International Standard Encryption Algorithm from Japan "Camellia"

NTT Information Sharing Platform Laboratories

Camellia website
http://info.isl.ntt.co.jp/crypt/eng/camellia/
E-mail: camellia@lab.ntt.co.jp

Why needs Camellia?

Camellia is the only international standard cipher
that is an alternative to the US standard cipher AES

- All information systems depending only on a single cipher (i.e. AES) seem to be unstable and risky
  - Alternative choice should be prepared because of the risk hedging
- Easy use as well as AES
  - Same Interface
  - Royalty-free license
  - Already adopted to various standardizations
  - Already loaded with various open source software

Features of Camellia

Camellia -

- **128-bit block cipher (allowing key sizes of 128, 192, and 256 bits)**, jointly developed in 2000 by NTT & Mitsubishi
  - Win-win collaboration on cryptography in Japan
- **World's highest security and efficiency** – technically comparable to AES
  - Many evaluations in the cryptographic community have published
- **Adopted as international standard** specification and recommended specification for the coming encryption algorithms
  - AES, Camellia, and SEED are only ciphers selected as the future ISO/IEC standard ciphers
  - Already adopted in IETF (TLS, IPsec, S/MIME, OpenPGP, XML) and RSA PKCS#11, etc.

Features of Camellia (Cont.)

- **Camellia essential patents can be used at no charge** by any Camellia user without concluding such royalty-free licensing agreement

  http://info.isl.ntt.co.jp/crypt/eng/info/chiteki.html
- NTT publishes **NTT's open source codes of Camellia free of charge through multiple open source software licenses (GPL, LGPL, BSD, MPL, and OpenSSL)**

  http://info.isl.ntt.co.jp/crypt/eng/camellia/source.html
- NTT **contributes to major open source communities**
  - Some major open source communities, e.g., Mozilla, OpenSSL, Linux, FreeBSD and Kerberos, have already supported Camellia into their open source software
- NTT **joined in Kerberos Consortium** as an executive advisory board member

Supported Open Source Software

Major OSS communities loaded Camellia to their tools/kernels as the first Japanese cipher

Open Source & Information by NTT
i. C-language code (GPL, LGPL, BSD, OpenSSL, MPL)
ii. Java code (GPL, BSD)
iii. Ruby Camellia package
iv. Guidance & Instructions (in Japanese)

OS Kernel	i. FreeBSD 6.4 (or later)/7.0 (or later)
	ii. Linux kernel 2.6.21 (or later)
	iii. Fedora Core 7 (or later)

Application	i. Firefox 3.0 (or later)
	ii. ipsec-tools 0.7 (or later)
	iii. GnuPG 2.0 (or later)
	iV. Kerberos KRB5 1.9 (or later)

Toolkit	i. OpenSSL toolkit 0.9.8c (or later) Notes: the option “enable-camellia” is needed when openssl-0.9.8x is built.
	ii. NSS (Network Security Services) 3.12 (or later)
	iii. Crypto++ library 5.4 (or later)
	iv. The Legion of the Bouncy Castle 1.30 (or later)
	v. GNU Transport Layer Security Library 2.20 (or later)

Third party codes	i. Camellia for Open Souce Softwares
	ii. Camellia for Python
	iii. Perl Camellia encryption module
	iv. openCrypto.NET
	v. Pascal source by Wolfgang Ehrhardt

SSL/TLS by Camellia

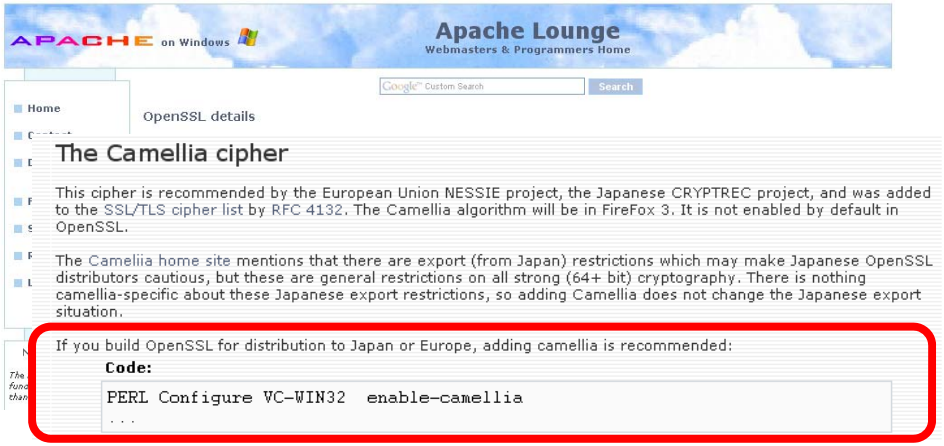
WWW Server
(Ex: EC site)

SSL/TLS by Camellia

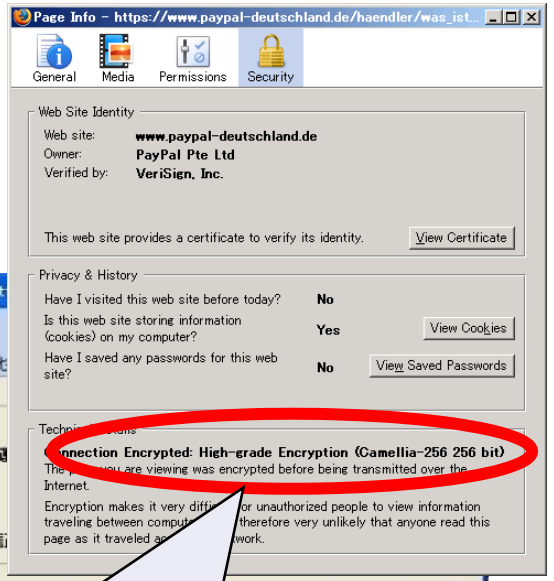
WWW Browser
(Ex: Customer)

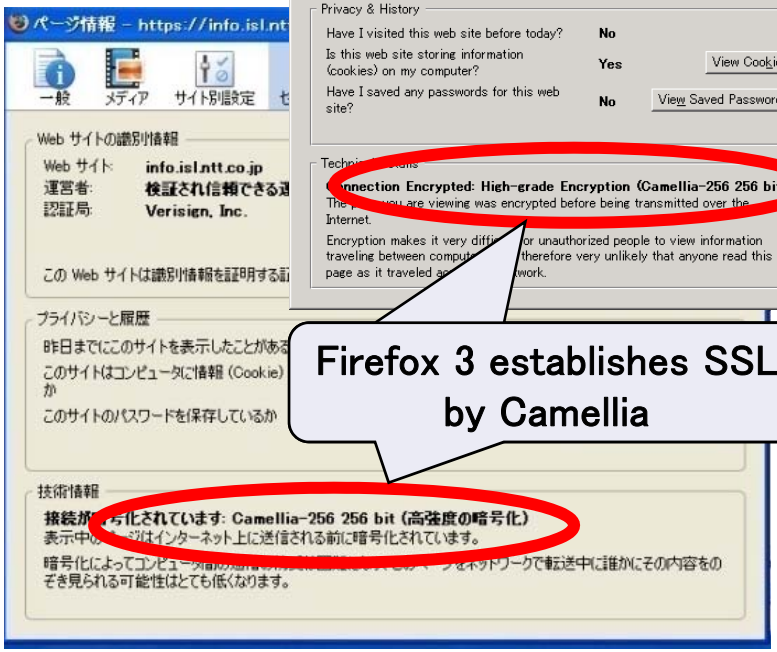
Camellia Sever:
Apache+OpenSSL

Browser: Firefox 3



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





Firefox 3 establishes SSL by Camellia

Notes: Camellia is already available by default in the bundled OpenSSL in the later OS kernels

Fedora Core 9 (or later), OpenSUSE 10.3 (or later), Gentoo Linux 2008.0 (or later), FreeBSD 7.0 (or later), FreeBSD ports 2007/6/12 (or later)

Standardization of Symmetric Ciphers

Camellia is internationally recognized as representative of Japanese ciphers

Notes: "X" mark means "selected"

