



US 20110067012A1

(19) **United States**(12) **Patent Application Publication****Eisen et al.**(10) **Pub. No.: US 2011/0067012 A1**(43) **Pub. Date: Mar. 17, 2011**(54) **SYSTEM AND METHOD FOR GENERATING
WHITE-BOX IMPLEMENTATIONS OF
SOFTWARE APPLICATIONS****Publication Classification**

(51) **Int. Cl.**
G06F 12/14 (2006.01)
G06F 9/44 (2006.01)
G06F 9/45 (2006.01)
(52) **U.S. Cl.** **717/140; 713/189**
(57) **ABSTRACT**

(75) Inventors: **Philip Allan Eisen**, Ottawa (CA);
Grant Stewart Goodes, Manotick
(CA); **Daniel Elie Murdock**,
Ottawa (CA)

(73) Assignee: **IRDETO CANADA
CORPORATION**, Ottawa, ON
(CA)

(21) Appl. No.: **12/992,318**

(22) PCT Filed: **May 25, 2009**

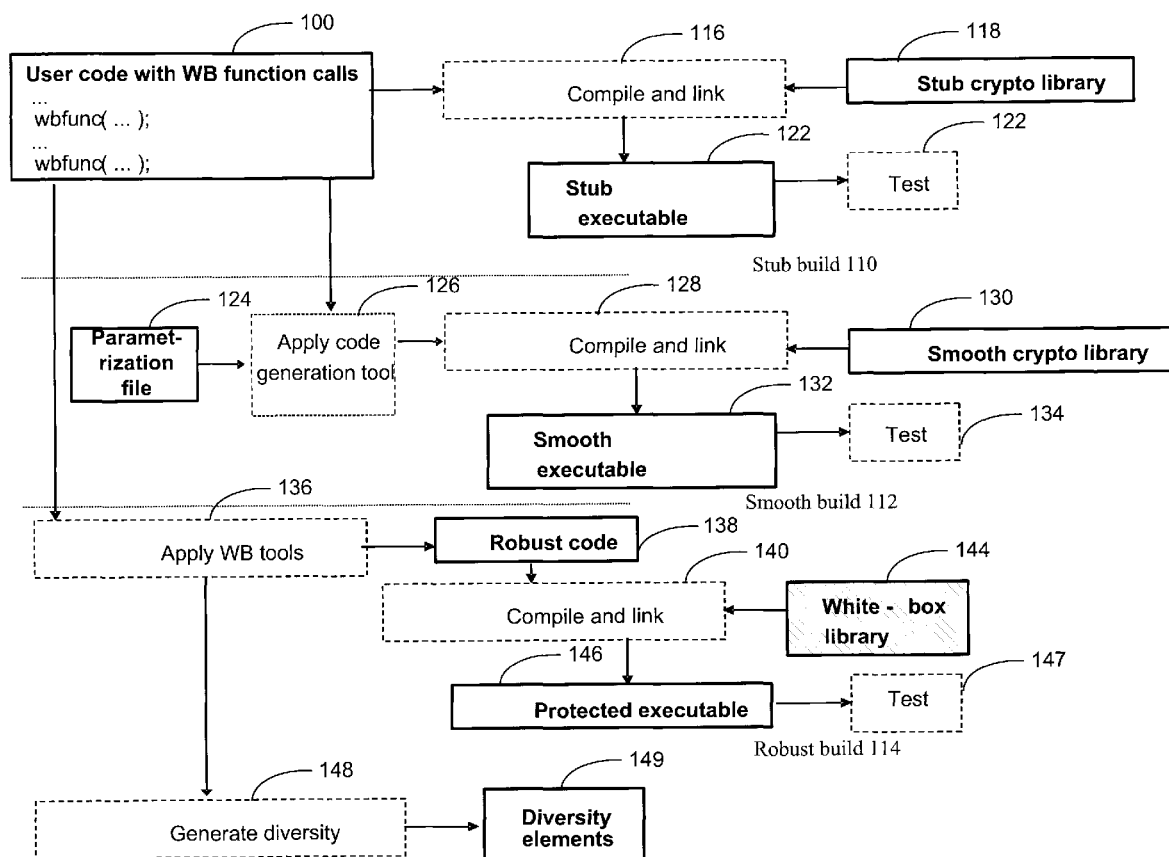
(86) PCT No.: **PCT/CA09/00755**

§ 371 (c)(1),
(2), (4) Date: **Nov. 12, 2010**

Related U.S. Application Data

(60) Provisional application No. 61/055,694, filed on May 23, 2008.

