(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) **1-0044439**

(51)[2019.01] **G07C 9/00**

(13) **B**

(21) 1-2020-01076

(22) 27/02/2020

(45) 25/03/2025 444

(43) 26/04/2021 397A

(71) CÔNG TY CỔ PHẦN ONYX VIỆT NAM (VN)
Số 121 phố Vương Thừa Vũ, phường Khương Trung, quận Thanh Xuân, thành phố Hà Nội

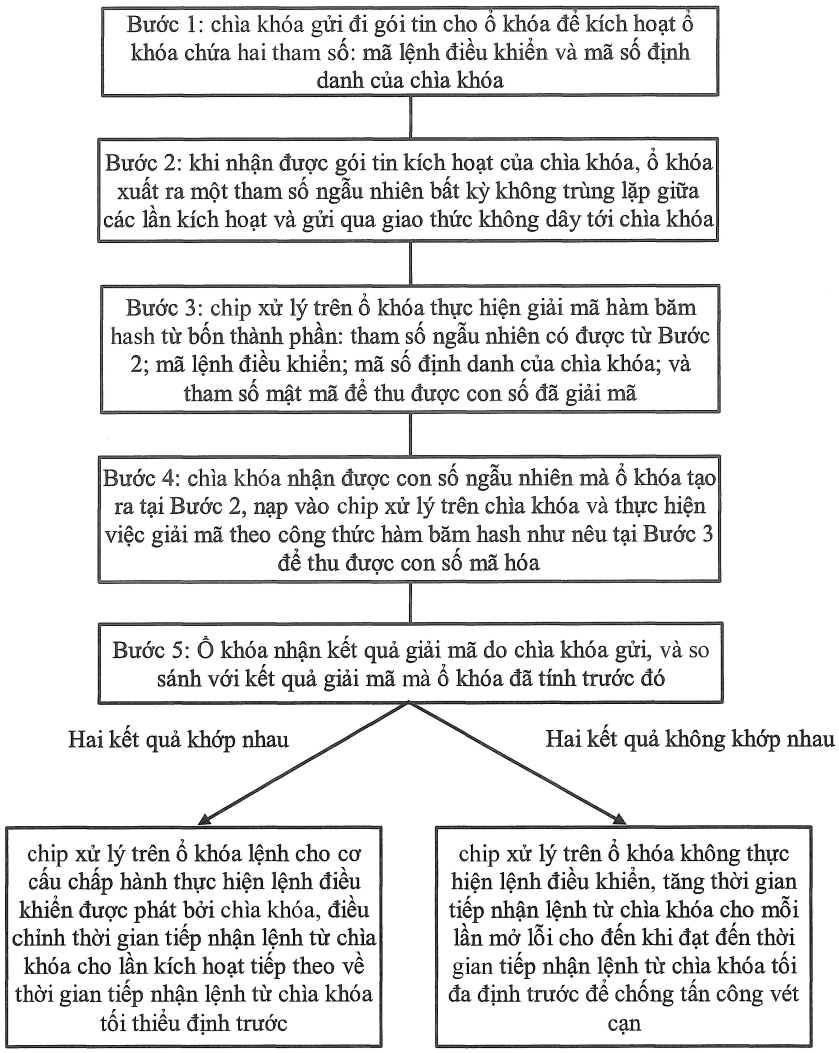
(72) Nguyễn Khương Tuấn (VN); Dương Quang Dũng (VN).

(54) PHƯƠNG PHÁP KÍCH HOẠT KHÓA TỪ XA SỬ DỤNG MẬT MÃ VÀ HỆ THỐNG THỰC HIỆN PHƯƠNG PHÁP NÀY

(21) 1-2020-01076

(57) Sáng chế đề cập đến phương pháp kích hoạt khóa từ xa sử dụng mật mã với cơ chế xác minh hai chiều giữa chìa khóa và ổ khóa, và hệ thống thực hiện phương pháp này. Trong đó, chìa khóa và ổ khóa cùng giải mã công thức hàm băm để xác minh mật mã trước khi thực hiện lệnh điều khiển. Ngoài ra, phương pháp kích hoạt khóa từ xa sử dụng mật mã của sáng chế còn bao gồm chế độ ngăn chặn tấn công mật mã theo thời gian bằng cách tăng thời gian tiếp nhận lệnh phát từ chìa khóa theo mỗi lần sai mật mã.

Hình 1



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp kích hoạt khóa từ xa sử dụng mật mã với cơ chế xác minh hai chiều giữa chìa khóa và ổ khóa, và hệ thống thực hiện phương pháp này. Phương pháp và hệ thống trên được áp dụng trong các lĩnh vực kỹ thuật: khóa điều khiển từ xa bằng sóng dành cho các loại cửa như: cửa ra vào, cửa cuốn, giếng trời, cổng, cửa sổ, cửa trượt,…; khóa điều khiển từ xa bằng sóng dành cho phương tiện giao thông: ô tô, ô tô điện, xe máy, xe máy điện, xe đạp điện…; bộ điều khiển kích hoạt từ xa bằng sóng dành cho các thiết bị điện có vị trí lắp đặt không thuận lợi cho việc điều khiển trực tiếp; bộ điều khiển kích hoạt từ xa bằng sóng dành cho các thiết bị điện có vị trí lắp đặt trong môi trường không cho phép việc điều khiển trực tiếp, ví dụ: môi trường phóng xạ, môi trường ô nhiễm sinh học; bộ điều khiển kích hoạt từ xa bằng sóng vô tuyến dành cho: các thiết bị kích hoạt cần đảm bảo an toàn và tránh sai sót, ví dụ: thiết bị kích nổ khai mỏ,…; ứng dụng thiết bị báo trộm; ứng dụng thiết bị thẻ định danh; dùng để thay thế cho các loại mã cố định; dùng để hay thế cho loại mã nhảy (MicroChip KeeLog). Các lệnh có thể là: đóng, mở, bắt đầu, dừng lại, hủy bỏ, hẹn giờ,…

Tình trạng kỹ thuật của sáng chế

Phương pháp kích hoạt khóa sử dụng mật mã đã được sử dụng từ lâu. Một trong những hệ mã phổ biến của phương pháp này mã nhảy (Rolling Code). Ra đời vào năm 1993, đây là hệ mã có tính bảo mật cao, trong đó mỗi lần kích hoạt thì thuật toán sẽ tạo ra một mã khác nhau và không trùng nhau. Tuy nhiên, mã nhảy tồn tại lỗ hổng bảo mật cho phép kẻ xấu có thể khai thác, đã được Samy Kamkar – một chuyên gia bảo mật công bố và trình diễn demo tại hội nghị DefCon23 năm 2015 tại Paris.

Hiện nay, thậm chí việc "đánh chìa khóa ô tô" được rao công khai trên mạng, nhưng không được chính hãng hay cơ quan nhà nước có thẩm quyền kiểm soát, chắc chắn rằng các thiết bị mà "thợ làm khóa" sử dụng để đánh chìa là một dạng "keygen" có thể bẻ gãy hệ thống mật mã của các hãng xe, và thông tin về mã đó có thể được lưu lại và sử dụng cho mục đích khác về sau.