		Nationality	ISO/IEC standard ciphers [ISO/IEC18033]	RSA PKCS#1	IETF standard ciphers				Government-related standard ciphers / recommended ciphers				
					SSL/TLS	IPsec	S/MIME	XML	US standard (FIPS/SP)	European Union recommended (NESSIE)	Japan recommended (CRYPTREC)	Korean standard	Canadian standard
128-bit block ciphers	**Camellia**	**Japan**	X	X	X [RFC4132]	X [RFC4312]	X [RFC3657]	X [RFC4051]	--	X	X	--	--
	AES	**USA**	X	X	X	X	X	X	X	X	X	--	X
	SEED	**Korea**	X	--	X	X	X	--	--	--	--	X	--
64-bit block ciphers	Triple DES	USA	X	X	X	X	X	X	X (Recommended)	--	X (Conditional)	--	X
	CAST-128	Canada	X	X	--	X	X	--	--	--	--	--	X
	MISTY1	Japan	X	--	--	--	--	--	--	X	X	--	--
	Blowfish	USA	--	X	--	--	--	--	--	--	--	--	--
	IDEA	Swiss	--	X	X	X	X	--	--	--	--	--	--
	RC2	USA	--	X	X	--	X	--	--	--	--	--	--
	RC5	USA	--	X	--	X	X	--	--	--	--	--	--
Stream ciphers	RC4	USA	--	X	X	--	--	X	--	--	X (Conditional)	--	--
	MUGI	Japan	X	--	--	--	--	--	--	--	X	--	--
	SNOW	Sweden	X	--	--	--	--	--	--	--	--	--	--

Transition

Users & Products equipped with Camellia

Welcome to use Camellia into any products !!

- Users

  Japanese government systems, Financial services, Online Game (eg. Capcom), SNS services (eg. mixi), Network services, Manufacturing systems, Universities, etc.

- Supported Venders

  More than 60 companies adopt Camellia into their products

NTT Software	CipherCraft/Mail, CipherCraft/VPN, CipherCraft/File, etc
NTT Electronics	Camellia LSI, IP Super-Compact MPEG-2 Codec, etc
NTT-AT	Smart Leak Protect, File Lock II, etc
Mitsubishi Electric	Cryptopia, MistyGuard(R)<CRYPTOFILE(R) PLUS>, etc
Renesas Technology	SH7781 MPU and MCU/SuperH RISC engine Family
AuthenTec (prev. SafeNet)	QuickSec Toolkit
THALES (prev. nCipher)	netHSM, nShield series, miniHSM
IAIK	IAIK-JCE, iSaSiLk, CMS-S/MIME, IAIK-XSECT
Bloombase	Spitfire Ethernet Encryptor, Spitfire StoreSafe, Spitfire Messaging, etc.

Security

Camellia achieves world's highest security level against state-of-the-art attacks and future unknown attacks

- **Published design rationale and self-evaluations**
  - Camellia is practically secure against known strong attacks, e.g. differential and linear cryptanalysis
- **No vulnerabilities against state-of-the-art attacks**
  - NO attacks are found against Camellia with any size of keys by the world's top-class researchers

  [FYI] In 2009, AES-192/256 can be theoretically broken using related-key attack proposed by Alex Biryukov, et al.
- **World's top-class resistant security (security margin)** against unknown attacks in the future

(2009.9 at the present time)

Breakable rounds	7	8	9	10	11	12	13	14	15	Original
128-bit keys	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	Unknown attacks up to *18 rounds*
256-bit keys	VSA: $2^{146.6}$	ISA: 2^{82} VSA: $2^{194.6}$ ICA: $2^{66.6}$	ISA: 2^{146}	Best known attack	HDC: 2^{256}	Unknown attacks	Unknown attacks	Unknown attacks	Unknown attacks	Unknown attacks up to *24 rounds*

Performance and Flexibility

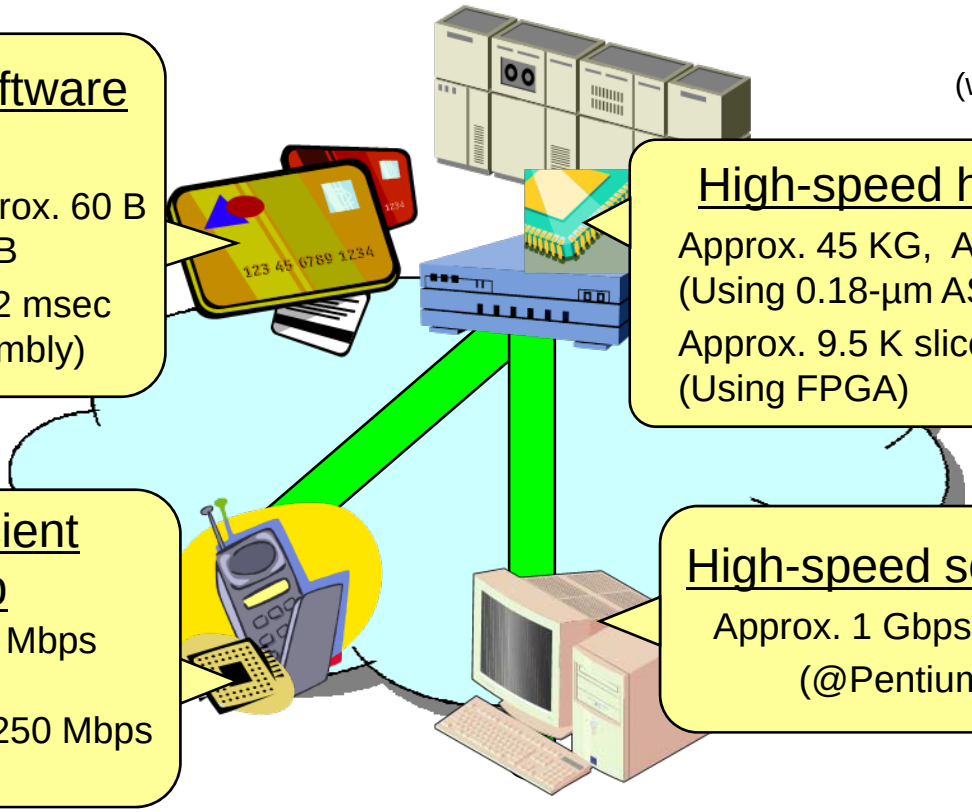
Camellia is extremely flexible and highly efficient according to circumstances

- Camellia possesses **high-speed software that is platform independent** such as PCs or smart cards
  - For PCs: Performance is achieved by using many registers, pre-computed large tables and powerful instruction sets
  - For smart cards: Containment of memory usage is achieved using small tables and on-the-fly subkey generation
- **World's smallest hardware implementation with world top-class efficiency**
  - Substitution tables are implemented using an inversion function over GF(2^8)
  - Encryption and decryption circuits can be shared since these procedures are identical except for the order of subkey insertion

Performance and Flexibility (Cont.)

