expist® IoTA

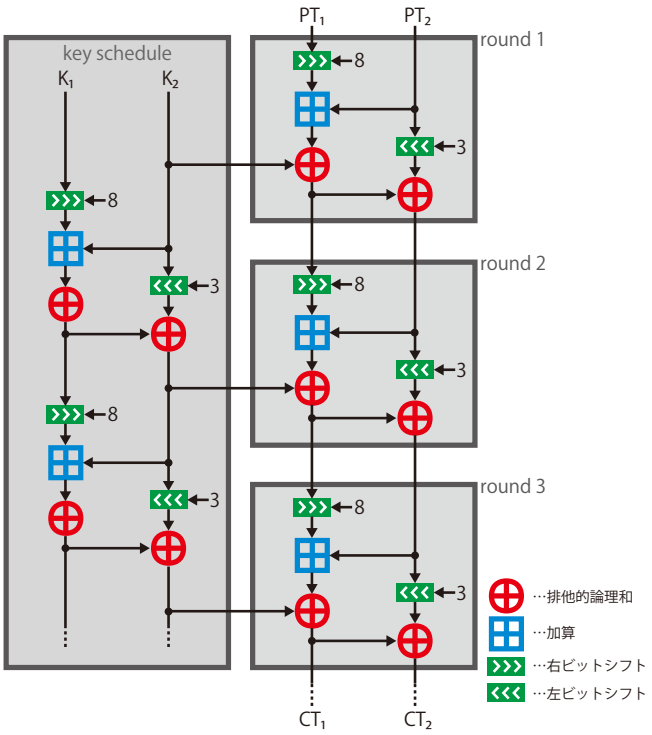
軽量暗号とは？

軽い ≠ 暗号強度が弱い

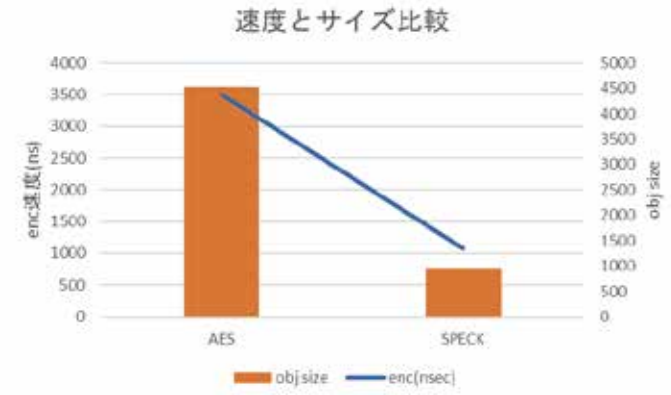
軽量暗号とは、リソース制約が存在するデバイスに実装可能な暗号技術です。ソフトウェア実装による軽量暗号軽量とは実装に必要なメモリサイズが少ない点が特徴で、暗号強度が十分強いアルゴリズムも存在します。決して軽量暗号イコール暗号強度が弱いというわけではありません。

IoTA で採用している軽量暗号

IoTA はアメリカ国家安全保障局が 2013 年に発表した SPECK 軽量暗号を採用しています。
SPECK はソフトウェア上で動作する暗号アルゴリズムの一種であり、少ないリソースでも強力な暗号処理を実現できる利点があります。多くの共通鍵暗号と同じように SPECK も平文を鍵長のブロックに分けて暗号化処理を行いますが、その処理は排他的論理和と加算、シフトのみから構成されるため、
専用ハードウェアや複雑な CPU 命令を必要とせず高速な動作が可能です。コネクテッドカーや医療機器、スマートメーター等さまざまなデバイス機器に導入することが可能です。



SPECK と AES の比較



左の図は、SPECK と現在一般的に使用されている共通鍵暗号である AES を、Raspberry Pi ZERO W 上で評価した結果になります (SPECK/AES 共に鍵長 256bit)。オブジェクトサイズにして約 1/4、暗号処理速度において約 3.5 倍、SPECK が優れていることがグラフから読み取れます。