이산대수 기반 공개키 암호 시스템의 도메인 구성 방법에 관한 연구

송기언*, 문종철***, 양형규**,원동호*
*성균관대학교 정보통신공학부
**강남대학교 컴퓨터공학과
***국가보안기술연구소
e-mail:{kesong, dhwon}@dosan.skku.ac.kr

A Study on Domain of Cryptosystem on the Discrete Logarithm Problem

Kieon Song*, Jongcheol Moon***, Hyungkyu Yang**, Dongho Won*
*Dept of Computer Engineering, Sungkyunkwan University
**School of Computer Media Engineering, Kangnam University
***National Security research Institute

요 약

이산대수 기반 암호 시스템은 도메인 구성상 공통의 도메인 파라미터(Domain parameter)를 사용하여, 다른 공개키 암호 시스템보다 키 분배의 경우 계산량이 적고 도메인 구성에 용이하다는 장점이 있다. 특히, 이러한 장점으로 다양한 환경에 적용 가능하도록 도메인을 구성할 수 있기 때문에 도메인 파라미터와 공개키/비밀키 쌍의 생성과 검증을 인증기관이 수행하거나 사용자가 수행함에 따라서 도메인의 구성에 많은 차이점이 나타난다. 본 논문에서는 도메인을 구성할 때 파라미터의 생성과 검증, 키 생성과 검증의 주체에 따른 장·단점을 분석하여 사용 환경에 적합한 시스템을 설계할 수 있도록 도메인 구성 방법에 대하여 기술한다.

1. 서론

최근 유/무선 인터넷의 확산으로 전자상거래가 발전하고 있으며, 이로 인해 많은 사용자가 서로간에 안전하게 개인정보를 전송하기 위해서 암호 기술을 사용하게 되었다. 암호 기술의 사용을 위해서는 먼저 사용자들 사이의 키 분배가 수행되어야 한다. 최근 공개키 암호 방식을 이용한 키 분배가 사용되고 있으며, 이산대수 문제와 소인수 분해 문제를 기반으로 하는 방식이 주를 이루고 있다. 현재 활발히 연구되고 있는 공개키 기반구조 환경에서는 효율적인 도메인 구성을 위해 이산대수 문제를 기반으로 하는 공개키 암호 시스템을 주로 사용하고 있다.[1,2,3]

암호 시스템은 도메인을 기반으로 암호 프로토콜을 수행하기 때문에, 도메인 파라미터의 구성 방식에 따라 암호 시스템의 안전성과 특성에 많은 차이가 생긴다. 따라서 본 논문에서는 도메인 파라미터와 키의 생성과 검증 주체에 따라서 도메인 구성 방식을 분류하고 장·단점을 분석한다. 이러한 분석결과를 기반으로 사용 환경과 목적을 고려한 도메인 구성 방법에 대하여 제안한다.

본 논문의 구성은 다음과 같다. 제 2절에서 이산대수 문제를 기반으로 하는 공개키 암호 시스템의 도메인 파라미터와 키의 생성·검증 알고리즘을 분석한다. 제 3장에서는 이산대수 기반의 도메인 구성 방식을 파라미터와 키의 생성·검증 주체에 따라서 분류하여 그 장·단점을 비교·분석한다. 마지막으로 제 4장에서 결론을 맺는다.

2. 관련연구

이산대수 문제를 기반으로 하는 암호 시스템에서는 도메인 파라미터를 생성·검증한 후 비밀키/공개키 쌍을 생성·검증하는 것이 전체 도메인 구성에서

중요한 부분을 차지한다. 본 절에서는 도메인 파라미터와 키의 생성·검증 알고리즘에 대해서 설명하고 알고리즘 수행시의 계산량에 대하여 알아본다. 계산량의 대부분을 차지하는 것은 소수의 생성과 판정이다. 파라미터나 공개키/비밀키 쌍을 생성하고 검증하는 알고리즘에 소수 판정 알고리즘이 포함되어 있는 것은 각각의 개인이 수행해야할 계산량이 증가하게 된다. 즉, 도메인을 구성하는 알고리즘들의 계산량을 분석하여 많은 연산이 필요한 알고리즘은 계산 능력이 좋은 객체(인증기관)가 수행하도록 도메인을 구성하여 효율성을 높일 수 있다. [4,5,6]

■ 기호 정의

[표 1]은 IEEE P1363/D13에 명시된 이산대수 기반 암호 시스템의 도메인 파라미터와 키의 생성·검증 알고리즘에 사용된 기호를 정의한 것이다.

