# Eliminating Power Side-Channel Leaks during Register Allocation

1st Given Name Surname
*dept. name of organization (of Aff.)*
*name of organization (of Aff.)*
City, Country
email address

2nd Given Name Surname
*dept. name of organization (of Aff.)*
*name of organization (of Aff.)*
City, Country
email address

3rd Given Name Surname
*dept. name of organization (of Aff.)*
*name of organization (of Aff.)*
City, Country
email address

***Abstract*—From a finer-grained perspective, considering about the Hamming Distance model in power side channel area.**
**I. bring up the potential leakage issue under HD model which involves about both source code (front-end) and executable file (back-end)**
**II. Utilize both explicit type inference's effectiveness (high speed in calculating the set operation, precalculate) and datalog's flexibility to propagate new rules, we present a novel detection approach for locating the HD_sensitive variables, which can be applied for practical source codes rather than merely for the probabilistic boolean programs.**
**Basically, our detection part not only exploits the register allocation information from backend to achieve the accuracy, but also adopts the combined datalog and precalculation approach to successfully handle the scalability issue.**
**(Do we need to mention partition here?)**
**III. By classifying the virtual registers into HD_sensitive and normal classes, we modified the LLVM backend part to make sure that all the state transitions of the register is independent of the private input variables(*key*).**
**== Spill the HD_sensitive virtual registers into memory (tricks to avoid allocating more spaces in stack)**
**== For HD_sensitive_2 type, we guarantee to allocate differer physical registers to the pair**
**(Do we need to mention that power consumption is related with the state transitions of register (HD model definition) here?)**

***Index Terms*—component, formatting, style, styling, insert**

## I. Introduction

This document is a model and instructions for LaTeX. Please observe the conference page limits.

## II. Ease of Use

### A. Maintaining the Integrity of the Specifications

## References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.
[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
[4] K. Elissa, "Title of paper if known," unpublished.
[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove the template text from your paper may result in your paper not being published.