**Mẫu số 01**

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**Độc lập - Tự do - Hạnh phúc**

---

**BẢN ĐĂNG KÝ XÉT CÔNG NHẬN ĐẠT TIÊU CHUẨN**

**CHỨC DANH: GIÁO SƯ**

**Mã hồ sơ:.....**

(Nội dung đúng ở ô nào thì đánh dấu vào ô đó: ☑; Nội dung không đúng thì để trống: ☐ )

Đối tượng đăng ký: Giảng viên ☐; Giảng viên thỉnh giảng ☑

Ngành: Công nghệ Thông tin; Chuyên ngành: Truyền thông và Mạng máy tính

## A. THÔNG TIN CÁ NHÂN

1. Họ và tên người đăng ký: Nguyễn Hiếu Minh

2. Ngày tháng năm sinh: 07/11/1971; Nam ☑; Nữ ☐; Quốc tịch: Việt Nam;

Dân tộc: Kinh; Tôn giáo: Không

3. Đảng viên Đảng Cộng sản Việt Nam: ☑

4. Quê quán: xã/phường, huyện/quận, tỉnh/thành phố: Nam Sơn, Sóc Sơn, Hà Nội.

5. Nơi đăng ký hộ khẩu thường trú (số nhà, phố, phường, quận, thành phố hoặc xã, huyện, tỉnh): số 48 Khu Tập thể Binh chủng Thông tin liên lạc, ngõ 117/10 Trần Cung, Cổ Nhuế 1, Bắc Từ Liêm, Hà Nội.

6. Địa chỉ liên hệ (ghi rõ, đầy đủ để liên hệ được qua Bưu điện): số 48 Khu Tập thể Binh chủng Thông tin liên lạc, ngõ 117/10 Trần Cung, Cổ Nhuế 1, Bắc Từ Liêm, Hà Nội.

Điện thoại nhà riêng: ; Điện thoại di động: 0989193571;

E-mail: hieuminhmta@gmail.com

7. Quá trình công tác (công việc, chức vụ, cơ quan):

Từ tháng, năm 09,1993 đến tháng, năm 08,1997: Cán bộ tại Ban máy tính, Phòng Đào tạo, Học viện Kỹ thuật Quân sự

Từ tháng, năm 09,1997 đến tháng, năm 12,1999: Học viên thạc sỹ tại Phòng Sau đại học, Học viện Kỹ thuật Quân sự

Từ tháng, năm 01,2000 đến tháng, năm 11,2002: Giáo viên tại Bộ môn Thông tin, Khoa Vô tuyến Điện tử, Học viện Kỹ thuật Quân sự

Từ tháng, năm 11,2002 đến tháng, năm 06,2006: Nghiên cứu sinh tại Khoa Công nghệ Thông tin, Trường Đại học Tổng hợp điện Quốc gia Xanh Pê Téc Bua (Saint Petersburg Electrotechnical University "LETI")

Từ tháng, năm 10,2006 đến tháng, năm 06,2016: Chủ nhiệm bộ môn tại Bộ môn An ninh mạng/ Công nghệ

mạng, Khoa Công nghệ Thông tin, Học viện Kỹ thuật Quân sự

Từ tháng, năm 06,2016 đến tháng, năm 07,2019: Chủ nhiệm khoa tại Khoa Điện tử Viễn thông, Học viện Kỹ thuật Mật mã, Ban Cơ yếu Chính phủ

Chức vụ hiện nay: Phó Viện trưởng; Chức vụ cao nhất đã qua: Phó Viện trưởng

Cơ quan công tác hiện nay: Viện Khoa học-Công nghệ mật mã, Ban Cơ yếu Chính phủ

Địa chỉ cơ quan: 21 Trúc Khê, Đống Đa, Thành phố Hà Nội

Điện thoại cơ quan:

Thỉnh giảng tại cơ sở giáo dục đại học (nếu có): Học viện Kỹ thuật mật mã

8. Đã nghỉ hưu từ tháng ... năm ...

Nơi làm việc sau khi nghỉ hưu (nếu có):

Tên cơ sở giáo dục đại học nơi hợp đồng thỉnh giảng 3 năm cuối (tính đến thời điểm hết hạn nộp hồ sơ): Học viện Kỹ thuật mật mã

9. Trình độ đào tạo:

- Được cấp bằng ĐH [3] ngày 06 tháng 08 năm 1993, số văn bằng: 47687, ngành: Vô tuyến điện, chuyên ngành: Thông tin; Nơi cấp bằng ĐH [3] (trường, nước): Học viện Kỹ thuật Quân sự, Việt Nam
- Được cấp bằng ThS [4] ngày 23 tháng 08 năm 2000, số văn bằng: 16648, ngành: Vô tuyến điện, chuyên ngành: Thông tin; Nơi cấp bằng ThS [4] (trường, nước): Học viện Kỹ thuật Quân sự, Việt Nam
- Được cấp bằng TS [5] ngày 23 tháng 06 năm 2006, số văn bằng: 004739, ngành: Công nghệ thông tin, chuyên ngành: Phân tích hệ thống, điều khiển và xử lý thông tin (05.13.01: System analysis, control and information processing); Nơi cấp bằng TS [5] (trường, nước): Đại học Tổng hợp kỹ thuật điện Quốc gia Xanh Pê Téc Bua, Liên bang Nga

10. Đã được bổ nhiệm/công nhận chức danh PGS ngày 09 tháng 11 năm 2010, ngành: Công nghệ thông tin

11. Đăng ký xét đạt tiêu chuẩn chức danh Giáo sư tại HĐGS cơ sở: Học viện Công nghệ Bưu chính Viễn thông

12. Đăng ký xét đạt tiêu chuẩn chức danh Giáo sư tại HĐGS ngành, liên ngành: Công nghệ thông tin

13. Các hướng nghiên cứu chủ yếu:

**Các hướng nghiên cứu chủ yếu được phân nhóm theo thứ tự ưu tiên như sau**:

(1). Nghiên cứu, phát triển các thuật toán mật mã (cryptographic algorithms): nghiên cứu, phát triển cơ sở toán học (một số bài toán khó mới trong mật mã (new hard problems)), các nguyên thủy mật mã (cryptographic primitives) và các thuật toán mật mã (cryptographic algorithms).

(2). Nghiên cứu, phát triển giải pháp an toàn thông tin (information security): dựa trên các kỹ thuật mật mã (nghiên cứu về bảo mật cơ sở dữ liệu (database security) hỗ trợ truy vấn trên dữ liệu mã hóa (executing query on encrypted database)); dựa trên các thuật toán học máy (nghiên cứu về phát hiện tấn công mạng (network attack detection using machine learning), tấn công kênh kề lên các thuật toán mật mã (side channel attacks) và phân tích các tấn công qua giao thức http (http attack detection)); một số giải pháp giấu tin bí mật (nghiên cứu về kỹ thuật giấu tin (steganography)).

(3). Nghiên cứu, phát triển giải pháp cơ sở dữ liệu lưu trữ khóa-giá trị hiệu năng cao cho các dịch vụ lưu trữ lớn

(high-performance key-value store for large-scale storage service).

**Hướng nghiên cứu xuyên suốt**: Phát triển các thuật toán mật mã. Đây là hướng nghiên cứu thuộc lĩnh vực khoa học mật mã (cryptography), nó đã được ứng viên xác lập và theo đuổi từ khi làm nghiên cứu sinh tiến sĩ tại trường Đại học Tổng hợp kỹ thuật điện Quốc gia Xanh Pê Téc Bua, Liên bang Nga.

*Hướng nghiên cứu số (1) được phân nhánh như sau*:

+ Phát triển các thuật toán mật mã khối hiệu năng cao (high performance block ciphers): Tìm kiếm và xây dựng các nguyên thủy mật mã và các thuật toán mật mã khối mới hiệu năng cao khi tích hợp trên ASIC và FPGA.

