**BÁO CÁO DỰ ÁN**

**I. THÔNG TIN CHUNG VỀ NHÓM DỰ ÁN**

**1.1 Mã đăng ký:** ICD25 – 054

**1.2 Tên dự án:** Thiết kế IP mã hóa giải mã DES trên ASICS

**1.3 Đội ngũ dự án**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **Vai trò trong dự án** | **Đơn vị công tác** |
| 1 | Kim Gia Bảo | Nhóm trưởng | Trường đại học Bách Khoa Đà Nẵng |
| 2 | Nguyễn Thị Uyên Phương | Thành viên | Trường đại học Bách Khoa Đà Nẵng |
| 3 | Lê Duy Hoàng | Thành viên | Trường đại học Bách Khoa Đà Nẵng |

**II. THÔNG TIN VỀ SẢN PHẨM**

**2.1 Vấn đề, tính cần thiết và lợi thế cạnh tranh của sản phẩm**

**a) Vấn đề cần giải quyết:**

Trong bối cảnh phát triển thành phố thông minh, việc truyền và xử lý dữ liệu giữa các thiết bị cảm biến, trung tâm điều khiển và hệ thống điều hành phải được thực hiện một cách an toàn và đáng tin cậy. Tuy nhiên, các dữ liệu này thường truyền qua mạng không dây hoặc các kênh có khả năng bị nghe lén, can thiệp hoặc giả mạo.

Vì vậy, bảo mật dữ liệu trở thành một yêu cầu cấp thiết, đặc biệt là với các ứng dụng như:

* Hệ thống giám sát giao thông và an ninh.
* Giao tiếp giữa các cảm biến môi trường, điện lưới, và hệ thống quản lý năng lượng.
* Truyền thông tin điều khiển từ trung tâm tới thiết bị đầu cuối (ví dụ: đèn giao thông, hệ thống tưới tự động...).

Giải pháp phần mềm thuần túy có thể không đáp ứng yêu cầu về tốc độ, độ trễ thấp và hiệu năng năng lượng cần thiết trong môi trường thực tế. Do đó, cần có một IP phần cứng chuyên dụng có khả năng mã hóa/giải mã dữ liệu ngay trên chip với tốc độ cao, tiêu thụ điện năng thấp và diện tích silicon hợp lý.

Dự án hướng đến thiết kế và hiện thực hóa IP mã hóa/giải mã DES trên nền tảng ASIC, nhằm giải quyết vấn đề này bằng một giải pháp phần cứng tích hợp, có thể nhúng vào các SoC phục vụ thành phố thông minh.

**b) Tính cần thiết của sản phẩm**

- **Khả năng ứng dụng vào thực tế thông qua các giải pháp của đô thị thông minh, tập trung vào chủ đề thành phố xanh. Đặc biệt có thể ứng dụng trong các giải pháp cụ thể: chuyển đổi số, môi trường, giao thông, y tế, năng lượng…**

Trong đô thị thông minh, đặc biệt với định hướng phát triển *thành phố xanh*, việc thu thập và truyền dữ liệu từ các cảm biến (về môi trường, chất lượng không khí, giao thông, điện năng...) là nền tảng cho các quyết định tự động và tối ưu hóa năng lượng. Tuy nhiên, dữ liệu trong hệ thống này thường di chuyển qua các kênh dễ bị tấn công, làm ảnh hưởng đến độ tin cậy của hệ thống và quyền riêng tư của người dùng.

Giải pháp IP phần cứng mã hóa/giải mã DES được thiết kế trong dự án mang lại tính bảo mật dữ liệu ở cấp độ phần cứng, có thể nhúng vào các SoC điều khiển cảm biến, thiết bị điều hành giao thông, hệ thống điện mặt trời thông minh, đồng hồ điện tử, và các thiết bị IoT môi trường. Nhờ đó:

* Dữ liệu môi trường và năng lượng được mã hóa ngay tại nguồn.
* Các chỉ thị điều khiển giao thông thông minh không bị can thiệp.
* Giảm rủi ro rò rỉ thông tin cá nhân trong hệ thống y tế thông minh.
* Góp phần đảm bảo an toàn thông tin, tăng tính bền vững của thành phố xanh.