- Performance of Camellia is **comparable to that of AES on any platform**
  - No disadvantage in terms of efficiency

(when using 128-bit key)



High performance software for smart cards

Memory usage of RAM: Approx. 60 B
ROM: Approx. 1.5 KB

Processing time: Approx. 2 msec (@15 MHz) (Using Assembly)

High-speed hardware chip

Approx. 45 KG, Approx. 2 Gbps (Using 0.18-µm ASIC)

Approx. 9.5 K slice, Approx. 400 Mbps (Using FPGA)

Compact and efficient hardware chip

Approx. 8 KG, Approx. 200 Mbps (Using 0.18-µm ASIC)

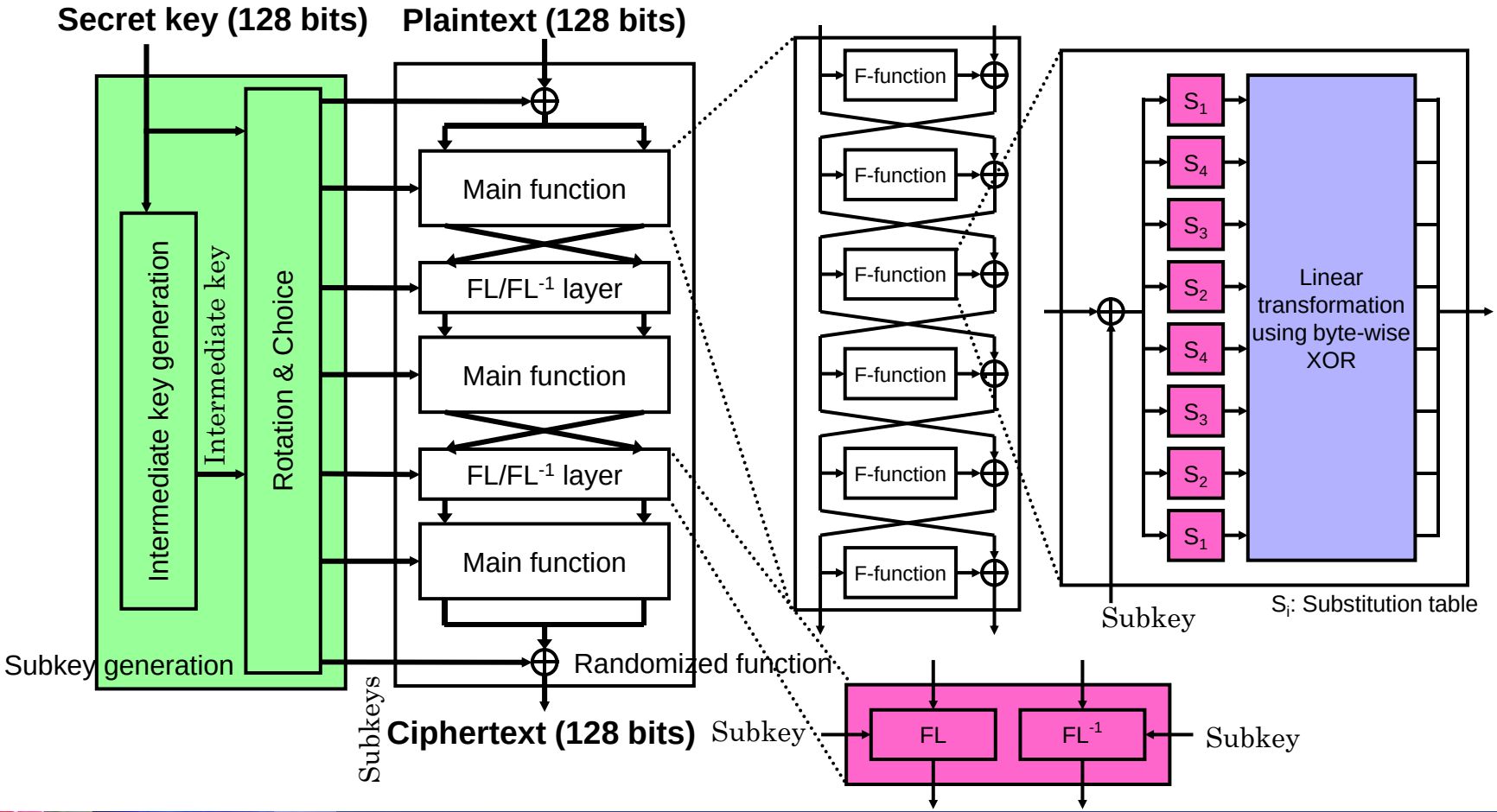
Approx. 2 K slice, Approx. 250 Mbps (Using FPGA)

High-speed software for PCs

Approx. 1 Gbps (Using Assembly) (@Pentium 4, 3.2 GHz)

Win-Win Collaboration on Crypto in Japan

NTT's know-how for designing ciphers suitable for high-speed software implementation	Mitsubishi's know-how for designing ciphers suitable for high-performance hardware implementation	New co-designing



What is “Camellia” – Origin of the Name

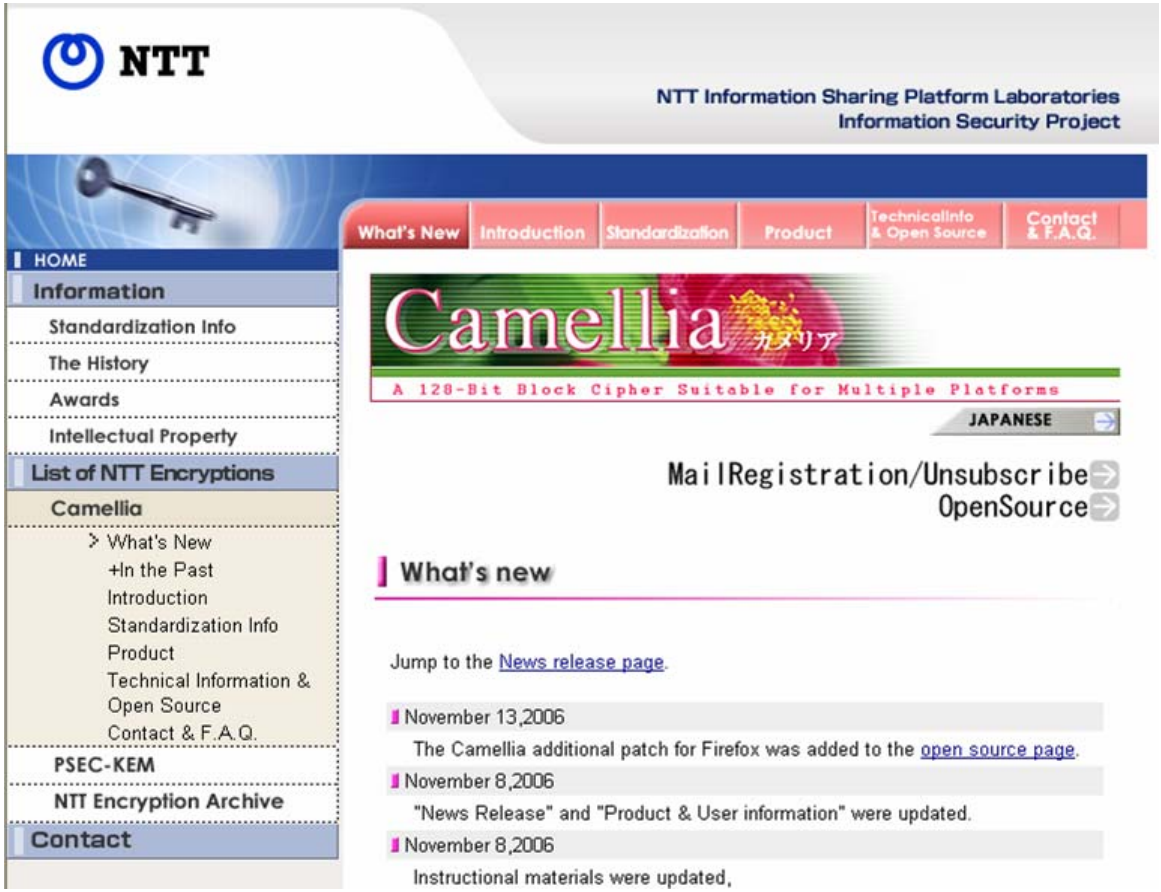
- Camellia (Tsubaki in Japanese)
  - Japan is the place of origin and the scientific name is Camellia japonica. In the language of flowers it means Good fortune and loveliness, gratitude.

- Our minds:
  - Although this encryption technology originates from Japan, after leaving Japan we want it to grow in various forms – as well as Camellia flowers

For More Detail …

- Please see the Camellia website !!

