



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11)



1-0054049

(51)^{2022.01} H04L 9/08; G06F 11/10; G06F 16/907 (13) B

(21) 1-2023-04402

(22) 01/12/2021

(86) PCT/US2021/061457 01/12/2021

(87) WO 2022/154889 A1 21/07/2022

(30) 17/147,110 12/01/2021 US

(45) 25/11/2025 452

(43) 27/11/2023 428A

(73) QUALCOMM INCORPORATED (US)

ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, CA
92121-1714, United States of America

(72) LI, Yanru (US); CHUN, Dexter Tamio (US).

(74) Công ty TNHH Quốc tế D & N (D&N INTERNATIONAL CO.,LTD.)

(54) PHƯƠNG PHÁP, HỆ THỐNG VÀ PHƯƠNG TIỆN ĐỌC ĐƯỢC BẰNG MÁY
TÍNH ĐỂ CHUYỂN DỮ LIỆU GIỮA CÁC BỘ NHỚ

(21) 1-2023-04402

(57) Sáng chế đề cập đến phương pháp, hệ thống và phương tiện đọc được bằng máy tính để chuyển dữ liệu giữa các bộ nhớ. Việc chuyển dữ liệu giữa các bộ nhớ có thể bao gồm bước đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất, xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không, và chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai. Việc chuyển có thể bao gồm bước bỏ qua bước xử lý thứ nhất nếu chỉ báo bỏ qua được khẳng định. Việc chuyển có thể còn bao gồm bước bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định. Sau khi bỏ qua bước xử lý thứ hai, dữ liệu có thể được lưu trữ trong bộ nhớ thứ hai.

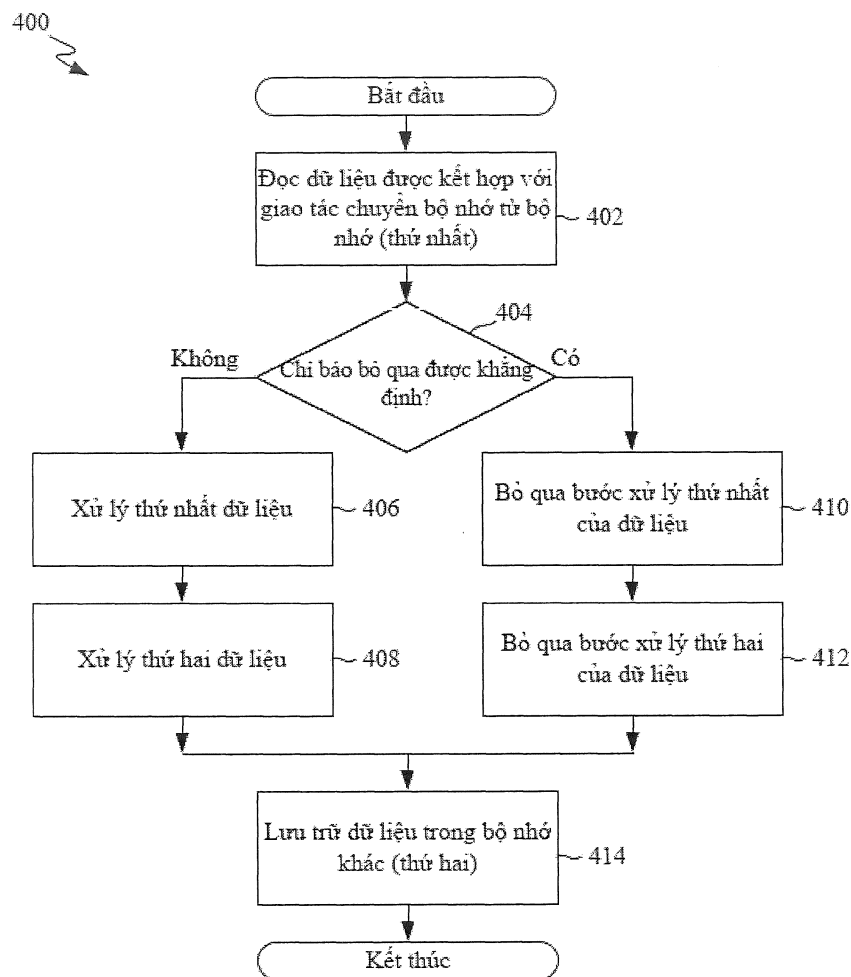


Fig.4

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến việc truyền trực tiếp dữ liệu được bảo vệ giữa các bộ nhớ.

Tình trạng kỹ thuật của sáng chế

Các thiết bị điện toán cầm tay (Portable computing device - PCD) đang trở thành nhu cầu thiết yếu đối với mọi người ở các cấp độ cá nhân và chuyên nghiệp. Các thiết bị này có thể bao gồm các điện thoại di động, các máy tính bảng, các máy tính cầm tay, các thiết bị hỗ trợ kỹ thuật số cầm tay (portable digital assistant - PDA), các máy điều khiển trò chơi cầm tay, và các thiết bị điện tử cầm tay khác. Các PCD thường chứa các mạch tích hợp hoặc các hệ thống trên chip (system-on-a-chip - SoC) bao gồm nhiều thành phần được thiết kế để hoạt động cùng nhau nhằm cung cấp chức năng cho người dùng. Ví dụ, SoC có thể chứa số lượng bất kỳ của các công cụ xử lý, chẳng hạn như các khối xử lý trung tâm (central processing unit - CPU) với nhiều lõi, các khối xử lý đồ họa (graphical processing unit - GPU), các khối xử lý nơron (neural processing unit - NPU), các bộ xử lý tín hiệu số (digital signal processor - DSP), các khối thu phát không dây (còn được gọi là các modem), v.v. SoC có thể được ghép nối với các thành phần khác trong PCD hoặc thiết bị điện toán khác, chẳng hạn như SoC khác, các chip bộ nhớ, v.v..

Có các trường hợp sử dụng hoặc các kịch bản hoạt động trong đó dữ liệu có thể được truyền trực tuyến hoặc được chuyển từ bộ nhớ này sang bộ nhớ khác. Dữ liệu có thể được chuyển giữa hai bộ nhớ trong cùng hệ thống (ví dụ, cùng SoC) hoặc từ bộ nhớ trong một hệ thống đến bộ nhớ trong một hệ thống khác (ví dụ, các SoC khác nhau). Công cụ xử lý, chẳng hạn như CPU, bộ điều khiển truy cập bộ nhớ trực tiếp (direct memory access -DMA), bộ tăng tốc bộ nhớ, v.v., có thể điều khiển các khía cạnh chuyển dữ liệu giữa các bộ nhớ.

Dữ liệu được lưu trữ trong bộ nhớ có thể được bảo vệ. Mã hóa là một ví dụ về một loại bảo vệ dữ liệu. Việc phát hiện và hiệu chỉnh lỗi sử dụng thông tin chẵn lẻ (ví dụ, các mã sửa lỗi hoặc “ECC”) là một ví dụ khác về việc bảo vệ dữ liệu. Việc xác

thực là một ví dụ khác về việc bảo vệ dữ liệu. Các loại xử lý khác cho dữ liệu được lưu trữ trong bộ nhớ là đã biết, bao gồm, ví dụ, nén và chống hủy giao dịch.

Khi dữ liệu được chuyển giữa các bộ nhớ, các hoạt động xử lý đảo ngược có thể được thực hiện liên quan đến các bộ nhớ nguồn và đích. Ví dụ, dữ liệu được lưu trữ trong bộ nhớ nguồn ở dạng được mã hóa có thể được giải mã sau khi đọc nó từ bộ nhớ nguồn, và sau đó dữ liệu được giải mã có thể được mã hóa lại trước khi lưu trữ nó trong bộ nhớ đích.

Bản chất kỹ thuật của sáng chế

Các hệ thống, các phương pháp, phương tiện đọc được bằng máy tính, và các ví dụ khác của việc chuyển dữ liệu giữa các bộ nhớ được bộc lộ ở đây.

Phương pháp ví dụ để chuyển dữ liệu giữa các bộ nhớ có thể bao gồm bước đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất. Phương pháp ví dụ cũng có thể bao gồm bước xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không. Phương pháp ví dụ có thể còn bao gồm bước chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai. Việc chuyển có thể bao gồm bước bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định. Việc chuyển có thể còn bao gồm bước bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định. Phương pháp ví dụ có thể còn bao gồm bước lưu trữ dữ liệu trong bộ nhớ thứ hai.

Hệ thống ví dụ để chuyển dữ liệu giữa các bộ nhớ có thể bao gồm bộ nhớ thứ nhất, bộ nhớ thứ hai, và logic điều khiển chuyển bộ nhớ. Logic điều khiển chuyển bộ nhớ có thể bao gồm logic xử lý thứ nhất và logic xử lý thứ hai. Logic điều khiển chuyển bộ nhớ có thể được tạo cấu hình để đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất. Logic điều khiển chuyển bộ nhớ có thể cũng được tạo cấu hình để xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không. Logic điều khiển chuyển bộ nhớ có thể còn được tạo cấu hình để bỏ qua việc áp dụng logic xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định. Logic điều khiển chuyển bộ nhớ có thể còn được tạo cấu hình để bỏ qua việc áp dụng logic xử lý thứ hai nếu chỉ báo bỏ qua được khẳng định. Logic điều

cho phép chuyển bộ nhớ có thể còn được tạo cấu hình để lưu trữ dữ liệu trong bộ nhớ thứ hai.

Hệ thống ví dụ khác để chuyển dữ liệu giữa các bộ nhớ có thể bao gồm phương tiện để đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất. Hệ thống ví dụ cũng có thể bao gồm phương tiện để xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không. Hệ thống ví dụ có thể còn bao gồm phương tiện để chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai. Phương tiện để chuyển có thể bao gồm phương tiện để bỏ qua bước xử lý thứ nhất nếu chỉ báo bỏ qua được khẳng định. Phương tiện để chuyển có thể còn bao gồm phương tiện để bỏ qua bước xử lý thứ hai nếu chỉ báo bỏ qua được khẳng định. Hệ thống ví dụ cũng có thể bao gồm phương tiện để lưu trữ dữ liệu trong bộ nhớ thứ hai.

Phương tiện đọc được bằng máy tính ví dụ để chuyển dữ liệu giữa các bộ nhớ có thể bao gồm phương tiện bất biến đọc được bằng máy tính có các lệnh được lưu trữ trên đó trong dạng có thể thực thi được bằng máy tính. Các lệnh, khi được thực thi bởi hệ thống xử lý của thiết bị điện toán, có thể tạo cấu hình hệ thống xử lý để đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất. Các lệnh, khi được thực thi bởi hệ thống xử lý, cũng có thể tạo cấu hình hệ thống xử lý để xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không. Các lệnh, khi được thực thi bởi hệ thống xử lý, có thể còn tạo cấu hình hệ thống xử lý để bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định. Các lệnh, khi được thực thi bởi hệ thống xử lý, có thể còn tạo cấu hình hệ thống xử lý để bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định. Các lệnh, khi được thực thi bởi hệ thống xử lý, có thể còn tạo cấu hình hệ thống xử lý để lưu trữ dữ liệu trong bộ nhớ thứ hai.

Mô tả vắn tắt các hình vẽ

Trên các hình vẽ, các số tham chiếu giống nhau dùng để chỉ các phần giống nhau trên các hình vẽ khác nhau trừ khi có chỉ định khác. Đối với các số tham chiếu có ký hiệu ký tự chữ cái chẳng hạn như “102A” hoặc “102B”, ký hiệu ký tự chữ cái có thể phân biệt hai phần hoặc thành phần giống nhau có mặt trên cùng một hình vẽ. Ký hiệu

ký tự chữ cái cho các số tham chiếu có thể được bỏ qua khi có ý định rằng một số tham chiếu bao gồm tất cả các phần có cùng số tham chiếu trên tất cả các hình vẽ.

Fig.1 là sơ đồ khối minh họa hệ thống để chuyển dữ liệu giữa các bộ nhớ, theo các phương án ví dụ.

Fig.2 là sơ đồ khối minh họa một hệ thống khác để chuyển dữ liệu giữa các bộ nhớ, theo các phương án ví dụ.

Fig.3 là sơ đồ khối minh họa một hệ thống khác nữa để chuyển dữ liệu giữa các bộ nhớ, theo các phương án ví dụ.

Fig.4 là lưu đồ minh họa phương pháp để chuyển dữ liệu giữa các bộ nhớ, theo các phương án ví dụ.

Fig.5 là sơ đồ khối chức năng minh họa chuỗi các hành động để điều khiển việc chuyển dữ liệu giữa các bộ nhớ, theo các phương án ví dụ.

Fig.6 là sơ đồ khối minh họa một hệ thống khác nữa để chuyển dữ liệu giữa các bộ nhớ, theo các phương án ví dụ.

Fig.7 là lưu đồ minh họa phương pháp để chuyển khóa giữa các bộ nhớ, theo các phương án ví dụ.

Fig.8 là sơ đồ khối của thiết bị điện toán cầm tay, theo các phương án ví dụ.

Mô tả chi tiết sáng chế

Từ “ví dụ” được sử dụng ở đây có nghĩa là “dùng làm ví dụ, trường hợp hoặc minh họa.” Từ “minh họa” có thể được sử dụng ở đây đồng nghĩa với “ví dụ”. Khía cạnh bất kỳ được mô tả ở đây dưới dạng “ví dụ” không nhất thiết phải được hiểu là ưu tiên hoặc có lợi hơn các khía cạnh khác. Thuật ngữ “được ghép nối” có thể được sử dụng ở đây có nghĩa được kết nối thông qua không hoặc nhiều phần tử xen kẽ, trái ngược với thuật ngữ “được kết nối trực tiếp,” có thể được sử dụng ở đây để có nghĩa được kết nối thông qua không có phần tử xen kẽ nào.

Như được minh họa trên Fig.1, theo phương án minh họa hoặc ví dụ, thiết bị điện toán 100 có thể bao gồm ít nhất một bộ xử lý 102, và ít nhất là bộ nhớ thứ nhất 104 và bộ nhớ thứ hai 106. Mặc dù không được thể hiện nhằm các mục đích ngắn gọn,

nhưng thiết bị điện toán 100 cũng có thể bao gồm các thành phần khác, chẳng hạn như, ví dụ, các bộ nhớ khác, các bộ xử lý khác, các giao diện, các bộ điều khiển công suất, v.v.. Bộ xử lý 102 và các bộ nhớ 104 và 106 có thể được liên kết bởi một hoặc nhiều bus hoặc các liên kết truyền thông dữ liệu khác. Thiết bị điện toán 100 có thể là thuộc loại bất kỳ. Tương tự, các bộ nhớ 104 và 106 có thể là thuộc loại bất kỳ. Bộ xử lý 102 có thể là, ví dụ, CPU, NPU, GPU, máy DMA, v.v., hoặc loại bộ xử lý bất kỳ khác, bao gồm các loại “bộ tăng tốc” được mô tả dưới đây. Mặc dù theo phương án được minh họa trên Fig.1 bộ xử lý 102 có dạng đơn nhất, nhưng theo các phương án khác bộ xử lý này có thể có dạng phân tán, bao gồm hai hoặc nhiều bộ xử lý. Ngoài ra, như được mô tả dưới đây, theo một số phương án các bộ nhớ 104 và 106 và bộ xử lý 102 có thể ở trên cùng chip với nhau, trong khi theo các phương án khác một hoặc nhiều thành phần này có thể ở trên các chip khác với một hoặc nhiều thành phần khác này. Bộ nhớ thứ nhất 104 và bộ nhớ thứ hai 106 mỗi trong số chúng có thể bao gồm số lượng và loại bất kỳ của các thiết bị lưu trữ dữ liệu vật lý.

Theo phương án được minh họa trên Fig.1, bộ xử lý 102 có thể được tạo cấu hình với logic xử lý thứ nhất 110 và logic xử lý thứ hai 112. Tuy nhiên, theo các phương án trong đó bộ xử lý này là phân tán, logic xử lý thứ nhất và thứ hai này có thể được phân tán giữa hai bộ xử lý. Logic xử lý thứ nhất 110 và logic xử lý thứ hai 112 có thể tương ứng với logic bộ xử lý được tạo cấu hình bằng việc thực thi của phần mềm tương ứng trên bộ xử lý 102, theo các nguyên tắc điện toán thông thường. Nghĩa là, bộ xử lý 102 có thể cung cấp hoặc bao gồm logic xử lý thứ nhất 110 và logic xử lý thứ hai 112 bằng việc được tạo cấu hình bởi phần mềm trong khi thực thi. Để ngắn gọn, các hành động hoặc các chức năng tương ứng có thể xảy ra dưới sự điều khiển của bộ xử lý được tạo cấu hình 102 có thể được xem là được thực hiện bởi logic xử lý thứ nhất 110 (ví dụ, hành động hoặc chức năng “xử lý thứ nhất”) hoặc logic xử lý thứ hai 112 (ví dụ, hành động hoặc chức năng “xử lý thứ hai”).

