ストリーム暗号RC4の
安全性評価

五十部　孝典　(神戸大学)

共同研究者
大東　俊博　(広島大学)
森井　昌克　(神戸大学)

協力者
塚畝　翼　(神戸大学)
長尾　篤　(神戸大学)
渡辺　優平　(神戸大学)

2012年11月

目 次

1 要旨

本稿では，ストリーム暗号 RC4 に対しての安全性評価結果を報告する．本評価では，主に以下の二つを行った．

1. RC4 に関してこれまで行われてきた安全性解析の調査.
2. SSL3.0/TLS1.0 以上で RC4 を利用する場合の安全性評価.

1.1 RC4 アルゴリズムに関する安全性解析

代表的なストリーム暗号アルゴリズムに対する攻撃としては，識別攻撃，内部状態復元攻撃，鍵回復攻撃，予測攻撃が挙げられる．これらの攻撃について現在の RC4 の解析状況について調査した．

識別攻撃は，キーストリームと呼ばれる出力系列を真性乱数と識別する攻撃であり，一つの鍵から生成されたキーストリームを用いる攻撃と複数の鍵から生成されたキーストリームの集合を用いる攻撃に分けられる．それぞれ，single key (strong) distinguisher, multiple key (weak) distinguisher と呼ばれる．RC4 に対しては，$2^{26.5}$ word のキーストリームを用いた single key distinguisher が最も効果的な攻撃として Mantin により提案されている [16]．また multiple key distinguisher として最も強力なものは，Mantin と Shamir により提案された 300 通りの異なる鍵から生成されたキーストリームの 2 byte 目を利用したものである [17]．この識別攻撃自体が現実的な安全性を脅かさないが，ストリーム暗号の出力が擬似乱数系列であることの安全性の前提が崩れてしまう．

内部状態復元攻撃はキーストリームから秘密鍵と等価な内部状態を求める攻撃である．ある時刻の内部状態を求めることができればそれ以降のキーストリームを求めることができる．内部状態の更新が可逆の場合は，それ以前のキーストリームも導出できる．RC4 に対しては，2^{241} の計算量でキーストリームから内部状態をすべて求めるアルゴリズムが Maximov と Khovratovich により提案されている [19]．これは，秘密鍵のサイズを 241 bit 以上にしても安全性が向上しないことを意味する．しかしながら，この攻撃は 128 bit key を用いた場合の安全性には直接影響しない．

鍵回復攻撃は，キーストリームから秘密鍵を直接求める攻撃である．キーストリームと秘密鍵間の相関を利用して，$2^{122.06}$ の計算量で 128 bit key を求めるアルゴリズムが Sepehrdad らにより提案されている [26]．この攻撃は偏りのあるキーストリームと秘密鍵間の関係式を用いて全数探索の効率化を行うタイプの攻撃で，このアプローチで現実的な計算量で攻撃可能になることは難しいと考えるが，全数探索と比較して大幅に攻撃計算量は削減されている．

予測攻撃は，出力であるキーストリームを予測する攻撃であり，代表的な攻撃として，Mantin の予測攻撃がある．この攻撃では，1 bit の予測が 2^{45} byte のキーストリームを使えば 85 パーセントの確率で成功し，1 byte の予測が 2^{50} byte のキーストリームを使えば 82 パーセントの確率で成功する [16].

その他の攻撃としては, Key collision に対する評価 [18, 5]，内部状態から秘密鍵を効果的に求める方法や [23, 2]，キーストリームから鍵長を求める方法 [12] なども提案されている．

以上のように，RC4 のアルゴリズム自体に対する解析は数多く行われているが，現実的な脅威になるような攻撃は現在のところ提案されていない．しかしながら，擬似乱数との識別が容易にでき，全数探索より十分効率的なアルゴリズムが提案されている事実より，厳密な意味で 128 bit security を擁しているとは言えない．

1.2 SSL3.0/TLS1.0 以上で RC4 を利用する場合の安全性評価

SSL3.0/TLS1.0 では，RC4 の秘密鍵は，master secret と呼ばれる共有秘密情報と乱数から, ハッシュ関数もしくは MAC 関数を用いて生成される．この鍵生成に関して解析を行ったが，脆弱性を見つけることができなかった．そこで本評価では，セッション毎に秘密鍵は random に生成されるものとした．RC4 の実装に対する攻撃としては WEP/WPA に対する攻撃が有名であるが，これらの攻撃は基本的には鍵の生成方法の脆弱性を利用した攻撃であるため，SSL3.0/TLS1.0 以上での RC4 に対しての適用は難しいと考える．

SSL3.0/TLS1.0 以上での RC4 を利用した場合の現実的な脅威となりうる攻撃として Broadcast setting での攻撃を考えた．これは，同じ平文をユーザ毎の秘密鍵を用いて暗号化して送る状況を想定する．この setting での攻撃としては，キーストリームの 2 byte 目が 0 になりやすいことを利用した Mantin と Shamir の攻撃がある [17]. この攻撃では $\Omega(N)$ のユーザ毎の鍵で生成された暗号文から，平文の 2 byte 目を特定することが可能である．ここで，N は RC4 の内部状態のサイズを表すパラメータであり, SSL/TLS では $N = 256$ のパラメータが用いられる．さらに，Maitra らにより $\Omega(N^3)$ のユーザ毎の鍵で生成された暗号文から，平文の 2–255 byte 目も高い確率で特定できることが示された [14]．しかし，上記の 2 つはあくまで理論的な評価であり，実際に Broadcast RC4 への安全性を考える場合，以下の疑問が残る．

1. これらの bias を用いた攻撃がもっとも強力な攻撃なのか.
2. 実際にこれらの bias のみで, 暗号文から平文を求めることができるのか.
3. [17, 14] の評価では, 攻撃で必要な暗号文数を下限で評価しているが，実際の攻撃ではどのくらいの暗号文が必要なのか.
4. 1 byte 目と 256 byte 以降の平文は求めることができるのか.

本評価では，Broadcast RC4 に対する更なる解析を行い，上記の質問に対して回答を与えた.

まず初めに，キーストリームの初めの 257 byte に関して, 既存の bias よりも強力ないくつかの bias を新たに見つけ, 証明を与えた．これらの新しい bias の

方が既存の bias より強くなる部分に関しては, これらのより強い bias の影響により，既存の bias のみを用いた場合, 平文を一意に決定することができない．そこで, 実際に平文復元攻撃を構成する際は，新しい bias と既存の bias をうまく組み合わせて使う必要がある．我々はこれらの bias を考慮した Broadcast RC4 への平文復元攻撃に最適な bias の set (**optimal bias set**) を導出した．optimal bias set はキーストリームの初めの 257 byte の最も強い bias の集合と考えることができる．

次に，上記の optimal bias set を用いて，実際に平文解読実験を計算機で行い，攻撃に必要な暗号文数を成功確率と共に見積もった．結果として，2^{32} 程度の異なる鍵で生成された暗号文があれば，optimal bias set を用いることにより, 確率 0.5 以上で平文の 1–257 byte の各 byte を復元できる．また 2^{24} 程度の暗号文数であっても，Z_1, Z_2, extended keylength-dependent bias などの強い bias の部分に関しては高確率で復元可能である．

さらに, 258 byte 以降の平文を効率よく求める方法を与えた．この手法は Matin により示された Digraph Repetition bias [16] と，本稿で求めた Z_1–Z_{257} の optimal bias set を組み合わせて，逐次的に求めていくものである．この手法を用いることにより，2^{34} 程度の暗号文から, 258 byte 以降の平文も暗号文のみから求めることができる．この Digraph Repetition bias は long term bias であるため, 258 byte 以降の任意の平文を求めることができる．理論的には，初めの 2^{50} bytes $\approx$ 1000 T bytes の平文は 2^{34} の異なる鍵で生成された暗号文から確率 0.97170. で導出可能である．

本評価では, Broadcast RC4 の実際的な安全性を評価するために, Broadcast setting での平文復元攻撃に最適な bias の set を導出し，計算機を用いて必要な暗号文数と成功確率を見積もった．結果として，Broadcast setting で RC4 を利用した場合は 2^{34} 程度の暗号文を集めることにより，2^{50} bytes $\approx$ 1000 T bytes の平文情報を暗号文のみから復元可能である．また 2^{24} 程度の暗号文であっても特定の平文 byte を高確率で求めることが可能である．さらに SSL/TLS の場合，session 毎に異なる鍵が生成されるため, Broadcast setting は Multi session attack としても考えることができる．Multi session attack では，攻撃対象の平文ブロックが繰り返し複数の session で同じ位置で用いられることを想定している [3]．よって，Broadcast setting，Multi session setting での RC4 の使用を用いる場合，上記の攻撃に注意が必要である．

2　ストリーム暗号 RC4 の構造

RC4 は 1987 年に RSA Data Security 社の Rivest によって開発された可変長鍵のストリーム暗号である．RC4 はソフトウェアによる高速処理性能に優れており，Adobe Acrobat や Lotus Notes などの商用のアプリケーションやインターネット用のプロトコルである SSL (Secure Sockets Layer) 3.0/TLS (Transport Layer Security) 1.0，無線 LAN 用のプロトコルである WEP (Wired Equivalent Privacy) 及び WPA (Wi-Fi Protected Access) などで広く使われており，最も使われているストリーム暗号の一つである．

RC4 は開発されて以来，そのアルゴリズムは非公開であったが，1994 年にソースコードがインターネット上に匿名で流されて実質的に仕様が公開された形になった．しかしながら，RSA Data Security 社は公開されたコードを公式に RC4 と認めておらず，公開されたコードは ARC4(Alleged RC4) や arcfour と表記される RC4 と等価な動作をするアルゴリズムとしてインターネット上で公開されている．本評価では，ARC4 のアルゴリズムを RC4 とみなした上で安全性を評価を行う．

RC4 は可変長の秘密鍵 K を用いる．鍵長は 8 bit から 2048 bit の間で選択できる．RC4 の内部状態 S は $N(=2^n)$ 個の要素の置換からなり，それぞれの要素は n ビットの変数である．n は RC4 が処理単位 (ワード長) である．また，RC4 は内部状態の更新で 2 つのポインタ i，j を用いており，それぞれ n bit の変数である．SSL3.0/TLS1.0 以上では 鍵長は 128 bit，$n = 8$，$N = 256$ が使われているため，本評価ではこのパラメータのみを扱う．

RC4 のアルゴリズムは鍵スケジューリングアルゴリズム (KSA : Key Scheduling Algorithm) と擬似乱数生成アルゴリズム (PRNG : Pseudo Random Number Generator) から構成される．鍵スケジューリングアルゴリズムでは，秘密鍵から N 個の要素の置換で構成される内部状態を生成する．擬似乱数生成アルゴリズムでは，内部状態を更新しながら 1 word 単位でキーストリーム Z_1, ..., Z_r, ... を生成する．ここで，r は PRGA のラウンド数である．Z_r は平文の r 番目の word P_r と XOR されて，暗号文の r 番目の word C_r を生成する．RC4 のアルゴリズムは Algorithm 1 に示す．ここで，$+$ は N を法とした算術加算である．

Algorithm 1 RC4 Algorithm

KSA(K)**:**

for $i = 0$ to $N - 1$ **do**
  $S[i] \leftarrow i$
end for
$j \leftarrow 0$
for $i = 0$ to $N - 1$ **do**
  $j \leftarrow j + S[i] + K[i \bmod l]$
  Swap $S[i]$ and $S[j]$
end for

PRGA(K)**:**

$i \leftarrow 0$
$j \leftarrow 0$
$S \leftarrow KSA(K)$
loop
  $i \leftarrow i + 1$
  $j \leftarrow j + S[i]$
  Swap $S[i]$ and $S[j]$
  Output $Z \leftarrow S[S[i] + S[j]]$
end loop

3 RC4の安全性について

本章では, 代表的なストリーム暗号アルゴリズムに対する攻撃である識別攻撃, 内部状態復元攻撃，鍵回復攻撃，予測攻撃を中心に既存の結果について述べる. いくつかの結果に関しては，追試を行い，実験的にサポートした. また今回新たに見つけた解析結果もいくつか加える.

3.1 識別攻撃

キーストリームを真性乱数と識別する識別攻撃は，multiple key distinguisher と single key distinguisher の 2 種類に分けられる.

3.1.1 Multiple Key Distinguisher

multiple key distinguisher は，複数の秘密鍵から生成されたキーストリームの集合を対象にした distinguisher である．RC4 に対する multiple key distingusher としては, FSE 2001 に Mantin と Shamir の提案したキーストリームの 2 byte 目の Z_2 の bias を利用したものがある [17]．この攻撃では，$Z_2 = 0$ になる確率が random な場合の 1/256 と比較して 2 倍高い 2/256 である bias を利用している. これは内部状態が特定の条件を満たしている場合に確率 1 で $Z_2 = 0$ のイベントが発生するためであり，理論的にも証明されている．文献 [17] では，識別に必要な sample 数を見積もるための理論値を以下の定理で与えている.

Theorem 1. **[17]** 二つの分布 X と Y において，*event* e の起こる確率が X では p, Y では $p(1+q)$ である場合，$O(1/pq^2)$ の *sample* があれば，*constant probability of success* で X と Y を識別可能である.

上記のケースでは，e をキーストリームの 2 byte 目が 0 とし，X を真性乱数の分布, Y を RC4 の出力の分布とすると，$p = 1/256$, $q = 1$ となる．ここで q は relative bias と呼ばれる．Theorem 1 より，この bias を利用すると約 200 通りの異なる鍵で暗号化された Z_2 の集合があれば，真性乱数と 0.64 の確率で識別することが可能である．また，キーストリームの 1 byte 目の bias を利用した攻撃も, CRYPTO 2002 で Mironov により提案されている [20]．これは理論的な証明はなく，実験的に Z_1 の分布に偏りがあることを求めており，この偏った分布を用いることにより，約 1700 通りの異なる鍵で暗号化された Z_1 の集合があれば，真性乱数と高確率で識別することが可能である．この bias の理論的な証明は 2011 年に Sen Gupta らによって行われた [11]. これらの攻撃は初めの数 byte のみを利用した攻撃であり, 初めの数 byte を破棄する実装の場合は防ぐことができる.

FSE 2004 で, Paul と Preneel は，初めの数 byte を捨てても識別攻撃を実行可能な bias を発見した [24]．これは，Z_{r+1} と Z_{r+2} $(r = 0 \bmod 256)$ において $Z_{r+1} = Z_{r+2}$ になる確率が random な場合と比較して，成立しにくい bias であ

表 1: $Z_{r+1} = Z_{r+2} \quad (r = 0 \bmod 256)$ の negative bias [24] の実験値

Z_{r+1}	Z_{r+2}	$Z_{r+1} = Z_{r+2}$ になる確率	relative bias q	$1/pq^2$ (log 2)
1	2	0.0038903282	-0.0040759808	23.87727406
257	258	0.0039051189	-0.0002895616	31.50768417
513	514	0.0039062651	0.0000038656	43.96175242
769	770	0.0039063384	0.0000226304	38.86275678
1025	1026	0.0039063974	0.0000377344	37.38752028
1281	1282	0.0039064339	0.0000470784	36.74915037
1537	1538	0.0039064805	0.0000590080	36.09745983
1793	1794	0.0039062736	0.0000060416	42.6732758
2049	2050	0.0039063195	0.0000177920	39.55682356
2305	2306	0.0039063602	0.0000282112	38.22674488
2561	2562	0.0039063480	0.0000250880	38.56528602
2817	2817	0.0039062629	0.0000033024	44.41610739
3073	3074	0.0039063370	0.0000222720	38.90881872
3329	3330	0.0039062725	0.0000057600	42.81099952
3585	3586	0.0039063775	0.0000326400	37.80599883
3841	3842	0.0039062429	-0.0000018176	46.13906766
4097	4098	0.0039062867	0.0000093952	41.39928939

る．理論的には，$Z_1 = Z_2$ になる確率は，$1/256 \cdot (1 - 1/256)$ であり，$r > 256$ においては，$1/256 \cdot (1 - 1/256^2)$ になる．Theorem 1 より，Z_1 と Z_2 では約 $2^{24} (= 2^8 \cdot 2^{8\times 2})$ の sample で，$r > 256$ においては約 $2^{40} (= 2^8 \cdot 2^{16\times 2})$ の sample で理論的には識別可能である．しかしながら，実験的には Z_{257} と Z_{258} の場合は 2^{32} で識別可能であったことが報告されている [24]．これは，関連する特定のイベントが起きやすいことに起因しているが，理論的な理由はわかっていない．我々は詳細にこの nagative bias を見積もるために，2^{40} の random に生成した秘密鍵を用いて計算機実験を行った．表 1 に実験結果を示す．表 1 より， Z_1 と Z_2 においては理論値通りの値で識別可能であり．Z_{257} と Z_{258} の場合には，[24] と同様に理論値より非常に高い bias が観測されている．それ以降に関しては，理論的には -2^{-16} 程度の negative relative bias が検出されるべきであるが，実験では観測できなかった．これは 2^{40} 以上の sample 数が必要な bias であるため，実験の sample 数が十分でないことも原因だと考えられる．ただ, この実験により, Z_{513} と Z_{514} から Z_{4097} と Z_{4098} では，$Z_{r+1} \neq Z_{r+2}$ のイベントの bias を利用した場合, 少なくとも 2^{40} の sample では識別することが難しいことを示唆している．

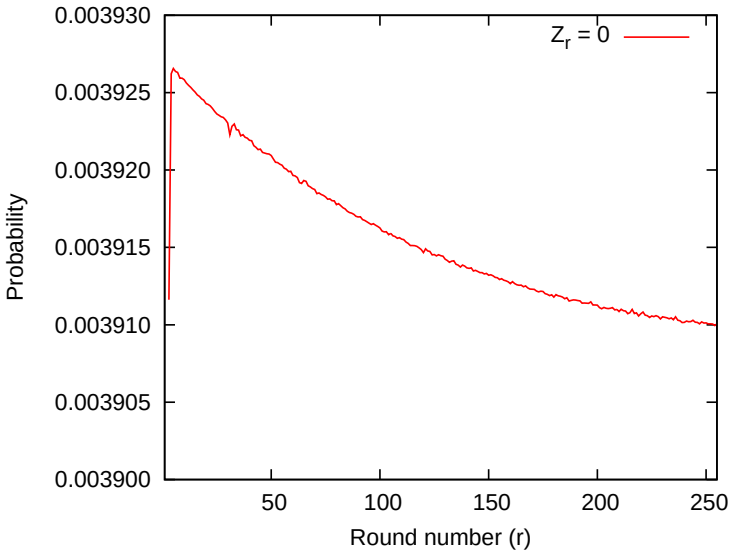


図 1: $Z_r = 0$ bias の実験値 $(1 \leq r \leq 255)$

表 2: $Z_r = 0 \quad (r = 256, 257)$ の実験値

Z_r	0 になる確率	relative bias q	$1/pq^2$ (log 2)
256	0.0039004963	−0.0014729472	26.81415714
257	0.0039115301	0.0013517056	27.06200663

FSE 2011 で Maitra らは，出力の 3 byte 目から 255 byte 目の bias を発見した [14]．出力の 2 byte 目が 0 に偏っていることはすでに Mantin と Shamir により示されていたが，文献 [17] では 2 byte 目以降では同様の bias は存在しないと予想されていた．しかしながら，実際には 3 byte 目から 255 byte 目も同様に 0 に偏っていることを実験的も理論的にも示した [14]．これらを使用することで 2^{24} の sample で理論的には真性乱数と識別できる．図 1 に 2^{40} の random に生成した秘密鍵を用いた実験値を示す．

我々はさらに 2^{40} の random に生成した秘密鍵を用いて計算機実験を行い，表 2 の新しい 0 に関する bias を発見した．これらを用いることにより，256 と 257 byte 目も攻撃に使うことが可能になる．この bias に関する理論的な証明はないが，それぞれ $2^{26.8}$ と $2^{27.0}$ の sample で識別できるため，最初の 255 byte を捨てた実装にも対して最も強力な multiple key distinguisher になる．

3.1.2 Single Key Distinguisher

Single key distinguisher はランダムに選ばれた一つの秘密鍵から生成されたキーストリームを真性乱数と識別する攻撃である．EUROCRYPT 1997 で Golic は Z_r と Z_{r+2} の最下位ビット間に相関があることを示し，$2^{44.7}$ byte のキーストリームの観測によって実行可能な識別攻撃を提案した [10]．FSE 2000 で, Fluhrer と McGrew によって Golic の方法が改良され，Z_r と Z_{r+1} 間の相関 (Digraph) を利用することで必要なキーストリームの byte 数を $2^{30.6}$ word まで減少させている [8]．さらに EUROCRYPT 2005 で, Mantin が Digraph の概念をさらに拡張した Digraph Repetition Bias を提案し，必要なキースリーム byte 数を $2^{26.5}$ word に削減した．これらは，初期キーストリームにのみ発生する bias ではなく，任意の bias において発生する bias であり, long term bias と呼ばれる．そのため，初期のキーストリームを捨てる実装においても有効な攻撃である．

3.2 内部状態復元攻撃

内部状態復元攻撃はキーストリームから秘密鍵と等価な内部状態を求める攻撃である．ASIACRYPT 1998 で Knudsen らによって RC4 に対する内部状態復元攻撃が提案された [13]．ここで, 内部状態は $N = 256$ の場合，256 の置換と 1 byte の 2 つの pointer i と j で構成されるため，全数探索の計算量は $2^{1700}(\approx 256!)$ と見積もられる, Knudsen らの方法はキーストリームを利用する枝刈りを備えた木探索アルゴリズムであり，攻撃に要する計算量は初期状態の全数探索の平方根程度である 2^{779} まで削減される．具体的にはキーストリームと内部状態で成立する $S_r^{-1}[Z_r] = (S_{r-1}[i_r] + S_{r-1}[j_r])$ mod 256 の検査式を用いて効率的に求めていく．白石らは Knudsen らの木探索アルゴリズムを深さ優先探索に修正することで計算量を削減している [28].

