SOAP기반의 ebXML 암호화 설계 및 성능분석

Design and Performance Analysis of SOAP based ebXML Cryptography Systems

강민구
한신대학교 정보통신학과

Min-Goo Kang(kangmg@hs.ac.kr)

요약

본 논문에서는 XML 문서보안을 위해 SOAP기반의 ebXML암호시스템을 RSA알고리듬을 이용한 설계 방안과, 전자상거래상의 거래문서를 암호화하고 전송하는 최적화된 문서 보안시스템의 설계방안을 제안한다. 또한, 제안한 ebXML문서의 암호화문서에 대한 성능비교를 위해 대칭키 방식인 DES와 3DES, 비대칭키 방식인 RSA암호화 방식 및 제안한 RSA 암호화 방식을 이용한다.

ebXML 암호시스템의 성능비교는 동일한 블록크기와 문서크기를 가지고 각각 100회씩을 암·복호화에 걸린 시간을 비교하였으며, 제안한 SOAP기반의 ebXML을 적용한 전자상거래 사이트의 성능평가를 통해 암호화 시간 및 복호화 시간의 네트워크 성능을 분석한다.

■ 중심어 : □SAOP□ebXML 암호시스템□RSA□네트워크 성능분석□ 전자상거래□

Abstract

In this paper, a SOAP based ebXML cryptography system is proposed for the optimum XML document encryption using RSA algorithm in e-Marketplace. And ciphering algorithms of DES, 3DES, RSA, and proposed RSA were used for the performance analysis of ebXML cryptography system.

The network performance of ciphering and deciphering times is evaluated for its enhancement of SOAP based ebXML ciphering e-Marketplace systems using the same block and document sizes by computer simulations.

■ keyword : □SAOP□ebXML Cryptography System□RSA□Network Performance□e-Marketplace□

I. 서 론

오늘날 기업과 기업 간의 정보시스템 통합이 전자상거래의 필수 전제 조건이긴 하지만 기업의 정보시스템 노출 우려와 비즈니스 프로세스, 문서 등이 상이하기 때문에 쉽지가 않다.

이러한 필요성으로 인해 XML이 등장하게 되었으며, 이후 확장성과 유연성, 그리고 변환의 편이성 등으로 인해 사실상 기업 간 거래의 표준으로 XML이 사용되고 있다.

* 본 논문은 2008년도 한신대학교 학술연구비 지원에 의하여 연구되었습니다.

접수번호 : #080927-007
접수일자 : 2008년 09월 27일
심사완료일 : 2008년 10월 30일
교신저자 : 강민구, e-mail : kangmg@hs.ac.kr

이것은 곧 모든 산업과 범세계적인 차원에서 비즈니스 모델에 관계없이 전자상거래를 할 수 있는 기술적인 표준제정에 초점을 맞추고 있다.

특히 ebXML(electronic business extensible Markup Language)은 많은 e-비즈니스 프레임워크 중에서 가장 포괄적이고 상세하다. ebXML은 XML을 이용하여 인터넷 기반의 전자상거래가 가능하도록 제정하고 있는 표준이다[1].

문제는 정보화 사회가 발전함에 따라 정보의 가치에 대한 인식이 새로워지고 정보에 대한 보호가치가 높아지면서, 많은 위험을 지니게 되었다는 점이다.

암호기술은 암호 알고리즘을 사용하여 평문을 알아보기 힘든 형태로 변화시키는 방법으로 암호를 수행할 때 사용된 키를 소유한 사람만이 암호문을 해독하여 평문을 얻을 수 있다.

무엇보다 인터넷상에서 이뤄지던 대부분의 거래행위가 HTML형태의 문서로 이루어지던 것이 이제는 전자상거래(e-Marketplace)가 복잡화, 다국적화 되면서 어느덧 한계를 보이기 시작했다[2]. 즉, HTML은 보안에 취약하고 전자상거래를 구현하기에는 많은 제약이 뒤따른다.

