解 説

離散対数問題解読世界記録更新への道
―676ビットの解読―

林 卓也　　高木 剛
九州大学大学院 数理学研究院
（2009年時，公立はこだて未来大学所属）

2009年12月，筆者らの所属するグループは有限体上の離散対数問題において，従来の解読世界記録を大きく上回る676ビットの離散対数問題の解読に成功した．本稿では，有限体上の離散対数問題とその解読アルゴリズム，解読実験の歴史について解説するとともに，676ビットの離散対数問題解読世界記録で利用した解読アルゴリズムや計算環境などについて報告する．

離散対数問題の解読記録更新

筆者らの所属する解読グループは2009年12月9日に有限体上の離散対数問題において，有限体GF($3^{6\cdot71}$)（位数: 676ビット）上の離散対数問題の計算に成功した．この結果により，2005年9月22日にフランスの研究者Joux, Lercierらのグループによって達成された613ビットの離散対数問題の解読記録を約60ビット更新した．この計算実験は独立行政法人情報通信研究機構と公立はこだて未来大学の共同研究の一環として行われた．

2010年2月23日に解読記録の更新についてプレスリリースを行い，新聞等から取材を受け，新聞やニュースサイトに掲載された．また，この結果は2010年5月にパリで開催された国際会議PKC 2010で発表を行った[5]．

離散対数問題

8月号青木和麻呂氏による解説記事「素因数分解技術の進展―RSA-768の分解達成への道のり―」は，公開鍵暗号の1つであるRSA暗号の安全性と密接な関係のある素因数分解問題についての解説であった．本稿では，素因数分解問題と同様に公開鍵暗号の安全性と密接に関係している計算問題である離散対数問題について解説する．素因数分解問題はRSA暗号の安全性と関係しているが，離散対数問題はDiffie-Hellman鍵交換やアメリカ政府標準ディジタル署名方式であるDSA，最近ではペアリング暗号など，さまざまな公開鍵暗号方式の安全性と関係している．本章では簡単な例を基に離散対数問題とは何か説明する．

次のような集合を考える．

$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

この集合は「整数a, bを乗算$a\times b$し，その結果を11で割って余りを取る$a\times b \pmod{11}$」という演算において閉じている．すなわち，$a, b \in S$に対し，$a\times b \pmod{11}$の結果が必ずSに入る．また，この演算は整数における乗算の自然な拡張であることから，結合法則$(a\times b)\times c \equiv a\times(b\times c) \pmod{11}$を満たすことが分かる．さらに，

$1\times1 \equiv 1 \pmod{11}$, $2\times6 \equiv 1 \pmod{11}$,
$3\times4 \equiv 1 \pmod{11}$, $4\times3 \equiv 1 \pmod{11}$,
$5\times9 \equiv 1 \pmod{11}$, $6\times2 \equiv 1 \pmod{11}$,

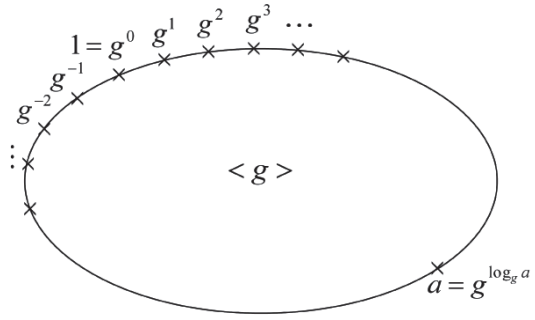

図 -1　巡回群と離散対数問題

$7\times8 \equiv 1 \pmod{11}$, $8\times7 \equiv 1 \pmod{11}$,

$9\times5 \equiv 1 \pmod{11}$, $10\times10 \equiv 1 \pmod{11}$,

となることから，集合Sの任意の元aに対して$a\times a^{-1} \equiv 1 \pmod{11}$を満たす逆元$a^{-1}$が集合$S$に存在する．このため，集合$S$は単位元が1で位数10の乗法群である．また，

