# KAIST Grand Challenge 30 Project 제안서

<table>
<tr><td rowspan="2">①연구제목</td><td colspan="2">국문</td><td colspan="4">복잡도와 공개열쇠 암호</td></tr>
<tr><td colspan="2">영문</td><td colspan="4">complexity and public key cryptography</td></tr>
<tr><td rowspan="5">②제안자</td><td rowspan="2">성명</td><td>국문</td><td>한상근</td><td rowspan="2">소속<br>학부/학과</td><td rowspan="2">수리과학</td></tr>
<tr><td>영문</td><td>Han, Sang Geun</td></tr>
<tr><td colspan="2">주요<br>연구분야</td><td colspan="3">암호, 정수론</td></tr>
<tr><td colspan="5">연구 impact 내용 서술</td></tr>
<tr><td colspan="5">a. 양자컴퓨터의 존재 가능성 여부를 복잡도 BQP class로 검증한다<br>b. 서로 다른 공개열쇠 암호들의 상대적 안전성을 경험치가 아닌 수학적으로 비교할 수 있도록 한다.</td></tr>
</table>

③제안내용

다음 장에 있습니다.

제안자 : 한상근 (인)

③제안내용

(1) 연구주제에 대한 개요, 일반적인 해결방안 등을 소개하는 세계적 연구현황, 본인의 독창적 해결법을 소개하는 연구방법을 제시
(2) 연구의 성격이 공고문의 신청자격에서 명시된 내용에 해당하는 이유를 명시
(3) 연구의 필요성, 기대효과 등은 필요 없음.
(4) 고등학생도 이해할 수 있는 평이한 언어로 2-3쪽 정도 작성

a. P vs NP 문제의 접근 방향을 세분화한다
b. 양자컴퓨터의 존재 가능성 여부를 복잡도 BQP class로 검증한다
c. 서로 다른 공개열쇠 암호들의 상대적 안전성을 경험치가 아닌 수학적으로 비교할 수 있도록 한다.

a. 복잡도 이론에서 P class가 NP class와 같은지 다른지 여부는 잘 알려진 문제이다. 이들 중 가장 어려운 NP-complete 문제는 자연수들 $a_1, a_2, \dots, a_n$과 자연수 $x$가 주어졌을 때 일부를 사용하여 $x$를

$$a_{i_1} + a_{i_2} + \dots + a_{i_s} = x \text{ 라고}$$

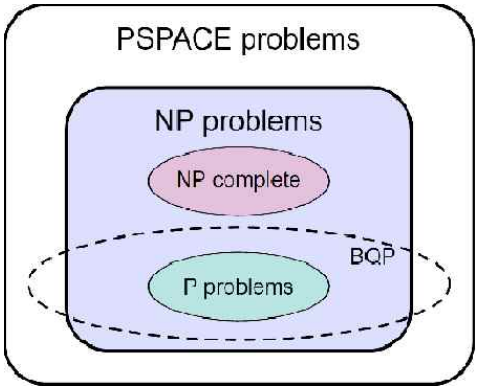
나타낼 수 있는가 하는 것이다. $n$개의 숫자가 있으므로 나타내는 방법 전체를 모두 찾아보면 문제를 해결할 수는 있는데, 경우의 수는 $2^n$개 까지 존재할 수 있으며, 이는 $n$의 지수함수이다.

P = NP이면 이 문제를 $n$의 다항식 번의 연산으로 풀어낼 수 있다는 의미이고, P $\neq$ NP이면 $n$의 다항식 번의 연산으로는 해결이 불가능하다는 의미이다.

사실 이 상태로는 문제가 너무 단순해서 단 하나의 매개변수 $n$이 나타나고 있는데, 새로운 매개변수 $t$를 추가로 도입해서 $a_i \leq t$인 문제들만 살펴보면 고정된 $t$에 대해서는 $nt$개의 숫자들을 뒤져보면 문제를 해결할 수 있다. 따라서 $t = n^{15}$라고 놓아도 $n^{16}$번의 다항식 번 연산으로 해결된다. 이 문제를 암호에 사용하려면 $t$가 $n$의 지수함수가 되어야 한다는 의미다. 이 연구주제에서는 NP-complete 문제에 $t$ 역할을 하는 새로운 매개변수들을 $(n, t)$ 등으로 하나 이상 추가하여 P vs NP 문제의 세분화된 분류구조를 살펴보는 것이다.

b. 최근 나타나는 양자 컴퓨터의 존재 가능성은, 양자 컴퓨터가 다항식 번의 연산에 해결하는 BQP class가 기존 P class와 다르다는 것과 동치인데, 만일 양자 컴퓨터가 존재한다면 전산이론의 Church-Turing 가설을 고쳐야하기 때문이다.