따라서 본 논문에서는 ebXML환경에서 전자상거래 시스템을 구축하여, 사용자와 관리자간에 이뤄지는 거래행위에 대한 암호화 기술을 적용하여 안전한 전자상거래서비스를 제공할 수 있는 보안 형식을 제시한다.

II. ebXML과 암호화

2.1 ebXML의 설계목적 및 암호시스템

지난 몇 년간 XML은 인터넷을 통한 새로운 e-biz 환경에서 상호 교환할 데이터의 구조를 정의하기 위한 최상의 방법으로 활용되고 있으며, EDI보다 더욱 개방적이고 융통성 있는 비즈니스 거래를 가능하게 한다[3].

또한, 전자상거래라는 혁신적인 비즈니스 모델에서는 EDI보다 XML이 더욱 적합할지도 모른다. 그러나 비즈니스 프로세스 요구사항을 만족시킨다. 데이터 항목들의 의미를 표준화해가는 문서 설계 단계는 문서가 어떤 형식으로 표현될 것인지에 대한 문법적인 문제와 다른 사안이다.

ebXML은 비즈니스 프로세스에 관한 한 기존의 EDI에 대한 투자가 새로운 XML 기반의 구조에서도 보호될 수 있는 프레임워크를 제공하고 있다. 즉 모든 거래당사자들에게 상호 운용하고 있으며, 안전하고 일관성 있는 방법으로 광범위한 e-비즈니스 정보사용이 가능하도록 개방된 XML 기반의 내부구조를 제공하는 것을 목적으로 한다[3].

2.2 암호화 시스템

암호화(Cryptography)는 중간에 누군가가 데이터를 가로채더라도 이를 읽을 수 없도록 함으로써 무결성을 확보하는 역할을 한다.

암호화를 위한 구성 요소는 크게 평문, 암호문(Ciphertext), 그리고 평문을 암호화하고 복호화하는 비밀키(Secret Key) 세 가지로 구성되며, 이것들은 암호화의 초석이 된다.

암호화 방식에는 키를 기반으로 두 가지로 나누어지며, 이를 대칭키 알고리즘과 비대칭키 알고리즘으로 분류한다. 대칭키 알고리즘은 암호키와 해독키가 동일한 알고리즘이며, 이 키는 노출되면 안 되기 때문에 비밀키(secret-key) 알고리즘 이라고도 한다.

또한 비대칭키 알고리즘은 공개키(public key) 알고리즘이라고도 하는데 이 방법은 개인키(private key)를 각자가 관리하고, 다른 사람에게 해독을 위한 공개키를 배포하는 방법이다.

III. XML문서 암호화 설계

3.1 암호시스템 구성

본 논문에서 구현하고자 하는 전자상거래의 기본 시스템은 다음의 [그림 1]과 같다[2].

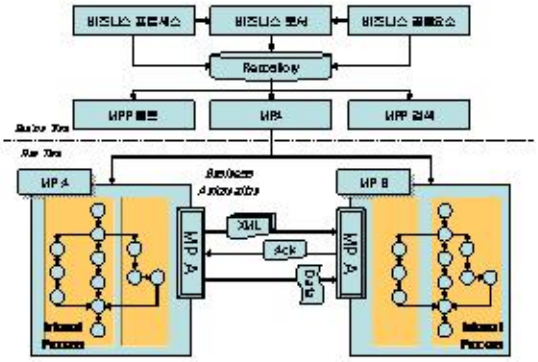

그림 1. 전자상거래 전체시스템

전자거래 A와 B가 있다고 가정하였을 때, A와 B는 공통적으로 ebXML 프레임워크상에서 거래하기 위한 시스템을 구축하여야 한다. 또한 자신이 구축해 둔 전자 거래 환경을 레지스트리에 등록하게 되고 거래 절차에 따라 판매자와 구매자간의 전자거래가 이루어지도록 한다[2].

