http://dx.doi.org/10.14400/JDC.2015.13.1.283

사용자 인증에 적합한 OTP 생성 알고리즘에 관한 연구

김동률
동명대학교 메카트로닉스학과

A Study on the OTP Generation Algorithm for User Authentication

Dong-Ryool Kim
Dept. of Mechatronics Engineering, Tongmyong University

요 약 일회용 패스워드는 정적인 패스워드 사용에 따른 위험을 해결하고 사용자 인증을 강화하기 위해 필요하다. 개인정보 유출에 따른 사용자를 인증을 강화하기 위해 OTP 생성 알고리즘이 중요시 되고 있다. 본 논문에서 제안하는 OTP 생성 알고리즘은 *Seed*값과 *Time*값을 이용하여 256비트 크기의 OTP Data를 생성하게 된다. 생성한 OTP Data를 행렬로 나열하고 불규칙적으로 32비트의 값을 추출하게 되는 이 값이 최종적인 OTP값이 된다. OTP 생성 횟수가 많을수록 제안하는 알고리즘이 기존 알고리즘에 비해 충돌내성의 확률이 낮음을 알 수 있다.

주제어 : 인증, 일회용패스워드, 난수, 추출함수, 충돌내성

Abstract A disposable password is necessary to avoid any danger by the use of a static password and reinforce the user's authentication. In order to prevent personal information from being exposed, OTP generation algorithm is regarded as important. The OTP generation algorithm we suggest in this thesis generates 256-bit-size OTP Data by using Seed value and Time value. This value that the generated OTP Data are arranged with a matrix and a 32-bit-value is extracted on an irregular basis becomes the final value. We can find out that the more OTP generation frequency we have, the lower probability of clash tolerance we get in our suggested algorithm, compared to the previous algorithm.

Key Words : Authentication, One Time Password, Random Number, Truncation Function, Collision Resistance

1. 서론

OTP(일회용 패스워드, One Time Password)는 무작위로 생성되는 난수의 일회용 패스워드를 이용하는 사용자 인증 방식이다. OTP는 정적인 패스워드 사용에 따른 위험을 해결하고 개인정보 유출에 따른 사용자 인증을 강화하기 위해 도입되었다. OTP 기술이 활발하게 사용되고 있는 이유는 전자적 해킹 위협의 증가로 강한 인증을 필요로 하는 요구와 함께 국내·외에서 활발하게 진행되고 있는 표준화 작업이 기술 활성화의 밑바탕이 되고

* 본 논문은 2013년 동명대학교 교내 학술연구비에 의하여 지원되었음
Received 22 October 2014, Revised 28 November 2014
Accepted 20 January 2015
Corresponding Author: Dong Ryool Kim
(Dept. of Mechatronics Engineering, Tongmyong University)
Email: drkim@tu.ac.kr

ISSN: 1738-1916

있기 때문이다. 2012년 3월 국내 전자금융 이용자중 OTP발생기를 발급받은 사람이 590만 명을 넘어섰다[1].

현재 국내외에 OTP 기반 인증기술은 전자금융 뿐 아니라 전자정부, 게임, 포털사이트 등으로 그 적용범위가 점차 늘어나고 있는 추세이다. 또한 스마트카드 환경에서 편리하게 사용가능한 USIM 기반 모바일 OTP 등의 기술 개발로 향후 OTP 기반의 인증 서비스는 계속 증가할 것으로 전망되고 있다[2].

일반적인 패스워드는 정적인 인증 수단으로 네트워크 상에서 도청으로 인해 패스워드 유출이 가능하여 불법적으로 재사용할 위험이 있다. 그러나 OTP는 이미 사용된 패스워드는 재사용 하지 않으므로 네트워크 도청을 통하여 패스워드를 알아냈다 하더라도 더 이상 사용할 수 없으므로 이러한 위험을 방지할 수 있다. OTP는 정적인 패스워드 사용에 따른 위험을 해결하고 개인정보 유출에 따른 사용자 인증을 강화하기 위해 도입되었다. OTP는 동적인 패스워드를 생성하는 OTP 토큰(Token)을 통해 비밀번호를 생성하며, OTP 생성매체에 의해 필요한 시점에 생성하고 매번 다른 번호를 생성한다[3,4,5,6].

