NICTにおける世界最先端の暗号安全性評価技術

ネットワークセキュリティ研究所
セキュリティ基盤研究室
盛合　志帆

ネットワーク社会の安全を守る暗号技術

ネットワークの発展とともに、暗号技術は
通信・交通・ビジネスの根幹を支える技術へ







暗号の安全性評価

日々進歩する解読技術や計算機能力を踏まえ
暗号技術の安全性を評価することは重要な課題

暗号の安全性
その暗号を最も効率のよいアルゴリズムで解読したときに必要な解読計算量（時間）で評価

– 解読計算量が2^k⇒その暗号の安全性は k ビット

例：2^{112}回の暗号化処理で鍵が見つかる場合
その暗号の安全性は 112ビットセキュリティ

暗号の安全性評価

Recommendation for Key Management – Part 1: General (Revised), NIST SP 800-57, 2007.

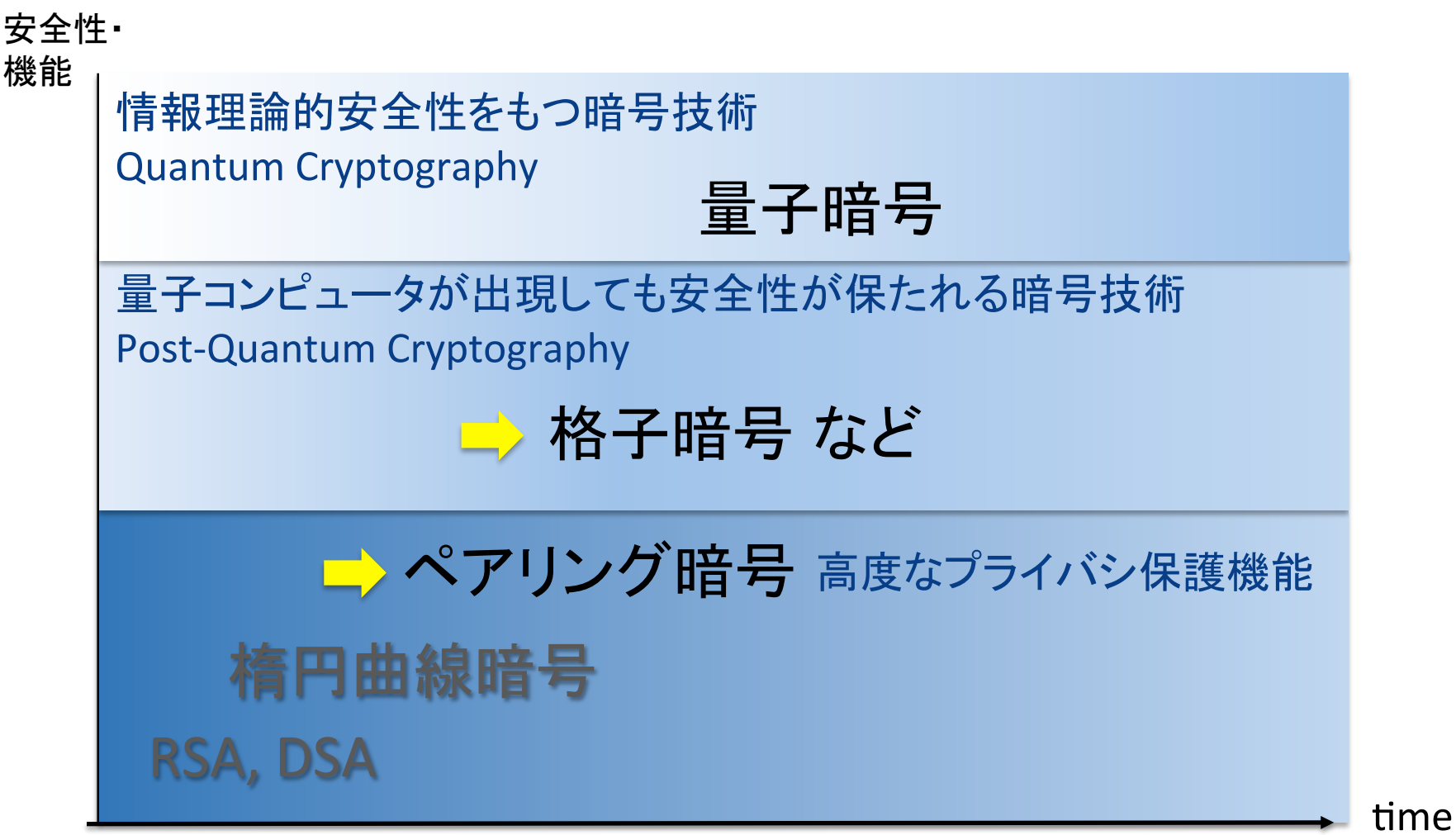
		暗号アルゴリズム強度指標に相当する鍵長 (bit)				
		～2010	2011～2030	2031～		
暗号アルゴリズム強度指標		80 bit セキュリティ	112 bit セキュリティ	128 bit セキュリティ	192 bit セキュリティ	256 bit セキュリティ
共通鍵暗号 (AESなど)		80	112	128	192	256
公開鍵暗号 デジタル署名	素因数分解問題に基づく方式 (RSAなど)	1024	2048	3072	7680	15360
	離散対数問題に基づく方式 (DSA, DHなど)	1024	2048	3072	7680	15360
	楕円曲線上の離散対数問題に基づく方式 (ECDSA, ECDHなど)	160	224	256	384	512
ハッシュ関数 (SHA-2など)		160	224	256	384	512

今年度達成した2つの世界記録

- **ペアリング暗号**の安全性評価
  - 次世代暗号の解読で世界記録を達成
    - ペアリング暗号の安全性を確立し、次世代暗号の標準化に貢献　(2012.6.18)

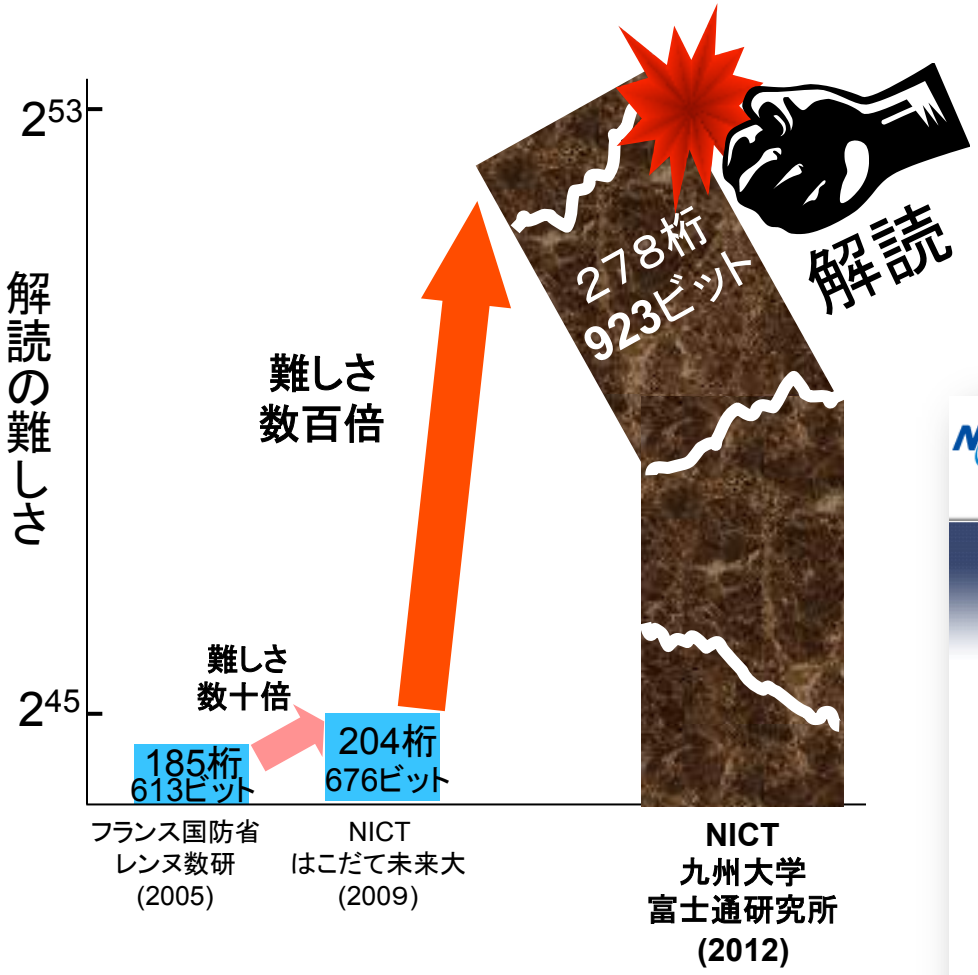
- **格子暗号**の安全性評価
  - クラウド向け暗号技術の安全性評価で世界新記録を達成
    - 暗号化したままデータを処理する“格子暗号技術”の実用化に向けて (2013.1.21)

次世代暗号


安全性・
機能
情報理論的安全性をもつ暗号技術
Quantum Cryptography
量子暗号
量子コンピュータが出現しても安全性が保たれる暗号技術
Post-Quantum Cryptography
格子暗号 など
ペアリング暗号
高度なプライバシ保護機能
楕円曲線暗号
RSA, DSA
time

ペアリング暗号の安全性評価

278桁のペアリング暗号解読成功 世界記録達成



「次世代暗号の解読で世界記録を達成
－ペアリング暗号の安全性を確立し、
次世代暗号の標準化に貢献－」
(NICT, 九州大学, 富士通研究所,
2012年6月18日プレスリリース)

独立行政法人
情報通信研究機構

NICTについて　研究紹介　成果・社会還元　プレスリリース　連携・支援制度　イベント&トピックス

トップページ ＞プレスリリース ＞次世代暗号の解読で世界記録を達成

ツイート 156　いいね！ 184　印刷

次世代暗号の解読で世界記録を達成

ペアリング暗号の安全性を確立し、次世代暗号の標準化に貢献

2012年6月18日

独立行政法人情報通信研究機構(以下NICT)[注1]、国立大学法人九州大学(以下九州大学)[注2]、株式会社富士通研究所[注3]は共同で、次世代の暗号として標準化が進められているペアリング暗号について、278桁長の暗号解読に成功し、世界記録を達成しました。従来、この桁長の暗号は解読に数十万年かかることから解読不可能とされ、開発段階で利用・普及への取組が数々見られましたが、今般、新しい攻撃法の適用により148.2日間で解読できる脆弱な暗号であることが実証されました。本成果は、わが国の電子政府や国際標準化機関等において、安全な暗号技術を利用するための根拠として活用され、次世代の暗号の標準化に役立てられます。

注1. 独立行政法人情報通信研究機構：理事長 宮原秀夫
注2. 国立大学法人九州大学：総長 有川節夫
注3. 株式会社富士通研究所：代表取締役社長 富田達夫、本社 神奈川県川崎市

278桁のペアリング暗号解読成功 世界記録達成

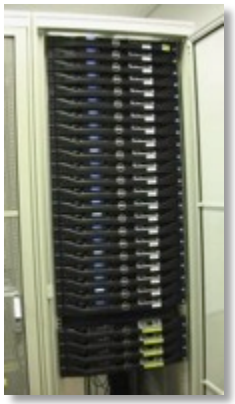
解読実験データ

- 延べ計算日数：148.2日
- 汎用コンピュータ：21台（252コア）
- Intel Xeon 1コアで102年分の計算時間に相当

解読に用いた計算機







ペアリング暗号
(Pairing-based Cryptgraphy)

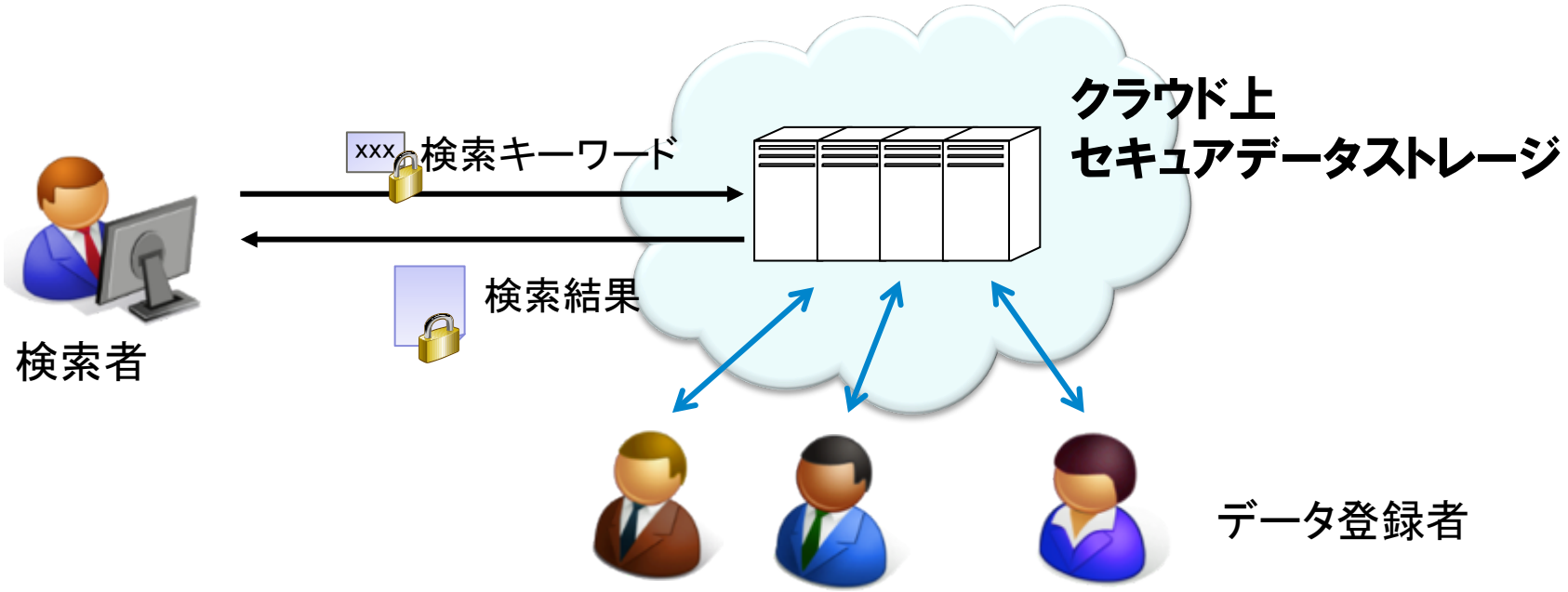
- ペアリング
  - × ペアのリング
  - ○ 双線形性という優れた性質をもつ写像

- ペアリング暗号
  - 2000–2001年に日・米の研究グループにより独立に提案
  - これまでの暗号技術ではできなかった高度なプライバシ保護機能が実現できる新しい技術