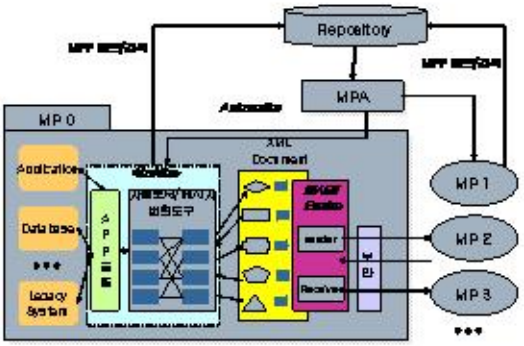

그림 2. MPA 기반의 세부시스템

이와 같은 경우, 전자거래 A와 B가 주고받게 되는 거래문서는 XML을 기본으로 하며, 네트워크 상(주로 웹서비스)에서 오고가는 XML문서에 공개키 암호화 방식을 적용시킴으로써 보다 안전한 거래행위가 이뤄지도록 한다[2].

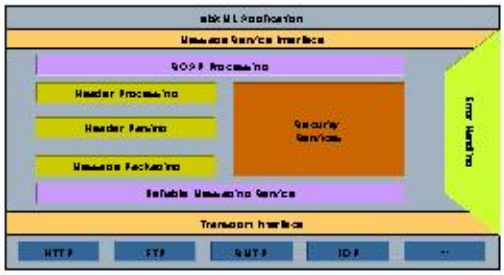

그림 3. ebXML 메시지 구조

이때 전송수준의 보안은 웹 서비스가 이용하는 프로토콜의 전송 계층 자체의 보안을 의미하며, 전송 수준의 보안이 중요한 이유는 SOAP 메시지가 전송계층에서 제공하는 데이터를 묶는 방식을 이용해서 캡슐화되기 때문이다[4].

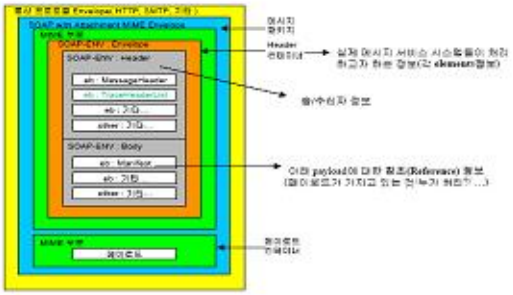

그림 4. SOAP 구조

3.2 제안 암호 알고리듬

본 논문에서 사용하는 암호화 방식은 비대칭 암호화 방식인 RSA 암호화 알고리즘을 적용하였다. 이는 XML 문서를 암호화 하는 방식에서 RSA만이 유일하게 XML 보안 표준에 명시되어 있기 때문이다.

또한 XML 서명 권고안은 비대칭 인증키를 사용하는 DSA 인증 알고리즘을 지원하지만, 이 알고리즘은 암호화에는 사용할 수 없고 디지털 서명에만 사용한다.

유사하게 XML 암호화 초안에서는 Diffie- Hellman 키 교환 알고리즘이라는 것도 명시해 놓았다. 이 알고리즘은 공개키 방식의 기반이 되는 알고리즘이고, 비대칭키를 사용하기는 하지만 비대칭 암호화는 아니며, 대칭키 암호화는 다음과 같이 중대한 문제를 가지고 있

다[2].

- 대칭키의 크기를 마음대로 조정할 수 없다.
- 부인(否認) 문제를 해결하지 못했다.
- 데이터 무결성에 대한 문제를 해결하지 못했다.

이러한 대칭키 암호화 방식에 비해 RSA 암호화 알고리즘은 먼저 키의 길이를 증가시키는 일은 쉽지만 이를 해독하는 계산시간은 오래 걸리기 때문에 상대적으로 안전하다.

또한, 여러 사람들이 공용으로 사용하는 시스템 상에서 비밀키를 안전하게 유포해야 하는 어려움을 겪지 않아도 된다. 공개키는 누구나 알아도 상관없는 값이기 때문에 공용 시스템에서도 단지 하나의 공개키와 개인키 쌍만을 유지하면 된다.

