타원곡선 암호알고리즘을 이용한 효율적인 디지털 컨텐츠 암호화 시스템

황 선 태* · 이 승 혁**

An Efficient Digital Contents Cryptosystem using Elliptic Curve Cryptography Algorithm

Suntae Hwang* · Seunghyuk Lee**

Abstract

Recently, as network and computer technologies are growing rapidly, most of business transactions are performed in cyber world. In spite of many advantages, the most concerns in Electronic Commerce are the information security matters, and the cryptosystem has been claimed as one of the proper means to settle this problem. In this paper, a partial encryption/decryption algorithm has been introduced to show the efficiency against the conventional method in which all the data are completely encoded. In our proposed scheme, the multimedia data can be efficiently encoded in a short time providing good data security. For example, the MP3 data can be securely protected with 10% encryption in our scheme. Moreover, the shuffling process at the end of partial encryption procedure provides higher level of data security.

Keywords : Partial Encryption, Digital Contents, ECC

논문접수일 : 2004년 2월 15일 논문게재확정일 : 2004년 8월 20일

* 대전대학교 정보통신인터넷공학부 부교수
** (주)니츠 정보보호기술연구소 연구원

1. 서 론

최근 들어, 네트워크(Network)와 컴퓨터 통신이 발전하면서 일상적으로 행하던 일부 거래가 컴퓨터 네트워크를 이용한 전자 공간에서 이루어지고 있다. 특히 인터넷(Internet)의 급속한 확산에 따라 전자상거래(Electronic Commerce)도 역시 급속히 확산되고 있는 실정이다. 이러한 전자상거래는 여러 가지 장점에도 불구하고 개방형 네트워크의 특성상 거래 전반에 걸친 정보들이 자칫 노출될 수 있다는 문제점을 지니고 있다. 이에 따라 전자상거래를 보다 활성화하기 위해서는 전자상거래의 신뢰성을 확보할 수 있는 정보보호 기술이 필수 선결 요소라 하겠다. 따라서 이와 관련하여 정보보호 문제를 해결할 수 있는 안전한 장치가 필요한데, 이러한 장치들 중의 하나로 제시되고 있는 것이 암호 알고리즘을 이용한 암호시스템(Cryptosystem)이다 [Froomkin, 1996 ; Sun, 2004].

디지털 컨텐츠(Digital Contents)란 각종 유무선 통신망을 통해 매매 또는 교환되는 디지털 정보를 통칭하는 말로 쓰인다. 예를 들어 인터넷이나 PC통신 등을 통해 제공되는 정보나 각종 프로그램, 비디오테이프, CD -ROM 등에 담긴 영화 또는 음악, 게임 소프트웨어 등이 이에 속한다. 이러한 디지털 컨텐츠는 네트웍을 통한 분배나 편집 및 수정이 용이할 뿐만 아니라 항구적이며, 검색이 편리하다는 장점들을 가지고 있다. 그러나, 디지털 컨텐츠가 많은 장점들을 가진 반면에 동시에 원본과 복사본의 구별이 거의 불가능하고, 적은 비용으로 손쉽게 대량의 불법복제 및 배포가 가능하며, 데이터의 위조나 변형, 저작권의 침해 등의 심각한 문제점들을 가지고 있다는 단점이 있다. 이러한 문제점들을 극복하기 위해 디지털 컨텐츠에 대한 여러 가지 정보보호 기법들이 연구되고 있다[박창섭, 1999].

대표적인 정보보호 기법으로 전통적 암호기법(Conventional Cryptography)과 공개키 기법(Public Cryptography)의 두 가지 범주가 있다. 전통적 기법은 대칭형 암호기법(Symmetric Cryptography)라고도 하며 메시지의 송신자, 수신자가 동일한 키를 공유하고 이 키를 이용하여 메시지를 암호화하고 복호화 하는 기법이다 [NIST, 1993]. 대표적인 알고리즘으로 DES, RC2, RC4, RC5, IDEA, Blowfish 등이 있다. 공개키 기법은 비대칭형 암호기법(Asymmetric Cryptography)라고도 하며, 두 개의 키를 사용하는 알고리즘을 정의함으로써 키를 교환하고 공유하는 문제를 해결하며, 두 개의 키 중 어느 것도 메시지를 암호화하는데 사용될 수 있다. 대표적인 알고리즘으로 RSA, Diffie-Hellman, ElGamal, 타원곡선(Elliptic Curve) 알고리즘 등이 있다 [박창섭, 1999 ; 최용락 1996]. 또 다른 정보보호 기법으로 전자서명(Digital Signature)이 있다. 메시지의 수신자는 메시지가 전송 도중 내용이 바뀌지 않았는지, 또는 제3자가 송신자를 가정하여 메시지를 보내지 않았는지를 확인할 수 있다[Rivest et al., 1978].

