暗号アルゴリズムの詳細評価

128bit-Block 暗号 RC6

最大線形 / 差分確率、最大線形 / 差分特性確率

評価者: 青木和麻呂 (NTT)

平成 13 年 1 月 11 日

要約 RC6 の差分解読法および線形解読法に対する安全性評価結果をまとめる。最も有効な攻撃は応募者自身による線形 Markov 性を仮定した場合の 6 段繰り返し表現の multiple path による重ね合わせを使った場合で、 16 段程度まで攻撃できる。RC6 の推奨段数は 20 段であるので、現在のところ RC6 は差分解読法、および線形解読法に対して安全であると考えられる。

Abstract This report summarizes the security evaluation of RC6 against differential cryptanalysis and linear cryptanalysis. The best attack breaks RC6 up to about 16 rounds using a mix of 6-round iterative characteristics by so-called multiple paths, under the assumption that RC6 has a property of linear Markovness. Since the nominal rounds of RC6 is 20, RC6 seems currently secure against differential cryptanalysis and linear cryptanalysis.

1 評価の方針 (はじめに)

以下の手順により評価を行なう。

1. **仕様書及び自己評価書全体の斜め読み**: RC6 の概要を学ぶ
2. **本報告書の関係箇所の抽出**: 本評価書は差分解読法および線形解読法以外に関する記述も多数あるので差分解読法及び線形解読法に関する記述のみを選択
3. **仕様書及び自己評価書の関係箇所の熟読**: 自己評価内容の理解
4. **妥当性検証**: 自己評価内容の正当性検証
5. **既発表論文の調査**: WWW などを用い調査

6. **既発表論文のまとめ**: 前手順で調査した論文の要約作成

7. **報告書作成**: 全作業のまとめ

2　自己評価書の記述内容の解説 (妥当性検証)

2.1　応募者の主張

自己評価所中の差分解読法、及び線形解読法に関する記述は 2 〜 3 頁に記述されている部分のみである。主張は以下の通りである。

- 5 ビット固定長の回転が線形解読、差分解読を複雑にしている。
- 繰り返し特性や、線形近似を得難いので進んだ差分解読法や線形解読法を使ったとしても最高ラウンド数 20 の RC6 攻撃を行うのは困難。
- RC6-32/8/b(8 段 RC6) は差分解読法によりおよそ 2^{76} 組の選択平文で、線形解読法によりおよそ 2^{60} 既知平文データで攻撃できると推定。つまり、少ない段数の RC6 でも攻撃に必要なデータ量は膨大である。
- RC6 の 20 段の差分攻撃では、 6 段繰り返し特性の利用が適切に見える。それを利用して、18 段特性利用の攻撃成功確率は 2^{-264}。より進んだ方法により若干は必要データ量を減らせるが、 RC6 への攻撃は成功しないと考えている。
- 線形解読法については、 5 ビット位置分の固定回転を使わない 2 段繰り返し表現が有効。16 段の RC6 攻撃には約 2^{142} の既知平文が必要。追加技術の利用により 2^{128} より若干は減らせるが、 RC6 の攻撃はできない。
- RC6 に対して、線形解読を行なうには 18 段の線形近似式の利用が適切であるが、 2^{182} 個の既知平文が必要。これは取得可能データ量を越えていて、技術の改善があり数字がわずかに減ったとしても RC6 の攻撃はできないとの判断。
- 詳細は文献 [10] に記述。

2.2　評価者の解釈

前節の応募者の主張に関して、評価者の常識に照らし合わせたところ、問題点は発見できなかった。ただ、自己評価書中には根拠として文献 [10] があげられているだけなので、正確な妥当性検証は行なえなかった。文献 [10](本稿では [CRRY98]) については、次節の該当箇所を参照されたい。

2.3 既発表論文の調査・まとめ

RC5 は RC6 を元に設計されている。 RC5 の評価のうち、

- 構造的なもの
- 暗号要素 (加算など)

の評価は RC6 にそのまま適用可能であるが、暗号全体の安全性を評価するには不十分である。従って、 RC6 に全く触れられていない評価については調査対象外とした。

RC6 は AES 候補の一つであったので、 AES 評価期間中様々な評価を受けた。この節では、それらの論文を取り上げ概要を報告する。但し、 RC6 に関する評価は国内外を通じ多数発表されており、たとえ差分解読法および線形解読法関連に限ったとしても、膨大な量になるので、重要でないと思われる結果は省いてある。

[BGG+99, A.1 章] RC6 の攻撃法のちょっとしたアイディアがある。文献 [GHJV00] に詳細があるのでそちらを参照されたい。

[BPV99] 基本的に RC5 に関する結果で、 RC6 については RC5 の結果が使えるかどうかについて「一部は使えるようだが、全体については検討中」とのこと。

[CRRY98] RC6 の設計者自身による評価。記述の殆どが差分解読法と線形解読法に対する安全性評価である。 RC6 の簡易版に対する評価から始め、最終的には RC6 そのものの評価を行なっている。差分解読法については差分のとり方として、 $\mathrm{GF}(2)^n$ と $\mathbf{Z}/2^n\mathbf{Z}$ の両方で評価してある。評価では、 6 段以内の繰り返し特性 (表現) を用い特性確率を出している。さらに、いわゆる multiple path の評価も行なっているが、これは差分や線形 Markov 性が成り立たない場合にも成り立つと仮定しての評価であるのでどの程度意味があるのか疑問である。いずれにしても、解読者がまず手をつけるであろう差分解読法および線形解読法に対しては押えてあるが、最大差分 (線形) 特性確率、最大平均差分 (線形) 確率なりで、安全性が証明されているわけではない。最も攻撃が成功した場合でも 16 段 (仕様は 20 段) 辺りが限界であるとの結論である。