CRYPTO 2008 で Miximov と Khovratovich により, Knudsen らの攻撃を改良した新しい攻撃方法が提案された [19]．この攻撃では，d-order w-generative pattern と呼ばれる特定のキーストリームのパターンを利用して 2^{241} の計算量でキーストリームから内部状態をすべて求めることができる．これは，秘密鍵のサイズを 241 bit 以上にしても安全性が向上しないことを意味する．しかしながらこれ以下の鍵長に関しては安全性の影響はない.

3.3 鍵回復攻撃

鍵回復攻撃は，キーストリームから秘密鍵を求める攻撃である．SAC 2010 で, Sepehrdad らによりキーストリームと内部状態間, 秘密鍵間の相関を利用して，$2^{122.06}$ の計算量で秘密鍵を求めるアルゴリズムが提案されている [26]．この攻撃は偏りのあるキーストリームと秘密鍵間の関係式を用いて全数探索の効率化を行うタイプの攻撃で，このアプローチで Practical な計算量で攻撃可能になることは難しいと考えるが，全数探索と比較して大幅に攻撃計算量は削減されている．

Weak key に基づく鍵回復攻撃もいくつか提案されている．Weak key とは，鍵空間の一部に存在している鍵の集合であり，今回のケースでは，全数探索よりも効率的に鍵回復攻撃を実行することが可能な特殊な鍵のクラスである．1995 年，Roos が特定の鍵においてキーストリームの先頭と鍵の先頭 byte に強い相関があることを発見し，weak key として定義した [25]．鍵空間全体のうち $2^{-10.9}$ の割合で Roos の weak key が存在し，この鍵においては鍵探索の際に 16 bit 分の探索を省略することができる．よって Roos の weak key を利用する攻撃では，鍵の探索において $2^{5.1}$ $(= 2^{16}/2^{10.9})$ bit 分の利得がある．さらに 2011 年，寺村らが predictive state を用いた weak key を定義し，Roos の weak key もこれに包括されることを示した [29]．Predictive state とは，FSE 2001 で Mantin と Shamir により示された PRGA における部分的な内部状態からいくつかのキーストリームが予測できる特殊な内部状態である [17]．a word の内部状態から b word のキーストリームが予測できるとき，これを b-predictive a-state と呼ぶ．寺村らは predictive state を導く鍵の条件を導出し，weak key として再定義した．寺村らの weak key の能力は predictive state のパラメータ a, b に依存する．特に 5-predictive 5-state を用いた攻撃の場合，特定のキーストリームを得る鍵のうち確率 $2^{-7.1}$ で weak key が存在し，秘密鍵の 40bit 分の探索を省略できる．鍵探索における利得は $2^{32.9}$ bit 分あり，特定のキーストリームに対して $2^{95.1}$ の計算量で 128 bit 鍵を回復することができる．ただし，この攻撃は特定のキーストリームが観測された場合に実行される攻撃である点が Roos の Weak key とは異なる．

我々は, さらに predictive state を用いる weak key の拡張を行い，同時に weak key の総数を導出した．まず寺村らの定義した weak key 以外にも predictive state を導く鍵が存在することを発見し，新たな weak key とした．また，weak key の数はこれまで深く議論されていなかったが，今回その総数についても明確にした．我々の定義した weak key はこれまで提案された寺村らの weak key，Roos の weak key を全て内包しており，その総数は $2^{118.58}$ になる．この詳細に関しては文献 [21, 22] を参照されたい.

3.4 予測攻撃

予測攻撃は，出力であるキーストリームを予測する攻撃であり，代表的な攻撃として，EUROCRYPT 2005 で提案された Mantin の予測攻撃がある．この攻撃では， Recyclable Fortuitous State と呼ばれる state を利用し, 1 bit の予測が 2^{45} byte のキーストリームを使えば 85 パーセントの確率で成功し，1 byte の予測が 2^{50} byte のキーストリームを使えば 82 パーセントの確率で成功する [16].

3.5 その他の性質

その他の攻撃としては, Key collision に対する評価 [18, 5]，内部状態から秘密鍵を効果的に求める方法や [23, 2]，キーストリームから鍵長を求める方法 [12] なども提案されている．

FSE 2009 で松井により, RC4 の Key collision に関する評価が提案された [18]. Key Collision とは，同じキーストリームを生成する異なる鍵のことを表し，一般的には等価鍵と呼ばれる．RC4 において, pointer を除いた内部状態は $2^{1684}(\approx 256!)$ であるため, birthday paradox により, 鍵長が 105 byte 以上の場合は理想的な KSA であっても collision は発生するが，RC4 の場合は 17 byte key であっても存在することが理論的に示された． また実験的にも 24 byte の collision pair が実際に示された．この攻撃は Chen らにより一般化され [5], この攻撃は関連鍵攻撃により鍵回復攻撃に利用できることも示された [4].

SAC 2007 で Paul らにより KSA の解析として，内部状態から秘密鍵を効果的に求める方法が提案された [23]．これは，FSE 2008 で Biham らにより更なる攻撃の改良が行われた [2]．この攻撃は，攻撃者が内部状態を知っていることが前提の攻撃であるため，直接的には RC4 の安全性には影響しない.

SAC 2011 で Sen Gupta らにより，鍵の長さに依存した key dependent bias が提案された [12]．この bias を利用することにより, キーストリームから鍵長を求めることができる.

3.6 RC4 の既存攻撃のまとめ

以上のように，RC4 のアルゴリズム自体に対する解析はアルゴリズムが公開され以降, 数多く行われているが，現実的な脅威になるような攻撃は現在のところ提案されていない．しかしながら，擬似乱数との識別が容易にでき，全数探索より十分効率的なアルゴリズムが提案されている事実より，厳密な意味で 128 bit security を擁しているとは言えない.

4 RC4 を SSL3.0/TLS1.0 以上で用いた場合の安全性について

本章では，暗号アルゴリズムとして RC4 を実際に SSL3.0/TLS1.0 に用いた場合の安全性について評価する．

4.1 SSL3.0/TLS1.0 での RC4 の利用方法

SSL3.0/TLS1.0 では，初めに公開鍵ベースの Handshake プロトコルを行い，*master secret* と呼ばれる 48 byte の秘密情報を共有する．そのあとに，その値と乱数からハッシュ関数（MD5, SHA-1）もしくは MAC 関数 (HMAC) 用いて用途別の session key, 初期ベクトル (IV) を生成する．この鍵生成に関して解析を行ったが，脆弱性を見つけることができなかった．そこで本評価では，セッション毎に RC4 で用いられる秘密鍵は random に与えられるものとした．鍵の生成の詳細については以下の文献を参照されたい [9, 6]

4.2 WEP/WPA に対して行われた攻撃の適用可能性

WEP/WPA は RC4 を利用した無線 LAN におけるセキュリティプロトコルである．しかしながら, WEP は 2001 年に Fluhrer, Mantin, Shamir により脆弱性を指摘されて以降 [7], 多くの攻撃方法が提案されており, 致命的な欠陥を持つプロトコルである．その中でも強力な攻撃として, SAC 2007 で Vaudenay と Vuagnoux により提案された VX attack が挙げられる [30]．VX attack は並列して WEP 鍵の和を計算することができる攻撃であるため，効率的に WEP 鍵を回復することが可能となる．ここで WEP は IV と WEP 鍵をビット連結することで秘密鍵を生成し，IV はパケットごとに異なる値が使用される．さらにこれを改良した攻撃が SAC 2010 で Sepehrdad らにより提案され，通信路上のパケットを 9,800 個観測することで確率 0.5 で WEP 鍵が回復されてしまう [26]．この攻撃では新たな攻撃式を提案することでより多くの WEP 鍵の候補値を計算することができる．

また EUROCRYPT 2011 において，4,000 個のパケットを観測するだけで WEP 鍵を回復する攻撃が Sepehrdad らによって提案された [27]．このとき WEP 鍵の回復に成功する確率は 0.5 である．この攻撃は既知の複数の bias を効果的に利用し, 正しい WEP 鍵を効率的に探索する．さらにこの方法を WPA の鍵探索に適用することができ，2^{38} 個のパケットを利用することで 128 bit の Temporal Key を回復することができる．ただし鍵回復に要する計算量は 2^{96} である．ここで Temporal Key は WPA において暗号化と復号の際に利用される鍵であり，事前に共有した秘密鍵から生成される．

以上のように WEP/WPA に対しては様々な攻撃方法が提案されており，無線 LAN においてこれらのセキュリティプロトコルでは，安全に通信を行うことは難しいと考えられる．一方でこれらの攻撃は基本的には秘密鍵の生成方法の脆弱

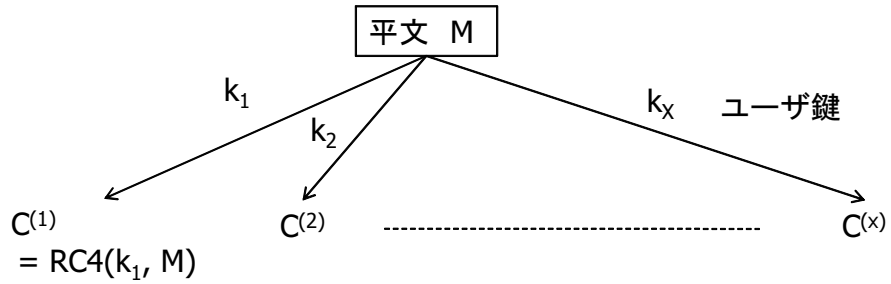


図 2: Broadcast Setting

性を利用した攻撃であるため，SSL3.0/TLS1.0 以上での RC4 に対しての適用は難しいと考える．

4.3 Broadcast setting での RC4 の安全性

SSL3.0/TLS1.0 以上での RC4 で現実的な脅威となりうる攻撃として Broadcast setting での攻撃が考えられる．Broadcast setting では，同じ平文を異なる秘密鍵を用いて暗号化して送る場合を想定する．本稿では，この Broadcast setting での RC4 のことを Broadcast RC4 と呼ぶ．図 2 に Broadcast setting の概要を示す．この setting は，コンテンツをユーザ毎の秘密鍵で暗号化して SSL/TLS で送る場合などが，実際のユースケースとして考えられる．

Broadcast RC4 への攻撃は，FSE 2001 に Mantin と Shamir により初めて示された [17]．この攻撃は, mulitple key distinguisher でも利用されたキーストリームの 2 byte 目が 0 になりやすい bias を利用している．この bias を利用することで, $\Omega(N)$ のユーザ毎の鍵で生成された暗号文があれば，平文の 2 byte 目を特定することが理論的に可能である．さらに，FSE2011 で, Maitra らにより $\Omega(N^3)$ のユーザ毎の鍵で生成された暗号文があれば，平文の 2–255 byte 目を特定することができることが理論的に示された [14]．以下これらの攻撃についての詳細を述べる．

4.3.1 Mantin-Shamir Attack

Mantin-Shamir Attack で用いている bias は以下の Theorem で与えられる．

Theorem 2. **[17]** *KSA* の後の *PRNG* の初期状態が $\{0 \dots N-1\}$ の置換の集合から *random* に選ばれた場合*,* キーストリームの *2 byte* 目が *0* になる確率は約 $\frac{2}{N}$ である*.*

$N = 256$ の場合, $\frac{2}{256}$ となる．この bias を用いて Broadcast RC4 への攻撃は次の Theorem で与えられる．

Theorem 3. [17] 一通りの平文 M に対して, k 通りの秘密鍵を用いて $RC4$ で暗号化された暗号文を $C^{(1)}\dots C^{(k)}$ とする. $k=\Omega(N)$ のとき, $C^{(1)}\dots C^{(k)}$ のみから M の *2 byte* 目を導出することが可能である.

これは, Theorem 1 の識別攻撃の成功確率より見積もられている. $C_i=P_i\oplus Z_i$ の関係式より, $Z_2=0$ の場合, $C_2=P_2$ が成立する. ここで Theorem 2 より, $Z_2=0$ は 2 倍の確率で発生する. よって, $k=\Omega(N)$ の C に対して, C_2 を値毎に count up して, 最も多く count された C_2 を P_2 とする. $N=256$ の場合, 2^8 通りの以上の random に生成された秘密鍵で生成された暗号文のみから平文の 2 byte 目を高確率で特定できる.

4.3.2 MPS 攻撃

FSE2011 で Maitra らにより, Z_2 以外の Z_3-Z_{255} も同様に 0 に bias していることが示された [14]. Mantin-Shamir の論文では, KSA の後の内部状態が random に N の置換の集合から選択されると仮定しているが, Maitra らは KSA の後の内部状態に bias があることを利用している. 具体的には Mantin の示した以下の KSA 後の bias を利用している.

Proposition 1. [15] *KSA* のあと, $0\le u\le N-1, 0\le v\le N-1$ に対して以下が成立する.

$$\Pr(S_0[u]=v)=\begin{cases}\frac{1}{N}\cdot\left((\frac{N-1}{N})^v+(1-(\frac{N-1}{N})^v)\cdot(\frac{N-1}{N})^{N-u-1}\right) & (v\le u)\\ \frac{1}{N}\cdot\left((\frac{N-1}{N})^{N-u-1}+(\frac{N-1}{N})^v\right) & (v>u).\end{cases}$$

また, この bias を考慮したときに, PRNG での $S_{r-1}[r]=r$ に関する bias は次の Lemma で与えられる.

Lemma 1. [14] $r\le 3$, $S_{r-1}[r]=r$ になる確率 $p_{r-1,r}$ は,

$$\Pr(S_{r-1}[r]=r)\approx\Pr(S_0[r]=r)\cdot\left(\left(\frac{1}{N}\right)^{r-1}-\frac{1}{N}\right)+1/N.$$

このとき, $Z_r=r$ に関する bias は以下の Theorem で与えられる.

Theorem 4. [14] $3\le r\le 255$ において, r 番目の出力が *0* になる確率は

$$\Pr(Z_r=0)\approx\frac{1}{N}+\frac{c_r}{N^2}.$$

ここで c_r は以下の式で与えられる.

$$\begin{aligned}c_r &= \left(\left(\frac{N-1}{N}\right)^r+\left(\frac{N-1}{N}\right)^{N-r-1}-\left(\frac{N-1}{N}\right)^{N-1}\right)\cdot\\ &\quad\left(\left(\frac{N-1}{N}\right)^{r-2}-\frac{1}{N-1}\right)\end{aligned}$$

具体的な c_r の bound は以下の通りである.

Corollary 1. [14]

$$\frac{1}{N}+\frac{0.98490994}{N^2}\geq \Pr(Z_r=0)\geq \frac{1}{N}+\frac{0.36757467}{N^2}$$

以上より, これらの bias を用いることで, $N=256$ の場合, 2^{24} 通り以上の random に生成された秘密鍵で生成された暗号文のみから平文の 3–255 byte 目を高確率で特定できる.

上記の理論値については [11] で更なる詳細な評価が行われ更新された.

Lemma 2. [11] $r\leq 3$, $S_{r-1}[r]=r$ になる確率は, 次で与えられる.

$$\Pr(S_1[r]=r)\cdot\left(1-\frac{1}{N}\right)^{r-2}+\sum_{t=2}^{r-1}\sum_{k=0}^{r-t}\frac{\Pr(S_1[t]=r)}{k!\cdot N}\cdot\left(\frac{r-t-1}{N}\right)^{k}\cdot\left(1-\frac{1}{N}\right)^{r-3-k}$$

ここで, $\Pr(S_1[t]=r)$ は以下で与えられる.

$$\Pr(S_1[t]=r)=\begin{cases}\sum_{X=0}^{N-1}\Pr(S_0[1]=X\wedge S_0[X]=r) & (t=1)\\ \Pr(S_0[1]=r)+\sum_{w\neq r}\Pr(S_0[1]=w\wedge S_0[r]=r) & (t=r)\\ \sum_{w\neq t}\Pr(S_0[1]=w\wedge S_0[t]=r) & (t\neq 1,r).\end{cases}$$

このとき, $Z_r=r$ に関する bias は以下の Theorem で与えられる.

Theorem 5. [11] $3\leq r\leq 255$ において, r 番目の出力が *0* になる確率は

$$\Pr(Z_r=0)\approx\frac{1}{N}+\frac{c_r}{N^2}.$$

ここで $c_r=\frac{N}{N-1}[N\cdot\Pr(S_{r-1}[r]=r)-1]$.

以上より, Broadcast RC4 への攻撃としては MS 攻撃と MPS 攻撃を用いることにより, 2^{24} 以上の暗号文を与えられた場合に平文の 2–255 byte を求めることができる.

5 すべての平文情報を導出可能なBroadcast RC4への暗号文単独攻撃

本章では，Broadcast RC4 に対する更なる安全性の評価を行う．具体的には新しい Broadcast RC4 への攻撃手法を提案する．

5.1 はじめに

Broadcast RC4 への攻撃としては，Mantin-Shamir の攻撃と Maitra らによる攻撃が知られている．FSE 2001 で，Mantin と Shamir によってキーストリームの 2 byte 目 Z_2 の bias を利用した Broadcast RC4 への攻撃が初めて提案された [17]．この攻撃では Z_2 が 0 になりやすいことを利用し，1 種類の平文に対して，$\Omega(N)$ の異なる鍵で生成された暗号文を集めることにより，平文の 2 byte 目が特定できることが示された．さらに，FSE 2011 で Maitra らにより，Z_3–Z_{255} も 0 に bias することが示され，$\Omega(N^3)$ の異なる鍵で暗号化された暗号文から平文の 3 byte 目から 255 byte 目も同様に導出できることが示された [14].

しかしながら，これらは RC4 の bias についてのあくまで理論的な結果であり，これらをもとに実際の Broadcast RC4 に対する平文復元攻撃に応用する際には以下の疑問点が挙げられる．

1. これらの bias を用いた攻撃がもっとも強力なのか?
2. 実際にこれらの bias のみで, 暗号文から平文を求めることができるのか?
3. [17, 14] の評価では, 攻撃で必要な暗号文数を下限 (Ω) で評価しているが, 実際の攻撃ではどのくらいの暗号文が必要なのか?
4. 1 byte 目と 256 byte 以降の平文は求めることができるのか?

