128ビットブロック暗号 *Camellia* アルゴリズム仕様書 更新情報

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 ‡

† 日本電信電話株式会社　‡ 三菱電機株式会社

2001 年 9 月 26 日

以下の内容が平成 12 年度提出のアルゴリズム仕様書に付け加えられました。

D　設計方針

日本電信電話株式会社 (以下では NTT と略す) と三菱電機株式会社 (以下では三菱電機と略す) が共同で開発した 128 ビットブロック暗号 *Camellia* を提案する。Camellia では、ブロック長が 128 ビット、鍵長が 128 または 192 または 256 ビットであり、次期米国政府標準暗号 (以下 AES; Advanced Encryption Standard) のインタフェースに準拠している。また、設計目標は以下のとおりである。

高い安全性　最近の暗号解読技術の進展には目を見張るものがある。このため、差分攻撃 [BS93] や線形攻撃 [M94] に代表される強力な暗号解読技術に対する安全性を定量的に評価することが新しい暗号を設計する上で必要不可欠なことであると考えられている。我々は、最新の暗号解読技術を利用して Camellia の安全性を評価し、2^{-128} 以上の確率を有するような差分特性や線形特性が Camallia には存在しないことを確認した。さらに、それら以外の攻撃法、例えば高階差分攻撃 [K95, JK97]、補間攻撃 [JK97, A00]、関連鍵攻撃 [B94, KSW96]、丸め差分攻撃 (truncated differential attacks) [K95, MT99]、ブーメラン攻撃 [W99]、スライド攻撃 [BW99, BW00] などに対しても安全であるように設計されている。

さまざまなプラットフォーム上での高い効率性　暗号システムはさまざまなアプリケーションで必要となるので、暗号アルゴリズムは幅広いプラットフォーム上で効率的に実装できることが望まれる。しかし、ソフトウェアとハードウェアの両面に適した 128 ビットブロック暗号アルゴリズムは数少ない。Camellia は、さまざまなプラットフォーム上での処理速度とともに、ハードウェアでのゲート数やスマートカードでの使用メモリ量などを考慮して、ハードウェアとソフトウェア両面できわめて効率的な実装が可能となるように設計されている。

Camelliaは、幅広いプラットフォーム上で効率的な実装が可能である8ビット入出力置換表 (s-box) と論理演算から構成されている。このため、低機能ICカードで利用されている8ビットCPUから、PCで広く使われている32ビットCPU、さらには64ビットCPUまで、ソフトウエアで効率的な実装が可能である。また、Camelliaでは、ソフトウェア実装に主眼を置いて設計されたいくつかの128ビットブロック暗号で広く使われている32ビット加算演算と乗算演算は使用しなかった。なぜなら、これらの算術演算は、Pentium II/IIIやAthlonのような特殊なプラットフォーム上では高速に実行されるが、それ以外のプラットフォームでは高速な処理とはいえず、また、ハードウェア実装においては、長いクリティカルパスを構成し、かつ回路規模が大きくなる原因ともなるためである。

Camelliaの置換表はハードウェア規模が最小になるように設計してある。つまり、4つの置換表は GF(2^8) 上の逆数関数のアフィン変換によって構成され、さらにその逆数関数はいくつかの GF(2^4) 上の演算によっても実現できる。これにより、置換表をより少ないゲート数で実装することが可能となっている。

鍵スケジュールは非常に簡単な構造を有し、暗号化処理の一部分を共用している。また、動的 (on-the-fly) な副鍵生成が可能であり、そのとき暗号化・復号を問わず同じ効率で副鍵が生成される。副鍵生成のためのメモリ使用量も極めて小さく、128ビット鍵では約32バイトのRAM、また192ビット鍵と256ビット鍵では約64バイトのRAM使用量で実装できる。

E 設計基準

E.1 F 関数

Camelliaのラウンド関数 (以下 F 関数) の設計指針は、E2の F 関数の設計指針 [KMA+98] を踏襲している。E2とCamelliaとの主要な差異は、ラウンド関数の構造を2段換字置換網 (SPN; Substitution-Permutation Network) から1段換字置換網に変更した点である。1段換字置換網構造をFeistel暗号のラウンド関数に利用したとき、差分特性確率や線形特性確率の上界値による理論的評価はより複雑になるものの、差分攻撃や線形攻撃に対する実際の安全性が同じ程度としたときの暗号化処理速度が改善されると期待される。この安全性評価については第6章で詳細を記しているので、そちらを参照されたい。

