US007558967B2

(12) **United States Patent**
Wong

(10) **Patent No.: US 7,558,967 B2**
(45) **Date of Patent: Jul. 7, 2009**

(54) **ENCRYPTION FOR A STREAM FILE IN AN FPGA INTEGRATED CIRCUIT**

(75) Inventor: **Wayne Wong**, Sunnyvale, CA (US)

(73) Assignee: **Actel Corporation**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 583 days.

(21) Appl. No.: **09/953,580**

(22) Filed: **Sep. 13, 2001**

(65) **Prior Publication Data**

US 2003/0163715 A1 Aug. 28, 2003

(51) **Int. Cl.**
H04L 9/18 (2006.01)

(52) **U.S. Cl.** **713/189**; 716/16; 716/17; 326/8; 326/38; 326/39; 713/191; 713/193

(58) **Field of Classification Search** 716/16–17; 326/8, 37–41, 4, 44; 380/44, 42, 37; 708/232, 708/626; 712/206; 713/191, 188, 189, 193
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,910,417	A		3/1990	El Gamal et al.	307/465
5,388,157	A		2/1995	Austin	380/4
5,406,627	A	*	4/1995	Thompson et al.	380/237
5,426,379	A	*	6/1995	Trimberger	326/39
5,451,887	A		9/1995	El Avat et al.	326/39
5,515,437	A	*	5/1996	Katta et al.	380/217
5,548,648	A	*	8/1996	Yorke-Smith	713/193
5,675,553	A		10/1997	O'Brien, Jr. et al.	367/135
5,768,372	A		6/1998	Sung et al.	
5,946,478	A	*	8/1999	Lawman	716/17
5,970,142	A		10/1999	Erickson	380/21
6,028,445	A	*	2/2000	Lawman	326/38
6,118,869	A	*	9/2000	Kelem et al.	380/44
6,205,574	B1	*	3/2001	Dellinger et al.	716/16
6,351,142	B1	*	2/2002	Abbott	326/39
6,357,037	B1	*	3/2002	Burnham et al.	716/17
6,446,242	B1	*	9/2002	Lien et al.	716/6
6,507,943	B1	*	1/2003	Kelem	716/16

(Continued)

FOREIGN PATENT DOCUMENTS

EP 1093056 * 4/2001

(Continued)

OTHER PUBLICATIONS

Microsoft Press Computer Dictionary, 3rd edition, Copyright 1997, p. 421.*

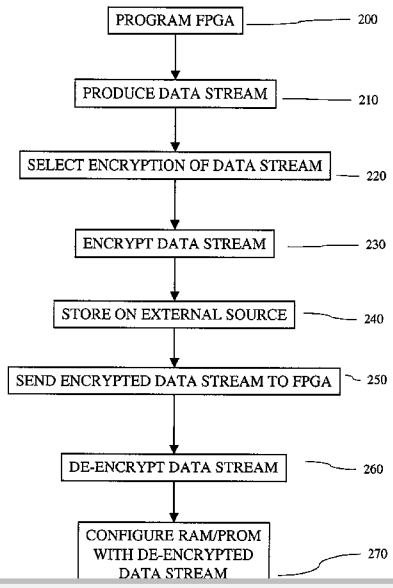
(Continued)

Primary Examiner—Kambiz Zand
Assistant Examiner—Yin-Chen Shaw
(74) *Attorney, Agent, or Firm*—Lewis and Roca LLP

(57) **ABSTRACT**

A system for encrypting and decrypting data in a data stream for programming a Field Programmable Gate Array (FPGA). The system allows for an enable bit to be set for a gap in the data stream and the data is then encrypted from the beginning of the gap. A gap being bits in said data stream that correspond to unprogrammed addresses of a memory in the field programmable gate array. The data is then decrypted by the FPGA when the bit stream is received and an enable bit is detected in a gap of the data stream.