Logic xử lý thứ nhất 110 có thể, trong số các chức năng khác, điều khiển các khía cạnh của giao tác bộ nhớ trong đó dữ liệu được chuyển giữa các bộ nhớ, chẳng hạn như từ bộ nhớ thứ nhất 104 đến bộ nhớ thứ hai 106 hoặc từ bộ nhớ thứ hai 106 đến bộ nhớ thứ nhất 104. Logic xử lý thứ hai 112 một cách tương tự có thể, trong số các chức năng khác, điều khiển các khía cạnh của giao tác bộ nhớ trong đó dữ liệu được

chuyển giữa các bộ nhớ, chẳng hạn như từ bộ nhớ thứ nhất 104 đến bộ nhớ thứ hai 106 hoặc từ bộ nhớ thứ hai 106 đến bộ nhớ thứ nhất 104. Giao tác chuyển bộ nhớ có thể được khởi tạo bởi logic xử lý thứ nhất 110, logic xử lý thứ hai 112, hoặc logic khác.

Dữ liệu là đối tượng của giao tác chuyển bộ nhớ giữa các bộ nhớ thứ nhất 104 và bộ nhớ thứ hai 106 có thể được bảo vệ. Các loại khác nhau của việc bảo vệ dữ liệu là đã biết với người có hiểu biết trung bình trong lĩnh vực và được dự tính theo các phương án ví dụ được mô tả ở đây. Ví dụ, dữ liệu có thể được lưu trữ trong bộ nhớ thứ nhất 110 hoặc bộ nhớ thứ hai 112 ở dạng được mã hóa trước khi chuyển dữ liệu. Mặt khác, hoặc ngoài ra, dữ liệu có thể được lưu trữ cùng với siêu dữ liệu tương ứng trong bộ nhớ thứ nhất 104 hoặc bộ nhớ thứ hai 106 trước khi chuyển dữ liệu. Ví dụ của siêu dữ liệu này là siêu dữ liệu chẵn lẻ (trong các ví dụ mã sửa lỗi (error-correcting code - ECC), đôi khi được gọi là hội chứng), có thể bảo vệ dữ liệu tương ứng chống lại các thay đổi bit lỗi (nghĩa là, việc hỏng dữ liệu). Một ví dụ khác của siêu dữ liệu này là bản tóm tắt để băm và xác thực. Liệu việc xử lý có tạo ra siêu dữ liệu bổ sung hay không phụ thuộc vào loại xử lý. Ví dụ, việc xử lý mã hóa tại chỗ có thể không tạo ra siêu dữ liệu bổ sung. Như được mô tả dưới đây, siêu dữ liệu có thể được lưu trữ tại một địa chỉ khác mà khác với địa chỉ tại đó dữ liệu ban đầu có thể được lưu trữ.

Mặc dù logic xử lý thứ nhất 110 và logic xử lý thứ hai 112 có thể thực hiện các chức năng hoặc các hoạt động khác nhau, ít nhất một hoạt động như vậy có thể được kích hoạt hoặc được thực hiện một cách có chọn lọc (và ngược lại, bị vô hiệu hóa hoặc bỏ qua một cách có chọn lọc) theo dấu hiệu được mô tả dưới đây. Nghĩa là, logic xử lý thứ nhất 110 và logic xử lý thứ hai 112 có thể được áp dụng một cách có chọn lọc cho dữ liệu cho bước xử lý thứ nhất và xử lý thứ hai dữ liệu một cách có chọn lọc. Việc bỏ qua các chức năng xử lý hoặc logic xử lý như vậy có thể giảm lượng thời gian cần thiết để chuyển dữ liệu, tiết kiệm công suất, và mang lại các lợi ích khác.

Hoạt động hoặc chức năng xử lý thứ nhất mà logic xử lý thứ nhất 110, khi được kích hoạt hoặc được áp dụng cho dữ liệu, có thể thực hiện có thể là đảo ngược của hoạt động hoặc chức năng xử lý thứ hai mà logic xử lý thứ hai 112, khi được kích hoạt hoặc được áp dụng cho dữ liệu, có thể thực hiện. Trong một ví dụ trong đó dữ liệu được chuyển từ bộ nhớ thứ nhất 104 đến bộ nhớ thứ hai 106, logic xử lý thứ nhất 110 có thể

giải mã dữ liệu sau khi dữ liệu được đọc từ bộ nhớ thứ nhất 104, và logic xử lý thứ hai 112 có thể mã hóa (nghĩa là, mã hóa lại) dữ liệu này trước khi dữ liệu được lưu trữ trong bộ nhớ thứ hai 106. Trên Fig.1, mũi tên nét đứt 114 về mặt khái niệm chỉ báo việc chuyển dữ liệu này từ bộ nhớ thứ nhất 104 đến bộ nhớ thứ hai 106, bao gồm việc giải mã bởi logic xử lý thứ nhất 110 và việc mã hóa lại bởi logic xử lý thứ hai 112. Mặt khác, hoặc ngoài ra, trong một ví dụ (không được thể hiện trên hình vẽ) trong đó dữ liệu được chuyển từ bộ nhớ thứ hai 106 đến bộ nhớ thứ nhất 104, logic xử lý thứ hai 112 có thể giải mã dữ liệu sau khi dữ liệu được đọc từ bộ nhớ thứ hai 106, và logic xử lý thứ nhất 110 có thể mã hóa lại dữ liệu này trước khi dữ liệu được lưu trữ trong bộ nhớ thứ nhất 104.

Việc liệu bước xử lý thứ nhất bởi logic xử lý thứ nhất 110 xảy ra hay được bỏ qua, và việc liệu bước xử lý thứ hai bởi logic xử lý thứ hai 112 xảy ra hay được bỏ qua, có thể dựa trên trạng thái của chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ. Do đó, việc chuyển dữ liệu từ bộ nhớ thứ nhất 104 đến bộ nhớ thứ hai 106 có thể bao gồm việc logic xử lý thứ nhất 110 giải mã dữ liệu được đọc từ bộ nhớ thứ nhất 104 nếu chỉ báo bỏ qua không được khẳng định, và bỏ qua giải mã dữ liệu được đọc từ bộ nhớ thứ nhất 104 nếu chỉ báo bỏ qua được khẳng định. Trong ví dụ này, việc chuyển dữ liệu từ bộ nhớ thứ nhất 104 đến bộ nhớ thứ hai 106 cũng có thể bao gồm việc logic xử lý thứ hai 112 mã hóa lại dữ liệu này nếu chỉ báo bỏ qua không được khẳng định, và bỏ qua việc mã hóa lại nếu chỉ báo bỏ qua được khẳng định. Việc bỏ qua việc giải mã dữ liệu sau khi dữ liệu được đọc từ bộ nhớ thứ nhất 104 và bỏ qua việc mã hóa lại dữ liệu này trước khi nó được lưu trữ trong bộ nhớ thứ hai 106 do đó bảo tồn dữ liệu ở dạng ban đầu (được mã hóa) của nó. Trên Fig.1, mũi tên nét đứt 116 khác về mặt khái niệm chỉ báo việc chuyển dữ liệu từ bộ nhớ thứ nhất 104 đến bộ nhớ thứ hai 106 trong đó việc giải mã bởi logic xử lý thứ nhất 110 được bỏ qua và việc mã hóa lại bởi logic xử lý thứ hai 112 được bỏ qua.

Như được mô tả dưới đây, việc bỏ qua việc giải mã dữ liệu được lưu trữ ở dạng được mã hóa trong bộ nhớ thứ nhất 104 và mã hóa lại dữ liệu được giải mã trước khi lưu trữ dữ liệu được mã hóa lại vào bộ nhớ thứ hai 106 có thể xảy ra khi, ví dụ, các khóa mã hóa (không được thể hiện trên Fig.1) được sử dụng để bảo vệ dữ liệu trong các bộ nhớ thứ nhất 104 và bộ nhớ thứ hai 106, một cách tương ứng, là giống hệt nhau.

Các ví dụ của các cách để cung cấp các khóa giống hệt này được mô tả dưới đây. Có thể có nhiều khóa, mỗi trong số chúng được kết hợp với vùng bộ nhớ. Ví dụ, logic xử lý thứ nhất 110 có thể sử dụng khóa thứ nhất để bảo vệ dữ liệu được lưu trữ trong vùng 118 trong bộ nhớ thứ nhất 104, và logic xử lý thứ hai 112 có thể sử dụng khóa thứ hai giống hệt khóa thứ nhất để bảo vệ dữ liệu được lưu trữ trong vùng 120 trong bộ nhớ thứ hai 106.

Như được minh họa trên Fig.2, theo một phương án minh họa hoặc ví dụ khác, thiết bị điện toán 200 có thể bao gồm CPU 202, bộ nhớ thứ nhất 204, bộ nhớ thứ hai 206, bộ điều khiển bộ nhớ thứ nhất 208, và bộ điều khiển bộ nhớ thứ hai 210, được liên kết bởi một hoặc nhiều bus hoặc các liên kết 212. Các bộ điều khiển bộ nhớ thứ nhất 208 và thứ hai 210 là các loại của các bộ xử lý hoặc các hệ thống xử lý. Các bộ điều khiển bộ nhớ thứ nhất 208 và thứ hai 210 có thể điều khiển một số khía cạnh của các giao tác bộ nhớ theo cách thông thường. Các chức năng của bộ điều khiển bộ nhớ là thông thường và do đó đã được biết rõ bởi người có hiểu biết trung bình trong lĩnh vực không được mô tả ở đây.

Bộ điều khiển bộ nhớ thứ nhất 208 có thể bao gồm bộ tăng tốc bộ nhớ thứ nhất 214. Bộ điều khiển bộ nhớ thứ hai 210 tương tự có thể bao gồm bộ tăng tốc bộ nhớ thứ hai 216. Các bộ tăng tốc bộ nhớ thứ nhất 214 và thứ hai 216 là các loại của các bộ xử lý hoặc các hệ thống xử lý. Theo phương án được minh họa, các bộ tăng tốc bộ nhớ thứ nhất 214 và thứ hai 216 có thể được bao gồm để giảm tải một số tác vụ xử lý hoặc các hoạt động mà nếu không có thể được thực hiện bởi CPU 202, chẳng hạn như các hoạt động được mô tả ở trên đối với logic xử lý thứ nhất 110 và thứ hai 112 (Fig.1). Ví dụ, bộ tăng tốc bộ nhớ thứ nhất 214 có thể được tạo cấu hình để, trong số các chức năng khác, mã hóa dữ liệu trước khi lưu trữ nó trong bộ nhớ thứ nhất 204 và để giải mã dữ liệu sau khi đọc nó từ bộ nhớ thứ nhất 204. Tương tự, bộ tăng tốc bộ nhớ thứ hai 216 có thể được tạo cấu hình để, trong số các chức năng khác, mã hóa dữ liệu trước khi lưu trữ nó trong bộ nhớ thứ hai 206 và để giải mã dữ liệu sau khi đọc nó từ bộ nhớ thứ hai 206.

Việc mã hóa và việc giải mã bởi các bộ tăng tốc bộ nhớ thứ nhất 214 và thứ hai 216 có thể được thực hiện và được bỏ qua một cách có chọn lọc, dựa trên trạng thái

của chỉ báo bỏ qua. Trong một ví dụ trong đó dữ liệu được chuyển từ bộ nhớ thứ nhất 204 đến bộ nhớ thứ hai 206, việc chuyển dữ liệu có thể bao gồm việc bộ điều khiển bộ nhớ thứ nhất 208 cung cấp dữ liệu được đọc từ bộ nhớ thứ nhất 204 cho bộ tăng tốc bộ nhớ thứ nhất 214 nếu chỉ báo bỏ qua không được khẳng định. Trong ví dụ này, việc chuyển dữ liệu cũng có thể bao gồm việc bộ điều khiển bộ nhớ thứ nhất 208 bỏ qua hoặc không cung cấp dữ liệu được đọc từ bộ nhớ thứ nhất 204 cho bộ tăng tốc bộ nhớ thứ nhất 214 nếu chỉ báo bỏ qua được khẳng định. Khi bộ điều khiển bộ nhớ thứ nhất 208 bỏ qua bộ tăng tốc bộ nhớ thứ nhất 214 trong khi đọc dữ liệu từ bộ nhớ thứ nhất 204, bộ tăng tốc bộ nhớ thứ nhất 214 không nỗ lực giải mã dữ liệu này, và bộ điều khiển bộ nhớ thứ nhất 208 chuyển dữ liệu ở dạng ban đầu (được mã hóa) của nó đến bộ điều khiển bộ nhớ thứ hai 210 thông qua liên kết 212. Trong ví dụ này, việc chuyển dữ liệu có thể còn bao gồm việc bộ điều khiển bộ nhớ thứ hai 210 cung cấp dữ liệu nhận được (thông qua liên kết 212) từ bộ điều khiển bộ nhớ thứ nhất 208 cho bộ tăng tốc bộ nhớ thứ hai 216 nếu chỉ báo bỏ qua không được khẳng định. Trong ví dụ này, việc chuyển dữ liệu có thể còn bao gồm việc bộ điều khiển bộ nhớ thứ hai 210 bỏ qua hoặc không cung cấp dữ liệu nhận được cho bộ tăng tốc bộ nhớ thứ hai 216 nếu chỉ báo bỏ qua được khẳng định. Khi bộ điều khiển bộ nhớ thứ hai 210 bỏ qua bộ tăng tốc bộ nhớ thứ hai 216 trong khi lưu trữ dữ liệu trong bộ nhớ thứ hai 206, bộ tăng tốc bộ nhớ thứ hai 216 không nỗ lực mã hóa dữ liệu này, và bộ điều khiển bộ nhớ thứ hai 210 lưu trữ dữ liệu ở dạng ban đầu (được mã hóa) trong đó nó đã được nhận. Trên Fig.2, mũi tên nét đứt 218 về mặt khái niệm chỉ báo việc chuyển dữ liệu từ bộ nhớ thứ nhất 204 đến bộ nhớ thứ hai 206 trong đó các bộ tăng tốc bộ nhớ thứ nhất 214 và thứ hai 216 không được bỏ qua. Mũi tên nét đứt 220 khác về mặt khái niệm chỉ báo việc chuyển dữ liệu từ bộ nhớ thứ nhất 204 đến bộ nhớ thứ hai 206 trong đó các bộ tăng tốc bộ nhớ thứ nhất 214 và thứ hai 216 được bỏ qua. Trong một số ví dụ, CPU 202 có thể đóng vai trò trong việc chuyển dữ liệu giữa các bộ nhớ 204 và 206, chẳng hạn như, ví dụ, khởi tạo giao tác chuyển bộ nhớ, xác định khi nào giao tác được hoàn tất, v.v..

Các khóa có thể được sử dụng để bảo vệ dữ liệu được mã hóa trong các bộ nhớ 204 và 206 theo cách được mô tả ở trên đối với phương án được minh họa trên Fig.1. Ví dụ, bộ điều khiển bộ nhớ thứ nhất 210 có thể sử dụng khóa thứ nhất để bảo vệ dữ liệu được lưu trữ trong vùng 222 trong bộ nhớ thứ nhất 204, và bộ điều khiển bộ nhớ

thứ hai 212 có thể sử dụng khóa thứ hai giống hệt khóa thứ nhất để bảo vệ dữ liệu được lưu trữ trong vùng 224 trong bộ nhớ thứ hai 206.

