NTT・三菱電機共同開発暗号
Camellia

NTT 情報流通プラットフォーム研究所

Camellia (カメリア) ホームページ

http://info.isl.ntt.co.jp/crypt/camellia/

E-mail: camellia@lab.ntt.co.jp

Camelliaとは　～ 世界を目指す国産暗号 ～

世界中で使われる日本発の暗号技術を目指して
＝ 国産技術で安心・安全な情報化社会の実現を ＝

- **2000年にNTTと三菱電機の技術力を結集して開発した128ビットブロック暗号（鍵長128/192/256ビット）**
- **国産初をはじめ多くの国際標準規格・推奨規格に採用**
- **Firefox3など国際的なオープンソースソフトウェアに搭載**

Camellia（日本語名：椿）
　日本原産の植物。学名はカメリア・ジャポニカ
　花言葉：Good fortune and loveliness, gratitude
その心は・・・
　日本の国産暗号技術ということのみならず、世界中の様々な環境で利用される暗号技術になってもらいたい
　～“椿”が世界中に広まって“カメリア”と名付けられたように～

Camelliaとは　～ 世界を目指す国産暗号 ～

米国政府標準暗号AES同等と評価された
世界唯一のAES代替国際標準暗号
～ 世界最高水準の安全性と処理性能の両立を実現 ～

- **世界で認められた最高水準の安全性を保証**
  - ８年以上も安全に利用され続けている安定した利用実績
  - AESよりも高い安全性（セキュリティマージン）を確保
  - 世界中の暗号研究者によって第三者検証された安全性
- **ソフトウェア実装・ハードウェア実装問わず、どんな利用環境でも世界トップクラスの処理性能を実現**
  - PC、ICカード、組込機器など、様々な利用環境に応じて最適な実装方法が選択できる高度な実用性

Camelliaとは　～ 実現した国産暗号初物語 ～

今までの暗号開発にはなかった
利用者ニーズ優先の“国産暗号初”を実現

- **多くの国際標準規格・推奨規格に採用**
  - インターネット標準暗号、ISO/IEC国際標準暗号等に採用
- **基本特許無償化＆本格的オープンソース展開を実施**
  - 特許無償許諾の手続き無しに利用可能
- **多くの国際的なオープンソースソフトウェアに搭載**
  - 国産技術で安心・安全な情報化社会を容易に実現するための基盤を整備
- **MITケルベロスコンソーシアム**に加盟
  - 欧米製品での利用促進

Camelliaの特徴 ～ オープンソース化施策 ～

世界中のオープンソースコミュニティが受け入れた
初めての国産暗号技術

"In the encryption world, new is bad. Older is better. Ciphers that have been reviewed, deployed, and attacked repeatedly (and survived!) are best."

NTT製オープンソース
❒ C (GPL, LGPL, BSD, OpenSSL, MPL)
❒ Java (GPL, BSD)
❒ Ruby Camelliaパッケージ
❒ ガイダンス・インストラクション資料

OS カーネル	❒ FreeBSD 6.4以降/7.0以降
	❒ Linux kernel 2.6.21以降
	❒ Fedora Core 7以降

アプリケーション	❒ Firefox 3.0以降
	❒ ipsec-tools 0.7以降
	❒ Kerberos - KRB5 1.9以降
	❒ GnuPG 2.0以降

暗号ツールキット	❒ OpenSSL toolkit 0.9.8c以降／1.0.0以降 注：1.0.0はそのままご利用いただけますが、0.9.8xではコンパイルオプションでenable-camelliaを指定する必要があります。詳しくはOpenSSLに関するガイダンス資料をご参照ください。
	❒ NSS (Network Security Services) 3.12以降
	❒ Crypto++ library 5.4以降
	❒ The Legion of the Bouncy Castle 1.30以降
	❒ GNU Transport Layer Security Library 2.20以降

第三者コード	❒ Camellia for Open Souce Softwares
	❒ Camellia for Python
	❒ Perl Camellia encryption module
	❒ openCrypto.NET
	❒ Pascal source by Wolfgang Ehrhardt

国産暗号によるSSL暗号通信が初めて可能に

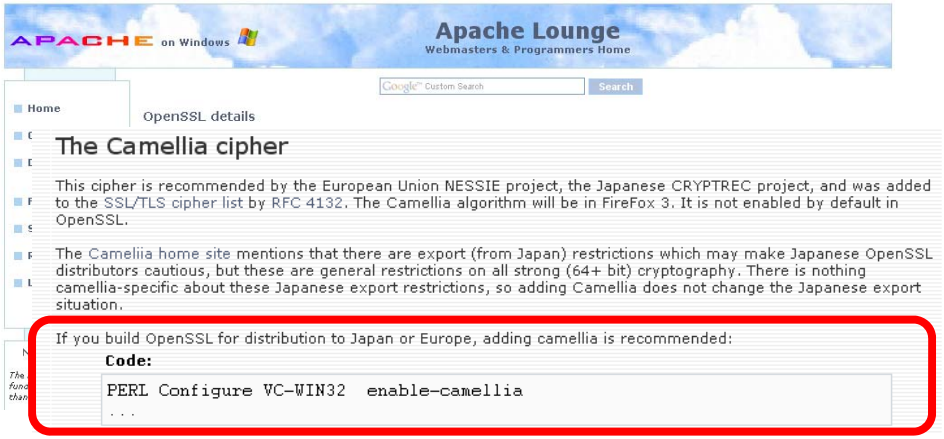
WWWサーバ
（例：ECサイト）

SSL/TLS暗号通信路 by Camellia

WWWブラウザ
（例：顧客）

Sever: Apache+OpenSSL
日本・欧州ではCamelliaを利用可能にすることを推奨

Browser: Firefox 3
「史上最速・最軽量」と「日本発の技術を搭載」がキーワード



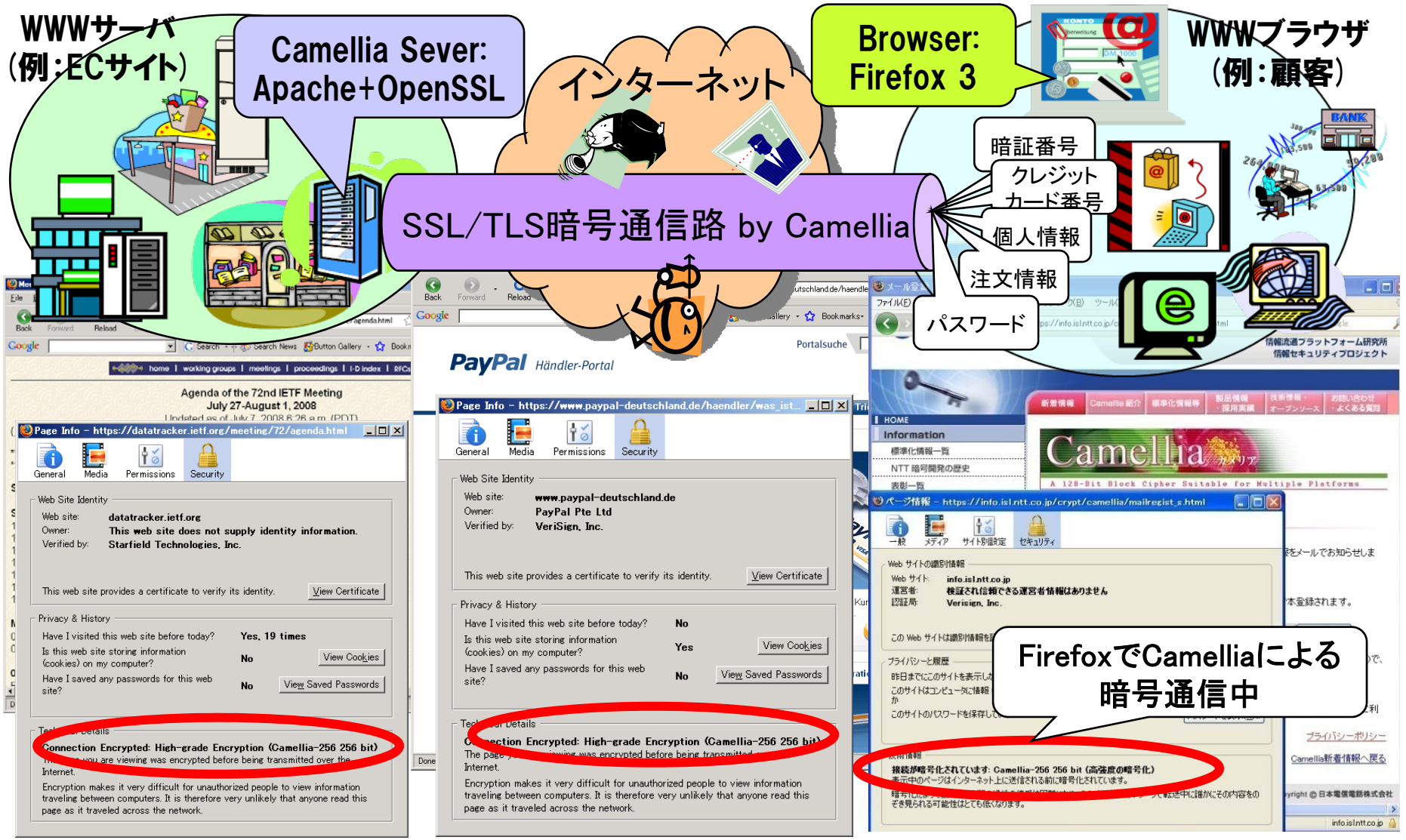
引用：Apache Lounge，http://www.apachelounge.com/forum/viewtopic.php?t=1992

引用：Mozilla Firefox 3 日本語版レビューアーズガイド

【参考】 Camelliaを利用可能にするためのガイダンス資料を公開しています。また、以下のOSに同梱されているOpenSSLではCamelliaが使えるバージョンのものがすでに組み込まれています。

Fedora Core 9以降、OpenSUSE 10.3以降、Gentoo Linux 2008.0以降、FreeBSD 7.0以降、FreeBSD ports 2007/6/12以降

国産暗号によるSSL暗号通信が初めて可能に



Camelliaの特徴 ～ 国際標準化実績 ～

国際的には日本を事実上代表する暗号と認知

標準化機関等	標準化概要
ISO/IEC	ISO/IEC国際標準暗号 (ISO/IEC18033-3)
NESSIE	欧州連合推奨暗号
CRYPTREC	電子政府推奨暗号
RSA Laboratories	暗号トークン標準インタフェース (RSA PKCS#11)
ITU-T	次世代ネットワーク(NGN)用暗号
TV-Anytime Forum/ETSI	次世代放送コンテンツ流通システム著作権管理・情報保護(DRM)用暗号

