



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0046349
(43) 공개일자 2020년05월07일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) G06Q 20/30 (2012.01)
(52) CPC특허분류
G06Q 20/382 (2013.01)
G06Q 20/30 (2013.01)
(21) 출원번호 10-2018-0127384
(22) 출원일자 2018년10월24일
심사청구일자 2018년10월24일

(71) 출원인
동서대학교 산학협력단
부산광역시 사상구 주례로 47(주례동,
동서대학교)
(72) 발명자
이훈재
대구광역시 수성구 청호로85안길 11 선빌라 501호
오혜리
부산광역시 동구 구봉북길4번가길 9
(뒷면에 계속)
(74) 대리인
김석계

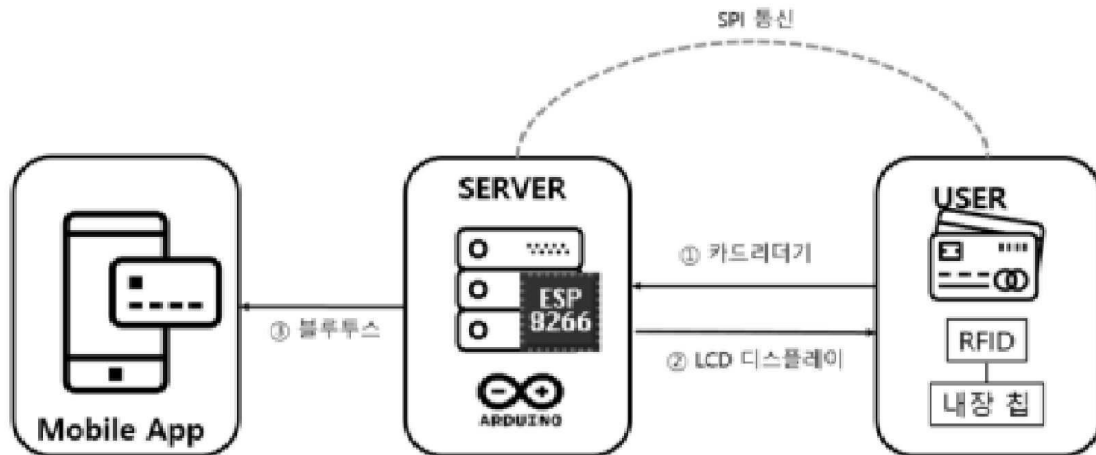
전체 청구항 수 : 총 3 항

(54) 발명의 명칭 OTP를 적용한 카드정보 제공방법

(57) 요약

본 발명 OTP를 적용한 카드정보 제공방법은 카드의 일회용 패스워드(OTP, One Time Password)를 생성하는 OTP생성단계; 상기 카드의 생성된 일회용 패스워드(OTP, One Time Password)와 UID(User ID)를 통해 OTN(One Time Number) 알고리즘을 생성하는 알고리즘 생성단계; 상기 OTN(One Time Number) 알고리즘을 통해 카드정보를 추출
(뒷면에 계속)

대표도 - 도1



하는 카드정보추출단계; 로 이루어지는 것으로,

본 발명 OTP를 적용한 카드정보 제공방법은 카드의 UID(User ID)와, 일회용 패스워드(OTP, One Time Password)를 통해 새로운 카드정보를 추출해주는 OTN(One Time Number) 알고리즘을 생성한 후, OTN(One Time Number) 알고리즘을 통해 하루 단위로 카드정보를 추출하는 것이되, 일회용 패스워드(OTP, One Time Password)는 128bit 크기 이내로 매회 변경하여 생성됨에 따라 카드정보도 매회 변경되는 것으로,

온라인, 오프라인에서 카드정보 유출을 방지하고자 카드의 카드번호가 스마트폰, PC 등의 외부장치에서 카드정보를 저장하는 등의 유출시에도 매회 카드의 카드정보가 변경되어, 외부장치에서는 카드정보의 사용이 불가능하여 네트워크 구간에서 탈취가 불가능하며, 금전적 피해 등의 악용되는 것을 방지하는 현저한 효과가 있다.

