

表データの最適セル秘匿処理に対する マッチング攻撃とその防御手法の検討

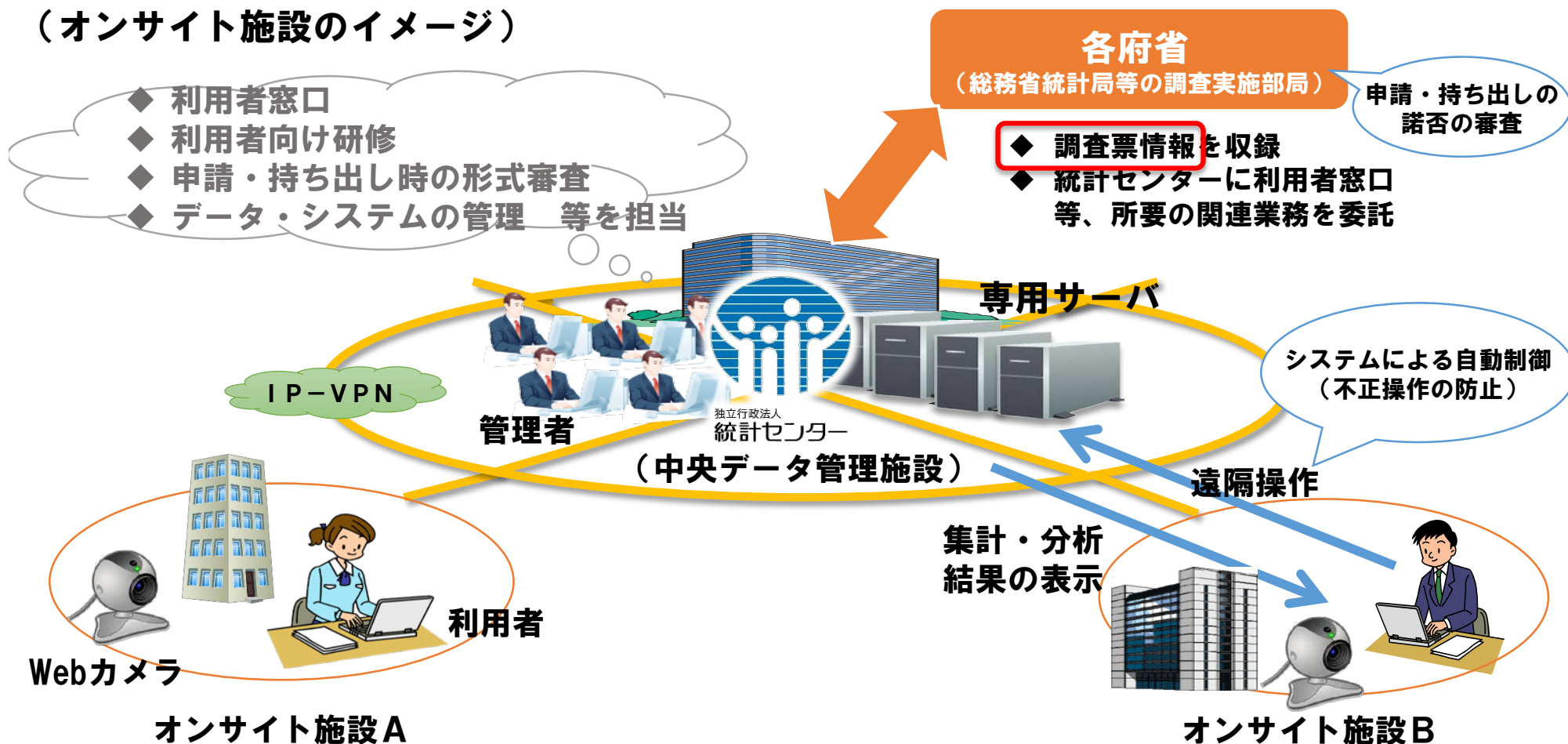
南 和宏 統計数理研究所
阿部穂日 総合研究大学院大学

2021年度統計関連連合大会企画セッション
「大規模データを対象にした匿名加工とプライバシー保護の動向」

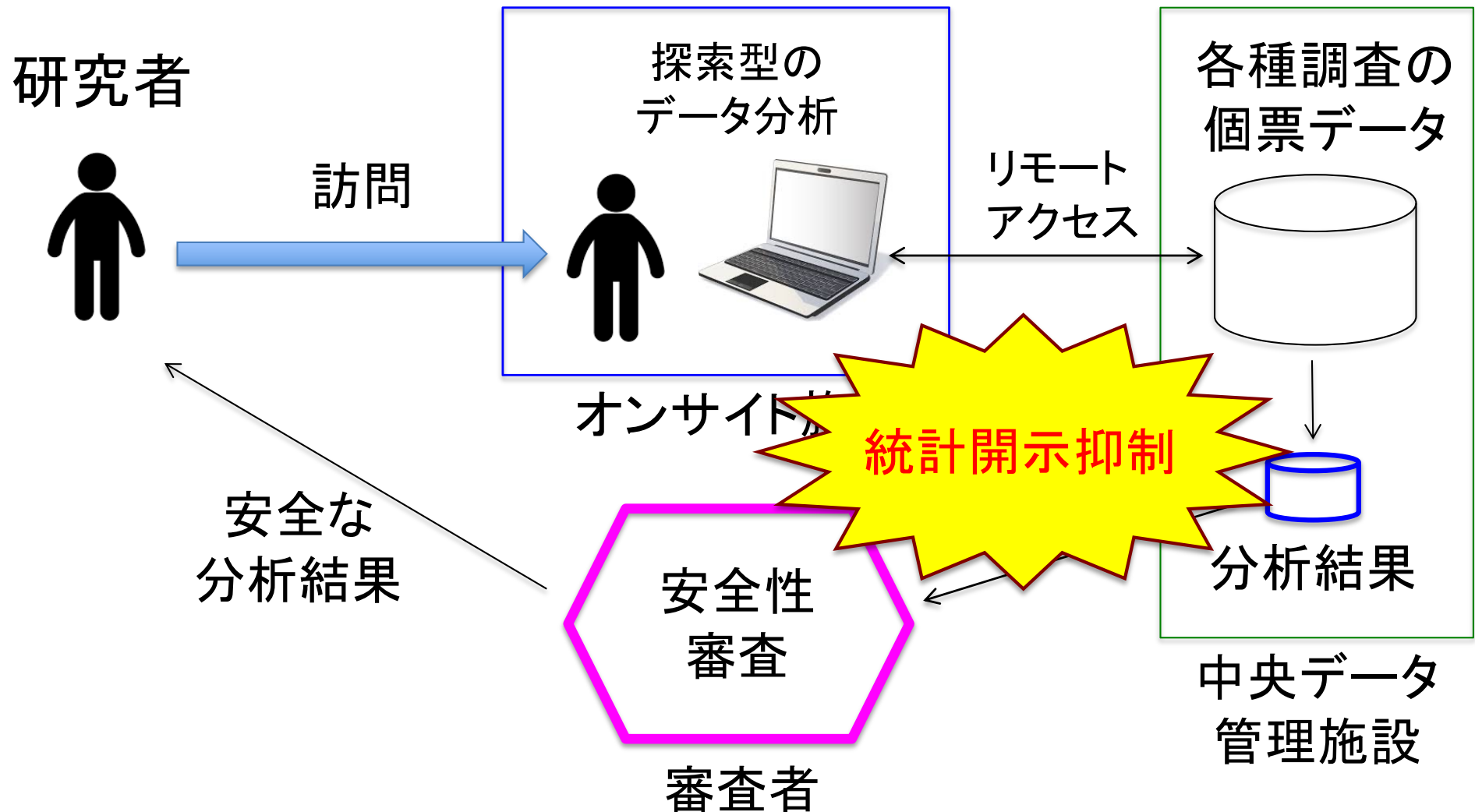
2021年9月7日

公的調査情報のオンライン利用

(オンサイト施設のイメージ)



