JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 4: 470~476, Apr. 2019

입력시간을 측정하는 쓰레드를 활용한 패턴 잠금 보안 강화 구현

안규황[1] · 권혁동[1] · 김경호[1] · 서화정[2*]

Implement pattern lock security enhancement using thread to measure input time

Kyuhwang An[1] · Hyeokdong Kwon[1] · Kyungho Kim[1] · Hwajeong Seo[2*]

[1]Graduate Student, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea
[2*]Assistant professor, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea

요 약

스마트폰에 적용된 패턴 잠금 기법 같은 경우 많은 사람들이 편리하게 사용하는 잠금 기법이다. 그러나 많은 사람들이 사용하는데 비해 패턴 잠금 기법에 대한 안전성은 정말 낮다. 패턴 잠금 기법은 사용자가 입력하는 드래그 방식을 어깨의 움직임을 보고 유추할 수 있는 shoulder surfing attack에 취약하며, 핸드폰 패드에 남아있는 지문 드래그 자국에 의해 smudge attack 또한 취약하다. 따라서 본 논문에서는 해당 취약점을 보안하기 위해 패턴 잠금 기법에 쓰레드를 활용하여 눌리는 시간을 체크하는 새로운 보안 방식을 추가하고자 한다. 각 점에서의 누른 시간에 따라 short, middle, long click으로 나누어지고, 그 방법을 사용하여 드래그하면 보안 성능이 3^n배 향상된다. 따라서 같은 'ㄱ' 방식으로 드래그 하더라도 각 점마다 누르는 시간에 따라 완전히 다른 패턴이 된다.

ABSTRACT

The pattern locking technique applied to smart phones is a locking technique that many people use conveniently. However, the safety of pattern locking techniques is very low compared with other techniques. The pattern locking technique is vulnerable to a shoulder surfing attack, which is based on the user's input and can be interpreted by looking at the movement of the shoulder, and the smudge attack is also vulnerable due to fingerprint drag marks remaining on the mobile phone pad. Therefore, in this paper, we want to add a new security method to check the pressed time by using a thread in the pattern locking scheme to secure the vulnerability. It is divided into short, middle, and long click according to the pressing time at each point. When dragging using the technique, security performance enhances 3^n tiems. Therefore, even if dragging in the same 'ㄱ' manner, it becomes a completely different pattern depending on the pressing time at each point.

키워드 : 드래그, 쓰레드, 어깨너머 공격, 추정 공격, 패턴 잠금

Key word : Drag, Pattern lock, Shoulder surfing attack, Smudge attack, Thread

Received 26 January 2019, **Revised** 6 February 2019, **Accepted** 22 February 2019

***Corresponding Author** Hwajeong Seo(E-mail:hwajeong84@gmail.com, Tel:+82-2-760-8033)
Assistant professor, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.4.470 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

2000년대 이후 스마트폰 보급이 대중화됨에 따라 개인식별번호(PIN, personal identification number) 방식인 키패드 보안 역시 화두에 올랐다. 스마트폰에는 잠금화면을 푸는 방식 중 패턴 인식 방식이 존재한다. 패턴 인식 방식이란 그림 1과 같이 3x3 형식으로 이루어진 구조로 9개의 점들 중 먼저 입력되는 순서와 패턴을 기억하여 그것이 하나의 비밀번호가 되는 방식이다.

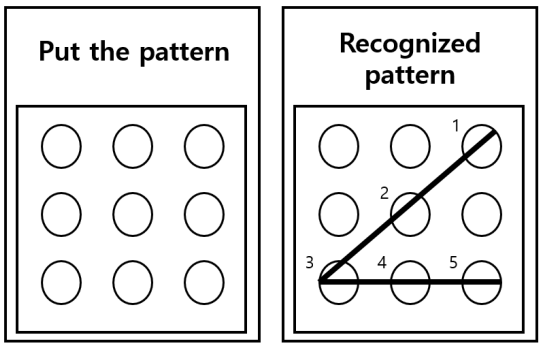

Fig. 1 Left) before put the pattern, Right) recognized pattern

사용자 측면에서 비밀번호를 누르는 방식보다 외우기 쉽고 동작하는데 있어 편리함을 느껴 많은 사람들이 사용하고 있지만, 전 세계에 있는 사람들이 즐겨 사용하는 방식인데 비해 보안 수준은 최하위다. 현재 핸드폰에서 사용하는 패턴 인식 같은 경우 별다른 사용 방법 없이 위에서 설명한 구조가 전부이다. 사용의 편리함에 따라 보안 강도 역시 낮아지는 것이다.