(52) CPC특허분류

G06Q 20/356 (2013.01)

(72) 발명자

김원희

부산광역시 금정구 금강로 503, 803동 201호

김현정

경상남도 김해시 전하로208번길 32

김기환

부산광역시 북구 화명대로 87 현대아파트 101동 1501호

장원태

부산광역시 북구 화명신도시로 194 화명한일유엔아이 109동 1802호

이 발명을 지원한 국가연구개발사업

과제고유번호 2018-E-G023-010100

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 사회맞춤형 산학협력 선도대학(LINC+) 육성사업

연구과제명 사회맞춤형 산학협력 선도대학(LINC+) 육성사업(산학협력 고도화형)

기 여 율 1/3

주관기관 동서대학교 산학협력단

연구기간 2017.04.01 ~ 2022.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호 1711073998

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보보호핵심원천기술개발(R&D)(국가공공정보보호인프라강화)

연구과제명 기만공격에 의한 AI 역기능 방지 기술 개발

기 여 율 1/3

주관기관 동서대학교 산학협력단

연구기간 2018.04.01 ~ 2020.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1D1A1B01011908

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공분야기초연구사업(기본연구지원사업)

기술 개발 연구과제명 사물인터넷/무인비행기(IoT/Drone)에 적합한 초경량-고속 암호/인증 및 물리적 해킹 방어

기 여 율 1/3

주관기관 동서대학교 산학협력단

연구기간 2016.06.01 ~ 2023.05.31

명세서

청구범위

청구항 1

카드의 일회용 패스워드(OTP, One Time Password)를 생성하는 OTP생성단계; 상기 카드의 생성된 일회용 패스워드(OTP, One Time Password)와 UID(User ID)를 통해 OTN(One Time Number) 알고리즘을 생성하는 알고리즘 생성단계; 상기 OTN(One Time Number) 알고리즘을 통해 카드정보를 추출하는 카드정보추출단계; 로 이루어지는 것을 특징으로 하는 OTP를 적용한 카드정보 제공방법

청구항 2

제 1항에 있어서, 상기 OTP생성단계, 알고리즘 생성단계, 및 카드정보 추출단계는 또다시 실행되는 것을 특징으로 하는 OTP를 적용한 카드정보 제공방법

청구항 3

제 2항에 있어서, 상기 일회용 패스워드(OTP, One Time Password)는 128bit의 크기를 가지는 것으로, 상기 일회용 패스워드(OTP, One Time Password)를 생성하기 위해 스트림 암호 방식을 사용하는 것을 특징으로 하는 OTP를 적용한 카드정보 제공방법

발명의 설명

기술 분야

- [0001] 본 발명은 OTP를 적용한 카드정보 제공방법에 관한 것으로, 보다 상세하게는 카드의 UID(User ID)와, 일회용 패스워드(OTP, One Time Password)를 통해 새로운 카드정보를 추출해주는 OTN(One Time Number) 알고리즘을 생성한 후, OTN(One Time Number) 알고리즘을 통해 하루 단위로 카드정보를 추출하는 것이되, 일회용 패스워드(OTP, One Time Password)는 128bit 크기 이내로 매회 변경하여 생성됨에 따라 카드정보도 매회 변경되는 것으로,
- [0002] 온라인, 오프라인에서 카드정보 유출을 방지하고자 카드의 카드번호가 스마트폰, PC 등의 외부장치에서 카드정보를 저장하는 등의 유출시에도 매회 카드의 카드정보가 변경되어, 외부장치에서는 카드정보의 사용이 불가능하여 네트워크 구간에서 탈취가 불가능하며, 금전적 피해 등의 악용되는 것을 방지하는 OTP를 적용한 카드정보 제공방법에 관한 것이다.