$2^0 \equiv 1 \pmod{11}$, $2^1 \equiv 2 \pmod{11}$,

$2^2 \equiv 4 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$,

$2^4 \equiv 5 \pmod{11}$, $2^5 \equiv 10 \pmod{11}$,

$2^6 \equiv 9 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$,

$2^8 \equiv 3 \pmod{11}$, $2^9 \equiv 6 \pmod{11}$,

$2^{10} \equiv 1 \pmod{11}$,

となることから群Sのすべての元は，指数部eが$0 \le e < 10$の範囲で2^eとして重複なく表現でき，巡回していることが分かる（$2^{10} \equiv 2^0 \pmod{11}$, $2^{11} \equiv 2^1 \pmod{11}$, ...である）．すなわち，$S$は2で生成される位数10の巡回群である．このとき，$S=<2>$と表現し，2をSの生成元と呼ぶ．

さて，上記の群Sにおいて，2を何乗すると10となるだろうか？　上記の表から$2^5 \equiv 10 \pmod{11}$より，この問題の答えは5であることが分かる．この問題が離散対数問題である．より一般には，生成元gによって生成される巡回群$G=<g>$の元$a \in G$において，「gを何乗するとaとなるか?」という問題である．このべき部分を通常の対数と同様に$\log_g a$と書く（**図-1**を参照）．$\log_g a$はGの位数Nに対し，$0 \le \log_g a < N$の範囲で一意に定まる整数である．

離散対数問題の難しさは，群Gの位数すなわちGの元の個数に依存する．上記の群Sでは，位数が10だったため2のべき乗を10回計算することですべての元を網羅することができた．しかしこのような総当たり法では，位数がより大きい群，たとえば2^{80}程度を位数に持つような群では，すべての元を計算するのに2^{80}回の群演算が必要となるため，現在のスーパーコンピュータを利用しても計算することが困難になる．現在，一般の巡回群における離散対数問題に対し最も高速な計算方法としてPollardのρ法が知られており，このアルゴリズムの計算量は位数Nに対し$O(\sqrt{N})$である．2^{160}程度の位数を持つ巡回群の離散対数問題をPollardのρ法で解くには2^{80}回程度の演算が必要となるため，2^{160}程度の位数の一般巡回群における離散対数問題を解くことは困難であると考えられている．

■ 有限体上の離散対数問題

先ほどの群Sに0を加えた集合

$\overline{S} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

は加法$a+b \pmod{11}$においても群であり，体となることが分かる．このように，有限個の元からなる体を有限体と呼び，その位数がqの場合，GF(q)と書く．集合$\overline{S}$は位数11の有限体であるため，GF(11)と書ける．有限体の位数は素数pのべきp^n（n：正整数）となることが知られている．たとえば，GF(2^3)は多項式を用いて

$GF(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

と表現できる．このとき，有限体の構造を実現するためにGF(11)における「11で割って余りを取る（mod 11)」という演算に相当するものとして，「GF(2)の元を係数とする3次の既約多項式$f(x)$（$f(x)=x^3+x+1$など）で割って余りを取る（mod $f(x)$)」という演算を行う必要がある．一般に，有限体GF(p^n)から0を除いた集合は位数(p^n-1)の乗法巡回群になることが知られており，これをGF(p^n)*と書く．本稿では，GF(p^n)*における離散対数問題について考える．これをGF(p^n)上の離散対数問題と呼ぶ．