ペアリング暗号で実現できる機能

検索可能暗号

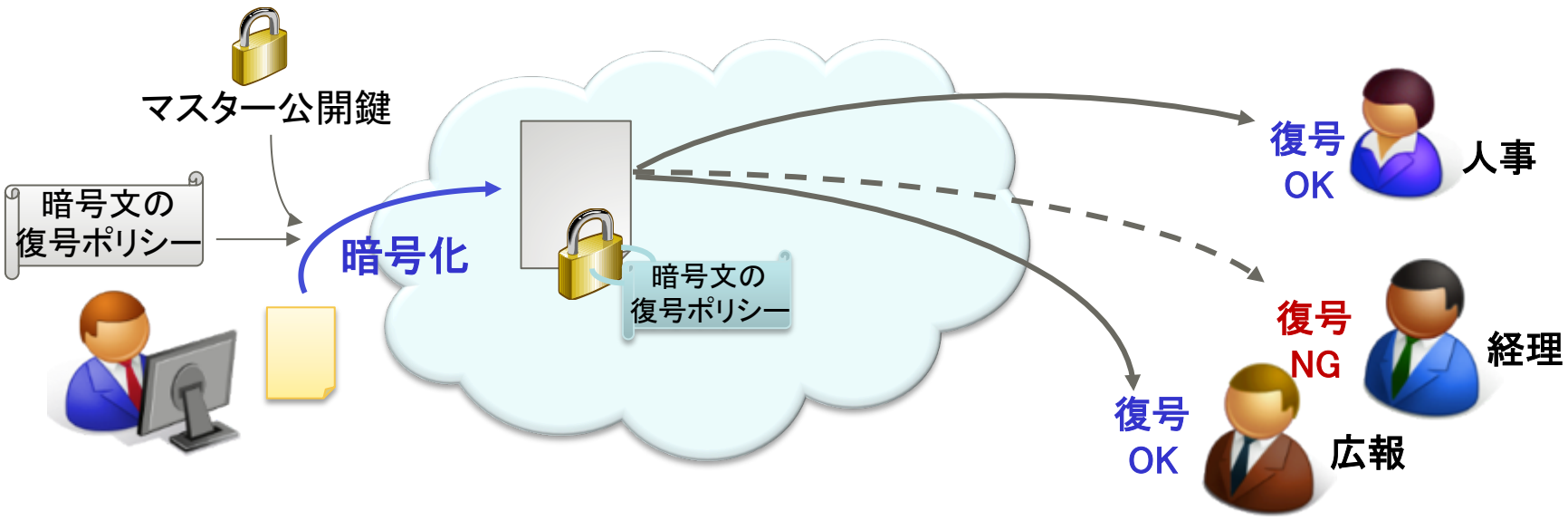
暗号化したままキーワード検索ができる機能



ペアリング暗号で実現できる機能

関数型暗号

暗号化時に柔軟なアクセス制御が設定できる機能



ペアリングとは？

数字の組(pair)を、うまく1個にする(～ing)数式。
これを暗号に応用したのが「ペアリング暗号」。

$$b = a^x$$

（簡略版）

ペアリングの数式

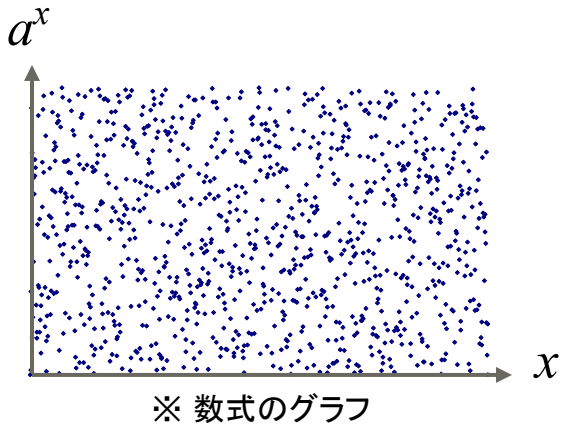
$$\eta_T(Q_\pi, Q_\pi) = \eta_T(Q_\pi, Q_e)^x$$

ペアリング暗号の解読

ペアリング暗号を解読するには、

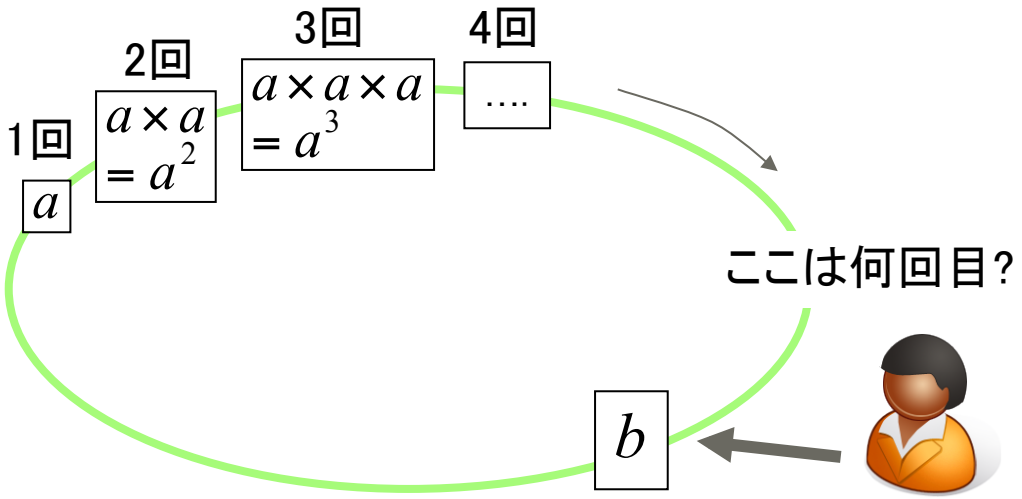
$b = a^{x}$ の **解** を求める

ペアリング暗号の数式
（簡略版）



※ 数式のグラフ

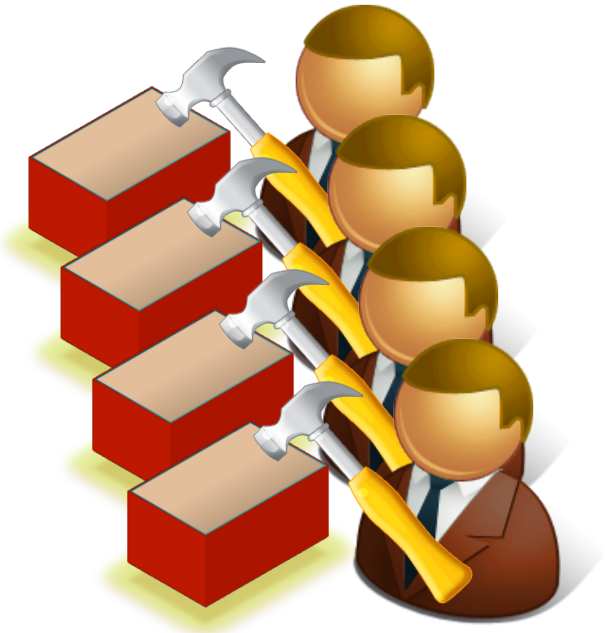
つまり、同じ数を繰り返し掛け算した「回数」を求める



今回の解読の基本アイデア

大きな1個の数式を解く　→(変換)→　大量の小さい式を解く

暗号の解読　　計算しやすい

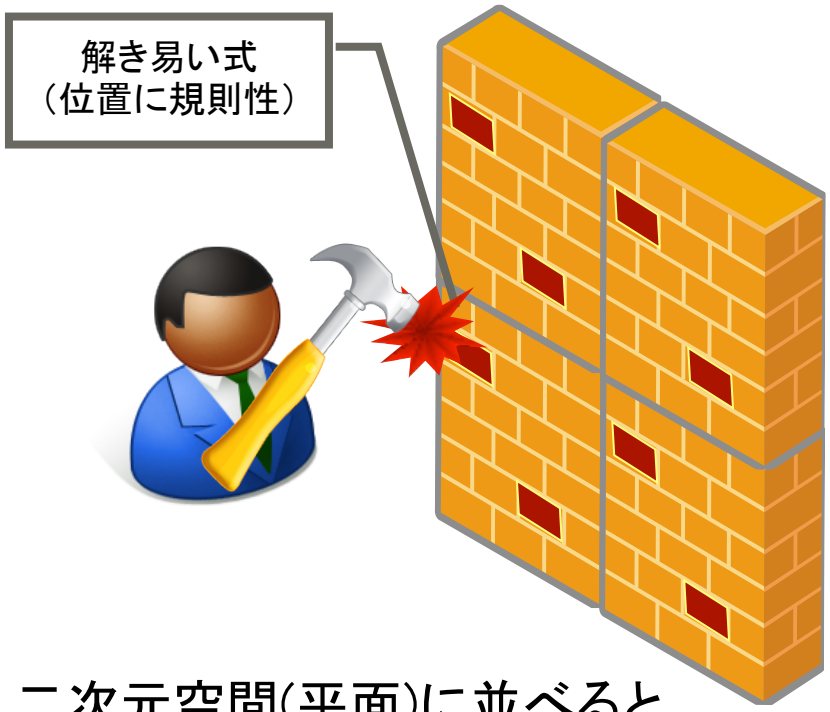


新しい解読法：
データ探索を二次元空間に拡張

従来

解き易さに関係なく
1個ずつ順に解く

新しい解読法



二次元空間(平面)に並べると、
解き易い式に規則性があることに着目。
ポイントを絞って解く。

数十倍の効率化

解読法改良の効果

スーパーコンピュータ「京」を使った場合、
今回の解読は当初 7.84年 相当の計算量

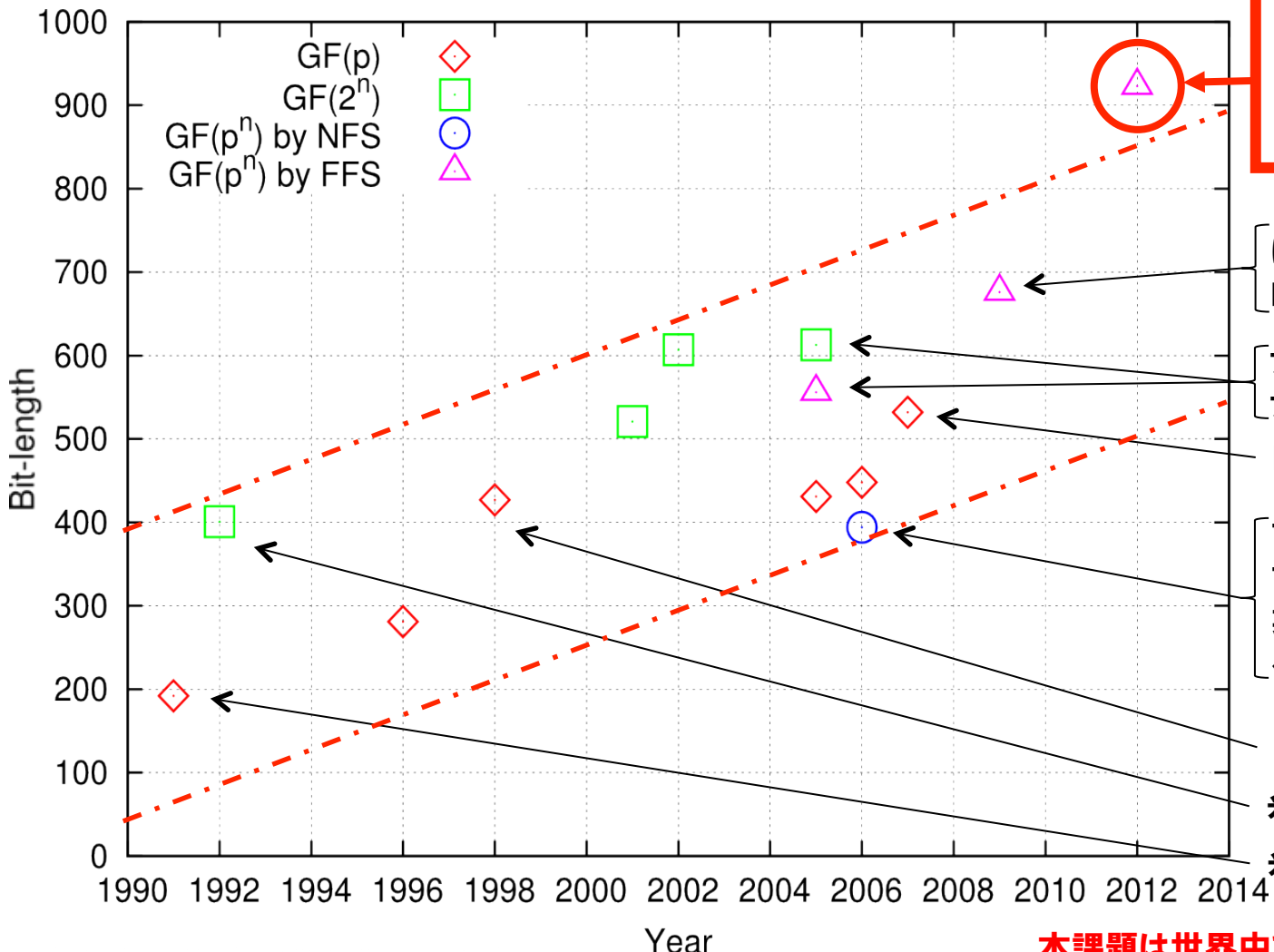
↓

解読方法の改良により13.6分 に短縮！

「京」
- 1秒間に1京510兆回の浮動小数点演算ができるスパコン(富士通開発)
- 2011年6月・11月のスパコンランキング（TOP500）で、二期連続世界一
- 2012年11月現在、タイタン(米クレイ)、セコイア(米IBM) に次ぐ3位