Trước khi hệ thống mã nhảy Rolling Code ra đời, phải kể đến một số hệ mã được sử dụng rộng rãi như là lựa chọn rẻ hơn cho người sử dụng như Fix Code – hệ mã được đặt cố định bảo mật bằng mạch cứng (chuyển mạch, hàn...) sử dụng các IC chuyên dụng như PT226x / PT227x, … hoặc Learning Code – hệ mã cho phép ổ khóa học mẫu của chìa khóa với số bit

mã hoá lớn hơn nên khả năng bảo mật cũng cao hơn, tuy nhiên có thể bị sao chép dễ dàng, hoặc có thể bị tấn công vét cạn toàn bộ dải mã dễ dàng, do đặc tính cố định của mã.

Ngoài ra, một số loại khóa thông minh mới (SmartKey) gặp phải tình huống: nếu ổ khóa nhận hàng loạt và liên tiếp nhiều lệnh kích hoạt sai mật mã hoặc các gói tin rác, có thể khiến cho ổ khóa bị treo, tức là rơi vào trạng thái hoạt động không bình thường, ví dụ: không thể nổ máy xe. Trường hợp này được gọi là tấn công từ chối dịch vụ (DDoS).

Các thế hệ khóa cũ đều có chung cơ chế giao tiếp một chiều. Tức là, chỉ có chìa khóa phát đi mật mã, ổ khóa nhận được mật mã và kiểm tra, nếu đúng mã là ghi nhận, mật mã có thể được sinh ra từ các hàm sinh mã khác nhau từ đơn giản đến phức tạp. Phương pháp hoạt động dựa trên giả định rằng: chỉ có chìa khóa đã ghép với ổ khóa mới có thể phát đi mật mã đúng, mà không có cơ chế xác minh lại, chính là điểm yếu rất lớn về bảo mật khiến mật mã có thể bị sao chép. Mặt khác, các hàm mã thường sử dụng có một số đặc tính toán học riêng, như là giả ngẫu nhiên, nhằm mục đích chống lại tấn công thống kê, và cần có các hàm đủ đơn giản để tích hợp vào phần cứng. Tuy nhiên, số lượng các hàm như vậy không có nhiều và chính vì vậy người ta có thể thực hiện khảo sát và tìm ngược lại hàm sinh mã đã sử dụng.

Do đó, có nhu cầu để giải quyết các vấn đề nêu trên, và đề xuất phương pháp kích hoạt khóa từ xa sử dụng mật mã với cơ chế xác minh mã cải tiến giúp ngăn chặn hành vi sao chép, bẻ gãy và truy tìm hàm sinh mã – cơ sở cho việc lộ mật mã, tấn công và đột nhập, có thể có chế độ ngăn chặn tấn công mật mã theo thời gian.

Bản chất kỹ thuật của sáng chế:

Mục đích của sáng chế là ngăn chặn hành vi sao chép, bẻ gãy và truy tìm hàm sinh mã – cơ sở cho việc lộ mật mã, tấn công và đột nhập, đồng thời ngăn chặn sự tấn công mật mã theo thời gian.

Để đạt được mục đích nêu trên, sáng chế đề xuất phương pháp kích hoạt khóa từ xa sử dụng mật mã gồm các bước sau:

Bước 1: Theo lệnh của người dùng, chìa khóa gửi đi gói tin cho ổ khóa để kích hoạt ổ khóa chứa hai tham số: mã lệnh điều khiển và mã số định danh của chìa khóa.

Trong đó, lệnh điều khiển có thể là bất kỳ lệnh nào được gán cho từ khóa quy ước và giá trị tương ứng được thiết kế sao cho tập hợp các giá trị của nó và tập hợp các giá trị đảo bit của nó không giao nhau, và mã số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa.

Bước 2: Nhận được gói tin kích hoạt của chìa khóa, nếu tham số định danh của chìa khóa trong gói tin gửi cho ổ khóa không khớp với tham số định danh đặt trước trên ổ khóa, hoặc chưa kết thúc khoảng thời gian tiếp nhận lệnh đặt trước, ổ khóa không có phản ứng.

Nếu tham số định danh của chìa khóa trong gói tin gửi cho ổ khóa khớp với tham số định danh đặt trên ổ khóa, chip xử lý tích hợp sẵn phần mềm nhúng trên ổ khóa xuất ra một con số ngẫu nhiên bất kỳ không trùng lặp giữa các lần kích hoạt trong thời gian định trước.

Con số ngẫu nhiên này được gửi qua giao thức không dây tới chìa khóa.

Con số ngẫu nhiên này có độ dài tối thiểu 24 bit, được sinh ra ngẫu nhiên dựa trên tham số kỷ nguyên thời gian và hằng số biểu thị kích thước không gian số sinh ngẫu nhiên cho hàm sinh số ngẫu nhiên.

Bước 3: Đồng thời với việc sản sinh ra con số ngẫu nhiên tại bước 2, chip tích hợp trên ổ khóa thực hiện giải mã theo hàm băm hash bao gồm bốn thành phần: con số ngẫu nhiên có được từ Bước 2; mã lệnh điều khiển; mã số định danh của chìa khóa; và tham số mật mã.

Trong đó, tham số mật mã được tính theo hàm băm cấu thành từ ba thành phần: tham số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa, tham số do nhà sản xuất khóa định nghĩa, và mã PIN là chuỗi số ngẫu nhiên do hệ thống tự động sinh ra mỗi khi người dùng ra lệnh thiết lập.

Kết quả của Bước 3, ổ khóa thu được một con số đã được giải mã.

Bước 4: Chìa khóa nhận được con số ngẫu nhiên mà ổ khóa tạo ra tại Bước 2 bằng giao thức không dây, nạp vào chip xử lý tích hợp trên chìa khóa và thực hiện việc giải mã theo công thức hàm băm hash như nêu tại Bước 3, kết quả giải mã thu được con số mã hóa, nếu không có sai sót nào trên đường truyền, con số này sẽ khớp với con số mà ổ khóa thu được tại Bước 3, sau đó, chìa khóa gửi thông tin về kết quả giải mã qua giao thức không dây tới ổ khóa trong khoảng thời gian định trước.

Bước 5: Ổ khóa nhận kết quả giải mã do chìa khóa gửi, và so sánh với kết quả giải mã mà ổ khóa đã tính trước đó.

Nếu hai giá trị trùng khớp, chip xử lý trên ổ khóa lệnh cho cơ cấu chấp hành thực hiện lệnh điều khiển được phát bởi chìa khóa, đồng thời điều chỉnh thời gian tiếp nhận lệnh từ chìa khóa cho lần kích hoạt tiếp theo về thời gian tiếp nhận lệnh từ chìa khóa tối thiểu định trước.

Nếu hai giá trị không khớp nhau hoặc không nhận được phản hồi trong vòng khoảng thời gian định trước, chip xử lý trên ổ khóa không thực hiện lệnh điều khiển, đồng thời ghi nhận đó là một lần mở lỗi và tăng thời gian tiếp nhận lệnh từ chìa khóa cho mỗi lần mở lỗi cho đến khi đạt đến thời gian tiếp nhận lệnh từ chìa khóa tối đa định trước để chống tấn công vét cạn.

Hệ thống thực hiện phương pháp kích hoạt khóa từ xa sử dụng mật mã theo sáng chế gồm:

Chìa khóa, bao gồm các nút bấm, mỗi nút bấm tương ứng với một lệnh như mở, đóng, lên, xuống,...; một nút bấm để cài đặt mã PIN; bộ phận phát sóng vô tuyến; bộ phận thu sóng và chip xử lý có chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước; nguồn điện. Ngoài ra, chìa khóa có thể bao gồm thêm: màn hiển thị đèn, chớp đèn, MCU.