또한 정보에 대한 암호화와 전자서명으로 데이터의 위·변조 및 해킹을 막을 수 있지만 스마트카드(Smart Card)를 이용하면 그 자체로 데이터를 암호화하고, 서명을 생성하며, 위·변조가 불가능한 가치이전을 가능케 해준다. 스마트카드란 외부환경에 독립적인 보안영역을 확보하기 위해 신용카드 크기의 플라스틱카드에 마이크로프로세서(Microprocessor)와 메모리(Memory)를 내장하여, 인증 및 보안기능을 제공하는 시스템이다[Fancher, 1997 ; Dreifus et al, 1998].

본 논문에서는 최근 유료화 추세에 따른 디지털 컨텐츠의 효율적인 권한관리를 위한 암복호화 기법을 제시하고자 한다. 아직도 많은 부분에서 3DES와 같은 대칭형 암호알고리즘이 쓰

이고 있지만, 대칭형 암호 방식의 최대 단점인 키 교환 문제를 효과적으로 해결하기 위해 공개키 암호 방식인 타원곡선 암호알고리즘을 이용한 부분 암복호화 알고리즘을 제안하고자 한다. 이렇게 함으로서 디지털 컨텐츠의 암복호화 시간을 단축시키고 서비스제공 서버 및 클라이언트의 부하를 경감시킬 수 있다.

본 논문은 연구목적 및 내용을 담은 서론을 제1장에서 다루고, 본 논문에서 사용된 타원곡선 암호화 알고리즘에 대한 이론적인 부분과 관련 내용에 대해 제2장에서 다룬다. 제3장에서는 제안한 디지털 컨텐츠 암호화 기법의 특징에 대해 설명하고, 제4장에서는 성능을 평가한다. 마지막으로 제5장에서 결론을 맺는다.

2. 타원곡선 암호알고리즘(Elliptic Curve Cryptography : ECC)

타원곡선(Elliptic Curve)은 최근 100여 년 동안 정수론 및 대수 기하학 분야에서 광범위한 연구가 있어 왔고, 특히, Andrew Wiles의 Fermat's Last Theorem 증명에서 매우 중요한 역할을 담당한 이론적 도구이기도 하였다. 또한 최근 소인수 분해, 소수 판정법 및 공개키 암호와 관련된 다양한 알고리즘을 설계하는데 이용되고 있다[8].

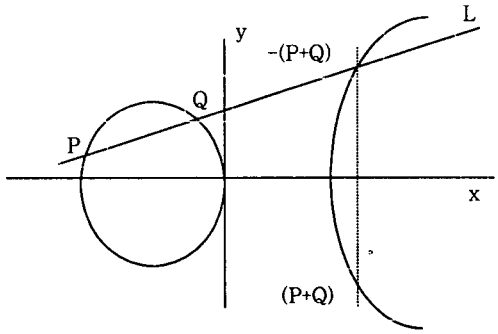
타원곡선을 이용한 공개키 암호 시스템 즉, 유한체(Finite Field)위에서 정의된 타원곡선 군(Group)에서의 이산대수 문제에 기초한 타원곡선 암호시스템(ECC)은 1985년 N. Koblitz와 V. Miller에 의해 처음 제안된 이후 활발히 연구되고 있다. 타원곡선 암호시스템은 기 존재하는 다른 공개키 스킴(Scheme)과 같은 안전도를 제공하는 데에 더 작은 키를 가지고 가능하다. 예를 들면 RSA 1024-bit 키와 ECC 160-bit 키를 갖는 암호시스템은 같은 안전도를 갖는다. 짧은 키 길이를 갖는다는 것은 암호시스템에서 필요한 대역폭(Bandwidth)과 메모리가 작아짐을 의미한다. 이것은 메모리 용량과 처리능력이 제한된 스마트카드의 응용에서 중요한 요소다[이인수, 1998].