A development suite for generating files, such as DRM-protected files, using white-box cryptography. The suite consists of a code generation tool, a data transformation engine, and a white-box data generation tool, and a white-box library. In the white-box cryptography context, the data transformation engine is used to protect the boundary between the cryptographic operation and the surrounding code. In particular, the data transformation engine is used to apply data transformations to the inputs to and outputs from the cryptographic operations. If the user specifies that transformations are required via a white-box parameterization file, the code generation tool puts the information specified by the user into a form the data transformation engine understands, namely as qualifiers on data variables and function prototypes. The data transformation engine then applies the specified transformations, and passes information to the data generation tool regarding which transformations were chosen.



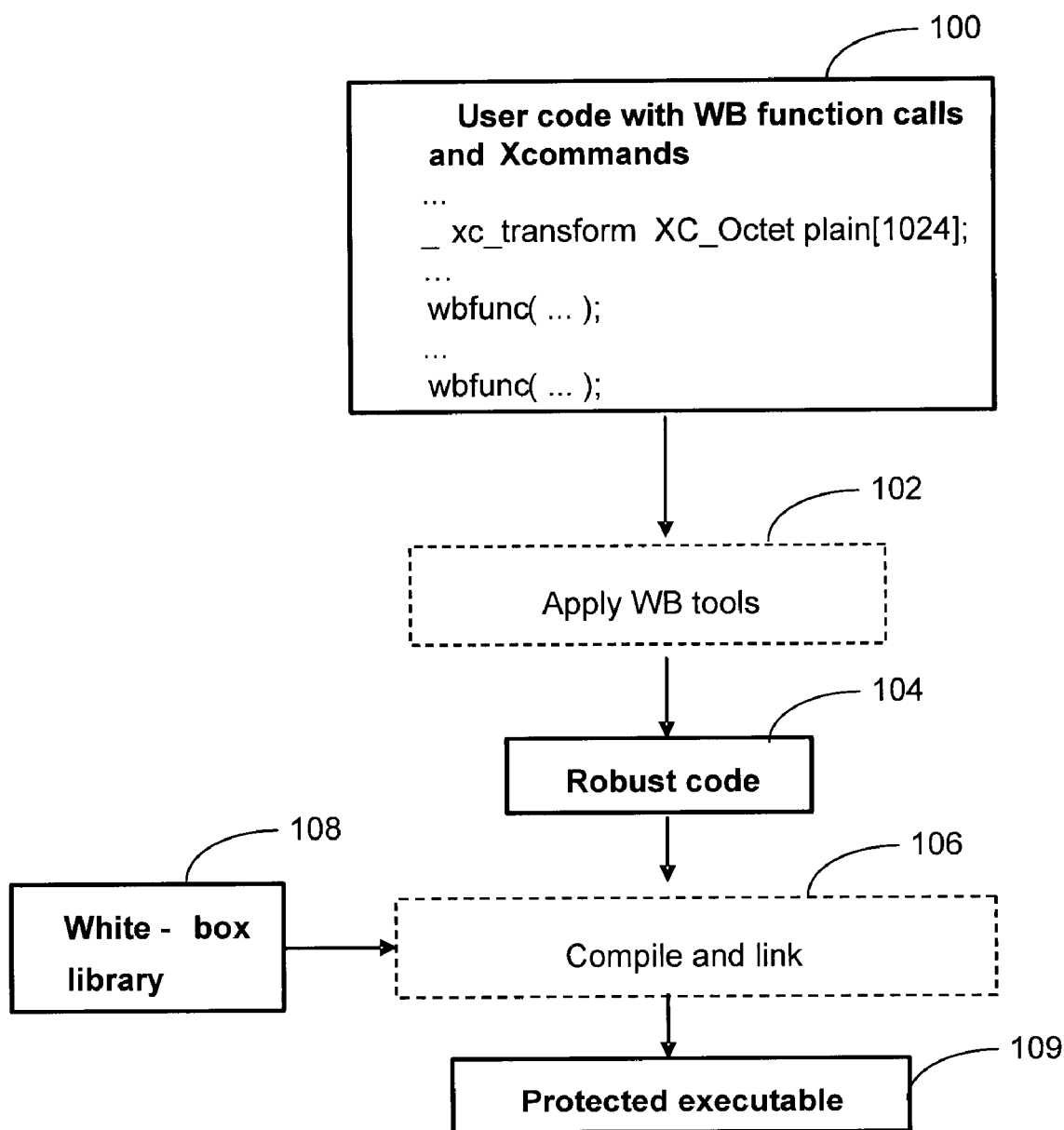


Figure 1

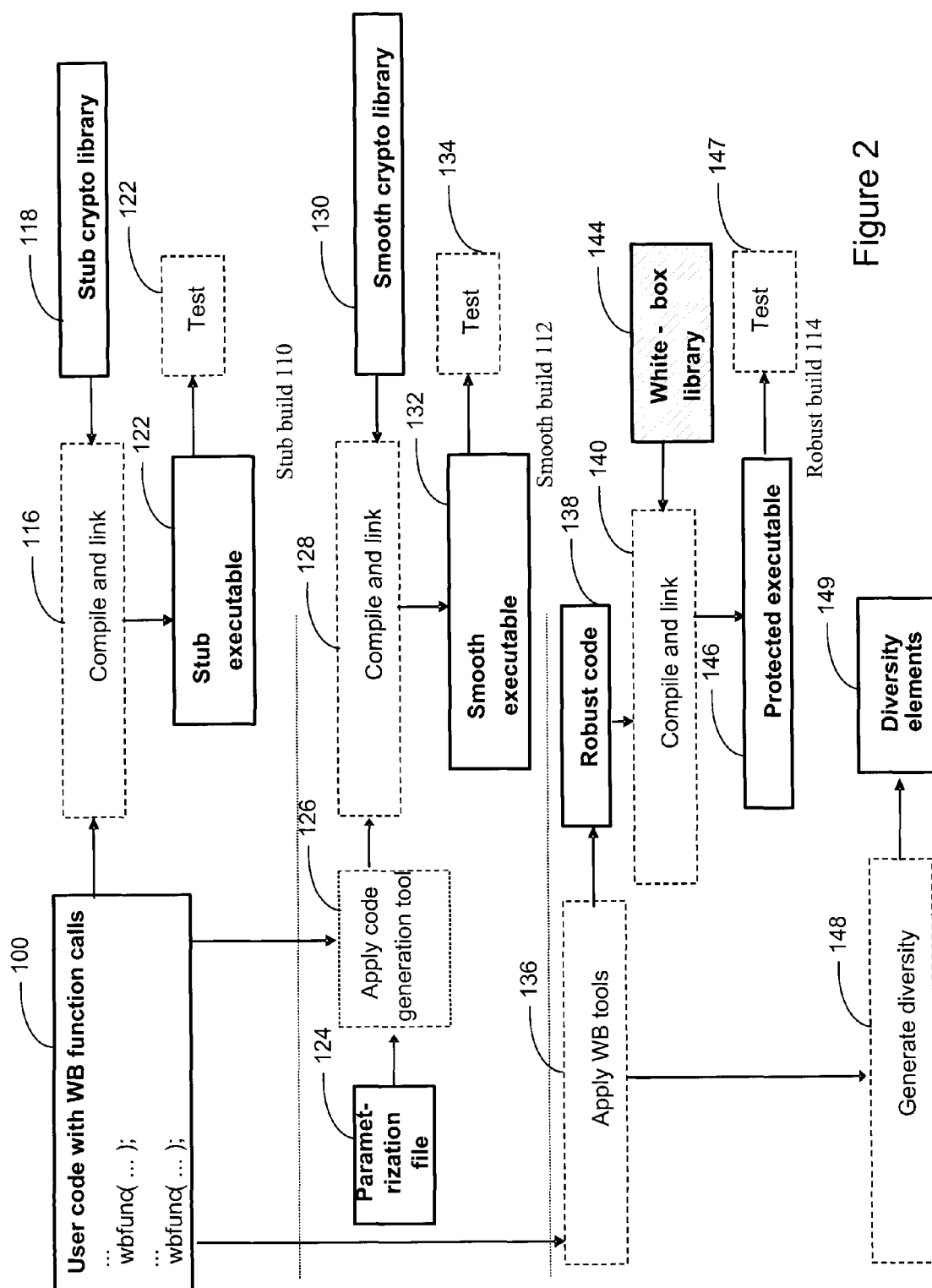


Figure 2

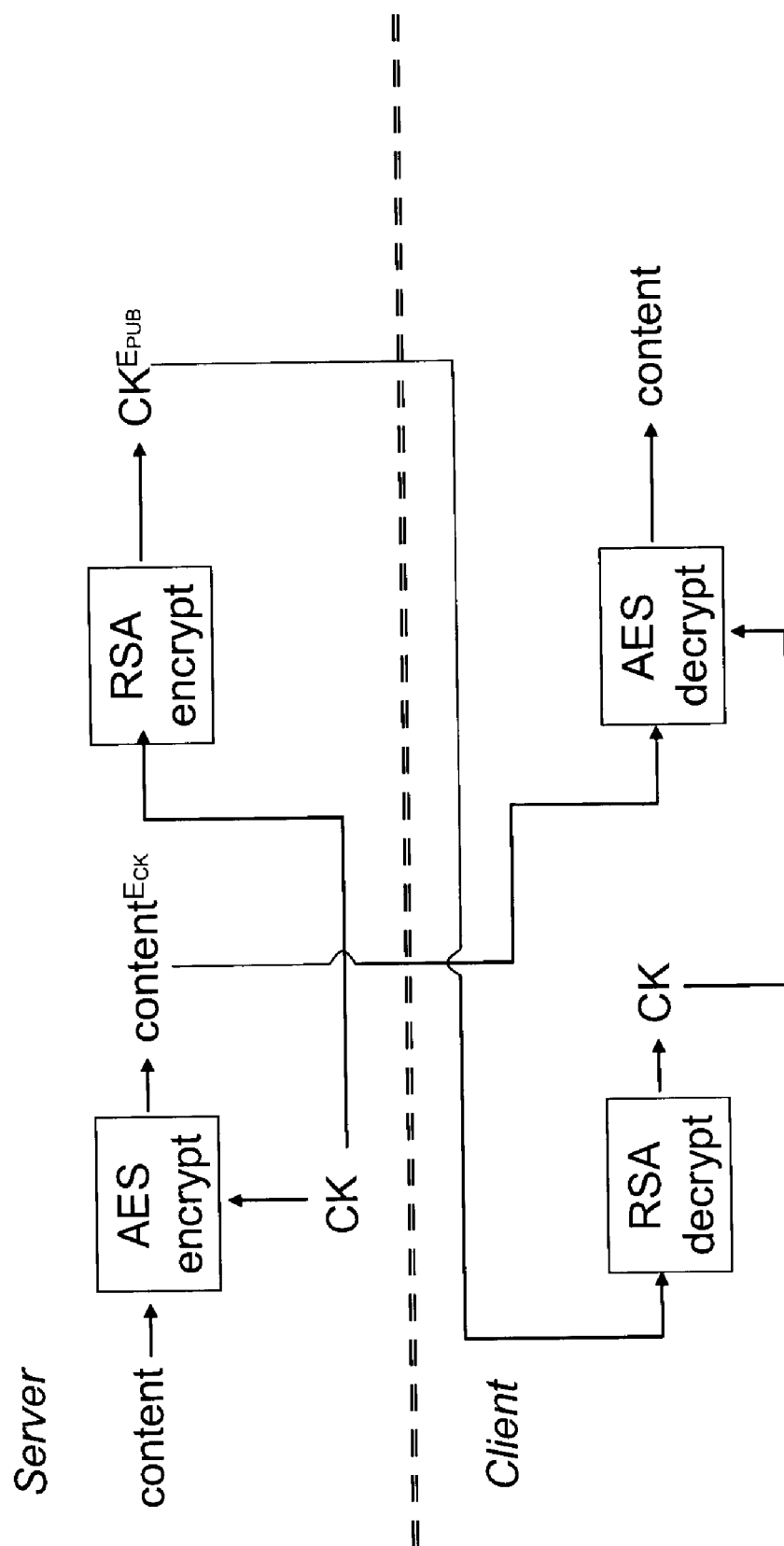


Figure 3

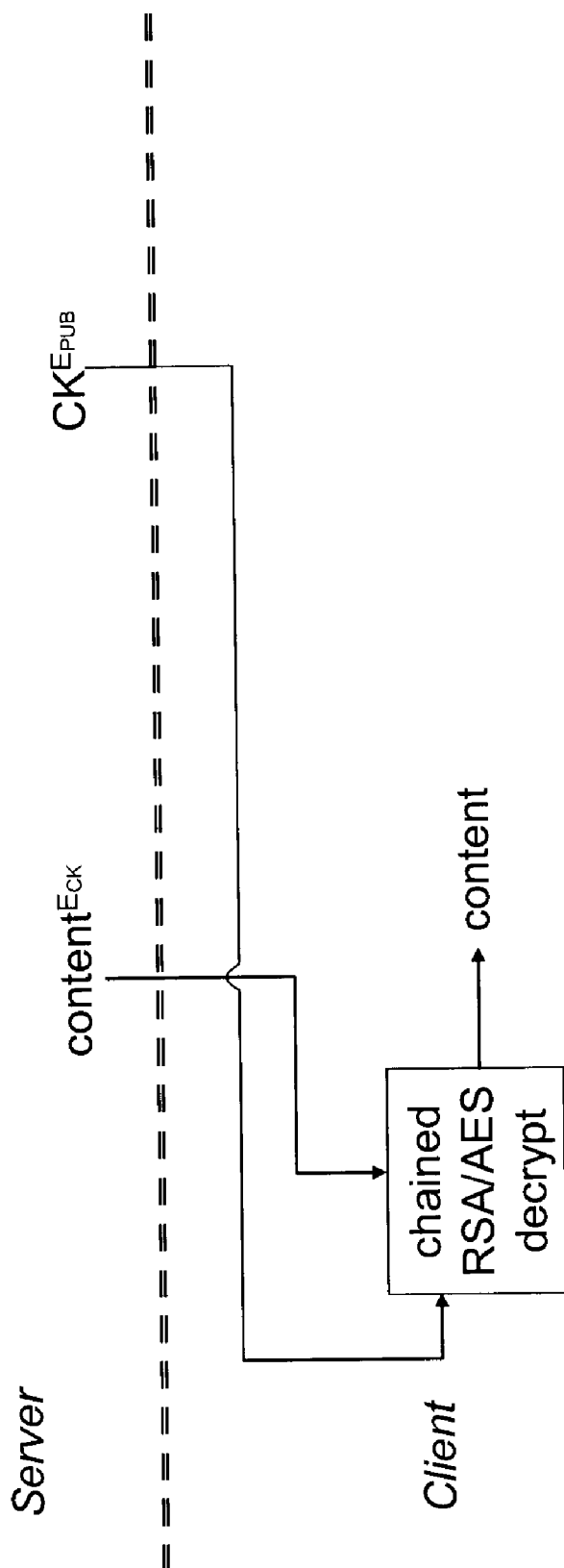


Figure 4

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.