배경 기술

- [0004] 대부분의 국내·외 온라인 결제 방식은 일반적으로 카드 정보(카드번호, 만료 기간, CVC)와 비밀번호를 올바르게 입력할 경우 정상적으로 정산처리가 이루어진다. 만약 사용자의 실수 혹은 정교하게 만들어진 결제 페이지를 통해 위의 정보가 해커에게 유출될 경우 금전적인 손해를 가지게 되며, 유출된 정황을 감지하고 이를 보완하기 위해서는 카드를 재발급 받는 방법이 유일하며, 재발급을 받기 전까지는 결제 서비스를 이용할 수 없다.
- [0005] 최근에는 편의점에서 1000원을 결제할 때도 신용카드를 사용하는 경우가 많으며 현금보다는 체크카드 및 신용카드를 주로 사용하며, 거래방식의 변화는 생활방식과 소비패턴의 변화를 일으키고 있다. 하지만, 급격하게 카드 사용비율이 높아지면서 보안상의 문제점도 나타나고 있다.
- [0006] 몇 가지 사례로 한국 온라인 쇼핑몰에서 600여 건의 신용카드 도용사고가 발생하였으며, 업계 관계자는 마그네틱 카드에 담긴 고객 정보가 일부 유출돼 신용카드 도용사고가 벌어진 것으로 추정하였다.
- [0007] 해외구매 역시 국내 신용카드가 무더기 해킹된 정황이 포착되었으며, 정보가 유출될 경우 무단 복제, 부정사용, 카드 번호 유출 등의 위험이 심각하다.
- [0008] 실제로 미국과 중국 등에서 몇 분 간격으로 수백 달러가 결제되거나 해외 사설 주차장 등 온라인뿐만 아니라 오

프라인 가맹점에서도 부정사용 사고가 발생했다.

- [0009] 신용카드의 카드번호, CVC, 비밀번호를 알면 해커의 신용카드의 카드번호, CVC, 비밀번호를 알면 해커의 불법적인 사용을 막지 못하는 실정으로, 온라인, 오프라인에서 카드번호 유출 확률을 개선하고자 한다.
- [0010] 최근에는 체크·신용카드 등의 오프라인의 카드 이외에 삼성페이, 애플페이 등의 스마트 페이, 즉 온라인전용 결제방식으로 결제하는 추이가 늘어나고 있으며, 추가적으로 비트코인을 사용하여 결제하는 전자지갑 앱, QR코드 스캔으로 결제하는 카카오페이 등 다양한 결제 방식이 등장하고 있다. 이처럼 다양한 결제 방식이 등장하면서 일반결제 방식의 안전성을 보완할 방법이 필요하다.
- [0011] 종래기술로서 등록특허공보 등록번호 제10-1099441호의 신용카드 결제데이터의 불법조작을 방지하기 위한 신용카드 결제 시스템 및 그 방법에는, 상호 간에 통신망으로 연결되어 있는 신용카드결제기, 뱅크(VAN)서버 및 카드사서버를 포함하는 신용카드 결제시스템으로서, 상기 뱅크서버는 신용카드거래 승인시마다 승인번호와는 구분되는 별도의 고유 일련번호인 비노출승인번호를 생성 발급하여 상기 신용카드결제기로 전송해 주고, 신용카드거래 승인취소시 기발급한 상기 비노출승인번호를 상기 신용카드결제기에 요청하고 전송받아, 자체 보관하고 있는 비노출승인번호와 상기 전송받은 비노출승인번호의 상호 일치 여부를 판별하여 승인취소 진행 여부를 결정하는 비노출정보 처리모듈; 및 상기 비노출정보 처리모듈이 발급한 상기 비노출승인번호를 저장 보관하는 데이터저장부를 포함하는 것을 특징으로 하는 신용카드 결제데이터의 불법조작을 방지하기 위한 신용카드 결제 시스템이라고 기재되어 있다.
- [0012] 다른 종래기술로서 등록특허공보 등록번호 제10-1320668호의 보안성이 향상된 신용카드 결제 서비스 제공방법에는, 신용카드 단말기 및 VAN 서버를 포함하여 신용거래를 승인하는 방법에 있어서, (a) 신용카드 단말기를 구동하는 소프트웨어를 인증하는 프로그램인증단계; (b) 신용카드 단말기 시스템과 서버가 최초로 통신할 때, 상기 신용카드 단말기 시스템을 인증하여 인증서를 발급하는 사용인증단계; (c) 결제정보와 인증서를 포함하여 신용거래승인을 요청하는 승인요청단계; (d) 상기 인증서와 매칭되는 신용카드 단말기의 하드웨어정보가 있을 경우에만 승인요청에 대하여 승인하는 승인단계; 를 포함하되, 상기 신용카드 단말기 시스템은 상기 신용카드 단말기와 상기 소프트웨어를 포함하는 것인 보안성이 향상된 신용카드 결제 서비스 제공방법이라고 기재되어 있다.
- [0013] 그러나 상기와 같은 종래의 구성은 신용카드의 카드번호, 카드인증코드(CVC, Card Verification Code), 비밀번호를 유출당하면 불법적인 사용을 막지 못하는 단점이 있었다.