以降の章では，GF(p), GF(2^n)，および$n \ne 1$, $p \ne 2$である有限体GF(p^n)について考える．GF(p)は素体

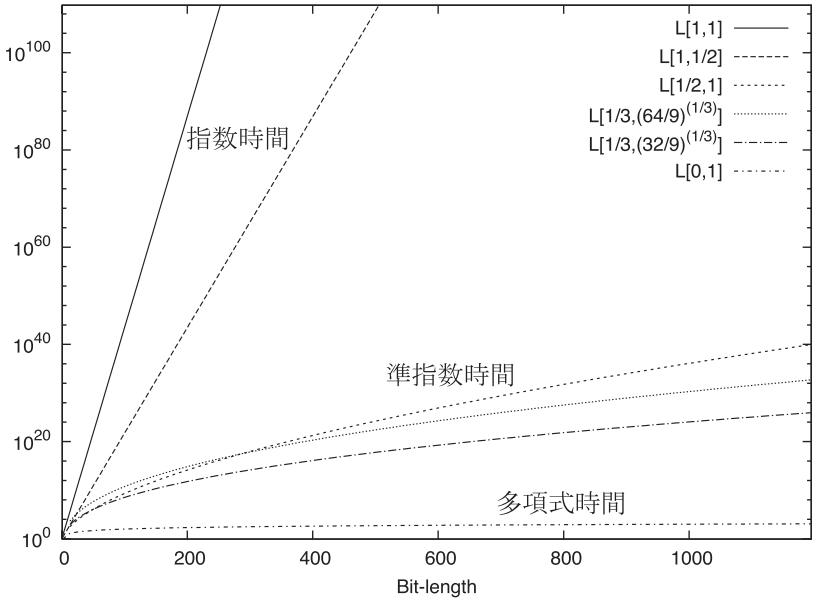

図-2　関数 $L_{p^n}[s, c]$ のグラフ．s=1 で指数時間，s=0 で多項式時間，0<s<1 で準指数時間を表す．

と呼ばれ，前に述べたようにDiffie-Hellman鍵交換やDSA，Elgamal暗号など，さまざまな離散対数暗号系に利用されている．GF(2^n)は，演算をビット列に対する演算(排他的論理和など)のみで記述できるため高速実装が可能である一方，後に述べるように早くからGF(2^n)上の離散対数問題をより効率的に解読できるアルゴリズムが知られており，暗号で利用されることは少ない．GF(p^n)上の離散対数問題は，2000年頃から研究が活発に行われているトーラス暗号やペアリング暗号の安全性と密接に関係することから，近年，解読実験が頻繁に行われている．

解読アルゴリズム

有限体上の離散対数問題では，指数計算法と呼ばれる高速な解読アルゴリズムが提案されており，GF(p^n)における$p^n \to \infty$に対する漸近的な計算量は，関数

$$L_{p^n}[s, c] = \exp((c+o(1)) (\log p^n)^s (\log \log p^n)^{1-s}) \quad (1)$$

を用いて表される．ただし，cは定数，sは$0<s<1$の範囲の実数であり，$o(1)$は$p^n \to \infty$で$o(1) \to 0$となる関数である．ここで，式(1)は，p^nのビット長に対しs=1で指数時間，s=0で多項式時間を表し，0<s<1では指数時間より高速かつ多項式時間より低速である準指数時間といわれるクラスを表す．**図-2**に，指数時間，多項式時間，および主要な準指数時間のグラフを示す．横軸は式(1)における位数p^nのビット長，縦軸は式(1)で$o(1)=0$とした計算量を対数表示で表している．指数時間と比較して，準指数時間が高速であることが分かる．

一方，位数が1000ビット程度では，後に述べる式(3)と式(4)の計算量である$L_{p^n}[1/3, (64/9)^{1/3}]$と$L_{p^n}[1/3, (32/9)^{1/3}]$が，それぞれ$10^{30} \approx 2^{100}$，$10^{24} \approx 2^{80}$ほどであり，$L_{p^n}[1/3, c]$の解読アルゴリズムを用いても現在の計算機では現実的な時間で解読を行うことが困難であると考えられる．しかし，このグラフは漸近的な計算量を基にした評価であるため，現実の暗号システムで利用される1000ビットから3000ビット程度の位数での正確な振舞いを知るためには，解読実験を行う必要がある．

■ 指数計算法

指数計算法のアイディアは1920年代にKraitchikによって考案されており，その後1970年代に素因数分解や離散対数問題の計算に応用された．1979年にAdlemanによって提案された指数計算法[1)]はGF(p)上の離散対数問題にのみ適用でき，その計算量は$L_p[1/2, c]$となることが示されている．本章では，指数計算法の例としてGF(p)におけるAdleman

の指数計算法を紹介する．

gをGF(p)*の生成元とし，$a \in$ GF(p)*の離散対数$\log_g a$を計算することを考える．ここで，NをGF(p)*の位数とする．すなわち，$N=p-1$である．

Step 1. ランダムに$z \in \{0, 1, ..., N-1\}$を取り，$g^z \bmod p$を計算し，$g^z \bmod p$を素因数分解する．ここで，$(g^z \bmod p) \in$ GF(p)*の因数分解が整数における素因数分解と一致している点がポイントである．ある閾値B以下の素数でのみ$g^z \bmod p$が割れていれば，

$$g^z \bmod p = \prod_{p_i \le B} p_i^{e_i} \quad (p_i: \text{素数})$$

と書くことができる．この式の対数を取ると，

$$z \equiv \sum_{p_i \le B} e_i \log_g p_i \pmod N \tag{2}$$

となる．「離散対数問題」章で述べたように，対数は(mod N)で計算する．これにより，$\log_g p_i$を変数とする法Nの合同式が得られる．Step 1を繰り返し行い，多くの関係式(2)を集める．

