지문과 스마트카드를 이용한 사용자 인증

김현성* · 정연기*

1. 서 론

오늘날 전자상거래나 신용 거래가 증가함에 따라 개인의 인증에 대한 요구는 더욱 더 증가하는 추세이다. 네트워크에서 개체 인증이란 어떤 사용자나 어플리케이션이 실제로 신고된 바로 그 사람인지를 판단하는 절차를 말하며 이러한 인증 서비스는 다음과 같은 3가지 형태의 기본정보를 기반으로 이루어진다.

- 개인이 소유하고 있는 것(스마트카드, 토큰)
- 개인의 신체적 특성(지문, 홍채, 목소리)
- 개인이 알고 있는 것(패스워드, PIN)

개인이나 조직체에서 허용하는 신뢰와 안전성 수준에 따라 네트워크 보안의 강/약 레벨은 다양하게 구현될 수 있으나 일반적으로 두 가지 형태의 인증정보가 결합되어 인증서비스가 제공될 것을 권장하고 있다. 이렇게 두 종류 이상의 인증정보가 결합되어 인증 서비스를 제공할 때 '강한 인증 서비스'를 제공한다고 한다. 특히, 지문은 사람에 있어서 유일한 특징과 변하지 않는 특성으로 인하여 개인의 인증이나 식별에 오랫동안 이용되어 왔다. 지문을 이용한 개인 인증은 미리 등록된 등록지문과 채취지문을 비교하여 두 지문의 유사도를 측정하여 동일 인물인지를 판단한다.

* 경일대학교 컴퓨터공학부 교수

Shamir에 의해 ID(Identification)정보에 기반한 서명기술이 제안된 이후 ID정보에 기반 한 많은 연구가 진행되었다[1]. Shamir의 방식은 가입자의 ID정보 자체가 공개키이며 비밀키 자체가 공개키 증명이다. 그러므로 시스템은 (식별자, 비밀키)의 쌍으로 구성된다. 이 방식은 저장하거나, 검증할 공개키 증명이 별도로 필요 없기 때문에 매우 효율적인 방식이다. 보다 일반적인 ID정보에 기반한 방식은 가입자의 공개키를 가입자의 ID정보와 관련된 어떤 값으로 대치하여 이용하는 방법이다[2].

Chaum등[3]은 이산대수를 이용한 영지식 대화형 프로토콜을 제안하였으며 Schnorr[4]는 여기서 아이디어를 얻어 mod p상의 이산 대수 문제를 이용하여 계산능력이 약한 스마트카드에 적합한 새로운 ID방식을 제안하였다. 그러나 엄밀한 의미에서 Schnorr 방식은 영지식은 아니다. 또한 Schnorr 방식은 ID를 이용한 방식이 아니므로 센터가 인증서를 생성해야 하는 단점이 있으며 검증자는 이 인증서를 검증해야 하는 단점이 있다. 1990년에 Girault[5]는 Schnorr 방식을 확장하였으며, 각 가입자의 공개정보와 ID정보를 결합하여 센터가 효율적인 공개키를 생성하는 ID방식을 제안하였다[4].

Okamoto [6]는 Diffie-Hellman의 키 분배방식에 ID정보를 이용한 인증을 첨가한 방식을 제안

하였다. 이 시스템은 공통 키 교환을 위한 낮은 통신의 복잡도를 이용하였으나 많은 대역폭 사용과 많은 계산량 부담, 그리고 위장공격등 안전성에 문제점을 안고 있다. 최근에 Shieh등[7]은 적은 계산량과 Okamoto 방식에서 나타나는 안전성 문제를 해결한 인증 프로토콜을 제안하였다. 그러나 Yen[8]에 의해서 이 기술은 메시지의 반복 공격과 알려지지 않은 키 공유 공격(Unknown key share attack)에 약하다는 분석이 있었다. 위 프로토콜들의 안전성은 RSA 공개키 암호 시스템과 같이 두 개의 큰 소수의 곱인 합성수의 인수분해 문제에 기반한다.

