東北大学
TOHOKU UNIVERSITY

Press Release

2023 年 11 月 8 日

報道機関　各位

国立大学法人東北大学

# 東北大学 MOOC 講座
# 「暗号学の現在―現代暗号入門」
# 新規開講のお知らせ
## ～現代暗号の特徴、社会インフラとの関わりや
## 将来の量子計算機時代についてご紹介～

【発表のポイント】

- 東北大学オープンオンライン教育開発推進センターでは、「世界と地域に開かれた大学」「市民の知的関心を受け止め、支え、育んでいける教育研究活動を積極的に推進する大学」の実現を目指し、2016 年度よりオンライン講座、東北大学 MOOC（注１）を開講しています。
- 2023 年度新規開講講座「暗号学の現在―現代暗号入門」について、本日 11 月 8 日（水）より受講登録を開始します。

【概要】

東北大学オープンオンライン教育開発推進センターでは、「世界と地域に開かれた大学」「市民の知的関心を受け止め、支え、育んでいける教育研究活動を積極的に推進する大学」の実現を目指し、2016 年度よりオンライン講座、東北大学 MOOC（注１）を開講しています。

2023 年度の新規講座として、高度教養教育・学生支援機構教養教育院　静谷啓樹総長特命教授、データ駆動科学・AI 教育研究センター　酒井正夫准教授、磯辺秀司准教授、小泉英介助教、長谷川真吾助教による「暗号学の現在―現代暗号入門」を開講します。今日の日常生活に広く深く浸透した現代暗号。その原理と特徴、基本的な機能、社会インフラとの関わり、そして将来の量子計算機時代の暗号について、要点を平易にご紹介します。

本日 11 月 8 日（水）より受講登録を開始します。ぜひご登録いただき、ご紹介いただけますと幸いです。

【詳細な説明】
　東北大学 MOOC は、無料オンライン講座プラットフォーム「gacco®（ガッコ）」にて、東北大学サイエンスシリーズ第 8 弾「暗号学の現在―現代暗号入門」を、2024 年 1 月 24 日（水）より開講いたします。受講登録は、本日 11 月 8 日（水）11 時より開始いたします。

## 講座内容


　数千年の歴史をもつ暗号は 1970 年代以降に根本的で急峻な変革を遂げ、今日、暗号の科学と技術は様々な形で日常生活に深く浸透するに至りました。これを現代暗号と呼びます。
　この講座では現代暗号の原理と特徴、基本的な機能、社会基盤との関わり、そして近い将来に求められる暗号の機能について、要点を平易に紹介します。これにより暗号を切り口として、情報社会の現在と未来を垣間見ることにもなります。
　なお、現代暗号は数学的な理論に基づくものですが、できるだけ直観的な説明に努め、記法や概念を定義するときは高等学校「数学 I」や「数学 A」の言葉を使うよう配慮します。

## 講座概要

【講　座　名】東北大学サイエンスシリーズ「暗号学の現在―現代暗号入門」
【講　師】静谷　啓樹（東北大学高度教養教育・学生支援機構教養教育院　総長特命教授 ）
　　酒井　正夫（東北大学データ駆動科学・AI 教育研究センター　准教授）
　　磯辺　秀司（東北大学データ駆動科学・AI 教育研究センター　准教授）
　　小泉　英介（東北大学データ駆動科学・AI 教育研究センター　助教）
　　長谷川　真吾（東北大学データ駆動科学・AI 教育研究センター　助教）
【受講者募集期間】2023 年 11 月 8 日（水）11:00 ～ 2024 年 3 月 20 日（水）10:00 まで
【講座公開期間】2024 年 1 月 24 日（水）15:00 ～ 2024 年 3 月 26 日（火）23:59 まで
【受　講　費】無　料
※gacco の会員登録（無料）がお済みでない方は、以下より会員登録をお願いいたします。
　gacco 会員登録ページ： https://lms.gacco.org/register

【受講申込先】受講方法・受講申込などは、以下のホームページをご覧ください。
https://lms.gacco.org/courses/course-v1:gacco+ga186+2024_01/about

**※本講座の修了者には、東北大学オリジナルの修了証とオープンバッジが授与されます。**

## 講座詳細

**Week1：現代暗号の基本的な道具**

現代暗号の安全性の基礎となる数学的仕組みについて解説します。それが一方向性関数で、順方向の計算は容易ですが、逆方向の計算は困難という性質を持ちます。この性質に基づく代表的な暗号方式の例を学び、現代暗号の基本的原理への理解を深めます。

1. イントロダクション
2. 一方向性関数１：素因数分解問題
3. 一方向性関数２：RSA 問題
4. 一方向性関数３：離散対数問題
5. ハッシュ関数・擬似乱数生成器
6. Diffie-Hellman 鍵共有方式
7. ElGamal 暗号方式
8. RSA 暗号方式
9. RSA 署名方式

**Week2：基本的な道具で実現できる機能**

前週の道具を駆使して、大規模で安全な情報システムを構成する際の部品となる様々な機能が達成できることを学びます。具体的には、印鑑に代わる署名や本人認証、データを暗号化したまま四則演算を行う秘密計算、秘密情報を複数人で分散して共有する仕組み、暗証番号を見せずに所持自体を証明するゼロ知識証明などです。

1. イントロダクション
2. デジタル署名１（基本的な署名方式）
3. デジタル署名２（グループ署名・ブラインド署名）
4. 秘密分散共有（仕組みと代表的な方式）
5. 秘密計算（準同型暗号とその応用例）
6. ゼロ知識証明１（基本機能の直観的説明）