+ Phát triển một số lược đồ chữ ký số (digital signature schemes), chữ ký số tập thể (multi-signature schemes), chữ ký số mù (blind signature, multi-blind signature schemes), chữ ký số nhóm (group signature schemes): Phát triển các lược đồ chữ ký số có tính chất đặc biệt để ứng dụng trong thực tiễn.

+ Phát triển các giao thức phân phối khóa (key exchange protocols), hệ mật khóa công khai (public key cryptography): Cải tiến và phát triển giao thức trao đổi khóa và các hệ mật khóa công khai có độ an toàn và hiệu quả dựa trên các bài toán khó phổ biến.

+ Phát triển một số giao thức mã hóa có thể chối từ (deniable encryption protocols): Cho phép xây dựng các giao thức mật mã có khả năng chống lại các tấn công cưỡng ép chủ động (active attacks) (các thuật toán mật mã truyền thống chỉ có khả năng chống lại các tấn công thụ động (passive attacks)).

+ Phát triển một số cấu trúc đại số không giao hoán (non-commutative associative algebras) và bài toán logarit rời rạc ẩn trên (hidden discrete logarithm problem over non-commutative associative algebras): Đây là một hướng nghiên cứu mới và nó được chứng minh có thể được sử dụng để xây dựng các hệ mật kháng lượng tử (quantum resistant cryptography). Các kết quả của hướng nghiên cứu này tạo ra một cơ sở toán học mới để phát triển các thuật toán mật mã hậu lượng tử.

*Hướng nghiên cứu số (2) được phân nhánh như sau*:

+ Nghiên cứu sử dụng học máy phát hiện tấn công mạng: Sử dụng các thuật toán học máy để phát triển các giải pháp phát hiện xâm nhập; Thực hiện tấn công kênh kề lên các thuật toán mật mã; Phân tích các tấn công qua giao thức http.

+ Phát triển các giải pháp bảo mật cơ sở dữ liệu: Phát triển các mô hình, thuật toán thực hiện bảo mật cơ sở dữ liệu thuê ngoài (outsourcing database) với khả năng thực hiện truy vấn trên dữ liệu mã hóa.

+ Phát triển một số giải pháp giấu tin và một số giải pháp đảm bảo an toàn mạng máy tính.

*Hướng nghiên cứu số (3)*:

+ Nghiên cứu, phát triển hệ thống lưu trữ dữ liệu hiệu năng cao: Thực hiện phát triển giải pháp lưu trữ khóa-giá trị hiệu năng cao cho các hệ thống lưu trữ dữ liệu lớn.

14. Kết quả đào tạo và nghiên cứu khoa học:

- Đã hướng dẫn (số lượng) 7 NCS bảo vệ thành công luận án TS;
- Đã hướng dẫn (số lượng) ... HVCH/CK2/BSNT bảo vệ thành công luận văn ThS/CK2/BSNT (ứng viên chức danh GS không cần kê khai nội dung này);
- Đã hoàn thành đề tài NCKH từ cấp cơ sở trở lên: 2 cấp Bộ; 2 cấp Cơ sở;
- Đã công bố (số lượng) 95 bài báo khoa học, trong đó 16 bài báo khoa học trên tạp chí quốc tế có uy tín;
- Đã được cấp (số lượng) 2 bằng độc quyền sáng chế, giải pháp hữu ích;
- Số lượng sách đã xuất bản 7, trong đó 7 thuộc nhà xuất bản có uy tín;
- Số lượng tác phẩm nghệ thuật, thành tích huấn luyện, thi đấu thể dục, thể thao đạt giải thưởng quốc gia, quốc tế: 0

15. Khen thưởng (các huân chương, huy chương, danh hiệu):

| TT | Tên khen thưởng | Cấp khen thưởng | Năm khen thưởng |
|---|---|---|---|
| 1 | Bằng khen | Bộ Quốc phòng | 2010 |
| 2 | Bằng khen | Học viện Kỹ thuật Quân sự | 2008, 2012, 201 |
| 3 | Chiến sĩ thi đua cơ sở | Học viện Kỹ thuật Quân sự | 1996, 2012, 201 |
| 4 | Giáo viên dạy giỏi | Học viện Kỹ thuật Quân sự | 2008, 2015 |
| 5 | Huy chương quân kỳ quyết thắng | Nhà nước | 2019 |
| 6 | Kỷ niệm chương bảo vệ an ninh tổ quốc | Bộ Công an | 2022 |

16. Kỷ luật (hình thức từ khiển trách trở lên, cấp ra quyết định, số quyết định và thời hạn hiệu lực của quyết định):

| TT | Tên kỷ luật | Cấp ra quyết định | Số quyết định | Thời hạn hiệu lực |
|---|---|---|---|---|
| Không có | | | | |

## B. TỰ KHAI THEO TIÊU CHUẨN CHỨC DANH GIÁO SƯ/PHÓ GIÁO SƯ

1. Tự đánh giá về tiêu chuẩn và nhiệm vụ của nhà giáo:

Là một nhà giáo quân đội thuộc biên chế Học viện Kỹ thuật Quân sự từ năm 9/1993 đến 6/2016, Học viện Kỹ thuật mật mã từ năm 16/6/2016 đến 8/2019 và giáo viên thỉnh giảng từ 8/2019 đến nay tôi tự nhận thấy mình luôn đáp ứng đầy đủ các tiêu chuẩn của một nhà giáo. Cụ thể:

- ***Về mặt phẩm chất, đạo đức nhà giáo***: bản thân có phẩm chất đạo đức tư tưởng tốt, lý lịch rõ ràng, là đảng viên Đảng Cộng sản Việt Nam từ năm 1993. Trong cuộc sống hàng ngày tôi luôn gương mẫu chấp hành tốt các chủ trương chính sách của Đảng, pháp luật Nhà nước và Điều lệ, quy định của đơn vị và Quân đội, thực hiện tốt các nghĩa vụ công dân.

- ***Về năng lực chuyên môn***: mặc dù bản thân đã được đào tạo cơ bản và đạt trình độ chuẩn về chuyên môn, tôi vẫn không ngừng học tập và nghiên cứu để nâng cao hơn nữa trình độ chuyên môn. Trong giảng dạy, tôi luôn giữ gìn phẩm chất, uy tín, danh dự của nhà giáo, tôn trọng nhân cách của người học, đối xử công bằng với người học, bảo
vệ các quyền, lợi ích chính đáng của người học. Bản thân tôi luôn nghiên cứu để xây dựng bài giảng có tính khoa học kết hợp với thực tiễn, sử dụng các phương tiện giảng dạy hiện đại làm cho bài giảng thêm phong phú, cố gắng để truyền tải đến người học lượng kiến thức cập nhật, phong phú và đầy đủ nhất.

Trong thời gian làm giảng viên đến nay bản thân đã vinh dự được đồng nghiệp và đơn vị tín nhiệm bầu chọn 03 lần cho danh hiệu "Chiến sỹ thi đua", 03 lần cho danh hiệu "Giáo viên Dạy giỏi" của Học viện Kỹ thuật Quân sự.

