US009311493B2

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

(10) **Patent No.: US 9,311,493 B2**
(45) **Date of Patent: Apr. 12, 2016**

(54) **SYSTEM FOR PROCESSING AN ENCRYPTED INSTRUCTION STREAM IN HARDWARE**

(71) Applicants: **Richard L. Griswold**, West Richland, WA (US); **William K. Nickless**, Richland, WA (US); **Ryan C. Conrad**, West Richland, WA (US)

(72) Inventors: **Richard L. Griswold**, West Richland, WA (US); **William K. Nickless**, Richland, WA (US); **Ryan C. Conrad**, West Richland, WA (US)

(73) Assignee: **BATTELLE MEMORIAL INSTITUTE**, Richland, WA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 8 days.

(21) Appl. No.: **13/954,487**

(22) Filed: **Jul. 30, 2013**

(65) **Prior Publication Data**

US 2015/0039905 A1 Feb. 5, 2015

(51) **Int. Cl.**

G06F 21/00	(2013.01)
G06F 21/60	(2013.01)
G06F 21/72	(2013.01)
G06F 21/76	(2013.01)

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

CPC ***G06F 21/602*** (2013.01); ***G06F 21/72*** (2013.01); ***G06F 21/76*** (2013.01)

(58) **Field of Classification Search**

USPC 713/190

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,465,901	A	8/1984	Best	
4,814,976	A	3/1989	Hansen et al.	
6,345,359	B1 *	2/2002	Bianco	713/190
7,086,088	B2	8/2006	Narayanan	
8,719,589	B2 *	5/2014	Henry et al.	713/190
2003/0046563	A1 *	3/2003	Ma et al.	713/190
2005/0283601	A1 *	12/2005	Tahan	713/2
2010/0153745	A1 *	6/2010	Onno et al.	713/190
2010/0246814	A1	9/2010	Olson et al.	
2011/0296202	A1	12/2011	Henry et al.	
2014/0173293	A1 *	6/2014	Kapland	713/190
2014/0229743	A1 *	8/2014	Roden et al.	713/190
2014/0281575	A1 *	9/2014	Springfield et al.	713/189
2014/0337637	A1 *	11/2014	Kiperberg et al.	713/189

FOREIGN PATENT DOCUMENTS

WO 2008054456 A2 5/2008

OTHER PUBLICATIONS

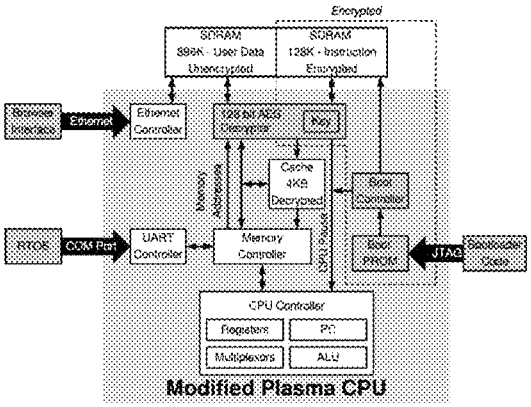
US 2010/0122095, 05/2010, Jones et al. (withdrawn).*

International Search Report/Written Opinion for International Application No. PCT/US2014/036675, International Filing Date May 4, 2014, Date of Mailing Jan. 9, 2015.

(Continued)

Primary Examiner — Jeffrey Pwu
Assistant Examiner — William Corum, Jr.
(74) *Attorney, Agent, or Firm* — A. J. Gokcek

(57) **ABSTRACT**

A system and method of processing an encrypted instruction stream in hardware is disclosed. Main memory stores the encrypted instruction stream and unencrypted data. A central processing unit (CPU) is operatively coupled to the main memory. A decryptor is operatively coupled to the main memory and located within the CPU. The decryptor decrypts the encrypted instruction stream upon receipt of an instruction fetch signal from a CPU core. Unencrypted data is passed through to the CPU core without decryption upon receipt of a data fetch signal.

41 Claims, 5 Drawing Sheets