通信情報保護論文誌
第9券 第4號 1999. 12

실험계획법을 이용한 평문·암호문 식별방법의 표본크기 선택에 관한 연구

박홍구* , 차경준* , 장호종* , 송정환* , 박성준**

On sample size selection for discernment of plain and cipher text using the design of experiments [1]

Hong Goo Park* , Kyung Joon Cha* , Ho Jong Jang*,
Jung Hwan Song* , Sung Jun Park**

요 약

암호알고리즘 출력문에 대한 난수성 검정은 평문과 암호문 식별에 중요한 역할을 하고 있다. 따라서, 현재 많이 사용되고 있고 난수성 검정방법들의 비교 및 분석은 필수적이라 할 수 있다. 또한 하나의 검정방법을 이용하고자 할 때 평문과 암호문을 식별할 수 있는 최소한의 데이터 크기는 실시간 검정 측면에서 많은 도움을 줄 수 있을 것이다. 본 논문에서는 대표적인 몇 개의 난수성 검정방법들에 대하여 평문과 암호문 식별에 대한 성공률을 실험을 통하여 분석하고 실험계획법을 이용하여 주어진 표본크기들 중에서 각 난수성 검정방법에 따른 하나의 최적의 표본크기를 제안한다.

Abstract

The randomness test for a sequence from an encription algorithm has an important role to make differences between plain and cipher text. Thus, it is necessary to investigate and analyze the currently used randomness tests. Also, in real time point of views, it would be helpful to know a minimum sample size which gives discernment of plain and cipher text. In this paper, we analyze the rate of successes for widely used nonparametric randomness tests to discern plain and cipher text through experiments. Moreover, for given sample sizes, an optimal sample size for each randomness test is proposed using the design of experiments.

1. 이 논문은 1999년도 한국정보보호센터의 지원에 의하여 연구되었음.
*한양대학교 수학과
**한국정보보호센터

Ⅰ. 서 론

최근 전자상거래 등 민간분야에서의 암호기술 사용이 증가함에 따라 암호기술이 제공하는 순기능을 최대한 활용하고 역기능을 최소화하기 위한 관리적인 차원에서의 암호기술 개발이 필요하다. 이것은 법제도적인 절차수립과 병행하여 정당한 목적으로 암호기술을 사용하는 사용자들에게 최대한의 신뢰성 있는 암호기술 사용의 자유를 보장하기 위한 선결과제인 키복구 기술개발이다. 그러나 키복구 시스템 사용 목적을 무력화시키는 이중 암호화(Double encryption)라는 문제점이 존재한다[1],[2],[3]. 이러한 문제점을 해결하기 위해서는 암호문·평문 판별기술 개발이 필요하다.

암호 알고리즘 설계시 출력문(암호문)이 난수이어야 함은 암호 알고리즘 설계시 필요조건이며 난수성을 조사하기 위해서는 많은 양의 암호문을 가지고 각종 통계적인 방법에 의하여 검증한다. 현재까지는 암호 알고리즘 출력문에 대한 난수성 검정방법들에 대해서만 연구되어 왔으며[4],[5],[6],[7], 검정을 위한 비교 및 분석이 이루어지기는 하였으나[8],[9],[10] 이론적으로 검정을 위한 최소한의 표본크기에 대한 연구결과는 정립되어 있지 않고 있다. 평문과 암호문을 구분할 수 있는 방법을 개발하기 위해서는 암호 알고리즘의 출력문이 가지고 있는 성질인 난수성을 조사하여야 하며 실시간이라는 조건이 부가됨으로써 적은 양의 데이터를 가지고서 판별하여야 한다는 어려움이 있다. 그러므로 적은 양의 데이터를 가지고 그 데이터가 암호문인지 평문인지를 판별하는 통계적인 방법에 대한 연구가 필요하다.

본 연구에서는 보편적으로 많이 사용되고 있는 frequency test, poker test, runs distribution test, 그리고 serial test를 주어진 데이터에 적용하여 평균 p-값과 성공률을 그래프와 함께 제시하고 비교 분석한다. 평문으로 그림파일(bmp), 실행파일(exe), 한글파일(hwp), 소리파일(wav), 그리고 압축파일(zip)을 선정하고 임의의 키와 위에 주어진 평문들을 가지고 DES(Data Encryption Standard)를 CBC(Cipher Block Chaining)모드로 생성한 데이터들을 암호문이라 가정한다. 이러한 데이터에 대해서 평문·암호문 식별에 대한 각 검정방법의 특성과 성공률을 분석한다.

또한 실험계획법 중 하나의 설계방법인 완전확률화계획법을 이용하여 하나의 난수성 검정방법에 대한 각 표본크기별 성공률을 비교하여 임의의 파일에 대한 평문·암호문 식별에 필요한 하나의 최소한 표본크기를 실험에 사용된 표본크기들 중에서 다중비교를 통하여 제안한다.

Ⅱ장에서는 본 연구에 사용된 분석방법과 비교방법에 대해서 설명하며 Ⅲ장에서는 실험을 통한 분석결과를 Ⅳ장에서는 전체적인 결론을 제시한다.

Ⅱ. 분석 및 비교 방법

1. 자료의 선정

본 연구에서 데이터는 임의로 선택한 하나의 파일에서 생성된 비트스트림을 가지고 암호 시스템을 이용한 새로운 비트스트림을 추출해내는 과정으로 연결된다. 실제 자료에 대한 공정성을 고려하면서 길이가 130kb인 임의의 파일을 선택하였다. 파일의 종류별로 그림파일(bpm), 실행파일(exe), 한글파일(hwp), 소리파일(wav), 그리고 압축파일(zip) 등 모두 5개의 파일을 무작위로 선정하였다. Visual C++ 프로그램을 이용하여 위의 파일들에 대한 비트스트림을 추출하였고 이를 평문으로 정의한다. 다음에 DES[11],[12]를 CBC모드로 적용하여 새로운 비트스트림을 생성하였고 이를 암호문으로 정의한다.

대다수의 블록 암호 알고리즘에서 출력문의 크기는 64비트 혹은 128비트 단위로 생성되므로 위에서 생성된 암호문과 평문에 대한 비트스트림에서 길이가 128, 256, 512, 1024비트인 100개의 부분수열을 추출한다. 따라서 각각의 평문, 암호문에서 발생된 2진 수열을 실시간의 개념으로 고정된 길이의 부분수열의 비트수를 늘려가며 다음에 제시된 4가지의 난수성 검정 방법에 적용하여 100개의 p-값을 구하고 그에 따른 성공률을 계산한다.