Ổ khóa, trên đó có bộ phận phát sóng; bộ phận thu sóng vô tuyến và chip xử lý có chứa phần mềm nhúng để thực thi việc mã hóa và giải mã theo công thức đã được cài đặt trước; cơ cấu chấp hành lệnh từ chip xử lý; nguồn điện. Ngoài ra, ổ khóa có thể bao gồm thêm: cổng phụ trợ để kết nối nút bấm đóng/mở bằng tay có thể kích hoạt bằng mã PIN; màn hiển thị đèn, chớp đèn hoặc màn LCD cỡ nhỏ để hiển thị thông tin; loa hoặc còi báo; cổng kết nối môđun wifi để mở rộng kết nối với smartphone, môđun phụ trợ.

Trong đó, công thức cài đặt trước trong phần mềm nhúng để giải mã trong chìa khóa trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã trong ổ khóa.

Chìa khóa và ổ khóa được đồng bộ với nhau bởi tham số mật mã được tính theo hàm băm cấu thành từ ba thành phần: tham số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa, tham số do nhà sản xuất khóa định nghĩa, và mã PIN là chuỗi số ngẫu nhiên do hệ thống tự động sinh ra mỗi khi người dùng ra lệnh thiết lập.

Mô tả vắn tắt các hình vẽ

Hình 1. là lưu đồ minh họa phương pháp kích hoạt khóa từ xa sử dụng mật mã theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Sau đây, sáng chế sẽ được mô tả chi tiết với các ví dụ kèm theo. Phương án thực hiện sáng chế sau đây được đưa ra làm ví dụ nhằm mục đích bộc lộ toàn bộ sáng chế với người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng. Tuy nhiên, các ví dụ không làm giới hạn sáng chế. Sáng chế bao gồm tất cả các biến thể, các phép tương đương và các lựa chọn thay thế thuộc tinh thần và phạm vi của sáng chế.

Cần phải hiểu rằng, nếu không có chỉ dẫn khác, các thuật ngữ được dùng trong bản mô tả nên được hiểu là đã được người có hiểu biết trung bình về lĩnh vực kỹ thuật này hiểu rõ và sử dụng rộng rãi. Các thuật ngữ được sử dụng trong bản mô tả sáng chế là nhằm mục đích mô tả các phương án cụ thể và không phải là để giới hạn. Các thuật ngữ như random_token, Keyword, KeyID/ SerialNumber, CypherKey, MasterKey, PIN được dùng để phân biệt các tham số mật mã khác nhau và không làm giới hạn sáng chế.

Theo một phương án của sáng chế, phương pháp kích hoạt khóa từ xa sử dụng mật mã là giao thức hai chiều giữa chìa khóa và ổ khóa, được thực hiện dưới dạng sóng vô tuyến tần số RF.

Phương pháp kích hoạt khóa từ xa sử dụng mật mã của sáng chế được thực hiện thông qua hai thành phần chính, gồm chìa khóa và ổ khóa.

(i) Trên chìa khóa có các nút bấm, mỗi nút bấm tương ứng với một lệnh như mở, đóng, lên, xuống,...; một nút bấm để cài đặt mã PIN; bộ phận phát sóng vô tuyến; bộ phận thu sóng và chip xử lý có chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước. Công thức cài đặt trước trong phần mềm nhúng để giải mã trong chìa khóa trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã trong ổ khóa;

(ii) Trên ổ khóa có bộ phận phát sóng; bộ phận thu sóng vô tuyến và chip xử lý có chứa phần mềm nhúng để thực thi việc mã hóa và giải mã theo công thức đã được cài đặt trước; cơ cấu chấp hành lệnh từ chip xử lý. Công thức cài đặt trước trong phần mềm nhúng để giải mã trong ổ khóa trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã trong chìa khóa;

Chìa khóa và ổ khóa được ghép cặp và đồng bộ với nhau bởi tham số mật mã (CypherKey) được tính theo hàm băm cấu thành từ ba thành phần: tham số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa (KeyID hay SerialNumber), tham số do nhà sản xuất khóa định nghĩa (Masterkey), và chuỗi số ngẫu nhiên do hệ thống tự động sinh ra mỗi khi người dùng ra lệnh thiết lập (mã PIN). Hàm sinh mã được sử dụng là hàm SHA, còn được gọi là mã hóa một chiều, do đó việc thu thập các bản mã không giúp ích cho việc tìm ngược ra các tham số đã sử dụng để sinh mã.

Theo một phương án ưu tiên, tham số mật mã CypherKey được xây dựng từ hàm băm SHA1 với ba tham số trên, có công thức như sau:

SHA1 (MasterKey, SerialNumber, PIN)

Trong đó:

- Masterkey là tham số do nhà sản xuất khóa định nghĩa;
- KeyID hay SerialNumber là tham số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa, có thể là nhà sản xuất ô tô, nhà sản xuất cửa cuốn,... hoặc bất kỳ nhà sản xuất thứ ba nào khác để phục vụ việc quản lý, và không bị giới hạn độ dài của dãy số;
- Mã PIN (personal id number) là chuỗi số ngẫu nhiên được hệ thống tự động sinh ra và thống nhất giữa ổ khóa và chìa khóa mỗi khi người dùng ra lệnh thiết lập. Người dùng có thể tùy ý đặt lại mã PIN bằng cách bấm vào một nút tương ứng trên chìa khóa. Khi đó, bộ xử

lý trên chìa khóa sẽ xuất ra một mã số ngẫu nhiên và gửi đến ổ khóa để lưu trữ và cùng sử dụng chung. Theo phương án của sáng chế, người dùng chỉ ra lệnh thiết lập mã PIN mà không được thông báo mã PIN.

Trong đó, Công thức tạo mã PIN là:

- Trường hợp thiết kế hệ thống người dùng không cần nhớ mã PIN:

$PIN = [P_0 - P_{pin\_lengh}]$

P_i = random(0-255) với mọi i = 0 => pin_lengh

pin_lengh: độ dài của mã PIN, có thể rất dài,

Theo một phương án ưu tiên, PIN dài 112 byte, và người sử dụng không cần nhớ mã PIN, nên không cần lưu trữ lại mã PIN;

- Trường hợp thiết kế hệ thống người dùng có thể cất và lưu trữ mã PIN cho các mục đích điều khiển khác:

$PIN = [P_0 - P_{pin\_lengh}]$

P_i = random('a'-'z', 'A'-'Z', '0'-'9') với mọi i = 0 => pin_lengh

pin_lengh: độ dài của PIN, có thể rất dài,

Theo một phương án ưu tiên khác, PIN dài 256 ký tự gồm số và chữ có phân biệt viết hoa và viết thường; việc in mã PIN này ra ngoài để lưu trữ yêu cầu phương pháp bảo mật riêng cho việc lưu trữ đó để đạt được bảo mật tối đa, và không thuộc phạm vi của sáng chế này.

