



Foundational Integration Verification of a Cryptographic Server

ANDRES ERBSEN, Google, USA

JADE PHILIPOOM, Google, Germany

DUSTIN JAMNER, Massachusetts Institute of Technology, USA

ASHLEY LIN, Massachusetts Institute of Technology, USA

SAMUEL GRUETTER, Massachusetts Institute of Technology, USA

CLÉMENT PIT-CLAUDEL, EPFL, Switzerland

ADAM CHLIPALA, Massachusetts Institute of Technology, USA

We present verification of a bare-metal server built using diverse implementation techniques and languages against a whole-system input-output specification in terms of machine code, network packets, and mathematical specifications of elliptic-curve cryptography. We used very different formal-reasoning techniques throughout the stack, ranging from computer algebra, symbolic execution, and verification-condition generation to interactive verification of functional programs including compilers for C-like and functional languages. All these component specifications and domain-specific reasoning techniques are defined and justified against common foundations in the Coq proof assistant. Connecting these components is a minimalistic specification style based on functional programs and assertions over simple objects, omniseantics for program execution, and basic separation logic for memory layout. This design enables us to bring the components together in a top-level correctness theorem that can be audited without understanding or trusting the internal interfaces and tools. Our case study is a simple cryptographic server for flipping of a bit of state through public-key authenticated network messages, and its proof shows total functional correctness including static bounds on memory usage. This paper also describes our experiences with the specific verification tools we build upon, along with detailed analysis of reasons behind the widely varying levels of productivity we experienced between combinations of tools and tasks.

CCS Concepts: • **Software and its engineering** → **Formal software verification**; **Semantics**; *Integration frameworks*; • **Security and privacy** → **Public key (asymmetric) techniques**.

Additional Key Words and Phrases: proof assistants, elliptic-curve cryptography, bare-metal programming

ACM Reference Format:

Andres Erbsen, Jade Philipoom, Dustin Jamner, Ashley Lin, Samuel Gruetter, Clément Pit-Claudel, and Adam Chlipala. 2024. Foundational Integration Verification of a Cryptographic Server. *Proc. ACM Program. Lang.* 8, PLDI, Article 216 (June 2024), 26 pages. <https://doi.org/10.1145/3656446>

1 INTRODUCTION

Formal verification can conclusively rule out deviations of a software component from its formal specification, and highly automated and effective verification tools are available for specific implementation and specification formats. However, specifications of computer-systems components

Authors' addresses: [Andres Erbsen](#), Google, Cambridge, USA; [Jade Philipoom](#), Google, Berlin, Germany; [Dustin Jamner](#), Massachusetts Institute of Technology, Cambridge, USA; [Ashley Lin](#), Massachusetts Institute of Technology, Cambridge, USA; [Samuel Gruetter](#), Massachusetts Institute of Technology, Cambridge, USA; [Clément Pit-Claudel](#), EPFL, Lausanne, Switzerland; [Adam Chlipala](#), Massachusetts Institute of Technology, Cambridge, USA.



This work is licensed under a Creative Commons Attribution 4.0 International License.

© 2024 Copyright held by the owner/author(s).

ACM 2475-1421/2024/6-ART216

<https://doi.org/10.1145/3656446>

$\mathbb{R}^n$ is a vector space over $\mathbb{R}$. The inner product $\langle \cdot, \cdot \rangle$ is defined by

$$\langle x, y \rangle = \sum_{i=1}^n x_i y_i.$$

The function $f: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$f(x) = \sum_{i=1}^n x_i^2.$$
 The function $g: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$g(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4.$$
 The function $h: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$h(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6.$$
 The function $k: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$k(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8.$$
 The function $l: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$l(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10}.$$

The function $m: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$m(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12}.$$
 The function $n: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$n(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12} + \sum_{i=1}^n x_i^{14}.$$
 The function $o: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$o(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12} + \sum_{i=1}^n x_i^{14} + \sum_{i=1}^n x_i^{16}.$$
 The function $p: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$p(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12} + \sum_{i=1}^n x_i^{14} + \sum_{i=1}^n x_i^{16} + \sum_{i=1}^n x_i^{18}.$$
 The function $q: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$q(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12} + \sum_{i=1}^n x_i^{14} + \sum_{i=1}^n x_i^{16} + \sum_{i=1}^n x_i^{18} + \sum_{i=1}^n x_i^{20}.$$

We define the function $r: \mathbb{R}^n \rightarrow \mathbb{R}$ by

$$r(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12} + \sum_{i=1}^n x_i^{14} + \sum_{i=1}^n x_i^{16} + \sum_{i=1}^n x_i^{18} + \sum_{i=1}^n x_i^{20} + \sum_{i=1}^n x_i^{22}.$$
 The function $s: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$s(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12} + \sum_{i=1}^n x_i^{14} + \sum_{i=1}^n x_i^{16} + \sum_{i=1}^n x_i^{18} + \sum_{i=1}^n x_i^{20} + \sum_{i=1}^n x_i^{22} + \sum_{i=1}^n x_i^{24}.$$

The function $t: \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by

$$t(x) = \sum_{i=1}^n x_i^2 + \sum_{i=1}^n x_i^4 + \sum_{i=1}^n x_i^6 + \sum_{i=1}^n x_i^8 + \sum_{i=1}^n x_i^{10} + \sum_{i=1}^n x_i^{12} + \sum_{i=1}^n x_i^{14} + \sum_{i=1}^n x_i^{16} + \sum_{i=1}^n x_i^{18} + \sum_{i=1}^n x_i^{20} + \sum_{i=1}^n x_i^{22} + \sum_{i=1}^n x_i^{24} + \sum_{i=1}^n x_i^{26}.$$

1 We f... h d h k... b Q
 g... P n g b p... 6 a p
 w s h... f... [] h... b
 d f... .

2 h... 6 in... 6
 h... 6 in... 6
 g... 6 h... 6
 M... f... a... *a a... in an
 w... a... f... a...
 f... h...