本章では, 上記のすべての疑問に対しての回答を与える．まず，$Z_2 = 0$ のときの Z_1 に関する新しい条件付き bias を提案し, 証明を与える．この bias を Mantin と Shamir の $Z_2 = 0$ の bias と組み合わせて使うことで，理論的には 2^{17} 以上の暗号文で平文の 1, 2 byte 目を導出することができる．1 byte 目に関しては，bias があることはすでに実験的にも理論的にも示させていたが [20, 11]，これを用いてどうのように効果的に平文復元攻撃に応用できるかは分かっていなかった．直接的にこの bias を用いた攻撃を構成すると 2^{24} 以上のデータが必要になることが予想される．そのため，この bias は $1/2^7$ のデータ量の約 2^{17} で導出できるため，Broadcast RC4 に対する非常に有効な bias である．

さらに，Z_3–Z_{255} においては $Z_r = 0$ よりも大きな 3 つの新しい bias $Z_3 = 131$, $Z_r = r$ と extended keylength-dependent bias を示す．ここで, extended keylength-dependent bias は SAC 2011 で証明された keylength-dependent bias [12] を拡張した新しい bias である．これらの新しい bias については理論的考察を与え, さらに実験的も正しいことを確認した．これらの新しい bias の方が $Z_r = 0$

bias より強くなる部分に関しては, $Z_r = 0$ bias のみを用いると新しい bias の影響により，平文を一意に決定できない．そこで, 実際に平文復元攻撃を構成する際は，これらの新しい bias と $Z_r = 0$ bias をうまく組み合わせて使う必要がある．我々はこれらの bias を考慮した平文復元攻撃に最適な bias の set (**optimal bias set**) を導出した．また, 理論的な証明はないが Z_{256} と Z_{257} に関して実験的に攻撃に有効な bias を発見し， optimal bias set に加えた．具体的には，optimal bias set はキーストリームの初めの 257 byte の各 byte における最も強い bias の集合である．

次に，上記の optimal bias set を用いて，実際に平文解読実験を計算機で行い，攻撃に必要な sample 数 (暗号文数) を成功確率と共に見積もる．結果として，2^{32} 程度の異なる鍵で生成された暗号文があれば，optimal bias set を用いることにより, 確率 0.5 以上で平文の 1–257 byte 目の各 byte を復元できる．1,2 byte 目や extended keylength-dependent bias などのさらに確率の高い bias は 2^{24} 程度の暗号文からでも高確率で推測することが可能である．

最後に, 258 byte 以降を効率よく求める方法を提案する．この方法は EUROCRYPT 2005 で Matin により示された Digraph Repetition bias [16] と，本稿で求めた Z_1–Z_{257} の optimal bias set を組み合わせて，逐次的に求めていくものである．この手法を用いることにより，2^{34} 程度の暗号文から 258 以降の平文も求めることができる．ここで，この Digraph Repetition bias は, long term bias であるため，258 byte 以降の任意のすべての平文を暗号文から求めることができる．また, これらの正当性も計算機実験で検証した．

以上より，本稿で, 我々が提案する Broadcast RC4 に対する攻撃はすべての平文情報が暗号文のみから求めることができる初めての Full Plaintext Recovery Attack である．

5.2 キーストリームの新しい Bias

本章では, Broadcast RC4 への攻撃に有効な 4 つの新しい bias, $Z_1 = 0|Z_2 = 0$, $Z_3 = 131$, $Z_r = r$ と extended keylength-dependent bias を説明する. $Z_1 = 0|Z_2 = 0$ bias は, 既知の $Z_2 = 0$ bias と組み合わせて用いることにより, P_1 を 2^{17} 通りの暗号文から求めることができる強力な bias である. $Z_3 = 131$, $Z_r = r$ と extended keylength-dependent bias は, Z_3–Z_{255} においては既知の $Z_r = 0$ よりも大きな 3 つの新しい bias である. まず, 各 bias に対しては理論な証明をして与えて, 実験値と比較して正当性を確認する. その後にこれらの特性を考慮して $Z_1 \dots Z_{255}$ に関する bias の中から, Broadcast RC4 への攻撃に最適な set (**optimal bias set**) を提案する.

5.2.1 Bias of $Z_1 = 0|Z_2 = 0$

$Z_2 = 0$ のときの Z_1 に関する新しい条件付き bias を提案する. この bias を用いることで, 平文の 1 byte 目に関する効率的な攻撃を構成することができる. さらにこの性質をうまく利用することで, 暗号文単独での key の推測攻撃も可能である.

まず, $Z_2 = 0$ のときの Z_1 に関する新しい条件付き bias を以下の Theorem より与える.

Theorem 6. $\Pr(Z_1 = 0|Z_2 = 0)$ は

$$\Pr(Z_1 = 0|Z_2 = 0) \approx \frac{1}{2} \cdot \left(\Pr(S_0[1] = 1) + (1 - \Pr(S_0[1] = 1)) \cdot \frac{1}{N}\right) + \frac{1}{2} \cdot \frac{1}{N}$$

である.

Proof. 次の 2 つの case について考える.

- $S_0[2] = 0$
  文献 [17] より, $\Pr(S_0[2]|Z_2 = 0) \approx \frac{1}{2}$ であるため, $Z_2 = 0$ が観測された場合は, $\Pr(S_0[2] = 0) = \frac{1}{2}$.
  ここで, $S_0[1] = 1$ と仮定すると, $i = 1$ において $j = S_0[i] = S_0[1] = 1$ となる. このとき,
  $$Z_1 = S_0[S_0[i] + S_0[j]] = S_0[S_0[1] + S_0[1]] = S_0[2] = 0,$$
  となる. 図 3 にこのイベントを示す.
  $S_0[1] \neq 1$ の場合に $Z_1 = 0$ になる確率が $\frac{1}{N}$ であるとすると
  $$\Pr(Z_1 = 0|S_0[2] = 0) = \frac{1}{2}(\Pr(S_0[1] = 1) + (1 - \Pr(S_0[1] = 1))\frac{1}{N}).$$
- $S_0[2] \neq 0$
  場合に $Z_1 = 0$ になる確率が $\frac{1}{N}$ であるとすると,
  $$\Pr(Z_1 = 0|S_0[2] \neq 0) = \frac{1}{2} \cdot \frac{1}{N}.$$

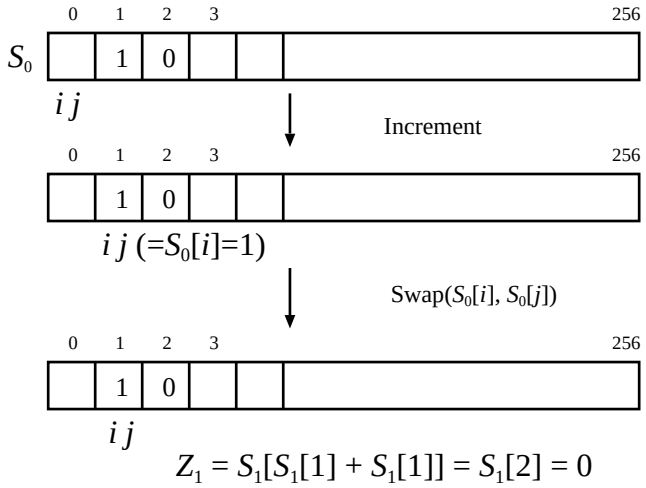


図 3: $Z_1 = 0|Z_2 = 0$ の Event

以上より,

$$\Pr(Z_1 = 0|Z_2 = 0) \approx \frac{1}{2} \cdot \left(\Pr(S_0[1] = 1) + (1 - \Pr(S_0[1] = 1)) \cdot \frac{1}{N}\right) + \frac{1}{2} \cdot \frac{1}{N}.$$

□

ここで, $N = 256$ のケースについて考える. $\Pr(S_0[1] = 1)$ は, Proposition 1 より求めることができ,

$$\Pr(S_0[1] = 1) = \frac{1}{256}\left(\left(\frac{1}{256}\right) + \left(1 - \left(\frac{1}{256}\right)\right)\left(\frac{1}{256}\right)^{254}\right) = 0.0038966.$$

よって,

$$\begin{aligned}\Pr(Z_1 = 0|Z_2 = 0) &= \frac{1}{2}(\Pr(S_0[1] = 1) + (1 - \Pr(S_0[1] = 1))\frac{1}{256}) + \frac{1}{2} \cdot \frac{1}{256} \\ &= 0.0058470 = 2^{-7.418} = 2^{-8} \cdot (1 + 2^{-1.009}).\end{aligned}$$

2^{40} の random に選択 key から生成された keystream による実験した結果, 実験値は $0.0058109 = 2^{-8} \cdot (1 + 2^{-1.036})$ となり，理論値が十分に正しいことを確認できた.

またこの bias から $\Pr(Z_1 = 0 \wedge Z_2 = 0)$ は,

$$\Pr(Z_1 = 0 \wedge Z_2 = 0) = P(Z_2 = 0) \cdot P(Z_1 = 0|Z_2 = 0),$$

で与えられ, $N = 256$ のときは,

$$\Pr[Z_1 = 0 \wedge Z_2 = 0] = \frac{2}{256} \times 2^{-7.418} = 2^{-14.418} = 2^{-16}(1 + 2^{0.996}).$$

このような bias は digraph bias と呼ばれ, 文献 [8, 11] で検討されているが, Long term bias としての検討であるため，このような初期のキーストリームにおける

非常に高い bias は報告されていない.

この $Z_2 = 0$ のときの $Z_1 = 0$ の bias を用いて効果的な Broadcast RC4 への平文復元攻撃が構成できる．また，暗号文単独での内部状態 (鍵) 推測攻撃へも応用可能である.

Broadcast RC4 攻撃 Mantin-Shamir Attack [17] とこの bias を組み合わせることで，P_1 を効率よく求める攻撃が構成できる．まず準備として, 求めたい平文に対して，2^{17} の異なる鍵で暗号化された暗号文を得る.

1. 2^8 の暗号文から平文の 2 byte 目 P_2 を特定 [17].
2. 2^{17} の暗号文の 2 byte 目 C_2 に対して, $C_2 \oplus P_2$ を計算し Z_2 を求める.
3. $Z_2 = 0$ のものを選択. $2^{10} \approx 2^{17} \cdot 2/256$ の暗号文が残る.
4. 残ったものに対して, もっともカウントされている C_1 を P_1 とする.

Step 4 において, $\Pr(Z_1 = 0|Z_2 = 0) = 2^{-7.418} = 2^{-8} \cdot (1 + 2^{-1.009})$ 程度の 0 への bias から, $C_1 = P_1 \oplus Z_1 = P_1$ になっているものが, Theorem 3 より $2^{10} \approx \frac{1}{2^{-8} \cdot (2^{-1.009})^2}$ の暗号文から特定可能である.

よって 2^{17} の異なる鍵で生成された暗号文から, 平文の 1, 2 byte 目を高確率で導出することができる．1 byte 目に関しては，bias があることはすでに実験的にも理論的にも示させていたが [20, 11]，これを用いてどうのように効果的に Broadcast RC4 への attack に応用できるかは分かっていなかった．単純に, この bias を用いた攻撃を構成すると 2^{24} のオーダーの bias であるため, 2^{24} 程度のデータが必要になることが予想される．そのため，この bias は約 $1/2^7$ のデータ量の 2^{17} で導出できるため，Broadcast RC4 に対する非常に効果的な攻撃である.

内部状態 (鍵) 推測攻撃 この bias を用いて内部状態推定攻撃にも応用できる．$Z_1 = 0$, $Z_2 = 0$ が観測されたときに, $S_0[1] = 1, S_0[2] = 0$ になっている確率は,

$$\begin{aligned} & P((S_0[1] = 1 \wedge S_0[2] = 0)|(Z_1 = 0 \wedge Z_2 = 0)) \\ = \ & \frac{P(S_0[1] = 1 \wedge S_0[2] = 0)}{\Pr(Z_1 = 0 \wedge Z_2 = 0)} \cdot \Pr((Z_1 = 0 \wedge Z_2 = 0)|(S_0[1] = 1 \wedge S_0[2] = 0)) \\ = \ & \frac{\frac{1}{256} \cdot \frac{1}{255}}{2^{-14.427}} \cdot 1 = 2^{-1.567}, \end{aligned} \tag{1}$$

となる．これに関して計算機で実験を行ったところ, 確率は $2^{-1.589}$ となり理論値が正しく近似していることを確認した．よって, これらが観測された場合, $S_0[1]$ と $S_0[2]$ を $2^{-1.589}$ の確率で推測可能であり, random guess の場合の成功確率は 2^{-16} であるため, $2^{14.41}$ 倍の advantage がある.

さらに, 内部状態-鍵間の Roos の以下の関係式を用いると鍵の推測も可能

である.

$$\begin{aligned} S_0[1] &= 1 + K[0] + K[1] \\ S_0[2] &= 3 + K[0] + K[1] + K[2] \end{aligned}$$

これらはそれぞれ 0.371, 0.368 の確率で成立する [23]. そのため, $Z_1 = 0$, $Z_2 = 0$ が観測されたとき上記を推測した場合の成功確率は, $0.371 \times 0.368 \times 2^{-1.589} = 2^{-4.45}$ となり, 鍵の推測に対しても $2^{11.55}$ 倍の advantage がある.

この攻撃は, Broadcast setting では暗号文単独で実行可能である. 具体的には, まず, 2^{17} の異なる鍵で生成された暗号文から, 平文の 1, 2 byte 目を導出することができる. その情報を用いて, キーストリームの 1, 2 byte 目が 0 であるものを探し, 上記の鍵推測攻撃を実行する.

5.2.2 Bias of $Z_3 = 131$

Z_3 に関する新しい bias を提案する. Z_3 に関しては, 既存の bias である文献 [14, 11] の $Z_i = 0$ $3 \leq i \leq 255$ も, Z_3 の場合は bias が理論値と比べてかなり小さくなることが実験的に知られている. ([14] の Fig. 1, [11] の Fig. 8 参照). そのため, Broadcast RC4 への攻撃を考えた場合, 理論値と比べてかなり多くの暗号文数が必要になる. 我々は, この Z_3 に対して, $Z_3 = 0$ と比較して十分強力な $Z_3 = 131$ の bias を発見した. この確率は以下の Theorem で与えられる.

Theorem 7. $\Pr(Z_3 = 131)$ は

$$\begin{aligned} \Pr\left(Z_3 = 131\right) \approx\ & \Pr(S_0[1] = 131) \cdot \Pr(S_0[2] = 128) + \\ & (1 - \Pr(S_0[1] = 131) \cdot \Pr(S_0[2] = 128)) \cdot 1/N \end{aligned}$$

である.

Proof. $S_0[1] = 131$ かつ $S_0[2] = 128$ の場合を考える. $i = 1$ の場合, $j = S_0[1] = 131$ となり, $S_0[1]$ と $S_0[131]$ の Swap により, $S_1[131] = 131$ が成立する.

次に, $i = 2$ の場合, $j = 131 + S_1[2] = 131 + S_0[2] = 131 + 128 = 3$ となり, $S_1[2]$ と $S_1[3]$ の Swap により, $S_2[3] = 128$ が成立する.

最後に, $i = 3$ の場合, $j = 3 + S_2[3] = 3 + 128 = 131$ となり, $S_2[3]$ と $S_2[131]$ の Swap により, $S_3[3] = 131$ と $S_3[3] = 128$ が成立する. このときの出力は $Z_3 = S_3[S_3[3] + S_3[131]] = S_3[131 + 128] = 131$ となる.

以上より, $S_0[1] = 131$ かつ $S_0[2] = 128$ の場合は確率 1 で $Z_3 = 131$ が成立する. 図 4 にこのイベントを示す.

他の場合での $Z_3 = 131$ が成立する確率を $1/N$ とすると

$$\begin{aligned} \Pr\left(Z_3 = 131\right) \approx\ & \Pr(S_0[1] = 131) \cdot \Pr(S_0[2] = 128) + \\ & (1 - \Pr(S_0[1] = 131) \cdot \Pr(S_0[2] = 128)) \cdot 1/N. \end{aligned}$$

□

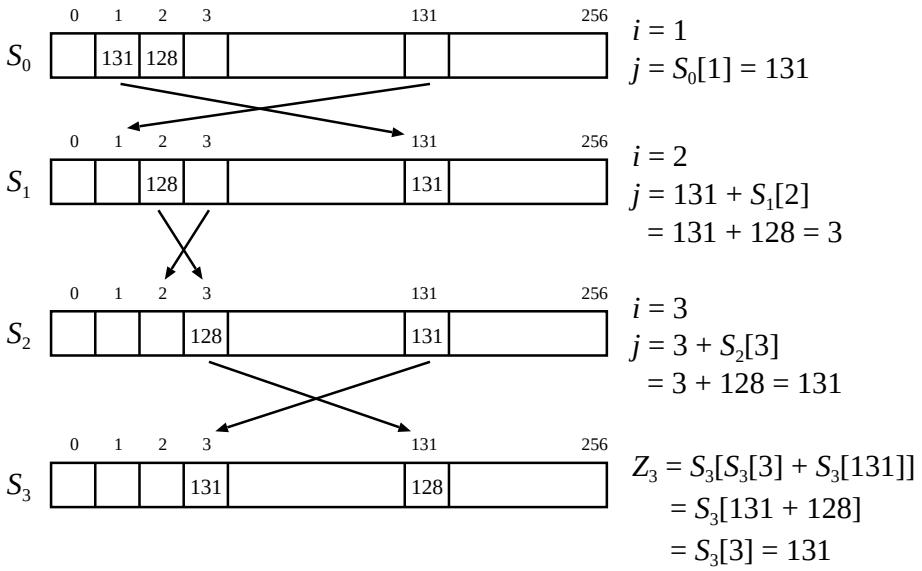


図 4: $Z_3 = 131$ の Event

ここで, $N = 256$ のケースについて考える. $\Pr(S_0[1] = 131)$ と $\Pr(S_0[2] = 128)$ は, Proposition 1 より求めることができ,

$$\Pr(S_0[1] = 131) = \frac{1}{256} \cdot \left(\left(\frac{255}{256} \right)^{256-1-1} + \left(\frac{255}{256} \right)^{131} \right) = 0.0037848.$$

$$\Pr(S_0[2] = 128) = \frac{1}{256} \cdot \left(\left(\frac{255}{256} \right)^{256-2-1} + \left(\frac{255}{256} \right)^{127} \right) = 0.0038181.$$

よって

$$\Pr\left(Z_3 = 131\right) \approx 0.0039206 = 2^{-8} \cdot (1 + 2^{-8.089}),$$

となる. 2^{40} の random に生成した鍵に対する keystream での実験では,

$$\Pr\left(Z_3 = 131\right) = 67350014/2^{34} = 0.0039204 = 2^{-8} \cdot (1 + 2^{-8.109}),$$

となり, 理論値は十分正しいことを確認した.

ここで既存の $Z_3 = 0$ の bias との比較を行う. 2^{40} の random に生成した鍵に対する keystream での実験では,

$$\Pr(Z_3 = 0) = 0.0039116 = 2^{-8} \cdot (1 + 2^{-9.512}),$$

となった. よって, $Z_3 = 131$ の方が強い bias であることが分かる. そのため, Broadcast RC4 への攻撃で Z_3 に対しては, $Z_3 = 131$ が $Z_3 = 0$ よりも多くカウントされることになるため, $Z_3 = 131$ を攻撃に用いる必要がある.