2. 난수성 검정 방법 및 실험계획법

(1) 난수성 검정 방법

난수성 검정 방법에서의 자료는 평문 혹은 암호문의 비트스트림이며 이러한 통계적 검정을 위한 귀무가설은 다음과 같이 설정된다.

H_0 : 비트스트림은 난수성을 만족한다.

난수성 검정을 위하여 일반적으로 많이 사용되고 있는 frequency test, poker test, runs distribution test, serial test[4],[9],[13],[14],[15],[16],[17],[18]를 선정하였다. 이때, 검정통계량은 모두 χ^2-분포를 따르며, 이 통계량 값이 설정된 유의수준 α에 대하여 χ^2_α 보다 크면 귀무가설을 기각한다. 즉 각각의 통계량 값에 대한 유의확률 p-값이 α보다 커지게 되면 비트스트림은 난수성을 만족한다고 할 수 있다. 여기서 귀무가설을 검정하기 위한 유의수준 α는 $\alpha=0.05$로 설정하였으며 모의실험을 위해 SAS/AF를 이용하여 모듈화된 알고리즘을 사용하였다.

(2) 실험계획법

① 완전확률화 계획법(Completely randomized design)

완전확률화 계획법은 어떤 관심 있는 특성치에 대한 인자의 영향을 조사하기 위하여 사용되어지는 실험계획법 중의 하나이다. 즉, 임의의 한 난수성 검정법에 대하여 검정을 통하여 구해지는 p-값을 특성치라 하면 실험에 사용되는 128, 256, 512, 1024 비트수를 인자 수준으로 간주하여 이 수준들 사이에 유의한 차이가 있는가, 다시 말하면, 비트수에 따라 평균 p-값에 차이가 있는가를 알아보기 위한 실험계획법이라 할 수 있다.

이 실험계획법을 본 연구에 적용하기 위하여 먼저 임의의 한 검정방법에 의하여 계산된 100개의 p-값으로 이루어진 자료의 구조를 보면 〈표 1〉과 같다.

여기서, p_{ij}는 i번째 비트수로 검정할 때 계산되는 j번째 p-값이 된다.

위의 실험에 대하여 인자의 수준이 I개 있고, 각 수준에서의 반복수가 똑같이 J인 일원배치법의 모형을 설정할 수 있으며, 이때 다음과 같은 통계적 모형을 설정할 수 있다.

표 1 완전확률화 계획법을 위한 자료의 구조

실험의 회수 / 비트수	1	2	3	.....	100
128	p_{11}	p_{12}	p_{13}	.....	$p_{1,100}$
256	p_{21}	p_{22}	p_{23}	.....	$p_{2,100}$
512	p_{31}	p_{32}	p_{33}	.....	$p_{3,100}$
1024	p_{41}	p_{42}	p_{43}	.....	$p_{4,100}$

<Table 1> Structure of data for completely randomized design

$$p_{ij} = \mu_i + e_{ij}, \quad i = 1,2,\cdots,I, \; j=1,2,\cdots,J.$$

여기서 μ_i는 수준 i에서의 모평균이고, e_{ij}는 평균이 0이고 분산이 σ^2_E인 정규분포를 따르는 오차항으로 가정한다. 또한, μ는 실험전체의 모평균으로 $\mu = \sum_{i=1}^{I} \mu_i / I$으로 정의하고 μ_i와 μ 간의 차이를 $a_i = \mu_i - \mu$로 표현하면

$$\begin{aligned} p_{ij} = \mu_i + e_{ij} &= \mu + (\mu_i - \mu) + e_{ij} \\ &= \mu + a_i + e_{ij} \end{aligned}$$

가 되며 이것이 완전확률화계획법의 구조식이 된다. 여기서 a_i는 비트수에서의 모평균 μ_i가 전체의 모평균 μ로부터 어느 정도의 치우침을 가지는가를 나타내는 수치로 주효과(main effect)라고 부르며

$$\begin{aligned} \sum_{i=1}^{I} a_i &= \sum_{i=1}^{I} (\mu_i - \mu) \\ &= \sum_{i=1}^{I} \mu_i - I\mu \\ &= 0 \end{aligned}$$

이 됨을 알 수 있다. 따라서 본 실험의 경우에 검정을 위한 귀무가설은

$$H_0 \; : \; a_1 = a_2 = a_3 = a_4$$

이며 다시 표현하면 임의의 한 난수성 검정방법에 대하여 4가지 비트수에 따른 성공률이 같다는 의미가 되고 이 의미는 결과적으로 비트의 크기가 검정에 영향을 주지 못한다고 말할 수 있다. 따라서, 귀무가설의 기각 여부에 따라 각 검정방법별로 그에 따른 적절한 검정표본의 크기를 제시할 수 있는 근거가 된다.

위에 언급된 가설은 분산분석표를 통하여 검정을 시행하게 되며 분산분석표의 형태는 다음 〈표 2〉와 같다.

여기서,

TSS(Total Sum of Squares) = 전체제곱합 = $\sum_{i=1}^{I}\sum_{j=1}^{J}(p_{ij}-\overline{p_{..}})^2$, $\overline{p_{..}}=\frac{1}{IJ}\sum_{i=1}^{I}\sum_{j=1}^{J}p_{ij}$,

SSE(Sum of Squares due to error) = 오차제곱합 = $\sum_{i=1}^{I}\sum_{j=1}^{J}(p_{ij}-\overline{p_{i.}})^2$, $\overline{p_{i.}}=\frac{1}{J}\sum_{j=1}^{J}p_{ij}$.

SST(Sum of Squares due to Treatment) = 처리제곱합 = TSS - SSE 이고

MST(Mean Squares due to Treatment) = 평균제곱합 = $\frac{SST}{I-1}$

MSE(Mean Squares due to Error) = 평균오차제곱합 = $\frac{SSE}{I(J-1)}$ 이며 $F=\frac{MST}{MSE}$ 이다. 이때, F-값이 유의수준 α에 대하여 $F > F_{1-\alpha}(I-1, I(J-1))$이면 귀무가설을 기각하며, $F_{1-\alpha}(I-1, I(J-1))$은 자유도 $(I-1, I(J-1))$인 F-분포의 $100(1-\alpha)$백분위수를 의미한다.

