

研究終了報告書

「バッテリーレス無線センサネットワークのためのポスト量子暗号計算技術」

研究期間：2018 年 10 月～2022 年 3 月

研究者：上野 嶺

1. 研究のねらい

バッテリーレス無線センサネットワーク（WSN: Wireless Sensor Network）は、自動車やドローンなどの自動運転や、インフラの健康診断、スマートホームやスマート工場などを実現する基盤技術の一つであり、Society 5.0 における戦略分野「移動革命の実現」や「インフラの維持管理による生産性向上」に貢献することが期待されている。一方で、これらの応用における耐用年数や規格化に必要となる年数は十数年～数十年とされ、また、メンテナンスフリー性や機器の信頼性向上の観点からも自立電源化やバッテリーレス化が強く求められる。

これらの WSN 応用におけるモジュールにおいても、従来の IoT システム同様、秘密情報の詐取やデータの改変・偽造といった攻撃に備える必要があり、耐用年数中や、規格化後も危殆化しない長期セキュリティの実装が強く求められる。そのような長期セキュリティを実現するための暗号技術として、ポスト量子暗号（PQC: Post-Quantum Cryptography）が盛んに研究されている。近年、ゲート型量子計算機の発展が目覚ましいが、大規模な量子計算機が実現されると現在利用されている公開鍵暗号（RSA 暗号や楕円曲線暗号）は効率的に解読可能なことが知られており、米国標準技術研究所（NIST）はそのような量子計算機の実現は 2030 年頃との予測を示している。PQC は、量子計算機を用いた暗号解読に対して耐性があるとされる公開鍵暗号の総称であり、量子計算機実用化後のセキュリティを実現するために必要不可欠な技術である。これから長期の利用が見込まれる応用においては、システム開発・設計段階からこのようなセキュリティを組み込む「セキュリティ・バイ・デザイン」がその安全な運用や規格化において極めて重要である。

PQC の実用化における大きな課題は実装コストであり、特に計算時間や鍵長、暗号文長について既存の公開鍵暗号よりも数倍～数百倍のコストを要求することもある。また、WSN モジュールを始めとする組み込み応用においては、暗号演算を実行する機器に物理的にアクセスして秘密情報を詐取する攻撃に対する耐性（耐タンパー性）が必要不可欠となる。本研究では、PQC をリソース制約の厳しい組み込み機器においても実現する計算技術を開発するとともに、PQC をタンパー攻撃を考慮しても安全に実装する技術の開発を行うことで、WSN を始めとする長期運用が必要なシステムにおける長期セキュリティの実現に寄与することを目指す。

2. 研究成果

(1) 概要

1 PQC の高効率計算技術の開発

本テーマでは、PQC の中でも最も鍵長を小さく長期セキュリティを実現できるが計算コストの大きい同種写像暗号と、その次に鍵長・通信量が小さい格子暗号に着目して、それらを効率的に実現するハードウェアアルゴリズムの開発を実施した。結果として、同種写像暗号の本研究開始時（2018 年）の最速実装約 20ms に対し、Xilinx Kintex Ultrascale+上において

2.4 ms で同暗号を実行可能なことを確認した。これは現在知られている同型デバイス(そして全ての FPGA)実装の中で最速である。また、格子暗号についても、格子暗号向けの新たな剰余演算手法を開発することにより、これまでで最も高速かつ高効率に格子暗号を実現するハードウェアの開発に成功した。加えて、PQC の安全・効率的な運用においては共通鍵暗号が一般に併用されるため、国際標準共通鍵暗号 AES を最も効率的に実行するハードウェアの開発も行った。

2 PQC を実装する際に生じる共通の脆弱性の発見と対策技術の開発・評価

本テーマでは、PQC のうち鍵交換や認証などに用いられる鍵カプセル化メカニズム (KEM) の実装における共通の脆弱性を発見し、NIST が開催中の PQC 公募コンペティションにおいて 2021 年段階で選考中の九つの KEM 候補のうち八つが発見した攻撃に対して脆弱であることを実験的に示した。また、提案攻撃に対する対策を検討し、その評価も行った。

