



(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)



1-0028778

(51)⁷ G07F 7/02; H01H 13/70

(13) B

(21) 1-2013-00302

(22) 22/07/2011

(86) PCT/CN2011/077473 22/07/2011

(87) WO 2012/022214 23/02/2012

(30) 201010261960.5 20/08/2010 CN

(45) 25/07/2021 400

(43) 27/05/2013 302A

(73) GRG BANKING EQUIPMENT CO., LTD. (CN)

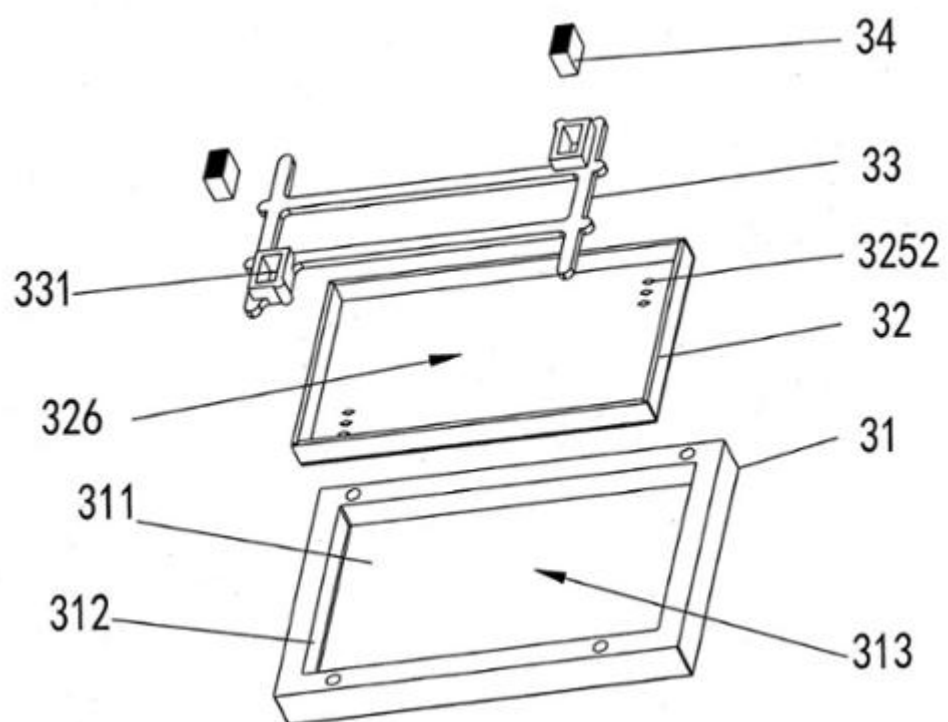
9 Kelin Road, Science City, Luogang District, Guangzhou, Guangdong 510663, P. R. China

(72) ZHANG, Junkun (CN); LIN, Zhulong (CN); HE, Jing (CN); HAN, Ying (CN).

(74) Công ty TNHH Sở hữu trí tuệ WINCO (WINCO CO., LTD.)

(54) BÀN PHÍM MÃ HOÁ CHỐNG CAN THIỆP TRÁI PHÉP

(57) Sáng chế đề cập tới bàn phím mã hoá chống can thiệp trái phép có hệ thống phát hiện và bảo vệ chống can thiệp trái phép theo nhiều hướng. Bàn phím mã hoá chống can thiệp trái phép này bao gồm: tấm gõ phím và bảng điều khiển chính. Bảng điều khiển chính bao gồm mạch điều khiển để thực hiện chức năng tự hủy. Mạch điều khiển được bịt kín cố định ở phía sau của bảng điều khiển chính nhờ cơ cấu bảo vệ chống can thiệp trái phép. Cơ cấu bảo vệ chống can thiệp trái phép được nối điện với mạch điều khiển. Cơ cấu bảo vệ chống can thiệp trái phép bao gồm: vỏ chống nhìn trộm (31) có mặt đáy (311) và thành bên (312) nhô ra thẳng đứng dọc theo các mép chu vi của mặt đáy, thành bên (312) cùng với mặt đáy (311) tạo thành hốc thứ nhất (313); bảng mạch chống can thiệp trái phép cứng (32) được bố trí bên trong hốc thứ nhất (313), và hốc thứ hai (326) được tạo ra nhờ mặt đáy và thành bên hình khuyên, mặt đáy của hốc thứ hai (326) có ít nhất một cặp chốt bằng vàng (3252) của mạch chống can thiệp trái phép cứng (32); và chất kết dính dẫn điện (34) được bố trí trong hốc thứ hai (326) để tạo ra mối nối điện của các chốt bằng vàng (3252) trên bảng mạch chống can thiệp trái phép cứng (32) và các chốt bằng vàng (3252) trên mạch điều khiển của bảng điều khiển chính.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới bàn phím mã hoá và cụ thể hơn, sáng chế đề cập tới bàn phím mã hoá chống can thiệp trái phép có hệ thống phát hiện và bảo vệ chống can thiệp trái phép theo hướng nhiều hướng.

Tình trạng kỹ thuật của sáng chế

Bàn phím mã hoá cứng của thiết bị tự phục vụ của ngân hàng tiếp nhận các thao tác nhập vào và mã hoá mật khẩu ngân hàng của chủ tài khoản, và do đó một khoá làm việc và một khoá chủ của ngân hàng được lưu trữ trong phần lõi xử lý của bàn phím. Nhằm mục đích xấu, một số tội phạm thường dùng các thanh nạy hoặc can thiệp vào bàn phím để lấy trộm mật khẩu và thậm chí là giải mã khoá làm việc và khoá chủ của ngân hàng để lấy trộm thông tin ngân hàng, điều này trực tiếp đe dọa an toàn của thông tin và tiền bạc của chủ tài khoản và ngân hàng.