현재 패턴인식에는 shoulder surfing attack[1]이 가능하다. shoulder surfing attack이란 어깨나 손의 움직임을 이용하여 비밀번호를 유추하는 방식으로 해당 패턴 잠금 방식에서는 멀리서도 손가락의 움직임을 유추하여 비밀번호 획득이 가능하다. Smudge attack[2] 또한 가능하다. Smudge attack은 비밀번호를 눌렀던 지문의 흔적으로 비밀번호를 유추하는 방식으로 패턴 잠금 장치의 경우 드래그 했던 손가락의 움직임을 획득하여 비밀번호를 획득할 수 있다. 만약 드래그한 모습이 핸드폰 액정에 그대로 남아있다면 드래그를 시작한 지점과 끝마치는 지점을 각각 바꿔서 시도해보는 단 2번의 시도 만에 비밀번호를 유추할 수 있다. 따라서 본 논문에서는 기존 패턴 잠금의 드래그 방식에서 벗어나지 않고 각 점에서 인식하는 시간을 추가하여 3n 만큼의 보안 확률이 늘어나는 새로운 기법을 국내 최초로 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 키패드 보안과 관련되어 선행되었던 연구 자료에 대해 알아볼 것이다. 3장에서는 본 논문의 제안 기법에 대하여 설명하고 4장에서는 해당 기법에 대한 성능 평가를 다룰 것이며, 마지막으로 5장에서는 결론으로 마무리할 예정이다.

Ⅱ. 관련 연구 동향

본 논문의 2장에서는 패턴 잠금을 기반의 키패드 보안에 관련된 2가지 연구 논문에 대하여 알아보며, 패턴 잠금 이외에 도어락에 적용된 보안 기법에 대하여 알아보겠다.

2.1. T-LOCK: 스마트폰용 삼중 요소 기반 패턴 락 인증 기법[3]

스마트폰용 삼중 요소 기반 패턴 락 인증 기법에서는 잠금을 해제하기 위한 요소로 패턴, 압력, 지문 3가지의 정보를 동시에 사용한다. 패턴은 기존의 패턴 락 잠금 기법과 같은 것으로 사용자가 지정한 패턴과 동일하게 입력하면 잠금이 해제되는 방식이다. 압력은 스크린에 패턴을 입력하는 중 스크린에 가해지는 압력을 측정하는 것으로 일정 구간별 또는 단위 시간마다 전체 구간에서 측정되는 압력 값을 인증에 사용한다. 이는 패턴을 입력할 때 사용자의 버릇이나 악력에 따라 동일 패턴이라도 서로 다른 압력 값이 나오며 만일 동일 사용자의 경우에는 비슷한 압력 값이 나올 것이라는 점에 기반한 기법이다. 마지막으로 지문은 스크린 자체에 지문 내장을 포함하여 패턴 입력 중 시작 점, 끝 점 또는 중간의 특정 점을 설정하여 패턴 입력 도중 지문까지 동시에 스캔하는 방법이다. 하지만 아직 전체 스크린에서 지문을 스캔할 수 있는 장비는 없기 때문에 도입은 불가능하다.