Step 2. 得られた関係式(2)を用いて連立1次合同式を構成し，それを解くことで，$\log_g p_i$を得る．

Step 3. 最後に，再度zをランダムにとり，今度は$ag^z \bmod p$について同様の計算をし，

$$ag^z \bmod p = \prod_{p_i \le B} p_i^{f_i}$$

となる分解が得られたとき，

$$\log_g a \equiv \sum_{p_i \le B} f_i \log_g p_i - z \pmod N$$

により，求めたい離散対数$\log_g a$が得られる．

■数体篩法・関数体篩法

1990年代には，素因数分解問題で提案された数体篩法（すうたいふるいほう）を応用してGF(p)上の離散対数問題を計算する手法がGordonによって提案され[4]，また，その多項式環上のアナロジーとして，関数体を利用してGF(p^n)上の離散対数問題を計算する関数体篩法（かんすうたいふるいほう）がAdlemanによって提案された[2]．数体篩法では，整数上での素因数分解と代数体での素イデアル分解を考え，そのアナロジーである関数体篩法では，多項式の既約多項式分解と関数体での素因子分解を考える．詳細については文献2)，4)を参照いただきたい．

数体篩法，関数体篩法は主に次の4ステップからなる．

Step i. 多項式選択ステップ：数体篩法，関数体篩法で利用するパラメータを選択するステップで，前節で述べた指数計算法にはない新たなステップ．数体篩法ではより高速に解読可能な「良いパラメータ」を探索する必要があるが，関数体篩法では良いパラメータを探索する効率的な方法が知られている．

Step ii. 関係探索ステップ：式(2)のような離散対数に関する関係式を集めるステップ．本質的には指数計算法のStep 1と同じだが，数体篩法や関数体篩法では「篩」と呼ばれる関係式を効率的に探索する計算方法が知られており，数体篩法では整数上で，関数体篩法では多項式環上で篩を行う．

Step iii. 線形代数ステップ：関係探索ステップで得られた連立1次合同式を解くステップ．指数計算法のStep 2と同じ．

Step iv. 特定の元の離散対数計算ステップ：線形代数ステップで得られた解から特定の元の離散対数を計算するステップ．指数計算法のStep 3と同じだが，数体篩法や関数体篩法でのみ利用できる高速なアルゴリズムが知られている．

離散対数問題における数体篩法や関数体篩法は，8月号素因数分解解説記事にて述べられた素因数分解における数体篩法と数学的に同じ原理に基づいており，実際に多項式選択ステップや関係探索ステップ☆1ではほぼ同じ計算をする．しかし，残り2ステップは素因数分解と離散対数問題で異なる計算をする．線形代数ステップは，素因数分解では(mod 2)で計算するのに対し，離散対数問題では位数Nに対して(mod N)で計算を行う．また，特定の元の離散対数計算ステップは素因数分解にはない離散対数問

☆1 8月号素因数分解解説記事の「数体篩法」章の「篩」が関係探索ステップにあたる．

題特有のステップである．

数体篩法や関数体篩法は指数計算法の準指数時間$L_{p^n}[1/2, c]$より高速なアルゴリズムであり，計算量は$L_{p^n}[1/3, c]$となることが示されている．ただし，GF(2^n)については，1984年にCoppersmithによって提案されたCoppersmith法[3]があり，計算量は同様に$L_{2^n}[1/3, c]$である．この後，SchirokauerやAdleman, Huangによって数体篩法，関数体篩法の適用範囲や計算量が改良され，数体篩法の計算量は，

$$L_{p^n}[1/3, (64/9)^{1/3}] \ (\log p > n^2) \quad (3)$$

関数体篩法の計算量は，

$$L_{p^n}[1/3, (32/9)^{1/3}] \ (p \leq n^{o(\sqrt{n})}) \quad (4)$$

となった．しかし，上記のp, nに対する条件を満たさない有限体については1993年にAdleman, Demarraisによって提案された指数計算法が最速で，$p>n$に対し$L_{p^n}[1/2, 2]$，$p<n$に対し$L_{p^n}[1/2, \sqrt{2}]$であり，$L_{p^n}[1/3, c]$となるアルゴリズムは知られていなかった．

