Eliptic Curve Digital Signature Algorithm Performance On An FPGA

Lennart Bublies
Department of Computer Engineering
University of Applied Sciences Wedel
22869 Wedel, Germany
Email: inf100434@fh-wedel.de

Leander Schulz
Department of Computer Engineering
University of Applied Sciences Wedel
22869 Wedel, Germany
Email: inf102143@fh-wedel.de

Prof. Dr. Sergei Sawitzki
Department of Computer Engineering
University of Applied Sciences Wedel
22869 Wedel, Germany
Email: saw@fh-wedel.de

This paper explains the implementation of the eliptic curve digital signature algortihm on an Altera DE2 FPGA. At first the mathematical background is described, followed by the explanation of our implementation details. We compare the performance with an optimized C implementation and achieve an improvement of XX %.

Nomenclature

A You may include nomenclature here.

α There are two arguments for each entry of the nomemclature environment, the symbol and the definition.

The primary text heading is boldface and flushed left with the left margin. The spacing between the text and the heading is two line spaces.

1 Introduction

This article illustrates preparation of ASME paper using LaTeX2ε. The LaTeX macro `asme2ej.cls`, the BibTeX style file `asmems4.bst`, and the template `asme2ej.tex` that create this article are available on the WWW at the URL address `http://iel.ucdavis.edu/code/`. To ensure compliance with the 2003 ASME MS4 style guidelines [1], you should modify neither the LaTeX macro `asme2ej.cls` nor the BibTeX style file `asmems4.bst`. By comparing the output generated by typesetting this file and the LaTeX2ε source file, you should find everything you need to help you through the preparation of ASME paper using LaTeX2ε. Details on using LaTeX can be found in [2].

In order to get started in generating a two-column version of your paper, please format the document with 0.75in top margin, 1.5in bottom margin and 0.825in left and right margins. Break the text into two sections one for the title heading, and another for the body of the paper.

The format of the heading is not critical, on the other hand formatting of the body of the text is the primary goal of this exercise. This will allow you to see that the figures are matched to the column width and font size of the paper. The double column of the heading section is set to 1.85in for the first column, a 0.5in spacing, and 4.5in for the second column. For the body of the paper, set it to 3.34in for both columns with 0.17in spacing, both are right justified.

The information that is the focus of this exercise is found in section 6. Please use this template to format your paper in a way that is similar to the printed form of the Journal of Mechanical Design. This will allow you to verify that the size and resolution of your figures match the page layout of the journal. The ASME Journal of Mechanical Design will no longer publish papers that have the errors demonstrated here.

ASME simply requires that the font should be the appropriate size and not be blurred or pixilated, and that lines should be the appropriate weight and have minimal, preferably no, pixilation or rasterization.

The journal uses 10pt Times Roman Bold for headings, but Times Bold is good enough for this effort. The text is set at 9pt Times Roman, and again Times will be fine. Insert a new line after the heading, and two lines after each section. This is not exactly right but it is close enough.

2 Very Very Very Very Very Very Very Very Very Very Very Long Heading

The heading is boldface with upper and lower case letters. If the heading should run into more than one line, the run-over is not left-flushed.

2.1 Second-Level Heading

The next level of heading is also boldface with upper and lower case letters. The heading is flushed left with the left margin. The spacing to the next heading is two line spaces.

2.1.1 Third-Level Heading.

The third-level of heading follows the style of the second-level heading.

3 Use of SI Units

An ASME paper should use SI units. When preference is given to SI units, the U.S. customary units may be given in parentheses or omitted. When U.S. customary units are given preference, the SI equivalent *shall* be provided in parentheses or in a supplementary table.

4 Footnotes[1]

Footnotes are referenced with superscript numerals and are numbered consecutively from 1 to the end of the paper[2]. Footnotes should appear at the bottom of the column in which they are referenced.

5 Mathematics

Equations should be numbered consecutively beginning with (1) to the end of the paper, including any appendices. The number should be enclosed in parentheses and set flush right in the column on the same line as the equation. An extra line of space should be left above and below a displayed equation or formula. LaTeX can automatically keep track of equation numbers in the paper and format almost any equation imaginable. An example is shown in Eqn. (1). The number of a referenced equation in the text should be preceded by Eqn. unless the reference starts a sentence in which case Eqn. should be expanded to Equation.

$$f(t) = \int_{0_+}^{t} F(t)dt + \frac{dg(t)}{dt} \tag{1}$$

6 Figures

All figures should be positioned at the top of the page where possible. All figures should be numbered consecutively and centered under the figure as shown in Fig. 1. All text within the figure should be no smaller than 7 pt. There should be a minimum two line spaces between figures and text. The number of a referenced figure or table in the text should be preceded by Fig. or Tab. respectively unless the reference starts a sentence in which case Fig. or Tab. should be expanded to Figure or Table.

