(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년03월31일
(11) 등록번호 10-1506564
(24) 등록일자 2015년03월23일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01)
(21) 출원번호 10-2014-0001866
(22) 출원일자 2014년01월07일
심사청구일자 2014년01월07일
(56) 선행기술조사문헌
KR101297936 B1
KR1020080054649 A

(73) 특허권자
한밭대학교 산학협력단
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
(72) 발명자
김은기
XXXXXXXXXXXXXXXXXXX
백민호
XXXXXXXXXXXXXXXXXXX
(뒷면에 계속)
(74) 대리인
추혁, 박종경, 원성수

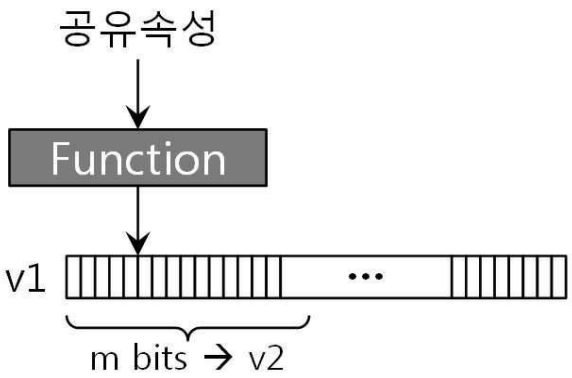
전체 청구항 수 : 총 3 항 심사관 : 문형섭

(54) 발명의 명칭 **공개키 기반 파라미터 자동생성기법**

(57) 요 약

본 발명은 공개키 기반 파라미터 자동생성기법에 관한 것으로서, 사용자들간 통신에 있어 공유되는 공유속성을 정의하고, 공유속성을 함수처리하여 해시함수값을 출력하고, 해시함수값으로부터 미리 설정된 비트값을 결정하고, 비트값에서 가장 가까운 소수를 소수 p로 정의하고, 원시근 a값을 5 또는 2로 하여, 계산된 p와 a값이 디페-헬만(Diffie-Hellman) 파라미터로 사용될 수 있는지를 확인하여 원시근 a를 정의한다. 본 발명에 따르면, 사용자간 키 교환을 위해 수행하는 연산에 있어 상호 공유속성을 통해 미리 비밀키를 생성 및 관리함으로써, 비밀키를 생성하기 위한 연산 시간을 감소시킬 수 있으며, 이에 따라 키 교환에 요구되는 시간을 실시간으로 단축시킬 수 있다.

대 표 도 - 도1



(72) 발명자

강정하

XXXXXXXXXXXXXXXXXXX

안재원

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

최범진

XXXXXXXXXXXXXXXXXXXXXXXXX

이 발명을 지원한 국가연구개발사업

과제고유번호 2013H1B8A2032154

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 2013년 지역혁신인력양성사업

연구과제명 IEEE p1609.2 Version 2 규격의 WAVE 보안 시스템 구현

기 여 율 1/2

주관기관 한밭대학교 산학협력단

연구기간 2013.05.01 ~ 2016.04.30

이 발명을 지원한 국가연구개발사업

과제고유번호 C0199293

부처명 중소기업청

연구관리전문기관 (사)한국산학연협회

연구사업명 2014년 산학협력 기술개발사업

연구과제명 하이패스 서비스 기반 eSafety 융복합형 단거리 전용 무선통신 단말 개발

기 여 율 1/2

주관기관 한밭대학교 산학협력단

연구기간 2014.06.01 ~ 2015.05.31

특허청구의 범위

청구항 1

사용자들간 통신에 있어 공유되는 공유속성을 정의하는 단계;

상기 공유속성을 함수처리하여 해시함수값을 출력하는 단계;

상기 해시함수값으로부터 미리 설정된 비트값을 결정하는 단계;

상기 비트값에서 가장 가까운 소수를 소수 p로 정의하는 단계; 및

원시근 a값을 5 또는 2로 하여, 계산된 p와 a값이 디페-헬만(Diffie-Hellman) 파라미터로 사용될 수 있는지를 확인하여 원시근 a를 정의하는 단계를 포함하는 공개키 기반 파라미터 자동생성기법.