個票データの機密情報を守る 統計開示抑制技術と安全性審査



表データの秘匿処理が一番難しい

度数表

	P ₁	P ₂	P ₃	合計
M ₁	20	24	28	72
M ₂	38	38	3	79
M ₃	40	39	42	121
合計	98	101	73	272

一次
秘匿

	P ₁	P ₂	P ₃	合計
M ₁	20	24	28	72
M ₂	38	38	NA	79
M ₃	40	39	42	121
合計	98	101	73	272

二次
秘匿

	P ₁	P ₂	P ₃	合計
M ₁	NA	24	NA	72
M ₂	NA	38	NA	79
M ₃	40	39	42	121
合計	98	101	73	272

最小度数ルール
(e.g., $x_i \geq 10$) に抵触

表データの制約条件

- $(r+c)$ 個の線形制約条件を含む
- 各セル値は非負

c 列

	a_{11}	$\cdots$	a_{1c}	$a_{1(c+1)}$	$\left. \sum_{j=1}^c a_{ij} = a_{i(c+1)} \quad i = 1, \dots, r \right\}$
	$\vdots$	$\ddots$	$\vdots$	$\vdots$	
	a_{r1}	$\cdots$	a_{rc}	$a_{r(c+1)}$	
r 行	$a_{(r+1)1}$	$\cdots$	$a_{(r+1)c}$	$a_{(r+1)(c+1)}$	

$\underbrace{\hspace{10em}}$

$$\sum_{i=1}^r a_{ij} = a_{(r+1)j} \quad j = 1, \dots, c$$

一次秘匿化したセルは十分な長さの 可能範囲が必要

- 秘匿化したセルの値の可能範囲がしきい値 δ 以上であることが必要
- 変数間の依存関係のチェックだけでは不十分

	P ₁	P ₂	P ₃	合計
M ₁	x_{11}	24	x_{13}	72
M ₂	x_{21}	38	x_{23}	116
M ₃	40	39	42	121
合計	98	101	110	309

$$\underline{a}_{23} = \min x_{23}$$

$$\text{subject to } x_{11} + x_{13} = 72 - 24$$

$$x_{21} + x_{23} = 116 - 38$$

$$x_{11} + x_{21} = 98 - 40$$

$$x_{13} + x_{23} = 110 - 42$$

$$(x_{11}, x_{13}, x_{21}, x_{23}) \geq 0$$

and

$$\overline{a}_{23} = \max x_{23}$$

$$\text{subject to } x_{11} + x_{13} = 72 - 24$$

$$x_{21} + x_{23} = 116 - 38$$

$$x_{11} + x_{21} = 98 - 40$$

$$x_{13} + x_{23} = 110 - 42$$

$$(x_{11}, x_{13}, x_{21}, x_{23}) \geq 0.$$



$$\min x_{23} = 20 \text{ and } \max x_{23} = 68$$

セル秘匿問題(CSP)

