東芝情報システム株式会社

高速！軽量！ストリーム暗号　Tritium®

● 汎用性
・小規模ゲートで電子回路化が容易
・プロセッサ機種非依存／コプロセッサ不要

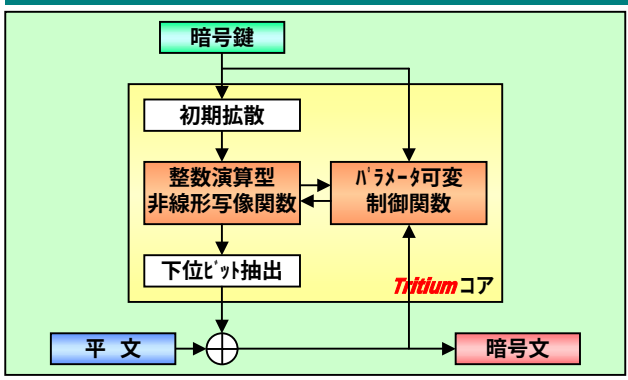
● 軽量性
・「暗号化」,「識別／認証」,「ハッシュ」機能を同一エンジンで提供

● 安全性
・FIPS，NIST乱数検定基準にて良好な乱数性を確認

● 高速性
・高速なストリーム暗号
・通信，ストリーミングに最適なバイト単位処理

● 多大鍵長も可
・スケーラブルで65536bit以上でも可
・鍵長の増加による処理速度の低下は僅か

Architecture
シンプルな構造で最大限のパフォーマンスを発揮！ソフトウェアから機器への組込みまで広範囲に対応！



Tritiumは、浮動小数点演算コプロセッサや剰余算用特殊コプロセッサを持たないような小型携帯端末など、限られた計算リソース下での運用を可能にする暗号方式で、長い鍵長を扱えること(512bit～65536bit)と、処理の高速性が特長です。

High Speed
鍵長による速度変化は僅少！暗号化プロセスがシステムの処理時間を圧迫しません！

ハードウェアIP　スペック

周波数	50MHz版	100MHz版
Gate数	6Kgate	7Kgate
処理速度	200Mbps	400Mbps
Cycle	2Clock (8bit)	

・3Kbit-SRAMが別途必要となります
・FPGA (50MHz版) にて実機検証済み

・合成ツール　：　Synopsys® Design Compiler
・合成ライブラリ：　0.18μm、1.5V
・RTL　：　Verilog-HDL
・鍵長　：　512bit

Multifunction
1つのコアエンジンで4つの動作モードを持ちます。「限られたスペースに多くの機能を！」という、お客様の声に応えます！

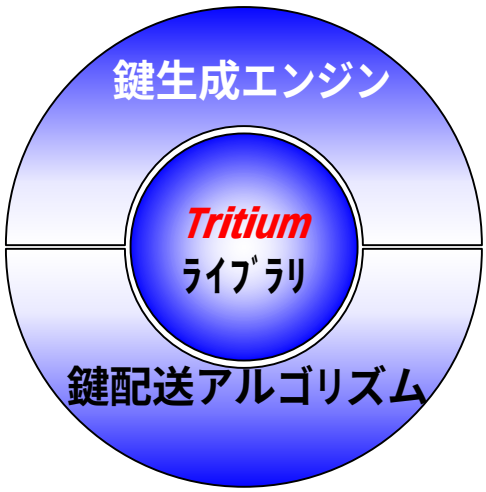
Tritium の動作モード

モード	入力	出力
暗号化モード	暗号鍵＋平文 (暗号文)	暗号文 (平文)
認証子生成モード	認証鍵	認証子
ハッシュ生成モード	平文	ハッシュ値
乱数生成モード	乱数シード	乱数列

Tritiumは暗号化モード以外に、認証子生成モード、改ざん検知、電子署名用途で用いられるハッシュ値生成モード、乱数生成モードの4つの動作モード (4機能) を備えます。これらの機能は、今日の様々な暗号化セキュリティ要件に対応しています。

東芝情報システム株式会社

Tritium®SDK



Tritiumの特長を試してみたい！というお客様の為に、SDK（Software開発キット）をご提供いたします。

TritiumSDKに含まれるもの
- **Tritium**暗号化ライブラリ
- 鍵生成エンジン
- 鍵配送アルゴリズム
- サンプルプログラム
- プログラミングマニュアル

（動作環境：Windows98,Me,2000,XP）

SDKにはコアとなる暗号化のライブラリ、そして暗号化に不可欠となる、「鍵」を生成する「鍵生成エンジン」、その「鍵」を相手に送る「鍵配送アルゴリズム」を同梱しています。基本的な機能を包含していますので開発者の方は、簡単にご評価を頂けます。

■参考：標準暗号と*Tritium*の処理速度

名　称		3DES	AES	*Tritium*
開発元		米国標準	米国標準	東芝情報ｼｽﾃﾑ
鍵長	[bit]	112 or 168	128	512
速度（暗号/復号）	[Mbps]	48.6 / 48.6	130.0 / 130.0	289.0 / 289.0
記述言語		C	C	C
モジュール容量	[byte]	44385	—	36864

※1：CRYPTREC Report 2001より抜粋

※2：左表の評価環境
PentiumIII650MHz
RAM 128Mbyte
Windows98SE
Visual C++ 6.0

■ソフトウェア　スペック

処理速度	CPU	OS
541Mbps	Pentium4（2GHz）	Linux
289Mbps	PentiumIII（650MHz）	Windows98

東芝情報システム株式会社

エンベデッドシステム営業事業部
〒210-8505川崎市川崎区日進町2番1号（東芝情報ｼｽﾃﾑﾋﾞﾙ）
TEL：044-246-8320(ﾀﾞｲﾔﾙｲﾝ)　FAX：044-246-8134
E-mail：Tritium@tjsys.co.jp
http://www.tjsys.co.jp/

お問い合わせ先