Journal Review Form

Manuscript # 18

Reviewer: 8

I. Describe the manuscript with just *a sentence or two* under each factor below.

1) What is the primary **focus or topic** of the manuscript?

The focus of this paper is counter measures of side-channel attacks on ICs, through various security measures taken against these attacks.

2) What is the **primary objective** of the manuscript (e.g. algorithm development, experimental verification, comparison of technique/method with other groups, improvement on prior work, characterization of device or other physical item, etc.)?

The primary objective of the manuscript is to compare different side channel attacks on an IC and methods used to protect against these attacks.

3) What **method** was used to reach the manuscript's objective?

The manuscript goes splits the review up into sections. Section 2 goes optimized design to secure differential logic gates. Section 3 describes the system level work flow and section 4 describes VLSI design flow of secure ICs. Section 5 describes the scan based attacks.

4) What **conclusion** was ultimately drawn in the manuscript?

There are various methods when looking at side channel attack resistant systems SABL, ECC, and WDDL.

5) The major **strengths** of the manuscript are . . .

Technical details as to how a certain vulnerability might operate with equations and graphical representation to back it up.

6) The major **weaknesses** of the manuscript are . . .

The conclusion did not summarize the benefits of the new methods properly

II. Rate the manuscript.

Place an X on the line next to each factor to rate the manuscript. An X close to "SD" is taken to mean that you strongly disagree with the statement, and an X close to "SA" is taken to mean that you strongly agree with the statement. If a factor is not applicable, then put a line through it. You may add comments to justify your answer or modify the measure.

Strongly Disagree						Strongly Agree	
SD:	___ :	___ :	___ :	___ :	X :	SA	The objectives of the manuscript were clear.
SD:	___ :	___ :	___ :	___ :	X :	SA	The manuscript topic is important.
SD:	___ :	___ :	___ :	X :	___ :	SA	The manuscript should be of interest to a large audience.
SD:	___ :	___ :	___ :	X :	___ :	SA	The literature review was thorough given the objectives.
SD:	___ :	___ :	___ :	X :	___ :	SA	References were complete and were appropriate.
SD:	___ :	___ :	___ :	X :	___ :	SA	The methodology was appropriate for the conclusions drawn.
SD:	___ :	___ :	___ :	X :	___ :	SA	The analysis was done correctly.
SD:	___ :	___ :	___ :	X :	___ :	SA	The results of analysis were correctly interpreted and/or conclusions were sound.
SD:	___ :	___ :	___ :	X :	___ :	SA	Tables and figures were appropriate and adequate.
SD:	___ :	___ :	___ :	___ :	X :	SA	Formatting and structure was appropriate.
SD:	___ :	___ :	___ :	X :	___ :	SA	Writing was clear and concise.
SD:	___ :	___ :	___ :	X :	___ :	SA	The manuscript was relatively free of issues of grammar, punctuation, and such.

III. Recommended disposition of the manuscript: *check one*.

_____ Do not accept for publication.

_____ Ask for major revisions and allow to again be reviewed if re-submitted.

_____ Ask for revisions and continue with a second review.

__X__ Accept with minor revisions.

_____ Accept as written with no need for any revisions.

IV. Additional questions (including technical), comments, or suggestions to be sent to the author(s):

When there is a DPA attack how does the leakage of the side channel information still accrue specifically and how well does the new methods protect against that leakage.