공개키 암호시스템의 효율성을 위해서는 계산량, 키의 크기 및 대역폭 등 3가지 다른 요소들을 고려하여야 한다. 계산량은 공개키와 비공개키를 계산하는 데에 드는 계산량을 말하며, ECC의 경우 RSA 또는 DSA보다 약 10배 정도의 빠른 수행속도를 보여준다. 또한 알고리즘도 사용하는 키의 길이에 따라 현재 사용하기에 적합한가 위험한가를 확인한다. 비대칭형 암호화 알고리즘은 큰 소수계산 등에 의존하기 때문에 대칭형 암호화기술과는 다른 컴퓨팅 파워를 요구하며 일반적으로 RSA알고리즘의 경우 최소한 768-bit 이상의 키를 사용할 것을 권하고 있다. ECC는 이러한 관점에서 타 공개키 암호시스템보다 효율적이다. 따라서 구현에 있어 이러한 점은 높은 속도, 적은 전력 및 코드 크기를 줄일 수 있음을 의미한다[Menezes, 1993 ; Koblitz, 1987].

유한체 상에 정의된 타원곡선에 대하여 타원곡선군은 3차 방정식을 만족하는 순서쌍들과 무한점을 포함한 집합을 말한다. 두 점의 덧셈군을 계산하는 방식으로는 동일한 점 즉, P = Q의 경우와 점 P ≠ Q인 경우로 나뉜다. <그림 1>은 타원곡선 위의 두 점 P와 Q가 서로 다른 경우로 이 두 점의 합 P + Q를 구하는 그래프이다. 먼저 서로 다른 점 P와 Q를 지나는 직선 L을 긋는다. 그러면 L과 원래의 타원곡선이 만나는 점이 반드시 존재하게 되고 그 점을 바로 -(P + Q)로 정의한다. 그리고 x축과 대칭이동되는 점이 암호화된 점인 (P + Q)가 된다.

두 번째로, <그림 1>에서 L이 접선이 되어서 P와 Q가 같은 경우, 같은 점 P를 더한 경

우로 P + P = 2P인 점을 구하는 방식이다. P ≠ Q인 경우와 같이 점 P에서 2P를 덧셈 연산으로 구하고, 접선 L을 그어 만나는 점을 -(2P)로 정한 후, x축을 기준으로 대칭 이동하여 암호화된 점 2P를 얻는다. 이렇게 정의된 연산에 의해서 유한군이 형성되고 그 군의 원소의 개수 즉, 좌표 점의 개수는 타원곡선이 정의된 유한체상의 원소의 개수가 된다.



〈그림 1〉 일반적인 형태의 Elliptic Curve 그래프

타원곡선 E는 $y2 \pmod p = x3 + bx + c \pmod p$ (b, c∈Zp)로 표현하며 무한원점(0)으로 구성되어 있다. p개의 원소를 갖는 유한체의 점들로 구성된 타원곡선 E(Zp)는 두 개의 점으로 구성되어 있다. 즉 P(x1, y1), Q(x2, y2)로 되어 있으며 $\{(x, y) \in (ZP, ZQ) \mid y2 = x3 + bx + c\} \cup \{0\}$로 표현한다. 여기서 E(Zp)의 원소인 P, Q가 주어졌을 때 타원곡선의 암·복호화는 Q = aP일때 a를 계산해 내는 것이 중요한 문제이다. 타원곡선 암호화 시스템은 타원곡선 상에서 점 P를 a번 더하는 계산이 주를 이룬다. 즉, Q = aP를 구하는 더하기 연산은 modular 덧셈을 통해 이루어진다. 또 타원곡선 암호화가 RSA 암호화 시스템보다 능률적인 이유는 소수 p의 값이 작아도 안전성이 뛰어나다는 것이다. 즉, 타원곡선 암호시스템의 안전도는 타원곡선 이산대수문제에 의존하고 있으며, 효율성은 aP를 얼마나 빠르게 계산해 낼 수 있는가에 달려있다. 타원곡선 알고리즘은 최초의 점에서 소수의 횟수만큼 덧셈연산에 의한 이동으로 마지막 최종의 점을 암호화 키로 갖기 때문에 암호화 키를 통한 원래의 점을 역 추적하기가 상당히 어렵다. 즉 Q = aP에서 암호화된 결과의 점 Q의 값을 알 때 정수형태의 비밀키 a와 초기의 점 P를 예측하기는 불가능하다.