Nói chung, bàn phím mã hoá có cơ cấu phát hiện và bảo vệ chống can thiệp trái phép, và mạch phát hiện và bảo vệ chống can thiệp trái phép. Khi bàn phím bị tác động bởi can thiệp vật lý trái phép, mạch phát hiện can thiệp trái phép xuất ra một tín hiệu tự hủy để thực hiện chức năng tự hủy của bàn phím mã hoá, nhờ đó ngăn không cho tội phạm lấy trộm thông tin ngân hàng.

Đơn yêu cầu cấp bằng sáng chế Trung Quốc số CN201489599U đề cập tới bàn phím mã hoá và cơ cấu phát hiện và bảo vệ chống can thiệp trái phép của nó. Bàn phím mã hoá này bao gồm vỏ chống nhìn trộm, giá đỡ vỏ chống nhìn trộm, lưới phát hiện và bảo vệ chống can thiệp trái phép, và chất kết dính dẫn điện. Lưới phát hiện và bảo vệ chống can thiệp trái phép được tiếp nhận ở phía trong vỏ chống nhìn trộm, và được kẹp chặt và cố định giữa vỏ chống nhìn trộm và giá đỡ vỏ chống nhìn trộm, và có nhiều chốt bằng vàng thứ nhất trên đó. Bảng mạch điều khiển chính trong bàn phím có mạch bảo vệ chống can thiệp trái phép có nhiều chốt bằng vàng thứ hai trên đó. Các chốt bằng vàng thứ nhất

và các chốt bằng vàng thứ hai được nối điện với nhau nhờ chất kết dính dẫn điện. Giá đỡ vỏ chống nhìn trộm có hốc ở vị trí tương ứng với các chốt bằng vàng thứ nhất, và chất kết dính dẫn điện được nạp đầy vào hốc này.

Lưới phát hiện và bảo vệ chống can thiệp trái phép nói trên là một bảng mạch dễ uốn hai lớp, và các mép chu vi của nó được gấp sao cho lưới phát hiện và bảo vệ chống can thiệp trái phép được tạo thành dạng khối và che bảng mạch điều khiển chính cần được bảo vệ. Do đó, không có khe hở giữa bảng mạch điều khiển chính và phần bên ngoài để đạt được mục đích chống can thiệp trái phép. Một mạch phát hiện chống can thiệp trái phép được bố trí trong bảng mạch dễ uốn và được che nhờ các dây dẫn phát hiện bằng cách sử dụng phương pháp dây dẫn dạng đường rôi. Mạch phát hiện để chống can thiệp trái phép được bố trí trên bề mặt của bảng mạch dễ uốn bằng một chốt bằng vàng, và được nối điện với mạch điều khiển của bảng mạch điều khiển chính để thực hiện chức năng tự hủy thông qua chốt bằng vàng. Khi bảng mạch dễ uốn bị tác động bởi can thiệp vật lý trái phép, tín hiệu tự hủy có thể được xuất ra do việc tạo ra sự ngắn mạch giữa bất kỳ hai dây dẫn liền kề nhau hoặc làm đứt hỏng bất kỳ dây dẫn nào. Do đó, chức năng tự hủy của bàn phím mã hoá được thực hiện, và thông tin nhạy cảm bị xoá bỏ ngay lập tức để ngăn không cho tội phạm lấy trộm thông tin ngân hàng.

Giải pháp kỹ thuật đã biết này có các nhược điểm sau:

Thứ nhất, vì bảng mạch dễ uốn chỉ có thể được tạo ra với hai lớp, trong đó lớp ngoài là lớp tiếp đất không có dây dẫn và lớp trong là lớp dây dẫn dạng đường rôi, và các chốt bằng vàng tại các phần nối giữa bảng mạch dễ uốn và bảng mạch điều khiển chính có chức năng bảo vệ là tương đối dày, tội phạm có thể dễ dàng cào lớp tiếp đất và nối các chốt bằng vàng tại hai đầu của lớp bên trong. Theo cách này, toàn bộ lớp dây dẫn dạng đường rôi bị hỏng chức năng làm ngắn mạch giữa các dây dẫn, và vì thế làm mất khả năng bảo vệ.

Thứ hai, do đặc tính dễ uốn của bảng mạch dễ uốn, tội phạm có thể chỉ ấn chặt các dây nối giữa bảng mạch dễ uốn và bảng mạch bảo vệ, và sau đó lật các phần khác của bảng mạch để làm lộ ra mạch bảo vệ và nhờ đó làm mất khả năng

bảo vệ.

Do vậy, cần phải đề xuất bàn phím mã hoá có hệ thống phát hiện và bảo vệ chống can thiệp trái phép theo nhiều hướng.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất bàn phím mã hoá chống can thiệp trái phép có hệ thống phát hiện và bảo vệ chống can thiệp trái phép theo nhiều hướng để ngăn chặn một cách hữu hiệu các hoạt động can thiệp bất hợp pháp nhằm lấy thông tin mật khẩu từ mặt trước và các mặt bên của bàn phím.

Để đạt được mục đích nêu trên, sáng chế đề xuất các giải pháp kỹ thuật như sau.

