2024年度大学院博士前期課程入学試験

大阪大学大学院工学研究科
電気電子情報通信工学専攻

専門科目試験問題
（情報通信工学コース）

（実施時間　１４：００ ～ １６：００）

【注　意　事　項】

１．問題用紙はこの表紙や白紙を除いて１３ページある．解答開始の指示があるまで開いてはいけない．解答開始後，落丁や不鮮明な箇所等があった場合は，手を挙げて監督者にその旨を伝えること．

２．試験問題は，「通信ネットワーク」，「情報理論」，「信号処理」，「論理回路と計算機システム」，「データ構造とアルゴリズム」，及び，「情報セキュリティ」の全部で６題あり，この順番に綴じられている．このうち，３題を選択し解答すること．

３．解答開始前に，別紙の「専門科目試験問題選択票」に記載の注意事項も読んでおくこと．

４．問題用紙は持ち帰ってもよい．

【通信ネットワーク】 解答は，黄色の解答用紙に記入すること．

1 台の基地局に N 台 $(N = 1,2,\dots)$ の無線端末が接続するスター型トポロジのネットワークを，M/M/1 待ち行列としてモデル化し解析することを考える．各端末はそれぞれ率 λ $(\lambda > 0)$ のポワソン過程に従って独立にパケットを生成し，自身の容量無限大のバッファに格納する．基地局は一度に 1 台の端末からのみパケットを受信でき，上記の N 台の端末バッファに格納されているパケットが伝送元端末を問わず生成時刻の早い順に一つずつ基地局へ伝送されるように送信権制御を行うとする．また，各パケットは基地局での受信が完了した時点において端末バッファから削除されるとする．一つのパケットの伝送開始から受信完了までに要する時間は，平均 $1/\mu$ $(\mu > N\lambda)$ の指数分布に従って独立かつ同一に分布すると仮定する．

このとき，以下の問いに答えよ．

(i) システム全体でのパケット生成間隔は平均 $1/(N\lambda)$ の指数分布に従う．この理由を説明せよ．

(ii) 時刻 t において i 番目 $(i = 1,2,\dots,N)$ の端末のバッファに格納されており，かつ伝送中でないパケットの数を $L_i(t)$ とする．また，時刻 t において伝送中であるパケットの数を $S(t)$ とし，システム内のパケット総数を $L(t) = S(t) + \sum_{i=1}^{N} L_i(t)$ と定義する．さらに，$L(t) = k$ である確率を $p_k(t)$ とする．$p_k(t)$ の t に関する導関数 $p_k'(t)$ を N，λ，μ，$p_{k-1}(t)$，$p_k(t)$，$p_{k+1}(t)$ のうち必要なものを用いて表せ．

(iii) 極限確率 p_k を，$p_k = \lim_{t\to\infty} p_k(t)$ と定義する．N, λ, μ のうち必要なものを用いて p_k を表せ．ただし，$\lim_{t\to\infty} p_k'(t) = 0$ $(k = 0,1,2\dots)$ を用いてもよい．

(iv) このシステムの定常状態における平均遅延時間を D とする．ただし，平均遅延時間とは，パケットが生成されてから基地局で受信完了となるまでの時間の平均である．N, λ, μ のうち必要なものを用いて D を表せ．

(v) 端末数 N に応じて伝送速度を $\mu = N\alpha$ となるように変化させることを考える．ただし α は，$\alpha > \lambda$ を満たす定数である．定常状態における平均遅延時間 D の $N \to \infty$ における極限値を求めよ．

(vi) 前問 (v) の状況を一般化し，端末数 N の関数 $f(N)$ $(N = 1,2,\dots)$ を用いて，端末数 N に応じた伝送速度 $\mu = f(N)$ を定めることを考える．次の三つの条件を全て満たす関数 $f(N)$ の例を挙げよ．