Ví dụ về công thức tạo CypherKey với tham số cụ thể:

MasterKey = "56464e4c48105feedd10b652520b6bdcd0ad66b0"

SerialNumber = "0123456789ABCDEF"

PIN = "42efda2d63c5b28d827b5173722185568e076522"

Khi đó:

CypherKey = SHA1(MasterKey, SerialNumber, PIN)

= SHA1(

"56464e4c48105feedd10b652520b6bdcd0ad66b00123456789ABCDEF42efda2d63c5b28d827b5173722185568e076522")

= "c677474d4adf3bcc2d7f2d41566462ae3dd47d72"

Tuy nhiên, sáng chế không bị giới hạn tại đây. Có thể sử dụng các hàm số mới hơn nhằm đạt mức độ bảo mật cao hơn, như hàm SHA3 hoặc hàm Keccak với số bit lớn hơn.

Sáng chế được thực hiện theo các bước sau:

Bước 1: Theo lệnh của người dùng, chìa khóa gửi đi gói tin cho ổ khóa để kích hoạt ổ khóa, lệnh đó chứa hai tham số: mã lệnh cần kích hoạt (đóng, mở, dừng….), còn gọi là Keyword, và mã số định danh của chìa khóa, còn gọi là KeyID hoặc SerialNumber. Cụ thể:

- Keyword là mã lệnh cần kích hoạt, dùng để phân biệt các lệnh cần thực hiện. Sáng chế không giới hạn số lượng mã lệnh đối đa.

- KeyID hoặc SerialNumber là mã số định danh của chìa khóa, do nhà sản xuất sản phẩm sử dụng khóa định nghĩa.

Theo một phương án ưu tiên, gói tin kích hoạt được biểu diễn bằng hàm số như sau:

[Keyword][KeyID]

Trong đó, Keyword có thể là bất kỳ lệnh nào được gán cho từ khóa quy ước và giá trị tương ứng, miễn là Keyword được thiết kế sao cho tập hợp các giá trị của nó {Keyword} và tập hợp các giá trị đảo bit của nó {~ Keyword} không giao nhau nhằm tối ưu hóa việc xử lý thông tin ở Bước 2. Ví dụ về Keyword như được thể hiện thể hiện trong Bảng 2:

Bảng 2: Ví dụ về Keyword

Tên	Từ khóa	Giá trị	Ghi chú
Đóng	CLOSE	0xD0	Cũng có thể mang ý nghĩa là: Hủy kích hoạt, hủy bỏ
Mở	OPEN	0xE0	Cũng có thể mang ý nghĩa là: kích hoạt, bắt đầu
Dừng	STOP	0xC0	
Lên	UP	0xB0	
Xuống	DOWN	0xA0	
Trái	LEFT	0x90	
Phải	RIGHT	0x80	
Đặt mã	SetPIN	0xFE	

Cần lưu ý rằng, bảng ví dụ trên không giới hạn số lượng các lệnh cũng như từ khóa và giá trị tương ứng của lệnh.

Theo một phương án của sáng chế, khi người dùng chọn lệnh Mở, khi đó, gói lệnh được phát đi có thể là: "E0000001"

Trong đó: Mở = "E0", KeyID = "000001"

Bước 2: Khi nhận được gói tin kích hoạt của chìa khóa, nếu mã số định danh của chìa khóa trong gói tin gửi cho ổ khóa không khớp với mã số định danh đặt trước trên ổ khóa, hoặc chưa kết thúc khoảng thời gian tiếp nhận lệnh đặt trước $T_{protect}$, ổ khóa không có phản ứng.

Nếu mã số định danh của chìa khóa trong gói tin gửi cho ổ khóa khớp với mã số định danh đặt trước trên ổ khóa thì chip xử lý tích hợp sẵn phần mềm nhúng trên ổ khóa xuất ra một tham số ngẫu nhiên random_token bất kỳ không trùng lặp giữa các lần kích hoạt. Random_token được gửi qua giao thức không dây tới chìa khóa trong thời gian tiếp nhận lệnh $T_{protect}$ đặt trước.

Ví dụ, nếu $T_{protect}$ = 500ms, thì sau 500ms kể từ khi lệnh được phát, mã số định danh trong gói tin khớp với mã số định danh trên ổ khóa thì ổ khóa sẽ phản ứng.

Con số ngẫu nhiên random_token có độ dài tối thiểu 24 bit, được sinh ra dựa trên tham số kỷ nguyên thời gian epoch_id và hằng số epoch_size biểu thị kích thước không gian số sinh ngẫu nhiên cho hàm sinh số ngẫu nhiên.

Theo một phương án của sáng chế, các random_token được sinh ra không trùng nhau, do việc chia mỗi kỷ nguyên (epoch) là một ngày sử dụng, epoch_id được đánh số từ 0-4095 tương ứng với 12 bit sử dụng và đánh số được các ngày trong hơn 11 năm kể từ ngày bắt đầu sử dụng, với token_lengh = 64 bit, epoch_size còn lại 64 - 12 = 52 bit, tức là các giá trị từ 0 đến 2^{53}-1, là không gian số sinh ngẫu nhiên cho hàm sinh số ngẫu nhiên.

Công thức để tính random_token như sau:

random_token = epoch_id * epoch_size + random(epoch_size)

Trong đó, tham số epoch_id là số hiệu kỷ nguyên thời gian

tham số epoch_size là một hằng số, biểu thị không gian số sinh ngẫu nhiên cho hàm sinh số ngẫu nhiên, cụ thể là kích thước còn lại của không gian số dành cho token sau khi đã chia theo các kỷ nguyên.

Ví dụ:

token_lengh = 64 bit; chia thành 4096 = 2^{12} kỷ nguyên (epoch) mỗi kỷ nguyên là một ngày

epoch = 127, tức là ngày thứ 127 kể từ ngày hệ thống đi vào hoạt động

epoch_size = $2^{(64-12)} = 2^{52}$

random_token = 127 * 2^{52} + random(0 => (2^{52} - 1))

ví dụ = 0x07FCC157341A7556|$_{HEX}$ = 575547432677045590|$_{DEC}$Theo phương án này, chỉ cần một bộ nhớ rất nhỏ, ví dụ lưu được 256 lần bấm nút trong một ngày, khi chia kỷ nguyên theo ngày, mà không làm suy giảm sự an toàn của mật mã.

Thuật toán trong công thức nêu trên không hạn chế số bit tối đa của random_token, tuy nhiên nên lựa chọn độ dài cho random_token theo năng lực xử lý của hệ thống; tần suất sử dụng theo kỷ nguyên quy định dung lượng bộ nhớ cần có để lưu trữ các token đã được sử dụng trong kỷ nguyên nhằm tránh bị tấn công thu thập từ điển.

Bước 3: Con số ngẫu nhiên tại Bước 2 cũng được gửi qua giao thức không dây tới chìa khóa.

Trên ổ khóa, tham số ngẫu nhiên được đưa vào chip tích hợp trên ổ khóa để giải mã theo Hàm băm hash được xây dựng từ hàm băm cơ sở là một hàm mã hóa bất đối xứng, có thể là bất kỳ trong các loại mã nào sau đây: MD5, SHA1, SHA2, SHA3 (hay còn gọi là Keccak512) và các phân hệ mã Keccak khác.

Hàm băm hash này bao gồm bốn thành phần: tham số ngẫu nhiên random_token có được từ Bước 2; mã lệnh điều khiển (Keyword); mã số định danh của chìa khóa (Key ID hoặc SerialNumber); và tham số mật mã (CypherKey) đã được giải thích trước đó.