Thông tin chẩn lẻ hoặc siêu dữ liệu khác tương ứng với dữ liệu được lưu trữ trong bộ nhớ thứ nhất 204 hoặc bộ nhớ thứ hai 206 cũng có thể được lưu trữ. Các hoạt động hoặc các chức năng xử lý liên quan đến siêu dữ liệu này có thể được thực hiện và được bỏ qua một cách có chọn lọc, dựa trên trạng thái của chỉ báo bỏ qua. Ví dụ, các hoạt động chẩn lẻ (ví dụ, việc tạo ra thông tin chẩn lẻ, việc phát hiện hoặc sửa lỗi, v.v.) bởi các bộ tăng tốc bộ nhớ thứ nhất 214 và thứ hai 216 có thể được thực hiện và được bỏ qua một cách có chọn lọc, dựa trên trạng thái của chỉ báo bỏ qua. Trong một ví dụ trong đó dữ liệu được bảo vệ chẩn lẻ được chuyển từ bộ nhớ thứ nhất 204 đến bộ nhớ thứ hai 206, việc chuyển dữ liệu có thể bao gồm việc bộ điều khiển bộ nhớ thứ nhất 208 cung cấp cả dữ liệu được đọc từ bộ nhớ thứ nhất 204 và thông tin chẩn lẻ tương ứng (ví dụ, mã sửa lỗi hoặc “ECC”) được đọc từ bộ nhớ thứ nhất 204 cho bộ tăng tốc bộ nhớ thứ nhất 214 nếu chỉ báo bỏ qua không được khẳng định, nhờ đó kích hoạt hoặc cho phép bộ tăng tốc bộ nhớ thứ nhất 214 thực hiện hoạt động sửa lỗi trên dữ liệu bằng cách sử dụng ECC. Trong ví dụ này, việc chuyển dữ liệu cũng có thể bao gồm việc bộ điều khiển bộ nhớ thứ nhất 208 bỏ qua bộ tăng tốc bộ nhớ thứ nhất 214 nếu chỉ báo bỏ qua được khẳng định, nhờ đó vô hiệu hóa hoặc loại trừ bộ tăng tốc bộ nhớ thứ nhất 214 khỏi việc thực hiện hoạt động sửa lỗi trên dữ liệu. Khi bộ điều khiển bộ nhớ thứ nhất 208 bỏ qua bộ tăng tốc bộ nhớ thứ nhất 214 trong khi đọc dữ liệu được bảo vệ chẩn lẻ từ bộ nhớ thứ nhất 204, bộ tăng tốc bộ nhớ thứ nhất 214 chuyển dữ liệu cũng như thông tin chẩn lẻ tương ứng ở dạng ban đầu của chúng đến bộ điều khiển bộ nhớ thứ hai 210 thông qua liên kết 212. Trong ví dụ này, việc chuyển dữ liệu và siêu dữ liệu có thể còn bao gồm việc bộ điều khiển bộ nhớ thứ hai 210 cung cấp dữ liệu nhận được từ bộ điều khiển bộ nhớ thứ nhất 210 cho bộ tăng tốc bộ nhớ thứ hai 216 nếu chỉ báo bỏ qua không được khẳng định, nhờ đó kích hoạt hoặc cho phép bộ tăng tốc bộ nhớ thứ hai 216 tái tạo ECC từ dữ liệu. Trong ví dụ này, việc chuyển dữ liệu có thể còn bao gồm việc bộ điều khiển bộ nhớ thứ hai 210 bỏ qua hoặc không cung cấp dữ liệu nhận được và ECC cho bộ tăng tốc bộ nhớ thứ hai 214 nếu chỉ báo bỏ qua được khẳng định, nhờ đó vô hiệu hóa hoặc loại trừ bộ tăng tốc bộ nhớ thứ hai 216 khỏi việc tái tạo ECC. Khi bộ điều khiển bộ nhớ thứ hai 210 bỏ qua bộ tăng tốc bộ nhớ thứ hai

216 trong khi lưu trữ dữ liệu được bảo vệ ECC trong bộ nhớ thứ hai 206, bộ điều khiển bộ nhớ thứ hai 210 lưu trữ dữ liệu và ECC tương ứng ở các dạng ban đầu trong đó bộ điều khiển bộ nhớ thứ hai 210 nhận dữ liệu và ECC tương ứng.

Do vị trí của ECC trong bộ nhớ thứ hai 206 phụ thuộc vào cấu hình tại logic xử lý thứ hai 112, logic xử lý thứ nhất 110 có thể không biết địa chỉ đích cho ECC trong bộ nhớ thứ hai 206. Do đó, logic xử lý thứ nhất 110 có thể sử dụng địa chỉ cơ sở của dữ liệu ban đầu tại bộ nhớ thứ hai 206 làm địa chỉ đích cho giao tác mang ECC. Do logic xử lý thứ hai 112 nhận giao tác (với chỉ báo bỏ qua, ví dụ, tín hiệu bus, được khẳng định để chỉ báo rằng giao tác này mang ECC và không phải dữ liệu ban đầu), logic xử lý thứ hai 112 có thể sử dụng cấu hình được lập trình trước của nó để tính toán địa chỉ đích cho ECC dựa trên địa chỉ của giao tác đang đến, là địa chỉ của dữ liệu ban đầu. Logic xử lý thứ hai 112 sau đó có thể lưu trữ ECC trong địa chỉ được tính toán trong bộ nhớ thứ hai 206.

Chỉ báo bỏ qua được mô tả ở trên có thể có dạng bất kỳ. Ví dụ, chỉ báo bỏ qua có thể là tín hiệu mà một thành phần tạo ra khi thành phần này đọc dữ liệu từ bộ nhớ bằng cách sử dụng bảng trang (không được thể hiện trên hình vẽ). Như được hiểu bởi người có hiểu biết trung bình trong lĩnh vực, bảng trang là cấu trúc dữ liệu trong đó được lưu trữ các ánh xạ hoặc các bản dịch giữa các địa chỉ bộ nhớ ảo và vật lý, do đó cho phép thành phần, chẳng hạn như CPU, bộ điều khiển bộ nhớ, bộ tăng tốc, v.v., xác định các địa chỉ vật lý là mục tiêu của giao tác bộ nhớ. Một hoặc nhiều bit trong bảng trang có thể có sẵn để lưu trữ cái đôi khi được gọi là thông tin thuộc tính phần cứng. Thuộc tính phần cứng dựa trên trang (Page-Based Hardware Attribute - PBHA) đã biết là ví dụ về thông tin thuộc tính phần cứng được lưu trữ trong bảng trang. Khi bảng trang được đọc, PBHA, hoặc các tín hiệu có nguồn gốc từ đó, có thể được truyền qua hệ thống bộ nhớ thông qua các bus như một phần của giao tác bộ nhớ. Theo một khía cạnh của sáng chế, trong một số ví dụ, bất kỳ trong số các bộ điều khiển bộ nhớ 208 hoặc 210 được mô tả ở trên (hoặc các bộ tăng tốc 214 hoặc 216 của chúng, một cách tương ứng) có thể đọc bit PBHA hoặc thông tin thuộc tính phần cứng khác được kết hợp với dữ liệu là đối tượng của giao tác chuyển bộ nhớ.

Trong một ví dụ trong đó dữ liệu được chuyển từ bộ nhớ thứ nhất 204 đến bộ nhớ thứ hai 206 (Fig.2), việc chuyển dữ liệu có thể bao gồm bộ điều khiển bộ nhớ thứ nhất 208 đọc bảng trang để xác định không chỉ địa chỉ trong bộ nhớ thứ nhất 204 tại đó dữ liệu được đặt mà cả thông tin thuộc tính phần cứng được kết hợp với địa chỉ này (hoặc vùng bộ nhớ chứa địa chỉ này). Thông tin thuộc tính phần cứng có thể có, ví dụ, giá trị là “1” để chỉ báo việc kích hoạt bước xử lý thứ nhất và bước xử lý thứ hai, và giá trị là “0” để chỉ báo việc bỏ qua bước xử lý thứ nhất và bước xử lý thứ hai. Theo đó, trong một ví dụ trong đó dữ liệu được chuyển từ bộ nhớ thứ nhất 204 đến bộ nhớ thứ hai 206 (Fig.2), thông tin thuộc tính phần cứng có thể có giá trị là “1” để chỉ báo việc kích hoạt kiểm tra lỗi (ví dụ, sửa lỗi) bởi bộ tăng tốc bộ nhớ thứ nhất 214 và kích hoạt việc tạo chẵn lẻ bởi bộ tăng tốc bộ nhớ thứ hai 216, và giá trị là “0” để chỉ báo việc bỏ qua việc kiểm tra lỗi bởi bộ tăng tốc bộ nhớ thứ nhất 214 và bỏ qua việc tạo chẵn lẻ bởi bộ tăng tốc bộ nhớ thứ hai 216. Trong một ví dụ trong đó bộ điều khiển bộ nhớ thứ nhất 208 đọc thông tin thuộc tính phần cứng này từ bảng trang như một phần của giao tác bộ nhớ trong đó bộ điều khiển bộ nhớ thứ nhất 208 đọc dữ liệu từ bộ nhớ thứ nhất 204, thông tin thuộc tính phần cứng có thể được truyền trên liên kết 212 cùng với dữ liệu như một phần của giao tác được đọc.

Trong ví dụ này, thông tin thuộc tính phần cứng chỉ báo cho các bộ điều khiển bộ nhớ 208 và 210 xem liệu có bỏ qua các bộ tăng tốc 214 và 216 hay không (hoặc mặt khác, chỉ báo trực tiếp cho các bộ tăng tốc 214 và 216 xem thực hiện các hoạt động chẵn lẻ hay bỏ qua các hoạt động chẵn lẻ). Tuy nhiên, trong các ví dụ khác thông tin thuộc tính phần cứng này một cách tương tự có thể chỉ báo cho các thành phần này xem thực hiện việc giải mã và mã hóa lại hay bỏ qua việc giải mã và mã hóa lại, xem thực hiện việc giải nén và nén lại hay bỏ qua việc giải nén và nén lại, v.v..

Như được minh họa trên Fig.3, các phương án khác nhau có thể bao gồm các thành phần ngoài các thành phần được mô tả ở trên. Thiết bị 300, có thể là ví dụ của thiết bị 100 được mô tả ở trên (Fig.1) hoặc 200 (Fig.2), có thể bao gồm các thành phần bổ sung này. Ví dụ, thiết bị 300 có thể bao gồm CPU 302, bộ nhớ truy cập ngẫu nhiên động (dynamic random access memory - DRAM) 304, bộ nhớ truy cập ngẫu nhiên không khả biến (non-volatile random access memory - NVRAM) 306, bộ điều khiển DRAM 308, và bộ điều khiển NVRAM 310, được liên kết bởi một hoặc nhiều bus

hoặc các liên kết 312. DRAM 304 có thể bao gồm, ví dụ, DRAM đồng bộ tốc độ dữ liệu gấp đôi (double data-rate synchronous DRAM - DDR-SDRAM). NVRAM 306 có thể bao gồm, ví dụ, bộ nhớ flash. Bộ điều khiển DRAM 308 có thể bao gồm bộ tăng tốc DRAM 314. Tương tự, bộ điều khiển NVRAM 310 có thể bao gồm bộ tăng tốc NVRAM 316. Các phần tử nêu trên của thiết bị 300 có thể là tương tự như các phần tử được mô tả ở trên của các thiết bị 100 hoặc 200. Ví dụ, DRAM 304 và NVRAM 306 có thể là các ví dụ của các bộ nhớ thứ nhất 204 và thứ hai 206, một cách tương ứng.

Ngoài các phần tử nêu trên, thiết bị 300 có thể bao gồm, ví dụ, các bộ xử lý khác, chẳng hạn như NPU 318, và các loại bộ nhớ bổ sung, chẳng hạn như bộ nhớ lưu trữ 320. Bộ điều khiển bộ nhớ lưu trữ 322 có thể được ghép nối với bộ nhớ lưu trữ 320. Thiết bị 300 cũng có thể bao gồm gốc tin cậy (root of trust - RoT) 324, bộ tạo khóa 326, và bộ bảo vệ có thể lập trình 328, có thể hoạt động chức năng theo cách được mô tả dưới đây. Thiết bị 300 có thể bao gồm các phần tử khác, chẳng hạn như RAM tĩnh (static RAM - SRAM) 330. Trong một số ví dụ của hoạt động, dữ liệu được chuyển giữa các bộ nhớ theo cách được mô tả ở trên theo các Fig.1 đến Fig.2 có thể được lưu trữ tạm thời trong RAM tĩnh 330, hoặc được lưu trữ hoặc được đệm tạm thời ở nơi khác, mà không rời khỏi phạm vi của phần mô tả.

CPU 302, các bộ điều khiển bộ nhớ 308, 310 và 322, NPU 318, RoT 324, bộ tạo khóa 326, bộ bảo vệ 328, và SRAM 330 có thể được chứa trên hệ thống trên chip (system-on-a-chip - SoC) 332. SoC 332 có thể được ghép nối với các thành phần khác của thiết bị 300 thông qua, ví dụ, bus liên kết thành phần ngoại vi (Peripheral Component Interconnect - PCI) 334 hoặc bus liên hệ thống khác. Theo đó, SoC 332 có thể bao gồm bộ điều khiển PCI 336. Bộ điều khiển PCI 336 có thể bao gồm bộ tăng tốc PCI 338, có thể hoạt động theo cách được mô tả dưới đây. Ngoại vi PCI 340 có thể được tạo cấu hình để truyền thông với SoC 332 thông qua bus PCI 334 và bộ điều khiển PCI 336.

Trên Fig.4, phương pháp ví dụ 400 để chuyển dữ liệu từ một bộ nhớ (“thứ nhất”) sang bộ nhớ khác (“thứ hai”) có thể được thực hiện trong bất kỳ trong số các thiết bị 100 (Fig.1), 200 (Fig.2) hoặc 300 (Fig.3) được mô tả ở trên hoặc thiết bị bất kỳ khác không nhất quán với phần mô tả sau. Trong phần mô tả sau đây về phương pháp

400, các thuật ngữ “bộ nhớ thứ nhất” và “bộ nhớ thứ hai” có thể bao gồm rộng hai bộ nhớ bất kỳ hoặc các thiết bị lưu trữ dữ liệu khác mà giữa chúng dữ liệu có thể được chuyển thông qua bus dữ liệu hoặc liên kết tương tự. Các bộ nhớ thứ nhất và thứ hai mỗi trong số chúng có thể bao gồm số lượng và loại bất kỳ của các thiết bị lưu trữ vật lý.

Như được chỉ báo bởi khối 402, phương pháp 400 có thể bao gồm bước đọc dữ liệu từ bộ nhớ thứ nhất. Như được chỉ báo bởi khối 404, phương pháp 400 có thể bao gồm bước xác định nếu chỉ báo bỏ qua được khẳng định. Như được chỉ báo bởi các khối 406 và 408, một cách tương ứng, phương pháp 400 có thể bao gồm bước xử lý thứ nhất và bước xử lý thứ hai dữ liệu nếu chỉ báo bỏ qua không được khẳng định. Ví dụ, bước xử lý thứ nhất có thể bao gồm ít nhất một trong số giải mã, kiểm tra chẵn lẻ, và giải nén, trong khi bước xử lý thứ hai có thể bao gồm ít nhất một trong số mã hóa lại, tạo chẵn lẻ lại, và nén lại, một cách tương ứng. Như được chỉ báo bởi các khối 410 và 412, một cách tương ứng, phương pháp 400 có thể bao gồm bước bỏ qua bước xử lý thứ nhất và bước xử lý thứ hai dữ liệu nếu chỉ báo bỏ qua được khẳng định. Như được chỉ báo bởi khối 414, phương pháp 400 có thể bao gồm bước lưu trữ dữ liệu trong bộ nhớ thứ hai hoặc sau việc xử lý (các khối 406 và 408) nếu chỉ báo bỏ qua không được khẳng định hoặc sau việc bỏ qua (các khối 410 và 412) nếu chỉ báo bỏ qua được khẳng định.

Ngoài ra, lưu ý rằng trong một ví dụ trong đó siêu dữ liệu tương ứng với dữ liệu cũng được lưu trữ (xem liệu trong cùng bộ nhớ như dữ liệu hay trong bộ nhớ khác), siêu dữ liệu một cách tương tự có thể được chuyển đến bộ nhớ khác theo phương pháp 400. Nghĩa là, việc chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai theo cách được mô tả ở trên cũng có thể bao gồm bước chuyển siêu dữ liệu được kết hợp bất kỳ từ bộ nhớ thứ nhất đến bộ nhớ thứ hai theo cách tương tự.

Trên Fig.5, đường điều khiển ví dụ hoặc trình tự các hành động để tạo cấu hình hệ thống để chuyển dữ liệu giữa các bộ nhớ được minh họa bằng cách sử dụng sơ đồ khối chức năng 500. Ví dụ được minh họa trên Fig.5 liên quan đến trường hợp sử dụng hoặc kịch bản hoạt động trong đó thiết bị, chẳng hạn như thiết bị 300 được mô tả ở trên (Fig.3), chuyển đổi từ chế độ hoạt động sang chế độ ngủ đông. Trong việc chuyển

đổi từ chế độ hoạt động sang chế độ ngủ đông, dữ liệu chẳng hạn như dữ liệu ngữ cảnh chính của hệ thống hoạt động có thể được chuyển từ DRAM 304 sang NVRAM 306. Do chế độ ngủ đông này đã được biết rõ bởi người có hiểu biết trung bình trong lĩnh vực, nên các khía cạnh không trực tiếp liên quan đến việc chuyển dữ liệu giữa các bộ nhớ không được mô tả chi tiết thêm ở đây.

Dữ liệu ngữ cảnh chính của hệ thống hoạt động có thể được lưu trữ ở dạng được mã hóa trong DRAM 304 trong khi thiết bị ở trong chế độ hoạt động và một cách tương tự có thể được lưu trữ ở dạng được mã hóa trong NVRAM 306 trong khi thiết bị ở trong chế độ ngủ đông. Trong ví dụ dưới đây, các khóa mã hóa được tạo ra và được sử dụng để kích hoạt việc truy cập vào dữ liệu ngữ cảnh chính cả trước và sau khi dữ liệu ngữ cảnh chính được chuyển.

