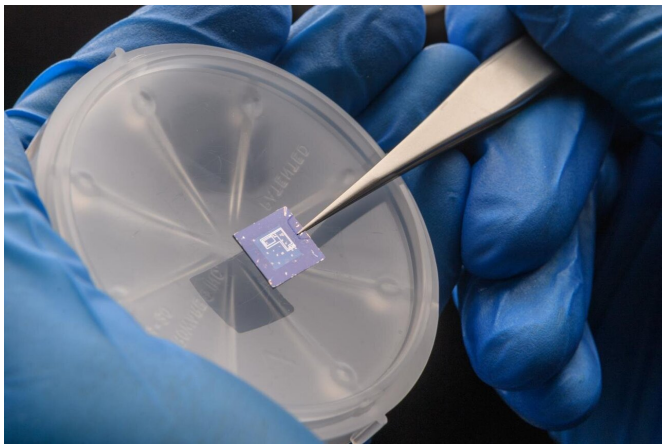
New transistor design disguises key computer chip hardware from hackers

7 December 2020



The four transistors on this chip were built out of a 2D material that disguises them from hackers. Credit: Purdue University /John Underwood

A hacker can reproduce a circuit on a chip by discovering what key transistors are doing in a circuit—but not if the transistor "type" is undetectable.

Purdue University engineers have demonstrated a way to disguise which transistor is which by building them out of a sheet-like material called black phosphorus. This built-in security measure would prevent hackers from getting enough information about the circuit to reverse engineer it.

The findings appear in a paper published Monday (Dec. 7) in *Nature Electronics*.

Reverse engineering chips is a common practice—both for hackers and companies investigating intellectual property infringement. Researchers also are developing X-ray imaging techniques that wouldn't require actually touching a chip to reverse engineer it.

The approach that Purdue researchers have demonstrated would increase security on a more fundamental level. How chip manufacturers choose to make this transistor design compatible with their processes would determine the availability of this level of security.

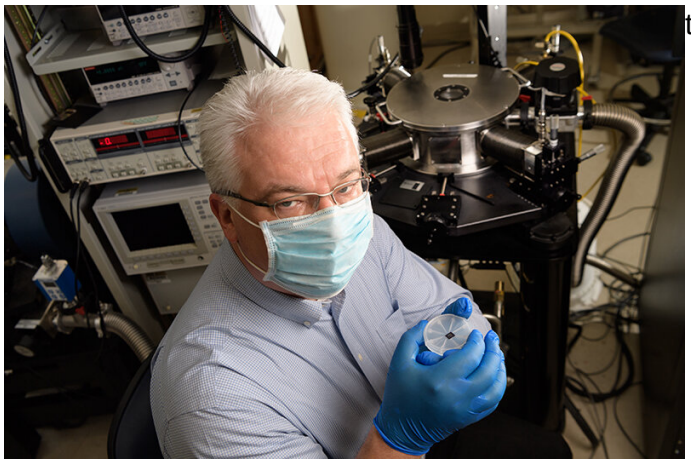
A chip computes using millions of transistors in a circuit. When a voltage is applied, two distinct types of transistors—an N type and a P type—perform a computation. Replicating the chip would begin with identifying these transistors.

"These two transistor types are key since they do different things in a circuit. They are at the heart of everything that happens on all our chips," said Joerg Appenzeller, Purdue's Barry M. and Patricia L. Epstein Professor of Electrical and Computer Engineering. "But because they are distinctly different, the right tools could clearly identify them—allowing you to go backwards, find out what each individual circuit component is doing and then reproduce the chip."

If these two transistor types appeared identical upon inspection, a hacker wouldn't be able to reproduce a chip by reverse engineering the circuit.

Appenzeller's team showed in their study that camouflaging the transistors by fabricating them from a material such as black phosphorus makes it impossible to know which transistor is which. When a voltage toggles the transistors' type, they appear exactly the same to a hacker.

While camouflaging is already a security measure that chip manufacturers use, it is typically done at the circuit level and doesn't attempt to obscure the functionality of individual transistors—leaving the chip potentially vulnerable to reverse engineering hacking techniques with the right tools.



Joerg Appenzeller, a Purdue professor of electrical and computer engineering, is developing ways to improve chip security using 2D materials. Credit: Purdue University photo/John Underwood

The camouflaging method that Appenzeller's team demonstrated would be building a security key into the transistors.

"Our approach would make N and P type transistors look the same on a fundamental level. You can't really distinguish them without knowing the key," said Peng Wu, a Purdue Ph.D. student of electrical and computer engineering who built and tested a prototype chip with black phosphorus-based transistors in the Birck Nanotechnology Center of Purdue's Discovery Park.

Not even the chip manufacturer would be able to extract this key after the chip is produced.

"You could steal the chip, but you wouldn't have the key," Appenzeller said.

Current camouflaging techniques always require more transistors in order to hide what's going on in the circuit. But hiding the transistor type using a material like black phosphorus—a material as thin as an atom—requires fewer transistors, taking up less space and power in addition to creating a better disguise, the researchers said.

The idea of obscuring the transistor type to protect chip intellectual property originally came from a theory by University of Notre Dame professor Sharon Hu and her collaborators. Typically, what gives N and P type transistors away is how they carry a current. N type transistors carry a current by transporting electrons while P type transistors use the absence of electrons, called holes.

Black phosphorus is so thin, Appenzeller's team realized, that it would enable electron and hole transport at a similar current level, making the two types of transistors appear more fundamentally the same per Hu's proposal.

Appenzeller's team then experimentally demonstrated the camouflaging abilities of black phosphorus-based transistors. These transistors are also known to operate at the low voltages of a computer chip at room temperature due to their smaller dead zone for electron transport, described as a small "band gap."

But despite the advantages of black phosphorus, the chip manufacturing industry would more likely use a different material to achieve this camouflage effect.

"The industry is starting to consider ultrathin, 2-D materials because they would allow more transistors to fit on a chip, making them more powerful. Black phosphorus is a little too volatile to be compatible with current processing techniques, but showing experimentally how a 2-D material could work is a step toward figuring out how to implement this security measure," Appenzeller said.

More information: Peng Wu et al, Two-dimensional transistors with reconfigurable polarities for secure circuits, *Nature Electronics* (2020). DOI: 10.1038/s41928-020-00511-7

Provided by Purdue University

APA citation: New transistor design disguises key computer chip hardware from hackers (2020, December 7) retrieved 9 December 2021 from https://techxplore.com/news/2020-12-transistor-disguises-key-chip-hardware.html