標準化機関等	標準化概要
日本初	SSL/TLS標準暗号 (RFC4132)
	IPsec標準暗号 (RFC4312, 5528, 5529)
	S/MIME標準暗号 (RFC3657)
IETF	XML標準暗号 (RFC4051)
	OpenPGP暗号 (RFC5581)
	Description of Camellia (RFC3713)

	提案国	ISO/IEC 国際標準	政府関連				IETF標準暗号				RSA PKCS#11
			米国政府標準	欧州連合推奨	電子政府推奨	韓国政府標準	SSL/TLS	IPsec	S/MIME	XML	
Camellia	日本	○	--	○	○	--	○	○	○	○	○
AES	米国	○	○	○	○	--	○	○	○	○	○
SEED	韓国	○	--	--	--	○	○	○	○	--	--
Triple DES	米国	○	○	--	△	--	○	○	○	○	○
CAST-128	カナダ	○	--	--	--	--	--	○	○	--	○
MISTY1	日本	○	--	○	○	--	--	--	--	--	--
IDEA	スイス	--	--	--	--	--	○	○	○	--	○
RC4	米国	--	--	--	△	--	○	--	--	○	○

Camelliaの特徴 ～ オープンソース化施策 ～

国産技術で安心・安全な情報化社会の実現を
～ 国際標準規格の国産暗号を簡単・便利に使いやすいものに ～

- **実装・利用における基本特許無償化を実施**

  http://info.isl.ntt.co.jp/crypt/info/chiteki.html

- **暗号エンジン・各種パッチのオープンソースを提供**

  http://info.isl.ntt.co.jp/crypt/camellia/source.html

  - C言語(GPL, LGPL, BSD, MPL, OpenSSL)
  - Java (GPL, BSD)

- **利用ガイダンス・インストラクション資料を提供**
  - OpenSSL利用ガイダンス　等
- **第三者ソースコード提供も歓迎**

Camelliaの特徴 ～ 採用実績 ～

http://info.isl.ntt.co.jp/crypt/camellia/product.html にて製品情報・採用実績を公開中

- **政府系システム：多数のシステムで稼働中**
- **民間系システム：**

  通信・情報サービス業界（例：株式会社ミクシィ）、ゲーム業界（株式会社カプコン）、金融機関、印刷業界、大学、電機メーカ などで稼動中
- **市販製品・サービス：60社以上のプロダクトで採用**

NTTソフトウェア	CipherCraft シリーズ	ルネサス	SH7781 SuperH RISC engine
NEL	Camellia LSI, SU1000 等	パナソニック電工	NetCocoon Analyzer
NTT-AT	Smart Leak Protect 等	IIJ-Tech	統合メールセキュリティソリューション「iiMail Suite」
NTTコム	セキュアファイル転送システムV-Pack 等	ｲﾝﾃﾘｼﾞｪﾝﾄｳｪｲﾌﾞ	内部情報漏洩対策システムCWAT
		ｺﾐｭﾆﾃｨｰｴﾝｼﾞﾝ	オンラインゲーム高速通信ミドルウェアVCE
NTT-IT	貼るパスワードHaruPa	AuthenTec（旧SafeNet）	QuickSec Toolkit
三菱電機	Cryptopia, MistyGuard 等	THALES（旧nCipher）	netHSM, nShield, miniHSM等
Canon	C-SELECT（JCMVP認証製品）	IAIK	IAIK-JCE, iSaSiLk, CMS-S/MIME, IAIK-XSECT
		Bloombase	Spitfire KeyCastle, Spitfire StoreSafe 等

Camelliaの特徴 ～ 安全性・信頼性 ～

国際的に認められた暗号開発実績のある NTTと三菱電機の技術力を結集した暗号設計

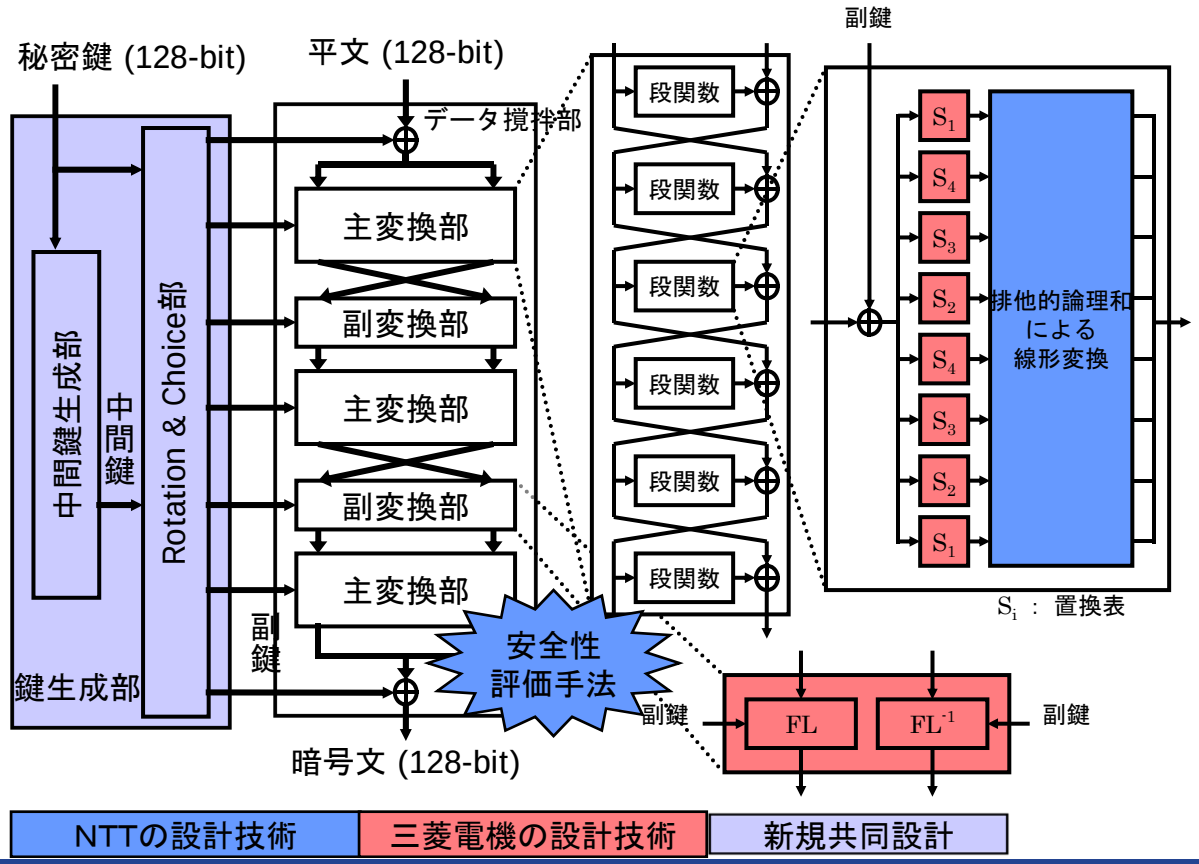
NTT
高速ソフトウェア実装に適した暗号設計技術

⊗

三菱電機
小型/高速ハードウェア実装に適した暗号設計技術

⊗

両社
暗号安全性評価技術（世界トップレベルの研究者）



Camelliaの特徴 ～ 第三者検証された安全性 ～

数値的に証明された世界最高水準の安全性実現
～ AESよりも高い攻撃耐性（セキュリティマージン）を確保 ～

- **設計方針としての透明性**
  - アルゴリズム・設計方針・安全性自己評価の完全公開
- **世界中の暗号研究者による約50件もの安全性評価**
  - 第三者検証によって最新の攻撃に対しても安全性を確認

  [参考] 2009年にAES（鍵長192, 256ビット）はBiryukovらが発見した関連鍵攻撃によって理論的解読に成功
- **解読技術の進展に対する将来的な安全性確保を考慮した高い攻撃耐性を維持**

（2009年9月時点）

攻撃可能段数	7	8	9	10	11	12	13	14	15	仕様段数
鍵長128ビット	解読可能	解読可能	解読可能	解読不可	解読不可	解読不可	解読不可	解読不可	解読不可	解読不可（18段）
鍵長256ビット	解読可能	解読可能	解読可能	解読可能	解読可能	解読不可	解読不可	解読不可	解読不可	解読不可（24段）

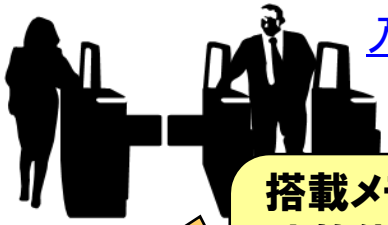
Camelliaの特徴 ～環境に応じた実装柔軟性～

利用環境に応じた世界最高水準の処理性能と実装柔軟性を実現するマルチプラットフォーム型暗号
～ 組込機器などで最高の実装性能を発揮 ～

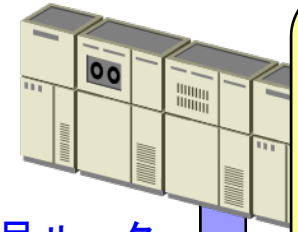
- **利用環境に応じた最適な実装方法の選択が可能**
  - 同一回路／手順で暗号化処理と復号処理が共用可能
  - 8-bitを主な処理単位とする全体構造と副鍵生成部
  - 論理演算とテーブル参照（逆元回路でも可）の組み合わせ

ソフトウェア	32-bit/64-bit CPU	■ 豊富なメモリ量と強力な命令セットで高速処理が可能 ■ テーブル参照以外は32ビット演算処理が可能
	ICカード（Smart card）	■ 限られたメモリ量と基本命令セットで効率的な実装が可能 ■ ローエンド型、ハイエンド型とで異なる実装が可能
ハードウェア	■ 小型・低消費電力設計（小規模実装用）にも高速・並列処理設計（高速実装用）にも対応可能なテーブルを採用 ■ 全体構造と鍵生成部の共有が可能な構造を採用	