이러한 ECC 암호화 방법은 유한체 k 위에서 정의된 타원곡선 E위의 점들로 덧셈군의 형태를 이루게 된다. 이 덧셈군의 더하기 연산은 기초 체(field) k에서의 산술 연산 몇 개를 포함하며, 하드웨어와 소프트웨어로 구현하기가 쉽다. 또한 이 덧셈군에서 이산대수를 사용하는 암호시스템은 유한체의 곱셈군에 기초한 시스템에 비해 두 가지 장점을 가지고 있다. 첫째, 이 군에서의 이산대수 문제는 매우 어렵다. 특히 같은 크기인 k 유한체에서의 이산대수 문제보다 더 어렵다. 다시 말하면, ECC는 작은 크기의 키를 가지고 현존하는 공개키 암호화 기법의 안전도를 보장받을 수 있다. 둘째, 타원곡선을 사용함에 따른 또 다른 이점은 비록 모든 사용자들이 같은 기초에 k를 사용하더라도 각 사용자가 다른 곡선 E를 선택할 수 있다. 결과적으로 모든 사용자들은 같은 하드웨어로 체(field) 연산을 실행하고, 요구되는 안전도를 위해 주기적으로 곡선 E를 변환시킬 수 있다 [정은희 & 이병관, 2002].

3. 부분 암복호화 알고리즘의 설계 및 구현

인터넷을 이용한 정보교환은 그 편리함에도 불구하고 인터넷의 특성상 정보의 도청과 변조라는 위협에 노출되기 쉽다. 더욱이 전체 정보의 암복호화에 소요되는 시간 등의 비용은 무시할 수 없다. 따라서 본 논문에서는 저비용으로 효율

적이고 안전한 디지털 컨텐츠 서비스를 제공할 수 있는 향상된 정보 암복호화 기법을 제안한다. 본 연구에서는 공개키 암호 알고리즘 중 상대적으로 키의 길이가 작으면서 높은 비도를 가지는 키의 길이 160-bit인 타원곡선 암호 알고리즘을 이용하여 데이터의 암복호화를 수행하고자 한다. 키의 크기가 160-bit인 타원곡선 암호 시스템은 키의 길이가 1024-bit인 RSA 암호 시스템의 비도와 같은 수준의 안전도를 갖는다.

본 논문에서 제안한 타원곡선 암호 알고리즘을 적용한 암복호화 알고리즘은 (그림 2)와 같다. 송신할 디지털 컨텐츠 데이터를 M이라고 하면 이것을 일정한 길이(단위 : Kbytes)의 블록인 m_b(b = 1, 2, ⋯, n)로 나눈다. 또한 나뉘어진 블록에 대해 암호화율(단위 : %)을 정하게 되는데, 이 암호화율은 데이터 전체를 암호화하지 않아도 충분히 정보 보호 효과를 얻을 수 있도록 정한다. 이 m_b의 크기와 암호화율은 각 컨텐츠별로 정보의 중요도에 따라 적절히 선정할 수가 있다. 즉, 텍스트형의 데이터는 중요도가 높은 경우 블록크기를 작게 하고 암호화율을 크게 하면 상대적으로 비도를 높일 수가 있게 된다. 이와 같은 블록크기과 암호화율 정보는 부분 암호화된 파일의 헤더 부분에 각각 4bytes와 2bytes 크기로 첨부된다. 반면 본 논문의 주된 고찰 대상인 정지영상이나 동영상, 음향 데이터 같은 경우는 작은 암호화율을 가지고도 높은 비도 효과를 얻을 수 있다. 이를 수식으로 표현하면,

