記者　各位

2006 年 6 月 14 日

株式会社デザイン･ゲートウェイ
代表取締役　篠原　秀和

ニュースリリース

AES 暗号処理方式 IP セキュリティ･システム「IP Lock」発売の件

株式会社デザイン･ゲートウェイ（東京都：代表取締役　篠原　秀和）は、信頼性の極めて高い AES 暗号技術を採用した、FPGA ロジックセキュリティ･システム「**IP Lock**」の発売を下記の通り発表します。

記

はじめに

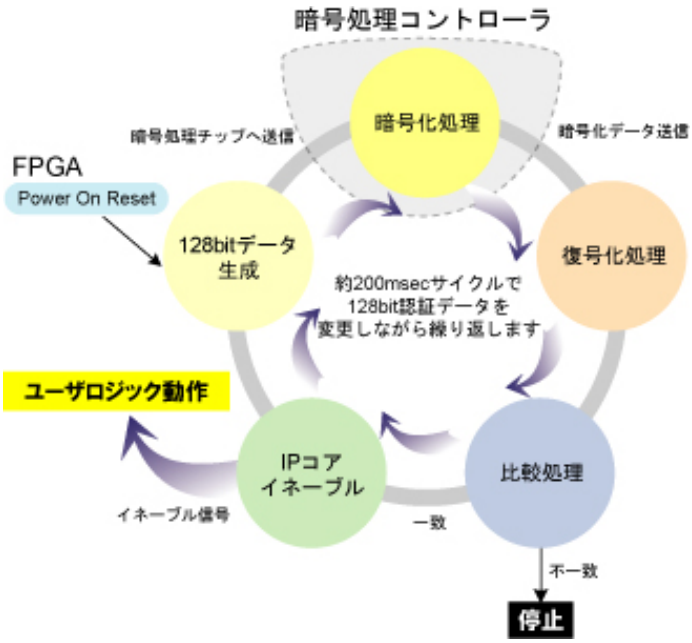
近年、エレクトロニクス製品の開発期間を短縮化するため FPGA が頻繁に採用されるようになりました。年々進む FPGA の大規模化･高機能化に伴い、内部にプログラムされる回路データの価値も飛躍的に高まっており、その設計資産(IP: Intellectual property)の保護が大きな課題となっております。

今回デザイン･ゲートウェイ社では、FPGA に組み込まれる IP 資産を保護するための IP コア＆暗号処理チップを開発、「**IP Lock**」として製品化いたしました。

「**IP Lock**」では、米国標準技術局により選定された共通暗号化方式の暗号化技術 AES（Advanced Encryption Standard）暗号方式を採用しております。AES は暗号化･復号化が高速、またトリプル DES より強固であり、DES に代わる次世代の暗号処理標準として金融関係、LAN セキュリティにおいて採用が増加している暗号方式です。

「**IP Lock**」は FPGA 内に共に組み込む IP コアとその FPGA に外部接続される暗号処理チップのセットで提供されます。

仕組みとしましては、任意の暗号キーを持つ IP コアを FPGA 内にユーザロジックと共に組み、128bit データを生成、暗号処理チップへ送信します。暗号処理チップは暗号化処理し FPGA へ認証データを返します。比較処理で一致した場合にのみ、ユーザロジックへイネーブル信号を出力、ユーザロジックが動作いたします。そして「**IP Lock**」では約 200 ミリ秒周期で認証データを変更･暗号化させることにより一層セキュリティを高め、スキャニングによる解析も事実上不可能としております(右図参照)。



今回デザイン･ゲートウェイ社では、「**IP Lock**」を幅広い用途でご使用頂くために、ユーザ ID をあらかじめ出荷時に書き込んだ暗号処理チップを 10 個または 30 個セットにした「ラボラトリーズパック」、ユーザが手元でユーザIDを書き込むことが可能な「IP Lock ライタ」と ID 未書き込みの「ブランクチップ」をご用意いたします。尚、現在、IP Lock コアは ALTERA 社と Xilinx 社の FPGA に対応しております。

特長:

- 暗号方式: AES-128 暗号方式
- セキュリティ: 約 200msec 周期で認証データを変更･暗号化
  暗号処理チップを外すとロジックの一部あるいはすべての機能が停止
- 暗号処理チップ: SOP8 ピンパッケージ
  FPGA との接続 I/O は 3 ピンのみ
- IP Lock コア: 消費リソース
  LE 約 1200, メモリビット約 24,500 (ALTERA 社 FPGA 使用時)
  約 400 スライス/1 ブロック RAM (Xilinx 社 FPGA 使用時)
  クロック入力不要
- 製品ラインナップ: ラボラトリーズパック(IP Lock コアと ID 書き込み済みチップのセット)
  IPL-010L (暗号処理チップ 10 個)
  IPL-030L (暗号処理チップ 30 個)
  IP Lock ライタ
  IPL-003WR
  ブランクチップ(ID 未書き込みのブランクチップ)
  IPL-CHP

商品名: **IP Lock (アイピーロック)**

ロゴ: IP Lock

出荷時期: 2006年7月より

開発／販売元: 株式会社デザイン･ゲートウェイ .

