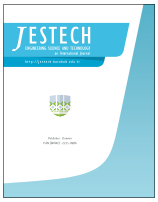
HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: www.elsevier.com/locate/jestch



Preprint Submitted to Elsevier

A Simulated Firmware Study on X86, ARM, RISC-V Platform and Security Enhancement For RISC-V

Loo, Tung Lun[a,b], Mohamad Khairi Ishak[b,b]

[a] Sungai Petani, 08000 Kedah, Malaysia
[b] USM, Malaysia

ARTICLE INFO

Article history:
Received 27 July 2021
Revised xx Month 2021
Accepted xx Month 2021
Available online xx Month 2021

Keywords:
RISC-V
Security
Firmware

ABSTRACT

In the era of Internet of Things, the number of connected embedded device went beyond 10 billion in 2020 and projected to hit 30 billion in 2025. All these active connected devices create a stronger market demand to the servers in the cloud. In 2019, COVID pandemic hit the world and caused a rise of demand for client devices, such as personal laptop and desktops, for remote education purpose. A well-defined bootloader chosen upon different ISA solution will ease the development process and shorten time to market, without jeopardizing security. As such, a study on bootloaders architecture, solutions, and security plays an important role in implementation the compute devices solutions today. There are many well-known open-source bootloaders solutions available today with long development and deployment history, such as UEFI/BIOS, Coreboot and Uboot. Recently, RISC-V as an open-source Instruction Set Architecture also gain a lot of fame in products creation and academic research purpose. In this paper, all Instruction Set Architecture boot flow, boot solutions and their associated security activities are studied, summarized, and experimented. A new proposed method to create a security block in Register Transfer Level to generate Secure Hash Algorithms 5 digest is also implemented using Field Programmable Gate Array. The tradeoff analysis here includes the numbers of logic required and boot time penalty comparison of running Secure Hash Algorithms 5 in bootloader and Register Transfer Level. With the proposed hardware implementation, it is observed that there is significant performance boost compared to software execution.

1. Introduction

All compute devices today are powered by a few processors Instruction Set Architectures (ISAs), predominantly x86, AMD, ARM, and MIPS which is later converged to RISC-V in 2021 (Jim Turley, EE Journal, 2021). These ISAs provide flexibilities and extensibilities to the different engineering audiences, creating tremendous opportunities today that benefits consumer in many custom applications and use cases, especially in the booming edge devices in Internet of Things world. While having multiple ISA options are good, it is often difficult to make a good decision on which architecture to go for, because there are many factors that contribute to design decision. Several key elements of consideration while picking an ISA are as below. 1. Time-To-Market (TTM) The TTM factor is about how easy it is to enable an embedded system with collaterals provided by the ISA provider. For example, the development time of an engineering team (often called OEM/ODM) taking a new 11th Generation Intel chip and providing a full solution with it. Several key factors that directly impact TTM are the availabilities of documentation, system level open-source references and manufacturing technology.2 2. Cost This factor includes cost of licensing, software, and hardware development cost that the OEM/ODM needs to pay to get the products released. 3. Design flexibilities The design flexibilities revolve around two key questions of "How easy it is to include a new custom IP in a new design?" and "How easy it is to land firmware, driver, and software support of a new IP?"

2. Installation

The package is available at author resources page at Elsevier http://www.elsevier.com/locate/latex/. The class may be moved or copied to a place, usually, `$TEXMF/tex/latex/elsevier/`, or a folder which will be read by LaTeX during document compilation. The TeX file database needs updation after moving/copying class file. Usually, we use commands like `mktexlsr` or `texhash` depending upon the distribution and operating system.

2.1. Subsection of Installation

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus

https://doi.org/xx.xxxx/j.jestch.20xx.xx.xxx

Fig. 1. Caption place holder.

a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

2.1.1. Subsubsection of Installation

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Installation Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

3. Front matter

The author names and affiliations could be formatted in two ways:

(1) Group the authors per affiliation.
(2) Use footnotes to indicate the affiliations.

See the front matter of this document for examples. You are recommended to conform your choice to the journal you are submitting to. Several figure, section, table representation examples are given as: Fig. 2(a) and (b). This is Section 2.1.1. Figure and table referencing can be given as Fig. 1 and Table 1. Two consecutive figures can be written as Figs. 1 and 2 or Figs. 1 and 2.

Table 1
This is a test caption. This is a test caption. This is a test caption. This is a test caption.

Col 1	Col 2	Col 3	Col4
12345	12345	123	12345
12345	12345	123	12345
12345	12345	123	12345
12345	12345	123	12345
12345	12345	123	12345

4. Bibliography styles

There are various bibliography styles available. You can select the style of your choice in the preamble of this document. These styles are Elsevier styles based on standard styles like Harvard and Vancouver. Please use BibTeX to generate your bibliography and include DOIs in URL style whenever available.

