T5 a low-cost side-channel disassembler that uses fine-grained EM signals to predict a program’s execution trace with high accuracy is proposed . Unlike conventional side-channel disassemblers, the proposed disassembler does not require extensive randomized instantiations of instructions to profile them . instead relying on leakage-model-informed sub-sampling of potential architectural states resulting from instruction execution . the proposed disassembler is shown to recover 97–99% of instructions from ..

Bart-Electromagnetic (EM) fields have been extensively studied as potent side-channel tools for testing the security of hardware implementations. The proposed disassembler consists of two phases: signals are collected with a relatively small EM probe, performing high-resolution scans near the chip surface. The measured signals from the numerous probe configurations are compiled into a hierarchical database by storing the min-max envelopes of the probed EM fields and differential signals derived from them, a novel dimension that increases the potency of the analysis. In the classification phase, signals measured for unknown instructions using optimal measurement configurations identified in the first phase are compared to the envelopes stored in the database to perform binary classification with majority voting, identifying candidate instruction classes at each hierarchical stage. It is shown to recover ∼97–99% of instructions from several test and application benchmark programs executed on the AT89S51 microcontroller. Back to Mail Online home. Back To the page you came from. The proposal is based on a four-stage hierarchical grouping of instructions by their length, size, operands, and functions. It uses EM signals to predict a program’s execution trace with high accuracy and is designed to be low-cost and high-accuracy. It was developed by the researchers at the University of California, San Diego, with funding from the National Institute of Standards and Technology (NIST) and the California Institute of Technology (CIT).

Gemini-This study presents a high-accuracy instruction disassembly method using electromagnetic (EM) measurements. The method employs a hierarchical classification approach to identify optimal measurement configurations and perform binary classification. It utilizes a hierarchical database of EM field envelope-to-envelope distances to differentiate instruction classes. The proposed disassembler consists of feature selection and classification phases, with each phase leveraging hierarchical grouping of instructions. This methodology enables accurate prediction of program execution traces using low-cost EM side-channel analysis, achieving a success rate of ∼97–99% in recovering instructions from various benchmark programs.

Gpt-4o-The research paper introduces a novel low-cost side-channel disassembler that leverages fine-grained electromagnetic (EM) signals to accurately predict a program’s execution trace. This innovative approach differs significantly from traditional side-channel disassemblers by eliminating the need for extensive randomized instantiations of instructions. Instead, it utilizes a leakage-model-informed sub-sampling method that captures potential architectural states resulting from instruction execution. This method is enhanced through a structured hierarchical approach, optimizing the process of instruction disassembly.

The disassembler operates in two main phases. The first phase, the feature-selection phase, involves collecting EM signals using a small EM probe that performs high-resolution scans close to the chip surface while profiling codes are executed. The signals gathered from various probe configurations are organized into a hierarchical database. This database stores the min-max envelopes of the probed EM fields and differential signals derived from these, introducing a new dimension to the analysis. The distances between these envelopes are assessed across the hierarchy to determine the optimal measurement configurations that maximize the differentiation between instruction classes.

In the second phase, the classification phase, the signals measured for unknown instructions using these optimal configurations are compared against the envelopes in the database. This comparison facilitates binary classification with majority voting, enabling the identification of candidate instruction classes at each hierarchical level. The disassembler categorizes instructions based on their length, size, operands, and functions across four hierarchical stages.

The effectiveness of this method is demonstrated through its high recovery rate of approximately 97-99% of instructions from various test and application benchmark programs executed on the AT89S51 microcontroller. This high accuracy showcases the potential of using structured, hierarchical EM signal analysis in side-channel disassembly, providing a powerful tool for security testing of hardware implementations.

Gpt-3-The research introduces a novel hierarchical classification method for accurate instruction disassembly using near-field electromagnetic (EM) measurements as a side-channel tool for hardware security testing. Unlike traditional methods, this low-cost disassembler leverages fine-grained EM signals to predict program execution traces with high precision without the need for extensive randomized instantiations. The approach involves leakage-model-informed sub-sampling of architectural states during instruction execution, enhanced by a structured hierarchical strategy. The disassembler comprises two phases: feature selection and classification. In the feature-selection phase, signals are collected using a small EM probe near the chip surface, creating a hierarchical database of min-max envelopes and differential signals to enhance analysis. The classification phase involves comparing signals from unknown instructions to stored envelopes for binary classification, employing majority voting to identify instruction classes at each hierarchical level. The disassembler employs a four-stage hierarchical grouping based on instruction length, size, operands, and functions. Experimental results demonstrate the disassembler's ability to recover approximately 97-99% of instructions from various test and application benchmark programs executed on the AT89S51 microcontroller. This innovative method showcases the potential of EM fields for precise side-channel disassembly, offering a promising approach for enhancing hardware security testing accuracy and efficiency.