Như được chỉ báo bởi mũi tên 502, bộ tạo khóa 326 có thể tạo ra một hoặc nhiều khóa phần cứng. Do khóa phần cứng này có thể không hiển thị với phần mềm, nên bộ tạo khóa 326 có thể cung cấp cho phần mềm với khóa truy cập (handle) cho các khóa phần cứng. Ví dụ, bằng cách sử dụng thông tin được mã hóa bảo mật bởi bộ bảo vệ 328 (Fig.3) bộ tạo khóa 326 có thể tạo ra khóa gốc ("Root_key"), có thể là loại khóa công khai. RoT 324 có thể nhận khóa truy cập cho khóa gốc từ bộ tạo khóa 326. Như được chỉ báo bởi mũi tên 508, RoT 324 có thể cung cấp khóa truy cập ("Handle_root") cho khóa gốc tới CPU 302 (ví dụ, cho chính hệ thống hoạt động). Như được chỉ báo bởi các mũi tên 510 và 514, CPU 302 (ví dụ, hệ thống hoạt động chính) có thể chuyển khóa truy cập cho bộ điều khiển DRAM 308 và bộ điều khiển NVRAM 310, sao cho bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316 có thể sử dụng khóa truy cập để lấy khóa phần cứng mà không để lộ giá trị của khóa cho phần mềm. Như được chỉ báo bởi các mũi tên 504 và 506, một cách tương ứng, RoT 324 có thể cung cấp cùng khóa gốc này cho cả bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316. RoT 324 cũng cung cấp thông tin phương pháp suy ra khóa cho cả bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316 mà bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316 mỗi trong số chúng có thể sử dụng để suy ra một hoặc nhiều khóa riêng tư từ khóa gốc. Do RoT 324 có thể cung cấp cùng thông tin phương pháp suy ra khóa cho cả bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316, nên bộ tăng tốc DRAM 314 và bộ tăng tốc

NVRAM có thể suy ra các khóa riêng tư giống hệt nhau mỗi lần chúng suy ra khóa riêng tư.

Trong một số ví dụ của hoạt động, bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316 mỗi trong số chúng có thể suy ra chỉ một khóa riêng tư bởi vì dữ liệu ngữ cảnh chính chiếm giữ chỉ một vùng (hoặc “đệm”) trong DRAM 304 và chỉ một vùng trong NVRAM 306. Trong các ví dụ khác của hoạt động, bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316 mỗi trong số chúng có thể suy ra nhiều hơn một khóa riêng tư bởi vì dữ liệu ngữ cảnh chính chiếm giữ nhiều hơn một vùng trong DRAM 304 và nhiều hơn một vùng trong NVRAM 306. Trong ví dụ được minh họa trên Fig.5, bộ tăng tốc DRAM 314 và bộ tăng tốc NVRAM 316 mỗi trong số chúng có thể suy ra một khóa (“Derived_key_1”) giống hệt khóa mà bộ kia suy ra.

Dữ liệu ngữ cảnh chính được lưu trữ trong DRAM 304 được bảo vệ bởi khóa được suy ra. Bộ điều khiển DRAM 308 và bộ tăng tốc DRAM 314 không cho phép thực thể bất kỳ, chẳng hạn như, ví dụ, CPU 302, truy cập dữ liệu ngữ cảnh chính được lưu trữ trong DRAM 304 trừ khi thực thể truy cập DRAM 304 sử dụng khóa truy cập cho khóa được suy ra (“Handle_1”) hoặc khóa truy cập cho khóa gốc (“Handle_root”).

CPU 302 có thể xác định xem có chuyển từ chế độ hoạt động sang chế độ ngủ đông theo cách thông thường hay không. Phần mềm trong đó CPU 302 hoạt động có thể bao gồm phần mềm lưu ngữ cảnh. Khi CPU 302 xác định chuyển đổi từ chế độ hoạt động sang chế độ ngủ đông, CPU 302, dưới sự điều khiển của phần mềm lưu ngữ cảnh, có thể khởi tạo việc chuyển dữ liệu ngữ cảnh chính từ DRAM 304 sang NVRAM 306. CPU 302 có thể khiến chỉ báo bỏ qua được khẳng định theo cách được mô tả ở trên, chẳng hạn như đọc thông tin thuộc tính bảng trang được kết hợp với vùng bộ nhớ trong đó dữ liệu ngữ cảnh chính được lưu trữ. Kết quả là, dữ liệu ngữ cảnh chính được chuyển ngoài DRAM 304 mà không có việc bộ tăng tốc DRAM 314 giải mã nó, và được chuyển vào NVRAM 306 mà không có việc bộ tăng tốc NVRAM 316 mã hóa lại nó. Thay thế cho việc CPU 302 điều khiển khía cạnh của việc chuyển dữ liệu mà khiến chỉ báo bỏ qua được khẳng định, công cụ xử lý bất kỳ khác, chẳng hạn như bộ điều khiển DRAM 308, bộ tăng tốc DRAM 314, bộ điều khiển NVRAM 310, bộ tăng tốc NVRAM 316, công cụ DMA (không được thể hiện trên hình vẽ), v.v., có

thể điều khiển khía cạnh đó của việc chuyển dữ liệu, như được mô tả ở trên đối với các ví dụ khác.

Trong ví dụ này, việc chuyển dữ liệu từ DRAM 304 đến NVRAM 306 có thể bao gồm không chỉ CPU 302 điều khiển việc chuyển của dữ liệu ngữ cảnh chính từ DRAM 304 đến NVRAM 306 mà cả điều khiển việc chuyển của khóa được suy ra (“Derived_key_1”) và khóa truy cập của nó (“Handle_1”) từ bộ tăng tốc DRAM 314 đến bộ tăng tốc NVRAM 316. Sau khi khóa được suy ra và khóa truy cập của nó được chuyển đến bộ tăng tốc NVRAM 316, dữ liệu ngữ cảnh chính được lưu trữ trong NVRAM 306 được bảo vệ bởi khóa được suy ra theo cùng cách trong đó dữ liệu ngữ cảnh chính được bảo vệ như khi nó được lưu trữ trong DRAM 304. Nghĩa là, bộ điều khiển NVRAM 310 và bộ tăng tốc NVRAM 316 không cho phép thực thể bất kỳ, chẳng hạn như, ví dụ, CPU 302, truy cập dữ liệu ngữ cảnh chính được lưu trữ trong NVRAM 306 trừ khi thực thể truy cập NVRAM 306 sử dụng khóa truy cập cho khóa được suy ra (“Handle_1”) hoặc khóa truy cập cho khóa gốc (“Handle_root”).

Thiết bị có thể chuyển đổi từ chế độ ngủ đông trở lại chế độ hoạt động. Trong ví dụ này, dữ liệu ngữ cảnh chính có thể được chuyển từ NVRAM 306 trở lại DRAM 304. Các hoạt động tương tự như các hoạt động được mô tả ở trên đối với việc chuyển dữ liệu ngữ cảnh chính từ DRAM 304 đến NVRAM 306 có thể được thực hiện trong việc chuyển dữ liệu ngữ cảnh chính từ NVRAM 306 đến DRAM 304.

Như được minh họa trên Fig.6, theo phương án ví dụ về việc chuyển dữ liệu giữa các bộ nhớ có thể bao gồm bước chuyển dữ liệu (và các khóa) thông qua bus dữ liệu liên hệ thống an toàn, chẳng hạn như, ví dụ, bus PCI 634. Mặc dù phần mô tả dưới đây liên quan đến phương án ví dụ trong đó bus dữ liệu liên hệ thống an toàn phù hợp với đặc tả kỹ thuật PCI, nhưng theo các phương án khác bus dữ liệu liên hệ thống này có thể là thuộc loại bất kỳ mà tạo đặc tính các bộ điều khiển bus được tạo cấu hình để mã hóa và giải mã dữ liệu tại các điểm cuối bus. Bus PCI 634 có thể được ghép nối giữa hệ thống thứ nhất, chẳng hạn như SoC thứ nhất 632A, và hệ thống thứ hai, chẳng hạn như SoC thứ hai 632B. SoC thứ nhất 632A, SoC thứ hai 632B, và bus PCI 634 có thể được bao gồm trong thiết bị 600. Một trong số các SoC thứ nhất 632A và thứ hai

632B có thể là ví dụ của SoC 332 được mô tả ở trên đối với Fig.3, và SoC còn lại có thể là ví dụ của thiết bị ngoại vi PCI 340 (Fig.3).

SoC thứ nhất 632A có thể bao gồm CPU 602A, bộ điều khiển DRAM 608A, và bộ điều khiển NVRAM 610A, được liên kết bởi một hoặc nhiều bus hoặc các liên kết 612A. Bộ điều khiển DRAM 608A và bộ điều khiển NVRAM 610A có thể được ghép nối với DRAM 604A và NVRAM 606A, một cách tương ứng. Bộ điều khiển DRAM 608A và bộ điều khiển NVRAM 610A có thể bao gồm bộ tăng tốc DRAM 614A và bộ tăng tốc NVRAM 616A, một cách tương ứng. SoC thứ nhất 632A cũng có thể bao gồm RoT 624A. SoC thứ nhất 632A có thể còn bao gồm bộ điều khiển PCI 636A được ghép nối với điểm cuối thứ nhất của bus PCI 634. Bộ điều khiển PCI 636A có thể bao gồm bộ tăng tốc PCI 638A. Mặc dù không được thể hiện nhằm các mục đích ngắn gọn, nhưng SoC thứ nhất 632A cũng có thể bao gồm các phần tử khác tương tự với các phần tử được mô tả ở trên đối với SoC 332 (Fig.3), chẳng hạn như bộ tạo khóa, bộ bảo vệ có thể lập trình, các bộ nhớ khác, các bộ điều khiển bộ nhớ, các bộ xử lý, v.v..

Tương tự, SoC thứ hai 632B có thể bao gồm CPU 602B, bộ điều khiển DRAM 608B, và bộ điều khiển NVRAM 610B, được liên kết bởi một hoặc nhiều bus hoặc các liên kết 612B. Bộ điều khiển DRAM 608B và bộ điều khiển NVRAM 610B có thể được ghép nối với DRAM 604B và NVRAM 606B, một cách tương ứng. Bộ điều khiển DRAM 608B và bộ điều khiển NVRAM 610B có thể bao gồm bộ tăng tốc DRAM 614B và bộ tăng tốc NVRAM 616B, một cách tương ứng. SoC thứ hai 632B cũng có thể bao gồm RoT 624B. SoC thứ hai 632B có thể còn bao gồm bộ điều khiển PCI 636B được ghép nối với điểm cuối thứ hai của bus PCI 634. Bộ điều khiển PCI 636B có thể bao gồm bộ tăng tốc PCI 638B. Mặc dù không được thể hiện nhằm các mục đích ngắn gọn, nhưng SoC thứ hai 632B cũng có thể bao gồm các phần tử khác tương tự với các phần tử được mô tả ở trên đối với SoC 332 (Fig.3), chẳng hạn như bộ tạo khóa, bộ bảo vệ có thể lập trình, các bộ nhớ khác, các bộ điều khiển bộ nhớ, các bộ xử lý, v.v..

Trong phần mô tả sau đây về ví dụ của việc chuyển dữ liệu giữa các bộ nhớ, các khía cạnh hoạt động của các SoC 332A và 332B là tương tự với các khía cạnh được

mô tả ở trên đối với SoC 332 (Fig.3) có thể được bỏ qua cho ngắn gọn. Ví dụ, các RoT 624A và 624B có thể cung cấp các khóa mã hóa theo cách được mô tả ở trên. Trong một ví dụ trong đó dữ liệu cần được chuyển từ DRAM 604A đến DRAM 604B, các khóa giống hệt có thể được cung cấp cho bộ tăng tốc DRAM 614A và bộ tăng tốc DRAM 614B.

Các khóa mã hóa khác có thể được cung cấp cho các bộ điều khiển PCI 636A và 636B bởi, ví dụ, mô-đun nền tảng tin cậy (Trusted Platform Module - TPM) 640. Các khóa được cung cấp cho các bộ điều khiển PCI 636A và 636B có thể là giống hệt nhau. TPM 640 có thể phù hợp với tiêu chuẩn được gọi là ISO/IEC 11889.

Giao thức PCI thông thường bao gồm tính năng chuyển dữ liệu an toàn. Bộ điều khiển PCI gửi có thể được kích hoạt một cách có chọn lọc để mã hóa dữ liệu trước khi truyền dữ liệu qua bus PCI, như được hiểu bởi người có hiểu biết trung bình trong lĩnh vực. Nếu bộ điều khiển PCI gửi mã hóa dữ liệu, giao thức PCI thông báo cho bộ điều khiển PCI nhận rằng các gói dữ liệu được mã hóa, và bộ điều khiển PCI nhận giải mã các gói dữ liệu này theo đó. Nếu bộ điều khiển PCI nhận không mã hóa dữ liệu, giao thức PCI thông báo cho bộ điều khiển PCI nhận rằng các gói dữ liệu không được mã hóa, và bộ điều khiển PCI nhận không nỗ lực giải mã các gói dữ liệu này.

Theo phương án ví dụ được minh họa trên Fig.6, các bộ điều khiển PCI 638A và 638B còn có thể được tạo cấu hình để phát hiện chỉ báo bỏ qua được mô tả ở trên. Trong cùng cách được mô tả ở trên đối với các phương án khác, giao tác đọc bộ nhớ có thể dẫn đến việc truyền chỉ báo bỏ qua trên liên kết 612A cùng với dữ liệu. Bộ tăng tốc PCI 638A có thể phát hiện xem chỉ báo bỏ qua có được khẳng định hay không. Tận dụng đặc tính chuyển dữ liệu an toàn PCI được mô tả ở trên bởi đó bộ điều khiển PCI gửi có thể được kích hoạt một cách có chọn lọc để mã hóa dữ liệu trước khi truyền dữ liệu qua bus PCI, bộ tăng tốc PCI 638A có thể được tạo cấu hình để bỏ qua việc mã hóa dữ liệu nếu chỉ báo bỏ qua được khẳng định.

Trước khi dữ liệu được chuyển thông qua bus PCI 634, bộ tăng tốc DRAM 614A có thể chuyển khóa bảo vệ dữ liệu này. Đặc tính chuyển dữ liệu an toàn PCI có thể được sử dụng để chuyển khóa thông qua bus PCI 634. Trong một ví dụ trong đó dữ liệu cần được chuyển từ DRAM 604A (trong đó dữ liệu nằm ở dạng được mã hóa) tới

DRAM 604B, bộ tăng tốc DRAM 614A có thể cung cấp khóa được sử dụng để bảo vệ dữ liệu được lưu trữ tới bộ điều khiển PCI 636A theo cách mà không khiến chỉ báo bỏ qua được khẳng định. Bộ điều khiển PCI 636A do đó mã hóa khóa trước khi gửi khóa qua bus PCI 634 đến bộ điều khiển PCI 636B. Bộ điều khiển PCI 636B sau đó giải mã khóa trước khi cung cấp khóa cho bộ tăng tốc DRAM 614B.

Trong một ví dụ trong đó dữ liệu cần được chuyển từ DRAM 604A đến DRAM 604B, bộ điều khiển PCI 636A có thể đọc dữ liệu từ DRAM 604A (thông qua bộ điều khiển bộ nhớ DRAM 608A) và chuyển dữ liệu thông qua bus PCI 634. Lưu ý rằng giao tác bộ nhớ này có thể được khởi tạo không chỉ bởi bộ tăng tốc DRAM 614A trong ví dụ này mà cả (trong các ví dụ khác) bởi bất kỳ trong số các bộ xử lý được mô tả ở trên khác, chẳng hạn như CPU 602A, bộ tăng tốc NVRAM 616A, hoặc bộ điều khiển PCI 636A (hoặc bộ tăng tốc PCI 638A của nó). Như một phần của giao tác bộ nhớ này, chỉ báo bỏ qua có thể trở nên được khẳng định theo cách được mô tả ở trên đối với các phương án khác. Nếu chỉ báo bỏ qua được khẳng định, không chỉ các bộ điều khiển bộ nhớ DRAM 608A và 608B bỏ qua việc mã hóa và giải mã, mà cả bộ điều khiển PCI 636A không mã hóa dữ liệu trước khi bộ điều khiển PCI 636A gửi dữ liệu qua bus PCI 634 tới bộ điều khiển PCI 636B. Như trong các ví dụ khác được mô tả ở trên, dữ liệu không được mã hóa lại trước khi nó được chuyển (trong ví dụ này, qua bus PCI 634) bởi vì dữ liệu nằm ở dạng được mã hóa trong bộ nhớ từ đó dữ liệu được đọc, và dữ liệu tiếp tục được nằm trong cùng dạng được mã hóa trong bộ nhớ mà dữ liệu được chuyển.

Bộ điều khiển PCI 636A có thể được tạo cấu hình để bao gồm chỉ báo bỏ qua như một phần của tải tin gói dữ liệu được chuyển. Bộ điều khiển PCI 636B có thể được tạo cấu hình để trích chỉ báo bỏ qua từ tải tin. Bộ điều khiển PCI 636B có thể được tạo cấu hình để cung cấp chỉ báo bỏ qua cùng với dữ liệu được nhận tới bộ tăng tốc DRAM 614B. Trong ví dụ này, bộ tăng tốc DRAM 614B có thể phát hiện rằng chỉ báo bỏ qua được khẳng định và do đó không nỗ lực giải mã dữ liệu trước khi lưu trữ dữ liệu trong DRAM 604B.