出典:理化学研究所

離散対数問題：解読世界記録の推移



今回の記録

NICT
九州大学
富士通研究所

はこだて未来大学
NICT

フランス・レンヌ大学
フランス国防省
ドイツ・ボン大学

フランス・レンヌ大学
フランス国防省
英・ブリストル大学
ベルギー・ルーベン大学

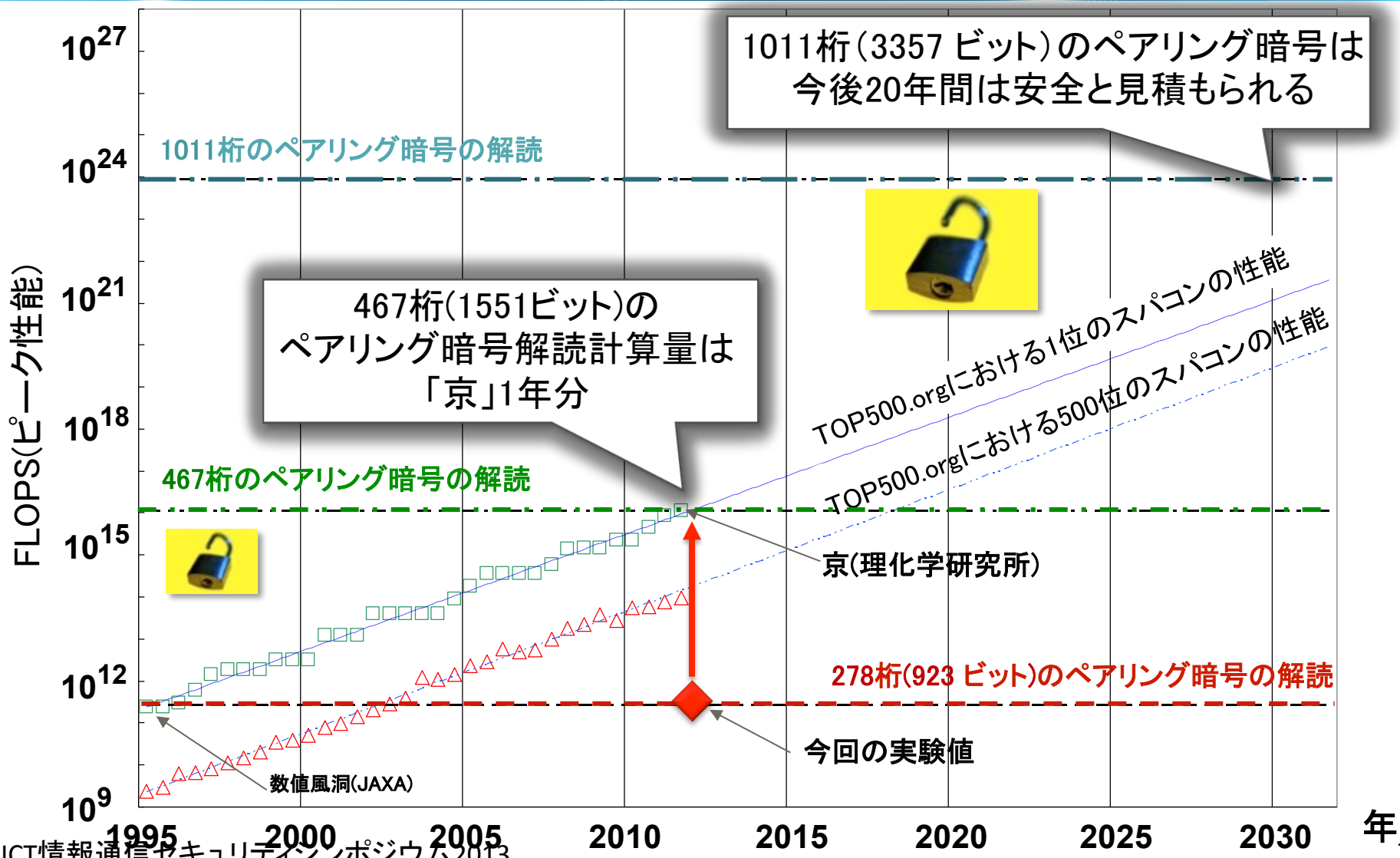
ドイツ・ザールランド大学

米・サンディア国立研究所

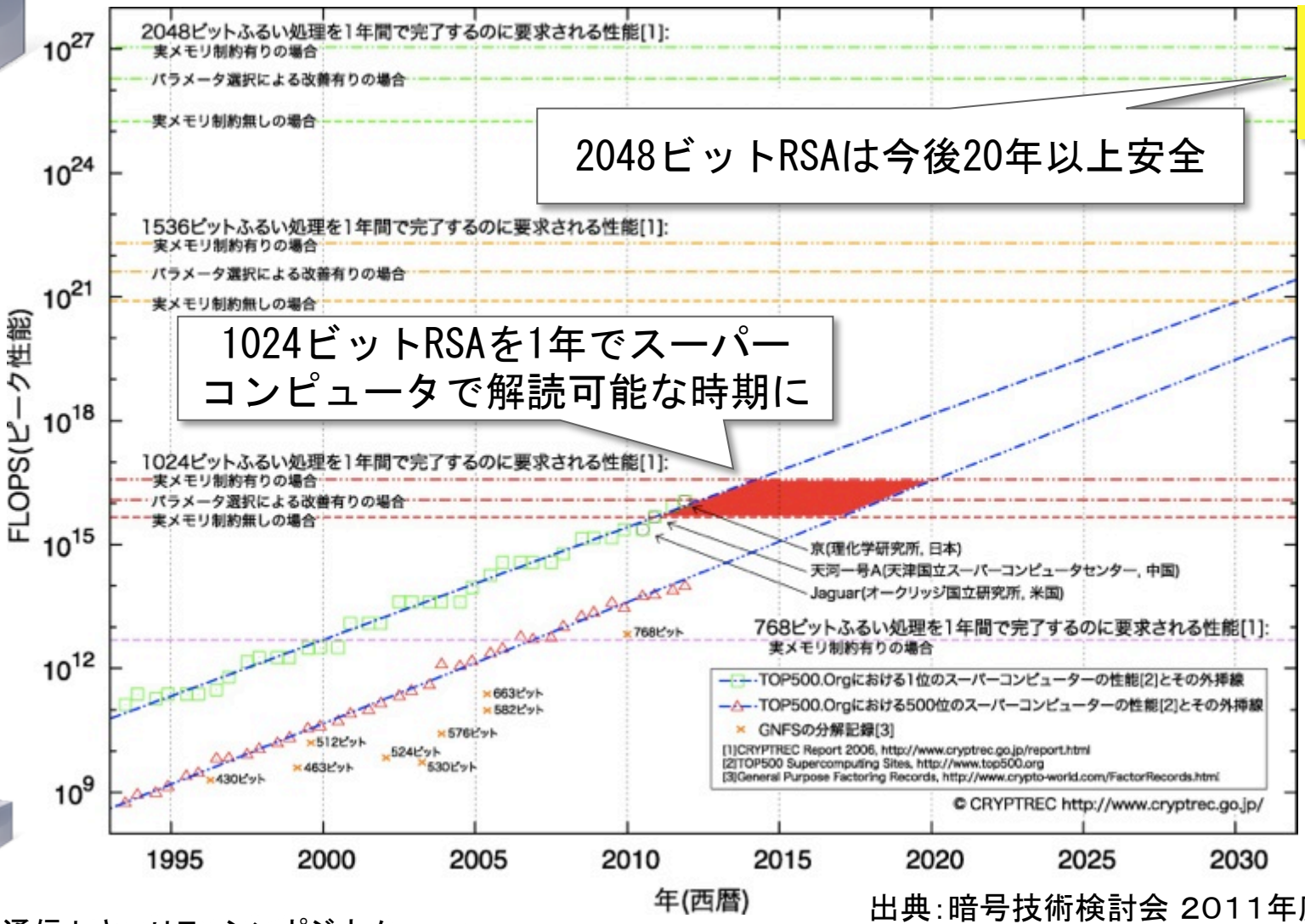
米・AT&T

本課題は世界中で活発に研究されてきた

安全なペアリング暗号は？



[参考] RSA暗号の安全性予測



2048ビット RSA

1024ビット RSA

出典:暗号技術検討会 2011年度報告書

ペアリング暗号の標準化動向

- IETF (Internet Engineering Task Force)
  - インターネットで利用される技術の標準化が進められている.
    - RFC5091 (2008): Identity-Based Cryptography Standard #1
    - RFC6508 (2012): Sakai-Kasahara Key Encryption

- IEEE (Institute of Electrical and Electronics Engineers)
  - IEEE P1363で公開鍵暗号全般の規格化が進められている.
    - IEEE P1363.3: Identity-Based Public Key Cryptography

- ISO/IEC JTC 1/SC27
  - 情報セキュリティ技術全般の国際標準化が進められている.
    - ISO/IEC 15946-5:2009, 情報技術 – セキュリティ技術 – 楕円曲線に基づく暗号技術 – 第5部: 楕円曲線生成
- ANSI X9F1
- TCG

格子暗号の安全性評価

格子最短ベクトル問題チャレンジ

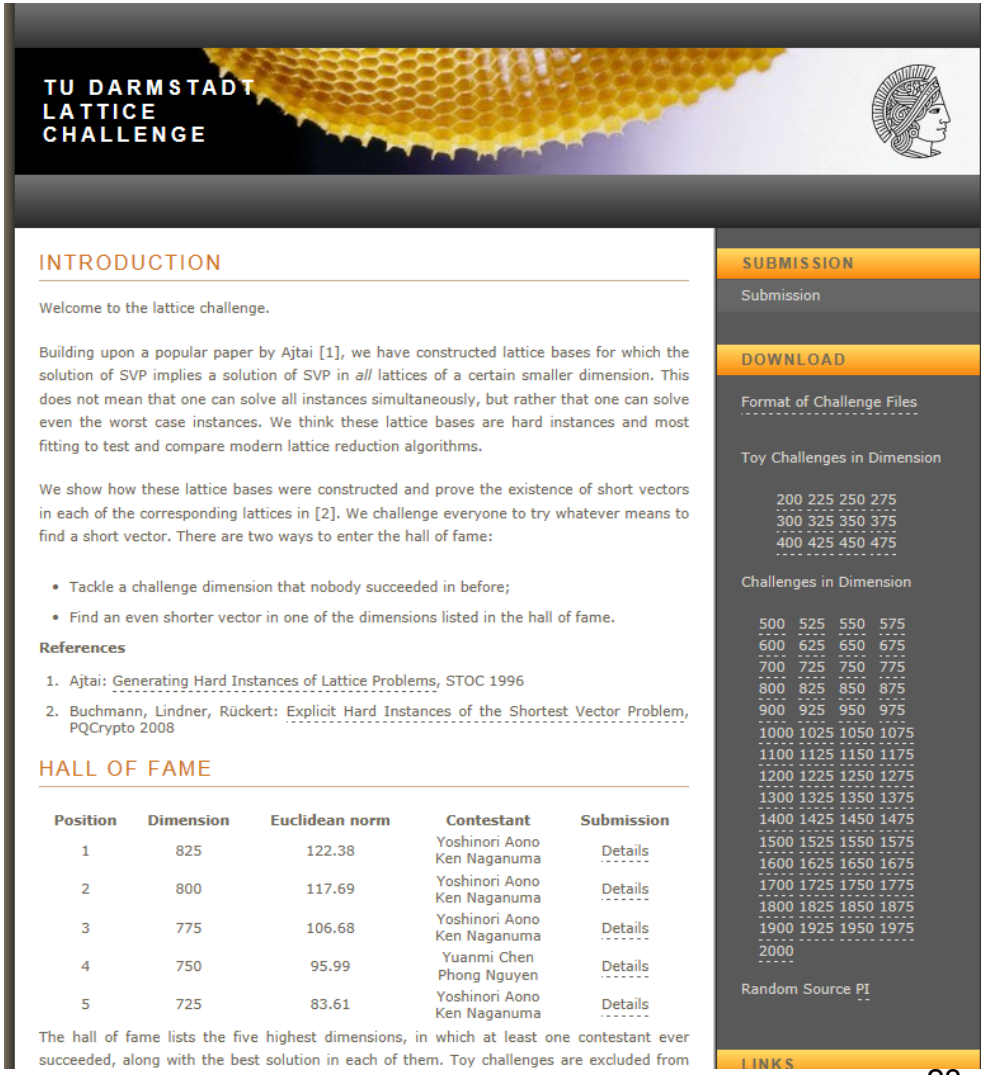
- TU Darmstadt Lattice Challenge

  http://www.latticechallenge.org/

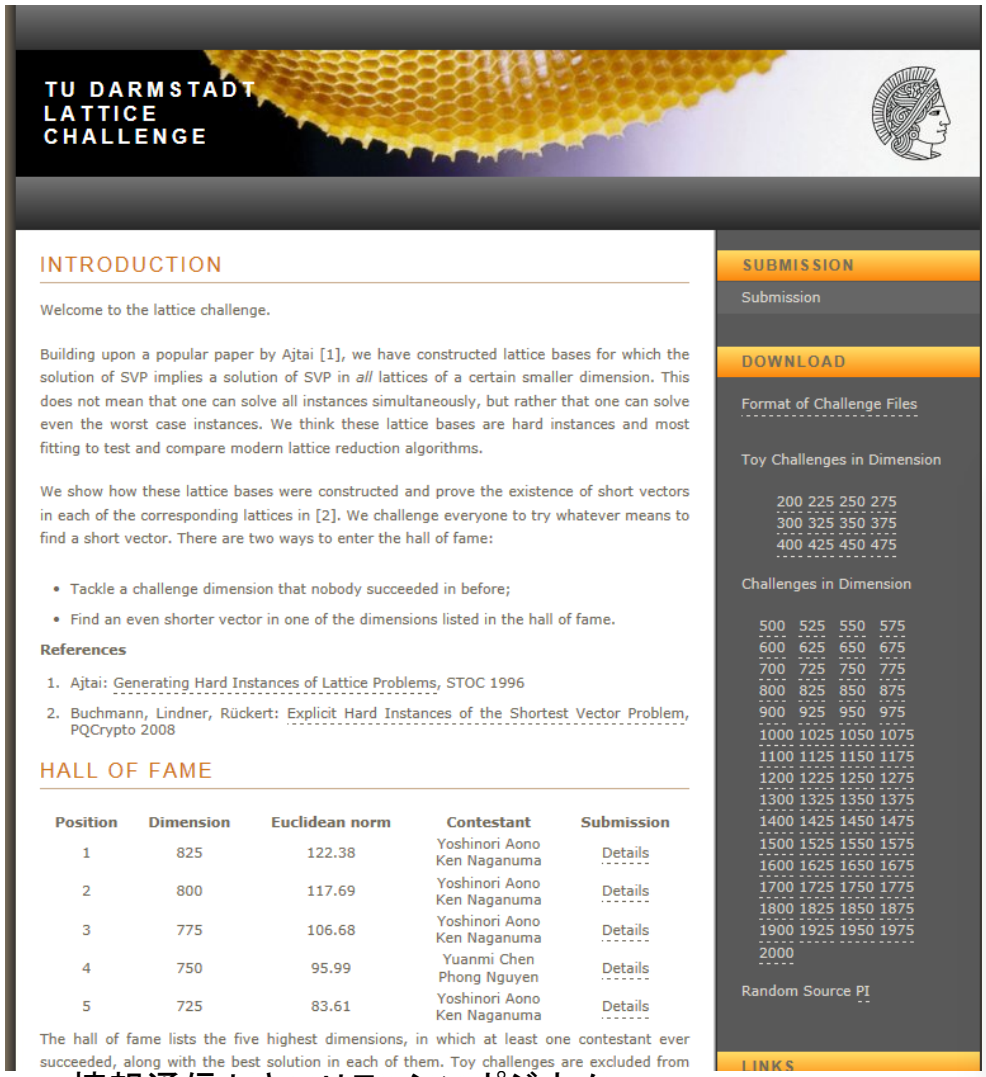
  – 独ダルムシュタット工科大学が2008年より主催している格子の最短ベクトル問題(SVP)のコンテスト

  – SVPの難しさを検証するため、500次元から2000次元までのチャレンジ問題が25次元刻みで出題

  – より高い次元、より短いベクトルの探索を目指して世界の著名な暗号研究者がしのぎを削っている



825次元の格子最短ベクトル問題を5.5日で解くことに成功



TU DARMSTADT
LATTICE
CHALLENGE

INTRODUCTION

Welcome to the lattice challenge.

Building upon a popular paper by Ajtai [1], we have constructed lattice bases for which the solution of SVP implies a solution of SVP in *all* lattices of a certain smaller dimension. This does not mean that one can solve all instances simultaneously, but rather that one can solve even the worst case instances. We think these lattice bases are hard instances and most fitting to test and compare modern lattice reduction algorithms.

We show how these lattice bases were constructed and prove the existence of short vectors in each of the corresponding lattices in [2]. We challenge everyone to try whatever means to find a short vector. There are two ways to enter the hall of fame:

- Tackle a challenge dimension that nobody succeeded in before;
- Find an even shorter vector in one of the dimensions listed in the hall of fame.

