한국산학기술학회논문지
Vol. 4, No. 3, pp. 150-154, 2003

안전한 FTP 서비스를 위한 부인방지 모듈 설계

이원호 · 오명관* · 한군희**

Design of Non-repudiation Module for Secure FTP Service

Lee won-ho, Oh myung-kwan* and Han kun-hee**

요 약 본 논문에서는 송신자와 수신자가 각자의 이익을 위해 메시지의 전송 사실을 부인하는 것을 방지하는 발신처 부인방지와 수신처 부인방지 서비스를 제공하고 통신망에서 오류에 의한 전송 실패와 수신자의 파일 수신 사실의 부인을 방지해 주는 전송 부인방지 서비스를 제공하는 FTP 모델을 설계한다. 설계된 FTP 모델은 GSS-API를 사용하여 소스 수준에서 호환성을 갖도록 안전성 서비스에 대해 일관된 인터페이스를 제공하고, 응용 클라이언트와 응용 서버간의 안전한 문맥을 확립하기 위해 세션 키를 사용하여 효율적인 키 사용으로 공개키 시스템에서의 오버헤드를 최소화하였다.

Abstract This paper designs the secure FTP model which provides origin non-repudiation and receipt non-repudiation service that sender and recipient profit of each other to prevent the repudiated of transmission of message and which provides the delivery non-repudiation service to prevent the repudiated of file reception and fact of the transmission failure of an error from the network. The FTP model which is designed to use the GSS-API and in order to have compatibility from source level, with security service it provided the interface which is consistent, establishes the secure context which application client and application server for is safe the session key which overhead from opening to the public key system with efficient key use and it used it minimized.

1. 서 론

급속한 정보화 추세에 따른 컴퓨터의 대량 보급과 전산망의 확대는 정보 이용의 편리성과 효율성을 극대화 시키고 있으며 국가 산업 경쟁력의 근간이 되고 있다. 이러한 정보화 추세는 정보의 신속한 제공, 다양한 정보의 접근 등 여러 측면에서 긍정적인 효과를 가져왔지만 시스템 장애, 컴퓨터 범죄, 컴퓨터 바이러스, 프라이버시 침해 등 역기능적인 부작용 또한 심각하게 대두되고 있다.

현대의 컴퓨팅 환경은 통신 시설의 발전과 인터넷의 발전으로 인해 개방형 분산 시스템 환경으로 가는 추세에 있다. 분산 시스템 환경에서는 컴퓨터가 네트워크에 연결되어 있고, 다양한 사용자가 공통적으로 서비스를 이용하기 때문에 고의적이든 아니든 심각한 보안 문제를 가지게 된다.

이러한 보안 문제를 해결하기 위한 대책으로 부분적인 정보보호 기능들이 제시되어 왔고, 종합적인 정보보호 문제 해결 보다는 지엽적인 문제를 해결하는 상용 정보보호 서비스 시스템의 개발이 주류를 이루고 있다. 그러나 이들 시스템은 단순한 인증이나 접근통제 서비스만이 적용되고 있는 실정에 있다. 이처럼, 지금까지는 메시지 기밀성, 사용자 인증성, 정보 무결성 보장, 전자서명 등의 다양하지만 지엽적인 보안 서비스를 제공해 오고 있었으나, 최근 인터넷 등과 같은 공중 통신로를 통하여 전자적인 서비스를 제공할 때에 약속된 프로토콜을 위반한 송 · 수신자 쌍방간의 행위에 기술적인 증거를 제공하고, 논쟁 발생시 법적 근거로 제공할 수 있는 부인방지라는 새로운 서비스가 필요하게 되었다. 즉, 암호화 및 전자서명을 이용한 전자문서교환, 전자계약, 전자상거래 등의 응용분야가 향후 크게 활성화 될 것으로 예상되지만 실제 적용에 있어서는 개인의 행위에 대한 부인 가능성이 있으며 이를 방지하기 위한 부인방지 서비스의 제공이 필요하다.

