情 報 保 護 學 會 誌
第 15 卷 第 4 號, 2005. 8

프라이버시 보호를 위한 안전한 계산과 그 응용에 관한 고찰

유 준 석*, 홍 도 원*, 정 교 일*

요 약

인터넷의 발달 및 사회의 정보화는 다양한 업무의 전자적 처리를 가능하게 하여 많은 편리함과 이점을 제공하고 있지만 다양한 보안상의 문제점들이 나타나고 있다. 최근에는 개인의 민감한 정보 노출이 큰 문제로 부각되고 있으며, 이를 기술적으로 해결하고자 하는 노력들이 이루어지고 있다. 본 고에서는 다양한 응용에서 프라이버시 보호에 대한 해결책을 제시할 수 있을 것으로 기대되는 안전한 계산 기술에 대해 전반적으로 소개하고 최근의 관련 연구 동향을 정리한다. 또한 안전한 계산 기술의 실제적인 적용 가능 분야에 대해서 알아보고 프라이버시 문제에 대한 해결책으로서 안전한 계산 기술의 가능성을 살펴본다.

Ⅰ. 서 론

오늘날 사회구조는 산업 사회에서 정보화 사회로 빠르게 변화하고 있으며, 이러한 변화는 현실 사회의 업무를 전자적으로 처리 가능하게 함으로써 생산성을 향상시키고 편리성을 제공하는 등 많은 이점을 제공하고 있다. 정보화 사회에서 기존에 문서로 관리되던 다양한 정보는 전자적으로 저장, 유통, 관리되어 집적화, 대량화 되고 있으며, 특히 민감한 개인 정보를 다루는 금융, 의료, 교육, 정부 등의 분야를 포함한 사회 전 분야에서 정보화 작업이 이루어짐에 따라 정보의 가치 또한 급격히 상승하고 있다. 이러한 과정에서 수집된 다양한 정보는 통계, 마케팅, 연구 등의 목적으로 폭넓게 활용되고 있으며, 정보의 활용도 상승에 따라 정보 유출 및 악용 위험 또한 커지고 있는 상황이다.

민감한 개인 정보 노출의 문제는 인터넷 및 통신의 발달을 통한 협력 작업이 활성화됨에 따라 더욱 빈번히 발생할 가능성을 안고 있으며, 최근 들어 세계 각 국에서는 이러한 문제를 인식하고 법률적, 제도적 장치를 통하여 프라이버시 보호를 위한 기반을 마련하고 있다. 하지만 정보 노출의 문제를 제도적 장치로만 막을 수는 없으며, 기술적 장치 또한 마련되어야 할 것이다.

이와 관련하여 세계적으로 다양한 프로젝트들이 진행되고 있다. 미국의 스탠포드와 예일대는 2004년부터 IBM, HP, Microsoft와 같은 대표적인 IT 기업 및 다양한 사용자 그룹 등과 함께 PORTIA(Privacy, Obligations, and Rights in Technologies Information of Assessment) 프로젝트를 통하여 개인정보 침해 방지를 위한 다각적인 방안을 연구하고 있다. 이 외에도 IBM은 프라이버시 보호 연구를 위한 별도의 연구기관을 두고 다수의 프로젝트를 진행중이며, 미국의 MIPA(Medical Information Privacy Assurance)와 유럽연합의 주요 국가와 캐나다가 함께 수행 중인 PISA(Privacy Incorporated Software Agent)에서도 다양한 관련 연구를 수행하고 있다.

최근까지도 민감한 개인정보 노출에 대한 보안 기술은 전통적인 접근제어를 이용한 시스템 차원의 보안 및 사용자 인증, 암호 알고리즘을 이용한 데이터 암호화 기술 등과 같이 비인가자에 의한 부당한 데이터 접근을 막는 기술이 주류를 이루고 있다. 그러나 개인정보는 정당한 사용자의 정보 활용 과정 중에도 발생할 수 있으며, 최근 연구는 이러한 정보 유출까지 방지하려는 방향으로 변화되고 있다. 이와 관련하여 안전한 다자간 계산(SMP, Secure Multi-party Computation) 기술이 데이터 마이닝, 통계 분석, 과학 계산 등 다양한 응용에서의 정보 노출 문제를 적절히 해결할 수 있는 유용한 방안으로 인식되어 활발히 연구되

* 한국전자통신연구원 정보보호연구단 ({jsyu92, dwhong, kyoil}@etri.re.krr)

고 있다.

본 논문에서는 민감한 개인정보 노출 문제에 대한 유용한 해결책으로 사용될 수 있는 양자간 및 다자간 환경에서 안전한 계산의 전반적인 내용과 최근 연구동향을 살펴보고자 한다. 또한 이러한 기술들이 실제 적용될 수 있는 가능성과 그 응용분야에 대해 기술한다.

II. 관련 연구 및 기술

2.1 안전한 계산의 개요

안전한 다자간 계산은 Yao에 의해 처음 그 개념이 제안된 이 후, Goldreich-Micali-Wigderson에 의해 일반화되었고 지금까지도 많은 연구가 이루어져 오고 있다.[1,2] 일반적으로 안전한 다자간 계산 개념은 개산 참여자들의 입력값으로부터 함수 f를 계산하는 데에 있어서 계산 과정 종료 후, 참여자들은 자신의 입력값과 계산된 결과, 그리고 이들로부터 유추할 수 있는 것 외에는 어떠한 정보도 얻을 수 없도록 하자는 것이다.[3,4]

안전한 다자간 계산의 이러한 목적은 TTP를 사용하면 쉽게 달성될 수 있다. 즉, 계산 참여자들은 자신의 입력값을 TTP에게 비밀리에 전달하고 TTP가 결과를 계산하여 각 참여자에게 비밀리에 전송하는 것이다. 하지만 TTP를 사용하지 않고 동일한 기능을 수행할 수 있다면 이는 안전성 관점에서 훨씬 우수한 프로토콜이며, 따라서 TTP를 사용하지 않는 안전한 다자간 계산이 암호학의 중요한 부분으로 자리 잡아 왔다.

지금까지의 연구에 의하면 유한 도메인에서 정의된 모든 함수는 안전한 다자간 계산이 가능한 것으로 알려져 있고 이는 함수에 대한 결과를 계산하는 이진회로 구성을 기초로 하여 설명이 가능하다. 즉, 트랩도어 일방향 순열(trapdoor one-way permutation)의 존재를 가정하여 불확실 전송(OT, Oblivious Transfer)을 달성할 수 있고 불확실 전송을 통해 안전한 양자간 계산 프로토콜을 구성 할 수 있다. 또한 안전한 양자간 계산은 약간의 수정을 통하여 다자간 환경으로 확장될 수 있다.[3,4]

안전한 양자간 및 다자간 계산의 전반적인 사항은 이하 내용에서 좀 더 자세히 설명하도록 한다.