Bàn phím mã hoá chống can thiệp trái phép bao gồm tám gỗ phím và bảng điều khiển chính. Bảng điều khiển chính bao gồm mạch điều khiển để thực hiện chức năng tự hủy. Mạch điều khiển này được bao quanh cố định ở phía sau của bảng điều khiển chính nhờ cơ cấu bảo vệ chống can thiệp trái phép. Cơ cấu bảo vệ chống can thiệp trái phép được nối điện với mạch điều khiển. Cơ cấu bảo vệ chống can thiệp trái phép này bao gồm:

vỏ chống nhìn trộm có mặt đáy và thành bên nhô ra thẳng đứng dọc theo các mép chu vi của mặt đáy, hốc thứ nhất được tạo ra nhờ thành bên và mặt đáy;

bảng mạch chống can thiệp trái phép cứng trong đó có bố trí mạch chống can thiệp trái phép, hốc thứ hai bao gồm mặt đáy và thành bên hình khuyên, ít nhất một cặp chốt bằng vàng của mạch chống can thiệp trái phép được bố trí trên mặt đáy của hốc thứ hai, bảng mạch chống can thiệp trái phép cứng được tiếp nhận bên trong hốc thứ nhất; và

chất kết dính dẫn điện được bố trí trong hốc thứ hai để tạo ra mối nối điện giữa các chốt bằng vàng của bảng mạch chống can thiệp trái phép cứng và các chốt bằng vàng của mạch điều khiển của bảng điều khiển chính.

Tốt hơn là, bảng mạch chống can thiệp trái phép cứng là bảng mạch in có ít nhất hai lớp mạch chống can thiệp trái phép.

Hơn nữa, một phía của các chốt bằng vàng ở cách xa bảng điều khiển

chính được che bởi ít nhất một lớp mạch chống can thiệp trái phép.

Tốt hơn là, bảng mạch chống can thiệp trái phép cứng là cấu trúc bảng mạch in bốn lớp trong đó lớp ngoài cùng là lớp tiếp đất và ba lớp còn lại là các lớp bảng mạch in có mạch chống can thiệp trái phép và được xếp chồng trên lớp ngoài cùng. Ba lớp này đều có dây dẫn dạng đường rôi ngoại trừ lớp trung gian qua các lỗ, và các khoảng trống đi dây tương đối rộng của dây dẫn dạng đường rôi của ba lớp của mạch chống can thiệp trái phép được bổ sung và che lẫn nhau.

Tốt hơn là, bảng mạch chống can thiệp trái phép cứng được tạo ra bằng cách lắp ráp năm bảng mạch in, trong đó bốn bảng mạch in được nối đầu với đầu để tạo ra thành bên hình khuyên. Thành bên hình khuyên này được nối điện với một bề mặt của bảng mạch in thứ năm, và mạch chống can thiệp trái phép hoàn chỉnh được tạo bởi năm bảng mạch.

Ngoài ra, ít nhất một trong số bốn bảng mạch in của thành bên hình khuyên được nối điện với bề mặt của bảng mạch in thứ năm.

Tốt hơn là, hai bảng mạch liền kề trong số năm bảng mạch in được nối điện bởi ít nhất hai mối nối hàn.

Tốt hơn là, giá chia bố trí chất kết dính dẫn điện được bố trí giữa bảng mạch chống can thiệp trái phép cứng và bảng điều khiển chính, và các lỗ xuyên để chứa chất kết dính dẫn điện được tạo ra ở giá chia bố trí chất kết dính dẫn điện ở các vị trí tương ứng với các chốt bằng vàng của bảng mạch chống can thiệp trái phép cứng và bảng điều khiển chính.

Tốt hơn là, phương pháp dây dẫn dạng đường rôi được áp dụng cho mạch chống can thiệp trái phép trong bảng mạch.

So sánh với các giải pháp đã biết, giải pháp kỹ thuật theo sáng chế có các ưu điểm sau đây.

Thứ nhất, bảng mạch chống can thiệp trái phép cứng được tạo cấu hình theo thiết kế của bảng mạch cứng có nhiều hơn hai lớp. Các chốt bằng vàng của mạch chống can thiệp trái phép được bố trí trên mặt trong cùng của bảng mạch chống can thiệp trái phép cứng, và phía sau của các dây dẫn tương đối dày trong mỗi lớp mạch được che bởi các dây dẫn của các lớp khác để có thể ngăn một

cách hữu hiệu không cho toàn bộ dây dẫn dạng đường rời bị vô hiệu quả do trạng thái ngắn mạch từ phía sau của mạch chống can thiệp trái phép gây ra bởi tội phạm, và có thể ngăn không cho lớp tiếp đất bị cào để nối các chốt bằng vàng bên trong. Do đó, mức độ khó khăn khi can thiệp trái phép được tăng lên đáng kể và sự an toàn của cơ cấu bảo vệ chống can thiệp trái phép được cải thiện.

Hơn nữa, vì vỏ bảo vệ chống can thiệp trái phép được tạo ra bằng cách lắp ráp các vật liệu cứng, vỏ bảo vệ chống can thiệp trái phép không thể bị uốn cong, và thậm chí khi bị uốn cong do lực mạnh, các mạch bên trong của nó sẽ bị phá hỏng. Do đó, có thể ngăn sự can thiệp bằng cách lật và nhờ đó làm tăng sự an toàn cho cơ cấu bảo vệ chống can thiệp trái phép.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ phối cảnh các chi tiết rời thể hiện bản phím mã hoá chống can thiệp trái phép theo sáng chế;

Fig.2 là hình vẽ phối cảnh các chi tiết rời thể hiện kết cấu của bảng mạch chống can thiệp trái phép cứng theo sáng chế;

Fig.3 là hình vẽ phối cảnh các chi tiết rời thể hiện kết cấu của cơ cấu chống can thiệp trái phép của bản phím mã hoá chống can thiệp trái phép theo sáng chế; và

Fig.4 là hình vẽ dạng sơ đồ thể hiện cách bố trí của các mạch trong các lớp khác nhau của cấu trúc bốn lớp của bảng mạch chống can thiệp trái phép cứng theo sáng chế.