발명의 내용

해결하려는 과제

- [0015] 따라서 본 발명 OTP를 적용한 카드정보 제공방법을 통하여, 카드의 UID(User ID)와, 일회용 패스워드(OTP, One Time Password)를 통해 새로운 카드정보를 추출해주는 OTN(One Time Number) 알고리즘을 생성한 후, OTN(One Time Number) 알고리즘을 통해 하루 단위로 카드정보를 추출하는 것이되, 일회용 패스워드(OTP, One Time Password)는 128bit 크기 이내로 매회 변경하여 생성됨에 따라 카드정보도 매회 변경되는 것으로,
- [0016] 온라인, 오프라인에서 카드정보 유출을 방지하고자 카드의 카드번호가 스마트폰, PC 등의 외부장치에서 카드정보를 저장하는 등의 유출시에도 매회 카드의 카드정보가 변경되어, 외부장치에서는 카드정보의 사용이 불가능하여 네트워크 구간에서 탈취가 불가능하며, 금전적 피해 등의 악용되는 것을 방지하는 OTP를 적용한 카드정보 제공방법을 제공하고자 하는 것이다.

과제의 해결 수단

- [0018] 본 발명 OTP를 적용한 카드정보 제공방법은 카드의 일회용 패스워드(OTP, One Time Password)를 생성하는 OTP생성단계; 상기 카드의 생성된 일회용 패스워드(OTP, One Time Password)와 UID(User ID)를 통해 OTN(One Time Number) 알고리즘을 생성하는 알고리즘 생성단계; 상기 OTN(One Time Number) 알고리즘을 통해 카드정보를 추출하는 카드정보추출단계; 로 이루어지는 것을 특징으로 한다.

발명의 효과

- [0020] 본 발명 OTP를 적용한 카드정보 제공방법은 카드의 UID(User ID)와, 일회용 패스워드(OTP, One Time Password)를 통해 새로운 카드정보를 추출해주는 OTN(One Time Number) 알고리즘을 생성한 후, OTN(One Time Number) 알고리즘을 통해 하루 단위로 카드정보를 추출하는 것이지, 일회용 패스워드(OTP, One Time Password)는 128bit 크기 이내로 매회 변경하여 생성됨에 따라 카드정보도 매회 변경되는 것으로,
- [0021] 온라인, 오프라인에서 카드정보 유출을 방지하고자 카드의 카드번호가 스마트폰, PC 등의 외부장치에서 카드정보를 저장하는 등의 유출시에도 매회 카드의 카드정보가 변경되어, 외부장치에서는 카드정보의 사용이 불가능하여 네트워크 구간에서 탈취가 불가능하며, 금전적 피해 등의 악용되는 것을 방지하는 현저한 효과가 있다.

도면의 간단한 설명

- [0023] 도 1은 본 발명 OTP를 적용한 카드정보 제공방법의 신용카드 일련번호 변경을 위한 작동원리를 전체적인 시스템 구성도
- 도 2는 본 발명 OTP를 적용한 카드정보 제공방법의 서버에서 수행되는 연산과정을 나타내는 순서도
- 도 3은 본 발명 OTP를 적용한 카드정보 제공방법의 OTN(One Time Number) 알고리즘에 대한 개념도
- 도 4는 본 발명 OTP를 적용한 카드정보 제공방법의 카드번호로 사용되는 일련번호 출력결과를 나타내는 개념도
- 도 5는 본 발명 OTP를 적용한 카드정보 제공방법의 스마트기기 어플리케이션을 통한 카드번호 출력결과 개념도
- 도 6은 본 발명 OTP를 적용한 카드정보 제공방법의 서버에서 연산된 카드번호 나타내는 개념도