② 최소유의차(Least Significant Difference : LSD)방법

완전확률화 계획법에서의 분산분석을 이용하여 각 비트수에 따른 평균 p-값의 차이가 없다는 귀무가설이 기각되었을 경우 어떤 비트수와 어떤 비트수 사이에 유의한 차이가 있는가를 구분하므로서 결과적으로 유의한 차이가 없는 비트수끼리 그룹화하는 방법이 된다. 즉, 동일한 그룹내에서는 평균 p-값의 차이가 없으므로 실시간 처리의 관점에서 본다면 동일 그룹내에서는 작은 비트수로 검정을 시행하여도 같은 성공률을 유지할 수 있는 효과를 얻게 된다. 또한, 귀무가설을 기각하지 못할 때에는 4가지 서로

표 2 분산분석표

요인	자유도	제곱합	평균제곱합	F-값
비트수	I-1	SST	MST	F
오차	$I(J$-1)	SSE	MSE	
총계	IJ-1	TSS		

<Table 2> Analysis of Variance Table

다른 비트수에 따른 평균 p-값의 차이가 없다는 의미이므로 전체가 하나의 그룹이 되고 이때, 가장 작은 비트수인 128비트로 검정을 하더라도 그 이상의 비트수로 검정을 시행한 것과 동일한 효과를 얻게 된다.

이는 R. A. Fisher에 의하여 제안된 방법으로 두 개 이상의 집단간 차이를 민감하게 구분해 내는 장점을 가지고 있으며 l비트와 m비트에 대한 평균 p-값 $\overline{p_{l.}}$과 $\overline{p_{m.}}$의 차이가

$$|\overline{p_{l.}}-\overline{p_{m.}}| > t_{1-\alpha/2}(I(J-1))\sqrt{\frac{2\hat{\sigma}^2}{J}}$$

이면 유의수준 α에서 유의한 차가 인정된다. 여기서, $t_{1-\alpha/2}(I(J-1))$는 자유도 $I(J-1)$인 t-분포의 $100(1-\alpha/2)$백분위수를 의미하며 $\hat{\sigma}^2 = MSE$가 된다[20].

Ⅲ. 결과 및 분석

1. 비모수적 검정 방법을 이용한 결과

아래의 〈표 3〉에서 〈표 6〉까지는 각각의 비트스트림에 대하여 비모수적 검정방법을 이용한 결과를 보여주고 있다. 여기에서 p-값은 난수성 검정에서 유의수준 α와 비교하여 작은 경우 평문으로, 큰 경우에는 암호문으로 판별하는 기준이 되고 있다. 평균 p-값은 100개의 부분수열에서 계산한 각각의 p-값의 평균을 나타내며 또한 평문이 평문으로 판정되는 성공률과 암호문이 암호문으로 판정되는 성공률을 보여주고 있다. 전체적으로 암호문의 p-값과 성공률은 상당히 높고 안정된 모습을 보이고 있으며

평문은 약간 불안정한 모습을 보여주고 있다. 특히 hwp파일은 비트수가 증가할 때 성공률이 감소하고 있는 모습을 보여주고 있는데 이는 hwp파일이 갖고 있는 특이한 성질이며 이는 그래프에서도 확인할 수 있다. (그림 1)에서 (그림 4)까지는 각각의 비트스트림에 대한 p-값을 도시화한 것이다. 각각의 난수성 검정방법에 대하여 비트수와 파일이름을 주제로 표기했으며, 수평축은 실험횟수를, 수직축은 암호문(c)과 평문(p)에 대한 각각의 모의실험에서 구한 p-값을 나타낸다. 또한 그래프의 p-값의 평균값(mean)과 표준편차(dev)를 제시하였다.

결과에서 쉽게 볼 수 있는 것은 암호문의 평균 p-값이 평문의 평균 p-값보다 비교적 높게 나타나고 있지만 비트수 별로 추세가 상당히 불안정하여 표준편차도 높다는 것을 알 수 있다. (그림 1)에서 (그림 4)까지에서 128비트와 1024비트에 대한 그래프는 삭제되어 있다. 이는 256비트와 512비트에 대한 그래프와 비교하여 비슷한 경향을 보이고 있기 때문에 분석에 무리가 따르지 않으리라 사료되어 삭제하였다.

이제 각각의 난수성 검정별로 비트스트림에 따른 성질에 대해 살펴보기로 한다.

(1) Frequency test

〈표 3〉을 보면 암호문에서의 평균 p-값은 0.4575-0.5374로서 상당히 높고 안정되어 있다고 할 수 있다. 또한 성공률에 있어서 암호문은 90% 정도로 안정적이며, 평문은 비교적 불안정하다는 것을 볼 수 있다. 평문의 경우 bmp, exe 파일의 평균 p-값은 낮고 따라서 성공률은 90% 이상으로 높게 안정되어 있으나 hwp, wav, zip 파일에서는 비교적 높고 성공률도 낮게 평가되고 있으며, 특히 hwp파일은 비트수가 증가할 때에도 p-값이 증가하고 성공률이 감소하는 특이한 경향을 보이고 있다. 이는 (그림 1)에서도 확인할 수 있는데 bmp 파일과 exe 파일은 암호문과 평문의 차이가 커서 비트수에 관계없이 뚜렷하게 구분할 수 있고, hwp 파일의 평문에서 약 9000여 비트 정도까지는 p-값이 0에 가깝다는 것을 볼 수 있다. wav 파일과 zip 파일에서는 평균의 차이가 크지만 그만큼 표준편차도 크기 때문에 암호문과 평문의 뚜렷한 차이를 찾아내기는 힘든 것으로 판단된다.

(2) Poker test

〈표 4〉를 보면 암호문에서의 평균 p-값은 0.4288-0.5424 로서 상당히 높고 성공률도 90% 이상으로 비트수에 관계없이 안정되어 있다. 평문의 경우 bmp, exe, wav 파일의 성공률도 상당히 높게 평가되어 있으며, zip 파일의 성공률은 비트수에 따라 큰 변화를 보이고 있다. (그림 2)에서도 bmp, exe, wav 파일과 zip 파일에서의 512 비트의 그래프는 암호문과 평문사이의 구분을 뚜렷하게 보여주고 있다. 하지만, hwp 파일의 256, 512비트의 그래프와 zip 파일에서의 256 비트의 그래프에서는 표준편차가 크기 때문에 확실한 차이를 찾아내기는 힘들다고 생각된다.

