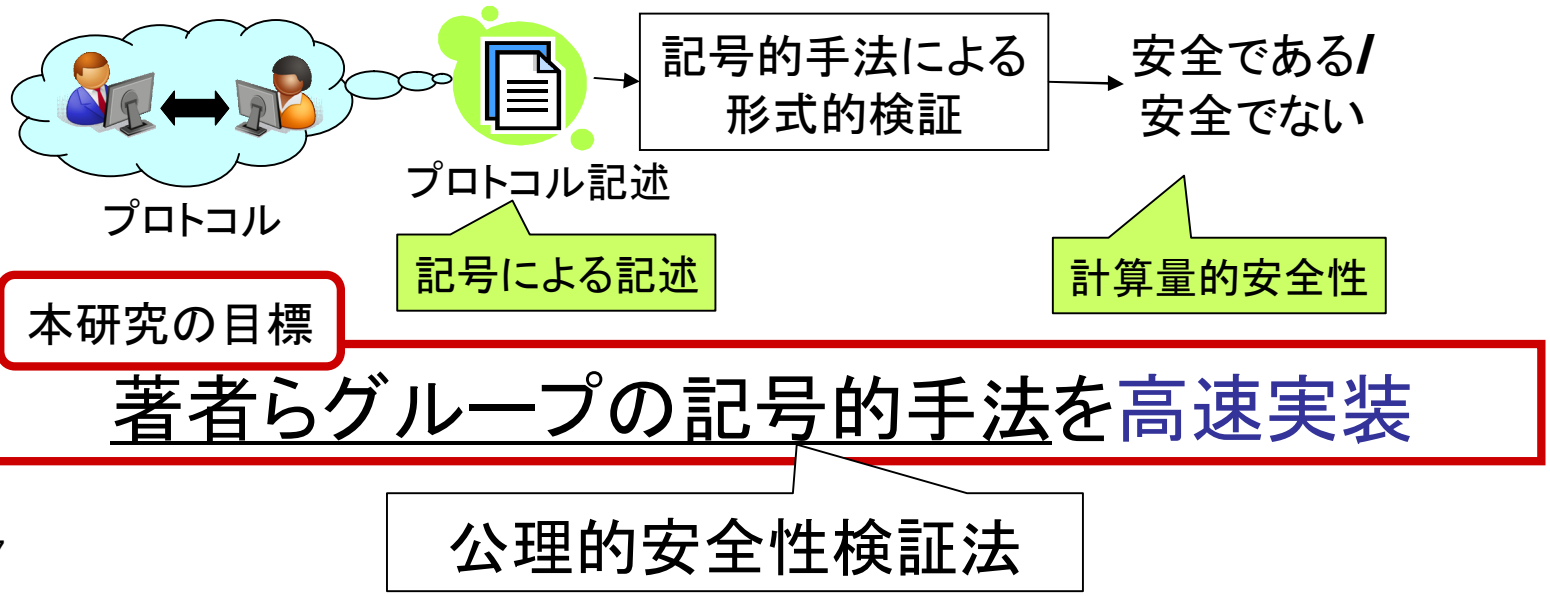
暗号プロトコルに対する公理的安全性検証法の主要処理の改良と実装

○鎌野 善樹, 鈴木 斎輝,
吉田 真紀, 藤原 融
大阪大学 大学院情報科学研究科

従来研究

- 計算量的安全性を記号的手法を用いて形式的に検証
  - 著者らのグループも着手[鈴木et al.,09]
- 他グループの記号的手法の多くは実装済み
- 著者らのグループの記号的手法 [吉田-藤原,97]は, ProVerifの手法と同等の検証能力をもつが未実装