[1]Examine the input file, asme2ej.tex, to see how a footnote is given in a head.

[2]Avoid footnotes if at all possible.

Fig. 1. The caption of a single sentence does not have period at the end

Fig. 2. While this figures is easily readable at a double column width of 6.5in, when it is shrunk to 3.25in column width the text is unreadable. This paper was held from production.

In the following subsections, I have inserted figures that have been provided by authors in order to demonstrate what to avoid. In each case the authors provided figures that are 3.25in wide and 600dpi in the .tif graphics format. The papers containing these figures have been held from production due to their poor quality.

6.1 The 1st Example of Bad Figure

In order to place the figure in this template using MSWord, select Insert Picture from File, and use wrapping that is top and bottom. Make sure the figure is 3.25in wide.

Figure '**??** was taken from a recent paper that was held from publication, because the text is fuzzy and unreadable. It was probably obtained by taking a screen shot of the computer output of the authors software. This means the original figure was 72dpi (dots per inch) on a computer screen. There is no way to improve the quality such a low resolution figure.

In order to understand how poor the quality of this figure is, please zoom in slightly, say to 200%. Notice that while the font of the paper is clear at this size, the font in the figures is fuzzy and blurred. It is impossible to make out the small symbol beside the numbers along the abscissa of the graph. Now consider the labels Time and Cost. They are clearly in fonts larger that the text of the article, yet the pixilation or rasterization, associated with low resolution is obvious. This figure must be regenerated at higher resolution to ensure quality presentation.

The poor quality of this figure is immediately obvious on the printed page, and reduces the impact of the research contribution of the paper, and in fact detracts from the perceived quality of the journal itself.

6.2 The 2nd Example of Bad Figure

Figure 2 demonstrates a common problem that arises when a figure is scaled down fit a single column width of 3.25in. The original figure had labels that were readable at full size, but become unreadable when scaled to half size. This figure also suffers from poor resolution as is seen in the jagged lines the ovals that form the chain.

This problem can be addressed by increasing the size of the figure to a double column width of 6.5in, so the text is readable. But this will not improve the line pixilation, and a large low resolution figure is less desirable than a small one. This also significantly expands the length of the paper, and may cause it to exceed the JMD nine page limit. Additional

Fig. 3. Another example of a figure with unreadable text. Even when the paper was expanded to double column width the text as shown in Fig. **??** was of such low quality that the paper was held from production.

Table 1. Figure and table captions do not end with a period

Example	Time	Cost
1	12.5	$1,000
2	24	$2,000

pages require page charges of $200 per page. It is best to regenerate the figure at the resolution that ensures a quality presentation.

6.3 The 3rd Example of Bad Figure

An author provided the high resolution image in Fig. 3 that was sized to a single column width of 3.25in. Upon seeing the poor quality of the text, the publisher scaled the image to double column width as shown in Fig. **??** at which point it took half of a page. The publisher went on to do this for all eight figures generating four pages of figures that the author did not expect. ASME stopped production of the paper even with the larger figures due to the pixilation of the font.

Clearly the text in this figure is unreadable, and it is doubtful that the author can print the output in a way that it is readable. This is a problem that the author must solve, not the publisher.

As you might expect, I have many more examples, but in the end the author is the best judge of what is needed in each figure. ASME simply requires that the image meet a minimum standard for font and line quality, specifically the font should be the appropriate size and not be blurred or pixilated, and that lines should be the appropriate weight and have minimal, preferably no, pixilation or rasterization.

7 Tables

All tables should be numbered consecutively and centered above the table as shown in Table 1. The body of the table should be no smaller than 7 pt. There should be a minimum two line spaces between tables and text.

8 Citing References

The ASME reference format is defined in the authors kit provided by the ASME. The format is:

> *Text Citation*. Within the text, references should be cited in numerical order according to their order of appearance. The numbered reference citation should be enclosed in brackets.

The references must appear in the paper in the order that they were cited. In addition, multiple citations (3 or more in the same brackets) must appear as a " [1-3]". A complete definition of the ASME reference format can be found in the ASME manual [1].

The bibliography style required by the ASME is unsorted with entries appearing in the order in which the citations appear. If that were the only specification, the standard BIBTEX unsrt bibliography style could be used. Unfortunately, the bibliography style required by the ASME has additional requirements (last name followed by first name, periodical volume in boldface, periodical number inside parentheses, etc.) that are not part of the unsrt style. Therefore, to get ASME bibliography formatting, you must use the `asmems4.bst` bibliography style file with BIBTEX. This file is not part of the standard BibTeX distribution so you'll need to place the file someplace where LaTeX can find it (one possibility is in the same location as the file being typeset).