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



Technical Details

Camellia Specifications

- Interface: Compatible with AES
  - Block length: 128 bits
  - Key length: 128, 192, and 256 bits
- Main structure: Similar to DES-like ciphers, not AES
  - 18-round Feistel structure for 128-bit key
  - 24-round Feistel structure for 192- and 256-bit keys
    - FL/FL^{-1} function layers: Inserted every 6 rounds
- Components
  - Round function (F-function): Byte-oriented SPN structure
  - FL/FL^{-1} function layers: Combination of AND, OR, Rotation, and XOR
  - Whitening: XOR
- Subkey generation
  - Intermediate keys are generated from secret key using 2-round Feistel structure
  - Subkeys are created from secret key and intermediate keys using Rotation & Choice technique

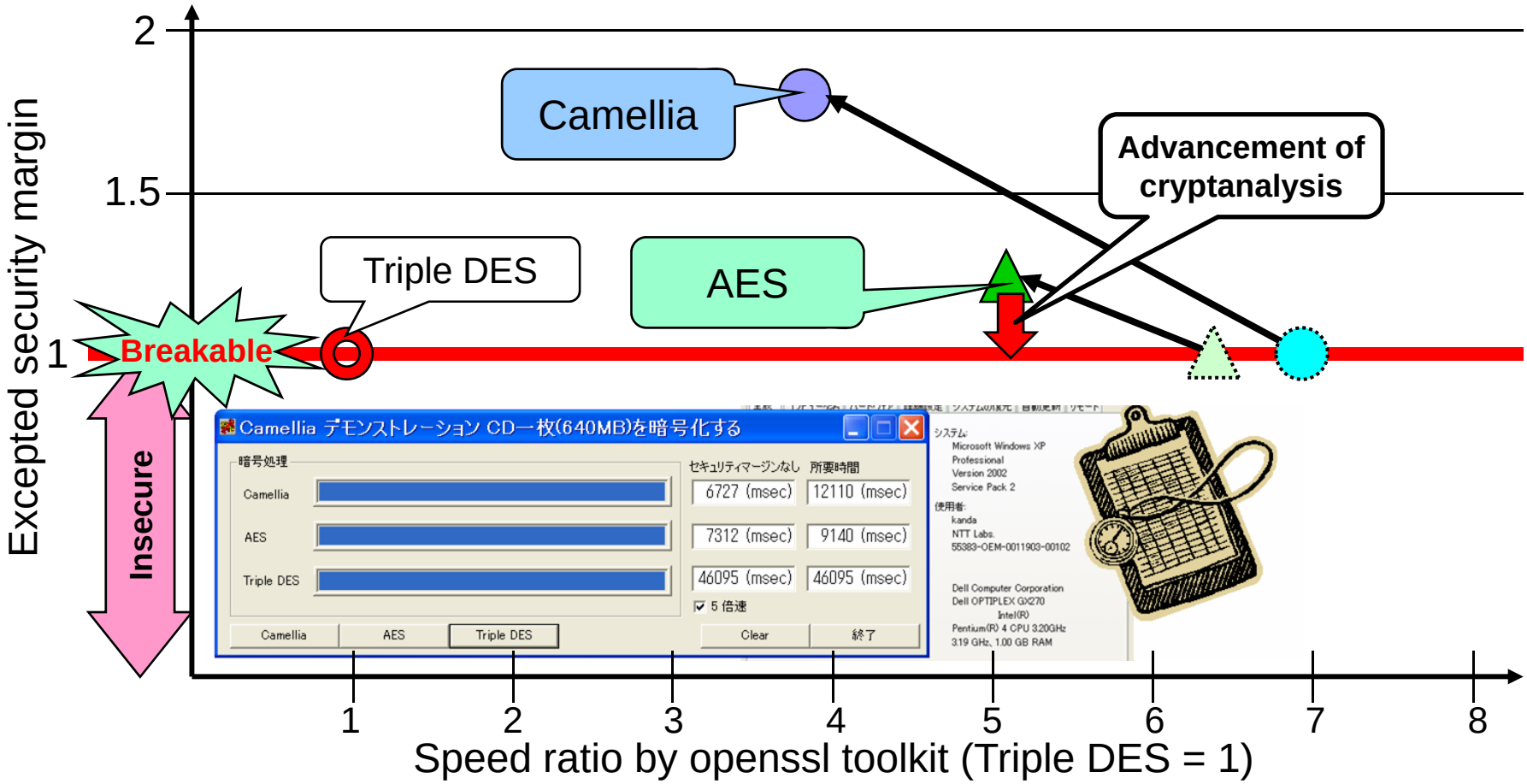
Software Performance for PCs

- **Available to software-based encryption for high-quality videos**

Processor	Language	Throughput (both encryption and decryption)			Notes
		128-bit key	192-bit key	256-bit key	
Core2 Duo E8400	ANSI C	**505 cycles (801Mbps@3.16GHz)**	**655 cycles (618Mbps@3.16GHz)**	**655 cycles (618Mbps@3.16GHz)**	**Open source code published on Camellia website** (Fedora)
	Java	**698 cycles (580Mbps@3.16GHz)**	**869 cycles (466Mbps@3.16GHz)**	**869 cycles (466Mbps@3.16GHz)**	
AMD Phenom 9850	ANSIC	**470 cycles (683Mbps@2.5GHz)**	**610 cycles (526Mbps@2.5GHz)**	**603 cycles (532Mbps@2.5GHz)**	**Open source code published on Camellia website** (FreeBSD)
Pentium 4	Assembly	**361 cycles (1.1 Gbps@3.2 GHz)**	**N/A**	**N/A**	Papers (WinXP, Hyper-threading off)
	C	**900 cycles (455 Mbps@3.2 GHz)**	**1168 cycles (351 Mbps@3.2 GHz)**	**1165 cycles (352 Mbps@3.2 GHz)**	**Old version of open source code published on Camellia website** (WinXP, Hyper-threading off)
		1008 cycles (216 Mbps@1.7 GHz)	**1376 cycles (158 Mbps@1.7 GHz)**	**1376 cycles (158 Mbps@1.7 GHz)**	NESSIE Performance Reports (Linux)
	Java	**1552 cycles (264 Mbps@3.2 GHz)**	**N/A**	**N/A**	**Old version of open source code published on Camellia website** (WinXP, Hyper-threading off)
Athlon64 3500+	Assembly	**175 cycles (1.6 Gbps@2.2 GHz)**	**N/A**	**N/A**	Two block parallel encryption (WinXP, Hyper-threading on)
		243 cycles (1.2 Gbps@2.2 GHz)	**N/A**	**N/A**	Bitslice encryption (WinXP, Hyper-threading on)
Pentium III	Assembly	**326 cycles (255 Mbps@650 MHz)**	**N/A**	**N/A**	CRYPTREC Report 2002 (Win98 SE)

Tradeoff Between Security and Efficiency

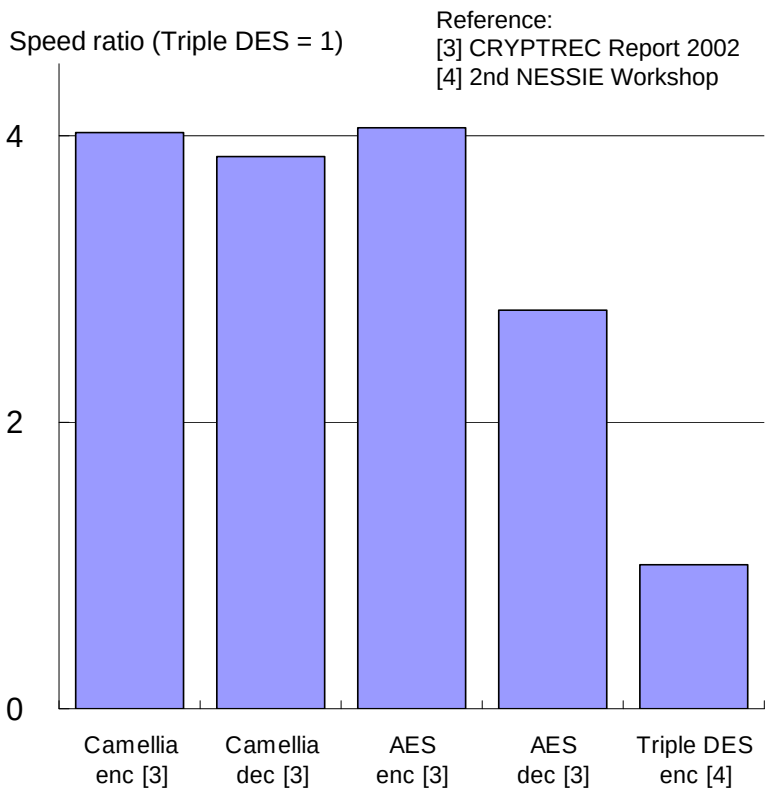
- **Good balance of security and performance**
  - Camellia gives greater importance to security than performance



