Автор: д.т.н. Рябко Б.Я.

Безусловно надежный («невскрываемый») шифр с небольшим секретным ключом, основанный на сжатии данных и рандомизации

В середине прошлого века К.Шеннон описал совершенные (т.е. «абсолютно невскрываемые») шифры с секретным ключом и показал, что у них длина ключа (т.е. слова в некотором алфавите) должна быть равна длине шифруемого сообщения, что существенно ограничивало сферу их применения. 20 лет назад были открыты классы «энтропийно-невскрываемых» шифров, свойства которых практически совпадали с совершенными, а длина секретного ключа была существенно меньше - пропорциональна (с небольшим коэффициентом) длине сообщения. В настоящей работе описано семейство энтропийно-невскрываемых шифров, длина секретного ключа у которых не зависит от длины сообщения [1,2]. Эти шифры используют методы «сжатия данных» и рандомизации, которые являются в некотором смысле противоположными – первые сокращают длину сообщения, а вторые-увеличивают. Возможно, эта парадоксальность подхода и позволила решить известную проблему. Отметим, что предложенные шифры могут найти широкое применение в системах защиты информации.

Публикации:

1. *Ryabko B.* Unconditionally secure short key ciphers based on data compression and randomization // Des. Codes Cryptogr. 2023. https://doi.org/10.1007/s10623-023-01195-8.
2. *Ryabko B.* Using data compression and randomisation to build an unconditionally secure short key cipher // 2022 IEEE Information Theory Workshop (ITW), Mumbai, India, 1-2 and 6-9 November.

Безусловно надежный («невскрываемый») шифр с небольшим секретным ключом, основанный на сжатии данных и рандомизации.

Автор: д.т.н. Рябко Б.Я.

В середине прошлого века К.Шеннон описал совершенные («абсолютно невскрываемые», что математически доказано) шифры с секретным ключом и показал, что у них длина ключа (т.е. слова в некотором алфавите) должна быть равна длине шифруемого сообщения, что существенно ограничивало сферу применения таких шифров. 20 лет назад были открыты классы «энтропийно-невскрываемых» шифров, свойства которых практически совпадали с совершенными, а длина секретного ключа была существенно меньше – пропорциональна (с небольшим коэффициентом) длине сообщения. Недавно удалось преодолеть и этот барьер: в 2022-2023 автором было описано семейство энтропийно-невскрываемых шифров, длина секретного ключа у которых не зависит от длины сообщения, см. [1,2]. Эти шифры используют методы «сжатия данных» и рандомизации, что довольно парадоксально – первые сокращают длину сообщения, а вторые – увеличивают. Возможно, эта парадоксальность подхода и позволила решить довольно известную проблему.

В 2022-2023 автором впервые в литературе было описано семейство «доказанно невскрываемых» шифров, у которых длина секретного ключа не зависит от длины шифруемого сообщения [1,2].

Разработкой «доказанно невскрываемых» шифров занимаются сотни исследователей во всем мире, однако автором впервые построены методы шифрования, для которых длина секретного ключа не зависит от длины сообщения. Предложенные могут найти широкое применение в системах защиты информации.

ПУБЛИКАЦИИ:

1. *Ryabko B.* Unconditionally secure short key ciphers based on data compression and randomization // Des. Codes Cryptogr. 2023. https://doi.org/10.1007/s10623-023-01195-8

2. *Ryabko B.* Using data compression and randomisation to build an unconditionally secure short key cipher //2022 IEEE Information Theory Workshop (ITW), Mumbai, India, 1-2 and 6-9 November.