

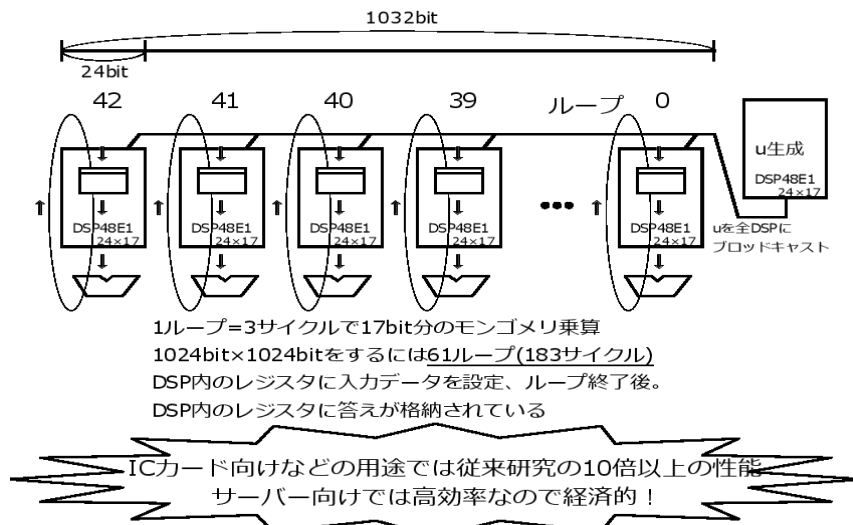
暗号プロセッサ SnakeCube に 8bit CPU を加え様々な暗号が可能に

商用クロードな暗号プロセッサ SnakeCube とオープンソースの 8bit CPU WZeta を組み合わせることで様々な暗号演算が可能になります。これらは同一設計者のよる独自の命令セットのプロセッサであり IC カードやレイテンシ性能を追求するサーバー向けに最適。

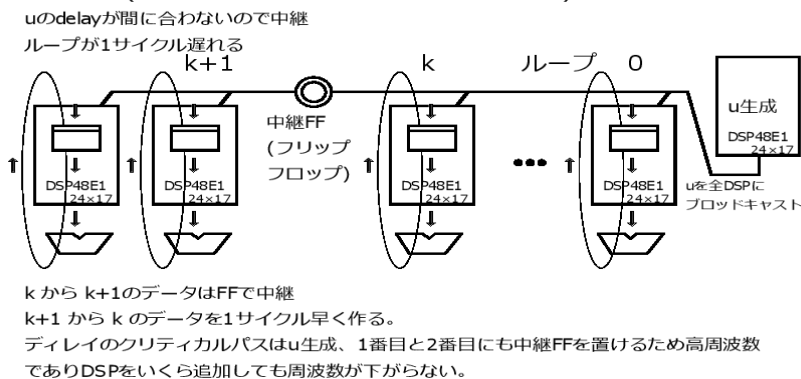
商用クロードな暗号プロセッサ SnakeCube とは

モンゴメリ乗算器を持つ暗号プロセッサ SnakeCube は 2018 年に平山直紀(Hirayama Naoki)によって発明され 2020 年に FPGA による実機で高性能かつ高効率であることが実証されました。デバイス依存が少なく廉価な FPGA でも性能を発揮するため多くのデバイスに実装できる経済性の高い暗号プロセッサ。SnakeCube は巨大な整数演算を得意としていますが SHA-2 などのハッシュ演算では多大な無駄が発生します。SnakeCube は 1999 年に RSA 暗号の性能で世界一だった大型コンピュータ (IBM 互換機) の暗号装置に搭載された暗号プロセッサ ICF3 の設計者によるもの。

RSA 2048bit復号化1回、1.74[ms]記録したSnakeCubeの
モンゴメリ乗算器(1024bit)を低価格なFPGAに実装した図



大きなモンゴメリ乗算器が実装できる仕組み
(大きな鍵長のRSA暗号ができる仕組み)



2020年8月に実機で1.74[ms]を計測したYouTube動画のURL

<https://youtu.be/beaFg0x8Qj8>

SnakeCube <https://snakecube.idletime.tokyo/> ↑数字のゼロ

(C)2018-2022 Naoki Hirayama

オープンソースの超軽量 8bit CPU WZeta とは

WZeta は少ないトランジスタ数で構成され、40 年以上前の Intel 8bit CPU 8080 のトランジスタ数と同等で数倍の性能が出る新種の命令セットの 8bit CPU。WZeta は 2019 年に期間限定公開されていましたが 2021 年 2 月にハードウェア開発コミュニティ elchika の「ハードウェア投稿作品キャンペーン」に応募、審査を通過したため本格的に開発を開始。全く別の CPU になったという経緯があります。他にないハードマクロ命令は複数の命令を 1 命令にする機能でプログラムメモリを節約、高速なサブルーチン、仮想マシンなど画期的に便利でコンパイラに新世界をもたらします。8bit のデータ幅のメモリをプログラムとデータで共用できるので メモリ 1 個で動作するためマイコンの製造コストを下げるのに役立ちます。各々の実装に依存しますが公式コア SDog は全命令 4 サイクルのため PWM 制御に向いています。また暗号のサイドチャンネル攻撃耐性があります。WZeta は全く独自のアーキテクチャでありオープンソースであることから世界的に普及することが期待できます。

