Any inexpensive tools to safely investigate side-channel attacks?

You are subscribed. Unsubscribe

No tags yet. + Add Tag

Sort replies by: Oldest first Newest first Most popular

Robert Watkins Signature Track . 9 days ago

With FPGA boards being somewhat inexpensive (<$100US) is it possible to use them in conjunction with a desktop system to observe side-channel attacks mentioned in the course?

If so, any tips on what equipment could be obtained simply?

0 · flag

Chuck Gollnick . 8 days ago

Near-field probes can be made for free (goggle for yourself). You'll need either a spectrum analyzer or a 'scope with FFT. With this, you can show how the EM emissions from a large IC vary over its area just with hand probing.

I remember my college days -- back when processors ran in the single-digit MHz range -- and we found that we could often tell which loop our processor was in by the buzz of its emissions as picked up by our conventional FM radio.

1 · flag

+ Comment

Hannes Tschofenig . 2 days ago

To measure power consumption you will have to buy an oscilloscope (or a cheaper version in form of the USB oscilloscope, such as those from Analog Discovery). This will, however, only get you the hardware.

It is probably better to take a look at the ChipWhisperer project (see https://www.assembla.com/spaces/chipwhisperer/wiki) where the original developer (Colin O'Flynn) also provides software to do the analysis. Without the software the learning curve would be pretty steep since you will have to write the DPA analysis code yourself. I am assuming you are interested in DPA and not SPA.

1 · flag

Nadine Goes Signature Track . an hour ago

Thank you for the reference. This is exactly what I needed.

0 · flag

+ Comment

Chuck Gollnick . 2 days ago

You could explore scan chain attacks using JTAG "dongles" and software that are available in the $50 range.

0 · flag

+ Comment

Robert Watkins Signature Track . 2 days ago

Thanks everyone for the tips! I'll dig in to see what I can find :)

↑ 0 ↓ · flag

+ Comment

New post

To ensure a positive and productive discussion, please read our forum posting policies before posting.

B | I | Link | <code> | Pic | Math | Edit: Rich | Preview

Make this post anonymous to other students

Subscribe to this thread at the same time

Add post