한편 이산대수문제의 안전성에 기반 한 기술은 Tsujii[9]에 의해 제안되었다. Tsujii의 암호시스템은 ElGamal의 공개키 시스템을 이용하여 ID방식에 기반 한 암호 시스템이었다. 이 시스템은 많은 계산량 뿐만 아니라 공모 문제와 같은 보안의 취약성을 갖고 있다. Gunther[10]는 유한 체의 곱셈 군에 기반을 둔 ID방식에 기반 한 키 교환 프로토콜을 제안하였다. 이 프로토콜은 전방향 보안(perfect forward secrecy)을 제공한다. Wang등[11]과 Yang등[12]은 스마트카드를 이용한 ID기반의 인증 프로토콜을 제안하였다. 이 프로토콜에서는 재전송 공격에 대응하기 위하여 시스템의 타임스탬프를 사용하였지만 여전히 재전송공격에 취약했고, 사용자의 ID정보 또한 위조될 수 있었다.

지금까지 언급한 ID방식에 기반 한 암호화 시스템은 다음의 문제점을 공유한다. ID방식을 구현할 때 실질적인 중요한 단점은 가입자가 자신의 비밀키를 선택할 수 없을 뿐만 아니라 가입자의 비밀키를 센터가 계산하며, 유효기간 동안 언제라도 센터가 재계산할 수 있다는 것이다. 그러므로, 사용자의 비밀키가 노출되면 그 사용자는 자신의 ID정보를 더 이상 사용할 수 없고 새로운 ID정보를 시스템으로부터 발급 받아야 하는 문제점이 있다. 본 논문에서는 ID방식에 기반 한 암호화 시스템의 장점을 유지하면서 이 방식의 문제점들을 해결할 수 있는 방안에 대해서 기술하고자 한다. 프로토콜 수행에 필요한 모든 정보는 외부로부터 보호하기 위해서 스마트카드에 저장되고 모든 연산은 스마트카드 내부에서 이루어진다. 또한, 스마트카드의 소유자 인증을 위하여 지문을 이용한다. 제안한 프로토콜은 관련된 프로토콜에 비해 보다 높은 안전성과 효율성을 제공할 수 있을 것이다.

2. 지문매칭을 통한 소유자 인증

일반적으로 지문인식에서 다루는 특징량(Feature volume)은 특징점과 특이점으로 구분할 수 있다. 이러한 특징량은 본인의 지문과 타인의 지문을 구분하는 중요한 요소가 되며, 융선과 골의 흐름을 포함한 것을 총칭한다. 지문에는 다양한 종류의 특징점들이 있으나, 여러 특징점들은 단점과 분기점의 조합으로 볼 수 있으며 대부분의 지문인식에서는 단점과 분기점만을 특징량으로 이용한다. 지문 영상의 처리의 과정은 그림 1과 같

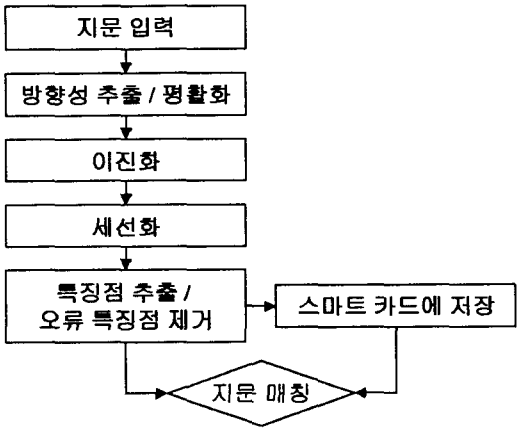


그림 1. 지문을 이용한 소유자 인증절차

다. 특징점 추출/오류 특징점 제거 부분이 일반적인 영상처리와 지문 영상 처리의 차이점이다. 매칭 단계에서는 등록된 지문 영상과 입력된 지문 영상의 특징점의 유사도를 측정한다.