[표 1] 기호 정의

기호	정의
q	필드의 크기를 나타내는 소수
r	$q-1$의 약수이며 g의 위수
g	$GF(p)$상의 원시 원소
k	$(q-1)/r$, 공통인자
w	공개키 (public key)
s	비밀키 (private key)

2.1 시스템 파라미터의 생성과 검증 알고리즘

■ 시스템 파라미터 생성 알고리즘

q의 최소값과 최대값(q_{min}, q_{max}), r의 최소값과 최대값(r_{min}, r_{max})을 입력으로 하여 q, r, g와 k를 출력하는 알고리즘이다. 알고리즘의 구성은 다음과 같다.[5]

① $r_{min} \le r \le r_{max}$인 랜덤 소수 r을 랜덤 소수 생성 알고리즘을 이용하여 생성

② $q_{min} \le q \le q_{max}$에서 $q \equiv 1 (\mathrm{mod}\ r)$를 만족하는 랜덤 소수 p를 랜덤 소수 생성 알고리즘을 이용하여 생성

③ $k=(q-1)/r$인 k를 계산

④ k와 r이 공통 인자를 갖고 있으면, ①단계부터 다시 시작

k와 r이 공통 인자를 갖고 있지 않으면, ⑤단계로 진행

⑤ $1<h<q-1$인 h를 선택

⑥ $g := h^k \mathrm{mod}\ p$를 계산

⑦ $g=1$이면, ⑤단계부터 다시 시작

⑧ q, r, g와 k를 출력

■ 시스템 파라미터 검증 알고리즘

q, r, g와 k를 입력으로 하여 각 입력값을 검증하여 "참(True)" 또는 "거짓(False)"을 출력하는 알고리즘이다. 알고리즘 구성 방식은 다음과 같다.[6,7]

① $q(q>2)$가 홀수임을 확인하고 소수 판정 알고리즘을 통해서 소수임을 확인

② $r(r>2)$가 홀수임을 확인하고 소수 판정 알고리즘을 통해서 소수임을 확인

③ g가 $1<g<q$인 정수임을 확인

④ $g^r \equiv 1 (\mathrm{mod}\ q)$임을 확인

⑤ k가 $kr=q-1$을 만족하는지 확인

⑥ k와 r이 공통 인자를 갖고 있지 않음을 확인

⑦ 모든 사항을 만족하면 "참(True)"을, 그렇지 않으면 "거짓(False)"을 출력

2.2 공개키/비밀키 쌍의 생성 알고리즘과 공개키 검증 알고리즘

■ 공개키/비밀키 쌍의 생성 알고리즘

q, r, g를 입력으로하여 공개키/비밀키 쌍 w, s을 출력으로 하는 알고리즘이다. 알고리즘 구성 방식은 다음과 같다.

① $0<s<r$인 랜덤수 s를 생성

② $GF(p)$상에서 $w := g^s$를 계산

③ w와 s를 출력

■ 공개키 검증 알고리즘

q, r, g와 w를 입력으로 w를 검증하여 "참(True)" 또는 "거짓(False)"을 출력하는 알고리즘이다. 알고리즘 구성 방식은 다음과 같다.

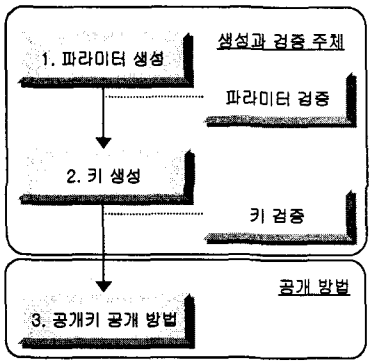
① w가 $1<w<q$임을 확인

② $GF(q)$상에서 $w^r=1$임을 확인
③ 모든 사항을 만족하면 "참(True)"을, 그렇지 않으면 "거짓(False)"을 출력

2.3 시스템 파라미터와 키의 생성과 검증 알고리즘 비교

소수 판정 알고리즘은 확률 알고리즘으로 많은 반복 수행으로 소수에 가까운 수를 찾아내기 때문에 많은 연산이 필요하다. 소수 판정 알고리즘이 포함된 파라미터의 생성과 검증 알고리즘이 키 생성·검증 알고리즘에 비해서 많은 연산을 필요로 한다.[8]