공개열쇠 암호인 소인수분해 문제는 Shor 알고리듬에 의해 BQP에 속하고, P에는 속하지 않는다고 여겨진다. 만일 양자 컴퓨터의 존재가설 BQP $\neq$ P이 옳지 않다면, BQP = P가 되어서 양자 컴퓨터가 할 수 있는 모든 작업은 기존 컴퓨터로도 수행할 수 있다는 것이며 사실은 양자 컴퓨터가 존재하지 않는다는 결론을 도출한다. 표준 가설을 가정하면 이들 사이의 포함관계는 다음과 같다.




NP-complete 문제처럼 BQP-complete 문제도 존재하는데 아직은 순수 수학적 개념으로만 표현된 BQP-complete 문제가 없다고 할 수 있다. 이 연구주제에서는 그래프나 행렬 등 여타 순수 수학적 개념으로만 표현된 BQP-complete 문제를 찾고, 거기에 새로운 매개변수 $t$ 역할을 매개변수들을 하나 이상 추가하여 P vs BQP 문제의 세분화된 분류구조를 살펴보는 것이다.

c. 모든 암호는 NP-complete 문제로 변환하는 것이 가능하다는 것은 잘 알려진 사실이다. 소인수분해 문제 등 공개열쇠 암호의 안전성은, 해독에 필요한 계산량에 대해 경험상 결과는 $2^{128}$ 번의 연산으로 해독 가능하다 등의 형태로 알려져 있지만, 이론적 결과는 거의 없다. 더구나 서로 다른 형태의 암호를 비교하는 유일한 방법은 현재로서는 경험상 계산량 하나뿐이다. 이 연구주제에서는 모든 공개열쇠 암호를 하나의 NP-complete 문제 또는 하나의 BQP-complete 문제

$$a_{i_1} + a_{i_2} + \ldots + a_{i_s} = x$$로 변환하여,

예를 들면 암호 시스템 A는 매개변수 NP-complete 문제에서 $(n,t) = (256, 10^{200})$인데 시스템 B는 $(n,t) = (237, 10^{195})$로 변환되므로 시스템 A가 B보다 더 안전하다는 형태의 이론적 판단기준을 제공하려 한다.

이 연구주제가 해당되는 항목은 다음과 같다.

1) 글로벌 난제
   양자 컴퓨터의 존재 가능성에 대한 복잡도 이론의 질문
2) 기초과학 분야에서 가장 근본적인 질문
   기존 컴퓨터의 Church-Turing 가설이 옳은지에 대한 질문
4) 외부에서 연구비를 받기 어려우나 학문 특성상 꼭 필요한 주제
   세계적으로 양자 컴퓨터의 제작연구에만 집중 투자하고 있음
5) 현재 핫 이슈가 아닌 주제
   세계적으로 양자 컴퓨터의 제작연구에만 집중 투자하고 있음
6) 10년 이내 상업화가 불가능한 주제
   공개열쇠 암호들의 상대적 안전성을 수학적으로 비교

# Proposal for KAIST Grand Challenge 30 Project

<table>
<tr><td rowspan="2">1. Title</td><td colspan="2">Korean</td><td colspan="3">복잡도와 공개열쇠 암호</td></tr>
<tr><td colspan="2">English</td><td colspan="3">complexity and public key cryptography</td></tr>
<tr><td rowspan="5">2. Principal Investigator(PI)</td><td rowspan="2">Name</td><td>Korean</td><td>한상근</td><td rowspan="2">Department</td><td rowspan="2">mathematical sciences</td></tr>
<tr><td>English</td><td>Han, Sang Geun</td></tr>
<tr><td colspan="2">Major Research Field</td><td colspan="3">cryptography, number theory</td></tr>
<tr><td colspan="5">Impact of research project</td></tr>
<tr><td colspan="5">a. Conjectures in quantum complexity theory and BQP class for the existence of quantum computer<br>b. Reduce all public key cryptosystem into a same NP complete problem for theoretical comparison</td></tr>
<tr><td>3. Project Summary</td><td colspan="5">In the next page.</td></tr>
<tr><td colspan="6">a. Provide the global research trends concerning the proposed research theme including an overview and general solutions.<br>b. Specify how the nature of the proposed research satisfy the requirements of eligibility(b).<br>c. No need to write research necessity and expected outcome.<br>d. Write in plain language within 2~3 pages.</td></tr>
</table>

Applicant : Han, Sang Geun (signature)