Mô tả chi tiết sáng chế

Sau đây, sáng chế sẽ được mô tả chi tiết theo các phương án thực hiện của nó có dựa vào các hình vẽ kèm theo. Hiển nhiên là, các phương án thực hiện được mô tả ở đây chỉ là các phương án thực hiện ưu tiên của sáng chế, và không phải là tất cả các phương án của sáng chế. Cần hiểu rằng, dựa trên các phương án được mô tả của sáng chế, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể tạo ra các thay đổi và cải biến khác nhau mà không nằm ngoài

phạm vi yêu cầu bảo hộ của sáng chế.

Fig.1 là hình vẽ phối cảnh các chi tiết rời thể hiện bàn phím mã hoá chống can thiệp trái phép theo sáng chế. Bàn phím mã hoá chống can thiệp trái phép 100 bao gồm tấm gỗ phím 1 và bảng điều khiển chính 2 có mạch điều khiển để thực hiện chức năng tự hủy. Cơ cấu bảo vệ chống can thiệp trái phép 3 được cố định vào phía sau của bảng điều khiển chính 2 và được nối điện với mạch điều khiển. Cơ cấu bảo vệ chống can thiệp trái phép 3 bao gồm vỏ chống nhìn trộm 31, bảng mạch chống can thiệp trái phép 32 và chất kết dính dẫn điện 34.

Vỏ chống nhìn trộm 31 có mặt đáy và thành bên nhô ra thẳng đứng dọc theo các mép chu vi của mặt đáy, và hốc thứ nhất được tạo ra nhờ thành bên và mặt đáy. Mạch bảo vệ chống can thiệp trái phép được tạo ra ở phía trong của bảng mạch chống can thiệp trái phép cứng 32. Mạch chống can thiệp trái phép được bố trí ở phía trong của bảng mạch chống can thiệp trái phép cứng 32. Hốc thứ hai bao gồm mặt đáy và thành bên hình khuyên. Ít nhất một cặp chốt bằng vàng của mạch chống can thiệp trái phép được bố trí tại mặt đáy của hốc thứ hai. Bảng mạch chống can thiệp trái phép cứng được bố trí trong hốc thứ nhất. Chất kết dính dẫn điện 34 được đưa vào trong hốc thứ hai để tạo ra mối nối điện giữa các chốt bằng vàng của bảng mạch chống can thiệp trái phép cứng và các chốt bằng vàng của mạch điều khiển của bảng điều khiển chính.

Ngoài ra, bàn phím mã hoá chống can thiệp trái phép có thể còn có giá chia bố trí chất kết dính dẫn điện 33 được bố trí giữa bảng mạch chống can thiệp trái phép cứng và bảng điều khiển chính. Các lỗ xuyên để chứa chất kết dính dẫn điện được tạo ra ở giá chia bố trí chất kết dính dẫn điện ở các vị trí tương ứng với các chốt bằng vàng của bảng mạch chống can thiệp trái phép cứng và bảng điều khiển chính.

Fig.2 là hình vẽ phối cảnh các chi tiết rời thể hiện kết cấu của bảng mạch chống can thiệp trái phép cứng theo sáng chế. Bảng mạch chống can thiệp trái phép cứng 32 bao gồm năm bảng mạch in (PCB: Printed Circuit Board) 321, 322, 323, 324 và 325. Các bảng mạch in 321, 322, 323 và 324 được nối đầu với đầu để tạo ra thành bên hình khuyên. Thành bên theo chu vi được nối điện với

mặt 3251 của bảng mạch in thứ năm 325. Các chốt bằng vàng 3252 được bố trí trên mặt 3251. Hai chốt dẫn điện được bố trí trên mỗi bảng mạch in 321, 322, 323 và 324, tương ứng. Tại mỗi chốt dẫn điện, từng bảng mạch in được nối điện với chốt dẫn điện trên bảng mạch in 325 thông qua hai mối nối hàn, nhờ đó năm bảng mạch tạo ra một mạch chống can thiệp trái phép hoàn chỉnh. Dựa trên đặc tính đi dây của mạch chống can thiệp trái phép, bảng mạch chống can thiệp trái phép cứng được tạo thành bằng cách lắp ghép năm bảng mạch, trong đó bốn bảng mạch in có thể được tạo cấu hình dạng thành bên theo chu vi được nối điện theo cách đầu cuối, và thành bên theo chu vi được nối điện với các chốt dẫn điện trên mặt của bảng mạch in thứ năm thông qua ít nhất hai mối nối hàn, nhờ đó mạch chống can thiệp trái phép được tạo thành bằng cách lắp ghép năm bảng mạch. Hiển nhiên là, phụ thuộc vào thiết kế, vẫn còn có nhiều cách thức tạo ra mỗi nối mạch của năm bảng mạch in, miễn là các mạch chống can thiệp trái phép có thể tạo ra một mạch tích hợp.