- 秘匿パターン $y_i \in \{0, 1\} \quad i = 1, \dots, n$

10	NA
5	80

 $\longleftrightarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

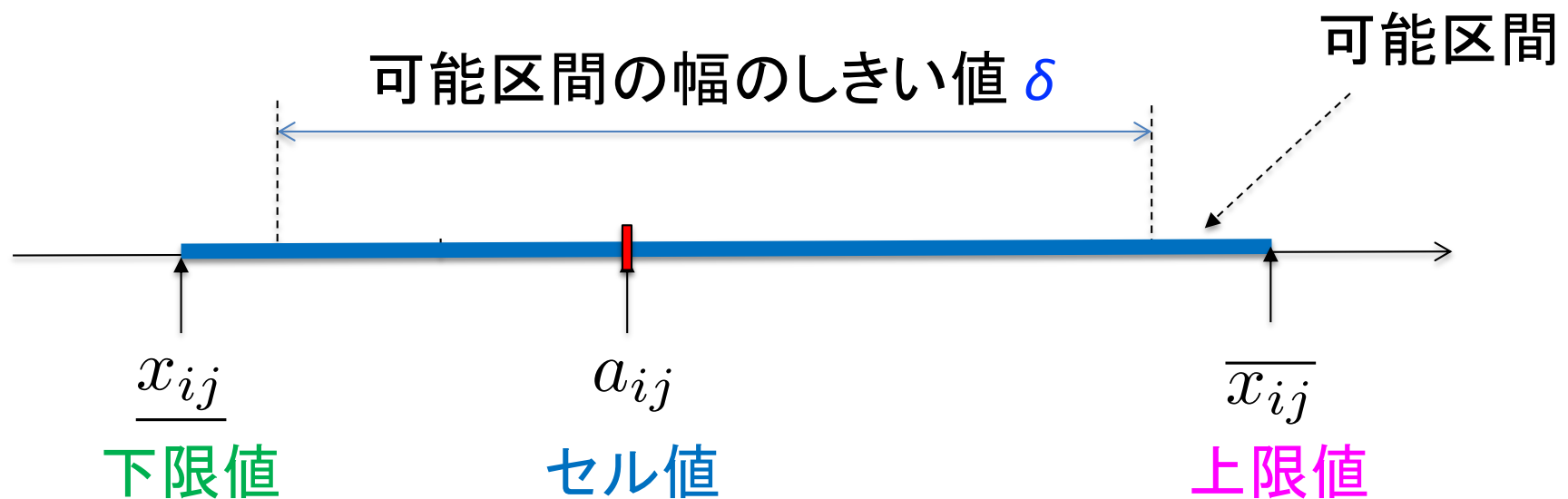
- 目的関数: 秘匿セル数

$$\sum_{i=1}^n y_i$$

- 拘束条件: 各一次秘匿セル値の機密性保護

可能区間の要件

$$\text{可能区間の幅 } w = \overline{x_{ij}} - \underline{x_{ij}} > \delta$$



行計、列計の線形さえ満たせば可能な値と暗黙に仮定

秘匿パターンによる マッチング攻撃

攻撃シナリオ



機密セルの値を推測



可能区間の幅のしきい値は
全てのセルに固定値を指定

- 度数表にのみ適用可能
- 数量表は攻撃の対象外

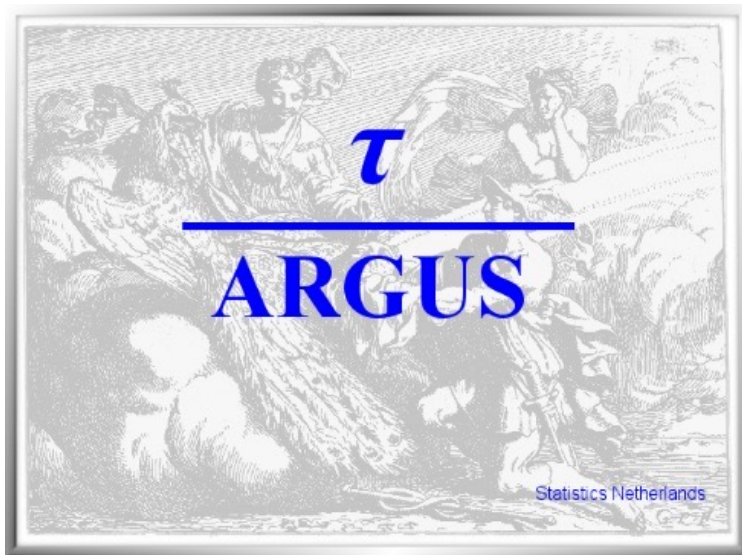
- 秘匿アルゴリズム
- セキュリティパラメータ
の知識をもつ

- 度数しきい値
- 可能区間の幅
しきい値

決定論的な表セル秘匿アルゴリズム

- τ -Argus

- Optimal
- Network



- SDCLink

[minami:uROS2017]