Trong một phương án ưu tiên, hàm băm nêu trên được thể hiện dưới dạng công thức như sau:

hash(random_token, Keyword, KeyID, CypherKey)

Ví dụ về câu đố hàm băm với tham số cụ thể với lệnh mở Keyword = E0:

random_token = 0x07FCC157341A7556|$_{HEX}$

Keyword = Mở = "E0", KeyID = "000001"

CypherKey = "c677474d4adf3bcc2d7f2d41566462ae3dd47d72"

Khi đó, hàm băm hash_lock do ổ khóa tính được tính như sau:

hash_lock = SHA1("07FCC157341A7556", "E0", "000001", "c677474d4adf3bcc2d7f2d41566462ae3dd47d72")

= "d0fba6adc7b6f7f8e7c1eb6275287ae26f90d064"

Kết quả của Bước 3, ổ khóa thu được một con số đã được giải mã.

Bước 4: Chìa khóa thu nhận được con số ngẫu nhiên mà ổ khóa tạo ra tại Bước 2, nạp vào chip xử lý tích hợp trên chìa khóa và thực hiện việc giải mã theo công thức hàm băm hash như nêu tại Bước 3. Kết quả giải mã thu được con số mã hóa, nếu không có sai sót nào trên đường truyền, con số này sẽ khớp với con số mà ổ khóa thu được tại Bước 3. Sau đó, chìa khóa gửi thông tin về kết quả giải mã qua giao thức không dây tới ổ khóa trong khoảng thời gian định trước T_{answer}.

Ví dụ về câu trả lời hàm băm hash_key do chìa khóa tính khi kích hoạt lệnh mở:

Ví dụ a:

Tất cả các tham số khớp nhau:

random_token = 0x07FCC157341A7556|HEX

Keyword = Mở = "E0", KeyID = "000001"

CypherKey = "c677474d4adf3bcc2d7f2d41566462ae3dd47d72"

Tức là nhận đúng random_token, lệnh mở "E0", chìa khóa có KeyID "000001"

Khi đó, hàm băm hash_key do chìa khóa tính được tính như sau:

hash_key = SHA1("07FCC157341A7556", "E0", "000001", "c677474d4adf3bcc2d7f2d41566462ae3dd47d72")

= "d0fba6adc7b6f7f8e7c1eb6275287ae26f90d064"

Là một kết quả đúng.

Ví dụ b:

KeyID/SerialNumber của chìa khóa không khớp với ổ khóa:

random_token = 0x07FCC157341A7556|HEX

Keyword = Mở = "E0", KeyID của chìa khóa đúng = "000001"

CypherKey = "c677474d4adf3bcc2d7f2d41566462ae3dd47d72"

Tức là nhận đúng random_token, yêu cầu mở "E0", nhưng chìa khóa trả lời có KeyID "000002".

Khi đó, hàm băm hash_key do chìa khóa tính được tính như sau:

hash_key = SHA1("07FCC157341A7556", "E0", "000002", "c677474d4adf3bcc2d7f2d41566462ae3dd47d72")

= "1f515d2cdd44d27bcdb9485a3a03b8b9835541f0"

Là một kết quả sai.

Tình huống này có thể xảy ra khi ai đó định giả mạo chìa khóa có KeyID = "000001".

Ví dụ c:

Mã lệnh không khớp:

random_token = 0x07FCC157341A7556|HEX

Keyword = Đóng = "D0", KeyID = "000001"

CypherKey = "c677474d4adf3bcc2d7f2d41566462ae3dd47d72"

Tức là nhận đúng random_token, chìa khóa có KeyID "000001", nhưng mã lệnh là Đóng "D0".

Khi đó, hàm băm hash_key do chìa khóa tính được tính như sau:

hash_key = SHA1("07FCC157341A7556", "D0", "000001", "c677474d4adf3bcc2d7f2d41566462ae3dd47d72")

= “c17977e5696f3f91286111ee3403077dd8186467”

Là một kết quả sai.

Tình huống này có thể xảy ra khi ai đó định giả mạo mã lệnh bằng cách sao chép hàm băm của lệnh Đóng và thay thế bằng lệnh Mở.

Ví dụ d:

Tham số mật mã CypherKey không khớp:

random_token = 0x07FCC157341A7556|HEX

Keyword = Mở = “E0”, KeyID = “000001”

CypherKey = “c677474d4adf3bcc2d7f2d41566462ae3dd47d72”

Tức là nhận đúng random_token, yêu cầu mở “E0”, chìa khóa có KeyID “000001”, nhưng CypherKey là 1 số khác, ví dụ:

CypherKey = “c677474d4adf3bcc2d7f2d41566462ae3dd47d73”, tức là chỉ sai khác một chút.

Khi đó, hàm băm hash_key do chìa khóa tính được tính như sau:

hash_key = SHA1(“07FCC157341A7556”, “E0”, “000001”, “c677474d4adf3bcc2d7f2d41566462ae3dd47d72”)

= “f166b36c5f6545cf5cd164b25adc28115e8ce862”

Là một kết quả sai.

Cần lưu ý rằng, các ví dụ trên được xem xét với các con số biểu diễn dưới hệ Hexa trong miền xâu ký tự, là miền biểu thị được dưới dạng văn bản. Trên máy tính và các con chip, các số này được lưu vào ô nhớ ở dạng tiết kiệm ô nhớ hơn. Tuy nhiên, sáng chế không bị giới hạn tại đây.

Ví dụ: CypherKey = “c677474d4adf3bcc2d7f2d41566462ae3dd47d72”

là dạng xâu ký tự, biểu diễn bằng 40 ký tự, trong máy tính được lưu bằng một con số 160 bit tức là 20 ô nhớ 8 bit.

Bước 5: Ổ khóa nhận kết quả giải mã do chìa khóa gửi, và so sánh với kết quả giải mã mà ổ khóa đã tính trước đó.

Nếu hai giá trị trùng khớp, chip xử lý trên ổ khóa lệnh cho cơ cấu chấp hành thực hiện lệnh được phát bởi chìa khóa.

Theo một phương án của sáng chế, nếu giá trị trùng khớp, chip xử lý điều chỉnh thời gian tiếp nhận lệnh từ chìa khóa $T_{protect}$ cho lần kích hoạt tiếp theo về thời gian tiếp nhận lệnh từ chìa khóa tối thiểu định trước $T_{protect\_min}$, tức là $T_{protect} = T_{protect\_min}$.

Ví dụ, nếu $T_{protect}$ = 500ms, $T_{protect\_min}$ = 500ms, thì khi đúng chìa khóa, $T_{protect}$ = 500ms.

Nếu hai giá trị khác nhau hoặc không nhận được phản hồi trong vòng khoảng thời gian định trước T_{answer}, chip xử lý trên ổ khóa không thực hiện lệnh điều khiển, đồng thời ghi nhận đó là một lần mở lỗi.

Cứ mỗi lần mở lỗi, chip xử lý tăng thời gian tiếp nhận lệnh từ chìa khóa $T_{protect}$ để chống tấn công vét cạn. Trong một phương án ưu tiên, thời gian tiếp nhận lệnh $T_{protect}$ sẽ tăng thêm 01 giây (s) sau mỗi lần mở lỗi cho đến khi đạt đến thời gian tiếp nhận lệnh từ chìa khóa tối đa định trước $T_{protect\_max}$, tức là $T_{protect} = T_{protect\_max}$.