인증 기술의 발달로 한 세션에서 패스워드 값을 사용 후 폐기하는 일회용 패스워드 값에 관한 연구가 활발히 진행되고 있다. RFC 1760 표준인 S/Key 인증방식에서는 해쉬 알고리즘인 SHA-1을 이용하여 일회용 패스워드를 생성한다. S/Key 방식은 모든 값이 평문으로 전송되어 공격자에게 쉽게 노출된다는 단점을 가지고 있다. 또한 서버의 난수인 Seed값이 동일하게 유지되기 때문에 N번의 로그인 횟수가 노출되면 공격자는 쉽게 다음 일회용 패스워드 값을 유추할 수 있다[8]. 김홍기[9]등은 기존의 일회용 패스워드에서 문제점을 해결하기위해 시간 값을 이용한 일회용 패스워드 생성 기법을 제안하였다.

최근 들어 모바일 사용자가 급속도로 증가하고 있는 상황이다. 모바일 서비스 분야는 뉴스, 자료 검색 등 정보 공유에서 게임, 쇼핑, 여행 등 정보이용 및 결재 분야로 확대되고 있다. 서비스 분야가 확대됨에 따라서 이용자에 대한 본인 확인의 필요성에 대한 요구가 더욱 증가하고 있다. 본 논문에서는 사용자 인증에 적합한 OTP 생성 알고리즘 모델을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존연구에 대하여 알아보고, 3장에서는 사용자 인증에 적합한 OTP 생성 알고리즘을 제안한다. 4장에서는 제안한 알고리즘에 대하여 비교·분석하고 5장에서 결론을 맺는다.

2. 관련연구

이 장에서는 기존 방식인 안전한 OTP 생성 알고리즘[7]으로 구성된 모바일 OTP 생성 모델을 분석한다. 사용자는 최초 자신이 '알고 있는 것'을 통해 사용자 식별 인증을 수행하게 된다. 사용자 식별 인증에 사용되는 정보로는 사용자의 ID와 PW을 사용한다. 사용자는 자신의 ID와 PW을 이용하여 식별 인증 시 본인임을 인증할 수 있다. 하지만 ID, PW만을 사용한 사용자 식별은 고정된 값으로써 타인에게 유출시 누구나 입력 할 수 있다는 문제점이 존재한다. 때문에 모바일 OTP을 이용하여 사용자를 재 인증함으로써 이중인증을 수행하여 보안을 강화하였다.

2.1 OTP 생성 방식

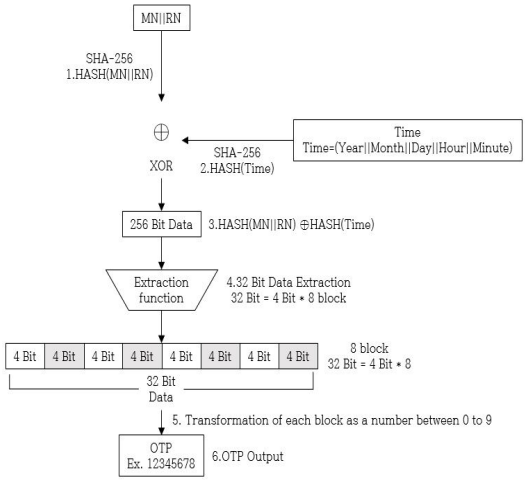
모바일 OTP에서 생성된 OTP 값은 오직 본인만이 생성 할 수 있어야 하며, 동일한 모바일 OTP을 소유한 사용자라도 타인의 OTP 값을 생성 할 수 없어야 한다. 또한 OTP 값은 일회성을 지녀야 하며, 타인이 OTP 값을 확보하게 되더라도 재사용을 통한 인증은 불가능해야 한다. 회원번호와 랜덤번호를 입력받은 모바일 OTP는 SHA-256을 이용해 256-비트의 고유 데이터를 설정하게 된다. 모바일 OTP 실행 시 256-비트의 고유 데이터는 시간 값과 함께 OTP 생성 알고리즘을 거쳐 특정 데이터 값을 생성하게 되며, 이 값은 다시 추출함수를 통하여 최종적으로 8자리의 OTP 값을 생성하게 된다.

① HASH(회원번호||랜덤번호) : 최초 모바일 OTP 실행 시 입력한 사용자의 회원번호와 WEB 서버로부터 발급 받은 랜덤번호 4자리를 SHA-256을 사용하여 256-비트의 데이터로 생성한다. 이때 HASH(회원번호||랜덤번호)는 OTP 생성 시 고유 입력 값으로써 모바일 OTP에 설정된다.

