Schedule and Abstracts

Tuesday, January 10, 2017
Lattice Based Cryptography

09:00 - 10:00	Damien Stehlé The learning with errors problem: from lattices to cryptography
10:00 - 11:00	Shweta Agrawal Interpolating Predicate and Functional Encryption, from Learning With Errors
	Coffee Break
11:30 - 12:30	Léo Ducas Exploiting Quantum Algorithms against Ideal-SVP
	Lunch
14:00 - 15:00	Kim Laine String Matching on Homomorphically Encrypted Data

Abstracts

Time: 09:00 – 10:00, Tuesday, Jan 10, 2017
Speaker: Damien Stehlé
Title: The learning with errors problem: from lattices to cryptography
Abstract:
The search variant of the Learning With Errors problem (LWE) is to recover s in (Z/qZ)^n from arbitrarily many samples of the form (a_i, <a_i, s> + e_i mod q), where the a_i's are chosen uniformly from (Z/qZ)^n, and the ``errors'' e_i in Z are sampled from some distribution supported on small numbers, typically an integer Gaussian distribution with standard deviation parameter \alpha q for \alpha = o(1).
Since its introduction by Oded Regev, the presumed hardness of LWE and its decision variant has served as a security foundation of numerous cryptographic primitives: public-key encryption [Reg09], fully homomorphic encryption [BV11], identity-based encryption [ABB10], attribute-based encryption [GVW13], among many others.
LWE is fundamentally related to Euclidean lattices, i.e., discrete subgroups of an R^n. The best known algorithms for LWE rely on lattice reduction algorithms. Perhaps more surprisingly, Regev [Reg09] gave a quantum reduction from standard worst-case lattice problems to LWE. A classical (but weaker) reduction was more recently proposed by Brakerski et al [BLPRS13].
In this talk, I will present LWE, describe how it can be used for public-key encryption, and stress its links with standard algorithmic problems on Euclidean lattices. I will also present a collection of problems that are computationally equivalent to LWE.

Bibliography

[ABB10] S. Agrawal, D. Boneh, X. Boyen: Efficient Lattice (H)IBE in the Standard Model. EUROCRYPT 2010: 553-572.

[BLPRS13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé: Classical hardness of learning with errors. STOC 2013: 575-584.

[BV11] Z. Brakerski, V. Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106.

[GoVaWe13] S. Gorbunov, V. Vaikuntanathan, H. Wee: Attribute-based encryption for circuits. STOC 2013: 545-554.

[Reg09] O. Regev: On lattices, learning with errors, random linear codes, and cryptography. J. ACM 56(6) (2009).

Time: 10:00 – 11:00, Tuesday, Jan 10, 2017

Speaker: Shweta Agrawal

Title: Interpolating Predicate and Functional Encryption, from Learning With Errors

Abstract:
We construct a functional encryption scheme for circuits which achieves a notion of security that interpolates predicate and functional encryption. Our scheme is secure based on the subexponential learning with errors (LWE) assumption. Our construction simultaneously achieves and improves upon the security of the current best known, and incomparable, constructions from standard assumptions, namely the predicate encryption scheme of Gorbunov, Vaikuntanathan and Wee (CRYPTO 2015) and the reusable garbled circuits scheme of Goldwasser, Kalai, Popa, Vaikuntanathan and Zeldovich (STOC 2013).
Our contributions may be summarized as follows.
1. We show that existing LWE based predicate encryption schemes [AFV11, GVW15] are completely insecure against a general functional encryption adversary (i.e. in the "strong attribute hiding" game). We demonstrate three different attacks, the strongest of which is applicable even to the inner product predicate encryption scheme [AFV11]. Our attacks are practical and allow the attacker to completely recover a from its encryption Enc(a) within a polynomial number of queries. This illustrates that the barrier between predicate and functional encryption is not just a limitation of proof techniques.
2. We provide a new construction that unifies and extends the constructions of Gorbunov et al. [GVW15] and Goldwasser et al. [GTKP$^+$13]. Our construction supports a single "decryption query" as in [GTKP$^+$13] in addition to an unbounded number of "non- decryption queries" as in [GVW15]. In particular, our construction yields an alternate candidate for reusable garbled circuits.
3. We upgrade the security of our construction, as well as [AFV11, GVW15], from selective to semi-adaptive, where the adversary may output the challenge after seeing the public parameters in the security game. Our transformation is generic, and applies to several LWE based selectively secure FE schemes.
4. We generalize the above scheme to support q decryption queries, for any polynomial q which is a-priori fixed. Our ciphertext size is independent of the size of the circuit as against [GVW12], and depends on the number of queries as $O(q^2)$ as against $O(q^4)$ [GTKP$^+$13, GVW12]. However, security is proven in a weaker game as compared to [GVW12].