References

1. Ajtai: Generating Hard Instances of Lattice Problems, STOC 1996
2. Buchmann, Lindner, Rückert: Explicit Hard Instances of the Shortest Vector Problem, PQCrypto 2008

HALL OF FAME

Position	Dimension	Euclidean norm	Contestant	Submission
1	825	122.38	Yoshinori Aono Ken Naganuma	Details
2	800	117.69	Yoshinori Aono Ken Naganuma	Details
3	775	106.68	Yoshinori Aono Ken Naganuma	Details
4	750	95.99	Yuanmi Chen Phong Nguyen	Details
5	725	83.61	Yoshinori Aono Ken Naganuma	Details

The hall of fame lists the five highest dimensions, in which at least one contestant ever succeeded, along with the best solution in each of them. Toy challenges are excluded from

SUBMISSION

Submission

DOWNLOAD

Format of Challenge Files

Toy Challenges in Dimension

200 225 250 275
300 325 350 375
400 425 450 475

Challenges in Dimension

500 525 550 575
600 625 650 675
700 725 750 775
800 825 850 875
900 925 950 975
1000 1025 1050 1075
1100 1125 1150 1175
1200 1225 1250 1275
1300 1325 1350 1375
1400 1425 1450 1475
1500 1525 1550 1575
1600 1625 1650 1675
1700 1725 1750 1775
1800 1825 1850 1875
1900 1925 1950 1975
2000

Random Source PI

LINKS

「クラウド向け暗号技術の安全性評価で世界新記録を達成
ー暗号化したままデータを処理する
格子暗号技術の実用化に向けてー」
(2013年1月21日プレスリリース)

NICT 独立行政法人 情報通信研究機構

NICTについて | 研究紹介 | 成果・社会還元 | プレスリリース | 連携・支援制度 | イベント&トピック

トップページ ＞プレスリリース ＞クラウド向け暗号技術の安全性評価で世界新記録を達成

ツイート 47 いいね！ 53 印刷

クラウド向け暗号技術の安全性評価で世界新記録を達成

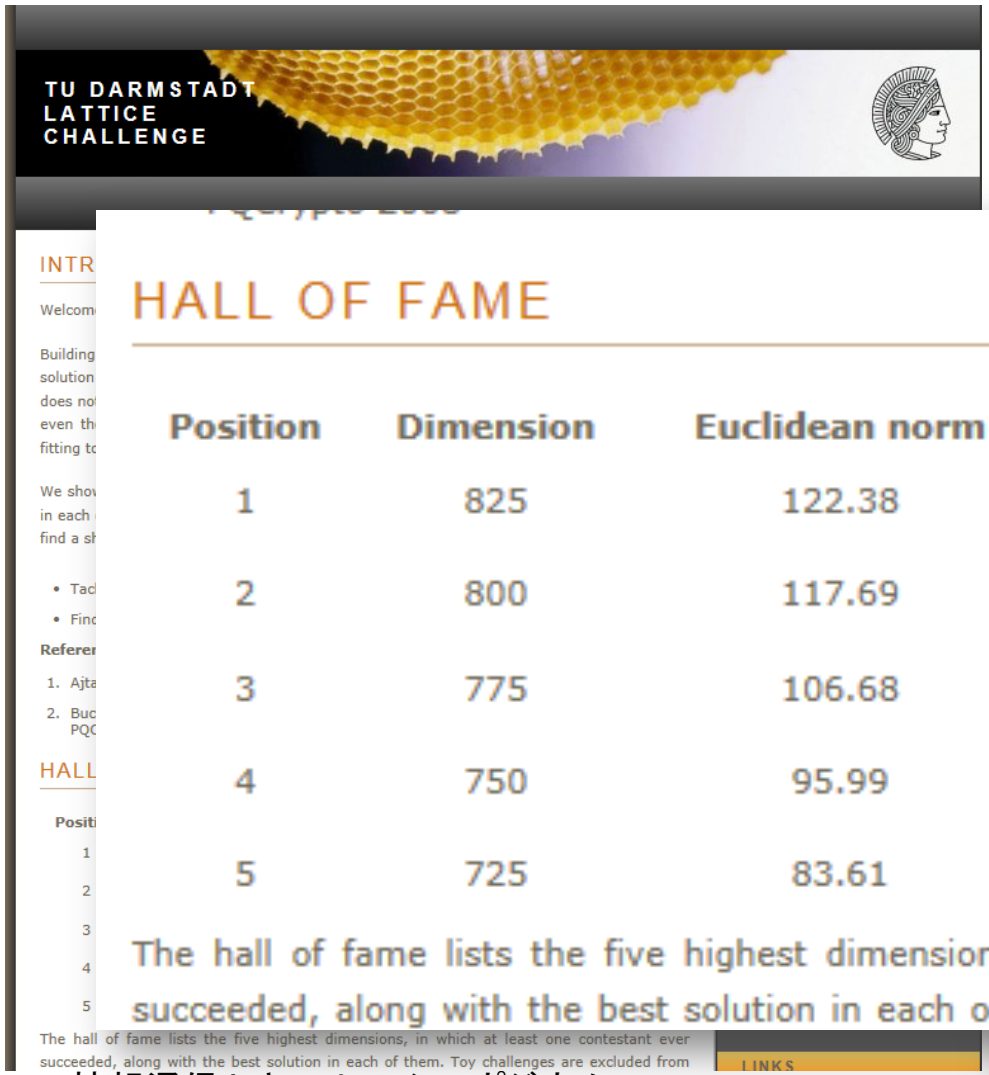
～暗号化したままデータを処理する"格子暗号技術"の実用化に向けて～

2013年1月21日

独立行政法人 情報通信研究機構(以下「NICT」、理事長:宮原 秀夫)は、暗号化したままデータを処理する技術である「完全準同型暗号」の安全性を支える「格子の最短ベクトル問題」の解析を行い、世界で初めて、825次元もの高い次元の問題を解くことに成功しました。

「完全準同型暗号」を利用すると、他へ機密データの内容を一切知らせることなく計算作業を託すことが可能となるなど、クラウド・コンピューティング等でのセキュリティ確保のためにこの暗号が活用されることが期待されています。「格子の最短ベクトル問題」の評価は、完全準同型暗号を安全に利用するために不可欠であり、実用化に向けた第一歩となるものです。

825次元の格子最短ベクトル問題を5.5日で解くことに成功



「クラウド向け暗号技術の安全性評価で世界新記録を達成

HALL OF FAME

Position	Dimension	Euclidean norm	Contestant	Submission
1	825	122.38	Yoshinori Aono Ken Naganuma	Details
2	800	117.69	Yoshinori Aono Ken Naganuma	Details
3	775	106.68	Yoshinori Aono Ken Naganuma	Details
4	750	95.99	Yuanmi Chen Phong Nguyen	Details
5	725	83.61	Yoshinori Aono Ken Naganuma	Details

The hall of fame lists the five highest dimensions, in which at least one contestant ever succeeded, along with the best solution in each of them. Toy challenges are excluded from

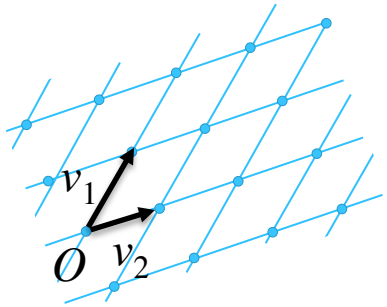
格子暗号 (Lattice-based Cryptography)

- 格子の最短ベクトル問題など、格子理論における難しい問題を安全性の根拠とする暗号方式
- 耐量子計算機暗号(Post-quantum Cryptography)の1つ
  - 量子コンピュータが実現すると、RSA, DSA, ECCなど現在広く利用されている公開鍵暗号の安全性が低下する (Shor,1994)
  - これに対し、格子暗号は量子コンピュータ実現後も高い安全性が保たれると期待されている

格子の最短ベクトル問題(SVP)

- 格子
  - 空間内の規則正しく並んだ点(ベクトル)の集合

2次元格子の例
v_1, v_2が基底

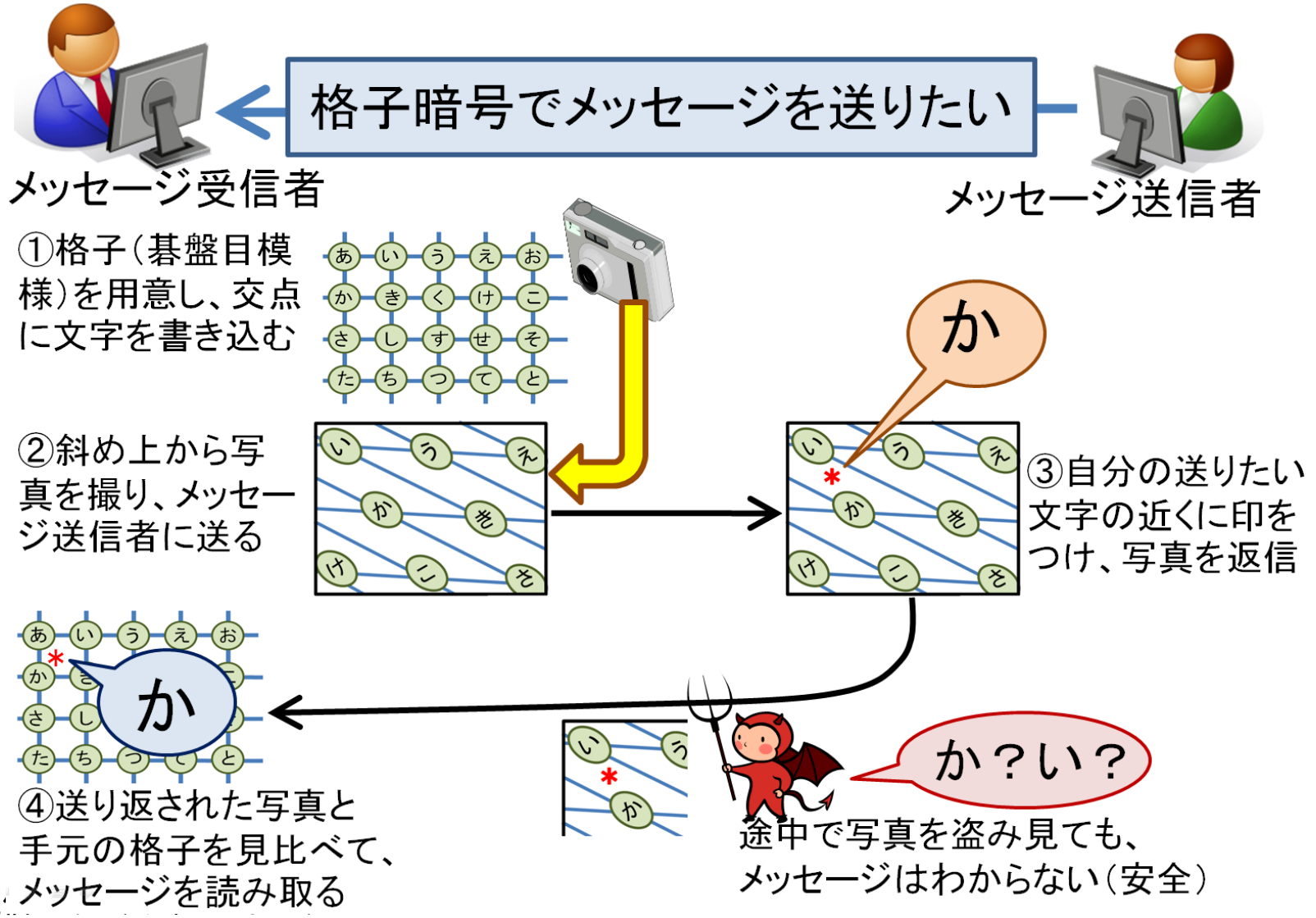


- 格子の最短ベクトル問題
  - 格子の基底が与えられたときに、原点以外で、最も原点に近い格子点を見つける問題
  - 大きな次元の格子では最短ベクトルを求める問題は非常に難しい (NP困難)

SVPの重要性

- 格子暗号の安全性評価
  - 量子コンピュータ出現後も利用できる暗号方式
  - 完全準同型暗号
    - 2009年に米IBMが格子理論を利用して、初めて完全準同型暗号の開発に成功
    - データを暗号化したままの状態で加算と乗算が行える暗号方式 ⇒ クラウド上での秘匿情報処理への応用
- RSAの安全性評価

格子暗号のしくみ


格子暗号でメッセージを送りたい
メッセージ受信者
メッセージ送信者
①格子（碁盤目模様）を用意し、交点に文字を書き込む
②斜め上から写真を撮り、メッセージ送信者に送る
か
③自分の送りたい文字の近くに印をつけ、写真を返信
か
④送り返された写真と手元の格子を見比べて、メッセージを読み取る
か？い？
途中で写真を盗み見ても、メッセージはわからない（安全）

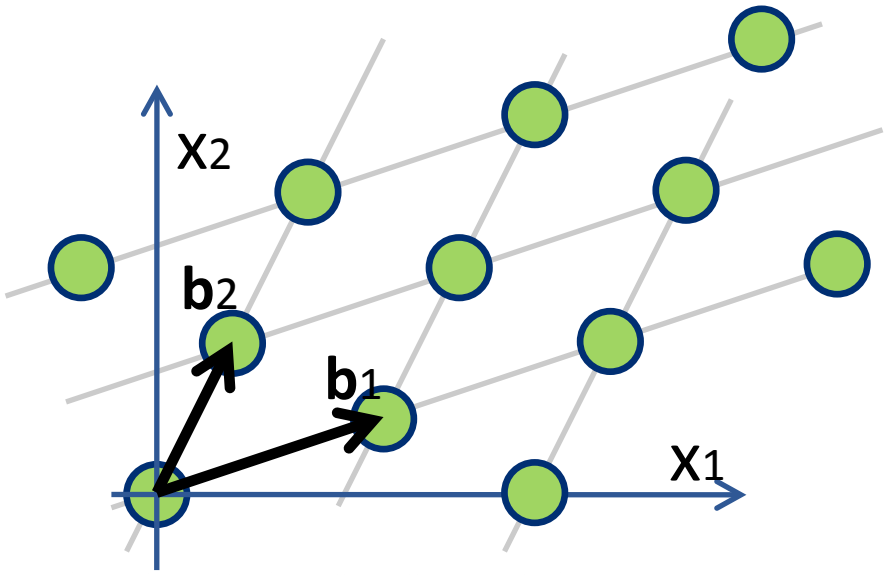
格子の定義

m次元空間の基底

$\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n \quad (n \leqq m)$

に対して、その整数係数一次結合を取ったもの

例：2次元空間で、$\mathbf{b}_1=(3,1)$, $\mathbf{b}_2=(1,2)$の場合、
以下の緑の点の集合



・この格子基底を横ベクトルを並べて、行列で

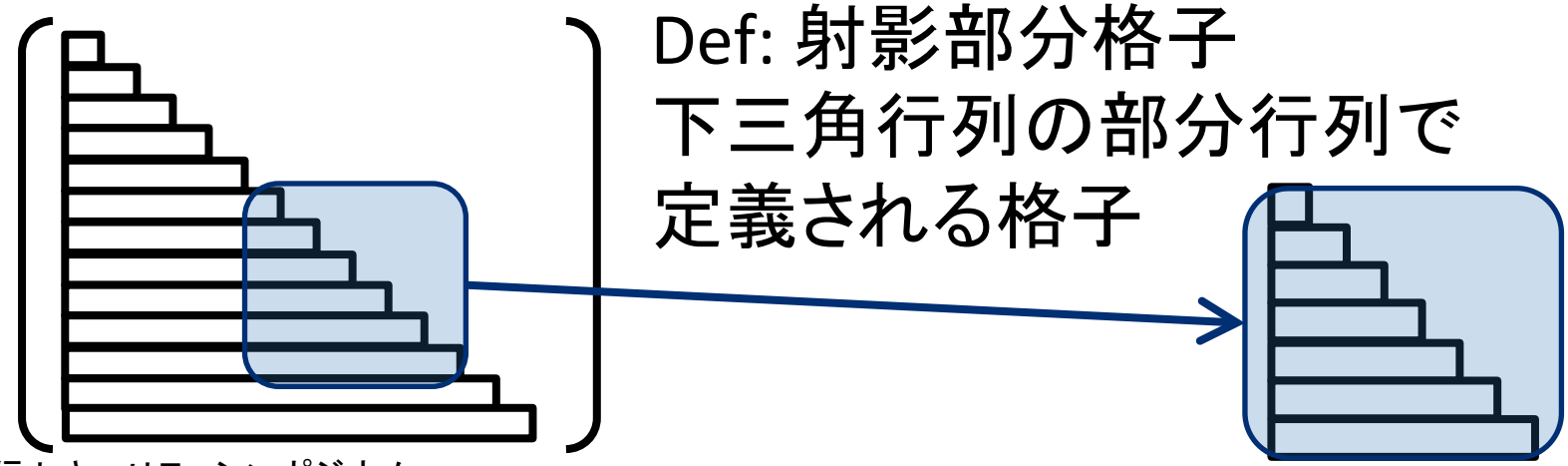
$$L=\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \begin{matrix} \leftarrow \mathbf{b}_1 \\ \leftarrow \mathbf{b}_2 \end{matrix}$$