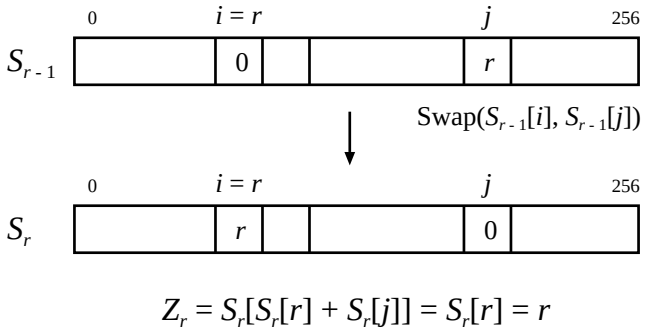


図 5: $Z_r = r$ の Event (Case 1)

5.2.3 Bias of $Z_r = r$

$Z_r = r \quad 3 \leq r \leq 255$ の bias を提案する．これは，既知の $Z_r = 0$ の bias とほぼ同じオーダーの確率で $3 \leq r \leq 255$ において存在する bias であるため，Broadcast RC4 に対する攻撃においては重要な bias である．

$Z_r = r$ の確率は以下の Theorem で与えられる．

Theorem 8. $\Pr(Z_r = r)$ は

$$\begin{aligned}\Pr\left(Z_r = r\right) \quad \approx \quad & p_{r-1,0} \cdot \frac{1}{N} + p_{r-1,r} \cdot \frac{1}{N} \cdot \frac{N-2}{N} + \\ & (1 - p_{r-1,0} \cdot \frac{1}{N} - p_{r-1,r} \cdot \frac{1}{N} - (1 - p_{r-1,0} - p_{r-1,r}) \cdot \frac{1}{N} \cdot 2) \cdot \frac{1}{N},\end{aligned}$$

である．ここで $p_{r-1,0} = \Pr(S_{r-1}[r] = 0)$, $p_{r-1,r} = \Pr(S_{r-1}[r] = r)$.

Proof. $i_r = r$ のとき出力 Z_r は,

$$\begin{aligned} Z_r \quad &= \quad S_r[S_r[i_r] + S_r[j_r]] = S_r[S_r[r] + S_{r-1}[i_r]], \\ &= \quad S_r[S_r[r] + S_{r-1}[i_r]] = S_r[S_r[r] + S_{r-1}[r]], \end{aligned}$$

で表される．

ここで，次の 4 つの case について考える．

case 1 : $S_{r-1}[r] = 0 \wedge S_r[r] = r$

case 2 : $S_{r-1}[r] = r \wedge S_r[r] = j_r - r \quad (j \neq r, r + r)$

case 3 : $S_{r-1}[r] \neq (0, r) \wedge S_r[r] = r - S_{r-1}[r]$

case 4 : $S_{r-1}[r] \neq (0, r) \wedge S_r[r] = r$

case 1 と case 2 は必ず $Z_r = r$ になるイベントで，case 3 と case 4 は必ず $Z_r \neq r$ になるイベントである．以下各 case について $\Pr(Z_r = r)$ になる確率を導出する．

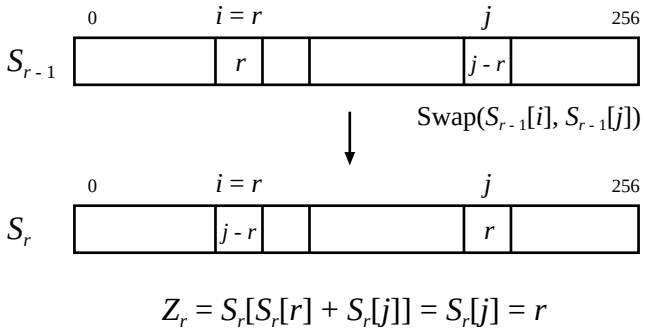


図 6: $Z_r = r$ の Event (Case 2)

Case 1 : $S_{r-1}[r] = 0 \wedge S_r[r] = r$
このとき，　$Z_r = S_r[S_r[r] + S_{r-1}[r]] = S_r[r+0] = S_r[r] = r$ となり，$\Pr(Z_r = r)$　$= 1$ となる．$S_r[r]$ は j により指された値であり，文献 [14] より，$j > 3$ の場合は，j は random にふるまうため，$S_r[r]$ の値も偏りはないと仮定する．このとき，$p_{r-1,0} = S_{r-1}[r] = 0$ と定義すると，

$$\Pr(S_{r-1}[r] = 0 \wedge S_r[r] = r) = p_{r-1,0} \cdot \frac{1}{N}.$$

図 5 にこのイベントを示す.

Case 2 : $S_{r-1}[r] = r \wedge S_r[r] = j_r - r$
このとき，　$Z_r = S_r[S_r[r]+S_{r-1}[r]] = S_r[j_r-r+r] = S_r[j_r] = S_{r-1}[r] = r$ となり，$\Pr(Z_r = r)$　$= 1$ となる．$S_r[r]$ は j により指された値であり，文献 [14] より，$j > 3$ の場合は，j は random にふるまうため，$S_r[r]$ の値も偏りはないと仮定する．$j_r = r$ のとき, $S_r[r] = 0$ になり，$Z_r = S_r[S_r[r]+S_{r-1}[r]] = S_r[0+r] = S_r[r] = 0$ になり，$\Pr(Z_r = r) = 0$ である．また $j_r = r + r$ のとき，$S_r[r] = r$ になり，$Z_r = S_r[S_r[r] + S_{r-1}[r]] = S_r[r + r] \neq r$ になり，$\Pr(Z_r = r) = 0$ である．よって，$j \neq r, r+$ の条件を満たす必要がある．

このとき，$p_{r-1,r} = S_{r-1}[r] = r$ と定義すると，

$$\Pr(S_{r-1}[r] = 0 \wedge S_r[r] = \text{ r }) = p_{r-1,r} \cdot \frac{1}{N} \cdot \frac{N-2}{N}.$$

図 6 にこのイベントを示す.

Case 3 : $S_{r-1}[r] \neq (0, r) \wedge S_r[r] = r - S_{r-1}[r]$
$Z_r = S_r[r - S_{r-1}[r] + S_{r-1}[r]] = S_r[r] = S_r[r]$ となる．このとき，$S_r[r] = r - S_{r-1}[r]$ は $S_{r-1}[r] \neq 0$ より，r にはならないため，$\Pr(Z_r = r) = 0$ となる．ここで,

$$\Pr(S_{r-1}[r] \neq (0, r) \wedge S_r[r] = r - S_{r-1}[r]) = (1 - p_{r-1,0} - p_{r-1,r}) \cdot \frac{1}{N}.$$

Case 4 : $S_{r-1}[r] \neq (0, r) \wedge S_r[r] = r$

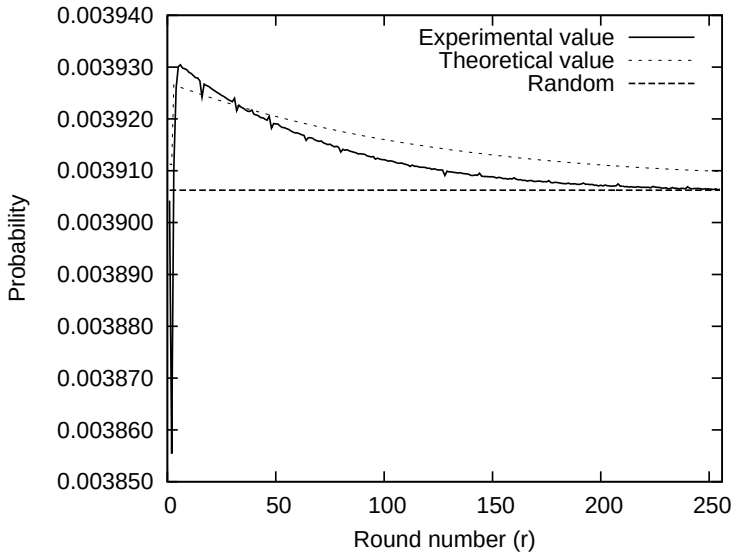


図 7: $Z_r = r$ の理論値と実験値

このとき，$Z_r = S_r[r + S_{r-1}[r]]$ となり $S_{r-1}[r] \neq 0$ より， r にはならないため，$\Pr(Z_r = r) = 0$ となる．ここで，$S_{r-1}[r] \neq 0$ かつ $r > 0$ より，$r \neq r - S_{r-1}[r]$ となり，case3 と case4 は独立な event であるため，

$$\Pr(S_{r-1}[r] \neq (0, r) \wedge S_r[r] = r - S_{r-1}[r]) = (1 - p_{r-1,0} - p_{r-1,r}) \cdot \frac{1}{N}.$$

以上より， その他の event では $Z_r = r$ が $\frac{1}{N}$ の確率で発生すると，

$$\begin{aligned}\Pr\left(Z_r = r\right) \quad \approx \quad & p_{r-1,0} \cdot \frac{1}{N} + p_{r-1,r} \cdot \frac{1}{N} \cdot \frac{N-2}{N} + \\ & (1 - p_{r-1,0} \cdot \frac{1}{N} - p_{r-1,r} \cdot \frac{1}{N} - (1 - p_{r-1,0} - p_{r-1,r}) \cdot \frac{1}{N} \cdot 2) \cdot \frac{1}{N}.\end{aligned}$$

□

ここで $p_{r-1,r}$ は Lemma 2 により計算可能である．同様に, $p_{r-1,0}$ は Lemma 2 を変形した以下の

$$\Pr(S_1[r] = 0) \left(1 - \frac{1}{N}\right)^{r-2} + \sum_{t=2}^{r-1} \sum_{k=0}^{r-t} \frac{\Pr(S_1[t] = 0)}{k! \cdot N} \left(\frac{r-t-1}{N}\right)^k \left(1 - \frac{1}{N}\right)^{r-3-k},$$

で求めることができる．

図 7 に理論値と 2^{40} のランダムに選択した鍵から生成したキーストリームの実験値の比較のグラフを示す. 弱冠のずれがあるのは, 理論値の計算の際に考慮できていないイベントが影響していると考えられる．そのため，これが完全にこの bias を証明したとは主張しないが，オーダーは合っているため, 主に影響しているイベントに関しては捕らえられていると考える．この bias は Z_3–Z_{255} で存在し, $Z_r = 0$ の bias と同程度であるため，Broadcast RC4 の攻撃の際には, 考慮する必要がある．$Z_r = 0$ と $Z_r = r$ の適切な選択については, 5.2.5 節で議論する．

表 3: $Z_r = -r$, $Z_r = 0$, $Z_r = r$ の実験値の比較

r	$\Pr(Z_r = -r)$	$\Pr(Z_r = 0)$	$\Pr(Z_r = r)$
16	$2^{-8} \cdot (1 + 2^{-4.811})$	$2^{-8} \cdot (1 + 2^{-7.714})$	$2^{-8} \cdot (1 + 2^{-7.762})$
32	$2^{-8} \cdot (1 + 2^{-5.383})$	$2^{-8} \cdot (1 + 2^{-7.880})$	$2^{-8} \cdot (1 + 2^{-7.991})$
48	$2^{-8} \cdot (1 + 2^{-5.938})$	$2^{-8} \cdot (1 + 2^{-8.043})$	$2^{-8} \cdot (1 + 2^{-8.350})$
64	$2^{-8} \cdot (1 + 2^{-6.496})$	$2^{-8} \cdot (1 + 2^{-8.244})$	$2^{-8} \cdot (1 + 2^{-8.664})$
80	$2^{-8} \cdot (1 + 2^{-7.224})$	$2^{-8} \cdot (1 + 2^{-8.407})$	$2^{-8} \cdot (1 + 2^{-9.052})$
96	$2^{-8} \cdot (1 + 2^{-7.911})$	$2^{-8} \cdot (1 + 2^{-8.577})$	$2^{-8} \cdot (1 + 2^{-9.351})$
112	$2^{-8} \cdot (1 + 2^{-8.666})$	$2^{-8} \cdot (1 + 2^{-8.747})$	$2^{-8} \cdot (1 + 2^{-9.732})$

5.2.4 Bias of Extended Keylength-dependent bias

Extended Keylength-dependent bias として，鍵長 l が 16 byte の場合に $Z_r = -r$ ($r = 16, 32, 48, 64, 80, 96, 112$) となる bias を提案する．表 3 に試行回数 2^{40} における Extended Keylength-dependent bias，$Z_r = 0$，$Z_r = r$ の実験値を示す．表 3 から Extended Keylength-dependent bias が他の 2 つより強力な bias であることが分かる．Extended Keylength-dependent bias は Keylength-dependent bias [12] を拡張した新しい bias である．Keylength-dependent bias は文献 [26] において実験的に示され，文献 [12] で証明が与えられた $Z_l = -l$ の bias である．しかし，文献 [26] では $l = 16$ の場合に $r > 48$ のパラメータでは役に立たないとして $r = 16$ の実験値しか記載していない．我々は実験によって $r = 16, 32, 48, 64, 80, 96, 112$ まで Broadcast RC4 への攻撃に有効であることを発見した．図 10 に表 3 の Extended Keylength-dependent bias の実験値 (Experimental value) と文献 [12] の理論式を用いて導出した確率 (Theoretical value of [12]) のグラフを示す．図 10 から，Experimental value と Theoretical value of [12] に大きなずれがあることが分かる．文献 [12] では $l < 48$ などの小さいパラメータの場合のみを考えており，また，$r = k \cdot l$ などの鍵 byte を繰り返し使う場合の挙動は考慮していない．このため文献 [12] の理論式は近似式として意味をなしていない．これらの問題点を解決し，未知のイベントを発見して理論的に bias の近似式を構成する．

$Z_r = -r$ が成立しているときの内部状態および状態遷移を解析した結果，以下の 3 つの比較的大きな bias を持つイベントから Extended Keylength-dependent bias が満たされることを発見した．

Source Event 1 : $S_{r-1}[r] = 2r \wedge S_r[r] = -r$

Source Event 2 : $f_{r-1} = -r$

Source Event 3 : $f_{r-1} \neq -r \wedge S_{r-1}[r] = 0$

表 4: E_1, E_2, E_3 の実験値と条件付き確率

r	$\Pr(E_1)$	$\Pr(E_2)$	$\Pr(Z_r = -r \mid E_2)$	$\Pr(E_3)$	$\Pr(Z_r = -r \mid E_3)$
16	0.0000196	0.0038998	0.0266066	0.0030881	0.0185482
32	0.0000186	0.0078119	0.0057877	0.0036847	0.0242181
48	0.0000169	0.0039107	0.0039338	0.0038805	0.0195860
64	0.0000160	0.0156367	0.0039003	0.0038698	0.0146792
80	0.0000154	0.0039061	0.0039464	0.0038687	0.0104982
96	0.0000147	0.0078133	0.0039161	0.0038525	0.0081722
112	0.0000143	0.0039030	0.0039195	0.0038742	0.0066151

このとき f_y は

$$f_y = \sum_{x=0}^{y} K[x] + \frac{y(y+1)}{2},$$

とする．以降，各イベントを E_1，E_2，E_3 と表記する．E_1，E_3 は我々が発見したイベントであり，E_2 は Keylength-dependent bias を満たすイベントである．$l = 16$ とした場合における各イベントの実験値を表 4 に示す．

Keylength-dependent bias において $\Pr(Z_l = -l \mid f_{l-1} = -l)$ は以下の Lemma で与えられる．

Lemma 3. [12] $f_{l-1} = -l$ のとき $Z_l = -l$ の確率 $\Pr(Z_l = -l \mid f_{l-1} = -l)$ は，

$$\frac{1}{N} + \left[1 - \frac{1}{N}\right] \cdot \left[\frac{1}{N} + \left[1 - \frac{l}{N}\right]\left[1 - \frac{1}{N}\right]^{N+l-2}\left[\left[1 - \frac{1}{N}\right]^{1+l} + \frac{1}{N}\right]\right] \cdot \left[\frac{1}{N} + \left[1 - \frac{1}{N}\right]^{l+1} \Pr(S_0[S_0[l-1]] = f_{l-1})\right],$$

である．ここで $\Pr(S_0[S_0[l-1]] = f_{l-1})$ は $1 \le l \le 32$ のとき文献 [12] の Proposition 4 により計算され，$l > 32$ の場合は $1/N$ とする．

$Z_r = -r$ $(r = 16, 32, 48, 64, 80, 96, 112)$ の確率は以下の Theorem で与えられる．

Theorem 9. $\Pr(Z_r = -r)$ は

$$\begin{aligned}\Pr(Z_r = -r) \quad \approx \quad & p_{r-1,2r} \cdot \frac{1}{N} + \Pr(Z_r = -r \mid f_{r-1} = -r) \cdot \Pr(f_{r-1} = -r) \\ & + \Pr(Z_r = -r \mid E_3) \cdot \Pr(E_3) \\ & + \left[1 - p_{r-1,2r} \cdot \frac{1}{N} - \Pr(f_{r-1} = -r) - \Pr(E_3)\right] \cdot \frac{1}{N},\end{aligned}$$

である．ここで $p_{r-1,2r} = \Pr(S_{r-1}[r] = 2r)$, $\Pr(E_3) = \Pr(f_{r-1} \neq -r \wedge S_{r-1}[r] = 0)$.

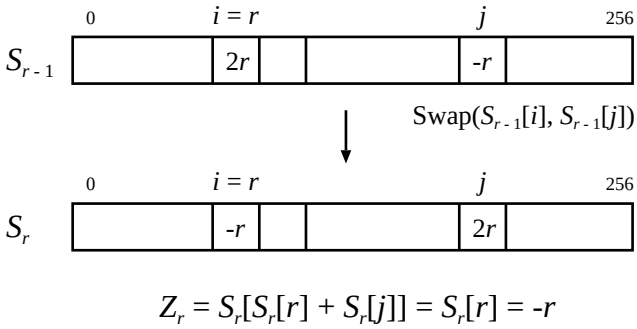


図 8: $Z_r = -r$ の Event (Case 1)

Proof. $i_r = r$ のとき出力 Z_r は,

$$\begin{aligned} Z_r &= S_r[S_r[i_r] + S_r[j_r]] = S_r[S_r[r] + S_{r-1}[i_r]] \\ &= S_r[S_r[r] + S_{r-1}[i_r]] = S_r[S_r[r] + S_{r-1}[r]], \end{aligned}$$

で表される.

ここで，次の 3 つの case について考える.

Case 1 : $S_{r-1}[r] = 2r \wedge S_r[r] = -r$

Case 2 : $f_{r-1} = -r$

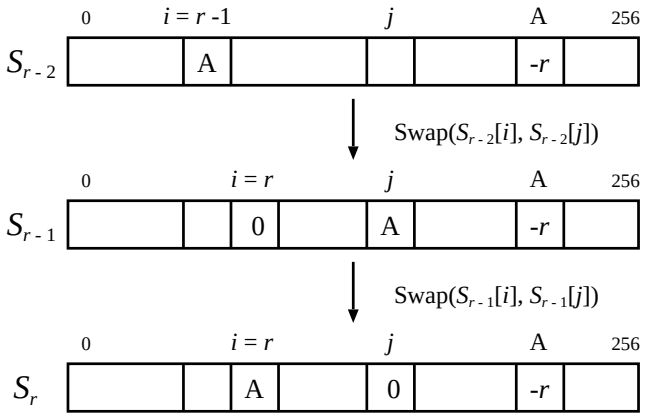
Case 3 : $f_{r-1} \neq -r \wedge S_{r-1}[r] = 0$

Case 1 は必ず $Z_r = -r$ になるイベントであり，Case 2 は Lemma 3 を拡張したイベントである．Case 3 は実験的に確認されたイベントであり，Case 3 を構成するイベントの一部については解析が完了している．しかし解析ができていない部分があるので，完全な証明は open problem とする．以下，各 case について $\Pr(Z_r = -r)$ を導出する.