条件 1： $f(N) > N\lambda$ $(N = 1,2,\dots)$

条件 2： $\lim_{N\to\infty} \frac{N\lambda}{f(N)} = 1$

条件 3： $N \to \infty$ のとき $D \to 0$

専門用語の英訳

スター型トポロジ	: star topology
待ち行列	: queue
率	: rate
ポワソン過程	: Poisson process
送信権制御	: transmission order control
指数分布	: exponential distribution
独立かつ同一に分布	: independent and identically distributed
導関数	: derivative
極限確率	: limiting probability
定常状態	: steady state
平均遅延時間	: mean delay
極限値	: limiting value

【情報理論】 解答は，桃色の解答用紙に記入すること．

標本空間 $\{0,1\}$ の要素をとる 2 つの確率変数 X と Y を考える．その X と Y の同時確率を表 1 に示す．以下の問いに答えよ．解答にあたっては，導出過程も示すこと．なお，エントロピーおよび相互情報量の単位はビットとせよ．

表 1

Y \ X	0	1
0	1/8	3/8
1	3/8	1/8

(i) X, Y のエントロピー $H(X)$, $H(Y)$ を求めよ．

(ii) Y で条件をつけた X の条件付きエントロピー $H(X \mid Y)$，および X で条件をつけた Y の条件付きエントロピー $H(Y \mid X)$ を求めよ．

(iii) X と Y の相互情報量 $I(X; Y)$ を求めよ．

次に，X と Y の積を W と定義する．さらに，標本空間 $\{0,1\}$ の要素を等確率でとる確率変数を K とし，W と K の和を 2 で割った余りを確率変数 Z と定義する．ここで，W と K は独立である．

(iv) W, Z のエントロピー $H(W)$, $H(Z)$ を求めよ．

(v) X, Y, W の同時エントロピー $H(X, Y, W)$，および X, Y, Z の同時エントロピー $H(X, Y, Z)$を求めよ．だたし，同時エントロピーは結合エントロピーとも呼ばれる．

(vi) Z で条件をつけた X の条件付きエントロピー $H(X \mid Z)$，Y, Z で条件をつけた X の条件付きエントロピー $H(X \mid Y, Z)$，X, Y で条件をつけた Z の条件付きエントロピー $H(Z \mid X, Y)$ を求めよ．

(vii) X と Z の相互情報量 $I(X; Z)$，および Z で条件をつけた場合の X と Y の相互情報量 $I(X; Y \mid Z)$ を求めよ．

専門用語の英訳

確率変数	random variable
エントロピー	entropy
条件付きエントロピー	conditional entropy
同時エントロピー	joint entropy
相互情報量	mutual information

【信号処理】 解答は，だいだい色の解答用紙に記入すること．

1. 離散時間信号処理システム L （以降，システムと呼ぶ）は，離散時間入力信号 $x[n]$ を処理し，離散時間出力信号 $y[n] = L[x[n]]$ を生成するシステムである．以下の問いに答えよ．なお，n は時刻を表す整数である．

(i) 離散時間入力信号を $ax_1[n] + bx_2[n]$ とする（aとbは定数）．システムにおける線形性の定義を離散時間出力信号 $y[n] = L[ax_1[n] + bx_2[n]]$ を用いて述べよ．また，下記に示すシステム (a)～(f) のうち，線形性を満たすものを全て選択せよ．

(ii) システムにおける時不変性の定義を離散時間出力信号 $y[n] = L[x[n]]$ を用いて述べよ．また，下記に示すシステム (a)～(f) のうち，時不変性を満たすものを全て選択せよ．

(iii) システムにおける因果性の定義を述べよ．また，下記に示すシステム (a)～(f) のうち，因果性を満たすものを全て選択せよ．

(iv) システムにおける BIBO（Bounded Input Bounded Output）安定の定義を述べよ．また，下記に示すシステム (a)～(f) のうち，BIBO 安定であるものを全て選択せよ．