(3) Runs distribution test

〈표 5〉에서 암호문은 비트수가 증가함에 따라 평균 p-값도 점차 증가하고 있으며 그 범위는 0.2651-0.4858 정도이다. 성공률은 90% 내외로 비교적 안정되어 있다고 할 수 있다. 평문의 경우 bmp, exe, wav 파일은 p-값이 낮고, 성공률도 높게 평가되었고, hwp 파일과 zip 파일의 경우, 위의 Poker test와 비슷한 결과를 보여주고 있다. (그림 3)에서도 실험횟수에 따른 p-값의 추이를 살펴보면 bmp, exe, wav 파일은 암호문과 평문사이를 뚜렷하게 구분하였고, zip 파일의 경우 표준편차가 높기 때문에 복잡한 패턴을 보여주고 있다.

(4) Serial test

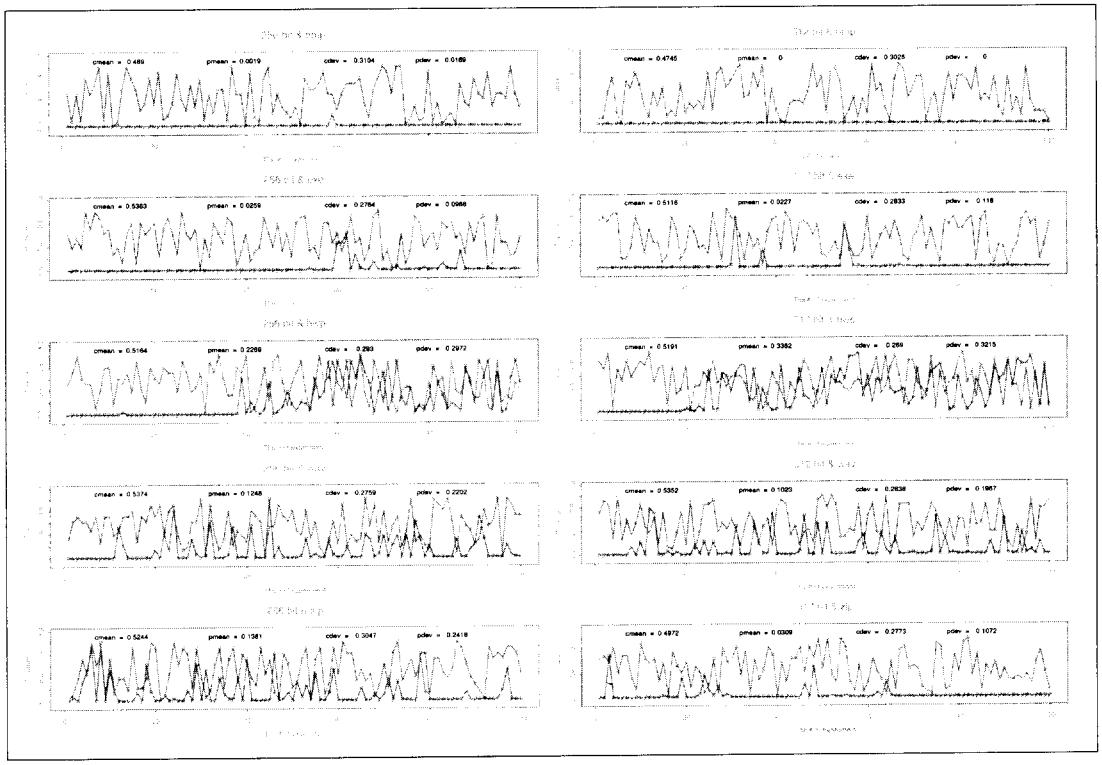
〈표 6〉를 보면 암호문의 평균 p-값은 0.4656-0.5884정도의 범위를 갖고 있으며, 이는 평문과 상당히 구분되어진다. 성공률도 90% 이상에서 결정되어지고 있다. 평문에서는 bmp, exe, wav 파일이 낮은 p-값과 높은 성공률을 보이고 있지만 hwp 파일과 zip 파일에서는 높은 p-값과 낮은 성공률을 보이고 있다. (그림 4)에서도 bmp, exe, wav 파일은 암호문과 평문을 쉽게 구별해 주고 있지만, hwp, zip 파일은 표준편차가 높기 때문에 암호문과 평문을 구별하기 어렵다는 것을 볼 수 있다.

표 3 빈도수 검정의 성공률

파 일	비트수	평 문		암 호 문	
		평균 p-value	성공률(%)	평균 p-value	성공률(%)
Bmp	128	0.0122	95	0.5186	93
	256	0.0019	99	0.4890	93
	512	0	100	0.4745	92
	1024	0.0001	100	0.4784	91
Exe	128	0.0148	96	0.4960	98
	256	0.0259	92	0.5363	96
	512	0.0227	96	0.5116	98
	1024	0.0091	96	0.4900	96
Hwp	128	0.0799	74	0.5370	95
	256	0.2269	47	0.5164	93
	512	0.3362	33	0.5191	94
	1024	0.3427	29	0.5308	95
Wav	128	0.0743	83	0.5362	98
	256	0.1248	67	0.5374	97
	512	0.1023	72	0.5352	99
	1024	0.1504	66	0.4799	97
Zip	128	0.2578	48	0.4575	95
	256	0.1381	65	0.5244	95
	512	0.0309	89	0.4972	97
	1024	0.0360	92	0.5257	92