と表現する

格子の表現

- どんな格子でも下三角行列で書ける
  - Gram-Schmidt基底による表現

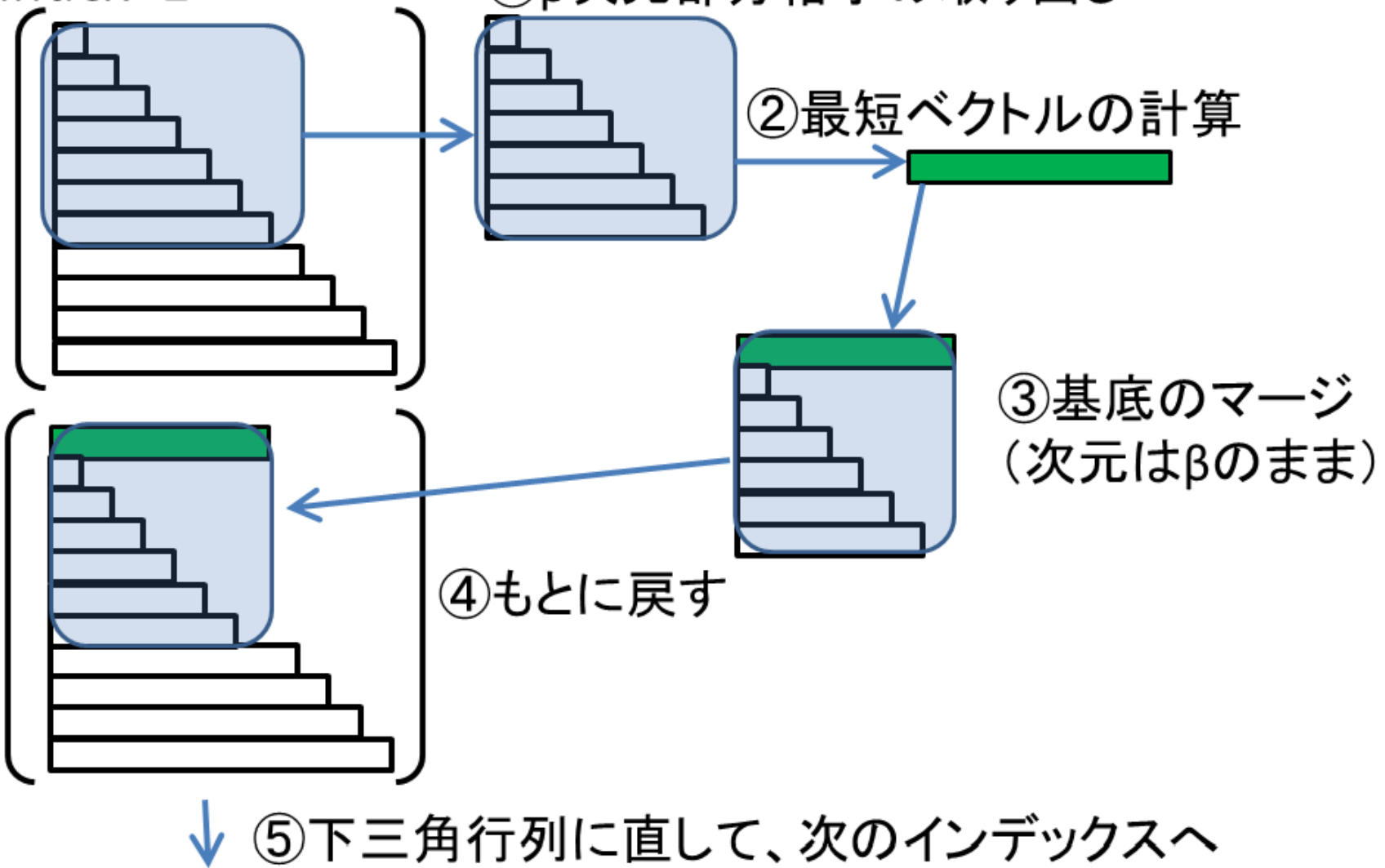
$$L=\begin{bmatrix} 5 & -1 & 4 & 9 & 3 \\ 4 & 2 & 10 & -3 & 3 \\ 1 & 0 & 2 & -6 & 7 \\ 0 & 6 & -9 & -1 & 3 \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{b}_4 \end{bmatrix} \Leftrightarrow \begin{bmatrix} \|\mathbf{b}_1^*\| & & & \\ \mu_{2,1}\|\mathbf{b}_1^*\| & \|\mathbf{b}_2^*\| & & \\ \mu_{3,1}\|\mathbf{b}_1^*\| & \mu_{3,2}\|\mathbf{b}_2^*\| & \|\mathbf{b}_3^*\| & \\ \mu_{4,1}\|\mathbf{b}_1^*\| & \mu_{4,2}\|\mathbf{b}_2^*\| & \mu_{4,3}\|\mathbf{b}_3^*\| & \|\mathbf{b}_4^*\| \end{bmatrix}$$

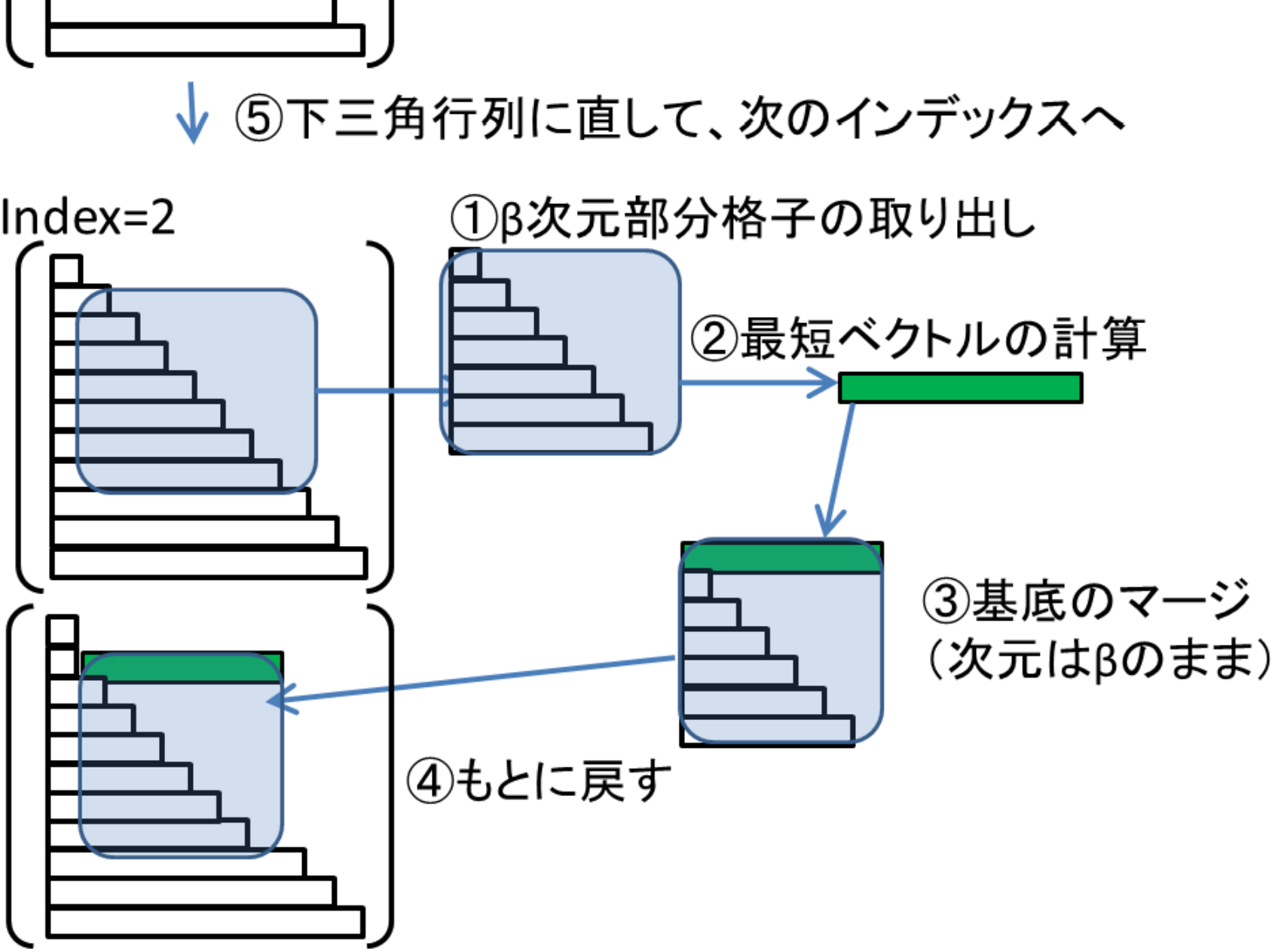


BKZアルゴリズム[Schnorr-Euchner 1991 ver.]

上から順に部分格子を取り、その最短ベクトルを求める

- Index=1




⑤下三角行列に直して、次のインデックスへ
• Index=2
①β次元部分格子の取り出し
②最短ベクトルの計算
③基底のマージ
（次元はβのまま）
④もとに戻す
⑤下三角行列に直して、次のインデックスへ

④もとに戻す

⑤下三角行列に直して、次のインデックスへ

⋮

⑤下三角行列にして、インデックスを次へ

Index=nになったら、

(i)　基底がβ-簡約になっていれば終了

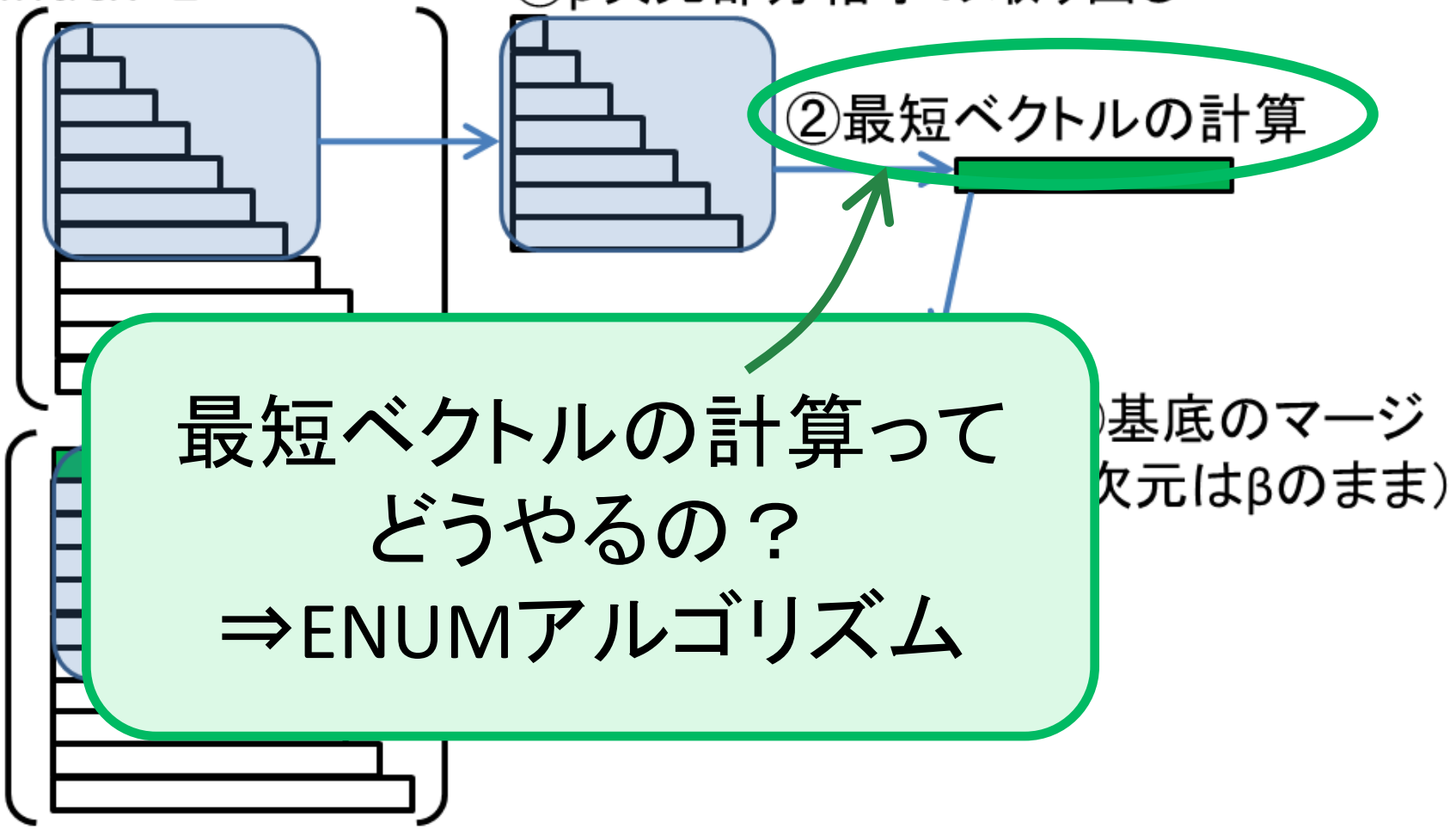
(ii)　そうでなければindex=1に戻る

※この無茶な終了条件は、NTL-BKZが遅い原因その①

BKZアルゴリズム[Schnorr-Euchner 1991 ver.]