16bit 固定長の命令セットはオペランドの 8bit だけで投機的に実行が開始できる命令セット。命令は 8bit×2 回の転送で CPU に送られます。このとき先に来た 8bit のコードだけで動作が開始できます。これを命令セットとして一貫させています。AES 暗号や RSA 暗号などでは 50~60%以上の命令でオペランド 投機実行が成功して命令の実行時間を 1 サイクル早めることができます。

例えば次の ADD 命令

ADD [n],A ; [n] = [n] + A

RSA や楕円暗号など多くの演算で良く使われる命令です。オペランド投機実行がなければ[n]の読み出しが遅れるため 命令の実行に 5 サイクルかかりますが、オペランド投機実行をすると 4 サイクルになります。プログラムコードの読み込みに 2 回、命令の実行に[n]のリード 1 回、 [n]のライト 1 回。合計 4 回のメモリアクセスが行われます。つまり、この命令は 4 サイクル以下にできない。

16bit 固定長の命令セットの最上位ビットは、モードによって 3 種類の動作をします。「パリティモード」には 2 つのモードが存在。命令コードの 1bit のパリティか、ハードマクロ命令の bit と合わせて 2bit パリティとするモード。パリティ無しの安価なメモリでパリティの信頼性を得られるメリットがあります。「高速モード」はレジスタを+1 しながら命令を同時に実行することで高速化します。トランジスタ数当たりの性能向上率の高い機能。「デバッグモード」では動作を止めることなくトレースデータを取得する目的で使えます。実装依存の機能ですがリアルタイムでなければバグが再現できない場合などで活躍。

2022 年 5 月現在、WZeta の公式サイトからは命令セットとゲートレベルの詳細な設計図がダウンロード可能。WZeta のシミュレータがダウンロードできるサイトも存在。Verilog のバイナリによるシミュレーションも可能。

FPGA による実機で 2048bit RSA 復号化 1 回、1.74[ms] を記録

2020 年 8 月に暗号プロセッサ SnakeCube の完全版を FPGA に実装し実測した記録は YouTube 動画として配信しています。 <https://www.youtube.com/watch?v=beaFg0x8Qj8>

FPGA ボードの 8 個の LED を使って演算結果を確認。設定したクロック周波数で動作していることを青色の LED の点灯で確認しています。測定条件は FPGA ボードは DIGILENT の Arty、FPGA は Xilinx の XC7A35TICSG324-1L コスト重視の Artix-7 です。スピードグレード -1 なので一番遅いもの。

FPGA 評価ボード Digilent Arty 搭載 FPGA: Xilinx XC7A35TICSG324-1L RSA 2048bit 復号化(CRT 有)の演算 1 回、1.74[ms]
--

Xilinx のホワイトペーパー「Zynq UltraScale+ MPSoC で暗号化処理を高速化」(WP512 (v1.0) 2019 年 5 月 21 日)の記録は 12.846[ms]なので約 7.4 倍ですが実測した SnakeCube の半導体プロセスは 2 ランクも格下なので同じなら 10 倍以上。Xilinx のホワイトペーパーに CRT の有無は記載されていませんが、Linux と FreeRTOS の性能差が 2 倍あるあたりを深読みすれば CRT 有と考えられます。

測定に使った verilog のソースコードを独立行政法人工業所有権情報・研修館(INPIT)および世界知的所有権機関 (WIPO) においてオンラインでタイムスタンプの証明書を取得しています。なお独立行政法人工業所有権情報・研修館(INPIT)のタイムスタンプ・サービスは 2021 年 3 月に終了していますが「アマノタイムスタンプサービス 3161」は有効です。

平山 直紀 殿

タイムスタンプトークン預入証明書

CERTIFICATE OF TIMESTAMP TOKEN DEPOSIT

以下のタイムスタンプトークンが預入日から独立行政法人工業所有権情報・研修館に預け入れられていることを証明する。

This is to certify that the following timestamp token has been deposited from the date of deposit indicated below
at the National Center for Industrial Property Information and Training of Japan.