With LATEX/BIBTEX, LATEX uses the citation format set by the class file and writes the citation information into the .aux file associated with the LATEX source. BIBTEX reads the .aux file and matches the citations to the entries in the bibliographic data base file specified in the LATEX source file by the `\bibliography` command. BIBTEX then writes the bibliography in accordance with the rules in the bibliography .bst style file to a .bbl file which LATEX merges with the source text. A good description of the use of BIBTEX can be found in [2, 3] (see how two references are handled?). The following is an example of how three or more references [1–3] show up using the `asmems4.bst` bibliography style file in conjunction with the `asme2ej.cls` class file. Here are some more [4–14] which can be used to describe almost any sort of reference.

9 Conclusions

The only way to ensure that your figures are presented in the ASME Journal of Mechanical Design in the way you feel is appropriate and meets the requirement for quality presentation is for you to prepare a double column version of the paper in a form similar to that used by the Journal.

This gives you the opportunity to ensure that the figures are sized appropriately, in particular that the labels are readable and match the size of the text in the journal, and that the line weights and resolutions have no pixilation or rasterization. Poor quality figures are immediately obvious on the printed page, and this detracts from the perceived quality of the journal.

I am pleased to provide advice on how to improve any figure, but this effort must start with a two-column version of the manuscript. Thank you in advance for your patience with this effort, it will ensure quality presentation of your research contributions.

10 Discussions

This template is not yet ASME journal paper format compliant at this point. More specifically, the following fea-

tures are not ASME format compliant.

1. The format for the title, author, and abstract in the cover page.
2. The font for title should be 24 pt Helvetica bold.

If you can help to fix these problems, please send us an updated template. If you know there is any other non-compliant item, please let us know. We will add it to the above list. With your help, we shall make this template compliant to the ASME journal paper format.

Acknowledgements

ASME Technical Publications provided the format specifications for the Journal of Mechanical Design, though they are not easy to reproduce. It is their commitment to ensuring quality figures in every issue of JMD that motivates this effort to have authors review the presentation of their figures.

Thanks go to D. E. Knuth and L. Lamport for developing the wonderful word processing software packages TEX and LATEX. We would like to thank Ken Sprott, Kirk van Katwyk, and Matt Campbell for fixing bugs in the ASME style file `asme2ej.cls`, and Geoff Shiflett for creating ASME bibliography stype file `asmems4.bst`.

References

[1] ASME, 2003. *ASME Manual MS-4, An ASME Paper*, latest ed. The American Society of Mechanical Engineers, New York. See also URL `http://www.asme.org/pubs/MS4.html`.

[2] Lamport, L., 1986. *LATEX: a Document Preparation System*. Addison-Wesley, Reading, MA.

[3] Goosens, M., Mittelbach, F., and Samarin, A., 1994. *The LATEX Companion*. Addison-Wesley, Reading, MA.

[4] Author, A., Author, B., and Author, C., 1994. "Article title". *Journal Name,* **1**(5), May, pp. 1–3.

[5] Booklet, A., 1994. Booklet title. On the WWW, at `http://www.abc.edu`, May. PDF file.

[6] Inbook, A., ed., 1991. *Book title*, 1*st* ed., Vol. 2 of *Series Title*. Publisher Name, Publisher address, Chap. 1, pp. 1–3. See also URL `http://www.abc.edu`.

[7] Incollection, A., 1991. "Article title". In *Collection Title*, A. Editor, ed., 3*rd* ed., Vol. 2 of *Series title*. Publisher Name, Publisher address, May, Chapter 1, pp. 1–3. See also URL `http://www.abc.edu`.

[8] Inproceedings, A., 1991. "Article title". In Proceedings Title, A. Editor and B. Editor, eds., Vol. **1** of *Series name*, Organization Name, Publisher Name, pp. 1–3. Paper number 1234.

[9] Mastersthesis, A., 2003. "Thesis Title". MS Thesis, University of Higher Education, Cambridge, MA, May. See also URL `http://www.abc.edu`.

[10] Misc, A., 2003. Miscellaneous Title. On the WWW, May. URL `http://www.abc.edu`.

[11] Proceedings, A., ed., 1991. Volume Title, Vol. 1 of *Proceedings Series*, Organization Name, Publisher Name. See also URL `http://www.abc.edu`.

[12] Phdthesis, A., 2003. "Thesis Title". PhD Thesis, University of Higher Education, Cambridge, MA, May. See also URL `http://www.abc.edu`.

[13] Techreport, A., 2003. Techreport title. Progress report 1, University of Higher Education, Cambridge, MA, May. See also URL `http://www.abc.edu`.

[14] Unpublished, A., 2003. Unpublished document title. See also URL `http://www.abc.edu`, May.

Appendix A: Head of First Appendix

Avoid Appendices if possible.

Appendix B: Head of Second Appendix

Subsection head in appendix

The equation counter is not reset in an appendix and the numbers will follow one continual sequence from the beginning of the article to the very end as shown in the following example.

$$a = b + c. \tag{2}$$