스마트카드[16]의 소유자 인증을 위해서 특징점에 기반을 둔 지문매칭 기법[14,15]을 사용한다. 스마트카드 소유자는 카드 발급과 동시에 스마트카드에 자신의 지문을 등록한다. 등록과정에서 시스템은 입력된 지문의 특징점 정보만을 스마트카드에 저장한다. 소유자 인증 시 등록된 지문과 입력된 지문의 일치여부에 따라서 그림 2와 같이 소유자임을 확인할 수 있다. 그림2는 미리 등록되어 있는 지문과 입력된 지문의 특징점정보를 이용한 매칭과정을 보여준다.

지문의 일치여부를 확인하기 위해서는 매칭 스코어 기법을 사용한다. 표 1에서 보여준 바와 같이

(a) 등록지문 (b) 입력지문 (c) 특징점정보

그림 2. 지문 매칭

매칭 스코어(Matching Score, MS)가 20%일 때 효율적인 시스템을 구성할 수 있다.

3. 사용자 인증 프로토콜

본 장에서는 지문과 스마트카드를 이용하여 참여자들을 서로 인증할 수 있는 ID 기반의 인증 프로토콜을 제안한다. 그림 3은 시스템의 전체 구성도를 보여준다.

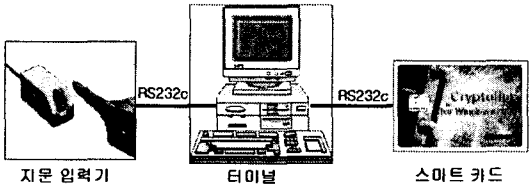


그림 3. 전체 시스템 구성

3.1 표기 및 초기설정

본 절에서는 제안된 프로토콜에서 사용될 용어와 표기법, 그리고 가정들을 정의하고 프로토콜이 시작하기 전에 참여자들 간에 동의할 내용을 기술한다.

프로토콜의 두 참여자 클라이언트(A)와 서버(B)는 합법적인 참여자들이다. A와 B는 안전하게 Z_n^* 상의 생성자인 g와 큰 소수인 n를 미리 공

표 1. 매칭 스코어에 따른 FRR 과 FAR.

MS / Finger	FRR(%)			FAR(%)		
	10%	15%	20%	10%	15%	20%
Right thumb	3.2	3.4	4.0	0.13	0.013	0.003
Right index	1.3	2.6	6.8	0.12	0.007	0.000
Right middle	5.2	11.6	21.3	0.13	0.017	0.002
Right third	12.0	19.3	28.8	0.14	0.013	0.000
Right little	10.0	23.6	40.1	0.12	0.010	0.000
Left thumb	7.4	10.1	14.8	0.14	0.013	0.001
Left index	2.1	6.0	12.2	0.12	0.014	0.002
Left middle	7.0	10.4	15.7	0.12	0.015	0.002
Left third	12.1	24.9	39.4	0.10	0.007	0.001
Left little	12.1	25.4	38.2	0.14	0.014	0.001

A, B	각각 클라이언트와 서버의 식별자
ID_i	클라이언트 i의 아이디
g	곱셈군(multiplicative group) Z_n^*의 생성자(generator)
n	큰 소수
PW_i	클라이언트에 의해 선택된 패스워드
SK	서버의 비밀키
SK^{-1}	Z_n^*상에서 SK의 역수
a	A에 의하여 생성된 Z_n^*의 임의의 원소 (지문 입력정보를 통하여 생성)
$f()$	일방향 해쉬 함수 (one-way hash function)

그림 4. 프로토콜을 위한 표기

유하고 있다고 가정한다. 또한 A는 패스워드 PW_i를 소유하고 있다고 하자. $f()$는 일방향 해쉬 함수(one-way hash function)이다. 표현의 간편함을 위해 프로토콜 수행에 있어서 'mod n' 연산은 생략한다.