E.2 P 関数

Camelliaの線形変換関数 (以下 P 関数) の設計方法は、E2の P 関数の設計方法 [KMA+98] を踏襲している。すなわち、実装効率性の観点から排他的論理和演算 (XOR) のみで構成され、また差分攻撃や線形攻撃に対する安全性の観点から分岐数 (branch number) が最良となるような線形変換関数を P 関数の候補としている。さらに、8ビットCPUでの実装のほか、32ビットCPU [AU00] および高機能ICカードでの高速なソフトウェア実装方法を考慮して、上記の候補の中から1つの P 関数を選択した。

E.3 置換表

高い安全性およびハードウェア小型化の観点から、GF(2^8) 上の逆数関数をアフィン変換した関数を利用して置換表を構成した。

GF(2^8) 上の関数における最大差分確率の最小値は 2^{-6} であることが証明されており、また最大線形確率の最小値も 2^{-6} となると予想されている。この 2^{-6} となる最良の最大差分確率と最大線形確率を達成する GF(2^8) 上の逆数関数をアフィン変換した関数が存在することから、これらの関数を置換表として採用した。このような置換表でのすべての出力ビットに対するブール多項式での次数は高いので、高階差分攻撃によって Camellia を解読することは困難である。また、GF(2^8) 上の逆数関数の入出力において実行される 2 つのアフィン関数によって置換表の GF(2^8) 上での表現が複雑になり、補間攻撃も効率的ではなくなる。さらに、4 つの異なる置換表を作ることによって、丸め差分攻撃 [MT99] に対する安全性が多少改善される。

ハードウェアの小型設計において、GF(2^8) 上の要素は部分体 GF(2^4) 上の係数の多項式としても表現することができることから、GF(2^4) 上の演算を何回か行うことによって置換表を実装することが可能である [MIYY88]。また、GF(2^8) 上の逆数関数の入出力において実行される 2 つのアフィン関数によって置換表の GF(2^4) 上での表現も複雑になる。

E.4 FL 関数と FL^{-1} 関数

FL 関数と FL^{-1} 関数は、構造の同型性を崩すために Feistel 構造の 6 段ごとに挿入される。このような関数を挿入する目的の 1 つは、現在知られていない攻撃に対する防護を図ることである。Feistel 構造の同型性が有する特徴のひとつに、暗号化処理と復号処理が副鍵の挿入順序を除いて同じ処理となっている点が挙げられる。そこで、Camellia は FL 関数と FL^{-1} 関数とを 6 段ごとに挿入するものの、上記の特性を損なわないようにしている。

FL 関数とその逆関数である FL^{-1} 関数の設計指針は、MISTY の FL 関数の設計指針を踏襲している [M97]。MISTY と Camellia との差異は、1 ビット循環シフトを加えたことである。これは、Camellia に対するバイト単位での暗号解読を難しくすることを意図すると同時に、ハードウェア規模や処理速度に対して負の影響が出ないようにするためのものである。これらの関数の設計方針は、固定された鍵に対しては (固定された) 線形変換になる一方で鍵の値によってその変換方法そのものが変わるようにすることである。すなわち、鍵が固定されている限り、これらの関数は (固定された) 線形変換となるので、平均差分確率や平均線形確率を大きくすることはない。さらに、論理積、論理和、排他的論理和 (XOR)、および循環シフトという論理演算によって構成されているので、ソフトウェアでもハードウェアでも高速な処理となっている。

E.5 鍵スケジュール

鍵スケジュールの設計指針は以下のとおりである。

1. 簡単な構成であり、さらに暗号化・復号の処理の一部分を共用できること。
2. 128 ビット鍵、192 ビット鍵、256 ビット鍵すべてについて副鍵生成回路が同様の鍵スケジュー

