Camellia の最大差分特性確率および最大線形特性確率について

評価者：NTT（神田　雅透）

2001 年 1 月 12 日

1　はじめに

1.1　Camellia の概要

Camellia は、2000 年に日本電信電話株式会社ならびに三菱電機株式会社より提案された 128 ビットブロック暗号であり、2000 年 5 月 ISEC 研究会 [1] ならびに第 7 回 Selected Areas in Cryptology, SAC2000 [2] にて論文発表されている。Camellia の基本構造は、データブロック長 128 ビット、鍵長 128/192/256 ビットの 18 段（鍵長 128 ビット）または 24 段（鍵長 192/256 ビット）Feistel 構造であり、6 段ごとに $\mathrm{FL}/\mathrm{FL}^{-1}$ 関数が挿入されている。

Camellia の設計方針では、安全性と実装性両面でのバランスを重視した設計が行われている。安全性の観点では、設計者らは、特に差分解読法、線形解読法、truncated differential cryptanalysis を主要な解読法であるとの考えのもと、設計時点でこれらの解読法に対する安全性を考慮した設計が行われている。

1.2　差分解読法及び線形解読法に対する安全性自己評価に関する記述

差分解読法及び線形解読法に対する自己評価は、自己評価書の第 6.1 節（差分解読法・線形解読法）に記述されている[1]。また、Camellia home page より Knudsen [6] による第三者評価結果[2]が入手可能である。本レポートでは、自己評価書の記述内容、学会発表論文ならびに第三者評価結果から、差分解読法及び線形解読法に対する安全性自己評価の妥当性を検証する。

1.3　差分解読法や線形解読法に対する安全性指標

差分解読法や線形解読法に対する安全性を示す指標として以下の 4 つが知られている。いずれの指標を用いて評価したのかによって、差分解読法や線形解読法に対する安全性評価の厳密性が異なることに注意されたい。最近では、以下に示す、“provable security” もしくは “practical security” を備えた暗号が望ましいとされている。

最大平均差分確率／最大平均線形確率　差分解読法や線形解読法に対する真の安全性を示す指標 [7, 10]。これらの確率が十分に小さいことが保証されれば、差分解読法や線形解読法に対して理論的に安全であることが証明される。しかし、全数探索並みの計算量が必要であるため、暗号全体についてこれらの確率を算出することは極めて困難である。

最大差分特性確率／最大線形特性確率　攻撃者が、計算機などによって、差分解読法や線形解読法により暗号を実際に解読する場合の安全性を示す指標 [3, 8]。これらの確率は計算機実験などにより算出できることが多い。しかし、計算機能力の向上や探索アルゴリズムの改良等によって、これらの確率が変わることがあるので、評価時点での差分解読法や線形解読法に対する安全性の限界を示しているにすぎないと考えるべきである。したがって、これらの確率が十分に小さいことが差分解読法や線形解読法に対して安全であることの必要条件であって、十分条件ではない。

[1] さらに関連するところでは第 6.2 節、第 6.3 節、第 6.4 節、第 6.5 節がある。

[2] このほかに、Yiqun Lisa Yin [13] による第三者評価結果もある。しかし、$\mathrm{FL}/\mathrm{FL}^{-1}$ 関数の効果と鍵スケジューリング部に焦点を当てた報告書であるので、本レポートでは取り上げない。

最大平均差分確率／最大平均線形確率の上界値 最大平均差分確率や最大平均線形確率の上界値を理論的に保証したことによって安全性を示す指標 [11]。これらの値が十分に小さいことが示されるのであれば、結果として最大平均差分確率や最大平均線形確率が十分に小さいことが保証される。この指標により差分解読法や線形解読法に対して安全であると示すことを “（差分解読法や線形解読法に対する）証明可能安全 (provable security)” という。

最大差分特性確率／最大線形特性確率の上界値 最大差分特性確率／最大線形特性確率の上界値を理論的に保証したことによって安全性を示す指標 [5, 12]。これらの値と最大平均差分確率や最大平均線形確率との間に理論的な関係はないため、これらの値が十分に小さいからといって、直接的に最大平均差分確率や最大平均線形確率が十分に小さいことが保証されるわけではない。しかし、実際の暗号の多くは、これらの値と最大平均差分確率や最大平均線形確率の値が極端に大きく離れているとは考えにくい。したがって、この指標により差分解読法や線形解読法に対して安全であると示すことを “（差分解読法や線形解読法に対する）実用的証明可能安全 (practical security)” という。実用的証明可能安全であることを証明するためには、128 ビットブロック暗号の場合、最大差分特性確率及び最大線形特性確率の上界値が 2^{-128} 以下となることが必要であるとされている。

