■1 群（信号・システム）- 3 編（暗号理論）

10 章 数理的技法による安全性証明

（執筆者：塚田恭章）［2008 年 11 月 受領］

■概要■

計算機プログラムや数学の証明にはバグ（bug）がしばしば混入する．特にプログラムや証明が複雑・大規模になるとバグの混入は避けられない．数理的技法（formal method，形式手法とも訳される）は，数理論理学の分野で蓄積された技術を用いてプログラムや証明の記述・解析・検証を厳密に（フォーマルに）行うことにより，バグの混入を著しく減少させる高信頼化手法の総称である．プログラムや証明のフォーマルな記述には，1 階述語論理（first-order logic）・様相論理（modal logic）・プロセス計算（process calculus）やそれらを拡張した様々な論理体系・計算系が目的や用途に応じて使用される．また，定理証明器（theorem prover）やモデル検査器（model checker）などのツールを活用することにより，プログラムや証明の解析・検証の主要部分を機械化・自動化することもできる．

数理的技法は，そのコストに見合うだけの高い信頼性が求められる対象に適用されることが多い．暗号や暗号プロトコルの安全性証明は，数理的技法の最も効果的な適用対象の一つである．近年，暗号や暗号プロトコルはますます複雑度を増しているため，安全性を厳密かつ機械的に保証する可能性を秘めた数理的技法への期待は更に高まっている．

1980 年代以降，暗号プロトコルの安全性を数理的技法によって証明するための様々な理論的枠組み（Dolev-Yao モデル，BAN 論理，ストランド空間，帰納的手法，spi 計算など）が提案され，有用なツールが多数開発された．数理的技法によるこれらの研究は，記号的（symbolic）アプローチとも呼ばれ，根底にある暗号は決して破られないという仮定のもとで，通信路に流れるメッセージを記号に抽象化してプロトコルの解析を行っている．

一方，暗号理論においては，根底にある暗号のぜい弱性も考慮に入れ，確率的多項式時間チューリング（Turing）機械の還元を中心とした計算論的（computational）アプローチにより安全性を解析するのが標準的である．プロトコルの実装に即した具体的な攻撃を扱えるなど，現実的な解析を行うには必須のアプローチであるが，その解析は一般に煩雑となりしばしばバグの混入を伴う．そこで，数理的技法による記号的アプローチと，現実的な解析に必須の計算論的アプローチとの関係を明らかにし，両者の長所を融合する試みに期待が寄せられている．

二つのアプローチを関連づけることは長らく課題であったが，2000 年に記号的安全性証明の計算論的健全性（数理的技法によって証明された記号的な安全性が，計算論的な安全性も保証する性質）に関する初の結果がアバディ（Abadi）とロガウェイ（Rogaway）によって示された．それ以降，新しい計算論的証明手法（汎用的結合可能性，ゲーム変換による証明手法など）の進展ともあいまって，数理的技法による安全性証明の研究が活性化している．

【本章の構成】

本章では暗号や暗号プロトコルの安全性を証明するための数理的技法について述べる．古典的な記号的アプローチ（10-1 節）と，近年研究が活性化している記号的／計算論的アプローチの融合（10-2 節）について，代表的結果を中心に説明する．

■1 群 - 3 編 - 10 章

10-1 記号的アプローチ

（執筆者：塚田恭章）[2008 年 11 月 受領]

暗号プロトコルの安全性を数理的技法によって証明する古典的アプローチでは，根底にある暗号は絶対に破られないという仮定のもとで，通信路に流れるメッセージを記号に抽象化して暗号プロトコルの解析を行う．これを記号的（symbolic）アプローチと呼ぶ．記号的アプローチの代表的な概念及び手法について説明する．

10-1-1 Dolev-Yao モデル

暗号プロトコルの実行及びそれに対する攻撃者の振る舞いを記号的にモデル化したものである．ドレブ（Dolev）とヤオ（Yao）によって定義され[12]，その後の記号的アプローチ全般の基礎となった．Dolev-Yao モデルにおいては，通信路に流れるメッセージは，メッセージ代数と呼ばれる理想化された代数構造上の項（term）として定式化される．そのうえで，攻撃者は，「暗号化されたメッセージを復号できるのは鍵を所有しているとき，またそのときに限る」などの基本的な制約のもとで，通信路に流れるすべてのメッセージに対し削除・複製・偽造・再送などの操作を行える能力があるものとして定式化された．

10-1-2 BAN 論理

バロウズ（Burrows），アバディ（Abadi），ニーダム（Needham）によって考案された BAN 論理[7]は，記号的アプローチによって暗号プロトコルの安全性を系統的に解析しようとした最初の試みの一つである．プロトコル参加者の信念（belief）に関する推論をフォーマルに行う論理体系であり，認証（authentication）に特化した安全性解析を行うように設計されている．典型的な推論規則として

$$\frac{A \models (A \overset{K}{\longleftrightarrow} B) \quad A \triangleleft \{X\}_K}{A \models (B \mid\sim X)}$$

