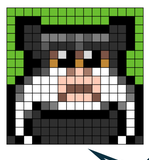
Rabbitモデルの検証結果における可読性向上のためのトレースグラフの構築

長谷川 光，　五十嵐 淳　　京都大学

背景: Rabbit

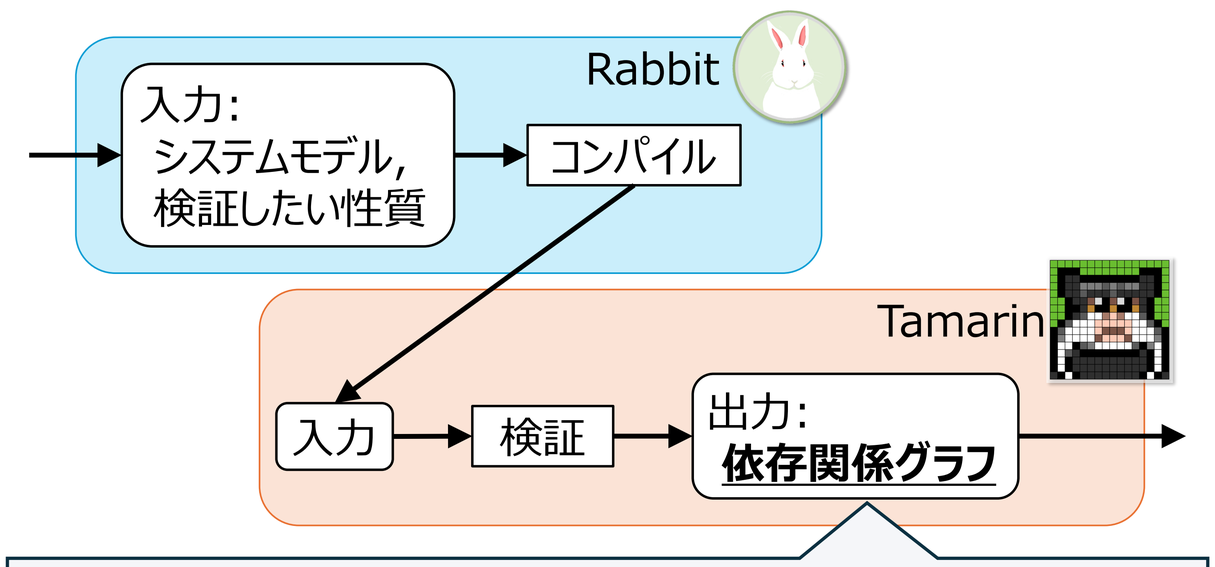
Rabbit [Inaba et al., '24][Park & Igarashi, '25]:
ネットワークシステムのモデリング言語