- R言語で実装
- 分析者と審査者の連携機能を強化

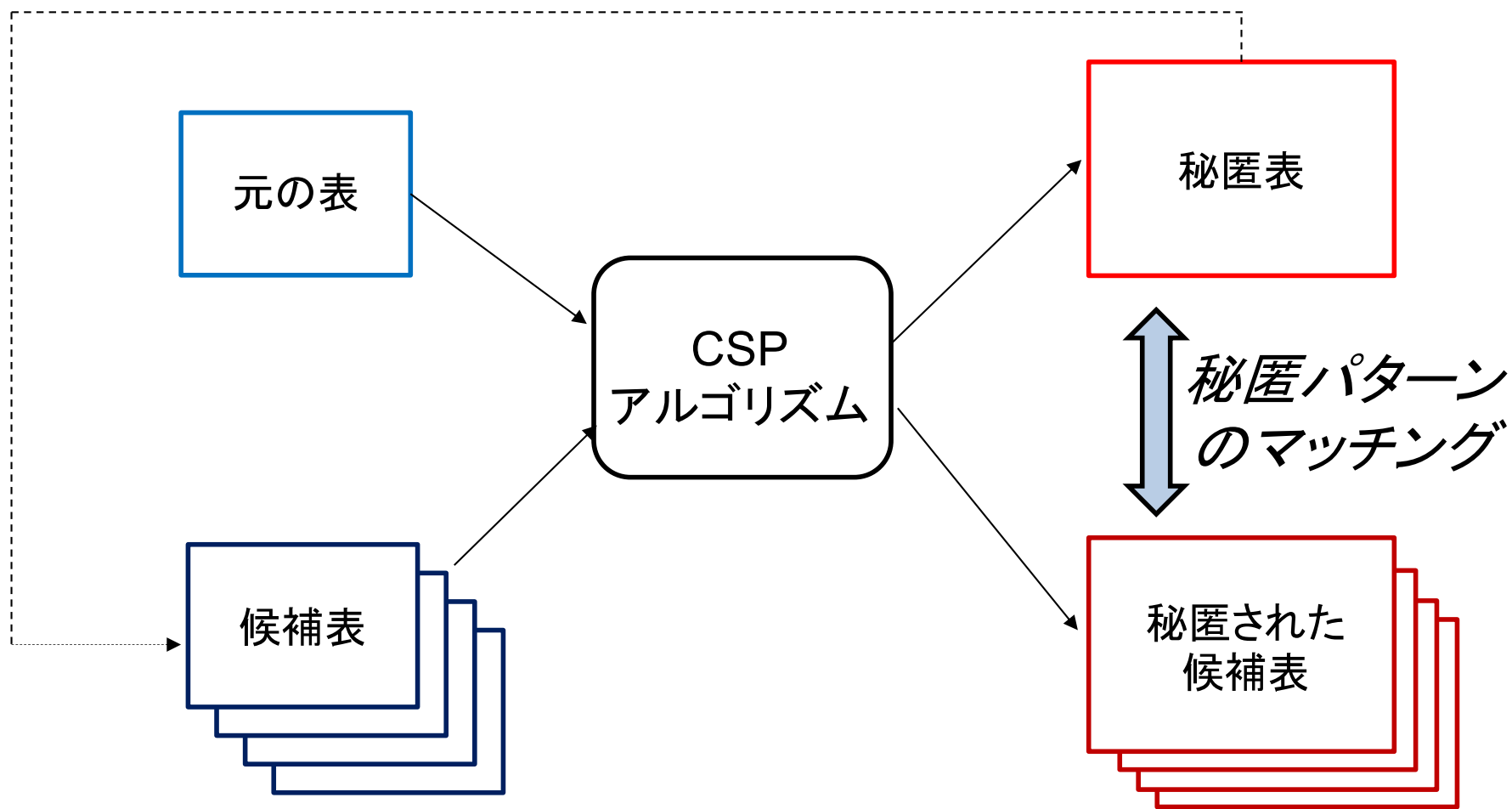


秘匿処理
関数

最適解が一つの場合、最適化アルゴリズムの出力は一意に決ま

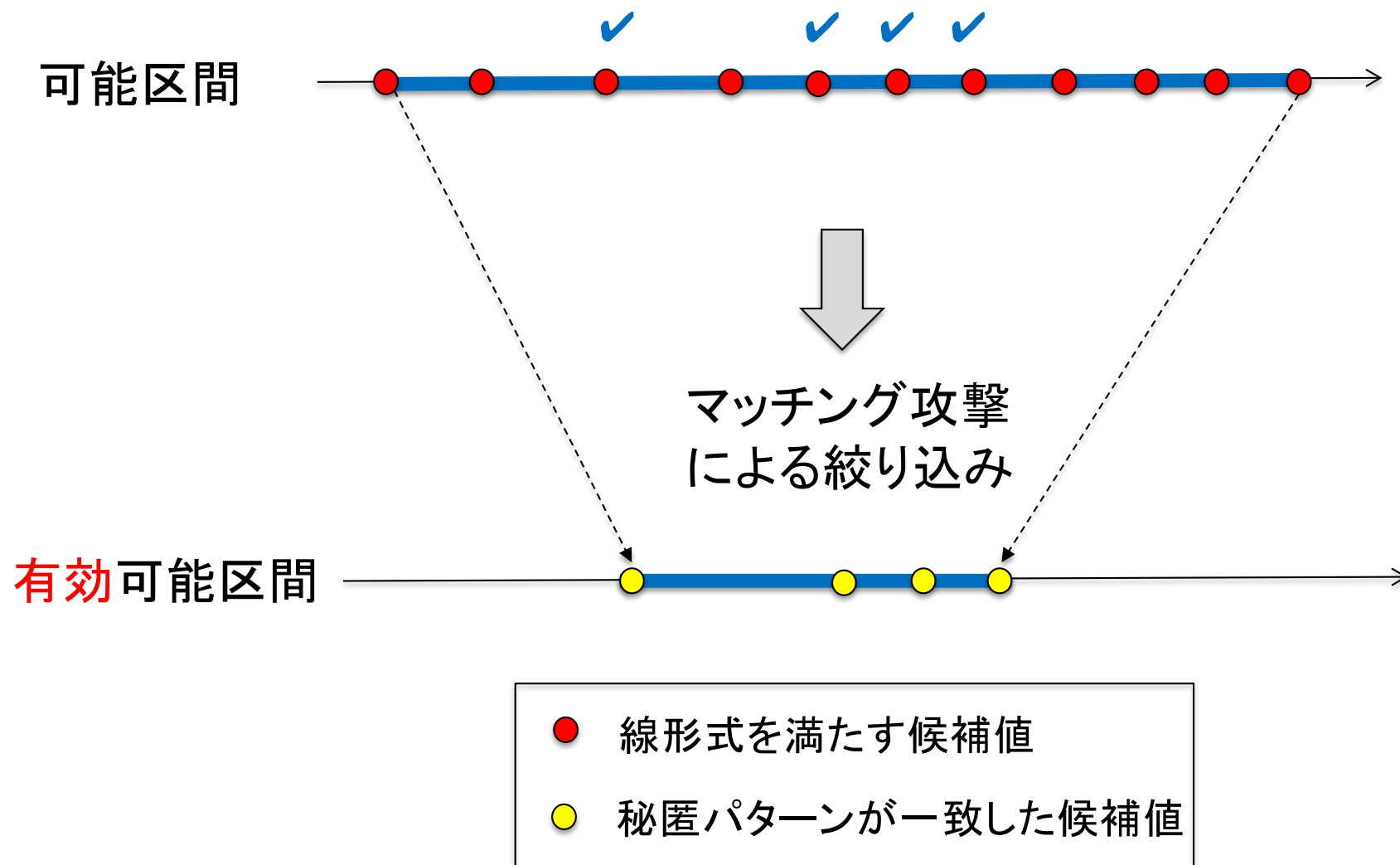
秘匿パターンのマッチングによる 候補テーブルの絞り込み

秘匿セルの値を補完



秘匿パターンが再現できた候補テーブルの値のみが真の候補値！

可能区間の絞り込み



評価実験

Q: マッチング攻撃で可能区間の条件が侵害される一次秘匿セルの割合はどの程度か？

- セル数: 16, 25, 36, 49の二次正方の度数分布表をランダムに各50個生成
 - セル値は平均15, 標準偏差10の正規分布から抽出
 - 線形和に関する拘束条件の零空間の次元が4以下となるよう生成
- Benders分割アルゴリズムで二次秘匿テーブルを作成
 - 度数しきい値: 5
 - 可能区間のしきい値: 8
- Benders分割アルゴリズムを用いた秘匿パターンマッチング攻撃を実施
 - 度数しきい値: 5
 - 可能区間のしきい値: 8
- 安全でない一次秘匿セルの割合を集計

マッチング攻撃で安全要件が破られた(可能区間の幅が8未満となった) 1次秘匿セル数

表セル数	一次秘匿セル数
16	104
25	170
36	230
49	271

マッチング攻撃



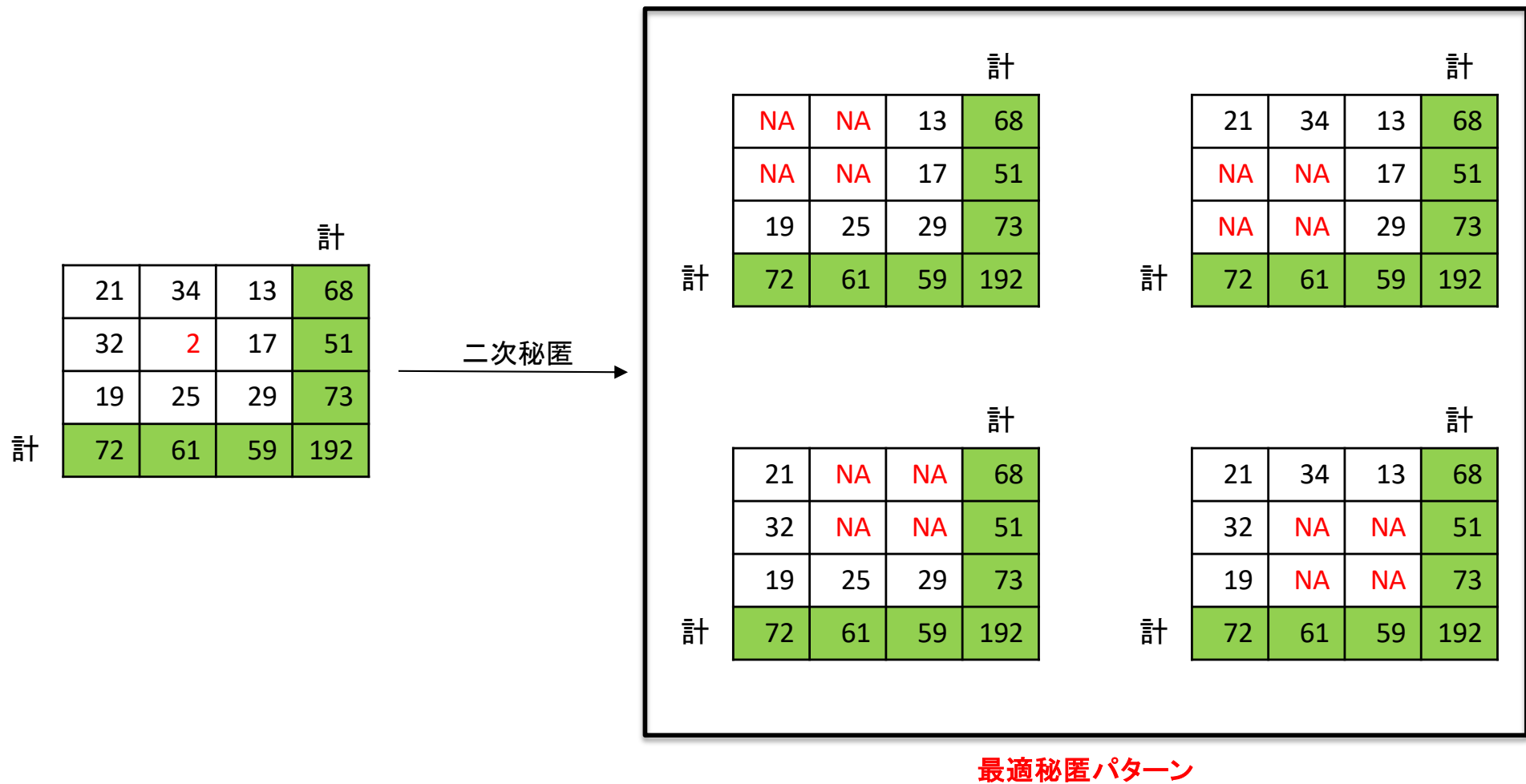
安全でない一次秘匿セル数	安全でない一次秘匿セルの割合
48	46%
117	69%
190	83%
226	83%