公理的安全性検証法の特長

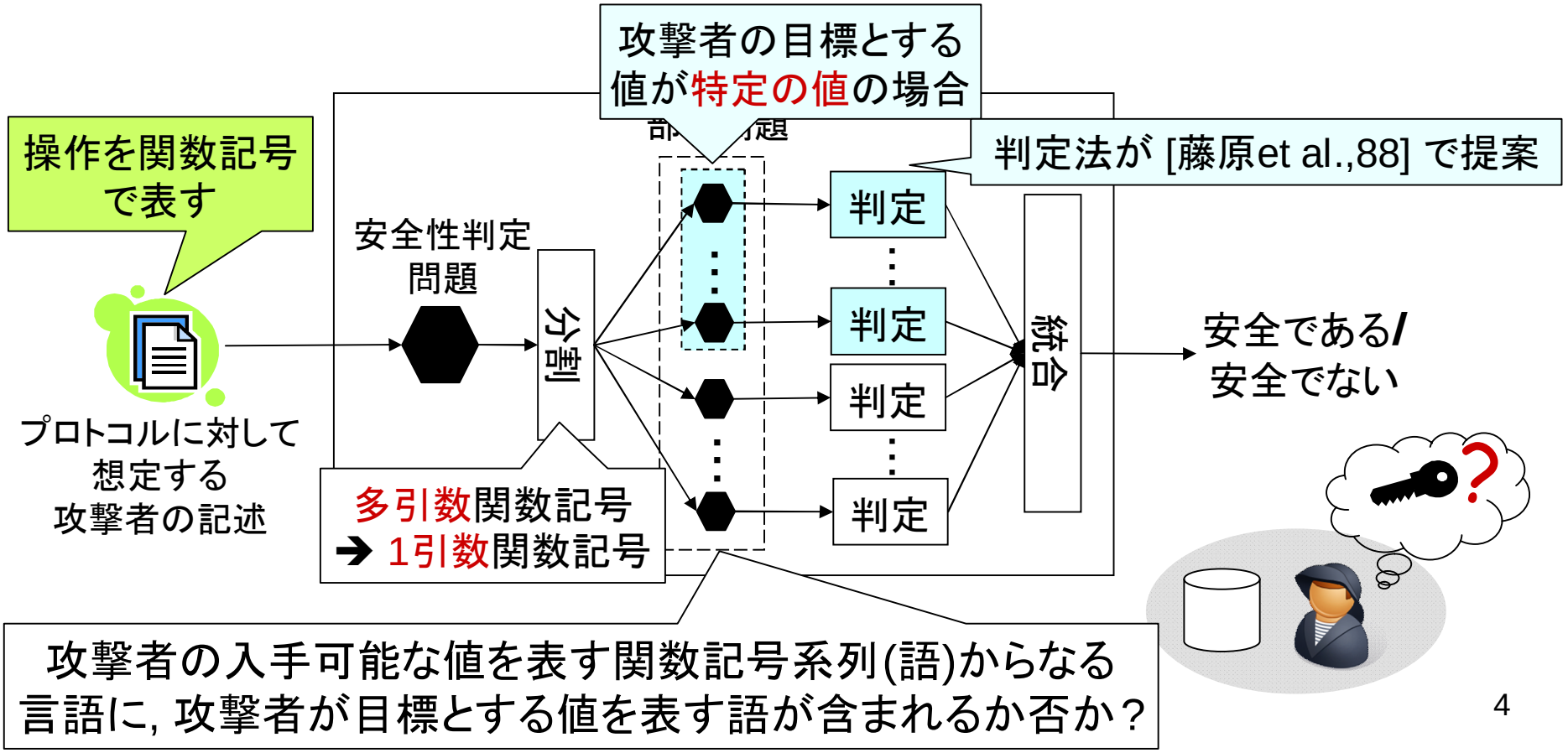
- ProVerifが基とする手法との比較により示す
  - 比較項目はProVerif との比較時によく挙げられる項目

	ProVerifが基とする手法	公理的安全性検証法
記述能力	多様なプリミティブを扱える ・共通・秘密鍵暗号, ハッシュ関数, DH鍵交換	
想定する実行状況	プロトコルの実行セッション回数の制限なし	
停止性	タグ付きプロトコルでの 停止性	十分条件を満たす プロトコルでの停止性
攻撃の再構成	攻撃の再構成が可能	

計算量的安全性証明への応用	汎用的結合可能安全性 [Canneti-Herzog,04] ゼロ知識証明 [Backes-Unruh,08] 観測等価性 [Comon-Lundh-Cortier,08]	汎用的結合可能安全性 ・相互認証プロトコル [鈴木et al.,SCIS09] ・鍵交換プロトコル [鈴木et al.,FAIS09]