Camelliaの特徴 ～様々な環境での高速処理～



入退出管理システム・
交通系システム

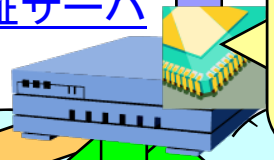


■ Gbpsクラスの高速ハードウェア実装
約45KG, 約2Gbps (0.18μm ASIC)
約9.5Kslice, 約400Mbps (FPGA)
（鍵長128ビット専用）
■ 高速なソフトウェア実装
■ 多くのクライアントからの要求を高速に処理

搭載メモリが少ないICカード・演算能力が低い小型CPU上でも高速かつコンパクトな実装
RAM:約60B, ROM:1.5KB以下
処理時間: 約2msec (@15MHz)
（鍵長128ビット、データサイズ128ビット）

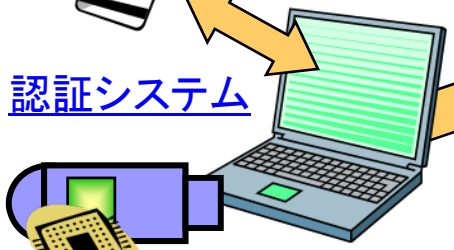
ICカード

暗号ルータ・
認証サーバ



暗号化ファイル
保管システム

認証システム



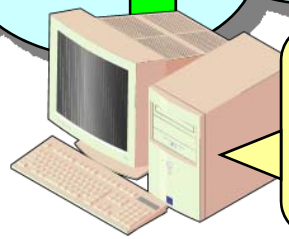
暗号通信路
インターネットサービス

持出可般媒体保護

携帯電話

低消費電力や低コスト生産ができる高効率小型ハードウェア実装
約8KG, 約200Mbps (0.18μm ASIC)
約2Kslice, 約250Mbps (FPGA)
（鍵長128ビット専用）

ハードウェア



HDTV級動画の暗号処理もできる高速ソフトウェア実装
約1Gbps (@Pentium 4, 3.2GHz)
（鍵長128ビット、アセンブラ）

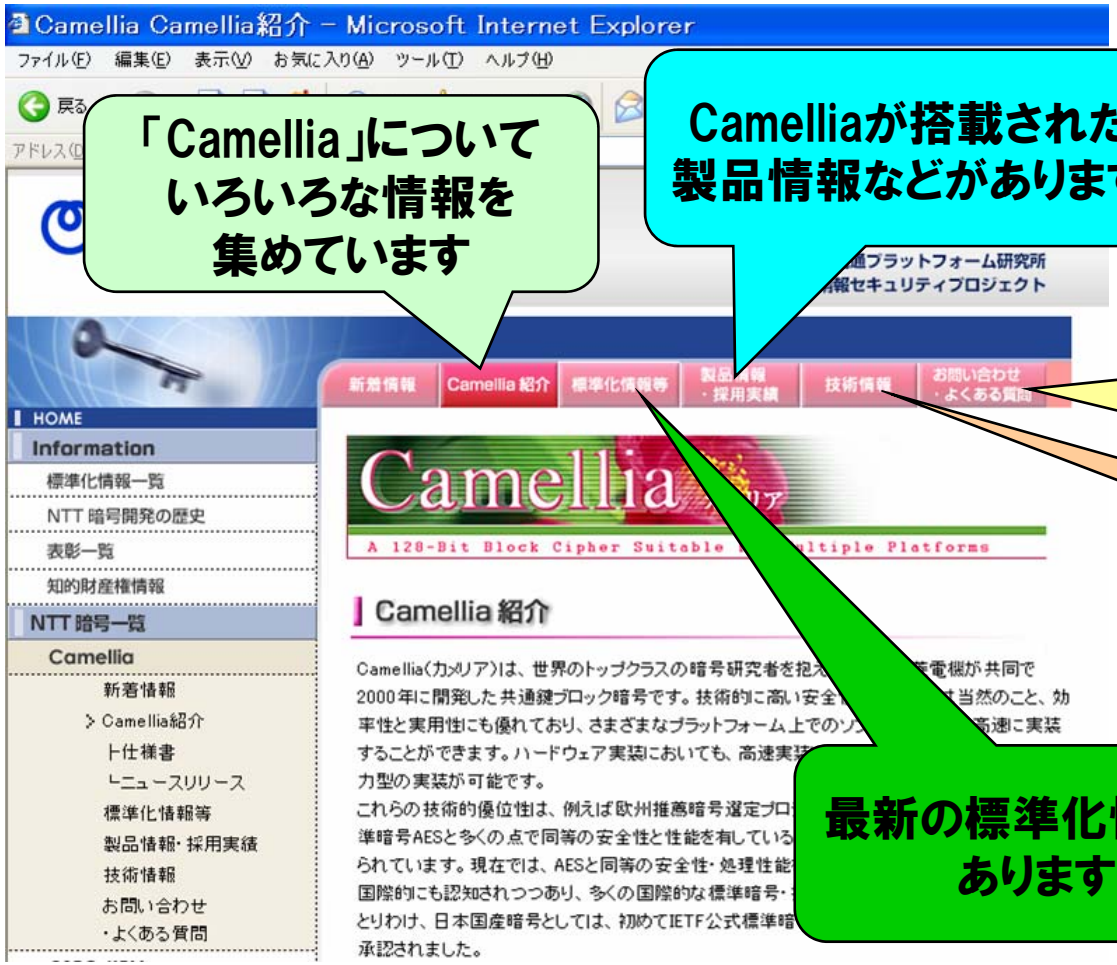
電子会議システム・DRMシステム

暗号ライブラリ

※性能値はトップデータです。実際の製品・システムでは性能が変わります。

Camelliaホームページ

http://info.isl.ntt.co.jp/crypt/camellia/index.html



「Camellia」について
いろいろな情報を
集めています

Camelliaが搭載された
製品情報などがあります

Camelliaに関する
問合せ先情報が
あります

Camelliaのオープン
ソースなどがあります

最新の標準化情報が
あります

最近のニュース記事等

- 08.06.17　Firefox 3リリース記者発表
  マイコミジャーナル、日経コミュニケーション、
  INTERNET Watch、ZDNet 等
- 07.10.23　テレビ東京・ワールドビジネスサテライト放映
  「深刻化　情報セキュリティー」
- 07. 9.16　Mozilla24イベント・インターネット中継講演
  「History of Camellia」
- 07. 9. 5　日経IT Pro記事
  「Firefox次期版がNTTと三菱電機の暗号化技術
  Camelliaを採用」
- 07. 9. 4　日経産業新聞1面特集記事
  「ネットNEXT 第2部インフラ変容」

技術詳細

Camelliaの仕様

- **AESインタフェース互換**
  - ブロック長 :128ビット
  - 鍵長 :128 / 192 / 256ビット
- **全体構造:**
  - 18段Feistel構造（128ビット鍵）
  - 24段Feistel構造（192/256ビット鍵）
    - 6段ごとに副変換部を挿入
- **構成要素:**
  - 段関数（F関数）: byte-oriented SPN構造
  - 副変換部: AND, OR, Rotation, XORで実現
  - 前処理・後処理: XOR
- **副鍵生成: 2段Feistel構造による中間鍵生成**
  - Rotation&choice方式による中間鍵と秘密鍵からの副鍵生成