[CRRY99] [CRRY98] における RC6 の簡略版に関する攻撃の改良。色々な暗号要素が RC6 で如何にうまく働いているかを主張。

[CY99] RC6 設計者の一部による評価。データ依存巡回シフトの差分確率の性質解析。 RC6 でうまく使われていると主張。

[GHJV00] χ^2 攻撃。最も強力な攻撃は

段数 14 段

既知平文数 2^{118} ブロック

メモリ 2^{112} ブロック

計算量 2^{122} 暗号化時間

との記述。殆んど同じ技術を使った若干強力な攻撃 [KM00] も提案されている。

[KM00] χ^2 攻撃。最も強力な攻撃は

段数 15 段

選択平文数 $2^{111.0}$ ブロック

との記述。また鍵空間中の $1/2^{80}$ の弱鍵については

段数 17 段

選択平文数 $< 2^{118}$ ブロック

とある。 RC6 の設計者は、これらの攻撃について文献 [CRRY98] での線形解読での評価と殆んど同じと主張している [RRY00]。

3 まとめ

RC6 は AES 暗号だったこともあり、様々な評価が行なわれてきた。しかし、どの差分解読、および線形解読も RC6 の推奨パラメータである RC6-32/20/{16,24,32} については、理論的な意味でさえも攻撃に成功していない。

RC6 は AES で評価されたとはいえ、提案から 3 年ほどしか経過していないことや、最大攻撃可能段数 16 程度と仕様の 20 段との差がそれほどあるわけではないことから、数年のうちに理論的な解読法が発見されるかもしれない。但し、応募者が主張しているように 7 年程度の歴史がある RC5 の経験を元に、 RC6 の設計時には既に知られていた差分解読法、および線形解読法に対して安全になるように設計されているので、理論的な方法に限ってでさえ、 RC6 の差分解読や線形解読はかなり困難なことと思われる。

参考文献

[BGG+99] O. Baudron, H. Gilbert, L. Granboulan, H. Handschuh, A. Joux, P. Nguyen, F. Noilhan, D. Pointcheval, T. Pornin, G. Poupard, J. Stern, and S. Vaudenay. Report on the AES Candidates. In *Second Advanced Encryption Standard Candidate Conference*, pp. 53–67, Hotel Quirinale, Rome, Italy, 1999. Information Technology Laboratory, National Institute of Standards and Technology.

[BPV99] J. Borst, B. Preneel, and J. Vandewalle. Linear Cryptanalysis of RC5 and RC6. In L. R. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 16–30, Berlin, Heidelberg, New York, 1999. Springer-Verlag.

[CRRY98] S. Contini, R. L. Rivest, M. J. B. Robshaw, and Y. L. Yin. The Security of the RC6^{TM} Block Cipher. (`http://www.rsasecurity.com/rsalabs/rc6/index.html`), 1998.

[CRRY99] S. Contini, R. L. Rivest, M. J. B. Robshaw, and Y. L. Yin. Improved Analysis of Some Simplified Variants of RC6. In L. R. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 1–15, Berlin, Heidelberg, New York, 1999. Springer-Verlag.

[CY99] S. Contini and Y. L. Yin. On Differential Properties of Data-Dependent Rotations and Their Use in MARS and RC6. In *Second Advanced Encryption Standard Candidate Conference*, pp. 230–239, Hotel Quirinale, Rome, Italy, 1999. Information Technology Laboratory, National Institute of Standards and Technology.

[GHJV00] H. Gilbert, H. Handschuh, A. Joux, and S. Vaudenay. A Statistical Attack on RC6. In B. Schneier, editor, *preproceedings of Fast Software Encryption Workshop 2000 (FSE 2000)*, New York, New York, 2000.

[KM00] L. R. Knudsen and W. Meier. Correlations in RC6 with a reduced number of rounds. In B. Schneier, editor, *preproceedings of Fast Software Encryption Workshop 2000 (FSE 2000)*, New York, New York, 2000.

[RRY00] R. L. Rivest, M. J. B. Robshaw, and Y. L. Yin. The Case for RC6 as the AES. Public Comments on AES Candidate Algorithms - Round 2 (available at `http://csrc.nist.gov/encryption/aes/round2/pubcmnts.htm`), 2000.

全体概要

要約 RC6 の差分解読法および線形解読法に対する安全性評価結果をまとめる。最も有効な攻撃は応募者自身による線形 Markov 性を仮定した場合の 6 段繰り返し表現の multiple path による重ね合わせを使った場合で、 16 段程度まで攻撃できる。RC6 の推奨段数は 20 段であるので、現在のところ RC6 は差分解読法、および線形解読法に対して安全であると考えられる。

Abstract This report summarizes the security evaluation of RC6 against differential cryptanalysis and linear cryptanalysis. The best attack breaks RC6 up to about 16 rounds using a mix of 6-round iterative characteristics by so-called multiple paths, under the assumption that RC6 has a property of linear Markovness. Since the nominal rounds of RC6 is 20, RC6 seems currently secure against differential cryptanalysis and linear cryptanalysis.