2.2 안전한 다자간 계산을 위한 요소기술

안전한 다자간 계산은 불확실 전송(OT, Oblivious Transfer), 위탁(commitment), 비밀분산(SS, Secret Sharing) 및 검증 가능한 비밀분산(VSS, Verifiable Secret Sharing), 영지식 증명(ZKIP, Zero-Knowledge Interactive Proof) 등의 다양한 요소기술에 기반하여 달성되며, 안전한 다자간 계산을 이해하기 위해서는 이러한 요소기술에 대한 이해가 필수적이다. 본 절에서는 안전한 다자간 계산 기술을 이해하는 데에 필요한 주요 기술에 대해서 간략히 살펴보도록 한다.

2.2.1 불확실 전송(OT, Oblivious Transfer)

불확실 전송은 두 참여자인 송신자 S와 수신자 R 간의 프로토콜로써 다음의 목적을 달성하기 위해 사용된다. 송신자 S는 비공개 입력비트 $b_1,...,b_n$을 가지고 수신자 R은 비공개 선택비트 $s \in \{1,..,n\}$를 가지고 있다(1-out of-n OT). 불확실 전송 프로토콜을 수행한 후, 수신자 R은 자신의 선택비트 s에 해당하는 b_s만을 획득하고 송신자 S가 소유한 나머지 비트에 대해서는 어떠한 정보도 얻지 못한다. 또한 송신자 S는 수신자 R이 몇 번째 입력비트를 얻었는지, 즉 선택비트 s에 대한 어떠한 정보도 알지 못한다. 여기서 전자의 경우는 송신자 보안(sender security), 후자는 수신자 보안(receiver security)라고 정의된다.[5]

불확실 전송은 다양한 문제에 기반하여 구성될 수 있으며, 임의의 함수 f를 계산하는 이진 회로에서 AND 게이트(이진 곱셈 연산)의 입력으로 사용 될 공유정보(additive share)를 구하는 과정에 이용된다.

2.2.2 위탁(Commitment)

위탁 문제는 개념적으로 금고를 예로 들어 설명할 수 있다. 비밀정보 s를 위탁하려는 사용자 A는 금고에 비밀정보 s를 넣고 잠근 뒤 금고를 열기 위한 키 조합을 기억한 후 사용자 B에게 금고를 전달한다. 이 때 사용자 B는 금고를 열기 위한 키 조합을 사용자 A로부터 얻기 전에는 금고를 열 수 없으므로 금고에 저장된 비밀정보 s를 알 수 없다는 특성을 지니며, 이를 은닉 속성(hiding property)이라고 한다. 또한 금고가 일단 위탁된 후에는 사용자 A가 금고에 들어있는 비밀정보 s를 변경할 수 없다는 특성을 가지며, 이를 구속 속성(binding property)이라고 한다. 암호학적 의미에서 위탁을 실현하기 위해서는 앞의 두 가지 속성이 만족되어야 한다. 이처럼 위탁이 이루어진 후, 사용자 A는 키 조합을 사용자 B에게 알려줌으로써 사용자 B가 비밀정보 s를 확인할 수 있게 한다.[4]

위탁은 다자간 계산의 비밀 분배 과정에서 딜러가 잘못된 분배값을 분배하지 못하도록 하고 재구성 단계

에서 참여자들이 잘못된 분배값을 내어놓는 것을 방지하는 데에 사용된다.

2.2.3 비밀분산(SS, Secret Sharing) 및 검증 가능한 비밀분산(VSS, Verifiable Secret Sharing)

비밀분산은 딜러와 다수의 에이전트 P_i(단, $i=1...n$) 사이의 프로토콜로써 Shamir가 처음 제안하였다.[6] 본 기법에서 딜러는 비밀정보 s를 특정 조건이 만족하는 분배값 s_i들로 나누어 각 에이전트에게 비밀리에 전달하고 이 후 일정한 임계치 이상의 에이전트들이 모일 경우에 다른 에이전트들에게 에 대한 정보 노출 없이 s를 복원해 낼 수 있다. 비밀분산은 안전한 양자간 계산을 다자간 환경으로 확장하는 데에 사용될 수 있지만 Shamir의 비밀분산 기법의 경우 딜러가 잘못된 분배값을 나누어주거나 비밀 복원 과정에서 에이전트가 일부러 잘못된 값을 내어놓는 등의 악의적인 공격자 환경에서는 안전하지 못하다.

이러한 문제를 해결하기 위해서 일반적으로 검증 가능한 비밀분산(VSS, Verifiable Secret Sharing) 기법이 사용되며, VSS는 Shamir의 비밀분산 기법에 위탁과 영지식 증명을 추가함으로써 달성될 수 있다.[4] VSS에서 딜러는 자신이 소유한 비밀정보 s에 대해 Shamir의 비밀분산 기법과 동일한 방법으로 분배값 s_i를 생성한다. 그리고 분배값 s_i에 대한 위탁값 C_i를 모든 에이전트에게 브로드캐스트하고, 해당 위탁값이 특정한 비밀정보의 분배값에 대한 것임을 모든 에이전트에게 영지식으로 증명한다. 또한 증명이 모든 에이전트에게 받아들여진 경우에만 P_i에게 분배값 s_i와 C_i에 대한 opening 정보를 비밀리에 전송함으로써 s에 대한 조각을 분배한다.[7]

분배값을 모아 s를 재구성하는 단계에서 에이전트 P_i는 자신의 분배값 s_i뿐 아니라 C_i에 대한 opening 정보를 함께 브로드캐스트하며, 다른 에이전트들은 C_i가 올바르게 열릴 경우에만 s_i를 정당한 분배값으로 받아들인다.

Ⅲ. 안전한 계산 기술

이미 언급한 바와 같이 안전한 다자간 계산 문제는 n명의 계산 참여자 $P_1,...,P_n$이 각 참여자들의 비밀정보 x_i를 입력으로 하는 임의의 공개 함수 $f(x_1,...,x_n)$를 계산하는 데에 있어서, 계산 종료 후에 각 참여자들이 계산 결과값 $y=f(x_1,...,x_n)$와 자신의 입력값 x_i, 그리고 이들로부터 유추할 수 있는 정보 외에는 알 수 없도록 하는 것이다.[3,4] 특히, 안전한 양자간 계산은 위 정의에서 계산 참여자가 두 명뿐인 특수한 경우(즉, $n=2$)로 생각할 수 있으며, 다자간 계산은 양자간 계산을 확장, 수정하여 달성될 수 있다.