(v) システムが，線形性と時不変性を満たし，記憶性を満たさないとき，離散時間入力信号 $x[n]$ と離散時間出力信号 $y[n]$ の関係を述べよ．

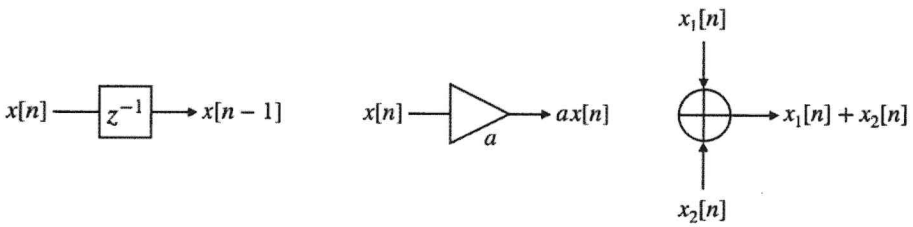
(a) $y[n] = x[5n]$	(b) $y[n] = \sum_{k=-\infty}^{\infty} x[k]$	(c) $y[n] = \sum_{k=-\infty}^{n} 2^{k-n}x[k]$
(d) $y[n] = n^2x[n]$	(e) $y[n] = (x[n])^2$	(f) $y[n] = x[n] + 1$

2. 入出力差分方程式

$$y[n] - ay[n-1] = bx[n] - cx[n-1]$$

で表される離散時間信号処理システムLについて，以下の問いに答えよ．なお，nは時刻を表す整数である．

(i) システムLの回路構成を下図に示す素子を使って図示せよ．素子は左から，1 タイムスロット遅延，定数倍，加算を表す．信号の方向を表す矢印を明示すること．



(ii) このシステムのz領域伝達関数$H(z)$を求めよ．

(iii) $a = 0, b = \frac{1}{2}, c = -\frac{1}{2}$のとき，このシステムの$0 \le \Omega \le \pi$における周波数応答は

$$Ae^{-j\frac{\Omega}{2}}$$

で表される．なお，jは虚数単位（$j^2 = -1$），Ωは正規化角周波数を表す．振幅特性Aを求めよ．

専門用語の英訳	
入出力差分方程式	input-output difference equation
離散時間信号処理システム	discrete-time signal processing system
z変換	z transform
伝達関数	transfer function
線形	linear
時不変	time-invariant
振幅特性	amplitude response
因果性	causality
安定性	stability
記憶	memory

【論理回路と計算機システム】 解答は，水色の解答用紙に記入すること．

A 君が 3 ビット桁上げ先見加算器を論理回路シミュレータで実装している．しかし，実装した回路が正しく動作しておらず，A 君は困っている．友人のあなたは，A 君が実装した論理回路を正しく動作させたいと考えている．

まず，一般的な桁上げ先見加算器の原理を考える．一般的に加算器は，n ビットの 2 進数 $X=(x_n,\dots,x_2,x_1)$ と $Y=(y_n,\dots,y_2,y_1)$ を加算し，n ビットの 2 進数 $S=(s_n,\dots,s_2,s_1)$ を出力する．ここで $x_i,y_i,s_i\ (i=1,\dots,n)$ は 0 また 1 の値を取る 2 値変数であり，2 進数表現においては添え字 i の値が小さい方を下位桁とする．この時，以下の問いに答えよ．なお，以降，論理式においては，2 値変数 x,y に関する論理積を xy，論理和を $x+y$，排他的論理和を $x\oplus y$ で表すものとする．

(i) 通常，加算器では，第 i 桁目の和出力 s_i と桁上げ信号 c_i を次の 2 つの式に基づいて計算する．

$$s_i=x_i\oplus y_i\oplus c_{i-1}=p_i\oplus c_{i-1}$$
$$c_i=x_iy_i+(x_i\oplus y_i)c_{i-1}=g_i+p_ic_{i-1}\qquad(1)$$