Ví dụ, nếu $T_{protect} = 500ms$, $T_{protect\_max} = 10s$, thì với mỗi lần sai chìa khóa, $T_{protect}$ sẽ tăng thêm 1s cho tới khi $T_{protect} = 10s$.

Ví dụ, nếu trả lời sai câu đố mã hóa 10 lần sẽ khiến mỗi lần nhập sau đó chỉ được tiếp nhận sau 10s, trong khi tấn công vét cạn BruteForce mã SHA256 đã rất khó và hầu như là không thể, thì với $T_{protect} = 10s$ thì việc tấn công còn khó khăn hơn.

Hệ thống thực hiện phương pháp kích hoạt khóa từ xa sử dụng mật mã theo phương án của sáng chế gồm:

Chìa khóa, trên đó có các nút bấm, mỗi nút bấm tương ứng với một lệnh như mở, đóng, lên, xuống,...; một nút bấm để cài đặt mã PIN; bộ phận phát sóng vô tuyến; bộ phận thu sóng và chip xử lý có chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước; nguồn điện. Ngoài ra, chìa khóa có thể bao gồm thêm: màn hiển thị đèn, chớp đèn, MCU,...

Ổ khóa, trên đó có bộ phận phát sóng; bộ phận thu sóng vô tuyến và chip xử lý có chứa phần mềm nhúng để thực thi việc mã hóa và giải mã theo công thức đã được cài đặt trước; cơ cấu chấp hành lệnh từ chip xử lý; nguồn điện. Ngoài ra, thiết bị ổ khóa có thể bao gồm thêm: cổng phụ trợ để kết nối nút bấm đóng/mở bằng tay có thể kích hoạt bằng mã PIN; màn hiển thị đèn chớp, đèn hoặc màn LCD cỡ nhỏ để hiển thị thông tin, loa hoặc còi báo, cổng kết nối môđun wifi để mở rộng kết nối với smartphone, môđun phụ trợ.

Công thức cài đặt trước trong phần mềm nhúng để giải mã trong chìa khóa trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã trong ổ khóa.

Chìa khóa và ổ khóa được ghép cặp và đồng bộ với nhau bởi tham số mật mã (CypherKey) được cấu thành từ hàm băm với ba thành phần: tham số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa (KeyID hoặc SerialNumber), tham số do nhà sản xuất khóa định nghĩa (Masterkey), và chuỗi số ngẫu nhiên do hệ thống tự động sinh ra mỗi khi người dùng ra lệnh thiết lập (PIN).

Hiệu quả đạt được của sáng chế:

Sáng chế giúp vô hiệu hóa hoàn toàn lỗ hổng bảo mật của phương thức bảo mật Rolling Code đang mắc phải. Do đó phương thức nghe lén rồi phát lại mã không có tác dụng. Bởi lẽ, mỗi lần chìa khóa phát đi gói tin kích hoạt, ổ khóa đều sinh ra một mã token ngẫu nhiên và không lặp lại, lập thành câu đố hàm băm yêu cầu chìa khóa phải trả lời để xác thực. Nếu ổ khóa bị chặn không nhận được gói tin kích hoạt, hoặc đã nhận gói tin kích hoạt và phát đi câu hỏi nhưng không nhận được câu trả lời trong khoảng thời gian đặt trước, thì lập tức giao thức giữa chìa khóa và ổ khóa bị hủy bỏ. Tức là việc lắng nghe và lưu lại thông tin trao đổi giữa ổ khóa và chìa khóa không giúp ích được cho bên lắng nghe nhằm can thiệp hay đột nhập sau này.

Phương pháp mà sáng chế đề xuất khiến việc giả mạo chìa khóa trở nên bất khả thi. Mỗi chìa khóa đều đồng bộ với ổ khóa bởi tham số mật mã, trong bản mô tả này gọi là CypherKey. Hàm sinh mã với tham số CypherKey được sử dụng là hàm SHA, được phát minh đầu năm 1993. Các hàm số này còn được gọi là mã hóa một chiều. Tức là việc thu thập các bản mã không giúp ích cho việc tìm ngược ra các tham số đã sử dụng để sinh mã. Tức là có thể công khai gửi đi các bản mã mà không phải lo ngại rằng sẽ bị lộ tham số mật mã CypherKey.

Cấu trúc ba thành phần của CypherKey đảm bảo chủ quyền của người sử dụng. Bởi PIN là một số rất dài, nhưng người sử dụng không thể biết PIN, nên nhà sản xuất khóa và nhà sản xuất sản phẩm sử dụng khóa không thể tự ý can thiệp vào sản phẩm đã cung cấp cho khách hàng. Cho dù vì lý do nào đó các thành phần mã do nhà sản xuất khóa và mã do nhà sản xuất sản phẩm sử dụng khóa bị lộ, khả năng xâm phạm cũng không thể xảy ra. Cũng vì thành phần mã PIN được hệ thống sinh ra ngẫu nhiên, CypherKey không thể bị trùng lặp giữa hai sản phẩm.

Việc sao chép chìa khóa khi không được ủy quyền từ nhà sản xuất sản phẩm sử dụng khóa cũng là không thể. Bởi lẽ, cấu trúc xây dựng chìa bao gồm ba thành phần cho phép phát triển phần mềm phân quyền riêng biệt, không thể tùy tiện sao chép nếu không được cấp phép. Điều này còn có thể cho phép nhà nước thiết lập một cơ quan chuyên trách kiểm soát các cơ sở, đại lý cung cấp dịch vụ về khóa.

Phương thức tấn công vét cạn BruteForce không có tác dụng bởi: Với tham số $T_{protect}$ được xem xét, việc hạn chế thời gian truy nhập liên tiếp vào ổ khóa với thời gian $T_{protect}$ dần từ $T_{protect\_min}$ đến $T_{protect\_max}$ có tác dụng như một tường lửa ngăn chặn việc thử liên tục các mã có thể, việc tấn công vét cạn không gian mã trở nên khó khăn vì tiêu tốn quá nhiều thời gian.

Thông tin trong mỗi giao thức chỉ dùng một lần và không thể giả mạo nên tấn công liên tiếp bằng các gói tin mô phỏng giao thức chỉ có thể cho kết quả sai, khi đó cơ chế chống tấn

công theo tham số $T_{protect}$ được xem xét và vô hiệu hóa tương tự như việc chống lại tấn công BruteForce.

Phương thức tấn công từ chối dịch vụ DDoS không có tác dụng bởi: với việc kiểm soát gói tin kích hoạt, các byte trong một gói tin phải liên tiếp nhau theo thời gian, giúp cho ổ khóa lọc bỏ được nhiễu không xử lý.

Sáng chế cho phép thiết kế phần cứng chìa khóa có thể hoạt động ở chế độ tiết kiệm năng lượng. Một lệnh kích hoạt luôn do phía chìa khóa khởi xướng, cho phép chìa khóa có thể đặt trạng thái ngủ, là trạng thái tiết kiệm năng lượng tối đa, và chỉ thức dậy hoạt động khi có tác động từ người sử dụng.

Phương pháp mà sáng chế đề xuất không bị suy giảm độ tin cậy theo thời gian. Khác với phương thức đồng bộ token của một số dạng token sử dụng đồng hồ đếm thời gian, việc đồng bộ token của sáng chế sử dụng phương pháp truyền trực tiếp qua sóng. Khi sử dụng đồng hồ đo thời gian, mức chi phí phù hợp cho thiết bị dân dụng thường sử dụng công nghệ dao động thạch anh, công nghệ này tích lũy sai số theo thời gian có thể lên tới 1s sau 1 năm, tức là nhanh chóng đến ngưỡng mất đồng bộ khi sử dụng.