2 自己評価書の妥当性検証

2.1 自己評価の妥当性

Camellia のラウンド関数の構成要素は基本構造部分が s-box と排他的論理和だけであり、また FL/FL^{-1} 関数の構成要素は論理積、論理和、排他的論理和及びローテーションである。

ラウンド関数が s-box と排他的論理和だけで構成される暗号においては、差分解読法や線形解読法に対する安全性を評価するために、active s-box の最少個数によって最大差分特性確率および最大線形特性確率の上界値を示す以下の定理が多く利用されている。この定理を利用することは、差分解読法や線形解読法に対する安全性評価を考慮した現在の暗号設計指針として極めて妥当とされている。

定理（文献 [12]） $\mathcal{D}$ を全体の active s-box の最少個数とし、s-box での最大差分（線形）確率を p_s とする。このとき、最大差分（線形）特性確率の上界値は、$p_s^{\mathcal{D}}$ で表される。

Camellia の差分解読法及び線形解読法に対する安全性評価にも、active s-box の最少個数によって最大差分特性確率及び最大線形特性確率の上界値を示す方法が利用されている。提案者は、差分解読法及び線形解読法に対する Camellia の安全性を評価する上で、active s-box の最少個数の数え方として以下の 3 つを挙げ、それぞれについて最大差分特性確率及び最大線形特性確率の上界値を求めている。評価結果概要は表 1及び表 2のとおりである。なお、Camellia の場合、s-box の最大差分確率は $p_s = 2^{-6}$、最大線形確率は $q_s = 2^{-6}$ である。

評価方法 1（文献 [4]） SPN 型ラウンド関数を利用した Feistel 暗号に対する active s-box の最少理論値に基づく最大差分特性確率及び最大線形特性確率の上界値

評価方法 2 探索による、Camellia に対する active s-box の最少個数に基づく最大差分特性確率及び最大線形特性確率の上界値

評価方法 3 探索による、FL/FL^{-1} 関数無しの Camellia に対する active s-box の最少個数に基づく最大差分特性確率及び最大線形特性確率の上界値

評価方法 1 については、最大差分特性確率及び最大線形特性確率の理論上界値が文献 [4] の定義 8 及び定理 3 より算出可能であり、Camellia の場合、s-box の最大差分確率 $p_s = 2^{-6}$、最大線形確率は $q_s = 2^{-6}$ ならびに分岐数 $\mathcal{B} = 5$ を代入することより求められる。この結果、**FL/FL^{-1} 関数を除いた（Camellia 型の）Feistel 暗号では 16 段以上の有効な差分特性及び線形特性が存在しないことが理論上保証**される。なお、評価手法 1 については SAC2000 に採録 [4] されており、**その正当性が第三者によっても確認されているものと考えられるので、これによる評価結果も十分に信頼できる**ものである。

表 1: Camellia の最大差分特性確率の上界値

段数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
評価方法 1			2^{-12}	2^{-30}		2^{-42}		2^{-66}				2^{-96}				2^{-132}
			(2)	(5)		(7)		(11)				(16)				(22)
評価方法 2	1	2^{-6}	2^{-12}	2^{-42}	2^{-54}	2^{-66}	2^{-72}	2^{-72}	2^{-78}	2^{-108}	2^{-120}	2^{-132}				
	(0)	(1)	(2)	(7)	(9)	(11)	(12)	(12)	(13)	(18)	(20)	(22)				
評価方法 3	1	2^{-6}	2^{-12}	2^{-36}	2^{-54}	2^{-66}	2^{-78}	2^{-90}	2^{-108}	2^{-126}	2^{-132}					
	(0)	(1)	(2)	(6)	(9)	(11)	(13)	(15)	(18)	(21)	(22)					

