研究課題別評価

1 研究課題名:

刺激応答型実時間システムの自動検証技術:安全性・信頼性技術の開発

2 研究者氏名:

大崎 人士

3 研究のねらい:

インターネットのような, 公衆ネットワーク回線を通じての通信においては, 暗号化による通信の秘密の保護が必要だが, そこでは破られにくい暗号法の技術と共に, 暗号化法を通信網の中で正しく生かして使う技術が必要である. 例えば, 正規の(想定する)データ受取人になりすまして, 暗号を解くための鍵を不正に入手されるようでは, いかに破られにくい暗号法を使用していても, データの秘匿性を保つことはできない. つまり, 鍵を不正に入手して暗号化されたデータを入手されるなどという攻撃を避けるための技術が要請される. 通信手順の安全性を確保することは, 解読が困難な暗号化法を考案する技術とは独立のものである. なぜなら, 秘密のデータを暗号化して受信者に伝えるとしても, 暗号法には復号法が必ずあり(さもないと受信者はデータを読み取れない), 復号化の方法も受信者に伝える必要がある. このときに, 暗号化にもちいるトリック(多くの場合は, 鍵)を横取りされないような通信手順が必要となる. ここで問題となるのは, 「なりすまし」などの悪意の第三者からの攻撃が決して成功しないことをどのようにして確かめるのかである.

本研究では, 情報科学における基礎技術を応用して, 情報システムの安全性を検証するための技術について研究する. 書換系(かきかえけい)およびツリーオートマトンの理論による数理的基礎を発展させて, リアクティブシステムの安全性を自動的に検証するための技術を開発し, 実際に, 自動検証ソフトウエア ACTAS を作成し, ソフトウエアの性能評価をもとにアルゴリズムの改良, 実用化の模索を行うことが具体的な目標である. さらに, 具体的な研究のプロセスと経て, 一連の研究活動がスパイラル状に展開し, 新たな研究シーズの発掘が行えたのであれば, 理想的結果が得られたと考える.

4 研究成果:

本研究の第一の目的は, 「自動化の利点を損なわずに, 柔軟な表現力をそなえた普遍性のあるモデル化法とその自動検査技法を開発すること」である. 暗号プロトコルの例に対しては, より広いクラスの暗号通信プロトコルを自然な表現によりモデル化し, 安全性を自動的に検証する, ことが具体例となる. しかし, 形式言語理論の世界では一般的に, 「より強力な表現力を求めると, 自動化の利点は失われる」と言われており, 本研究の理論的基礎であるツリーオートマトンについても, この考察が当てはまると推察する. なぜなら, 従来のツリーオートマトンでは, 自動検証に適した演算を構成的に定義することや, 各種の決定判定問題を解消することはできるが, その表現力は必ずしも十分であるとは言えない. 例えば, $x = y$ のような, 線形方程式の(自然数上の)解空間を表現することは困難である. また, 交換則($x + y = y + x$)や結合則($(x + y) + z = x + (y + z)$)を仮定すると, 受理言語の閉包性

($t \in L$ かつ $t = s$ ならば, $s \in L$)が失われる. そこで本研究では, 従来のツリーオートマトンを拡張した新たな枠組みである等式付ツリーオートマトンを理論的背景にして,『表現力についての研究』と『自動計算についての研究』を行った. 前者の研究では, この新しい数理的なモデルについての閉包演算および決定問題の解決をした. 後者の研究では, 等式付ツリーオートマトンを基礎として, リアクティブシステムのための自動検証方法を考案し, 現実的な時間で安全性を検証するためのアルゴリズムの開発や, 近似計算アルゴリズムの開発などの研究を行った. 以降の節では, 本研究プロジェクトで得られた研究成果の概要について述べる.

4. 1 表現についての研究

先ず, 2001 年に, 世界にさきがけて「等式付ツリーオートマトン」という理論概念を導出した. 等式付ツリーオートマトンは, 交換則や結合則を仮定しても受理言語の閉包性を失うことはない. しかも従来のツリーオートマトンのように:

- 空(くう)判定問題が決定可能であること
- 受理言語上の集合演算について閉じていること

が多くの場合で成り立つだろうという予想があった. 本研究では, 形式表現としての性質を調べることにより, 等式付ツリーオートマトンの特性を明らかにすることを目指した.