タイムスタンプトークンを特定する情報 Identification Information of the Deposited Timestamp Token

ハッシュ値 Hash Value	64F9048AECAA46D04F865CDB9D24185B B31835994DCDF6580C437CB9D1C8CA1E EE1219DFD48618EC7709A2BEB40E1971 330FE938AE5F4C97575CD4EBE0AB4019
ハッシュアルゴリズム Hash Algorithm	SHA-512
タイムスタンプ付与時刻* Date and Time of Providing Timestamp *	2020/08/27 00:34:31.773
TSA公開鍵証明書の有効期限* Date and Time of TSA Public Key Certificate Expiration*	2030/10/17 18:07:47
署名者 Signer	アマノタイムスタンプサービス3161 (Type-T1)

タイムスタンプトークン預入日*: 2020/08/27
Date of Deposit *: 2020/08/27

証明書発行日*: 2020/08/27
Date of Certification *: 2020/08/27

独立行政法人工業所有権情報・研修館
The National Center for Industrial Property Information and Training
東京都港区虎ノ門4丁目3番1号城山トラストタワー8階
Shiroyama Trust Tower 8th floor, 4-3-1, Toranomom, Minato-ku, Tokyo, Japan



理事長 久保 浩三
President & Chief Executive Officer Kozo Kubo

※日本標準時 (年/月/日 時:分:秒)
※Japan Standard Time (YYYY/MM/DD hh:mm:ss)



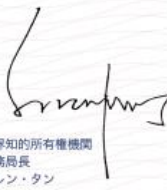
証明書ID: WDTS-PC-00002244

世界知的所有権機関 (World Intellectual Property Organization) は、
2020/09/30 14:43 UTC の時点において、NAOKI HIRAYAMA が、
以下の電子ファイルを保有していたことを証する。

電子ファイル名:	SnakeCube2020_08_27
電子ファイルのフィンガープリント:	f6c177341c2e64700fbd6a3397f6d8f222486c7b56a3101f0f6c5ce79eff5568

本証明書は、上記の電子ファイル及び当該ファイルに関連付けられたWIPO PROOFトークンの提示を受けて
2021/10/13 05:04 UTC に発行された。

シリアル番号: -377191322493647381398062560338860632419021618688 | ポリシー: 1.3.6.1.4.1.48669.2.1.1
タイムスタンプ局 (TSA): O = World Intellectual Property Organization | OI = CHE-462.076.735 | C = CH



世界知的所有権機関
事務局長
ダレン・タン

暗号半導体チップにおける『ナオキの法則』

半導体業界ではムーアの法則が有名ですが、ムーアの法則は集積回路上のトランジスタ数は「2年ごとに倍になる」という指標のような経験則です。似たような法則として平山 直紀(Naoki Hirayama)が 2018年に発明した SnakeCube から、後世の人に役立つ指標になるナオキの法則(Naoki's law)を提案します。詳しくは次のブログにありますが、RSA 暗号は鍵長が2倍になると計算量が8倍になります。SnakeCube は「鍵長2倍で計算時間4倍」を恐らく保証します。つまり、あるプロセスのデバイスでデータを取るとナオキの法則を使って、そのデバイスで鍵長を大きくした場合の精密な性能が予測できるのです。

<https://icf.hatenablog.com/entry/2022/01/27/074607>

SnakeCube の応用と今後

10万ビットの RSA 暗号の演算をするため 10万ビットの整数演算を1度に計算する SnakeCube のアーキテクチャは実現可能です。このため量子コンピュータの量子ビット数の限界を鍵長が超えれば、ブレイクスルーがあるまで当面、RSA 暗号でも安心できるかもしれません。楕円暗号の演算にも利用できますが楕円暗号は鍵を大きくする毎に安全性を考える必要があります。一方、RSA 暗号は鍵長に依存しないため、鍵を大きくするだけで安全性を再考する必要がありません。このため RSA はシステムのコストを下げることに貢献する場合があります。量子コンピュータの進歩や解読アルゴリズムの発明により、すべての公開鍵暗号が崩壊することも考えられます。そういう問題のために巨大整数を使った新しい公開鍵暗号、安全性の根拠となる困難性を多数、考えておくことは必要であり SnakeCube は役に立ちます。また将来のアプリ、準同型暗号で活躍する可能性もあります。

次世代 SnakeCube では量子コンピュータの解読に強い耐量子暗号を SnakeCube に実装していきます。従来暗号も新暗号も演算可能となるようにしていきます。汎用的な SIMD プロセッサを RSA 暗号に対応させた場合、十分に効率がでません。SnakeCube を耐量子暗号に対応させたほうが効率的ではないかと考えるため耐量子暗号の国内の研究者とともに開発を進めていくことになることが予想されています。

Web サイト

暗号プロセッサ SnakeCube 公式サイト <https://snakecube.idletime.tokyo/>

8bit CPU WZeta 公式サイト <https://wzeta.idletime.tokyo/>

暗号半導体チップにおける『ナオキの法則』 <https://icf.hatenablog.com/entry/2022/01/27/074607>

本件に関する問い合わせ先

平山 直紀

E-mail: snakecube@idletime.tokyo

twitter @__canal

返信がない場合、自宅電話 04-2952-4934 平山 直紀まで