따라서 RSA 알고리즘은 디지털 서명에도 사용되고 비대칭키를 사용하므로 본 논문에서는 RSA 알고리즘을 이용한다.

3.3 XML 문서암호화

XML 암호화 연산은 크게 두 가지 사용사례로 나뉜다. 하나는 임의의 옥텟을 암호화하는 연산이고, 다른 하나는 XML 데이터를 암호화하는 연산이다. 이러한 구분이 필요한 이유는 XML 암호화 초안에서 XML 데이터의 암호화와 일반적인 옥텟의 암호화 사이에 약간 다른 의미를 부여하고 있기 때문이다.

XML 암호화는 XML문서의 내용이 의도된 사용자에게만 구별 가능하고, 그 외의 사람들에게는 알 수 없도록 XML문서를 암호화하는 방법을 기술한다.

W3C XML 암호화 작업 그룹은 XML문서와 그 일부분을 포함한 디지털 콘텐츠를 암·복호화하는 절차를 개발하고, 의도된 사용자만이 복호화할 수 있도록 정보들과 암호화된 내용을 표시하는데 사용하는 XML 구문을 정의한다. XML 암호화는 전달되는 정보뿐 아니라 저장된 정보에 대해서도 기밀성을 제공한다.

IV. ebXML문서암호화 구현시스템

4.1 ebXML 문서시스템 구현

본 논문에서는 웹 환경에서 서버와 클라이언트간의 거래 문서를 주고받을 때 거래문서인 XML 문서를 암호화시킴으로써, 사용자간의 안전한 거래가 가능하도록 한다. 작성된 XML 문서의 구조를 해석하고, 해석되어진 문서의 요소를 검색하여 중요한 거래 정보가 담겨있는 요소 부분을 암호화한다.

이와 같이 구현되어진 암호화 시스템은 부분암호화뿐만 아니라 전체 암호화도 가능하도록 설계되었다[5].

4.2 ebXML 문서 암호화

4.2.1 암호화 처리 과정

암호화되어야 하는 데이터를 옥텟 열로 변환한다. 직접적으로 암호화될 데이터가 XML요소나 XML요소 내용일 경우의 옥텟열은 요소 혹은 요소내용을 UTF-8로 부호화한 문자열이다.

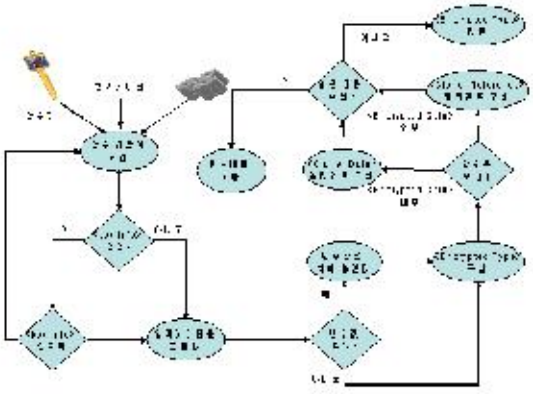

그림 5. ebXML 암호알고리듬 설계

이런 표현을 얻기 위해서 표준화된 XML 규격화 알고리즘을 사용할 수 있다. 특히 XML이 다른 명칭 공간 선언이나 명칭공간 속성들을 포함하는 환경에서 복호화 되어야 할 경우, 데이터 순차적으로 규격화된 XML의 사용을 고려해야 한다. 이는 이러한 차이점들이 데이터의 의미를 원하지 않는 방향으로 변화시킬 수 있기 때문이다.

4.2.2 복호화 처리 과정

본 논문에서 구현하고자 하는 ebXML 복호 알고리듬의 설계 내용은 [그림 6]과 같고, ebXML 암호화 구조와 명세내용은 [그림 7]과 같다[5].

