東芝情報システム株式会社

EDSFair with FPGA/PLD Design Conference
IPフリーマーケット

Tritium® 暗号IPのご紹介

平成18年1月26日

東芝情報システム株式会社

エンベデッドシステム・ソリューショングループ

東芝情報システム株式会社

今日の暗号化技術に求められている要素

- **頑強性／複雑性**
  コンピュータ性能の向上／解読の困難さ

- **高速性**
  映画，音楽等（有料コンテンツ）　暗号化ストリーミング配信

- **軽量性**
  携帯端末，ICカード，ユビキタス環境

強さ ⇔ 高速，軽量
相反する要素の解決

東芝情報システム株式会社

Tritium とは？

東芝情報システムオリジナルの
カオス理論を応用した、
共通鍵方式の
ストリーム暗号です

東芝情報システム株式会社

Tritium の特長

- カオス現象を利用

  ⇒ シンプル（＝高速）かつ複雑

- 暗号化 ＋ 認証（ﾁｬﾚﾝｼﾞ・ﾚｽﾎﾟﾝｽ型）

  ⇒ カオスコア部を共有 → 軽量性

- 整数演算、ビット演算

  ⇒ 特殊コプロセッサ類不要、汎用的
  ⇒ 小規模システム向き

- 鍵長が多大長

  ⇒ ～65536-bit（以上）

[平均解読年数]

56-bit	：約 1．2日
64-bit	：約 2年7ヶ月
128-bit	：約 111年
256-bit	：約 329年
512-bit	：約 767年
1024-bit	：約 1642年
	：

※平均的な能力のPCを100万台並列接続し、
その能力が年に1．5倍となると仮定して計算

東芝情報システム株式会社

パフォーマンス

*Tritium*はAESに比べて「4倍」の長さの鍵長で、処理速度は「2倍以上」を実現しています。

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	128	512
暗号タイプ		BLOCK	BLOCK	STREAM
■ソフトウェア実装(※1)				
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
■回路実装				
(1).回路規模優先				
速度	[Mbps]	170.3	235.2	200
回路規模	[Gate]	5700	5300	6422
(2).速度優先				
速度	[Mbps]	646.5	2245.6	400
回路規模	[Gate]	13700	33900	7210

（※1）　Pentium III 650MHz / RAM 128Mbyte / Windows98 SE / Visual C++ 6.0

東芝情報システム株式会社

応用製品のご紹介

Tritium は以下の2製品をラインナップしています。

ソフトウェア開発キット

Tritium SDK

暗号ハードウェアIP

Tritium HW/IP

東芝情報システム株式会社

TritiumSDK

Ver2.0
まもなく発売予定!!

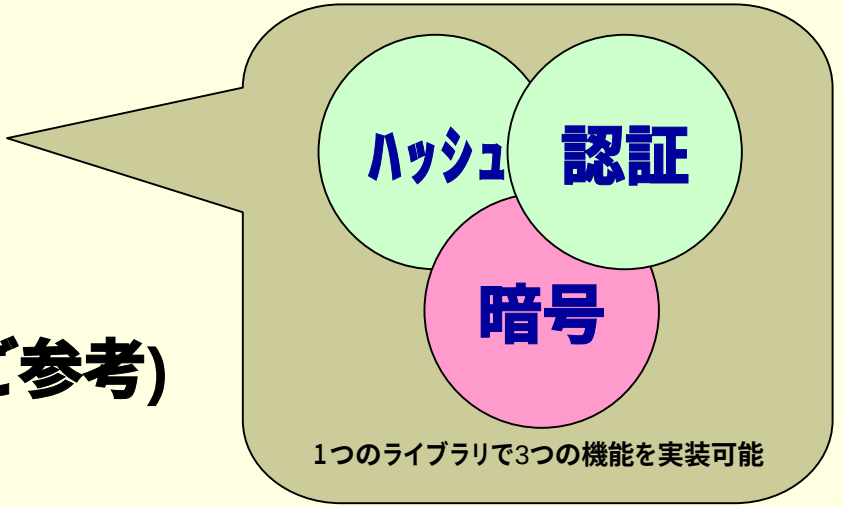
お客様の製品に、セキュリティ機能実装するため、Tritium暗号ライブラリを提供します。