注: （ ）内は active s-box の最少個数

表 2: Camellia の最大線形特性確率の上界値

段数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
評価方法 1			2^{-12}	2^{-30}		2^{-42}		2^{-66}				2^{-96}				2^{-132}
			(2)	(5)		(7)		(11)				(16)				(22)
評価方法 2	1	2^{-6}	2^{-12}	2^{-36}	2^{-54}	2^{-66}	2^{-72}	2^{-72}	2^{-78}	2^{-102}	2^{-120}	2^{-132}				
	(0)	(1)	(2)	(6)	(9)	(11)	(12)	(12)	(13)	(17)	(20)	(22)				
評価方法 3	1	2^{-6}	2^{-12}	2^{-36}	2^{-54}	2^{-66}	2^{-78}	2^{-84}	2^{-108}	2^{-120}	2^{-132}					
	(0)	(1)	(2)	(6)	(9)	(11)	(13)	(14)	(18)	(20)	(22)					

注: （ ）内は active s-box の最少個数

また、提案者は、評価方法 1 は Feistel 暗号での一般理論であるので、Camellia に特化した場合の評価結果は、より安全であると主張している。その傍証として、計算機実験による active s-box の最少個数を探索し、弱鍵による FL/FL^{-1} 関数を含めた場合でも 12 段以上の有効な差分特性及び線形特性が存在しないこと（評価方法 2）、FL/FL^{-1} 関数を除いた場合には 11 段以上の有効な差分特性及び線形特性が存在しないこと（評価方法 3）が示されている。この計算機実験においては、文献 [9] をベースにしていると記載されている。文献 [9] の探索との差異は、確率表現であったものを active s-box の個数表現に変更した点と、弱鍵による FL/FL^{-1} 関数での効果を考慮している点である。

2.2 L. R. Knudsen 報告書概要

L. R. Knudsen による報告書は 12 ページ[3]にわたり、そのうち差分解読法及び線形解読法に対する評価結果は第 1.1 節に記載されている[4]。

第 1.1 節での記述によれば、Knudsen は、期待される active s-box の最少個数から差分解読法や線形解読法に対して平均的にどの程度の安全性があるかの見積もりを行っている。その見積もりに際し、以下のような推測のもと、6 段での最大差分特性確率と最大線形特性確率はとも 2^{-108} 程度と見積もっている[5]。

- Camellia のラウンド関数の構成上、1 段あたりの active s-box の平均個数は 3 個以上になると期待される。したがって、ここでの評価においては 1 段あたり 3 個の active s-box で構成されるような経路が存在すると仮定する。
- active s-box での最大差分確率と最大線形確率はともに 2^{-6} であるので、この値を採用する。

この評価結果は、Knudsen の知見による推測に基づくものであり、必ずしも最良の結果であるとは断定できないが、かなり攻撃者に有利な見積もりをしたとしても、差分解読法や線形解読法に対して平均的にこの程度の安

[3] この他に一般的な解読法の概要が 5 ページにわたり記載されている。
[4] さらに関連するところでは第 1.2 節がある。
[5] 線形解読法に対する評価として、報告書の中では 6 段での最大バイアスが 2^{-55} 程度と記述されている。(最大線形特性確率) = (2 × 最大バイアス)^2 となることが知られていることより、最大線形特性確率は 2^{-108} 程度となる。

全性は期待できることを示している。ちなみに、第 1.2 節では、差分解読法の拡張である、truncated differential cryptanalysis に対する安全性を詳しく検証している。これによれば、FL/FL^{-1} 関数無しの 7 段の Camellia についてランダム関数との識別が可能（Fact 3）であるが、それ以上は困難であると期待されると結論づけている。

これらの結果から、**差分解読法及び線形解読法に対しては、7, 8 段程度が実際の攻撃可能段数になるであろう**との期待が得られる。つまり、これらの結果（予想）は、差分解読法や線形解読法による解読が、計算機実験結果である表 1や表 2で示した提案者の想定する攻撃の範囲内に留まる可能性が極めて高いことを意味していると考えるのが妥当である。したがって、**Knudsen の結果と矛盾しないことから、提案者の主張する安全性が十分に期待できるものと考えることが出来、Camellia が上述した実用的証明可能安全 (practical security) を満たしている**ことになる。

3 まとめ — 妥当性の判定

本レポートでは、自己評価書の記述内容、学会発表論文ならびに第三者評価結果から、差分解読法及び線形解読法に対する安全性自己評価の妥当性を検証した。

まず、**Camellia の評価方針として active s-box の最少個数に基づいて最大差分特性確率と最大線形特性確率の上界値を見積もる手法を採用したことは、現在の暗号設計指針の観点からみて妥当な選択**であるといえる。また、提案者が主張する最少個数の算出方法が、理論的評価（評価手法 1）と計算機実験（評価手法 2, 3）の両方で実施されており、差分解読法及び線形解読法に対する安全性評価として十分な結果を提出しているものと考える。