30 Claims, 4 Drawing Sheets



U.S. PATENT DOCUMENTS

6,526,557	B1 *	2/2003	Young et al.	716/16
6,654,889	B1 *	11/2003	Trimberger	713/191
6,735,291	B1 *	5/2004	Schmid et al.	379/189
6,738,962	B1 *	5/2004	Flaherty et al.	716/17
6,756,811	B2 *	6/2004	Or-Bach	326/41
6,904,527	B1 *	6/2005	Parlour et al.	713/189
6,931,543	B1 *	8/2005	Pang et al.	713/193
2001/0032318	A1 *	10/2001	Yip et al.	713/190
2001/0056546	A1 *	12/2001	Ogilvie	713/200

FOREIGN PATENT DOCUMENTS

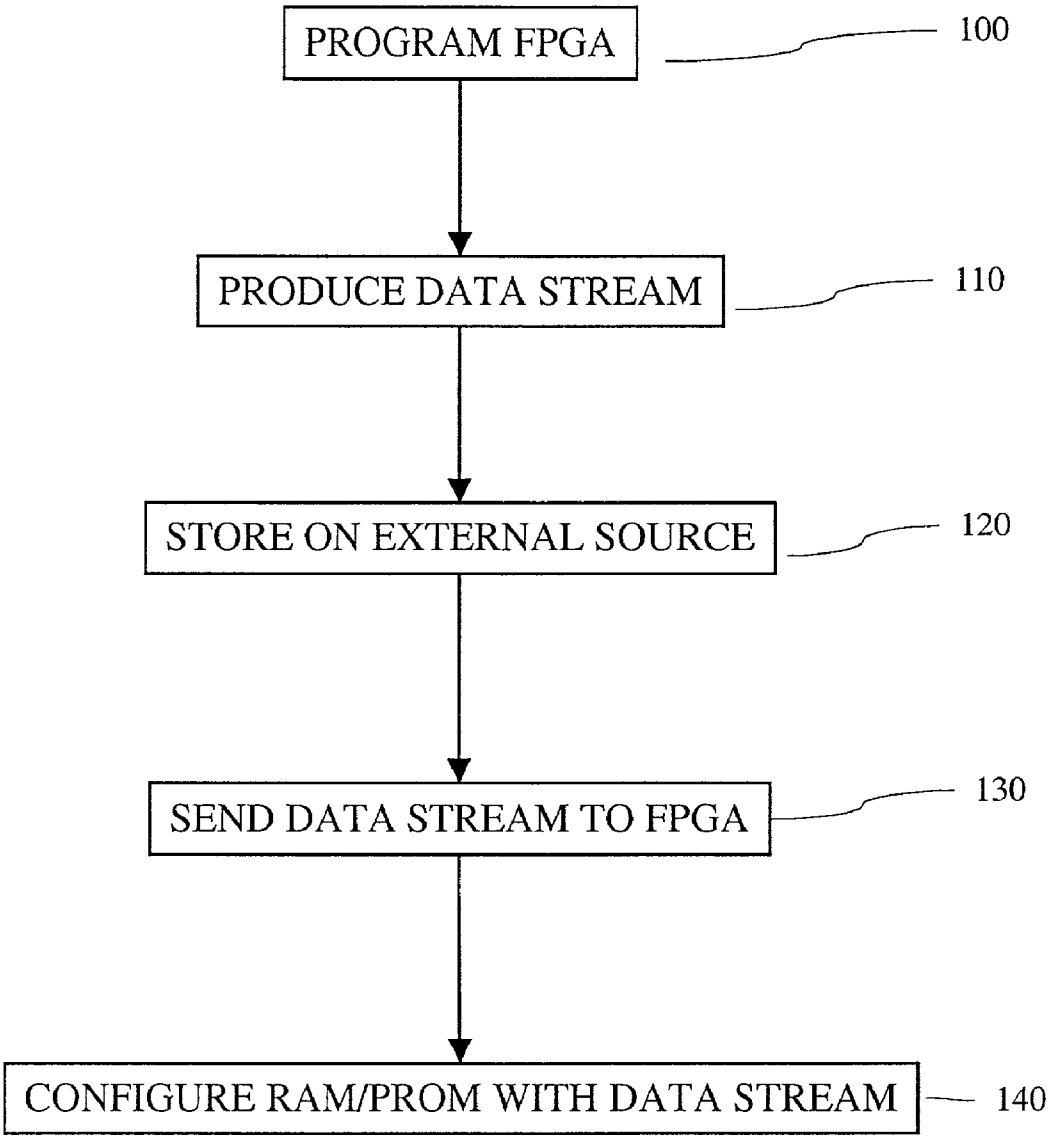
JP	05056267	A	3/1993
JP	7-281596	A	10/1996
JP	2000-76075	A	3/2000
JP	2000-78023	A	3/2000
JP	2005-518691	A	6/2005

OTHER PUBLICATIONS

Glenn, R. and Kent, S., "The NULL Encryption Algorithm and Its Use with IPsec," RFC 2410,Network Working Group, Nov. 1998, UR http://www.faqs.org/ftp/rfc/pdf/rfc2410.txt.pdf, 6 pages.