Trên Fig.7, phương pháp 700 để chuyển khóa như một phần của phương pháp để chuyển dữ liệu từ hệ thống thứ nhất đến hệ thống thứ hai sử dụng bus liên hệ thống

an toàn (ví dụ, PCI) được minh họa. Như được mô tả ở trên đối với các phương án khác, dữ liệu có thể nằm ở dạng được mã hóa trong bộ nhớ trong hệ thống thứ nhất. Như được chỉ báo bởi khối 702, phương pháp 700 có thể bao gồm bước đọc khóa được kết hợp với dữ liệu được chuyển. Như được chỉ báo bởi khối 704, phương pháp 700 có thể còn bao gồm bước mã hóa khóa sử dụng bộ điều khiển bus dữ liệu (ví dụ, PCI) trong hệ thống thứ nhất. Như được chỉ báo bởi khối 706, bộ điều khiển bus dữ liệu sau đó có thể gửi khóa (ở dạng được mã hóa) đến hệ thống thứ hai qua bus liên hệ thống. Bộ điều khiển bus dữ liệu (ví dụ, PCI) trong hệ thống thứ hai có thể nhận và giải mã khóa, như được chỉ báo bởi khối 708. Bộ điều khiển bus dữ liệu trong hệ thống thứ hai sau đó có thể cung cấp khóa cho bộ điều khiển bộ nhớ, bộ tăng tốc bộ nhớ, hoặc bộ xử lý khác bảo vệ dữ liệu khi dữ liệu được lưu trữ trong bộ nhớ trong hệ thống thứ hai. Như được chỉ báo bởi khối 710, bộ nhớ này có thể lưu trữ khóa và nếu không thì sử dụng khóa để bảo vệ dữ liệu được lưu trữ.

Như được mô tả ở trên đối với các phương án khác, bộ điều khiển bus dữ liệu trong hệ thống thứ nhất có thể bỏ qua việc mã hóa dữ liệu được bảo vệ bởi khóa được tham chiếu ở trên khi bộ điều khiển bus dữ liệu gửi dữ liệu qua bus dữ liệu. Tương tự, bộ điều khiển bus dữ liệu trong hệ thống thứ hai có thể bỏ qua việc giải mã dữ liệu khi nó nhận dữ liệu qua bus dữ liệu. Trong hệ thống thứ hai, bộ điều khiển bus dữ liệu, bộ điều khiển bộ nhớ, bộ tăng tốc bộ nhớ, hoặc bộ xử lý khác có thể lưu trữ dữ liệu được nhận trong bộ nhớ trong hệ thống thứ hai. Dữ liệu do đó nằm trong bộ nhớ trong hệ thống thứ hai trong cùng dạng được mã hóa trong đó nó nằm trong bộ nhớ trong hệ thống thứ nhất.

Như được minh họa trên Fig.8, các phương án ví dụ của các hệ thống và các phương pháp để chuyển dữ liệu giữa các bộ nhớ có thể được cung cấp trong thiết bị điện toán cầm tay (PCD) 800. PCD 800 có thể là ví dụ của bất kỳ trong số các thiết bị 100 (Fig.1), 200 (Fig.2), 300 (Fig.3), 600 (Fig.6) được mô tả ở trên, v.v. Cần lưu ý rằng các liên kết giữa các thành phần của PCD 800 được thể hiện dưới dạng khái niệm trên Fig.8 và không nhằm mục đích đại diện cho các bus dữ liệu hoặc các liên kết dữ liệu vật lý khác. Thay vào đó, các bộ xử lý khác nhau và các bộ nhớ của PCD 800 có thể được liên kết theo cách tương tự như cách được mô tả ở trên đối với các Fig.1 đến Fig.3 và Fig.6.

PCD 800 có thể bao gồm SoC 802. SoC 802 có thể bao gồm CPU 804, GPU 806, DSP 807, bộ xử lý tín hiệu tương tự 808, hoặc các bộ xử lý khác. CPU 804 có thể bao gồm nhiều lõi, chẳng hạn như lõi thứ nhất 804A, lõi thứ hai 804B, v.v., tới lõi thứ N 804N. Trong một số ví dụ của SoC 802, CPU 804 có thể được gọi là bộ xử lý ứng dụng.

Bộ điều khiển hiển thị 810 và bộ điều khiển màn hình chạm 812 có thể được ghép nối với CPU 804. Màn hiển thị màn hình chạm 814 bên ngoài SoC 802 có thể được ghép nối với bộ điều khiển hiển thị 810 và bộ điều khiển màn hình chạm 812. PCD 800 có thể còn bao gồm bộ giải mã video 816 được ghép nối với CPU 804. Bộ khuếch đại video 818 có thể được ghép nối với bộ giải mã video 816 và màn hiển thị màn hình chạm 814. Cổng video 820 có thể được ghép nối với bộ khuếch đại video 818. Bộ điều khiển bus nối tiếp đa năng (universal serial bus - USB) 822 cũng có thể được ghép nối với CPU 804, và cổng USB 824 có thể được ghép nối với bộ điều khiển USB 822. Thẻ module định danh thuê bao (subscriber identity module - SIM) 826 cũng có thể được ghép nối với CPU 804.

Một hoặc nhiều bộ nhớ có thể được ghép nối với CPU 804. Một hoặc nhiều bộ nhớ có thể bao gồm cả bộ nhớ khả biến và bất biến. Các ví dụ của các bộ nhớ khả biến bao gồm bộ nhớ truy cập ngẫu nhiên tĩnh (static random access memory - SRAM) 828 và các RAM động (dynamic RAM - DRAM) 830 và 831. Các bộ nhớ này có thể là ở bên ngoài SoC 802, chẳng hạn như DRAM 830, hoặc bên trong SoC 802, chẳng hạn như DRAM 831. Bộ điều khiển DRAM 832 được ghép nối với CPU 804 có thể điều khiển việc ghi dữ liệu vào, và việc đọc dữ liệu từ, các DRAM 830 và 831. Theo các phương án khác, bộ điều khiển DRAM này có thể được bao gồm trong bộ xử lý, chẳng hạn như CPU 804.

CODEC âm thanh nổi 834 có thể được ghép nối với bộ xử lý tín hiệu tương tự 808. Ngoài ra, bộ khuếch đại âm thanh 836 có thể được ghép nối với CODEC âm thanh nổi 834. Các loa âm thanh nổi thứ nhất 838 và thứ hai 840, một cách tương ứng, có thể được ghép nối với bộ khuếch đại âm thanh 836. Ngoài ra, bộ khuếch đại micrô 842 có thể được ghép nối với CODEC âm thanh nổi 834, và micrô 844 có thể được ghép nối với bộ khuếch đại micrô 842. Bộ dò sóng vô tuyến điều chế tần số (frequency

modulation - FM) 846 có thể được ghép nối với CODEC âm thanh nổi 834. Anten FM 848 có thể được ghép nối với bộ dò sóng vô tuyến FM 846. Ngoài ra, các tai nghe âm thanh nổi 850 có thể được ghép nối với CODEC âm thanh nổi 834. Các thiết bị khác có thể được ghép nối với CPU 804 bao gồm một hoặc nhiều camera kỹ thuật số (ví dụ, CCD hoặc CMOS) 852. Ngoài ra, bàn phím 860, thiết bị đeo đầu mono với micrô 862, và thiết bị rung 864 có thể được ghép nối với bộ xử lý tín hiệu tương tự 808.

Bộ thu phát tần số vô tuyến (radio frequency - RF) hoặc modem 854 có thể được ghép nối với bộ xử lý tín hiệu tương tự 808 và CPU 804. Bộ chuyển mạch RF 856 có thể được ghép nối với modem 854 và anten RF 858. Mặc dù theo phương án được minh họa modem 854 được bao gồm trong cùng SoC 802 có CPU 804 và các bộ xử lý khác nhau, nhưng theo các phương án khác modem này có thể là ở bên ngoài SoC này, ví dụ, chip riêng biệt, và chính nó có thể được gọi là một loại của SoC.

SoC 802 có thể có một hoặc nhiều bộ cảm biến nhiệt bên trong hoặc trên chip 870A và có thể được ghép nối với một hoặc nhiều bộ cảm biến nhiệt bên ngoài hoặc ngoài chip 870B. Bộ điều khiển bộ chuyển đổi tương tự sang kỹ thuật số (analog-to-digital converter - ADC) 872 có thể chuyển đổi các mức sụt điện áp được tạo nên bởi các bộ cảm biến nhiệt 870A và 870B thành các tín hiệu kỹ thuật số. Nguồn cấp 874 và mạch tích hợp quản lý công suất (Power Management Integrated Circuit - PMIC) 876 có thể cấp nguồn cho SoC 802.

Mặc dù các bus hoặc các liên kết dữ liệu khác bên trong SoC 802 không được thể hiện trên hình vẽ cho các mục đích ngắn gọn, nhưng SoC 802 có thể được ghép nối với thiết bị ngoại vi PCI 878 thông qua bus PCI 880. Các ví dụ của thiết bị ngoại vi PCI 878 có thể bao gồm các bộ đệm dữ liệu camera, các bộ đệm dữ liệu đồ họa, hoặc các thiết bị ngoại vi khác có các bộ nhớ.

Firmware hoặc phần mềm có thể được lưu trữ trong bất kỳ bộ nhớ nào được mô tả ở trên, chẳng hạn như DRAM 830 hoặc 831, SRAM 828, v.v. hoặc có thể được lưu trữ trong bộ nhớ cục bộ có thể truy cập trực tiếp bởi phần cứng bộ xử lý trên đó phần mềm hoặc firmware thực thi. Việc thực thi của firmware hoặc phần mềm này có thể điều khiển các khía cạnh của bất kỳ trong số các phương pháp được mô tả ở trên hoặc tạo cấu hình các khía cạnh bất kỳ trong số các hệ thống được mô tả ở trên. Bất kỳ bộ

nhớ hoặc phương tiện lưu trữ bất biến nào khác có firmware hoặc phần mềm được lưu trữ trong đó ở dạng có thể đọc được bằng máy tính để thực thi bởi phần cứng bộ xử lý có thể là ví dụ của "phương tiện có thể đọc được bằng máy tính", như thuật ngữ này được hiểu trong từ điển sáng chế.

Việc chuyển dữ liệu giữa các bộ nhớ theo sáng chế có thể được bao gồm trong bất kỳ trong số các hệ thống, các phương pháp, phương tiện đọc được bằng máy tính ví dụ, v.v., được mô tả ở trên. Các phương án thay thế sẽ trở nên rõ ràng đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật mà sáng chế thuộc về. Do đó, mặc dù các khía cạnh được chọn đã được minh họa và được mô tả chi tiết, nhưng có thể hiểu rằng các thay thế và sửa đổi khác nhau có thể được thực hiện trong đó.

Các ví dụ triển khai được mô tả trong các mục được đánh số dưới đây:

1. Phương pháp để chuyển dữ liệu giữa các bộ nhớ, phương pháp này bao gồm các bước:

đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất;

xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai, việc chuyển bao gồm bước bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định, việc chuyển còn bao gồm bước bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định; và

lưu trữ dữ liệu trong bộ nhớ thứ hai.

2. Phương pháp theo mục 1, trong đó việc chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai còn bao gồm bước xử lý thứ nhất dữ liệu được đọc từ bộ nhớ thứ nhất nếu chỉ báo bỏ qua không được khẳng định và bước xử lý thứ hai dữ liệu là kết quả từ bước xử lý thứ nhất nếu chỉ báo bỏ qua không được khẳng định.

3. Phương pháp theo mục 2, trong đó bước xử lý thứ hai bao gồm hoạt động đảo ngược của bước xử lý thứ nhất.

4. Phương pháp theo mục 3, trong đó:

bước xử lý thứ nhất bao gồm ít nhất một trong số giải mã, kiểm tra chẵn lẻ, và giải nén; và

bước xử lý thứ hai bao gồm ít nhất một trong số mã hóa, tạo chẵn lẻ, và nén.

5. Phương pháp theo mục 3, trong đó:

việc đọc dữ liệu bao gồm bước đọc dữ liệu từ vùng bộ nhớ thứ nhất;

bước xử lý thứ nhất dữ liệu được đọc từ bộ nhớ thứ nhất bao gồm giải mã dữ liệu được đọc từ vùng bộ nhớ thứ nhất;

bước xử lý thứ hai bao gồm mã hóa lại dữ liệu là kết quả từ việc giải mã;

việc lưu trữ dữ liệu bao gồm bước lưu trữ dữ liệu là kết quả từ việc giải mã trong vùng bộ nhớ thứ hai; và

chỉ báo bỏ qua chỉ báo khóa mã hóa là chung cho vùng bộ nhớ thứ nhất và vùng bộ nhớ thứ hai.

6. Phương pháp theo mục 5, còn bao gồm bước tạo chỉ báo bỏ qua dựa trên thông tin thuộc tính bảng trang được kết hợp với vùng bộ nhớ thứ nhất.

7. Phương pháp theo mục 2, còn bao gồm các bước:

đọc siêu dữ liệu được kết hợp với dữ liệu từ bộ nhớ thứ nhất;

chuyển siêu dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai, trong đó bước xử lý thứ nhất dữ liệu được đọc từ bộ nhớ thứ nhất bao gồm sử dụng siêu dữ liệu nếu chỉ báo bỏ qua không được khẳng định, và bỏ qua bước xử lý thứ nhất bao gồm bảo tồn siêu dữ liệu nếu chỉ báo bỏ qua được khẳng định; và

lưu trữ siêu dữ liệu được bảo tồn trong bộ nhớ thứ hai.

8. Phương pháp theo mục 1, còn bao gồm các bước:

đọc khóa được kết hợp với dữ liệu;

mã hóa khóa sử dụng bộ điều khiển bus dữ liệu thứ nhất được ghép nối với bus dữ liệu;

chuyển khóa được mã hóa từ bộ nhớ thứ nhất đến bộ nhớ thứ hai sử dụng bộ điều khiển bus dữ liệu thứ nhất và bus dữ liệu;

giải mã khóa được mã hóa sử dụng bộ điều khiển bus dữ liệu thứ hai được ghép nối với bus dữ liệu; và

lưu trữ khóa được giải mã trong bộ nhớ thứ hai kết hợp với dữ liệu.

9. Phương pháp theo mục 8, trong đó bus dữ liệu là bus liên kết thành phần ngoại vi (Peripheral Component Interconnect - PCI).

10. Hệ thống để chuyển dữ liệu giữa các bộ nhớ, hệ thống này bao gồm:

bộ nhớ thứ nhất;

bộ nhớ thứ hai; và

logic điều khiển chuyển bộ nhớ bao gồm logic xử lý thứ nhất và logic xử lý thứ hai, logic điều khiển chuyển bộ nhớ được tạo cấu hình để:

đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất;

xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

bỏ qua việc áp dụng logic xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định;

bỏ qua việc áp dụng logic xử lý thứ hai cho đầu ra của logic xử lý thứ nhất nếu chỉ báo bỏ qua được khẳng định; và

lưu trữ dữ liệu trong bộ nhớ thứ hai.

11. Hệ thống theo mục 10, trong đó logic điều khiển chuyển bộ nhớ còn được tạo cấu hình để:

áp dụng logic xử lý thứ nhất cho dữ liệu được đọc từ bộ nhớ thứ nhất nếu chỉ báo bỏ qua không được khẳng định; và

áp dụng logic xử lý thứ hai cho đầu ra của logic xử lý thứ nhất nếu chỉ báo bỏ qua không được khẳng định.

12. Hệ thống theo mục 11, trong đó logic xử lý thứ nhất và logic xử lý thứ hai được tạo cấu hình để thực hiện các hoạt động đảo ngược.

13. Hệ thống theo mục 12, trong đó:

logic xử lý thứ nhất được tạo cấu hình để thực hiện ít nhất một trong số giải mã, kiểm tra chẵn lẻ, và giải nén; và

logic xử lý thứ hai được tạo cấu hình để thực hiện ít nhất một trong số mã hóa, tạo chẵn lẻ, và nén.

14. Hệ thống theo mục 12, trong đó:

logic xử lý thứ nhất được tạo cấu hình để đọc dữ liệu từ vùng bộ nhớ thứ nhất và giải mã dữ liệu;

logic xử lý thứ hai được tạo cấu hình để mã hóa lại dữ liệu được giải mã bởi logic xử lý thứ nhất và lưu trữ dữ liệu được mã hóa lại bởi logic xử lý thứ hai trong vùng bộ nhớ thứ hai; và

chỉ báo bỏ qua chỉ báo khóa mã hóa là chung cho vùng bộ nhớ thứ nhất và vùng bộ nhớ thứ hai.

15. Hệ thống theo mục 14, trong đó logic điều khiển chuyển bộ nhớ được tạo cấu hình để tạo chỉ báo bỏ qua dựa trên thông tin thuộc tính bảng trang được kết hợp với vùng bộ nhớ thứ nhất.

16. Hệ thống theo mục 10, trong đó logic điều khiển chuyển bộ nhớ còn được tạo cấu hình để:

đọc siêu dữ liệu được kết hợp với dữ liệu từ bộ nhớ thứ nhất;

áp dụng logic xử lý thứ nhất cho dữ liệu được đọc từ bộ nhớ thứ nhất bằng cách sử dụng siêu dữ liệu nếu chỉ báo bỏ qua không được khẳng định;

bỏ qua việc áp dụng logic xử lý thứ nhất để bảo tồn siêu dữ liệu nếu chỉ báo bỏ qua được khẳng định; và

lưu trữ siêu dữ liệu được bảo tồn trong bộ nhớ thứ hai.