ここで $p_i=x_i\oplus y_i$，$g_i=x_iy_i$ である．この時，第 i 桁目の 2 変数 s_i,c_i に関する真理値表を x_i,y_i,c_{i-1} を用いてそれぞれ書け．

(ii) 桁上げ先見加算器では，c_i を式(1)の漸化式を展開して計算する．この時，$i=1,2,3$ における各 c_i の論理式を，$p_i,g_i\ (i=1,2,3)$ と c_0 を用いた積和形で表せ．ただし，冗長な項を新たに加えてはいけない．

(iii) 桁上げ信号 c_3 の論理式を c_0 と $P_1=p_3p_2p_1$，$G_1=g_3+p_3g_2+p_3p_2g_1$ を用いた積和形で表せ．

次に，A 君が実装した図 1 の回路を修正することを考える．図中の IN_1 や OUT_1 は各ユニットの入力・出力端子のラベル，U_1 などは論理素子のラベルである．p_i,g_i を計算する PG 生成ユニット，s_i を計算する ADD ユニット，p_i,g_i から c_i を計算する CLA コアユニットのうち，PG 生成ユニットと ADD ユニットに誤りがないことは確認済みである．この時，以下の問いに答えよ．

(iv) A 君が実装した桁上げ先見加算器に，$X=(1,1,1),Y=(0,0,0)$ を入力した場合の出力値 $S=(s_3,s_2,s_1)$ と c_3 の値を示せ．また，2 進数の加算として正しい結果か否かもあわせて答えよ．$c_0=0$ とする．

(v) 問い(ii)と(iii)で得た展開式に従って，図 1 の CLA コアユニットを修正したい．次の例に示すような入力端子ラベルと論理素子ラベルを用いた説明文によって，修正すべき 2 箇所を答えよ．ただし，各論理素子の入力ノード数の変更（2 入力/3 入力）は可能であるが，新たな論理素子を追加してはいけない．

例 1「U_2 への入力を，IN_1 から IN_2 へ接続しなおす」（これで 1 箇所）
例 2「U_1 と IN_3 を新たに接続する」（これで 1 箇所）

最後に，修正された上記 3 ビット CLA コアユニットを用いて，9 ビットの 2 進数入力へ対応可能な 9 ビット CLA コアユニットを実装することを考える．$p_i,g_i\ (i=1,\dots,9),c_0$ と CLA コアユニット 4 つを図 2 のように配置し，各ユニットを木構造状に接続すれば，9 ビット CLA コアユニットを構成できる．この時，以下の問いに答えよ．

(vi) 桁上げ信号 c_6 の論理式を $P_j = p_{3j}p_{3j-1}p_{3j-2}$, $G_j = g_{3j} + p_{3j}g_{3j-1} + p_{3j}p_{3j-1}g_{3j-2}$ $(j = 1, 2)$ と c_0 を用いた積和形で表せ．P_1, G_1 と P_2, G_2 はそれぞれ，CLA コアユニット 1 および 2 から出力される値である．

(vii) CLA コアユニット 2, 3 および 4 における入力端子 IN_0 に接続すべき出力端子もしくは入力値をそれぞれ答えよ．ただし，出力端子を接続する場合は「CLA コアユニット 1 の OUT_1」のように指定せよ．また，値を入力する場合は p_i, g_i $(i = 1, \ldots, 9)$, c_0 から 1 つ選んで指定せよ．CLA コアユニット 4 を活用するとよい．

