様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　２５　日現在

機関番号：　３４３１５
研究種目：　若手研究(B)
研究期間：　2012～2014
課題番号：　２４７１０１９０

研究課題名（和文）ＬＳＩトロイ回路の対策に関する研究―社会に忍び寄るＬＳＩテロリストから人々を守る

研究課題名（英文）A study of countermeasure for Hardware Trojan

研究代表者
熊木　武志（Kumaki, Takeshi）

立命館大学・理工学部・任期制講師

研究者番号：６０４５２５９６

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：LSI開発におけるグローバリゼーションに伴い懸念されているのが，ハードウェアトロイと呼ばれる回路である．この回路は開発者の意図しない機能を持つものであり，悪意ある第三者によって仕込まれる．そして発症条件が揃うと，隠された機能が活性化し，様々な被害を及ぼす．本研究では，ハードウェアトロイ検証のために開発した実験用ボードを用いて，トリプルDESやAES暗号化回路に仕込んだハードウェアトロイについてその脅威を調べた．実験では，検証用ボードを用いたARMコアベースのSoCにおいて，暗号処理の無効化，及び秘密鍵の流出という被害を確認することができた．また，対策回路についても，基礎技術を確立した．

研究成果の概要（英文）：In recent years, several researches for hardware Trojan and its detecting method are becoming to active rapidly.The hardware Trojan is implanted as hardware modification to conventional LSIs. After a trigger, which is an activate signal to satisfy event condition occurs, hardware Trojan-implanted chips are modified the original function to enable an adversary to control, monitor, communication and so on. Thus, an adversary can disable or destroy a system, or the Trojan can leak confidential information and secret keys convertly to the adversary.
In this research, a verification board, which can execute the ARM-based SOC processing, is developed with a CPU and a FPGA. Especially, a hardware Trojan, which is implanted the cryptographic triple DES and AES circuits, is implemented in a Xilinx FPGA and is able to leak plain text and a secret-key after encrypting processing.

研究分野：　電子情報工学

キーワード：　ハードウェアトロイ　セキュリティ　組込み機器　LSI　暗号　AES　DES　FPGA

１．研究開始当初の背景

この 2～3 年，米国を中心に LSI テロリストの罠から国民生活を守るための研究が政府主導のもと活発化している．LSI テロリストはあらかじめ悪意のある回路を物理的に LSI に組み込んでおき，経済，交通，通信，及び軍事等，あらゆる面で混乱を起こそうとする．しかしながら日本では政府はもとより，半導体企業を始め，研究者においてもその脅威についての研究・対策が殆ど取られていない．

２．研究の目的

本研究は，LSI に組み込まれる悪意のある回路，「ハードウェアトロイ」の仕組みを研究するとともに，その対策回路の開発を行う．また，その成果を国内外に広く発信することで，我が国における LSI テロリスト対策推進の先駆けとする．

３．研究の方法

・平成 24 年度

諸外国の研究状況をサーベイし，暗号を利用するシステム，及びモバイル機器を対象としたハードウェアトロイを開発，また，トロイ起動条件となるトリガの研究を行う．

・平成 25 年度

前年度に開発したハードウェアトロイに対し，並列データ処理回路と連想メモリを融合したマルチメディア処理コアをベースとした対策回路を作成，その効果を確認する．

・平成 26 年度

ハードウェアトロイのターゲットを大規模インフラシステムと想定し，ハードウェアトロイ，及び対策回路のプロトタイプ実験環境製作することで被害とその対策効果を検証する．

４．研究成果

ハードウェアトロイの被害は最近ニュースや雑誌でも多く取り上げられるようになってきており，日本の論文誌でも関連の研究が見られるようになってきた．我々は重要な情報を扱う事が多いため，LSI テロリストに狙われやすく，扱う秘密情報が漏洩すると国家的な損害にも繋がる暗号回路に対してハードウェアトロイを開発し，その被害を検証した．AES と DES アルゴリズムの仕組みを利用して，クロックサイクル数に変化が無くハードウェア量の増分も数%ながら秘密鍵や平文を外部に漏えいさせることができた．また，そういったハードウェアトロイを検知することのできる監視回路を作成し，これらの代表的な暗号アルゴリズムに対してその効果を実証した．監視の仕方はテストパターンを定期的に SoC 内部の様々な回路に入力しそのレスポンスを比較するものである．なお，これらの検証には世界的はシェアを誇る ARM プロセッサと，再構成可能素子である FPGA を組み合わせたハードウェアトロイ検証用装置を開発して実機による確認を行った．本装置は ARM ベースの SoC を模擬できるものであり，特に組込み機器に仕込まれるハードウェアトロイの検証に適しているものである．また，FPGA をソケットに格納しているためリバースエンジニアリング時に仕込まれるハードウェアトロイについても検証可能である．研究実績として，雑誌論文 6 件（日本語 2 件，英語 4 件），国際学会発表 28 件，その他国内発表多数であった．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　6　件）