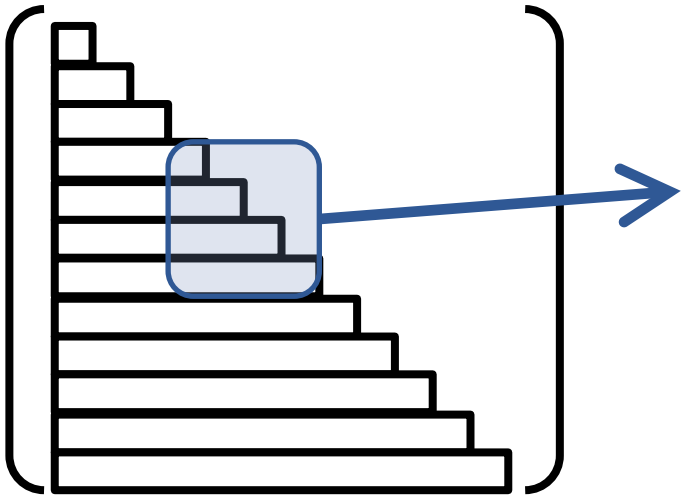
上から順に部分格子を取り、その最短ベクトルを求める

- Index=1



ENUMアルゴリズム[Kannan@STOC1983]

- 最短ベクトルを求めるための厳密アルゴリズム

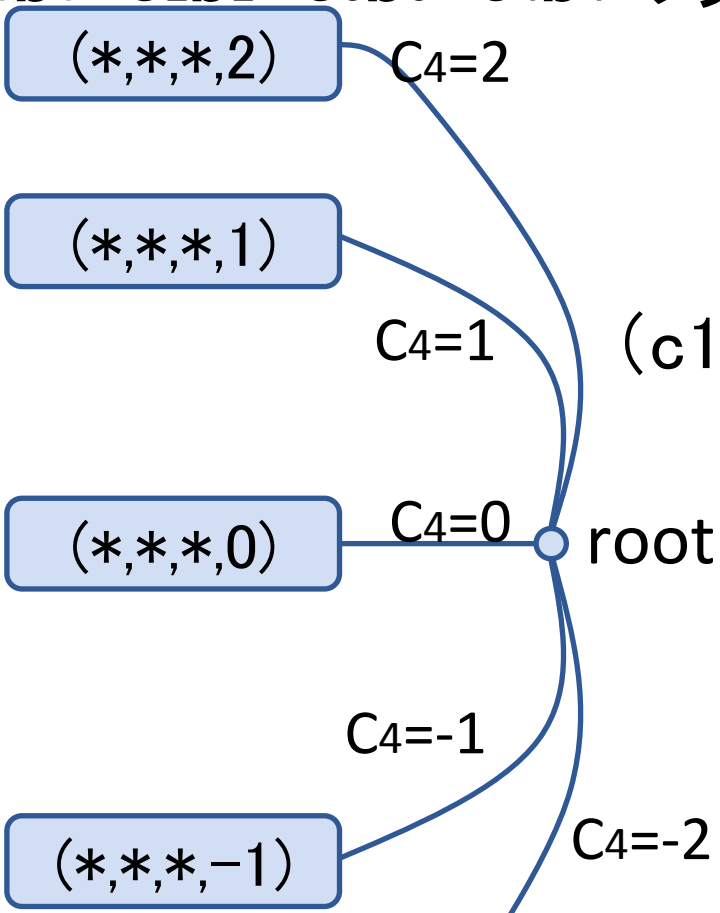


$$L=\begin{bmatrix}\mathbf{b}_1\\ \mathbf{b}_2\\ \mathbf{b}_3\\ \mathbf{b}_4\end{bmatrix}=\begin{bmatrix}3 & & & \\ 2 & 3 & & \\ -1 & 1 & 2 & \\ 0 & 2 & -1 & 1\end{bmatrix}$$

- 方針： 一次結合$c_1\mathbf{b}_1+c_2\mathbf{b}_2+c_3\mathbf{b}_3+c_4\mathbf{b}_4$を全て調べ、最短の非ゼロベクトルを探索
  - c4,c3,c2,c1の順に決定
  - 探索木を作って枝刈り：$\min|\mathbf{b}_i| = \sqrt{6}$ を使う

$$L=\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}=\begin{bmatrix} 3 & & & \\ 2 & 3 & & \\ -1 & 1 & 2 & \\ 0 & 2 & -1 & 1 \end{bmatrix} \qquad \min|bi|=\sqrt{6}$$

- Step 1: c_4の決定
- $c_1b_1+c_2b_2+c_3b_3+c_4b_4$の第4成分は固定される

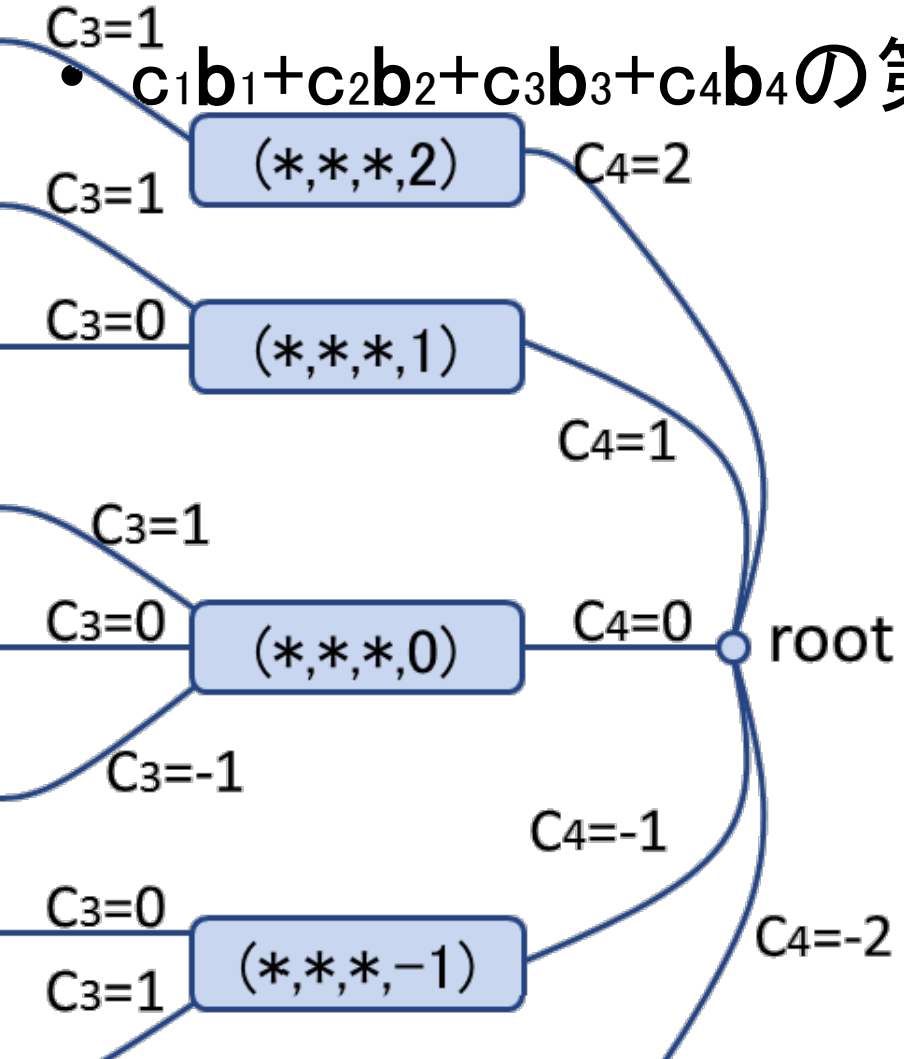


※ (*,*,*,3) は出てこない

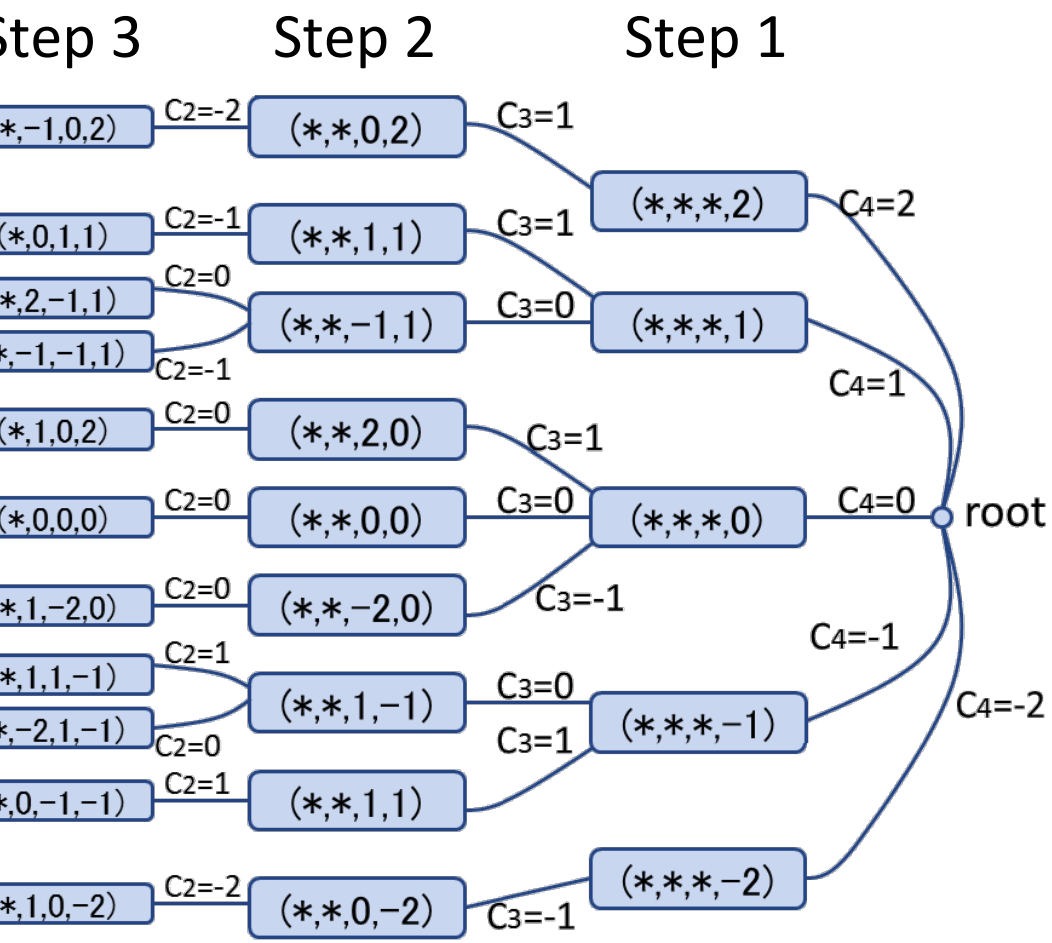
（c1,c2,c3をどう選んでも長さ>$\sqrt{6}$）

$$L=\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}=\begin{bmatrix} 3 & & & \\ 2 & 3 & & \\ -1 & 1 & 2 & \\ 0 & 2 & -1 & 1 \end{bmatrix} \qquad \min|bi|=\sqrt{6}$$

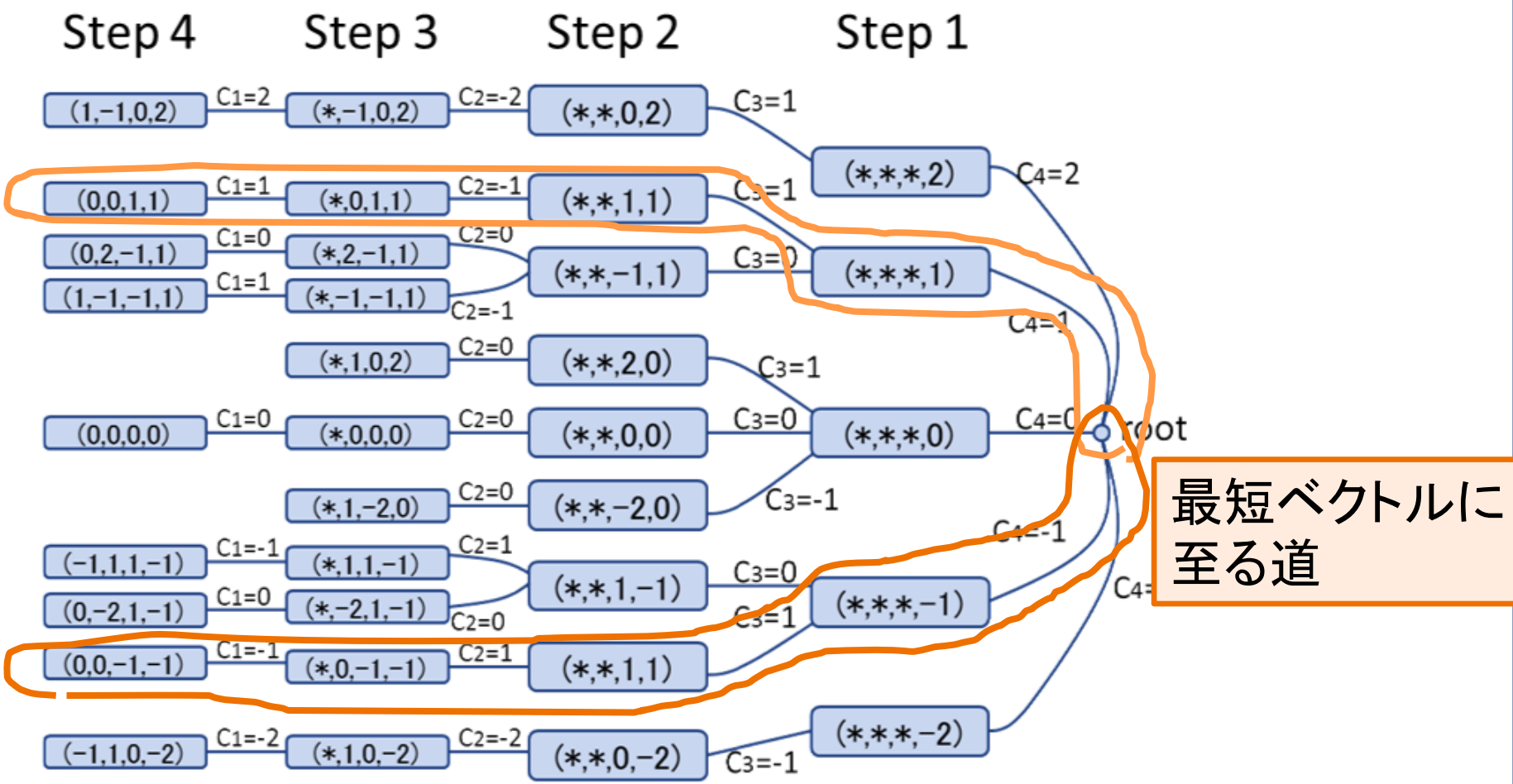
- Step 2: c_3の決定
- $c_1b_1+c_2b_2+c_3b_3+c_4b_4$の第3,4成分は固定される



$$L=\begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{b}_4 \end{bmatrix}=\begin{bmatrix} 3 & & & \\ 2 & 3 & & \\ -1 & 1 & 2 & \\ 0 & 2 & -1 & 1 \end{bmatrix} \qquad \min|bi|=\sqrt{6}$$