Software Performance for Smart Cards

- **World's highest performance even under containment of memory usage**
  - Few additional costs are needed even if decryption is required

Processor	Memory usage		Speed per block (128-bit message)	
	RAM [bytes]	ROM [bytes]	Encryption / decryption [cycles]	Subkey generation [cycles]
Z80	63	1,698	**28,382 (5.68 msec)**	**5,146 (1.03 msec)**
	60	1,268	**(enc. w subkey gen.) 35,951 (7.19 msec)** **(dec. w subkey gen.) 37,553 (7.51 msec)**	
8051	32	990	**10,217 (10.22 msec)**	
H8/3113	Unknown	Unknown	**4,100 (1.64 msec)**	**2,380 (0.95 msec)**
AE45X	60	Unknown	**(enc. w subkey gen.) 8,136 (1.11 msec)** **(dec. w subkey gen.) 8,658 (1.18 msec)**	
SLE66 CLX320P	248	1,279	**17,920 (2.64 msec)**	**6,144 (0.91 msec)**
	58	1,311	**(enc. w subkey gen.) 24,064 (3.55 msec)** **(dec. w subkey gen.) 24,576 (3.62 msec)**	
M32Rx/D	44	8,684	**1,236 (12.36 msec)**	**642 (6.42 msec)**



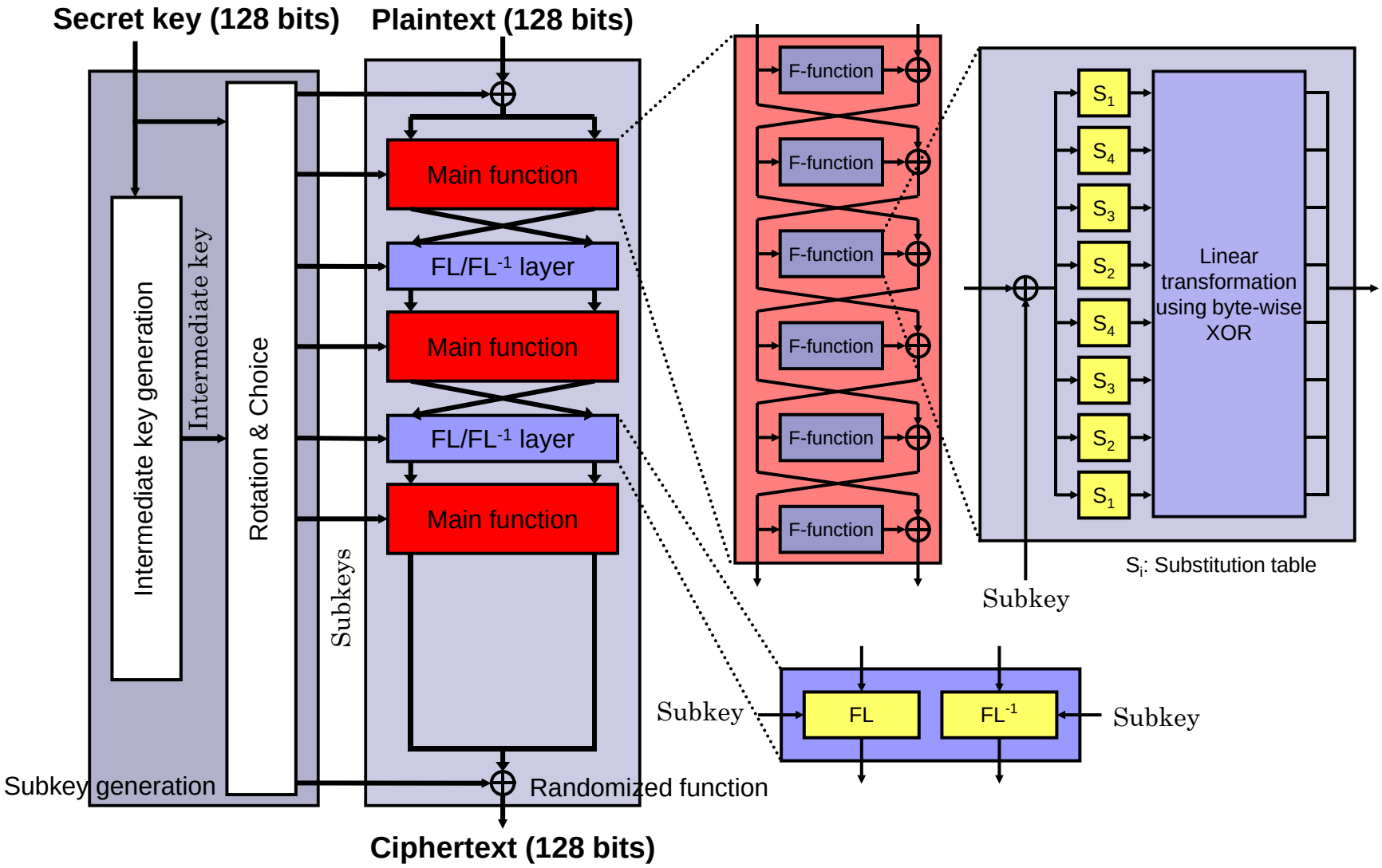
Hardware Performance

- Designed **world's smallest circuit for 128-bit block ciphers (smaller than 10 Kgates)** with world top-class efficiency

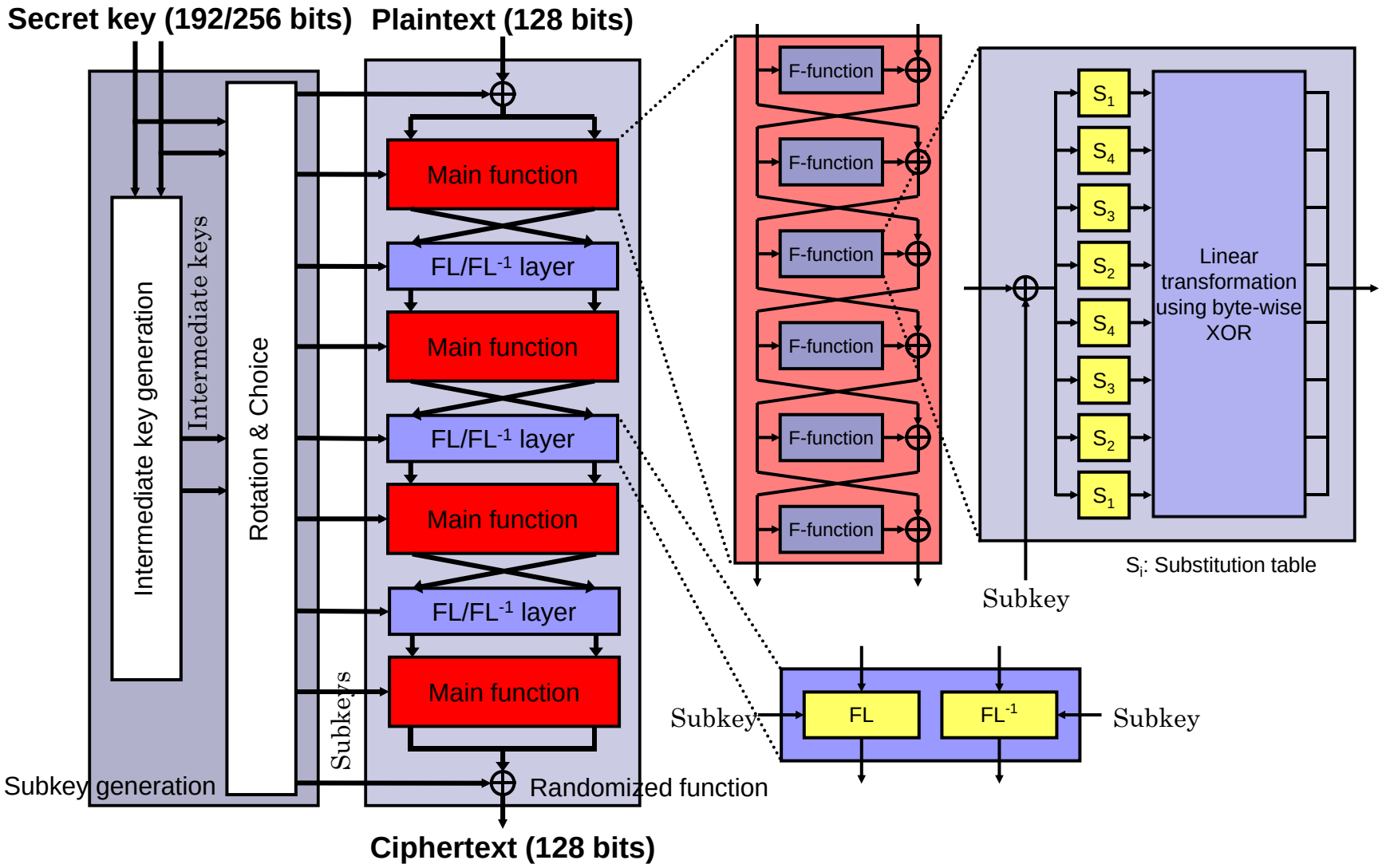
(when using 128-bit key)