本研究中に得られた研究成果の一覧を次頁の図1と図2にまとめる. (1)交換則・結合則を仮定するか, 結合則のみを仮定するか, (2)正則な遷移規則のみをもつと仮定するか, 正則な遷移規則に加えて単調な(monotone)イプシロン遷移規則をもつと仮定するか, の場合分けにより, 生じる表現力に違いを確かめた. 理論概念の導出以来の未解決の問題とされていた, 交換則結合則付き単調ツリーオートマトン(monotone AC-tree automata)についての以下の定理を導けたことが, 本テーマでの最大の研究成果であった.

交換則結合則付単調ツリーオートマトンの受理言語のクラスは,

1. 交換則結合則付正規ツリーオートマトンの受理言語のクラスを, 真に包含している,
2. 補集合の演算について閉じていない,
3. 包含関係(⊆)の判定問題が決定不可能である.

いっぽう, 等式付ツリーオートマトンによる自動検証の可能性を理論的に裏付けるためには, 空判定問題が決定可能になるための十分条件を調べることが, 一つの重要なカギとなる. アルゴリズム実装のためには, 空判定の計算量を測定することも必要である. 空判定が, 計算量的に実装がむずかしい場合であっても, 近似判定法があるかどうかを検討することにより, 多くの具体的な検証例を手がけることも可能になる. 本研究では, 上述(1)と(2)の場合分けのすべて対して, 空判定についての考察を行った. そしてこの考察をもとに, 結合則と交換則をうまく扱うことのできなかった従来の理論では秘密保持性の自動検証が難しいとされていた「Diffie-Hellman の鍵交換プロトコル」や「Shamir のスリーパス・プロトコル」を使う暗号通信手順が, 等式付ツリーオートマトンによる自動検証の対象に含められることを示すことができた.

Closure under Boolean operations

	regular	AC-regular	AC-monotone
closed under $\cup$	✓	✓	✓
closed under $\cap$	✓	✓	✓
closed under $(\ )^c$	✓	✓	×

regular TA $<$ regular AC-TA $<$ monotone AC-TA

	regular	A-regular	A-monotone
closed under $\cup$	✓	✓	✓
closed under $\cap$	✓	×	✓
closed under $(\ )^c$	✓	×	✓

regular TA $<$ regular A-TA $<$ monotone A-TA

図1 ブール閉包性とツリー言語階層 §

Decidability results

	regular	AC-regular	AC-monotone
$t \in \mathcal{L}(\mathcal{A}/\mathrm{AC})$?	✓ (LOGCFL)	✓ (NP-complete)	✓ (PSPACE-compl.)
$\mathcal{L}(\mathcal{A}/\mathrm{AC}) = \varnothing$?	✓	✓	✓
$\mathcal{L}(\mathcal{A}/\mathrm{AC}) \subseteq \mathcal{L}(\mathcal{B}/\mathrm{AC})$?	✓	✓	×

	regular	A-regular	A-monotone
$t \in \mathcal{L}(\mathcal{A}/\mathrm{A})$?	✓ (LOGCFL)	✓ (P-time)	✓ (PSPACE-compl.)
$\mathcal{L}(\mathcal{A}/\mathrm{A}) = \varnothing$?	✓	✓	×
$\mathcal{L}(\mathcal{A}/\mathrm{A}) \subseteq \mathcal{L}(\mathcal{B}/\mathrm{A})$?	✓	×	×

図2 決定可能性と計算量 §

§ PRESTO 実施中に得られた成果は**青色**で示します.