3 深層学習技術の暗号モジュール安全性評価への応用

近年、深層学習のサイドチャネル攻撃分野における極めて高い優位性が数多く報告されている。本研究においても、上述の PQC KEM に対する攻撃において深層学習に基づくサイドチャネル情報解析を活用している。一方で、これまでの深層学習サイドチャネル攻撃は実験評価に基づく報告がほとんどであり、多くの未解決問題を抱えているとともに深層学習サイドチャネル攻撃の最適性や限界に関する理論的考察は少なかった。本テーマでは、理論的考察とともにこのような未解決問題のいくつかを解決することで深層学習サイドチャネル攻撃に対して安全な暗号モジュールの設計方法の理論的基礎の構築に貢献した。

4 確率的計算を用いた秘匿計算技術の開発

準同型暗号に基づく秘匿計算はビッグデータ(IoT や WSN など)を活用して得られるものを含む)の利活用とプライバシー保護の両立を実現するための技術として期待されている。本テーマでは、確率的計算と準同型暗号を組み合わせた新たな秘匿計算手法し、さらに PQC である格子暗号と組み合わせることで従来の準同型暗号よりも優位となりうることを秘匿機械学習推論などへの応用を通して示した。

(2) 詳細

1 PQC の高効率計算技術の開発

本テーマでは、組み込み機器への適用を目的として、最も鍵長が短い計算コストが大きい PQC である同種写像暗号およびその次に鍵長が短い格子暗号を効率的に計算する技術の開発を実施した。

同種写像暗号の計算コストのほとんどは虚二次拡大体の剰余乗算が占めるため、まず、剰余数系 (RNS: Residue Number System) や Quotient pipelining などの冗長表現を用いた高速な虚二次拡大体乗算器を開発した。RNS は整数を互いに素な複数の整数による剰余を用いた表現であり、その並列性から特に高速実装に向いていると言われる。本テーマでは、RNS により剰余乗算を実現する代表的なハードウェアアーキテクチャである Cox-Rower

アーキテクチャをベースに、その虚二次大体上の演算を並列かつ高速に実行するデータパスを設計するとともに、さらにそれを同種写像暗号全体を高速に実行するために最適化した。また、Quotient pipelining は冗長表現を用いたモンゴメリ乗算のハードウェアアルゴリズムであり、RNS と同様に低遅延な乗算器の実現に有用であることに加え、高い並列性を有している。こちらについても上述と同様のデータパス設計および最適化を行った。

さらに、その乗算器の高速性および並列化可能性を最大限活用した同種写像暗号ハードウェアアーキテクチャを開発した。表 1 に Xilinx Kintex Ultrascale+ に RNS ベースアーキテクチャを実装した場合の性能を示す。表 1

表 1：提案 RNS ベース乗算器に基づく同種写像暗号ハードウェアと既存手法の性能比較。

	# LUTs	# DSPs	Fmax (MHz)	Latency (ms)
提案手法	43,708	1,089	325.9	2.4
既存手法	21,657	240	299.4	3.3

より、提案乗算器はリソースの消費が大きいものの、高速に同種写像暗号を実行可能なことが確認できる。同種写像暗号はリソース消費と実行速度のトレードオフを活用することが難しいため、本成果は特に低遅延が重要な応用において有用であると言える。また、表 2 に Xilinx Vertex 7 に Quotient pipelining ベース乗算器を実装した場合の性能と同種写像暗号 SIKEp434 の実行時間見積もりを示す。こちらについても同様に同種写像暗号を高速に実行できることが確認できる。なお、表 2 内の数値は乗算器のみを実装した場合のリソース消費を表しているため、同種写像暗号アーキテクチャ全体を実装した場合は、メモリなどの最低限必要になるリソースがオフセットとして含まれるため、低遅延に実行可能な提案乗算器の方が同種写像暗号を効率的に実行できる可能性があると言える。