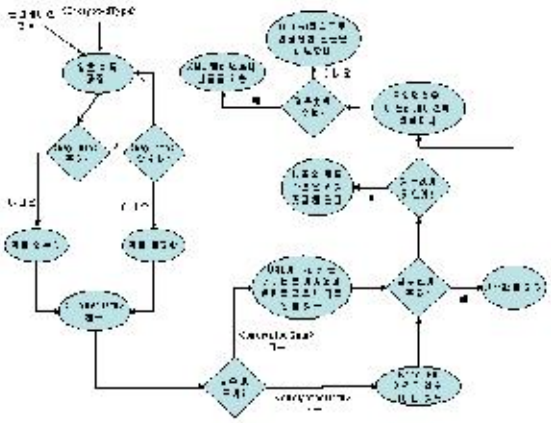

그림 6. ebXML 복호 알고리듬 설계

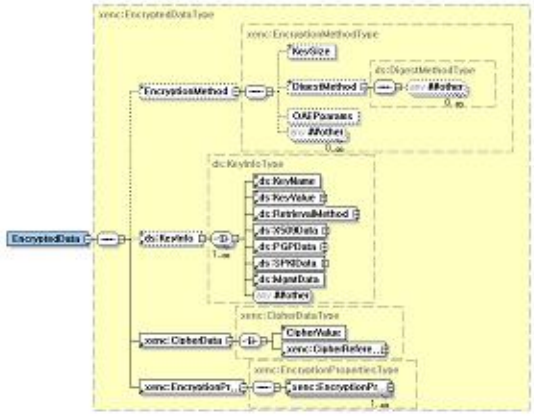

그림 7. ebXML 암호화 구조와 명세내용

[그림 7]의 ebXML 암호화 구조와 명세내용과 같이 <EncryptedData>나 <EncryptedKey>를 복호화를 위한 애플리케이션으로 <EncryptedMethod>, <KeyInfo>, 그리고 CipherData 요소를 얻는다.

이때, 암호화 알고리즘과 매개변수를 결정하고 복호화 키 정보를 얻는다. 복호화 키 정보가 <KeyInfo> 요소의 자식으로써 <EncryptedKey> 요소에 의해 표현되거나, <RetrievalMethod> 요소에 의해 참조되거나 <KeyName>에 의해 명명된다면, 키를 얻기 위해 이 처리 과정을 다시 적용한다.

적용한 후에 복호화를 위한 데이터를 얻고, 이 데이터를 검색하여 몇몇 변환을 적용시키거나 애플리케이션의 목적에 맞는 방법을 적용한다. 적용된 암호화 알고리즘, 매개변수, 그리고 키 정보를 이용해 암호문을 복호화한다.

4.3 XML 문서 암호화 고찰

온라인상에서 거래당사자간인 사용자 A와 B가 있다고 가정하였을 때, 사용자 A가 사용자 B에게 공개키 B를 요청해서 사용자 B는 비밀키 B를 이용하여 공개키 B를 생성한 후 사용자A에게 공개키 B를 알려준다.

이때 사용자 A는 사용자 B에게 받은 공개키 B를 사용하여 거래문서인 XML문서를 암호화 하였으며, 사용자 B는 사용자 A에게서 받은 자료를 비밀키 B를 사용하여 암호화된 XML문서를 복호화한다.

사용자 A에게 본인임을 증명하기 위해 비밀키 B를 사용하여 암호화를 함으로써, 사용자 B에게 받은 자료를 공개키 B를 이용하여 복호화하고, 자료를 받은 사람이 사용자 B임을 확인한다. 이로써 두 거래당사자인 사용자 A와 사용자 B 사이의 XML문서는 암호화되어 안전하게 전달되어질 수가 있게 된다.

