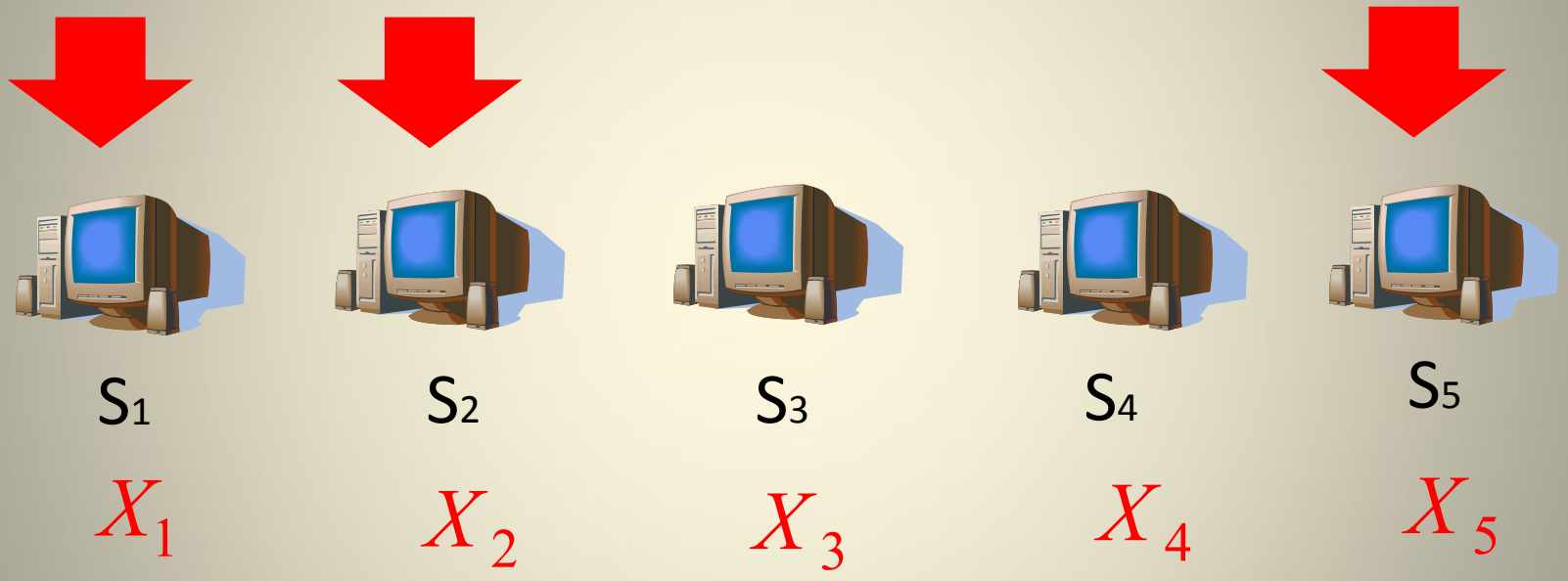
Seminar in Cryptography: research projects

Vitaly Skachek

Institute of Computer Science
University of Tartu

vitaly.skachek (at) ut.ee

Private information retrieval using linear codes



- **S. Blackburn and T. Etzion,** "PIR Array Codes with Optimal PIR rate", http://arxiv.org/pdf/1607.00235.pdf
- **A. Fazeli, A. Vardy, and E. Yaakobi**, "PIR with Low Storage Overhead: Coding instead of Replication", available at http://arxiv.org/abs/1505.06241.

PIR protocols:

- Computational PIR
- Information-theoretic PIR

Results:

- Constructions
- Bounds on the parameters

McEliece Cryptosystem
(assymetric cryptosystem, 1978)

Alice:

- Efficient error-correcting code with generator matrix G that corrects t errors
- Random k x k matrix S
- Random n x n permutation matrix P
- Transmits $F = SGP$ (public key)

McEliece Cryptosystem

Bob:

- Encodes the message m as $s = mF + r$, where r is a random vector with t nonzero symbols

Alice:

- Computes sP^{-1}
- Decodes the result (removes r)
- Multiplies by S^{-1} from the left