Case 1 : $S_{r-1}[r] = 2r \wedge S_r[r] = -r$
このとき，$Z_r = S_r[S_r[r] + S_{r-1}[r]] = S_r[(-r) + 2r] = S_r[r] = -r$ となり $\Pr(Z_r = -r) = 1$ となる．$S_r[r]$ は j により指された値であり，文献 [14] より，$j > 3$ の場合は j は random にふるまうため，$S_r[r]$ の値も偏りはないと仮定する．ここで，$p_{r-1,2r} = \Pr(S_{r-1}[r] = 2r)$ と定義すると,

$$\Pr(S_{r-1}[r] = 2r \wedge S_r[r] = -r) = p_{r-1,2r} \cdot \frac{1}{N}.$$

図 8 にこのイベントを示す.
Case 2 : $f_{r-1} = -r$
Lemma 3 を $l = 16$ の場合に $Z_r = -r \mid f_{r-1} = -r$ というイベントに拡張して考える．このとき，$S_{r-1}[r] = 0 \wedge S_r[S_{r-2}[r-1]] = -r$ であれば，$Z_r = S_r[S_r[r] + S_{r-1}[r]] = S_r[0 + S_{r-2}[r-1]] = S_r[S_{r-2}[r-1]] = -r$ となる．Lemma



$$Z_r = S_r[S_r[r] + S_r[j]] = S_r[\mathrm{A}] = -r$$

図 9: $Z_r = -r$ の Event (Case 2,3)

3 では $f_{l-1} = -l$ の条件において $S_{l-1}[l] = 0 \wedge S_l[S_{l-2}[l-1]] = -l$ となるイベントが考えられている．これを用いると，

$$\begin{aligned}\Pr(Z_r = -r \mid E_2) \cdot \Pr(E_2) \quad \approx \quad & \Pr(f_{r-1} = -r) \cdot \left[\frac{1}{N} + \left[1 - \frac{1}{N}\right]\right. \\ & \cdot \left[\frac{1}{N} + \left[1 - \frac{r}{N}\right]\left[1 - \frac{1}{N}\right]^{N+r-2}\left[\left[1 - \frac{1}{N}\right]^{1+r} + \frac{1}{N}\right]\right] \\ & \left.\cdot \left[\frac{1}{N} + \left[1 - \frac{1}{N}\right]^{r+1} \Pr(S_0[S_0[r-1]] = f_{r-1})\right]\right].\end{aligned}$$

図 9 にこのイベントを示す．ここで，$f_{r-1} = -r$ の成立確率について述べる．鍵長を 16 としたとき，$K[x] = K[x \bmod 16]$ となる．これを考慮すると $r = 16 \cdot k$ のとき $f_{r-1} = -r$ は

$$\begin{aligned} f_{r-1} &= k \cdot (K[0] + \ldots + K[15]) + \frac{16 \cdot k(16 \cdot k - 1)}{2} \\ &= -16 \cdot k \pmod N, \end{aligned}$$

となり，

$$k \cdot (K[0] + \ldots + K[15]) = -16 \cdot k - \frac{16 \cdot k(16 \cdot k - 1)}{2} \pmod N,$$

を満たす秘密鍵が選択された場合に式が成立する．$k = 1, 3, 5, 7$ の場合は $(K[0] + \ldots K[15])$ が式を満たすものは 1 通りしかなく確率は $1/N$ になる．$k = 2$ および $k = 6$ のときには 2 通りとなるため確率は $2/N$，$k = 4$ のときには 4 通りとなるため確率は $4/N$ に向上することが分かる．この性質は表 4 によって実験的にも確認している．

Case 3 : $f_{r-1} \neq -r \wedge S_{r-1}[r] = 0$

このとき，$S_r[S_{r-2}[r-1]] = -r$ であれば，$Z_r = S_r[S_r[r] + S_{r-1}[r]] = S_r[0 +$

表 5: Case 3 の条件付き確率の理論値と実験値

r	$\Pr(Z_r = -r \mid E_3)$
16	0.0074864
32	0.0073027
48	0.0071216
64	0.0069428
80	0.0067656
96	0.0065898
112	0.0064148

$S_{r-2}[r-1]] = S_r[S_{r-2}[r-1]] = -r$ となる．よって図 9 と同様のイベントにより bias が成立していると考えられる．確率 $\Pr(Z_r = -r|E_3)$ は Lemma 3 における $\Pr(S_l[S_{l-2}[l-1]] = -l|f_{l-1} = -l)$ と同様の手順で導出すると

$$\Pr(Z_r = -r|E_3) = \frac{1}{N} + \left[1 - \frac{1}{N}\right]^{r+1} \cdot \Pr(S_0[S_0[r-1]] = -r).$$

ここで，$\Pr(S_0[S_0[r-1]] = -r)$ は

$$\Pr(S_0[S_0[r-1]] = -r) = \sum_{x=0}^{255} \Pr(S_0[r-1] = x \wedge S_0[x] = -r),$$

により算出する．理論値は表 5 に示す．表 4 の実験値と比較すると，大きな差があることがわかる．これより，Case 3 においては未発見のイベントが存在すると考えられる．未発見のイベントの詳細な証明については open ploblem とする．図 10 における Theoretical value の導出には表 4 の実験値を用いる．
以上より，

$$\begin{aligned}\Pr(Z_r = -r) \quad \approx \quad & p_{r-1,2r} \cdot \frac{1}{N} + \Pr(Z_r = -r \mid f_{r-1} = -r) \cdot \Pr(f_{r-1} = -r) \\ & + \Pr(Z_r = -r \mid E_3) \cdot \Pr(E_3) \\ & + \left[1 - p_{r-1,2r} \cdot \frac{1}{N} - \Pr(f_{r-1} = -r) - \Pr(E_3)\right] \cdot \frac{1}{N}.\end{aligned}$$

□

ここで $p_{r-1,2r}$ は Lemma 2 を変形した以下の

$$Pr(S_1[r] = 2r)\left(1 - \frac{1}{N}\right)^{r-2} + \sum_{t=2}^{r-1}\sum_{k=0}^{r-t} \frac{Pr(S_1[t] = 2r)}{k! \cdot N}\left(\frac{r-t-1}{N}\right)^k \left(1 - \frac{1}{N}\right)^{r-3-k},$$

で求めることができる．

図 10 に $Z_r = -r$ $(r = 16, 32, 48, 64, 80, 96, 112)$ の Theorem 9 による理論値のグラフを示す．実験値と理論値に若干の誤差が存在する．これは理論値の計算の際に考慮できていないイベントの影響だと考えられるが，オーダーは合って

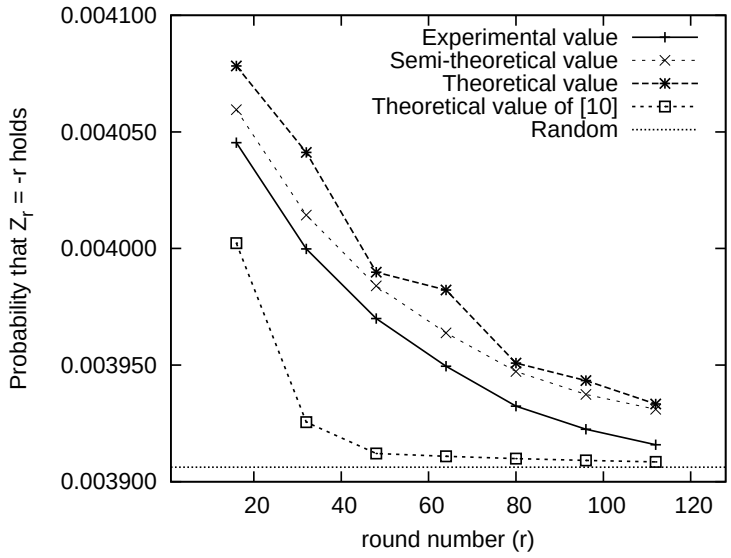


図 10: $Z_r = -r$ の理論値と実験値

いるため，理論的考察の観点ではこの近似式で十分だと考える．また，文献 [12] の理論式より良く近似できていることが確認できる．さらに，表 4 に示した各イベントの実験値を Theorem 9 の理論式に代入し，確率を導出した．導出した値を Semi-theoretical value とする．図 10 より，Semi-theoretical value により Theorem 9 をシミュレートすることで近似精度の改善が確認できた．表 4 の実験値にそった各イベントの厳密な評価は open ploblem とする．

5.2.5 Optimal Bias Set

表 6 に optimal bias set を示す．P_1, P_3, P_{32}, P_{48}, P_{56}, P_{80}, P_{96}, P_{112} に関しては, 本章で示した既存の bias よりも強力な bias を攻撃に用いる．ここで, $Z_r = 0$ [14] と我々の示した $Z_r = r$ の比較を行う．図 11 に $Z_r = 0$ と $Z_r = r$ の実験値を示す．この図より P_{31} までは $Z_r = r$ の bias が大きく, それ以降 $Z_r = 0$ が大きくなるため, 表 6 ではそのようになるように選択した．よって optimal bias set は, $Z_1, \ldots, Z_{255}$ での最も強い bias の set である．これについては次節の実験により，正当性を保証する

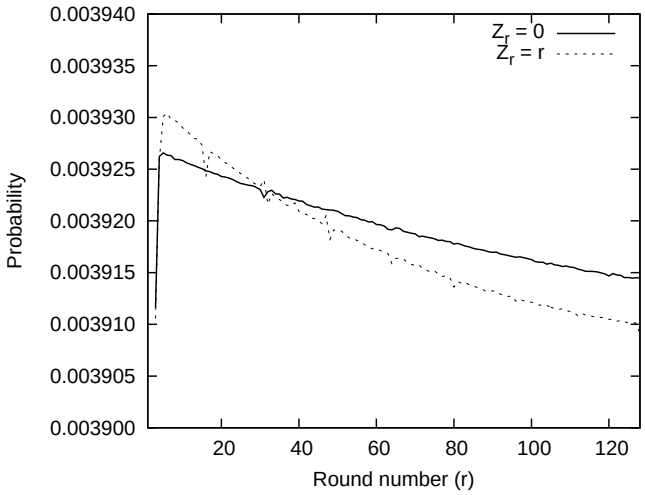


図 11: $Z_r = 0$ と $Z_r = r$ の比較 ($3 \leq r \leq 255$)

5.3 Broadcast RC4 に対する平文解読実験

我々は, 先ほど定義した optimal bias を用いて，Broadcast RC4 に対する解読実験を行った. 実験の詳細は以下の通りである.

1. ランダムに攻撃対象の平文 P を生成する.
2. 2^x のランダムに生成した秘密鍵で P を暗号化して 2^x 通りの暗号文を生成する.
3. 生成した暗号文の各 byte に対して, 頻度表を生成し, 最もカウントされているものを optimal bias set で XOR されたものとし, $P_i = C_i \oplus Z_i$(optimal bias set) で平文を復元する.

P_1 に関しては, 5.2.1 で述べたように Z_2 に対する条件付き bias を用いるため, P_2 を復元したのちに $Z_2 = 0$ になっているものを選択し頻度表を作成する.

上記の実験を, 256 通りの平文に対して, $2^6, \ldots, 2^{35}$ 通りの秘密から生成された暗号文に対して行った. 図 12 に P_1–P_3, P_5, P_{16} の実験結果を示す. 横軸は攻撃に用いる暗号文数を，縦軸は成功確率を表している. ここで成功確率とは 256 通りの平文のうち何通りが成功したかを示すものである. たとえば任意の byte において, 256 の平文において, 100 の平文のケースで正しく平文を復元できた場合は成功確率は $0.390625 (= 100/256)$ となる. 図より, P_2 に対しては 2^8 以上の暗号文数から成功確率が上昇し始め, 2^{12} 程度で成功確率が 1 になる. これまで, [17] では Ω で見積もられているのみであったが, 今回その暗号文数と成功確率の関係を明らかにした. 同様に P_2, P_{16} に関しては従来の評価では, 2^{16} 以上という評価であったが成功確率を 1 にするためには, 2^{20} 程度の暗号文数が必要である. 今回新しく見つけた P_3 に関する結果も明らかにした. [14] で示された P_5 に関し

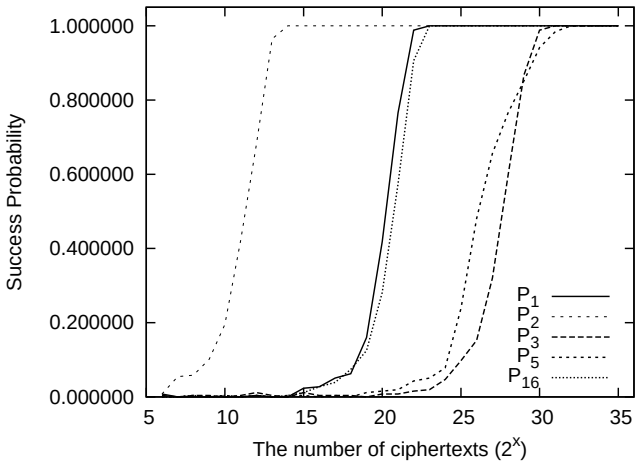


図 12: $P_{1,2,3,5,16}$ の暗号文数毎の攻撃成功確率

ては, 2^{24} 以上の暗号文数から成功確率が上昇し始め, 2^{31} 程度で成功確率が 1 になる.

次に, 暗号文数に対する攻撃の成功確率を byte 毎に説明する. 図 13 に暗号文数が 2^{24}, 2^{28}, 2^{32}, 2^{35} の場合の平文の各 byte の成功確率を示す. ここで Random に, 平文の各 byte を guess した場合の成功確率は $1/256 = 0.00390625$ である. 暗号文数を増やすことに応じて成功確率が上昇し, 2^{32} 以上の暗号文数ですべての平文 byte で成功確率が 0.5 を上回る. これは, optimal bias set が最も確率の高い bias set であることを意味し, 最適な set であることが分かる. しかしながら, 2^{35} まで暗号文数を増やしても, 成功確率が 1 にはならない. これは, 1 番高い bias と 2 番目に高い bias の差が小さいことが原因で成功確率を 1 にするためにはさらに多くの暗号文数が必要であると予想される.

図 14 に頻度表で上位 2 つに対して optimal bias set を XOR した場合の成功確率を示した. これは, 2 つの候補に正しい平文が含めれている場合を成功として見積もったため, Random に, 平文の各 byte を guess した場合の成功確率は $2/256 = 0.0078125$ となる. これによると 2^{34} の暗号文数で成功確率は 1 になった. この場合平文の値は一意には絞れないが, 各 byte は 2 つまで絞りこむことができる. また上位 3 の候補に対して optimal bias set を XOR したものも Table 15 に示す. Appendix にさらに詳細な暗号文数と成功確率の関係を示すグラフを掲載している. ここで平文一種類に対して, 図 13-15 の実験結果を得るためには, 1 CPU core (Intel(R) Core(TM) i7 CPU 920@2.67GHz) で約 1 日かかる. 本評価では, 256 種類の平文に対し実験を行っている.

Optimal bias set を用いた Broadcast RC4 の平文解読攻撃による攻撃成功確率の平均値を暗号文数毎に表 7 に示す. 2^{32} の sample 数があれば, 1–257 byte の平文 byte を平均確率 0.9 以上で推測することが可能である. また, 平文の最初の 100 byte および 257 byte の解読に成功する確率が $1/256$ (or $2/256, 3/256$) $\cdot 5$ になる暗号文数を表 8 に示す. これは random guess に対して 5 倍以上のアドバン

テージある暗号文数を最初の 100 byte と 257 byte 全てにおいて評価している．2^{25} 以上で 100 byte の平文を十分高確率で推測可能である．

以上より Broadcast RC4 に対しては，2^{32} の暗号文数があれば，1–257 byte の大部分の平文 byte を高確率 (0.9 以上) で決定することが可能である．また，1,2 byte 目や extended keylength-dependent bias などの確率の高い bias は 2^{24} 程度の sample で高確率で推測することが可能である．

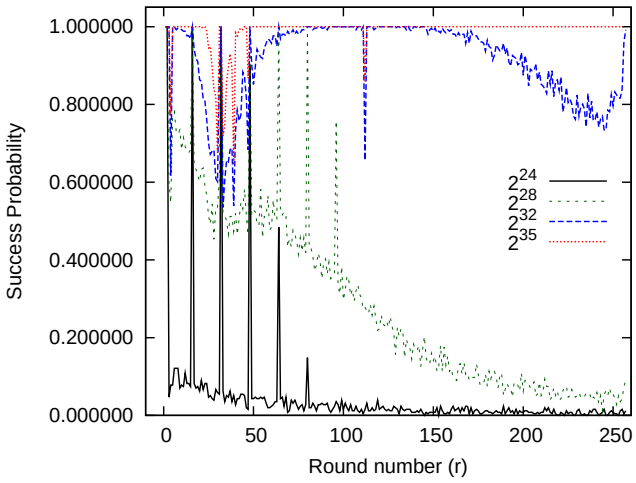


図 13: 暗号文数毎の P_r $(1 \leq r \leq 257)$ の攻撃成功確率 (one candidate)

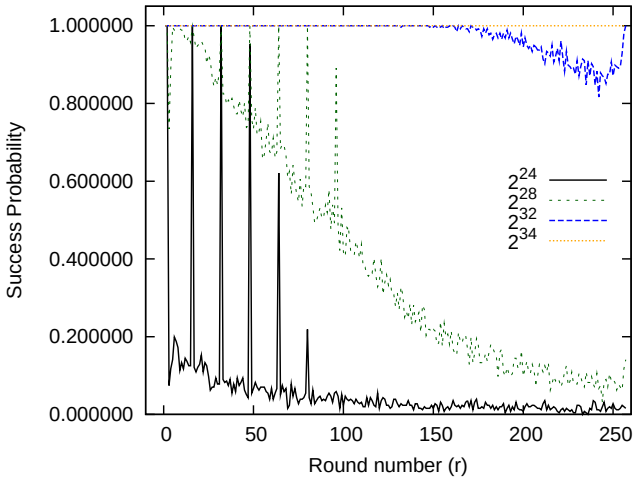


図 14: 暗号文数毎の P_r $(1 \leq r \leq 257)$ の攻撃成功確率 (two candidates)

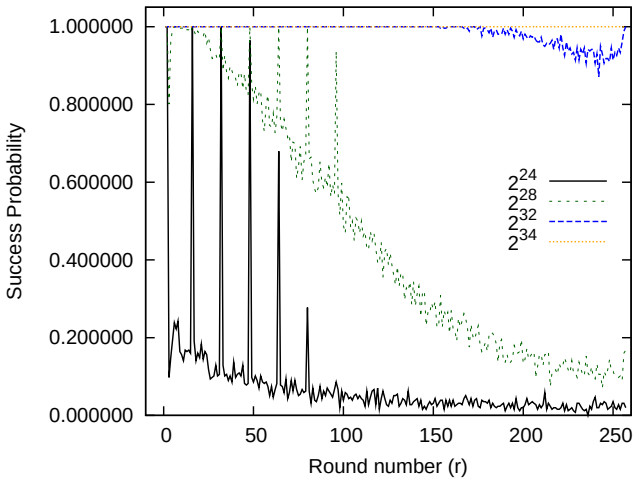


図 15: 暗号文数毎の P_r $(1 \leq r \leq 257)$ の攻撃成功確率 (three candidates)

5.4 258 byte 目以降の平文の導出方法

本節では 258 byte 目以降の平文の効率的な導出方法を提案する．前節までの optimal bias set を用いた方法はキーストリームの初期の byte のみに生じる bias に注目しており，$r \geq 258$ の範囲の P_r の復元には適用できない．r が大きい平文 byte を復元するためには任意の時刻で生じる bias (long-term bias) を利用する必要がある．最も強力な long-term bias は Mantin によって提案された digraph repetition bias ($ABSAB$ bias とも呼ばれている) [16] である．我々は $Z_1, \ldots, Z_{257}$ の optimal bias set と $ABSAB$ bias を組み合わせることで P_{258} 以降の平文 byte を逐次的に復元する方法を与える．

5.4.1 Based Long-term Bias ($ABSAB$ bias) [16]

$ABSAB$ bias はキーストリームの 2byte 単位のシンボル（digraph）の分布の統計的な偏りのことであり，同じ digraph が短いギャップ S で繰り返されやすいことに注目している．ギャップ S は $ABAB$ なら S は無し，$ABCAB$ なら S は C，$ABCDAB$ なら S は CD のように定義される．ギャップ S の長さを G としたとき，$ABSAB$ bias は具体的には以下の式で表すことができる．

$$Z_r \,||\, Z_{r+1} = Z_{r+2+G} \,||\, Z_{r+3+G} \quad \text{for } G \geq 0, \tag{2}$$

ここで $||$ は byte の連結である．式 (2) の成立確率は Theorem 10 で与えられる．

Theorem 10. [16] *For small values of G the probability of the pattern $ABSAB$ in RC4 streams where S is a G-word string is* $(1 + e^{(-4-8G)/N}/N) \cdot 1/N^2$.