2.2. TinyLock: Affordable defense against smudge attacks on smart phone pattern lock systems[4]

기존 패턴 락은 입력을 완료하고 손을 스크린에서 떼는 순간 잠금이 해제되기 때문에 스크린 상에는 지문이

그대로 남으며 근처에 화면을 보는 다른 사람이 있다면 보는 것만으로도 패턴을 파악할 수 있다. TinyLock은 패턴 입력 부분을 매우 작게 만들고 두 공간으로 나눈다. 사용자가 입력을 할 때는 그리드 내부의 입력부에 손을 올리고 패턴을 그려서 잠금을 해제할 수 있다. 이는 기존의 패턴 락과 동일한 부분이지만 그리드 내부의 입력부는 매우 작기 때문에 사용자의 손가락에 가리게 되어 누군가가 화면을 보더라도 패턴이 손가락에 가리기에 패턴을 파악하기 어렵게 만든다. 사용자는 자신의 손가락에 입력이 가리지만 그리드 외부에 똑같은 모양이 있기 때문에 해당 공간을 보면서 자신의 입력을 유추해낼 수 있다. 또한 TinyLock은 입력이 완료되었을 때 손가락을 스크린에서 떼는 것이 아닌 원형으로 돌려서 입력이 끝났음을 알리는 방식을 사용한다. 이는 패턴 입력이 완료되고 마지막에 원형으로 돌리는 과정에서 입력부의 지문을 전부 원형으로 만들기 때문에 다른 사람이 지문을 보더라도 원형의 지문만 남아있기에 패턴 파악이 어려워진다.

Ⅲ. 제안 기법

본 논문에서 제안하는 기법에 대하여 직접 구현하였으며, 해당 구현 결과물에 대하여 동영상 촬영을 하였고 youtube[5]에서 확인할 수 있다[1]. 또한 구현 코드는 github[6]에 올려놔 open source로 공개하였으며[2], 구현 환경은 표 1과 같다.

Table. 1 The information of experiment environment

Device	Nexus 5X
OS	Android
Version	API 28
Display	420dpi

현재 우리가 사용하는 패턴 잠금은 각 포인트마다 어디서부터 드래그가 시작되었고 어느 방향으로 나가는지 혹은 끝마치는지에 대한 정보밖에 담고 있지 않아 서론에서도 언급했듯이 보안에 매우 취약한 모델이다. 따라서 이를 해결하고자 각 포인트마다 눌리는 시간을 인식하는 모델을 제안한다.

각 포인트에서는 손가락이 해당 포인트를 어디서 드래그 했는지와 누르는 시간을 체크한다. 누르는 시간을 체크하는 이유는 그림 1의 오른쪽과 같이 드래그를 한다고 가정했을 때 현재 우리가 사용하는 모델에서는 하나의 드래깅 밖에 포함된 정보가 없다. 그러나 만약 각 포인트마다 입력하는 시간을 짧게, 중간, 길게 총 3단계로 나눠서 인식한다면 각 포인트 마다 3^n배 만큼의 보안 강도가 올라간다.

사용자가 직접 본 논문에서 제안하는 기법이 적용 된 패턴 잠금 방법을 사용할 경우 드래그를 하여 각 포인트들을 지나칠 때 마다 진동이 발생하게 된다. 실제로 사용할 때는 그림 2와 같이 short, middle, long click이라는 정보가 화면에 보여 지지 않고 핸드폰에 진동을 줘 사용자만 알 수 있게끔 한다. 짧게 터치 했을 경우엔 진동이 발생하지 않고, 중간 단계로 터치 했을 경우엔 1회 진동이 발생한다. 긴 단계로 터치 했을 경우엔 2회 진동이 그 즉시 발생하여 사용자는 내가 짧게 눌렀는지 길게 눌렀는지 바로 파악할 수 있다. 그림 2는 제안하는 기법에 대한 구현 이미지이며, 사진에 나와 있는 문구는 진동이라는 특성상 증명할 방법이 없어 진동을 문구를 이용하여 설명하는데 대체한다.

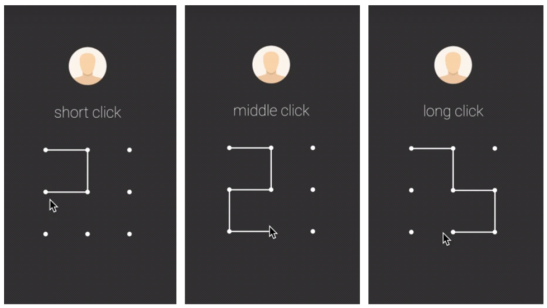

Fig. 2 Suggested solution

본 기법을 제안하는데 있어 쓰레드(thread)를 활용하였다. 쓰레드란 하나의 프로그램에서 동시에 여러 가지 일을 처리하게 해주는 기법으로 그림 3을 보면 쓰레드를 사용하지 않는 프로세스(process)의 경우 func1이 종료가 되어야지 func2가 불리게 된다. 그러나 쓰레드를 사용하는 프로세스의 경우 func1과 func2를 동시에 사용할 수 있어 쓰레드를 사용하지 않는 프로세스보다 수행시간이 현저히 짧아질 수 있다는 장점이 있다.