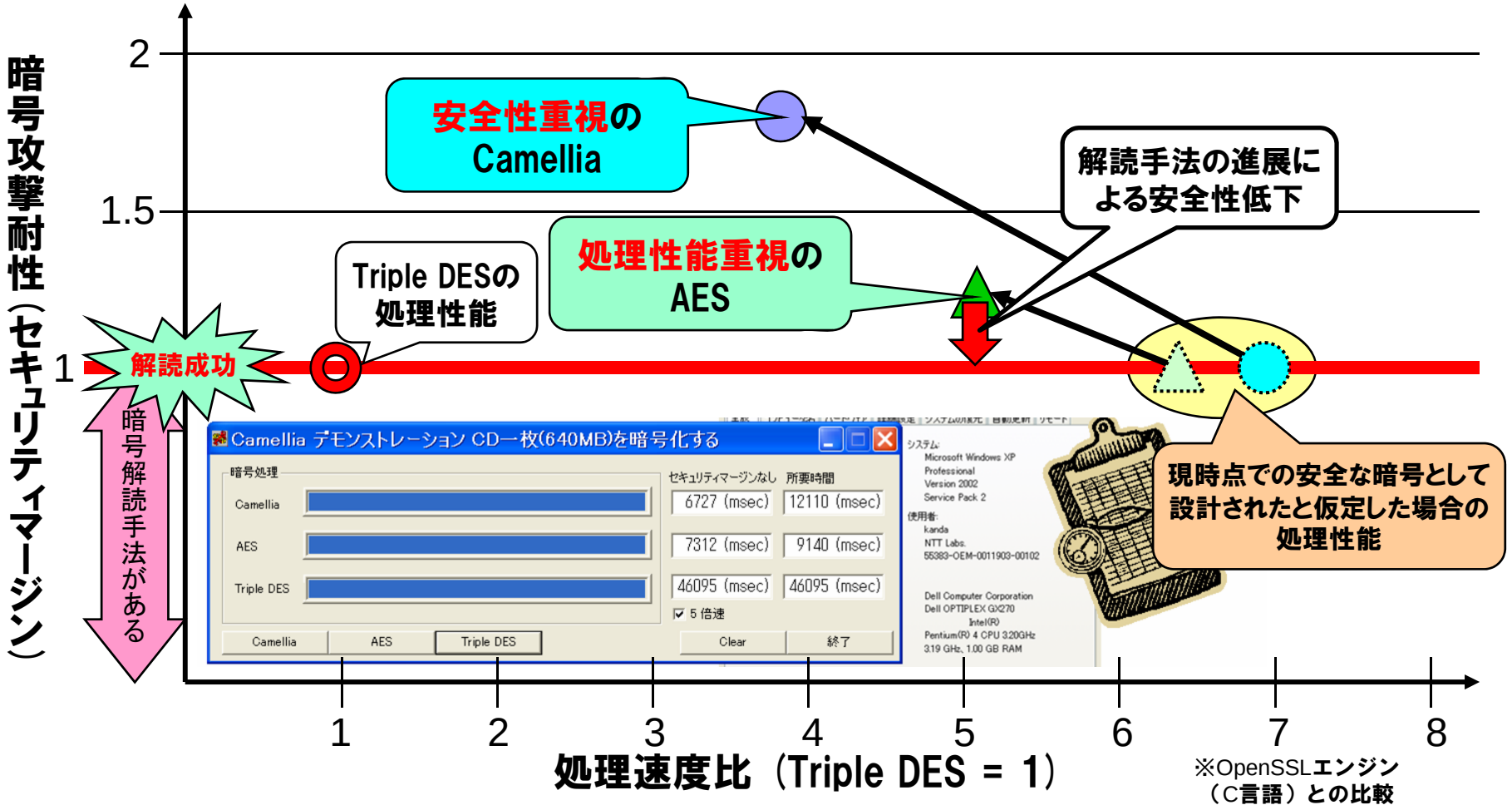
実装性能 ～ソフトウェア実装～

- 動画でも十分に対応可能なソフトウェア処理性能

プロセッサ	実装言語	処理速度(暗号化・復号とも同じ)			注釈
		鍵長128ビット	鍵長192ビット	鍵長256ビット	
Core2 Duo E8400	ANSI C	505 cycles (801Mbps@3.16GHz)	655 cycles (618Mbps@3.16GHz)	655 cycles (618Mbps@3.16GHz)	ホームページ掲載のオープンソース (Fedora)
	Java	698 cycles (580Mbps@3.16GHz)	869 cycles (466Mbps@3.16GHz)	869 cycles (466Mbps@3.16GHz)	
AMD Phenom 9850	ANSI C	470 cycles (683Mbps@2.5GHz)	610 cycles (526Mbps@2.5GHz)	603 cycles (532Mbps@2.5GHz)	ホームページ掲載のオープンソース (FreeBSD)
Pentium 4	アセンブラ	361cycles (1.1Gbps@3.2GHz)	N/A	N/A	SCIS 2006 2C3論文 (WinXP, Hyper-threading off)
	C言語	900 cycles (455Mbps@3.2GHz)	1168 cycles (351Mbps@3.2GHz)	1165 cycles (352Mbps@3.2GHz)	旧オープンソース (WinXP, Hyper-threading off)
		1008 cycles (216Mbps@1.7GHz)	1376 cycles (158Mbps@1.7GHz)	1376 cycles (158Mbps@1.7GHz)	NESSIE報告書 D21 (Linux)
	Java	1552 cycles (264Mbps@3.2GHz)	N/A	N/A	旧オープンソース (WinXP, Hyper-threading off)
Athlon64 3500+	アセンブラ	175 cycles (1.6Gbps@2.2GHz)	N/A	N/A	2ブロック並行暗号化 (WinXP, Hyper-threading on)
		243 cycles (1.2Gbps@2.2GHz)	N/A	N/A	ビットスライス暗号化 (WinXP, Hyper-threading on)
Pentium III	アセンブラ	326 cycles (255Mbps@650MHz)	N/A	N/A	CRYPTREC報告書 (Win98 SE)

Camelliaの特徴 ～安全性と処理性能の両立～

- 世界最高水準の暗号攻撃耐性と高速処理を両立

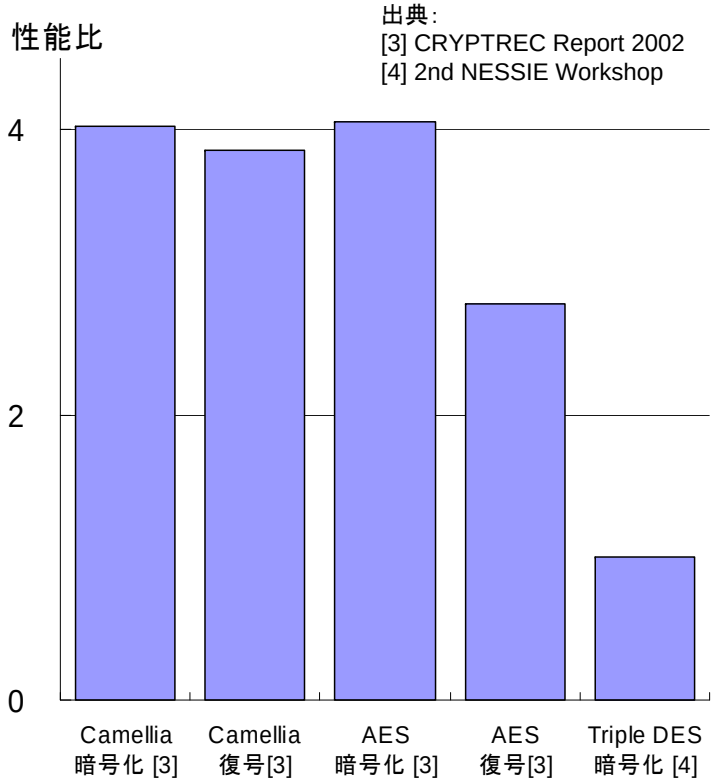


実装性能比較 ～ICカードソフトウェア実装～

- ICカードなど搭載メモリが少ない環境でも高速な実装
  - 世界最高クラスの実装性能
  - 暗号化と復号で処理速度がほぼ同じ

プロセッサ	RAM [bytes]	ROM [bytes]	暗号化 [cycles]	鍵生成 [cycles]
Z80	63	1,698	28,382 (5.68 msec)	5,146 (1.03 msec)
	60	1,268	(暗号化) 35,951 (7.19 msec) (復号) 37,553 (7.51 msec)	
8051	32	990	10,217 (10.22 msec)	
H8/3113	---	---	4,100 (1.64 msec)	2,380 (0.95 msec)
AE45X	60	---	(暗号化) 8,136 (1.11 msec) (復号) 8,658 (1.18 msec)	
SLE66 CLX320P	248	1,279	17,920 (2.64 msec)	6,144 (0.91 msec)
	58	1,311	(暗号化) 24,064 (3.55 msec) (復号) 24,576 (3.62 msec)	
M32Rx/D	44	8,684	1,236 (12.36 msec)	642 (6.42 msec)