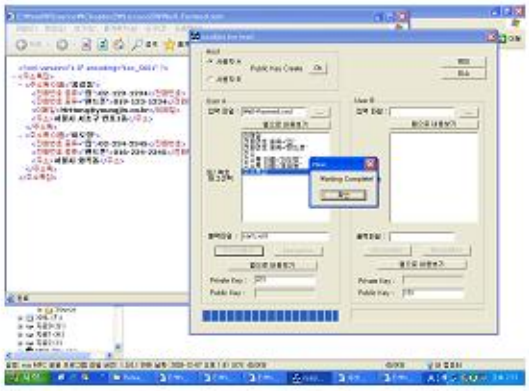

그림 8. RSA를 적용한 암호화 초기화면

그림 9. SOAP을 적용한 메시지 구조

4.4 SOAP 적용한 문서 암호시스템 성능분석

4.4.1 성능분석용 시스템모델 구성

테스트를 실행하기 위해 사용한 시스템 기반 구성을 나타내고 있으며, 성능차이에 대한 주요 지표는 처리량과 대기 시간을 기준으로 한다.

4.4.2 SOAP기반 XML암호문서의 리소스 성능분석

본 논문에서는 SOAP을 이용한 서비스에서는 일반적인 SOAP 프로토콜이 가지고 있는 단점을 보완 하여 설계를 한다. 일반적으로 SOAP 프로토콜은 SOAP 메시지를 생성하기 전에 XML 데이터를 파싱한 후 직렬화하여 전송한다.

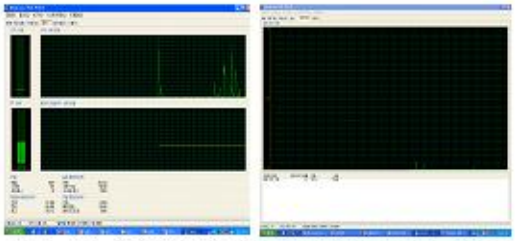

그림 10. SOAP환경에서 XML문서의 리소스 분석

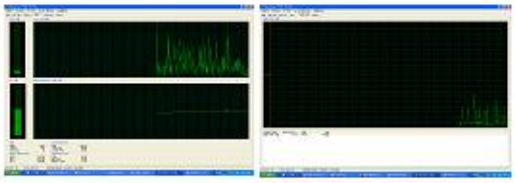

그림 11. 일반 웹환경에서 XML문서의 리소스 분석

또한 전송받은 SOAP 메시지는 헤더를 파싱한 후에 메시지 내에 있는 XML 데이터를 다시 한번 파싱을 한다. 따라서 일반적인 SOAP 구조에서 클라이언트가 요청을 한 후 서버에게 응답을 받기 위해서는 SOAP 클라이언트와 SOAP 서버에서 각각 2번씩 4번의 파싱 과정을 거치게 된다.

하지만 본 논문에서는 요청 과정에서 SOAP 서버의 파싱과정과 응답과정에서의 SOAP 클라이언트 파싱과정을 생략한다. 이것은 SOAP 프로토콜 메시지 처리 과정에서의 지연이 XML 데이터의 파싱과정에서 생기기 때문이다.

따라서 본 논문에서는 SOAP 프로토콜의 XML 데이터의 처리과정에서 생기는 지연을 수정하기 위해 파싱 과정을 생략한다. 기존의 웹 환경에서의 XML 문서 전송방식과 SOAP을 적용시켜 전송시킨 방식을 가지고 시스템에 미치는 영향을 비교 평가한다.

[그림 10]과 같이 동일한 XML 문서를 암호화하여 SOAP을 적용시키고, [그림 11]은 SOAP을 적용시키지 않은 상태에서 전송하였을 때 SOAP을 적용시킨 문서가 동일한 시스템의 리소스를 적게 차지한다.

4.4.3 제안한 RSA 암호/복호시간에 의한 성능분석

본 논문에서는 암호화의 성능비교를 대칭키 방식인 DES와 3DES, 비대칭키 방식인 RSA 암호화 방식과 본 논문에서 제안된 RSA 암호화 방식을 이용한다.

성능비교는 동일한 블록크기와 문서크기를 가지고 각각 100회씩을 암·복호화하여 걸린 시간을 비교하였으며 그 결과는 다음 [그림 12][그림 13]과 같다.

