B-003

代数仕様言語CafeOBJによるセキュリティプロトコルの形式化
Formalization of security protocol in CafeOBJ

加藤 淳 * 中村 正樹 * 緒方 和博 † 二木 厚吉 *
Atsushi Kato Masaki Nakamura Kazuhiro Ogata Kokichi Futatsugi

1. はじめに

近年，インターネットに代表される広域情報ネットワークの急速な普及および発展にともない，ネットワークセキュリティに対する安全性の重要性が増して，多くの通信プロトコルが考案されている．ネットワーク上でメッセージを暗号化し，通信者間の秘密通信機能を持つ通信プロトコルであるセキュリティプロトコルは，電子商取引や電子選挙等への適用が期待されている．

しかし，安全性が保証されているような強固な暗号技術を用いても，セキュリティプロトコルに欠陥がある場合，それは安全な通信が行えるとはいえない．安全な通信を保証するセキュリティプロトコルを考案することは非常に重要なことである．セキュリティプロトコルの欠陥を人間の直感による判断や，プロトコル運用の中で発見することは非常に難しい．

形式手法による検証によりよく知られたプロトコルの不具合が報告されたことで，その有効性が期待され，多くの方法が提案されている [1, 2].

本研究では，代数仕様言語 CafeOBJ を用いてセキュリティプロトコルの仕様を形式的に記述する．例題として共通鍵暗号を用いた認証プロトコル，Otway-Rees プロトコルを用いる．具体的にはセキュリティプロトコルを観測遷移機械でモデル化を行い，作成したモデル，すなわち観測遷移機械を CafeOBJ で記述する [2].

2. 代数仕様言語 CafeOBJ

代数仕様言語 CafeOBJ は主に自然数等の抽象データ型の記述に用いる始代数と，抽象機械に記述に用いる隠蔽代数に基礎をおいている．CafeOBJ には 2 種類のソート (型) がある．抽象データ型を表す可視ソートと，抽象機械の状態空間を表す隠蔽ソートである．隠蔽ソートについては，抽象機械の状態を変化させるのに用いる作用演算と，抽象機械の状態を観察するのに用いる観測演算の 2 種類の演算がある．

3. 観測遷移機械

対象システムのモデルの作成に観測遷移機械 (Observational transition systems) を用いる [2]．観測遷移機械では，対象システムに関連する値およびそれらが状態遷移によりどのように変化するのかを状態の外部から観察することでモデルを作成する．対象システムの状態空間を包含する状態空間 Υ の存在を仮定し，状態空間の各要素を状態と呼ぶ．観測遷移機械 $\mathcal{S}$ は 3 組の $\langle \mathcal{O}, \mathcal{I}, \mathcal{T} \rangle$ で定義され，各要素は観測の集合 $\mathcal{O}$，初期状態の集合 $\mathcal{I}$，条件付遷移規則の集合 $\mathcal{T}$ を表している．

観測遷移機械 $\mathcal{S}$ は CafeOBJ を用いて記述する．状態空間 Υ は CafeOBJ の隠蔽ソートに相当する．$\mathcal{S}$ の観測 $\mathcal{O}$，初期条件 $\mathcal{I}$，遷移規則 $\mathcal{T}$ はそれぞれ観測演算，隠蔽ソートの定数，操作演算で宣言する．これらの意味は等式によって与えられる．CafeOBJ 処理系は，記述された等式を左から右への書き換え規則として用いて，与えられた項を書き換える．この実行可能性により，記述したシステムのシミュレーションを行ったり，システムがある性質を有することを検証することができる．

4. Otway-Rees Protocol

1987 年に Otway と Rees により共通鍵暗号方式を用いた認証プロトコルが提案された [3, 4]．このプロトコルの目的は主体 A と B に認証局 S が A と B の共通鍵を発行し分配することである．X と Y との間の共通鍵を K_{xy} とし，それにより暗号化した文を $\{...\}_{K_{xy}}$ と書く．暗号文は共通鍵の持ち主 X，Y にしか復号することはできない．Otway-Rees プロトコルは次のように記述できる：

Message1 $A \to B$: $M, A, B, \{N_a, M, A, B\}_{K_{as}}$
Message2 $B \to S$: $M, A, B,$ $\{N_a, M, A, B\}_{K_{as}}, \{N_b, M, A, B\}_{K_{bs}}$
Message3 $S \to B$: $M, \{N_a, K_{ab}\}_{K_{as}}, \{N_b, K_{ab}\}_{K_{bs}}$
Message4 $B \to A$: $M, \{N_a, K_{ab}\}_{K_{as}}$

Message1，2 によって，主体 A，B は認証局に対して A-B 間の共通鍵を生成してほしいという要求を送信する．ここで M，N_a，N_b はノンスと呼ばれ，それぞれの主体が生成する類推不能な値である．各主体は暗号文の中のノンスを確かめることで，そのメッセージがプロトコルにしたがって送られてきたものであることを確認する．認証局は受け取った 2 つの暗号文を復号して，ノンス M と識別子 A,B がそれぞれ一致することを確認する．一致すれば認証局は A，B の共通鍵 K_{ab} を生成し，各ノンス N_A，N_B と共通鍵のセットを生成し A，B に渡す．A，B は受け取った暗号文を復号しノンスを確かめることで，確かに認証局からの返答であると確認することができる．

5. Otway-Rees 認証プロトコルのモデル化

5.1 モデルで使用するデータ型の定義

まず，信頼できる主体，信頼できない主体 (侵入者)，認証局のデータ型の定義を行う．信頼できる主体は，プロトコルに則った動作のみを行う．侵入者はプロトコルに則った主体の動作に加え，ネットワークを流れるメッセージを盗聴し，盗聴した情報を基にメッセージの偽造を行ったりする．認証局は唯一存在し，他の主体や侵入者によるなりすましはないものとする．

* 北陸先端科学技術大学院大学, Japan Advanced Institute of Science and Technology (JAIST)
† (株) NEC ソフトウェア北陸, NEC Software Hokuriku, Ltd.