Here are four sample references: [1] [1, 2] [1, 3] [1–11].

5. Floats

Figures may be included using the command, `\includegraphics` in combination with or without its several options to further control graphic. `\includegraphics` is provided by graphic[s,x].sty which is part of any standard LaTeX distribution. graphicx.sty is loaded by default. LaTeX accepts figures in the postscript format while pdfLaTeX accepts *.pdf, *.mps (metapost), *.jpg and *.png formats. pdfLaTeX does not accept graphic files in the postscript format.

The `table` environment is handy for marking up tabular material. If users want to use multirow.sty, array.sty, etc., to fine control/enhance the tables, they are welcome to load any package of their choice and cas-dc.cls will work in combination with all loaded packages.

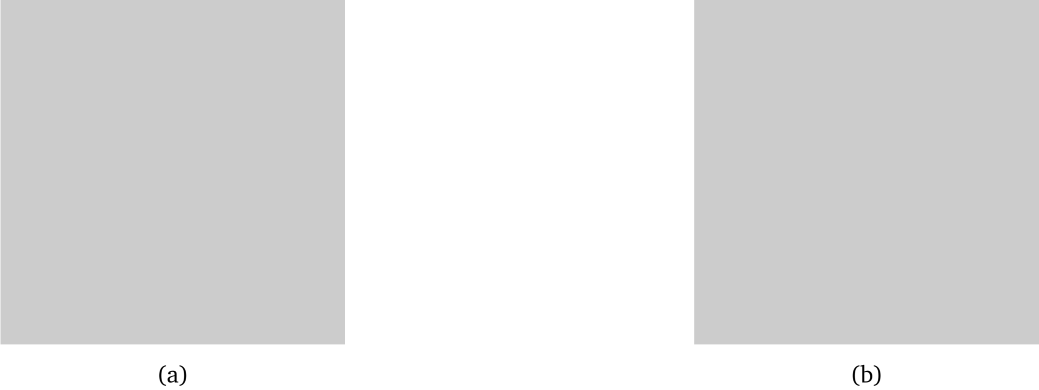
6. Theorem and theorem like environments

cas-dc.cls provides a few shortcuts to format theorems and theorem-like environments with ease. In all commands, the options that are used with the `\newtheorem` command will work exactly in the same manner. cas-dc.cls provides three commands to format theorem or theorem-like environments:

```
\newtheorem{theorem}{Theorem}
\newtheorem{lemma}[theorem]{Lemma}
\newdefinition{rmk}{Remark}
\newproof{pf}{Proof}
\newproof{pot}{Proof of Theorem \ref{thm2}}
```

The `\newtheorem` command formats a theorem in LaTeX's default style with italicized font, bold font for theorem heading and theorem number at the right hand side of the theorem heading. It also optionally accepts an argument which will be printed as an extra heading in parentheses.

```
\begin{theorem}
 For system (8), consensus can be achieved with
 $\|T_{\omega z}$ ...
   \begin{eqnarray}\label{10}
   ....
   \end{eqnarray}
\end{theorem}
```



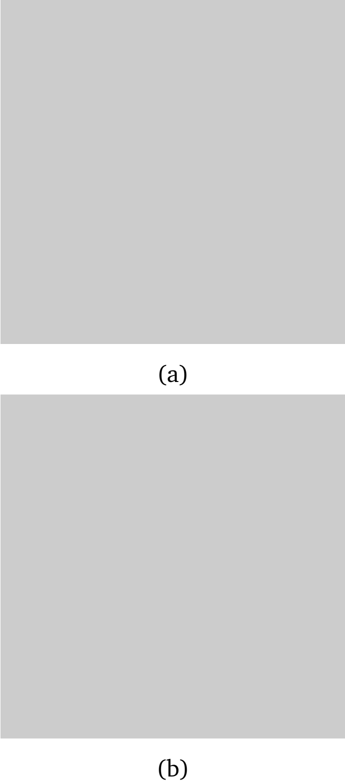
(a)

(b)

Fig. 2. (a) First subfigure, and (b) second subfigure. Caption place holder. This is the subfigure landscape example on double column.

Table 2
This is a test caption. This is a test caption. This is a test caption. This is a test caption.

Col 1	Col 2	Col 3	Col4	Col5	Col6	Col7
12345	12345	123	12345	123	12345	123
12345	12345	123	12345	123	12345	123
12345	12345	123	12345	123	12345	123
12345	12345	123	12345	123	12345	123
12345	12345	123	12345	123	12345	123



(a)

(b)

Fig. 3. Put your caption here. This is the subfigure example on single column.