따라서, 일관된 정보보호 정책을 가지고 통합 정보보호 기능을 수행할 수 있는 시스템이 필요하며, 이 시스템은 정보보호 서비스에 대한 인터페이스인 GSS-API를 개발하여 응용 프로그램 개발자에게 각각의 응용 프로그램에 부합하는 정보보호 기능을 구현할 수 있는 환경을 만들어줄 수 있어야 한다. 어떤 특정한 응용 서비스를 원하는 사용자가 허가를 받은 사용자라면 응용 서

대천대학
*혜전대학
**천안대학교

버와 통신할 때 정보보호 서비스가 복합적으로 작용하여 안전한 통신을 할 수 있도록 하는 것이다.

본 논문에서는 위에서 언급한 통합 정보보호 기능을 수행하는 시스템에서 최근의 통신환경에서 필수적으로 요구되고 있는 부인방지 서비스의 제공을 위한 요소를 설계하고 설계된 부인방지 서비스 제공 요소를 적용하여 안전성을 확보한 FTP 모델을 제안하고자 한다. 본 논문의 구성은 2장에서는 통합 정보보호 기능을 수행하는 시스템의 일반적인 개요와 하부 메커니즘, 부인방지 서비스의 응용분야에 대해 소개하며, 3장에서 부인방지 서비스를 제공하는 안전한 FTP 모델을 제안하며, 마지막 4장에서 결론 및 향후 연구 방향에 대해 논의하도록 하겠다.

2. 시스템 개요 및 부인방지 서비스

2.1 통합 정보보호 시스템 개요

통합 정보보호 시스템은 시큐리티 도메인 서버, 응용 클라이언트, 응용 서버의 세 부분으로 나뉘어져 있다.(Figure1)

응용 클라이언트가 특정한 응용 서비스를 요청하면 시큐리티 도메인 서버의 도움으로 인증이 이루어지고 권한속성과 안전한 세션을 위한 세션키를 분배받게 된다. 응용 클라이언트는 응용 서버가 세션키를 확립하기 위한 정보를 보내주고 이에 따라 응용 서버가 세션키를 분배받은 후에는 응용 클라이언트와 응용 서버 간에 안전한 통신이 가능해 지는 것이다. 시큐리티 도메인 서버에는 인증 서버(Authentication Server), 권한속성 서버(Privilege Attribute Server), 키 분배 서버(Key Distribution Server)가 있고 각 시큐리티 도메인 서버내의 안전한 데이터를 저장하는 장소인 시큐리티 관리 정보 베이스(SMIB)가 있다.

각 서버들의 기능을 간단히 살펴보면, 인증 서버는 사용자에 대한 신분을 도전-응답 방식을 사용하여 확인

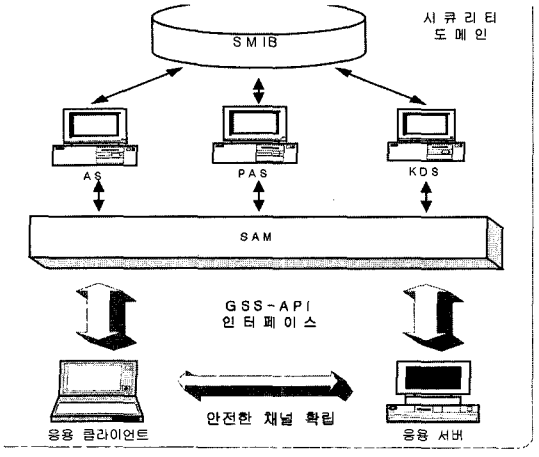

Figure 1. 시큐리티 도메인 시스템

해 주고, 권한속성 서버는 사용자에 대한 권한 속성 즉 접근통제를 위해 권한속성 인증서(Privilege Attribute Certificate)와 키 분배 서버에 접근할 수 있는 티켓을 발부해 준다. 키 분배 서버의 역할은 양단간에 안전한 세션 확립을 위한 키 분배이다. 세션 키에 대한 정보를 생성하고 다중의 도메인인 경우는 키 분배 서버의 공개키 메커니즘을 활용하여 안전하고 효율적인 키 분배를 한다. 생성하는 데이터는 응용 서버에 접근을 허락하는 서비스 티켓과 각 사용자에 대한 공개키 관리 등의 역할을 수행한다.

2.2 시스템의 특징

2.2.1 GSS-API

GSS-API는 시큐리티 신임장이나 기본 신임장을 사용한다. 신임장에는 시큐리티 서버가 클라이언트나 응용 서버에게 보내는 정보가 들어 있는데, 시큐리티 서버와 클라이언트, 서버 사이의 공유되는 비밀 정보도 포함되어 있다. 그래서 클라이언트나 서버의 패스워드나 세션키로 암호화한다. 신임장을 받은 클라이언트 사이에 시큐리티 문맥이 확립되어 안전한 채널을 확립하게 된다.

