

「Private Information Retrieval: Coding Instead of Replication」

講演者: Professor Alexander Vardy
University of California, San Diego

日時: 平成29年9月1日(金) 16:15~18:15

場所: 情報科学系講義棟2階 13・4講義室

講演要旨:

Private information retrieval protocols allow a user to retrieve a data item from a database without revealing any information about the identity of the item being retrieved. Specifically, information-theoretic k -server PIR, the database is replicated among k non-communicating servers, and each server learns nothing about the item retrieved by the user. The effectiveness of PIR protocols is usually measured in terms of their communication complexity, which is the total number of bits exchanged between the user and the servers. However, another important cost parameter is the storage overhead, which is the ratio between the total number of bits stored on all the servers and the number of bits in the database. Since single-server information-theoretic PIR is impossible, the storage overhead of all existing PIR protocols is at least 2 (or k , in the case of k -server PIR).

In this work, we show that information-theoretic PIR can be achieved with storage overhead arbitrarily close to the optimal value of 1, without sacrificing the communication complexity. Specifically, we prove that all known k -server PIR protocols can be efficiently emulated, while preserving both privacy and communication complexity but significantly reducing the storage overhead. To this end, we distribute the n bits of the database among $s+r$ servers, each storing n/s coded bits (rather than replicas). Notably, our coding scheme remains the same, regardless of the specific k -server PIR protocol being emulated. For every fixed k , the resulting storage overhead $(s+r)/s$ approaches 1 as s grows; explicitly we have $r < k \sqrt{s}(1 + o(1))$. Moreover, in the special case $k = 2$, the storage overhead is only $1 + (1/s)$.

In order to achieve these results, we introduce and study a new kind of binary linear codes. We call them k -server PIR codes, although they could be also called "availability codes". We then show how such codes can be constructed from Steiner systems, from one-step majority-logic decodable codes, from constant-weight codes, and from certain locally recoverable codes. We also establish several bounds on the parameters of k -server PIR codes, and tabulate the results for all $s \leq 32$ and $k \leq 16$.

講演者略歴:

Alexander Vardy (S'88-M'91-SM'94-F'99) was born in Moscow, U.S.S.R., in 1963. He earned his B.Sc. (summa cum laude) from the Technion—Israel Institute of Technology, in 1985, and Ph.D. from the Tel-Aviv University, Israel, in 1991. During 1985—1990 he was with the Israeli Air Force, where he worked on electronic counter measures systems and algorithms. During the years 1992 and 1993 he was a Visiting Scientist at the IBM Almaden Research Center, in San Jose, CA. From 1993 to 1998, he was with the University of Illinois at Urbana-Champaign, first as an Assistant Professor then as an Associate Professor. He is now a Professor in the Department of Electrical Engineering, the Department of Computer Science, and the Department of Mathematics, all at the University of California San Diego (UCSD). While on sabbatical leave from UCSD, he has held long-term visiting appointments with the Centre National de la Recherche Scientifique (CNRS), Sophia-Antipolis, France, the École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, and the Technion, Israel.

参加申込・予約は不要です。直接会場にお越しください。

お問合せ先: 共通事務管理課共通事務第二係 (E-mail: is-secr)