TritiumSDK =「ソフトウェア開発キット」です。

TritiumSDKには、暗号・認証・改ざん検知機能を実装する際に必要な

- **ソフトウェアライブラリ**
- **開発用のマニュアル**
- **実装サンプルコード(ご参考)**

が含まれております。



東芝情報システム株式会社

Tritium HW-IP

セキュリティ機能を実現する為の暗号ハードウェアIPです

- 合成ツール　：Synopsys® Design Compiler
- 合成ライブラリ　：0.18μm、1.5V
- RTL　：Verilog-HDL
- 合成結果

DVD映像で5～8Mbps、ハイビジョンクラスで80Mbps程度。Tritiumで余裕の実装を！

周波数	Gate規模	処理速度
50MHz	6．4KGate	200Mbps
100MHz	7．2KGate	400Mbps

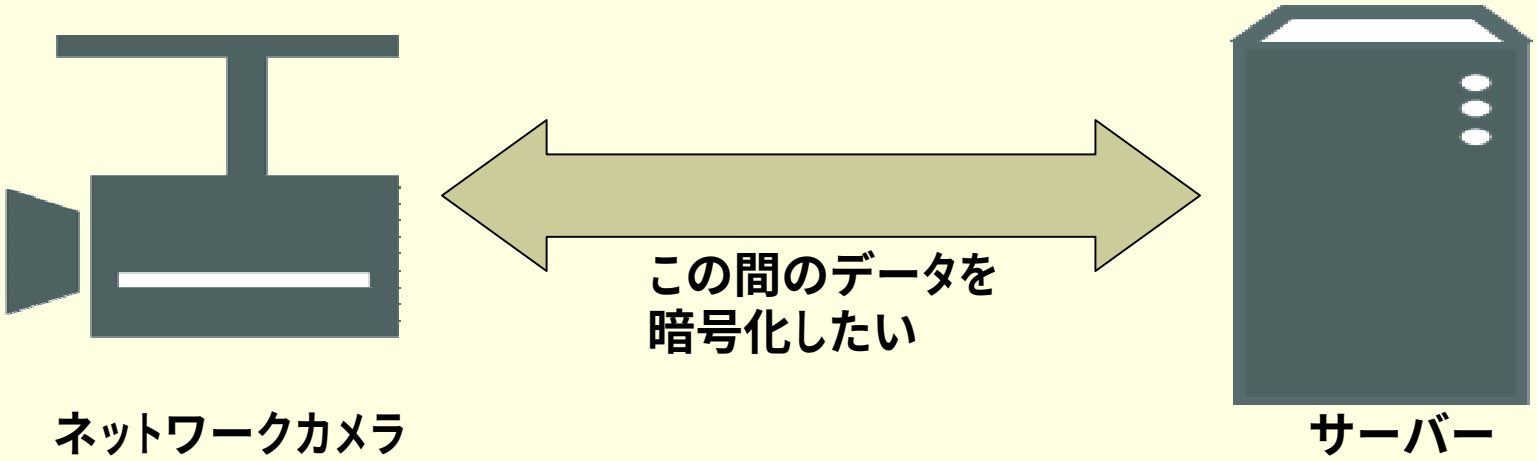
＊3Kbit-SRAMが別途必要となります

■ ポイント

▪小規模な回路で高いパフォーマンスを発揮！！

東芝情報システム株式会社

*Tritium*応用例　(ネットワークカメラへの実装)



応用のポイント

- 既存のハードウェアは変更せずに暗号に対応したい
  このため、小型の暗号が望ましい。
- 動画の暗号に対応させるため、高速な暗号が必要です。

東芝情報システムでは、今回ご紹介した*Tritium*をはじめ様々なセキュリティー製品と、経験豊かなスタッフでお客様の問題にお応え致します。

TOSHIBA

東芝情報システム株式会社

＜弊社連絡先＞

エンベデッドシステム営業事業部

TEL:044－246－8590

E-mail：tritium_sales@tjsys.co.jp