第14回TOPPERS活用アイデア・アプリケーション開発コンテスト 活用アイデア部門

銀賞: 並列プログラミング言語Elixir(エリクサー)からTOPPERSカーネル利用C・アセンブリコードを生成するサイドチャネル攻撃防御指向コンパイラ

銅賞: 箱庭時間管理手法に関する先行研究調査と改良

受賞の言葉

北九州市立大学 山崎 進

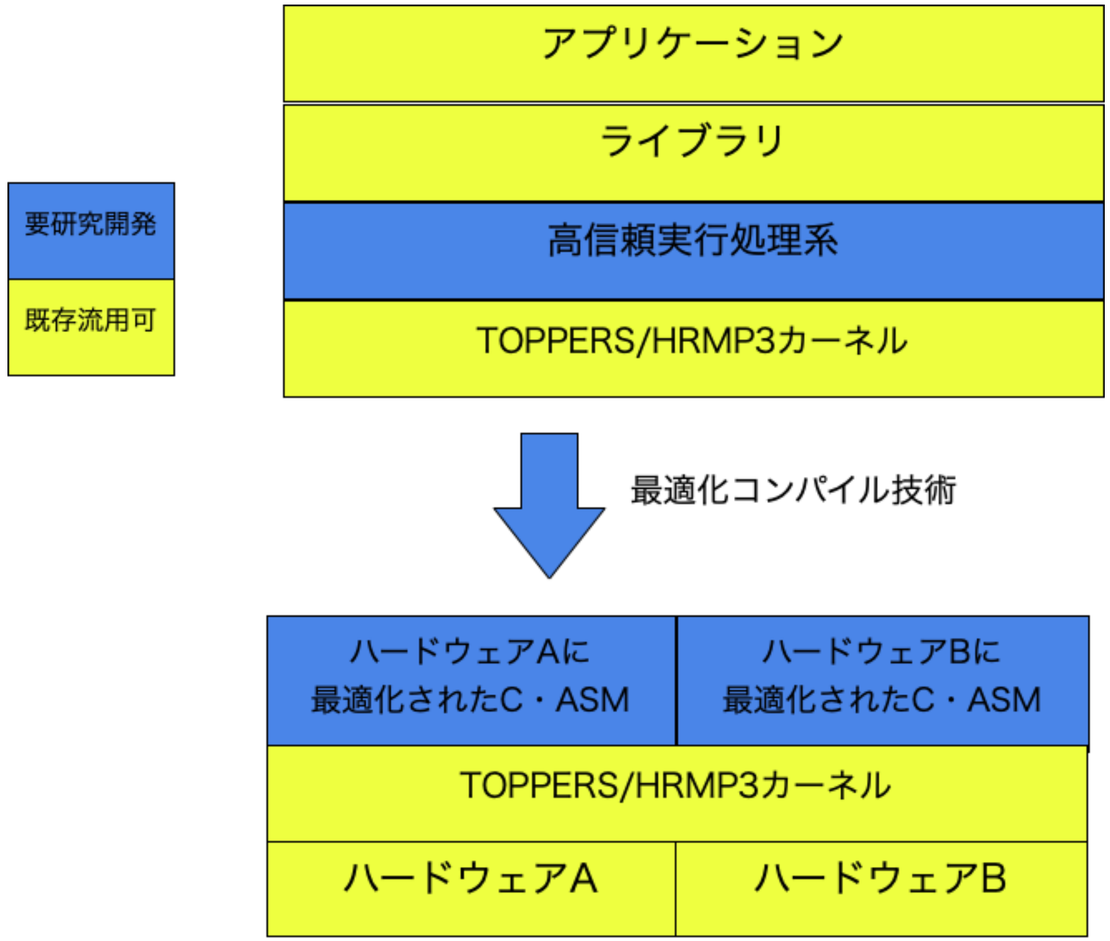
© 2024 Susumu Yamazaki

銀賞: 並列プログラミング言語Elixir(エリクサー)からTOPPERSカーネル利用C・アセンブリコードを生成するサイドチャネル攻撃防御指向コンパイラ

© 2024 Susumu Yamazaki

提案手法

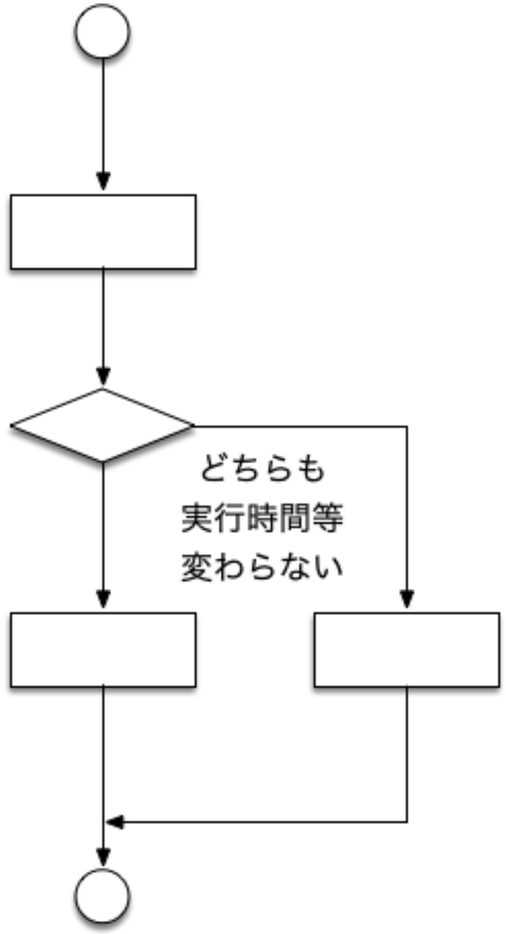
- 山崎進研究室で培ってきたElixirのコード生成・最適化技術を踏まえ，Elixirのコードから HRMP3カーネルを利用するC・アセンブリコードを生成する