Phương pháp mà sáng chế đề xuất có thể hoạt động trên nhiều thiết bị khác nhau với các tính năng khác nhau để ra lệnh điều khiển từ xa nhằm xác thực.

Nhờ việc sử dụng mã sửa sai và giao thức phát lại tin khi nhận sai, phương pháp mà sáng chế đề xuất cho phép thiết bị có thể hoạt động trong môi trường có nhiều nhiễu điện từ. Phương pháp này có ưu điểm so với phương pháp "phát lặp lại nhiều đoạn mã" hiện đang được sử dụng trên nhiều loại chìa khóa ở chỗ, trong môi trường bình thường, chỉ cần truyền một lần là chính xác đến đích thay vì truyền nhiều lần khiến cho chìa khóa tiêu tốn năng lượng nhiều hơn, và trong môi trường nhiễu, việc giao tiếp vẫn đạt hiệu quả tương đương hoặc cao hơn so với phương pháp phát lặp lại nhiều lần.

Giao thức hai chiều giữa chìa khóa và ổ khóa của sáng chế có thể công khai, công thức xây dựng hàm hash với các tham số có thể công khai, có thể sao chép cách thực hiện theo cách hợp pháp hoặc bất hợp pháp, xong không thể dùng nó để xâm phạm hệ thống khóa sử dụng phương pháp kích hoạt khóa từ xa sử dụng mật mã của sáng chế. Đây là một khác biệt rất lớn so với thuật toán KeeLog của hãng Microchip.

YÊU CẦU BẢO HỘ

1. Phương pháp kích hoạt khóa từ xa sử dụng mật mã bao gồm:

bước 1: theo lệnh của người dùng, chìa khóa gửi đi gói tin cho ổ khóa để kích hoạt ổ khóa chứa hai tham số: mã lệnh điều khiển và mã số định danh của chìa khóa,

bước 2: nhận được gói tin kích hoạt của chìa khóa, nếu mã số định danh của chìa khóa trong gói tin gửi cho ổ khóa không khớp với mã số định danh đặt trước trên ổ khóa, hoặc chưa kết thúc khoảng thời gian tiếp nhận lệnh đặt trước, ổ khóa không có phản ứng,

nếu mã số định danh của chìa khóa trong gói tin gửi cho ổ khóa khớp với mã số định danh đặt trên ổ khóa, chip xử lý tích hợp sẵn phần mềm nhúng trên ổ khóa xuất ra một tham số ngẫu nhiên bất kỳ không trùng lặp giữa các lần kích hoạt,

tham số ngẫu nhiên này được gửi qua giao thức không dây tới chìa khóa;

bước 3: đồng thời, trên ổ khóa, chip xử lý tích hợp thực hiện giải mã theo hàm băm hash từ bốn thành phần: tham số ngẫu nhiên có được từ bước 2; mã lệnh điều khiển; mã số định danh của chìa khóa; và tham số mật mã,

trong đó, tham số mật mã được tính theo hàm băm cấu thành từ ba thành phần: mã số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa, mã số do nhà sản xuất khóa định nghĩa, và mã PIN là chuỗi số ngẫu nhiên do hệ thống tự động sinh ra mỗi khi người dùng ra lệnh thiết lập;

kết quả của bước 3, ổ khóa thu được một con số đã được giải mã;

bước 4: Chìa khóa nhận được con số ngẫu nhiên mà ổ khóa tạo ra tại bước 2, nạp vào chip xử lý tích hợp trên chìa khóa và thực hiện việc giải mã theo công thức hàm băm hash như nêu tại bước 3, kết quả giải mã thu được con số mã hóa, nếu không có sai sót nào trên đường truyền, con số này sẽ khớp với con số mà ổ khóa thu được tại bước 3,

sau đó, chìa khóa gửi thông tin về kết quả giải mã qua giao thức không dây tới ổ khóa trong khoảng thời gian định trước;

bước 5: ổ khóa nhận kết quả giải mã do chìa khóa gửi, và so sánh với kết quả giải mã mà ổ khóa đã tính trước đó,

nếu hai giá trị trùng khớp, chip xử lý trên ổ khóa lệnh cho cơ cấu chấp hành thực hiện lệnh điều khiển được phát bởi chìa khóa,

nếu hai giá trị không khớp nhau hoặc không nhận được phản hồi trong vòng khoảng thời gian định trước, chip xử lý trên ổ khóa không thực hiện lệnh điều khiển.

2. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm 1, trong đó tại bước 1, mã lệnh điều khiển có thể là bất kỳ lệnh nào được gán cho từ khóa quy ước và giá trị tương ứng được thiết kế sao cho tập hợp các giá trị của nó và tập hợp các giá trị đảo bit của nó không giao nhau, và mã số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa.

3. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm 1 hoặc 2, trong đó tại bước 2, con số ngẫu nhiên có độ dài tối thiểu 24 bit, được sinh ra ngẫu nhiên dựa trên tham số kỷ nguyên thời gian và hằng số biểu thị kích thước không gian số sinh ngẫu nhiên cho hàm sinh số ngẫu nhiên.

4. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó hàm băm được sử dụng có thể là bất kỳ hàm số nào có khả năng mã hóa một chiều như hàm SHA3 hoặc hàm Keccak với số bit lớn hơn.

5. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó mã PIN được xác định theo công thức:

PIN = [P0 - Ppin_lengh]

P_i = random(0-255) với mọi i = 0 => pin_lengh

pin_lengh: độ dài của mã PIN, có thể rất dài.

6. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm 5, trong đó mã PIN có dung lượng 112 byte.

7. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó, tại bước 5, nếu hai giá trị trùng khớp, chip xử lý điều chỉnh thời gian tiếp nhận lệnh từ chìa khóa cho lần kích hoạt tiếp theo về thời gian tiếp nhận lệnh từ chìa khóa tối thiểu định trước.

8. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó, tại bước 5, nếu hai giá trị không khớp nhau hoặc ổ khóa không nhận được phản hồi trong vòng khoảng thời gian định trước, ổ khóa ghi nhận đó là một lần mở lỗi, đồng thời, chip xử lý tăng thời gian tiếp nhận lệnh từ chìa khóa cho mỗi lần mở lỗi cho đến khi đạt đến thời gian tiếp nhận lệnh từ chìa khóa tối đa định trước để chống tấn công vét cạn.

9. Phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm 5, trong đó chip xử lý tăng thời gian tiếp nhận lệnh từ chìa khóa cho mỗi lần mở lỗi thêm 1 giây và thời gian tiếp nhận lệnh từ chìa khóa tối đa định trước là 10 giây.