Japanese Patent Application No. 2003-527602 (Publicatiion No. 2005-518691) Notice of Allowance and English translation of Information Sheet for prior art listed in Notice of Allowance dated Sep. 30, 2008, 4 pages.

* cited by examiner



PRIOR ART

FIG. 1

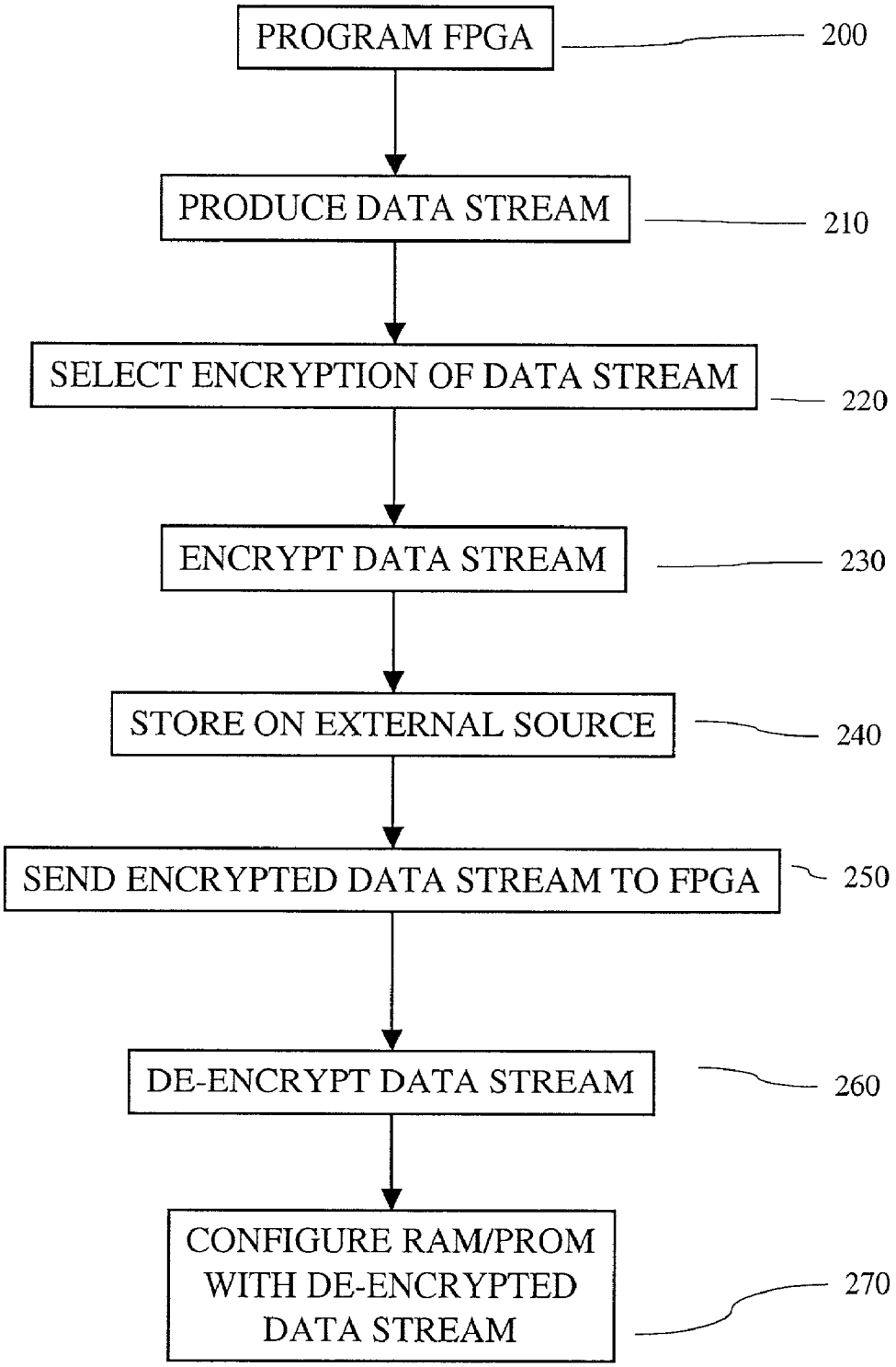


FIG. 2

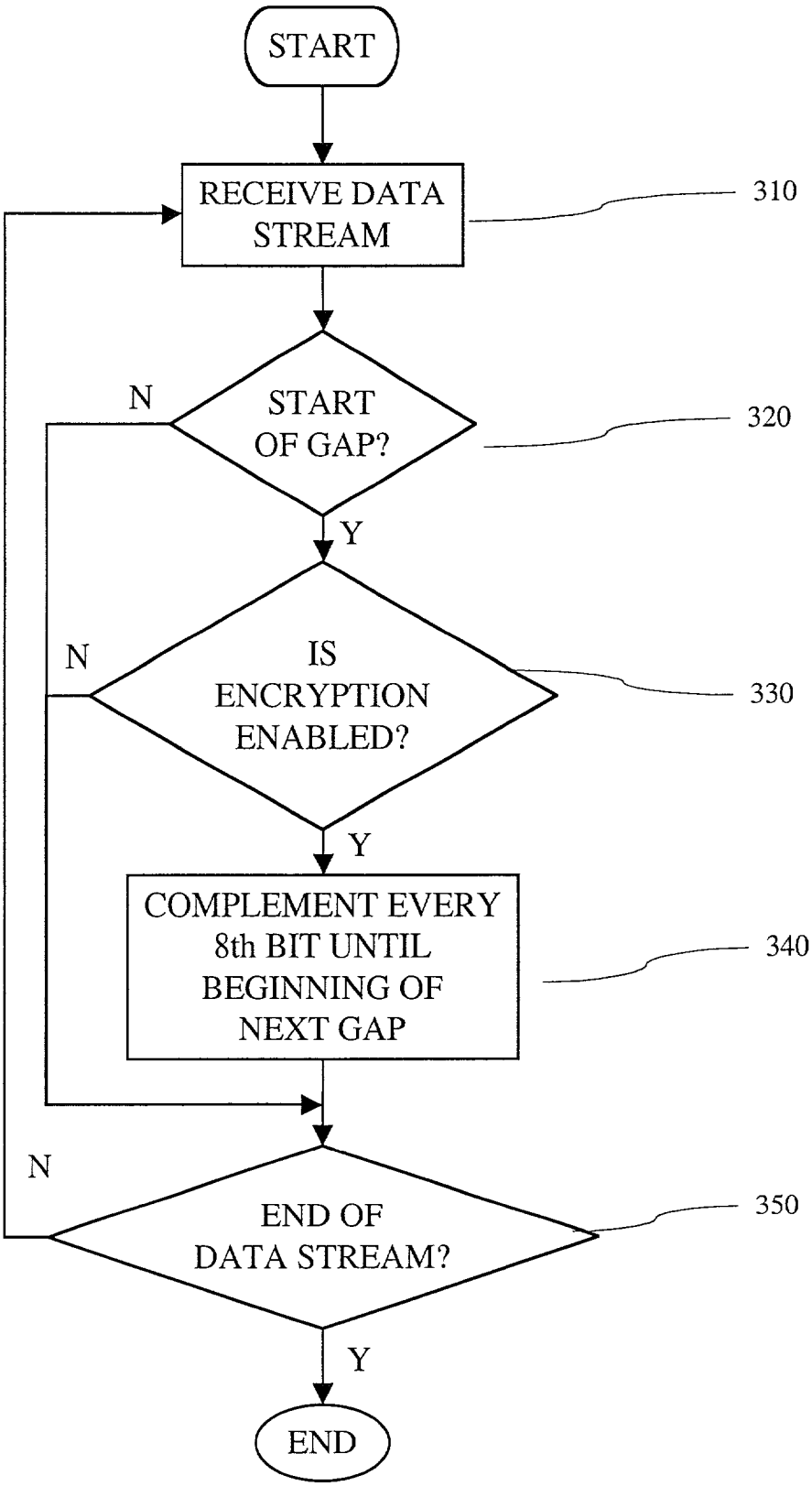


FIG. 3

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.