- 手続き的な記述で直感的にモデル化
- 形式検証の専門家でなくても扱いやすい

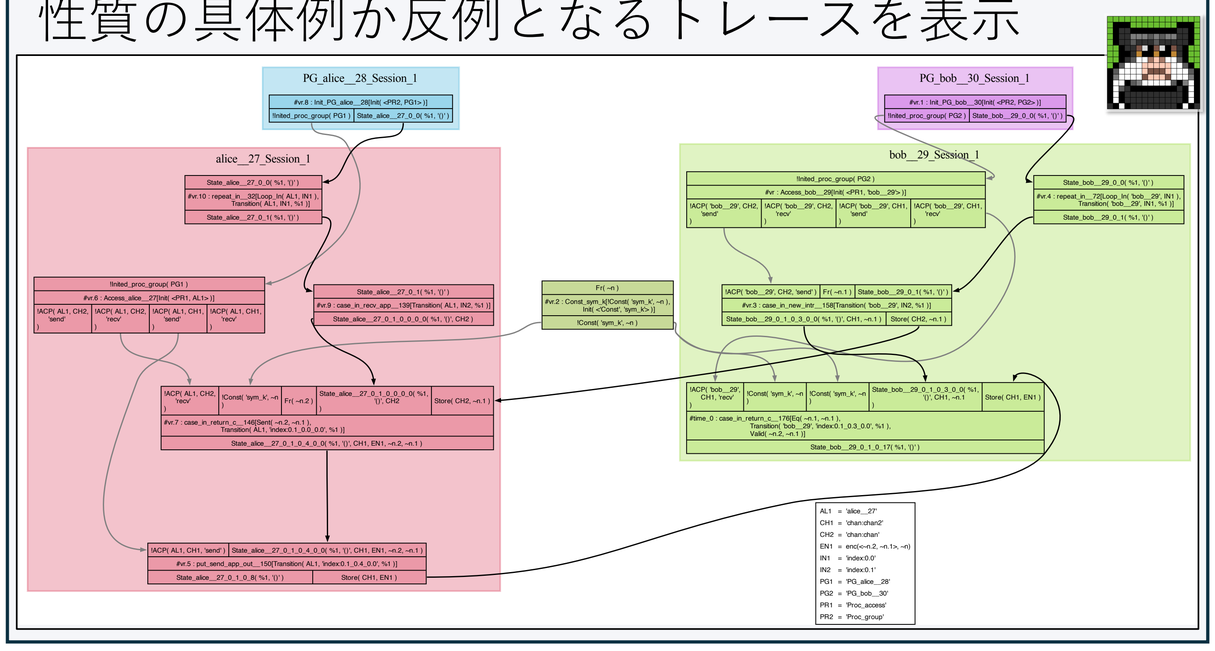


Tamarin [Schmidt et al., '12]:
Rabbitモデルをバックエンドで検証

- 数学的な記述でモデル化する検証ツール



性質の具体例か反例となるトレースを表示



課題点

出力されたトレースに含まれる
バグや脆弱性を
具体的に把握することは重要

Tamarinが出力する依存関係グラフは

- Tamarin特有の記法に基づく
- Rabbitコンパイラが生成した内部変数を含む

などの要因により、Rabbitユーザーにとって難解

目的

Rabbitユーザー向けに**検証結果の可読性を高めたい**

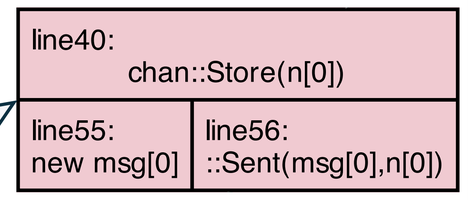
貢献

- **トレースグラフ**の提案
  - Rabbitコードと対応する新たな出力様式
- Tamarinによる出力からトレースグラフへの変換プログラムを実装
  - 50個程度の例で適切な変換の実行を確認