Bảng mạch chống can thiệp trái phép cứng 32 được tạo ra bằng cách lắp ráp bằng các vật liệu cứng và không thể bị uốn cong, và ngay cả khi bảng mạch chống can thiệp trái phép cứng 32 bị cong do lực mạnh, các mạch phía trong của nó sẽ bị phá hỏng. Do đó, có thể ngăn sự can thiệp bằng cách lật và nhờ đó tăng sự an toàn cho vỏ bảo vệ chống can thiệp trái phép.

Fig.3 là hình vẽ phối cảnh các chi tiết rời thể hiện kết cấu của cơ cấu chống can thiệp trái phép của bàn phím mã hoá chống can thiệp trái phép theo sáng chế. Cơ cấu bảo vệ chống can thiệp trái phép 3 bao gồm vỏ chống nhìn trộm 31. Vỏ chống nhìn trộm 31 có mặt đáy 311 và thành bên 312 nhô ra thẳng đứng dọc theo các mép chu vi của mặt đáy. Hốc thứ nhất 313 được tạo ra nhờ thành bên 312 và mặt đáy 311. Bảng mạch chống can thiệp trái phép cứng 32 được tiếp nhận ở phía trong của hốc thứ nhất 313. Hốc thứ hai 326 được tạo ra bởi mặt đáy của bảng mạch in 325 và thành bên quanh chu vi được tạo ra bằng cách nối bốn bảng mạch in còn lại (321, 322, 323 và 324) theo cách đầu cuối. Một cặp chốt bằng vàng 3252 của mạch chống can thiệp trái phép được bố trí trên mặt đáy của hốc thứ hai 326, nghĩa là mặt phía trong 3251 của bảng mạch

in 325. Các chột bằng vàng 3252 của mạch chống can thiệp trái phép trên bảng mạch chống can thiệp trái phép cứng 32 được nối điện với các chột bằng vàng (không được thể hiện trên hình vẽ) của mạch điều khiển của bảng điều khiển chính 2 nhờ chất kết dính dẫn điện 34. Để đảm bảo độ chính xác và tin cậy ở chỗ tiếp giáp giữa chất kết dính dẫn điện 34 và các chột bằng vàng của bảng mạch chống can thiệp trái phép cứng 32 và của bảng điều khiển chính, giá chia bố trí chất kết dính dẫn điện 33 được bố trí giữa bảng mạch chống can thiệp trái phép cứng 32 và bảng điều khiển chính 2, và các lỗ xuyên 331 để chứa chất kết dính dẫn điện được tạo ra trong giá chia bố trí chất kết dính dẫn điện 33 ở các vị trí tương ứng với các chột bằng vàng của bảng mạch chống can thiệp trái phép cứng 32 và của bảng điều khiển chính 2. Thiết kế của giá chia bố trí chất kết dính dẫn điện đảm bảo rằng chất kết dính dẫn điện không thể bị dịch chuyển hoặc uốn cong giữa bảng mạch chống can thiệp trái phép cứng 32 và bảng điều khiển chính 2, và đảm bảo rằng trạng thái dẫn điện của các mạch giữa bảng mạch chống can thiệp trái phép cứng 32 và bảng điều khiển chính 2 không bị ảnh hưởng tới. Theo một phương án thực hiện của mạch chống can thiệp trái phép của bảng mạch chống can thiệp trái phép cứng 32, giá chia bố trí chất kết dính dẫn điện 33 gần như có dạng hình vuông hoặc “□”, và các lỗ xuyên 331 để chứa chất kết dính dẫn điện 34 được bố trí ở mép ngoài tại phần cạnh giao nhau của giá chia bố trí chất kết dính dẫn điện 33 tương ứng với các chột bằng vàng 3252 của bảng mạch cứng 32.

Fig.4 là hình vẽ dạng sơ đồ thể hiện cách bố trí của các mạch trong các lớp khác nhau của cấu trúc bốn lớp của bảng mạch chống can thiệp trái phép cứng. Bảng mạch chống can thiệp trái phép cứng 32 có thiết kế bảng mạch in bốn lớp, trong đó lớp ngoài cùng là lớp tiếp đất 3a và các lớp trung gian 3b và 3c đều có dây dẫn dạng đường rời ngoại trừ các lỗ xuyên lớp trung gian 3x. Các lỗ xuyên lớp trung gian 3x được bố trí ở bên cạnh các chột bằng vàng 3252. Nhiều mối hàn truyền tín hiệu 3e được bố trí trên mặt trong cùng 3d. Phần phía sau của các chột bằng vàng 3252 được nối với bảng mạch điều khiển chính được che bởi các dây dẫn của các lớp trung gian 3b và/hoặc 3c. Các mối hàn truyền tín hiệu

tương ứng với các mối hàn truyền tín hiệu 3e được tạo ra trên các mặt của bốn bảng mạch khác để tạo ra bảng mạch chống can thiệp trái phép cứng dạng hốc 32. Khi lắp ráp, các mối hàn truyền tín hiệu tương ứng được nối điện nhờ hàn thiếc để tạo ra mạch chống can thiệp trái phép hoàn chỉnh.

Trong thiết kế của bảng mạch cứng có nhiều hơn hai lớp, mặt sau của các dây dẫn tương đối dày của các chốt bằng vàng 3252 của lớp trong cùng 3d được che bởi các dây dẫn của (các) lớp trung gian 3b và/hoặc 3c để có thể ngăn chặn một cách hữu hiệu không cho toàn bộ dây dẫn dạng đường rỗng bị vô hiệu hóa do trạng thái ngắn mạch từ phía sau của mạch chống can thiệp trái phép gây ra bởi tội phạm, và cũng có thể ngăn không cho lớp tiếp đất bị cào để nối các chốt bằng vàng 3252 bên trong. Do đó, mức độ khó khăn khi can thiệp trái phép tăng lên đáng kể và sự an toàn của cơ cấu bảo vệ chống can thiệp trái phép 3 được cải thiện.

