Innovative R&D by NTT

Tamarin Proverによる 投票プロトコルの安全性検証

櫻田英樹
NTTコミュニケーション科学基礎研究所

研究の動機

[Kremer and Ryan ‘05]は電子投票プロトコルFOO [Fujioka *et al.*, ’92]の様々な性質を検証したが、

- 投票の適格性（eligibility）として「正規の投票者だけが投票できる」ことを検証したが**「1回だけ投票できる」ことを検証していない**
- プロトコルで用いられている暗号プリミティブのうち、**ブラインド署名の形式化(記号モデル)が計算論的に健全**でない。

本研究の概要

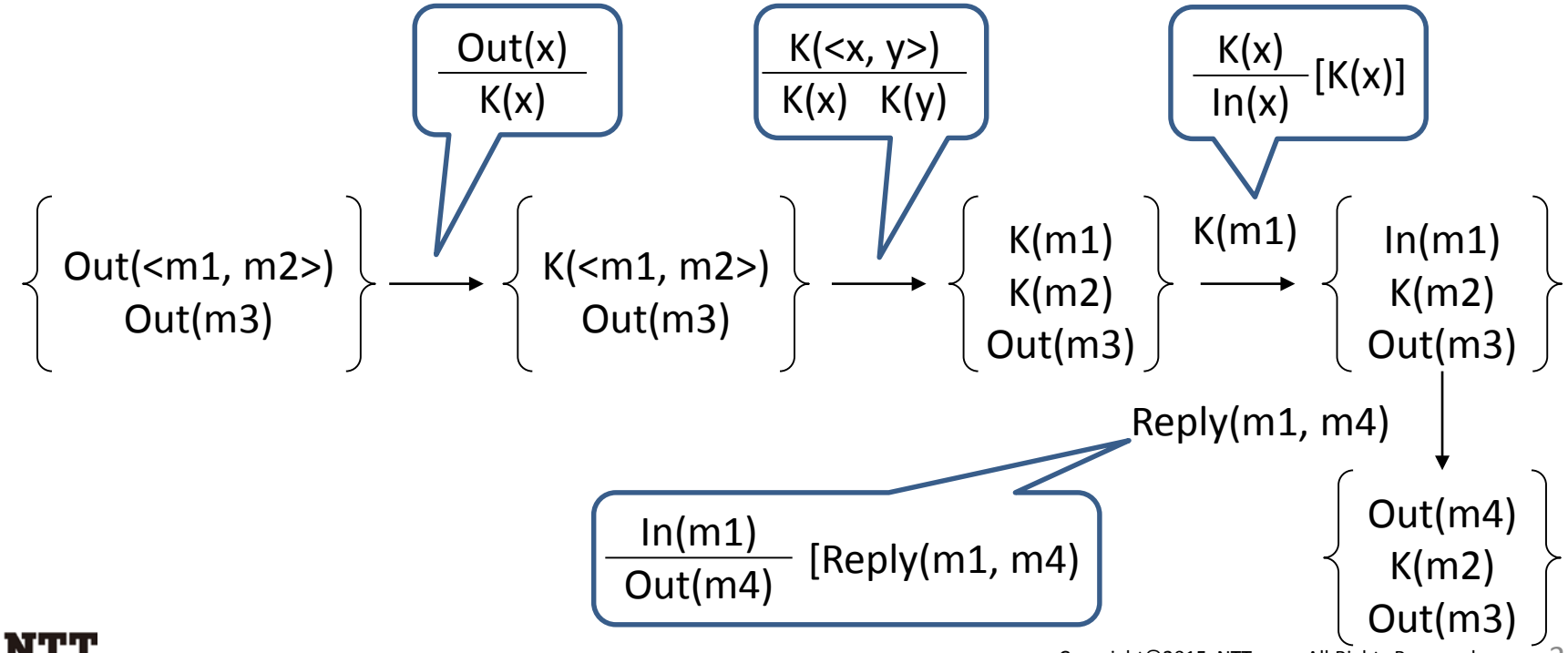
電子投票プロトコルFOOにおける投票の適格性を検証。特に

- 「正規投票者が**1回だけ**投票できる」という本来の適格性を定式化・検証
- ブラインド署名の記号モデルとして**計算論的に健全なもの[Sakurada '12]**を使用

