寺内研
研究室紹介

教員紹介

寺内 多智弘(てらうち たちお)

- 1978年生まれ
  - 本籍：栃木県宇都宮市
- 14-28歳を米国で過ごす
  - コロンビア大学(学士号)　カリフォルニア大学バークレー校(博士)
- 2007.1～2011.3 東北大学 助教
- 2011.4～2014.3 名古屋大学 准教授
- 2014.4～2017.9 北陸先端科学技術大学院大学 教授
- 2017.9～ 現在　早稲田大学 教授

研究内容 (cf. 紹介資料・ホームページ)

専門分野：プログラミング言語

- **主な研究テーマ**
  - 新しいプログラミング言語・言語機能(型システムなど)の開発
    - 依存型(dependent type)や交差型など先進的型システムの研究など
  - プログラム検証
    - コード解析によるプログラムの正しさの自動検証
  - プログラム合成
    - バグ修正パッチやセキュリティ攻撃耐タンパコードの自動生成など
  - 自動定理証明
    - 新しいSATソルバ・SMTソルバなど自動定理証明・制約解消アルゴリズムの研究
  - セキュリティに関する研究
    - プログラム検証による情報漏洩の検出や耐タンパコードの生成など

背景：ソフトウェアバグによる社会問題

近年の事例

- 金融機関システム不具合によるATMの機能停止(2011)
- HeartbleedバグによるOpenSSLの脆弱性(2014)
- ソフトウェアバグによる衛星喪失(2016)
- ソフトウェアバグによる1000名以上の従業員個人情報流出(2017)

損害は急増傾向：600億ドル(2002 NIST)→**1.1兆ドル**(2016 Tricentis)

テスト実行など従来のソフトウェア開発手法だけでは複雑化するソフトウェアの品質の担保が困難

研究のねらい：コンピュータアルゴリズムにより、機械的かつ正式にプログラムの正しさの検証や正しいプログラムの合成をしよう。

例題1：タイミング攻撃の検出・防衛

```
bool checkpass (char[] guess) {
  int i = 0;
  while (i < n) {
    if (pass[i] != guess[i]) return false;
    i++;
  }
  return true;
}
```

実行時間を観測できる攻撃者は、効率よく機密(pass)を盗み出せる。

近年の成果(jww Yale大学等米国の研究グループ)

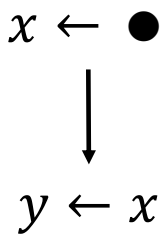
- プログラム検証によるタイミング攻撃可能性の検証 [PLDI'17]
- Bucketingという防衛手法についての研究 [POST'19,J. Comp. Sec.'20]

例題2 (jww 山内蒼太@寺内研M2)

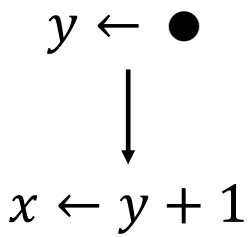
問：正しいのはどれでしょう？ (ただしx, yは整数を領域とする)

True 1. $\forall x \exists y. x \leq y$　　**False** 2. $\exists y \forall x. x \leq y$

- 問題をゲームと見なし、必勝戦略を生成することにより解く



1.におけるヨプレイヤーの必勝戦略



2.における∀プレイヤーの必勝戦略

SMTソルバ(量化子なし式の定理証明アルゴリズム)と組み合わせることで、複雑な量化子付き論理式の真偽を効率よく判定することが可能に

より詳しくは個別面談で

- 新型コロナウィルス感染症に関する自粛要請のため、オープンハウスは中止ですが、個別面談を受け付けます。希望日時を書いたメールを送ってください。

- メールアドレス： terauchi@waseda.jp
- 面談場所：62号館 209B
  - 希望があればオンラインでの面談も受け付けます。

配属決定後の連絡

- 配属決定後の集合についてはメールで連絡します。