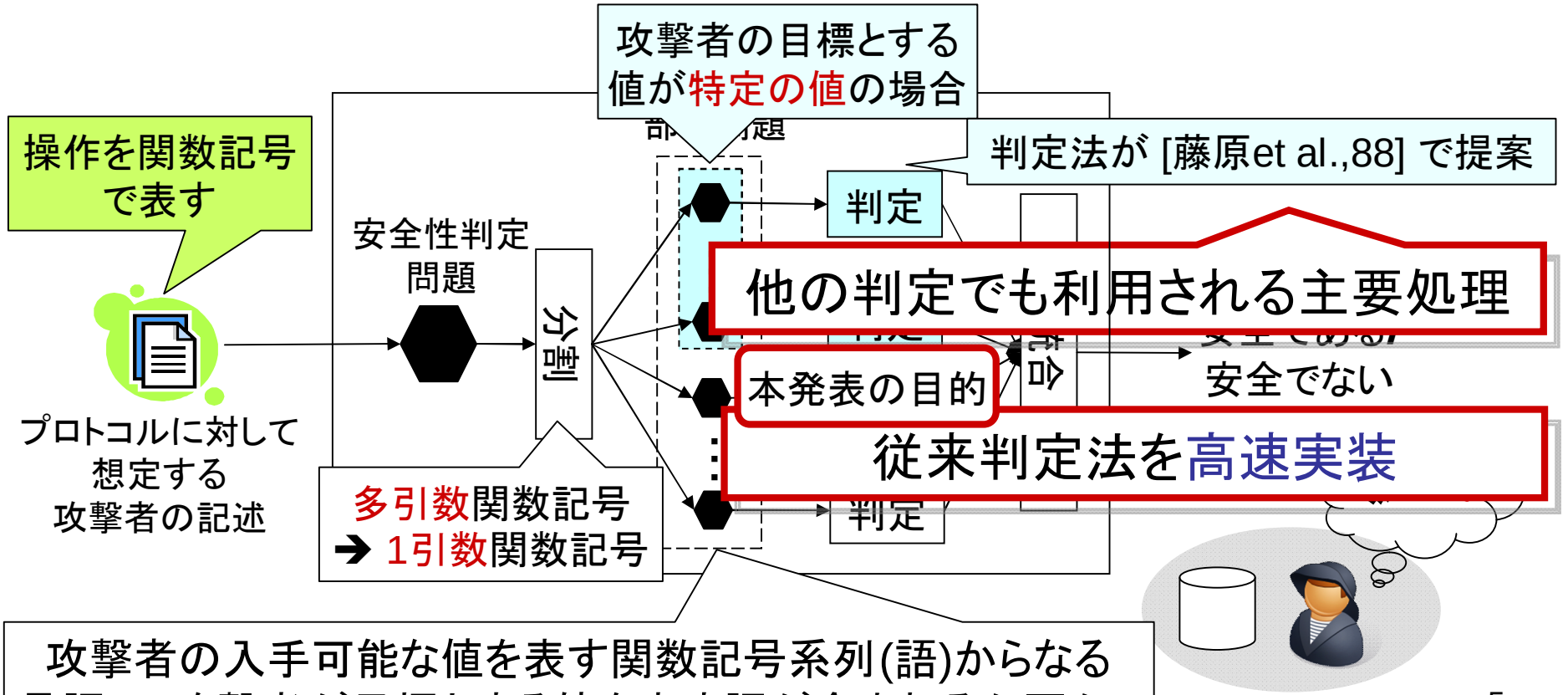
公理的安全性検証法

- 入力：プロトコルに対して想定する攻撃者の記述
- 出力：攻撃者に対して安全か否かの判定結果
  - 安全性判定問題を部分問題に分割して解く



公理的安全性検証法

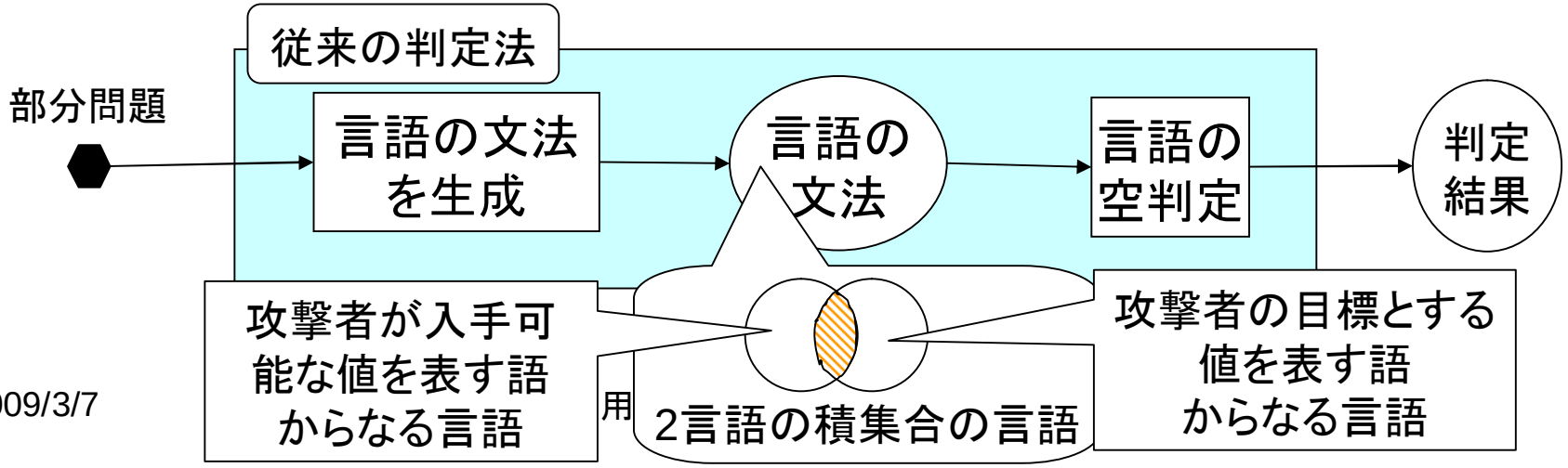
- 入力：プロトコルに対して想定する攻撃者の記述
- 出力：攻撃者に対して安全か否かの判定結果
  - 安全性判定問題を部分問題に分割して解く



