$$\gcd(e, \varnothing) = 1$$

을 만족하는 $1 < e < \varnothing$에서의 random 정수를 계산한다. 마지막으로

$$ed \equiv 1 \pmod{\varnothing}$$

를 만족하는 $1 < d < \varnothing$에서의 유일한 정수 d를 구해서 (n, e)는 공개키로 하고 d는 개인키로 사용한다.

다음은 암호화 과정인데 먼저 공개키 (n, e)를 획득하고 대칭키에서의 비밀키인 permutation e를 구간 $[0, n-1]$에서의 정수 m으로 표현하고

$$c = m^e \pmod{n}$$

이 암호화된 메시지가 된다. 따라서 entity A가 암호화한 (M', c)를 entity B에게 보내게 되고 B는 자신의 개인키 d를 이용하여

$$m = c^d \pmod{n}$$

을 계산함으로써 c에 대응되는 m을 구하고 m^{-1}에 의해 M'에 대응하는 M을 구할 수 있다.

RSA 암호 시스템의 안전성은 큰 정수의 소인수분해가 어렵다는 것에 그 근거를 두고 있다. 공격자의 목적은 공개된 정보 (n, e)를 이용해서 개인키 d를 구하는 것이다. 이 문제를 RSA 문제라고 하는데 공격자가 RSA 문제를 해결할 수 있는 방법은 n을 소인수분해 해서 $\varnothing$와 d를 구하는 것이다. 일단 d가 구해지면 공격자는 암호문 c를 복호화 할 수 있다. 따라서 공개키 (n, e)로부터 비밀키 d를 구하는 문제는 n을 소인수분해 하는 문제와 계산적으로 같다는 것을 알 수 있다.

다른 방법으로 공격자가 $n = pq$와 $\varnothing$를 알고 있다면 다음의 두 방정식에 의해 쉽게 n을 소인수분해 할 수 있다. 미지수 p, q에 대해

$$n = pq, \quad \varnothing = (p-1)(q-1)$$

두 번째 식에 $q = \frac{n}{p}$을 대입함으로써 다음과 같은 미지수 p에 대한 이차방정식을 얻는다.

$$p^2 - (n - \varnothing + 1)p + n = 0$$

이 방정식의 근은 p와 q일 것이다. 따라서 공격자는 $\varnothing$를 알 수 있게 되고 그 경우 이 암호계는 깨지게 된다. 하지만 $\varnothing$를 안다는 것은 n을 소인수분해 하는 문제와 같으므로 이 작업 또한 쉽지가 않다.

3. 지수분포하에서의 베이즈 추정치

응용수학과 김 지 환
지도교수 박 춘 일

This thesis is to compare and analyze the error among the Bayes estimators, GMLE of the

state availability A, true value of A, based on Sinha and Guttman's proposal of the Bayes estimaors of the parameters and reliability under the squared-error loss function and the general classes of the noninformative prior distribution for the one-parameter exponertial distribution(1976). Also we compare and analyze the error on Trader's discussion of the Bayes estimators of the parameters and reliability under the squared-error loss function and truncated normal distribution as a conjugate prior distribution(1985).

We will obiatin the Bayes estimators and the GMLE of A under noninformative and conjugate prior distribution ; 1) when failure times X and repair times Y follow exponential distribution, 2) when failure times X and repair times Y follow exponential distribution and gamma distribution respectively.

4. 신뢰도 최적화 문제에 대한 Web-site Solver의 개발에 관한 연구

(A study on the Development of Web-site Solver for solving the Reliability Redundancy Optimization problems)

응용수학과 원 해 연
지도교수 김 재 환

본 논문에서는 인터넷의 폭발적인 성장에 부응하여 아직까지 개발이 안된 신뢰도 중복설계의 최적해를 구하기 위한 Web-site solver를 개발하였다. 본 논문에서 개발한 solver는 사용자 인증, 시스템 선택, 자료입력, 입력한 자료의 확인 등의 4단계의 모든 자료입력과정이 Web-site 상에서 이루어진다. 본 논문의 solver에서는 직렬 시스템, 병렬 시스템, 콤플렉스 시스템의 신뢰도 중복설계 문제를 다루었으며, 인터넷을 통해 자료가 입력된 후에는, 본 논문에서 개발한 효율적인 발견적 합성 알고리듬(Hybrid-Heuristic Algorithm)에 의해 신뢰도 최적해가 구해진다.

본 논문에서는 신뢰도의 최적해를 구하기 위해 지역 최적해(local optimum)에 도달하는 위험성을 줄이기 위한 발견적 합성알고리듬을 개발하였다. 이 알고리듬은 유전자 알고리듬과 재 최적화과정(reoptimization procedure)인 변형된 SA로 구성된다.

유전자 알고리듬은 자연계에 있는 생물의 진화과정에서 개체군(population) 중에서 환경에 대한 적합도(fitness)가 높은 개체가 높은 확률로 살아남아 재생(reproduction)할 수 있게 되며, 이때 교배(crossover) 및 돌연변이(mutation)로서 다음 세대(generation)의 개체군을 형성하게 된는데, 이와 같은 생물의 진화과정을 인공적으로 모델링한 알고리듬이다. SA 알고리듬은 Metropolis에 의해 처음으로 고안되었으며, Kirkpatrick등이 최적화 문제를 해결하기 위해 SA 알고리듬을 적용하였다. 특히, Cerny는 TSP(Travelling Salesman Problem) 문제에 대한 SA 알고리듬을 개발하였다. 본 논문에서는 유전자 알고리듬에 의해 구해진 해를 개선시키기 위해 변형된 SA 알고리듬을 고안하여 재 최적화 과정(reoptimization procedure)으로 사용하였다.