본 장에서는 안전한 양자간 계산에 대해 설명한 후, 이를 확장하여 안전한 다자간 계산을 달성하는 내용에 대해서 전반적으로 설명한다.

3.1 안전한 양자간 계산

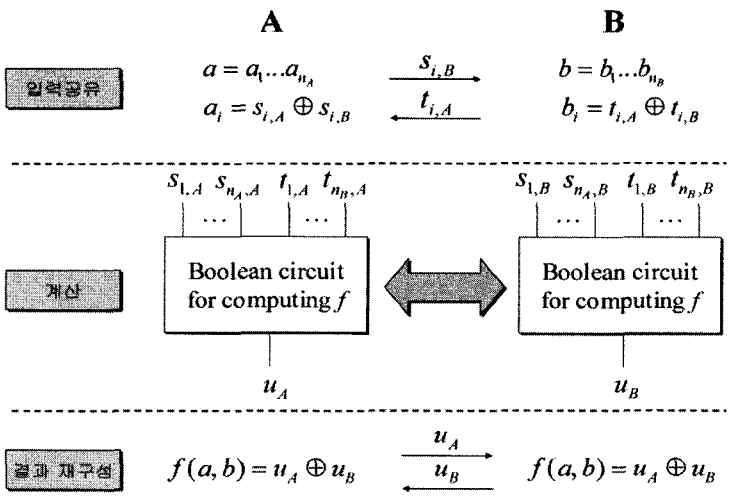
유한체 상의 모든 함수 f는 안전하게 계산될 수 있다고 알려져 있으며, 또한 불확실 전송을 사용하면 이를 달성할 수 있다는 것이 증명되었다.[1,8] 일반적으로 임의의 함수에 대한 계산은 이진 회로로 구성될 수 있으며, 임의의 함수에 대한 안전한 다자간 계산은 이러한 이진 회로의 구성을 바탕으로 달성된다.

간단한 예로 두 계산 참여자 A와 B가 각각 n_A비트 크기의 입력 a와 n_B비트 크기의 입력 b를 가지며, 한 비트의 출력을 내는 함수 $f:\{0,1\}^{n_A}\times\{0,1\}^{n_B}\rightarrow\{0,1\}$를 안전하게 계산하는 경우를 살펴보자. 함수 f는 다항식 시간에 계산될 수 있고 두 참여자는 함수 f를 알고 이를 계산하는 이진 회로를 가지고 있다고 가정하자. 이 때 참여자들이 가진 이진 회로는 n_A+n_B개의 입력 단자와 한 개의 출력 단자를 가지는 방향성 비순환 그래프(directed acyclic graph)로 생각할 수 있다. 그래프에서 입력과 출력부를 제외한 나머지 노드들은 이진 NOT, XOR, AND 연산에 해당하는 게이트들로 이루어져 있으며, 입력부에 값이 주어지면 각 값들은 그래프의 위상을 따라가면서 각 게이트에서 해당 연산을 수행하게 되고 결국 회로의 출력단에 결과값 $f(a,b)$가 설정된다.

일단 두 참여자가 이진 회로를 공유한 후, 함수 f를 안전하게 계산하기 위해서 참여자들은 다음의 세 단계로 구성된 프로토콜을 수행하며, 그림 1은 이를 도식화하여 보여주고 있다.

단계 1. 입력 공유(Input sharing)

참여자 A는 자신의 n_A비트 크기의 입력 a의 각 비트 a_i에 대해서 $a_i=s_{i,A}\oplus s_{i,B}$를 만족하는 두 개의 랜덤한 비트 $s_{i,A}$, $s_{i,B}$를 선택하여 $s_{i,B}$를 참여자 B에게 전송한다. 참여자 B도 동일하게 $b_i=t_{i,A}\oplus t_{i,B}$를 만족하는 $t_{i,A}$, $t_{i,B}$를 랜덤하게 선택하여 $t_{i,A}$를 참여자 A에게 전송한다. 각 참여자는 상대편으로부터 전달받은



〔그림 1〕 안전한 양자간 계산 프로토콜의 구성 예

값을 그림 1에서 보는 바와 같이 회로의 적절한 입력단에 설정한다.

입력 공유 단계는 각 참여자의 입력이 상대방에게 노출되는 것을 방지하기 위해서 수행되며, 여기서 s와 t를 공유정보(additive share)라고 한다.

단계 2. 계산(Computation)

입력 공유 단계를 통해 이진회로의 입력이 정해지면 회로의 위상에 따라 계산이 이루어지며, 이는 게이트별로 순차적으로 진행되거나 다수의 게이트에서 병렬적으로 진행될 수도 있다. 이 때 현재 게이트로의 입력은 입력 공유를 통해 얻어진 공유정보이며, 따라서 사용자 A와 B가 가진 회로의 각 게이트에서 처리된 결과값 u_A, u_B 또한 랜덤한 값으로써 사용자 A와 B의 원래 입력에 대한 어떠한 정보도 노출하지 않는다. 하지만 u_A와 u_B를 더하면 원래 입력에 대한 출력과 동일한 값을 얻게 된다. 이러한 불변성은 이진 회로의 NOT, XOR, AND 연산 게이트들에 대해서 모두 유지된다.

단계 3. 결과 재구성(Output reconstruction)

각 참여자는 회로의 출력단으로 나온 결과값을 상대 참여자에게 공개하고 각 참여자는 상대방으로부터 수신한 값과 자신의 결과값을 더하여 $f(a,b)$를 계산할 수 있다.

하지만 위의 예제는 두 계산 참여자가 준정직한(semi-honest) 경우, 즉 참여자들이 프로토콜 수행 과정 중의 메시지를 통해 어떠한 정보를 얻으려는 노력은 하지만 정해진 프로토콜을 그대로 따르는 경우에만 안전하며, 참여자들이 프로토콜을 따르지 않는 악의적인(malicious) 공격자 환경에서는 안전하지 않다. 예를 들어 부정한 참여자는 올바르지 않은 공유값을 상대에게 제공함으로써 상대방으로 하여금 잘못된 계산 결과를 얻게 하는 반면 자신은 올바른 계산 결과를 얻을 수 있다.

이처럼 악의적인 공격자가 존재하는 환경에서 프로토콜의 안전성을 확보하기 위해서는 앞에서 설명한 위탁 및 영지식 증명 등의 기술적인 요소들이 추가적으로 필요하며, 이를 통해 모든 참여자들이 준정직한 참여자처럼 행동하도록 만들 수 있다.[3,4] 이에 대해서는 다음 절에서 좀 더 살펴보도록 하며, 자세한 내용은 〔3, 4〕를 참고하기 바란다.