非決定論的アルゴリズムへの拡張

非決定論的セル秘匿アルゴリズムの 導入によるマッチング攻撃の防止

- マッチング攻撃は、現在のセル秘匿アルゴリズムが決定論的であり、**同じ表からは常に同じ秘匿表が出力**されることを利用している
- ランダム要素を加えた非決定論的アルゴリズムを用い、**同じ表から異なる秘匿表が出力**され得る場合、マッチング攻撃は防止できる

最適秘匿パターンは一般に複数存在する



最適秘匿パターンのうち1つをランダムに出力するアルゴリズムを検討

ダミーの一次秘匿セルの追加による ランダムネスの導入

	P ₁	P ₂	P ₃	Sum
M ₁	13	79	13	105
M ₂	31	75	1	107
M ₃	21	53	17	91
Sum	65	207	31	303

一次秘匿

	P ₁	P ₂	P ₃	Sum
M ₁	13	79	13	105
M ₂	31	75	-	107
M ₃	21	53	17	91
Sum	65	207	31	303

一次秘匿されていないセルから
ダミーの一次秘匿セルを一つ選ぶ

	P ₁	P ₂	P ₃	Sum
M ₁	*	*	*	105
M ₂	x	*	-	107
M ₃	21	53	17	91
Sum	65	207	31	303

二次秘匿

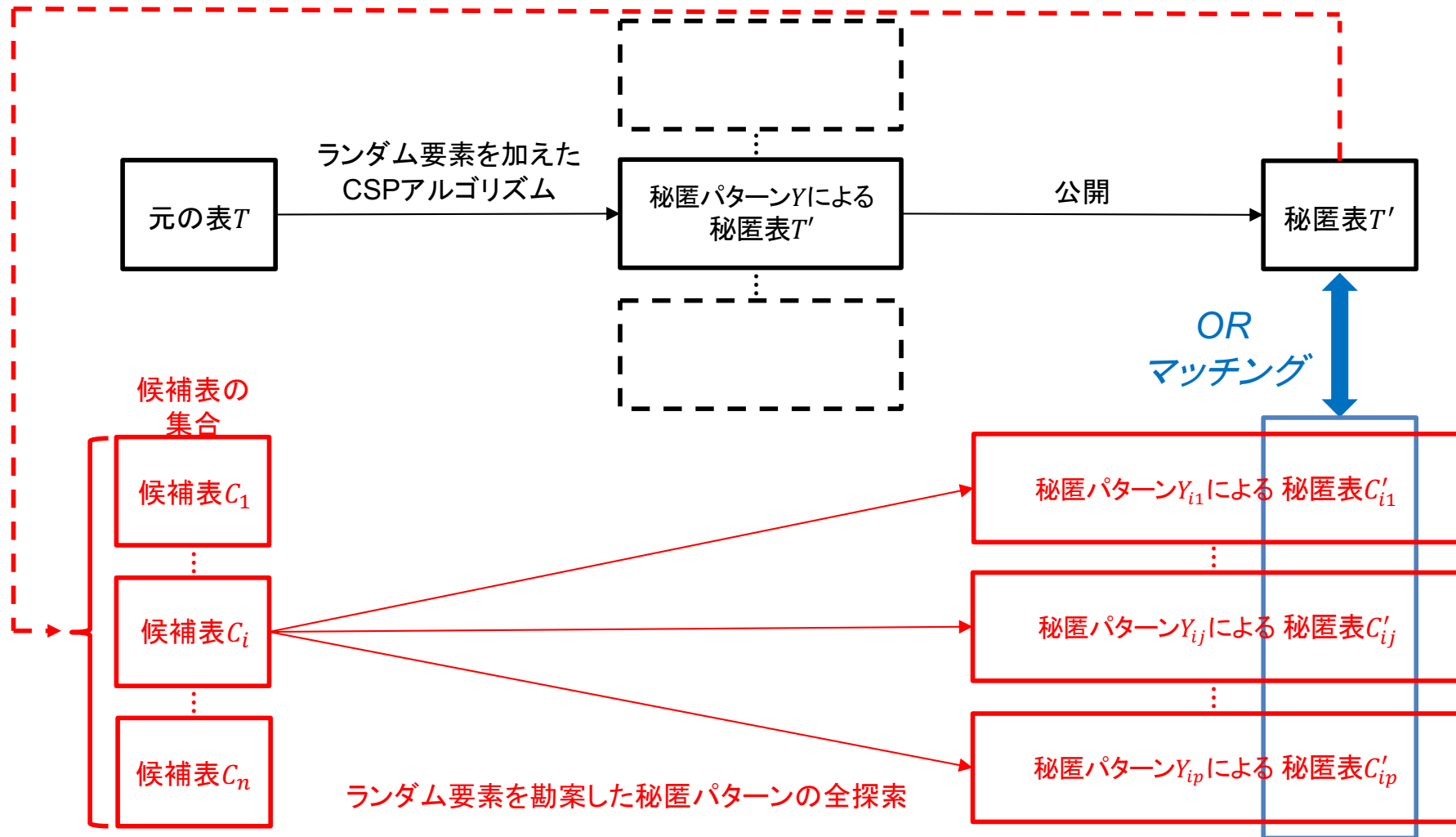
	P ₁	P ₂	P ₃	Sum
M ₁	13	79	13	105
M ₂	x	75	-	107
M ₃	21	53	17	91
Sum	65	207	31	303

乱数要素の追加による情報損失の増加

- セル数36の二次正方の度数分布表をランダムに各50個生成
 - セル値は平均15, 標準偏差10の正規分布から抽出
- 決定論的アルゴリズム・非決定論的アルゴリズムで秘匿し、秘匿されたセルの数・割合を比較

	一次秘匿セル数	秘匿セル数	秘匿セルの割合
非決定論的 アルゴリズム	260	482	0.27
決定論的 アルゴリズム	210	417	0.23
差分	50	65	

しかし、非決定論的アルゴリズムに対する 広義のマッチング攻撃は存在する



マッチング攻撃で安全要件(可能区間の幅のしきい値)が破られた一次秘匿セル数

	一次 秘匿 セル数	うち 安全で ない	有効可能区間の幅							
			0	1	2	3	4	5	6	7
決定論的 アルゴリズム	199	164	46	28	39	40	6	3	1	1
非決定論的 アルゴリズム		140	57	26	22	17	4	6	2	6

安全でない一次秘匿セルの割合:

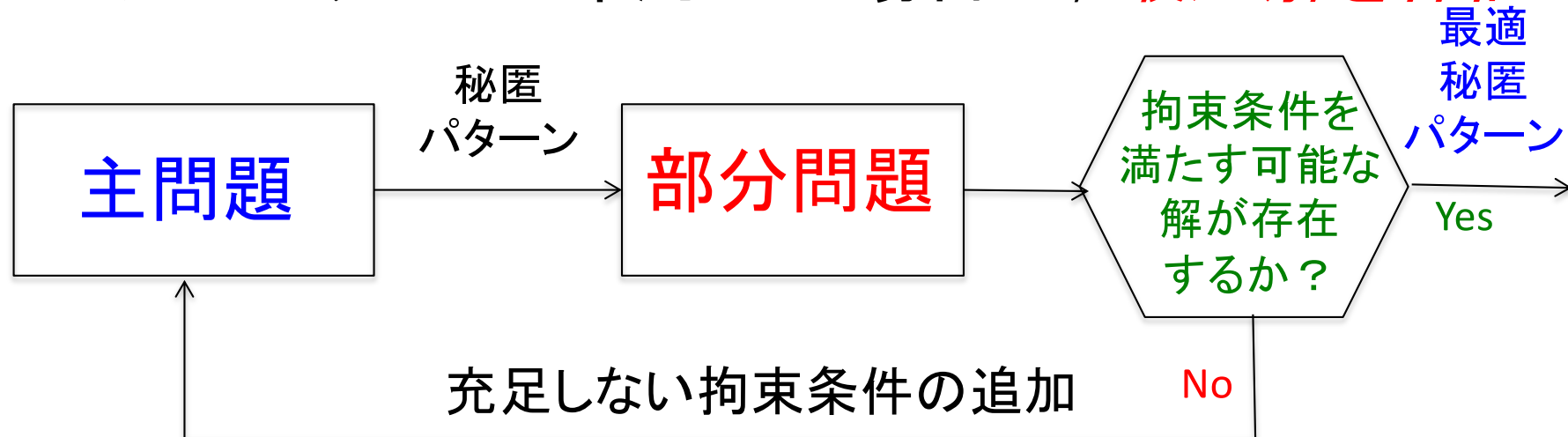
決定論的アルゴリズム82.4% ⇨ 非決定論的アルゴリズム70.4%



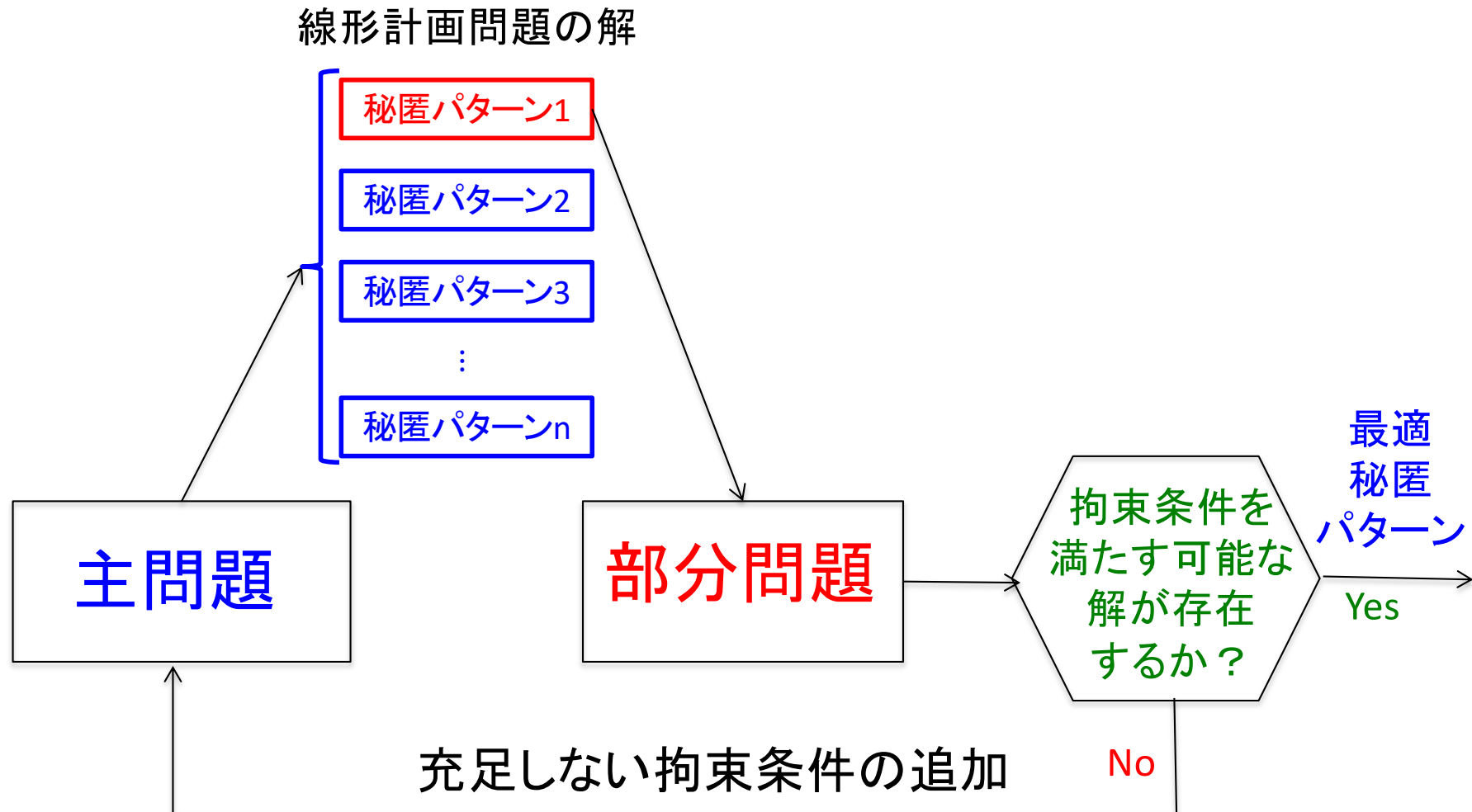
ダミーセルの導入はやめて、複数の最適秘匿パターンから一つをランダムに選択する手法を検討

Benders分割によるセル秘匿アルゴリズムの拡張

- 主問題と部分問題に分割
 - 主問題: 拘束条件を満たす秘匿パターンの最適化
 - 部分問題: 秘匿パターンを確認し、安全な秘匿でない場合は拘束条件を追加
- 大部分の問題で効率的に実行
- アルゴリズムが終了した場合は, **最適解を保証**

