Asymmetric Cryptosystem Using Careful Synchronization

Jakub Ruszil
Jagiellonian University
Cracow
Poland

February 2023

Abstract

We present public-private key cryptosystem which utilizes the fact that checking whether a partial automaton is carefully synchronizing is $PSPACE$-complete, even in the case of a binary alphabet.

1 Introduction

Cryptography is essential branch of mathematics since the ancient times. It's main purpose is to ensure the privacy of information between sender and receiver sent through a possibly observed channel. Nowadays we differ symmetric cryptography - where the key used to cipher the message is the same as the one to decipher it - and asymmetric, where the key to cipher the message is commonly known and the one to decipher it is known only to the receiver of the message. In other words asymmetric cryptography is referred to as a public key cryptography, or a public-private key cryptography. The idea of public key cryptography was first mentioned in a confidential report GCHQ [4] (UK Government Communications Headquarters) and later independently by Diffie and Hellman in 1976 [27] along with the first practical public key cryptosystem based on knapsack problem. The mostly known asymmetric cryptosystem (RSA) was invented by Rivest, Shamir and Adleman in 1978 [17] and is applicable since then to encryption and digital signatures.

The concept of synchronization of finite automata is essential in various areas of computer science. It consists in regaining control over a system by applying a specific set of input instructions. These instructions lead the system to a fixed state no matter in which state it was at the beginning. The idea of synchronization has been studied for many classes of complete deterministic finite automata (DFA) [1, 2, 5, 9, 10, 16, 18, 20, 23, 22, 24, 25] and non-deterministic