청구항 2

공유속성을 해시한 해시함수값으로부터 미리 설정된 비트값을 결정하는 단계;

상기 비트값이 소수인지를 판단하는 단계;

상기 비트값이 소수가 아니면 비트값에서 1을 빼는 연산을 계속 수행하고, 상기 비트값이 소수이면 제1원시근인 5를 선택하는 단계;

상기 제1원시근인 5가 상기 비트값의 원시근인지를 판단하는 단계;

상기 제1원시근인 5가 상기 비트값의 원시근인 경우에는 상기 비트값과 제1원시근을 선택하고, 상기 제1원시근인 5가 상기 비트값의 원시근이 아닐 경우에는 제2원시근인 2를 선택하는 단계;

상기 제2원시근인 2가 상기 비트값의 원시근인지를 판단하는 단계; 및

상기 제2원시근인 2가 상기 비트값의 원시근인 경우에는 상기 비트값과 제2원시근을 선택하고, 상기 제2원시근인 2가 상기 비트값의 원시근이 아닌 경우에는 상기 비트값에서 1을 빼는 연산을 계속 수행하는 단계를 포함하는 공개키 기반 파라미터 자동생성기법.

청구항 3

제1항 또는 제2항에 있어서,

상기 공유속성은, 일정 비트로 정의된 블록들의 조합으로 구성되고, 각 블록들이 상호 연결되어 연속적으로 정의되는 공개키 기반 파라미터 자동생성기법.

명 세 서

기 술 분 야

[0001] 본 발명은 공개키 암호화 기법에 관한 것으로, 더욱 상세하게는 상호 공유속성을 이용하여 공개키 기반 암호화를 위한 파라미터를 자동생성하는 공개키 기반 파라미터 자동생성기법에 관한 것이다.

배 경 기 술

[0002] 상호 통신의 보안에 있어, 인증된 키 교환은 매우 중요한 문제 가운데 하나이다. 키 교환 프로토콜은 분배된 키를 소유한 사용자들간 보안을 수행할 수 있는 방법 중 하나이다. 이러한 키 교환 프로토콜에 어떤 의도된 사용자들에 대한 상호 인증을 제공하는 키 교환 프로토콜을 인증된 키 교환(AKA) 프로토콜이라 한다. 다양한 인증기법들 중 전형적인 인증서 기반의 공개키 기반 구조(Public Key Infrastructure, PKI)는 인증하고자 하는 상대

방의 공개키에 대하여 신뢰 기관으로부터 발급된 인증서를 기반으로 한다.

[0003] 최근 표준안에 제안된 키 교환 프로토콜은 공개키 암호 시스템을 이용하는 두 실체로 구성된 프로토콜로서, 안전성은 디피-헬만(diffie-hellman) 문제의 어려움에 기반을 두고 있다. 디피-헬만 문제는 소수 p을 위수로 하는 순환군 G에서 생성원에 대하여 G의 원소 a^x와 a^y가 주어졌을 때 a^{xy}를 발견하는 문제이다.

[0004] 이 문제는 널리 연구된 이산 대수 문제와 거의 동일한 문제로 알려져 있다. 이산 대수 문제는 소수 p을 위수로 하는 순환군 G에서 생성원 a에 대하여 a^x가 주어졌을 때 x를 발견하는 문제로 계산적으로 다루기 어려운 문제이다.

[0005] 이와 같이, 디피-헬만은 미리 공유하고 있는 암호 없이 간단한 정수 계산만을 통해 키 일치를 수행할 수 있으나, 메시지 재사용 공격(Message Replay Attack), 메시지 재전송 공격(Message Redirection Attack) 등과 같은 Man-In-The-Middle 공격, 메시지 변조 공격(Degenerate Message Attack) 등과 같은 정수론에 기반한 공격에 취약하며, 분산 컴퓨팅과 컴퓨팅 능력의 향상에 따라 이러한 공격들이 용이해지고 있다. 그에 반해 유비쿼터스 네트워크로 진화하기 위해서는 사용자 휴대장치 및 통신 시스템 구성 요소들은 전력 사용 및 메모리의 제한을 가지게 된다.

[0006] 통신에 참여하는 사용자들이 소수 p와 원시근 a를 공유함에 있어, 소수 p와 원시근 a를 한쪽 사용자가 생성하여 상대방 사용자에게 전송하거나, 게시판 등에 소수 p와 원시근 a를 게시함으로써 이러한 공격들이 더욱 용이해질 수 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 공개특허공보 제10-2012-0097729호(공개일 2012.09.05.)

발명의 내용

해결하려는 과제

[0008] 따라서, 본 발명은 상기한 종래 기술의 문제점을 해결하기 위해 이루어진 것으로서, 본 발명의 목적은 상호 공유속성을 이용하여 공개키 기반 암호화를 위한 파라미터를 자동생성하는 공개키 기반 파라미터 자동생성기법을 제공하는데 있다.