1) https://github.com/kyu-h/PressTime_PatternLock_PIN
2) https://youtu.be/OEOkHHQPTgA

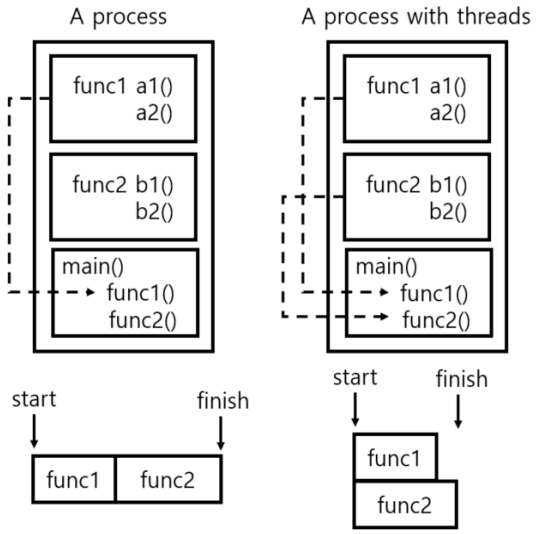

Fig. 3 The processes without or with threads

본 논문에서 제안하는 기법에 쓰레드를 사용한 목적은 시간이 경과함을 체크해주기 위함이다. 그림 4를 보면 쓰레드를 이용하여 시간을 체크하는 방식을 슈도코드(pseudocode)를 활용하여 작성하였다.

A라는 쓰레드는 각 포인트에 진입하는 시간을 체크하며 다른 B라는 쓰레드에서는 실시간으로 시간의 경과를 체크한다. 이때 특정 시간이 지난다면 B 쓰레드는 경과 시간에 따라 짧게 눌렀는지 길게 눌렀는지 체크해 바로바로 사용자에게 피드백을 전달한다.

Algorithm 1 Check press time with thread

```
Input: press time
Output:
  Thread start when activity created
  Get user press time in real time

  IF press time is smaller than 1
    text change to "short click"
  ELSE IF press time is bigger than 1 and smaller than 2
    text change to "middle click"
  ELSE IF press time is bigger than 2
    text change to "long click"
  ELSE
    clearing text area
```

Fig. 4 Pseudo code that shows how to check the pressing time using thread

Ⅳ. 성능 평가

본 장에서는 보안 키패드에서 비밀번호를 탈취하기 위해 흔히 사용되는 공격인 shoulder surfing attack, smudge attack, key logging attack에 대하여 얼마나 안전한 보안 성능을 가지고 있는지 평가해보겠다.

4.1. Shoulder surfing attack

Shoulder surfing attack은 사용자의 어깨나 손의 움직임을 보고 비밀번호를 유추하는 공격이다. 그림 5의 왼쪽과 같이 현재 우리가 사용하는 키패드의 패턴 잠금 기법의 경우 하나의 패턴에는 하나의 경우의 수 밖에 존재하지 않아 만약 다른 사용자가 악의적 목적으로 드래깅하는 모습을 엿보고 해당 드래깅을 기억해 핸드폰에 담겨 있는 정보를 탈취하고자 한다면 속수무책으로 당하게 된다. 그러나 본 논문에서 제안하는 시스템의 경우 기존의 키패드와 동일하게 드래깅을 해도 하나의 포인트에는 3가지 정보(짧게, 중간 길게) 중 하나가 담기기 때문에 3^n만큼의 경우의 수가 증가하게 된다. 그림 5의 오른쪽을 기준으로 3^5개의 경우의 수가 생기게 된다. 따라서 shoulder surfing attack을 활용하여 패턴 모양을 유추하였다고 할지라도, 각 좌표가 갖고 있는 입력 시간에 대한 정보는 알 수 없기 때문에 비밀번호 탈취가 불가능하게 된다. 본 논문에서 제시하는 기법은 좌표의 수가 많아질수록 경우의 수는 배로 증가하게 되어 기존의 단 하나의 경우의 수밖에 존재하지 않는 기법보다 3^n 배 만큼의 성능 향상을 보여준다.