Trên đây sáng chế đã được mô tả chi tiết theo các phương án thực hiện ưu tiên của nó. Cần hiểu rằng, dựa trên các phương án được mô tả của sáng chế, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể tạo ra các thay đổi và cải biến khác nhau mà không nằm ngoài phạm vi yêu cầu bảo hộ của sáng chế.

Yêu cầu bảo hộ

1. Bàn phím mã hoá chống can thiệp trái phép bao gồm tám gõ phím và bảng điều khiển chính, trong đó bảng điều khiển chính bao gồm mạch điều khiển để thực hiện chức năng tự hủy, mạch điều khiển này được bao quanh cố định ở phía sau của bảng điều khiển chính nhờ cơ cấu bảo vệ chống can thiệp trái phép, cơ cấu bảo vệ chống can thiệp trái phép này được nối điện với mạch điều khiển, khác biệt ở chỗ, cơ cấu bảo vệ chống can thiệp trái phép bao gồm:

vỏ chống nhìn trộm có mặt đáy và thành bên nhô ra thẳng đứng dọc theo các mép chu vi của mặt đáy, hốc thứ nhất được tạo ra nhờ thành bên và mặt đáy;

bảng mạch chống can thiệp trái phép cứng trong đó có bố trí mạch chống can thiệp trái phép, hốc thứ hai bao gồm mặt đáy và thành bên hình khuyên, ít nhất một cặp chốt bằng vàng của mạch chống can thiệp trái phép được bố trí trên mặt đáy của hốc thứ hai, bảng mạch chống can thiệp trái phép cứng được tiếp nhận bên trong hốc thứ nhất; và

chất kết dính dẫn điện được bố trí trong hốc thứ hai để tạo ra mối nối điện giữa các chốt bằng vàng của bảng mạch chống can thiệp trái phép cứng và các chốt bằng vàng của mạch điều khiển của bảng điều khiển chính.

2. Bàn phím mã hoá chống can thiệp trái phép theo điểm 1, trong đó bảng mạch chống can thiệp trái phép cứng là bảng mạch in có ít nhất hai lớp mạch chống can thiệp trái phép.

3. Bàn phím mã hoá chống can thiệp trái phép theo điểm 2, trong đó một phía của các chốt bằng vàng ở cách xa bảng điều khiển chính được che bởi ít nhất một lớp mạch chống can thiệp trái phép.

4. Bàn phím mã hoá chống can thiệp trái phép theo điểm 1, trong đó bảng mạch chống can thiệp trái phép cứng là cấu trúc bảng mạch in bốn lớp trong đó lớp ngoài cùng là lớp tiếp đất và ba lớp còn lại là các lớp bảng mạch in có mạch chống can thiệp trái phép và được xếp chồng trên lớp ngoài cùng, ba lớp này đều có dây dẫn dạng đường rôi ngoại trừ lớp trung gian qua các lỗ, và các khoảng trống đi dây tương đối rộng của dây dẫn dạng đường rôi của ba lớp của mạch chống can thiệp trái phép được bổ sung và che lẫn nhau.

5. Bàn phím mã hoá chống can thiệp trái phép theo điểm 1, trong đó bảng mạch chống can thiệp trái phép cứng được tạo ra bằng cách lắp ráp năm bảng mạch in, trong đó bốn bảng mạch in được nối đầu với đầu để tạo ra thành bên hình khuyên, thành bên hình khuyên này được nối điện với một bề mặt của bảng mạch in thứ năm, và mạch chống can thiệp trái phép hoàn chỉnh được tạo bởi năm bảng mạch.
6. Bàn phím mã hoá chống can thiệp trái phép theo điểm 5, trong đó ít nhất một trong số bốn bảng mạch in của thành bên hình khuyên được nối điện với bề mặt của bảng mạch in thứ năm.
7. Bàn phím mã hoá chống can thiệp trái phép theo điểm 5, trong đó hai bảng mạch liền kề trong số năm bảng mạch in được nối điện bởi ít nhất hai mối nối hàn.
8. Bàn phím mã hoá chống can thiệp trái phép theo điểm 1, trong đó giá chia bố trí chất kết dính dẫn điện được bố trí giữa bảng mạch chống can thiệp trái phép cứng và bảng điều khiển chính, và các lỗ xuyên để chứa chất kết dính dẫn điện được tạo ra ở giá chia bố trí chất kết dính dẫn điện ở các vị trí tương ứng với các chốt bằng vàng của bảng mạch chống can thiệp trái phép cứng và bảng điều khiển chính.
9. Bàn phím mã hoá chống can thiệp trái phép theo 1, trong đó dây dẫn dạng đường rỗng được áp dụng cho mạch chống can thiệp trái phép trong bảng mạch.