<Table 3> Success rate of frequency test

그림 1 빈도수 검정의 p-값



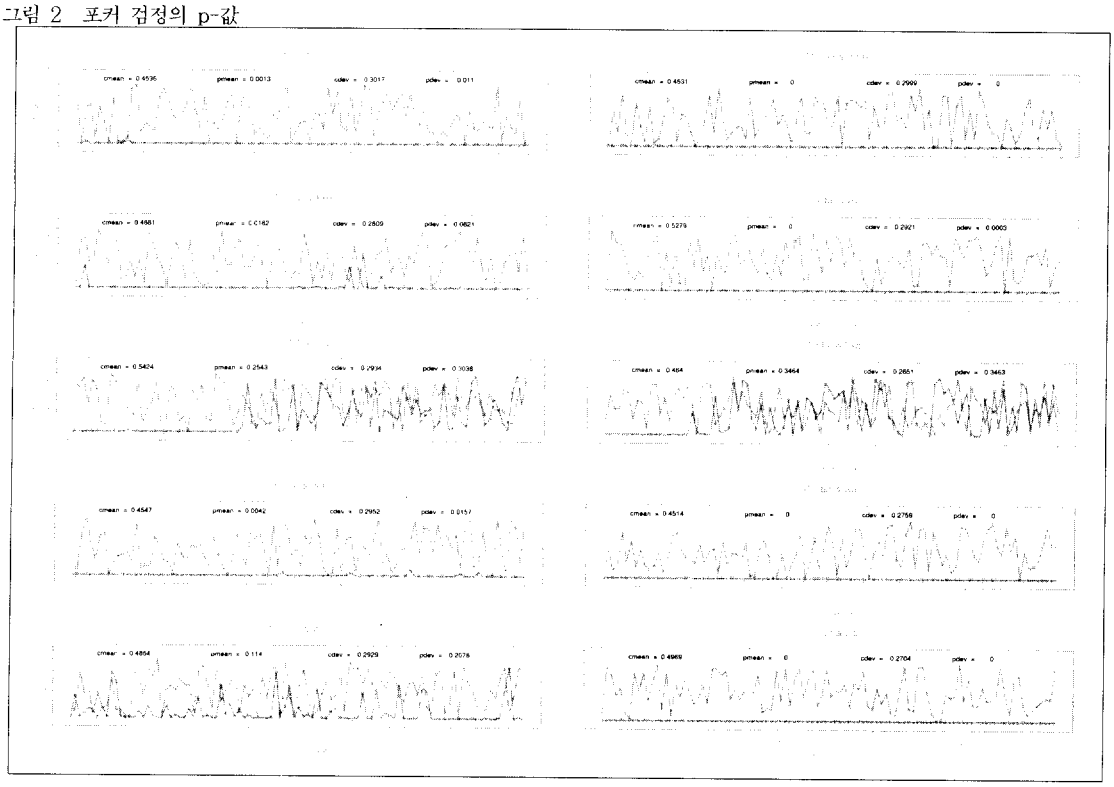
(Fig. 1) p-value of frequency test

표 4 포커 검정의 성공률

파 일	비트수	평 문		암 호 문	
		평균 p-value	성공률(%)	평균 p-value	성공률(%)
Bmp	128	0.0167	93	0.4515	87
	256	0.0013	99	0.4536	88
	512	0	100	0.4531	90
	1024	0	100	0.4288	92
Exe	128	0.0168	97	0.4708	96
	256	0.0182	96	0.4681	96
	512	0	100	0.5279	95
	1024	0	100	0.5119	95
Hwp	128	0.1331	70	0.4737	95
	256	0.2543	42	0.5424	96
	512	0.3464	36	0.4640	95
	1024	0.3822	19	0.4513	95
Wav	128	0.0117	96	0.5081	96
	256	0.0042	96	0.4547	91
	512	0	100	0.4514	94
	1024	0.0001	100	0.4793	93
Zip	128	0.2033	43	0.4890	95
	256	0.1140	67	0.4854	92
	512	0	100	0.4969	97
	1024	0.0015	98	0.4872	91

<Table 4> Success rate of poker test

그림 2 포커 검정의 p-값



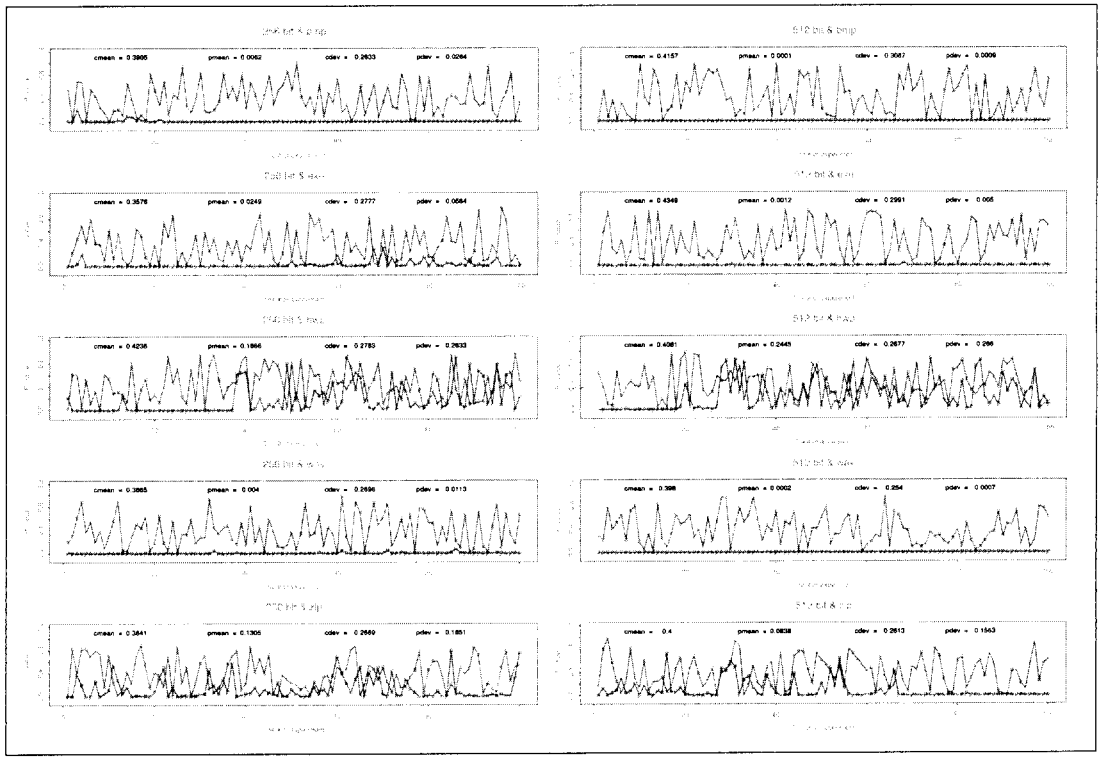
(Fig. 2) p-value of poker test

표 5 런 분포 검정의 성공률

파 일	비트수	평 문		암 호 문	
		평균 p-value	성공률(%)	평균 p-value	성공률(%)
Bmp	128	0.0511	80	0.3216	90
	256	0.0062	96	0.3905	92
	512	0.0001	100	0.4157	90
	1024	0	100	0.4375	89
Exe	128	0.0211	93	0.2651	85
	256	0.0249	87	0.3576	88
	512	0.0012	100	0.4349	92
	1024	0	100	0.4512	88
Hwp	128	0.0587	76	0.3444	90
	256	0.1866	52	0.4236	93
	512	0.2445	40	0.4081	90
	1024	0.2422	30	0.4242	90
Wav	128	0.0207	89	0.2915	81
	256	0.0040	98	0.3865	91
	512	0.0002	100	0.3980	95
	1024	0	100	0.4858	95
Zip	128	0.1358	44	0.3114	82
	256	0.1305	54	0.3841	89
	512	0.0838	71	0.4000	93
	1024	0.0024	99	0.4829	97