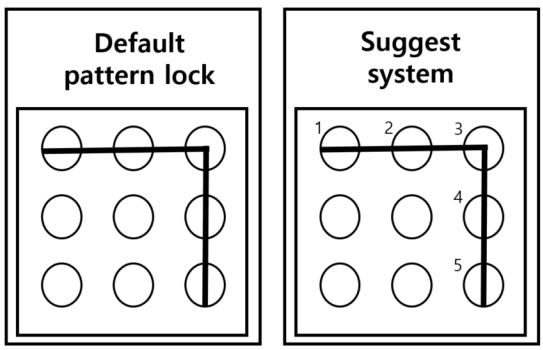

Fig. 5 Comparing default pattern lock with suggest system

4.2. Smudge attack

Smudge attack이란 키패드 화면에 남아있는 지문으로 비밀번호를 유추하는 공격으로 패턴 잠금 같은 경우 2가지의 확률로 비밀번호를 탈취할 수 있다. 그림 5의 왼쪽을 기준으로 시작 포인트를 (1, 1)로 할지 (3, 3)으로 할지 결정하여 최대 2번 만에 비밀번호를 탈취할 수 있다. 그러나 본 논문에서 제안하는 기법의 경우 그리는 패턴을 알고 있다고 할지라도 3^n배 만큼의 경우의 수가 증가하고 시작 포인트의 위치를 모르기 때문에 시작 포인트에 따라 3^n배가 추가로 요구된다. 따라서 $2*3^n$만큼 경우의 수가 증가하여 brute force attack[7]을 활용하는 전체 경우의 수를 입력해보지 않는 이상 비밀번호를 탈취하는 것은 불가능하다. 본 제안 기법에서는 brute force attack역시 방지하기 위해 5번 이상 틀리면 1분간 아무것도 할 수 없는 lock 상태가 되며 그 이상으로 시도할 경우 5^n분만큼 lock을 하게 만들어 brute force attack도 막을 수 있게 설계하였다.

4.3. Key logging attack

Key logging attack은 앞에서 언급했던 두 가지 공격 방법과는 다른 공격 방법을 취한다. 앞선 두 공격은 사용자가 비밀번호를 입력한 이후에 이루어지는 공격이지만 key logging attack은 사용자가 비밀번호를 입력하는 중간에 비밀번호를 탈취하는 공격 방법이다. 구체적인 공격방법은 그림 6과 같다.

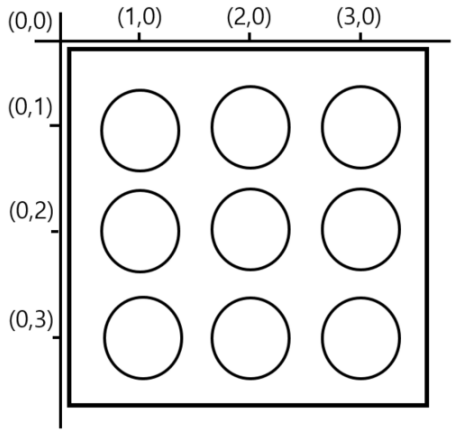

Fig. 6 The absolute positions of each buttons

기존 키패드에서 비밀번호를 입력하고자 할 때 입력하는 번호의 위치가 항시 고정되어 있기 때문에 공격자는 해당 절대 좌표 값을 기반으로 비밀번호를 탈취하게 된다. 예를 들어 1행 3열에 있는 번호를 클릭할 경우 (3.1) 이라는 좌표 값을 탈취하여 어떤 키를 눌렀는지 유추하는 공격이다. 그러나 본 논문에서 제안하는 기법은 좌표 값을 중간에 탈취 당한다고 할지라도 하나의 포인트에는 3가지 경우의 수가 존재하여 이 역시 각 포인트마다 3^n만큼 복잡도를 갖게 된다.

따라서 최종적으로 기본 패턴 잠금 기법과 본 논문에서 제안하는 기법에 대한 3가지 공격법(shoulder surfing attack, smudge attack, key logging attack)을 비교해 본다면 표 2와 같은 결과가 나오게 되며, 기존에 제안된 패턴 잠금 기술보다 약 3^n배 향상된 보안 성능을 나타낸다.