과제의 해결 수단

[0009] 상기와 같은 목적을 달성하기 위한 본 발명의 공개키 기반 파라미터 자동생성기법은, 사용자들간 통신에 있어 공유되는 공유속성을 정의하는 단계; 상기 공유속성을 함수처리하여 해시함수값을 출력하는 단계; 상기 해시함수값으로부터 미리 설정된 비트값을 결정하는 단계; 상기 비트값에서 가장 가까운 소수를 소수 p로 정의하는 단계; 및 원시근 a값을 5 또는 2로 하여, 계산된 p와 a값이 디페-헬만(Diffie-Hellman) 파라미터로 사용될 수 있는지를 확인하여 원시근 a를 정의하는 단계를 포함하는 것을 특징으로 한다.

[0010] 한편, 본 발명의 공개키 기반 파라미터 자동생성기법은, 공유속성을 해시한 해시함수값으로부터 미리 설정된 비트값을 결정하는 단계; 상기 비트값이 소수인지를 판단하는 단계; 상기 비트값이 소수가 아니면 비트값에서 1을 빼는 연산을 계속 수행하고, 상기 비트값이 소수이면 제1원시근을 선택하는 단계; 상기 비트값과 제1원시근이 적절한가를 판단하는 단계; 상기 비트값과 제1원시근이 적절할 경우에는 상기 비트값과 제1원시근을 선택하고, 상기 비트값과 제1원시근이 적절하지 않을 경우에는 제2원시근을 선택하는 단계; 상기 비트값과 제2원시근이 적절한가를 판단하는 단계; 및 상기 비트값과 제2원시근이 적절할 경우에는 상기 비트값과 제2원시근을 선택하고, 상기 비트값과 제1원시근이 적절하지 않을 경우에는 상기 비트값에서 1을 빼는 연산을 계속 수행하는 단계를 포

함하는 것을 특징으로 한다.

[0011] 상기 공유속성은, 일정 비트로 정의된 블록들의 조합으로 구성되고, 각 블록들이 상호 연결되어 연속적으로 정의되는 것이 바람직하다.

발명의 효과

[0012] 상술한 바와 같이, 본 발명에 의한 공개키 기반 파라미터 자동생성기법에 따르면, 사용자간 키 교환을 위해 수행하는 연산에 있어 상호 공유속성을 통해 미리 비밀키를 생성 및 관리함으로써, 비밀키를 생성하기 위한 연산 시간을 감소시킬 수 있으며, 이에 따라 키 교환에 요구되는 시간을 실시간으로 단축시킬 수 있다.

[0013] 또한, 암호화된 스트리밍 서비스를 제공하는 통신기기에 적용할 경우, 서비스 통신기기에 서비스를 요청하는 다수의 통신기기에 대하여 신속하게 응답할 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예로서, 공유속성 데이터를 함수처리하여 v_1과 v_2를 구하는 과정을 나타낸 도면이다.

도 2는 본 발명의 일 실시예로서, v_2를 이용하여 p와 a를 정하는 흐름도이다.

도 3은 본 발명의 일 실시예로서, 해시함수의 내부처리 개념도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 본 발명은 상호 공유속성들, 예를 들어 송수신측 IP 주소, 날짜, 시간, 위치 등을 포함하는 상호 공통으로 인식할 수 있는 정보를 이용하여 소수 p와 원시근 a를 생성하여 공개키 기반 암호화가 이루어지는 것을 특징으로 한다.

[0016] 한편, 본 발명의 설명에 있어, Diffie-Hellman 키 교환 프로토콜에 대해 먼저 설명한 후, 본 발명의 공개키 기반 파라미터 자동생성기법에 대해 설명하기로 한다.

[0017] Diffie-Hellman 키 교환 프로토콜은, 예를 들어, 앨리스(Alice)와 밥(Bob)과 같은 쌍방 또는 엔티티들은 공통 모듈러스 p와 단위군(group of units)의 큰 부분군의 생성원 a 모듈로 p의 이용에 동의하면, 통상 Diffie-Hellman, D-H는 소수 모듈러스로써 연산하지만, 비소수 모듈러스가 여기에서 이용된다. 일반적으로, 앨리스와 밥은 각기 그들의 비밀키들 x 및 y를 선택하고, 각각 $A = a^x \pmod p$ 및 $B = a^y \pmod p$을 계산하고, A와 B를 교환한다. 그리고 나서 앨리스는 공유 비밀 $S = B^x \pmod p \equiv a^{xy} \pmod p$을 계산할 수 있고, 또한 밥도 공유 비밀 $S = A^y \pmod p \equiv a^{xy} \pmod p$을 계산할 수 있다. 도청자들은 일반적으로 이산 대수 문제 모듈로 p를 풀지 않고서는 S를 계산할 수 없다.