Type	Design library	Throughput	Area size	Efficiency
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
	Commercial-based product	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 implementation)	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 implementation)	25,440 Mbps	19,482 slices	---

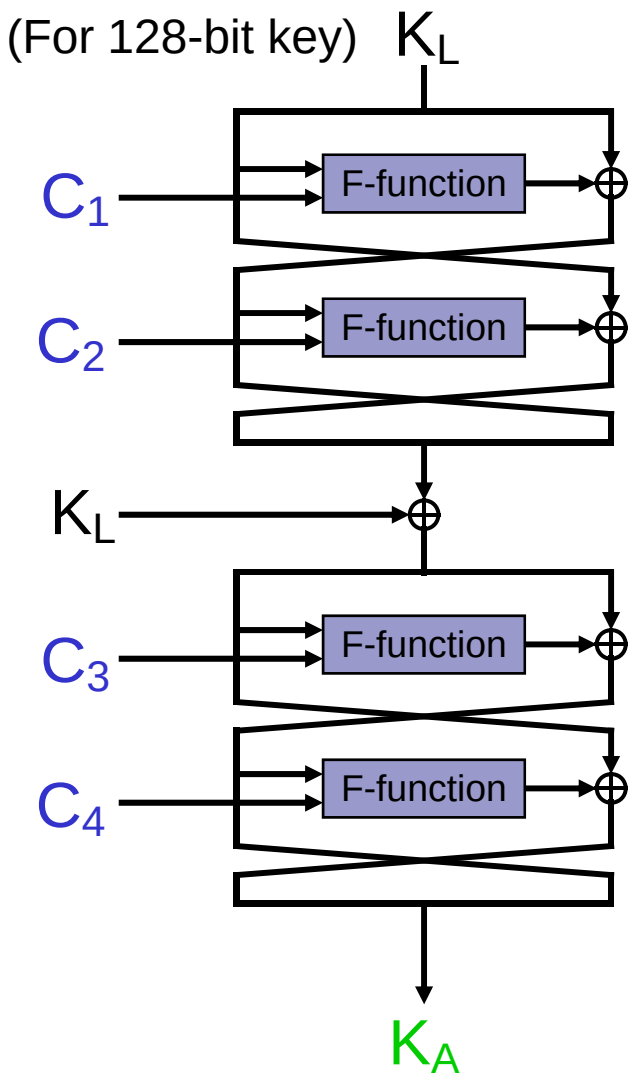
Sketch of Procedure for 128-bit Key



Sketch of Procedure for 192-&256-bit Keys



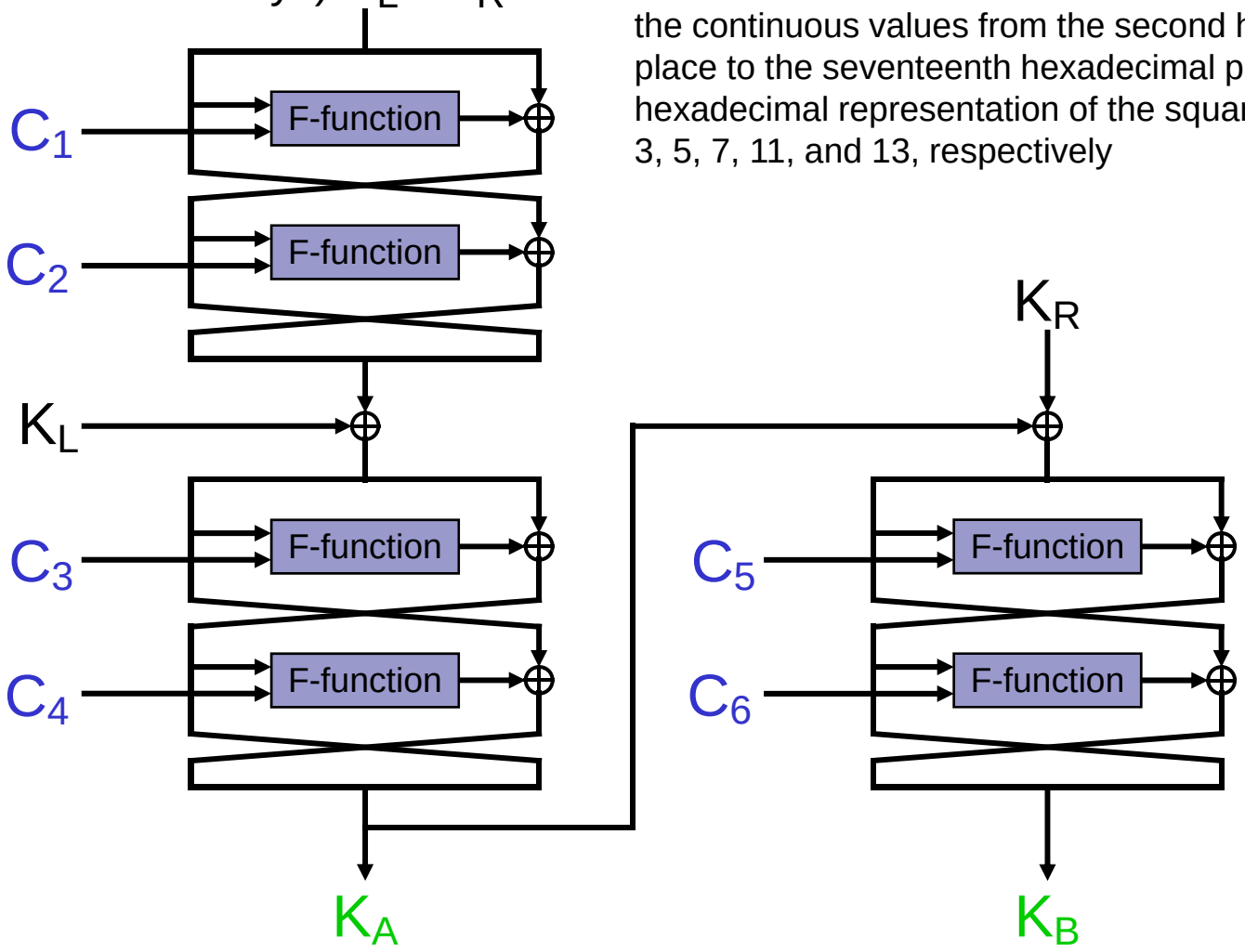
Sketch of Intermediate Key Generation



Constants C_i:
the continuous values from the second hexadecimal place to the seventeenth hexadecimal place of the hexadecimal representation of the square root of 2, 3, 5, and 7, respectively