Time: 11:30 – 12:30, Tuesday, Jan 10, 2017

Speaker: Léo Ducas

Title: Exploiting Quantum Algorithms against Ideal-SVP

Abstract:
Lattice based cryptography is often praised for its resistance to quantum algorithms: even quantum computers should not be able to find short vectors in arbitrary ideals (SVP). Yet, for efficiency reason, it is tempting to rely on special classes of lattices arising from Algebraic Number Theory (ideals, modules).

Recent progress in quantum computing has showed that certain problems over ideals are in fact solvable in quantum polynomial time, such as finding an arbitrary generator of a principal ideal (PIP). Yet solving PIP is not directly sufficient to solve ideal-SVP, in particular those quantum algorithms give no guarantee of the shortness of their outputs.

In this talk, we will give an overview of the notions at play (unit-group, class-group) and show how to exploit those quantum algorithms to find mildly short vectors in ideal lattices. This result in polynomial time quantum algorithm to solve Ideal-SVP for large (sub-exponential) approximations factors. While this does not directly imply the insecurity of any cryptosystem, this shows a quantum hardness gap between generic lattices and ideal ones.

Time: 14:00 – 15:00, Tuesday, Jan 10, 2017

Speaker: Kim Laine

Title: String Matching on Homomorphically Encrypted Data

Abstract:

In this talk I will discuss the problem of string matching on homomorphically encrypted data, leading to a surprisingly efficient protocol for privately querying homomorphically encrypted datasets. As a concrete demonstration, I will discuss the performance of this protocol on the homomorphic encryption challenge in the 2016 iDASH Secure Genome Analysis competition. Time permitting, I will present other promising applications and future research directions.

Wednesday, January 11, 2017
Communication Complexity

09:00 - 10:00	Arkadev Chattopadhyay Composition and Simulation Theorems via Pseudo-random properties
10:00 - 11:00	Rahul Jain Separations in communication complexity using cheat sheets and information complexity
	Coffee Break
11:30 - 12:30	Or Meir Toward the KRW conjecture: Cubic Formula Lower Bounds via Communication Complexity
	Lunch
14:00 - 15:00	Sourav Chakraborty Communication Complexity and connection to Lower Bounds in Property Testing
15:00 – 16:00	Jaikumar Radhakrishnan Communication assisted agreement distillation

Abstracts

Time: 09:00 – 10:00, Wednesday, Jan 11, 2017
Speaker: Arkadev Chattopadhyay
Title: Composition and Simulation Theorems via Pseudo-random properties.

Abstract:

We generalize the deterministic simulation theorem of Raz and McKenzie (1999), to any inner-function which satisfies a certain hitting property. We prove that Inner-Product (IP) satisfies this property, and as a corollary we obtain deterministic simulation theorem for an inner-function gadget with logarithmic block-size with respect to the arity of the outer function. This answers an open question posed by Goos, Pitassi and Watson (2015).

Our result also implies the previous results for the Indexing inner-function.S

We consider a natural strengthening of the hitting property used above that is also satisfied by IP. We conjecture that this strengthened property is sufficient to prove a randomized simulation theorem. Such simulation theorems are not known. We prove a randomized communication-complexity lower bound for the composed function --- OrderedSearch o IP --- by lifting the randomized query-complexity lower-bound of OrderedSearch to the communication-complexity setting by using the above pseudo-random properties and other things. To do this, we extend ideas from a paper of Raz and Wigderson (1989). We think that the techniques we develop will be useful in proving a randomized simulation theorem.

This is joint work with Michal Koucky, Bruno Loff and Sagnik Mukhopadhyay.

Time: 10:00 – 11:00, Wednesday, Jan 11, 2017
Speaker: Rahul Jain
Title: Separations in communication complexity using cheat sheets and information complexity.
Abstract:
While exponential separations are known between quantum and randomized communication complexity for partial functions (Raz [1999]), the best known separation between these measures for a total function is quadratic, witnessed by the disjointness function. We give the first super-quadratic separation between quantum and randomized communication complexity for a total function, giving an example exhibiting a power 2.5 gap. We further present a 1.5 power separation between exact quantum and randomized communication complexity, improving on the previous (approximately) 1.15 separation by Ambainis [2013]. Finally, we present a nearly optimal quadratic separation between randomized communication complexity and the logarithm of the partition number, improving upon the previous best power 1.5 separation due to Goos, Jayram, Pitassi, and Watson [2015].