② HASH(Time) : 30초 단위로 다른 값을 생성하는 것과 동일한 시간대에 서버와 모바일 OTP의 동일한 OTP 생성을 위해 시간을 이용하여 동기화를 이룬다. 이때 Time 값은 (Year||Month||Day||

Hour||Minute)의 값을 이용하며, OTP 생성시간은 30초 단위로 이루어지므로 Second값을 읽어와 Second< 30초인 경우 Time 데이터의 첫 비트를 0으로 설정하며, Second>=30초인 경우 Time 데이터의 첫 비트 값을 1로 설정한다. 마지막으로 HASH(회원번호||랜덤번호)의 데이터와 XOR 연산을 하기 위해 SAH-256을 사용해 256-비트의 데이터로 만든다.

③ HASH(회원번호||랜덤번호) XOR HASH(Time) : 모바일 OTP의 최초 입력 값 HASH(회원번호||랜덤번호)과 Time 값을 XOR 연산함으로써 30초마다 OTP입력 값이 다르게 된다.



[Fig. 1] Flow of OTP generation

2.2 OTP 추출함수

OTP는 매 생성 시 다른 값을 추출할 수 있는 추출함수이어야 한다.

데이터를 연산에 의해 특정 비트만을 추출해 32-비트의 결과 값으로 만드는 과정이다. 이때 추출되고 남은 데이터는 모두 손실시킴으로써 제 3자로 하여금 본래의 데이터 조합이 무엇인지 알지 못하게 하며, 매 생성 시 특정 비트만을 선택하여 결과 값을 만듦으로써 OTP값 생성 시 중복되는 것을 최소화 한다.

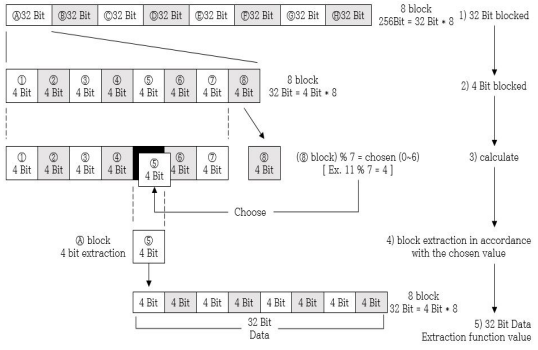
① 32-비트 블록화 : 최초 추출함수로 들어오는 256-비트 데이터를 32-비트씩 8블록으로 나눈다.

② 4-비트 블록화 : 32-비트 블록화 과정에서 나누어진 8블록 중 1블록 당 1개씩, 총 8블록에서 8개의 OTP 값을 추출한다. 이를 위해 8블록 중 첫 번째 블록을 선택하고 다시 32-비트 데이터를 4-비트씩 8블록으로 나눈다.

③ 선택 값 계산 : 4-비트씩 8블록으로 나뉜 데이터 중 마지막 8번째 블록을 선택. (8번째 블록 값 % 7) 연산을 통해 0~6 사이의 정수 값을 구한다. 이때 구해진 값은 8번째 블록을 제외한 7개의 블록 중 한 개의 블록을 선택하는 선택 값으로 사용된다.

④ 선택 값에 따른 블록 추출 : 0~6 사이의 정수 값 중 구해진 1개의 선택 값에 따라 남은 7블록 중 한 개의 특정 블록을 선택하여 추출한다.

⑤ 32-비트 Data 추출 함수 값 : 최초 256-비트 데이터 8블록을 한 블록씩 각각 나)~라)까지의 연산을 반복해 1블록(32-비트 Data)에서 특정 값 1개를 추출(4-비트 Data), 총 8블록에서 8개의 특정 값을 추출하여 구성한 32-비트 Data 추출 값을 구한다.



[Fig. 2] Truncation function

각 블록을 0~9 사이의 숫자로 변형 : 8블록의 각 4-비트 데이터들을 10진수 10으로 나누어 나머지를 구하는 방식으로 0~9사이의 10진수로써 변형한다. 이 과정을 통해 나온 8블록의 10진수들은 최종적으로 8개의 OTP 값으로 출력되게 된다.