3.2 안전한 다자간 계산

안전한 다자간 계산은 안전한 양자간 계산을 수정, 확장하여 달성될 수 있다고 이미 언급하였다. 가장 기본적인 확장 방법은 각 참여자들이 입력 공유 단계에서 계산 참여자 수만큼 공유정보를 생성, 분배하고 계산 단계에서 참여자들 사이에 불확실 전송을 수행하는 것이다. 하지만 이러한 확장 방법은 악의적인 공격자 환경에서 프로토콜의 안전성을 제공하지 못 한다. 간단한 예로 악의적인 공격자 환경에서 매수된 참여자는 다른 참여자들의 분배값을 수신하여 자신만 계산 결과를 안 상태에서 프로토콜을 떠나거나 혹은 잘못된 분배값을 다른 참여자에게 제공함으로써 프로토콜을 방해할 수도 있다.

이러한 악의적인 공격자 환경에서의 문제를 해결하기 위한 핵심 기술로 검증 가능한 비밀분산(VSS) 기술이 사용되며, VSS는 앞 장의 2.3절에서 설명된 방법을 통해 정직한 참여자들이 안전하게 입력을 공유하고 올바른 결과를 얻을 수 있도록 보장한다. 이는 VSS 기법이 위탁 및 영지식 증명 기법을 통해 딜러 및 참여자들을 강제적으로 준정직하게 행동하도록 만들기 때문이다. 또한 VSS에서는 일정한 임계치 t명 이상의 참여자들이 모인 경우에만 결과를 계산해 낼 수 있다는 특성을 가지며, 따라서 t명 미만의 참여자가 매수되었다 하더라도 프로토콜의 안전성을 보장할 수 있다. 지금까지의 연구 결과에 의하면 암호학적 모델에서 임계치 $t < n/2$, 정보 이론적 모델에서는 $t < n/3$인 것으로 알려져 있다.[9]

Ⅳ. 이슈 및 동향

안전한 다자간 계산 개념이 제안된 이후로 프로토콜의 효율성과 안전성에 관한 사항은 항상 주요 주제로 다루어져 왔으며, 이러한 연구 방향은 최근까지도 이어져 오고 있다. 특히 최근 들어서는 다양한 분야에서 특정 응용에 안전한 다자간 계산 기술을 접목하려는 연구가 활발히 이루어지고 있다. 이하 내용에서는 안전한 다자간 계산의 주요 연구 주제 및 최근의 연구 동향에 대해서 설명한다.

4.1 프로토콜 안전성

안전한 다자간 계산에서 프로토콜의 안전성은 공격자 및 기타 사항들을 가정한 특정 모델 하에서 미리 정의된 안전성 조건을 만족하는가 여부에 따라 판단된다. 본 절의 이하 내용에서는 다자간 계산 프로토콜의 안전성을 평가하는 데에 필요한 가정과 안전성 의미에 대해서 설명한다.

4.1.1 공격자 모델

프로토콜의 안전성을 논하기 위해서 가장 기본적으로 가정되어야 하는 것이 공격자 모델이다. 일반적으로 다자간 계산에서 공격자는 프로토콜 참여자들 중 일정 수의 참여자를 매수하여 그들의 행동을 제어할 수 있을 뿐만 아니라 매수된 참여자들이 협력하는 형태로 동작하도록 할 수 있다고 가정한다. 공격자는 행동 양식에 따라 표 1처럼 분류되며, 준정직한 공격자는 수동적 공격자(passive adversary)라고도 불리고 악의적인 공격자는 능동적 공격자(active adversary), 비잔틴 공격자(Byzantine adversary) 등으로도 불린다.

〔표 1〕 일반적인 공격자 모델 분류

분 류	설 명
준정직한 공격자 (semi-honest adversary)	공격자는 매수된 참여자가 가진 모든 정보(내부 데이터 및 프로토콜 수행 과정에서 수신한 데이터)를 얻을 수 있으나 참여자는 프로토콜을 여전히 따름
악의적인 공격자 (malicious adversary)	공격자는 매수된 참여자를 완전히 제어하며, 참여자가 프로토콜을 벗어나는 행동을 수행하도록 할 수 있음

〔표 2〕 공격자의 능력에 따른 분류

분 류	설 명
계산적 설정 (computational setting)	공격자의 계산 능력은 다항식 시간으로 제한되며, 이 경우에 안전성은 증명되지 않은 가정, 예를 들어 일방향 트랩도어 순열의 존재 등에 기반하여 이루어짐
정보 이론적 설정 (information-theoretic setting)	공격자의 계산 능력은 무한대임을 가정하며, 이 경우에 안전성은 특별한 가정 없이 증명 가능함
비표준 설정 (non-standard setting)	공격자의 계산 능력이 무한대임을 가정하지만 다른 조건(메모리, 통신채널 등)을 제한하며, 이 경우에 안전성은 특별한 가정 없이 증명 가능함

또한 공격자는 매수할 참여자의 선택 시점에 따라서 비적응적 공격자(non-adaptive adversary)와 적응적 공격자(adaptive adversary)로 세분된다. 비적응적 공격자는 정적 공격자(static adversary)로도 불리며, 이 경우 공격자는 매수할 참여자를 프로토콜 시작 전에 모두 선택하게 된다. 반면 적응적 공격자는 자신이 가진 정보에 기반하여 프로토콜 중에 언제라도 매수할 참여자를 선택할 수 있다. 이 외에도 공격자 모델은 소유한 능력에 따라서 표 2와 같이 분류되기도 한다.

4.1.2 통신 모델

통신 모델은 계산 참여자들 사이의 메시지 전달에 어떤 특성을 가진 채널이 사용되는지를 정의한다. 기본적으로 통신 모델은 암호학적 모델과 정보 이론적 모델로 구분할 수 있으며, 표 3에서 두 모델의 차이를 설명하고 있다. 암호학적 모델에서 안전성은 공격자가 다항식 시간의 계산 능력을 지닌다는 가정의 암호학적 관점에서만 보장되며, 계산적 모델(computational model)이라고도 불린다. 하지만 정보 이론적 모델에

〔표 3〕 기본 통신 모델

분 류	설 명
암호학적 모델 (cryptographic model)	공격자는 전송되는 모든 메시지에 접근할 수 있으나 정직한 참여자들 사이에 교환되는 메시지를 변경할 수는 없음
정보 이론적 모델 (information-theoretic model)	공격자는 정직한 참여자들 사이에 교환되는 메시지에 대한 정보조차 얻을 수 없음

서는 참여자들 사이에 안전한 채널이 존재한다고 가정한다. 즉, 공격자가 무한 계산 능력을 지녔다 하더라도 통신 내용의 안전성이 보장된다. 이런 의미에서 정보 이론적 모델은 안전한 통신로(secure channel)를 가정한 모델이라고 불리기도 한다.

