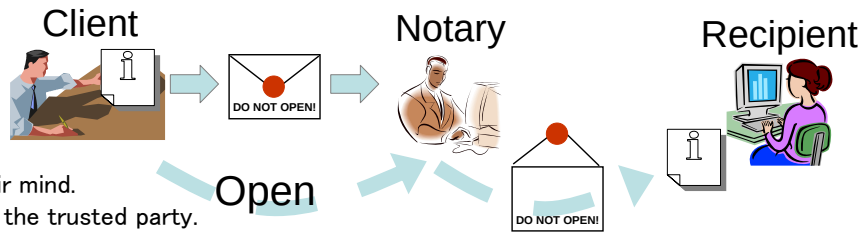
Information-Theoretically Secure Commitment Based on Noisy Channel

KIRILL MOROZOV (Research Team for Physical Analysis, RCIS, AIST)

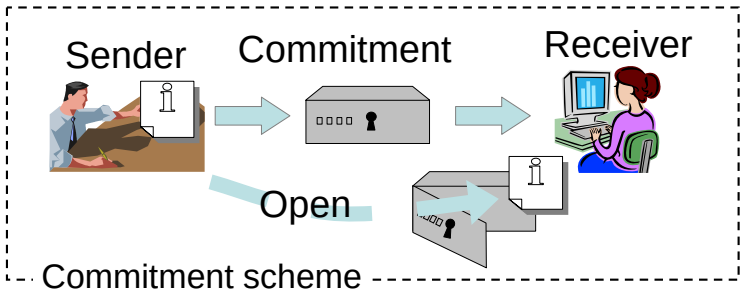
Example: A notary holds a note made by his client. The notary does not disclose it without the client's will. Also, the notary guarantees that the client does not change his mind later.

Problem: The notary may disclose the note at any time or may help his client to change their mind. From security point of view, it is better to avoid the trusted party.

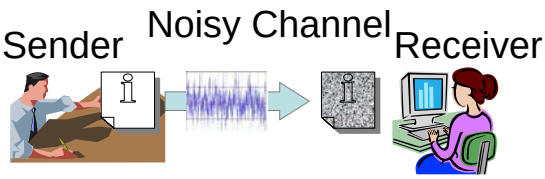


Commitment is a scheme where a sender locks his message into a virtual depository box and passes it on to the receiver who cannot open it himself. Later in time, the sender may open the box but he will not be able to change his mind and open something else.

Cryptographic Applications: electronic voting, electronic payments, secure computation, zero-knowledge proofs, etc.



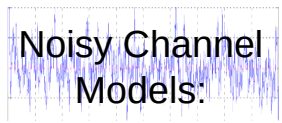
Information-Theoretic Security Using Noise. Any communication channel has noise. Engineers fight noise to improve quality of service, but cryptographers can use it to increase security!
Information-theoretic security guarantees that the cheater has only a very little chance to succeed. Since some information is lost to noise, no computer can possibly recover it (even if it has all the time of the universe).
This means virtually everlasting protection – a good solution for long-term security.



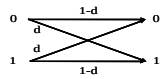
Research Objectives: To choose an adequate noise model, to utilize it to build a secure commitment scheme, and to assess how efficiently the scheme uses the noise.

Previous works: Constructions from binary symmetric channel (BSC), discrete memoryless channel (DMC), and channel with additive white Gaussian noise (AWGN). Introducing *bit commitment capacity*. The main objective is to use as realistic model as possible.

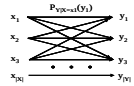
Research aspiration: 1) Investigate the case of channels with fading and memory – for wireless setting; 2) Investigate the case of "unfair" Gaussian channel – when the cheater has partial control over the channel noise. Need to know when bit commitment with unconditional security is possible in such setting, and what is the commitment capacity of such the channel



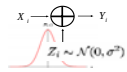
BSC – binary input/output (i/o)



DMC – finite i/o alphabets



AWGN – continuous i/o



Selected references:

1. C. Crepeau, Efficient Cryptographic Protocols Based on Noisy Channels, Proc. EUROCRYPT '97, LNCS 1233, pp. 306--317, 1997.
2. A. Winter, A. C. A. Nascimento, H. Imai, Commitment Capacity of Discrete Memoryless Channels, Proc. 9th IMA ICCC, LNCS 2898, pp. 35--51, 2003.
3. J. Barros, H. Imai, A.C.A Nascimento, S. Skudlarek, Bit Commitment over Gaussian Channels, Proc. ISIT '06, pp. 1437-1441, 2006.
4. Frederique Oggier, K.M., A Practical Scheme for String Commitment based on the Gaussian Channel, Proc. ITW' 08, pp. 328-332, 2008.

Impact to Society: The answer to the these research questions will enable us to implement *a real hardware prototype* for information-theoretically secure bit commitment which is the ultimate goal of our research