3.2 프로토콜의 수행

제안된 프로토콜은 등록 단계와 로그인 단계, 그리고 검증 단계의 3단계로 구성된다. 먼저, 등록 단계에서는 원격 서버가 클라이언트에게 스마트카드를 발급하고, 스마트카드를 발급받은 사용자는 자신의 지문 정보를 스마트카드에 등록한다. 서버로부터 스마트카드를 발급받은 사용자는 로그인 단계에서 스마트카드를 카드리더기에 입력하고 지문인식장치에 자신의 지문을 입력한다. 그러면 사용자의 터미널은 로그인 요청을 원격서버에 전달한다. 검증 단계에서는 서버가 받은 메시지가 정확한지 여부를 확인하고 로그인 요구를 받아들일지를 판단한다.

가) 등록 단계

1단계. 클라이언트 A는 자신의 ID_i와 패스워드 PW_i를 원격서버 B에게 안전한 방법으로 전송한다.

2단계. 원격서버 B는 클라이언트 A의 스마트카드 식별자인 CID_i를 생성하고 S_i와 h_i를 다음과 같이 계산한다.

$$S_i = ID_i^{SK}$$

$$h_i = g^{PW_i \cdot SK}$$

여기서 SK는 서버의 비밀키이고, CID_i는 검증 단계에서 스마트카드의 유효성 검증을 위해서 사용될 스마트카드의 아이디이다.

3단계. 원격서버 B는 스마트카드의 메모리에 $n, g, f(), ID_i, S_i$, 그리고 h_i를 저장하고 그 카드를 클라이언트 A에게 발급한다.

4단계. 클라이언트 A는 발급받은 스마트카드에 자신의 지문 정보를 등록한다. 지문을 등록할 때는 입력된 지문정보로부터 특징점을 추출하여 추출된 특징점 정보를 저장하며, 이러한 정보는 스마트카드의 소유자 인증에 사용된다.

등록 단계는 원격 서버에 새로운 가입자가 생기거나 가입자가 자신의 패스워드를 바꾸고자 하는 경우에만 수행된다.

나) 로그인 단계

로그인을 위해서 클라이언트 A는 카드리더기에 자신의 스마트카드를 입력하고 스마트카드 소유자 인증을 위해서 자신의 지문을 지문입력기에 입력하고, 원격서버의 로그인에 필요한 정보인 ID_i와 패스워드 PW_i를 입력한다. 지문을 통한 사용자 인증이 성공할 경우에만 스마트카드는 다음과 같은 로그인 절차를 수행한다.

1단계. 입력된 지문 좌표계의 해쉬된 정보를 이용하여 임의의 정수 a를 생성하고 다음을 계산한다.

$$X_i = g^{a \cdot PW_i}$$

$$Y_i = S_i \cdot h_i^{a \cdot f(CID_i, T_i)}$$

여기서 T_i는 시스템의 현재 시스템클럭이고, $f(x,y)$는 해쉬함수이다. 지문이 입력될 때마다 특징점 정보를 위한 다른 입력지도가 생성된다 [13,17]. 그러므로 해쉬 함수가 적용된 입력지도는 효율적인 일회용 난수(One-time random number)로 사용될 수 있다.

2단계. 다음 메시지 M을 원격서버 B에 보낸다.

$M = \{ ID_i, CID_i, X_i, Y_i, T_i \}$

다) 검증 단계

서버는 클라이언트 A로부터 받은 메시지의 검증을 통하여 A가 정당한 사용자인지를 결정한다. 이러한 검증을 위하여 메시지 M이 원격 서버의 시스템클럭 T_s에 도착했다고 가정한다. 서버는 다음의 절차를 수행한다.

1단계. ID_i와 CID_i가 사용자의 유효한 아이디이고 적법한 스마트카드의 아이디인지를 각각 확인한다. 만약 부적법한 정보이면 로그인 요청을 거절한다.