17. Hệ thống theo mục 10, trong đó logic điều khiển chuyển bộ nhớ bao gồm:

bộ điều khiển bus dữ liệu thứ nhất trong hệ thống thứ nhất, hệ thống thứ nhất bao gồm bộ nhớ thứ nhất, bộ điều khiển bus dữ liệu thứ nhất được tạo cấu hình để:

đọc khóa được kết hợp với dữ liệu;

mã hóa khóa; và

chuyển khóa được mã hóa trên bus dữ liệu; và

bộ điều khiển bus dữ liệu thứ hai trong hệ thống thứ hai được ghép nối với hệ thống thứ nhất bởi bus dữ liệu, hệ thống thứ hai bao gồm bộ nhớ thứ hai, bộ điều khiển bus dữ liệu thứ hai được tạo cấu hình để:

nhận khóa được mã hóa trên bus dữ liệu;

giải mã khóa được mã hóa; và

lưu trữ khóa được giải mã trong bộ nhớ thứ hai kết hợp với dữ liệu.

18. Phương pháp theo mục 17, trong đó bus dữ liệu là bus liên kết thành phần ngoại vi (PCI).

19. Hệ thống theo mục 10, trong đó:

logic xử lý thứ nhất được kết hợp với bộ nhớ thứ nhất và được tạo cấu hình để:

đọc dữ liệu từ bộ nhớ thứ nhất;

xác định xem chỉ báo bỏ qua có được khẳng định hay không;

xử lý dữ liệu được đọc từ bộ nhớ thứ nhất nếu chỉ báo bỏ qua không được khẳng định; và

bỏ qua việc xử lý dữ liệu được đọc từ bộ nhớ thứ nhất nếu chỉ báo bỏ qua được khẳng định; và

logic xử lý thứ hai được kết hợp với bộ nhớ thứ hai và được tạo cấu hình để:

xác định xem chỉ báo bỏ qua có được khẳng định hay không;

xử lý dữ liệu được xuất bởi logic xử lý thứ nhất nếu chỉ báo bỏ qua không được khẳng định;

bỏ qua việc xử lý dữ liệu được đọc từ bộ nhớ thứ nhất nếu chỉ báo bỏ qua được khẳng định;

lưu trữ dữ liệu được xuất bởi logic xử lý thứ hai trong bộ nhớ thứ hai nếu chỉ báo bỏ qua không được khẳng định; và

lưu trữ dữ liệu được đọc từ bộ nhớ thứ nhất trong bộ nhớ thứ hai nếu chỉ báo bỏ qua được khẳng định.

20. Hệ thống theo mục 19, trong đó:

logic xử lý thứ nhất bao gồm bộ tăng tốc bộ nhớ thứ nhất; và

logic xử lý thứ nhất bao gồm bộ tăng tốc bộ nhớ thứ hai.

21. Hệ thống để chuyển dữ liệu giữa các bộ nhớ, hệ thống này bao gồm:

phương tiện để đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất;

phương tiện để xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

phương tiện để chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai, phương tiện để chuyển bao gồm phương tiện để bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định, phương tiện để chuyển còn bao gồm phương tiện để bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định; và

phương tiện để lưu trữ dữ liệu trong bộ nhớ thứ hai.

22. Hệ thống theo mục 21, trong đó phương tiện để chuyển còn bao gồm:

phương tiện để xử lý thứ nhất dữ liệu nếu chỉ báo bỏ qua không được khẳng định; và

phương tiện để xử lý thứ hai kết quả của phương tiện để xử lý thứ nhất nếu chỉ báo bỏ qua không được khẳng định.

23. Hệ thống theo mục 21, trong đó phương tiện để xử lý thứ hai bao gồm sự đảo ngược của phương tiện để xử lý thứ nhất.

24. Hệ thống theo mục 23, trong đó:

phương tiện để xử lý thứ nhất bao gồm ít nhất một trong số phương tiện để giải mã, phương tiện để kiểm tra chẵn lẻ, và phương tiện để giải nén; và

phương tiện để xử lý thứ hai bao gồm ít nhất một trong số phương tiện để mã hóa, phương tiện để tạo chẵn lẻ, và phương tiện để nén.

25. Phương pháp theo mục 23, trong đó:

phương tiện để xử lý thứ nhất bao gồm phương tiện để giải mã;

phương tiện để xử lý thứ hai bao gồm phương tiện để mã hóa lại;

phương tiện để đọc dữ liệu bao gồm phương tiện để đọc dữ liệu từ vùng bộ nhớ thứ nhất;

phương tiện để lưu trữ dữ liệu bao gồm phương tiện để lưu trữ dữ liệu trong vùng bộ nhớ thứ hai; và

chỉ báo bỏ qua chỉ báo khóa mã hóa là chung cho vùng bộ nhớ thứ nhất và vùng bộ nhớ thứ hai.

26. Hệ thống theo mục 25, còn bao gồm phương tiện để tạo chỉ báo bỏ qua dựa trên thông tin thuộc tính bảng trang được kết hợp với vùng bộ nhớ thứ nhất.

27. Hệ thống theo mục 21, trong đó:

phương tiện để đọc dữ liệu còn để đọc siêu dữ liệu được kết hợp với dữ liệu từ bộ nhớ thứ nhất;

phương tiện để chuyển dữ liệu còn để chuyển siêu dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai, trong đó phương tiện để xử lý thứ nhất dữ liệu bao gồm phương tiện để sử dụng siêu dữ liệu nếu chỉ báo bỏ qua không được khẳng định và phương tiện để bảo tồn siêu dữ liệu nếu chỉ báo bỏ qua được khẳng định; và

phương tiện để lưu trữ dữ liệu còn để lưu trữ siêu dữ liệu được bảo tồn trong bộ nhớ thứ hai.

28. Hệ thống theo mục 21, còn bao gồm:

phương tiện để đọc khóa được kết hợp với dữ liệu;

phương tiện để mã hóa khóa sử dụng bộ điều khiển bus dữ liệu thứ nhất được ghép nối với bus dữ liệu;

phương tiện để chuyển khóa được mã hóa từ bộ nhớ thứ nhất đến bộ nhớ thứ hai;

phương tiện để giải mã khóa được mã hóa sử dụng bộ điều khiển bus dữ liệu thứ hai được ghép nối với bus dữ liệu; và

phương tiện để lưu trữ khóa được giải mã trong bộ nhớ thứ hai kết hợp với dữ liệu.

29. Phương tiện đọc được bằng máy tính để chuyển dữ liệu giữa các bộ nhớ, phương tiện đọc được bằng máy tính này bao gồm phương tiện bất biến đọc được bằng máy tính có các lệnh được lưu trữ trên đó ở dạng có thể thực thi được bằng máy tính khi được thực thi bởi hệ thống xử lý của thiết bị điện toán tạo cấu hình hệ thống xử lý để:

đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất;

xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định;

bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định; và

lưu trữ dữ liệu trong bộ nhớ thứ hai.

30. Phương tiện đọc được bằng máy tính theo điểm 29, trong đó các lệnh còn tạo cấu hình hệ thống xử lý để:

xử lý thứ nhất dữ liệu nếu chỉ báo bỏ qua không được khẳng định; và

xử lý thứ hai kết quả của bước xử lý thứ nhất dữ liệu nếu chỉ báo bỏ qua không được khẳng định.

31. Phương tiện đọc được bằng máy tính theo mục 30, trong đó:

các lệnh tạo cấu hình hệ thống xử lý để xử lý thứ nhất dữ liệu bằng việc tạo cấu hình hệ thống xử lý để thực hiện ít nhất một trong số giải mã, kiểm tra chẵn lẻ, và giải nén; và

các lệnh tạo cấu hình hệ thống xử lý để xử lý thứ hai kết quả của bước xử lý thứ nhất dữ liệu bằng việc tạo cấu hình hệ thống xử lý để thực hiện ít nhất một trong số mã hóa, tạo chẵn lẻ, và nén.

32. Phương tiện đọc được bằng máy tính theo mục 30, trong đó các lệnh còn tạo cấu hình hệ thống xử lý để tạo chỉ báo bỏ qua dựa trên thông tin thuộc tính bảng trang.

33. Phương tiện đọc được bằng máy tính theo mục 30, trong đó các lệnh còn tạo cấu hình hệ thống xử lý để:

đọc siêu dữ liệu được kết hợp với dữ liệu từ bộ nhớ thứ nhất;

chuyển siêu dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai, trong đó các lệnh tạo cấu hình hệ thống xử lý để xử lý thứ nhất dữ liệu sử dụng siêu dữ liệu nếu chỉ báo bỏ qua không được khẳng định và tạo cấu hình hệ thống xử lý để bỏ qua bước xử lý thứ nhất cho dữ liệu để bảo tồn siêu dữ liệu nếu chỉ báo bỏ qua được khẳng định; và

lưu trữ siêu dữ liệu được bảo tồn trong bộ nhớ thứ hai.

34. Phương tiện đọc được bằng máy tính theo mục 30, trong đó các lệnh còn tạo cấu hình hệ thống xử lý để:

đọc khóa được kết hợp với dữ liệu nếu chỉ báo bỏ qua được khẳng định;

mã hóa khóa sử dụng bộ điều khiển bus dữ liệu thứ nhất được ghép nối với bus dữ liệu;

chuyển khóa được mã hóa từ bộ nhớ thứ nhất đến bộ nhớ thứ hai sử dụng bộ điều khiển bus dữ liệu thứ nhất và bus dữ liệu;

giải mã khóa được mã hóa sử dụng bộ điều khiển bus dữ liệu thứ hai được ghép nối với bus dữ liệu; và

lưu trữ khóa được giải mã trong bộ nhớ thứ hai kết hợp với dữ liệu.

YÊU CẦU BẢO HỘ

1. Phương pháp để chuyển dữ liệu giữa các bộ nhớ, phương pháp này bao gồm các bước:

tạo ra khóa truy cập (handle) cho khóa gốc và thông tin suy ra khóa với gốc của modul tin cậy;

gửi khóa truy cập với gốc của modul tin cậy tới bộ xử lý;

bộ xử lý cung cấp khóa truy cập cho bộ tăng tốc thứ nhất của bộ nhớ thứ nhất và cho bộ tăng tốc thứ hai của bộ nhớ thứ hai, bộ nhớ thứ nhất bao gồm bộ nhớ truy cập ngẫu nhiên động, bộ nhớ thứ hai bao gồm bộ nhớ truy cập ngẫu nhiên không khả biến;

gửi khóa gốc và thông tin suy ra khóa với gốc của modul tin cậy tới bộ tăng tốc thứ nhất và bộ tăng tốc thứ hai;

các bộ tăng tốc thứ nhất và thứ hai suy ra các khóa riêng tư dựa trên khóa truy cập và khóa gốc để mã hóa dữ liệu trong các bộ nhớ thứ nhất và thứ hai;

bộ xử lý đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất;

bộ xử lý tạo chỉ báo bỏ qua dựa trên thông tin thuộc tính của bảng trang từ dữ liệu được đọc được kết hợp với giao tác bộ nhớ từ bộ nhớ thứ nhất;

xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai, việc chuyển bao gồm bước bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định, việc chuyển còn bao gồm bước bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định, cả việc bỏ qua bước xử lý thứ nhất cho dữ liệu và việc bỏ qua bước xử lý thứ hai cho dữ liệu đều tránh việc sử dụng các khóa riêng tư bởi các bộ tăng tốc thứ nhất và thứ hai; và

lưu trữ dữ liệu trong bộ nhớ thứ hai.

2. Phương pháp theo điểm 1, trong đó việc chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai còn bao gồm bước xử lý thứ nhất dữ liệu được đọc từ bộ nhớ thứ nhất nếu chỉ báo bỏ qua không được khẳng định và bước xử lý thứ hai dữ liệu là kết quả từ bước xử lý thứ nhất nếu chỉ báo bỏ qua không được khẳng định.
3. Phương pháp theo điểm 2, trong đó bước xử lý thứ hai bao gồm hoạt động đảo ngược của bước xử lý thứ nhất.
4. Phương pháp theo điểm 3, trong đó:
 - bước xử lý thứ nhất bao gồm ít nhất một trong số giải mã, kiểm tra chẵn lẻ, và giải nén; và
 - bước xử lý thứ hai bao gồm ít nhất một trong số mã hóa, tạo chẵn lẻ, và nén.
5. Phương pháp theo điểm 3, trong đó:
 - việc đọc dữ liệu bao gồm bước đọc dữ liệu từ vùng bộ nhớ thứ nhất;
 - bước xử lý thứ nhất dữ liệu được đọc từ bộ nhớ thứ nhất bao gồm giải mã dữ liệu được đọc từ vùng bộ nhớ thứ nhất sử dụng một trong các khóa riêng tư;
 - bước xử lý thứ hai bao gồm mã hóa lại dữ liệu là kết quả từ việc giải mã sử dụng một trong các khóa riêng tư;
 - việc lưu trữ dữ liệu bao gồm bước lưu trữ dữ liệu là kết quả từ việc giải mã trong vùng bộ nhớ thứ hai; và
 - chỉ báo bỏ qua chỉ báo ít nhất một khóa riêng tư là chung cho vùng bộ nhớ thứ nhất và vùng bộ nhớ thứ hai.
6. Phương pháp theo điểm 5, trong đó chỉ báo bỏ qua được kết hợp với vùng bộ nhớ thứ nhất.
7. Phương pháp theo điểm 1, trong đó bộ nhớ thứ nhất lưu trữ dữ liệu ngữ cảnh chính được mã hóa.
8. Phương pháp theo điểm 1, còn bao gồm bước: bộ xử lý xác định để chuyển đổi từ chế độ hoạt động sang chế độ ngủ đông.
9. Hệ thống để chuyển dữ liệu giữa các bộ nhớ, hệ thống này bao gồm:

gốc của môđun tin cậy tạo ra khóa truy cập cho khóa gốc và thông tin suy ra khóa và gửi khóa truy cập với gốc của môđun tin cậy tới bộ xử lý;

bộ xử lý cung cấp khóa truy cập cho bộ tăng tốc thứ nhất của bộ nhớ thứ nhất và cho bộ tăng tốc thứ hai của bộ nhớ thứ hai, bộ nhớ thứ nhất bao gồm bộ nhớ truy cập ngẫu nhiên động, bộ nhớ thứ hai bao gồm bộ nhớ truy cập ngẫu nhiên không khả biến;

gốc của môđun tin cậy gửi khóa gốc và thông tin suy ra khóa tới bộ tăng tốc thứ nhất và bộ tăng tốc thứ hai;

các bộ tăng tốc thứ nhất và thứ hai suy ra các khóa riêng tư dựa trên khóa truy cập và khóa gốc để mã hóa dữ liệu trong các bộ nhớ thứ nhất và thứ hai; và

logic điều khiển chuyển bộ nhớ bao gồm logic xử lý thứ nhất và logic xử lý thứ hai và bộ xử lý, logic điều khiển chuyển bộ nhớ được tạo cấu hình để:

có bộ xử lý đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất, bộ xử lý tạo chỉ báo bỏ qua dựa trên thông tin thuộc tính của bảng trang từ dữ liệu được đọc được kết hợp với giao tác bộ nhớ từ bộ nhớ thứ nhất;

xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

bỏ qua việc áp dụng logic xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định;

bỏ qua việc áp dụng logic xử lý thứ hai cho đầu ra của logic xử lý thứ nhất nếu chỉ báo bỏ qua được khẳng định, cả việc bỏ qua áp dụng logic xử lý thứ nhất và việc bỏ qua áp dụng logic xử lý thứ hai đều tránh việc sử dụng các khóa riêng tư bởi các bộ tăng tốc thứ nhất và thứ hai; và

lưu trữ dữ liệu trong bộ nhớ thứ hai.

10. Hệ thống theo điểm 9, trong đó logic điều khiển chuyển bộ nhớ còn được tạo cấu hình để:

áp dụng logic xử lý thứ nhất cho dữ liệu được đọc từ bộ nhớ thứ nhất nếu chỉ báo bỏ qua không được khẳng định; và

áp dụng logic xử lý thứ hai cho đầu ra của logic xử lý thứ nhất nếu chỉ báo bỏ qua không được khẳng định.

11. Hệ thống theo điểm 10, trong đó logic xử lý thứ nhất và logic xử lý thứ hai được tạo cấu hình để thực hiện các hoạt động đảo ngược.

12. Hệ thống theo điểm 11, trong đó:

logic xử lý thứ nhất được tạo cấu hình để thực hiện ít nhất một trong số giải mã, kiểm tra chẵn lẻ, và giải nén; và

logic xử lý thứ hai được tạo cấu hình để thực hiện ít nhất một trong số mã hóa, tạo chẵn lẻ, và nén.