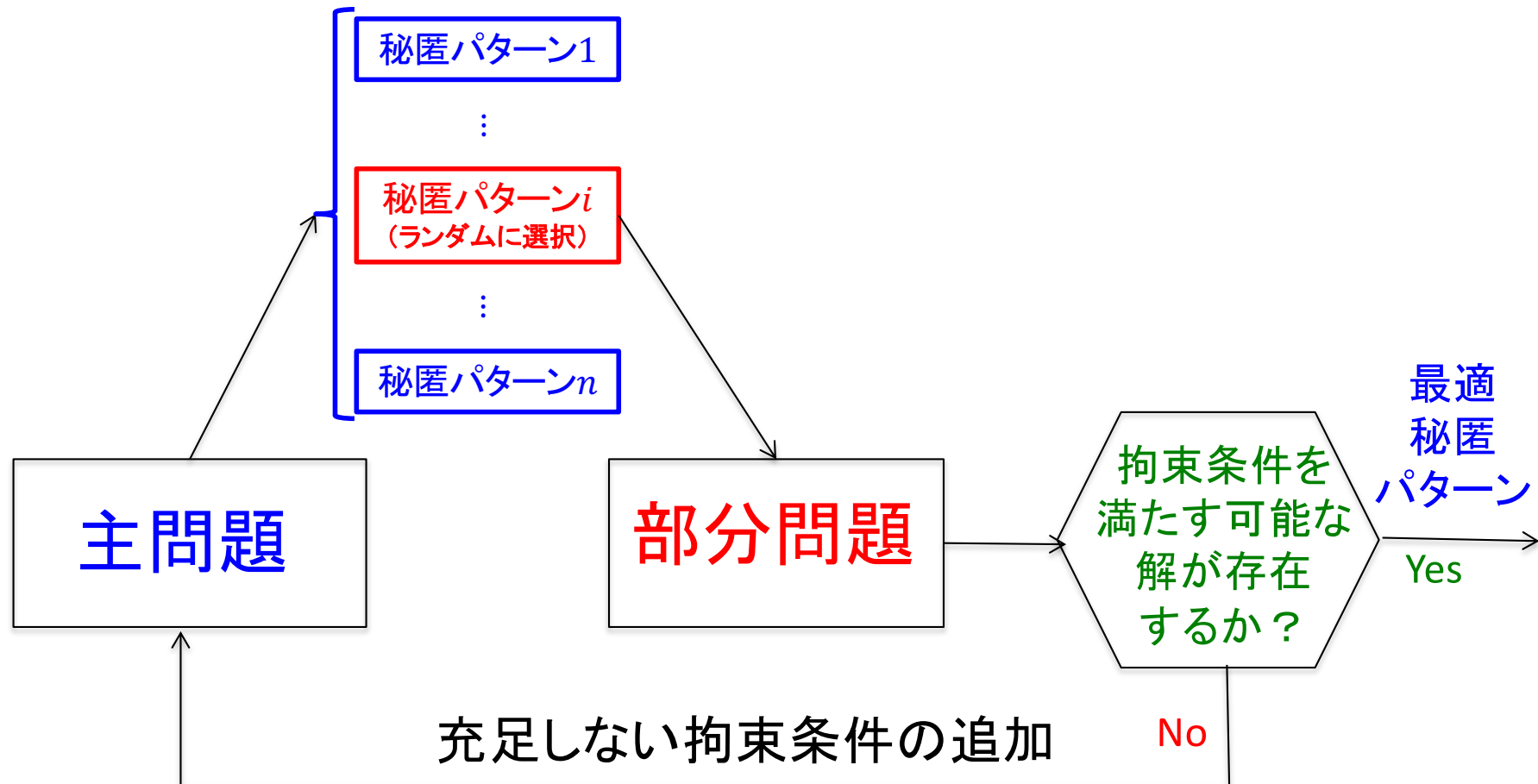


主問題では毎回秘匿パターンを導出



主問題の解である秘匿パターンを ランダムに選択

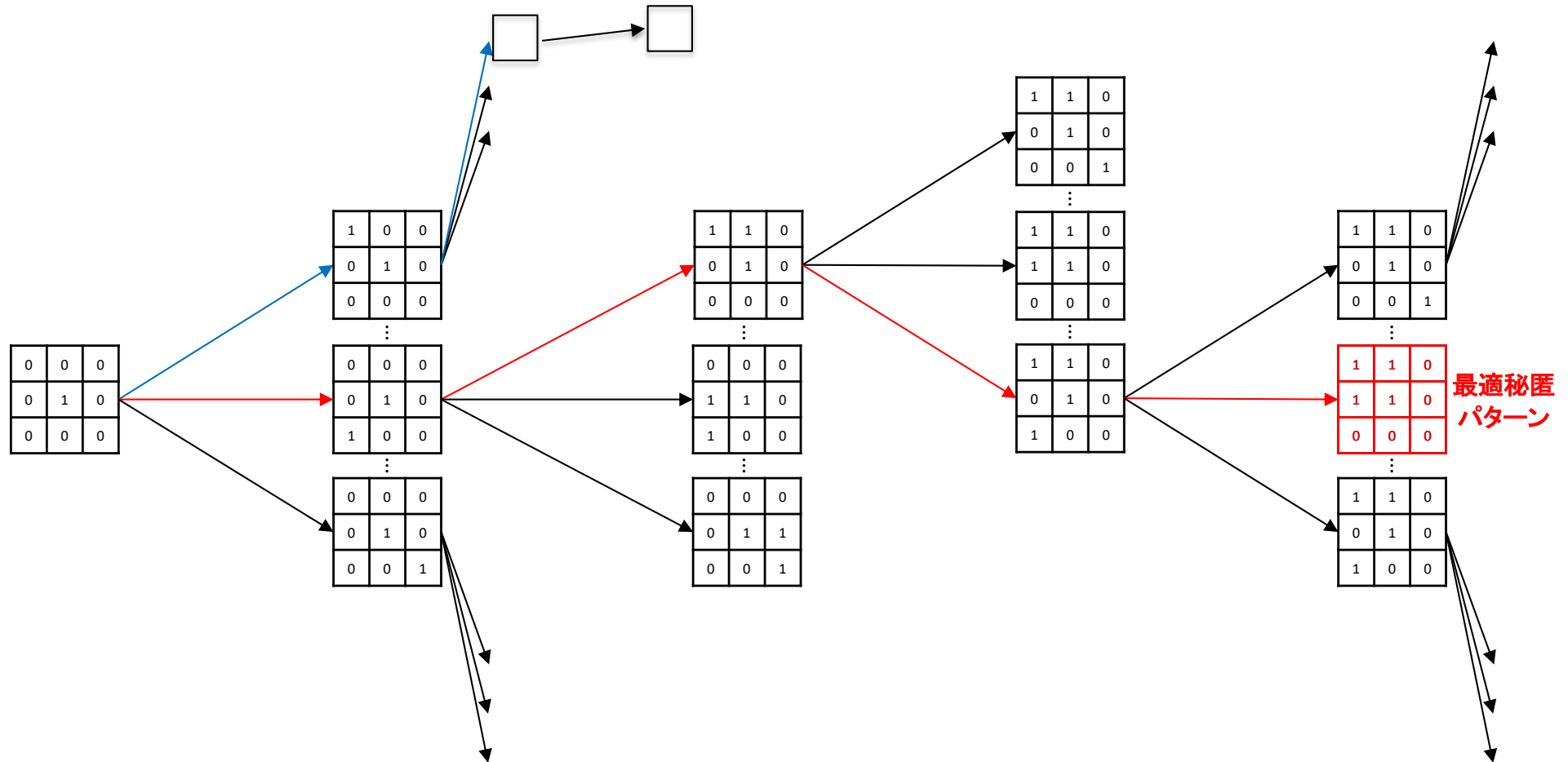
線形計画問題の解



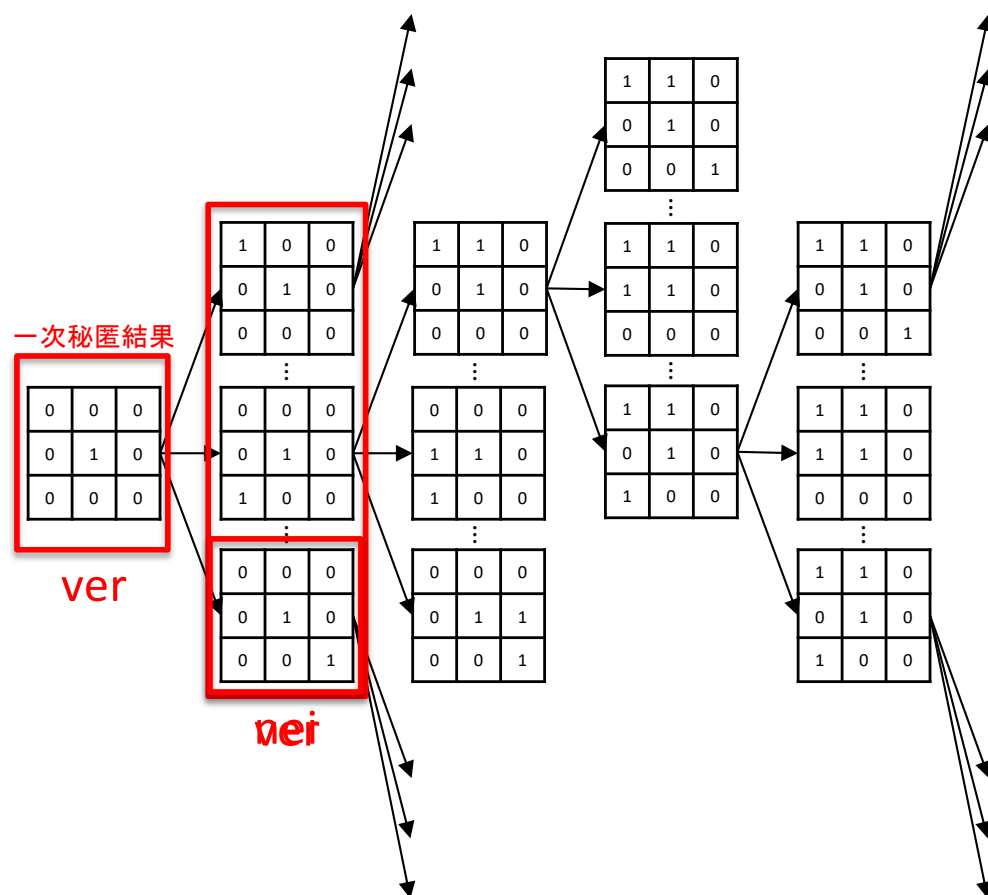
非決定論的なBenders分割では、秘匿パターン・ツリーをランダムに探索し、リーフノードに到達する

頂点：秘匿パターンと拘束条件の組

辺：各点の拘束条件から主問題を解いた解であることを意味



マッチング攻撃には秘匿セルツリーの全探索が必要



1. 最初の点をtodoストックへ格納
2. todoから点verを取り出す
3. verの拘束条件を主問題で解き, verに隣接する点の集合neiを探索
4. neiの各点の秘匿パターンを部分問題で解き, 安全に秘匿されているかを確認し, 秘匿が不十分な場合は拘束条件を追加
5. neiのうち秘匿が完了していない点をtodoへ格納
6. todoが空でなければ2.へ戻る

実験の結果: グラフ探索が終了しない

考察

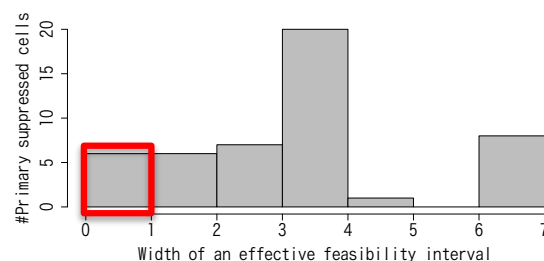
- 最適秘匿パターンの選択問題はNP-困難
 - 最悪ケースでは指数時間の計算量が必要
 - つまり、秘匿パターンの列挙は、(NP-困難 × 秘匿パターンツリーのリーフノード数)の計算時間が必要
- 今回のBenders分割アルゴリズムにも該当
 - 主問題と部分問題のループで秘匿パターンが振動し、解が収束しない問題が知られており、[Baena20]ではその安定化に取り組んでいる → プライバシー保護の観点からはこの問題を放置するのが望ましい？