$M = \prod_{b=1}^{n} m_b$. 여기서 n은 전체 블록의 개수이며, $\prod$는 m_b들의 Concatenation 함수를 나타낸다. 이 표현을 이용하여 전송하고자 하는 전체 정보의 암호화 과정을 식으로 표현하면 다음과 같다.

$$M' = \prod_{t=1}^{T} (E(m_{2t-1}) \prod m_{2t}) \prod \left(\prod_{t=2T+1}^{n} m_t \right).$$

여기서

$T = \lceil n \times \frac{\text{암호화율}}{100} \rceil$, E는 Encryption 함수 그리고 M'은 암호화된 결과이다. 암호화 과정을 거친 데이터 M'은 암호화가 된 부분 m_{2t-1} ($t = 1, \cdots, T$)와 암호화가 되지 않은 부분 m_{2t}($t = 1, \cdots, T$), m_t($t = 2T+1, \cdots, n$)로 나뉘게 된다. 이 식에서 암호화율은 최대 50%를 넘을 수 없고 $n \geq 2$이다. 그러나 이 상태로 데이터를 전송하게 되면 해킹 등에 의해 부분 암호화된 정보 중 암호화 안 된 일정 뒷부분의 일부가 노출될 가능성이 있다. 이러한 문제를 가능한 한 해결하고 비도를 더욱 높이기 위해 전송하기 이전에 부분 암호화된 전체 블록들의 순서를 뒤바꾸어 주는 Shuffling 함수 $H()$를 적용하여 M'식의 각 블록들의 순서를 뒤섞은 후 송신한다. 이 함수 $H()$의 알고리즘은 (그림 3)과 같이 구현하였다. 이 Shuffling 함수는 전송되는 암호화된 데이터의 헤더에 정해진 크기로 탑재하거나, 암복호화 프로그램 내에 저장하여 수행시킬 수 있다. 여기서는 결과 분석을 위한 시뮬레이션 목적으로 간단히 Random Number 발생을 이용하여 블록들을 Shuffling 하였다. 암호화된 데이터를 Shuffling하고 복호화 시 Restoring 하는 시간은 무시할 수 있을 만큼 빠른 속도로 이루어지기 때문에 전체적인 정보처리 시간에는 거의 영향을 미치지 못한다. 수신단 측에서는 수신된 암호화 데이터를 Shuffling 함수의 역함수(Restoring Function)를 적용하여 원래의 암호화된 데이터 순서로 바꾼 후 복호화를 수행하게 된다.

```
SUMLOOP (i) {
    Session_key[i] = random.seed;
}
Key_generate(Secret_key, Public_key);
if(Open(file))
{
        fread(file, M);
        Ratio = (M/100) * Ratio;
m_B = M;
    fclose(file);
}
Cipher_file = Elliptic_Encryption( ∏_{t=1}^{T} (E(m_{2t-1}) ∏ m_{2t})  ∏( ∏_{t=2T+1}^{n} m_t ) )
Shuffled_file = H(Elliptic_Encryption( ∏_{t=1}^{T} (E(m_{2t-1}) ∏ m_{2t})  ∏( ∏_{t=2T+1}^{n} m_t )));
fwrite(Shuffled_file);
endif;
```

↓ 전 송

```
if(Open(file))
{
        fread(file, Shuffled_file);
}
Restored_file = H(Shuffled_file);
Decrypt_file = Elliptic_Decryption(Restored_file);
M = fwrite(Decrypt_file);
fclose(file);
endif;
```

〈그림 2〉 부분 암복호화 알고리즘

```
#define Cipher_File_Size  ∏_{t=1}^{T} (E(m_{2t-1}) ∏ m_{2t})  ∏ ( ∏_{t=2T+1}^{n} m_t)

if(Open(file))
{
    fread(file, Cipher_file);
}
While(Random_Block_Size < Cipher_File_Size)
{
    memcpy(buf, Cipher_file_Size+Random_Block_Size);
    Random_Block_Size += Random_number;
}
fwrite(Ordered_Cipher_file);
flcose(file);
endif;
```

↓ 전 송

```
if(Open(file))
{
        fread(file, Ordered_Cipher_file);
}
While(Random_Block_Size < Ordered_Cipher_File_Size)
{
    memcpy(buf, Ordered_Cipher_file_Size+Random_Block_Size);
    Random_Block_Size += Same_Random_number;
}
S = fwrite(Reordered_Cipher_file);
fclose(file);
endif;
```

〈그림 3〉 Random Shuffling Function H() 알고리즘

4. 실험결과 및 성능 분석

본 장에서는 타원곡선 암호 알고리즘을 이용하여 디지털 컨텐츠 데이터의 상대적인 부분 암복호화 속도를 측정하고, 제안한 기법의 성능을 평가하였다. 시뮬레이션을 위한 운영체제로는 LINUX를 사용하였으며 개발 사양은 <표 1>과 같다.

