ストリーム暗号安全性検証用
グレブナー基底計算プログラム
開発報告

2005年2月28日

株式会社アイビス
渡辺秀行

プロジェクト概要

- 内容
  - グレブナー基底を求めるプログラムを作成する
  - IPAのグリッドコンピュータ上で動作させる
- 目的
  - 暗号の安全性検証の研究に利用できるツールの提供
  - IPAのグリッドコンピュータの有効な利用法として

暗号の安全性検証との関連(1)

■■■

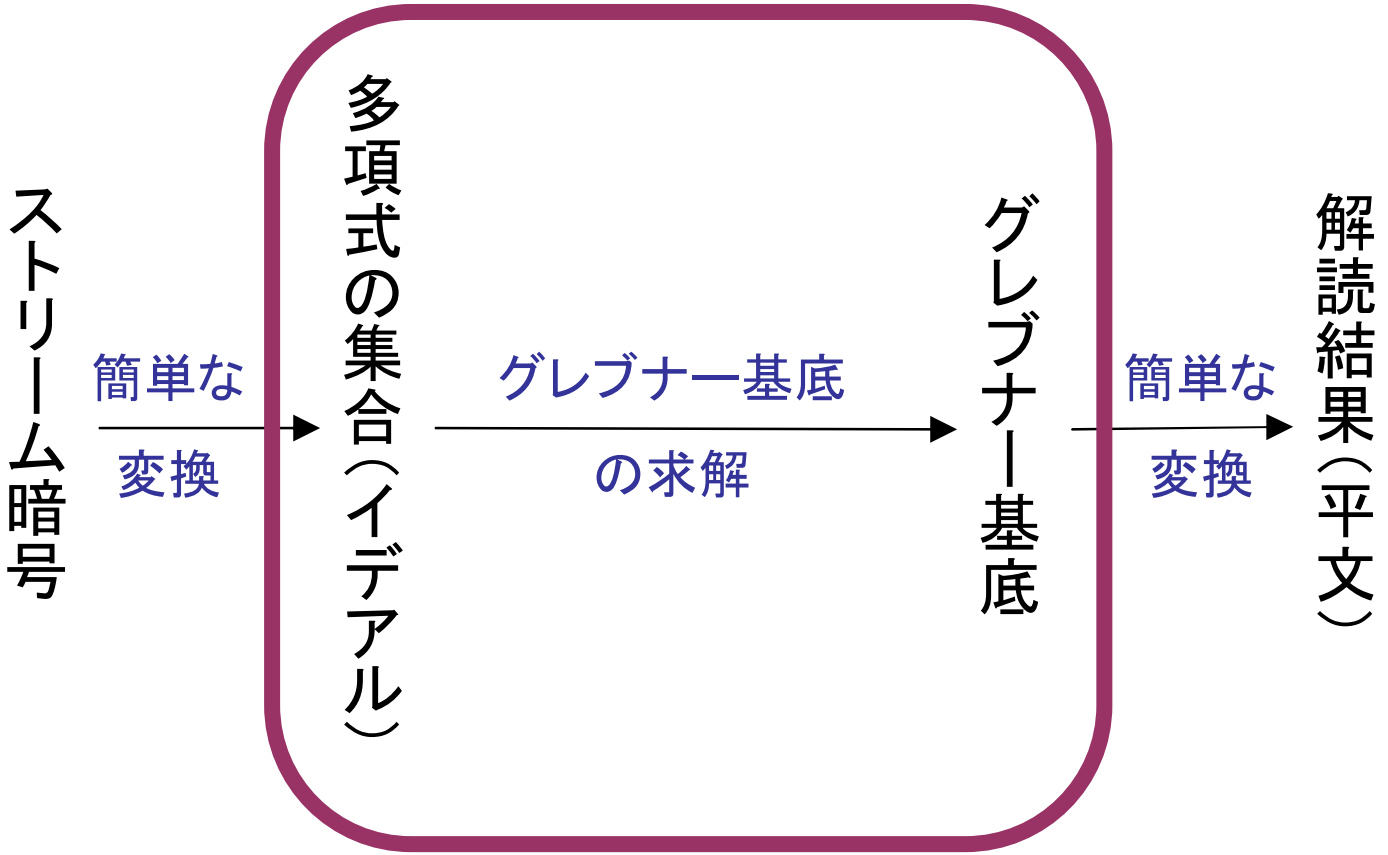
- 暗号の安全性検証とは
  - 検証対象の暗号が安全かどうかを判定する
  - 実際に解読できれば安全ではない
- 安全性の証明は？
  - 検証対象の暗号に対し、▪規模を縮小したものの解読に必要な時間を計測