## 3. Project Summary

a. Provide the global research trends concerning the proposed research theme including an overview and general solutions.
b. Specify how the nature of the proposed research satisfy the requirements of eligibility(b).
c. No need to write research necessity and expected outcome.
d. Write in plain language within 2~3 pages.

a. Multi-dimensional parameterized P vs NP problem

b. Conjectures in quantum complexity theory and BQP class for the existence of quantum computer

c. Reduce all public key cryptosystem into a same NP-complete problem for theoretical comparison

a. In complexity theory, the question "P class = NP class ?" is very well known. Among those the most difficult NP-complete problem is this : Given natural numbers $a_1, a_2, \ldots, a_n$ and a target $x$, find an expression for $x$ as

$$a_{i_1} + a_{i_2} + \ldots + a_{i_s} = x.$$

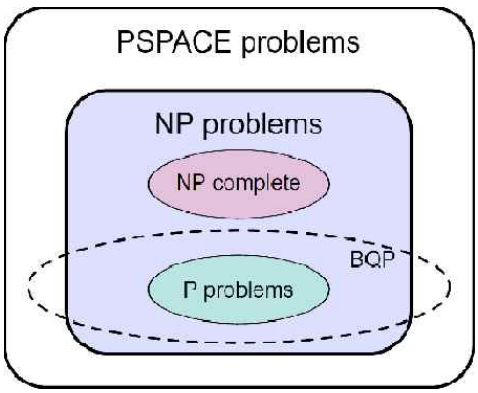
Since we are given $n$ numbers, we may search for all possible combinations and find a solution, if it exists, by trying all $2^n$ summations which is an exponential function of $n$.

The answer P = NP means that we can solve this problem with basic operations within a polynomial time of $n$, and the answer P $\neq$ NP means that it is not possible within a polynomial time of $n$.

In fact this description of NP-complete problem is so simple that only one parameter $n$ appears in the problem. If we introduce another parameter $t$ and look for only those problems with $a_i \leq t$, then we see that for a fixed $t$, considering only possible $nt$ numbers is enough. Even when $t = n^{15}$ only considering numbers $n^{16}$ times is enough. To use this NP-complete problem for cryptography $t$ has to be an exponential function of $n$. In this project the applicant will introduce at least one extra parameters $(n, t)$ to NP-complete problem and study the fine structures of P vs NP problem.

b. Recently proposed quantum computer implies that the BQP class, problems which can be solvable within a polynomial time using quantum computer, is different from P class those problems solvable within a polynomial time using current computer. Hence the conjecture BQP $\neq$ P means that quantum computer exists and BQP = P means that quantum computer does not exist and furthermore we have to modify the Church-Turing thesis of theoretical computer science.

Integer factorization problem used in RSA public key cryptosystem is broken by Shor's algorithm and hence belong to BQP class. Researchers assume that it does not belong to P class. If BQP = P, the RSA cryptosystem will be broken by current computer and current computer can simulate the quantum computer. Inclusion relations diagram among the complexity classes are as follows under standard conjectures.




As the most difficult NP problem exists as NP-complete problem, the most difficult BQP problem exists and is called as BQP-complete problem. However BQP-complete problem can not be described only in terms of pure mathematics like a graph problem or a linear algebra problem. Still one needs a concept of quantum physics. In this project, the applicant will search for a description of BQP-complete problem in terms of graph theory or a linear algebra and try to add new parameters to see the fine structures of P vs BQP problem.

c. It we well known that any cryptosystem can be transformed into NP-complete problem. However all we know today about the security of cryptosystem is described as like "one needs $2^{128}$ basic operations to break this system" with no theoretical results. Moreover the only way to compare two cryptosystems of different type is empirical running time. In this project, the applicant will transform all public key cryptosystem into one NP-complete problem or one BQP-complete problem

$$a_{i_1} + a_{i_2} + \ldots + a_{i_s} = x.$$

If successful, for example a cryptosystem A can be represented as a parameter NP-complete problem $(n,t) = (256, 10^{200})$ while another cryptosystem B is represented as a parameter NP-complete problem $(n,t) = (237, 10^{195})$ and it will imply that system A is secure than system B.

This project meets the KG challenge 30 standards as follows.

- Global challenges

  Question about the existence of quantum computer in terms of complexity theory conjecture

- The most fundamental questions in basic sciences

  Question whether current Church-Turing thesis has to be changed

- Topics for which getting outside funding is difficult

  World is heavily investing in trying to build quantum computer without knowing the existence of quantum computer

- Topics which are not currently counted among the hot ones

  World is heavily investing in trying to build quantum computer without knowing the existence of quantum computer

- Topics of which commercialization is out of reach within the next 10 years

  Compare the relative safety of public key cryptosystems with mathematical theory