<표 1> 개발 사양

구 분	사 양	비 고
CPU	Intel Pentium-III 433MHz	
Main Memory	64MB	
OS	LINUX ver. 6.2	Kernel Ver. 2.2.16
개발도구	ANSI C	cc 및 gcc Compiler

성능평가를 위해 <표 2>와 같은 4가지 종류의 디지털 컨텐츠 데이터를 대상으로 부분 암호화 및 복호화를 수행한다.

<표 2> 성능평가 대상의 디지털컨텐츠 데이터

구 분	크기(Byte)	파일형식
Droid	687KB	JPG
Cant	551KB	ASX
Nonmun	689KB	HWP
Dup	1851KB	MP3

각 종류의 디지털 컨텐츠 파일은 데이터 블록을 10 Kbytes, 20 Kbytes, 30 Kbytes, 40 Kbytes와 같이 임의의 크기로 나누었고, 암호화율도 10%, 20%, 30%, 40%의 비율로 나누어 각각의 암복호화 시간를 측정하였다. 또한 시뮬레이션을 위해 샘플 디지털 컨텐츠 데이터 크기를 작은 것으로 선정하여 테스트를 수행 하였다.

<표 3>은 블록크기, 암호화율에 따른 암복호화 시간을 나타내고 있으며, 제안한 알고리즘을 적용했을 경우 Block 크기가 달라져도 동일한 컨텐츠의 동일한 암호화율에서는 암복호화 속도가 거의 일정함을 알 수 있다. 이 표에서 암복호화 시간치는 시스템과 프로그램 구현상의 주관적인 문제로 인해 그 의미를 갖지 못하며, 단지 상대적인 비교치로서만 그 의미가 있다. 또 Shuffling Time은 200 내지 300ms 정도로 암복호화시 거의 무시할 수 있을 정도의 시간이나, 블록들의 순서를 무작위로 뒤섞는 Shuffling을 통해 비도를 한층 높일 수 있다. 또한 암호화율이 증가할수록 디지털 컨텐츠 데이터의 암복호화 시간이 증가함을 볼 수 있다.

<표 3> 디지털 컨텐츠별 부분 암복호화 시간

E : Encryption Time(min.), D : Decryption Time(min.)