このギャップを埋めたのが，2006年にJoux, Lercier, Smart, Vercauterenによって提案された数体篩法である[6]．この数体篩法では，$p \geq L_{p^n}[1/3, c]$となるGF(p^n)上の離散対数問題を$L_{p^n}[1/3, c]$で計算可能である．これにより，すべてのGF(p^n)上の離散対数問題に対して$L_{p^n}[1/3, c]$での計算が可能となった．また，$\log p \approx \sqrt{n} \log n$を満たす場合は，さらに高速に計算が可能な関数体篩法の改良が2005年にJoux, Lercierによって提案されており，$L_{p^n}[1/3, 3^{1/3}]$での計算が可能である．

離散対数問題解読の歴史

1980年代までは離散対数問題の解読実験に関する発表はほとんど行われていなかったが，1989年にMcCurleyによって離散対数問題解読コンテスト“McCurley's challenge”（賞金$100）が発表されるなど，1980年代後半から有限体GF(p)やGF(2^n)に対する解読実験に関する発表が報告されるようになった．1991年にLaMacchia, Odlyzkoによって報告された解読実験では，ネットワークファイルシステムの個人認証で実際に利用されていたGF(p)（p:192ビットの素数）上の離散対数問題の解読に成功した．また，1992年にGordon, McCurleyによってGF(2^{401})上の離散対数問題の解読が行われた．

数体篩法が提案された1992年以降は，数体篩法を利用して解読記録の更新が行われ，1998年にはDenny, Weberのグループが，約3カ月の計算の末にMcCurley's challengeであるGF(p)（p:427ビットの特殊な素数）の解読に成功し，CRYPTO '98においてMcCurleyより賞金$100が授与された．

2000年代に入ると解読実験がさらに活発に行われ，以下のように解読記録の更新が行われた．2001年にJoux, Lercierのグループによって GF(2^{521})上の離散対数問題が解読され，翌年2002年にはThoméのグループが，1年超という長い計算の末，GF(2^{607})上の離散対数問題の解読に成功した．さらに2005年にはJoux, Lercierのグループが GF(p)（p:431ビットの素数），GF(2^{613})，GF(370801^{30})（556ビットの位数）など，さまざまな有限体の離散対数問題解読世界記録を樹立した．この解読記録更新は，計算機性能の進歩だけでなく，Joux, Lercierらが自ら提案した関数体篩法や数体篩法のアルゴリズムの改良によるところが大きい．このように，解読アルゴリズムの進歩が解読記録を伸ばす大きな要因となっている．

解読アルゴリズムの進歩と計算記録のビット長のグラフをGF(p)，GF(2^n)，GF(p^n)に分け，**図-3**に示す．また，現在の有限体上の離散対数問題計算世界記録を**表-1**に示す．それぞれの世界記録の実験環境および計算時間と比較して8月号素因数分解解説記事で述べられた規模が非常に大きいのは，素因数分解の困難性が公開鍵暗号のデファクトスタンダードであるRSA暗号の安全性の根拠であるため，現在までに多くの大規模解読実験により世界記録が更新されており，さらなる記録更新には数グループが共同で数年規模の計算を行う必要があったためと思われる．

