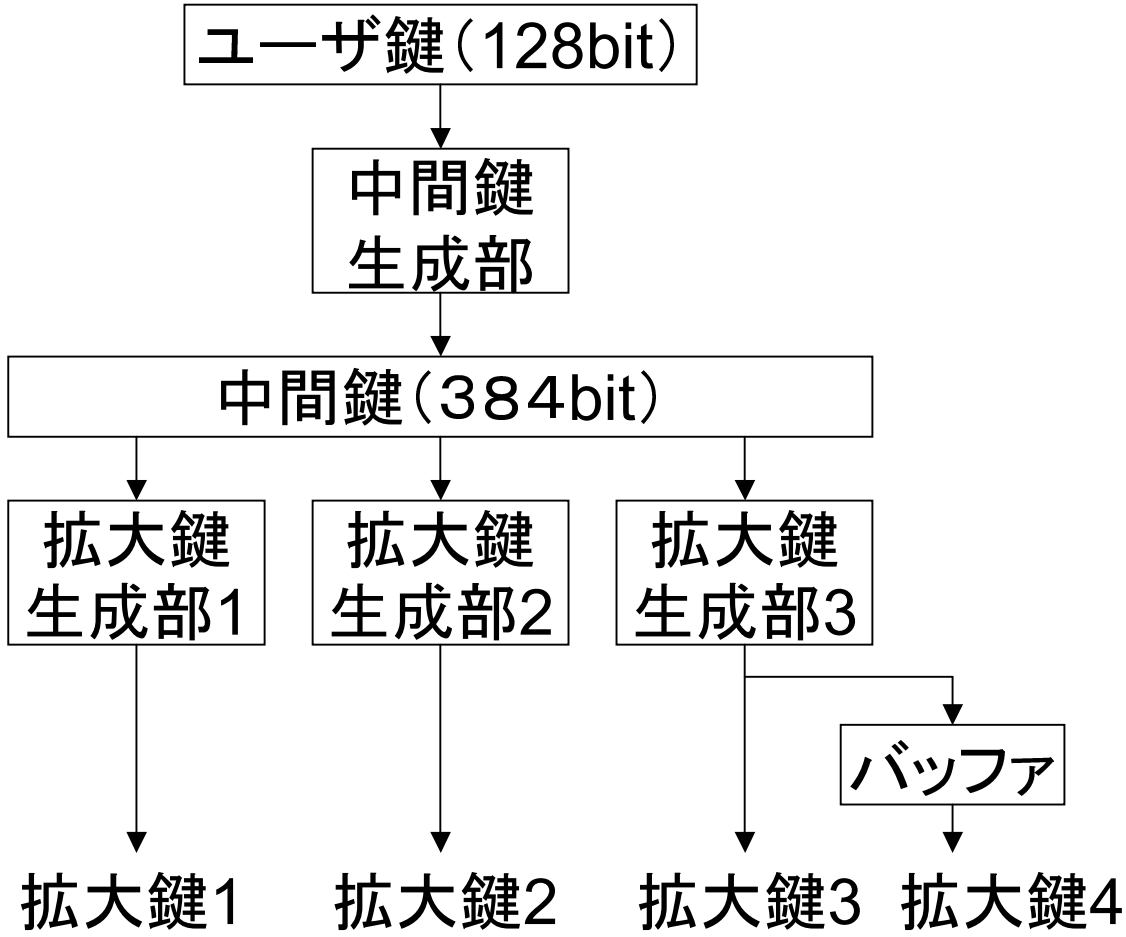
鍵スケジュール部の構成



最大4個/cycle必要

平均3個/cycle必要

回路使用率の向上



実装結果（ハードウェア）

テクノロジ	構成		回路規模（KGate）	処理速度（Mbps）	効率（Mbps/Kgate）
0.25 μm	大規模（unroll）		226	1290	5.7
	中規模（loop）		63	964	15.3
	小規模（loop）		33	264	8
0.18 μm	小規模（loop）		8.9	200	22.5
	高速（loop）	速度重視	26.4	1423	54.0
		効率重視	21.6	1293	60.0

富士通製0.18μmテクノロジCMOSプロセスASIC CS81シリーズ使用
SYNOPSYS社製Design Compiler 2000.05-1
コマーシャルワースト

まとめ

- IA-32上で高速実装可能
  - 二次キャッシュを効率的に使用
  - 非均等S-Boxを(16,16)実装
  - C言語で270cycle/回を実現
- ハードウェアでも高速実装可能
  - いわゆるRISC構成で回路効率向上
  - R+I/2, B+I, 拡大鍵生成3個の構成
  - 26 KGateで1.4 Gbpsを実現

FUJITSU

THE POSSIBILITIES ARE INFINITE