2. Thời gian, kết quả tham gia đào tạo, bồi dưỡng từ trình độ đại học trở lên:
- Tổng số năm thực hiện nhiệm vụ đào tạo: 22 năm 0 tháng
- Khai cụ thể ít nhất 06 năm học, trong đó có 03 năm học cuối liên tục tính đến ngày hết hạn nộp hồ sơ (ứng viên GS chỉ khai 3 năm cuối liên tục sau khi được công nhận PGS):

| TT | Năm học | Số lượng NCS đã hướng dẫn | | Số lượng ThS/CK2/BSNT đã hướng dẫn | Số đồ án, khóa luận tốt nghiệp ĐH đã HD | Số giờ chuẩn gd trực tiếp trên lớp | | Tổng số giờ chuẩn gd trực tiếp trên lớp/số giờ chuẩn gd quy đổi/số giờ chuẩn định mức (*) |
|---|---|---|---|---|---|---|---|---|
| | | **Chính** | **Phụ** | | | **ĐH** | **SĐH** | |
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 03 năm học cuối | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4 | 2019 - 2020 | 4 | | 3 | | | 45 | 45/238/81 |
| 5 | 2020 - 2021 | 2 | | 3 | | 60 | 105 | 165/393/81 |
| 6 | 2021 - 2022 | 2 | | 3 | | 32 | 75 | 107/306/81 |

***(*) - Trước ngày 25/3/2015, theo Quy định chế độ làm việc đối với giảng viên ban hành kèm theo Quyết định số 64/2008/QĐ-BGDĐT ngày 28/11/2008, được sửa đổi bổ sung bởi Thông tư số 36/2010/TT-BGDĐT ngày 15/12/2010 và Thông tư số 18/2012/TT-BGDĐT ngày 31/5/2012 của Bộ trưởng Bộ GD&ĐT.***

***- Từ 25/3/2015 đến nay, theo Quy định chế độ làm việc đối với giảng viên ban hành kèm theo Thông tư số 47/2014/TT-BGDĐT ngày 31/12/2014 của Bộ trưởng Bộ GD&ĐT.***

***- Từ ngày 11/9/2020 đến nay, theo Quy định chế độ làm việc của giảng viên cơ sở giáo dục đại học ban hành kèm theo Thông tư số 20/2020/TT-BGDĐT ngày 27/7/2020 của Bộ trưởng Bộ GD&ĐT; định mức giờ chuẩn giảng dạy theo quy định của thủ trưởng cơ sở giáo dục đại học, trong đó định mức của giảng viên thỉnh giảng được tính trên cơ sở định mức của giảng viên cơ hữu.***

3. Ngoại ngữ

3.1. Ngoại ngữ thành thạo phục vụ chuyên môn: Nga D, Anh C

a) Được đào tạo ở nước ngoài ☑:

- Học ĐH ☐; Tại nước: ; Từ năm đến năm

- Bảo vệ luận văn ThS ☐ hoặc luận án TS ☑ hoặc TSKH ☐; Tại nước: Liên bang Nga năm 2006

b) Được đào tạo ngoại ngữ trong nước ☐:

- Trường ĐH cấp bằng tốt nghiệp ĐH ngoại ngữ: số bằng: ; năm cấp:

c) Giảng dạy bằng tiếng nước ngoài ☐:

- Giảng dạy bằng ngoại ngữ:

- Nơi giảng dạy (cơ sở đào tạo, nước):

d) Đối tượng khác ☐; Diễn giải:

3.2. Tiếng Anh (văn bằng, chứng chỉ):

4. Hướng dẫn NCS, HVCH/CK2/BSNT đã được cấp bằng/có quyết định cấp bằng

| TT | Họ tên NCS hoặc HVCH/ CK2/ BSNT | Đối tượng | | Trách nhiệm hướng dẫn | | Thời gian hướng dẫn từ ... đến ... | Cơ sở đào tạo | Ngày, tháng, năm được cấp bằng/có quyết định cấp bằng |
|---|---|---|---|---|---|---|---|---|
| | | NCS | HVCH/ CK2/ BSNT | Chính | Phụ | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | Đỗ Thị Bắc | X | | X | | 01/2010 đến 09/2014 | Học viện Kỹ thuật Quân sự | 12/05/2015 |
| 2 | Nguyễn Trung Thành | X | | X | | 05/2012 đến 05/2016 | Học viện Kỹ thuật Quân sự | 31/03/2017 |
| 3 | Đặng Minh Tuấn | X | | | X | 09/2011 đến 09/2016 | Viện Khoa học Công nghệ Quân sự | 14/11/2017 |
| 4 | Đào Tuấn Hùng | X | | X | | 09/2012 đến 09/2016 | Viện Khoa học Công nghệ Quân sự | 9/11/2018 |
| 5 | Đỗ Việt Bình | X | | X | | 09/2012 đến 09/2016 | Viện Khoa học Công nghệ Quân sự | 01/02/2019 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 6 | Hồ Kim Giàu | X | | X | | 10/2016 đến 10/2019 | Học viện Kỹ thuật Quân sự | 21/04/2022 |
| 7 | Nguyễn Tấn Đức | X | | X | | 03/2016 đến 03/2020 | Học viện Công nghệ Bưu chính Viễn thông | 19/05/2021 |

*Ghi chú:* Ứng viên chức danh GS chỉ kê khai thông tin về hướng dẫn NCS.

5. Biên soạn sách phục vụ đào tạo từ trình độ đại học trở lên

| **TT** | **Tên sách** | **Loại sách (CK, GT, TK, HD)** | **Nhà xuất bản và năm xuất bản** | **Số tác giả** | **Chủ biên** | **Phần biên soạn (từ trang ... đến trang)** | **Xác nhận của cơ sở GDĐH (Số văn bản xác nhận sử dụng sách)** |
|---|---|---|---|---|---|---|---|
| Trước khi được công nhận PGS/TS | | | | | | | |
| 1 | Giáo trình cơ sở kỹ thuật an ninh mạng | GT | Quân đội nhân dân, năm 2007 | 5 | VC | (126-193) | Học viện KTQS (Giấy chứng nhận số 2151 /GCN-HV) |
| 2 | Cơ sở kỹ thuật mạng máy tính | GT | Quân đội nhân dân, năm 2007 | 3 | VC | (88-107; 140-208) | Học viện KTQS (Giấy chứng nhận số 2151 /GCN-HV) |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | Kỹ thuật lập trình phần mềm an toàn | GT | Quân đội nhân dân, năm 2007 | 5 | VC | (40-103) | Học viện KTQS (Giấy chứng nhận số 2151 /GCN-HV) |
| 4 | Cơ sở lý thuyết truyền tin | TK | Khoa học và Kỹ thuật, năm 2008 | 2 | CB | (47-116; 185-266) | Học viện KTQS (Giấy chứng nhận số 2151 /GCN-HV) |
| Sau khi được công nhận PGS/TS | | | | | | | |
| 5 | An ninh hệ thống mạng máy tính | GT | Quân đội nhân dân, năm 2013 | 5 | CB | (11-42; 187-253) | Học viện KTQS (Giấy chứng nhận số 2151 /GCN-HV) |
| 6 | Digitals signature schemes: from theory to design | TK | Quân đội nhân dân, năm 2015 | 3 | CB | (19-136; 233-378) | Học viện KTQS (Giấy chứng nhận số 2151 /GCN-HV) |
| 7 | Mật mã hậu lượng tử | TK | Khoa học và Kỹ thuật, năm 2022 | 1 | MM | (Toàn bộ) | Viện Khoa học và Công nghệ Quân sự (Giấy chứng nhận số 50 / ĐT-SĐH) |

Trong đó, số lượng (ghi rõ các số TT) sách chuyên khảo do nhà xuất bản có uy tín xuất bản và chương sách do nhà xuất bản có uy tín trên thế giới xuất bản, mà ứng viên là chủ biên sau PGS/TS: 0 ( [5] [6] [7] )

*Lưu ý:*

- Chỉ kê khai các sách được phép xuất bản (Giấy phép XB/Quyết định xuất bản/số xuất bản), nộp lưu chiểu, ISBN (nếu có).

- Các chữ viết tắt: CK: sách chuyên khảo; GT: sách giáo trình; TK: sách tham khảo; HD: sách hướng dẫn; phần ứng viên biên soạn cần ghi rõ từ trang…. đến trang…… (ví dụ: 17-56; 145-329).