2단계. $(T_i - T_s) \leq \Delta T$ 연산을 통해서 적법한 시간 간격에 메시지가 보내졌는지를 확인한다. 여기서 ΔT 는 전송 지연을 고려한 적법한 시간 간격이다. 적법한 시간 간격 ΔT는 네트워크 환경에 따라 다양하게 조정될 수 있다.

3단계. 다음 수식이 맞는지 체크한다.

$$Y_i^{SK^{-1}} \equiv ID_i \cdot X_i^{f(CID_i, T_i)}$$

이 수식은 클라이언트에 의해 입력된 패스워드 PW_i가 서버에 의해 발급된 스마트카드에 등록된 패스워드와 일치할 때만 성립한다. 이 수식이 성립할 때만 서버가 클라이언트의 접근을 허락한다.

4. 분 석

이장에서는 지문을 이용한 난수 생성에서 고려할 사항들을 살펴보고 암호학적 안전성 분석을 제시한다.

4.1 난수로서의 지문

무엇보다도 본 논문에서 제안한 기법은 ElGamal 암호화 시스템을 이용하기 때문에 생성된 난수는 비밀키로서 매우 중요한 의미를 갖는다. 그러므로 만약 동일한 난수가 한번이상 사용된다면 공격자는 난수와 이전 통신 세션들에서 도청한 정보를 이용하여 비밀키를 계산할 수 있을 것이다. 그러

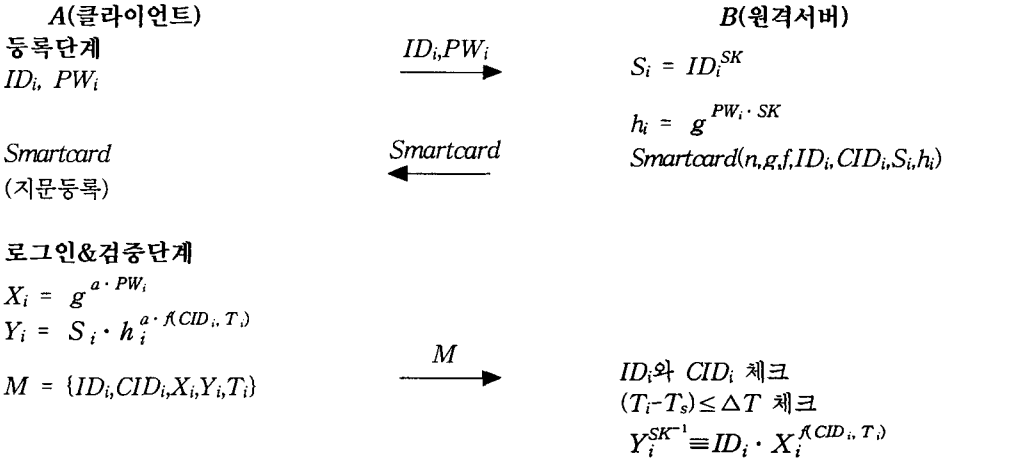


그림 5. 제안한 프로토콜

므로 일회용 난수의 생성은 본 논문의 기법에서 아주 중요한 요소이다. 그러나 아무리 기술이 뛰어나고 지문의 특성을 잘 아는 클라이언트라고 하더라도 동일한 지문입력을 반복해서 생성할 수 없다[13,14,17]. 따라서, 본 논문의 기법에서는 특징점에 기반 한 지문 인증 시스템(MFVS, Minutia-based Fingerprint Verification System)을 이용하여 일회용 난수를 생성하였다. 이 MFVS에서는 매번 지문이 입력 될 때마다 다른 특징점 지도가 생성된다.

4.2 안전성 분석

제안한 기법은 패스워드 추측공격(Password guessing attack)과 메시지 재전송 공격(Message replay attack), 그리고 위장공격(Impersonation attack)의 세가지 측면에서 안전성을 분석한다. 패스워드 인증 기법은 사용자 인증에 있어서 가장 널리 사용되고 있는 기법이다. 그러나 사용자들은 패스워드를 선택할 때 패스워드 추측공격이 가능할 수 있는 쉽게 기억할 수 있는 패스워드를 선택하는 경향이 있다. 일반적으로 패스워드 추측공격은 온라인 패스워드 추측공격과 오프라인 패스워드 추측공격으로 나뉜다.