7. ゼロ知識証明２（少しフォーマルな説明）
8. ゼロ知識証明３（証明の具体例）
9. ゼロ知識証明４（証明できることの限界）

**Week3：暗号技術と現代社会システム**

いくつかの暗号技術の高度な組み合わせと巧妙な運用によって、地球規模の巨大な社会インフラが編まれている現状を学びます。具体的には、ウェブサイトの信頼性を担保する PKI、通信を保護する SSL/TLS、そして世界経済で存在感を増す暗号資産などに焦点を絞ります。

1. イントロダクション
2. インターネット（IPSEC、TLS）
3. 公開鍵暗号基盤（PKI）
4. 電子マネー（交通系カードほか）
5. ブロックチェーン１（全体像、暗号資産）
6. ブロックチェーン２（動作原理、運用の仕組み）
7. ブロックチェーン３（活用例：NFT）
8. ブロックチェーン４（活用例：スマートコントラクト）
9. ブロックチェーン５（社会インフラとしての期待と課題）

**Week4：量子計算機時代の新しい暗号**

現代暗号が抱える本質的な課題と、その解決への取り組みの現状を学びます。実は近い将来、量子計算機が本格的に実用化されると、現在は一方向性と考えられている関数が、そうではなくなることが判っています。そこで、量子計算機にとっても困難と考えられている計算問題を使って、新時代の一方向性関数を構成する試みが活発化しています。その代表例を紹介し、未来につなげて講座を閉じます。

1. イントロダクション
2. 古典計算機と量子計算機（基本的な差異）
3. ショアのアルゴリズム（素因数分解問題の解法）
4. 耐量子計算機暗号の候補（依拠する問題による分類）
5. 格子上の問題１（最短ベクトル問題）
6. 格子上の問題２（LWE 問題）
7. 格子暗号１（米国国立標準技術研究所よる標準化動向）
8. 格子暗号２（標準方式候補の概要）
9. 今後の展望（むすびに代えて）

## 講師紹介

**静谷　啓樹（しずや　ひろき）**
東北大学教養教育院 総長特命教授
1987 年東北大学大学院工学研究科博士課程修了（工学博士）。
東北大学助手、助教授を経て 1995 年同大教授。2023 年より現職、東北大学名誉教授。専門は理論計算機科学、特に計算量理論と暗号理論。

**酒井　正夫（さかい　まさお）**
東北大学データ駆動科学・AI 教育研究センター 准教授
1974 年 6 月生まれ。富山県出身。
東北大学大学院工学研究科博士後期課程修了後、同大学情報シナジーセンター助手、同大学高等教育開発推進センター講師、同大学教育情報基盤センター准教授を経て、現職。学位：博士（工学）東北大学
専門はデータ科学。特にブロックチェーン技術を用いた個人情報の保護と活用に取り組んでおり、開発技術の社会実装にも取り組んでいる。

**磯辺　秀司（いそべ　しゅうじ）**
東北大学データ駆動科学・AI 教育研究センター 准教授
東北大学大学院情報科学研究科システム情報科学専攻 博士後期課程修了後、東北大学教育情報基盤センターなどを経て、2019 年 10 月より現職。代数学、特に群論の暗号理論への応用に取り組んでいる。

**小泉　英介（こいずみ　えいすけ）**
東北大学データ駆動科学・AI 教育研究センター 助教
2005 年東北大学大学院理学研究科博士後期課程修了、博士（理学）。
東北大学高等教育開発推進センター助手、助教、東北大学教育情報基盤センター助教を経て、2019 年 10 月より現職。
現在の専門は情報・データ科学教育および情報セキュリティに関連する数学。

**長谷川　真吾（はせがわ　しんご）**
東北大学データ駆動科学・AI 教育研究センター 助教
2009 年東北大学大学院情報研究科博士課程修了（博士（情報科学））。
東北大学教育情報基盤センター助教を経て 2019 年より現職。
専門は情報セキュリティ、特に暗号理論。

## 東北大学 MOOC のシリーズについて

東北大学では、JMOOC にて下記の 2 シリーズを展開しております。今後も新規開講講座が追加されます。
また、再開講も随時行っていく予定ですので、ぜひ他講座にもご参加ください。

**東北大学サイエンスシリーズ**

- 第 1 弾 解明：オーロラの謎
- 第 2 弾 東日本大震災の教訓を活かした実践的防災学へのアプローチ ―災害科学の役割
- 第 3 弾 銀河考古学入門～銀河の形成と進化を辿る～
- 第 4 弾 進化発生学入門－恐竜が鳥に進化した仕組み－
- 第 5 弾 放射線安全社会入門～リスクの知見を暮らしに～
- 第 6 弾 痛みと麻酔科学
- 第 7 弾 人間脳科学入門
- 第 8 弾 暗号学の現在―現代暗号入門

**東北大学で学ぶ高度教養シリーズ**

- 第 1 弾 memento mori -死を想え-
- 第 2 弾 男と女の文化史

・第 3 弾 家族と民法
・第 4 弾 社会の中の AI～人工知能の技術と人間社会の未来展望～
・第 5 弾 化粧で学ぶ心理学
・第 6 弾 自己理解の心理学

注 1.　MOOC：Massive Open Online Courses の略。Web 上で誰でも無料で参加可能な、大規模かつオープンな講義を提供し、修了者に対して修了証を発行する教育サービスです。2012 年より米国を中心として、主要大学および有名教授によるオープンオンライン講座として公開され、世界中で多様な学習者が受講しています。

【参考】
東北大学オープンオンライン教育開発推進センターウェブサイト
https://mooc.tohoku.ac.jp/

【問い合わせ先】
東北大学オープンオンライン教育開発推進センター
担当　垣見、柴田、小林
電話:  022-795-4933
E-mail:　secretary.mooc@grp.tohoku.ac.jp