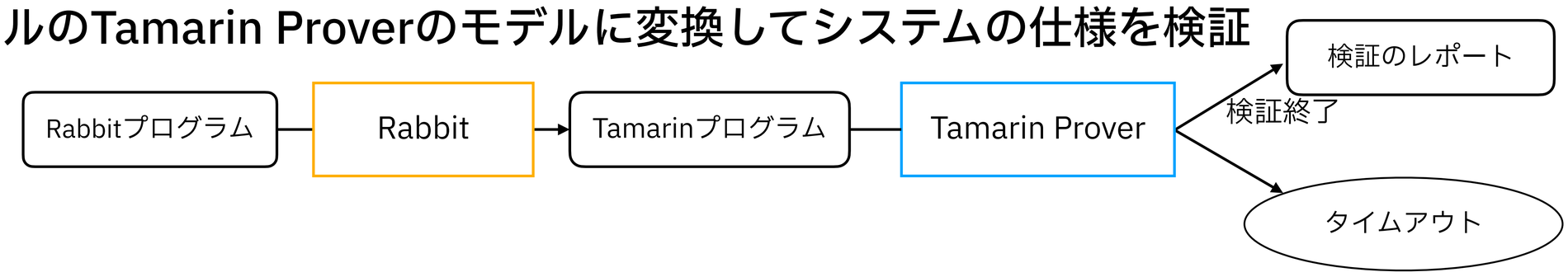
ユーザーによる仮定の宣言を可能とする Rabbit処理系の拡張と検証の高速化

北川 聖也，五十嵐 淳
京都大学

背景: Rabbit [Inaba et al., ’24][Park & Igarashi., 25’]

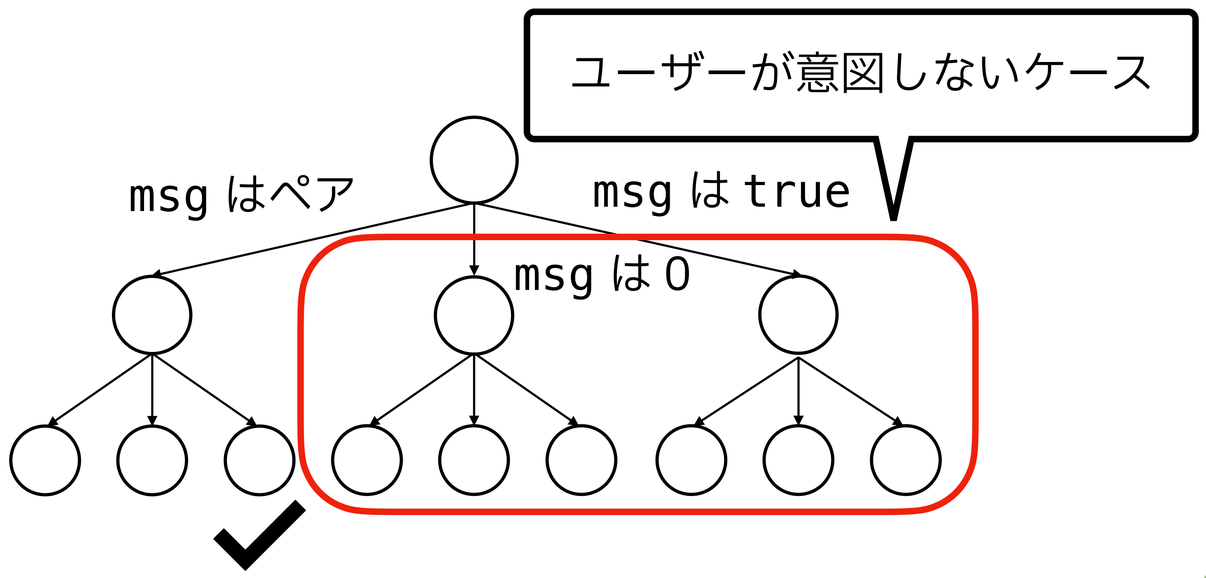
ネットワーク通信を行うシステムのモデリング言語
低レベルな概念をサポート（プロセス、ファイルシステム、メモリなど）
プロトコル検証ツールのTamarin Proverのモデルに変換してシステムの仕様を検証



RabbitはTamarinに変数がどのようなものであるかを明示的に伝える手段がなく、Tamarinはユーザーが意図しない実行まで考慮してしまう

```
var msg = receive(ch) in
var x = fst(msg) in
var y = snd(msg) in
```