Figure 1에서 보면 알 수 있듯이 사용자(응용 클라이언트나 응용 서버)는 GSS-API를 호출함으로써 하부 메커니즘을 이용하게 된다. 사용자는 메커니즘의 작동에 관해서는 알 필요가 없고 GSS-API가 일반적인 형태로 제공하는 서비스들의 인터페이스를 이용하여 정보보호 서비스를 제공받는다[2].

2.2.2 공개키 생성 메커니즘

사용자가 전자 서명 서비스를 요구할 경우 클라이언트 시스템에서는 사용자에 대한 공개키 쌍을 생성한다[6]. 그리고 사용자 공개키에 대한 인증서를 생성하여 인증서에 대한 공증을 받기 위해 키 분배 서버에게 인증서를 보낸다. 이 인증서를 수신한 키 분배 서버는 자신의 비밀 키로 전자 서명하여 인증서에 대한 공증을 하고 클라이언트 시스템에게 되돌린다. 안전한 채널이 확립된 이후에 전송되는 데이터에 대해서는 각 사용자가 자신의 비밀 키로 전자 서명하고 또한 응용 서버 측에서 수신한 데이터는 사용자의 공개키로 검증한다[1].

2.2.3 세션 키 생성 메커니즘

안전한 통신을 하기 위한 채널 확립을 위해 양측의 정보보호 서비스 문맥 관리기는 기본 키와 세션 키 패키지를 소유하게 된다.

일단 키 정보를 공유하게 되면 세션 키를 생성하는 요소들을 가지고 문맥 확립 동안에만 사용하는 무결성 세션 키와 기밀성 세션 키를 생성한다. 이러한 방법으로 생성한 결과값을 키로 사용함으로 키 생성에 대한 안전성을 보장할 수

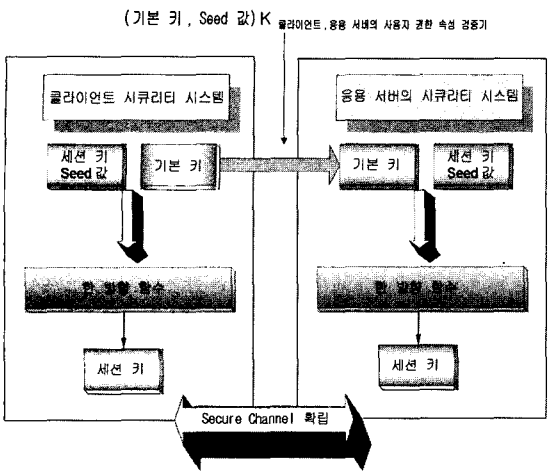

Figure 2. 세션 키 생성 구조

있게 되고 키를 생성한 시드 값의 유출을 방지할 수 있다.

2.3 부인방지 서비스의 응용분야

인터넷 등과 같은 공중 통신로를 통하여 전자적인 정보를 교환할 경우 송·수신자간에 상호 약속된 프로토콜을 위반하고 자신의 행위를 부인하는 위험성이 상존하게 된다. 예를 들면 인터넷 쇼핑몰을 통해 물건을 구입한 후 정당하게 지불을 완료했으나 상점에서 지불받지 못했다고 부인을 하는 경우 고객은 손해를 입을 수 있다. 부인방지 메커니즘에 근간한 다양한 부인방지 서비스가 실제 제공된다면 대부분의 응용분야에서 이와 같은 논쟁을 미연에 방지하고 적절히 해결할 수 있는 기반구조로 사용될 수 있다. 부인방지 서비스의 적용 가능한 응용분야로는 다음과 같은 것들이 있다.

1) 전자계약

국내에서는 전자서명법이 제정되어 1999년 하반기부터 발효되었다. 이에 따라 전자적인 수단으로 이루어지는 계약이 기존의 인감을 이용한 물리적인 계약과 동일한 효력을 인정받게 되며 향후 정보화 사회로의 발전에 큰 역할을 할 것으로 기대된다. 공정한 전자계약이 이루어지려면 프로토콜을 위반하거나 행위를 부인하는 것을 방지할 수 있는 부인방지 서비스가 반드시 필요하다.