3 O is... 6... a in... []
 h... 6 n... f... is... on... b... b
 The... f... 6 eff... f... h...
 a... in... 6... f... 6 h... Thus h
 f... a... in... h... f... in... is
 often... f... h... a... a...
 ,... d... d... f... 6 h...
 s... a a p... h... h...
 h... f... 6 a... h d f... f... h... . s... h t...
 .

3

We h... in... h

We h... 6... in a... b... 6
 h... p... o h... C's... a...
 " " s n : / s : R B : >
 { m = m * s s * B ^ m * d d * R ^
 s = n > Z ^ d = n > Z ^ n < 3
 t' m = m * s d s * R ^ t ' }

The... h... a... a... h... b
 a... 6... d... h... h...
 e... h... f... h... , h... f... h...
 f... f... (R... B) in... h...
 (m *) al... h... R... h... h... is... in...
 h... h... is... R... (of) h... h... in...
 e... h... is... o... The... h... B... is... in...
 b... h... h... We... h... a m *
 s... h... f... s... s * B... h...
 h... f... h... d... h...
 d... h... f... in... a... h... a...
 h... h... h... is... ,
 g... h... f... h... h... a... d...
 h... dst = src, s... f... d = s... R s = R. h... h...
 h... h... a... h... f... h...
 Ye... h... h... h... h... h...
 h... 6... h... h... h... h... h...
 h... h... h... h... h... h... h...

⁴The... 6... f... is... h... a... h... h... h... h...
 h... h... h... h... h... h... h... h... h... h...

$$f(e) = \{ \{ l = 0 \} \} \cup \{ \{ p = p + \$ \quad l = l - \$ \} \}$$

H k n a ~~del~~ æ h n j n , b t t g n
 u n j n k ~~del~~ b l v s n æ l h
 O t e T l v h g n æ l n n h T p l s h a ~~del~~ æ l
 n h j n f i n n h æ f l o w 6 h j n h l y k p l s 6
 d f i d l o , æ h b n n æ l s i g j n l 6 n æ v
 (f i d y , ~~del~~ æ h l v h p k g n æ l æ h æ æ l æ l
 h æ b ~~del~~ f n n 2)

[illegible]

We find that the probability of a subject being in the 'b' category is significantly higher than the probability of a subject being in the 'a' category. The mean value for the 'b' category is 6.7, while the mean value for the 'a' category is 6.1. The difference between the two means is 0.6, which is statistically significant at the 0.05 level.

After the period of the 18th century, the English language has been enriched by a large number of words from other languages, especially from French, Latin, and Greek. This process of borrowing has continued to the present day, and it is one of the main reasons why the English language is so rich and varied.

[illegible]

6 h 10 al d h 10
 6 h 10 al d h 10
 6 h 10 al d h 10
 6 h 10 al d h 10

14

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10
 14 h 10 al d h 10

1. In the first part of the book, the author discusses the importance of understanding the cultural context of the text. This is particularly relevant in the study of ancient texts, where the cultural background of the authors and the audience can significantly influence the interpretation of the text.

2. The second part of the book focuses on the linguistic analysis of the text. This involves a detailed examination of the vocabulary, grammar, and syntax of the text. The author provides a comprehensive overview of the linguistic features of the text, which is essential for a thorough understanding of the text.

3. The third part of the book deals with the historical context of the text. This includes a discussion of the historical events and figures that are mentioned in the text. The author provides a detailed account of the historical background of the text, which is crucial for a proper understanding of the text.

4. The fourth part of the book is devoted to the literary analysis of the text. This involves a close reading of the text, paying attention to the literary devices and techniques used by the author. The author provides a detailed analysis of the literary features of the text, which is essential for a thorough understanding of the text.

5. The fifth part of the book is a conclusion, where the author summarizes the findings of the study. The author provides a comprehensive overview of the results of the study, which is essential for a thorough understanding of the text.

6. The sixth part of the book is a bibliography, where the author lists the sources used in the study. This is a standard feature of academic writing, and it provides a clear and concise list of the sources used in the study.

7. The seventh part of the book is an index, where the author lists the topics covered in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the topics covered in the book.

8. The eighth part of the book is a glossary, where the author defines the key terms used in the book. This is a standard feature of academic writing, and it provides a clear and concise definition of the key terms used in the book.

9. The ninth part of the book is a list of abbreviations, where the author lists the abbreviations used in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the abbreviations used in the book.

10. The tenth part of the book is a list of footnotes, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the footnotes used in the book.

11. The eleventh part of the book is a list of references, where the author lists the references used in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the references used in the book.

12. The twelfth part of the book is a list of appendices, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the appendices used in the book.

13. The thirteenth part of the book is a list of figures, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the figures used in the book.

14. The fourteenth part of the book is a list of tables, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the tables used in the book.

15. The fifteenth part of the book is a list of charts, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the charts used in the book.

16. The sixteenth part of the book is a list of maps, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the maps used in the book.

17. The seventeenth part of the book is a list of photographs, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the photographs used in the book.

18. The eighteenth part of the book is a list of videos, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the videos used in the book.

19. The nineteenth part of the book is a list of audio files, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the audio files used in the book.

20. The twentieth part of the book is a list of other resources, where the author provides additional information on the topics discussed in the book. This is a standard feature of academic writing, and it provides a clear and concise list of the other resources used in the book.

