KISTEC 教育講座

量子時代のセキュリティを理解する

～耐量子計算機暗号，高機能暗号～

9月18日（木）・19日（金）

ご受講方法を選べます
対面開催
オンライン併設

全日程 2 日
1日のみ受講も可

※詳細はホームページをご覧ください。
https://www.kistec.jp/learn/researcher/ango/

量子計算機時代の暗号技術の課題・最新動向に触れたい、基礎理論を学びなおしたいとお考えの研究者・技術者の皆様へお届けする講座です。

9/18（木）　暗号技術概要、量子計算機による暗号解読の基礎、高機能暗号

時間	講義	内容	講師
10：00 −10：30	全体概要（オリエンテーション）と暗号技術の基礎	本講座の紹介の後、現代の暗号技術の理論と全体概要、今後の展望について概説する。	國廣　昇　氏（筑波大学　教授）
10：30 −12：30	量子計算機による暗号解読の基礎	量子アルゴリズムの中でも Shor のアルゴリズムを紹介し、量子コンピュータと暗号の関係に関して概説する。	
14：00 −16：00	証明可能安全性と高機能暗号	暗号や署名と言った単純な機能だけでなく、暗号化したまま統計処理などの計算が可能である準同型暗号や、署名者の匿名性を担保するグループ署名などの高機能暗号が注目を集めている。この講義では、量子時代において活用が期待される高機能暗号を紹介するとともに、その安全性や実社会への応用事例なども含めて説明する。	江村　恵太　氏（金沢大学　准教授）

9/19（金）　格子理論の基礎、耐量子計算機暗号の標準化動向、耐量子計算機暗号

時間	講義	内容	講師
10：00 −12：00	格子と格子暗号の基礎	量子計算機による解読にも耐性を持つ格子暗号とその安全性を支える格子問題について概説する。具体的には、格子がもつ基本性質と代表的な格子問題と求解法を説明すると共に、代表的な格子暗号方式を紹介する。	安田　雅哉　氏（立教大学　教授）
13：30 −14：00	NIST による耐量子計算機暗号の標準化動向	NIST による耐量子計算機暗号の標準化が進んでいる。これまでの候補暗号選定の経緯および標準化の動向について紹介する。	國廣　昇　氏（筑波大学　教授）
14：00 −16：00	耐量子計算機暗号	量子計算機でも解読できない暗号として格子暗号は代表的であるが、現在 NIST により標準化が進められている格子暗号は、実用性を高めるために数学的に特殊な構造をもった格子に基づいて構成されている。その理解は標準格子暗号方式を実装する上でも必須の知識となっており、本講義では、標準化されたハッシュ関数署名と共に、構造付き格子に基づく格子暗号に関して技術説明を行う。	高島　克幸　氏（早稲田大学　教授）

対象者

企業、研究機関にご所属で、
- ◆量子時代の暗号技術について学び始めたい方
- ◆情報通信、サイバーセキュリティ分野の技術開発に携わる方
- ◆新たなコンピュータの開発を目指す方、コンピュータ技術（ハード、ソフトウェア）のセキュリティや暗号技術に携わる方
- ◆DX、IoTの導入、設計に携わる方
- ◆暗号技術の開発、実装に携わる方
- ◆数学（mod計算、ベクトルなど）に馴染みがあり、暗号技術に関心をお持ちの方
- ◆現代の暗号（共通鍵暗号、公開鍵暗号、デジタル署名、RSA暗号等）からさらに進んだ技術の導入を検討している方

・・・・・・など

定員 15 名（先着順）

主催（地独）神奈川県立産業技術総合研究所

カリキュラム編集者からのメッセージ

暗号技術は、既に私たちの生活にすっかり溶けこみ、暗号なしでは、もはや生活することはできません。今、広く利用されている RSA 暗号や楕円曲線暗号などの公開鍵暗号は、現代の暗号技術の基盤であるにもかかわらず、量子時代の到来により、瞬く間に解読されてしまう可能性があります。そのため、安全に使える暗号技術を準備しておくことが、情報通信技術の必須課題となっています。