3. 생성과 검증 주체에 따른 암호 시스템의 도메인 구성



[그림 1] 도메인 구성 과정

[그림 1]은 도메인 구성 과정을 나타낸다. 이산대수 기반의 모든 공개키 암호 시스템은 도메인 파라미터를 이용하여 생성된 키를 가지고 동작하게 된다. 그렇기 때문에 공개키 기반 암호 시스템의 안전성을 보장하기 위해서는 올바른 도메인 파라미터와 공개키/비밀키 쌍의 생성·검증이 매우 중요하다. 또한 공개 방법도 도메인의 특징을 구별하는 중요한 요소가 된다. 본 절에서는 사용 환경에 적합하고 효율적인 도메인 구성을 위해 파라미터와 키를 생성하고 검증하는 주체에 따라 발생되는 장·단점을 비교 분석한다.

3.1 파라미터 생성과 검증

도메인 파라미터의 생성·검증은 키의 생성·검증에 비해 많은 계산량을 필요로 한다. 각 사용자가 암호 통신을 위해서 자신이 소속된 시스템의 파라미터를 생성하는 것은 많은 시스템 자원의 낭비를 가져오게 된다. 그러나 신뢰기관(i.e.인증기관)이 도메인 파라미터를 생성하여 공개한다면 안전한 도메인 파라미터의 설정함으로써 각 사용자가 도메인 파라미터를 생성하지 않고 키를 생성하여 사용할 수 있기 때문에 매우 효율적이다. 반면에 각 사용자가 도메인 파라미터를 따로 생성할 경우에는 상대방은 도메인 파라미터의 검증을 필요로 한다. 파라미터의 검증 또한 생성과 같이 많은 계산이 필요하기 때문에 개인이 도메인 파라미터를 생성하는 것은 매우 비효율적이다. 그러나 신뢰기관이 파라미터를 생성하고 검증한다면 각각의 개인은 신뢰기관을 믿고 파라미터의 검증을 수행하지 않아도 된다.

3.2 공개키/비밀키 쌍의 생성과 검증

공개키/비밀키 쌍의 생성은 도메인 파라미터의 생성과 마찬가지로 생성 주체에 따라 그 특징이 분류된다. 크게 각 사용자가 파라미터를 이용하여 공개키/비밀키 쌍을 생성하는 경우와 신뢰기관이 키 쌍을 생성하여 분배하는 경우로 분류할 수 있으며, 각 방식의 장·단점을 고려하여 사용 환경에 따라 적용할 수 있다.

- 사용자가 키를 생성하는 경우
  비밀키는 사용자만이 알고 있기 때문에 각 사용자의 비밀키를 이용하여 신뢰기관이 사용자로 위장하는 것이 불가능하다. 하지만 키 분실이나 다른 잘못된 사용으로 인해 분쟁이 발생했을 경우 중재가 어려운 단점이 있다. 이를 예방하기 위해 신뢰기관이 키 복구 시스템을 따로 운영할 수 있다.

- 신뢰기관이 키를 생성하는 경우
  신뢰기관의 키 생성은 중앙집중식 키 관리가 용이하다는 장점이 있다. 이는 조직 안에서 외부에서의 공격으로부터 안전한 통신에 사용하기 적합하다. 하지만 신뢰기관이 각 사용자의 비밀키를 알고 있기 때문에 신뢰기관이 사용자로 위장하는 것이 가능하다는 문제로 인해 신뢰기관의 높은 신뢰성이 요구된다.

■ 공개키 검증

공개키 기반구조에서 키를 이용하여 통신을 할 경우 공개키의 인증이 필요하다. 공개키의 인증은 신뢰기관의 공개키에 대한 검증(Validation of Public key)과 소유자 검증(Proof of Possession)을 통해 발행된 공개키 인증서를 통해 이루어진다. 즉, 개인이 키를 생성하거나 신뢰기관이 키를 생성하는 경우 모두 신뢰기관이 공개키 인증서를 발행함으로써 공개키의 검증과 소유주 검증이 이루어지고 있다. 그러나 신뢰기관이 존재하지 않는 통신을 할 때는 상대방이 생성한 키의 검증과 소유자 검증이 암호 시스템에 포함되어야한다.