があり，「鍵 K は参加者 A と参加者 B のみが共有する鍵であると A が信じており，かつ，X の K による暗号化を含むメッセージを A が受信したならば，B が以前に X を含むメッセージを送信したと A は信じている」と読む．各参加者の初期知識を表す公理とこれらの推論規則を適用し，例えば「K は A と B のみが共有する鍵であると B が信じていると A も信じている」を表す $A \models B \models (A \overset{K}{\longleftrightarrow} B)$ など，認証に関する論理式が導出可能かどうかを解析する．Otway-Rees，Kerberos，Yahalom，CCITT（現 ITU-T）X.509 など多数のプロトコルの解析に用いられ，記述の冗長性やバグの解消に効果を上げた．また GNY 論理や SvO 論理などの後継論理にも拡張された．ただし，BAN 論理は全参加者が正直（honest）であるという仮定を置くなど保証する安全性に限界もある．例えば，その後ロウ（Lowe）によって発見されたニーダム・シュレーダー（Needham-Schroeder）公開鍵暗号プロトコル[16]に対する中間者攻撃（man-in-the-middle attack）[14]は，BAN 論理では検出することはできなかった．

10-1-3 ストランド空間

ストランド空間（strand space）はグットマン（Guttman）らによって考案された暗号プロト

コル解析手法である[13]．ストランド（strand）とは，個々のプロトコル参加者の実行トレースを指す．例えば，Needham-Schroeder 公開鍵暗号プロトコル[16]のイニシエータ（initiator）A 及びレスポンダ（responder）B のストランドはそれぞれ $\langle +\{N_A, A\}_{K_B}, -\{N_A, N_B\}_{K_A}, +\{N_B\}_{K_B}\rangle$ 及び $\langle -\{N_A, A\}_{K_B}, +\{N_A, N_B\}_{K_A}, -\{N_B\}_{K_B}\rangle$ と記される．ここで，+ 及び – はそれぞれメッセージの送信及び受信を表す．因果関係について閉じたストランドの集合をバンドル（bundle）という．**図 10･1** は Needham-Schroeder 公開鍵暗号プロトコルへの中間者攻撃を表す一つのバンドルである．個々のストランド内のアクション間因果関係を表す $\Longrightarrow$ と，ストランド間のメッセージ送受信に伴う因果関係を表す $\longrightarrow$ という 2 種類の有向辺によって，各バンドルは半順序集合とみなすことができる．解析にあたっては，ある特定のストランドに着目し，それを含み得るすべてのバンドルに対し安全性に相当する性質が成り立つかどうかを調べる．このとき，各バンドルは有限かつ整礎（well-founded）な半順序集合であるため，帰納法による証明が適用可能である．ストランド空間は数学的に厳密な理論であると同時に我々の直観に合致した自然なアプローチであるため，様々なプロトロル解析に用いられた．モデル検査器と定理証明器を組み合わせたツール Athena も開発されている．

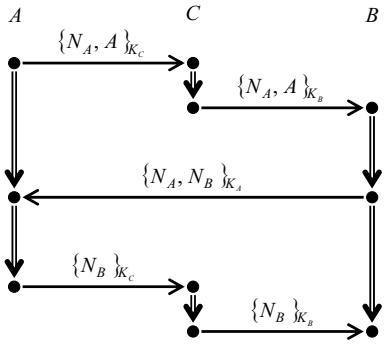

図 10･1　Needham-Schroeder **公開鍵暗号プロトコルに対する中間者攻撃**

10-1-4 帰納的手法

ポールソン（Paulson）は，自身が開発した証明支援系 Isabelle を利用し帰納的手法（inductive approach）によってプロトコル検証の機械化・自動化を目指した[17]．Dolev-Yao モデルにおけるプロトコル実行トレースの全体を帰納的に定義し，秘匿性（secrecy）や認証などの安全性を実行トレース上の性質として定式化し，Isabelle を用いて帰納法によって証明するアプローチをとる．TLS（Transport Layer Security）や SET（Secure Electronic Transaction）プロトコルの検証などに適用された．

