様式Ａ－７４

ひらめき☆ときめきサイエンス～ようこそ大学の研究室へ～KAKENHI　プログラム概要

課題番号	19HT0016	分野	数学・工学	キーワード	仮想通貨，ブロックチェーン，確率

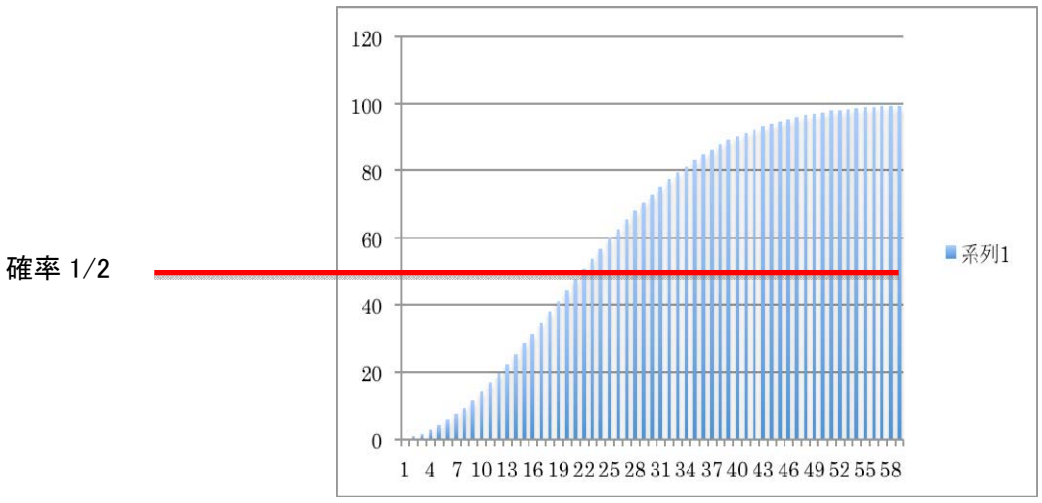
研究機関名	秋田大学				
プログラム名	仮想通貨の仕組みとブロックチェーン				
先生（代表者）	山村　明弘（やまむら　あきひろ）・理工学研究科・教授（学部長）				
自己紹介	離散数学と呼ばれる数学の中でも新しい分野で研究しています。直感と違う不思議な数式でも，少し視点を変えると理解できることがよくあります。そのような体験を通して数学の面白さに魅了されてきました。今は，応用が少ないと見られがちな数学が実社会で大活躍していることに新鮮な興味を感じています。				
開催日時・募集対象	８月９日（金）	受講対象者	高校生	募集人数	２０名
集合場所・時間	秋田大学理工学部７号館 209 教室	（集合時間）	９：００		
開催会場	秋田大学理工学部（手形キャンパス）　理工学部7号館 住所：〒010-8502　秋田県秋田市手形学園町1－1 アクセスマップ URL：https://www.akita-u.ac.jp/honbu/access/				

内　　容

「通貨」とは何でしょうか？「通貨」はどうして社会の中で受け入れられているのでしょうか？伝統的な通貨の特性を理解して，それとは異なる仮想通貨の仕組みを理解します。そこでは，数学が活躍していることがわかるでしょう。ところで，仮想通貨とは一見無関係に思える次の質問に答えられるでしょうか。

Q：教室の中に何人の生徒が集まれば，同じ誕生日の人が二人いる確率が 1/2 を超えるのでしょうか？

答えは意外な人数です。この奇妙な確率の問題は，仮想通貨の構成に必要となる暗号技術のハッシュ関数に関連しています。グループに分かれて，ハッシュ関数に関する模型を使った実験と，素因数分解問題を活用した公開鍵暗号による暗号通信の計算機実験を体験して，数学が社会で活躍する様子を覗いてみます。



スケジュール	
9:00–9:30	受付（集合場所：理工学部 7 号館 209 教室）
9:30–9:45	開講式（挨拶，オリエンテーション，科研費の説明）
9:45–10:30	講義①「素因数分解と公開鍵暗号」
10:30–10:45	休憩
10:45–11:30	実験①「RSA 暗号で暗号化してみよう」
11:30–12:00	講義②「ハッシュ関数とは？」
12:00–12:15	質疑応答
12:15–13:15	昼食，休憩（大学食堂）
13:15–14:00	講義③「仮想通貨の仕組みとブロックチェーン」
14:00–14:30	実験②「バースデーパラドックスのシミュレーション」
14:30–14:50	クッキータイム（受講生，講師，大学生の歓談）
14:50–15:35	実験③「ハッシュ関数の衝突を発見しよう」
15:35–15:50	休憩
15:50–16:20	実験結果の発表と討論
16:20–16:50	修了式（未来博士号の授与）
16:50	終了，解散

持　ち 物
筆記用具

特 記 事 項
・昼食は大学食堂を利用するか，またはご持参下さい。 ・クッキータイムで間食するので，アレルギーがある方は事前にお知らせ下さい。

《お問合せ・お申込先》

所 属・氏 名 ：	地方創生・研究推進課　総務・研究助成担当 加賀屋　聡一（かがや　そういち）
住　　所 ：	〒010-8502　秋田県秋田市手形学園町1−1
TEL 番 号 ：	018-889-3003
FAX 番 号 ：	018-889-2928
E − mail ：	gakujutu@jimu.akita-u.ac.jp

申込締切日 ：	**令和元年　7月26日（金）**

※当プログラムは先着順にて受付を行います。

《プログラムと関係する先生（実施代表者）の科研費》

研究代表者	研究期間	研究種目	課題番号	研究課題名
山村明弘	H27-29	基盤研究（C）	15K0004	非可換代数の公開鍵暗号への応用と汎用ハッシュ関数の組合せ論的構成

★この科研費について、さらに詳しく知りたい方は、下記をクリック！

http://kaken.nii.ac.jp/

※国立情報学研究所の科研費データベースへリンクします。