①熊木武志, 塚田靖史, 吉川雅弥, 小倉　武, 藤野　毅, "ハードウェアトロイ検証環境の開発と暗号回路を用いた実装及び評価," 電子情報通信学会論文誌 (A), J98-A 巻, 4 号, pp. 313-326, 2015. 査読有

②T. Kumaki, K. Nakao, K. Hozumi, T. Ogura and T. Fujino, " Development of compression tolerable and highly implementable watermarking method for mobile devices," IEICE Trans-actions on Information & Systems, Vol. E97-D, No. 3, pp. 593-596, 2014. 査読有

③T. Kumaki, T. Fujita, M. Nakanishi, and T. Ogura, " Morphological pattern spectrum and block cipher processing based image-manipulation detection," IEICE Transactions on Nonlinear theory and its applications, Vol. 4, No. 4, pp. 400-418, 2013. 査読有

④Y. Murakami, T. Honda, Y. Yanagihara, T. Kumaki, T. Ogura, and T. Fujino, " Morphological pattern spectrum-based objects detection for protecting privacy," Journal of Signal Processing, Vol. 17, No. 4, pp. 155-158, 2013. 査読有

⑤本多隼也，望月陽平，熊木武志，藤野毅，"ストリーム暗号 CryptMT のデータ並列処理による高速化手法及び SIMD 型組み込みプロセッサによる実装と評価," 電子情報通信学会論文誌 (D), J96-D 巻，3 号，pp. 495-505，2013. 査読有

⑥T. Kumaki, Y. Murakami, S. Itaya, K. Nakao, T. Ogura, and T. Fujino, " Max-plus algebra-based morphological wavelet transform watermarking for highly-parallel processing with mobile embedded processor," Journal of Signal

Processing, Vol. 16, No. 6, pp. 547-556, 2012. 査読有

〔学会発表〕(計 28 件)

① T. Kumaki, T. Fujino and T. Koide, "Interleaved-bitslice AES encryption and decryption with massive-parallel mobile embedded processor," IEEE Asia pacific Conference on Circuits and Systems (APCCAS), 2014.11.19, ANN インターコンチネンタル石垣リゾート (沖縄・石垣市)

②Y. Yanagihara, T. Honda, T. Kumaki and T. Fujino, "Live demonstration: Hierarchical masked image filtering technology on security-camera privacy protection," IEEE International Symposium on Circuits And Systems (ISCAS), 2014.6.2, メルボルン (オーストラリア)

③M. Yoshikawa, D. Takeuchi and T. Kumaki, "Reset Siganal Aware Hardware Trojan Trigger," International Conference on Advances in Engineering and Technology, 2014.3.29, Puhana (India)

④T. Hitomi, T. Honda, R. Hori, T. Kumaki and T. Fujino, "Hardware controller of camera sensor node using IR array sensor and CMOS image sensor for ultra-low-power operation,"RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2014.3.3, Hawaii (USA)

⑤K. Nakao, T. Kumaki, T. Ogura and T. Fujino, "A cropping robust digital watermarking algorithm using morphological wavelet transform based on max-plus algebra," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2014.3.3, Hawaii (USA)

⑥S. Fujimoto, T. Honda, T. Kumaki, M. Kimata and T. Fujino, "Human detection algorithm using low-resolution infrared image in wireless sensor networks," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2014.3.3, Hawaii (USA)

⑦T. Honda, K. Nakagawa, Y. Yanagihara, T. Kumaki, M. Kimata and T. Fujino, "Lightweight privacy protection in intermittent-sensing image sensor node," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2014.3.2, Hawaii (USA)

⑧T. Tokunaga, Y. Tanito, T. Kumaki, T. Fujita and T. Ogura, "L2 decomposition of adaptive directional morphological wavelet transform," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2014.3.1, Hawaii (USA)

⑨S. Sawada, T. Fujita, K. Iwanaga, T. Kumaki, M. Nakanishi and T. Ogura, "Multiple contour expansion method by CA based pixel level snakes," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2014.3.1, Hawaii (USA)

⑩M. Yoshikawa, Y. Mori and T. Kumaki, "Implementation aware Hardware Trojan Trigger," International Conference on Industrial Electronics and Applications, 2014.2.28, 杭州市 (中国)

⑪T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki and T. Fujino, "Hierarchical image-scrambling method with scramble-level controllability for privacy protection," IEEE International MidWest Symposium on Circuits And Systems (MWSCAS), 2013.8.7, Colombus (USA)