때로는 능동적 공격자 환경에서 모든 참여자들이 사용할 수 있는 브로드캐스트 채널을 가정하기도 한다. 일반적으로 능동적 공격자 환경에서 매수된 참여자는 브로드캐스팅 시에 참여자들에게 동일한 메시지를 브로드캐스트하지 않고 각기 다른 메시지를 전달할 수도 있으며, 정직한 참여자들은 이러한 사실을 알지 못할 수 있다. 하지만 브로드캐스트 채널을 가정한 통신 모델에서 참여자들은 자신이 수신한 메시지가 정직한 참여자로부터 변경 없이 수신되었음을 확신할 수 있다.

또한 다자간 계산에서 채널은 동기 채널(synchronous channel)과 비동기 채널(asynchronous channel)로 구분되기도 한다. 우선 동기 채널은 프로세서가 일정 시간범위 안에서 동기를 맞출 목적으로 클락을 가지며, 메시지가 전송되면 정해진 시간 안에 메시지의 도착이 보장되는 채널이다. 즉, 프로토콜이 일정 라운드의 메시지를 통해 진행된다고 가정할 때 각 라운드에서 프로토콜 참여자는 다른 참여자에게 메시지를 보내고 전송된 모든 메시지는 다음 라운드가 시작되기 전에 전달된다. 반면 비동기 채널에서는 메시지의 전송이나 전송 시간의 한계가 보장되지 않는다.

4.1.3 안전성 정의 및 개념

전통적으로 프로토콜의 안전성은 앞에서 가정한 다양한 조건의 모델 하에서 프로토콜이 이루고자 하는 목적을 달성하였는지의 여부로 판단하며, 안전한 다자간 계산에서 전통적인 의미의 안전성은 다음 두 가지를 목적으로 하고 있다.

□ Correctness: 공격자는 정직한 참여자의 계산 결과값에 영향을 줄 수 없으며, 어떠한 참가자도 잘못된 계산 결과를 가지지 않는다.

□ Privacy: 공격자는 매수된 참여자의 입력과 결과값이 내포하고 있는 정보가 아닌 정직한 참여자의 입력값에 대해서 알지 못한다.

하지만 특정 문제에 따라서는 위의 두 가지 요구사항 외에 fairness나 robustness 등의 추가적인 요구사항을 정의하여 사용하기도 한다. 그러나 요구사항을 나열함으로써 안전성을 정의하는 것은 나열된 요구사항들이 해당 문제에 대한 모든 고려사항을 담고 있는지 확신하기 어려울뿐더러 적용되는 문제에 따라 요구사항을 새로 정의해야 한다는 단점이 있다.

최근에 R. Canetti는 이러한 기존 안전성 개념의 문제를 인식하고 〔10〕에서 UC 안전성(universal composable security)이라고 불리는 일반적이고 강력한 안전성 개념을 제안하였다. 〔10〕에서는 암호 프로토콜을 분석, 표현하는 새로운 틀을 제안하고 이를 기반으로 보안 요구사항을 표현하는 일반적인 방법을 기술하고 있다. 지금까지 프로토콜의 안전성은 일반적으로 프로토콜 참여자가 분리된 하나의 프로토콜만을 수행하는 단일 모델(stand-alone model) 환경에서 정의되고 증명되어 왔다. 하지만 이러한 설정은 인터넷과 같이 여러 참여자들에 의해 다수의 프로토콜들이 동시에 수행되는 현실적인 환경에서 안전성을 보장하지 못한다. 하지만 〔10〕에서 정의된 안전성 개념을 사용하면 여러 참여자가 다수의 프로토콜을 동시에 수행하는 병발 모델(concurrent model)에서도 프로토콜의 안전성을 보장할 수 있다. UC 안전성은 이전 방법들에 비해 훨씬 일반적이고 강력한 안전성 개념을 제공하며, UC 안전성 개념이 제안된 이후 다자간 계산 및 기타 암호 프로토콜의 안전성 증명은 이에 기초하여 이루어지고 있는 추세이다.

4.2 프로토콜 효율성

효율성은 다자간 계산에 있어서 가장 중요한 이슈 중 하나이며, 다자간 계산 개념이 제안된 이후 꾸준히 연구되어 오고 있는 분야이다. 이는 다자간 계산 기술의 유용함에도 불구하고 이를 실제 응용에 적용하는 데에 있어서 가장 큰 장애로 인식되는 것이 프로토콜의 비효율성 문제이기 때문이다.

일반적으로 다자간 계산에서의 효율성은 크게 두 가지 측면에서 고려되는데 첫째가 프로토콜 수행 중에 참여자들 사이에서 이루어지는 메시지 교환 횟수를 따

지는 라운드 복잡도와 둘째로 교환되는 메시지의 크기를 따지는 통신 복잡도이다. 참고적으로 문헌에 따라서는 메시지 복잡도가 통신 복잡도와 동일한 의미로 사용된다.

라운드 복잡도 줄이는 것은 암호 프로토콜의 효율성을 향상시키기 위한 가장 일반적인 접근 방법으로 안전한 다자간 계산의 경우 초기부터 많은 관련 연구가 이루어져 왔다.[11-16] 최근에는 안전한 통신로 채널과 브로드캐스트 채널을 가정한 악의적인 공격자 모델에서 3 라운드의 메시지 교환이면 모든 함수를 안전하게 계산할 수 있다는 것이 증명되었다.[16,17]

반면 통신 복잡도 측면에서의 효율성은 [18]에서 처음 고려되기 시작하여 비교적 최근에 들어서 주목받기 시작하였다. 관련 연구에 따르면 일반적으로 낮은 라운드 복잡도를 가지는 프로토콜들은 높은 통신 복잡도를 가지며, 통신 복잡도가 라운드 복잡도 보다 프로토콜의 효율성에 더 큰 영향을 미친다고 알려지고 있다.[19,20] 따라서 최근의 효율성 관련 연구는 라운드 복잡도를 유지하면서 통신 복잡도를 낮추고자 하는 방향으로 이루어지는 추세이다.

표 4는 메시지 복잡도와 관련된 최근의 연구결과를 비교하여 보여주고 있다. 표 4에서 임계치는 프로토콜이 견뎌낼 수 있는 악의적인 공격자의 한계이며, n은 계산 참여자의 수, m은 곱셈 연산 게이트 수를 나타낸다.

