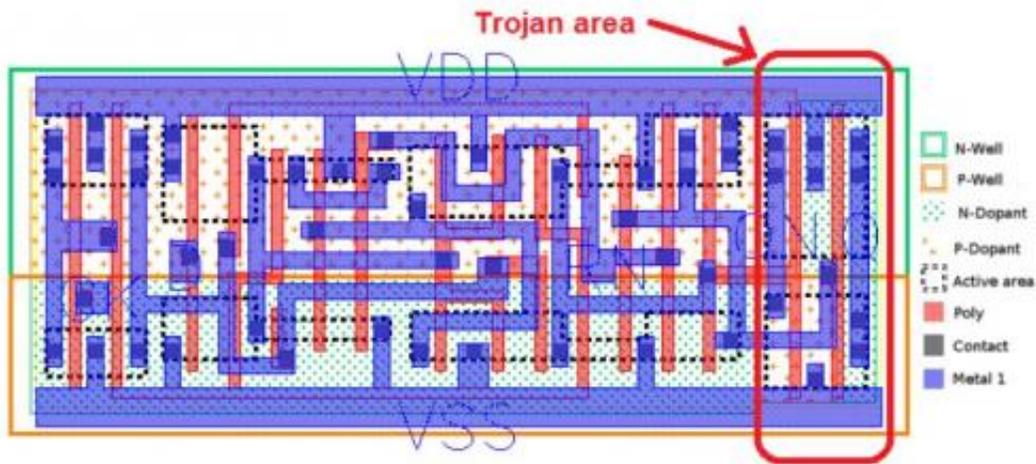


# Researchers report on hardware Trojans that are undetectable

September 19 2013, by Nancy Owano



Layout of the Trojan DFFR X1 gate. Credit: Georg T. Becker et al.

(Phys.org) —Worries that the security of integrated circuits used in critical systems by the military and industry can be compromised are all the more real with the release of a research paper titled "Stealthy Dopant-Level Hardware Trojans." The authors are a research team from United States, the Netherlands, Switzerland and Germany. They showed that integrated circuits can be maliciously compromised. The changes elude detection. Even physical inspection of the chip will not pick up the changes made. The authors discussed how they succeeded in modifying a circuit and yet detection mechanisms did not find anything amiss. The authors wrote that "we propose an extremely stealthy approach for

implementing hardware Trojans below the gate level."

Instead of adding additional circuitry to the target design, the researchers inserted their hardware Trojans by changing "the dopant polarity of existing transistors."

That way, the modified circuit nonetheless appeared as legitimate on all wiring layers, including all metal and polysilicon. The team said that their family of Trojans was resistant to most detection techniques such as fine-grain optical inspection and checks against "golden chips."

The researchers tested their Trojan on Intel's [random number generator](#) design used in Ivy Bridge processors, as well as a Side-channel Trojan.

In deciding on this second case, the authors said that, after showing how their dopant Trojan could be used to compromise the security of a real world system, they turned to the second case study, where they wanted to emphasize the flexibility of the dopant Trojan. "Instead of modifying the logic behavior of a design, the dopant Trojan is used to establish a hidden side-channel to leak out [secret keys](#)."

What do they mean by dopant? *Threatpost* [said](#) that "Dopant is a material that is added to [semiconductor material](#) that enables it to be electrically conductive." *Computerworld* explains doping as a [process](#) for modifying the electrical properties of silicon by introducing impurities such as gallium and phosphorous into the crystal. Changes made at the atomic level are difficult to detect.

Explaining their work further, the authors said that "In this paper we introduced a new type of sub-transistor level hardware Trojan that only requires modification of the dopant masks. No additional transistor gates are added and no other layout mask needs to be modified. Since only changes to the metal, [polysilicon](#) or active area can be reliably detected

with optical inspection, our dopant Trojans are immune to optical inspection."

This type of Trojan under discussion is said to pose a great challenge. The authors commented that "They set a new lower bar on how much overhead can be expected from a hardware Trojan in practice (i.e. zero!)." The authors recommended that future work should include developing new methods to detect these "sub-transistor level hardware Trojans."

**More information:** Research paper: Stealthy Dopant-Level Hardware Trojans—[people.umass.edu/gbecker/BeckerChes13.pdf](https://people.umass.edu/gbecker/BeckerChes13.pdf)

© 2013 Phys.org

Citation: Researchers report on hardware Trojans that are undetectable (2013, September 19) retrieved 19 April 2024 from <https://phys.org/news/2013-09-hardware-trojans-undetectable.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.