本発表の目的･手段･結果

- 目的
  - [藤原et al.,88]の判定法を具体化し, 実装
- 手段
  - 言語の文法サイズを削減

  ⇒文法生成の計算量は増えるが, 空判定の計算量を大幅削減
- 結果 (Needham-Schroederプロトコルの部分問題)
  - 言語の文法サイズを約4%まで削減
  - 検証に要する時間は約0.16秒で, 十分現実的

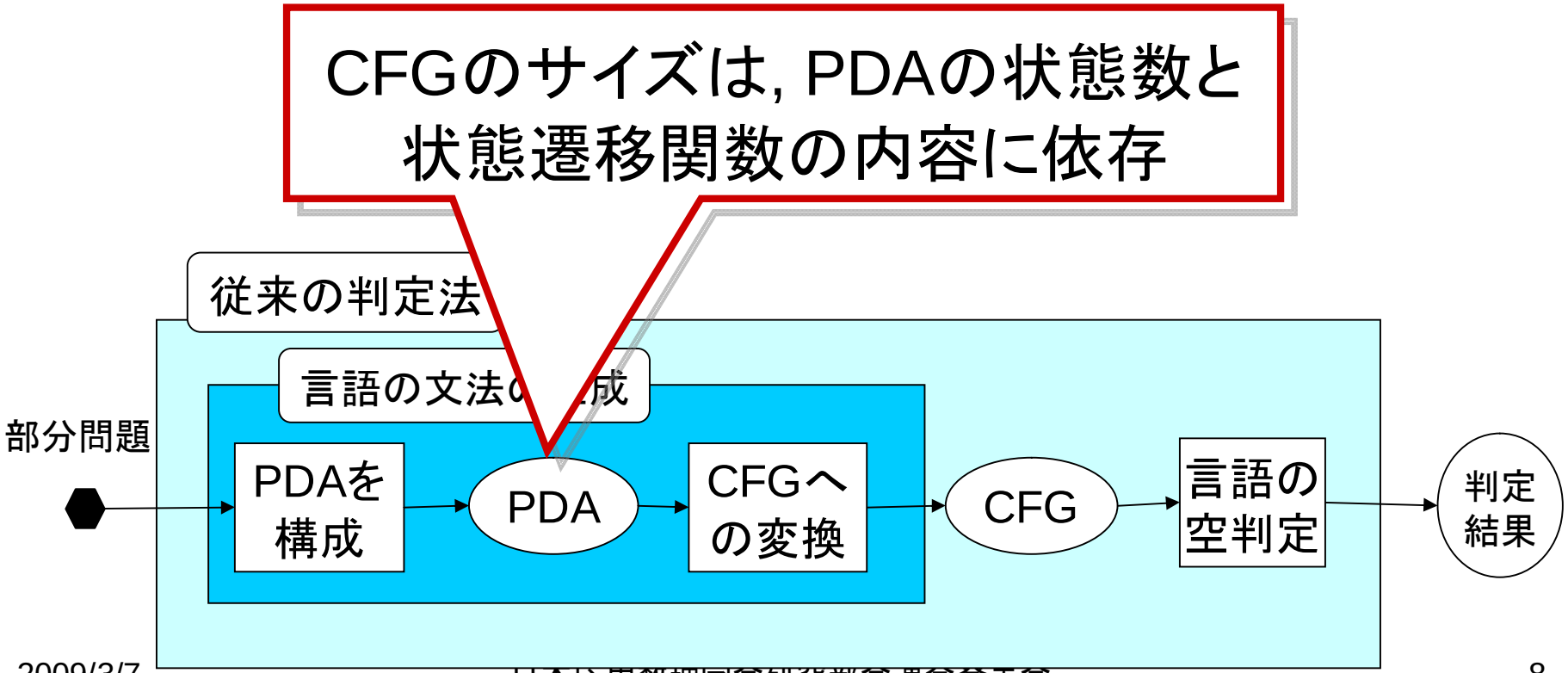


以降の発表内容

- 従来判定法
- アイデア
- 実装の概要と実験結果