表 2：提案 Quotient pipelining 乗算器と既存手法の性能と同種写像暗号実行時間の見積もり。

	# Slices	# LUTs	# FFs	# DSPs	Fmax (MHz)	Latency for $\mathbb{F}_{p,2}$ mult (ns)	Slice-Latency product (m)	Latency (us)		
								KeyGen	Encaps	Decaps
既存手法 1	607	1,905	1,119	43	281.37	335.34	0.204	2,441.67	4,170.85	4,444.94
既存手法 2	18,669	55,188	15,033	0	122	581.92	10.86	5,430.63	9,276.61	9,886.22
既存手法 3	12,840	48,965	5,843	0	157.6	330.02	4.35	2,648.68	4,510.17	4,813.78
既存手法 4	1,566	4,840	3,171	120	96.2	530.40	0.83	4,261.73	7,255.72	7,744.75
提案手法	12,926	44,238	37,500	0	306.9	169.42	2.20	1,360.03	2,315.86	2,471.76

次に、格子暗号ハードウェアの設計について述べる。多くの格子暗号では数論変換 (NTT: Number Theoretic Transform) と呼ばれる有限体上のフーリエ変換が全体の実装コストのほとんどを占めるため、NTT の実装方法が盛んに研究されている。さらに、NTT の中でも乗算および剰余演算に大きなコストがかかるため、これらの演算を効率的に行う NTT データパスの開発が格子暗号全体の高効率化において重要と言える。そこで本テーマでは、格子暗号の多くの剰余がプロ素数で与えられることに着目し、Compressed K^2 -reduction と呼ばれる新たな格子暗号向け剰余演算手法と、それを用いた NTT データパスを開発した。表 3 に、提案データパスを用いた NTT アーキテクチャと、

表 3：提案 NTT ハードウェアと既存手法の性能比較

同パラメータ (Kyber と呼ばれる格子暗号などで利用される代表的なパラメータの一つ) を用いた既存手法の性能を示す。表 3 よ

	NTT/NTT クロックサイクル数	動作周波数 [MHz]	実行時間 [μs]	消費リソース			
				LUTs	FFs	DSPs	BRAM
既存手法 1	512/576	161	3.18	1,737	1,167	2	3
既存手法 2	904/904	190	4.76	948	352	1	2.5
提案手法 (面積重視)	902/902	206	4.37	296	181	1	1.5
提案手法 (効率重視)	455/455	216	2.11	579	417	2	3
提案手法 (速度重視)	268/268	216	1.24	904	811	4	2.5

り、提案アーキテクチャが最も効率的に Kyber の NTT を実現可能なことが確認できる。

2 PQC を実装する際に生じる共通の脆弱性の発見と対策技術の開発・評価

PQC は公開鍵暗号の一種であり、その中でも鍵カプセル化メカニズム (KEM) は鍵交換や認証などを実現する基盤技術である。公開鍵暗号への暗号解読攻撃は選択平文攻撃と選択暗号文攻撃に大別される。後者は前者よりも強力な攻撃であり、実用には選択暗号文攻撃に対して安全であることが必要である。一方で、選択暗号攻撃に対して安全な公開鍵暗号を力節構成することは極めて難しいため、PQC KEM アルゴリズムの設計では、まず、公開鍵暗号を構成するための (耐量子性を有する) 数学的問題に基づいて選択平文攻撃に対して安全な公開鍵暗号化スキーム (PKE) を構築し、その PKE に対し藤崎・岡本 (FO) 変換と呼ばれる処理を適用して選択暗号文攻撃に対して安全な KEM を実現する手法が一般的に用いられる。

KEM や FO 変換の理論的安全性は十分に評価されている。一方で、KEM を実装する際には物理的な脆弱性が生じる可能性があり、その中でも代表的なものがサイドチャネル情報 (消費電力や漏洩電磁波など) を解析して秘密情報を詐取するサイドチャネル攻撃に対する脆弱性である。本テーマでは、FO 変換時の処理のサイドチャネル情報を解析することでほとんど全ての PQC KEM の秘密鍵を詐取できる脆弱性を発見した。より詳細には、FO 変換時の処理のサイドチャネル情報を利用することで、内部で使われている PKE に選択平文攻撃を適用可能なことを発見した。また、それを実現するための具体的な方法も提案し、NIST の PQC 公募コンペティションの 2021

年段階の九つの KEM 候補のうち八つが提案する方法により秘密鍵詐取が可能であることを実験的に示した。表 5 に、実機実験評価による NIST PQC の KEM 候補を破るために必要なサイドチャネル波形数を示す。表 5 より、ほとんどの KEM が現実的な波形数で秘密鍵を詐取されてしまうことが確認できる。