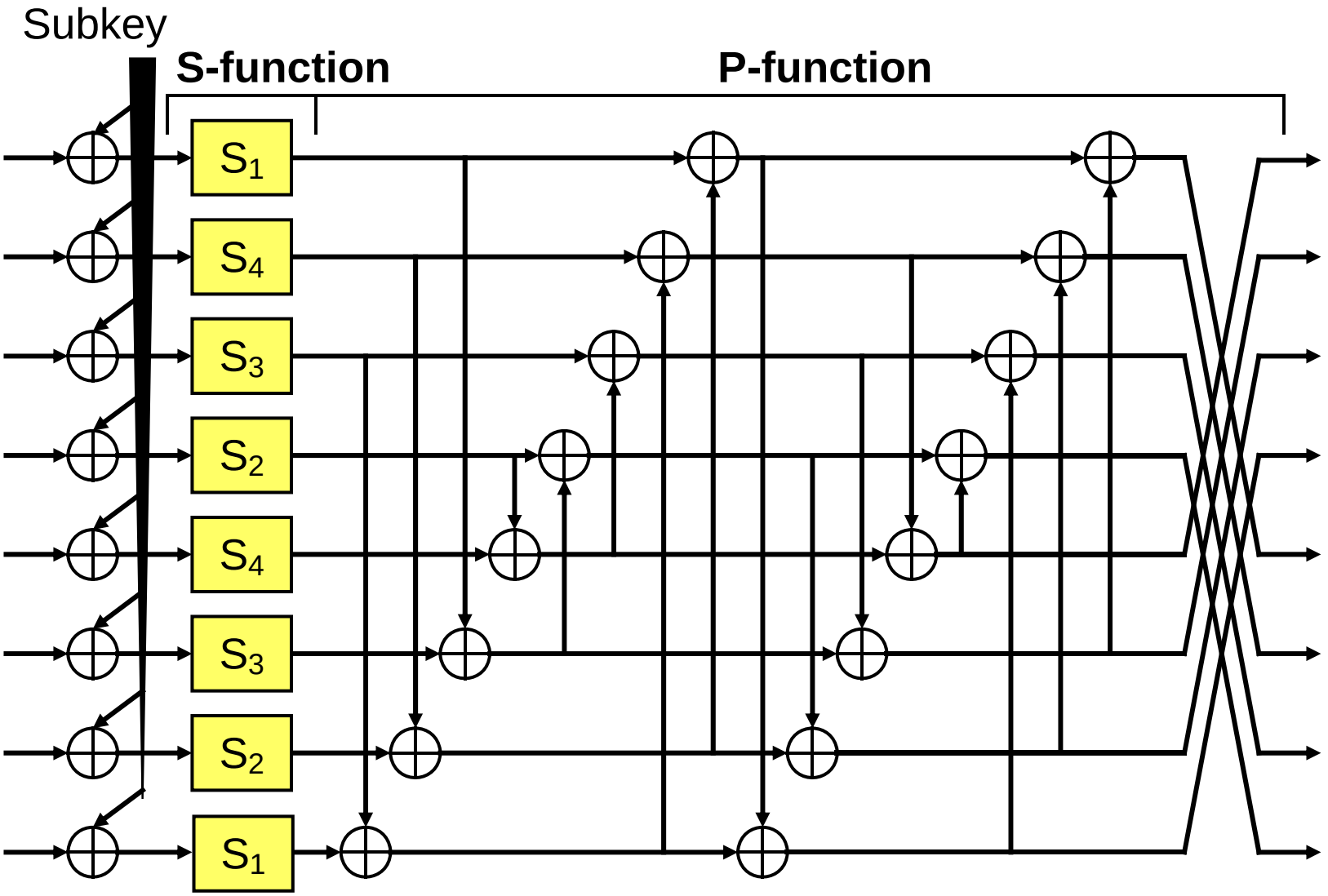
Sketch of Intermediate Key Generation (Cont.)

(For 192-/256-bit keys) $K_L \oplus K_R$



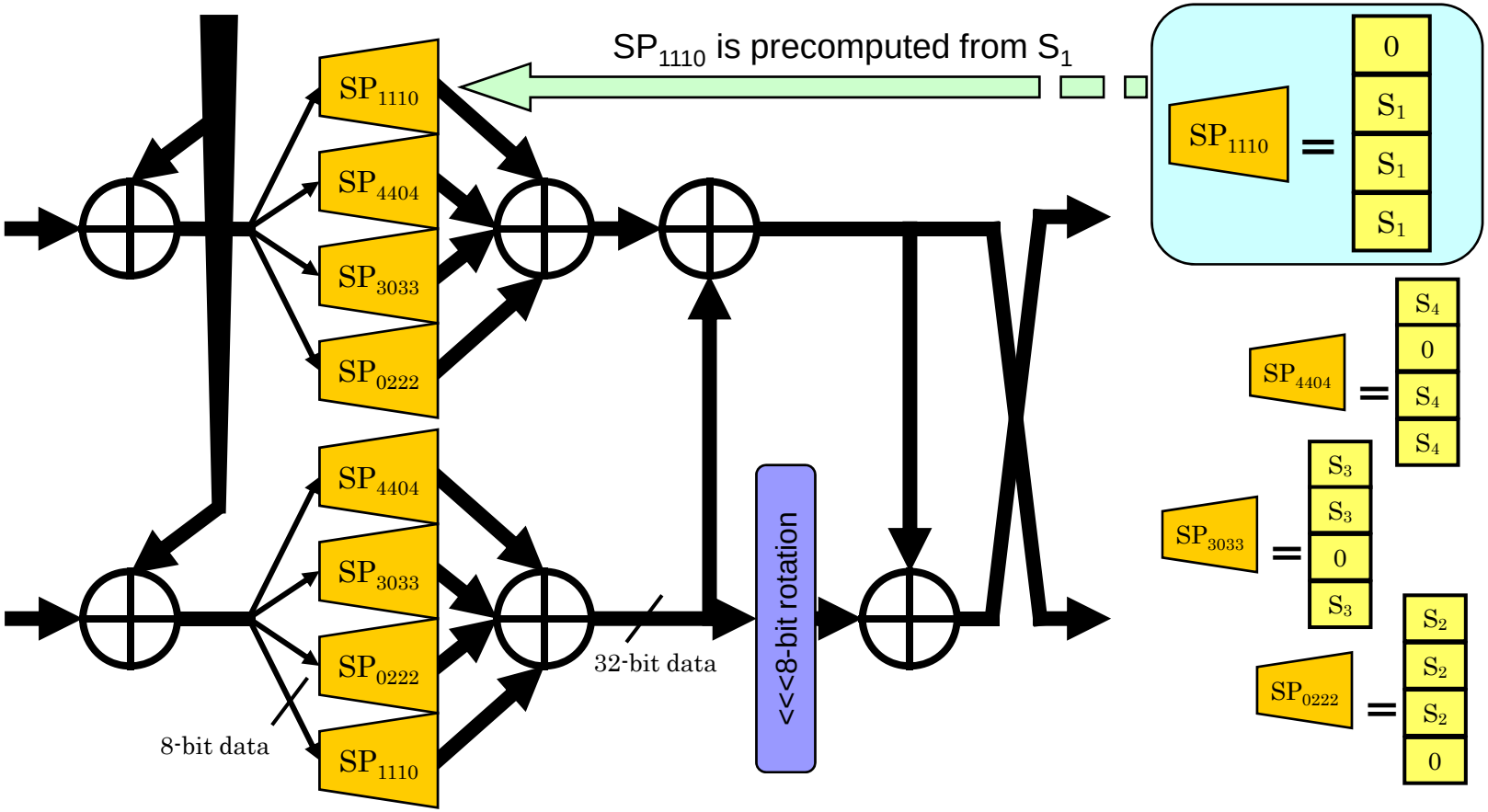
Constants C_i:
the continuous values from the second hexadecimal place to the seventeenth hexadecimal place of the hexadecimal representation of the square root of 2, 3, 5, 7, 11, and 13, respectively

Sketch of Round Function (F-function)



