Project name: The Libre-SOC Gigabit Router

Project number: 2021-02-052

Most recent payment: 2024-08-30

RfP Details

Date submitted: 2024-08-30 at 14:09

Payment: no

Deliverables review: pending

Payment approval: pending

Recipient: Luke Kenneth Casson Leighton

3. Creation of the HDL Code for the Instructions and Associated Unit-Tests	€1200

Subtask https://bugs.libre-soc.org/show_bug.cgi?id=772

Total amount requested for this task: €1200

4. High-Level Demos of Cryptographic and Other Relevant Algorithms	€3300

Subtask https://bugs.libre-soc.org/show_bug.cgi?id=773

Total amount requested for this task: €3300

7. Formal proofs and unit tests for cryptoprimitives €3750

Subtask: https://bugs.libre-soc.org/show_bug.cgi?id=840

Total amount requested for this task: €3750

Total requested amount in this RfP: €8250

Results:

```
Top level page detailing main deliverables: <a
href="https://libre-
soc.org/crypto_router_asic">https://libre-
soc.org/crypto_router_asic</a>/
Pinspec: <a href="https://libre-
soc.org/crypto_router_asic/crypto_router_pinspec">htt
ps://libre-
soc.org/crypto_router_asic/crypto_router_pinspec</a>/
NGI Router: <a href="https://libre-
soc.org/crypto_router_asic/ngi_router">https://libre-
soc.org/crypto_router_asic/ngi_router</a>/
NGI Router Diagram: <a href="https://libre-
soc.org/crypto_router_asic/ngi_router.svg">https://li
bre-soc.org/crypto_router_asic/ngi_router.svg</a>

Listed below: each task completed in the NLnet top-
level gigabit crypto router project, with references
to the relevant reports.

1. **NLnet Gigabit Crypto Router Project
Management**: Coordinated project timelines, budget
allocations, and deliverables, addressing challenges
in communication and execution (Bug #589).
```

[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=589)

2. **Development of the SETNE/SETBNE Instruction**: Implemented and tested the SETNE and SETBNE instructions for use in cryptographic applications (Bug #770).
[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=770)

3. **CMP/TST Set Field**: Successfully developed the CMP and TST set field logic, crucial for condition checks in cryptographic operations (Bug #771).
[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=771)

4. **Trap-and-Mask Implementation**: Integrated trap-and-mask functionality to enhance security protocols in the crypto router (Bug #772).
[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=772)

5. **INVL/INVB Instruction Development**: Designed and implemented the INVL and INVB instructions for invalidating cache lines, important for cryptographic processes (Bug #773).

[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=773)

6. **EFSCR and MFFS/MTFS Instruction Implementation**: Developed and tested the EFSCR, MFFS, and MTFS instructions, which are critical for floating-point operations in cryptography (Bug #774).

[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=774)

7. **Formal Proof of Correctness for CR Int/FP**: Conducted formal proofing for the correctness of Condition Register (CR) Integer and Floating-Point operations (Bug #775).
[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=775)

8. **Arithmetic Operations (ADD/AND/OR/XOR) Testing**: Completed and verified arithmetic operations like ADD, AND, OR, and XOR to ensure their accuracy in cryptographic contexts (Bug #776).
[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=776)

9. **MV.X/MV.Y Implementation and Testing**:

Developed and validated the MV.X and MV.Y instructions, crucial for vector processing in cryptographic algorithms (Bug #840).
[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=840)

10. **Formal Verification of Core Functionality**: Completed formal verification of core functions and instructions, ensuring the reliability and security of the crypto router's operations (Bug #1044).
[Bug Report](https://bugs.libre-soc.org/show_bug.cgi?id=1044)

These efforts collectively advanced the development of a secure, high-performance gigabit crypto router, meeting the NLnet grant’s objectives.

Remarks:

Request status

Deliverables approval:	pending
Transaction approval:	pending
Payment	no

Back to overview

Make a new request