2) 전자상거래

최근 인터넷 쇼핑, 온라인 주식거래, 인터넷 은행 등 전자상거래 시장이 크게 활성화되고 있다. 전자상거래는 현금이 오고 가는 상거래로서 만일 행위의 부인이 가능하다면 전자상거래의 기반 자체가 흔들리게 되며, 공정한 전자상거래가 이루어지기 위해서는 부인방지 서비스가 필수적으로 사용되어야 한다.

3) 온라인 요금납부

최근 인터넷이 발달하면서 기존의 각종 요금 납부 방식이 온라인 방식으로 대체되는 추세에 있다. 즉 전자우편을 통한 요금청구, 온라인 지불, 전자영수증 등이 가능한 것이다. 이러한 요금 납부 방식이 이용되려면 적절한 부인방지 서비스가 제공되어야 한다. 특히 온라인 지불에 대해 전자영수증을 받은 경우 이의 유효성을 부인방지 서버가 확인해 주고 사용자 시스템의 고장 시에도 유효성을 증명해줄 수 있도록 부인방지 토큰을 저장해 주는 서비스도 필요하다고 하겠다.

3. 부인방지 기능을 갖는 FTP 설계

3.1 부인방지 서비스의 필요성

기존에 서비스되고 있는 FTP들은 사용자의 ID와 패스워드가 평문으로 전송되기 때문에 안전한 인증 메커니즘을 가질 수 없고, 또한 FTP서버가 클라이언트의 호스트나 네트워크의 신뢰성을 확인할 수 없어서 침입자에 의한 파괴, 변조, 데이터의 불법 유출 등이 발생할 수 있다. 이러한 문제점은 전자상거래 등 여러 분야에서 FTP를 적극 활용하는데 있어 심각한 장애 요소가 되고 있다. 이에 인증, 접근통제, 무결성, 기밀성 서비스 등을 FTP에서 제공할 수 있도록 하는 연구들이 진행되고 있다.

하지만 이들 서비스만으로는 허가된 내부 사용자에 의한 불법 행위 발생 등에 대해서는 안전성을 보장할 수가 없다. 즉, 메시지의 수신자가 메시지 수신 사실 자체를 부인하거나, 수신된 메시지 내용을 변조하여 자신에게 이로운 변조된 메시지를 받았노라고 하는 행위, 메시지의 송신자가 메시지의 발신사실 자체를 부인하거나, 송신된 메시지를 변조하여 자신에게 이롭도록 수정한 후 자신이 보낸 메시지라고 주장하는 행위를 막지 못한다[3, 6]. 본 논문에서는 이러한 행위를 사전에 방지하여 보다 안전한 FTP 서비스를 제공할 수 있도록 부인방지 서비스가 제공되는 FTP 모델을 설계한다.

3.2 특징

기존의 FTP가 기본적인 정보보호 서비스를 제공하지 못하므로, 서비스를 제공하기 위해서는 추가적인 모듈이 설계되어 첨가되어야 한다.

이 모듈은 기존 FTP의 파일 전송 모듈과 규칙기반 접근통제를 제공하기 위한 ACL 관리 모듈, GSS-API 처리 모듈, 부인방지 정책 관리 모듈 등이다.

설계된 FTP 모듈의 구조는 Figure 3과 같다. 시큐리티 도메인 시스템의 구축으로 설계된 FTP는 다음과 같은 특징을 갖는다.

· 사용자가 시큐리티 도메인의 인증서버에 의해 인증되어 있기 때문에 응용에서의 개별적인 인증과정이 필요 없으므로 FTP의 로그인시에 사용자 인증이 필요 없다.

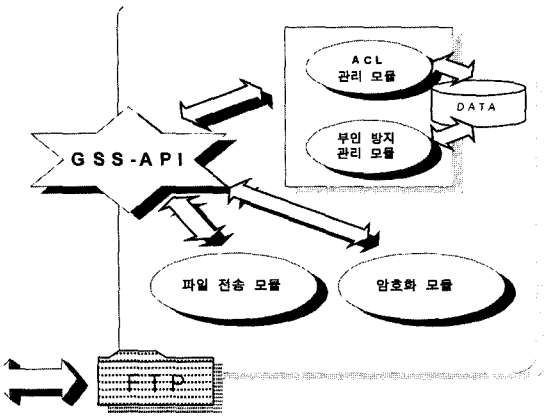

Figure 3. 설계된 FTP의 구조

· 사용자는 권한속성 인증서의 규칙(role)정보에 의해 접근권한을 가지므로 FTP는 규칙기반 접근통제를 사용한다.