ル回路で実行できること。さらに、128 ビット鍵での鍵スケジュールはその回路の一部分を利用して実現できること。

3. 副鍵生成時間は暗号化処理時間よりも短いこと。
   1 つの秘密鍵で大量のデータを暗号化する場合には鍵セットアップ時間はあまり重要ではないかもしれない。しかし、秘密鍵が頻繁に変更されるようなアプリケーションでは鍵軽快性 (key agility) が重要となる。鍵軽快性の基本的要素の一つが副鍵生成時間である。
4. 動的 (on-the-fly) 副鍵生成が可能であること。
5. 動的 (on-the-fly) 副鍵生成時に、暗号化用の副鍵生成と復号用の副鍵生成の両方が同じ効率で計算できること
   いくつかの暗号では、暗号化用の副鍵生成と復号用の副鍵生成とが異なるものがある。また、Rijndael [DR98] や Serpent [ABK98] などのように、暗号化用の副鍵は逐次的に生成できるが、復号用の副鍵は最終の暗号化用副鍵から逆順に生成しなければならないような暗号もある。
6. 等価鍵が存在しないこと。
7. 関連鍵攻撃やスライド攻撃ができないこと。

指針 1 と 2 は主にハードウェアの小型実装を目的とした項目であり、指針 3、4 および 5 は実際のアプリケーションにおける優位性を持たせるための項目である。指針 6 および 7 は安全性に関する項目である。

副鍵生成のために必要となるメモリ量は非常に小さい。128 ビット鍵での Camellia の実装では、秘密鍵 K_L 用の 16 バイト (=128 ビット) と中間鍵 K_A 用の 16 バイト (=128 ビット) との合計 32 バイトが必要なメモリ量である。同様に、192 ビット鍵および 256 ビット鍵の実装では合計 64 バイト必要となる。

F バージョン情報

Camellia は、同一の名称、かつ同一の仕様で以下に発表及び応募を行なっている。

論文発表

- 電子情報通信学会 ISEC 研究会
  青木, 市川, 神田, 松井, 盛合, 中嶋, 時田, 「128 ビットブロック暗号 Camellia」信学技報 ISEC2000-6, 2000 年 5 月.

- 国際会議 SAC 2000
  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 — Design and Analysis —,” In Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 2000, Proceedings, Lecture Notes in Computer Science 2012, pp.39-56, Springer-Verlag, 2001.

標準化機関への応募

- ISO 18033
- NESSIE
- IETF
  下記の Internet-Draft を提出.
  - J. Nakajima and S. Moriai,“A Description of the Camellia Encryption Algorithm” <draft-nakajima-camellia-02.txt>
  - S. Moriai,“Addition of the Camellia Encryption Algorithm to TLS” <draft-ietf-tls-camellia-01.txt>

G オブジェクト識別子

Camellia のオブジェクト識別子は Internet-Draft “ A Description of the Camellia Encryption Algorithm ”に記載されている。以下にその抜粋を示す。

- 鍵長 128 ビット, CBC モード
  ```
  id-camellia128-cbc OBJECT IDENTIFIER ::=
  { iso(1) member-body(2) 392 200011 61 security(1)
   algorithm(1) symmetric-encryption-algorithm(1) camellia128-cbc(2) }
  ```
- 鍵長 192 ビット, CBC モード
  ```
  id-camellia192-cbc OBJECT IDENTIFIER ::=
  { iso(1) member-body(2) 392 200011 61 security(1)
  algorithm(1) symmetric-encryption-algorithm(1) camellia192-cbc(3) }
  ```
- 鍵長 256 ビット, CBC モード
  ```
  id-camellia256-cbc OBJECT IDENTIFIER ::=
  { iso(1) member-body(2) 392 200011 61 security(1)
  algorithm(1) symmetric-encryption-algorithm(1) camellia256-cbc(4) }
  ```

H 利用実績・推奨用途など

Camelliaは共通鍵ブロック暗号が利用できるあらゆる領域に適用可能で、なかでも、暗号通信、認証に非常に適している。

Camelliaは多くのプラットフォーム上に効率良く実装可能で、PC 等で利用される 32 ビット /64 ビット CPU やローエンド /ハイエンド IC カード上でのソフトウェア実装に適するほか、ASIC, FPGA 等の小型・高速ハードウェア実装にも適している。

Camelliaの応用に関する詳細な情報は三菱電機の情報セキュリティ技術ホームページ http://www.security.melco.co.jp/から得ることができる。

参考文献

[A00] K. Aoki. Practical Evaluation of Security against Generalized Interpolation Attack. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, Vol. E83-A, No. 1, pp. 33–38, 2000. (A preliminary version was presented at SAC'99).

