

Представлена симетрична криптографія для шифрування і розшифровки інформації яка може бути ефективним чином реалізована апаратним або програмним способом. Симетрична криптографія використовує генератор ключів так, щоб криптографія не залежала від одного статичного криптографічного ключа. Генератор ключів являє собою величину або набір величин, з яких генерується перший ключ. Генератор ключів істотно збільшує обчислювальну складність диференційного криптоаналізу і інших криптографічних атак. В одному з прикладів здійснення винаходу генератор ключів оновлюється з використанням односторонніх функцій, що демонструють лавинний ефект, який створює непередбачувану послідовність ключів, які використовуються в процесі шифрування або розшифрування. В одному з прикладів здійснення винаходу динамічний ключ отримують з генератора ключів за допомогою односторонньої функції хешування. В одному з прикладів здійснення винаходу блоковий шифр використовує різні динамічні ключі для шифрування кожного блоку звичайного тексту, де кожен ключ отримують з різного генератора ключів.