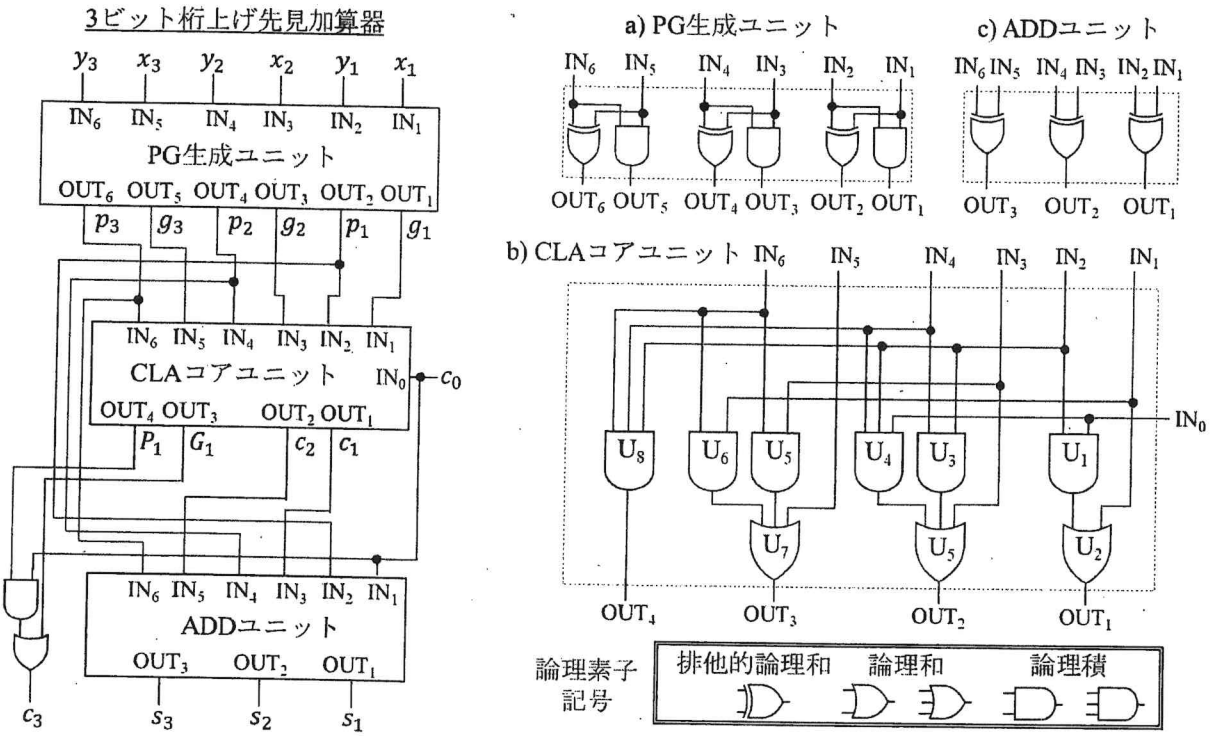
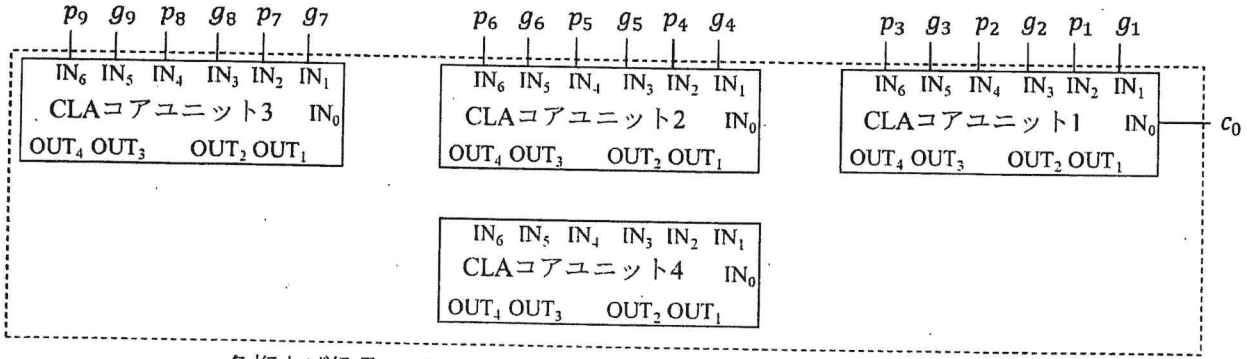