3. OTP 생성 알고리즘 제안

OTP 생성 알고리즘은 사용자 인증에 필요한 OTP

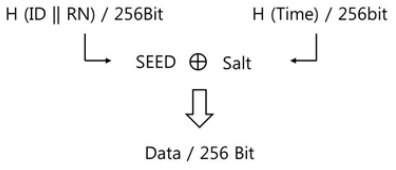
값을 생성하기 위해 입력 값을 받아 OTP Data를 생성한다. 생성된 OTP Data는 추출함수를 이용하여 최종적으로 OTP값을 얻는다.

제안하는 방법은 Seed값과 Times값을 이용하여 256-비트 크기의 OTP Data를 생성하게 된다. 생성한 OTP Data를 행렬로 나열하고 불규칙적으로 32-비트의 값을 추출하게 되는 이 값이 최종적인 OTP값이 된다.

3.1 OTP Data 생성

Seed값에서 OTP을 추출하게 되면 수회 이상 반복적으로 OTP값을 생성하여 분석하거나, SMS로 전송되는 OTP값을 분석해서 다음번에 생성될 OTP값을 예측할 수도 있다. 문제점을 보완하기 위해서 Seed값에 특정 값을 Salt하여 Data을 생성하는 방법을 제안하며, Data 생성 방법은 [Fig. 3]과 같다.

여기서, Salt란 패스워드 보호에서 패스워드 해시를 변환하는 데 사용되는 무작위 문자열을 말한다. 다른 사용자가 동일 시스템 내에서 동일한 패스워드를 사용하더라도 유일하게 식별함으로써 충돌을 방지하기 위해 해시에 첨가되며, 또한 해커들이 패스워드를 사용해 시스템에 잠입하는 것을 어렵게 하기 위해 해시에 첨가된다.



[Fig, 3] Data generation

Salt값으로 사용된 $H(Time)$은

$$H(T_0 \| T_1 \| T_2 \| \cdots \| T_7)$$

과 같다. T_i을 생성하여 연접한 후 해시함수(SHA-256)를 이용해 256-비트의 Salt값을 생성한다.

OTP값을 추출하기 위하여 생성된 Data을 비트 값으로 나타내지 않고 좌표를 이용해 256-비트의 Data을 16×16 크기의 행렬로 나열한다.

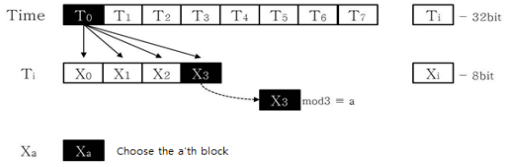
$$Build(data) = \begin{vmatrix} B_{(0,0)} & B_{(0,1)} & \cdots\cdots & B_{(0,15)} \\ B_{(1,0)} & B_{(1,1)} & \cdots\cdots & B_{(1,15)} \\ \vdots & \vdots & \vdots & \vdots \\ B_{(15,0)} & B_{(15,1)} & \cdots\cdots & B_{(15,15)} \end{vmatrix}$$

Data의 256-비트의 첫 번째 값을 $B_{(0,0)}$의 위치에, 두 번째 값을 $B_{(0,1)}$의 위치에 나열하는 과정으로 마지막 256번째 값을 $B_{(15,15)}$까지 나열한다.

3.2 OTP 추출함수 및 OTP값 생성

생성된 Data에서 T_i의 값을 이용하여 좌표 값($B_{(i,j)}$)을 선택한 다음에 OTP값을 추출한다. 이 과정을 $Coordinate()$라고 정의한다.

- 단계 1 : T_0을 8-비트씩 4개로 블록화 한다. 4개의 블록 중 X_3을 선택하여 mod 3 연산을 결과 값을 a라고 하였을 때 8-비트씩 블록화 된 나머지 3개의 블록 중 X_a을 선택하게 된다.



- 단계 2 : 나열된 행렬에서 행의 좌표를 구하기 위해서 선택된 X_a의 -1번째 블록을 선택한다. 이때 X_3블록을 선택할 수 없으며 $a-1$의 값이 -1일 경우 2로 대체한다. 즉 $X_{(a-1)\ (\mathrm{mod}\ 3)}$이고 행은 16행으로 이루어져 있으므로

$$X_{(a-1)\ (\mathrm{mod}\ 3)}(\mathrm{mod}\ 16)$$

연산을 통해 행의 좌표 값 i을 구한다.