<Table 5> Success rate of runs distribution test

그림 3 런 분포 검정의 p-값



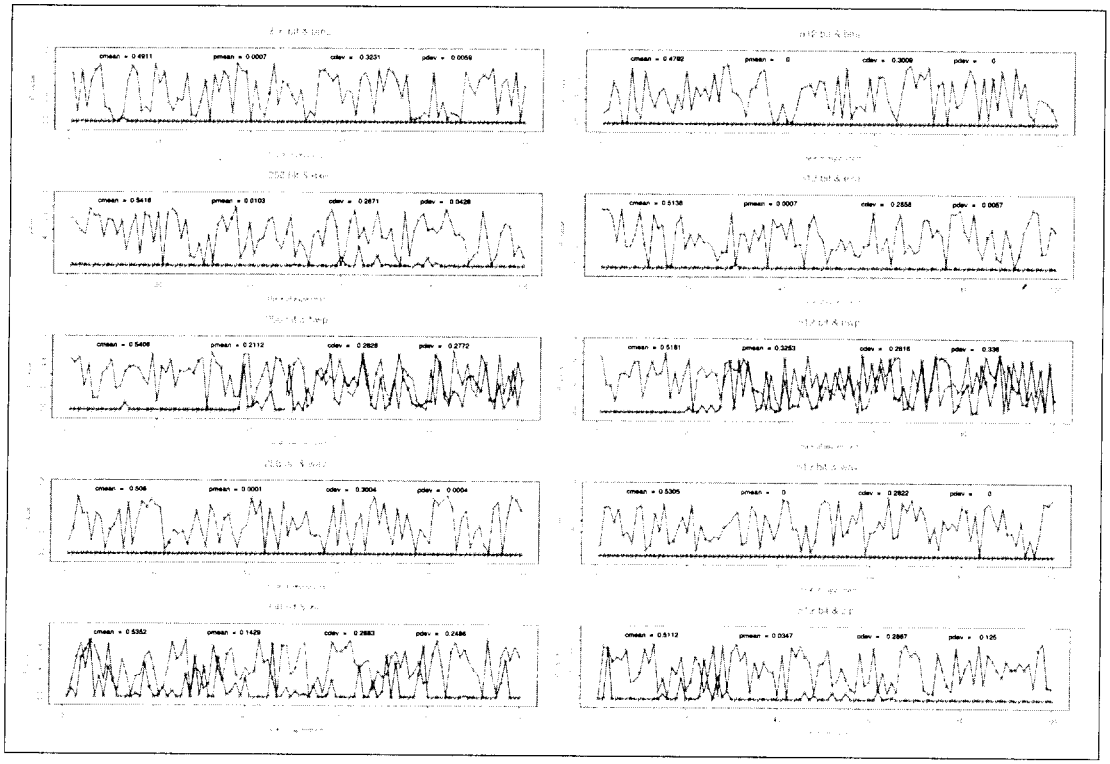
(Fig. 3) p-value of runs distribution test

표 6 순차 검정의 성공률

파 일	비트수	평 문		암 호 문	
		평균 p-value	성공률(%)	평균 p-value	성공률(%)
Bmp	128	0.0161	96	0.5155	95
	256	0.0007	99	0.4911	93
	512	0	100	0.4792	91
	1024	0	100	0.4656	91
Exe	128	0.0167	97	0.5014	94
	256	0.0103	95	0.5416	94
	512	0.0007	99	0.5138	97
	1024	0	100	0.4854	95
Hwp	128	0.0833	77	0.5884	96
	256	0.2112	46	0.5406	95
	512	0.3253	31	0.5181	95
	1024	0.2750	27	0.5150	94
Wav	128	0.0026	99	0.4897	98
	256	0.0001	100	0.5080	95
	512	0	100	0.5305	97
	1024	0	100	0.5089	96
Zip	128	0.2433	45	0.4780	95
	256	0.1429	66	0.5352	93
	512	0.0347	88	0.5112	98
	1024	0.0177	92	0.5386	99

<Table 6> Success rate of serial test

그림 4 순차 검정의 p-값



(Fig. 4) p-value of serial test

2. 최소유의차 방법을 이용한 다중비교의 결과

〈표 7〉에서는 각각의 스트림에서 비트수에 따른 평균 p-값을 비교하여 비트수가 검정에 영향을 주는지를 분석한 표이다. 이를 위해 비트스트림에 대하여 p-값의 평균을 계산하고, 최소유의차(Least Significant Difference) 방법을 사용하여 어느 비트간에 p-값이 다른지에 관한 다중비교를 수행한다. 여기에서 보여지는 세 가지 영문자 A, B, C는 그룹화하는 것을 의미하는 것으로 같은 문자로 표시되어 있는 비트들 사이에는 평균 p-값에 차이가 없다는 것을 의미하며, 다른 문자로 표시되어 있는 비트들은 다른 그룹으로 구분되어진다는 것을 뜻한다. 또한 F-값은 총변동에 대한 정도를 나타내고 있으며, 다중비교에서의 의미는 유의수준 α보다 작을 때, 전체 비트들 사이에서 유의한 차이가 있음을 의미한다.

(1) Frequency test

암호문의 경우에 모든 비트스트림에 대하여 평균 p-값의 차이가 없다. 즉, 4가지 서로 다른 비트수에 따른 성공률에 차이가 없다는 것을 의미한다. 이는 F-값이 높다는 것을 보아도 쉽게 알 수 있다. 평문의 경우에 bmp 파일과 exe 파일은 비트수에 따른 성공률의 차이가 없다고 할 수 있다. 하지만 hwp 파일과 zip 파일에서는 128비트의 그룹, 256비트의 그룹, 그리고 (512, 1024)비트의 그룹으로 분리되며, wav 파일의 경우 그룹화할 때 발생하는 오류를 감안하면 최소한의 그룹화는 가능하나 F-값이 0.05보다 크므로 그룹화가 무의미하다고 판단된다. 따라서 frequency test를 위해 요구되어지는 최소의 비트수를 평문의 경우, 512비트로 정하여도 비트스트림의 난수성을 파악하는데 적절하다고 볼 수 있으며, 암호문의 경우에는 128비트만으로도 충분한 검정을 수행할 수 있다고 판단된다.