발명을 실시하기 위한 구체적인 내용

- [0024] 본 발명 OTP를 적용한 카드정보 제공방법은 카드의 일회용 패스워드(OTP, One Time Password)를 생성하는 OTP생성단계; 상기 카드의 생성된 일회용 패스워드(OTP, One Time Password)와 UID(User ID)를 통해 OTN(One Time Number) 알고리즘을 생성하는 알고리즘 생성단계; 상기 OTN(One Time Number) 알고리즘을 통해 카드정보를 추출하는 카드정보추출단계; 로 이루어지는 것을 특징으로 한다.
- [0025] 또한, 상기 OTP생성단계, 알고리즘 생성단계, 및 카드정보 추출단계는 반복 실행되는 것을 특징으로 한다.
- [0026] 또한, 상기 일회용 패스워드(OTP, One Time Password)는 128bit의 크기를 가지는 것으로, 상기 일회용 패스워드(OTP, One Time Password)를 생성하기 위해 스트림 암호 방식을 사용하는 것을 특징으로 한다.
- [0029] 본 발명을 첨부 도면에 의해 상세히 설명하면 다음과 같다.
- [0030] 도 1은 본 발명 OTP를 적용한 카드정보 제공방법의 신용카드 일련번호 변경을 위한 작동원리를 전체적인 시스템 구성도, 도 2는 본 발명 OTP를 적용한 카드정보 제공방법의 서버에서 수행되는 연산과정을 나타내는 순서도, 도 3은 본 발명 OTP를 적용한 카드정보 제공방법의 OTN(One Time Number) 알고리즘에 대한 개념도, 도 4는 본 발명 OTP를 적용한 카드정보 제공방법의 카드번호로 사용되는 일련번호 출력결과를 나타내는 개념도, 도 5는 본 발명 OTP를 적용한 카드정보 제공방법의 스마트기기 어플리케이션을 통한 카드번호 출력결과 개념도, 도 6은 본 발명 OTP를 적용한 카드정보 제공방법의 서버에서 연산된 카드번호 나타내는 개념도이다.
- [0031] 본 발명에 대해 구체적으로 기술하면, 본 발명 OTP를 적용한 카드정보 제공방법은
- [0032] 카드의 일회용 패스워드(OTP, One Time Password)를 생성하는 OTP생성단계;
- [0033] 상기 카드의 생성된 일회용 패스워드(OTP, One Time Password)와 UID(User ID)를 통해 OTN(One Time Number) 알고리즘을 생성하는 알고리즘 생성단계;
- [0034] 상기 OTN(One Time Number) 알고리즘을 통해 카드정보를 추출하는 카드정보추출단계; 로 이루어지는 것이다.