· 세션 키 사용에 의해 안전한 채널이 확립되었으므로 FTP 클라이언트와 서버간의 기밀성이 보장된다.

· 분쟁 발생시에 해결을 위해 사용되는 부인방지 증명서는 사용자가 직접 수정하거나 위조할 수 없도록 시큐리티 도메인 서버에 의해 SMIB에 저장되고 관리되므로 부인방지 증명서의 무결성과 기밀성이 보장된다.

3.3 FTP 서비스의 운영 정책

FTP 서버는 관리자에 의해 3가지 운영 정책으로 부인방지 서비스를 제공한다.

· 정책 1 : FTP 클라이언트와 세션 키를 사용하여 기밀성 서비스만을 제공한다.

· 정책 2 : FTP 클라이언트의 요청 메시지에 대한 발신처 부인방지 증명서를 요구하고, 전송하는 파일과 함께 수신처 부인방지 증명서를 전송하여 클라이언트의 요청에 대해 부인방지 서비스를 제공해준다

· 정책 3 : 클라이언트의 파일 수신 사실에 대한 부인을 방지하기 위해 전송 부인방지 증명서를 요구하는 것으로 클라이언트는 전송 부인방지 증명서를 서버에 제출하지 않으면 파일을 암호화한 세션 키를 얻기 위한 시드 값을 얻지 못하게 되어 수신한 파일에 대해 복호화 작업을 수행할 수 없게 된다.

3.4 부인방지 증명서의 종류

FTP 서비스에서는 다음과 같은 3가지 부인방지 증명서가 사용된다.

· 발신처 부인방지 증명서(EOO)

클라이언트가 요청한 메시지에 대해 클라이언트의 비밀키로 전자서명을 한 증명서로 FTP 서버가 분쟁 발생에 대비해 SMIB에 저장한다.

· 수신처 부인방지 증명서(EOR)

FTP 서버가 클라이언트가 전송한 메시지의 수신 사실을 부인하는 것을 방지하기 위한 것으로 서버의 비밀키로 전자서명을 한 증명서로 클라이언트에 의해 SMIB에 저장된다.

· 전송 부인방지 증명서(EOD)

클라이언트가 요청한 파일에 대해 FTP가 파일을 전송하면 클라이언트는 파일을 수신했음을 서버에게 통지하는 증명서로 클라이언트가 파일을 수신하고도 이 사실을 부인하는 것을 방지한다. 클라이언트는 전송 부인방지 증명서를 서버에게 전송하지 않으면 서버에게서 파일을 암호화한 세션 키를 얻기 위한 기본 키 값을 얻지 못하므로 수신한 파일을 복호화할 수 없게 된다.

이들 증명서에는 부인방지 증명서 타입, 송신자의 식별자, 수신자의 식별자, 증명서 생성자의 식별자, 요청한 메시지 의 다이제스트, 증명서가 생성된 때를 식별할 수 있는 신뢰할 수 있는 타임스탬프 등의 정보가 들어간다[5].

3.5 프로토콜 흐름도

부인방지 서비스를 위해 정책별로 프로토콜이 확장되었다. 정책 2가 적용되는 경우에는 클라이언트는 발신처 부인방지 증명서를 전송하고, FTP 서버는 수신처 부인방지 증명서와 파일을 전송해 준다. 정책 3이 적용되는 경우 FTP서버는 파일을 제 2의 세션키로 암호화해서 전송해주며, 클라이언트는 전송 부인방지 증명서를 FTP 서버에 전송해 주어서 FTP 서버에게서 제 2의 세션 키를 생성하기 위한 기본 키를 수신 받아야 파일을 복호화하여 사용할 수 있다. 이 프로토콜들은 사용자가 직접 전자서명을 하고, 증명서를 다시 전송하는 것이 아니라 시큐리티 도메인 내에 인증서버에 한 번 인증을 받으면 시큐리티 도메인의 모든 시스템에 같은 정보가 유효하기 때문에 다시 로그인을 할 필요 없이 FTP의 내부 모듈서 정보보호 서비스를 모두 처리해 주는 것이다. 응용에서 GSS-API를 이용해 사용자에게 투명한 하부 메커니즘을 작동하기 때문에 편리함을 제공하고 있다.