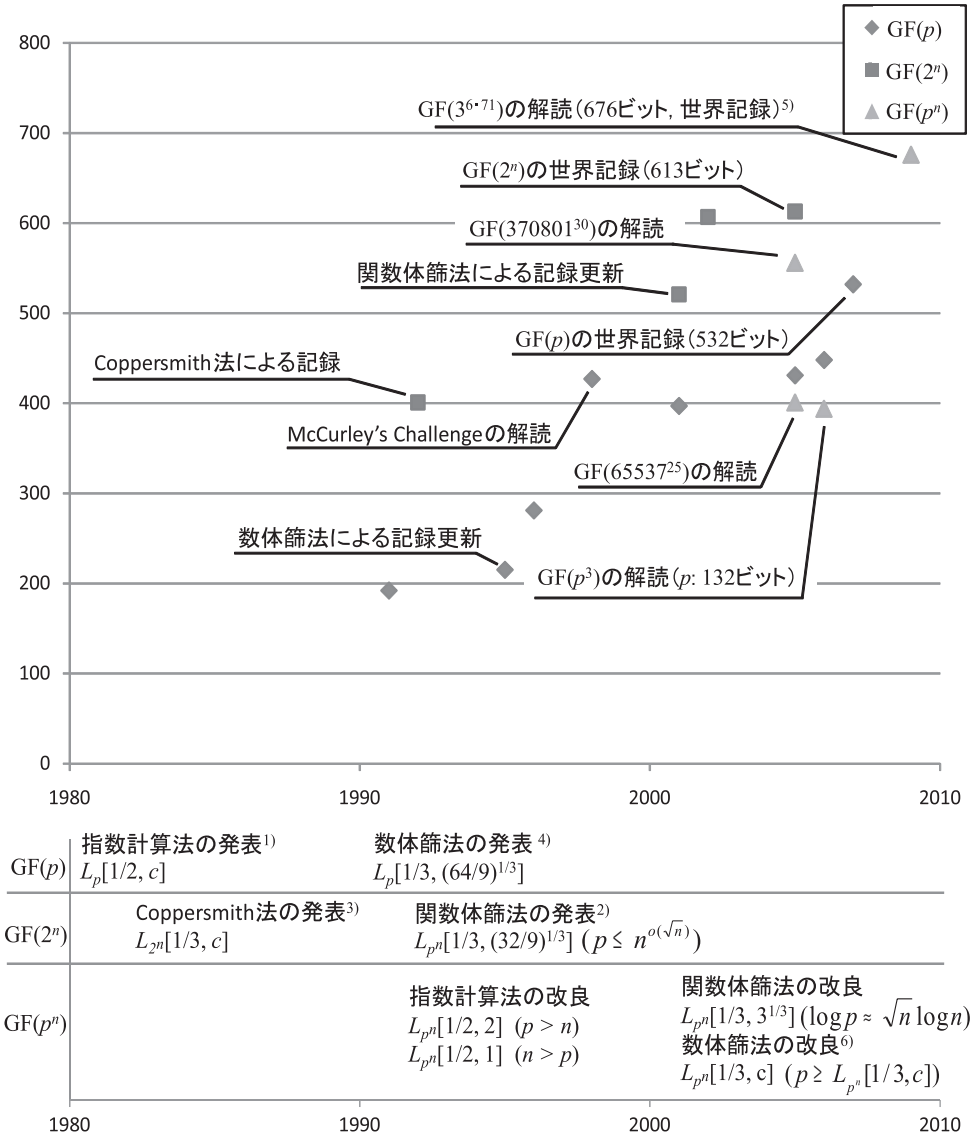

図 -3　有限体上の離散対数問題の解読アルゴリズム（下図）と解読記録の進展（上図）

有限体	GF(p)	GF(2^n)	GF(p^3)	GF(370801^{30})	**GF(3^{6n})**
発表者	Kleinjung ら*1	Joux ら*2	Joux ら*3	Joux ら*2	**林ら*4**
日付	2007/2/5	2005/9/22	2006/8/23	2005/9/11	**2009/12/9**
アルゴリズム	数体篩法	関数体篩法	数体篩法	関数体篩法	**関数体篩法**
計算環境（関係探索ステップ）	Many CPUs	4 nodes of 16 Itanium 2 (1.3GHz)	16 Alpha processors (1.15GHz)	16 Alpha processors (1.15GHz)	**Xeon (2.83GHz) 計 96 コア**
計算環境（線形代数ステップ）	12-24 Xeon (3.2GHz)	4 nodes of 16 Itanium 2 (1.3GHz)	16 Alpha processors (1.15GHz)	16 Alpha processors (1.15GHz)	**Xeon (2.83GHz) 計 80 コア**
計算時間	33 日	17 日	19 日	0.5 日	**33 日**
ビット長	532	613	394	556	**676**

*1 ドイツのボン大学数学研究所のグループによる実験.
*2 フランスの国防省およびレンヌ数学研究所のグループによる実験.
*3 フランスの国防省，レンヌ数学研究所，イギリスのブリストル大学およびベルギーのレーベン大学のグループによる実験.
*4 公立はこだて未来大学および情報通信研究機構のグループによる実験.

