

Generation of Physical Random numbers

物理乱数生成技術の開発

NEW

独自乱数発生理論により小型パッケージ化した物理乱数生成ICを開発中。試作ICにてFIPS規格を十分に満足できる実力を確認しており、2003年春に汎用、高速、高品位の物理乱数生成ICのサンプル出荷を予定しております。また、物理乱数を用いた応用製品も順次開発して参ります。

物理乱数とは

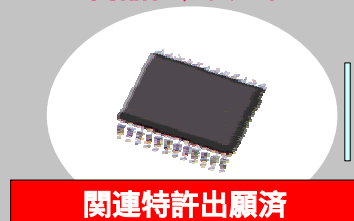
乱数とはランダムな値の配列であり、疑似乱数（算術乱数）と物理乱数（自然乱数）があります。疑似乱数はソフトウェアや固定的なロジック等により生成される為、乱数の周期やパターンが予測される可能性があります。物理乱数は自然界のランダムな現象を用いて生成されるので、周期性やパターンが無く乱数を予想することが出来ません。

物理乱数の優位性と開発経緯

乱数は通信や金融等各分野で利用されており、暗号生成源等現代の情報化社会における安全とセキュリティ確保に必要不可欠な要素であります。予測困難な物理乱数を利用すれば、応用分野の安全とセキュリティが飛躍的に強化されますが、現在は小型で低コスト、高速、高品位の物理乱数デバイスが手軽に入手できない為に、疑似乱数が多く用いられております。

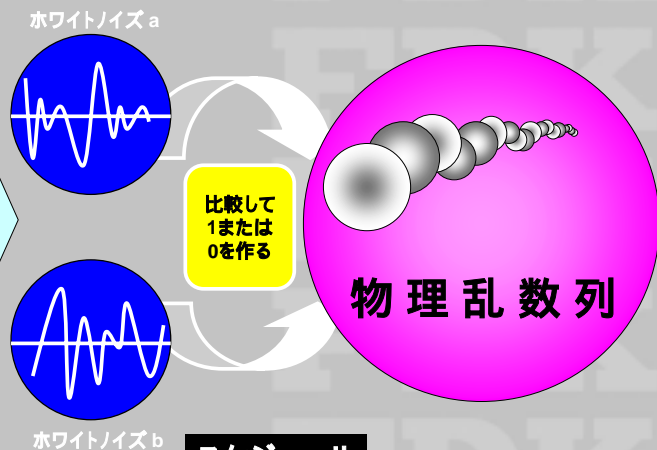
汎用物理乱数生成IC

超小型、低コスト、高速、
高品位、安全性



関連特許出願済

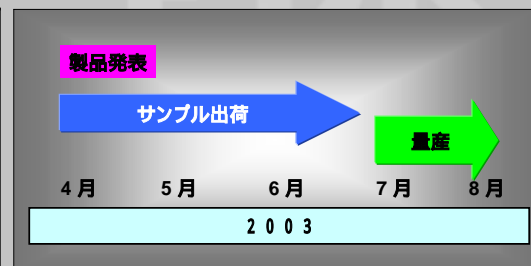
基本イメージ



仕様

乱数源	半導体内部熱雑音
生成速度	~250 KBit / Sec
乱数出力	16 Bit ^パ ラレル / 1Bit ^シ リアル
乱数品位	FIPS140 規格
パッケージ	SSOP 24Pin、鉛フリー対応
定格電圧	3.3 V

スケジュール



用途

・携帯電話、無線LAN、ブルートゥース機器、ゲーム機、スマートカード、セキュリティ関係「ホームセキュリティ」、「カーセキュリティ」、「入室管理」・・・その他 多数

(注) 物理乱数パテント使用についても、ご相談にのります。弊社営業担当にご相談下さい。

当カタログの記載内容は、改良のため予告なく変更することや、製造を中止する事があります。ご注文に際しては弊社営業担当部門にご確認ください。