次に，プロトコルで用いられる暗号文やメッセージ等のデータ型を定義する．メッセージのデータ構成子は複数の引数を持っている．Message1〜Message4 の各データ構成子は次のような演算子 m1，m2，m3，m4 で表す：

```
[Msg]
op m1 : Pr Pr Pr Nonce Pr Pr Ci1 -> Msg
op m2 : Pr Pr Se Nonce Pr Pr Ci1 Ci1 -> Msg
op m3 : Se Se Pr Nonce Ci2 Ci2 -> Msg
op m4 : Pr Pr Pr Nonce Ci2 -> Msg
```

それぞれ，Pr は主体，Se は認証局，Nonce ノンス，Cin は暗号文を表す可視ソートである．各演算子の最初の引数はメッセージの送信者，2 番目の引数はメッセージの見かけ上の送信者，3 番目の引数はメッセージの受信者となっている．4 番目以降の引数は暗号文等のメッセージ本体である．

ネットワークはメッセージの集合としてモデル化する．ネットワークが空であるときはメッセージが一度も送信されていないことを意味する．一度ネットワークに流れたメッセージはその集合に追加され，侵入者は集合上のメッセージをいつでも参照可能となるように定義する．

5.2 Otway-Rees 認証プロトコルのモデル

観察可能なプロトコル内部の値を決め，プロトコルの振舞を遷移規則としてモデル化し，観察可能な値がどのように変化するか定義する．

状態の集合を隠蔽ソート Sys として宣言する．観測演算には，プロトコルでそれまでに使用したノンスの集合を観察する uv と，プロトコルに関連するメッセージを媒介するネットワークを観察する nw，およびセッションごとに生成される共通鍵の集合を観察する sk の 3 つを宣言する：

```
bop uv : Sys -> Uvalue
bop nw : Sys -> Network
bop sk : Sys -> ShareKey
```

初期条件は，任意の初期状態を表す定数を宣言し，次のように記述し，また次のような等式によって観測演算の初期状態における返戻値を宣言する：

```
op init : -> Sys
--
eq uv(init) = empty .
eq nw(init) = void .
eq sk(init) = ...
```

等式はそれぞれ観察する集合が空集合であることを意味している．

作用演算には，プロトコルに則り Message1〜Message4 を送信するそれぞれの遷移規則 4 種類に対応する 4 つの作用演算を宣言する．作用演算の記述例は次のようになる：

```
bop mes1 : Sys Pr Pr Nval Nval -> Sys
--
ceq uv(mes1(S,A,B,M,Na))
 = M Na uv(S)
   if not(M \in uv(S) and N_a \in uv(S)) .
ceq nw(mes1(S,A,B,M,Na)) = ...
ceq sk(mes1(S,A,B,M,Na) = ...
```

Nval はノンスのための可視ソートである．作用演算 mes1 はプロトコルに則り，Message1 を送信する遷移規則に対応する．mes1(S,A,B,M,Na) はある状態 $\mathcal{S}$ に対して，M がこのプロトコルの 1 つのセッション自体のノンスを表しており，Na が A で表される主体が B で表される主体に Message1 を送るために生成したノンスを表している．一つ目の等式では作用演算 mes1 の事後状態がノンスの集合 uv にノンス M，Na を加えていることを表している．

また，侵入者が収集した暗号文およびノンスを用いてメッセージを捏造する遷移規則 8 種類に対応する 8 つの作用演算を宣言する．

6. まとめと今後の課題

本研究では，振舞仕様に基づく共通鍵暗号を用いた認証プロトコル，Otway-Rees プロトコルの代数仕様言語 CafeOBJ による形式的記述を行った．代数的な仕様記述は，可読性や理解の容易さの点で強みがある．また，検証したい性質を CafeOBJ で記述し，CafeOBJ 処理系で実行させることで示したいことの検証を行うことができる．

今後の課題として，検証したい性質を明かにし，Otway-Rees 認証プロトコルの検証を行う．振舞仕様に基づく安全性の検証は，公開鍵暗号を用いた NSLPK 認証プロトコルをはじめ，ある程度の規模のものまで適切に扱えることが実証されている [2]．

本研究で例題として取り上げた Otway-Rees 認証プロトコルと NSLPK 認証プロトコルの例を比較し，認証プロトコル一般に対する形式的記述・検証の方法論を確立させ，SSH など現実的に利用されているようなプロトコルに適用させることも今後の課題のひとつである．

参考文献

[1] 金城直樹：セキュリティプロトコルの代数モデルに基づく形式化，北陸先端科学技術大学院大学，修士論文，2001.

[2] 緒方和博, 二木厚吉：書き換えによるセキュリティプロトコルの帰納的検証, コンピュータソフトウェア, vol.20, No3, pp.54-72, 2003.

[3] L.Paulson： The Inductive Approach to Verifying Cryptographic Protocols, *Journal of Computer Security,* Vol.6, pp.85-128, 1998.

[4] M.Burrows, M.Abadi, and R.M.Needham： A logic of authentication. *Proceedings of the Royal Society of London,* 426:pp.233-271, 1989.