**- Khả năng ứng dụng vào các sản phẩm công nghệ điện tử, công nghệ IoT, công nghệ AI, công nghệ tính toán biên… đóng góp vào sự tiến bộ xã hội và kinh tế cho một thành phố thông minh.**

* Thiết bị IoT: giúp các thiết bị đầu cuối (như cảm biến môi trường, thiết bị điều khiển năng lượng) có khả năng mã hóa ngay tại phần cứng mà không cần bộ xử lý trung tâm.
* Điện toán biên (Edge Computing): tăng cường bảo mật khi dữ liệu được xử lý và ra quyết định tại biên mà không phụ thuộc vào đám mây, từ đó giảm độ trễ và tiết kiệm băng thông.
* Thiết bị AI: bảo vệ dữ liệu huấn luyện, cảm biến đầu vào, và kết quả dự đoán của mô hình AI trong các hệ thống giám sát hoặc hỗ trợ y tế.
* Hệ thống SoC tùy chỉnh: dễ dàng nhúng IP DES vào các chip ứng dụng cụ thể (ASIC), tăng hiệu suất và tiết kiệm điện năng – điều đặc biệt quan trọng với các thiết bị sử dụng pin, năng lượng tái tạo.

Sự tích hợp này giúp giảm chi phí hệ thống, tăng cường an toàn và hiệu năng – đóng góp thiết thực vào sự phát triển bền vững và kinh tế của thành phố thông minh.

**c) Lợi thế cạnh tranh của dự án** *(Đâu là tính mới, tính đột phá làm nổi bật sản phẩm của dự án so với sản phẩm tương tự trên thị trường?)*

Dự án IP mã hóa/giải mã DES mang lại nhiều lợi thế nổi bật so với các giải pháp phần mềm hay phần cứng truyền thống:

* Tối ưu hóa cho ASIC: thiết kế tập trung vào khả năng tổng hợp tốt (synthesizable), tiết kiệm diện tích silicon, tốc độ cao và tiêu thụ năng lượng thấp.
* Có thể nhúng dễ dàng vào hệ thống SoC hoặc vi mạch tùy chỉnh dùng trong thành phố thông minh.
* Thiết kế mô-đun: có thể mở rộng hoặc thay thế bằng các thuật toán mạnh hơn (AES, 3DES…) tùy ứng dụng mà vẫn giữ kiến trúc phần cứng linh hoạt.
* Chi phí thấp và không phụ thuộc công nghệ độc quyền: thích hợp cho các tổ chức, đơn vị trong nước nghiên cứu và triển khai ứng dụng bảo mật không phụ thuộc vào bên thứ ba.

**2.2 Phương pháp nghiên cứu, các kết quả thiết kế/mô phỏng của sản phẩm**

**a) Phương pháp nghiên cứu/thực hiện dự án** *(Dự án mô tả thiết kế, mô tả các nội dung thực hiện nghiên cứu, quá trình mô phỏng thiết kế, phương pháp đánh giá kiểm tra thiết kế theo công nghệ nhóm đã sử dụng cũng như các phần mềm kỹ thuật phục vụ nghiên cứu để tạo nên các kết quả dự thi [1-Bản thiết kế, 2-Kết quả mô phỏng, 3-Thiết kế vật lý, 4-Kết quả đánh giá kiểm tra DRC/LVS và 5-Kết quả tổng hợp ra gdsII file]. Đối với các dự án theo hướng FPGA/SoC có thể thay thế mục 3-5 bằng 3-Kết quả tổng hợp trên SoC/FPGA cụ thể và 4-Đánh giá kiểm tra trên SoC/FPGA [tài nguyên, tốc độ, công suất tiêu thụ])*

***1-Bản thiết kế:***

Thuật toán DES sử dụng khóa 56 bit và hoạt động theo nguyên lý hoán vị và thay thế qua 16 vòng lặp (rounds).