McEliece Cryptosystem

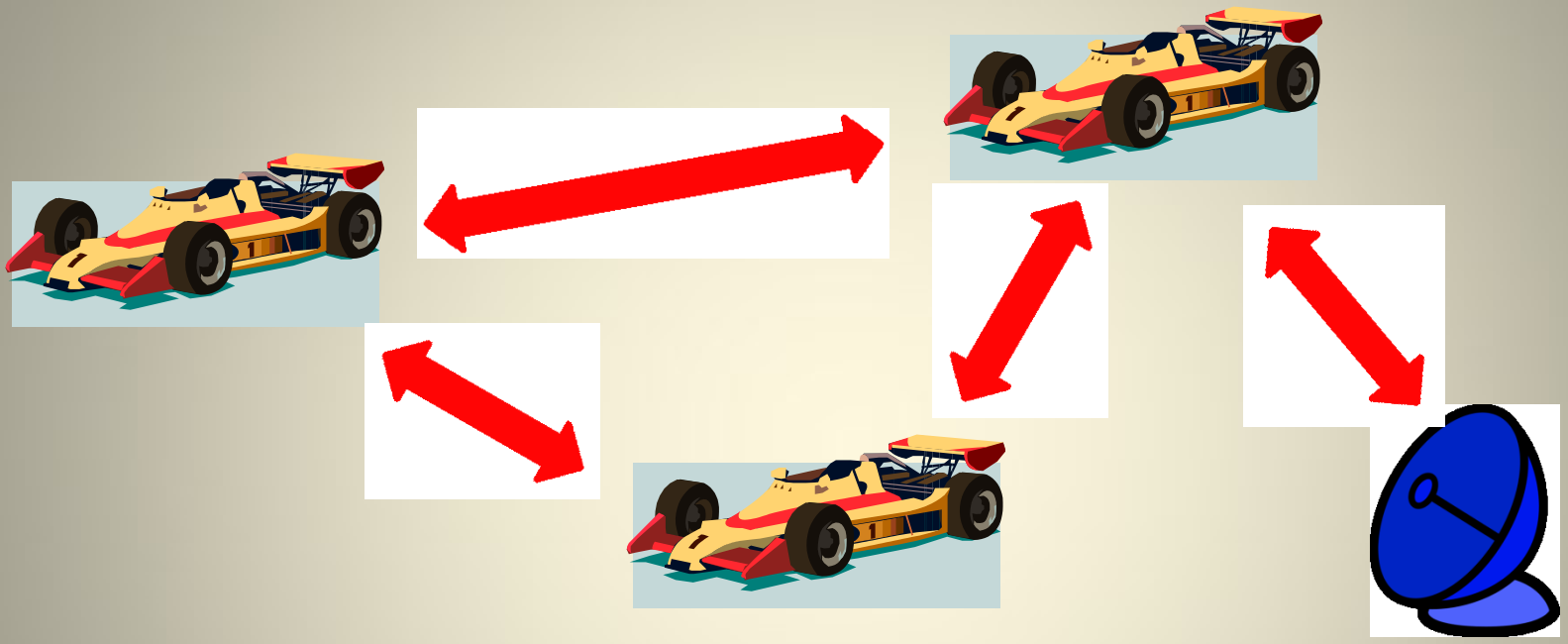
- Original paper uses Goppa codes
- What about LDPC codes? Can they be used in the cryptosystem. Where is the weakness? How this can be repaired?

- M. Baldi, M. Bodrato, F. Chiaraluce, "A New Analysis of the McEliece Cryptosystem Based on QC-LDPC Codes", Volume 5229, Lecture Notes in Computer Science, pp. 246-262.
- M. Baldi, „LDPC codes in the McEliece cryptosystem: attacks and countermeasures“.

Security of vehicle communications

- Future roads
- V2V and V2I communications
- Security concerns

Security of vehicle communications



- Tim Leinmüller et al., *"Sevecom-secure vehicle communication“*
- Rens van der Heijden, "*Security Architectures in V2V and V2I Communication"*

Vitaly Skachek

Institute of Computer Science
University of Tartu

vitaly.skachek (at) ut.ee