4.3 기타 이슈

안전한 다자간 계산 문제가 제안된 이후, 최근까지도 이 분야에서의 연구는 프로토콜의 효율성 향상과 안전성을 증명 하는 등의 이론적인 측면에 초점이 맞추어져 오고 있다. 하지만 근래에 들어서 안전한 다자간 계산 기술을 실용적인 응용에 접목하려는 노력들이 나타나는 추세이다.[23-26] 아직까지 안전한 다자간 계산의 비효율성이 문제로 지적되고 있지만 이처럼 안전한 다자간 계산 기술을 특정 응용 및 세부 문제에 적용함으로써 좀 더 효율적인 프로토콜의 개발이 가능할 것으로 예상되며, 데이터 마이닝, 통계 분석, 데이터베이스 질의, 과학 계산 등의 다양한 응용에서 그러한 가능성을 보여주고 있다.[27-28] 이에 대한 내용은 V장에서 좀 더 살펴보도록 하겠다.

또한 이미 언급한 내용 외에도 [29]에서는 유한체 상에서만 이루어져 오던 안전한 다자간 계산 기술을 새로운 수학적 이론에 기반하여 구성함으로써 기존 다자간 계산 기술의 문제를 개선시키고자 하였으며, [9]과 [30]에서는 복수개의 임계치를 제공하여 임계치의 범위에 따라 각기 다른 안전성을 제공할 수 있는 새로운 개념을 소개하고 있다.

V. 다자간 계산 기술의 응용

안전한 다자간 계산은 최근 들어 다양한 응용에서 발생할 수 있는 민감한 정보 노출의 문제를 효과적으로 해결할 수 있는 우수한 도구로 인식되고 있다. 이러한 인식을 바탕으로 지금까지 이론적 수준에 머물던 연구를 탈피하여 실제적인 응용과 접목하려는 노력들이 다양하게 시도되고 있으며, 본 장에서는 다자간 계산의 적용이 가능한 응용 분야와 문제들에 대해서 기술한다. 참고로 설명하는 내용이 모든 다자간 계산 문제를 다루고 있지는 않으며, 여기에 언급된 것 외에도 많은 응용이 있을 수 있다.

5.1 데이터 마이닝

데이터 마이닝은 대용량 데이터로부터 유용하게 활용될 수 있는 지식을 효과적으로 찾아내는 지식 탐사(knowledge discovery)의 한 연구 분야로써 최근에는 기업 업무의 효율적 수행과 생산성 향상을 위해 적극적으로 활용되고 있는 추세이다. 하지만 이처럼 대량의 데이터베이스로부터 데이터를 분석하고 효과적인 결과를 추출하는 과정에서 민감한 개인 정보 및 비밀정보가 유출될 가능성이 있으며, 이에 대한 해결책이 절실히 요구되고 있다. 데이터 마이닝 과정 중에는 수많은 연산을 수행하며, 다음과 같은 연산들에 있어

[표 4] 메시지 복잡도 비교

분 류	임계치	안전성	필드 수
HM01[20]	$t < n/3$	unconditionally secure	$O(mn^2)$
HMP00[19]	$t < n/3$	unconditionally secure	$O(mn^3)$
CDN01[21]	$t < n/2$	conditionally secure	$O(mn^3)$
CDDHR99[22]	$t < n/2$	conditionally secure	$O(mn^4)$

서 안전한 다자간 계산 기술이 적용될 수 있을 것으로 기대되고 있다.

분류(Classification)

사용자 A가 비공개 데이터 집합 D_1, 사용자 B가 비공개 데이터 집합 D_2를 가지고 있다고 가정하자. 각 데이터베이스는 (속성, 값)이 쌍으로 이루어진 구조화된 데이터베이스로써 각 열은 트랜젝션, 각 행은 다른 값을 가지는 하나의 속성이다. 그리고 속성들 중 하나는 클래스 속성으로 지정된다. 이 때 사용자 A와 B는 상대방에게 자신의 데이터베이스 내용을 노출시키지 않고 $D_1 \cup D_2$에 기반한 결정트리(decision tree)를 구성하고자 한다.

군집화(Data clustering)

사용자 A가 비공개 데이터 집합 D_1, 사용자 B가 비공개 데이터 집합 D_2를 가지고 있다고 가정하자. 이 때 사용자 A와 B는 상대방에게 자신의 데이터베이스 내용을 노출시키지 않고 $D_1 \cup D_2$에 대한 데이터 클러스터링을 함께 수행하고자 한다.

연관규칙(Mining association rules)

사용자 A가 비공개 데이터 집합 D_1, 사용자 B가 비공개 데이터 집합 D_2를 가지고 있다고 가정하자. 이 때 사용자 A와 B는 상대방에게 자신의 데이터베이스 내용을 노출시키지 않고 $D_1 \cup D_2$에 대한 연관규칙(association rule)을 함께 생성하고자 한다.

데이터 일반화, 요약, 특성화(Data generalization, summarization and characterization)

사용자 A가 비공개 데이터 집합 D_1, 사용자 B가 비공개 데이터 집합 D_2를 가지고 있다고 가정하자. 이 때 사용자 A와 B는 상대방에게 자신의 데이터베이스 내용을 노출시키지 않고 $D_1 \cup D_2$를 일반화하거나 요약, 특성화 하고자 한다.

5.2 데이터베이스 질의

본 문제는 다자간 계산 기술을 적용한 응용 중에서 가장 활발히 연구되고 있는 분야 중 하나이며, PIR (Private Information Retrieval)로 잘 알려져 있다. PIR은 다자간 계산 기술을 이용하여 아래 기술한 목표를 이론적으로 이미 달성하였으나 좀 더 효율적인 프로토콜을 개발하려는 방향으로 최근까지 연구가 이루어지고 있다.

데이터베이스 질의(Database query)

사용자 A는 스트링 q, 사용자 B는 스트링의 집합 $T=\{t_1,...,t_n\}$로 구성된 데이터베이스를 가지고 있다고 가정하자. 사용자 A는 데이터베이스 질의 q를 통하여 사용자 B의 데이터베이스에 질의 q에 대한 스트링 t_i가 있는지 알고 싶다. 프라이버시 측면에서 사용자 B는 사용자 A의 질의 q를 알 수 없거나 q에 대한 응답을 알 수 없어야 하고 사용자 A는 질의 결과로부터 얻을 수 있는 정보 외에 사용자 B의 데이터베이스 내용을 알 수 없어야 한다.

5.3 통계 분석

본 문제는 수많은 응용에 적용이 가능하다. 예를 들어, 어떤 은행에서 고객의 연령이 금융 활동에 영향을 미치는지 알고 싶어 하지만 은행은 단지 고객의 금융 거래 정보만을 가지고 있고 연력에 대한 정보가 없다고 하자. 이 경우 은행은 사람들의 출생 정보를 가지고 있는 정부 기관 등의 도움을 얻을 필요가 있다. 하지만 정부는 법률에 의거해 신상정보를 공개할 수 없고 은행 또한 고객들의 금융활동 내역을 공개할 수 없다. 이와 같은 문제에 대한 해결책으로 안전한 다자간 계산 기술이 사용될 수 있다.

