US010142098B2

(12) **United States Patent**
**Suresh et al.**

(10) **Patent No.: US 10,142,098 B2**
(45) **Date of Patent: *Nov. 27, 2018**

(54) **OPTIMIZED SHA-256 DATAPATH FOR ENERGY-EFFICIENT HIGH-PERFORMANCE BITCOIN MINING**

(71) Applicant: **Intel Corporation**, Santa Clara, CA (US)

(72) Inventors: **Vikram B. Suresh**, Hillsboro, OR (US); **Sudhir K. Satpathy**, Hillsboro, OR (US); **Sanu K. Mathew**, Hillsboro, OR (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 119 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/196,698**

(22) Filed: **Jun. 29, 2016**

(65) **Prior Publication Data**

US 2018/0006808 A1 Jan. 4, 2018

(51) **Int. Cl.**

| | |
|---|---|
| ***H04L 9/32*** | (2006.01) |
| ***H04L 9/06*** | (2006.01) |
| ***G09C 1/00*** | (2006.01) |

(52) **U.S. Cl.**

CPC ..... ***H04L 9/0643*** (2013.01); ***G09C 1/00*** (2013.01); *H04L 2209/12* (2013.01)

(58) **Field of Classification Search**

CPC ..... H04L 9/0643; H04L 2209/12; G09C 1/00
USPC ..... 713/181
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 2008/0107259 | A1 | 5/2008 | Satou | |
| 2009/0058478 | A1 | 3/2009 | Lin | |
| 2009/0119407 | A1* | 5/2009 | Krishnan | H04L 63/0281 709/228 |
| 2010/0086127 | A1 | 4/2010 | Grinchuk et al. | |
| 2012/0084568 | A1* | 4/2012 | Sarikaya | H04L 9/3066 713/176 |
| 2014/0093069 | A1 | 4/2014 | Wolrich et al. | |
| 2016/0109870 | A1 | 4/2016 | Firu et al. | |
| 2016/0112200 | A1 | 4/2016 | Kheterpal et al. | |
| 2016/0125040 | A1 | 5/2016 | Kheterpal et al. | |

(Continued)

FOREIGN PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| WO | 2015077378 | A1 | 5/2015 |
| WO | 2016046821 | A1 | 3/2016 |

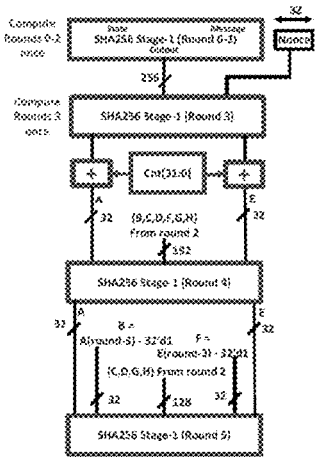
OTHER PUBLICATIONS

PCT, International Search Report and Written Opinion of the International Searching Authority for International Application No. PCT/US2017/035136, dated Sep. 8, 2017, 13 pages.

(Continued)

*Primary Examiner* — Mohammad W Reza
(74) *Attorney, Agent, or Firm* — Lowenstein Sandler LLP

(57) **ABSTRACT**

A processing system includes a processor to construct an input message comprising a plurality of padding bits and a hardware accelerator, communicatively coupled to the processor, comprising a first plurality of circuits to perform a stage-1 secure hash algorithm (SHA) hash based on the input message, wherein the hardware accelerator comprises a first data path coupled between a first reference node and a first input node of the first plurality of circuits to feed a first padding bit of the plurality of padding bits to the first input node.

**16 Claims, 14 Drawing Sheets**