Our results are the communication analogues of separations in query complexity proved using the recent cheat sheet framework of Aaronson, Ben-David, and Kothari [2016]. Our main technical results are randomized communication and information complexity lower bounds for a family of functions, called lookup functions, that generalize and port the cheat sheet framework to communication complexity.

Time: 11:30 – 12:30, Wednesday, Jan 11, 2017
Speaker: Or Meir
Title: Toward the KRW conjecture: Cubic Formula Lower Bounds via Communication Complexity

Abstract:

One of the major challenges of the research in circuit complexity is proving super-polynomial lower bounds for de-Morgan formulas. Karchmer, Raz, and Wigderson suggested to approach this problem by proving that formula complexity behaves “as expected” with respect to the composition of functions. They showed that this conjecture, if proved, would imply super-polynomial formula lower bounds.

In this talk, I will present the background on this conjecture and the known results I will then describe a new proof of the special case where the inner function is the parity function. While this special case was already known to follow from a work of Hastad, our proof seems to be more generalizable for other cases.

Joint work with Irit Dinur.

Time: 14:00 – 15:00, Wednesday, Jan 11, 2017

Speaker: Sourav Chakraborty
Title: Communication Complexity and connections to Lower Bounds in Property Testing

Abstract:
Property testing is the subject of designing sub-linear algorithms for testing whether a given input satisfies a given property or is ``far'' from satisfying the property. As with any field of theoretical computer science proving lower bounds is a challenging task. The use of communication complexity for lower bounds in property testing started with the paper of Blais-Brody-Matulef in which they gave a lower bound on the query complexity for distinguishing a k-junta from a (k+2)-junta, when the queries are made to the truth-table of the function. Since then the connection between property testing and communication complexity has got stronger over the years with lot more lower bounds of query complexity being obtained through the use of communication complexity. We will be looking at some of the classic works in this area and also present a lower bound result (using communication complexity) for testing whether a Boolean function is a Bent function.

Time: 15:00 – 16:00, Wednesday, Jan 11, 2017
Speaker: Jaikumar Radhakrishnan
Title: Communication assisted agreement distillation
Abstract:
Bogdanov and Mossel (2011) consider the following problem.
"Suppose Alice receives a string of unbiased independent random bits and Bob receives a noisy copy of the same bits, where each bit is flipped with probability eps < 1/2. Alice and Bob wish to extract a common sequence of k random bits."
We study the relationship between communication and the probability of agreement. Suppose Alice wishes to send Bob a message of delta k bits in order to ensure that their k-bit outputs agree with probability 2^{-gamma k}. How big must delta be as a function of gamma? We show the following:

delta(gamma) >= C (1-gamma) - 2 sqrt{C(1-C) gamma},

where C = 4 eps (1-eps).
This implies that that for delta(gamma) = 0, we have gamma >= eps/(1-eps), recovering the original result of Bogdanov and Mossel.
In this talk, we will describe the above trade-off, which is based on the standard hypercontractivity inequality.
We also obtain strategies that show that this trade-off between communication and the probability of error is asymptotically tight.

(This is part of joint work with Venkat Guruswami.)

Thursday, Jan 12, 2017

	Algorithms ⇔ Lower Bounds
09:00 - 10:00	Rahul Santhanam The Minimum Circuit Size Problem and its Complexities
10:00 - 11:00	Srikanth Srinivasan The Polynomial method for lower bounds and algorithms
	Coffee Break
11:30 - 12:30	Discussions
	Lunch
	Homomorphic Secret Sharing
14:00 - 15:00	Yuval Ishai **Homomorphic Secret Sharing, Part I:** Homomorphic Secret Sharing for Branching Programs from DDH
15:00 - 16:00	Elette Boyle **Homomorphic Secret Sharing, Part II:** Group-Based Secure Computation: Optimizing Rounds, Communication, and Computation
	Coffee Break
16:30 - 17:30	Niv Gilboa **Homomorphic Secret Sharing, Part III:** Function Secret Sharing from One-Way Functions

Abstracts

Time: 09:00 – 10:00, Thursday, Jan 12, 2017

Speaker: Rahul Santhanam

Title: The Minimum Circuit Size Problem and its Complexities

Abstract:
Recent work in complexity theory has emphasized the links between complexity lower bounds and algorithmic problems such as circuit satisfiability, derandomization and learning. An important computational problem in this connection is the Minimum Circuit Size Problem (MCSP), where the input is the truth table of a Boolean function and the question is whether the function has small circuits.