株式会社デザイン･ゲートウェイの紹介：

株式会社デザイン･ゲートウェイ（代表取締役：篠原　秀和、資本金 10,000,000 円）は、2001 年 11 月に設立されたシステム提案型の設計会社、次世代を担う先進のハードウェア設計を中心に設計開発業務を行っている。詳細については、www.dgway.com/を参照。

所在地

□ 本社　〒184-0012 東京都小金井市中町 3 丁目 23 番地 17 号
Tel. 050-3588-7915 Fax. 050-3588-7915

□ Design Gateway Co,.Ltd (R&D センター)　54 BB Building 12th Fl., Sukhumvit 21(Asoke), Klongtoey-Nua, Wattana, Bangkok 10110 Thailand
Tel. (66) 2261-2277, Fax. (66) 2261-2290

添付資料 IP Lock 写真、ランダムシード結果 [図 1～図 5]

この記事に対する問い合わせ先

株式会社デザイン･ゲートウェイ　営業推進部　石川 康彦
E-mail：info@dgway.com fax：050-3588-7915

以上

添付資料　IP Lock 写真、ランダムシード結果

図 1　IP Lock 暗号処理チップ外観写真

図 3 ユーザ基板上実装例

図 2　IP Lock ライタ外観写真

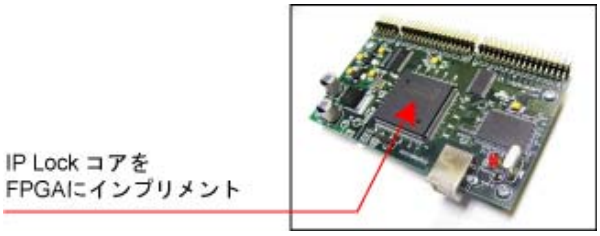
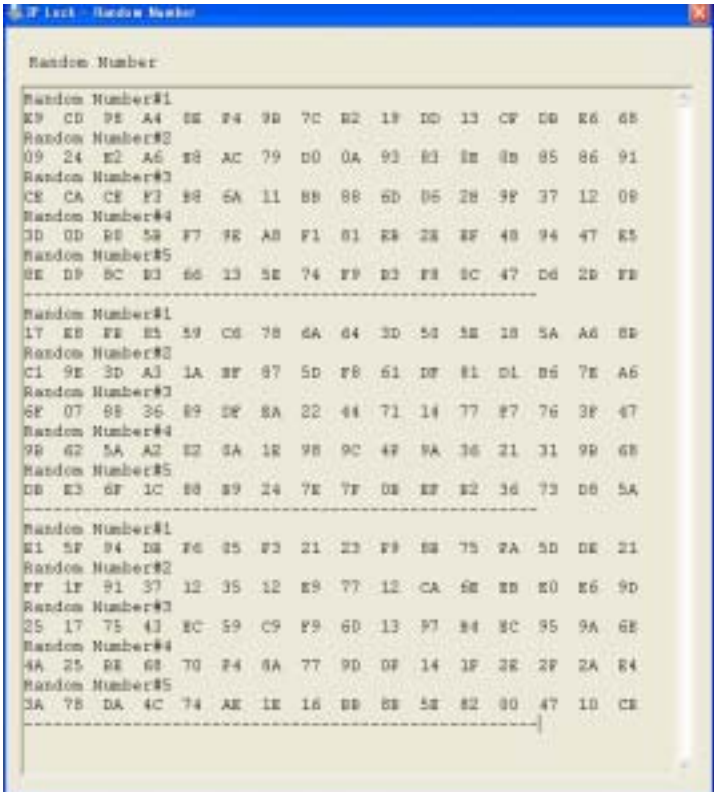


図 4　FPGA に IP Lock コアをインプリメント



```
Random Number

Random Number#1
E9  CD  9E  A4  8E  F4  9B  7C  B2  19  DD  13  CF  DB  E6  6B
Random Number#2
09  24  E2  A6  B8  AC  79  D0  0A  93  B3  8E  0B  85  86  91
Random Number#3
CE  CA  CE  F3  B8  6A  11  B9  B8  6D  D6  28  9F  37  12  09
Random Number#4
3D  0D  B8  5B  F7  9E  A8  F1  01  E8  2E  BF  48  94  47  E5
Random Number#5
8E  D9  BC  B3  66  13  5E  74  F9  D3  F8  BC  47  D6  2D  F8
------------------------------------------------------------
Random Number#1
17  E8  FE  E5  59  C6  78  6A  64  3D  5C  5E  18  5A  A6  8B
Random Number#2
C1  9E  3D  A3  1A  BF  87  5D  F8  61  DF  81  D1  B6  7E  A6
Random Number#3
6F  07  88  36  B9  DF  8A  22  44  71  14  77  E7  76  3F  47
Random Number#4
98  62  5A  A2  E2  8A  1E  98  9C  4F  9A  36  21  31  9B  6B
Random Number#5
DB  E3  6F  1C  B8  B9  24  7E  7F  D8  EF  E2  36  73  D8  5A
------------------------------------------------------------
Random Number#1
E1  5F  94  D8  F6  B5  F3  21  23  F9  B8  75  9A  5D  DE  21
Random Number#2
FF  1F  91  37  12  35  12  E9  77  12  CA  6E  EB  E0  E6  9D
Random Number#3
25  17  75  43  EC  59  C9  F9  6D  13  F7  B4  EC  95  9A  6E
Random Number#4
4A  25  BE  68  70  F4  8A  77  9D  DF  14  1F  2E  2F  2A  E4
Random Number#5
3A  7B  DA  4C  74  AE  1E  16  B8  B8  5E  E2  80  47  1D  CE
------------------------------------------------------------
```

IPLock のランダムシード･ジェネレータからの出力サンプルコピーです。このデータは IP Lock のデモソフトにて表示される機能で、電源投入から5回分のランダム･シードを表示しており、この画面は電源 UP を3度試行した結果を画面コピしたものです。ランダムシード･ジェネレータが生成するシードのランダム性が十分であることがわかります。

図 5　ランダム･シード結果