Table. 2 Number of cases for get the secret pattern

	Default pattern lock	Suggest system
Shoulder surfing attack	1	3^n
Smudge attack	2	$3^n * 2$
Key logging attack	1	3^n

4.4. Convenience

보안과 편리성은 반비례 관계를 갖고 있다. 즉 그림 7과 같이, 보안 성능이 향상되면 될수록 사용자 편리성은 줄어들게 되고, 사용자 편리성이 향상되면 보안 성능이 떨어지게 된다. 따라서 두 선이 만나는 곳에서의 적절한 선택이 필요하다.

본 논문에서 제안하는 입력시간을 측정하는 쓰레드를 활용한 키패드의 경우 보안 성능은 향상 되지만, 기존 키패드 보다 불편함을 초래한다. 그러나 그것이 많은 것을 요구하는 정도는 아니기 때문에 실제로 사용한 사용자들은 이 정도의 불편함은 감수할 수 있다고 말하였다.

Fig. 7 The convenience and security

Ⅴ. 결 론

키패드 보안은 과거에서부터 각종 연구[8]가 수행되고 있으며, 본 논문에서는 실생활에서 많이 사용하는 패턴 잠금 기법에 보안 문제점을 발견하고 이를 해결하기 위해 각 포인트에 입력하는 시간을 활용하여 동일한 모양의 패턴이라고 할지라도 3^n배 만큼의 경우 수를 늘리는 기법을 제안하였다. 사용자가 평소에 사용하던 패턴 잠금 방식에서 크게 다르지 않아 한번 정도 사용해보면 바로 어떻게 사용해야할지 익히게 되고 원래 사용했던 것과 비슷하여 보안적 측면은 크게 증가하면서도 편리함은 그대로이다.

본 제안 기법은 안드로이드 스마트폰 상에서 실제로 구현 및 테스트가 진행되었으며 구현 영상을 녹화하여 youtube상에 올려두었고, 구현 코드는 본 논문의 저자의 github 사이트에 올려두었다. 또한 기존 패턴 잠금 기법과 본 논문에서 제안하는 기법의 성능 테스트를 실제로 진행하면서 기존 기법에 비해 3^n배 만큼의 보안 성능이 향상되었음을 확인할 수 있었다.

ACKNOWLEDGEMENT

This work was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017 R1C1B5075742) and was partly supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2014-1-00743) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation). This research of Hwajeong Seo was financially supported by Hansung University.

References

[1] UCSIS. Shoulder Surfing attack in graphical password authentication [Internet]. Available: https://arxiv.org/ftp/arxiv/papers/0912/0912.0951.pdf.

[2] A. J. Aviv, K. L. Gibson, E. Mossop, and J. M. Smith, “Smudge Attacks on Smart phone Touch Screens,” *Woot,* 10: 1-7, 2010.

[3] C. Dongmin, “Application Adaptive Pattern-based Authentication Method for Smartphones,” *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology* vol. 8, no. 2, pp. 59-67, February 2018.

[4] T. Kwon, and S. Na, “TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems,” *Computers & Security*, 42, pp. 137-150, 2014.

[5] Youtube. The video of how it works [Internet]. Available: https://youtu.be/OEOkHHQPTgA.

[6] Github. The open source of press time pattern lock PIN [Internet]. Available: https://github.com/kyu-h/PressTime_PatternLock_PIN.

[7] A. Karawash. Brute Force Attack [Internet]. Available: https://www.researchgate.net/profile/Ahmad_Karawash/publication/299645572_Data_protection_and_Brute_Force_attack/links/5703c19e08aeade57a25ae7b/Data-protection-and-Brute-Force-attack.pdf.

[8] H. J. Seo, and H. W. Kim, “Secure Keypad with Encrypted Input Message,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 18, no. 12, pp. 2899-2910, Dec. 2014.

안규황(Kyu-hwang An)

2018년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 암호구현, IoT 보안, 블록체인

권혁동(Hyeok-dong Kwon)

2018년 2월: 한성대학교 정보시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, 암호구현

김경호(Kyung-ho Kim)

2019년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2019년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 시스템 보안, 암호화 구현

서화정(Hwa-jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야 : 정보보호, 암호화 구현, IoT