MCSP belongs to NP, but it and its variants have several unusual and interesting features, which distinguish it from other natural problems in NP. I will discuss these features, survey previous work on the problem, and explain the relevance of MCSP to circuit lower bounds, learning and natural proofs.

Time: 10:00 – 11:00, Thursday, Jan 12, 2017

Speaker: Srikanth Srinivasan

Title: The Polynomial method for lower bounds and algorithms

Abstract:
The polynomial method has long been used to prove lower bounds for certain classes of circuits (Razborov, Smolensky). More recently, Ryan Williams and others have shown how to exploit this method for designing algorithms as well. This talk will illustrate both lower bound and algorithmic results via polynomials.

Time: 14:00 – 15:00, Thursday, Jan 12, 2017

Speaker: Yuval Ishai

Title: **Homomorphic Secret Sharing, Part I:** Homomorphic Secret Sharing for Branching Programs from DDH

Abstract:

The talk will be the first of a sequence of 3 talks (the other two will be given by Elette Boyle and Niv Gilboa).

Fully homomorphic encryption (FHE) is a powerful cryptographic tool that can be used to minimize the communication complexity of secure computation protocols. However, known FHE schemes rely on a relatively narrow set of assumptions and algebraic structures that are all related to lattices. Moreover, the efficiency of known FHE schemes still leaves much to be desired.

We present a new technique for succinct secure computation that replaces FHE by ''homomorphic secret sharing'' and can be based on discrete-log-type assumptions. More concretely, under the Decisional Diffie-Hellman (DDH) assumption, we construct a 2-out-of-2 secret sharing scheme that supports a compact evaluation of branching programs on the shares. We use this to obtain succinct secure computation protocols for branching programs and other new DDH-based applications that previously required FHE.

Joint work with Elette Boyle and Niv Gilboa

Time: 15:00 – 16:00, Thursday, Jan 12, 2017

Speaker: Elette Boyle

Title: **Homomorphic Secret Sharing, Part II:** Group-Based Secure Computation: Optimizing Rounds, Communication, and Computation

Abstract:

We further explore the power of "group-based" cryptographic protocols, namely ones that only rely on a cryptographically hard (Abelian) group. Our results build on the recent DDH-based construction of homomorphic secret sharing for branching programs, improving the asymptotic and concrete efficiency of protocols that employ this construction along several dimensions.

In this talk, I will focus on one such result: optimizing protocol round complexity. For any constant number of parties, we obtain 2-round MPC protocols based on a PKI setup under the DDH assumption. Prior to our work, such protocols were only known using fully homomorphic encryption or indistinguishability obfuscation.

We also briefly discuss some optimizations in communication and computation complexity, which in turn yield the first constant-rate oblivious transfer protocol under DDH, as well as concrete efficiency improvements of several orders of magnitude.

Joint work with Niv Gilboa and Yuval Ishai

Literature pointer: partially based on Crypto 2016 paper, mostly on a yet-unpublished work

Time: 16:30 – 17:30, Thursday, Jan 12, 2017

Speaker: Niv Gilboa

Title: **Homomorphic Secret Sharing, Part III:** Function Secret Sharing from One-Way Functions

Abstract:

Function secret sharing (FSS) is a secret sharing scheme for functions. More concretely, the goal of FSS is to split a function f from a function family F into succinctly described f_1,...,f_m, such that f(x)=f_1(x)+...+f_m(x) for every input x, and every strict subset of the f_i computationally hides f. FSS can be viewed as a dual version of homomorphic secret sharing, where the roles of the function and input are reversed.

FSS schemes that are based on one-way functions are desirable theoretically, with the aim of basing security on the weakest possible requirements, and practically, enabling the use of fast symmetric-key primitives such as AES. Two interesting function families that admit FSS schemes from one-way functions are the family of point functions and the family of decision trees.

Applications of FSS for point functions include private retrieval from databases, anonymous messaging and worst case to average case reductions for languages in PSPACE and EXPTIME. Applications of FSS for decision trees include a wider class of private database queries, such as range queries or products of ranges. For input domain {0,1}^n and security parameter k, we show a two-party FSS scheme for point functions with query length O(nk) and a two-party FSS scheme for decision trees with query length O(Tk) for a tree of size T. We show multi-party FSS schemes for both function families with query length a square root of the trivial FSS scheme.

We round up the talk by considering the case of FSS schemes in the presence of malicious clients, and construct verifiable FSS schemes, identifying malicious queries, for point functions and related function families. The schemes are black box, require minimal interaction between the servers and add constant overhead to the computational complexity of FSS applications.