상관계수와 회귀분석(Correlation and regression analysis)

사용자 A가 비공개 데이터 집합 $D_1=(x_1,...,x_n)$, 사용자 B가 비공개 데이터 집합 $D_2=(y_1,...,y_n)$를 소유하고 있다(단, x_i, y_i는 각각 변수 x, y에 대한 값). 이 때 사용자 A와 사용자 B는 비공개 데이터 집합에 대한 정보노출 없이 다음 결과를 알기 원한다.

- x와 y 간 상관계수: 두 변수 x와 y 사이의 선형 관계 강도
- 회귀선: 변수 x의 값이 주어졌을 때 변수 y 값을 제공하는 방정식

5.4 기하학 계산

안전한 다자간 계산은 다양한 기하학적인 계산 문제에 있어서도 적용될 수 있다. 간단한 예로 동맹 관계인 두 국가 A와 B를 생각해 보자. 국가 A는 국가 C와 전쟁 중이며, 조만간 C의 특정 지역에 폭격을 가할 계획을 가지고 있다. 그러나 A는 C의 내부에 있을지 모르는 B의 비밀 조직에 피해를 주고 싶지 않다.

하지만 A는 폭격 위치를 B에게 알려주기를 원하지 않으며, B 또한 비밀조직의 위치가 A에게 알려지지 않기를 바란다. 이러한 경우에 안전한 다자간 계산이 효과적으로 활용될 수 있을 것이다.

교차점(Intersection)

사용자 A는 비공개 도형 a, 사용자 B는 비공개 도형 b를 가지고 있고 사용자 A와 B는 두 도형의 교차 여부를 알고 싶어 한다. 하지만 사용자 A와 B 모두 상대방을 포함한 어느 누구에게도 자신의 도형에 대한 정보가 노출되기 원하지 않으며, 교차되는 곳이 있을 경우에 그 상대적인 위치조차 알려지기를 원하지 않는다.

위치 포함(Point-inclusion)

사용자 A는 비공개 점 z, 사용자 B는 비공개 다각형 P를 가지고 있고 사용자 A와 B는 z가 P의 내부에 속하는지 알기를 원한다. 하지만 사용자 A와 B 모두 상대방을 포함한 어느 누구에게도 z나 P에 대한 정보가 노출되기 원하지 않으며, z가 P의 내부에 있을 경우에 그 상대적인 위치조차 알려지기를 원하지 않는다.

영역 탐색(Range searching)

사용자 A는 비공개 영역, 사용자 B는 N개의 비공개 점을 가진다. 이 때 사용자 A와 B는 서로 데이터에 대한 노출 없이 사용자 A의 영역에 속해 있는 사용자 B의 점의 개수를 알기 원한다.

최단거리 지점(Closest pair)

사용자 A가 N개의 비공개 점, 사용자 B 또한 M개의 비공개 점을 가진다. 이 때 사용자 A와 B는 $N+M$개의 점 중에서 가장 가까이 있는 두 개의 점을 알기 원한다.

5.5 기타 응용

앞 절에서 언급한 분야 외에도 다음과 같은 문제에 대해 안전한 다자간 계산 기술이 적용될 수 있으며, [27]과 [28]에서는 이러한 문제들에 대해서 기술하고 있다.

선형 시스템(Linear systems)

사용자 A가 $M_1x=b_1$으로 표현되는 m 개의 비공개 방정식, 사용자 B가 $M_2x=b_2$로 표현되는 $n-m$개의 방정식을 가지며, x는 n차 벡터이다. 이 때 사용자 A와 B는 두 방정식을 만족하는 벡터 x를 알기 원한다.

선택 문제(Selection problem)

사용자 A가 비공개 데이터 집합 D_1, 사용자 B가 비공개 데이터 집합 D_2를 가지고 있다. 이 때 사용자 A와 B는 두 데이터의 합집합 $D_1 \cup D_2$에서 중앙값 혹은 k번째로 작은 값을 알기 원한다.

정렬 문제(Sorting problem)

사용자 A가 비공개 데이터 집합 D_1, 사용자 B가 비공개 데이터 집합 D_2를 가지고 있다. 이 때 사용자 A와 B는 두 데이터의 합집합 $D_1 \cup D_2$에서 각 구성요소들을 정렬하기를 원한다.

Ⅵ. 결 론

사회의 정보화 과정에서 개인 정보 유출 문제가 심각한 사회 문제로 대두되고 있으며, 세계 각 국에서는 법적, 제도적 장치뿐만 아니라 기술적으로 이를 해결하려는 노력을 기울이고 있다. 최근 들어 안전한 다자간 계산 기술은 프라이버시 보호 문제를 해결할 수 있는 유용한 기술의 하나로 인식되고 있으며, 다양한 분야에서 관련 연구가 이루어지고 있다.

전통적으로 안전한 다자간 계산 기술에서는 효율성과 안전성에 관한 이론적 연구가 주를 이루고 있으며, 최근까지도 이는 주요 연구 주제로 다루어져 오고 있다. 하지만 근래에 들어서는 안전한 계산 기술을 세부적인 응용 및 문제에 적용함으로써 좀 더 실용적인 기술로 발전시키려는 노력들이 나타나고 있는 추세이며, 이와 같은 접근을 통하여 좀 더 효율적인 다자간 계산 프로토콜 개발이 가능할 것으로 예상된다. 이러한 가능성을 보여주는 분야로 데이터 마이닝, 통계 분석, 과학 계산 등이 있으며, 향후 더 많은 응용 가능 분야가 생겨날 것으로 예상된다.

미래 사회에서는 모든 데이터가 전자적으로 처리되고 이들을 활용하는 새로운 응용들이 꾸준히 생겨날 것이며, 이러한 환경에서 민감한 개인 정보를 안전하게 유지할 수 있는 기술의 확보 여부는 향후 국가 경쟁력에 있어서 매우 중요하게 평가될 것이다.