Theorem 1. *For system (8), consensus can be achieved with* $\|T_{\omega z}$ ...

$$\lambda_{1S}/2\pi\,(\epsilon_{Cu2O}-1)^{1/2} = 414\,\mathring{A} \gg a_B = 4.6\,\mathring{A} \tag{1}$$

The `\newdefinition` command is the same in all respects as its `\newtheorem` counterpart except that the font shape is roman instead of italic. Both `\newdefinition` and `\newtheorem` commands automatically define counters for the environments defined.

Fig. 4. The evanescent light - $1S$ quadrupole coupling ($g_{1,l}$) scaled to the bulk exciton-photon coupling ($g_{1,2}$). The size parameter kr_0 is denoted as x and the PMS is placed directly on the cuprous oxide sample ($\delta r = 0$, See also Fig. 3).

The `\newproof` command defines proof environments with upright font shape. No counters are defined.

Theorem 2. *The* WGM *evanescent field penetration depth into the cuprous oxide adjacent crystal is much larger than the* QE *radius:*

$$\lambda_{1S}/2\pi\,(\epsilon_{Cu2O}-1)^{1/2} = 414\,\mathring{A} \gg a_B = 4.6\,\mathring{A}$$

Definition 1. The bulk and evanescent polaritons in cuprous oxide are formed through the quadrupole part of the light-matter interaction:

$$H_{int} = \frac{ie}{m\omega_{1S}}\mathbf{E}_{i,s}\cdot\mathbf{p}$$

Fig. 5. Schematic of formation of the evanescent polariton on linear chain of PMS. The actual dispersion is determined by the ratio of two coupling parameters such as exciton-WGM coupling and WGM-WGM coupling between the microspheres.

$$\lambda_{1S}/2\pi\left(\epsilon_{Cu2O}-1\right)^{1/2} = 414\ \text{Å} \gg a_B = 4.6\ \text{Å} \tag{2}$$

$$y_t = \phi_1 y_{t-1} + \epsilon_t \tag{3}$$

$$R_0 = 0 \tag{4a}$$

$$N_0 = 0 \tag{4b}$$

$$D\left(C_A, C_B\right) = \min X_A \in C_A, X_B \in C_B d\left(X_A, X_B\right) \tag{5}$$

$$y_t = \phi_1 y_{t-1} + \epsilon_t \tag{6}$$

PROOF OF THEOREM 2. The photon part of the polariton trapped inside the PMS moves as it would move in a micro-cavity of the effective modal volume $V \ll 4\pi r_0^3/3$. Consequently, it can escape through the evanescent field. This evanescent field essentially has a quantum origin and is due to tunneling through the potential caused by dielectric mismatch on the PMS surface. Therefore, we define the *evanescent* polariton (EP) as an evanescent light - QE coherent superposition as in Eq. (2). Eq. (6) can be referenced in this form. Multiple equations can be represented as in Eqs. (5) and (6). Multiple consecutive equations can be shown as Eqs. (3)–(6).

7. Enumerated and Itemized Lists

cas-dc.cls provides an extended list processing macros which makes the usage a bit more user friendly than the default LaTeX list macros. With an optional argument to the `\begin{enumerate}` command, you can change the list counter type and its attributes. If you would like to use classical enumeration/itemize styles, you may comment out "Customized Enumeration" section in the cas-common.sty file and use `\usepackage{enumerate}` or `\usepackage{enumitem}` that can be added to the cas-dc.cls file instead.

```
\begin{enumerate}[1.]
\item The enumerate environment starts with an optional
  argument `1.', so that the item counter will be suffixed
  by a period.
\item You can use `a)' for alphabetical counter and '(i)'
 for roman counter.
 \begin{enumerate}[a)]
   \item Another level of list with alphabetical counter.
   \item One more item before we start another.
   \item One more item before we start another.
   \item One more item before we start another.
   \item One more item before we start another.
```

Further, the enhanced list environment allows one to prefix a string like ‘step’ to all the item numbers.

```
\begin{enumerate}[Step 1.]
 \item This is the first step of the example list.
 \item Obviously this is the second step.
 \item The final step to wind up this example.
\end{enumerate}
```

(1) The enumerate environment starts with an optional argument ‘1.’ so that the item counter will be suffixed by a period as in the optional argument.

(2) If you provide a closing parenthesis to the number in the optional argument, the output will have closing parenthesis for all the item counters.

(3) You can use ‘(a)’ for alphabetical counter and ’(i)’ for roman counter.
   - a) Another level of list with alphabetical counter.
   - b) One more item before we start another.
      - (i) This item has roman numeral counter.
      - (ii) Another one before we close the third level.
   - c) Third item in second level.

(4) All list items conclude with this step.

