

平成25年度 卒業研究報告書概要

課程, 学籍番号, 氏名	課程: 電気・電子情報 工学課程, 学籍番号: B123251, 氏名: 田中 佑		
工学分野名: 情報通信システム分野		指導教員名: 市川 周一 藤枝 直輝	
題 目: 耐タンパー性向上のための命令メモリ暗号化手法の評価 (Evaluation of instruction memory encryption for anti-tampering)			
Abstract In recent embedded systems, tamper resistance is important. Memory encryption techniques such as XOM may be used, while they require more hardware than simple techniques such as the diversification of instruction set. The performance overhead of memory encryption tends to be large, considering the resource and performance requirements in embedded systems. This study examines the instruction memory decryption for tamper resistance. The contents of instruction memory are encrypted beforehand. AES was adopted for encryption and decryption. The target processor is Plasma. A buffer is added between Plasma and an AES decryption circuit to resolve the difference of the bit width. According to the evaluation results, the hardware amount was increased by 92 [%], while the performance was reduced by 19 [%].			
概 要 近年の組み込みシステムにおいては、解析・盗用・改ざんによる情報の流出やシステムの海賊版の流布といった脅威が発生している。そのためこのような脅威に対する防御性すなわち耐タンパー性は重要性を増している。一般的に安全性の高い暗号化手法はハードウェア量が多く、性能オーバーヘッドも大きい。しかし組み込みシステムでは、ハードウェア量や性能面で厳しい制約を課せられることが多い。 澤田らは比較的簡易な耐タンパー性向上手法として、命令セットの多様化手法を提案した。この手法は、ハードウェアのコストや性能オーバーヘッドが小さい経済的な手法である。しかし、攻撃者がメモリの中身を覗き見できるような状況では安全性が低い。メモリの暗号化に関する先行研究には XOM があるが、ハードウェア量の増加に関する検討が不十分ではないかと思われる。 本研究では、メモリの暗号化による耐タンパー性向上手法を実装した。暗号化するのは命令メモリに限定し、命令列はあらかじめ暗号化されているものとする。暗号化・復号には AES を使用する。研究目的は、メモリの復号回路実装によるハードウェア量・性能の変化を測定することである。 実装方法として、OpenCores で公開されている Plasma に東北大学の青木研究室で公開されている AES による復号回路を追加した。しかし、Plasma と AES では扱うデータ幅が異なる。そこで Plasma と復号回路の間に buffer を追加し、Plasma の DRAM Controller を修正することでデータ幅が揃うようにした。また DRAM Controller から読み込まれる値が、復号すべき命令メモリなのか復号する必要がないデータメモリなのかをアドレスで判別するよう設計した。 復号回路実装前後でのハードウェア量・性能の変化を測定した。測定には Xilinx ISE 14.5 と Dhrystone ベンチマークを使用した。測定の結果、実装後はハードウェア量が 92 [%] 増加し、性能が 19 [%] 低下することが確認できた。 増加したハードウェア量の削減案として、復号回路の一部を FPGA 固有の RAM 領域で置き換える手法が考えられる。追加した復号回路の一部に多量の LUT で構成されている部分があり、その部分を RAM 領域で置き換えることができればハードウェア量の削減が見込めるのではないかとと思われる。 低下した性能を改善する案として、I/D cache の構成を再考する手法が考えられる。現時点の I/D cache ではデータメモリと命令メモリを区別していない。そこでデータメモリと命令メモリの使用領域を分割し、DRAM から命令メモリが読み出される頻度を少なくできれば、復号による性能低下を改善できるのではないかと考えられる。			

発表する際の課程を記入

電気・電子情報工学

課程

発表番号

55

(学籍が他課程所属の学生も発表する課程を記入すること)