[0018] 이산 대수들에 기초하는 시스템을 이용하는 디지털 서명에 두 개의 부분이 일반적으로 존재한다. 하나는 임시키이고, 나머지 하나는 Diffie-Hellman 공유 비밀 S로부터 유도되는 대칭키를 이용하여 서명되는 문서이다. 임시키는 일반적으로 큰값을 가지며, 이는 서명자, 예를 들어 앨리스가, 이를 무작위로 선택된 비밀키로부터 생성한다.

[0019] 이하, 본 발명의 공개키 기반 파라미터 자동생성기법에 대하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[0020] 도 1은 본 발명의 일 실시예로서, 공유속성 데이터를 함수처리하여 v_1과 v_2를 구하는 과정을 나타낸 도면이다.

[0021] 도 1을 참조하면, 사용자들간 통신에 의해 특정속성을 공유하게 된다. 이하, 특정속성을 "공유속성"이라 한다.

[0022] 공유속성 데이터에 대해 양측 사용자간 약속 등에 의해 특정 공유속성 데이터를 정의하게 된다.

[0023] 공유속성 데이터가 정의되면 함수처리를 통해 해시함수값 v_1을 출력한다. v_1은 최소 1024 비트 이상이다.

[0024] 이어서 해시함수값 v_1은 미리 약속된 정의에 따라 비트값을 결정하게 되고, 이 비트값에 가장 가까운 소수를 소수 p로 정의하게 된다.

[0025] 이어서, 원시근 a값을 5 또는 2로 하여, 계산된 p와 a값이 디페-헬만(Diffie-Hellman) 파라미터로 사용될 수 있는지를 확인하여 원시근 a를 정의한다.

[0026] 도 1에 도시된 바와 같이, n비트(=v_1)의 해시함수값 중에서 앞쪽 m비트(=v_2)를 임의로 설정한다.

[0027] v_2에 가장 가까운 소수를 p로 정의한다.

[0028] 원시근 a값을 5 또는 2로 하여, 계산된 p와 a값이 디페-헬만(Diffie-Hellman) 파라미터로 사용될 수 있는지를 확인하여 원시근 a를 정의한다.

[0029] 이와 같은 본 발명의 공개키 기반 파라미터 자동생성기법은 상호 공유속성들, 예를 들어 송수신측 IP 주소, 날짜, 시간, 위치 등을 포함하는 상호 공통으로 인식할 수 있는 정보를 이용하여 소수 p와 원시근 a를 생성하게 된다. 물론, 숫자 시퀀스, 선택된 번호, 알파벳 또는 숫자문자 워드, 심볼 문자들, 또는 이들의 조합을 통해 상호 공유속성들을 정의할 수 있다. 이후, 모듈러스 p와 알려진 인수들의 구성을 통해 소수 p와 원시근 a를 공개시키지 않고서도 비밀키 생성 및 암호화가 가능하다.

[0030] 도 2는 본 발명의 일 실시예로서, v_2를 이용하여 p와 a를 정하는 흐름도이다.

[0031] 도 2를 참조하면, 먼저 m비트(=v_2)가 소수인지를 판단한다(S1).

[0032] v_2가 소수가 아니라고 판단되면 v_2에서 1을 빼는 연산을 계속 수행한다(S2).

[0033] 한편, v_2가 소수이면, p=v_2, a=5로 설정한다(S3).

[0034] 소수 p와 원시근 a가 적절한가를 판단한다(S4).

[0035] 소수 p와 원시근 a가 적절하면 소수 p와 원시근 a를 선택한다(S7).

[0036] 한편, 소수 p와 원시근 a가 적절하지 않다고 판단되면, 원시근 a=2로 변경한다(S5).

[0037] 소수 p와 원시근 a가 적절한가를 판단한다(S6).

[0038] 소수 p와 원시근 a가 적절하면 소수 p와 원시근 a를 선택한다(S7).

[0039] 한편, 소수 p와 원시근 a가 적절하지 않다고 판단되면 v_2에서 1을 빼는 연산을 수행하고(S2), 리턴한다.

[0040] 도 3은 본 발명의 일 실시예로서, 해시함수의 내부처리 개념도이다.

[0041] 도 3을 참조하면, 일정 비트로 정의된 블록들이 조합되며, 각 블록들은 상호 연결되어 연속적으로 정의되게 된다.