本テーマでは、発見した脆弱性に対する対策手法の検討も行った。結果として、Threshold Implementation と呼ばれるハードウェアベースのマスキングが対策として有効であることを実験的に確認した。

表 4: 発見したサイドチャネル攻撃の標準化候補への適用。適切な対策が施されていない場合は様々な KEM の秘密鍵が現実的な波形数で詐取されてしまう。

KEM type	Scheme	Instance	# Traces for attack phase	
			Non-masked implementations	Masked software
Lattice	Kyber	Kyber-512	3,072	7,680
		Kyber-1024	6,144	15,360
	Saber	LightSaber-KEM	6,144	15,360
		FireSaber-KEM	6,144	15,360
	FrodoKEM	FrodoKEM-640	51,200	128,000
		FrodoKEM-1344	86,016	215,040
	NTRU	ntruhrs701	5,608	14,020
		ntruhrs2048509	2,036	5,090
		ntruhrs4096821	3,284	8,210
	NTRU Prime	ntrupr653	2,612	6,530
		ntrupr1277	5,108	12,770
		sntrup653	5,424	13,560
		sntrup1277	10,350	25,875
		hqc128	36,222	90,555
Code	HQC	hqc256	117,072	292,680
		Level 1	6M	15M
	BIKE	Level 5	N/A	N/A
		Classic McEliece	Any	N/A
	SIKE	SIKEp434	548	1,370
Isogeny	SIKE	SIKEp751	956	2,390

3 深層学習技術の暗号モジュール安全性評価への応用

近年、深層学習のサイドチャネル攻撃分野における極めて高い優位性が数多く報告されており、本研究においても、上述の攻撃においても深層学習にサイドチャネル情報解析を活用している。一方で、これまでの深層学習サイドチャネル攻撃は実験評価に基づく報告がほとんどであり、多くの未解決問題を抱えているとともに深層学習サイドチャネル攻撃の最

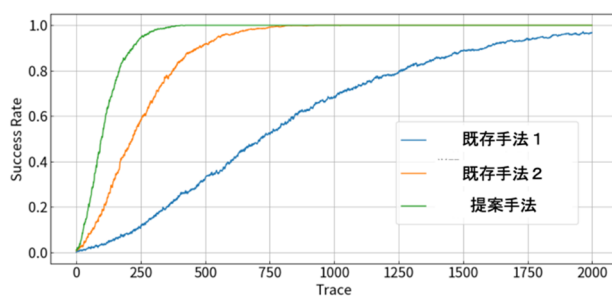


図 1：既存手法と提案手法による深層学習サイドチャネル攻撃の評価結果。横軸はサイドチャネル波形数攻撃成功数で縦軸はそのときの攻撃成功確立。提案手法はより少ない波形数で攻撃が成功するかどうかを評価できる。

適性や限界に関する理論的考察は少なかった。本テーマでは、深層学習サイドチャネル攻撃における主要な未解決問題の一つであったデータ不均衡問題の解析を行い、その根本的な解決策を提案した。これにより、深層学習サイドチャネル攻撃のより正確な性能評価が可能になり(図 1)、より安全な暗号モジュールの設計に寄与することが期待される。

4 確率的計算を用いた秘匿計算技術の開発

準同型暗号に基づく秘匿計算はビッグデータ(IoT や WSN など)を活用して得られるものを含む)のり活用とプライバシー保護の両立を実現するための技術として期待されている。本テーマでは、確率的計算と準同型暗号を組み合わせた新たな秘匿計算手法し、さらにPQCである格子暗号と組み合わせることを提案した。さらに、提案スキームをプライバシー保護機械学習推論へ応用し、計算コストの観点から提案スキームが従来の準同型暗号に基づく秘匿計算技術よりも優位となりうることを示した(表 4)。

表 4: 提案手法 (HESC) と既存手法によるプライバシー保護機械学習推論のアイヤメ分類への適用。提案手法を用いることで実行時間を約半分に削減。

	BFV	CKKS	HESC w/ BFV	HESC w/ CKKS
B2S	0	0	0.488	1.355
Enc	5.038	7.415	1.741	2.015
NN	411.242	89.931	2.422	1.856
Dec	1.968	0.656	31.707	25.527
S2B	0	0	4.939	9.516
Total	418.248	98.002	41.297	40.269