理論的な研究成果のさらに詳しい解説は省略するが，個々の技術的な研究成果については，すでに研究論文としてまとめて，その多くは国際研究集会にて発表している．また近年，等式付ツリーオートマトンに関する研究が，世界的な広がりをみせており，最新の研究成果はおもに以下の国際研究集会などで報告されている：

- International Conference on Rewriting Techniques and Applications（RTA）
- International Conference on Logic for Programming, Artificial Intelligence and Reasoning（LPAR）
- International Conferences on Foundations of Software Sciences and Computer Structures（FOSSACS）

いずれの会議も，会議録が Springer-Verlag 社の LNCS シリーズとして出版されている．

4．2　自動計算についての研究

等式付ツリーオートマトンの理論を生かしたシステム開発をすることにより，検証の自動化についての検討を行った．本研究で開発したのは，結合則交換則付ツリーオートマトンを入力として，各種の演算や判定問題の解消を行うためのシステムである．オートマトンの基本的な演算である，共通集合や和集合（∪，∩），所属判定や空判定（∈，≠∅）の機能を備えていることから，ACTAS（Associative Commutative Tree Automata Simulator）と命名した．ACTAS では，結合則交換則付ツリーオートマトン A と結合則交換則書換系 R を与えて，A の受理言語の R による書換閉包を受理する結合則交換則付ツリーオートマトンを求めることができる．図 3 は，実際に ACTAS で書換閉包を計算したときに表示されるインターフェース画面である．

書換系とは，書換規則の有限集合で，書換規則は項の順序対で，$l \to r$ と書く．項 t と書換規則 $l \to r$ が与えられたときに，t の中に l のパターンにマッチする部分項が存在したとき，その部分項は r に置き換えられ，この関係を書換関係と呼ぶ．項 t から項 t' に項書換え系 R に含まれる規則で書換えられるとき，$t \to_R t'$ と書く．また，t から 0 回以上の書換えで t' に到達するとき，$t \to_R^* t$ と書く．結合則交換則付ツリーオートマトンは，結合則交換則付書換系の特殊なクラスとみなすことができることから，書換系とツリーオートマトンは，理論的な親和性がよく，書換系の研究成果をツリーオートマトンへ応用することも容易である．実際に，ツリーオートマトンの各種演算や問題解消系を利用して，書換閉包を計算することができた．ツリーオートマトン A の受理言語を L と表すとき，L の R による書換え閉包というのは，L に含まれる項から R によって書換えて得られる項全てからなる集合 $\{ t \mid s \to_R^* t, s \in L \}$ である．書換閉包の計算手続きは，一般に停止性を保証することはできないため，ACTAS では結合則交換則付ツリーオートマトン A と結合則交換則書換系 R を与えられたときに，(1) A の受理言語の R による書換閉包，(2) A の受理言語の R による書換閉包を含む集合（強近似書換閉包），(3) A の受理言語の R による書換閉包に含まれる集合（弱近似書換閉包）のいずれを計算するのか，を選択可能にした．特に，弱近似を行うアルゴリズムでは，いくつかのパラメータを指定することで，現実的な時間で計算の実行を終了させることが可能である．書換閉包の計算と同様に，空判定も弱近似判定や強近似判定が適用可能であるため，これらの機能を組み合わせて，モデル検査を実現した．暗号プロトコルの安全性自動検証への適用に関する考察は，論文 2（国際研究集会）にまとめた．現在は，研究交流のあるイリノイ大学計算機科学科研究者らと，検証用計算ライブラリを開発