G の値が異なる $ABSAB$ bias を同時に利用する，すなわち成立確率が異なる bias を同時に取り扱う場合には以下の Lemma で示される discrimination を利用する．

Lemma 4. [16] *Let X and Y be two distributions and suppose that the independent events $\{E_i: 1 \leq i \leq k\}$ occur with probabilities $p_X(E_i) = p_i$ in X and $p_Y(E_i) = (1 + b_i) \cdot p_i$ in Y. Then the discrimination D of the distributions is $\sum_i p_i \cdot b_i^2$.*

この discrimination D は単一の bias の場合は $D = p \cdot q^2$ のように対応する．Mantin は bias がある分布とランダムな分布を確率 $1 - \alpha$ で識別するためのサンプル数を以下の Lemma で与えている．

Lemma 5. [16] *The number of samples that is required for distinguishing two distributions that have discrimination D with success rate $1 - \alpha$ (for both directions) is $(1/D) \cdot (1 - 2\alpha) \cdot log_2 \frac{1-\alpha}{\alpha}$.*

この Lemma は Broadcast RC4 の平文復元攻撃において，discrimination D とサンプル数 $N_{ciphertext}$ が与えられたときに bias を含んだ分布 (式が成立する分布) を 1 つのランダムな分布 (式が成立しない分布) から分離できる確率が一定 (constant) になることを示している．この一定の確率を $\Pr_{distingush}$ と表記する．

5.4.2 *ABSAB* bias と optimal bias set を組み合わせた逐次的導出法

Broadcast RC4 の平文復元攻撃において，*ABSAB* bias は以下の方程式によって利用される．

$$\begin{aligned}
&(C_r \,||\, C_{r+1}) \oplus (C_{r+2+G} \,||\, C_{r+3+G}) \\
&= (P_r \oplus Z_r \,||\, P_{r+1} \oplus Z_{r+1}) \oplus (P_{r+2+G} \oplus Z_{r+2+G} \,||\, P_{r+3+G} \oplus Z_{r+3+G}) \\
&= (P_r \oplus P_{r+2+G} \oplus Z_r \oplus Z_{r+2+G} \,||\, P_{r+1} \oplus P_{r+3+G} \oplus Z_{r+1} \oplus Z_{r+3+G}) \quad (3)
\end{aligned}$$

ABSAB bias のイベントである式 (2) が成立するとき，上式からキーストリームの情報が排除され，平文と暗号文の関係式 $(C_r \,||\, C_{r+1}) \oplus (C_{r+2+G} \,||\, C_{r+3+G}) = (P_r \oplus P_{r+2+G} \,||\, P_{r+1} \oplus P_{r+3+G}) = (P_r \,||\, P_{r+1}) \oplus (P_{r+2+G} \,||\, P_{r+3+G})$ が得られる．

しかしながら，ストレートフォワードな方法では，識別攻撃のように G の値が異なる関係式を組み合わせて利用することは困難である．G の値が異なるとき，r を適切に選んだとしても関係式は異なってしまう．例えば，(round r and $G = 1$) と (round $r + 1$ and $G = 0$) に関する関係式を考えた場合，関係式の右側はそれぞれ $(P_r \,||\, P_{r+1}) \oplus (P_{r+3} \,||\, P_{r+4})$ と $(P_{r+1} \,||\, P_{r+2}) \oplus (P_{r+3} \,||\, P_{r+4})$ のようになる．このように独立した式しか得られない場合，異なる G の *ABSAB* bias を集中させて利用できないため，Broadcast RC4 の平文復元攻撃を効率的に実行することが困難となる．

我々は，既知の平文 byte の情報を用いる逐次型の方法によって上記の問題を解決する．例えば，(round r and $G = 1$) と (round $r + 1$ and $G = 0$) に関する関係式を考えた場合，もし P_r，P_{r+1} および P_{r+2} の値を事前に推測していたとすると，関係式の左側の未知変数は両方とも $(P_{r+3} \,||\, P_{r+4})$ のように同じ表現に

なる．このように G が異なる複数の関係式をマージすることで効率的に平文を復元することが可能となる．このとき，$P_1, \ldots, P_{257}$ は optimal bias set から推測するとして，P_{258} 以降の平文 P_r for $r = 258, 259, \ldots, P_{MAX}$ を $ABSAB$ bias を使って効率的に復元する方法を以下に与える．ここで，$ABSAB$ bias のパラメータは $G = 0, 1, \ldots, G_{MAX}$ とする．

Step 1 各暗号文について $C_{258-3-G_{MAX}}, C_{258-2-G_{MAX}}, \ldots, C_{P_{MAX}}$ を得て，$r = 258, \ldots, P_{MAX}$ および $G = 0, \ldots, G_{MAX}$ の全ての組み合わせに対して $(C_{r-3-G} \,||\, C_{r-2-G}) \oplus (C_{r-1} \,||\, C_r)$ のための頻度表 $T_{count}[r][G]$ へカウントする．ここで，式 (2) が成立するとき $(C_{r-3-G} \,||\, C_{r-2-G}) \oplus (C_{r-1} \,||\, C_r) = (P_{r-3-G} \,||\, P_{r-2-G}) \oplus (P_{r-1} \,||\, P_r)$ が成立する．

Step 2 $r = 258$ をセットする．

Step 3 P_r の値を推測する．

Step 3.1 $G = 0, 1, \ldots, G_{MAX}$ の全てに対して，既に推測している $P_{r-3-G_{MAX}}, \ldots, P_{r-2}$ の値を利用して $T_{count}[r][G]$ のカウント数を $(P_{r-1} \,||\, P_r)$ のための頻度表 $T_{marge}[r]$ のカウント数に変換してマージする．

Step 3.2 既に推測している P_{r-1} の値を利用して，$T_{marge}[r]$ から P_r のための頻度表 $T_{guess}[r]$ を作る．具体的には，与えられた P_{r-1} に対応する P_r のカウント数を $T_{marge}[r]$ から抜き出して $T_{guess}[r]$ にカウントする．$T_{guess}[r]$ の中で最も頻度が高い値を正しい P_r として推測する．

Step 4 r をインクリメントする．もし，$r = P_{MAX} + 1$ であればアルゴリズム終了する．そうでなければ，Step 3 へ．

$T_{marge}[r]$ から平文 byte を推測するとき，$N^2 - 1$ 個の誤った候補の全てから正しい候補が識別されるときに正しい値が推測される．誤った候補がランダムな分布になると仮定すると，$T_{marge}[r]$ からの推測で正しい候補が得られる確率は $(\mathrm{Pr}_{distingush})^{N^2-1}$ となる．Step 3.2 では P_{r-1} を用いて $T_{marge}[r]$ から $T_{guess}[r]$ に変換することで，誤った候補の個数を $N^2 - 1$ から $N - 1$ へ減らしている．$T_{guess}[r]$ からの推測で正しい候補が得られる確率は $(\mathrm{Pr}_{distingush})^{N-1}$ となり，$T_{marge}[r]$ から得る場合と比べて $1/(\mathrm{Pr}_{distingush})^{N+1}$ 倍高くなる．したがって，Step 3.2 のテーブルの縮小処理は攻撃を更に最適化できていることがわかる．

5.4.3 Experimental Results

我々のアルゴリズムの有効性を示すために $P_{258}, \ldots, P_{261}$ ($P_{MAX} = 261$) を復元する実験を行った．$ABSAB$ bias のパラメータは D の増加が収束する程度の値として $G_{MAX} = 63$ を選択した (このとき，$D = 2^{-28.0}$)．攻撃の際に観測できる暗号文数は 2^{30} から 2^{34} まで変化させることとし，攻撃に利用する $P_1, \ldots, P_{257}$ もこの暗号文から optimal bias set (candidate one) を用いて推測したものを用

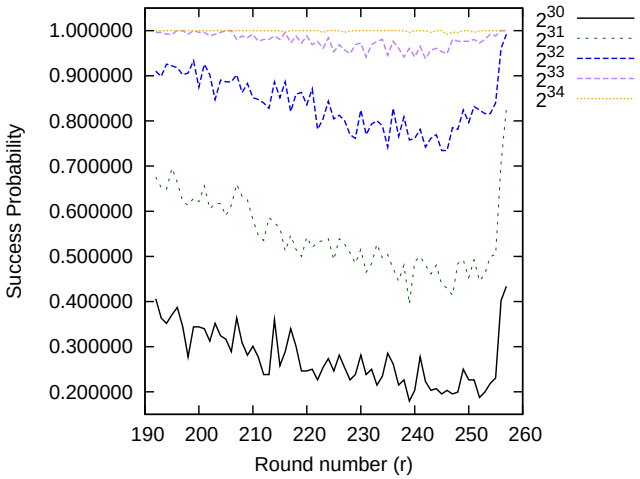


図 16: 暗号文数毎の P_r $(192 \leq r \leq 257)$ の攻撃成功確率 (one candidate))

いる．試行回数は 256 回としたとき，$P_{258}, \ldots, P_{261}$ の復元の成功確率を表 9 に示す．ここで平文一種類に対して, 図 13-15 の実験結果を得るためには, 1 CPU core (Intel(R) Core(TM) i7 CPU 920@2.67GHz) で約一週間かかる．また，逐次型の方法で用いる $P_{192}, \ldots, P_{257}$ の復元の成功確率は図 16 に示す.

興味深いことに，暗号文数 2^{34} のときに，逐次型の方法に用いる $P_1, \ldots, P_{257}$ で確率 1 で復元できない byte があるにも関わらず，$P_{258}, \ldots, P_{261}$ は全て確率 1 で復元できている．これは複数の bias を組み合わせて利用することで，逐次型の方法に用いる平文 byte がわずかに誤る程度の影響は受けにくくなっているからと推測できる．本実験では P_{261} までの復元を実行しているが，$ABSAB$ bias は long-term bias であるため，それ以後の byte の復元においても同様の確率で遷移していくと考えられる．よって，我々の逐次型の方法は 2^{34} の暗号文で P_r $(r \geq 258)$ をほぼ確率 1 で復元することができる．

ここで，2^{34} の暗号文が与えられたときの P_{262} 以降の復元成功確率について考える．Lemma 5 と $D = 2^{-28.0}$ より，2^{34} の暗号文があれば，確率 $\Pr_{distinguish} = 1 - 10^{-19}$ で random stream と識別可能である．そのとき，誤った候補がランダムな分布になると仮定すると, $(N-1)$ の誤った候補から正しい候補を抽出できる確率は $(\Pr_{distinguish})^{N-1}$ で抑えられる．よって，我々の攻撃では平文の $(257+X)$ bytes 目は確率 $((\Pr_{distinguish})^{N-1})^X = (\Pr_{distinguish})^{(N-1)\cdot X}$ で復元可能である．たとえば, $X = 2^{40}$ and $X = 2^{50}$ のとき， 成功確率はそれぞれ 0.99997, 0.97170 になる．

表 6: Optimal bias set

r	Strongest bias for Z_r	Prob.(Theoretical)	Prob.(Experimental)
1	$Z_1 = 0 \mid Z_2 = 0$ (Our)	$2^{-8} \cdot (1 + 2^{-1.009})$	$2^{-8} \cdot (1 + 2^{-1.036})$
2	$Z_2 = 0$ [17]	$2^{-8} \cdot (1 + 2^{0})$	$2^{-8} \cdot (1 + 2^{0.002})$
3	$Z_3 = 131$ (Our)	$2^{-8} \cdot (1 + 2^{-8.089})$	$2^{-8} \cdot (1 + 2^{-8.109})$
4	$Z_4 = 0$ [14]	$2^{-8} \cdot (1 + 2^{-7.581})$	$2^{-8} \cdot (1 + 2^{-7.611})$
5–15	$Z_r = r$ (Our)	max: $2^{-8} \cdot (1 + 2^{-7.609})$ min: $2^{-8} \cdot (1 + 2^{-7.718})$	max: $2^{-8} \cdot (1 + 2^{-7.335})$ min: $2^{-8} \cdot (1 + 2^{-7.535})$
16	$Z_{16} = 240$ [12]	$2^{-8} \cdot (1 + 2^{-4.671})$	$2^{-8} \cdot (1 + 2^{-4.811})$
17–31	$Z_r = r$ (Our)	max: $2^{-8} \cdot (1 + 2^{-7.740})$ min: $2^{-8} \cdot (1 + 2^{-7.892})$	max: $2^{-8} \cdot (1 + 2^{-7.576})$ min: $2^{-8} \cdot (1 + 2^{-7.839})$
32	$Z_{32} = 224$ (Our)	$2^{-8} \cdot (1 + 2^{-5.176})$	$2^{-8} \cdot (1 + 2^{-5.383})$
33–47	$Z_r = 0$ [14]	max: $2^{-8} \cdot (1 + 2^{-7.896})$ min: $2^{-8} \cdot (1 + 2^{-8.049})$	max: $2^{-8} \cdot (1 + 2^{-7.868})$ min: $2^{-8} \cdot (1 + 2^{-8.039})$
48	$Z_{48} = 208$ (Our)	$2^{-8} \cdot (1 + 2^{-5.651})$	$2^{-8} \cdot (1 + 2^{-5.938})$
49–63	$Z_t = 0$ [14]	max: $2^{-8} \cdot (1 + 2^{-8.070})$ min: $2^{-8} \cdot (1 + 2^{-8.222})$	max: $2^{-8} \cdot (1 + 2^{-8.046})$ min: $2^{-8} \cdot (1 + 2^{-8.238})$
64	$Z_{64} = 192$ (Our)	$2^{-8} \cdot (1 + 2^{-6.085})$	$2^{-8} \cdot (1 + 2^{-6.496})$
65–79	$Z_r = 0$ [14]	max: $2^{-8} \cdot (1 + 2^{-8.244})$ min: $2^{-8} \cdot (1 + 2^{-8.396})$	max: $2^{-8} \cdot (1 + 2^{-8.223})$ min: $2^{-8} \cdot (1 + 2^{-8.376})$
80	$Z_{80} = 176$ (Our)	$2^{-8} \cdot (1 + 2^{-6.574})$	$2^{-8} \cdot (1 + 2^{-7.224})$
81–95	$Z_r = 0$ [14]	max: $2^{-8} \cdot (1 + 2^{-8.417})$ min: $2^{-8} \cdot (1 + 2^{-8.568})$	max: $2^{-8} \cdot (1 + 2^{-8.398})$ min: $2^{-8} \cdot (1 + 2^{-8.565})$
96	$Z_{96} = 160$ (Our)	$2^{-8} \cdot (1 + 2^{-6.970})$	$2^{-8} \cdot (1 + 2^{-7.911})$
97–111	$Z_t = 0$ [14]	max: $2^{-8} \cdot (1 + 2^{-8.589})$ min: $2^{-8} \cdot (1 + 2^{-8.738})$	max: $2^{-8} \cdot (1 + 2^{-8.570})$ min: $2^{-8} \cdot (1 + 2^{-8.722})$
112	$Z_{112} = 144$ (Our)	$2^{-8} \cdot (1 + 2^{-7.300})$	$2^{-8} \cdot (1 + 2^{-8.666})$
113–255	$Z_t = 0$ [14]	max: $2^{-8} \cdot (1 + 2^{-8.759})$ min: $2^{-8} \cdot (1 + 2^{-10.042})$	max: $2^{-8} \cdot (1 + 2^{-8.760})$ min: $2^{-8} \cdot (1 + 2^{-10.041})$
256	$Z_{256} \neq 0$ (Our)	N/A	$2^{-8} \cdot (1 - 2^{-9.407})$
257	$Z_{257} = 0$ (Our)	N/A	$2^{-8} \cdot (1 + 2^{-9.531})$

表 7: 成功確率の平均値 (1–257 byte)

暗号文数	candidate 1	candidate 2	candidate 3
2^{31}	0.78499	0.89455	0.91912
2^{32}	0.91469	0.97662	0.98624
2^{33}	0.96840	0.99860	0.99947
2^{34}	0.98302	1	1
2^{35}	0.98925	1	1

表 8: random guess と比較して advantage のある暗号文数

解読する平文の長さ	candidate 1	candidate 2	candidate 3
100byte	2^{25}	2^{25}	2^{25}
257byte	2^{29}	2^{29}	2^{28}

表 9: P_r $(r \geq 258)$ の攻撃成功確率.

# of ciphertexts	P_{258}	P_{259}	P_{260}	P_{261}
2^{30}	0.003906	0.003906	0.000000	0.000000
2^{31}	0.039062	0.007812	0.003906	0.007812
2^{32}	0.386719	0.152344	0.070312	0.027344
2^{33}	0.964844	0.941406	0.921875	0.902344
2^{34}	1.000000	1.000000	1.000000	1.000000

5.5 まとめ

本章では, Broadcast setting で RC4 を使う場合の評価を行った．まず，既知の bias よりも強い 4 つの新しい bias を示し，実験的にも確認した．そして，我々はこれらの bias を考慮した平文復元攻撃に最適な bias の set である optimal bias set を導出した．次に，上記の optimal bias set を用いて，実際に平文解読実験を計算機で行い，攻撃に必要な sample 数 (暗号文数) を成功確率と共に見積もった．結果として，2^{32} 程度の異なる鍵で生成された暗号文があれば，optimal bias set を用いることにより, 確率 0.5 以上で平文の 1–255 byte 目の各 byte を復元できる．また, 証明はついていないが Z_{256} と Z_{257} に関して実験的に攻撃に有効な bias を発見した．これをさらに用いることで, 平文の 1–257 byte が復元可能になる．

最後に, 258 byte 以降を効率よくもとめる方法を提案した．この方法は EUROCRYPT2005 で Matin により示された Digraph Repetition bias [16] と，本稿で求めた Z_1–Z_{257} の optimal bias set を組み合わせて，逐次的に求めていくものである．この手法を用いることにより，2^{34} 程度の暗号文から 258 byte 以降の平文も求めることができる．ここで，この Digraph Repetition bias は, long term bias であるため，258 byte 以降の任意のすべての平文を暗号文から求めることができる．理論的には，初めの 2^{50} bytes $\approx$ 1000 T bytes の平文は 2^{34} の異なる鍵で生成された暗号文から確率 0.97170. で導出可能である．

以上より，我々の攻撃では, 任意の平文を暗号文のみから導出できる Full Plaintext Recovery Attack でありかつ，現実的なデータ量で攻撃可能である．

謝辞

本評価における計算機実験の一部は広島大学情報メディア教育研究センター HPC グリッドシステムおよび情報爆発 InTrigger プラットフォームを用いて実施した．ここに記して謝意を表す．

参考文献

[1] Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors. *Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers*, volume 4876 of *Lecture Notes in Computer Science*. Springer, 2007.

[2] Eli Biham and Yaniv Carmeli. Efficient reconstruction of rc4 keys from internal states. In Kaisa Nyberg, editor, *FSE*, volume 5086 of *Lecture Notes in Computer Science*, pages 270–288. Springer, 2008.

[3] Brice Canvel, Alain P. Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a ssl/tls channel. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 583–599. Springer, 2003.

[4] Jiageng Chen and Atsuko Miyaji. A new practical key recovery attack on the stream cipher rc4 under related-key model. In Xuejia Lai, Moti Yung, and Dongdai Lin, editors, *Inscrypt*, volume 6584 of *Lecture Notes in Computer Science*, pages 62–76. Springer, 2010.

[5] Jiageng Chen and Atsuko Miyaji. Generalized analysis on key collisions of stream cipher rc4. *IEICE Transactions*, 94-A(11):2194–2206, 2011.

[6] T. Dierks and C. Allen. The tls protocol version 1.0, 1999. `http://www.ietf.org/rfc/rfc2246.txt`.

[7] Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of rc4. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography*, volume 2259 of *Lecture Notes in Computer Science*, pages 1–24. Springer, 2001.