出典:
[3] CRYPTREC Report 2002
[4] 2nd NESSIE Workshop



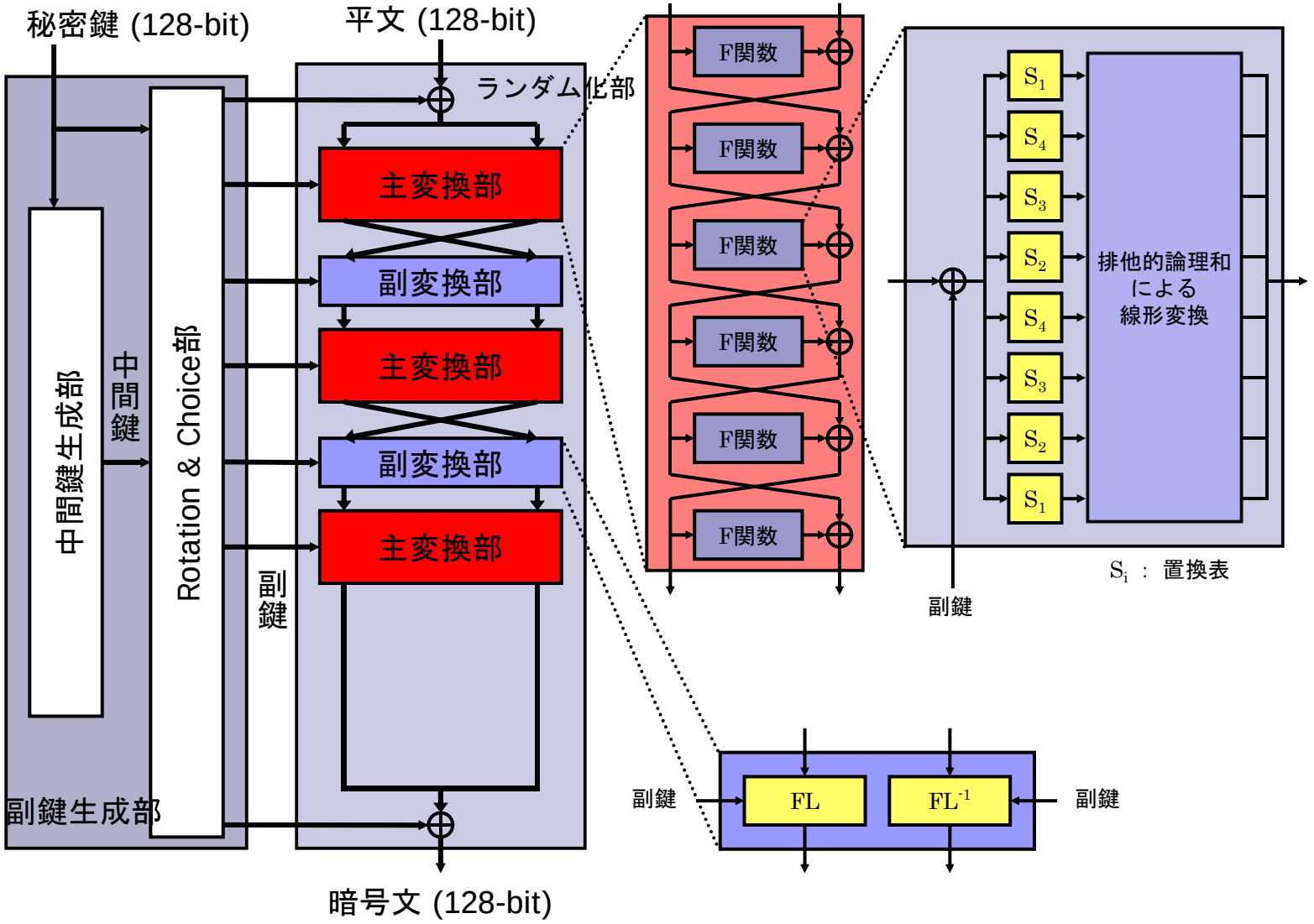
実装性能 ～ハードウェア実装～

- **世界最小クラス(回路規模)かつ世界最高水準性能**
  - 10KG以下の回路規模でも高速な処理を実現

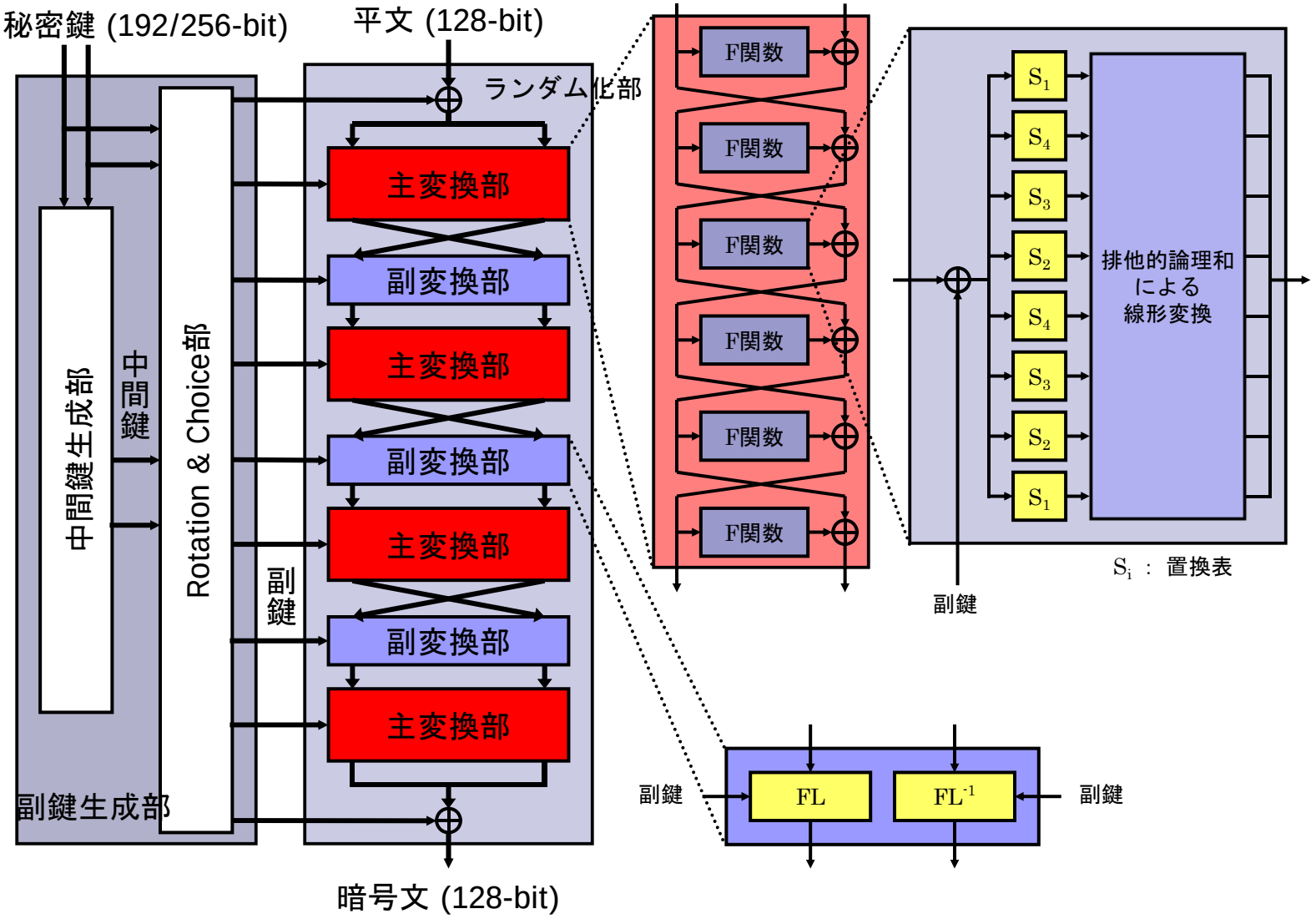
(128ビット鍵)

種類	ライブラリ	処理速度	回路規模	処理効率
ASIC	MELCO 0.18 μm	1,881.3 Mbps	44.3 KG	42.47
		1,050.9 Mbps	11.9 KG	88.52
		177.7 Mbps	8.1 KG	21.87
		71.5 Mbps	6.4 KG	11.23
	商用製品	71 Mbps	6.4 KG	11.09
	IBM 0.13 μm	2,154.9 Mbps	29.8 KG	72.31
		1,907.6 Mbps	20.8 KG	91.76
		325.8 Mbps	6.5 KG	50.12
	IBM 0.18 μm	567.3 Mbps	9.1 KG	62.34
		204.6 Mbps	6.3 KG	32.66
FPGA	Xilinx VertexE	401.9 Mbps	9,426 slices	42.64
		227.4 Mbps	1,780 slices	127.76
	(Pipeline実装)	6,750 Mbps	9,692 slices	---
	Xilinx Vertex3200E	369.0 Mbps	8,957 slices	42.14
		223.7 Mbps	1,678 slices	133.31
	(Pipeline実装)	25,440 Mbps	19,482 slices	---

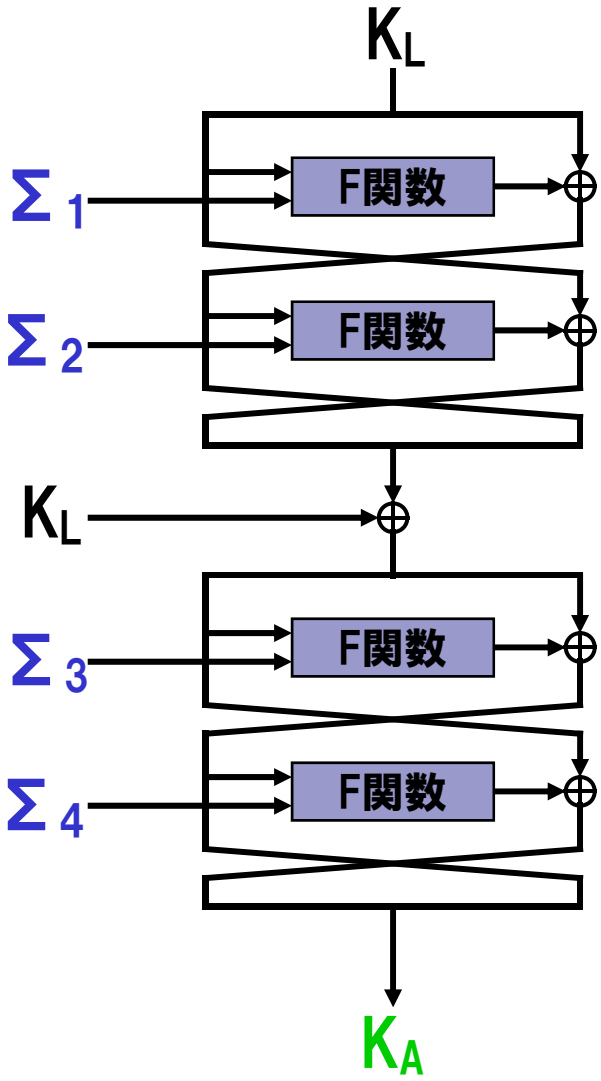
Camelliaの略図(128ビット鍵長)



Camelliaの略図(192/256ビット鍵長)



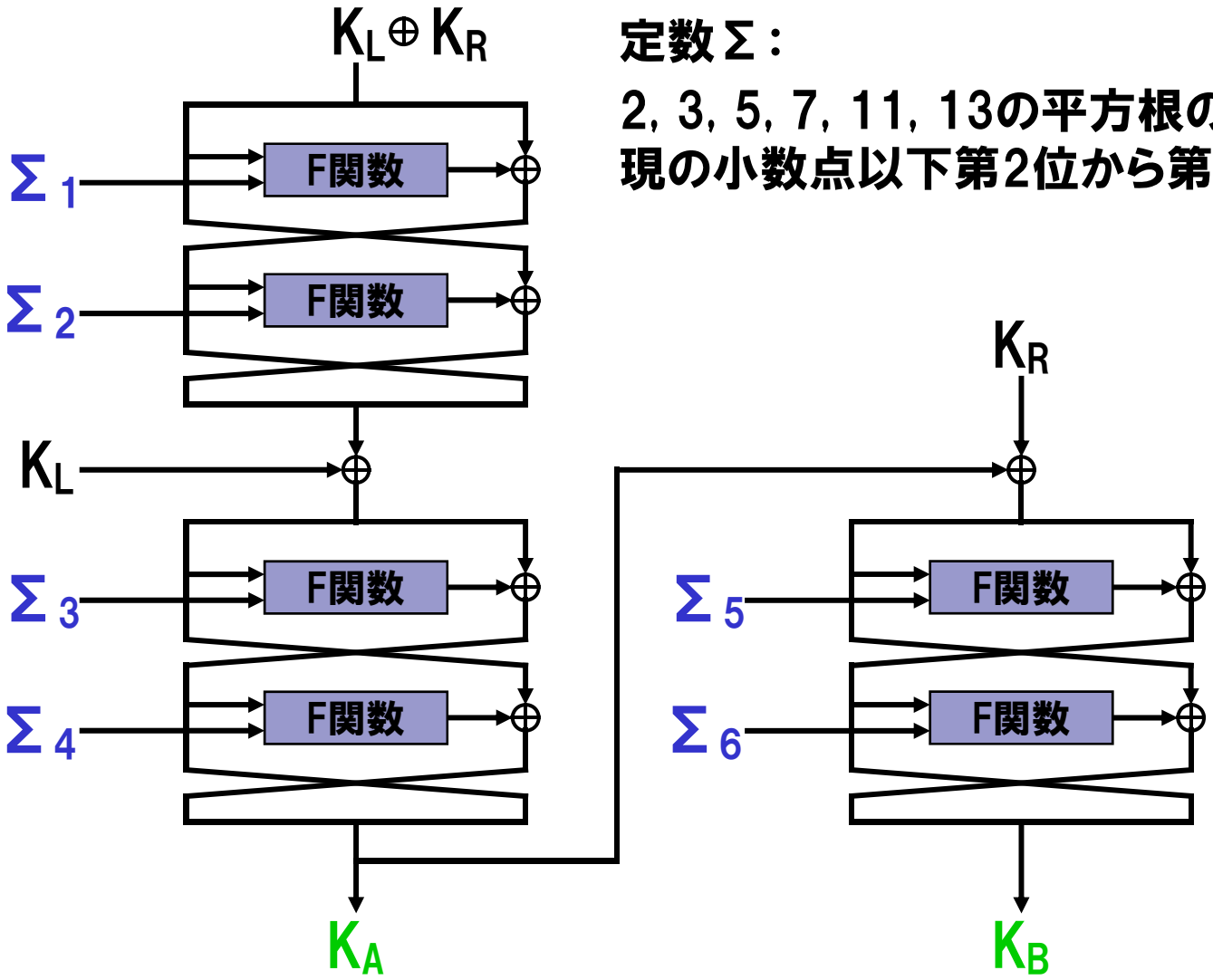
中間鍵生成部の略図(128ビット鍵長)



定数Σ:

2, 3, 5, 7の平方根の16進数表現の小数点以下第2位から第17位

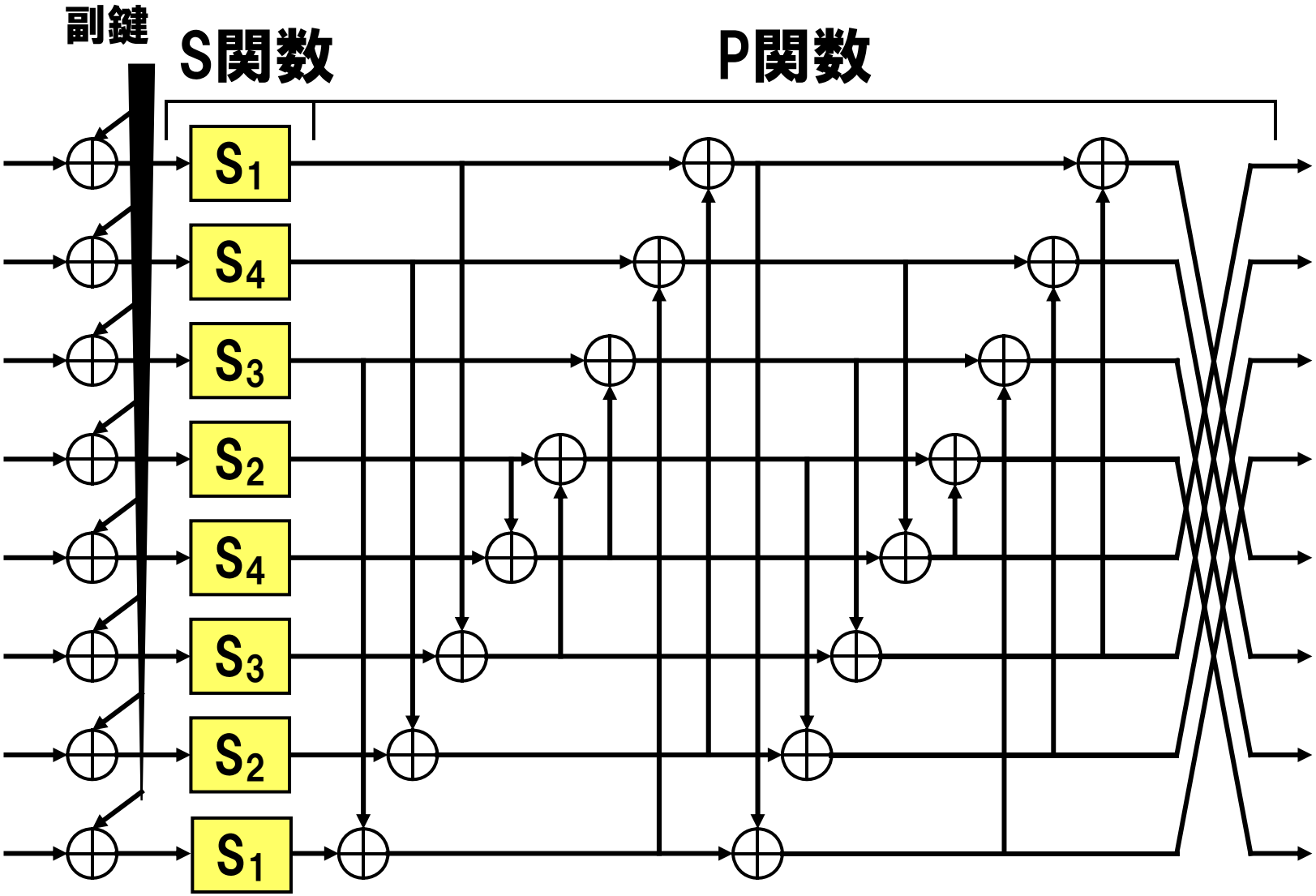
中間鍵生成部の略図(192/256ビット鍵長)



定数Σ:

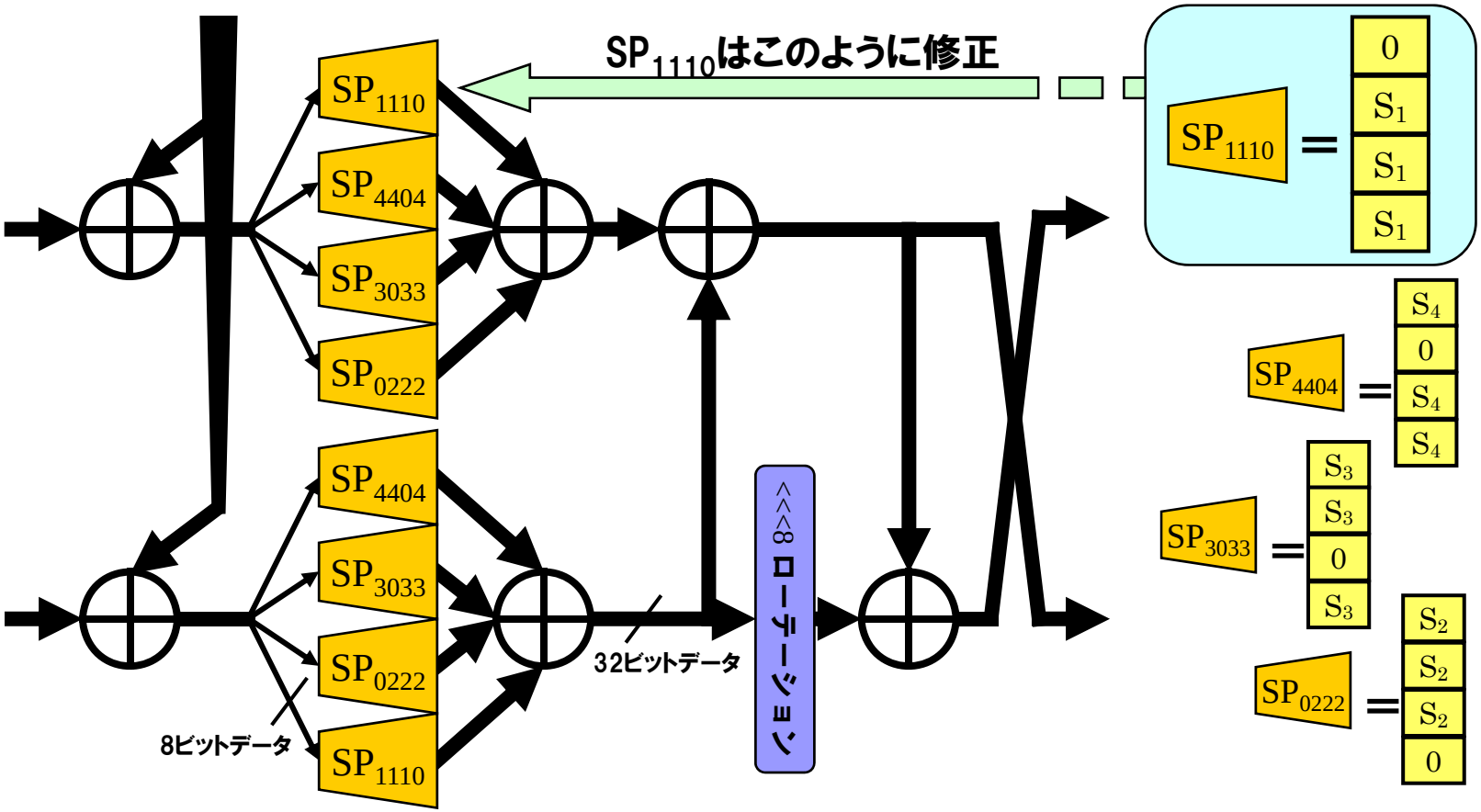
2, 3, 5, 7, 11, 13の平方根の16進数表現の小数点以下第2位から第17位