[0042] 실시예

[0043] 제1 단말기와 제2 단말기간 미리 정의된 설정에 따라 공유속성을 결정한다.

[0044] 공유속성에 대응하여 제1 단말기와 제2 단말기가 디피 헬만(Diffie-Hellman) 키 교환 변수인 소수 p와 원시근 a를 구한다.

[0045] 제1 단말기와 제2 단말기는 통신 세션에 대한 비밀키를 각각 선택한다.

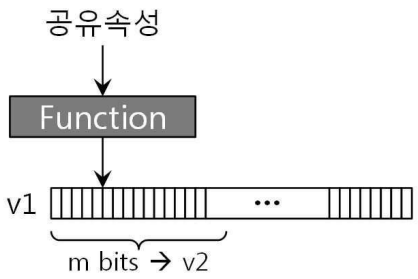
[0046] 제1 단말기와 제2 단말기는 비밀키, 소수 p 및 원시근 a을 이용하여 공개키를 생성하여 상호 단말기로 전송한다.

[0047] 이에 제1 단말기와 제2 단말기는 자신의 비밀키를 이용하여 공유 비밀 S를 계산하여 보안 통신을 수행한다.

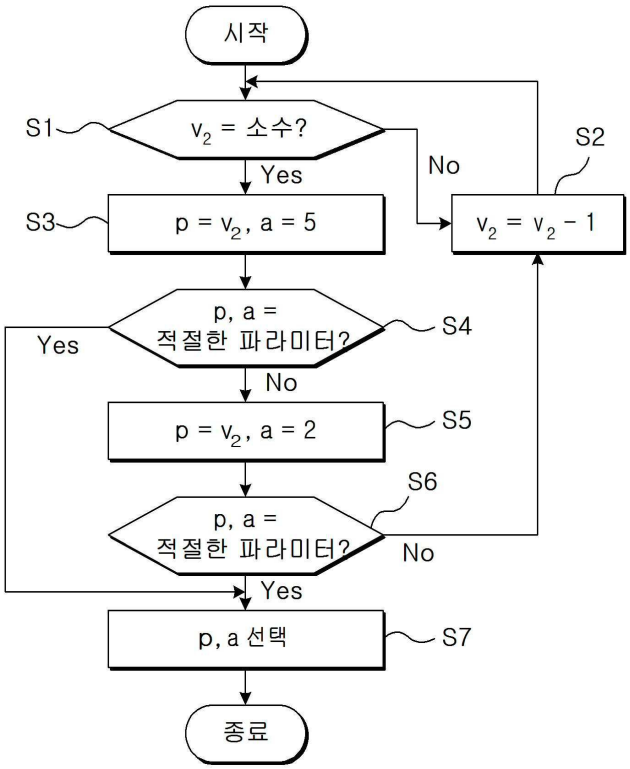
[0048] 이상에서 몇 가지 실시예를 들어 본 발명을 더욱 상세하게 설명하였으나, 본 발명은 반드시 이러한 실시예로 국한되는 것이 아니고 본 발명의 기술사상을 벗어나지 않는 범위 내에서 다양하게 변형실시될 수 있다.

도면

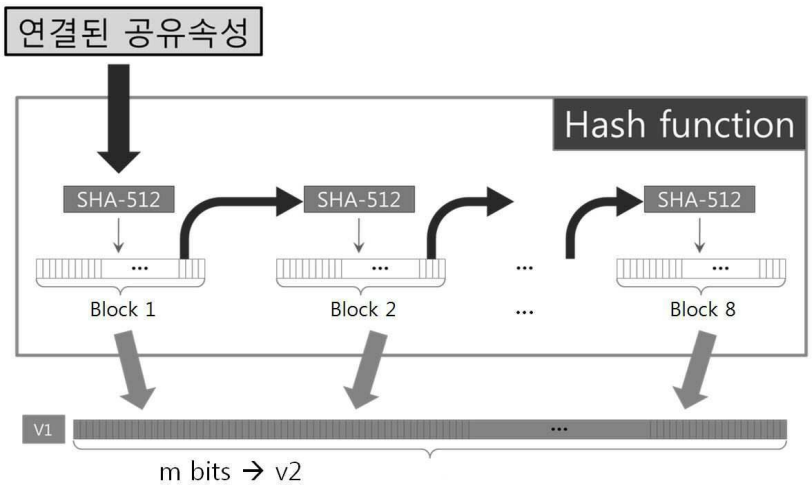
도면1



도면2



도면3


연결된 공유속성
Hash function
SHA-512
SHA-512
SHA-512
Block 1
Block 2
Block 8
V1
m bits → v2