TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: Một số hệ mã hóa với quyền giải mã linh động

Chuyên ngành: Hệ thống thông rin

Mã số:9.48.01.04

Họ và tên NCS: Trịnh Văn Anh

Người hướng dẫn khoa học:

1. GS.TS Nguyễn Bình
2. TS. Hồ Văn Hương.

Cơ sở đào tạo: Học viện Công nghệ Bưu chính Viễn thông

I. NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN

1. Đề xuất một hệ mã hóa quảng bá đa kênh (MCBE) dựa trên hệ Delerablee [25] có độ hiệu quả và an toàn tương tự như hệ [47, 15] nhưng ở dạng mã hóa công khai, ai cũng có thể thực hiện mã hóa được, không còn ở dạng bí mật (mình trung tâm với khóa bí mật mới có thể thực hiện mã hóa).
2. Đề xuất một hệ mã hóa dựa trên thuộc tính có chính sách ở bản mã (CP-ABE) mới có độ dài bản mã là hằng số, nhưng có khóa bí mật ngắn hơn các hệ mã CP-ABE có cùng tính chất là có độ dài bản mã là hằng số. Điểm yếu của hệ đề xuất so với các hệ mã này là có mức độ an toàn yếu hơn.
3. Luận án dựa trên hệ CP-ABE hiện có [42], xây dựng một hệ CP-ABE mới hỗ trợ tìm kiếm trên dữ liệu đã được mã hóa và người dùng tự tạo ra được cửa sập cho mình mà không cần nhờ đến bên thứ ba.

II. VẤN ĐỀ TIẾP TỤC NGHIÊN CỨU

1. Xây dựng hệ MCBE có độ dài khóa bí mật ngắn hơn các hệ hiện có mà vẫn giữ được độ dài bản mã là hằng số;
2. Xây dựng hệ phi tập trung hóa MCBE, hiện nay vẫn chưa tồn tại hệ phi tập trung hóa MCBE nào;
3. Xây dựng hệ CP-ABE có tính chất là cả đội dài bản mã và độ dài khóa bí mật đều là hằng số. Lưu ý rằng các hệ mã hóa quảng bá đã có tính chất này nên tồn tại hệ CP-ABE như vậy là khả thi.

Xác nhận của người hướng dẫn khoa học **Nghiên cứu sinh**

GS.TS Nguyễn Bình **TS. Hồ Văn Hương** **Trịnh Văn Anh**

BẢN TRÍCH YẾU LUẬN ÁN TIẾN SĨ

Tên tác giả luận án: Trịnh Văn Anh

Tên luận án: Một số hệ mã hóa với quyền giải mã linh động

Ngành học: Hệ thống thông tin

Mã số: 9.48.01.04

Tên đơn vị đào tạo: Học viện Công nghệ Bưu chính Viễn thông

I. Mục đích và đối tượng nghiên cứu của luận án

Đề tài tập trung nghiên cứu các hệ mã hóa quảng bá, các hệ mã hóa quảng bá đa kênh và các hệ mã hóa dựa trên thuộc tính, nhằm đạt được các mục tiêu chính sau đây:
1. Nắm bắt được tổng quan tình hình nghiên cứu hiện nay của các hệ mã hóa quảng bá, các hệ mã hóa quảng bá đa kênh và các hệ mã hóa dựa trên thuộc tính;
2. Xây dựng được hệ mã hóa quảng bá đa kênh mới khắc phục được các điểm yếu của các hệ Multi-channel BE hiện có như tốc độ giải mã chậm và chỉ authority mới có khả năng mã hóa (ở dạng mã hóa khóa bí mật);

3. Xây dựng được các hệ ABE mới có các tính chất như độ dài bản mã ngắn (là hằng số không phụ thuộc vào số thuộc tính), độ dài khóa bí mật và tốc độ giải mã ở mức chấp nhận được, hỗ trợ chức năng tìm kiếm trên dữ liệu đã được mã hóa.

II. Các phương pháp nghiên cứu đã sử dụng

1. Tìm hiểu một số kỹ thuật hiện có để xây dựng các hệ mã hóa quảng bá, hệ mã hóa quảng bá đa kênh hiệu quả;
2. Nghiên cứu việc xây dựng hệ mã hóa quảng bá đa kênh mới dựa trên các kỹ thuật xây dựng các hệ mã hóa quảng bá hiện có, đặc biệt là từ hệ mã hóa quảng bá Delerablee [25] và các cải tiến của nó [55, 56];
3. Tìm hiểu tất cả các kỹ thuật hiện có để xây dựng các hệ mã hóa dựa trên thuộc tính hiệu quả;
4. Nghiên cứu việc xây dựng hệ mã hóa dựa trên thuộc tính mới dựa trên các kỹ thuật xây dựng các hệ mã hóa quảng bá và các hệ mã hóa quảng bá đa kênh hiện có, đặc biệt tập trung vào việc xây dựng các hệ mã hóa dựa trên thuộc tính có tính chất là độ dài bản mã là hằng số và tìm kiếm trên dữ liệu đã được mã hóa;

5. Nghiên cứu sự an toàn của một số hệ mã hóa dựa trên thuộc tính hiện có.

III. Các kết quả chính và kết luận

Các kết quả chính của luận án:

1. Đóng góp thứ nhất: Đề xuất một lược đồ mã hóa quảng bá đa kênh dựa trên hệ Delerablee [25] có độ hiệu quả và an toàn tương tự như hệ [47, 15] nhưng ở dạng mã hóa công khai, không còn ở dạng bí mật. Được công bố tại công trình số 4.
2. Đóng góp thứ hai: Đề xuất lược đồ CP-ABE mới, có khóa bí mật ngắn hơn các hệ CP-ABE khác. Các hệ khác có cùng tính chất, độ dài bản mã là hằng số. Điểm yếu của đề xuất so với các hệ mã này là, có mức độ an toàn yếu hơn các hệ khác cso cùng tính chất. Nội dung đề xuất được công bố tại công trình số 4.
3. Đóng góp thứ 3: Đề xuất mới, dựa trên hệ ABE hiện có [42], xây dựng một lược đồ ABE mới hỗ trợ tìm kiếm trên dữ liệu đã được mã hóa; được công bố tại công trình số 2.

Kết luận:

Các hệ mã hóa với quyền giải mã linh động như mã hóa quảng bá, hệ mã hóa quảng bá đa kênh hay mã hóa dựa trên thuộc tính đang được sử dụng rộng rãi trong thực tế hiện nay, đặc biệt trong các ứng dụng như truyền hình trả tiền, chia sẽ files, social network (facebooks, twitter,...), lưu trữ an toàn dữ liệu trên đám mây cho mọi loại ứng dụng như e-Health, chính phủ điện tử, ... Tuy nhiên vẫn còn nhiều vấn đề mở đối với ba loại hệ mã hóa này mà các nhà nghiên cứu hiện nay vẫn chưa giải quyết được. Và những đóng góp trong luận án của Nghiên cứu sinh góp thêm phần nghiên cứu về lĩnh vực này hiện nay.

Xác nhận của người hướng dẫn khoa học **Nghiên cứu sinh**

GS.TS Nguyễn Bình **TS. Hồ Văn Hương** **Trịnh Văn Anh**