Kiến trúc thiết kế gồm các khối chính:

* **Key Expansion**: sinh khóa con từ khóa chính cho 16 vòng.
* **Initial Permutation & Final Permutation**: thực hiện hoán vị dữ liệu đầu vào và đầu ra.
* **16 Round Function (F-function)**: gồm E-expansion, XOR với khóa con, S-boxes và P-permutation.
* **Control Unit**: điều khiển trình tự mã hóa hoặc giải mã.

Thiết kế hỗ trợ 2 chế độ:

* **Encrypt (mã hóa)**
* **Decrypt (giải mã)**
  1. **Design Specification:**
* **DES Core.**

A diagram of a computer code

AI-generated content may be incorrect.

+ Chức năng: Khối lõi DES chịu trách nhiệm mã hóa hoặc giải mã một khối dữ liệu đầu vào 64 bits và chuỗi khóa 64 bits, đầu ra của khối là chuỗi dữ liệu kết quả dài 64 bits và tín hiệu thông báo khối đã hoàn thành một quá trình mã hóa/giải mã hoặc khối đang rảnh.

**A table of information

AI-generated content may be incorrect.**

* Thiết kế:

A diagram of a computer system

AI-generated content may be incorrect.

* Waveform:

A close-up of a graph

AI-generated content may be incorrect.

* **DES Round Key Block.**

A diagram of a round key

AI-generated content may be incorrect.

+ Chức năng: Khối này chịu trách nhiệm tạo ra 16 khóa vòng từ khóa chính với đầu vào là chuỗi khóa chính dài 64 bits và các tín hiệu điều khiển, đầu ra là chuỗi khóa vòng dài 48 bits

**A screen shot of a computer

AI-generated content may be incorrect.**

+ Thiết kế:

A diagram of a computer

AI-generated content may be incorrect.

+ Waveform:

A close-up of a check

AI-generated content may be incorrect.

* **DES Data Encryption.**

A diagram of a block diagram

AI-generated content may be incorrect.

+ Chức năng: Khối này thực hiện quá trình mã hóa/giải mã chuỗi dữ liệu đầu vào 64 bit, đầu ra của khối là chuỗi dữ liệu 64 bits sau khi đã được mã hóa/ giải mã.

A white and black text on a white background

AI-generated content may be incorrect.

+ Thiết kế:

A diagram of a computer

AI-generated content may be incorrect.

+ Waveform:

A close-up of a graph

AI-generated content may be incorrect.

* **DES Controller.**

A diagram of a computer component

AI-generated content may be incorrect.

+ Chức năng: Khối này tạo ra các tín hiệu điều khiển cho các mạch được trình bày ở trên, bao gồm một bộ đếm và một bộ tạo tín hiệu để điều khiển chu kỳ khóa mới và thực thi vòng lặp tiếp theo.

**A screenshot of a computer

AI-generated content may be incorrect.**

+ Thiết kế:

A diagram of a computer

AI-generated content may be incorrect.

+ Waveform:

A blue and white drawing

AI-generated content may be incorrect.

***2-Kết quả mô phỏng:***

Nhóm đã lập một danh sách testcase trong hai trường hợp: mã hóa và giải mã để kiểm tra chức năng của lõi DES.

**+ Encryption:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Encryption** | | | |
| Key | Plaintext | Ciphertext | Pass |
| AABB09182736CCDD | 3F9A1C4D62B8E705 | 98F67F69D67EF233 | ☑ |
| 0123456789ABCDEF | 9DEFA341B6C77210 | FCC66504E080DDE2 | ☑ |
| FEDCBA9876543210 | A7C5B038D4E902F | 986E4C7DC5EC0CA4 | ☑ |
| 0F1571C947D9E859 | C0DEBA5E12345678 | 5A1C332F5343A3E2 | ☑ |
| A1B2C3D4E5F60718 | E32D184AA905F3C | 57B06FABF7460681 | ☑ |
| 133457799BBCDFF1 | 5FEC0931D842716A | ACF5AE45705F125D | ☑ |
| 0123456789ABCDEF | 0C3B98F17A2D65BE | B415F781215933A3 | ☑ |
| 1A2B3C4D5E6F7081 | A92B41EE34F6DC98 | 1AAF6A909C0765BD | ☑ |
| 0E329232EA6D0D73 | 62EF839C00B1A754 | 714CA38C76AB764A | ☑ |
| 7CA110454A1A6E57 | D4B690218FAEC377 | 42DD96C19A8DC22D | ☑ |