3. 今後の展開

1, 2 PQC の実装およびその安全性評価に関して

本研究における PQC の実装やその安全性評価に関する成果は、NIST による PQC 公募コンペティション選考に貢献したと考えている。したがって、本成果により、より高効率かつ高安全な PQC 実装が世の中に普及することが期待される。PQC の一部はすでに実用化(例えば Amazon Web Service など)されているが、NIST PQC 公募コンペティションのポートフォリオ策定によりこのような PQC の併用および PQC への移行は今後数年でさらに増えると考えられる。以上より、本成果は今後の PQC 搭載システムの安全性向上と標準化活動に貢献する。

3 深層学習サイドチャネル攻撃に関して

深層学習サイドチャネル攻撃は2018年頃から急速に報告が増え始めた比較的新しい分野であり、未解決問題も数多く残っている。深層学習サイドチャネル攻撃は極めて強力な攻撃であり、ここにおける未解決問題を解決することで(これまで理論上でしか議論されてこなかったような)極めて強力なサイドチャネル攻撃を実験的に実現できる可能性がある。これにより、サイドチャネル攻撃の限界が判明し、実験的にそれが評価可能となることで、サイドチャネル攻撃に対して極めて高い安全性を有する対策技術の開発が可能になり、高安全な暗号モジュールの普及に貢献すると期待している。

4 秘匿計算技術について

本研究期間では、機械学習推論への適用において、小規模なデータセットにおける既存技術に対する優位性を確認した。一方で、より大きなデータセットにおける優位性は不明である。今後より大きなデータセットへの拡張およびその評価を行うことで、実用に耐える現実世界の応用へ展開することができると考えている。

4. 自己評価

達成状況

当初計画していた主な達成目標であるPQCの高速・高効率については、当初取り扱う予定であった同種写像暗号と格子暗号について世界最先端の関連研究と比べても優位となりうるものを設計できたと考えている。また、実装安全性評価については、ほとんど全てのPQC KEMについて適用可能な脆弱性の発見とその理論的確立、さらにその対策の検討と評価を行うことができたため、当初計画していたことを高い水準で達成できたと考えている。その上で、さらに当初の計画にはなかった深層学習サイドチャネル攻撃への展開もできた。

一方で、設計した回路は要素技術のプロトタイプにとどまっており、当初計画していた実際のWSNモジュールへの適用や評価まで実施することができなかった。これはPQCを高速・効率的に実現するデータパスの設計に想定以上に期間を要してしまったためであり、大きな反省点であるとともに今後の展望としている。

研究の進め方

当初計画していたPQCの高効率実装に関しては上述のとおりデータパス設計に想定以上の期間を要してしまった。一方で、PQCの実装安全性評価に関しては、基礎理論の構築から実機評価実験、そして対策の評価まで筋道立てて実施することができたため、成果としても非常によくまとまったものが出せたと感じている。さらに、その過程において利用した深層学習技術について、本研究とのより深い関連を見出して深層学習サイドチャネル攻撃へ展開できたことにより当初の計画を超えて本研究の可能性を大きく広げられたと考えている。

研究成果の科学技術・経済への波及効果

上述のとおり、本研究におけるPQCの実装やその安全性評価に関する成果は、今後のPQC搭載システムの安全性向上とPQC標準化活動に貢献すると考えている。また、暗号技術やセキュリティは、通常、情報システムにおける機能要件となることは少ないものの、PQCのような長期セキュリティを実現する技術の普及や標準化は、セキュリティ上の脆弱性に関

連する経済損失や、危殆化に伴うメンテナンスやアップデートのコストを大きく削減することに貢献すると言える。

学術的観点においては、本研究で発見した実装脆弱性は PQC KEM のほとんど全てに影響を与えるものであり、今後 KEM の実装関連研究に対して大きな影響を与えている。深層学習サイドチャネル攻撃に関しても、理論解析による深層学習サイドチャネル攻撃評価の高精度化はより安全な暗号実装の実現に大きく貢献するものであり、学术界・産業界ともに大きな影響があるものである。