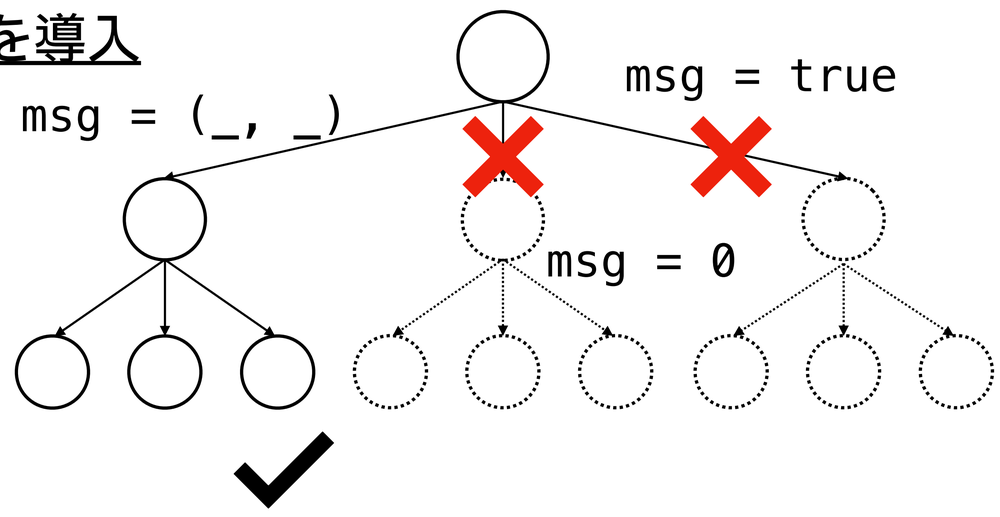
msg の要素を取り出す
→ msg はペアという意図



本研究: assume宣言によるRabbitの拡張

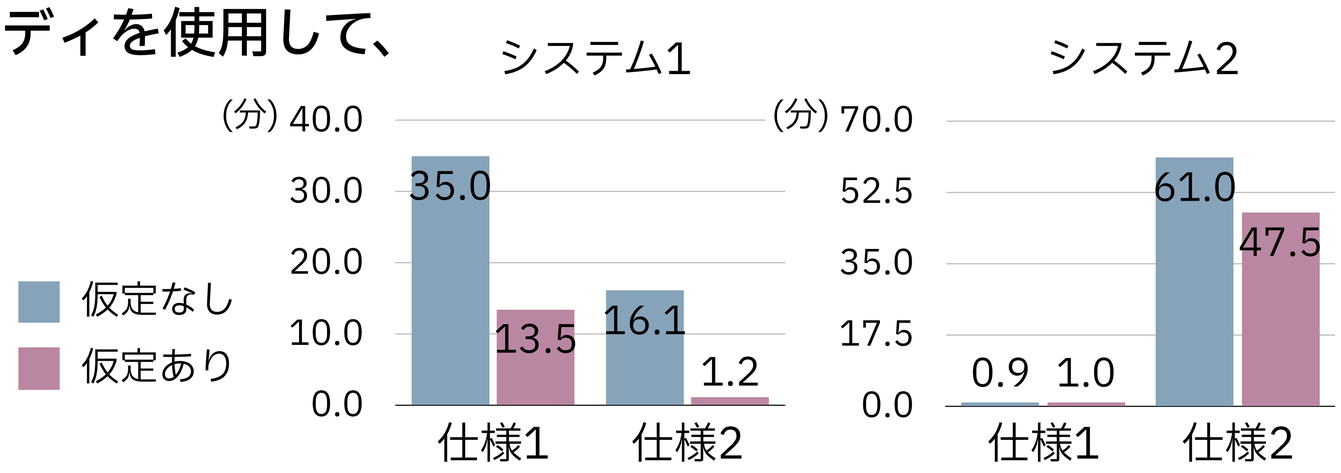
ユーザーがプログラム中で成り立つ性質を明示的に宣言することで,
探索しなくてよい分岐を指示
ユーザーが明示的に仮定を宣言する **assume コマンドを導入**

```
var msg = receive(ch) in
assume [msg = (_, _)] in
var x = fst(msg) in
var y = snd(msg) in
```



実験: assumeによる検証時間の変化を評価

[Park & Igarashi., ’25] によるケーススタディを使用して、
仮定の有無による検証時間の変化を比較
検証時間の短縮を確認できた



今後の課題: 型やデータフロー解析を用いた高速に検証可能な入力プログラムの生成