図 1　A 君が実装した 3 ビット桁上げ先見加算器



各桁上げ信号 c_i $(i = 1, \ldots, 8)$ はいずれかの出力端子の値と対応付けられる

図 2　9 ビット CLA コアユニットの構成の一部

専門用語の英訳

桁上げ先見加算器	carry look-ahead adder (CLA)
加算器	adder
排他的論理和	exclusive OR
真理値表	truth value table
漸化式	recurrence formula / recurrence relation
論理式	logical formula, logical expression
積和形	sum-of-products form

【データ構造とアルゴリズム】　解答は，青色の解答用紙に記入すること．

1. キューとは入力されたデータを順番に格納し，先に格納したデータから順番に取り出すことができる先入れ先出し型のデータ構造である．キューの実装方法の一つにリングバッファを用いる方法がある．リングバッファの末尾にデータを追加する操作を push_back，リングバッファの先頭のデータを削除する操作を pop_front と呼ぶこととする．以下の問い (i), (ii) に答えよ．

   (i) 図 1 はリングバッファとして十分に大きな長さ N の配列を用いたキューの C 言語による実装である．[A], [B], [C] を埋めて実装を完成させよ．ただし queue の front, back はリングバッファの先頭および末尾を示す変数である．

   (ii) 図 1 の実行結果を示せ．

   両端キューはキューを拡張したデータ構造であり，リングバッファを用いて実装できる．両端キューは push_back と pop_front に加えて，リングバッファの先頭にデータを追加する操作 push_front，リングバッファの末尾のデータを削除する操作 pop_back を備えている．以下の問い (iii), (iv) に答えよ．

   (iii) 図 1 に push_front を追加する．push_front の実装を述べよ．

   (iv) 図 1 に pop_back を追加する．pop_back の実装を述べよ．

図 1. リングバッファを用いたキューの実装（C 言語）

```
#include <stdio.h>
#include <stdlib.h>
#define N 100

typedef struct queue {
    int front, back;
    int buffer[N];
}queue;

void push_back(queue* Q, int x){
    Q->buffer[Q->back] = [ A ];
    Q->back = [ B ];
    return;
}

void pop_front(queue* Q){
    Q->front = [ C ];
    return;
}

int main(void){
    queue* Q = malloc(sizeof(queue));
    Q->front = 0;
    Q->back = 0;
    push_back(Q, 2);
    push_back(Q, 3);
    push_back(Q, 5);
    printf("%d\n", Q->buffer[Q->front]);
    pop_front(Q);
    printf("%d\n", Q->buffer[Q->front]);
    pop_front(Q);
    return 0;
}
```

2. n 個の相異なる整数が，図 2 に示されるように全体として左から右に向かって整数値の昇順に長さ n の配列 D に格納されている．配列は m 個のブロックに分割されており，各ブロックは左から順番に $i = 1, \ldots, m$ の番号を有し，ブロック i は nr_i 個の要素を持つ．ここで各 r_i は $0 < r_i < 1$ でかつ nr_i が整数となるものであるとし，さらに $\sum_{i=1}^{m} r_i = 1$ を満たす．各ブロック i 内の要素は右端から左に向かって $j = 1, \ldots, nr_i$ の番号を有し，ブロック i の j 番目の要素の整数を $x_{i,j}$ と表す．ここで D から一様ランダムに整数 x を選び，この配列において $x_{i,j} = x$ となる要素番号 i, j を以下の手順により探索する．

   Step 1: $i = 1$ から始めて左から右に向かって逐次各ブロック i の右端の要素の $x_{i,1}$ と x について比較 $x_{i,1} < x$ を行い，この不等式を満たさない最小の番号 i を有するブロック i を探索する．

   Step 2: Step 1 で探索したブロック i 内で $x_{i,j} = x$ となる要素が見つかるまで，右端の要素の $x_{i,1}$ から左に向かって各要素の $x_{i,j}$ と x の比較を繰り返す．