⑫K. Nakao, K. Hozumi, T. Kumaki, T. Ogura and T. Fujino, "Development of effective information-hiding method for embedded systems," IEEE International MidWest Symposium on Circuits And Systems (MWSCAS), 2013.8.7, Colombus (USA)

⑬T. Kumaki, M. Yoshikawa and T. Fujino, "Cipher-destroying and secret-key-emitting hardware Trojan against AES core," IEEE International MidWest Symposium on Circuits And Systems (MWSCAS), 2013.8.6, Colombus (USA)

⑭T. Matsui, T. Fujita, Y. Tsuji, T. Kumaki, M. Nakanishi and T. Ogura, "Evaluation of advanced pixel-level snakes on cellular hardware plat-form," IEEE International NEW circuit and systems conference on Circuits And Systems (NEWCAS), 2013.6.17, Paris (France)

⑮R. Hori, K. Nakagawa. T. Honda, T. Kumaki and T. Fujino, "Low power sensor system using smart analog under normally off operation," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2013.3.7,

Hawaii (USA)

⑯T. Honda, K. Nakagawa, T. Kumaki, M. Kimata and T. Fujino, "Development of low-power camera sensor node using infrared array sensor and CMOS image sensor," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2013.3.7, Hawaii (USA)

⑰Y. Murakami, T. Honda, Y. Yanagihara, T. Kumaki, T. Ogura and T. Fujino, "Use of morphological pattern spectrum to detect objects and protect privacy," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2013.3.6, Hawaii (USA)

⑱Y, Tanito, T. Tokunaga, M. Nawata, T. Kumaki, T. Fujita, and T. ogura, "Adaptive multi-directional morphological wavelet transform and it's compression efficiency," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2013.3.6, Hawaii (USA)

⑲ M. Yoshikawa, T. Tsukadaira and T. Kumaki, "Trojan circuit for countermeasures against fault analysis attacks," World Academy of Science, Engineering and Technology, 2013.2.14, Kuala Lumpur (Malaysia)

⑳M. Yoshikawa, R. Satoh and T. Kumaki, "Hardware Trojan for security LSI," IEEE International conference on Consumer Electronics (ICCE), 2013.1.11, Las Vegas (USA)

㉑ T. Kumaki, Z. B. Rafi'i, T. Fujita, M. Nakanishi and T. Ogura, "Morphological pattern spectrum-based image manipulation detector," International symposium on Nonlinear and its Applications (NOLTA), 2012.10.25, Palma (Spain)

㉒T. Takeda, T. Kumaki, and T. Fujino, "Highly-Parallel triple DES processing with massive-parallel SIMD matrix evaluation board," International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), 2012.7.6, 札幌コンベンションセンター (北海道・札幌市)

㉓ L. Meng, T. Kumaki, K. Yamazaki, T. Ogura, and S. Oyanagi, "A branch target address predictor for reducing the BTB miss by using CAM," IEEE symposium on low-power and high-speed chips (Cool Chips), 2012.4.18-20, 横浜情報文化センター (神奈川県・横浜市)

㉔ H. Yoshikawa, T. Kumaki, and T. Fujino, "Highly-Parallel AES processing for five confidentiality modes with massive-parallel SIMD matrix processor," Synthesis And System Integration of Mixed Information technologies (SASIMI), 2012.3.9, B-con plaza (大分県・別府市)

㉕ Y. Tsuji, T. Fujita, T. Matsui, T. Kumaki, M. Nakanishi, and T. Ogura, "An implementation of pixel level snake to cellular hardware platform," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2012.3.6, Hawaii (USA)

㉖ Z. B. Rafi'i, T. Kumaki, T. Fujita, M. Nakanishi, and T. Ogura, "Implementation results and application of real-time morphological pattern spectrum analyzer on cellular-automata hardware," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2012.3.5, Hawaii (USA)

㉗Y. Murakami, M. Osawa, S. Itaya, N. Matsumoto, K. Nakao, T. Kumaki, T. Ogura, and T. Fujino, "Highly-Parallel watermarking implementation for max-plus algebra morphological wavelet transform with massive-parallel SIMD matrix evaluation board," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2012.3.4, Hawaii (USA)

㉘M. Nawata, S. Shirai, M. Nakai, T. Kumaki, T. Fujita, and T. Ogura, "Compression efficiency study of directional morphological wavelet transform," RISP International workshop on Nonlinear Circuits, communications and Signal Processing (NCSP), 2012.3.4 , Hawaii (USA)

６．研究組織

(1)研究代表者

熊木　武志　　(Kumaki, Takeshi)
立命館大学・理工学部・任期制講師
研究者番号：60452596