- まとめと今後の課題

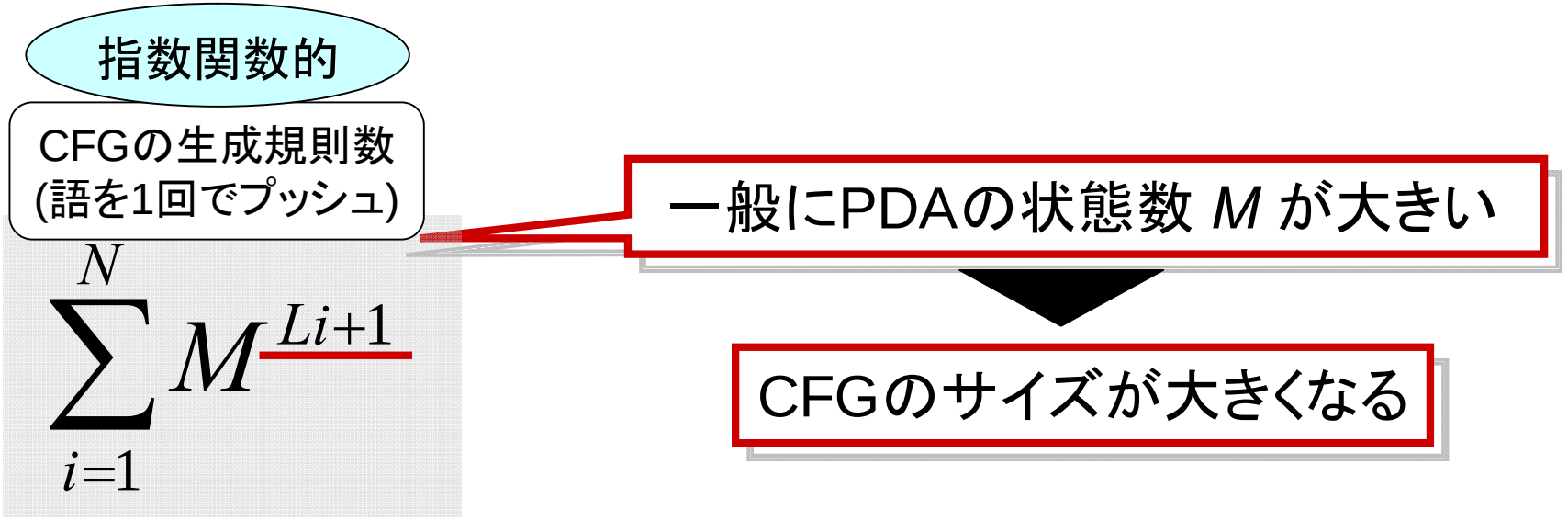
従来判定法

- 部分問題から生成する文法は文脈自由文法(CFG)
- まずプッシュダウンオートマトン(PDA)を構成し, CFGに変換



従来判定法で構成するPDAとCFG

- PDA: 部分問題で指定される複数の語とスタック内の語が一致するか否かを判定し, 語をプッシュ
- CFGへの変換: [Hopcroft-Ullman,79]のアルゴリズム
- CFG: 生成規則数はプッシュする語の長さに対し指数関数的に増加