13. Hệ thống theo điểm 11, trong đó:

logic xử lý thứ nhất được tạo cấu hình để đọc dữ liệu từ vùng bộ nhớ thứ nhất và giải mã dữ liệu sử dụng một trong các khóa riêng tư;

logic xử lý thứ hai được tạo cấu hình để mã hóa lại dữ liệu được giải mã bởi logic xử lý thứ nhất sử dụng một trong các khóa riêng tư và lưu trữ dữ liệu được mã hóa lại bởi logic xử lý thứ hai trong vùng bộ nhớ thứ hai; và

chỉ báo bỏ qua chỉ báo ít nhất một khóa riêng tư là chung cho vùng bộ nhớ thứ nhất và vùng bộ nhớ thứ hai.

14. Hệ thống theo điểm 13, trong đó chỉ báo bỏ qua được kết hợp với vùng bộ nhớ thứ nhất.

15. Hệ thống theo điểm 9, trong đó

bộ nhớ thứ nhất lưu trữ dữ liệu ngữ cảnh chính được mã hóa.

16. Hệ thống theo điểm 9, trong đó bộ xử lý xác định xem có chuyển đổi từ chế độ hoạt động sang chế độ ngủ đông hay không.

17. Hệ thống theo điểm 9, trong đó:

logic xử lý thứ nhất bao gồm bộ tăng tốc bộ nhớ thứ nhất; và

logic xử lý thứ hai bao gồm bộ tăng tốc bộ nhớ thứ hai.

18. Hệ thống để chuyển dữ liệu giữa các bộ nhớ, hệ thống này bao gồm:

gốc của modul tin cậy tạo ra khóa truy cập cho khóa gốc và thông tin suy ra khóa và gửi khóa truy cập với gốc của modul tin cậy tới bộ xử lý;

bộ xử lý cung cấp khóa truy cập cho bộ tăng tốc thứ nhất của bộ nhớ thứ nhất và cho bộ tăng tốc thứ hai của bộ nhớ thứ hai, bộ nhớ thứ nhất bao gồm bộ nhớ truy cập ngẫu nhiên động, bộ nhớ thứ hai bao gồm bộ nhớ truy cập ngẫu nhiên không khả biến;

gốc của modul tin cậy gửi khóa gốc và thông tin suy ra khóa tới bộ tăng tốc thứ nhất và bộ tăng tốc thứ hai;

các bộ tăng tốc thứ nhất và thứ hai suy ra các khóa riêng tư dựa trên khóa truy cập và khóa gốc để mã hóa dữ liệu trong các bộ nhớ thứ nhất và thứ hai;

phương tiện để đọc dữ liệu được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất;

bộ xử lý để tạo chỉ báo bỏ qua dựa trên thuộc tính phân cứng dựa trên trang của bảng trang từ dữ liệu được đọc được kết hợp với giao tác bộ nhớ từ bộ nhớ thứ nhất;

phương tiện để xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

phương tiện để chuyển dữ liệu từ bộ nhớ thứ nhất đến bộ nhớ thứ hai, phương tiện để chuyển bao gồm phương tiện để bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định, phương tiện để chuyển còn bao gồm phương tiện để bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định, cả phương tiện để bỏ qua bước xử lý thứ nhất cho dữ liệu và phương tiện để bỏ qua bước xử lý thứ hai cho dữ liệu đều tránh việc sử dụng các khóa riêng tư bởi các bộ tăng tốc thứ nhất và thứ hai; và

phương tiện để lưu trữ dữ liệu trong bộ nhớ thứ hai.

19. Hệ thống theo điểm 18, trong đó phương tiện để chuyển còn bao gồm:

phương tiện để xử lý thứ nhất dữ liệu nếu chỉ báo bỏ qua không được khẳng định; và

phương tiện để xử lý thứ hai kết quả của phương tiện để xử lý thứ nhất nếu chỉ báo bỏ qua không được khẳng định.

20. Hệ thống theo điểm 18, trong đó phương tiện để xử lý thứ hai bao gồm sự đảo ngược của phương tiện để xử lý thứ nhất.

21. Hệ thống theo điểm 20, trong đó:

phương tiện để xử lý thứ nhất bao gồm ít nhất một trong số phương tiện để giải mã, phương tiện để kiểm tra chẵn lẻ, và phương tiện để giải nén; và

phương tiện để xử lý thứ hai bao gồm ít nhất một trong số phương tiện để mã hóa, phương tiện để tạo chẵn lẻ, và phương tiện để nén.

22. Hệ thống theo điểm 20, trong đó:

phương tiện để xử lý thứ nhất bao gồm phương tiện để giải mã sử dụng một trong các khóa riêng tư;

phương tiện để xử lý thứ hai bao gồm phương tiện để mã hóa lại sử dụng một trong các khóa riêng tư;

phương tiện để đọc dữ liệu bao gồm phương tiện để đọc dữ liệu từ vùng bộ nhớ thứ nhất;

phương tiện để lưu trữ dữ liệu bao gồm phương tiện để lưu trữ dữ liệu trong vùng bộ nhớ thứ hai; và

chỉ báo bỏ qua chỉ báo ít nhất một khóa riêng tư là chung cho vùng bộ nhớ thứ nhất và vùng bộ nhớ thứ hai.

23. Hệ thống theo điểm 22, trong đó chỉ báo bỏ qua được kết hợp với vùng bộ nhớ thứ nhất.

24. Hệ thống theo điểm 18, trong đó

bộ nhớ thứ nhất lưu trữ dữ liệu ngữ cảnh chính được mã hóa.

25. Phương tiện đọc được bằng máy tính để chuyển dữ liệu giữa các bộ nhớ, phương tiện đọc được bằng máy tính này bao gồm phương tiện bất biến đọc được bằng máy tính có các lệnh được lưu trữ trên đó ở dạng có thể thực thi được bằng máy tính

khi được thực thi bởi hệ thống xử lý của thiết bị điện toán tạo cấu hình hệ thống xử lý để:

tạo ra khóa truy cập cho khóa gốc và thông tin suy ra khóa với gốc của modul tin cậy;

gửi khóa truy cập với gốc của modul tin cậy tới bộ xử lý;

bộ xử lý cung cấp khóa truy cập cho bộ tăng tốc thứ nhất của bộ nhớ thứ nhất và cho bộ tăng tốc thứ hai của bộ nhớ thứ hai, bộ nhớ thứ nhất bao gồm bộ nhớ truy cập ngẫu nhiên động, bộ nhớ thứ hai bao gồm bộ nhớ truy cập ngẫu nhiên không khả biến;

gửi khóa gốc và thông tin suy ra khóa với gốc của modul tin cậy tới bộ tăng tốc thứ nhất và bộ tăng tốc thứ hai;

các bộ tăng tốc thứ nhất và thứ hai suy ra các khóa riêng tư dựa trên khóa truy cập và khóa gốc để mã hóa dữ liệu trong các bộ nhớ thứ nhất và thứ hai;

đọc dữ liệu với bộ xử lý được kết hợp với giao tác chuyển bộ nhớ từ bộ nhớ thứ nhất;

bộ xử lý tạo chỉ báo bỏ qua dựa trên thông tin thuộc tính của bảng trang từ dữ liệu được đọc được kết hợp với giao tác bộ nhớ từ bộ nhớ thứ nhất;

xác định xem chỉ báo bỏ qua được kết hợp với giao tác chuyển bộ nhớ có được khẳng định hay không;

bỏ qua bước xử lý thứ nhất cho dữ liệu nếu chỉ báo bỏ qua được khẳng định;

bỏ qua bước xử lý thứ hai cho dữ liệu nếu chỉ báo bỏ qua được khẳng định, cả việc bỏ qua bước xử lý thứ nhất cho dữ liệu và việc bỏ qua bước xử lý thứ hai cho dữ liệu đều tránh việc sử dụng các khóa riêng tư bởi các bộ tăng tốc thứ nhất và thứ hai; và

lưu trữ dữ liệu trong bộ nhớ thứ hai.

26. Phương tiện đọc được bằng máy tính theo điểm 25, trong đó các lệnh còn tạo cấu hình hệ thống xử lý để:

xử lý thứ nhất dữ liệu nếu chỉ báo bỏ qua không được khẳng định; và

xử lý thứ hai kết quả của bước xử lý thứ nhất dữ liệu nếu chỉ báo bỏ qua không được khẳng định.

27. Phương tiện đọc được bằng máy tính theo điểm 26, trong đó;

các lệnh tạo cấu hình hệ thống xử lý để xử lý thứ nhất dữ liệu bằng việc tạo cấu hình hệ thống xử lý để thực hiện ít nhất một trong số giải mã, kiểm tra chẵn lẻ, và giải nén; và

các lệnh tạo cấu hình hệ thống xử lý để xử lý thứ hai kết quả của bước xử lý thứ nhất dữ liệu bằng việc tạo cấu hình hệ thống xử lý để thực hiện ít nhất một trong số mã hóa, tạo chẵn lẻ, và nén.

28. Phương tiện đọc được bằng máy tính theo điểm 26, trong đó

bộ nhớ thứ nhất lưu trữ dữ liệu ngữ cảnh chính được mã hóa.

29. Phương tiện đọc được bằng máy tính theo điểm 25, trong đó bộ xử lý xác định chuyển đổi từ chế độ hoạt động sang chế độ ngủ đông.