[ABK98] R. Anderson, E. Biham, and L. Knudsen. Serpent: A Flexible Block Cipher With Maximum Assurance. In *The First AES Candidate Conference*, 1998.

[AU00] K. Aoki and H. Ueda. Optimized Software Implementations of E2. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, Vol. E83-A, No. 1, pp. 101–105, 2000. (The full paper is available on `http://info.isl.ntt.co.% linebreak[3]jp/e2/RelDocs/`).

[B94] E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. *Journal of Cryptology*, Vol. 7, No. 4, pp. 229–246, 1994. (The extended abstract was appeared at EUROCRYPT'93).

[BS93] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[BW99] A. Biryukov and D. Wagner. Slide Attacks. In L. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 245–259, Berlin, Heidelberg, New York, 1999. Springer-Verlag.

[BW00] A. Biryukov and D. Wagner. Advanced Slide Attacks. In S. Vaudenay, editor, *Advances in Cryptology — EUROCRYPT2000*, Volume 1807 of *Lecture Notes in Computer Science*, pp. 589–606, Berlin, Heidelberg, New York, 2000. Springer-Verlag.

[DR98] J. Daemen and V. Rijmen. *AES Proposal: Rijndael*, 1998. (`http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`).

[JK97] T. Jakobsen and L. R. Knudsen. The Interpolation Attack on Block Cipher. In E. Biham, editor, *Fast Software Encryption — 4th International Workshop, FSE'97*, Volume 1267 of *Lecture Notes in Computer Science*, pp. 28–40, Berlin, Heidelberg, New York, 1997. Springer-Verlag.

[K95] L. R. Knudsen. Truncated and Higher Order Differentials. In B. Preneel, editor, *Fast Software Encryption — Second International Workshop*, Volume 1008 of *Lecture Notes in Computer Science*, pp. 196–211. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[KMA+98] M. Kanda, S. Moriai, K. Aoki, H. Ueda, M. Ohkubo, Y. Takashima, K. Ohta, and T. Matsumoto. A New 128-bit Block Cipher ***E2***. Technical Report ISEC98-12, The Institute of Electronics, Information and Communication Engineers, 1998. (in Japanese).

[KSW96] J. Kelsey, B. Schneier, and D. Wagner. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In N. Koblitz, editor, *Advances in Cryptology — CRYPTO'96*, Volume 1109 of *Lecture Notes in Computer Science*, pp. 237–251. Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[M94] M. Matsui. Linear Cryptanalysis Method for DES Cipher. In T. Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, Volume 765 of *Lecture Notes in Computer Science*, pp. 386–397. Springer-Verlag, Berlin, Heidelberg, New York, 1994. (A preliminary version written in Japanese was presented at SCIS93-3C).

[M97] M. Matsui. New Block Encryption Algorithm MISTY. In E. Biham, editor, *Fast Software Encryption — 4th International Workshop, FSE'97*, Volume 1267 of *Lecture Notes in Computer Science*, pp. 54–68, Berlin, Heidelberg, New York, 1997. Springer-Verlag. (A preliminary version written in Japanese was presented at ISEC96-11).

[MIYY88] M. Matsui, T. Inoue, A. Yamagishi, and H. Yoshida. A note on calculation circuits over GF(2^{2n}). Technical Report IT88-14, The Institute of Electronics, Information and Communication Engineers, 1988. (in Japanese).

[MT99] M. Matsui and T. Tokita. Cryptanalysis of a Reduced Version of the Block Cipher E2. In L. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 71–80, Berlin, Heidelberg, New York, 1999. Springer-Verlag. (Japanese version was presented at SCIS99.).

[W99] D. Wagner. The Boomerang Attack. In L. R. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 156–170, Berlin, Heidelberg, New York, 1999. Springer-Verlag.

更新履歴

- C.2.7 節　(誤)Pentium II 以降で採用された → (正)Pentium III 以降で採用された
- C.2.7 節　式 (3) 中の SP_1, SP_2, SP_3, SP_4 のみを用いて実装する場合の計算式の誤植を訂正
- D ～ H 章　追加