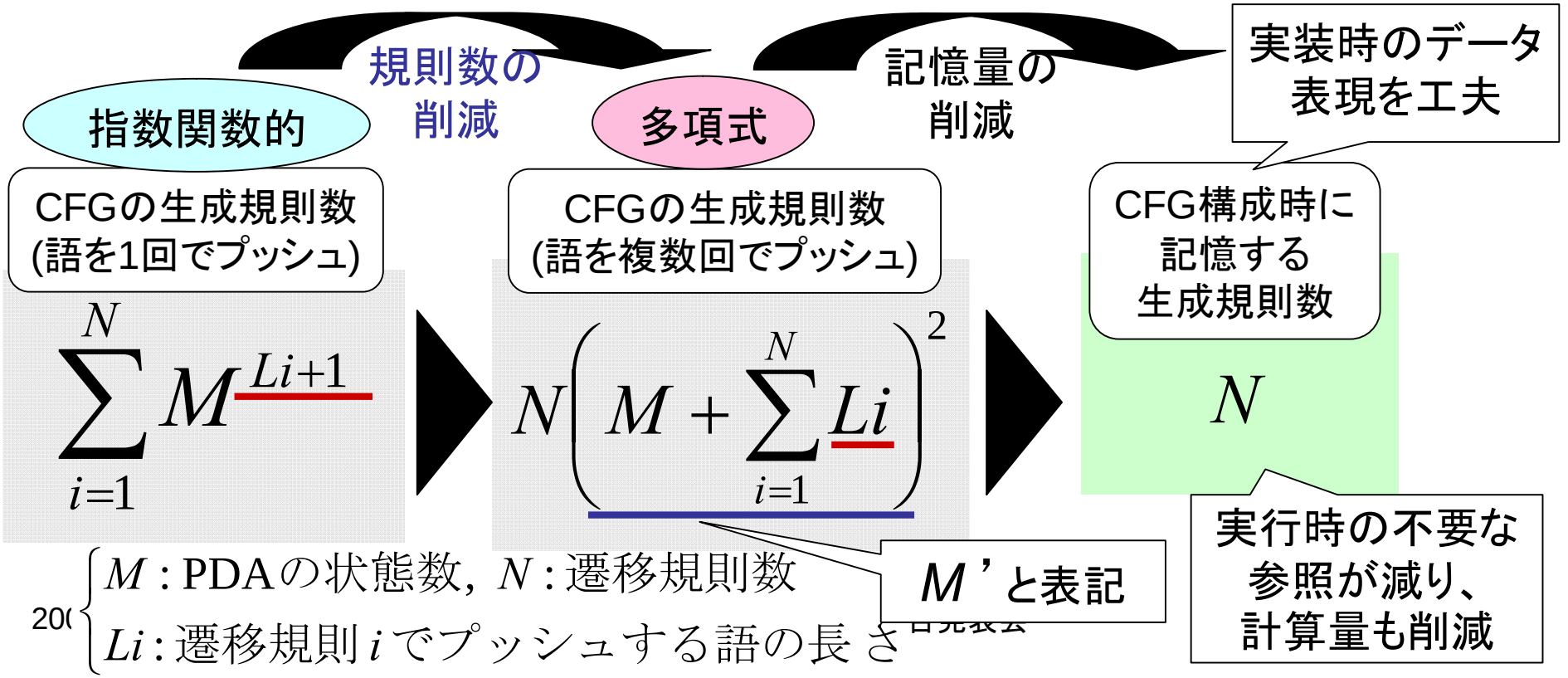


M : PDAの状態数, N : 遷移規則数
Li : 遷移規則 i でプッシュする語の長さ

CFG生成規則数の削減アイデア

- この問題におけるPDAの構成を工夫する
  - 語を1記号ずつ複数回に分けてプッシュするように定める

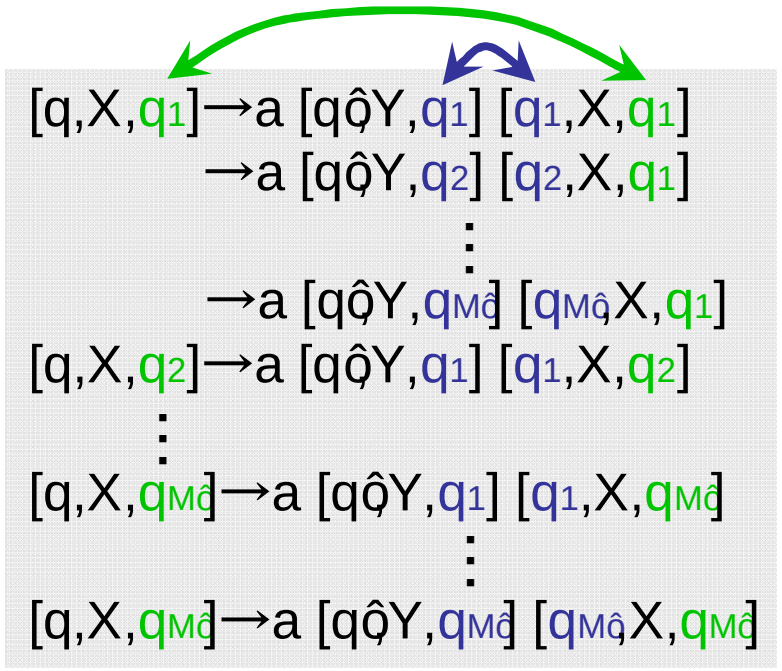
⇒ もとの語の長さに対してPDAの状態数は線形的に増えるが, CFGの生成規則数は多項式まで削減



CFGの生成規則

Å PDAの1つの遷移規則に対して, $(M')^2$個構成される

例：PDAの遷移規則 (q,a,X)→(qôY X)に対して構成されるCFGの生成規則
(状態q で入力記号がa,スタック先頭記号がXのとき,
状態qôに遷移しスタックに新たにYをプッシュ)



PDAの任意状態(M'個)の組み合わせ

$(M')^2$ 個の生成規則

(q1,é ,qMô：PDAの全状態.)