  →実際の解読に必要なマシンパワーの推測

暗号の安全性検証との関連(2)

■ ■ ■

- 本プロジェクトの範囲(赤枠部分)



開発上の戦略(1)

- 開発の順序について
  - 並列化よりも、▪▪▪単体マシンでの動作速度改善を優先して行なった。これは単体動作の速度改善が100倍以上見込まれたからである。
    ▪
- 並列化の方針について
  - グリッドマシンの ▪構成の強み ▪を生かし、ノード間の通信はNFS経由とした。
  - 通信は大きな単位で行ない、通信の際のロスを防いだ。

開発上の戦略(2)

- 暗号系への適用のための戦略
  - 暗号系のグレブナー基底は線型式を含むことが多い。このことを利用して計算を省略することが可能
- 並列化の戦略
  - 通常の場合の並列化とは異なり、部分問題に分割し、再結合する方法をとった

成果 ―速度比較(1)

- 以下の入力で速度の比較を行なった
  - ベンチマークとして有名なcyclic(2n)（C2n)
  - Cnから最高次の式を省いたもの(Dn)
  - C5をReductionしたもの (R)
  - C5の式を一部変形し、非対称にしたもの(P)
  - 26文字からなる式(X)

成果―速度比較(2)

プログラム@環境＼ベンチマーク	7問題		X	D12	D13	D14	D15	D16	C10	C12	C14	C16
F2(改) cygwin@Pentium-M 1.5GHz	0.2	0.2	0.2	3.5	11.5	40.9	589	#	0.2	0.2	0.2	0.2
F2(改) @opteron(1mpu/1node)	0.2	0.2	0.2	2.1	7.8	25.1	218	1350	0.2	0.2	0.2	0.2
P2(改) @opteron(64mpus/64nodes)	*	*	*	8.7	9.6	22.3	48.7	476	*	*	*	*
Magma @Pentium-M 1.5GHz	φ	φ	φ	5	12	30	∞	∞	φ	φ	5	∞

単位(秒)

(注)