まとめ

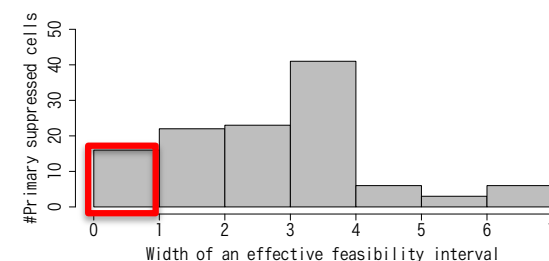
- 表セル秘匿問題は、機密セルの値を隠す最適な秘匿パターンの決定問題である
- 秘匿セル変数の解空間を探索するマッチング攻撃により、一次秘匿セルの安全性が侵害される
- 複数存在する最適秘匿パターンのうち1つをランダムに出力する非決定論的CSP アルゴリズムについて、特定状況における論理的安全性を考察した
- 最適秘匿パターン全探索にかかる**平均の**計算困難性の理論的、実証的評価が今後の課題
- Benders分割アルゴリズムの**解の振動の発生条件の解明**とアルゴリズムへの明示的な組み込みの検討

有効可能区間の幅の分布

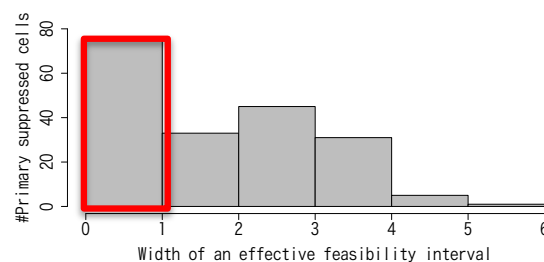
#Cells in a table	Width of an effective feasibility interval	#Unsafe cells
16	0	6
	1	6
	2	7
	3	20
	4	1
	5	0
	6	4
	7	4
25	0	16
	1	22
	2	23
	3	41
	4	6
	5	3
	6	5
	7	1
36	0	75
	1	33
	2	45
	3	31
	4	5
	5	0
	6	1
	7	0
49	0	92
	1	33
	2	28
	3	57
	4	4
	5	4
	6	5
	7	3



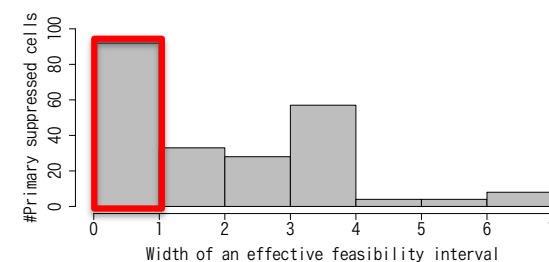
(a) Tables with 16 cells



(b) Tables with 25 cells



(c) Tables with 36 cells



(d) Tables with 49 cells