し，ACTAS への統合を計画している．詳しくは，http://texas.cs.uiuc.edu/ceta/ を参照されたい．

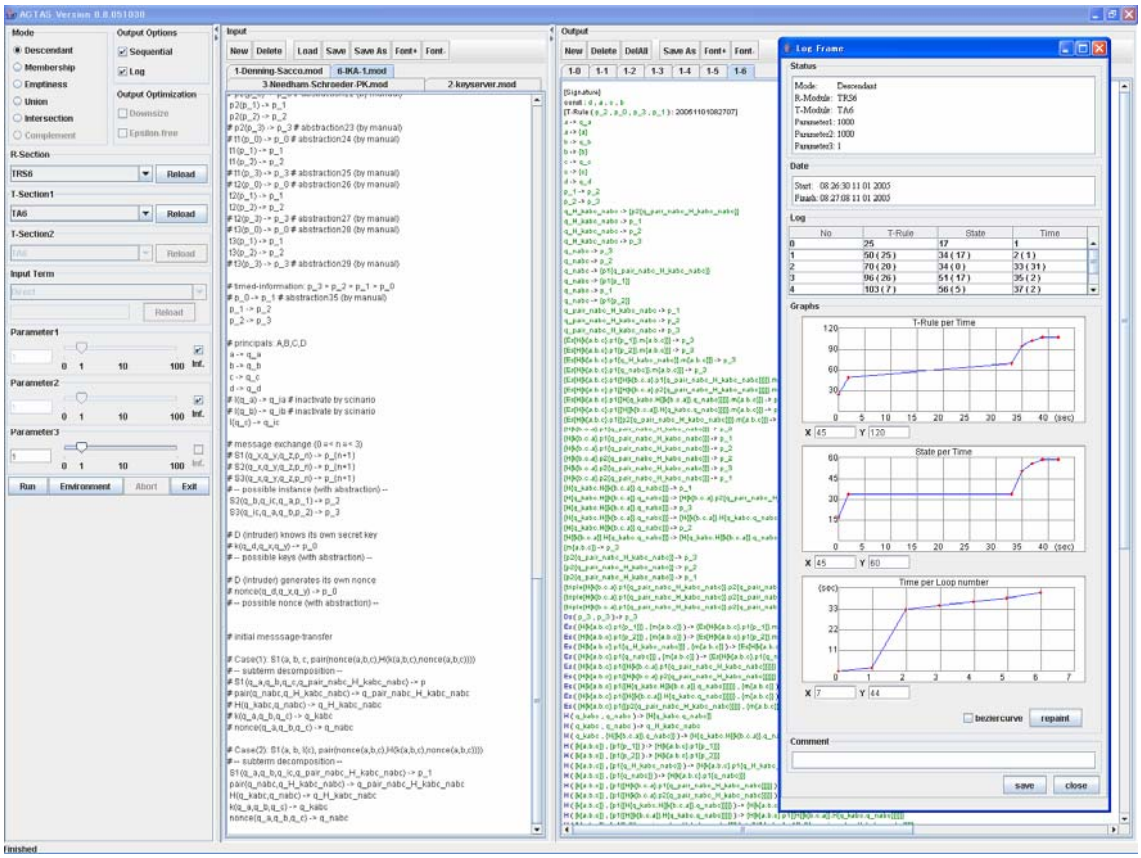

図3　ACTAS インターフェース

5　自己評価：

本研究中に開発した暗号通信手順の安全性自動検証法は，リアクティブシステムと呼ばれる「動作中に外界からの多様な刺激を受けて，その刺激と内部状態から応答を決定する」装置全般に適用可能である．線形等式による動作制約をもつシステムなどをモデル化することができ，近似アルゴリズムを用いれば，ある程度の規模のシステムであっても自動検証可能である．また，等式付ツリーオートマトンに関する最近の研究では，本研究者のアイデアとしてだけにとどまらず，現在では，構造化文書の検証，型推論エンジンの設計，プログラムの整合性検査など，様々な方面に活用する試みがなされている．本研究の成果は，情報科学の問題に端を発しながら，さらに今後は一般の情報システムの安全性や整合性検査へ適用することが検討されことになると考える．

リアクティブシステムの代表的な例である，銀行のオンラインシステムや携帯電話等の通信システムなどは，いちど稼働させてしまうと容易に停止させることが出来ない．安全で安定した情報システムの整備が社会的な急務となっている現在，稼働前に十分な安全性の検証をおこなうことへの社会的ニーズに応えることを，今後の研究目標としたい．また，大規模システムやマスプロダクトに対しては，検証で発見された誤りにより設計変更を余儀なくされた場合に，損失を極力小さく抑える必要があるため，

設計の初期段階で検証できなければならないという要求もあるため，業種を問わず適用可能な検証技術としていくための技術汎用化も今後の研究課題である.