このために検証ツールTamarin [Schmidt *et al.*, CSF ’12; S&P ’14] を利用

プロトコル検証ツールTamarin

- 多重集合（同じ要素が複数回の出現）を利用
  ネットワークの状態＝多重集合
  プロトコルの実行＝多重集合の書換
- 多重集合により、“状態”をうまく扱える



電子投票プロトコルFOO（概略）

- 投票の匿名性と適格性の両立のため、投票者は管理者が署名した投票を匿名通信路から送信
- 投票を管理者にも秘密にするため、ブラインド署名を用いて管理者の署名を取得

TamarinでのFOOの定式化（一部）

「管理者は投票者Vの投票の署名を検証し、投票に署名して送信、ただし各署名者につき１度だけ」

$$\frac{!Vk(\$V, vkv)\quad !SkA(\sim ska)\quad In(\langle sig, blinded\_ballot\rangle)\quad Not\_signed\_for(V)}{Out(bsign(blinded\_ballot, \sim ska))\quad Not\_used(bsign(blinded\_ballot, \sim ska))}$$

ルールの適用により、Not_signed_for(V)が書き換えられる（消える）ため、このルールは投票者Vに対しては「１度だけ」使われる

ブラインド署名

- ユーザ・署名者・検証者の３者間プロトコル
  1. 参加者はテキストmをブラインド化β＝B(m)して署名者に送信
  2. 署名者はβに署名σ＝S_sk(β)して返す
  3. 参加者はσから署名σ’を得る（unblind）
  4. 検証者はm, σ’を検証（上記σ’については成功）
- 安全性
  - 偽造不能性：署名者の実行回数分しか署名を得られない
  - 秘匿性：アンブラインドするまでmは秘密

[Kremer and Ryan ‘05]のモデル化

- 「参加者がテキストmを正しい手順でブランド化し、それに署名者が署名にした場合のみ署名が得られる」というモデル
- しかし、これはブラインド署名の安全性からは導かれないため、攻撃を見逃すおそれがある [Sakurada, ’13]

[Sakurada, ’13]のモデル化

- ブラインド署名の偽造不能性を忠実にモデル化、計算論的健全性を証明
  （≒攻撃を見逃さないモデル化を達成）
- Tamarinでのルール記述（一部）

$$\frac{!SkA(\sim ska)\quad In(bsign(fblind(r, vk(\sim ska)), \sim ska))\quad In(m)\quad Not\_used(bsign(fblind(r, vk(\sim ska)), \sim ska))}{Out(sign(m, \sim ska))}$$

- ルールの適用によりNot_used(…)を消費、このbsign(…)は今後は使えない（⇨偽造不能性）

Tamarinにおける適格性の定式化

Innovative R&D by NTT

直観的定義

集計者が投票c0, c1を（異なる時点で）受理したなら、それぞれそれを投票した異なる投票者V0とV1存在する

形式的定義

```
lemma eligibility:
  "All c0 c1 #i #j.
   (Accept_vote(c0) @ #i & Accept_vote(c1) @ #j & not(#i = #j))
   ==>  (Ex V0 V1 #g #h. ((  Voter_started(V0, c0) @ #g
                           & Voter_started(V1, c1) @ #h
                           & not(V0 = V1)))
```

NTT

検証結果

- 適格性「正規投票者のみが１度だけ投票可能」を自動的に検証できた
- ただし、「署名からテキストを取り出せる」などのルールを追加すると停止しなくなる
- 実行環境・検証時間

CPU：Xeon x5690 @ 3.47GHz （６コア）× 2

（※並列実効されるためコア数が多いほうよい）

メモリ：約50GB

OS：Ubuntu Linux 14.04.01 LTS

ソフトウェア：Tamarin Prover 0.8.6.1

検証時間：約56秒

まとめ

これまで形式検証が行われてこなかった電子投票プロトコルFOOにおける投票の適格性を、検証ツールTamarinを利用して検証

特に

- 「正規投票者が**1回だけ**投票できる」という本来の適格性を定式化・検証
- ブラインド署名の記号モデルとして**計算論的に健全なもの[Sakurada '12]**を使用

  ⇨「攻撃を見逃さない検証」が可能に