- 단계 3 : 열의 좌표를 구하기 위해서 선택된 X_a의 +1번째 블록을 선택한다. X_3블록은 선택할 수 없으며 $a+1$ 의 값이 3일 경우 0으로 대체한다. 즉 $X_{(a+1)\ (\mathrm{mod}\ 3)}$이며 열 또한 16열로 이루어져 있으므로

$$X_{(a+1)\ (\mathrm{mod}\ 3)}\ (\mathrm{mod}\ 16)$$

연산을 통해 열의 좌표 값 j을 구한다.

- 단계 4 : 선택된 행렬 $B_{(i\ j)}$을 기준으로 행 또는 열의 값만을 증가시켜 4개의 비트를 추출하게 된다. 만약 $X_a \equiv 0\ (\mathrm{mod}\ 2)$이면

$$B_{(i,j)},\ B_{(i+1,j)},\ B_{(i+2,j)},\ B_{(i+3,j)}$$

의 비트 값을 추출하게 된다. 만약 $X_a \equiv 1 \pmod 2$ 이라면

$$B_{(i,j)},\ B_{(i,j+1)},\ B_{(i,j+2)},\ B_{(i,j+3)}$$

의 비트 값을 추출하게 된다. 이때 i 및 j의 값이 15을 넘을 경우 다시 0으로 돌아가게 된다. 즉 $X_a \equiv 0 \pmod 2$일 경우

$$B_{(i \pmod{16},\ j)},\ B_{((i+1) \pmod{16},\ j)},$$
$$B_{((i+2) \bmod 16,\ j)},\ B_{((i+3) \bmod 16,\ j)}$$

의 4개 비트를 추출하게 된다. 추출된 4개의 비트를 연접하여 C_n을 구하게 된다.

- 단계 5 : 각 T_i을 $Coordinate()$하여 추출한 C_n을 $C_n \pmod{10}$ 연산을 하여 십진수 정수로 표현을 하고 이 값들을 연접한 값이 OTP값이 된다.

4. OTP 생성 모델의 분석

제안하는 OTP 생성 알고리즘과 기존 알고리즘과의 차이점을 분석하고, 또한, 기존 알고리즘과 제안 알고리즘을 통해 생성된 OTP값의 충돌내성을 비교 분석한다.

4.1 알고리즘 분석

제안 알고리즘은 '인바운드 OOB OTP 방식'으로서 3분간의 입력 대기시간을 가지며 OTP 재생성을 요청하거나, 입력대기 시간이 초과되지 않는 이상 OTP값을 재생성 하지 않는다. OTP SEED만으로 OTP Data를 생성하면 항상 같은 값이 만들어진다. 따라서 제안 알고리즘에서는 생성된 OTP Data에 Salt를 하여 OTP값 생성 시에 매번 다른 OTP Data를 만들도록 하였다.

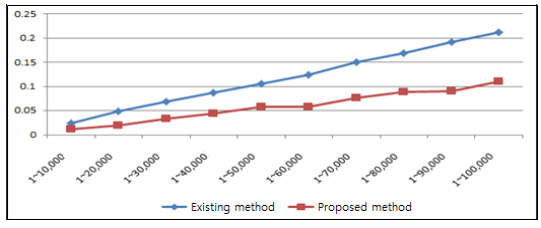
기존 알고리즘에서는 OTP Data를 알게 되면 OTP을 생성할 수 있다는 취약점이 존재한다. 하지만 제안 알고리즘에서는 Time값을 이용해 좌표 값을 얻고, 해당 좌표의 비트 값으로 OTP값을 생성한다. 따라서 OTP Data를 알게 되더라도 생성되는 OTP값을 추측하기가 어렵다. OTP값 입력 대기시간 3분이 존재하지만 최초 입력 오류 시에 OTP값은 자동적으로 삭제되어 무차별 대입 공격으로부터 안전하다.

4.2 OTP 충돌내성 분석

OTP는 일회성을 지닌 패스워드란 뜻이다. 일회성이란 매 사용 시 마다 패스워드 값을 새로이 생성함으로 이전에 생성한 값이 재사용되지 않는 것을 말한다. 하지만 사용한 값이 재사용되지 않는다면 사용할 수 있는 값들은 점차적으로 줄어들어 공격자에 의한 추측성에 대하여 안정성을 보장하지 못 하게 된다. 사용자가 8자리의 값을 가지는 OTP값을 사용할 시 99,000,000개 이상의 OTP값을 생성하게 된다면 공격자에 다음 생성되는 OTP값을 유추 할 수 있기 때문이다. 일정주기 마다 특정한 OTP값이 생성되는 것이 보인다면 공격자는 일정주기마다 생성되는 OTP값을 사용하여 공격 할 수 있다. 또한 새로 생성한 OTP값이 이전에 생성한 값과 자주 겹치게 된다면 공격자는 기존에 생성된 OTP값들을 수집하여 다음 생성되는 OTP값을 유추할 수 있다. 그러므로 새로 생성되는 OTP값은 기존에 생성된 값과 관계가 없어야 하며 잦은 중복을 일으켜서는 안 된다.

