# 10th Central European Conference on Cryptology

# Committing with partial knowledge of group order

Vadym Fedyukovych

Commitment schemes. Binding and hiding properties. Discrete Logarithm and Decisional Diffie-Hellmann problems.

Pedersen commitment scheme for element of $\mathbb{Z}_q$ for a prime $q$. Homomorphic property of commitment scheme and proof of knowledge protocol with negligible error.

Integer commitment scheme anf groups of order that is unknown to committing party. Computationally binding on assumption of unknown group order. Computationally hiding on assumption of Discrete Logarithm problem.

Problem of generating and testing committment scheme parameters.

Setup with no trusted parties. Option to generate commitment scheme parameters by either committing or receiving party.
Achieving either binding or hiding properties.

It was observed that each party wants to generate parameters yourself to not let the other party to choose weak parameters.

Both parties can contribute to choosing parameters.
Each party can choose two prime numbers and output the product.
Parties compute in a ring of residue classes modulo 4 primes.

Meeting interests of both parties by joint generation of commitment scheme parameters with groups of partially known order.

Thank you! Questions?

About the author: interactive proof systems (protocols) for approximate matching, codeword of Goppa code and upper bound on error weight, graph isomorphism and Hamiltonicity, multiple substring matching.
`http://vf.org.ua/`

Research started while visiting National University of Singapore.