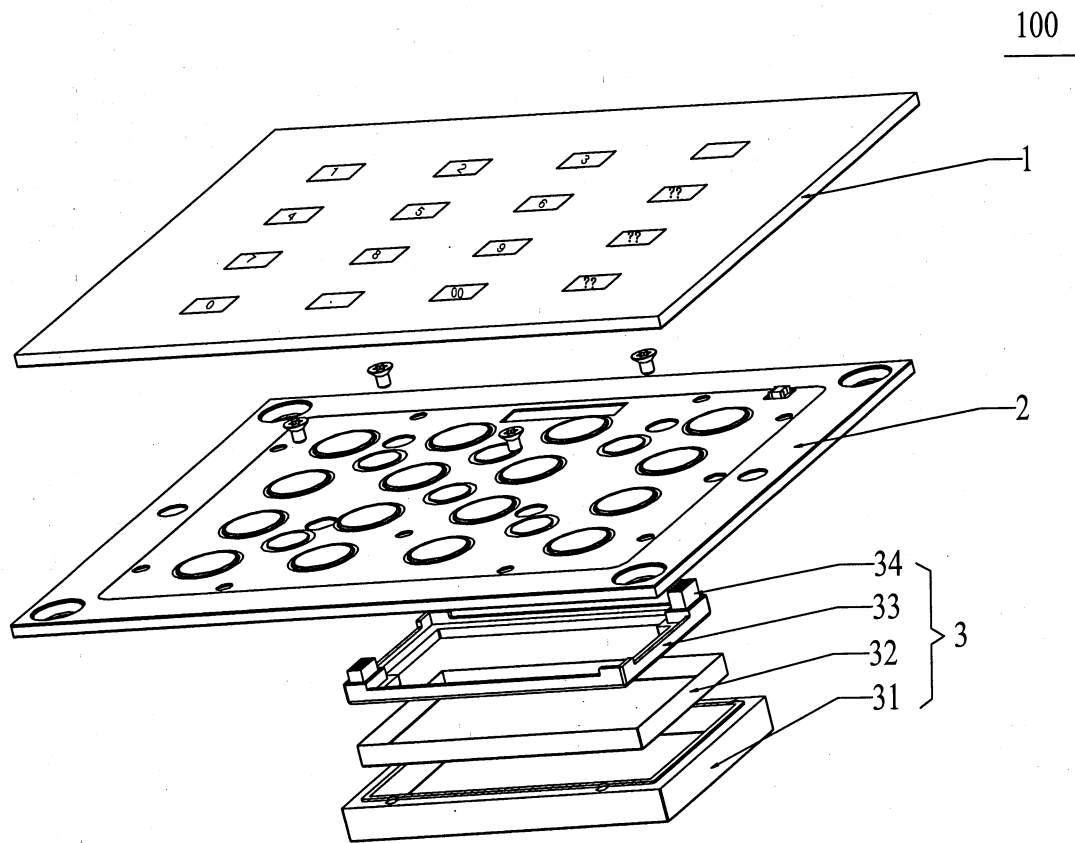


Fig.1

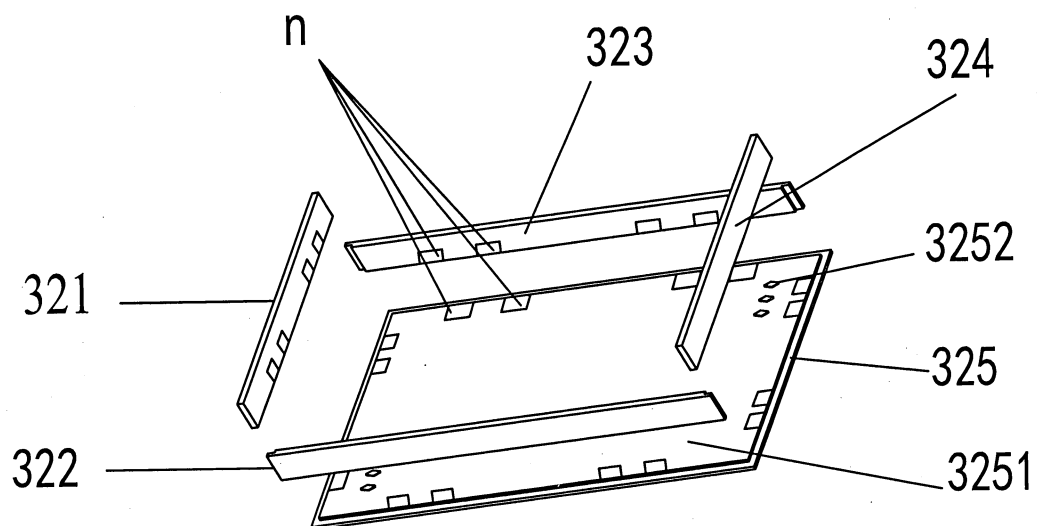


Fig.2