(2) Poker test

암호문에서 hwp 파일은 위에서 언급한 것과 마찬가지로 그룹화가 가능한 것처럼 보이나 F-값이 0.05보다 크므로 그룹화가 무의미하고, 나머지 파일들에 대하여는 p-값에서의 차이가 크지 않으며, 또한 F-값에서도 비트수 별로 유의한 차이가 있지 않다는 결과를 얻을 수 있었다. 평문에서는 exe 파일을 제외한 모든 파일에서 유의한 차이가 있다는 결과를 얻었다. 특히 hwp 파일과 zip 파일의 경우에는 128비트의 그룹, 256비트의 그룹, (512, 1024)비트의 그룹으로 구분되어지는데 이는 F-값이 0.0001 정도로 각 그룹간 차이가 크다고 할 수 있다. 결국, poker test의 경우, 최소의 비트수를 평문에서는 512비트로 정하는 것이 적절하다고 할 수 있으며 암호문에서는 128비트로 정하는 것이 검정을 수행하는데 적절하다고 할 수 있을 것이다.

(3) Runs distribution test

암호문을 보면 bmp 파일은 (128, 256)비트 그룹과 (256, 512, 1024)비트 그룹으로 분리되고 exe 파일은 128비트의 그룹, 256비트 그룹, (512, 1024)비트의 그룹으로 분리된다. wav 파일은 128비트 그룹, (256, 512)비트 그룹 그리고 1024비트의 그룹으로 분리된다는 것을 발견할 수 있으며 zip 파일은 (128, 256), (256, 512), 1024비트의 그룹으로 분리되는 것을 알 수 있다. 또한 각각의 F-값에서 hwp 파일을 제외한 모든 파일의 비트스트림이 통계적으로 유의하게 차이가 있다는 결과를 얻을 수 있었다. 평문에서도 bmp 파일 그리고 wav 파일에 대하여는 128비트의 그룹과 (256, 512, 1024)비트의 그룹으로 분리되며, zip 파일에 대하여는 (128, 256)비트 그룹, 512비트의 그룹, 1024비트의 그룹이 유의하게 그룹간 차이가 있다는 것을 알 수 있다. 따라서 runs distribution test를 할 경우, 최소의 비트수를 암호문과 평문에서 1024비트로 정하여 검정을 수행하는 것이 적당할 것이라고 생각된다.

(4) Serial test

암호문에서는 F-값이 모두 높게 유지되고 모든 비트스트림이 유의하게 차이가 있지 않다는 것을 알 수 있다. 따라서 요구되어지는 최소의 비트수는 128비트로 정할 수 있을 것이다. 암호문에서 wav 파일은 모두 같은 그룹으로 판정되었으며, 나머지 파일들에 대하여는 128비트 그룹, (256, 512)비트와 1024비트 정도의 그룹으로 구분되어 있는 것을 볼 수 있다. bmp, exe 파일의 경우 오류를 고려할 때 그룹화가 가능하기는 하나 F-값이 0.05보다 크므로 그룹화는 무의미하다고 판단된다. 따라서 검정을 위해 요구되어지는 최소의 비트수는 평문에서 512비트로 정할 수 있으며, 암호문에서는 단지 128비트의 비트스트림으로 난수성을 파악하는데 충분하다고 할 수 있다.

표 7 최소유의차 방법을 이용한 다중비교

	평 문					암 호 문				
frequency test	F-값	128	256	512	1024	F-값	128	256	512	1024
bmp	0.1614	A	A	A	A	0.7474	A	A	A	A
exe	0.5698	A	A	A	A	0.6769	A	A	A	A
hwp	0.0001	C	B	A	A	0.9427	A	A	A	A
wav	0.1029	B	A,B	A,B	A	0.3874	A	A	A	A
zip	0.0001	A	B	C	C	0.3140	A	A	A	A
Poker test										
bmp	0.0016	A	B	B	B	0.9204	A	A	A	A
exe	0.0611	A,B	A	B	B	0.3383	A	A	A	A
hwp	0.0001	C	B	A	A	0.1020	A,B	A	A,B	B
wav	0.0123	A	A,B	B	B	0.4700	A	A	A	A
zip	0.0001	A	B	C	C	0.9929	A	A	A	A
Runs distribution test										
bmp	0.0001	A	B	B	B	0.0202	B	B,A	A	A
exe	0.0042	A	A	B	B	0.0001	C	B	A	A
hwp	0.0001	B	A	A	A	0.1220	B	A	A,B	A
wav	0.0001	A	B	B	B	0.0001	C	B	B	A
zip	0.0001	A	A	B	C	0.0001	C	B,C	B	A
Serial test										
bmp	0.0639	A	B	B	B	0.5694	A	A	A	A
exe	0.0972	A	A,B	B	B	0.5739	A	A	A	A
hwp	0.0001	C	B	A	A,B	0.3529	A	A	A	A
wav	0.1525	A	A	A	A	0.7914	A	A	A	A
zip	0.0001	A	B	C	C	0.2912	A	A	A	A

<Table 7> Multiple comparison using least significant difference

Ⅳ. 결 론

본 연구에서는 암호 알고리즘을 통해 생성된 출력 수열의 난수성을 판별하기 위해 4가지 비모수적 난수성 검정방법을 사용하여 암호문과 평문의 p-값과 성공률을 확인하였다. 〈표 1〉에서 〈표 4〉까지는 평문의 경우, hwp 파일은 비트수가 증가하면서 평균 p-값이 증가하고 성공률이 감소하는 경향을 보였다. 이는 hwp 파일이 갖고 있는 특이한 성질로서 파일을 작성할 때 디폴트로 정해지는 수열 때문에 대략 9000여 비트까지 p-값이 0에 가까운 형태로 나타나는 현상이라고 판단된다. 다른 평문 파일들은 몇몇 경우를 제외하고 비트수가 증가할 때 평균 p-값이 감소하고 성공률이 증가하는 경향을 보였다. 암호문의 경우 모든 비트스트림에서 90% 내외의 높고 안정된 성공률을 보여주었다. (그림 1)에서 (그림 4)까지를 보면, 대체로 평문의 평균 p-값은 암호문의 평균 p-값보다 낮으며, 비트수가 증가할 때, 암호문과 평문에서의 p-값의 폭이 증가하고 있다. 이러한 경향에서 볼 수 있듯이, 난수성을 평가하기 위해 많은 비트수가 요구되어 진다고 할 수 있다. 하지만, 그러한 경우, 계산 시간의 문제, 또는 크기가 작은 파일의 난수성 탐지 불능 등의 문제가 발생할 수도 있다. 따라서 임의의 데이터에 대하여 난수성을 판별하는데 최소한의 데이터 크기를 정하기 위해 분산분석에서 사용되는 최소유의차 방법을 이용하여 비트수 간에 유의한 차이가 있는지 살펴본 결과, frequency test, poker test, serial test에서는 512비트, 그리고 runs distribution test에서는 1024비트를 최소로 요구되어지는 비트수로 결정할 수 있다.