5. 主な研究成果リスト

(1) 代表的な論文(原著論文)発表

研究期間累積件数: 3件

1. Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, and Naofumi Homma, “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(1), pp. 296–322 (2021)

本論文では、耐量子性鍵カプセル化メカニズム (KEM) で一般に用いられている再暗号化処理の電力/電磁波を解析することで、KEM の秘密鍵を詐取できることを示した。提案手法を用いることで、NIST の PQC 公募コンペティションの九つの KEM 候補 (2021 年段階) のうち八つの秘密鍵詐取が可能なことを実験的に示した。また、対策技術についても検討・評価し、Threshold Implementation と呼ばれるハードウェアマスキングが対策として有効なことを確認した。

2. Akira Ito, Kotaro Saito, Rei Ueno, and Naofumi Homma, “Imbalanced Data Problems in Deep Learning-Based Side-Channel Attacks: Analysis and Solution,” *IEEE Transactions on Information Security and Forensics*, 16, pp. 3790–3802. (2021)

深層学習を用いたサイドチャネル攻撃においては、データ不均衡問題により攻撃性能が正確に測れない問題が指摘されていた。本論文では、データ不均衡問題が深層学習サイドチャネル攻撃にどのような場合にどのような影響を及ぼすかを明らかにした上で、そのデータ不均衡問題の影響をどの程度受けているかの定量的な評価手法を提案した。さらに、データ不均衡問題を根本的に解決する新たな攻撃評価手法を提案し、既存手法と比較して提案手法の優位性を実験的に確認した。

3. Rei Ueno, Sumio Morioka, Noriyuki Miura, Kohei Matsuda, Makoto Nagata, Shivam Bhasin, Yves Mathieu, Tarik Graba, Jean-Luc Danger, and Naofumi Homma, “High Throughput/Gate AES Hardware Architectures Based on Datapath Compression,” *IEEE Transactions on Computers*, 69(4), pp. 534–548. (2020)

本論文では、世界で最もよく使われる共通鍵暗号 AES を効率的に実行するハードウェアの設計を行った。提案ハードウェアは、合成体算術と呼ばれる AES の演算に最も適した数体表現を用いるとともに、その変換・逆変換のオーバーヘッドをレジスタタイミングや命令順序交換といった手法を用いて最大限抑制する。さらに、セレクタの削減や回路共有などの回路設計技法に加えて、乗法的オフセットと呼ばれる新たな最適化手法を提案した。結果として、提

案 AES ハードウェアは従来の最も高効率なハードウェアと比べて約半分のエネルギーで AES 暗復号を実行できることを確認した。

(2) 特許出願

研究期間全出願件数: 1 件 (特許公開前のものも含む)

1	発 明 者	上野 嶺, 本間 尚文
	発 明 の 名 称	秘匿計算装置、秘匿計算方法およびプログラム
	出 願 人	東北大学
	出 願 日	2019/12/24
	出 願 番 号	特願2019-232752
	概 要	ストカスティック計算と呼ばれる確率的計算を暗号文上で評価可能な暗号化方式およびその準同型評価方法. ビッグデータ利活用とプライバシー保護の両立を効率的に実現するための技術として期待される.

(3) その他の成果 (主要な学会発表、受賞、著作物、プレスリリース等)

1. Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma, “Fault-Injection Attacks against NIST’s Post-Quantum Cryptography Round 3 KEM Candidates,” In: Proceedings of the 27th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2021), Vol. 13091, LNCS, Springer, pp. 33-61. (2021)
2. Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, and Naofumi Homma, “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs,” International Conference on Cryptographic Hardware and Embedded Systems. 2022 年 9 月発表予定.
3. プレスリリース, 量子コンピュータにも耐性を持つ次世代暗号を安全に実現する技術を開発・実証 (2022 年 1 月予定).
4. ハードウェアセキュリティ研究会若手奨励賞, 剰余数系を用いた同種写像暗号の高速ハードウェア実装, 2021 年 12 月 10 日.
5. Rei Ueno, “Hardware Implementation of Block Cipher: Case Study Using AES,” The 9-th Asian-workshop on Symmetric Key Cryptography, 2019. (招待講演)