신뢰기관이 포함된 암호 시스템과 신뢰기관이 포함되지 않은 암호 시스템은 각각의 장·단점이 있다. 신뢰기관이 포함된 암호 시스템은 암호 시스템을 구성하는데 많은 비용과 노력이 필요로 한다. 하지만 암호통신을 할 경우 공개키의 검증이 인증서를 통해 이루어지므로 효율적이라 할 수 있다. 신뢰기관이 포함되지 않은 암호 시스템은 신뢰기관을 위한 비용과 노력이 필요 없다는 장점이 있지만 인증서를 발행하는 주체가 없기 때문에 암호 통신을 위해서 실제 수행되는 프로토콜에 공개키 검증 부분을 포함 시켜야 한다. 즉, 인증서를 이용하지 않을 경우 프로토콜이 더욱 복잡해지고 사용자의 계산 부담이 커지게 된다.

3.3 공개키 공개 방법

공개키 암호 시스템은 공개키의 공개 방법에 따라 시스템의 구조가 달라진다. 자신의 공개키를 자신이 갖고 있다가 암호 통신을 할 때 상대방에게 전송하는 방법이 있으며, 공개 디렉토리(directory)에 등록하여 통신하는 상대방이 디렉토리에서 공개키를 가져오는 방법이 있다. 공개 디렉토리에 등록하는 방법은 현재 공개키 기반구조에서 사용되고 있다.

4. 결론 및 향후 연구 방향

암호 시스템의 도메인 설계자는 사용 환경과 목적에 따라 효율적인 시스템이 되도록 설계해야 한다. 본 논문에서는 사용 환경에 적합하고 효율적인 도메인 구성을 위해 파라미터 생성, 키 생성, 공개키 공개의 주체를 인증기관과 사용자로 구분하여 수행주체에 따라 발생하는 장·단점을 기술하였다.

본 논문의 도메인 구성 방법을 무선 환경에 적용해 볼 수 있다. 무선 환경에서는 유선 환경에 비해서 높은 통신비용, 무선 단말기의 계산 능력, 메모리 부족 등의 단점으로 인해 무선 단말기에서의 파라미터의 생성, 검증의 능력이 부족함으로 신뢰기관이 필요하다. 그러나 키 생성, 검증은 파라미터의 생성, 검증에 비해서 적은 계산이 소요되기 때문에 무선 단말기의 계산 능력에 따라 개인이 키 생성, 검증을 수행하도록 도메인을 구성할 수 있다.

이와 같이 사용 환경과 목적 그리고 사용자의 연산 능력을 고려하여 도메인을 구성하면 암호 시스템을 보다 안전하고 효율적으로 설계하는 것이 가능하다. 향후 보다 세분화된 방법으로 시스템 설계상의 특징을 분석하여 사용환경에 최적화된 암호 시스템을 사용할 수 있도록 해야 한다. 그러므로 보다 최적화된 암호 시스템을 위해 도메인 구성 요소들에 대한 연구가 더욱 필요하다.

참고문헌

[1] PKI X.509 "Intranet X.509 Public Key Infrastructure Certificate and CRL Profile", 1999. 1

[2] B. Schneier "Applied Cryptography, 2nd Edition", 1996

[3] T. ElGamal "A public key cryptosystem and a signature scheme based on discrete logarithms", 1985

[4] IEEE "IEEE P1363/D13, Standard Specifications for Public Key Cryptography", 1999.12

[5] ANSI X9.80 "Public Key Cryptography for the Financial Services Industry : Prime Number Generation and Validation Methods, draft", 1998

[6] Miller-Rabin "Probabilistic algorithm for testing primality", 1980. 9, 273-280

[7] G.L MILLER, "Riemann's hypothesis and tests for primality", 1976, 300-317

[8] Alfred J.Menezes, Paul C.van Oorschot, Scott A.Vanstone, " Handbook of Applied Cryptography", 1996.10