CFG生成規則の記憶量の削減アイデア

- CFGのデータ形式を工夫する
  - PDAの任意の状態を表す ô* ôを導入
- 空判定時に必要とする文法規則を適宜追加する
  - 不要な規則参照・記憶量がなくなり, 計算量・記憶量を削減

[q,X,q_1]→a [qôY,q_1] [q_1,X,q_1]
→a [qôY,q_2] [q_2,X,q_1]
⋮
→a [qôY,$q_{M'}$] [$q_{M'}$,X,q_1]
[q,X,q_2]→a [qôY,q_1] [q_1,X,q_2]
⋮
[q,X,$q_{M'}$]→a [qôY,q_1] [q_1,X,$q_{M'}$]
⋮
[q,X,$q_{M'}$]→a [qôY,$q_{M'}$] [$q_{M'}$,X,$q_{M'}$]

(q_1,é ,$q_{M'}$ô : PDAの全状態.)

最低限必要な部分のみを記憶

データ形式

[q,X, ＊]→a [qôY, ＊] [＊ ,X, ＊]

CFG構成時の生成規則の記憶数:

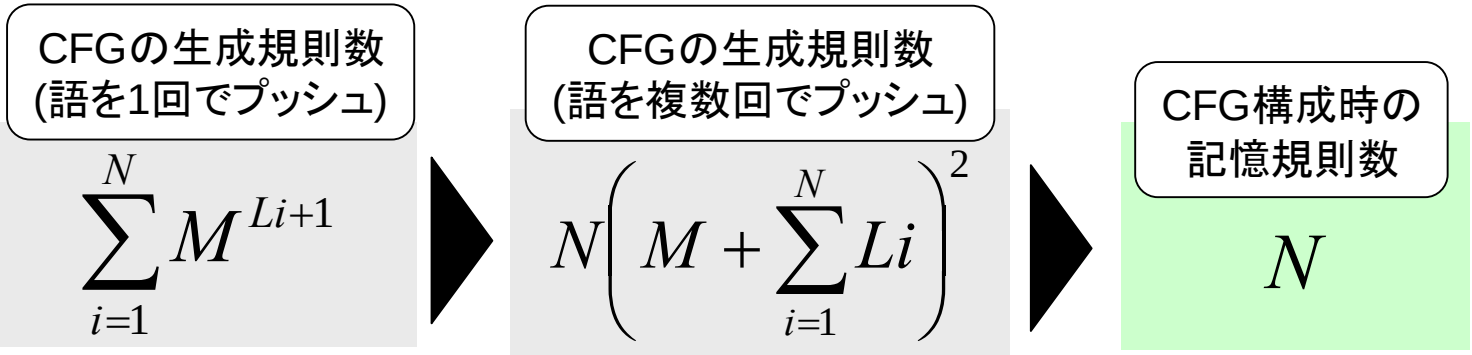
$$N\left(M'\right)^2 \Rightarrow N$$

実装概要と評価実験

- 実装言語と規模
  - 言語: C言語　規模: 2200行程度
- 実験目的
  - 2つの削減アイデアの効果の確認
  - 検証に要する時間の確認
- 実験環境(使用PCスペック)