6. Thực hiện nhiệm vụ khoa học và công nghệ đã nghiệm thu

| TT | Tên nhiệm vụ khoa học và công nghệ (CT, ĐT...) | CN/PCN/TK | Mã số và cấp quản lý | Thời gian thực hiện | Thời gian nghiệm thu (ngày, tháng, năm) / Xếp loại KQ |
|---|---|---|---|---|---|
| Trước khi được công nhận PGS/TS | | | | | |
| 1 | Xây dựng và thực hiện thuật toán mật mã khối trên công nghệ FPGA cho mục đích thiết kế chế tạo các thiết bị bảo mật thông tin | CN | ĐTCS-HVKTQS, cấp Cơ sở | 01/12/2007 đến 01/12/2008 | 26/03/2009 / Xuất sắc |
| 2 | Đánh giá bộ sản phẩm "Ứng dụng bộ công cụ bảo mật mạng máy tính Quân sự" | CN | ĐTCS-HVKTQS, cấp Cơ sở | 01/05/2009 đến 01/05/2010 | 26/5/2010/ Khá |
| Sau khi được công nhận PGS/TS | | | | | |
| 3 | Nghiên cứu thiết kế, chế tạo mô hình thiết bị bảo mật thông tin ứng dụng thuật toán mật mã hiệu năng cao | CN | ĐT-BQP, cấp Bộ | 03/09/2009 đến 03/04/2010 | 22/4/2011 / Đạt |
| 4 | Nghiên cứu, xây dựng giải pháp bảo mật cơ sở dữ liệu lớn hỗ trợ phát triển Chính phủ điện tử | CN | 12/ĐTCB/2018, cấp Bộ | 01/10/2018 đến 01/09/2019 | 28/8/2020 / Đạt |

- Các chữ viết tắt: CT: Chương trình; ĐT: Đề tài; CN: Chủ nhiệm; PCN: Phó chủ nhiệm; TK: Thư ký.

7. Kết quả nghiên cứu khoa học và công nghệ đã công bố (bài báo khoa học, báo cáo khoa học, sáng chế/giải pháp hữu ích, giải thưởng quốc gia/quốc tế):

7.1.a. Bài báo khoa học, báo cáo khoa học đã công bố:

| TT | Tên bài báo/báo cáo KH | Số tác giả | Là tác giả chính | Tên tạp chí hoặc kỷ yếu khoa học/ISSN hoặc ISBN | Loại Tạp chí quốc tế uy tín: ISI, Scopus (IF, Qi) | Số lần trích dẫn (không tính tự trích dẫn) | Tập, số, trang | Tháng, năm công bố |
|---|---|---|---|---|---|---|---|---|
| Trước khi được công nhận PGS/TS | | | | | | | | |
| 1 | Шифр и хэш-функция на основе управляемых элементов F3/1 | 2 | Không | Вопросы защиты информации (НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ) ISSN: 2073-2600 | - Hệ thống CSDL quốc tế khác | | 2, 65, 2-7 | 02/2004 |
| 2 | Шифр с высокой интегральной эффективностью аппаратной реализации | 3 | Không | Вопросы защиты информации (НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ) ISSN: 2073-2600 | - Hệ thống CSDL quốc tế khác | | 2, 65, 7-14 | 02/2004 |
| 3 | К синтезу щифров на основе операций, зависящих от ключа | 3 | Không | IX Санкт-Петербургская Международная Конференция «Региональная информатика-2004 (РИ-2004)» | - Hệ thống CSDL quốc tế khác | | 145-148 | 06/2004 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4 | Оптимизация аппаратной реализации криптографических функции в телекоммуникационных устройствах | 2 | Có | IX Санкт-Петербургская Международная Конференция «Региональная информатика-2004 (РИ-2004)» | - Hệ thống CSDL quốc tế khác | | 141-144 | 06/2004 |
| 5 | Итеративная криптосхема с раундовой функцией на основе управляемых подстановочно-перестановочных сетей | 2 | Có | Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции | - Hệ thống CSDL quốc tế khác | | 189-192 | 10/2005 |
| 6 | Влияние выбора управляемых элементов на стойкость криптосхемы Dolphin-128 | 2 | Có | Материалы IV Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России». Санкт-Петербург, 14-16 июня. СПб.: СПОИСУ | - Hệ thống CSDL quốc tế khác | | 148-152 | 06/2005 |
| 7 | Nghiên cứu xây dựng và thực hiện thuật toán mật mã tốc độ cao | 2 | Không | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 116, 83-91 | 09/2006 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8 | Một giải pháp nâng cao độ bền vững của mật mã khối chống lại thám mã vi sai | 4 | Có | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 121, 82-90 | 12/2007 |
| 9 | Đánh giá tốc độ thực hiện của các thuật toán AES trên nền phần mềm | 3 | Có | Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự (JMST) ISSN: 1859-1043 | | | 18, 72-75 | 03/2007 |
| 10 | Design and estimate of a new fast block cipher for wireless communication devices | 3 | Có | Advanced technologies for communications, ATC 2008 ISBN: 978-1-4244-2680-5 | - Scopus | 8 | 409-412 | 10/2008 |
| 11 | New Multisignature Protocols Based on Ramdomized Signature Algorithms | 3 | Có | 2008 IEEE international conference on research, innovation and vision for the future in computing & communication technologies ISBN: 978-1-4244-2379-8 | - Hệ thống CSDL quốc tế khác | 7 | | 07/2008 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 12 | Xây dựng thủ tục sinh khóa phức tạp cho thuật toán mật mã tốc độ cao Crypt(D)_128 | 2 | Không | Các công trình nghiên cứu khoa học, nghiên cứu triển khai công nghệ thông tin và truyền thông (Research and Development on Information & Communication Technology) ISSN 1859-3526 | | | 19, 113-118 | 02/2008 |
| 13 | Phương pháp tổ hợp thẻ và thuộc tính trong giấu tin trên định dạng siêu văn bản | 2 | Không | Tạp chí khoa học và Công nghệ, Đại học Thái Nguyên (TNU Journal of Science and Technology) ISSN 1859-2171, 2374-9098 | | | 59, 11, 51-57 | 11/2009 |
| 14 | Đánh giá các đặc trưng thống kê của thuật toán mật mã Crypt(D)_128 | 4 | Không | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 126, 5-11 | 02/2009 |
| 15 | Protocols for Simultaneous Signing Contracts | 2 | Có | Advanced technologies for communications, ATC 2009 (IEEE Xplore) ISBN: 978-1-4244-5139-5 | - Scopus | 3 | 31-34 | 12/2009 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 16 | Tấn công khóa có liên kết và kiểu trượt trên thuật toán mật mã khối Hawk-64 | 2 | Có | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 129, 107-115 | 08/2009 |
| 17 | Nâng cao hiệu quả thực hiện các thuật toán mật mã vành elliptic trên FPGA | 3 | Không | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 130, 43-53 | 10/2009 |
| 18 | Nghiên cứu giải pháp bảo mật dựa trên các dòng lệnh dư thừa trong mã nguồn | 3 | Không | Tạp chí khoa học và Công nghệ, Đại học Thái Nguyên (TNU Journal of Science and Technology) ISSN 1859-2171, 2374-9098 | | | 67, 5, 57-63 | 03/2010 |
| 19 | Flexible Multisignature Scheme using Russia Standard Gost R 34.10-94 | 2 | Không | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 134, 45-53 | 06/2010 |
| 20 | Phát triển một số giao thức trao đổi khóa | 1 | Có | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 134, 15-23 | 06/2010 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 21 | Two New Discrete Logarithm Problem based Multisignature Schemes | 2 | Có | Tạp chí khoa học và Kỹ thuật, HVKTQS (Journal of Science and Technique) ISSN: 1859-0209 | | | 133, 33-44 | 04/2010 |
| 22 | New Digital Multisignature Scheme with Distinguished Signing Responsibilities | 2 | Không | IJCSNS International Journal of Computer Science and Network Security, Special Issues: Communication Network and Security ISSN: 1738-7906 | - Hệ thống CSDL quốc tế khác | 5 | 10, 1, 51-57 | 01/2010 |
| 23 | Скоростные хэш-функции на основе управляемых перестановок | 4 | Không | Вопросы защиты информации (НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ) ISSN: 2073-2600 | - Hệ thống CSDL quốc tế khác | | 2, 89, 2-6 | 02/2010 |
| 24 | New SDDO-Based Block Cipher for Wireless Sensor Network Security | 3 | Có | IJCSNS International Journal of Computer Science and Network Security, Special Issues: Communication Network and Security ISSN: 1738-7906 | - Hệ thống CSDL quốc tế khác | 23 | 10, 3, 54-60 | 03/2010 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 25 | KT64: A New Block Cipher Suitable to Efficient FPGA Implementation | 3 | Có | IJCSNS International Journal of Computer Science and Network Security, Special Issues: Communication Network and Security ISSN: 1738-7906 | - Hệ thống CSDL quốc tế khác | 9 | 10, 1, 10-18 | 01/2010 |
| Sau khi được công nhận PGS/TS | | | | | | | | |
| 26 | Một số cải tiến trên giao thức trao đổi khóa Diffie-Hellman | 4 | Không | Các công trình nghiên cứu, phát triển và ứng dụng công nghệ thông tin và truyền thông ISSN: 1859-3526 | | | 24, 4, 75-84 | 11/2010 |
| 27 | On functionality extension of the digital signature standards | 5 | Có | Advanced Technologies for Communications (ATC), 2011 International Conference on ISBN: 978-1-4577-1207-4 | - Scopus | 3 | 6-9 | 09/2011 |
| 28 | Đề xuất xây dựng hệ thống chia sẻ tài nguyên dựa trên hệ lưu trữ phân tán và kiểm soát truy cập | 3 | Không | Tạp chí khoa học và Công nghệ, Đại học Thái Nguyên (TNU Journal of Science and Technology) (ISSN 1859-2171, 2374-9098; e-ISSN 2615-9562) | | | 89, 10, 67-74 | 10/2011 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 29 | An Effective and Secure Cipher Based on SDDO | 3 | Không | International Journal of Computer Network and Information Security (IJCNIS) ISSN Print: 2074-9090, ISSN Online: 2074-9104 | - Hệ thống CSDL quốc tế khác | 16 | 11, 1-10 | 10/2012 |
| 30 | Blind signature protocol based on difficulty of simultaneous solving two difficult problems | 4 | Có | Applied Mathematical Sciences ISSN: 1314-7552 (online) ISSN: 1312-885X (print) | Tạp chí Q4 - Scopus | 21 | 139, 6, 6903 - 6910 | 12/2012 |
| 31 | Phát triển thuật toán mật mã khối hiệu năng cao | 2 | Không | Hội thảo quốc gia lần thứ XV: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông - Hà Nội, Nhà xuất bản Khoa học kỹ thuật | | | 489-495 | 12/2012 |
| 32 | Crypt(BM)_64A - A New Cipher oriented to Wireless Sensor Networks | 4 | Không | The 2012 International Conference on Advanced Technologies for Communications (ATC 2012) ISBN: 978-1-4673-4352-7 | - Scopus | 1 | 294-299 | 01/2013 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 33 | New multisignature schemes with distinguished signing authorities | 2 | Có | International Conference on Advanced Technologies for Communications (ATC 2012) ISBN: 978-1-4673-4352-7 | - Scopus | 4 | 283-288 | 01/2013 |
| 34 | Digital Signature Schemes from Two Hard Problems | 3 | Không | International Conference on Green and Human Information Technology 2013 (ICGHIT2013) ISBN: 978-94-007-6738-6 | - Scopus | 6 | 817-825 | 05/2013 |
| 35 | Security evaluation of the SPECTR-128 block cipher | 7 | Không | Applied Mathematical Sciences ISSN: 1314-7552 (online) ISSN: 1312-885X (print) | Tạp chí Scopus Q3 - Scopus | | 7, 140, 6945-6960 | 05/2013 |
| 36 | A high speed block cipher algorithm | 2 | Không | International Journal of Security and Its applications ISSN: 1738-9976 (Print) ISSN: 2207-9629 (Online) | Tạp chí Scopus Q3 - Scopus | 2 | 7, 6, 43-54 | 07/2013 |
| 37 | High-Speed Block Cipher Algorithm Based on Hybrid Method | 2 | Không | Ubiquitous Information Technologies and Applications Lecture Notes in Electrical Engineering ISBN: 978-3-642-41670-5 | - Scopus | 4 | 280 285-291 | 04/2014 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 38 | 240-bit Collective Signature Protocol in a Non-cyclic Finite Group | 4 | Không | 2014 International Conference on Advanced Technologies for Communications (ATC 2014) ISBN: 978-1-4799-6955-5 | - Scopus | 2 | 467-470 | 02/2015 |
| 39 | Interval type-2 fuzzy logic C-means clustering algorithm on GPU for instrusion detection problem | 4 | Không | International conference on Green and Human Information Technology 2015 | - Hệ thống CSDL quốc tế khác | | 227 - 230 | 02/2015 |
| 40 | Zing Database: high-performance key-value store for large-scale storage service2 | 2 | Không | Vietnam Journal of Computer Science ISSN: 2196-8888 | - Hệ thống CSDL quốc tế khác | 27 | 1, 2, 13-23 | 02/2015 |
| 41 | ZDB-High performance key-value store | 2 | Không | Information and Communication Technologies (WICT), 2013 Third World Congress on ISBN: 978-1-5090-0010-4 | - Scopus | | 311-316 | 06/2015 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 42 | Improving on the integrated Diffie-Hellman-GOST. R94 key agreement protocols | 4 | Không | Information and Communication Technologies (WICT), 2013 Third World Congress on ISBN: 978-1-5090-0010-4 | - Scopus | 1 | 106-110 | 06/2015 |
| 43 | BFC: High-performance distributed big-file cloud storage based on key-value store | 3 | Không | 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD 2015) ISBN: 978-1-4799-8676-7 | - Scopus | 7 | 1-6 | 06/2015 |
| 44 | Giải pháp bảo đảm an toàn cơ sở dữ liệu trong môi trường OUTSOURCE | 4 | Có | Nghiên cứu Khoa học và Công nghệ trong lĩnh vực An toàn thông tin (Journal of Science and Technology on Information security) ISSN 2615-9570 | | | 1, 47-56 | 09/2015 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 45 | Một số lược đồ chữ ký số mù mới dựa trên hai bài toán DLP và ECDLP | 4 | Không | Tạp chí Khoa học và Công nghệ - Đại học Thái Nguyên (TNU Journal of Science and Technology) ISSN 1859-2171, 2374-9098; e-ISSN 2615-9562 | | | 135, 5, 3-11 | 09/2015 |
| 46 | Forest of distributed B+ tree based on key-value store for big-set problem | 2 | Không | DASFAA 2016 International Workshops: BDMS, BDQM, MoI, and SeCoP, Dallas, TX, USA, April 16-19, 2016 ISBN: 978-3-319-32054-0 | - Scopus | 2 | 268-282 | 04/2016 |
| 47 | Distributed and High Performance Big-File Cloud Storage Based on Key-Value Store | 2 | Không | International Journal of Networked and Distributed Computing ISSN (Online): 2211-7946 ISSN (Print): 2211-7938 | Tạp chí Scopus Q3 - Scopus | 1 | 3, 4, 159-172 | 07/2016 |
| 48 | Group Signature Protocol Based on Collective Signature Protocol and Masking Public Keys Mechanism | 4 | Không | International Journal of Emerging Technology and Advanced Engineering ISSN 2250 – 2459 (Online) | - Hệ thống CSDL quốc tế khác | 4 | 6, 6, 1-5 | 06/2016 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 49 | Họ thuật toán mật mã khối mới cho các mạng truyền dữ liệu thời gian thực | 4 | Không | Tạp chí Khoa học Công nghệ - Đại học Thái Nguyên (TNU Journal of Science and Technology) ISSN: 1859-2171, 2734-9098 | | | 157, 12/1, 211-217 | 10/2016 |