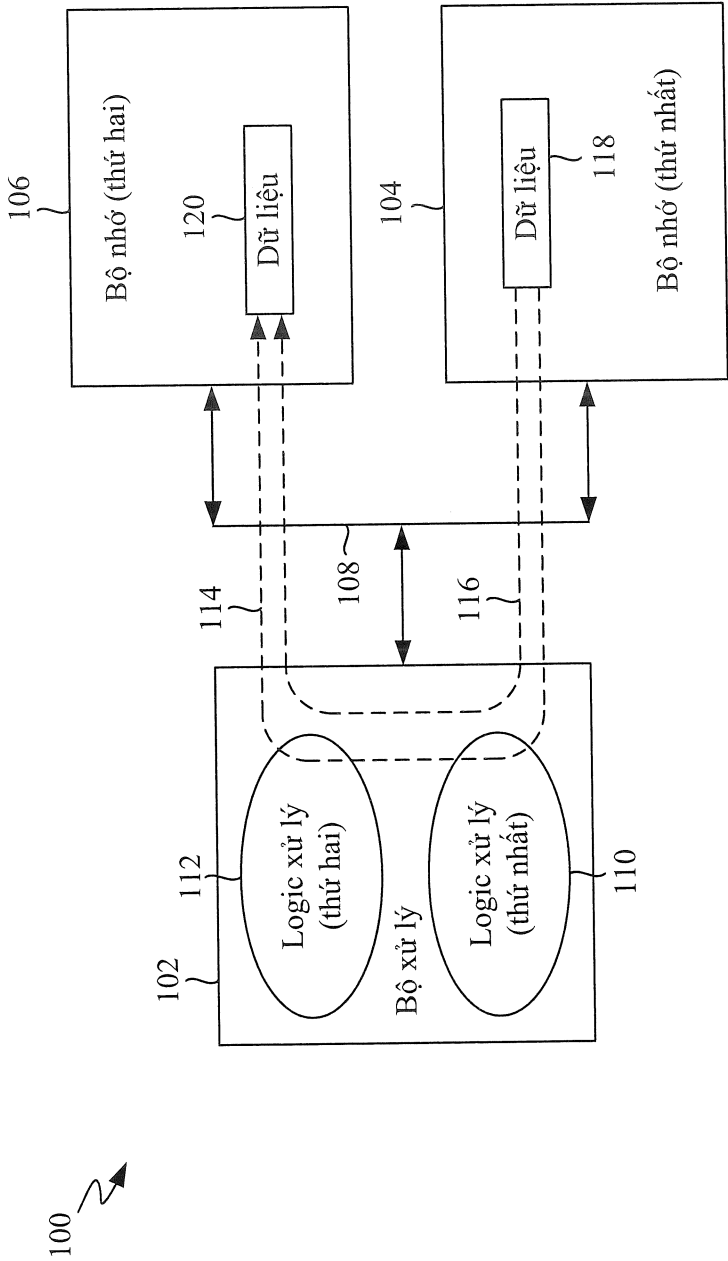


Fig.1

2/8

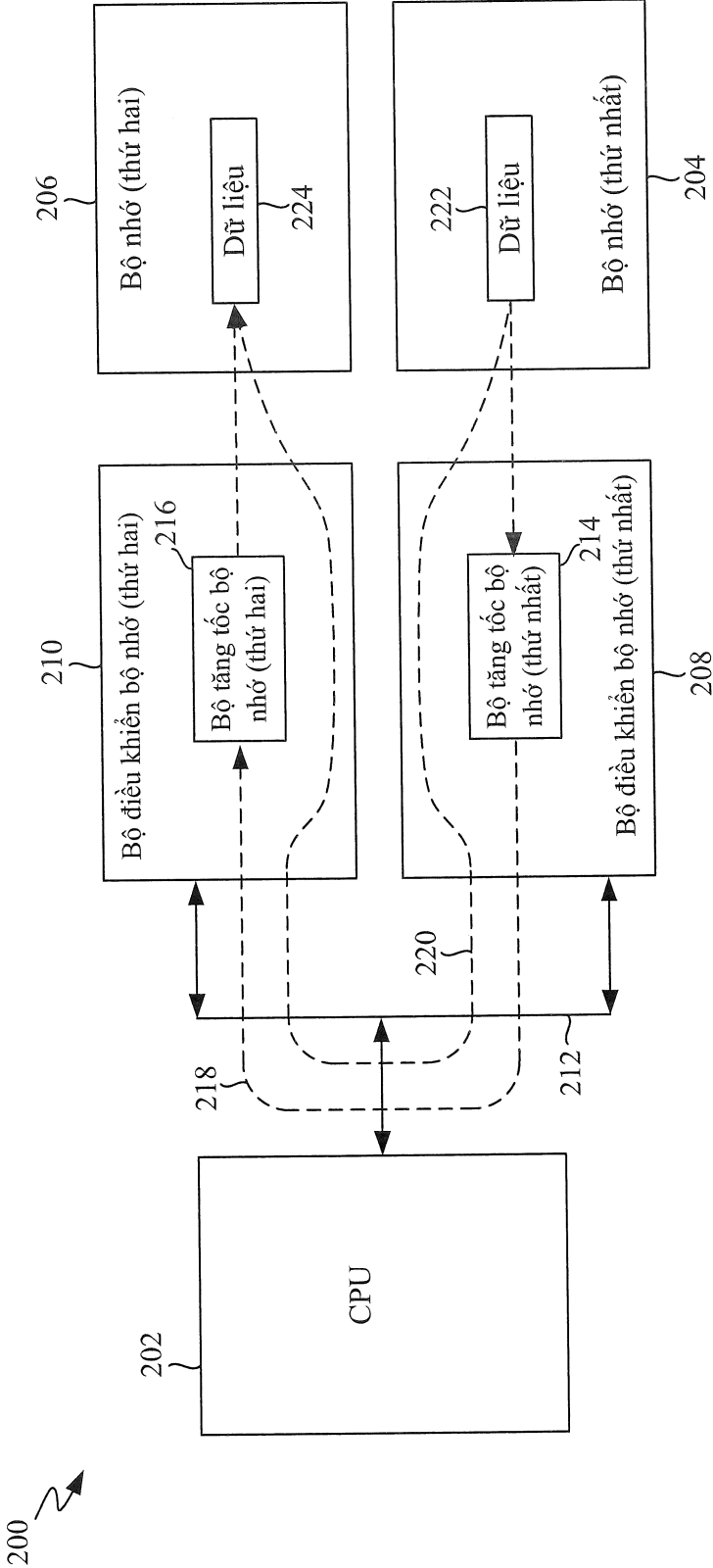


Fig.2

3/8

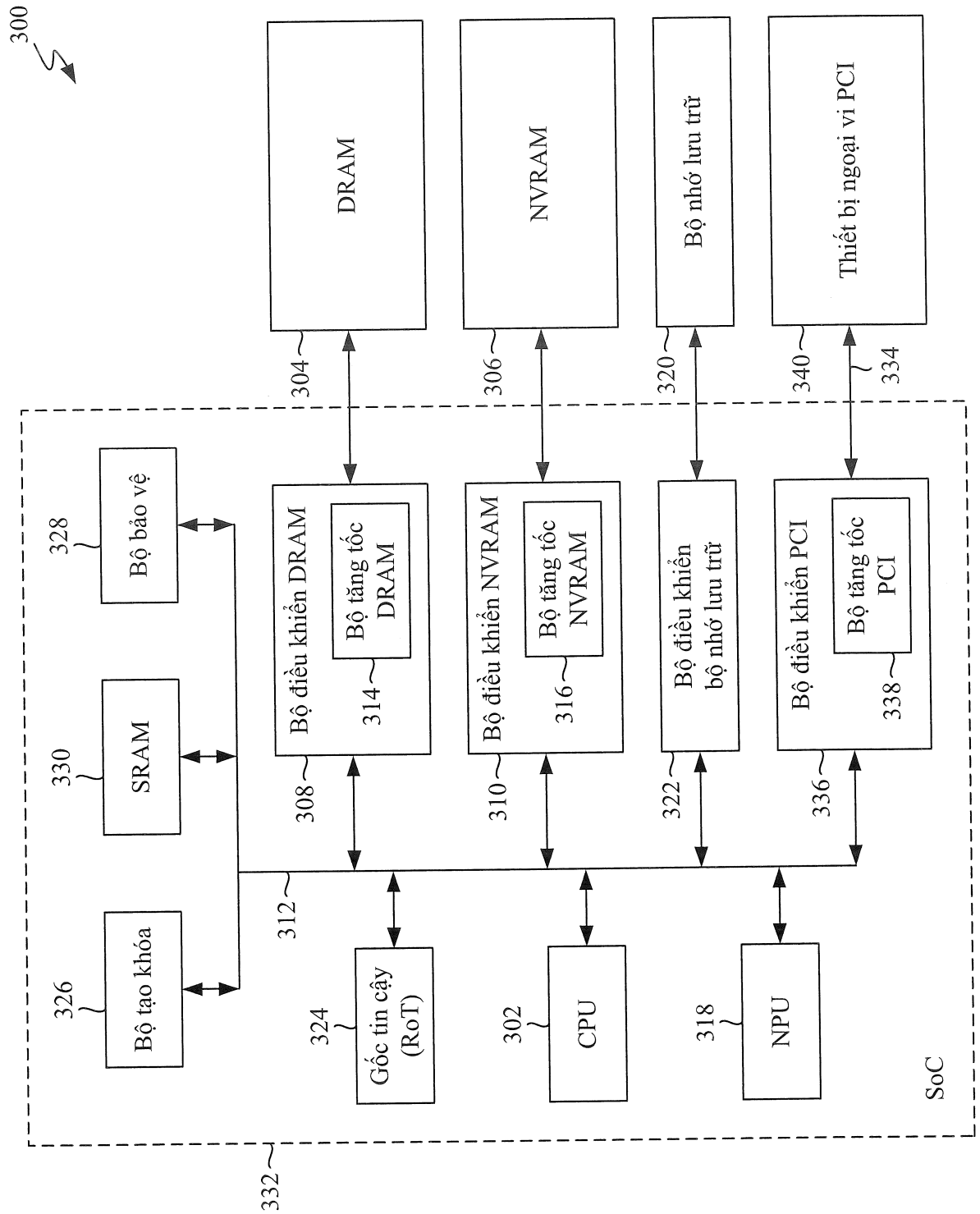


Fig.3

4/8

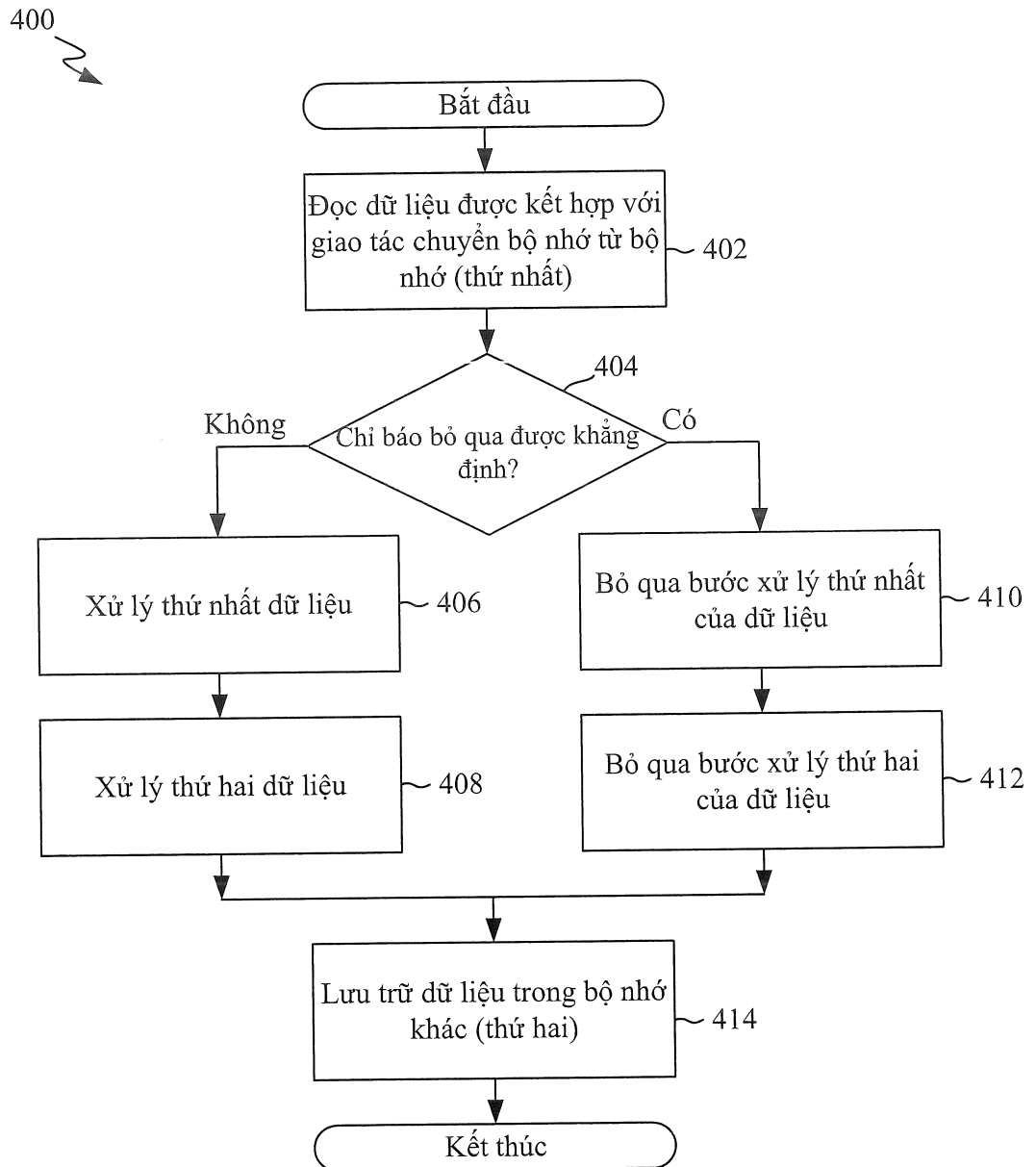


Fig.4

5/8

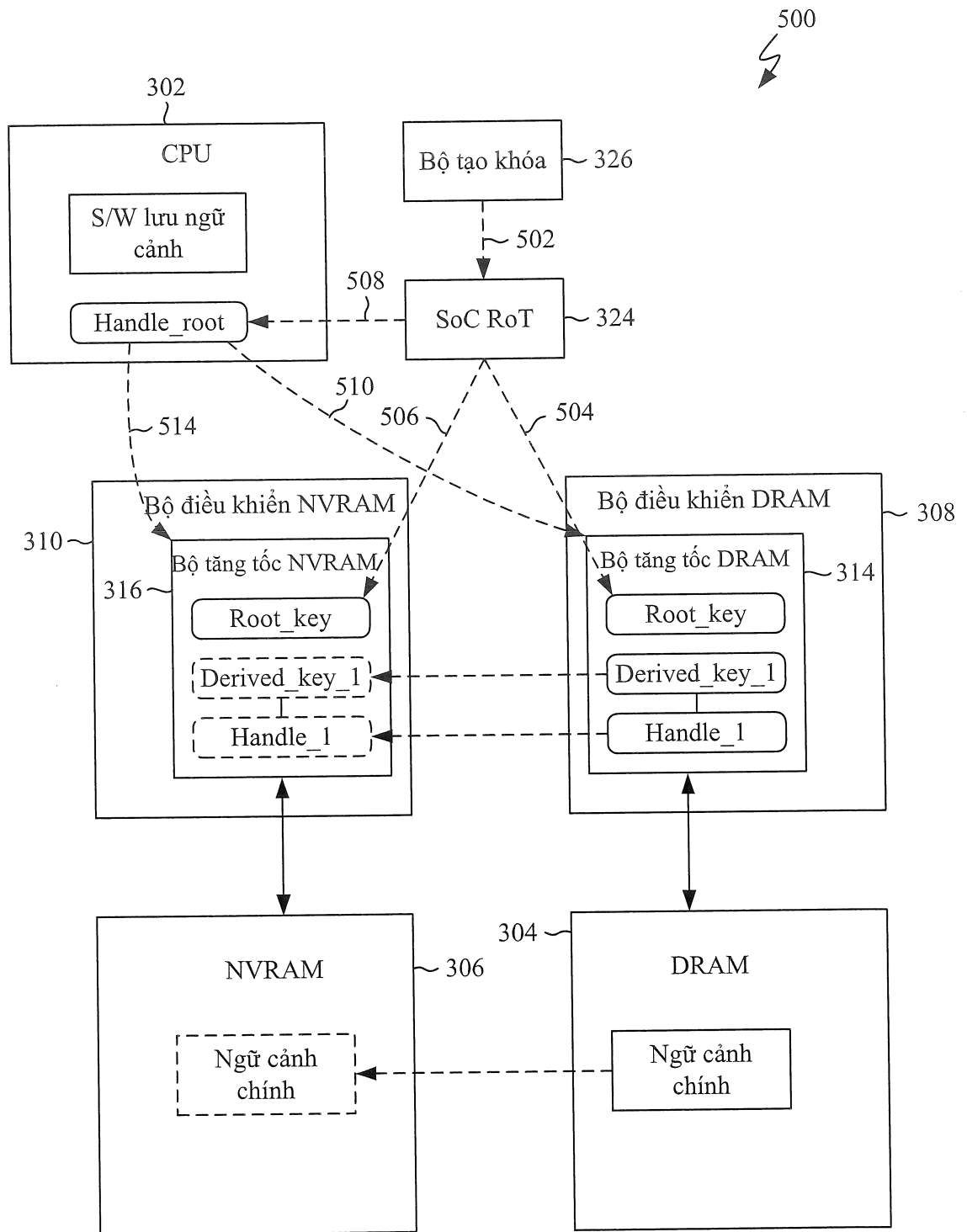


Fig.5

6/8

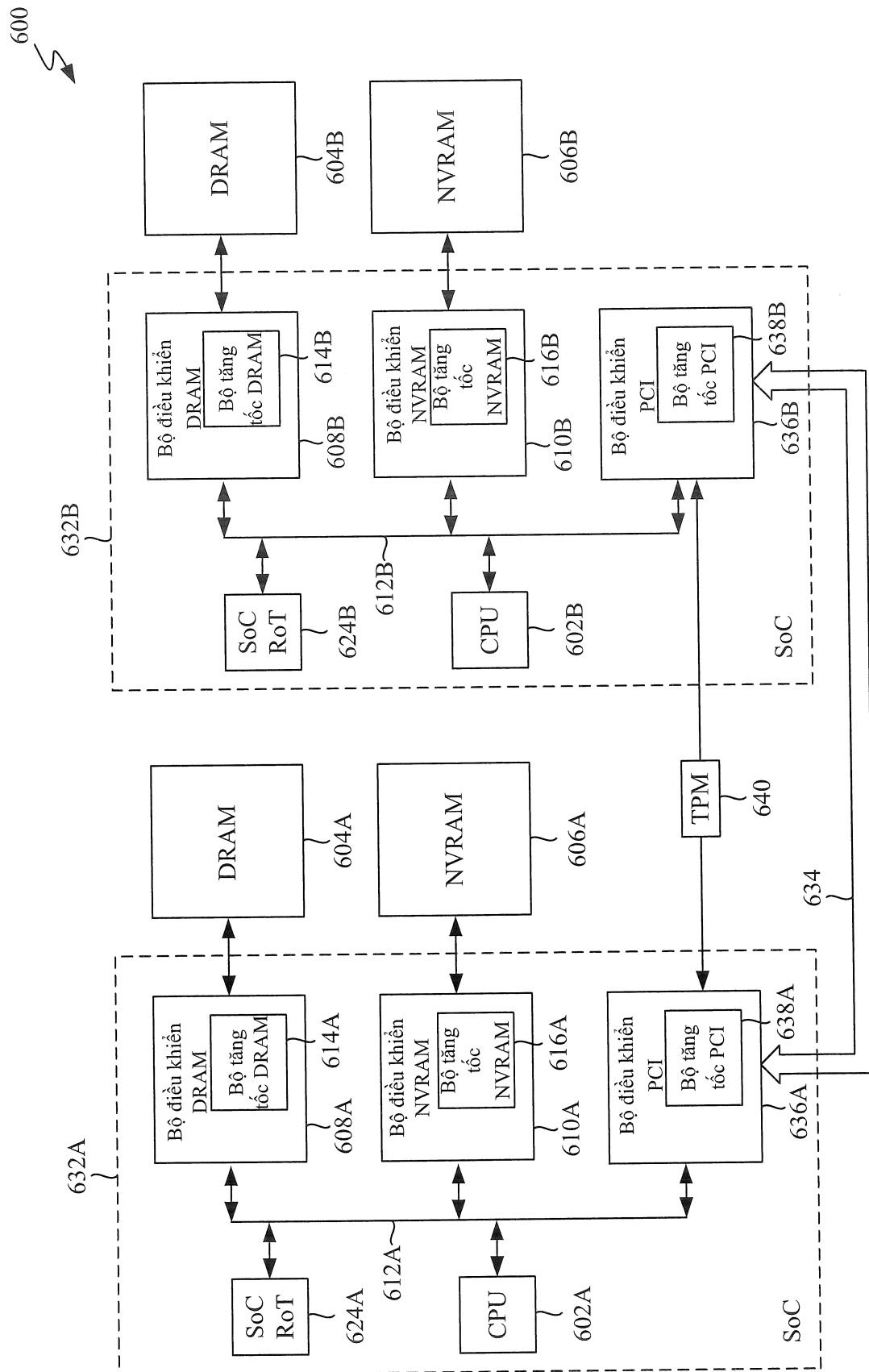


Fig. 6

7/8

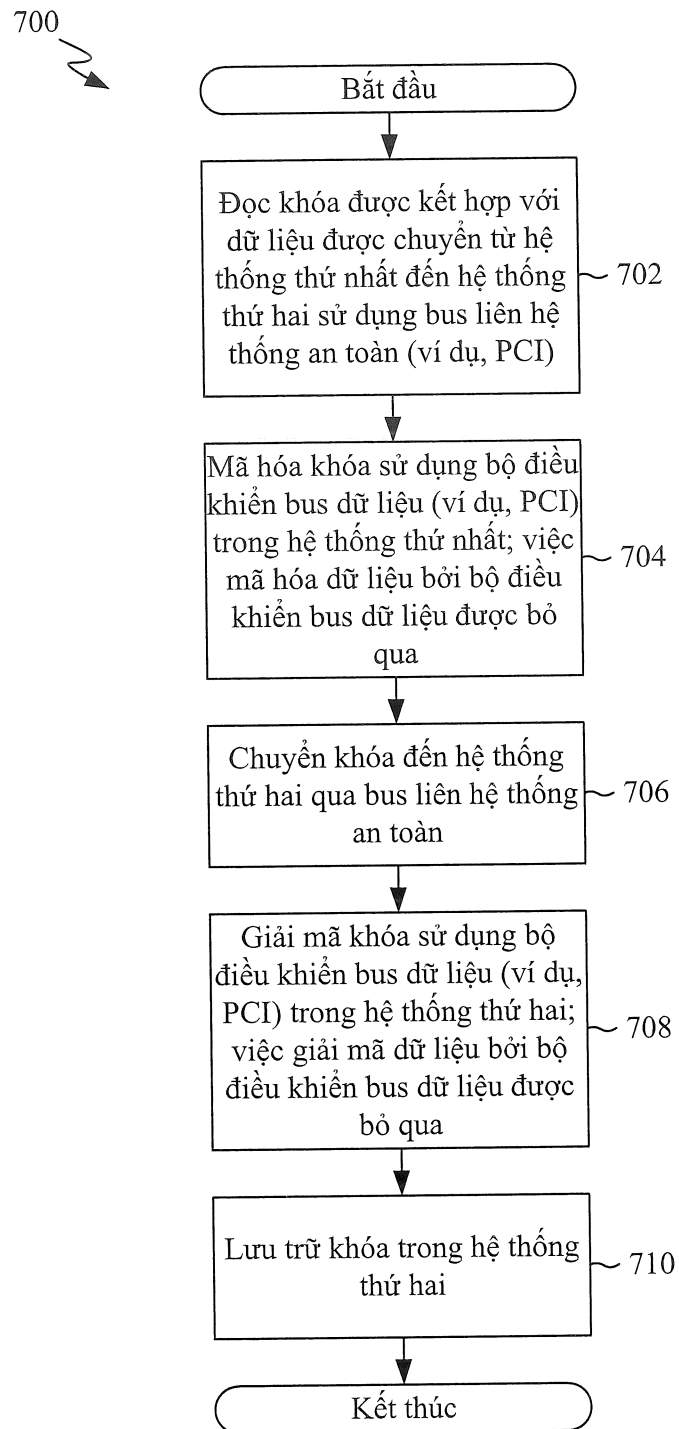


Fig.7

8/8