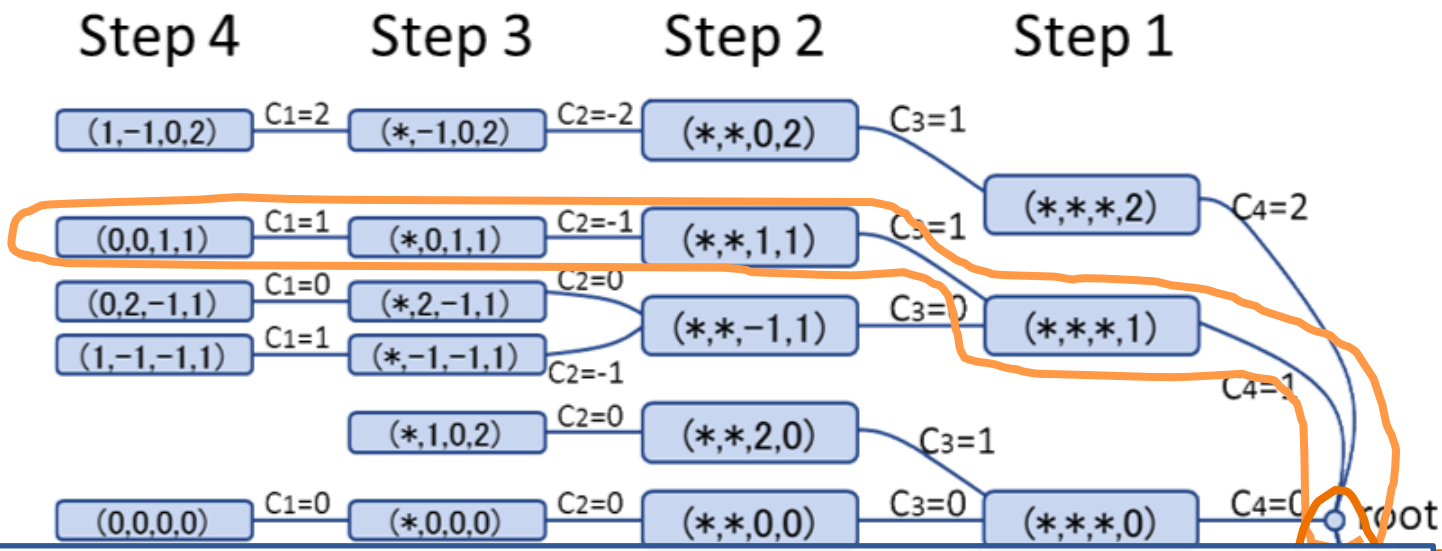


$$L=\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}=\begin{bmatrix} 3 & & & \\ 2 & 3 & & \\ -1 & 1 & 2 & \\ 0 & 2 & -1 & 1 \end{bmatrix} \qquad \min|bi|=\sqrt{6}$$



最短ベクトルに至る道

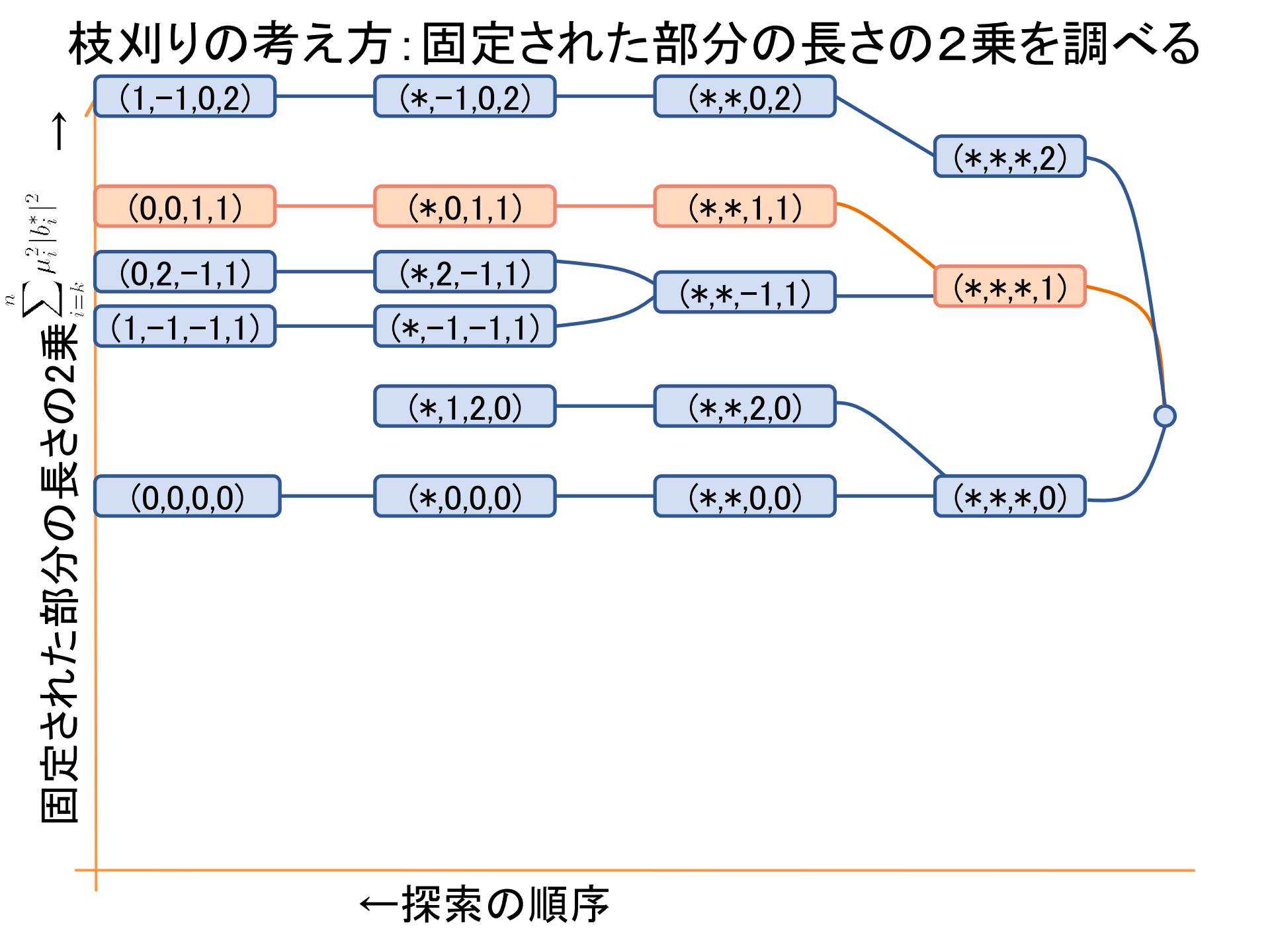
$$L=\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}=\begin{bmatrix} 3 & & & \\ 2 & 3 & & \\ -1 & 1 & 2 & \\ 0 & 2 & -1 & 1 \end{bmatrix} \qquad \min|bi|=\sqrt{6}$$