しかし、暗号技術を議論する上で、安全性だけを気にするわけにはいきません。暗号化し、安全に情報を保持することだけがゴールではなく、暗号化した上で、その情報をいかに有効活用するかが重要です。それにも関わらず、労力をかけて集めた有用なデータでさえ、秘密にしてしまう事例も多く見られます。こうした状況に対して、データを暗号化したままなんらかの有用な計算ができる準同型暗号、秘匿計算などの高機能暗号は、応用技術として広がりつつあります。ビットコインを代表例とするブロックチェーン技術も暗号技術を基礎としたものであり、今後、さらにこの分野の応用・開発が加速していくことでしょう。

本講座では、書籍「暗号の理論と技術 量子時代のセキュリティ理解のために」の 2 章，5 章，6 章，9 章を中心に講義します．耐量子計算機暗号を一通り理解することを目標に，格子の理論，量子計算機に対する暗号の脅威を理解したうえで，NIST による標準化動向，標準化暗号について概観します．さらに，今後ますます利用が期待される高機能暗号についても説明します．企業の方々が基礎から応用までの幅広く知識を習得することを目的とし、特に、独学ではキャッチアップすることが難しい最先端技術に関しても、わかりやすく解説します。

受講料

ご受講日数をお選びいただけます。

区　分	全日程	1 日受講
A　一般	38,000円	24,000円
B　KISTEC パートナー団体会員 C　神奈川県内中小企業＊	30,400円	
D　C 以外の神奈川県内企業 E　神奈川県内在住の個人の方	34,200円	

※ 神奈川県内中小企業とは事業所が神奈川県内にあり、資本金が3億円以下、または、企業全体の従業員が300人以下である企業をさします。

会場

かながわサイエンスパーク内　講義室
（神奈川県川崎市高津区坂戸 3-2-1）

オンライン受講も可能です
(ZOOM 使用)
※ 対面受講またはオンライン受講の選択制
※ 諸状況によりオンライン開催のみとなる可能性がございます。

ご受講の皆様に、講師の共著『暗号の理論と技術 量子時代のセキュリティ理解のために』（2024 年，講談社）を進呈致します（お申込みお一人につき一冊）。講義内容の復習にお役立てください。

申込要項

必ずご確認の上お申し込みください。

- オンライン受講の方は、必ずZOOMの推奨環境を事前にご確認ください。 PC、インターネット通信環境（有線LAN接続、Wi-Fi推奨）、PCに接続可能なマイク、カメラ、スピーカーをご用意ください。（PCに内蔵されている場合は不要）
- 受講資格はお申込みをいただいた方(1 申込 1 名)に限ります。
- 申込締切後、受講決定者には受講票・受講料請求書等の必要書類をお送りします。オンライン受講をお申し込みの場合、受講日前日までにお申込みいただいたご住所へ印刷テキストをお送りします。
- 申込締切後でも、定員に余裕がある場合はお申込みを受付けられる場合がありますのでお問合せください。
- 全受講コースお申込みの場合、全日程の出席者には「修了証」を送付いたします。
- 講義中、許可なく講義内容の一部、およびすべてを複製、転載または撮影、配布、印刷など、第三者の利用に供することを禁止します。
- やむを得ない事情により、日程・内容等の変更や中止をする場合があります。
- その他、お申込みについてご不明な点は、主催者へお問い合わせください。

詳細はこちら

HP からお申込みいただけます。
https://www.kistec.jp/learn/researcher/ango/

お問い合わせ

地方独立行政法人
KISTEC 神奈川県立産業技術総合研究所
〒213-0012 神奈川県川崎市高津区坂戸 3-2-1　KSP 東棟 1 F
Tel (044)819-2033
E-mail　manabi@kistec.jp　URL　https://www.kistec.jp/

申込書にご記入いただいた個人情報は、当所の事業等に関する情報や参加者募集の案内などの範囲内で利用または提供いたします。
個人情報は、取扱目的以外に利用したり、第三者に提供することはありません。

（コースID：25ウ）