[8] Scott R. Fluhrer and David A. McGrew. Statistical analysis of the alleged rc4 keystream generator. In Bruce Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 2000.

[9] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The ssl protocol version 3.0, 1996. `http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt`.

[10] Jovan Dj. Golic. Linear statistical weakness of alleged rc4 keystream generator. In Walter Fumy, editor, *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pages 226–238. Springer, 1997.

[11] Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. (non-)random sequences from (non-)random permutations - analysis of rc4 stream cipher. Cryptology ePrint Archive, Report 2011/448, 2011. `http://eprint.iacr.org/`.

[12] Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. Proof of empirical rc4 biases and new key correlations. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, pages 151–168. Springer, 2011.

[13] Lars R. Knudsen, Willi Meier, Bart Preneel, Vincent Rijmen, and Sven Verdoolaege. Analysis methods for (alleged) rc4. In Kazuo Ohta and Dingyi Pei, editors, *ASIACRYPT*, volume 1514 of *Lecture Notes in Computer Science*, pages 327–341. Springer, 1998.

[14] Subhamoy Maitra, Goutam Paul, and Sourav Sengupta. Attack on broadcast rc4 revisited. In Antoine Joux, editor, *FSE*, volume 6733 of *Lecture Notes in Computer Science*, pages 199–217. Springer, 2011.

[15] Itsik Mantin. Analysis of the stream cipher rc4. Master's Thesis, The Weizmann Institute of Science, Israel, 2001. `http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html`.

[16] Itsik Mantin. Predicting and distinguishing attacks on rc4 keystream generator. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 491–506. Springer, 2005.

[17] Itsik Mantin and Adi Shamir. A practical attack on broadcast rc4. In Mitsuru Matsui, editor, *FSE*, volume 2355 of *Lecture Notes in Computer Science*, pages 152–164. Springer, 2001.

[18] Mitsuru Matsui. Key collisions of the rc4 stream cipher. In Orr Dunkelman, editor, *FSE*, volume 5665 of *Lecture Notes in Computer Science*, pages 38–50. Springer, 2009.

[19] Alexander Maximov and Dmitry Khovratovich. New state recovery attack on rc4. In David Wagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 297–316. Springer, 2008.

[20] Ilya Mironov. (not so) random shuffles of rc4. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 304–319. Springer, 2002.

[21] Atsushi Nagao, Toshihiro Ohigashi, Takanori Isobe, and Masakatu Morii. New classes of weak keys on rc4 using predictive state, 2012. Computer Security Symposium 2012.

[22] Atsushi Nagao, Toshihiro Ohigashi, Takanori Isobe, and Masakatu Morii. How to expand weak-key space of rc4, 2013. The 30th Symposium on Cryptography and Information Security (to appear).

[23] Goutam Paul and Subhamoy Maitra. Permutation after rc4 key scheduling reveals the secret key. In Adams et al. [1], pages 360–377.

[24] Souradyuti Paul and Bart Preneel. A new weakness in the rc4 keystream generator and an approach to improve the security of the cipher. In Bimal K. Roy and Willi Meier, editors, *FSE*, volume 3017 of *Lecture Notes in Computer Science*, pages 245–259. Springer, 2004.

[25] Andrew Roos. A class of weak keys in the RC4 stream cipher, 1995. Two posts in sci.crypt.

[26] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Discovery and exploitation of new biases in rc4. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *Lecture Notes in Computer Science*, pages 74–91. Springer, 2010.

[27] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Statistical attack on rc4 - distinguishing wpa. In Kenneth G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 343–363. Springer, 2011.

[28] Yoshiaki Shiraishi, Toshihiro Ohigashi, and Masakatu Morii. Internal-state reconstruction of a stream cipher rc4. *IEICE Transactions*, 86-A(10):2636–2638, 2003.

[29] Ryoichi Teramura, Toshihiro Ohigashi, Hidenori Kuwakado, and Masakatu Morii. Generalized classes of weak keys on rc4 using predictive state. *IEICE Transactions*, 94-A(1):10–18, 2011.

[30] Serge Vaudenay and Martin Vuagnoux. Passive-only key recovery attacks on rc4. In Adams et al. [1], pages 344–359.

A　平文解読実験の詳細データ

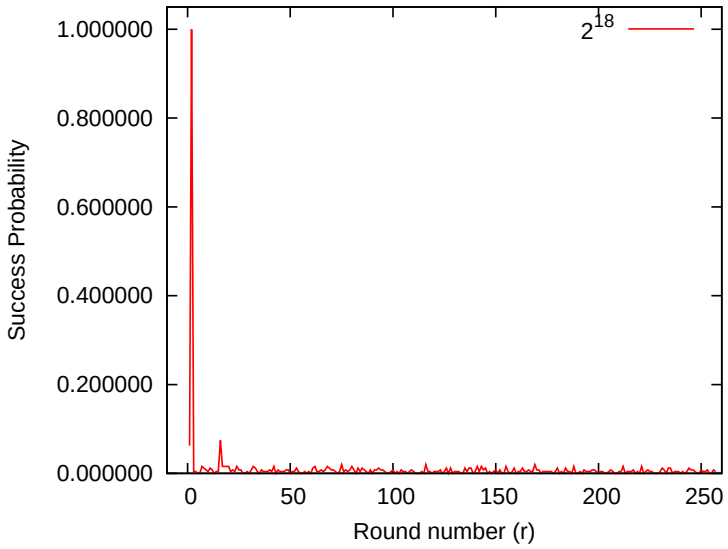


図 17: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{18} samples (one candidate)

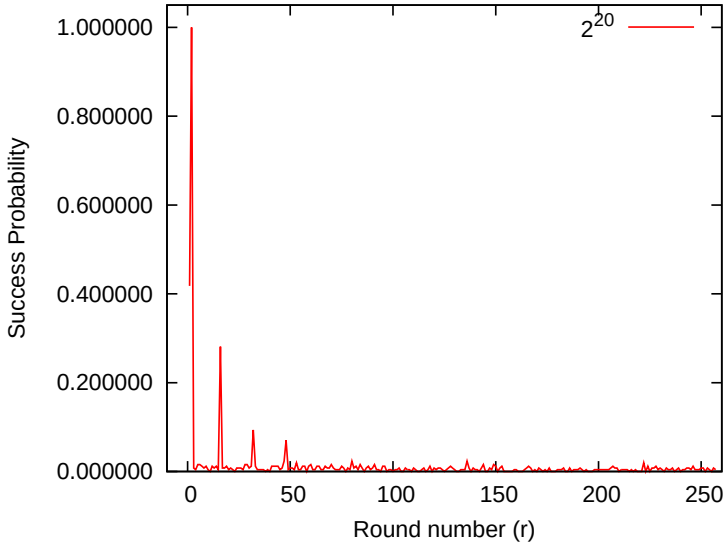


図 18: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{20} samples (one candidate)

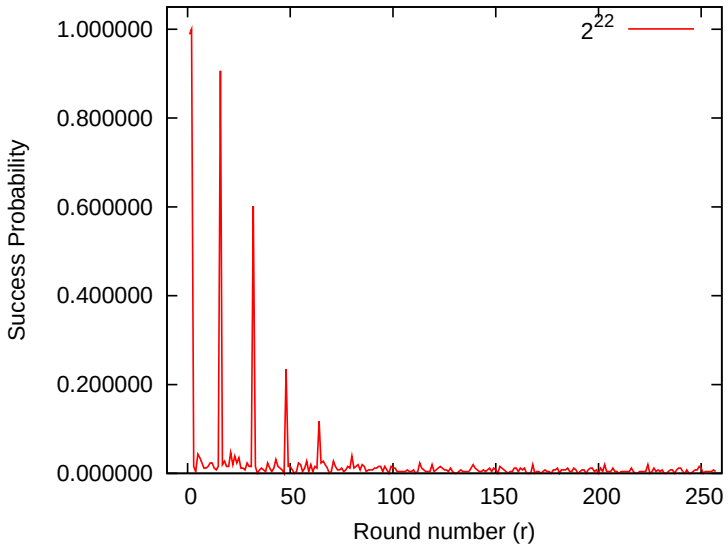


図 19: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{22} samples (one candidate)

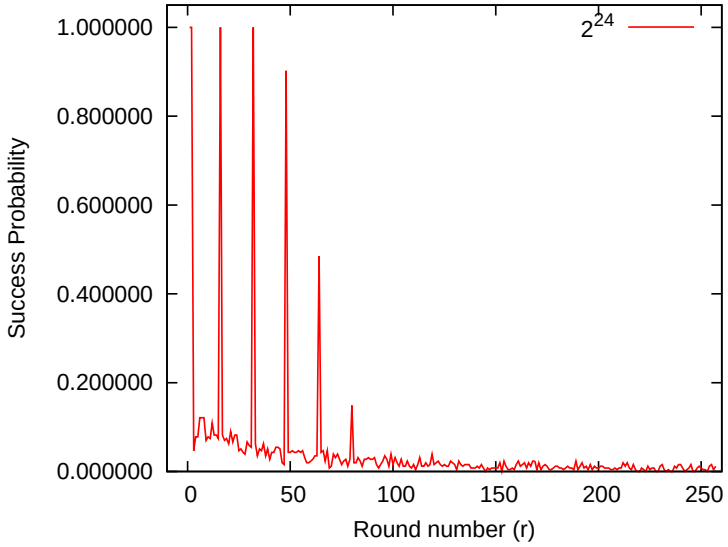


図 20: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{24} samples (one candidate)

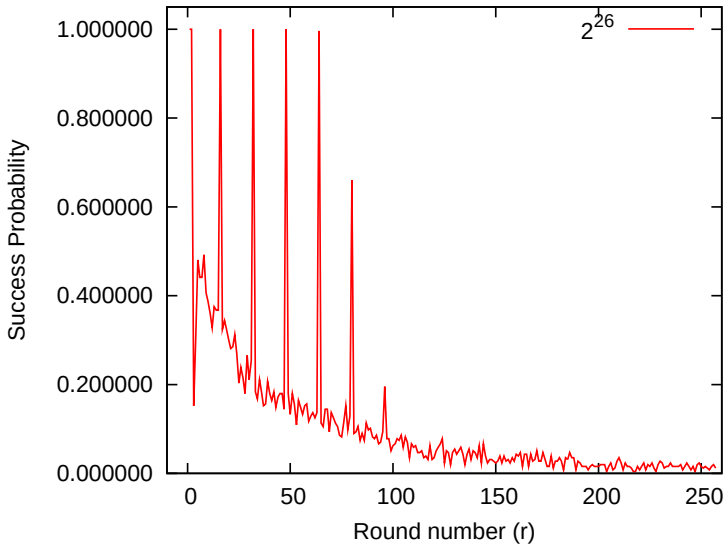


図 21: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{26} samples (one candidate)

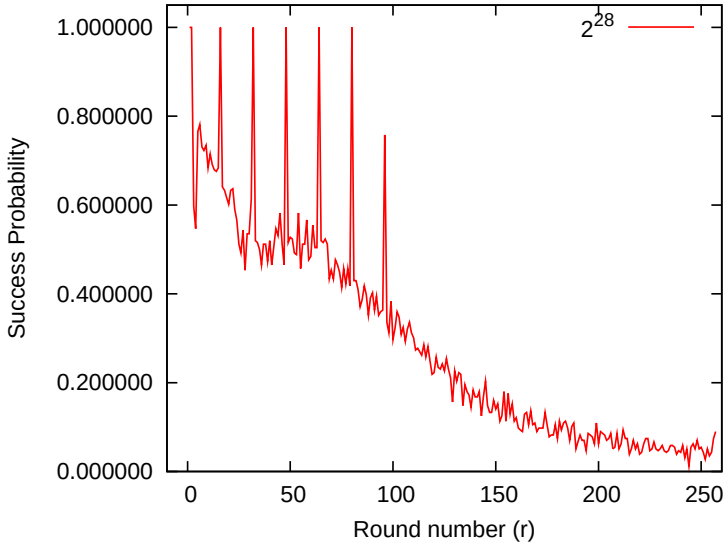


図 22: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{28} samples (one candidate)

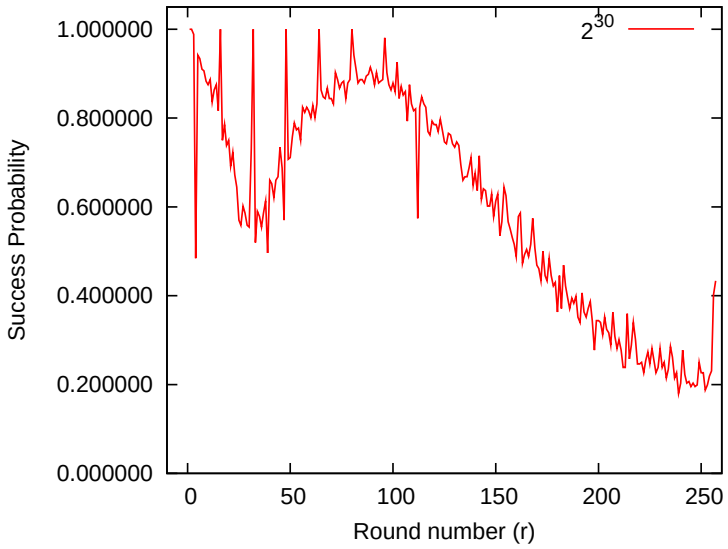


図 23: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{30} samples (one candidate)

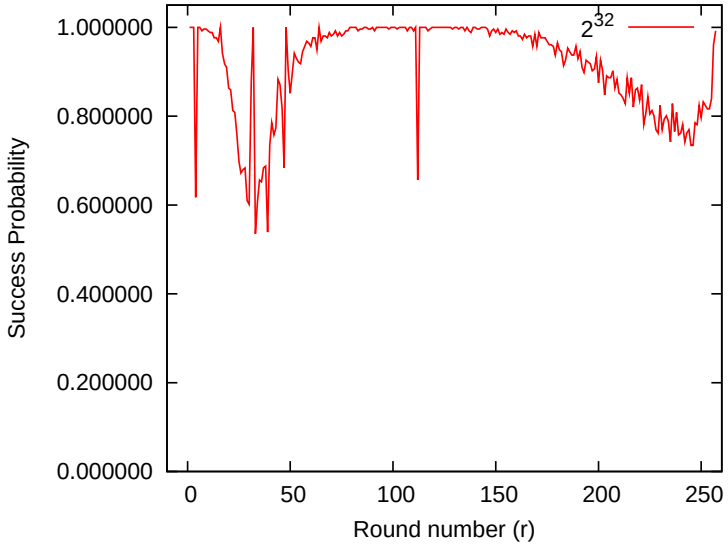


図 24: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{32} samples (one candidate)

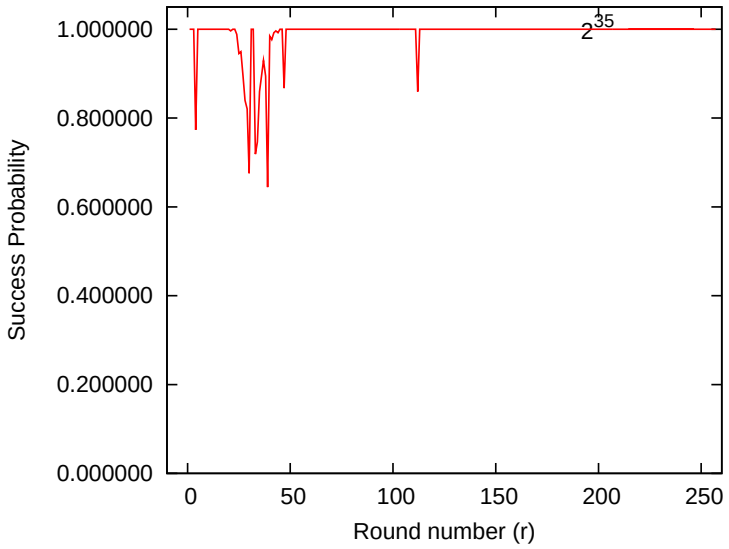


図 25: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{35} samples (one candidate)

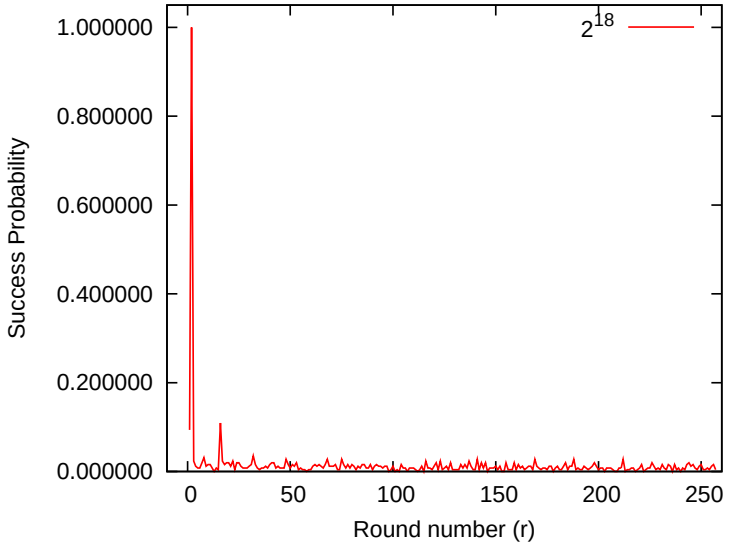


図 26: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{18} samples (two candidates)

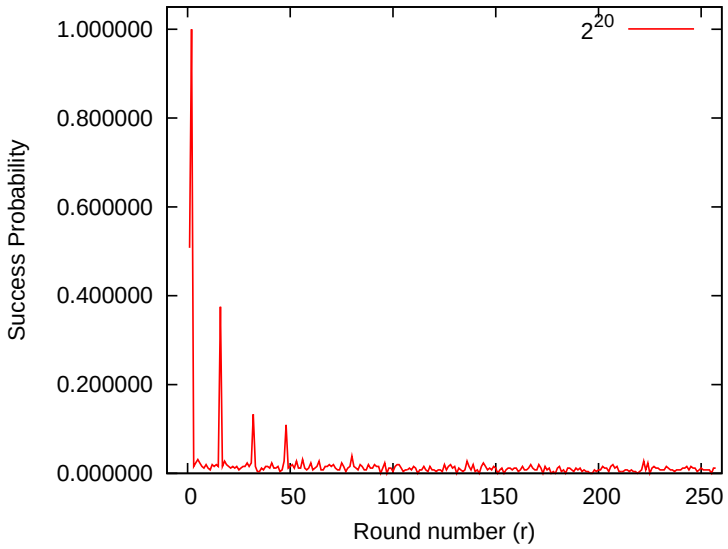


図 27: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{20} samples (two candidates)

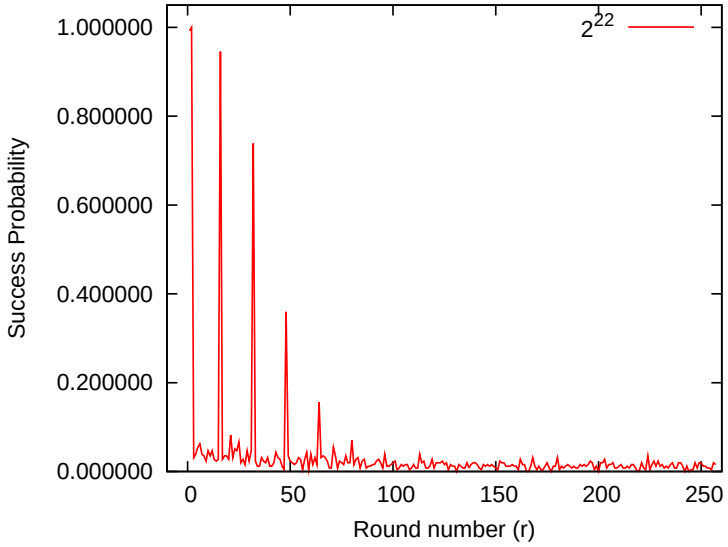


図 28: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{22} samples (two candidates)