EOO = [클라이언트 ID, 서버 ID, H(FTP서비스 요청 메시지), 타임스탬프] 클라이언트비밀키

EOR = [클라이언트 ID, 서버 ID, H(EOO), 타임스탬프] 서버비밀키

EOD = [FTP 로그정보, 타임스탬프]클라이언트비밀키

4. 결론 및 향후 연구

본 논문에서는 분산 통신망 환경에서 송수신자간의 부인방지 서비스와 파일 전송에 대한 전송 부인방지 서

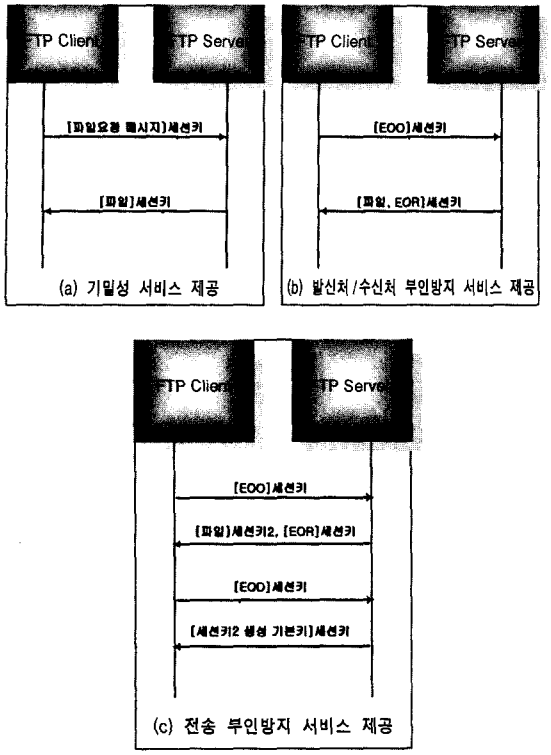

Figure 4. 정책별 프로토콜 흐름도

비스가 제공되는 FTP서비스를 제안하였다. 세션키의 사용으로 공개키 시스템에서의 오버헤드를 최소화한 효율적인 암호화 시스템과 GSS-API를 이용하여 시큐리티 도메인 내에서 응용에 독립적으로 부인방지 서비스가 제공될 수 있도록 설계되었다. 관리자가 보안 수준에 따라 정책 운영 레벨을 선택하여 부인방지 서비스를 제공 할 수 있도록 하였다. 부인방지 서비스가 제공되면 신뢰할 수 있는 통신망을 제공할 수 있게 될 것이고 지불 처리 프로토콜과의 확장을 하면 전자상거래 등의 응용에서 활용할 수 있을 것이다.

향후에는 구현된 시큐리티 도메인의 시큐리티 서버들과 안전한 FTP와의 연동이 이루어져야하며, 응용 개발시에 가장 중요한 것이 편리성과 신속성, 안정성이므로 계속적인 테스트를 통해 요구사항을 해결되어야 한다. 또한, GSS-API의 표준에서는 부인방지 서비스를 지원하지 않기 때문에 약간의 변형을 하여 사용하였는데, 표준화 동향 등을 조사하여 확장된 GSS-API 표준에 맞도록 수정이 이루어져야 할 것이다.

참고문헌

[1] 김동규 외, 분산통신망 환경 통합 정보보호서비스 소프트웨어 기술, 유니텍(주), 1998.
[2] J. Linn, GSS-API Ver. 2, RFC 2078, 1997.
[3] ISO/IEC 13888 - 1, 2, 3, "Information Technology - Security Techniques - Non-repudiation", ISO/IEC JTC1 SC27, 1997, 1998.
[4] J. Nechvatal, "Public-Key Cryptograp hy", NIST, 1991.
[5] J. Zhou, D. Gollmann, "A Fair Non- repudiation Protocol", Proceedings of 1996 IEEE Symposium Security and Privacy, 1996.
[6] J. Zhou, D. Gollmann, "Observations on Non-repudiation", Proceedings of Asiacryp t'96, 1996.