1. Magmaは現在最速と言われているグレブナー基底求解プログラム
2. F2・P2(改)は、単体mpu用のプログラム、P2(改)は、並列用のプログラム
   (ともに本プロジェクトの成果)

【凡例】

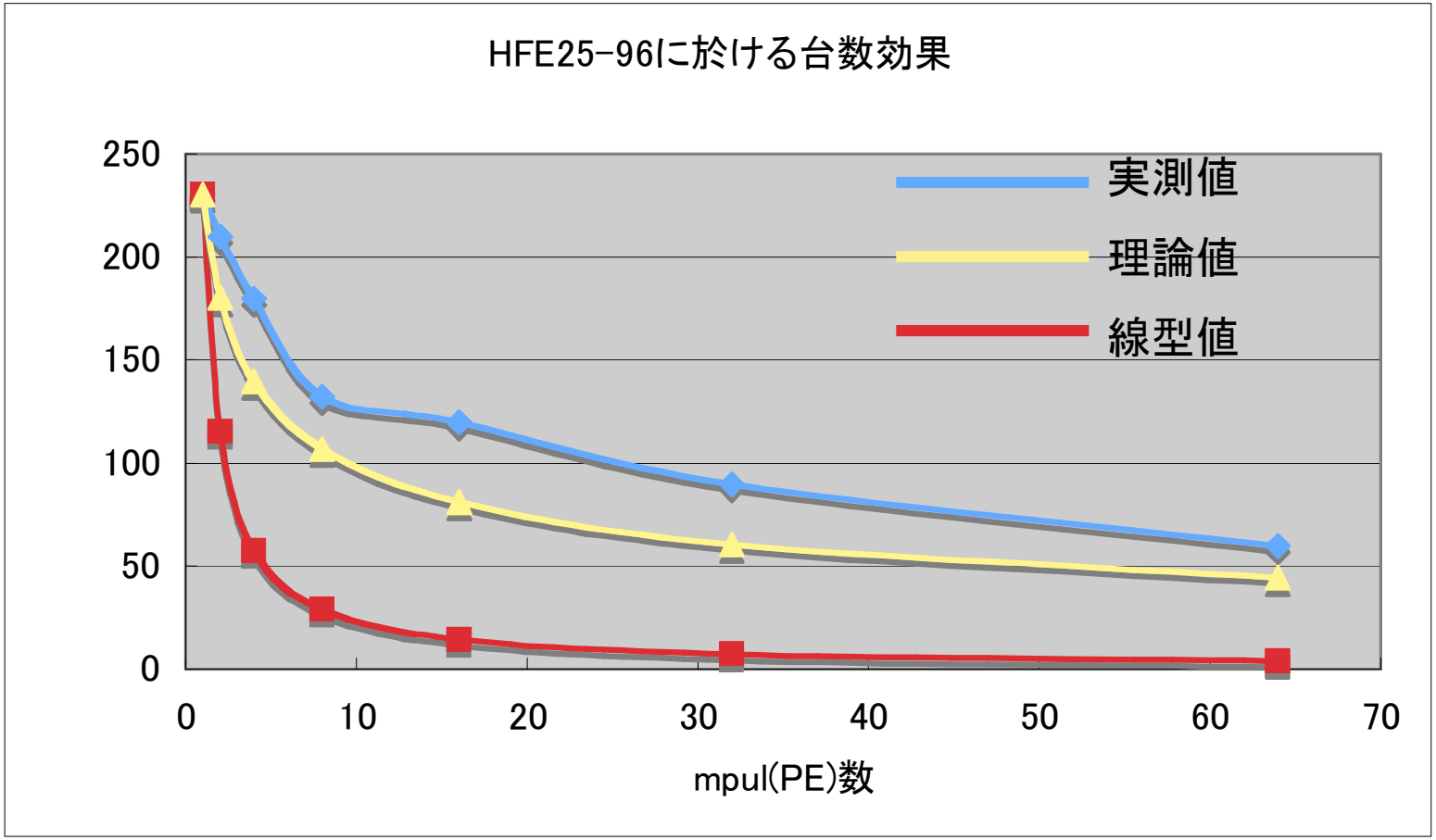
Φ: 1秒未満。Magmaは別のPCの時計を見ながら秒単位での測定

#: メモリ不足による終了

*: 単体mpuの場合にすでに1秒未満のため、並列による測定は行なっていない

∞: 計算が一向に進まないため、途中でプログラムを停止させた。おそらくメモリ不足と思われる。

HFE暗号への適用


HFE25-96に於ける台数効果
250
200
150
100
50
0
0
10
20
30
40
50
60
70
mpul(PE)数
実測値
理論値
線型値

課題、今後の展開

- 単体マシンアルゴリズムとして
  - 式の持ち方の改善（常に行列で持つなど）
  - 高速なrow echelon matrixの算出
  - 暗号に特化した戦略の研究
- 並列アルゴリズムとして
  - ペア単位での 並列化方法の 改良
  - 部分問題に分ける際、親子関係を多世代にすることの検討
  - 行列演算など、細部の単位での並列化