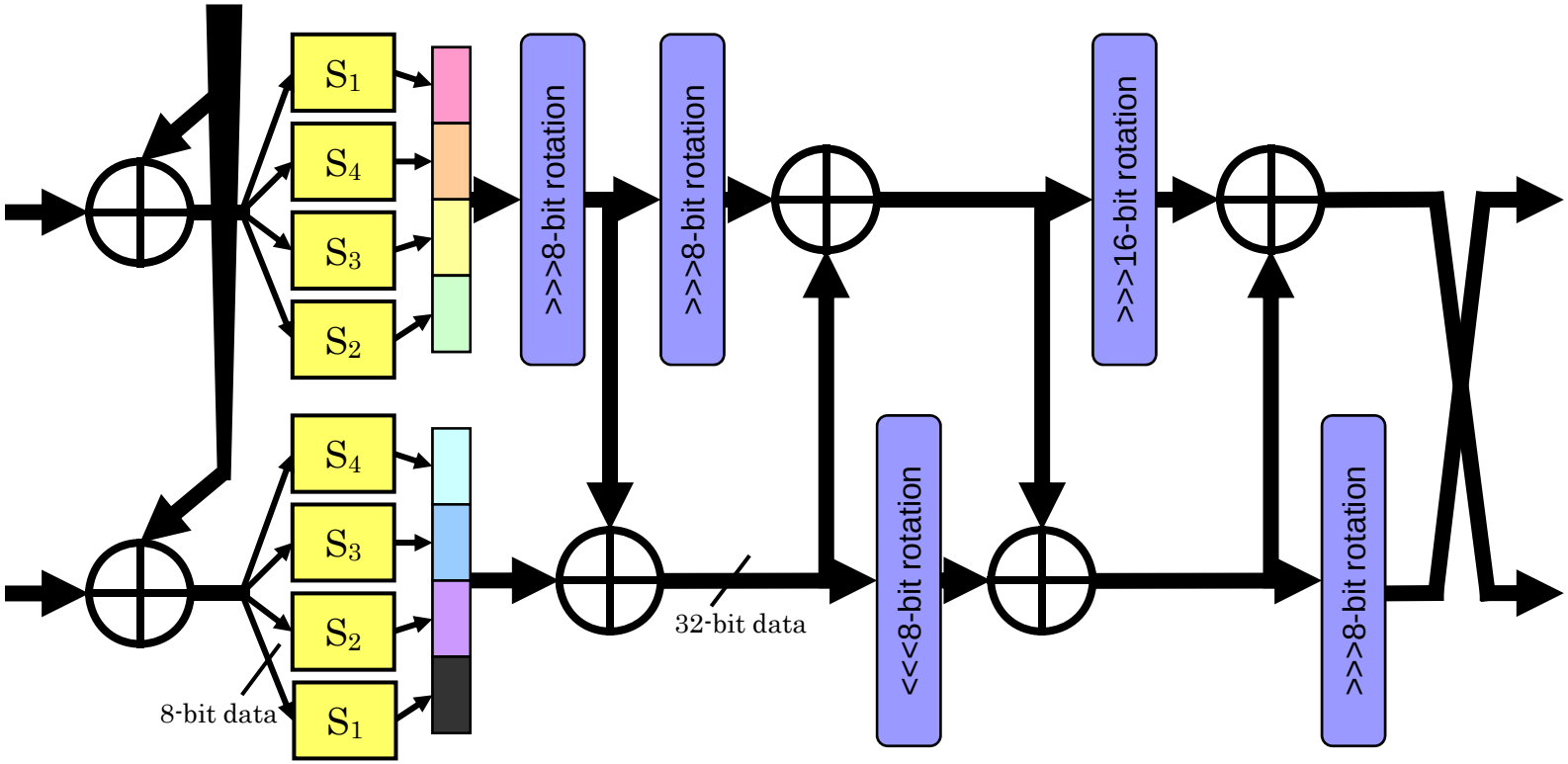
Useful Implementation for 32-bit CPU

- Using an equivalent round function with large S-boxes
  - This technique is very effective on CPUs equipped with 4-KB cache



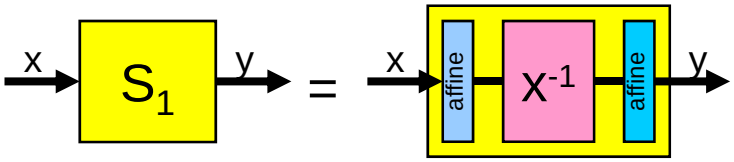
Useful Implementation for Embedded CPU

- Equivalent round function based on 32-bit operations without changing S-boxes
  - This technique is effective on smart cards and embedded CPUs with memory constraints

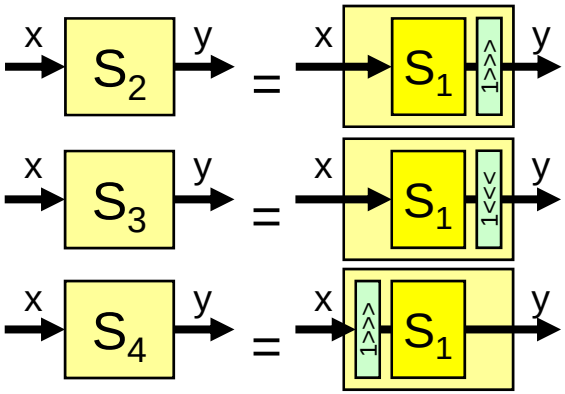


Useful Implementation for Reducing Memory

- **Reducing capacity of S-boxes**
  - This technique is effective on smart cards, embedded CPUs, and small hardware design with ROM constraints

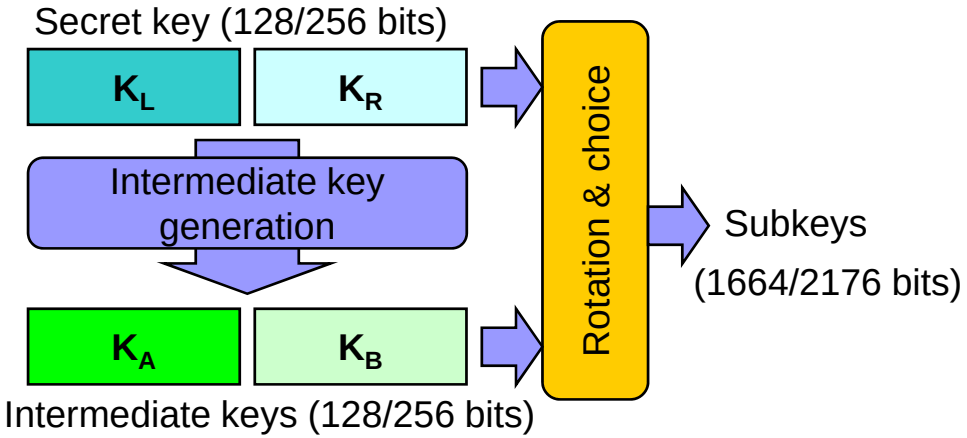


S_1 is affine equivalent to an inversion function over GF(2^8)



S_2, S_3, and S_4 can be computed only from S_1

- **Reducing memory usage of subkey generation**
  - This technique is effective on smart cards, embedded CPUs, and small hardware design with RAM constraints



- On-the-fly subkey generation technique can be used with secret key and intermediate keys
- If only 128-bit secret keys are acceptable, only K_L and K_A are required

Security Evaluation Overview

Best known attacks can break the reduced-versions of Camellia in only with 9-rounds (128-bit key) or 11-rounds (256-bit key), while original versions require 18-rounds and 24-rounds, resp. (2009.9 at the present time)

Breakable rounds		**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
128-bit keys	Modified-versions (except FL/FL^{-1} layers)	ISA: $2^{10.6}$ ICA: $2^{5.8}$	ISA: 2^{18} VSA: $2^{18.6}$ ICA: $2^{13.7}$ 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^{90} ICA: $2^{119.4}$		IDC: 2^{126}	**Unknown attacks**	**Unknown attacks**	**Unknown attacks**	**Unknown attacks**
	Reduced-versions			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-bit keys	Modified-versions (except FL/FL^{-1} layers)	-	-	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**
	Reduced-versions			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**

References:
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