次に、表1や表 2の記載内容についての妥当性を述べる。まず、**理論的評価については、その評価手法が SAC2000 に採録されており、理論の正当性が第三者によっても確認されているものと考えられるので、これによる評価結果は十分に信頼**できる。また、**計算機実験結果についても、第三者評価である L. R. Knudsen の結果と矛盾しないことから、提案者の主張する安全性が十分に期待**できるものと考える。

なお、現時点で知られている実際の攻撃結果として最良のものは以下のものである。

文献 [6] 7 段での truncated differential の存在確率が約 2^{-95} であり、ランダム関数から同じ truncated differential が出力される確率が 2^{-96} であるような truncated differential が存在する。これを利用した truncated differential cryptanalysis により、約 2^{68} 個の選択平文を使って、FL/FL^{-1} 関数無しの 7 段の Camellia とランダム関数との識別が可能である。

以上の結果より、**差分解読法及び線形解読法に対する安全性評価について、提案者の主張に誤りはない**と判断する。すなわち、16 段以上の有効な差分特性及び線形特性が存在しないことが理論上保証されているうえ、実際には 12 段以上の有効な差分特性及び線形特性が存在しないと十分に期待される。これより、**Camellia は（差分解読法や線形解読法に対して）実用的証明可能安全 (practical security) を満たしている**ことになる。

なお、提案者の自己評価結果も Knudsen の評価も、“攻撃者に最も有利な経路が存在した” との仮定のもとで最大差分特性確率や最大線形特性確率の上界値を見積もっているだけであり、実際にそのような経路が存在することまでは示していない。逆にいえば、もしそのような経路が存在しないのならば、それだけ差分解読法や線形解読法による攻撃が困難になるということを意味している。したがって、現時点では、差分解読法や線形解読法によってどこまで実際に攻撃可能であるのかの正確な段数を述べることは出来ないが、実際には 8〜 10 段程度が攻撃可能段数となり、**提案者の主張よりもさらに安全性が高いのではないかと期待**される。

参考文献

[1] 青木和麻呂、市川哲也、神田雅透、松井充、盛合志帆、中嶋純子、時田俊雄、“128 ビットブロック暗号 *Camellia*,” 信学技報 *ISEC2000-6*, 2000.

[2] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, “Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms,” Preproceeding of *Selected Areas in Cryptology — 7th Annual International Workshop, SAC2000*, pp.41–54, 2000. LNCS to appear.

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer-Verlag, 1993. (The extended abstruct appeared at CRYPTO'90 and Journal of Cryptology, Vol.4, No.1, 1991)

[4] M. Kanda, "Practical Security Evaluation against Differential and Linear Attacks for Feistel Ciphers with SPN Round Function," Preproceeding of *Selected Areas in Cryptology — 7th Annual International Workshop, SAC2000*, pp.326–340, 2000. LNCS to appear.

[5] L. R. Knudsen, "Practically secure Feistel ciphers," *Fast Software Encryption — Cambridge Security Workshop*, LNCS **809**, pp.211–222, 1994.

[6] L. R. Knudsen, "Analysis of Camellia," *Camellia home page*, `http://info.isl.ntt.co.jp/camellia`.

[7] X. Lai, J. L. Massy, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," *Advances in Cryptology — EUROCRYPT'91*, LNCS **547**, pp.17–38, 1991.

[8] M. Matsui, "Linear Cryptanalysis Method for DES cipher," *Advances in Cryptology — EUROCRYPT'93*, LNCS **765**, pp.386–397, 1994.

[9] 松井充、"ブロック暗号 E2 の差分経路探索," 信学技報 *ISEC99-19*, 1999.

[10] K. Nyberg, "Linear Approximation of Block Ciphers," *Advances in Cryptology — EUROCRYPT'94*, LNCS **950**, pp.439–444, 1991.

[11] K. Nyberg and L. R. Knudsen, "Provable Security against a Differential Attack," *Journal of Cryptology*, Vol.8, No.1, pp.27–37, 1995.

[12] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. DcWin, "The Cipher SHARK," *Fast Software Encryption — Third International Workshop*, LNCS **1039**, pp.99–112, 1996.

[13] Yiqun Lisa Yin, "A Note on the Block Cipher Camellia," *Camellia home page*, `http://info.isl.ntt.co.jp/camellia/`.