10. Hệ thống thực hiện phương pháp kích hoạt khóa từ xa sử dụng mật mã theo điểm bất kỳ trong số các điểm từ 1 đến 9, hệ thống này bao gồm:

chìa khóa, bao gồm các nút bấm, mỗi nút bấm tương ứng với một lệnh như mở, đóng, lên, xuống, và tương tự; bộ phận phát sóng vô tuyến; bộ phận thu sóng và chip xử lý có chứa phần mềm nhúng để thực thi việc giải mã theo công thức đã được cài đặt trước; nguồn điện;

ổ khóa, trên đó có bộ phận phát sóng; bộ phận thu sóng vô tuyến và chip xử lý có chứa phần mềm nhúng để thực thi việc mã hóa và giải mã theo công thức đã được cài đặt trước; cơ cấu chấp hành lệnh từ chip xử lý; nguồn điện;

chìa khóa và ổ khóa được đồng bộ với nhau bởi tham số mật mã được tính theo hàm băm cấu thành từ ba thành phần: tham số định danh của chìa khóa do nhà sản xuất sản phẩm sử dụng khóa định nghĩa, tham số do nhà sản xuất khóa định nghĩa, và mã PIN là chuỗi số ngẫu nhiên do hệ thống tự động sinh ra mỗi khi người dùng ra lệnh thiết lập;

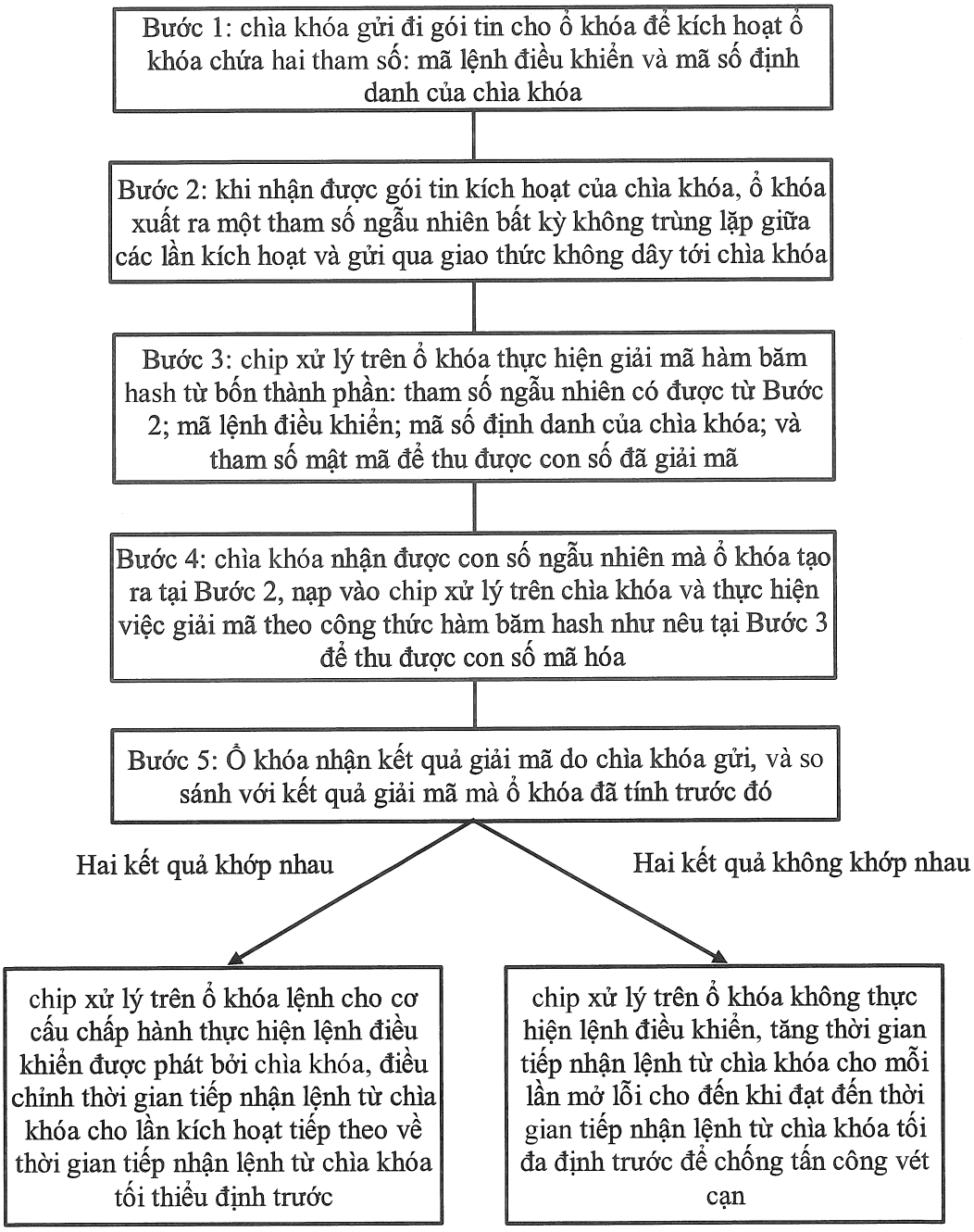
trong đó công thức cài đặt trước trong phần mềm nhúng để giải mã trong chìa khóa trùng với công thức cài đặt trước trong phần mềm nhúng để giải mã trong ổ khóa.

11. Hệ thống theo điểm 10, trong đó chìa khóa có thể bao gồm thêm một nút bấm để cài đặt mã PIN.

12. Hệ thống theo điểm 10 hoặc 11, trong đó ổ khóa có thể bao gồm thêm cổng phụ trợ để kết nối nút bấm đóng/mở bằng tay có thể kích hoạt bằng mã PIN.

13. Hệ thống thực hiện phương pháp kích hoạt khóa từ xa theo điểm bất kỳ trong số các điểm từ 10 đến 12, trong đó ổ khóa còn bao gồm thêm cổng kết nối mở rộng kết nối internet.

Hình 1


Bước 1: chìa khóa gửi đi gói tin cho ổ khóa để kích hoạt ổ khóa chứa hai tham số: mã lệnh điều khiển và mã số định danh của chìa khóa
Bước 2: khi nhận được gói tin kích hoạt của chìa khóa, ổ khóa xuất ra một tham số ngẫu nhiên bất kỳ không trùng lặp giữa các lần kích hoạt và gửi qua giao thức không dây tới chìa khóa
Bước 3: chip xử lý trên ổ khóa thực hiện giải mã hàm băm hash từ bốn thành phần: tham số ngẫu nhiên có được từ Bước 2; mã lệnh điều khiển; mã số định danh của chìa khóa; và tham số mật mã để thu được con số đã giải mã
Bước 4: chìa khóa nhận được con số ngẫu nhiên mà ổ khóa tạo ra tại Bước 2, nạp vào chip xử lý trên chìa khóa và thực hiện việc giải mã theo công thức hàm băm hash như nêu tại Bước 3 để thu được con số mã hóa
Bước 5: Ổ khóa nhận kết quả giải mã do chìa khóa gửi, và so sánh với kết quả giải mã mà ổ khóa đã tính trước đó
Hai kết quả khớp nhau
Hai kết quả không khớp nhau
chip xử lý trên ổ khóa lệnh cho cơ cấu chấp hành thực hiện lệnh điều khiển được phát bởi chìa khóa, điều chỉnh thời gian tiếp nhận lệnh từ chìa khóa cho lần kích hoạt tiếp theo về thời gian tiếp nhận lệnh từ chìa khóa tối thiểu định trước
chip xử lý trên ổ khóa không thực hiện lệnh điều khiển, tăng thời gian tiếp nhận lệnh từ chìa khóa cho mỗi lần mở lỗi cho đến khi đạt đến thời gian tiếp nhận lệnh từ chìa khóa tối đa định trước để chống tấn công vét cạn