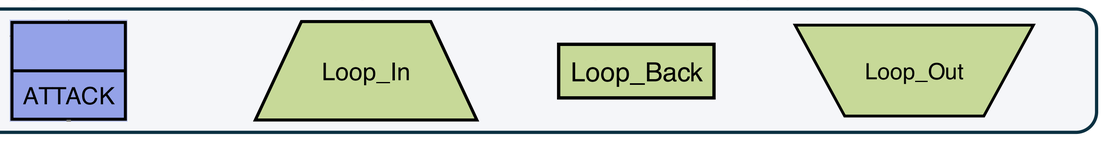
提案: トレースグラフ

- 各ノードは操作の一まとまりに対応

Rabbitのコード断片を表示
上段:実行条件　下段:実行内容

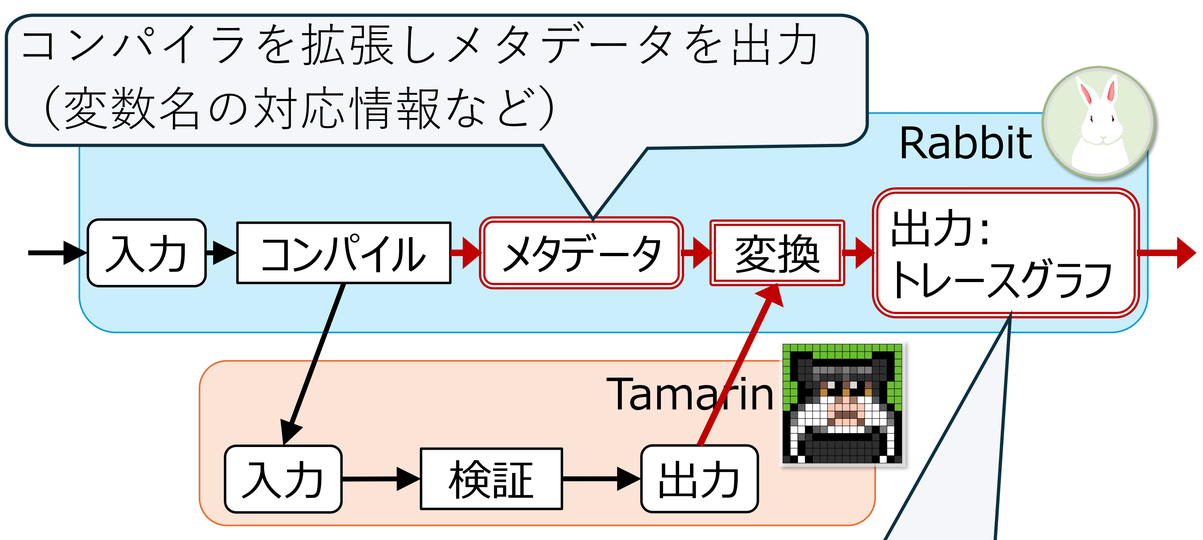


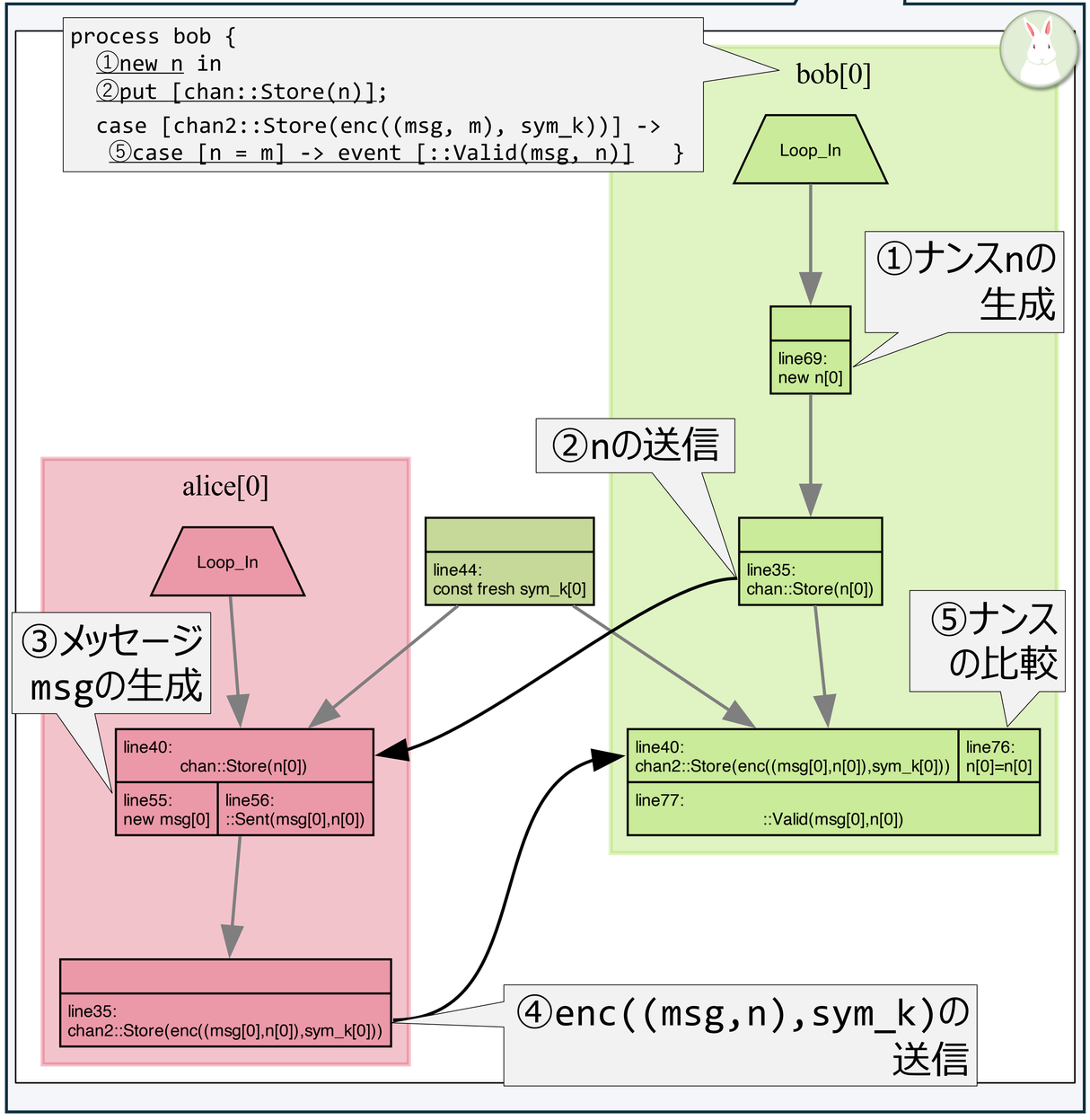
- 攻撃やループが含まれれば特別な表示



- 有向辺によって実行順序を指定

コンパイラを拡張しメタデータを出力
（変数名の対応情報など）





- 不要な表示情報を削減
- Rabbitユーザー向けに逆翻訳

実行の流れが目で追いやすく、
元のRabbitコードとの対応が取りやすくなった。

今後の課題

- グラフ画像をより見やすく
- 画像以外の形式で情報を補足