10-1-5 spi 計算

アバディ（Abadi）とゴードン（Gordon）の spi 計算（spi-calculus）[3]は，代表的な並行プ

ロセス計算の一つであるミルナー（Milner）の π 計算（π-calculus）を拡張し，暗号プリミティブが扱えるようにした計算系である．並行プロセス計算の理論的成果，特にプロセス間の観測等価性（observational equivalence）の理論を，暗号プロトコルの解析に応用する．例えば，プロトコル P があるデータを秘匿するとは，任意の M 及び M' に対し，データが M の場合のプロトコル実行インスタンス $P[M]$ と M' の場合のインスタンス $P[M']$ が観測等価であることと定義される．$P[M]$ と $P[M']$ が観測等価であるとは，攻撃者を表す任意の文脈 $C[\ ]$ に対して，$C[P[M]]$ と $C[P[M']]$ が同じように振る舞うことを意味する．観測等価性の証明手法として，双模倣（bisimulation）を利用する方法が提案されている．

■1 群 - 3 編 - 10 章

10-2 記号的／計算論的アプローチの融合

（執筆者：塚田恭章）[2008 年 11 月 受領]

従来より暗号理論においては，確率的多項式時間チューリング（Turing）機械の枠組みを用いて暗号プロトコルの解析を行う計算論的（computational）アプローチが標準的であった．本節では，近年著しい進展を見せている記号的／計算論的アプローチの融合について説明する[1, 2]．融合の方法は大きく二つに分類される．一つは，記号的な推論に計算論的解釈を与えることにより，煩雑になりやすい計算論的な解析を機械化も可能な記号的な解析に帰着させようとするものである（10-2-1 節，10-2-2 節）．もう一つは，より直接的に，計算論的な解析を論理体系・計算系の中で定式化したうえで記号的アプローチに基づく自動検証技術を導入するものである（10-2-3 節）．

10-2-1 計算論的健全性

計算論的な解析を記号的な解析に帰着させる最初の試みはアバディ（Abadi）とロガウェイ（Rogaway）による[4]．彼らは，完全な共通鍵暗号方式を前提として，Dolev-Yao モデルにおけるメッセージ項の間に記号的な等価関係を定義した．そして，二つのメッセージ項が等価であるとき，そのメッセージ項によって実際に生成されるビット列の確率分布が計算論的に識別不能（indistinguishable）であることを示した．これを，メッセージ項の記号的等価関係は計算論的健全性（computational soundness）をもつという．後に，ミッチャンチオ（Micciancio）とワリンスキ（Warinschi）はこの逆（完全性）も成り立つことを示した．

更に，Micciancio と Warinschi は，Abadi と Rogaway の結果を発展させ，計算論的健全性が能動的攻撃者の存在を仮定しても成立することを示した[15]．すなわち，IND-CCA 安全な公開鍵暗号の使用を前提とすれば，記号的な攻撃のトレースが存在しないとき，対応する計算論的なトレースも（無視できるほど小さい確率を除いて）存在しないことを示した．この定理において，計算論的なトレースは（無視できる確率を除いて）記号的なトレースに対応するという事実が本質的である．これを通常マッピング補題（mapping lemma）と呼ぶ．

10-2-2 結合可能性への記号的アプローチ

大きなプロトコルを見通しよく設計し，安全性の証明を簡略化するためには，プロトコル設計をモジュラー化することが望ましい．汎用的結合可能性（universal composability）はこれを可能にするフレームワークであり，理想機能（ideal functionality）を部品とする大きなプロトコルがあったとき，理想機能を実現（realize）する実プロトコルでその理想機能を置き換えても，全体のプロトコルの理想機能が保存されることが保証される．

汎用的結合可能性への記号的アプローチとして，記号的な解析によって理想機能の実現可能性を導く研究，すなわち汎用的結合可能性に対する計算論的健全性の研究が行われている．カネッティ（Canetti）とハーゾグ（Herzog）は，鍵交換プロトコルを例として，記号的な解析から鍵交換の理想機能の実現可能性が導かれることを，マッピング補題を通じて証明した[9]．また，バックス（Backes）らは，汎用的結合可能性によく似たモデルのうえで，Dolev-Yao のモデルに相当する理想機能（理想的暗号ライブラリ）を考え，これが実際の暗号ライブラリによって実現できることを示した．これにより，汎用的結合可能性の枠組みでも Dolev-Yao

モデル（に相当する理想的暗号ライブラリ）を用いてプロトコルの安全性を保証できることが明らかになった[5]．一方，ミッチェル（Mitchell）らは，部品プロトコルの性質からより大きな全体プロトコルの性質を導出するための枠組みとしてプロトコル合成論理（protocol composition logic）を提案し，この論理に計算論的解釈を与えることで，記号的／計算論的な推論の融合を行っている[11]．

10-2-3 ゲーム変換による安全性証明の機械化

暗号プロトコルの安全性はしばしばゲームを用いて定義される．適切な暗号学的な仮定のもとで，そのゲームに対する攻撃者のアドバンテージ（悪意ある敵の攻撃成功確率と偶然攻撃が成功する確率の差）が無視できるほど小さいことを示す．典型的な証明手法は，プロトコルへの攻撃を，根底にある暗号を破る攻撃に還元するというものである．近年，この還元を見通しよく行うために，ゲームの一部を系統立てて書き換えていくゲーム変換（game transformation）の方法論が確立しつつある．