6 研究総括の見解:

安心性や安全性は，今日の情報システムにとって最も重要な要件であるが，大崎氏の研究は情報科学の基礎技術である形式仕様化や形式検証技術によりこの問題の解決を図ろうとするものである. 大崎氏は，従来のツリーオートマトンを拡張した新しい等式つきツリーオートマトンの概念を独自に考案し，その理論展開を図ると同時に，それにもとづいて形式検証のためのツール群を構築し，リアクティブシステムのための自動検証システムを開発した. 等式つきツリーオートマトンは国際的にも高く評価され，新しい研究分野として認識されている. 国際的共同研究を活発に行い，成果を着実にあげると同時に，著名な国際会議での論文発表やチェアー，プログラム委員などを務め，国際的評価も高い. 非常に高く評価できる研究である.

7 主な論文等:

論 文(国際研究集会)

1. 大崎人士，Jean-Marc Talbot，Sophie Tison，Yves Roos:“Monotone AC-Tree Automata”. In proceedings of 12th International Conference on Logic for Programming, Artificial Intelligence and Reasoning(LPAR'05)，Montego Bay(Jamaica). Lecture Notes in Computer Science 3855 巻，337-351 頁，Springer-Verlag，2005.
2. 大崎人士，高井利憲:“ACTAS: A System Design for Associative and Commutative Tree Automata Theory”. In proceedings of 5th International Workshop on Rule-Based Programming(RULE'04)，Electronic Notes in Theoretical Computer Science，124 巻，97-111 頁，Elsevier Science，2005 .
3. 大崎人士，関浩之，高井利憲:“Recognizing Boolean Closed A-Tree Languages with Membership Conditional Rewriting Mechanism”. In proceedings of 14th International Conference on Rewriting Techniques and Applications (RTA'03)，Lecture Notes in Computer Science，2706 巻，483-498 頁，Springer-Verlag，2003.
4. 大崎人士，高井利憲:“Equational Tree Automata: Towards Automated Verification of Network Protocols”. 京都大学数理解析研究所講究録，1318 号，48-52 頁，京都大学，2003.
5. 大崎人士，高井利憲:“Decidability and Closure Properties of Equational Tree Languages”. In proceedings of 13th International Conference on Rewriting Techniques and Applications (RTA'02)，Lecture Notes in Computer Science，2378 巻，114-128 頁，Springer-Verlag，2002.
6. Joe Hendrix，大崎人士，Mahesh Viswanathan:“Propositional Tree Automata” . 論文草稿，2006.(国際会議投稿中)

論 文(その他)

7. 大崎人士，Joe Hendrix，José Meseguer:“Sufficient Completeness Checking with Propositional Tree Automata”.

産業技術総合研究所研究速報 AIST-PS-2005-013, 産業技術総合研究所, 2005.

システム紹介

8. 大崎人士, 高井利憲:“ACTAS: Associative and Commutative Tree Automata Simulator”. 4th International Conference on Application of Concurrency to System Design（ACSD’04), 2004.

研究交流

1. Université des Sciences et Technologies de Lille（リール・フランス;2005 年 5 月 21 日－6 月 15 日）.
2. École Normale Supérieure de Cachan（パリ・フランス;2004 年 8 月 28 日－9 月 30 日）.
3. University of Illinois at Urbana-Champaign（アーバナ・イリノイ州;2004 年 1 月 10 日－3 月 31 日）.
4. 京都大学数理解析研究所（京都;2004 年 7 月 26 日－7 月 30 日）.

外部委員

1. Program Committee Member:18th International Workshop on Unification（UNIF’04）, Cork（Ireland）,（2004 年 7 月開催）.
2. Program Committee Member:16th International Conference on Rewriting Techniques and Applications（RTA’05）, 奈良市,（2005 年 4 月開催）.
3. Organizing Chair:16th International Conference on Rewriting Techniques and Applications（RTA’05）, 奈良市,（2005 年 4 月開催）.
4. Conference Co-Chair:Federated Conference on Rewriting, Deduction and Programming（RDP’05）, 奈良市,（2005 年 4 月開催）.

など.