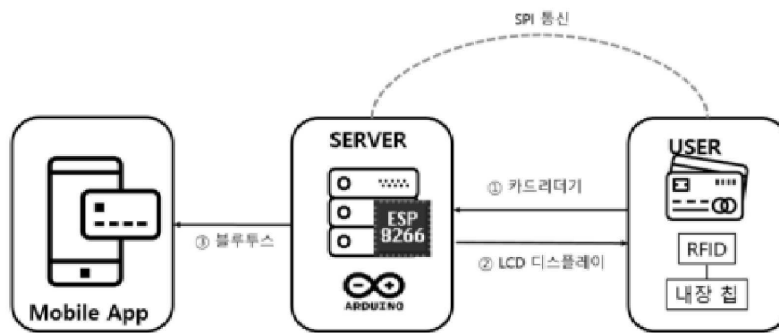
- [0036] 일실시예로써, 상기 OTP생성단계, 알고리즘 생성단계, 및 카드정보 추출단계는 서버에서 처리하는 것이며, 상기 서버에서 처리된 카드정보는 서버에 등록된 장치의 요청에 따라 전송되는 것이다. 이때, 상기 서버에 등록된 장치는 카드, 스마트기기(스마트폰 등) 등인 것이다.
- [0037] 다른 실시예로써, 상기 OTP생성단계만 서버에서 처리하여, 일회용 패스워드(OTP, One Time Password)를 서버에 등록된 장치로 보내며, 상기 서버에 등록된 장치에서 알고리즘 생성단계 및 카드정보 추출단계를 진행할 수 도 있다.
- [0039] 이때, 상기 서버에 등록된 장치에서는 디스플레이가 형성되어 카드정보를 출력할 수 있는 것이다.
- [0041] 한편, 상기 OTP생성단계, 알고리즘 생성단계, 및 카드정보 추출단계는 일정 조건에 따라 또다시 실행되는 것으로, 예를들면, 상기 일정 조건은 1분, 1시간, 1일 등의 일정 시간마다이거나, 또는 카드정보가 1회, 3회 등의 일정 횟수 사용된 후인 것이다.
- [0043] 상기 UID(User ID)는 카드마다 다르게 되어있는 식별할 수 있는 고유 번호인 것이다.
- [0044] 상기 일회용 패스워드(OTP, One Time Password)는 128bit의 크기를 가지는 것으로, 상기 일회용 패스워드(OTP, One Time Password)를 생성하기 위해 스트림 암호 방식을 사용하며, 스트림 암호 방식은 고속 처리가 되어, 고속 통신이 가능하므로 통신 지연이 없어 실시간으로 이루어지는 통신에 사용되는 것이다.
- [0045] 상기 스트림 암호 방식의 알고리즘은 이진 키 수열의 배타적 논리합(XOR) 연산과 이진화된 평문을 실행하여 암호문을 생성하는 것이다.
- [0046] 특히, 상기 스트림 암호 방식은 암호화할 입력값과 난수열을 독립적으로 생성하는 경우, 동기식 스트림 암호, 입력값과 난수열 생성에 영향을 끼치는 경우 비동기식 스트림 암호 방식으로 분류할 수 있으며,
- [0047] 본 발명에서는 상기 스트림 암호 방식으로 동기식 스트림 암호인 일회용 패스워드(OTP, One Time Password)를 사용하는 것이다.
- [0049] 상기 OTN(One Time Number) 알고리즘은 사용자의 카드 일련번호를 변경하기 위해 OTP를 활용하여 카드정보와 혼합하여 임시 정보를 생성하는 알고리즘인 것이되,
- [0050] 하기의 식 1과 같이 일회용 패스워드(OTP, One Time Password)를 생성하는 방법으로, 고객 고유 정보(Seed)와 카드 번호(Card Number)를 혼합하여 128비트(bit) LSTM(Long Short-Term Memory)의 초기값으로 활용한 후, 현재 시간(Time) 정보를 통해 임의의 횟수만큼 LSTM(Long Short-Term Memory)을 동작시키고, 동작이 끝나면 LSTM(Long Short-Term Memory)에 저장된 정보는 무작위로 섞인 상태가 되고, 해당 정보는 서버와, 서버에 등록되며 사용자가 가진 장치에서만 알 수 있게 되는 것이다.
- [0051] [식 1]
$$OTP_i = LSTM(Seed_{user} + CardNumber_{user})_{Time}$$
- [0053] 상기 서버에서 사용자에게 16자리의 카드번호 가운데 8자리 번호를 생성하기 위하여 LSTM(Long Short-Term Memory)의 주소를 임의로 선정하고, 동시에 사용자가 서버에게 남은 카드번호를 생성하기 위하여 임의의 위치 정보를 선정한다.
- [0054] 위의 과정을 도 4와 도 5에 도시된 바와 같이, 서버에 등록된 장치로써 아두이노 또는 스마트기기를 통해 구현과 동작이 가능한 것이며, 도 6처럼 사용자들에게 직관적으로 카드번호를 출력할 수 있는 것이다.
- [0056] 그러므로 상기 OTN(One Time Number) 알고리즘과 카드를 결합하여, 사용자의 카드번호, 고객정보 등의 정보가 외부로 유출되어 악용되는 상황을 방지하고, 실시간으로 사용자가 16자리 카드번호가 변경되는 것을 확인할 수 있도록 제공하며, 하드웨어 모듈을 핵심적인 기술만 가진 카드정보의 크기로 줄여 카드 보안 체계 강화 외에 전

자인증, 공인인증, 사물인터넷(IoT)분야에 활용하여 사용자에게 편리함을 줄 수 있다.