따라서 기존 알고리즘[7]과 제안 알고리즘의 충돌내성에 대해서 비교하여 분석하였다. OTP값 생성에는 동일한 사용자의 정보로 만들어진 하나의 OTP SEED를 이용하였으며, 각 알고리즘으로 생성한 OTP값 100,000개를 기준으로 충돌되는 정도를 분석하였다. 충돌내성 확률은 '(평균*100)/OTP 생성'로 계산하였다.

기존 알고리즘과 제안 알고리즘으로 생성된 각각의 OTP값의 충돌내성 확률은 [Fig. 4]과 같이 OTP 생성 횟수가 많을수록 제안하는 알고리즘이 기존 알고리즘에 비해 충돌내성이 낮음을 알 수 있다.



[Fig. 4] Compared with OTP collision resistance

5. 결론

일반적인 패스워드는 정적인 인증 수단으로 네트워크

상에서 도청으로 인해 패스워드 유출이 가능하여 불법적으로 재사용할 위험이 있다. 그러나 OTP는 이미 사용된 패스워드는 재사용하지 않으므로 네트워크 도청을 통하여 패스워드를 알아냈다 하더라도 더 이상 사용할 수 없으므로 이러한 위험을 방지할 수 있다. 최근 들어 모바일 사용자가 급속도로 증가하고 있는 상황이다. 모바일 서비스 분야는 뉴스, 자료 검색 등 정보 공유에서 게임, 쇼핑, 여행 등 정보이용 및 결재 분야로 확대되고 있다. 서비스 분야가 확대됨에 따라서 이용자에 대한 본인 확인의 필요성에 대한 요구가 더욱 증가하고 있다. 본 논문에서는 사용자 인증에 필요한 OTP 생성 알고리즘 모델에서 안전성 평가와 OTP 충돌내성이 기존 알고리즘보다 많이 향상 되었다. 따라서 제안된 모델은 다양한 본인 인증 분야에 활용될 것이다.

ACKNOWLEDGMENTS

This research was supported by the Tongmyong University of Research Grants 2013(2013A004).

REFERENCES

[1] Financial Security Agency, “Aggregate of OTP Issued Amount”, Internal data, 2012.

[2] S. H. Song, G. N. Kim, “OTP Standardization at Home and Abroad”, Review of KIISC, Vol. 22, No. 2, pp. 30-36, 2012.

[3] S. Y. Kim, S. H. Min,, H. M. Jeong, “A Study on Identification Service Model in The Mobile Environment”, Korea Internet & Security Agency, 2009.

[4] S. H. Seo, U. J. Kang, “OTP Technology and Case Studies on Domestic Banks”, Review of KIISC, Vol. 17, No. 3, 2007.

[5] D. H. Choi, S. J. Kim, D. H. Won, “One-time Password Technology Analysis and Standardization”, Review of KIISC, Vol. 17, No. 3, 2007.

[6] Financial Security Agency, “Financial Security Weekly Information”, 2006.

[7] Y. S. Jeong, S. H. Han, S. S. Shin, “A Study on Mobile OTP Generation Model”, The Journal of digital policy & management, Vol. 10, No. 2, pp. 183-191, 2012.

[8] Neil M Haller, “The S/Key One-Times Password System,” RFC 1760, 1995.

[9] H. G. Kim, I. Y. Lee, “A Study on One-time Password Authentication Scheme Enhanced Randomness”, Proceedings of the Korea Multimedia Society Conference, Vol. 13, No. 2, 2010.

김 동 률(Kim, Dong Ryool)

- 2005년 2월 : 울산대학교 수학과 (이학박사)
- 2009년 2월 : 경남대학교수학과(이학박사)
- 2011년 ~ 현재 : 동명대학교 메카트로닉스공학과 조교수
- 관심분야 : 금융보안, OPT, 암호알고리즘, 콘텐츠 보안
- E-Mail : drkim@tu.ac.kr