| 50 | Finding roots in non-cyclic finite groups as primitive for digital signature | 3 | Không | The NAFOSTED Conference on Information and Computer Science (NICS) ISBN: 978-1-5090-2098-0 | - Scopus | | 206-211 | 09/2016 |
| 51 | A Method for Clustering and Identifying HTTP Automated Software Communication | 4 | Không | Advances in Information and Communication Technology, Advances in Intelligent Systems and Computing (Springer) ISBN: 978-3-319-49072-4 | - Scopus | | 538 53-62 | 12/2016 |
| 52 | New Block Ciphers for Wireless Moblile Netwoks | 4 | Không | Advances in Information and Communication Technology, Advances in Intelligent Systems and Computing ISBN: 978-3-319-49072-4 | - Scopus | 3 | 538 393-402 | 12/2016 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 53 | Integrating Multisignature Scheme into the Group Signature Protocol | 5 | Không | Advances in Information and Communication Technology, Advances in Intelligent Systems and Computing ISBN: 978-3-319-49072-4 | - Scopus | 4 | 538 294-301 | 12/2016 |
| 54 | Hai lược đồ ký số tập thể ký tuần tự dựa trên bài toán Logarit rời rạc | 4 | Không | Tạp chí nghiên cứu khoa học và kỹ thuật (Viện Khoa học và Công nghệ quân sự) ISSN: 1859-1043 | | | 47, 93-99 | 02/2017 |
| 55 | Speed up Querying Encrypted Data on Outsourced Database | 4 | Có | International Conference on Machine Learning and Soft Computing, International Conference Proceedings Series by ACM ISBN: 978-1-4503-4828-7 | - Scopus | 3 | 47-52 | 01/2017 |
| 56 | New Blind Signature Protocols Based on a New Hard Problem | 4 | Có | The International Arab Journal of Information Technology ISSN: 16833198, 23094524 | Tạp chí SCIE; Scopus:Q2 - SCIE ***IF: 0.72*** | 6 | 3, 14, 307-313 | 05/2017 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 57 | Xây dựng các lược đồ chữ ký số tập thể có phân biệt trách nhiệm ký tuần tự dựa trên bài toán logarit rời rạc và khai căn | 2 | Không | Tạp chí Khoa học và Công nghệ-Đại học Đà Nẵng (UD-JST) ISSN 1859-1531 | | | 112, 3, 100-104 | 04/2017 |
| 58 | Về một hàm băm mềm dẻo | 2 | Không | Tạp chí khoa học và Công nghệ Đại học Thái Nguyên (TNU Journal of Science and Technology) ISSN: 1859-2171, 2734-9098 | | | 169, 09, 209-215 | 10/2017 |
| 59 | No-key Protocol for Deniable Encryption | 5 | Có | 4th international conference on information system design and intelligent application Print ISBN: 978-981-10-7511-7 Online ISBN: 978-981-10-7512-4 | - Scopus | 5 | 672 96-104 | 03/2018 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 60 | Deniability of Symmetric Encryption Based on Computational Indistinguishability from Probabilistic Ciphering | 5 | Có | 4th international conference on information system design and intelligent application Print ISBN: 978-981-10-7511-7 Online ISBN: 978-981-10-7512-4 | - Scopus | 5 | 672 209-218 | 03/2018 |
| 61 | A Hybrid Threshold Group Signature Scheme with Distinguished Signing Authority | 3 | Không | 4th international conference on information system design and intelligent application Print ISBN: 978-981-10-7511-7 Online ISBN: 978-981-10-7512-4 | - Scopus | 1 | 672 64-72 | 03/2018 |
| 62 | Method for Pseudo-probabilistic Block Encryption | 5 | Có | 3rd EAI International Conference on Industrial Networks and Intelligent Systems Print ISBN: 978-3-319-74175-8 Online ISBN: 978-3-319-74176-5 | - Scopus | 1 | 221 321-331 | 01/2018 |
| 63 | New Blind Multisignature Schemes based on Signature standards | 5 | Có | 2017 International Conference on Advanced Computing and Applications (ACOMP) ISBN 978-1-5386-0606-3 | - Hệ thống CSDL quốc tế khác | 2 | 23-27 | 06/2018 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 64 | Authenticated key exchange, signcryption and deniable signcryption protocols based on two hard problems | 6 | Có | 2017 International Conference on Advanced Computing and Applications (ACOMP) ISBN 978-1-5386-0606-3 | - Hệ thống CSDL quốc tế khác | 1 | 16-22 | 06/2018 |
| 65 | Lược đồ chữ ký số mù, chữ ký số mù tập thể mới dựa trên hai bài toán khó | 3 | Không | Hội nghị Quốc gia lần thứ XX về Điện tử, Truyền thông và Công nghệ Thông tin (National Conference on Electronics, Communications and Information Technology – REV-ECIT) | | | 95-100 | 10/2017 |
| 66 | New Blind Multi-Signature Schemes Based on ECDLP | 5 | Có | International Journal of Electrical and Computer Engineering (IJECE) ISSN 2088-8708, e-ISSN 2722-2578 | Tạp chí Scopus Q2 - Scopus | 2 | 2, 8, 1074-1083 | 04/2018 |
| 67 | An Application for Monitoring and Analysis of HTTP Communications | 3 | Không | Journal of Communications ISSN: 1796-2021 (Online); 2374-4367 (Print) | Tạp chí Scopus Q4 - Scopus | | 8, 13, 456-462 | 08/2018 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 68 | Phát triển giao thức trao đổi khóa an toàn dựa trên hai bài toán khó | 2 | Không | Tạp chí Nghiên cứu KH&CN quân sự, Số Đặc san CNTT ISSN 1859-1043 | | | 156-163 | 11/2018 |
| 69 | Post-quantum Cryptoschemes: New Finite Non-commutative Algebras for Defining Hidden Logarithm Problem | 6 | Có | ICCASA 2018, ICTCC 2018: Context-Aware Systems and Applications, and Nature of Computation and Communication Print ISBN 978-3-030-06151-7, Online ISBN 978-3-030-06152-4 | - Scopus | 1 | 266 183-194 | 12/2018 |
| 70 | Stream Pseudo-probabilistic Ciphers | 6 | Có | ICCASA 2018, ICTCC 2018: Context-Aware Systems and Applications, and Nature of Computation and Communication Print ISBN 978-3-030-06151-7, Online ISBN 978-3-030-06152-4 | - Scopus | 1 | 266 36-47 | 12/2018 |
| 71 | Pseudo-probabilistic Block Ciphers and their Randomization | 6 | Có | Journal of Ambient Intelligence and Humanized Computing Electronic ISSN 1868-5145, Print ISSN 1868-5137 | Tạp chí SCIE, Scopus Q1 - SCIE ***IF: 3.02*** | 11 | 5, 10, 1977-1984 | 05/2019 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 72 | Management and changing of key for encrypted data in outsourced database | 2 | Không | Le Quy Don Technical University-Section on Information and Communication Technology (LQDTU-JICT) | | | 13 77-90 | 06/2019 |
| 73 | New Blind Signature Protocols Based on Finite Subgroups with Two-Dimensional Cyclicity | 4 | Có | Iranian Journal of Science and Technology, Transactions of Electrical Engineering Electronic ISSN 2364-1827, Print ISSN 2228-6179 | Tạp chí SCIE, Scopus Q4 - SCIE ***IF: 1.06*** | | 1, 43, 277-287 | 07/2019 |
| 74 | Xác thực cơ sở dữ liệu mã hoá thuê ngoài dựa trên xác thực lô | 2 | Không | Tạp chí khoa học và Công nghệ Đại học Thái Nguyên (TNU Journal of Science and Technology) eISSN: 2615-9562; ISSN: 1859-2171, 2734-9098 | | | 2014, 11, 107-116 | 08/2019 |
| 75 | Blind multi-signature scheme based on factoring and discrete logarithm problem | 3 | Không | TELKOMNIKA (Telecommunication, Computing, Electronics and Control) ISSN: 1693-6930, e-ISSN: 302-9293 | Tạp chí Scopus Q3 - Scopus | 2 | 5, 17, 2327-2334 | 10/2019 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 76 | Post-quantum Commutative Encryption Algorithm | 4 | Có | ICCASA 2019, ICTCC 2019: Context-Aware Systems and Applications, and Nature of Computation and Communication Print ISBN: 978-3-030-34364-4 Online ISBN: 978-3-030-34365-1 | - Scopus | 4 | 298 205-214 | 11/2019 |
| 77 | Lược đồ bầu cử điện tử không truy vết dựa trên lược đồ chữ ký số tập thể mù | 3 | Không | Journal of Science and Technology on Information and Communications ISSN: 2525-2224 | | | 03&04 17-25 | 03/2020 |
| 78 | A Study on Batch Verification Scheme in Outsourced Encrypted Database | 3 | Không | SoICT 2019: Proceedings of the Tenth International Symposium on Information and Communication Technology ISBN: 978-1-4503-7245-9 | - Scopus | | 502-507 | 12/2019 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 79 | Digital Signature Algorithms Based on Hidden Discrete Logarithm Problem | 5 | Có | Frontiers in Intelligent Computing: Theory and Applications. Advances in Intelligent Systems and Computing, Springer Print ISBN: 978-981-13-9919-0 Online ISBN: 978-981-13-9920-6 | - Scopus | 1 | 1014 1-12 | 10/2019 |
| 80 | New Modes of Using Block Ciphers: Error Correction and Pseudo-probabilistic Encryption | 6 | Có | Frontiers in Intelligent Computing: Theory and Applications. Advances in Intelligent Systems and Computing, Springer Print ISBN: 978-981-13-9919-0 Online ISBN: 978-981-13-9920-6 | - Scopus | | 1014 57-68 | 10/2019 |
| 81 | Post-quantum Commutative Deniable-Encryption Algorithm | 8 | Có | Advances in Intelligent Systems and Computing Print ISBN: 978-981-15-2779-1 Online ISBN: 978-981-15-2780-7 | - Scopus | 2 | 1125 993-1005 | 04/2020 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 82 | A Research on Clustering and Identifying Automated Communication in the HTTP Environment | 5 | Không | Advances in Intelligent Systems and Computing Print ISBN: 978-981-15-2779-1 Online ISBN: 978-981-15-2780-7 | - Scopus | | 1125 1069-1079 | 04/2020 |
| 83 | Chứng minh tính đúng đắn, an toàn và chối từ của phương pháp mã hóa theo khối giả xác suất | 3 | Không | Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự (Journal of Military Science and Technology (JMST)) ISSN: 1859-1043 | | | 65 175-185 | 02/2020 |
| 84 | Hybrid model in the block cipher applications for high-speed communications networks | 6 | Có | International Journal of Computer Networks & Communications (IJCNC) ISSN: 0975 – 2293; e-ISSN: 0974 - 9322 | Tạp chí Scopus Q4 - Scopus | | 4, 12, 55-70 | 07/2020 |
| 85 | New Primitives of Controlled Elements F2/4 for Block Ciphers | 5 | Có | International Journal of Electrical and Computer Engineering (IJECE) ISSN 2088-8708, e-ISSN 2722-2578 | Tạp chí Scopus Q2 - Scopus | 1 | 5, 10, 5470-5478 | 10/2020 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 86 | A new method for designing post-quantum signature schemes | 4 | Có | Journal of Communications ISSN: 1796-2021 (Online); 2374-4367 (Print) | Tạp chí Scopus Q3 - Scopus | 2 | 10, 15, 747-754 | 10/2020 |
| 87 | Improving the Feature Set in IoT Intrusion Detection Problem Based on FP-Growth Algorithm | 4 | Không | 2020 International Conference on Advanced Technologies for Communications (ATC) ISBN: 978-1-7281-8065-6 Online ISSN: 2162-1039 | - Scopus | 2 | 18-23 | 11/2020 |
| 88 | Post-quantum Digital-signature Algorithms on Finite 6-dimensional Non-commutative Algebras | 5 | Có | Future Data and Security Engineering. FDSE 2020. Lecture Notes in Computer Science(), Springer Print ISBN: 978-3-030-63923-5 Online ISBN: 978-3-030-63924-2 | - Scopus | | 12466 325-341 | 11/2020 |
| 89 | Feature Generation by K-means for Convolutional Neural Network in Detecting IoT System Attacks | 5 | Không | 2021 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT) ISBN: 9781665449519 | - Scopus | 1 | 1-5 | 12/2021 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 90 | Hybrid deniable and short-key encryption protocols based on the authentication procedure | 8 | Không | 2020 International Conference on Advanced Computing and Applications (ACOMP) ISBN-13: 978-1-7281-8167-7 ISSN: 2688-0202 | - Hệ thống CSDL quốc tế khác | | 1-6 | 02/2021 |
| 91 | Post-quantum blind signature protocol on non-commutative algebras | 7 | Có | Journal of Computer Science and Cybernetics ISSN: 1813-9663 | | | 4, 37, 495-509 | 10/2021 |
| 92 | Effective Feature Extraction Method for SVM-Based Profiled Attacks | 3 | Có | Computing and Informatics ISSN 1335-9150 (print) ISSN 2585-8807 (online) | Tạp chí SCIE; Scopus: Q3 - SCIE ***IF: 0.319*** | | 5, 40, 1108–1135 | 12/2021 |
| 93 | The Multi-objective Optimization of the Convolutional Neural Network for the Problem of IoT System Attack Detection | 3 | Không | MCO 2021: Modelling, Computation and Optimization in Information Systems and Management Sciences Print ISBN: 978-3-030-92665-6 Online ISBN: 978-3-030-92666-3 | - Scopus | | 363 350-360 | 12/2021 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 94 | A Novel Version of the Hidden Logarithm Problem for Post-quantum Signature Algorithms | 6 | Có | Theoretical Computer Science ISSN: 0304-3975 | Tạp chí SCIE; Scopus:Q2 - SCIE ***IF: 0.827*** | | 921 36-49 | 06/2022 |
| 95 | Blind Signature Protocol Based on Hidden Discrete Logarithm Problem Set in a Commutative Algebra | 5 | Có | Iranian Journal of Science and Technology, Transactions A: Science Electronic ISSN: 2364-1819 Print ISSN: 1028-6276 | Tạp chí SCIE; Scopus:Q2 - SCIE ***IF: 1.194*** | | 46 323–332 | 02/2022 |