   以下の問いに答えよ．

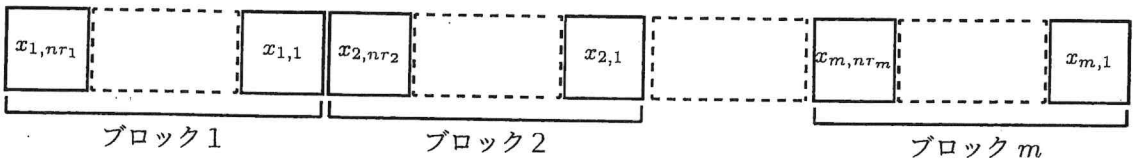


図 2. n 個の相異なる整数を全体として左から右に向かって昇順に格納した配列。
配列は m 個のブロックに分割されている。

(i) ブロック i に $x_{i,j} = x$ となる要素が含まれる確率 $P(i)$ を答えよ．さらに $i = 1, \ldots, m$ に亘る Step 1 における $x_{i,1} < x$ の比較回数の期待値を答えよ．

(ii) ブロック i に x と等しい要素が含まれる場合において，$x_{i,j}$ が $x_{i,j} = x$ となる条件付き確率 $P(j \mid i)$ を答えよ．同じくブロック i に x と等しい要素が含まれる場合において，$j = 1, \ldots, nr_i$ に亘る Step 2 における $x_{i,j} = x$ の比較回数の期待値を答えよ．

(iii) 任意のブロック i に含まれる $x_{i,j}$ が $x_{i,j} = x$ となる確率 $P(i,j)$ を答えよ．さらに D に含まれることが判っている任意の x について，Step 1 と Step 2 により $x_{i,j} = x$ となる要素番号 i, j を探索するのに必要な総比較回数の期待値を答えよ．

(iv) 問い (iii) で求めた総比較回数の期待値を最小化する r_i $(i = 1, \ldots, m)$ を求めよ．ただし，必ずしも nr_i が整数となるものに限らず各 r_i を任意の実数として扱い，かつ総比較回数の期待値は各 r_i で微分可能として良い．

(v) 問い (iv) の答えが示す総比較回数の期待値を最小化する r_i $(i = 1, \ldots, m)$ の性質を，Step 1 と Step 2 の処理内容に基づいて論述せよ．

専門用語の英訳

キュー	queue
先入れ先出し	First-In First-Out
リングバッファ	ring buffer
両端キュー	double-ended queue
整数	integer
昇順	ascending order
配列	array
格納	storing
分割	partition
要素	element
探索	search
逐次	Sequentially
右端	right end
期待値	expected value
総比較回数	total number of comparisons

【情報セキュリティ】 解答は，緑色の解答用紙に記入すること．

有限体の乗法群 $\mathbb{Z}_p^*$ 上の ElGamal 公開鍵暗号化方式は以下のように定義される．p を素数とし，有限体 $\mathbb{Z}_p = \{0,1,\ldots,p-1\}$ とその乗法群は $\mathbb{Z}_p^* = \{1,2,\ldots,p-1\}$, $g \in \mathbb{Z}_p^*$ は位数が素数 q の元とする．ここで，g をベースポイントと呼び，$g^\ell = 1 \pmod p$ となる最小の正整数 ℓ を g の位数という．なお，$g^\ell = 1 \pmod p$ は $g^\ell - 1$ が p で割り切れることを意味する．ElGamal 公開鍵暗号化方式における鍵生成では，秘密鍵 x を $\mathbb{Z}_q$ の乗法群 $\mathbb{Z}_q^*$ から一様ランダムに選択し，公開鍵を $y = g^x \pmod p$ とする．ElGamal 公開鍵暗号化方式の暗号化関数を Enc と表すと，平文 $m \in \mathbb{Z}_p^*$ の暗号文は，$\mathbb{Z}_q^*$ から一様ランダムに選択した r を用いて，$\mathrm{Enc}(m) = (g^r \pmod p, my^r \pmod p)$ で与えられる．一方，ElGamal 公開鍵暗号化方式の復号関数を Dec と表す．以下の問い (i) - (iv) に答えよ．