段関数(F関数)の詳細図



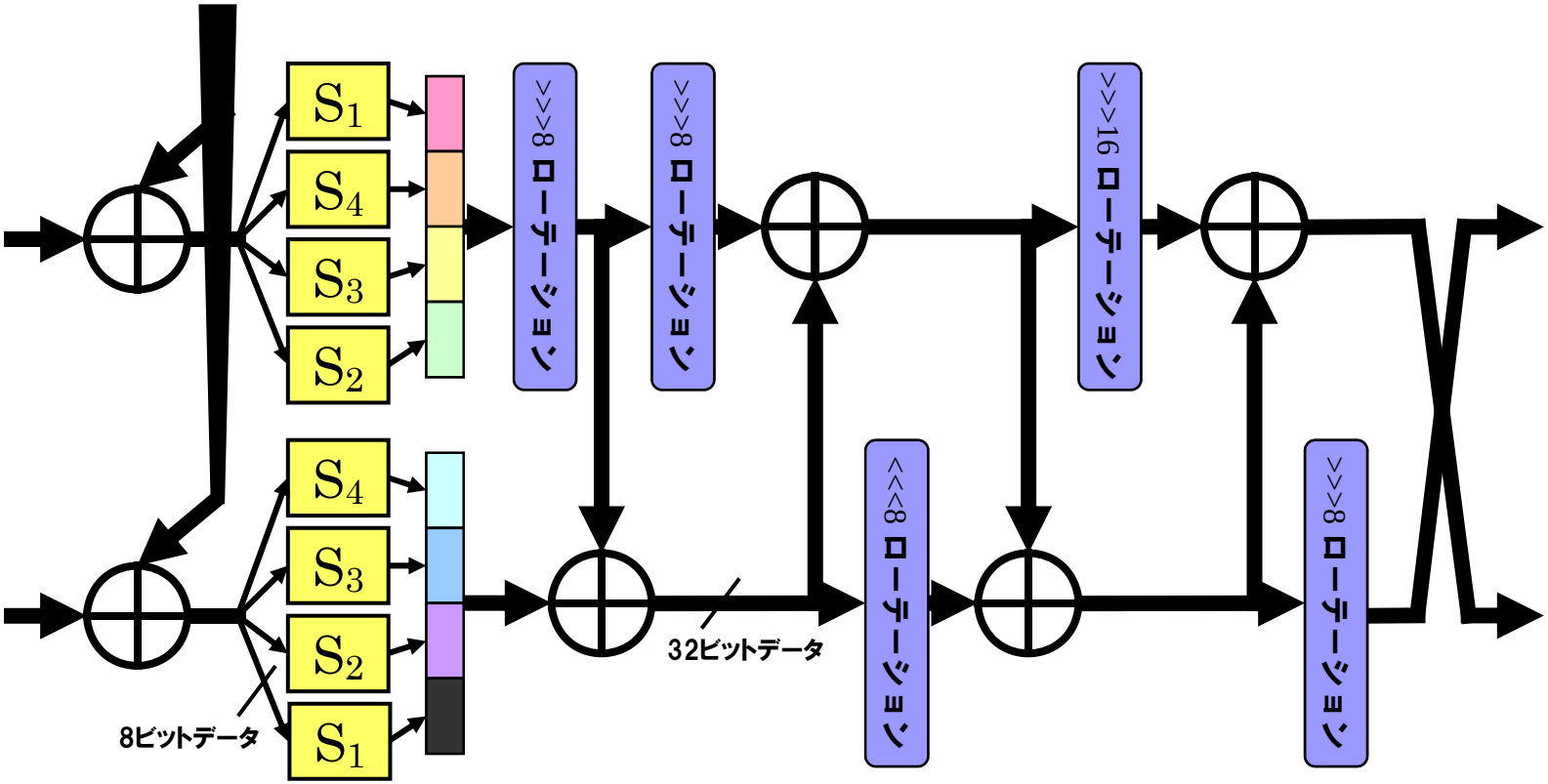
代表的なCamellia高速化手法 for 32-bit CPU

- Sboxを大きなテーブルに修正した等価段関数
  - 4KB以上の1次キャッシュをもつCPUに対して非常に効果的



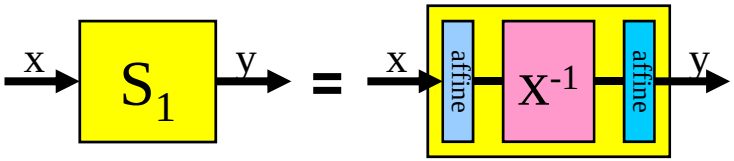
代表的なCamellia高速化手法 for メモリレス型

- Sboxを修正せずに16/32ビット変数を使用する等価段関数
  - 搭載メモリ量が少ないICカードや組込系CPUに対して効果的

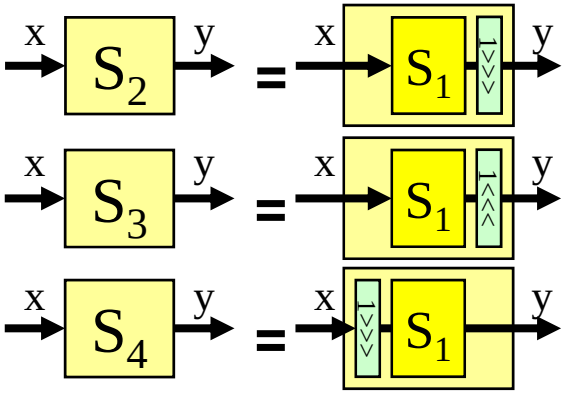


代表的なCamellia実装手法 for 使用メモリ削減

- **Sboxサイズの削減**
  - 搭載ROMが非常に少ないICカードや組込系CPU、小型ハードウェアに対して効果的

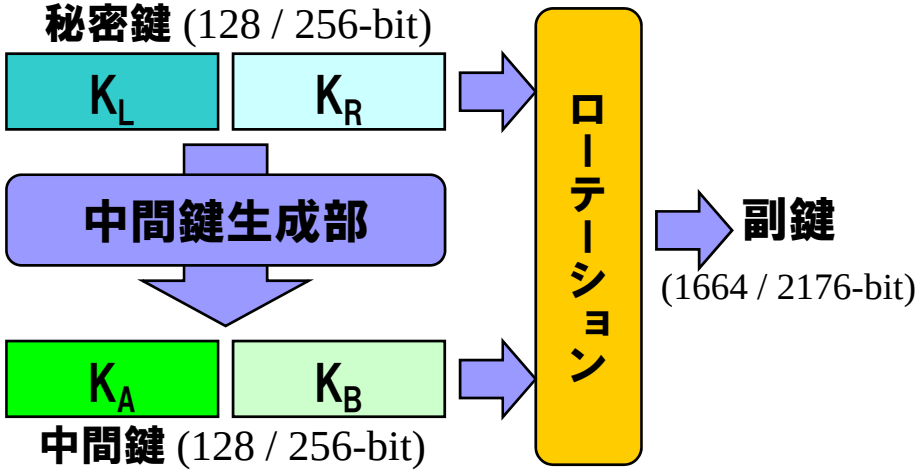


S_1はアフィン変換と逆元算で構成
（逆元算回路でS_1の計算可能）



S_2, S_3, S_4は S_1とローテーションで構成
（S_1から他のSboxは計算可能）

- **副鍵展開領域の削減**
  - 搭載RAMが非常に少ないICカードや組込系CPU、小型ハードウェアに対して効果的



副鍵を全展開しておかなくても、秘密鍵と中間鍵を保持しておけば、ローテーション処理だけで副鍵が生成可能
さらに、鍵長128ビット限定ならば K_R と K_B も保持不要

安全性評価のまとめ

- 18段中最大9段（128ビット鍵）／24段中最大11段（256ビット鍵）までしか理論的攻撃が成功していない

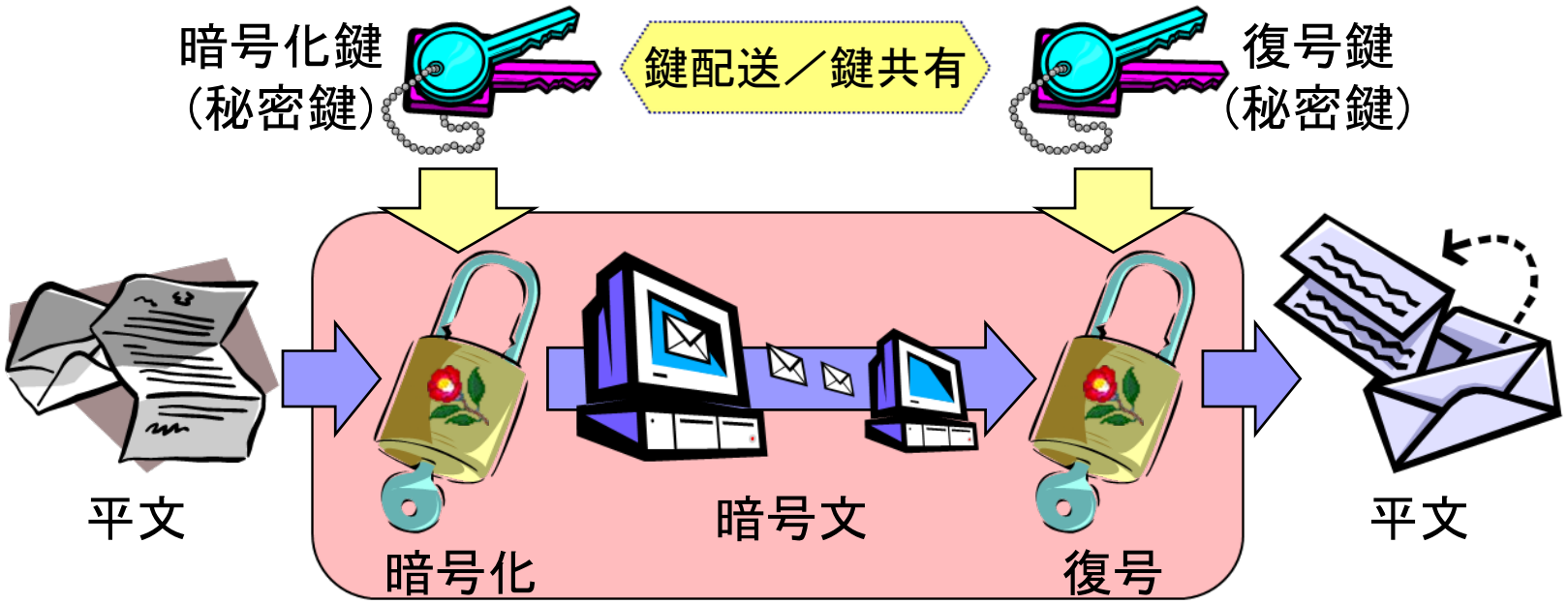
攻撃可能段数		5	6	7	8	9	10	11	12	13	14	15
128ビット鍵利用	副変換部なし	ISA: $2^{10.6}$ ICA: $2^{5.8}$	ISA: 2^{18} VSA: $2^{18.6}$ ICA: $2^{11.5}$ HDC: 2^{18}	ISA: 2^{58} VSA: $2^{33.5}$ ICA: $2^{54.7}$ HDC: 2^{57} TDC: 192	VSA: $2^{74.6}$ ICA: $2^{94.9}$ HDC: 2^{120} TDC: $2^{55.6}$	VSA: $2^{86.9}$ ICA: $2^{119.4}$		IDC: 2^{126}	Unknown attacks	Unknown attacks	Unknown attacks	Unknown attacks
	副変換部有			ISA: $2^{58.6}$ VSA: $2^{90.6}$	ISA: 2^{98} ICA: $2^{74.6}$	ISA: 2^{122}	Unknown attacks	Unknown attacks	Unknown attacks	Unknown attacks	Unknown attacks	Unknown attacks
256ビット鍵利用	副変換部なし	–	–	ISA: 2^{50} VSA: $2^{25.6}$ ICA: $2^{46.7}$	VSA: $2^{66.6}$ ICA: $2^{78.9}$	VSA: 2^{122} ICA: $2^{143.4}$ HDC: 2^{188}	VSA: 2^{186} ICA: $2^{207.4}$ HDC: 2^{252}	VSA: 2^{250}	(VSA: $2^{250.8}$)		IDC:$2^{232.5}$	Unknown attacks
	副変換部有			VSA: $2^{146.6}$	ISA: 2^{82} VSA: $2^{194.6}$ ICA: $2^{66.6}$	ISA: 2^{146}	ISA: 2^{210}	HDC:2^{256}	Unknown attacks	Unknown attacks	Unknown attacks	Unknown attacks

出典:
Duo Lei, Li Chao, and Keqin Feng, "New Observation on Camellia," SAC 2005, LNCS 3897
Guan Jie, and Zhang Zhongya, "Improved Collision Attack on Reduced Round Camellia," CANS 2006, LNCS 4301
Lei Duo, Chao Li, and Keqin Feng, "Square Like Attack on Camellia," ICICS 2007, LNCS 4861
Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman, "Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1," CT-RSA 2008, LNCS 4964