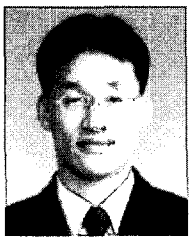
참 고 문 헌

[1] A. C. Yao, "Protocols for Secure Com-

putation", Proc. of IEEE FOCS '82, pp. 160-164, 1982.
[2] O. Goldreich, S. Micali and A. Wigderson, "How to Play Any Mental Game or Completeness Theorem for Protocols with Honest Majority", Proc. of ACM STOC '87, pp. 218-229, 1987.
[3] O. Goldreich, "Secure Multi-Party Computation (Final (incomplete) Draft, Version 1.4)", available at http://www.wisdom.weizmann.ac.il/~oded/PS/prot.ps
[4] R. Cramer, "Introduction to Secure Communication", Lecture Note of Aarhus Summer school in Cryptography and Data Security, 2000.
[5] S. Even, O. Goldreich and A. Lempel, "A Randomized Protocol for Signing Contract", Communications of the ACM, vol. 28, 1985.
[6] A. Shamir, "How to Share a Secret", Communications of the ACM, vol. 22, 1979.
[7] P. Feldman, "A Practical Scheme for Non-interactive Verifiable Secret Sharing", Proc. of IEEE FOCS '87, pp. 427-437, 1987.
[8] O. Goldreich and R. Vainish, "How to Solve any Protocol Problem: An Efficiency Improvement", Proc. of Crypto '87, pp. 73-86, 1987.
[9] M. Fitzi, T. Holenstein and J. Wullschleger, "Multi-party Computation with Hybrid Security", Proc. of Eurocrypt 2004, pp. 419-438, 2004.
[10] R. Canetti, "Universally Composable Security: A New Security Paradigms for Cryptographic Protocols(Extended Abstract)", Proc. of 42th IEEE FOCS, pp. 136-145, 2001.
[11] J. Bar-Ilan and D. Beaver, "Non-Cryptographic Fault-Tolerant Computing in a Constant Number of Rounds", Proc. of 8th ACM PODC, pp. 201-209, 1989.
[12] D. Beaver, S. Micali and P. Rogaway, "The Round Complexity of Secure Protocols(Extended Abstract)", Proc. of 22th ACM STOC, pp. 503-513, 1990.
[13] U. Feige, J. Kilian and M. Naor, "A Minimal Model for Secure Computation(Extended Abstract)", Proc. of 26th ACm STOC, pp. 554-563, 1994.
[14] Y. Ishai and E. Dushilevitz, "Randomizing Polynomials: A New Representation with Applications to Round-Efficient Secure Computation", Proc. of 41th ACM FOCS, 2000.
[15] Y. Lindell, "Parallel Coin-Tossing and Constant-Round Secure Two-Party Computation", Proc. of Crypto 2001, pp. 171-189, 2001.
[16] R. Gennaro, Y. Ishai, E. Kushilevitz and T. Rabin, "The Round Complexity of Verifiable Secret Sharing and Secure Multicast", Proc. of 33th ACM STOC, 2001.
[17] R. Gennaro, Y. Ishai, E. Kushilevitz and T. Rabin, "On 2-Round Secure Multiparty Computation", Proc. of Crypto 2002, pp. 178-193, 2002.
[18] D. Beaver, J. Feigenbaum, J. Kilian and P. Rogaway, "Security with Low Communication Overhead(Extended Abstract)", Proc. of Crypto '90, pp. 62-76, 1990.
[19] M. Hirt, U. Maurer and B. Przydatek, "Efficient Secure Multi-party Computation(Extended Abstract)", Proc. of Asysacrypt 2000, pp. 143-161, 2000.
[20] M. Hirt and U. Maurer, "Robustness for Free in Unconditional Multi-party Computation", Proc. of Crypto 2001, pp. 101-118, 2001.
[21] R. Cramer, I. Damgard and J. B. Nielsen, "Multipary Computation from Threshold Homomorphic Encryption", Proc. of Eurocrypt 2001, pp. 280-300, 2001.
[22] R. Cramer, I. Damgard, S. Dziembow-

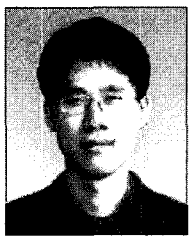
ski, M. Hirt and T. Rabin, "Efficient Multiparty Computation Secure against an Adaptive Adversary", Proc. of Eurocrypt '99, pp. 311-326, 1999.
[23] Y. Lindell and Benny Pinkas, "Privacy Preserving Data Mining", Proc. of Crypto 2000, pp. 36-54, 2000.
[24] W. Du and M. J. Atallah, "Privacy-Preserving Cooperative Scientific Computations", Proc. of 14th IEEE Computer Security Foundations Workshop, pp. 273-282, 2001
[25] W. Du and M. J. Atallah, "Prptocols for Secure Remote Database Access with Approximate Matching", Proc. of ACMCCS 2000, 2000.
[26] M. J. Atallah and W. Du, "Secure Multi-Party Computational Geometry", Proc. of WADS 2001, 2001.
[27] W. Du and M. J. Atallah, "Secure Multi-Party Computation Problems and Applications: A Review and Open Problems", Proc. of New Security Paradigms Workshop, 2001.
[28] W. Du and Z. Zhan, "A Practical Approach to Solve Secure Multi-Party Computation Problems", Proc. of New Security Paradigms Workshop, 2002.
[29] R. Cramer, S. Fehr, Y. Ishai and E. Kushilevitz, "Efficient Multi-party Computation over Rings", Proc. of Eurocrypt 2003, pp. 596-613, 2003.
[30] M. Fitzi, M. Hirt, T. Holenstein and J. Wullschleger, "Two-Threshold Broadcast and Detectable Multi-Party Computation", Proc. of Eurocrypt 2003, pp. 51-67, 2003.

〈著 者 紹 介〉



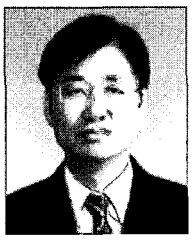
유 준 석 (Joonsuk Yu)
정회원

1999년 2월 : 성균관대학교 정보공학과 졸업
2001년 2월 : 성균관대학교 전기전자 및 컴퓨터공학부 석사
2001년 1월~현재 : 한국전자통신연구원 연구원
〈관심분야〉 암호이론, 암호 프로토콜, PETs, 이동인터넷



홍 도 원 (Dowon Hong)

1994년 2월 : 고려대학교 수학과 졸업
1996년 2월 : 고려대학교 수학과 석사
2000년 2월~현재 : 고려대학교 수학과 박사
2000년 4월~현재 : 한국전자통신연구원 팀장
〈관심분야〉 암호이론, 정보보호이론, 이동통신 정보보호



정 교 일 (Kyoil Chung)

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 8월 : 한양대학교 산업대학원 전자계산학과 석사
1997년 8월 : 한양대학교 전자공학과 박사
1980년 12월~1981년 11월 : 엠시스템즈
1981년 12월~1982년 2월 : 한국전기통신연구원 위촉연구원
1982년 3월~현재 : 한국전자통신연구원 정보보호기반그룹장/책임연구원
〈관심분야〉 정보보호, IC카드, Biometrics, 국가기반보호, 신호처리