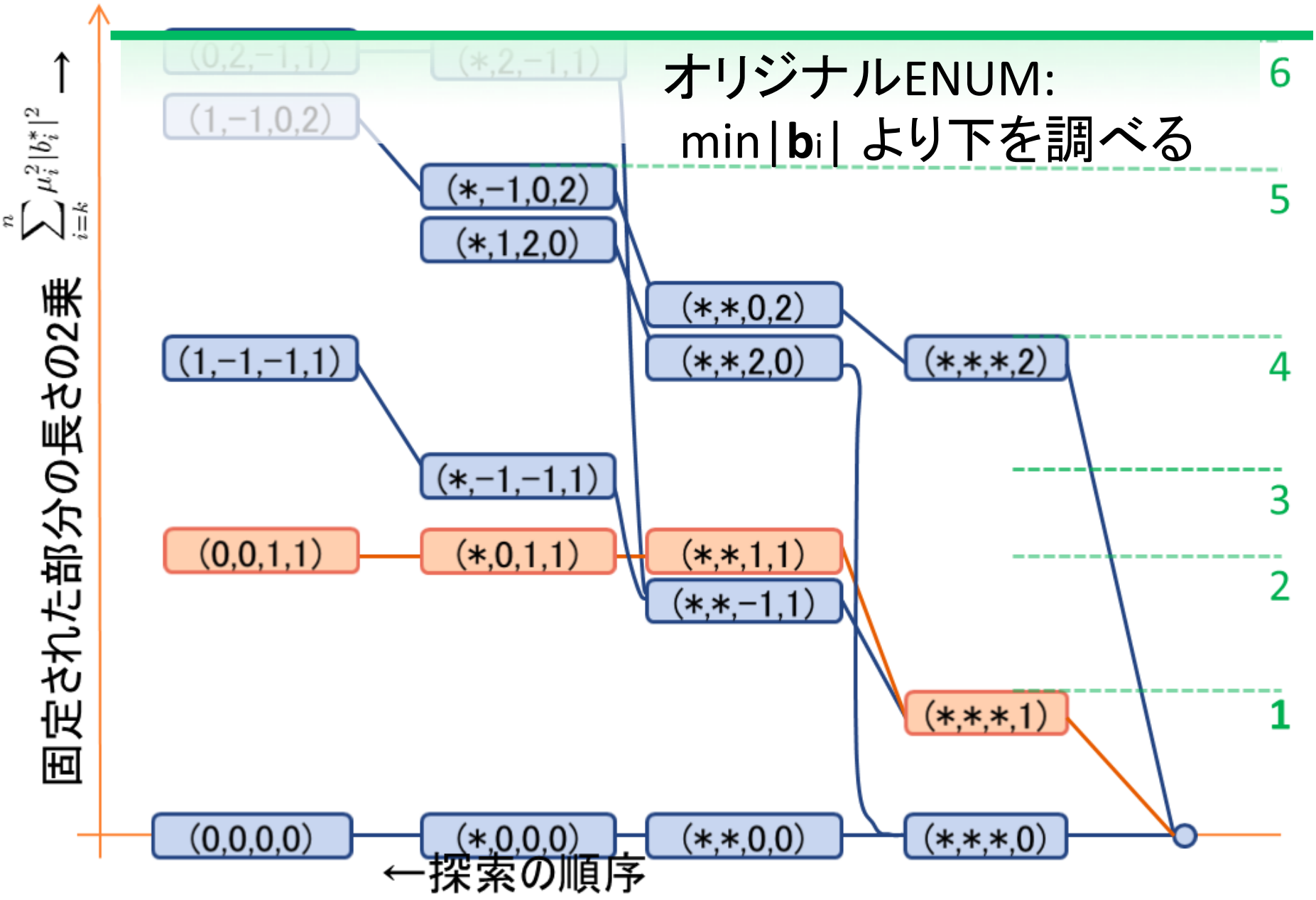
最短ベクトルに至る道

実際には、対称性から調べるノードは半分
⇒もっと減らせないか？
（最短ベクトルに至る道を効率よく調べたい）
どうやって探索木の枝刈りをするか？

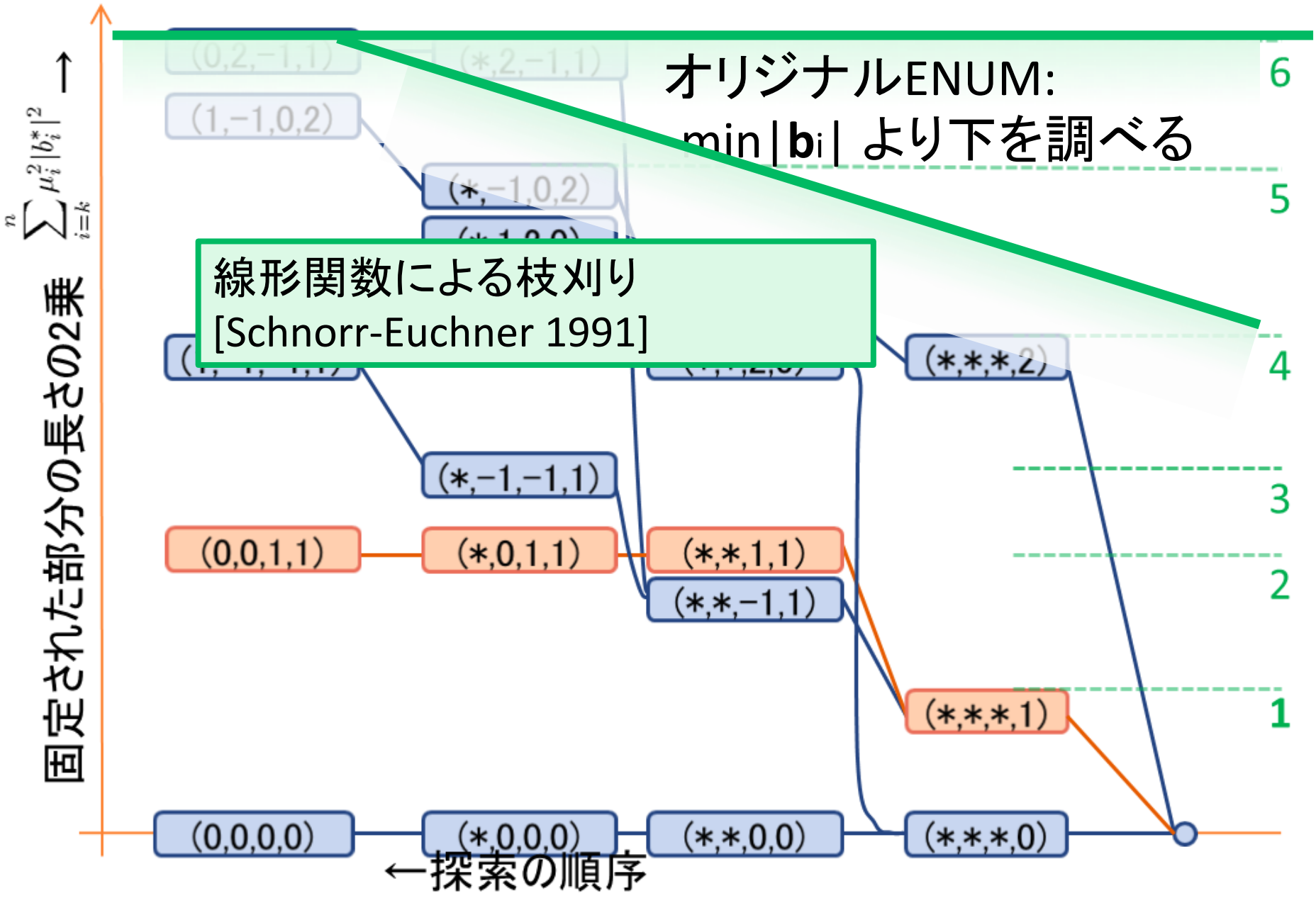
枝刈りの考え方：固定された部分の長さの2乗を調べる



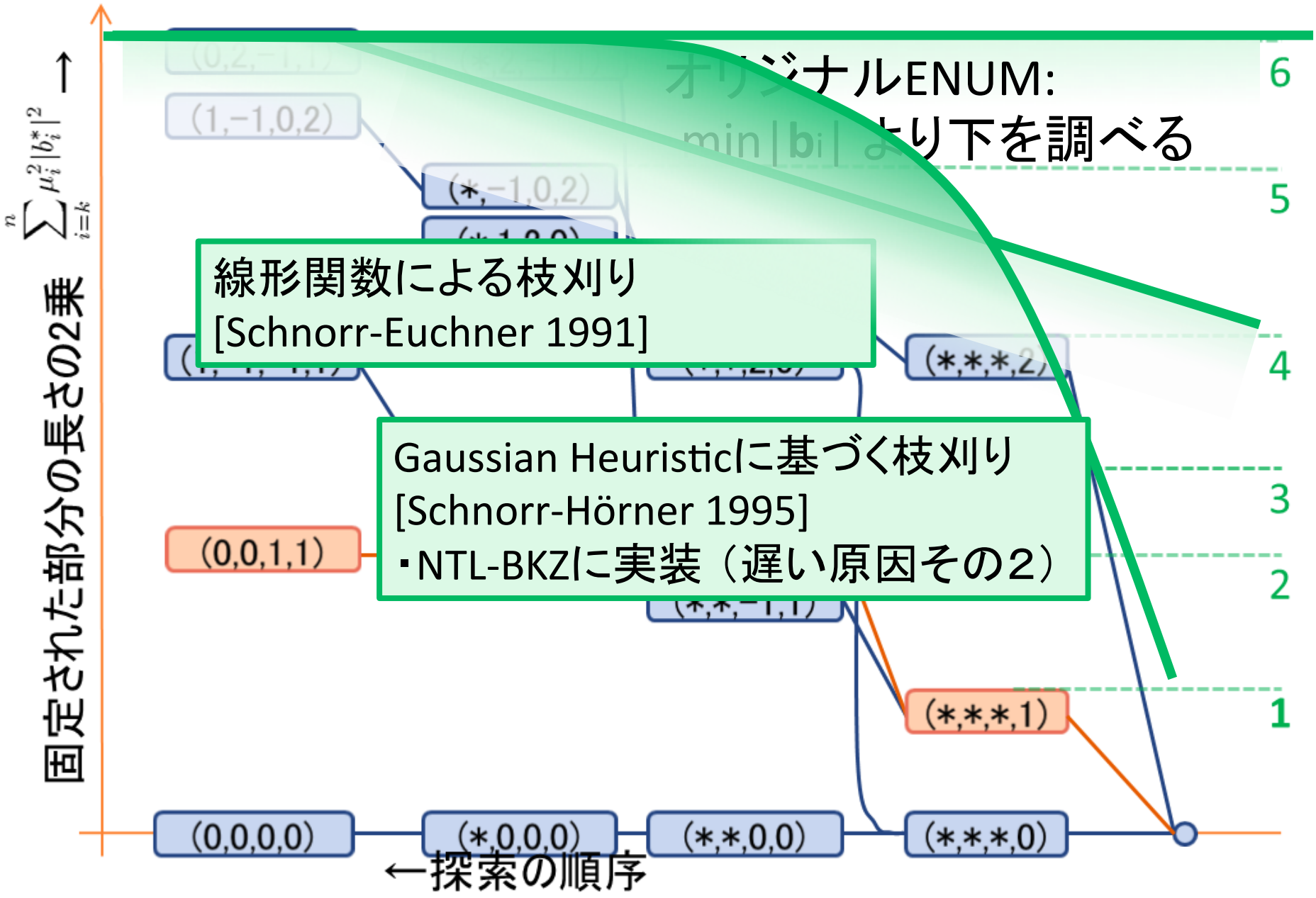
枝刈りの考え方：固定された部分の長さの2乗を調べる



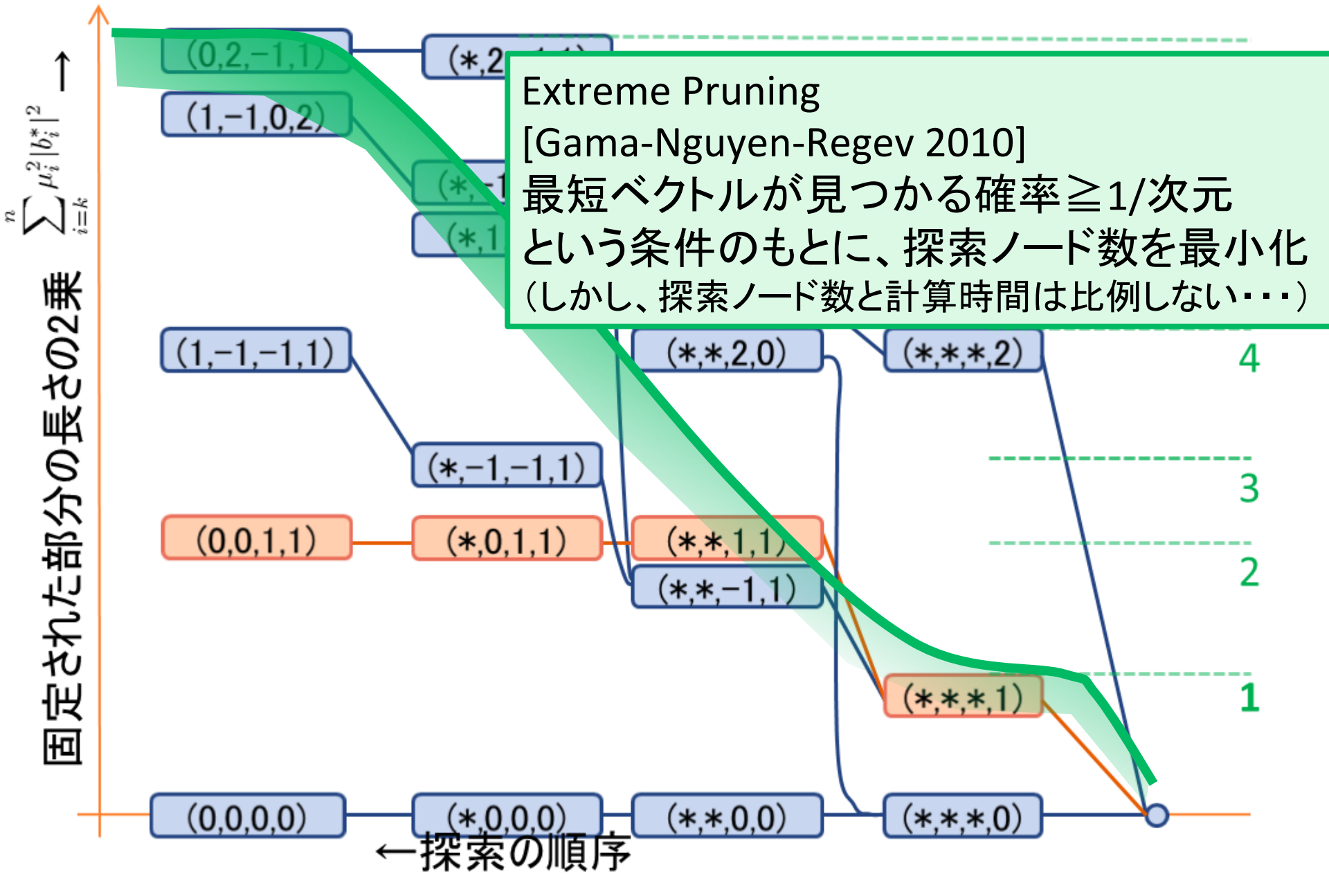
枝刈りの考え方：固定された部分の長さの2乗を調べる



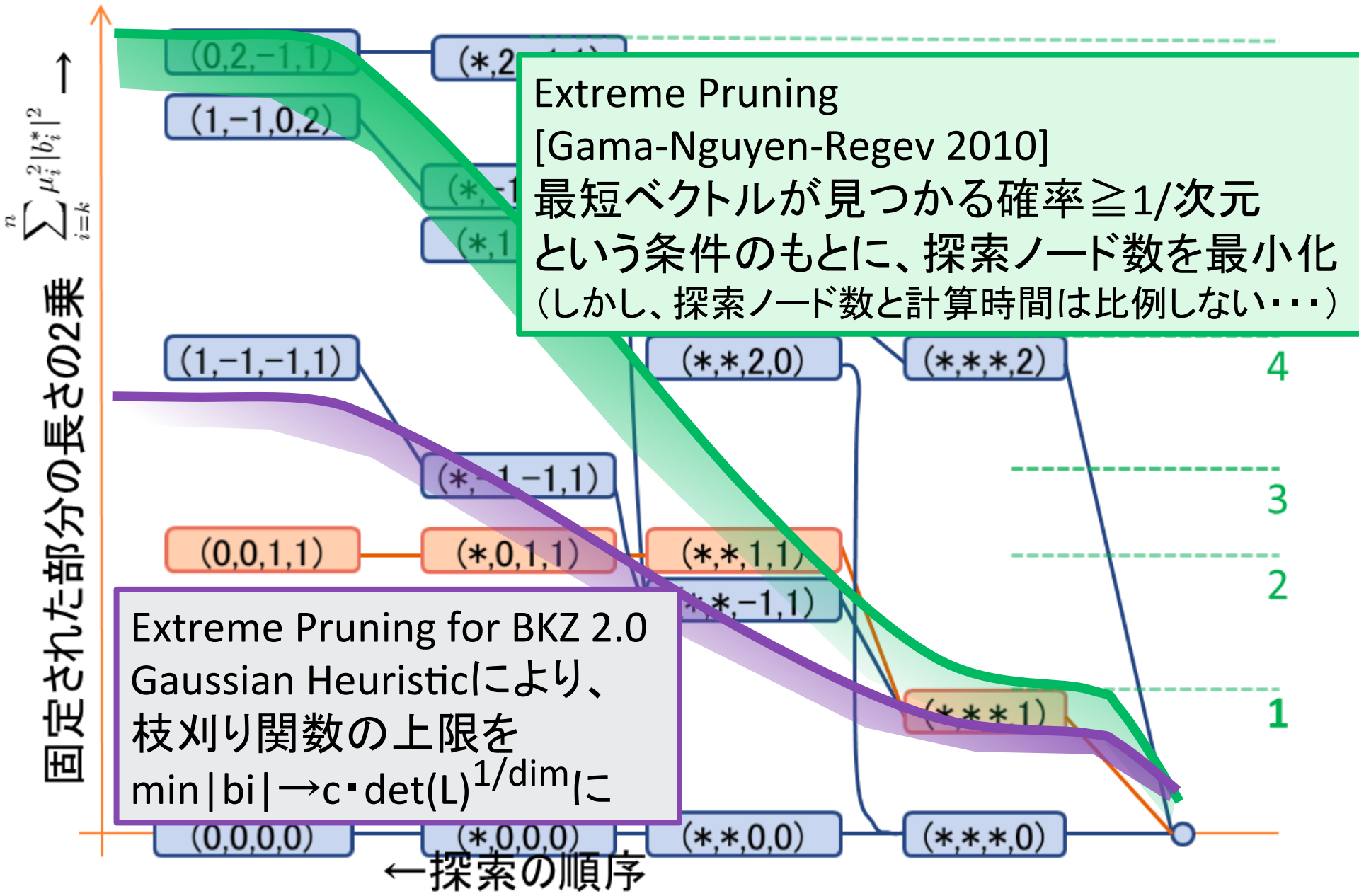
枝刈りの考え方：固定された部分の長さの2乗を調べる



枝刈りの考え方：固定された部分の長さの2乗を調べる



枝刈りの考え方：固定された部分の長さの2乗を調べる



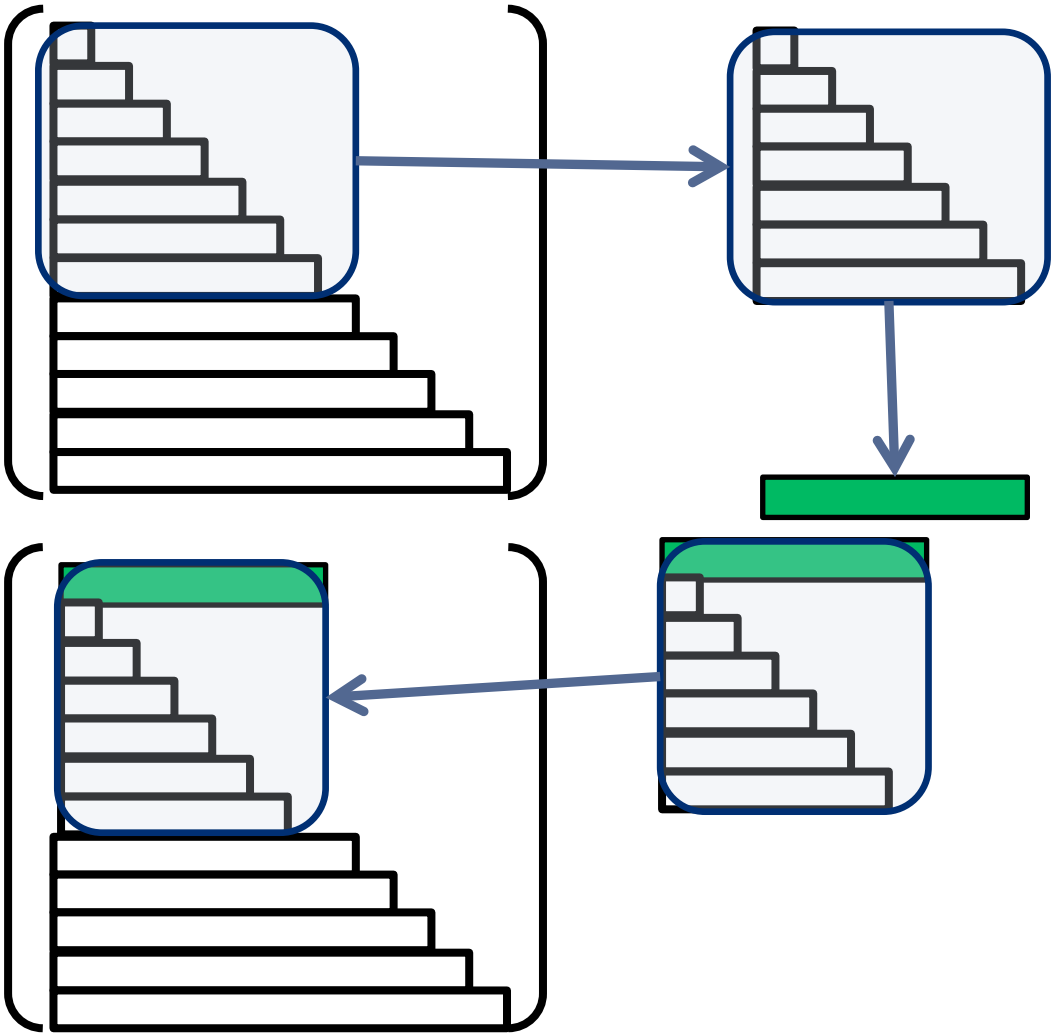
Extreme Pruning
[Gama-Nguyen-Regev 2010]
最短ベクトルが見つかる確率≧1/次元
という条件のもとに、探索ノード数を最小化
（しかし、探索ノード数と計算時間は比例しない・・・）

Extreme Pruning for BKZ 2.0
Gaussian Heuristicにより、
枝刈り関数の上限を
$\min|b_i| \rightarrow c \cdot \det(L)^{1/\dim}$に

BKZ 2.0アルゴリズム

BKZアルゴリズムの厳密さを犠牲にして、高速化したもの

オリジナルBKZ+4つの改良



改良①
ENUMの高速化のために再帰的にBKZをかける

改良②ENUMにおけるEP、③枝刈り関数の上限の変更

改良④ TerminatingBKZ
終了条件を「β-簡約」から「一定回数ループしたら終了」に変更

まとめ

- 今年度、NICTで世界記録を達成した2つの暗号安全性評価の研究成果について紹介
- ペアリング暗号
  - クラウド等でのプライバシ保護を実現する技術として期待されている
  - 現在の技術で解ける限界を評価し、今後20年間安全に使えるサイズを算出
- 格子暗号
  - 量子コンピュータが実現しても高い安全性を維持できる長期利用可能な暗号技術
  - 格子の最短ベクトル問題がどの次元まで解けるかを評価. 実用化に向けてより高速な解読アルゴリズムの開発と大規模な実験により安全性を検証していく