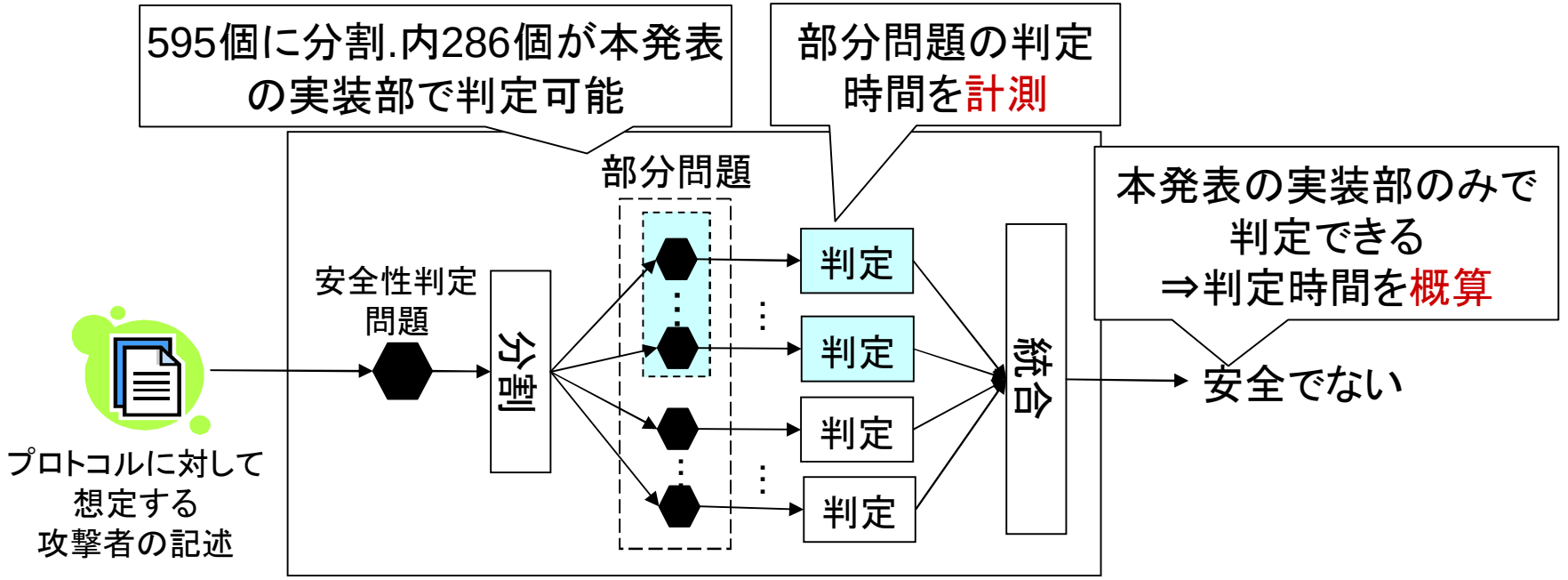
  OS: Windows XP

  CPU: Intel(R) Corei7-920 2.93GHz　メモリ容量: 3GB



検証対象

- 検証例としてよく用いられる安全でないプロトコル [Needham-Schroeder, 78]
- 分割した部分問題の一部の判定時間を計測
  - 結果から, 全体の安全性判定時間を概算



実験結果

- 2つの削減アイデアによる規則数・記憶量の削減
  - 規則数4%, 記憶量0.2%まで削減
- 検証に要した時間
  - 4個の部分問題の判定時間を計測
    - 1個平均0.16秒で判定
  - 全体の安全性判定時間を概算
    - 286個の部分問題判定： 0.16秒 × 286= 45. 8秒
  - cf. ProVerifでは0.07秒で検証

ProVerifに及ばないが,
十分現実的

まとめと今後の課題

- まとめ
  - 公理的安全性検証法の主要処理を具体化し, 実装
    - CFGのサイズの削減
  - 実験により, CFGのサイズと検証に要する時間を評価
- 今後の課題
  - 実装の改良による処理時間の更なる短縮
  - 公理的安全性検証法の未実装部分の高速実装
    - 繰り返し利用される部分の結果を一部再利用して検証時間を短縮

参考文献(1)

- [Abadi-Rogaway,00] M.Abadi and P.Rogaway, ``Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption),'' In Proc. IFIP Int. Conf. on Theoretical Computer Science(TCS 2000), LNCS vol.1872, pp.3-22, 2000.
- [Backes-Unruh,08]M. Backes and D. Unruh, ``Computational soundness of symbolic zero-knowledge proofs against active attackers,'' 2008. Online available http://www.infsec.cs.uni-sb.de/~unruh/publications/backes08computational.html.
- [Comon-Lundh-Cortier,08]H.Comon-Lundh and V.Cortier, ``Computational soundness of observational equivalence,''
  In Proc. 15th ACM conference on Computer and communications security(CCS'08), pp.109-118, 2008.
- [Hopcroft-Ullman,79] J.E.Hopcroft and J.D.Ullman, ``Introduction to Automata Theory, Languages, and Computation,'' Addison-Wesley, 1979.
- [Needham-Schroeder,78] R. Needham and M. Schroeder, ``Using Encryption for Authentication in Large Networks of Computers,'' Communications of the ACM, vol.21, no.12, pp.993-999, 1978.

参考文献(2)

- [藤原et al.,88]藤原 融, 壺井 久史, 高田 豊雄, 嵩 忠雄, ``受領証の偽造可能性の判定問題について,'' SCIS 1988, L2, 1988.
- [鈴木et al.,SCIS09]鈴木斎輝, 吉田真紀, 藤原融, ``相互認証の汎用的結合可能な安全性の解析のための形式的手法,'' SCIS 2009,4C2-4, 2009.
- [吉田-藤原,97] M.Yoshida and T. Fujiwara, ``A Sufficient Condition for Unforgeability Problem for the Receipt of Any Message to Be Decidabel,'' IEICE Tech. Rep. ISEC97-57, vol.97, pp.45-56, 1997.