- 온라인 패스워드 추측공격 : 공격자가 온라인으로 추측된 패스워드를 사용하여 원격 서버의 검증 단계를 통과하려는 시도 공격이다. 이러한 공격은 원격 사용자가 인증 실패 횟수를 확인함으로서 쉽게 막을 수 있다.

- 오프라인 패스워드 추측공격 : 공격자가 인증을 위한 메시지를 자신의 시스템에 저장하고 그 메시지로부터 패스워드 정보를 추측하고 오프라인으로 검증하기 위한 공격이다. 그러므로 원격서버는 이 공격을 탐지할 수 없다.

오프라인 패스워드 추측공격을 막기 위한 방법은 주고받는 메시지에 공격자가 추측한 패스워드의 정확성 여부를 검증할 수 있는 어떠한 정보도 제공하지 않는 것이다. 본 논문의 기법에서 공격자가 패스워드 PW_i를 획득할 수 있는 유일한 방법은 값 $h_i = g^{PW_i SK}$을 통해서 PW_i를 추측하는 것이다. 그러나 이 방법은 값 h_i가 안전한 스마트카드에 저장되어 있어서 사용자 인증 없이는 직접적으로 그 값에 접근할 수 없기 때문에 불가능하다. 또한, 만약 공격자가 h_i를 알아내더라도 공격자는 유한필드상의 이산대수 문제를 풀어야 패스워드 PW_i를 알 수 있기 때문에 본 논문에서 제안한 기법은 패스워드 추측공격에 안전하다.

본 논문의 기법은 시스템클럭을 사용하기 때문에 메시지 재전송 공격에 안전하다. 로그인 요청 메시지 $Y_i = S_i \cdot h_i^{r \cdot f(CID_i, T_i)}$에서 시스템클럭을 사용한다. 공격자가 메시지 재전송 공격을 하기 위해서는 이전 세션에서 획득한 Y_i의 시스템클럭 T_i를 $(T_i - T_s) \leq \Delta T$를 만족하는 T'로 변경할 수 있어야 한다. 그러나 이 문제역시 이산대수의 어려움에 근거하고 있다.

마지막으로 본 논문의 기법은 위장공격에 안전하다. 적법한 사용자가 타인을 위장하기 위해서는 위장하고자 하는 사용자의 아이디와 패스워드를 알아야만 한다. 그러나 적법한 사용자의 아이디와 패스워드는 연산 $S_i = ID_i^{SK}$와 $h_i = g^{PW_i SK}$에 의존적이다. 위장 공격을 위해서는 두 식으로부터 원격서버의 비밀키 SK를 알아야 하지만 이 값을 찾는 것 역시 이산대수의 어려움에 근거하고 있다.

5. 결 론

본 논문에서는 ID기반의 패스워드 인증 프로토콜을 제안하였다. 제안된 프로토콜은 ID방식에 기반 한 암호화 시스템의 장점을 유지하면서 기존

의 ID방식의 문제점들을 해결하였다. 본 논문에서 제안한 프로토콜은 프로토콜 수행에 필요한 모든 정보는 외부로부터 보호하기 위해서 스마트카드에 저장되고 모든 연산은 스마트카드 내부에서 이루어진다. 또한, 스마트카드의 소유자 인증을 위하여 지문을 이용하였다. 프로토콜의 안전성 분석에서 보여 준 바와 같이 제안한 프로토콜은 관련된 프로토콜에 비해 보다 높은 안전성과 효율성을 제공한다.

참 고 문 헌

[1] A.Shamir, "Identity-based cryptosystems and signature schemes", CRYPTO'84, pp. 47-53, 1985.