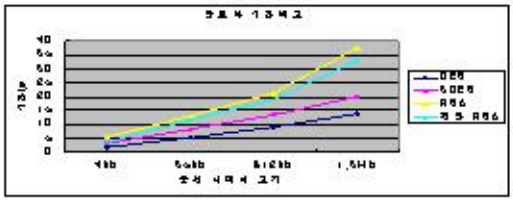

그림 12. SOAP 기반 ebXML의 암호화 시간비교

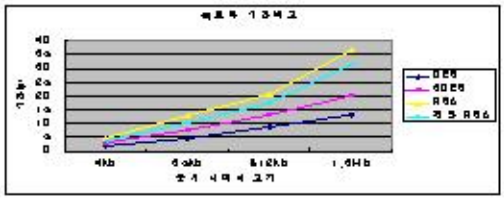

그림 13. SOAP 기반 ebXML 복호화 시간비교

[그림 12]와 [그림 13]에서 비대칭키 알고리즘을 사용하는 암호화는 특히 데이터 크기가 클 경우에 매우 느리고, 제안한 RSA 알고리듬의 성능이 우수하다. 이는 대용량 크기의 ebXML 데이터 암호화를 수행할 때는 사용되지 않고, 대용량의 데이터를 암호화할 경우에는 대칭 알고리즘을 사용해야하며, 비대칭 알고리즘은 키 교환을 수행할 때 사용할 수 있다.

V. 결 론

본 논문에서는 전자상거래상의 XML문서를 RSA 기반 알고리즘을 적용한 문서를 암호화시키고, 이를 ebXML 환경에서 거래문서를 주고받을 때 발생할 수 있는 문서정보의 유출을 방지하기 위해 XML문서를 RSA기반의 알고리즘을 적용하여 문서를 암호화하는 설계방안을 제안한다.

또한 제안한 XML문서의 암호화에 대한 성능분석을 위해 SOAP을 적용한 전자상거래 사이트의 성능평가를 통해 암호화시간과 복호화 시간의 네트워크 성능을 분석하였다.

컴퓨터 시뮬레이션 분석의 결과로 기존 방식과 비교하여 암호화속도는 부분암호화와 비슷하며, 부분암호화에 비해 안정성 측면에서 기존방식보다 안전하다.

향후 연구방향으로 ebXML 응용서비스 통합과 다양한 공급자 간의 상호운용을 위한 기반 정보보호 기술에 대한 연구가 필요하다.

참 고 문 헌

[1] http://www.ebXML.org

[2] 이만영, 김지홍, 송유진, 염흥열, 이임영, *인터넷 보안기술*, 생능출판사 pp.64-103, 2002.

[3] 박창섭, *암호이론과 보안*, 대영사, pp.178-179, 1999.

[4] T. Imamura, B. Dillaway, and E. Simon, *XML Encryption Syntax and Processing*, 2002.

[5] T. Imamura, B. Dillaway, and E. Simon, *XML Encryption Syntax and Processing*, 2002.

[6] F. Daniela and K. Donald, "Storing and Querying XML Data using an RDBMS," IEEE Data Engineering Bulletin., Vol.22, No.3, pp.27-34, 1999.

[7] J. P. Mueller, *Using SOAP*, 2001(9).

[8] 이진호, 홍성찬, 강민구, 문혜준, "ebXML을 이용한 문서 암호화시스템 설계 및 구현", 2004년 한국인터넷정보학회 춘계학술발표대회, 2004(5).

저 자 소 개

강 민 구(Min-Goo Kang) 정회원

- 1986년 2월 : 연세대학교 전자공학과(공학사)
- 1989년 2월 : 연세대학교 전자공학과(공학석사)
- 1994년 2월 : 연세대학교 전자공학과(공학박사)
- 1985년~1987년 : 삼성전자 통신연구소 연구원
- 1997년~1998년 : 오사카대학 통신공학과 Post Doc.
- 1994년~2000년 : 호남대학교 정보통신공학과 교수
- 2000년~현재 : 한신대학교 정보통신학과 교수

<관심분야> : 모바일정보통신, 디지털방송통신시스템