디지털 컨텐츠	암호화율 / 블록크기	10%	20%	30%	40%	전체
droid.jpg (687 KB)	10KB	E : 2.18 D : 1.35	E : 4.35 D : 2.75	E : 6.48 D : 4.10	E : 8.65 D : 5.48	E : 14.72 D : 10.55
	20KB	E : 2.45 D : 1.52	E : 4.27 D : 2.68	E : 6.68 D : 4.20	E : 8.52 D : 5.35	
	30KB	E : 2.52 D : 1.62	E : 4.55 D : 2.83	E : 6.38 D : 3.97	E : 9.07 D : 5.67	
	40KB	E : 2.40 D : 1.50	E : 4.85 D : 3.00	E : 7.25 D : 4.48	E : 8.42 D : 5.25	
cant.asx (551 KB)	10KB	E : 2.28 D : 1.48	E : 4.92 D : 2.33	E : 7.07 D : 4.28	E : 8.02 D : 5.95	E : 10.97 D : 7.48
	20KB	E : 2.56 D : 1.58	E : 4.42 D : 2.65	E : 7.27 D : 4.70	E : 8.08 D : 5.70	
	30KB	E : 2.83 D : 1.92	E : 4.70 D : 3.83	E : 7.40 D : 5.48	E : 8.48 D : 5.50	
	40KB	E : 3.13 D : 1.77	E : 4.37 D : 2.13	E : 8.02 D : 5.35	E : 8.08 D : 5.52	
nonmun.hwp (689 KB)	10KB	E : 2.15 D : 1.37	E : 4.25 D : 2.77	E : 6.43 D : 4.08	E : 8.65 D : 5.37	E : 14.38 D : 9.88
	20KB	E : 2.45 D : 1.48	E : 4.20 D : 2.65	E : 6.70 D : 4.12	E : 8.48 D : 5.28	
	30KB	E : 2.70 D : 1.68	E : 4.52 D : 2.80	E : 6.30 D : 3.97	E : 9.05 D : 5.60	
	40KB	E : 2.42 D : 1.50	E : 4.87 D : 2.98	E : 7.25 D : 4.50	E : 8.38 D : 5.20	
dup.mp3 (1851 KB)	10KB	E : 5.82 D : 3.70	E : 11.62 D : 7.40	E : 17.22 D : 11.02	E : 23.05 D : 14.57	E : 43.43 D : 32.72
	20KB	E : 6.05 D : 3.78	E : 11.47 D : 7.20	E : 17.17 D : 10.55	E : 23.82 D : 14.92	
	30KB	E : 6.40 D : 3.97	E : 11.77 D : 7.35	E : 17.25 D : 10.73	E : 24.45 D : 15.43	
	40KB	E : 6.05 D : 3.75	E : 12.07 D : 7.50	E : 17.18 D : 10.48	E : 26.63 D : 16.75	

이는 암복호화 데이터 크기가 증가 할수록 시간 관련 비용이 증가함을 나타낸다. 특히 시뮬레이션 결과에서 동일한 암호화 율인 경우, 암호화 시에 가능한 한 블록크기가 작고 블록 수가 많은 것이 블록크기가 크고 수가 적은 것보다 정보보호에 훨씬 유리하다. 그 이유는 블록 크기가 큰 경우에 비 암호화 정보가 경우에 따라 쉽게 노출될 가능성이 있기 때문이다. 따라서 제안한 알고리즘의 정보보호 효과는 정보의 중요도에 따른 블록크기와 암호화율의 선정에 의해 결정됨을 알 수 있다. 예를 들어, MP3 데이터의 경우 10 KBytes의 블록크기, 10%의 암호화율만을 가지고도 충분한 정보보호 효과를 얻을 수 있다. 또한 암호화를 할 때, 데이터의 Header 정보도 함께 암호화함으로서 데이터의 해킹 시에도 암호화된 데이터의 Format과 Shuffling 함수의 정보가 노출되지 않음으로 인해 이중 보안의 효과가 있다.

5. 결 론

통신망을 이용한 전자상거래는 대부분 개방형 구조(Open Architecture)를 기반으로 이루어지고 있으며, 현재 무한대로 확장되어 나가는 디지털 컨텐츠의 권한 관리 기능을 강화하여야 할 필요성이 제기되고 있다. 따라서 막대한 양의 디지털 컨텐츠를 효율적으로 관리하고 유통 질서를 확립하기 위하여 기존의 전체 암호화 기법에 비해 경제적이고 개량된 부분 암호화 기법을 본 논문에 제시한다.

본 연구에서는 디지털 컨텐츠를 제공해주는 서버 및 클라이언트의 부하를 경감시키고자 한층 효율적인 타원곡선 알고리즘을 이용해 키를 생성 및 분배하고, 또한 부분 암복호화 방식을 구현하였다. 부분 암복호화 방식은 데이터를 임의의 수의 일정한 블록들로 나눈 다음, 선정된 암호화율을 적용하는 방법으로 디지털 컨텐츠 제공 서버의 정보처리 시간을 줄일 수 있으며, 특히 암호화된 데이터를 전송하기 전에 무결성을 높이기 위하여 블록들의 순서를 무작위로 섞는 Shuffling을 통해 비도를 한층 높일 수 있다. 또한 시뮬레이션으로부터 디지털 컨텐츠 데이터 전체를 암호화하는 것보다 부분적으로 암복호화 하고 Shuffling 하는 기법이 정보처리 시간 면에서 훨씬 효율적임을 알 수 있는데 이는 결국 암호화하는 정보의 양을 줄일수록 암복호화 시간을 절약할 수 있음을 나타내고 있다. 또한 부분 암호화 기법은 정보의 중요도에 따라 암호화율과 블록 크기를 조절함으로서 적절한 정보보호와 암복호화 시간 단축의 이점을 동시에 제공한다. 특히 동일한 암호화율인 경우, 암호화 블록 크기가 작고 블록 수가 많은 것이 블록 크기가 크고 수가 적은 것보다 정보보호에 훨씬 유리함을 알 수 있다.