(i) $p = 23$ であるとき，ベースポイント $g = 2$ の位数を求めよ．

(ii) $p = 23$, ベースポイント $g = 2$，秘密鍵 $x = 5$ に対する公開鍵 $y \in \mathbb{Z}_p^*$ を求めよ．

(iii) 暗号化関数は平文空間となる群から暗号文空間となる群への写像と考えることができる．ElGamal 公開鍵暗号化方式では平文空間は群 $\mathbb{Z}_p^*$ で，暗号文空間は $\mathbb{Z}_p^*$ の直積群 $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$ となる．つまり，ElGamal 公開鍵暗号化方式の暗号化関数は群 $\mathbb{Z}_p^*$ から群 $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$ への写像 $\mathrm{Enc}(m) = (g^r \pmod p, my^r \pmod p)$ と書ける．ElGamal 公開鍵暗号化方式には準同型性があること，つまり，任意の二つの平文 $m_1, m_2 \in \mathbb{Z}_p^*$ の暗号文 $\mathrm{Enc}(m_1), \mathrm{Enc}(m_2)$ を用いて，$m_1 \cdot m_2 \in \mathbb{Z}_p^*$ の暗号文が構成できることを示せ．

(iv) 暗号文の解読では攻撃者の能力の仮定が重要になる．図 1 に示した選択暗号文攻撃では，解読対象の暗号文 c^* を入手した攻撃者は，c^* とは異なる任意の暗号文 c を復号オラクルに入力し，その復号結果 m を入手できる環境で，c^* の復号文 m^* を解読する．ここで，攻撃者が入手した暗号文が，$p = 23$, ベースポイント $g = 2$，公開鍵 $y = 9$ の ElGamal 公開鍵暗号化方式で暗号化された $c^* = (18, 9)$ であるとする．選択暗号文攻撃で $m^* = \mathrm{Dec}(c^*)$ を解読するステップに関する問い (1) - (3) に答えよ．

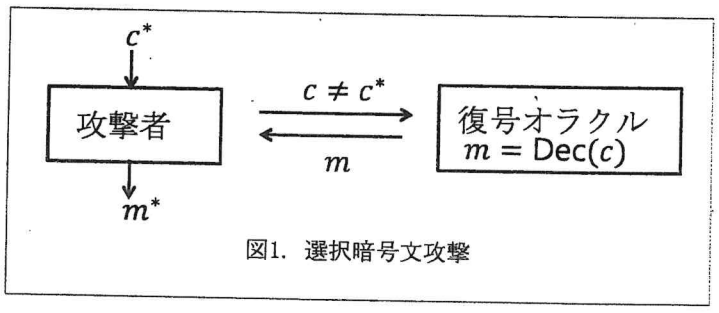


図1. 選択暗号文攻撃

(1) 復号オラクルに入力する暗号文を平文 2 の暗号文 Enc(2) として構成する．このとき，$r = 2$ とした時の Enc(2) を求めよ．

(2) 前問 Enc(2) を用いて，c =Enc(2)$\cdot c^*$ を求めよ．

(3) 前問の c について，$c \neq c^*$ であることから c を復号オラクルに入力し，Dec(c) = 6 を入手したとする．このとき，m^* を求めよ．

専門用語の英訳	
有限体	finite field
乗法群	multiplicative group
位数	order
ベースポイント	base point
公開鍵暗号化方式	public-key encryption scheme
公開鍵	public key
秘密鍵	secret key
暗号化	encryption
復号	decryption
選択暗号文攻撃	chosen ciphertext attack
復号オラクル	decryption oracle