© 2024 Susumu Yamazaki

サイドチャネル耐性(マスキング)

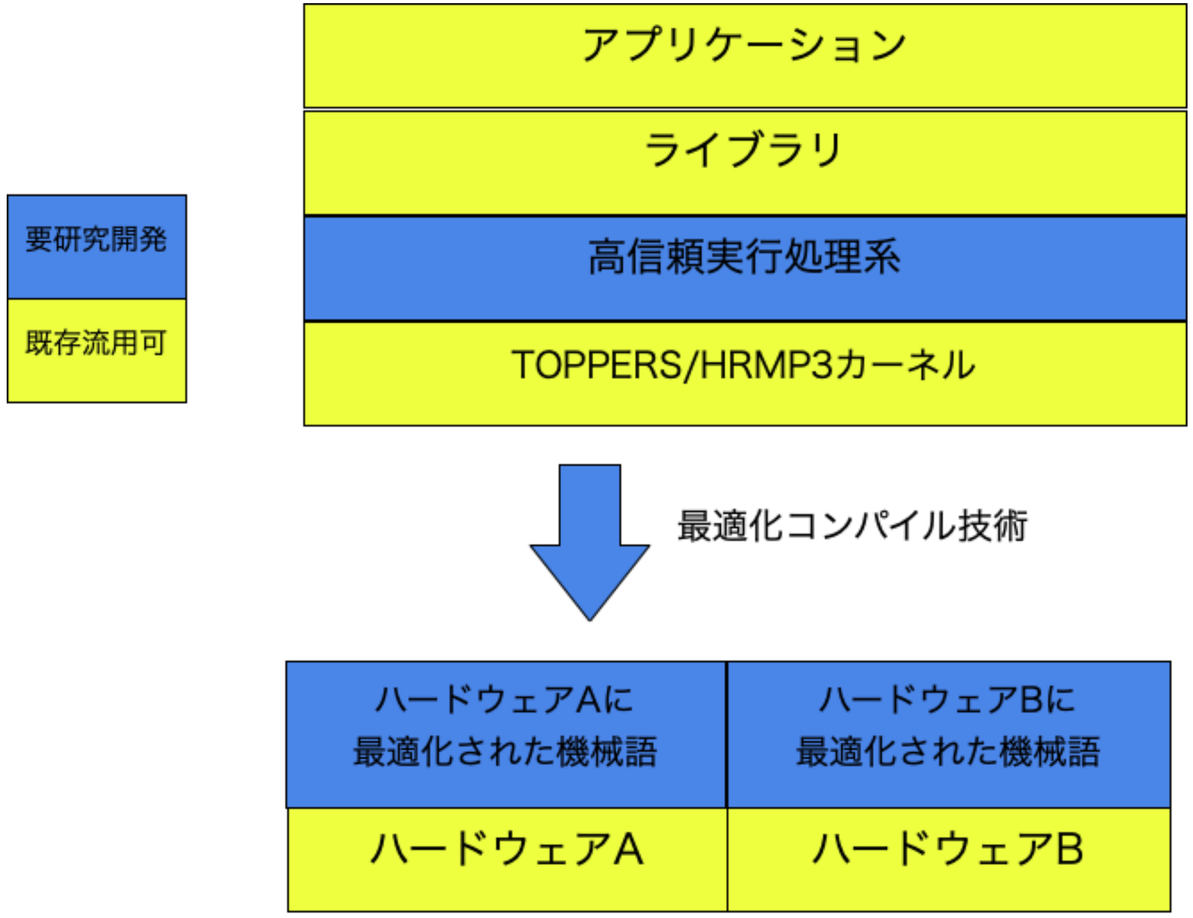
- 組込みシステムへのサイドチャネル攻撃の脅威
  - 次の情報を統計分析することで，悟られることなく秘密情報を傍受可能
    - プロセスの実行時間，プロセッサの消費電力，プロセッサから放射される電磁波等
- マスキング
  - 条件分岐のどの経路においても実行時間や使用する演算ユニットを変えないようにする(右図)
  - 実行時間・消費電力・電磁波等を計測して統計分析しても有意な差を見出せないようにすることでサイドチャネル攻撃を根絶



© 2024 Susumu Yamazaki

Elixirだけでなくコンパイラも同様に研究

- 組込みシステム研究会
  - 新規のC言語処理系を実装することによる
    組込みシステム研究にもたらす価値
    についての考察
- TOPPERS/HRMP3カーネルをコンパイルできるようなCコンパイラを新規開発
  1. 過度なコード最適化の抑制
  2. 形式手法をCコードに適用
  3. コード最適化の等価性保証
  4. サイドチャネル攻撃耐性を備えたコード生成



© 2024 Susumu Yamazaki

銅賞: 箱庭時間管理手法に関する先行研究調査と改良

© 2024 Susumu Yamazaki

提案

- 箱庭では，並行して動作する個々のシミュレータが独立して時間管理しているのを同期することが求められる.
- 箱庭の時間管理方式は，先行研究としてFMIを挙げた上で，並列化容易な分散制御方式を提案しているが，理論的背景が不足しているとのことである.
- そこで，先行研究を徹底調査し，現行方式の妥当性と改良を検討する.
- 現時点で我々が着目している先行研究の体系は次の3つである.
    1. 1980年代ごろに盛んに研究された，因果律を保持するような並行かつ論理的な時間管理手法
    2. メモリー貫性モデル
    3. 分散データベース
- これらについて徹底的に先行研究を調査し，現行方式の妥当性を検証し，必要であれば改良を提案する.

© 2024 Susumu Yamazaki