**+ Decryption:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Decryption** | | | |
| DES Data | Key | DES Result | Pass |
| 29D2EDB72190AC76 | 3132333435363738 | ADB14D50057C44AA | ☑ |
| D8C03A29329D03A2 | 4142434445464748 | D2B7AE0E26A333FE | ☑ |
| 2B50B717FBC69097 | 3837363534333231 | 09778E23E1F2A135 | ☑ |
| 2FC9DA56D0C13F7C | 50415353574F5244 | 1F96C089420D51AE | ☑ |
| 9B03DE9949A1A322 | 48454C4C4F313233 | 2E69204072DEBDCC | ☑ |
| C9CE7DD892C1AE1B | 4142434445464731 | 0914B0D2A87859A4 | ☑ |
| C04A421C8D44EF00 | 4142434445464732 | 4210B1B7806CEA3A | ☑ |
| FD22AFDAA769B37B | 4142434445464733 | 7207232A9E1A6785 | ☑ |
| E6017920410F7F96 | 4142434445464734 | 0CF516F7741B0454 | ☑ |
| DBE2057A420EC6EF | 4142434445464735 | 91DB0188F46B940D | ☑ |

**Waveform checklist:**

|  |
| --- |
|  |
| **A screen shot of a computer  AI-generated content may be incorrect.** |
| **A screen shot of a computer  AI-generated content may be incorrect.** |
| **A screen shot of a computer  AI-generated content may be incorrect.** |
| **A screen shot of a computer  AI-generated content may be incorrect.** |
| **A computer screen with green lines  AI-generated content may be incorrect.** |
| **A screen shot of a computer  AI-generated content may be incorrect.** |
| **A screen shot of a computer  AI-generated content may be incorrect.** |
| **A computer screen with green lines  AI-generated content may be incorrect.** |
| **A screen shot of a computer  AI-generated content may be incorrect.** |
| **Nhận xét:**  Sau khi mô phỏng bằng Modelsim, kết quả thu được sau khi mã hóa, giải mã khớp với checklist tạo ra ban đầu. |

**b) Kết quả thiết kế & mô phỏng của sản phẩm demo** *(Dự án trình bày sản phẩm hoàn thiện hình thành từ quá trình nghiên cứu bao gồm: 1-Bản thiết kế, 2-Kết quả mô phỏng, 3-Thiết kế vật lý, 4-Kết quả đánh giá kiểm tra DRC/LVS và 5-Kết quả tổng hợp ra gdsII file chuẩn bị cho tapout. Đối với các dự án theo hướng FPGA/SoC có thể thay thế mục 3-5 bằng 3-Kết quả tổng hợp trên SoC/FPGA cụ thể và 4-Đánh giá kiểm tra trên SoC/FPGA [tài nguyên, tốc độ, công suất tiêu thụ])*

|  |  |  |  |
| --- | --- | --- | --- |
| **Kết quả** | **Hình ảnh chứng minh** | | **Mô tả** |
| Bản thiết kế | *[có thể có nhiều hình ảnh minh chứng, print out trực tiếp trên công cụ thiết kế]* | |  |
| Mô phỏng thiết kế | *[cần cung cấp nhiều hình ảnh minh chứng thể hiện nhóm dự án tự thực hiện, print out trực tiếp trên công cụ mô phỏng]* | |  |
| Thiết kế  vật lý | *[cần cung cấp nhiều hình ảnh minh chứng thể hiện nhóm dự án tự thực hiện, print out trực tiếp trên công cụ thiết kế]* | |  |
| Đánh giá kiểm tra DRC/LVS | *[print out trực tiếp trên công cụ đánh giá kiểm tra]* | |  |
| Tổng hợp ra gdsII file chuẩn bị cho tapout | *[print out trực tiếp trên công cụ tổng hợp gdsII]* | |  |
|  | |  | |