- Trong đó: Số lượng (ghi rõ các số TT) bài báo khoa học đăng trên tạp chí khoa học quốc tế có uy tín mà UV là tác giả chính sau PGS/TS: 11 ( [30] [56] [66] [71] [73] [84] [85] [86] [92] [94] [95] )

7.1.b. Bài báo khoa học, báo cáo khoa học đã công bố ***(Dành cho các chuyên ngành thuộc ngành KH An ninh và KH Quân sự được quy định tại Quyết định số 25/2020/QĐ-TTg)***

| TT | Tên bài báo/báo cáo KH | Số tác giả | Là tác giả chính | Tên tạp chí hoặc kỷ yếu khoa học/ISSN hoặc ISBN | Thuộc danh mục tạp chí uy tín của ngành | Tập, số, trang | Tháng, năm công bố |
|---|---|---|---|---|---|---|---|
| Không có | | | | | | | |

- Trong đó: Số lượng (ghi rõ các số TT) bài báo khoa học đăng trên tạp chí khoa học uy tín của ngành mà UV là tác giả chính sau PGS/TS:

7.2. Bằng độc quyền sáng chế, giải pháp hữu ích

| TT | Tên bằng độc quyền sáng chế, giải pháp hữu ích | Tên cơ quan cấp | Ngày tháng năm cấp | Tác giả chính/ đồng tác giả | Số tác giả |
|---|---|---|---|---|---|

| Sau khi được công nhận PGS/TS | | | | | |
|---|---|---|---|---|---|
| 1 | Phương pháp hình thành và kiểm tra chữ ký số tập thể dựa trên đường cong Elliptic, để chứng thực các văn bản điện tử | Cục Sở hữu trí tuệ/ Bộ Khoa học và Công nghệ | 25/08/2010 | Nguyễn Hiếu Minh (Chủ bằng độc quyền) | 5 |
| 2 | Phương pháp tạo lập và kiểm tra chữ ký số tập thể dựa trên bài toán logarit rời rạc để chứng thực các văn bản điện tử | Cục Sở hữu trí tuệ/ Bộ Khoa học và Công nghệ | 08/03/2011 | Nguyễn Hiếu Minh (Chủ bằng độc quyền) | 5 |