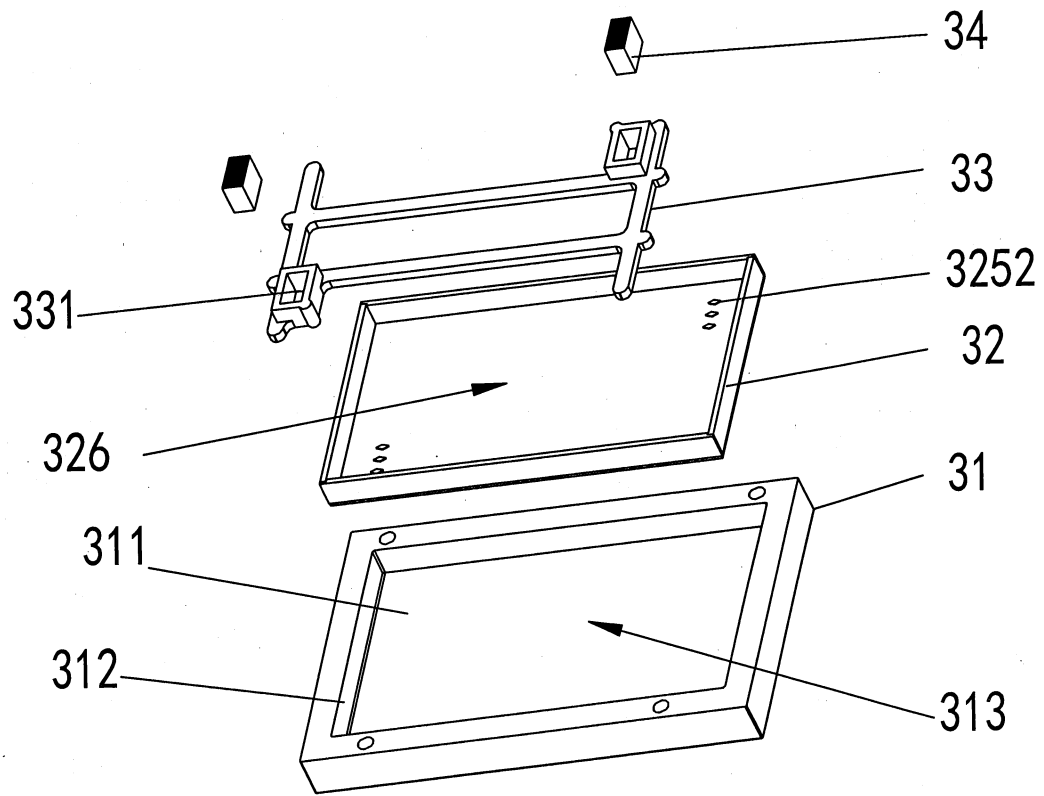


FIG. 3

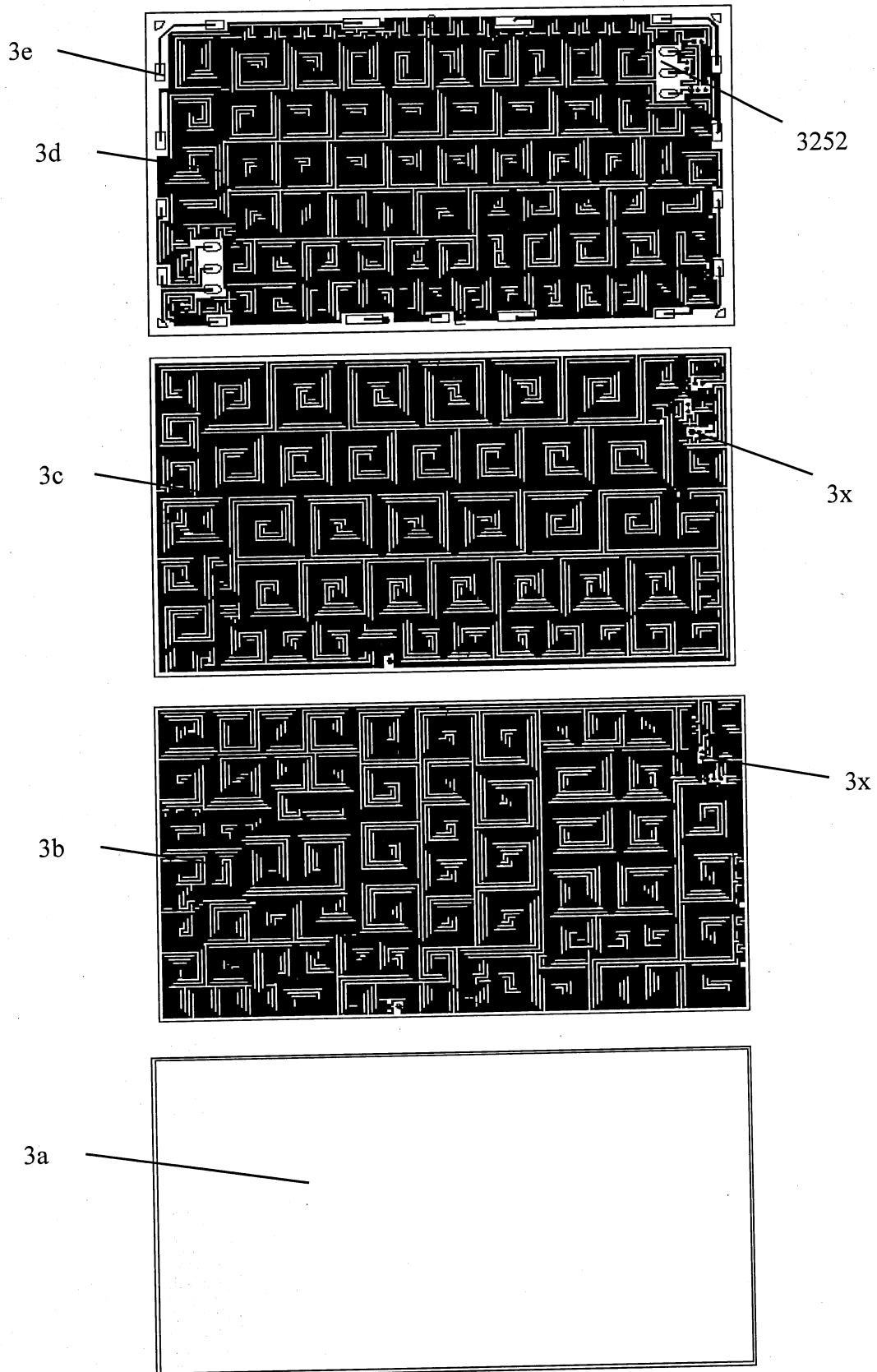


FIG. 4