[2] 권창영, 김경신, 원동호, "ID를 이용한 암호시스템에 관한 고찰", 한국통신정보보호학회지. 제4권, 제1호, 1994. 3.

[3] D.Chaum, J.H.Evertse, J.van de Graaf, "An improved protocol for demonstration possession of discrete logarithms and some generalizations", Eurocrypt'87, pp. 127-141, 1987.

[4] Schnorr, "Efficient identification and signatures for smart cards", Eurocrypt'89, pp. 686-689, 1989.

[5] M.Girault, "An identity-based identification scheme based on discrete logarithms modulo a composite number", Eurocrypt'90, pp. 481-486, 1990.

[6] E.Okamoto, K.Tanaka, "Key distribution system based on identification information", Proc. GLOBECON'87, pp. 108-111, 1987.

[7] S.P.Shieh, W.H.Yang, H.M.Sun, "An authentication protocol without trusted third party", IEEE Commun. Lett., Vol. 1, pp. 87-89, 1997. 5.

[8] S-M.Yen, "Cryptanalysis of an authentication and key distribution protocol", IEEE Commun. Lett., Vol. 3, pp. 7-8, 1999. 1.

[9] S.Tsujii, K.Kurosawa, "ID-based cryptosystem", ISEC89-51, pp. 25-31, 1989.

[10] G.Gunther, "An identity-based key exchange protocol", Eurocrypt'89, pp. 29-37, 1990.

[11] S.J.Wang, J.F.Chang, "Smart card based secure authentication scheme", Computers and Security, Vol. 15, No. 3, pp. 231-237, 1996.

[12] W.H.Yang, S.P.Shieh, "Password authentication schemes with smart cards", Computers and Security, Vol. 18, No. 8, pp. 727-733, 1999.

[13] J.K.Lee, S.R.Ryu, K.Y.Yoo, "Fingerprint-based remote user authentication scheme using smart cards", IEE Elect. Lett., Vol. 38, No. 12, p. 554-555, 2002. 6.

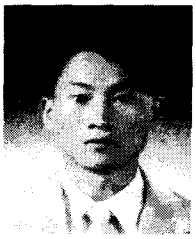
[14] N.K.Ratha, A.K.Jain, "A real-time matching system for large fingerprint databases", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 18, pp. 799-813, 1996.

[15] I.G.Bae, B.H.Joe, J.H.Bae, K.Y.Yoo, "Online fingerprint verification system using direct minutia extraction", Proc. ISCA 13th Int. Conf. CAINE, pp. 120-123, 2000.

[16] B.Schneier, "Applied cryptography", John Wiley & Sons, 1996.

[17] W.Rankl, W.Effing, "Smart card handbook", Chanterelle Translations, 1997.

[18] H.S.Kim, S.W.Lee, K.Y.Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints", ACM Operating Systems Review, pp. 32-41, Oct. 2003.



김 현 성

- 1996년 2월 경일대학교 컴퓨터공학과 공학사
- 1998년 2월 경북대학교 컴퓨터공학과 공학석사
- 2002년 2월 경북대학교 컴퓨터공학과 공학박사
- 2002년 3월~현재 경일대학교 컴퓨터공학부 교수
- 관심분야 : 정보보안, 암호 알고리즘, 암호 프로세서 설계, IDS, PKI

정 연 기

- 1982년 2월 영남대학교 전자공학과 졸업 (공학사)
- 1984년 2월 영남대학교대학원 전자공학과 졸업 (공학석사)
- 1996년 2월 영남대학교대학원 전자공학과 졸업 (공학박사)
- 1985년 3월~1990년 2월 가톨릭상지대학 전산정보처리과 조교수
- 1990년 3월~현재 경일대학교 IT대학 컴퓨터공학부 교수
- 1998년 1월~1998년 12월 호주 뉴캐슬대학교 전기 및 컴퓨터공학과 교환교수
- 관심분야 : 멀티미디어 통신, 초고속 정보 통신망, 통신망 운용관리
- E-mail : ykchung@bear.kyungil.ac.kr