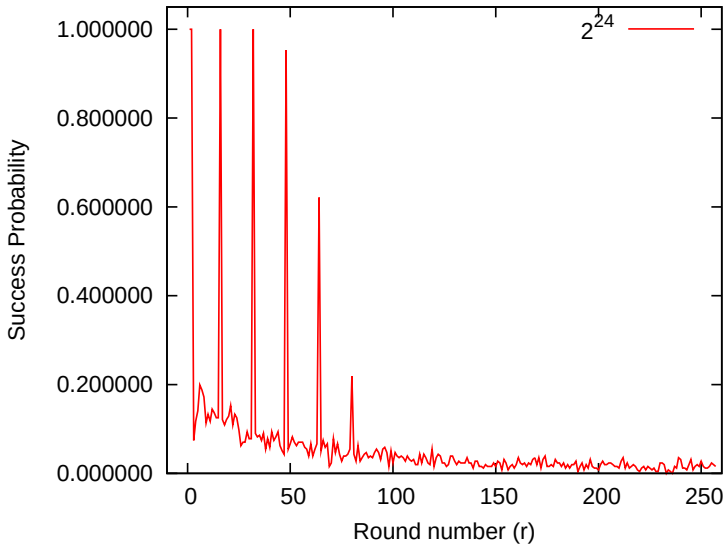


図 29: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{24} samples (two candidates)

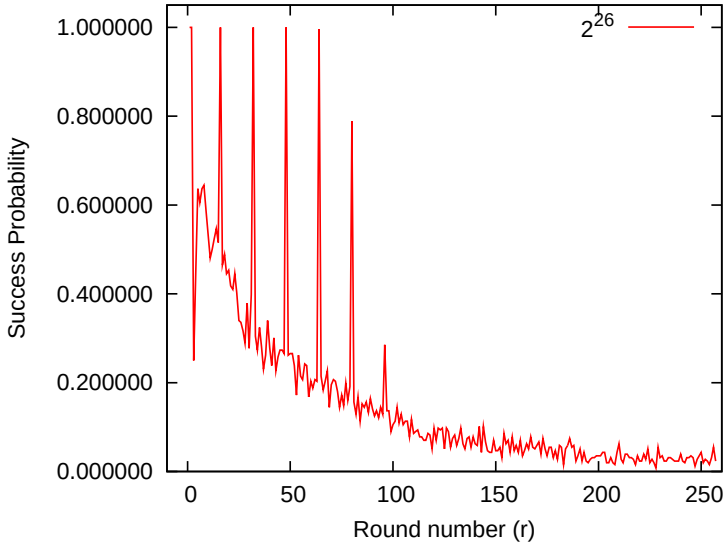


図 30: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{26} samples (two candidates)

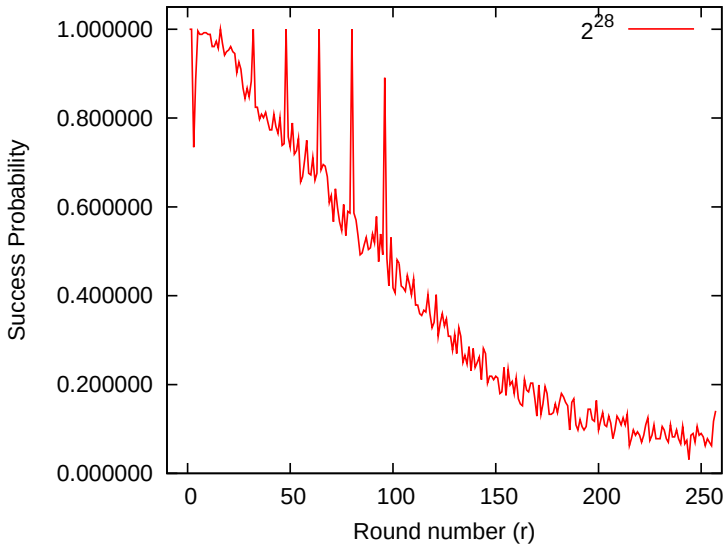


図 31: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{28} samples (two candidates)

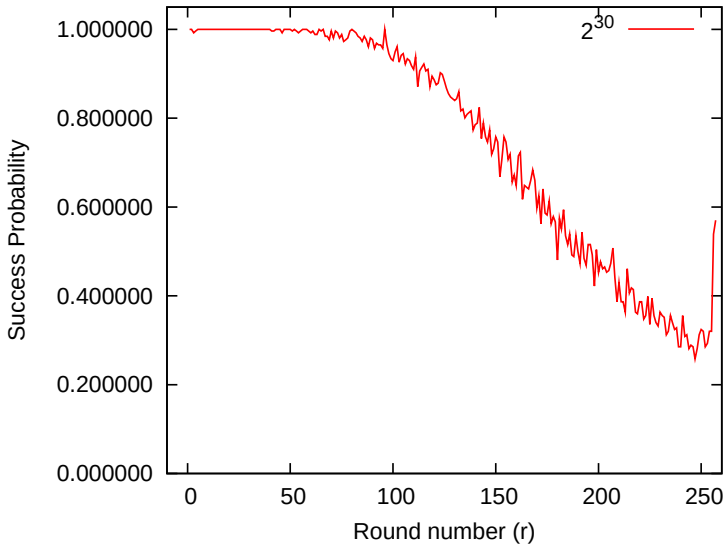


図 32: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{30} samples (two candidates)

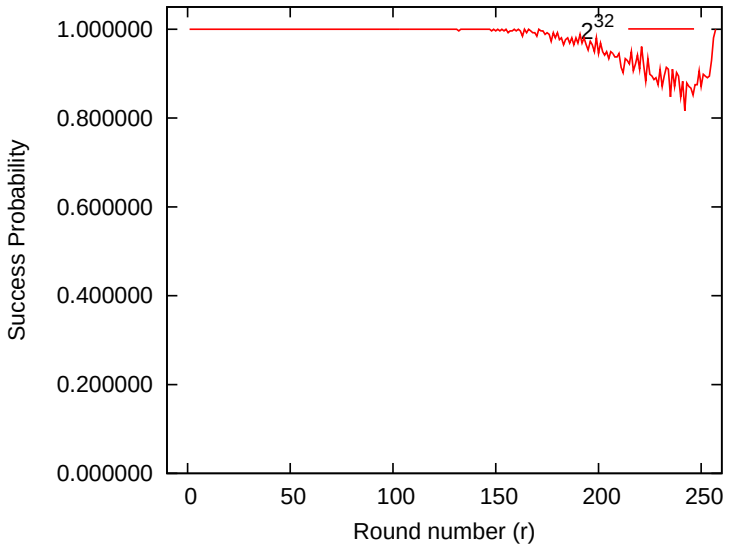


図 33: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{32} samples (two candidates)

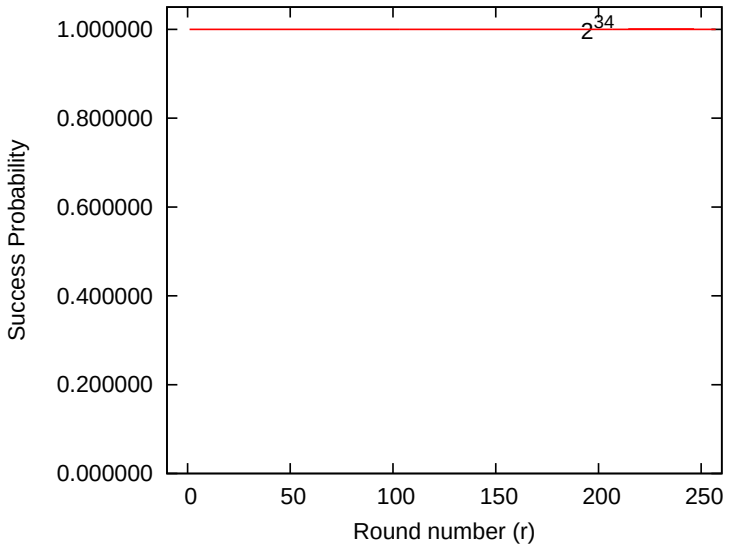


図 34: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{34} samples (two candidates)

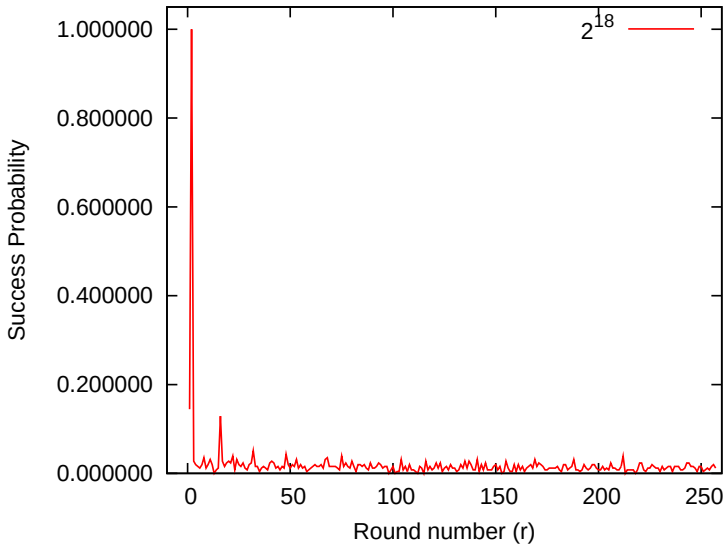


図 35: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{18} samples (three candidates)

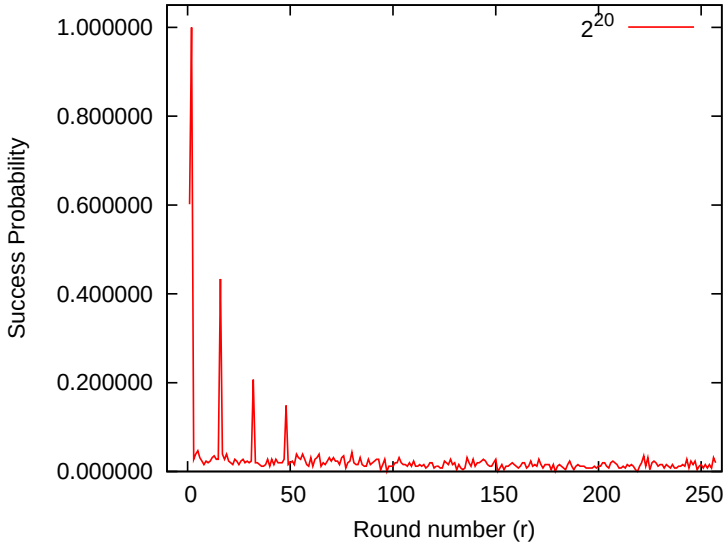


図 36: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{20} samples (three candidates)

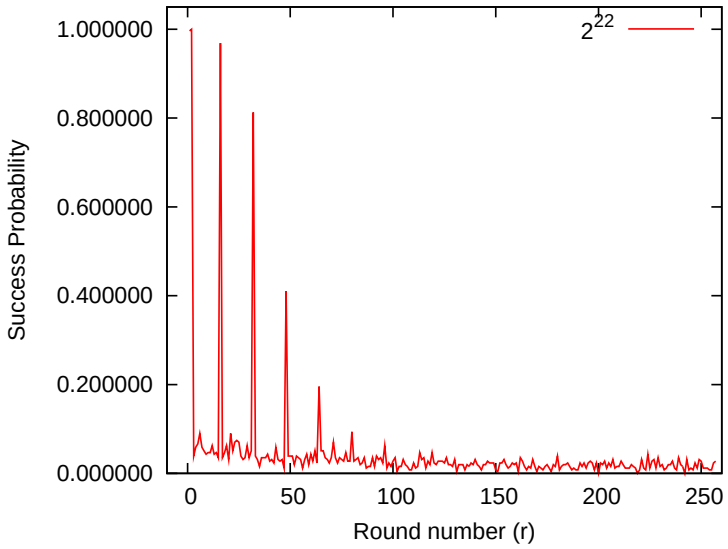


図 37: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{22} samples (three candidates)

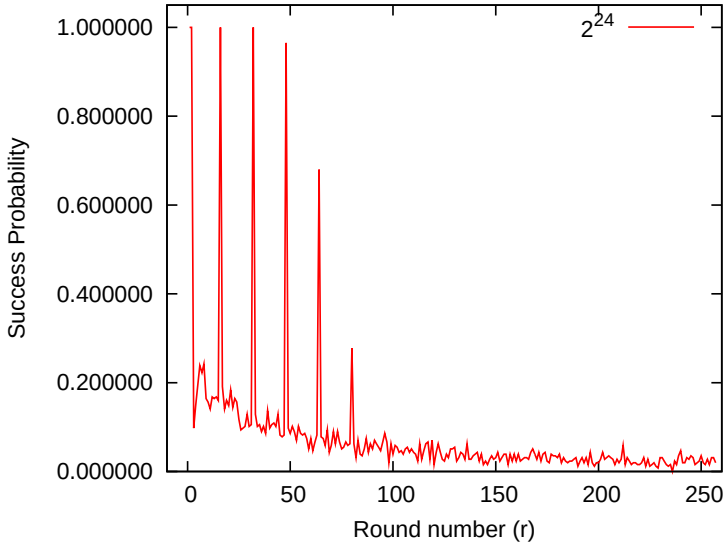


図 38: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{24} samples (three candidates)

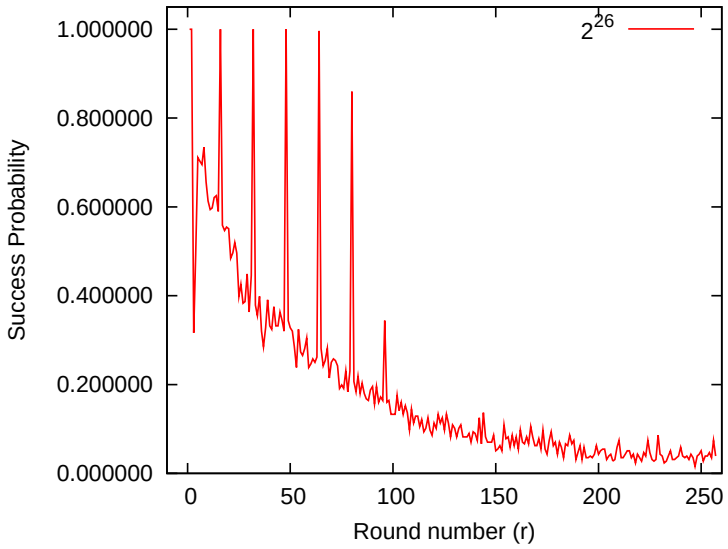


図 39: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{26} samples (three candidates)

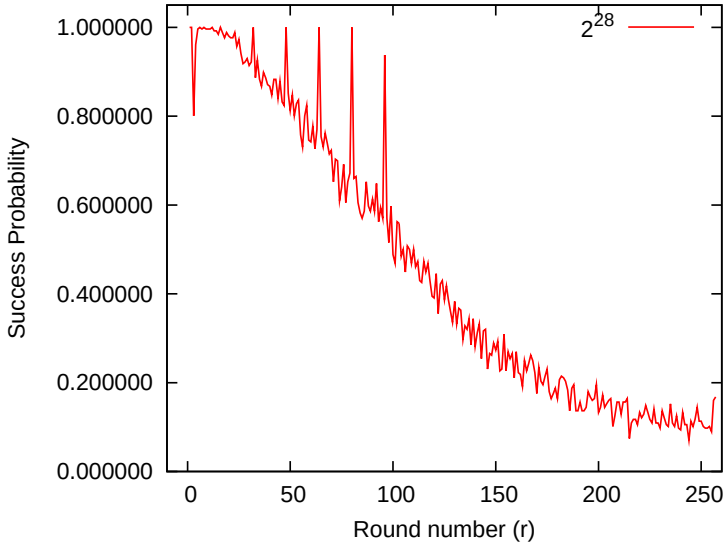


図 40: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{28} samples (three candidates)

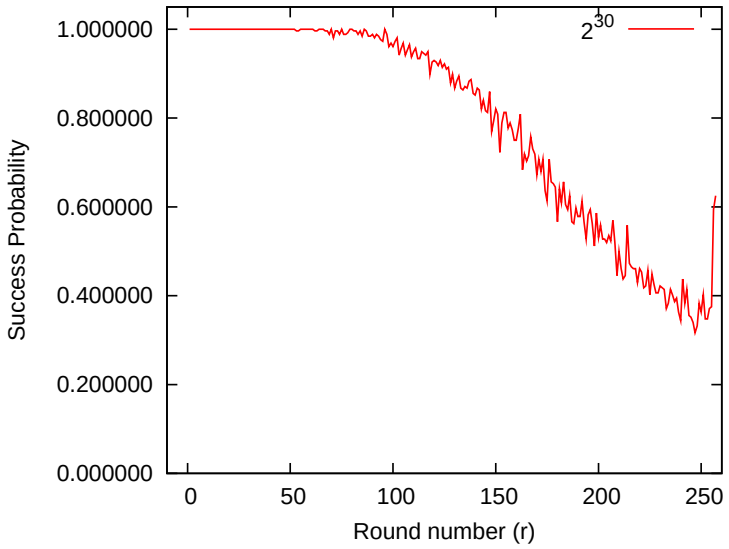


図 41: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{30} samples (three candidates)

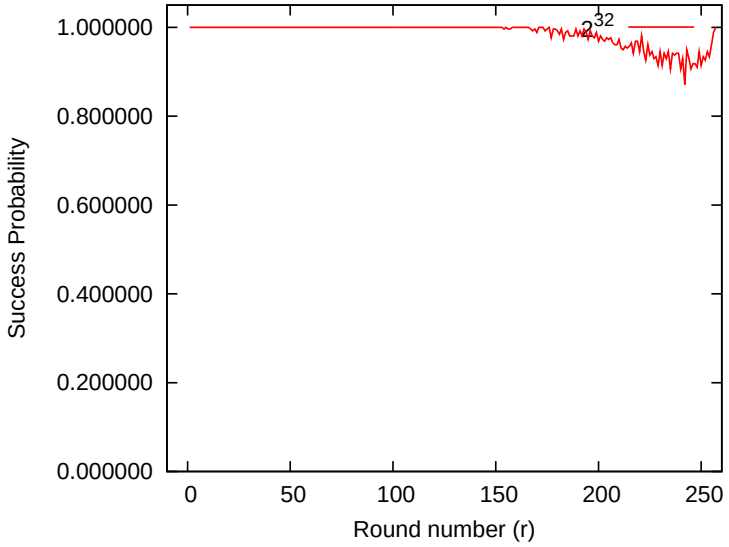


図 42: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{32} samples (three candidates)

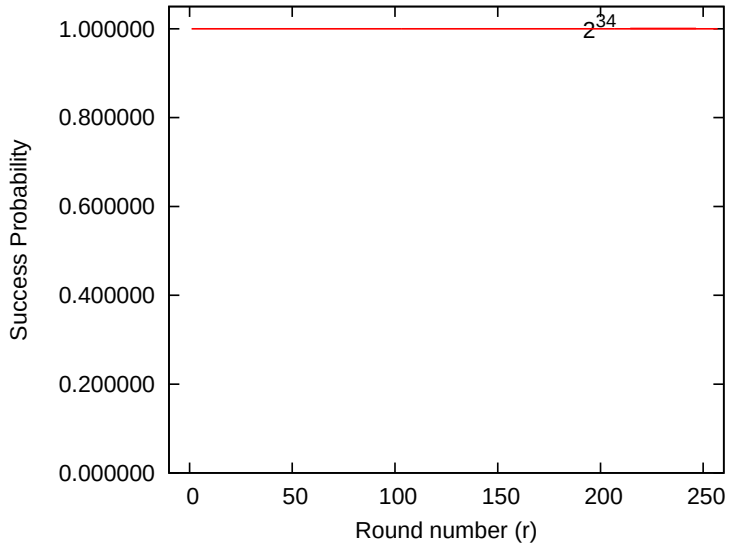


図 43: Success probability for P_r $(1 \leq r \leq 257)$ with 2^{34} samples (three candidates)