- Trong đó: Số lượng (ghi rõ các số TT) bằng độc quyền sáng chế, giải pháp hữu ích được cấp, là tác giả chính sau PGS/TS: 1 2

7.3. Tác phẩm nghệ thuật, thành tích huấn luyện, thi đấu thể dục thể thao đạt giải thưởng quốc gia, quốc tế (đối với ngành Văn hóa, nghệ thuật, thể dục thể thao)

| TT | Tên tác phẩm nghệ thuật, thành tích huấn luyện, thi đấu TDTT | Cơ quan/tổ chức công nhận | Văn bản công nhận (số, ngày, tháng, năm) | Giải thưởng cấp Quốc gia/Quốc tế | Số tác giả |
|---|---|---|---|---|---|
| Không có | | | | | |

- Trong đó: Số lượng (ghi rõ các số TT) tác phẩm nghệ thuật, thành tích huấn luyện, thi đấu đạt giải thưởng quốc tế, là tác giả chính/hướng dẫn chính sau PGS/TS:

8. Chủ trì hoặc tham gia xây dựng, phát triển chương trình đào tạo hoặc chương trình/dự án/đề tài nghiên cứu, ứng dụng khoa học công nghệ của cơ sở giáo dục đại học đã được đưa vào áp dụng thực tế:

| TT | Chương trình đào tạo, chương trình nghiên cứu ứng dụng KHCN | Vai trò UV (Chủ trì/ Tham gia) | Văn bản giao nhiệm vụ (số, ngày, tháng, năm) | Cơ quan thẩm định, đưa vào sử dụng | Văn bản đưa vào áp dụng thực tế | Ghi Chú |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Đào tạo đại học ngành Truyền thông và Mạng máy tính năm 2011-2012 | Chủ trì | (2011-2012) Giấy chứng nhận: Số: 2302/GCN-HV | Học viện Kỹ thuật Quân sự | (2011-2012) Giấy chứng nhận: Số: 2302/GCN-HV | Thời gian UV là Chủ nhiệm Bộ môn An ninh mạng – Khoa CNTT/ HVKTQS |
| 2 | Đào tạo đại học các chuyên ngành An ninh hệ thống thông tin và chuyên ngành Bảo đảm an toàn thông tin năm 2014-2015 | Tham gia | (2014-2015) Giấy chứng nhận: Số: 2302/GCN-HV | Học viện Kỹ thuật Quân sự | (2014-2015) Giấy chứng nhận: Số: 2302/GCN-HV | Thời gian UV là Chủ nhiệm Bộ môn An ninh mạng – Khoa CNTT/ HVKTQS |
| 3 | Đào tạo thạc sĩ các ngành Hệ thống thông tin, Khoa học máy tính, Công nghệ phần mềm năm 2013-2014 | Tham gia | (2013-2014) Giấy chứng nhận: Số: 2302/GCN-HV | Học viện Kỹ thuật Quân sự | (2013-2014) Giấy chứng nhận: Số: 2302/GCN-HV | Thời gian UV là Chủ nhiệm Bộ môn An ninh mạng – Khoa CNTT/ HVKTQS |
| 4 | Đào tạo tiến sĩ ngành Cơ sở toán học cho tin học năm 2012-2013 | Tham gia | (2012-2013) Giấy chứng nhận: Số: 2302/GCN-HV | Học viện Kỹ thuật Quân sự | (2012-2013) Giấy chứng nhận: Số: 2302/GCN-HV | Thời gian UV là Chủ nhiệm Bộ môn An ninh mạng – Khoa CNTT/ HVKTQS |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | Đào tạo tiến sĩ Chuyên ngành An toàn thông tin năm 2018 | Tham gia | 29-QN/ĐUH ngày 26/3/2018 Quyết nghị về việc mở đào tạo tiến sĩ ATTT | Học viện Kỹ thuật mật mã | Biên bản thông qua hồ sơ đề nghị cho phép đào tạo chuyên ngành ATTT trình độ TS ngày 7/9/2018 | Thời gian UV là Chủ nhiệm Khoa Điện tử - Viễn thông HVKTMM |

9. Các tiêu chuẩn còn thiếu so với quy định cần được thay thế bằng bài báo khoa học quốc tế uy tín*:

a) Thời gian được bổ nhiệm PGS

Được bổ nhiệm PGS chưa đủ 3 năm: thiếu (số lượng năm, tháng):

b) Hoạt động đào tạo

- Thâm niên đào tạo chưa đủ 6 năm (ƯV PGS), còn thiếu (số lượng năm, tháng):

- Giờ giảng dạy

+ Giờ chuẩn giảng dạy trực tiếp trên lớp không đủ, còn thiếu (năm học/số giờ thiếu):

+ Giờ chuẩn giảng dạy quy đổi không đủ, còn thiếu (năm học/số giờ thiếu):

- Hướng dẫn chính NCS/HVCH,CK2/BSNT:

+ Đã hướng dẫn chính 01 NCS đã có Quyết định cấp bằng TS (ƯV chức danh GS) ☐

Đề xuất CTKH để thay thế tiêu chuẩn hướng dẫn 01 NCS được cấp bằng TS bị thiếu:

+ Đã hướng dẫn chính 01 HVCH/CK2/BSNT đã có Quyết định cấp bằng ThS/CK2/BSNT (ƯV chức danh PGS) ☐

Đề xuất CTKH để thay thế tiêu chuẩn hướng dẫn 01 HVCH/CK2/BSNT được cấp bằng ThS/CK2/BSNT bị thiếu:

c) Nghiên cứu khoa học

- Đã chủ trì 01 nhiệm vụ KH&CN cấp Bộ (ƯV chức danh GS) ☐

Đề xuất CTKH để thay thế tiêu chuẩn chủ trì 01 nhiệm vụ KH&CN cấp Bộ bị thiếu:

- Đã chủ trì không đủ 01 nhiệm vụ KH&CN cấp cơ sở (ƯV chức danh PGS) ☐

Đề xuất CTKH để thay thế tiêu chuẩn chủ trì 01 nhiệm vụ KH&CN cấp cơ sở bị thiếu:

- Không đủ số CTKH là tác giả chính sau khi được bổ nhiệm PGS hoặc được cấp bằng TS:

+ Đối với ứng viên chức danh GS, đã công bố được: 03 CTKH ☐; 04 CTKH ☐

Đề xuất sách CKUT/chương sách của NXB có uy tín trên thế giới là tác giả chính thay thế cho việc ƯV không đủ 05 CTKH là tác giả chính theo quy định:

+ Đối với ứng viên chức danh PGS, đã công bố được: 02 CTKH ☐

Đề xuất sách CKUT/chương sách NXB có uy tín trên thế giới là tác giả chính thay thế cho việc ƯV không đủ 03 CTKH là tác giả chính theo quy định:

***Chú ý: Đối với các chuyên ngành bí mật nhà nước thuộc ngành KH An ninh và KH Quân sự, các tiêu chuẩn không đủ về hướng dẫn, đề tài khoa học và công trình khoa học sẽ được bù bằng điểm từ các bài báo khoa học theo quy định tại Quyết định số 25/2020/QĐ-TTg.***

d) Biên soạn sách phục vụ đào tạo (đối với ứng viên GS)

- Không đủ điểm biên soạn sách phục vụ đào tạo:

- Không đủ điểm biên soạn giáo trình và sách chuyên khảo:

## C. CAM ĐOAN CỦA NGƯỜI ĐĂNG KÝ XÉT CÔNG NHẬN ĐẠT TIÊU CHUẨN CHỨC DANH:

Tôi cam đoan những điều khai trên là đúng, nếu sai tôi xin chịu trách nhiệm trước pháp luật.

Hà Nội., ngày 29 tháng 06 năm 2022

Người đăng ký

(Ký và ghi rõ họ tên)