表 -1　有限体上の離散対数問題の解読世界記録

図-4　解読に利用したサーバ. Quad-Core Xeon 搭載のラックサーバ 12 台，Quad-Core Xeon × 2 搭載のサーバ 6 台の計 18 台.

解読世界記録更新の概要

筆者らが所属する解読グループが行った解読記録の更新について述べていく．扱った問題は，次世代公開鍵暗号として注目を集めているペアリング暗号の安全性の根拠となっている$GF(3^{6n})$上の離散対数問題である．計算環境から現実時間で計算可能なビット長の最大値を算出し，今回は$GF(3^{6\cdot 71})$上の離散対数問題の計算を行った．この有限体の位数は676ビットであり，有限体上の離散対数問題の計算世界記録の中でも最も大きなビット長である．解読アルゴリズムは，2006年にJoux, Lercierによって提案された関数体篩法を用いた．我々は関係探索ステップに多項式篩，線形代数ステップに並列Lanczos法，特定の元の離散対数計算ステップにspecial-q descentを実装した．さらに，自明な離散対数の関係式であるfree relationの利用や，線形代数ステップで扱う連立1次合同式の未知数を圧縮するGalois actionなどの高速化手法を利用することで，関係探索ステップは8倍，線形代数ステップは36倍の高速化に成功した．計算はIntel Quad-Core Xeon E5440 (2.83GHz) × 2 CPUs, 16GB RAMを搭載した計算機が5台，Intel Quad-Core Xeon X5355 (2.66GHz) × 2 CPUs, 16GB RAMを搭載した計算機が1台，Intel Quad-Core Xeon L5420 (2.33GHz) × 1 CPU, 4GB RAMを搭載した計算機が12台の計18台，96コアを使用した（**図-4**）．計算の詳細については文献5)を参照いただきたい．

2009年9月下旬から計算を開始し，当初の予定では10月下旬に終了予定だったが，計算の大規模化による想定外のバグがいくつか発見され，そのバグフィックスに時間を要したため，最終的には12月9日まで解読実験を行う必要があった．

今回の計算では$GF(3^{6\cdot 71})$を$GF(3^6)$の71次拡大体として表現する．この際$GF(3^6)$は，適当な6次のGF(3)上既約多項式をランダムに選ぶことにより，$GF(3)[z]/(z^6+2z+2)$と構成した☆2．また，$GF(3^6)[x]$の元を表現するために，ある整数を3進展開したときのi桁を$z^{((i-1) \bmod 6)}\ x^{\lfloor (i-1)/6 \rfloor}$の係数とする写像$\psi$を定義する．たとえば，0xを16進表記の接頭語としたとき，$\texttt{0x2dd}=(1000011)_3$であるから，$\psi(\texttt{0x2dd})=x+(z+1)$となる．

71次の既約多項式として次のものを計算し，$GF(3^{6\cdot 71})$を$GF(3^6)[x]/(f(x))$として構成した．

$$f(x) = \psi(\texttt{0x9 2d3e5daf 5ac01130}$$
$$\texttt{4e6909f7 09cc8833 baa757d3}$$
$$\texttt{17dc6f99 9c8b98b5 ab8baa01}$$
$$\texttt{d68ec151 aec39e2e ed081c79}$$
$$\texttt{d851066b 3ffb2a4f a3e19c1e}$$
$$\texttt{cef46675 0918a26d 9c7cacd4}$$
$$\texttt{8d74ccfe 2c1d3b79 e81e6138}$$
$$\texttt{ab06aef4}).$$

生成元$g=\psi(\texttt{0x456})=x+(z^5+z^4+2z^3+z)$に対し次の元（$\psi$（円周率$\pi$の10進上位202桁））をターゲットとして離散対数の計算を行う．

$$\pi(x) = \psi(\lfloor \pi \times 10^{202} \rfloor)$$
$$= (z^4+z^3+2z^2+1)x^{70}+\ldots$$
$$+ (z^5+2z^4+2z^3+z^2+2)$$

計算の結果，$\pi(x)$の離散対数$\log_g \pi(x)$が次のように得られた．

☆2　$GF(3^6)$における乗算，逆元演算，3乗算等の既約多項式が関係する演算は，事前計算したテーブルを利用して計算した．このため，これらの演算速度は既約多項式の選び方によらない．

$\log_g \pi(x)$ = 0x8 78b54797 2fb6ff9b
57add5d5 11f69de6 a3853f98
68d53cc0 5b531076 2872ac6a
320874bf ba6d66d6 8e5e245f
39778f02 31ae791a acbab8c7
5ee6850c 9f5df0e5 f6b8ab0b
95d8bdb1 aea95b1f bad82465
25590f66.