ISA: Improved Square Attack / VSA: Variant Square Attack
ICA: Improved Collision attack
IDC: Impossible Differential Cryptanalysis
HDC: Higher Order Differential Cryptanalysis
TDC: Truncated Differential Cryptanalysis

参考

共通鍵暗号

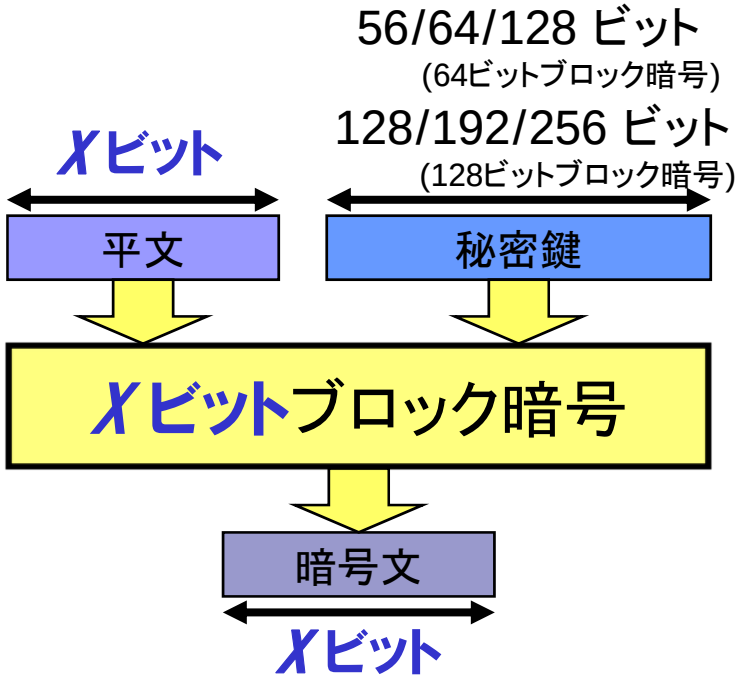


- **共通鍵暗号の特徴**
  - 暗号化・復号処理が高速（公開鍵暗号より1000倍以上高速）
    - 主にメッセージデータの暗号化・復号や高速認証に利用
  - 暗号化処理・復号処理において同一の秘密鍵を使用
    - (事前に)鍵配送／鍵共通が別途必要

ブロック暗号の将来について

- **現在主流の64ビットブロック暗号から安全性を高めた次世代の128ビットブロック暗号へ移行しつつある**
  - 平文のブロック長が異なる(鍵長の違いではない)
  - 1997年以前は64ビットブロック暗号、それ以降は128ビットブロック暗号が開発

米国政府	米国政府標準暗号をAESに一本化 DESは米国政府標準暗号から廃止 Triple DESは米国政府標準暗号から推奨暗号へ格下 2010年に 2-key Triple DES は廃止予定
NESSIE	64ビットブロック暗号を Normal-Legacy、128ビット(以上の)ブロック暗号を Normal と分類
CRYPTREC	新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128ビットブロック暗号を選択することが望ましい



次世代暗号の比較　#1

暗号名	Camellia	AES	SEED
開発元	NTT・三菱電機	NIST（米国商務省・国立標準技術研究所）	KISA（韓国情報保護振興院）
開発年	2000	1998 Rijnmen, Daemenが開発 2001 米国政府標準暗号認定	1998
政府規格	電子政府推奨暗号	米連邦情報処理標準規格（FIPS）	韓国情報通信標準規格（KICS）　など
	■「e-Japan重点計画」による総務省・経済産業省主管の実施施策の一環 ■ 12個の推奨暗号のひとつ	「連邦情報セキュリティ管理法（FISMA法）」および「大統領令」に基づく、米国連邦政府システムに対する唯一の暗号強制規格	「情報通信網利用促進および情報保護等に関する法律」などに基づく、政府機関に対する唯一の暗号強制規格
その他の規格	ISO/IEC国際標準暗号、欧州連合推奨暗号など	ISO/IEC国際標準暗号、欧州連合推奨暗号、無線LANなど	ISO/IEC国際標準暗号
現状	■ 官公庁向けシステムをはじめとするSE/SI案件で導入 ■ 三菱電機・NTTグループほかから市販製品を発売 ■ 国外では事実上日本を代表する暗号と認識	■ 金融機関における標準仕様としても採用 ■ 事実上の次期デファクト暗号として様々な標準化や製品供給が進展	■ 韓国内の金融機関での標準仕様としても採用 ■ 690以上の韓国企業、大学、研究所で利用 ■ 韓国内におけるSEEDとAESの両立が促進

次世代暗号の比較　#2

暗号名	Camellia	AES	SEED
鍵長	128/192/256 ビット	128/192/256 ビット	128 ビット
セキュリティマージン	1.8 – 2.0	1.25 – 1.4	（2.0以下）
構造	Feistel構造	SPN構造	Feistel構造
適用領域	◎ ICカード、小型ハードウェア ○ ソフトウェア	◎ ソフトウェア ○ ICカード、高速ハードウェア	○ ソフトウェア、高機能ICカード × ハードウェア、低機能ICカード
技術的論点	■ 安全性がほぼ正確に見積もり ■ セキュリティマージンは大きい	■ 安全性がほぼ正確に見積もり ■ セキュリティマージンはやや小さい	■ 鍵長が128ビットしか使えない ■ 32ビット算術演算を利用しているため、正確な安全性評価ができているわけではない
	■ 論理演算とテーブル参照（逆元回路で代用可）を利用	■ 論理演算とテーブル参照（逆元回路で代用可）を利用	■ テーブル参照と32ビット算術演算を併用
	■ どのプラットフォームでも効率的な実装可能 ■ 暗号化と復号の処理が共用でき、かつ算術演算を使用しないので、特にICカードや小型ハードウェア実装に有利	■ どのプラットフォームでも効率的な実装可能 ■ 処理並列性が高いので、様々な高速化手法を組込むことが可能	■ PC上でのソフトウェア処理では高速 ■ 低機能ICカードやハードウェア実装には適さない
	■ 暗号化と復号の処理が共用できるので暗号化と復号とで処理速度が大きく異なることはない	■ 暗号化と復号の処理が基本的に異なるので、両方の実装が必要 ■ 原理的に復号処理のほうが暗号化処理よりも負荷が大きいので、ICカード上などでは暗号化と復号とで処理速度が大きく異なる場合がある	■ 暗号化と復号の処理が共用できるので、暗号化と復号とで処理速度が大きく異なることはない

標準化動向 #1

- **AESプロジェクト（1997.1 – 2000.10）**

  Advanced Encryption Standard

  - DES/Triple DESに替わる新米国政府標準暗号選定プロジェクト
  - 米国商務省・国立標準技術研究所（NIST）が実施
  - 15件の公認応募暗号（応募自体は21件）から、2段階の評価選抜を経て「Rijndael」を選抜
  - 米国政府標準暗号 FIPS 197 として制定
- **NESSIEプロジェクト（2000.1 – 2003.3）**

  New European Schemes for Signature, Integrity, and Encryption

  - 暗号に関する欧州の産業力向上などを目的とした、強力な欧州連合推奨暗号選定プロジェクト
  - 欧州連合傘下の欧州委員会が策定する情報社会プログラム第5次R&D計画の一環として実施
  - ブロック暗号では、17件の応募暗号から2段階の評価選抜を経て3件（MISTY1, Camellia, SHACAL-2）を選抜。AESを加えた4件を選定

標準化動向 #2

- **CRYPTRECプロジェクト（2000.5 – 2003.3）**

  Cryptography Research and Evaluation Committees
  - 電子政府用調達暗号の推奨リスト作成プロジェクト
  - 総務省・経済産業省（事務局:IPA, NICT）が主体となり実施
  - ブロック暗号では、11件の応募暗号から10年以上は安全に利用できると判断された7件に加え、Triple DESとAESを合わせた9件を推奨リストに掲載
- **ISO/IEC 18033-3（1999.12 – 2005.5）**
  - 初めてのISO/IEC国際標準暗号策定作業

    cf. ISO/IEC 9979 暗号登録制度は廃止
  - 次世代ブロック暗号としては Camellia, AES, SEED のみを選定
- **IETF**

  Internet Engineering Task Force
  - インターネットでの事実上の標準規格を策定する国際的な団体
  - 次世代秘匿用インターネット標準暗号としては、AES, Camellia, SEEDのみを選定

共通鍵暗号標準化の現状

		開発国	ISO/IEC国際標準暗号（◎）	RSA PKCS#11（◎）	インターネット標準暗号（◎）				政府系標準暗号（◎）・推奨暗号（○）				
					SSL/TLS	IPsec	S/MIME	XML	米国政府 FIPS/SP	欧州連合 NESSIE	日本政府 CRYPTREC	韓国政府	カナダ政府
128ビットブロック暗号	Camellia	日本	◎	◎	◎	◎	◎	◎	—	○	○	—	—
	AES	米国	◎	◎	◎	◎	◎	◎	◎	○	○	—	◎
	SEED	韓国	◎	—	◎	◎	◎	—	—	—	—	◎	—
	CIPHERUNICORN-A	日本	—	—	—	—	—	—	—	—	○	—	—
	Hierocrypt-3	日本	—	—	—	—	—	—	—	—	○	—	—
	SC2000	日本	—	—	—	—	—	—	—	—	○	—	—
移行推奨	Triple DES	米国	◎	◎	◎	◎	◎	◎	○	—	○（条件付）	—	◎
64ビットブロック暗号	CAST-128	カナダ	◎	◎	—	◎	◎	—	—	—	—	—	◎
	MISTY1	日本	◎	—	—	—	—	—	—	○	○	—	—
	Blowfish	米国	—	◎	—	◎	—	—	—	—	—	—	—
	IDEA	スイス	—	◎	◎	◎	◎	—	—	—	—	—	—
	RC2	米国	—	◎	◎	—	◎	—	—	—	—	—	—
	RC5	米国	—	◎	—	◎	◎	—	—	—	—	—	—
	CIPHERUNICORN-E	日本	—	—	—	—	—	—	—	—	○	—	—
	Hierocrypt-L1	日本	—	—	—	—	—	—	—	—	○	—	—
ストリーム暗号	RC4	米国	—	◎	◎	—	—	◎	—	—	○（条件付）	—	—
	MUGI	日本	◎	—	—	—	—	—	—	—	○	—	—
	SNOW	スウェーデン	◎	—	—	—	—	—	—	—	—	—	—
	MULTI-S01	日本	（モード）	—	—	—	—	—	—	—	○	—	—