8. Cross-references

In electronic publications, articles may be internally hyperlinked. Hyperlinks are generated from proper cross-references in the article. For example, the words Fig. 1 will never be more than simple text, whereas the proper cross-reference `\ref{tiger}` or `\Cref{tiger}` may be turned into a hyperlink to the figure itself: Fig. 1. In the same way, the words Ref. [1] will fail to turn into a hyperlink; the proper cross-reference is `\cite{Knuth96}`. Cross-referencing is possible in LaTeX for sections, subsections, formulae, figures, tables, and literature references.

9. Bibliography

Two bibliographic style files (`*.bst`) are provided — model1-num-names.bst, model2-names.bst, and elsarticle-num.bst — the first one can be used for the numbered scheme. This can also be used for the numbered with new options of natbib.sty. The second one is for the author year scheme. When you use model2-names.bst, the citation commands will be like `\citep`, `\citet`, `\citealt` etc. However when you use model1-num-names.bst, you may use only `\cite` command. The third one is used in this template which is resembling to the final layout.

`thebibliography` environment. Each reference is a `\bibitem` and each `\bibitem` is identified by a label, by which it can be cited in the text:

In connection with cross-referencing and possible future hyperlinking, it is not a good idea to collect more that one literature item in one `\bibitem`. The so-called Harvard or author-year style of referencing is enabled by the LaTeX package natbib. With this package the literature can be cited as follows:

- Parenthetical: `\citep{WB96}` produces (Wettig & Brown, 1996).
- Textual: `\citet{ESG96}` produces Elson et al. (1996).
- An affix and part of a reference: `\citep[e.g.][Ch. 2]{Gea97}` produces (e.g. Governato et al., 1997, Ch. 2).

In the numbered scheme of citation, `\cite{<label>}` is used, since `\citep` or `\citet` has no relevance in the numbered scheme. natbib package is loaded by cas-dc with `numbers` as default option. You can change this to author-year or harvard scheme by adding option `authoryear` in the class loading command. If you want to use more options of the natbib package, you can do so with the `\biboptions` command. For details of various options of the natbib package, please take a look at the natbib documentation, which is part of any standard LaTeX installation.

10. Conclusion

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Appendix A

Appendix sections are coded under `\appendix`.

`\printcredits` command is used after appendix sections to list author credit taxonomy contribution roles tagged using `\credit` in frontmatter.

A.1 Subsection of appendix a

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Eq. (A.1) can be referenced in this form in the Appendix A.

$$y_t = \phi_1 y_{t-1} + \epsilon_t \tag{A.1}$$

A.1.1 Subsubsection of appendix a

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Declaration of competing interest / Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors would like to thank the editors and anonymous reviewers for providing insightful suggestions and comments to improve the quality of research paper.

References

[1] S. Fortunato, Community detection in graphs, Phys. Rep.-Rev. Sec. Phys. Lett. 486 (2010) 75–174. URL: http://dx.doi.org/10.1016/j.physrep.2009.11.002.

[2] M.E.J. Newman, M. Girvan, Finding and evaluating community structure in networks, Phys. Rev. E. 69 (2004) 026113. URL: https://doi.org/10.1103/PhysRevE.69.026113.

[3] C. Vehlow, T. Reinhardt, D. Weiskopf, Visualizing fuzzy overlapping communities in networks, IEEE Trans. Vis. Comput. Graph. 19 (2013) 2486–2495. URL: https://doi.org/10.1109/TVCG.2013.232.

[4] Q. Chen, T.T. Wu, M. Fang, Detecting local community structure in complex networks based on local degree central nodes, Physica A. 392 (2013) 529–537.

[5] A. Clauset, M.E.J. Newman, C. Moore, Finding community structure in very large networks, Phys. Rev. E. 70 (2004) 066111.

[6] B. Fabricio, Z. Liang, Fuzzy community structure detection by particle competition and cooperation, Soft Comput. 17 (2013) 659–673.

[7] S. Gregory, Fuzzy overlapping communities in networks, J. Stat. Mech.-Theory Exp. (2011) P02017.

[8] S. Fortunato, M. Barthelemy, Resolution limit in community detection, Proc. Natl. Acad. Sci. U. S. A. 104 (2007) 36–41.

[9] E. Hullermeier, M. Rifqi, A fuzzy variant of the rand index for comparing clustering structures, in: in Proc. IFSA/EUSFLAT Conf., 2009, pp. 1294–1298.

[10] T. Nepusz, A. Petróczi, L. Négyessy, F. Bazsó, Fuzzy communities and the concept of bridgeness in complex networks, Phys. Rev. E. 77 (2008) 016107.

[11] M.E.J. Newman, Network data, http://www-personal.umich.edu/~mejn/netdata/ (2013).