676ビットの解読記録の意義

本稿では，離散対数問題の概要と有限体上の離散対数問題の解読アルゴリズム，解読実験の歴史について解説し，筆者らが所属するグループが達成した676ビットの有限体上の離散対数問題解読世界記録の概要について述べた．

676ビットの離散対数問題は，現状安全であるとされる1000ビット程度のものと比べると300ビット以上の大きな差があり，今回利用した解読環境では1000ビット程度の離散対数問題を解くには数百年単位の時間が必要である．しかし，今回の解読実験ではまだ利用していない高速化技術がいくつかあり，さらに解読記録が伸びることが予想できるため，この解読記録が1000ビット程度の離散対数問題が現実時間では解読困難であることを保証するものではない．

また，今回扱った有限体GF(3^{6n})の離散対数問題の困難性は，次世代公開鍵暗号として注目を集めているペアリング暗号の安全性の根拠となっている．ペアリング暗号の安全性評価を行うためには，今後も継続的に解読実験を行い，その困難性を精密に評価していく必要があるだろう．

謝辞　本解読実験は，CRYPTREC（http://www.cryptrec.go.jp/）の支援を受け，情報通信研究機構セキュリティ基盤グループとの共同研究の一環として実施されました．関係者の方々に深く感謝いたします．

参考文献

1) Adleman, L. M. : A Subexponential Algorithm for Discrete Logarithms with Applications to Cryptography, Proc. 20th Annual Symposium on Foundations of Computer Science (FOCS 1979), pp.55-60 (1979).
2) Adleman, L. M. : The Function Field Sieve, Proc. Algorithmic Number Theory Symposium (ANTS-I), Lecture Notes in Computer Science, Vol.877, pp.108-121 (1994).
3) Coppersmith, D. : Fast Evaluation of Logarithms in Fields of Characteristic Two, IEEE Transactions on Information Theory, Vol.IT-30, No.4, pp.587-594 (1984).
4) Gordon, D. M. : Discrete Logarithms in GF(p) using the Number Field Sieve, SIAM Journal on Discrete Mathematics, Vol.6, No.1, pp.124-138 (1993).
5) Hayashi, T., Shinohara, N., Wang, L., Matsuo, S., Shirase, M. and Takagi, T. : Solving a 676-bit Discrete Logarithm Problem in GF(3^{6n}), Proc. 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010), Lecture Notes in Computer Science, Vol.6056, pp.351-367 (2010).
6) Joux, A., Lercier, R., Smart, N. and Vercauteren, F. : The Number Field Sieve in the Medium Prime Case, Proc. Advances in Cryptology - CRYPTO 2006, Lecture Notes in Computer Science, Vol.4117, pp.326-344 (2006).

（平成22年7月1日受付）

林　卓也（学生会員）t-hayashi@math.kyushu-u.ac.jp

2008年公立はこだて未来大学システム情報科学部卒業．2010年同大学院システム情報科学研究科博士（前期）課程修了．現在，九州大学大学院数理学府博士後期課程在学中．2010年より日本学術振興会特別研究員DC1．本会コンピュータセキュリティシンポジウムCSS2009学生論文賞受賞．公開鍵暗号の安全性解析に関する研究に従事．電子情報通信学会学生会員，IACR会員．

高木　剛（正会員）takagi@math.kyushu-u.ac.jp

1993年名古屋大学理学部数学科卒業．1995年同大学院理学研究科修士課程修了．同年日本電信電話（株）入社．2001年Dr.rer.nat.（ダルムシュタット工科大学）．その後，ダルムシュタット工科大学情報科学部助教授を経て，2005年公立はこだて未来大学システム情報科学部准教授，2008年より同大学教授，2010年より九州大学大学院数理学研究院教授，現在に至る．第8回船井情報科学振興賞受賞．暗号および情報セキュリティに関する研究に従事．電子情報通信学会，IACR各会員．