이번 연구에서 각 검정방법에 따른 비트수에 대한 p-값을 구하고 그에 관한 그래프를 그려보았다. 이때, 각각의 실험에서 p-값의 변화를 볼 수 있었으며, 전체적으로 평문에 대한 p-값이 암호문에 대한 p-값보다 안정적이라는 것을 알 수 있었다. 이와 같은 난점을 해결하기 위해 암호문에서는 p-값이 안

정적으로 높게 측정되는 난수를 발생시키는 것이 중요하며, 평문 검정에서는 2진 비트스트림에 내재되어 있는 다양한 속성을 검정할 수 있는 방법을 채택하도록 하는 것이 중요할 것으로 생각된다. 따라서 유일한 검정방법에 의존하는 것보다 다양한 검정방법을 사용하여 암호화에 필요한 모의난수의 난수성을 다각적인 측면에서 검증하는 것이 바람직하리라고 사료된다. 또한, 실험의 특성과 시간의 제약 등에 의하여 본 연구에서는 128, 256, 512, 1024비트에 관한 실험을 시행하였으나 연구된 결과를 토대로 좀 더 세분화된 비트수에 관한 실험이 이루어진다면 더 나은 결과도 도출될 수 있으리라 사료된다.

참 고 문 헌

[1] Seungjoo Kim,Insoo Lee,Masahiro Mambo and Sungjun Park, "On the difficulty of key recovery systems", to appear on Proceeding of ISW'99, Information Security Workshop, Springer-Velag, Lecture Notes in Computer Sciences, December 1999

[2] M. Blaze, "Protocol failure in the escrowed encryption standard", The 2nd ACM Conference on Computer and Communications Security, pp.59-67, November 1994

[3] B. Pfitzmann and M. Waidner, "How to break fraud-detectable key recovery", *ACM Operating System Review* 32(1), pp.23-28, January 1998

[4] D. Knuth, "The art of computer programming : seminumerical algorithms, 2", *Addison Wesley*, 1973

[5] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, 28, pp.656-715, 1949

[6] J. Gait, "A new nonlinear pseudorandom number generator", *IEEE Transactions on Software Engineering, SE-3*, pp.359-363, September 1977

[7] R. R. Jueneman, "Analysis of certain aspects of output feedback mode", *Advances in Cryptology-Proceedings of CRYPTO '82, Plenum Press*, pp.99-127, 1983

[8] NIST, "NIST randomness testing for round 1 AES candidates", http://www.nist.gov/aes, 1999

[9] 한국정보보호센터, "128비트 블록 암호 알고리즘 (SEED)개발 및 분석보고서", http:\\www.kisa.or.kr/technology/sub1/128-seed.pdf

[10] H. M. Gustafson, "Statistical analysis of symmetric cipher", Doctoral Thesis, *Queensland University of Technology*, pp.35-138, 1996

[11] FIPS, "Data encription standard", *Federal Information Processing Standard Publication*, 46, National Bureau of Standards, Washington DC, 1977

[12] 한국전자 통신연구소, "현대암호학", pp.58-66, 1991

[13] H. Beker and F. Piper, "Cipher systems : The protection of communications", *Wiley*, 1982.

[14] A. M. Mood, "The distribution theory of runs", *Annals of Mathematical Statistics*, 11, pp.367-392, 1940

[15] I. J. Good, "The serial test for sampling numbers and other tests for

randomness", *Proceedings of the Cambridge Philosophical Society*, 49, pp.276-284, 1953

[16] I. J. Good, "On the serial test for random sequences", *Annals of Mathematical Statistics*, 28, pp.262-264., 1957

[17] D. J. Sheskin, "Handbook of parametric and nonparametric statistical procedures", *CRC Press Inc*, pp.140-143, 1997

[18] J. D. Gibbons, "Nonparametric statistical inference", 2nd edition, *Marcel Dekker Inc.*, New York, pp.68-90, 1985.

[19] 박성현, "현대실험계획법", 민영사, 1996

[20] R. A. Fisher, "The design of experiments", 4th edition, *Oliver and Boys*, Edinburg, 1947

著者紹介 ----------

박 홍 구(Hong Gu Park) 정회원

1981년 2월 : 한양대학교 수학과 졸업
1989년 12월 : North Texas University 박사
1996년 3월~현재 : 한양대학교 수학과 부교수

〈관심분야〉 대수학, 암호학

차 경 준(Kyung Joon Cha) 정회원

1981년 2월 : 한양대학교 수학과 졸업
1990년 5월 : Southern Methodist University 박사
1993년 3월~현재 : 한양대학교 수학과 부교수

〈관심분야〉 통계학

장 호 종(Ho Jong Jang) 정회원

1981년 2월 : 한양대학교 수학과 졸업
1991년 12월 : North Carolina State University 박사
1995년 3월~현재 : 한양대학교 수학과 부교수

〈관심분야〉 수치해석

송 정 환(Jung Hwan Song) 정회원

1984년2월 : 한양대학교 수학과 졸업
1993년5월 : Rensselaer Polytechnic Institute 박사
1999년 3월~현재 : 한양대학교 수학과 조교수

〈관심분야〉 암호학, 최적론(선형계획법)

박 성 준(Sung Joon Park) 정회원

1983년 2월 :한양대학교 수학과 졸업
1996년 2월 : 성균관대학교 박사
1985년 1월~1994년 3월 : 한국전자통신연구원
1996년 4월~현재 : 한국정보보호센터 기반기술팀장

〈관심분야〉 암호학, 정보이론