このゲーム変換による安全性証明を機械化・自動化しようとする研究が盛んである．ブランシェ（Blanchet）とポアンシュバル（Pointcheval）は，確率的なプロセス計算（process calculus）の中で書き換え規則をフォーマルに扱うことでゲーム変換の機械化・自動化を実現した[6]．実際，開発した証明器 CryptoVerif を用いて，FDH（full-domain hash）署名の UF-CMA（unforgeability under chosen-message attacks）偽造不能性などを自動検証している．また，コリン（Corin）とデン・ハートク（den Hartog）は，命令的なプログラムの検証を行う論理体系として定着しているホーア（Hoare）論理を確率的に拡張し，ゲーム変換の正しさをフォーマルに示している[10]．

関連する研究として，Canetti らは，タスク構造確率的 I/O オートマトン（task-structured probabilistic I/O automaton）と呼ばれる計算系を用いて，汎用的結合可能性のスタイルに則って定式化された安全性を書換え規則の適用によってフォーマルに証明するための方法を提示している[8]．実際に，ハードコア述語（hard-core predicate）の存在という計算論的な仮定のもとで，紛失通信（oblivious transfer）プロトコルの安全性を証明している．

■参考文献

1) 萩谷昌己, “数理的技法による情報セキュリティの検証,” 応用数理，vol.17, no.4, pp.8-15, 2007.
2) 岡本龍明：“はん用的結合可能性と数理的技法,” 信学誌, vol.90, no.6, pp.451-456, 2007.
3) M. Abadi and A.D. Gordon, “A calculus for cryptographic protocols: The spi calculus,” Inf. Comput., vol.148, no.1, pp.1-70, 1999.
4) M. Abadi and P. Rogaway, “Reconciling two views of cryptography (the computational soundness of formal encryption),” J. Cryptology, vol.15, no.2, pp.103-127, 2002.
5) M. Backes, B. Pfitzmann, and M. Waidner, “A composable cryptographic library with nested operations,” Proc. 10th ACM Conf. Computer and Communications Security, pp.220-230, 2003.
6) B. Blanchet and D. Pointcheval, “Automated security proofs with sequences of games,” Advances in Cryptology—CRYPTO 2006, Springer, LNCS 4117, pp.537-554, 2006.
7) M. Burrows, M. Abadi, and R.M. Needham, “A logic of authentication,” ACM Trans. Comput. Syst., vol.8, no.1, pp.18-36, 1990.

8) R. Canetti, L. Cheung, D.K. Kaynar, M. Liskov, N.A. Lynch, O. Pereira, and R. Segala, “Analyzing security protocols using time-bounded task-PIOAs,” Discrete Event Dynamic Systems, vol.18, no.1, pp.111-159, 2008.
9) R. Canetti and J. Herzog, “Universally composable symbolic analysis of mutual authentication and key-exchange protocols,” Proc. Third Theory of Cryptography Conference, Springer, LNCS 3876, pp.380-403, 2006.
10) R. Corin and J. den Hartog, “A probabilistic Hoare-style logic for game-based cryptographic proofs,” Proc. 33rd International Colloquium on Automata, Languages and Programming, Springer, LNCS 4052, pp.252-263, 2006.
11) A. Datta, A. Derek, J.C. Mitchell, and B. Warinschi, “Computationally sound compositional logic for key exchange protocols,” Proc. 19th IEEE Computer Security Foundations Workshop, pp.321-334, 2006.
12) D. Dolev and A. Yao, “On the security of public key protocols,” IEEE Trans. Inform. Theory, vol.29, no.2, pp.198-207, 1983.
13) F.J. Thayer Fábrega, J.C. Herzog, and J.D. Guttman, “Strand spaces: Proving security protocols correct,” J. Comput. Security, vol.7, no.2-3, pp.191-230, 1999.
14) G. Lowe, “Breaking and fixing the Needham-Schroeder public-key protocol using FDR,” Software—Concepts and Tools, vol.17, no.3, pp.93-102, 1996.
15) D. Micciancio and B. Warinschi, “Soundness of formal encryption in the presence of active adversaries,” Proc. First Theory of Cryptography Conference, Springer, LNCS 2951, pp.133-151, 2004.
16) R.M. Needham and M.D. Schroeder, “Using encryption for authentication in large networks of computers,” Commun. ACM, vol.21, no.12, pp.993-999, 1978.
17) L.C. Paulson, “The inductive approach to verifying cryptographic protocols,” J. Comput. Security, vol.6, no.1-2, pp.85-128, 1998.