Joint work with Elette Boyle and Yuval Ishai

Friday, January 13, 2017
Partition Functions, Polynomials, and Optimization

09:00 - 10:00	Piyush Srivastava An introduction to approximate counting
10:00 - 11:00	Amit Deshpande Determinantal Point Processes (algorithms and applications)
	Coffee Break
11:30 - 12:30	Piyush Srivastava Approximate counting, correlation decay, and zeros of partition functions
	Lunch
14:00 - 15:00	Nisheeth Vishnoi Convex Programming Approaches for the Permanent
15:00 - 16:00	Nisheeth Vishnoi Real Stable Polynomials and Gurvits' Inequality
	Coffee Break
16:30 - 17:30	Damian Straszak Real Stable Polynomials and Computing Partition Functions

Abstracts

Speaker: Piyush Srivastava

Talk 1: 09:00 – 10:00, Friday, Jan 13, 2017
Title: An introduction to approximate counting
Abstract:
This talk will introduce approximate counting via some of the classical examples of such problems, many of which will be developed in greater detail in the other talks in the workshop. These examples will include combinatorial problems such as the counting of matchings and independent sets in graphs and the approximate computation of the permanent. We will also see the connections that these problems have with statistical mechanics where they are known under the name of the computation of the partition function, and see examples such as the Ising model that arose first in that context.
We will then look at the variety of algorithmic techniques that have been brought to bear upon these problems: Markov chain Monte Carlo, correlation decay, and more recently, the stability theory of polynomials. The starting point of many of these techniques is the classical relationship between approximate counting and approximate sampling: an idea that we will look at in some detail. We will also discuss the origins of some of these techniques from ideas in statistical mechanics.

Talk 2: 11:30 -- 12:30, Friday, Jan 13, 2017
Title: Approximate counting, correlation decay, and zeros of partition functions
Abstract:
The location of (complex) zeros of generating functions of combinatorial objects (such as matchings in graphs) has been a classical topic of study in statistical physics and combinatorics, starting with the work of Lee and Yang in the 1950s. More recently, starting with ideas of Scott and Sokal and of Barvinok, there has been progress on using information on the location of such zeros to design algorithms for approximate counting. In particular, these results include efficient approximate computation of the generating function of independent sets (known as the hard core partition function in statistical mechanics) at *negative* values of the parameter. Via classical results of Shearer and Scott and Sokal these latter values represent the best possible "probability of success" that can be guaranteed by the Lovasz local lemma.
This talk will survey the background, the high level ideas, and the techniques underlying some of these results.

Time: 10:00 – 11:00, Friday, Jan 13, 2017
Speaker: Amit Deshpande
Title: Determinantal Point Processes (algorithms and applications)
Abstract:
Determinantal Point Processes (DPPs) are probabilistic models of repulsion that originated in quantum physics and random matrix theory, with recent applications in computer science and machine learning. DPPs define distributions over subsets of a given ground set, and exhibit interesting properties such as negative correlation. In this talk, I will start by explaining important properties of DPPs that lead to their efficient algorithmic applications. Towards the end, I'll mention their relations to deeper mathematical problems on mixed discriminants as well as their practical variants useful in the study of diversity and fairness in subsampling data.
Joint work with Elisa Celis, Tarun Kathuria, Damian Straszak, and Nisheeth Vishnoi.

Time: 14:00 – 16:00, Friday, Jan 13, 2017
Speaker: Nisheeth Vishnoi:
Titles and Abstracts:

Talk 1: Convex Programming Approaches for the Permanent
In this talk I will survey some recent convex programming based approaches to estimate the permanent of a nonnegative matrix and show interconnections between them.
Based on joint work with Damian Straszak

Talk 2: Real Stable Polynomials and Gurvits' Inequality
In this talk I will present a proof of the influential inequality by Gurvits which is used to obtain the approximation ratio in one of the convex-programming based estimation algorithm for the permanent. The proof will be self-contained and rely on the theory of real stable polynomials that will be introduced.

Time: 16:30 – 17:30, Friday, Jan 13, 2017

Speaker: Damian Straszak

Title: Real Stable Polynomials and Computing Partition Functions

Abstract: In this talk I will present some new results on counting and optimization problems in a fairly general model where an oracle access to a polynomial is given and the goal is to compute a certain sum of its coefficients or find the maximum coefficient subject to constraints. We introduce a new convex programming relaxation to solve these problems and show that it provides decent estimates whenever the input polynomial is real stable and the constraints are matroidal.

Based on joint work with Nisheeth K. Vishnoi