- [0059] 따라서 본 발명 OTP를 적용한 카드정보 제공방법은 카드의 UID(User ID)와, 일회용 패스워드(OTP, One Time Password)를 통해 새로운 카드정보를 추출해주는 OTN(One Time Number) 알고리즘을 생성한 후, OTN(One Time Number) 알고리즘을 통해 하루 단위로 카드정보를 추출하는 것이되, 일회용 패스워드(OTP, One Time Password)는 128bit 크기 이내로 매회 변경하여 생성됨에 따라 카드정보도 매회 변경되는 것으로,
- [0060] 온라인, 오프라인에서 카드정보 유출을 방지하고자 카드의 카드번호가 스마트폰, PC 등의 외부장치에서 카드정보를 저장하는 등의 유출시에도 매회 카드의 카드정보가 변경되어, 외부장치에서는 카드정보의 사용이 불가능하여 네트워크 구간에서 탈취가 불가능하며, 금전적 피해 등의 악용되는 것을 방지하는 현저한 효과가 있다.

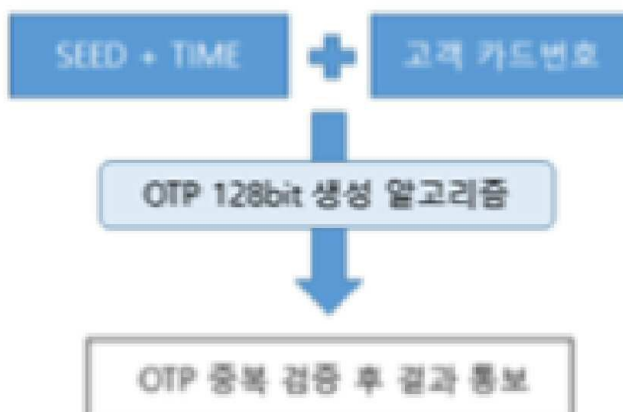
도면

도면1

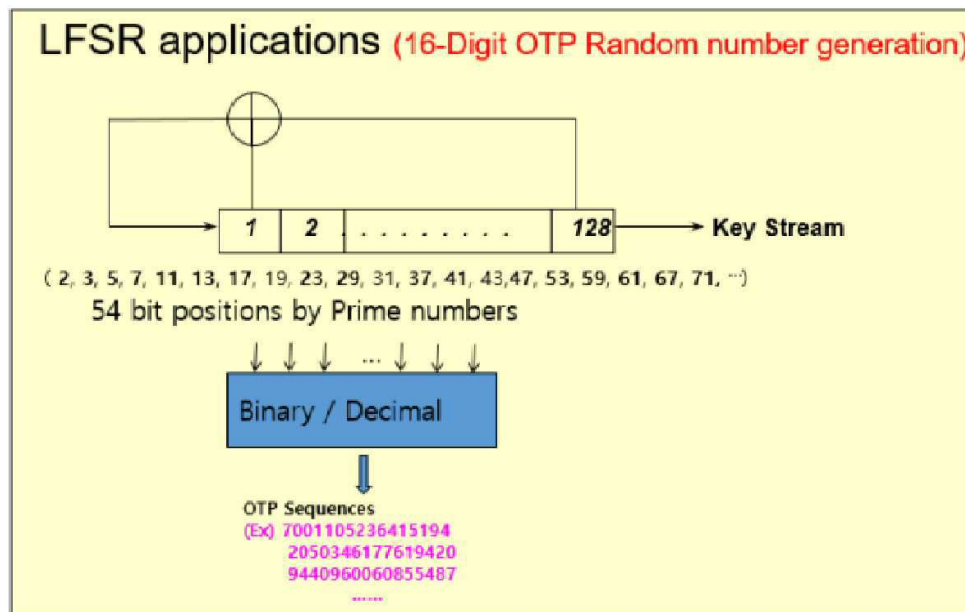


도면2

<SERVER 확대- 사용자 카드번호 이용한 OTP>



도면3



도면4

```

5 step: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
Shift move : |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
OTP result : | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
number result : 0 0 0 0 0 0 0 0 0 0 1024 3072 3072 11264
-----

6 step: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
Shift move : |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
OTP result : | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
number result : 0 0 4 12 28 28 28 28 28 28 1052 1052 1052 10
-----
1052

7 step: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
Shift move : |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
OTP result : | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
number result : 1 1 1 9 25 57 57 57 57 569 1593 3641 3641 36
-----
3641

8 step: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
Shift move : |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
OTP result : | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
number result : 0 2 2 10 10 10 74 74 74 74 1098 1098 5194 51
-----
5194

7001 1052 3641 5194

```

도면5



도면6