본 논문에서 제안한 부분 암호화 시스템은 MP3 데이터의 경우 10 KBytes의 Block Size, 10%의 암호화율만을 가지고도 충분한 정보보호 효과를 얻을 수 있는 만큼, 영상이나 음향 디지털 컨텐츠와 같이 데이터 양이 많고 품질에 이용자가 매우 민감한 경우에 활용성이 크다 하겠다. 따라서 디지털 컨텐츠 데이터의 종류에 따라 적절한 블록 크기와 암호화율을 선정한다면 저비용을 들여 상대적으로 높은 정보보호 효과 및 정보처리 속도를 얻을 수 있다. 이는 계속 증가하고 있는 포털 서비스 업체들의 경쟁력을 한층 더 높일 수 있을 것이며, 나아가 전자상거래 전반에 걸쳐 널리 활용될 수 있을 것이다.

참 고 문 헌

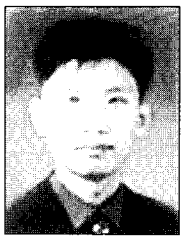
[1] 박창섭, '암호이론과 보안', 초판, 대영사, 1999.

[2] 이인수, "RSA 공개키암호 시스템 현황", 한국정보보호센터, 1998년 5월.
[3] 정은희, 이병관, "ECSSL(Elliptic Curve SSL) 기반 DIT(Digital Investment Trust) 에이전트", 정보처리학회논문지B, 제9-B권 제5호, 2002년 10월, pp. 599-608.
[4] 최용락, 소우영, 이재광, 이임영, '통신망 정보보호', 초판, 도서출판 그린, 1996.
[5] 홍도석, "포털서비스의 동향과 전망", 통신시장, 통권 제26호, 1999년 8월-10월.
[6] Dreifus, H., and Monk, J., "Smart Cards", 1st Ed., John Wiley & Sons, 1998.
[7] Fancher, C.H., "In your pocket : smartcards", IEEE Spectrum, Feb. 1997, pp. 47-53.
[8] Froomkin, A., "The Essential Role of Trusted Third Parties in Electronic Commerce", Ver. 1.02. Oct. 1996.
[9] Koblitz, N., "Elliptic Curve Cryptosystems", Math. of Computation, Vol. 48, 1987, pp. 203-209.
[10] Menezes, A.J., "Elliptic Curve Public Key Cryptosystems", Kluwer Acad. Pub. 1993.
[11] NIST FIPS PUB 46-2 (supercedes FIPS PUB 46-1), U.S. Department of Commerce, Dec. 1993.
[12] Rivest, R.L., Shamir, A., and Adleman, L.M., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, Feb. 1978, pp. 120 -126.
[13] Sun, H., "Computer and Network Security", Lecture by Rivest of MIT, http://theory.lcs. mit.edu, 2004.
[14] http://cnscenter.future.co.kr.

저자소개

황 선 태

서강대학교 수학과에서 학사, 미국 Case Western Reserve University 전자계산학과 석사 및 박사학위를 취득하였다. KIST 연구원, 현대전자연구소 책임연구원을 거쳐 현재 대전대학교 정보통신공학과 교수로 재직중이며 주요 관심분야는 정보보안, 스마트카드 기술/응용 등이다.



이 승 혁

대전대학교 정보통신공학과에서 학사 및 석사를 마치고, (주)코네스, ETRI 위촉연구원을 거쳐 현재 (주)니츠 정보보호기술연구소 연구원으로 근무중이며, 주요 관심분야는 Smart Card, 정보보안 등이다.

◈ 이 논문은 2004년 2월 15일 접수하여 1차 수정을 거쳐 2004년 8월 20일 게재확정되었습니다.