

電気・電子情報工学専攻	学籍番号	133242	指導教員氏名	市川 周一 藤枝 直輝
申請者氏名	佐藤 清広			

## 論 文 要 旨 (修士)

論文題目	位置レジスタを付加した命令レジスタファイルにおける耐タンパ性手法
------	----------------------------------

近年、解析・盗用・改ざんに対して組込みソフトウェアを保護する能力の重要性が増加している。この能力は耐タンパ性と呼ばれる。ソフトウェアの解析を例にとれば、命令と機械語の対応関係を隠蔽することで、逆アセンブルを防止でき、耐タンパ性を高められる。

組込みソフトウェアの耐タンパ化に命令セットランダム化 (ISR: Instruction set randomization) と呼ばれる手法がある。ISR は命令と機械語の対応関係を変更・追加する手法であり、軽量の命令メモリの難読化に位置付けされる。Hines らは命令レジスタファイル (IRF: Instruction Register File) と位置レジスタ (Positional register) を提案した。IRF は使用頻度の高い命令を格納したテーブルである。位置レジスタは過去に実行された命令が参照したレジスタ番号を記録するレジスタファイルであり、IRF に付加して効果を高めるために利用する。これらはコード圧縮による消費電力削減のために提案された手法であった。これに対して藤枝らの先行研究では IRF を用いた ISR を行い、IRF が耐タンパ性向上に利用できることを明らかにした。

本研究は位置レジスタのアプローチが耐タンパ性を高めるためにも利用できると考え、IRF に位置レジスタを付加してさらなる耐タンパ性向上を達成することを目的とする。位置レジスタの表現へ命令変換を行う際、位置レジスタの表現を使うべきか、また 1 つの命令に複数の位置レジスタの表現がある場合、それらのどれを使うべきかという選択肢が存在する。本研究では、命令表現の選択方法として貪欲法を使用して、出現頻度の高い表現をもつ命令を順次その表現に変換していく手法を提案した。比較のため、出現頻度を考慮せず、固定の優先度で可能な限りすべての命令を位置レジスタの表現に置き換える方法も検討する。また耐タンパ性を向上させるために有効な位置レジスタの設計として、位置レジスタの記録対象をすべてのレジスタとするだけでなく、一部のレジスタに限定した設計も検討した。限定する方法はデスティネーションレジスタとソースレジスタに分けて記録する“用途ベース”と、rs, rt, rd フィールドを分けて記録する“フィールドベース”を検討した。

提案手法を MIPS 命令セットに適用し、先行研究で定義された耐タンパ性指標を評価基準として先行研究の結果と比較を行った。まず出現頻度を考慮せず、固定の優先度で可能な限りすべての命令を位置レジスタの表現に置き換えた場合、耐タンパ性指標は最低で 6.7 % 低下した。一方、本研究で提案した貪欲法に基づき出現頻度の高い表現をもつ命令を順次その表現に変換していった場合、耐タンパ性指標は最大で 6.6 % 増加した。この耐タンパ性指標の増加は、位置レジスタを付加しない 1024 エントリの IRF において 256 エントリの増加に相当する。