様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １９ 日現在

機関番号：１１２０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８０
研究課題名（和文）GPGPUを用いた超高速疑似乱数発生法に関する研究

研究課題名（英文）Implementation of Ultra-High-Speed Pseudo-Random-Number Generator

研究代表者
吉田　等明（Yoshida, Hitoaki）

岩手大学・教育学部・教授

研究者番号：００２２０６６６

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：Pascalアーキテクチャを持つGPUを用いて，従来の14倍に相当する１秒間に4.383×10の12乗ビットという高速化を実現した。これまではカオスの長期予測不可能性によっていた堅牢性を，ランダム性を付加することによって大幅に向上させた。アルゴリズムの基本部分を見直すことにより，サイドチャンネル攻撃にも耐えうるものとした。周期については，4200個のカオス時系列を並列に動作させることで，10の22432乗という超長周期を可能とした。また，カオス時系列の個数と周期の対数との間に良い直線性があることを見出した。これによって，必要な長さの周期を持つ乱数発生器をデザインすることが可能となった。

研究成果の学術的意義や社会的意義
倍精度浮動小数点型演算を用いて実装した装置については，ハイエンドのGPUを用いてインターネットのバックボーンの暗号化に利用可能である。これにより伝送途中での盗聴を防ぐことができる。
固定小数点型演算方式で実装した装置については，浮動小数点演算をサポートしていない組み込み系デバイスやIoT機器の情報セキュリティ強化にも応用できると期待できる。近年，スマートフォンやIoT機器の情報セキュリティ対策が叫ばれており，重要な要素技術になるものと考えられる。最近のスマートフォンには，高性能のGPUが搭載されているものが増えているため暗号・復号時のCPUへの負荷を減らすことが可能となった。

研究成果の概要（英文）：The faster pseudo-random number generator is implemented by GPU which has Pascal architecture. The rate of generation has reached 4.383 Tb/s with double-precision-floating-point arithmetic and 1.779 Tb/s with fix-point arithmetic. Additional randomness has made the time series securer, and the revised basic algorithm has made it resistant to side-channel-attack and extended the period to 10 to the 22432th power by parallel-working 4200 chaotic-time-series on GPU. The period by 4200 time-series is too huge for security application in real life, however we have found fine relation ship between the number of time series and the logarithm of the periods. In order to determine the necessary number of time series for a cipher application the approximation curve is useful.

研究分野：情報工学

キーワード：カオス　疑似乱数　疑似乱数発生器　GPU　超長周期　超高速

[illegible]

[illegible]

[illegible]

[illegible]

([illegible] GPGPU[illegible]

S[illegible]c9×3[illegible] rS GPGPU[illegible]G[I[illegible]

[illegible]Mvb[6•

0,2b[illegible]×

GPUc[illegible] µ [illegible] GPU [illegible]M• GPGPU@

8[illegible]K[illegible] 3[illegible] CPU [illegible]K[illegible]•

G[illegible]A@[illegible]6G[illegible]0[illegible]M•

[illegible] 300 Gbps 82x9×3[illegible] *

K[illegible]• KK* [illegible]Ac GPU b[illegible]C$ ~ [illegible]

c8[illegible]K8e8[illegible] GPU b3[illegible] *

9×3[illegible]M7b e8[illegible] 5[illegible] 9×3[illegible]W

1,2b2

b GPU [a 9×3 b2 M S u M b

NVIDIA kb Pascal [illegible] GPU MC2K8[illegible]

[6 Kepler b32/[illegible] Pascal [c[illegible] 3 V

w 3.5 V L2 × 3 VW8GbCb2

/]b6vSM81M/×c]T

E=2 3]TEg8(1[

l bn[0MrS [illegible]b5,W9×36×

bV M

2[illegible]

[illegible] GPGPU 8MSu

28 ce1Mvbt[illegible]WS

29 c Pascal [illegible] GPU 8b 14 b9×3KSr

SGr[cb6× YW8S[illegible] MG

WMIOSrS[illegible]4(0bMG

7v vbKS8c 4200 b(448I

OG[10^{22432} 82x6×KS b468c

dNsMG[AGK8 10^{22432} c0[V

86×8[6Wb2[3OS[6MU

Figure 1 gKS (4bb P b6,8)6

G0bKS Gb(V[bc $R^2 = 1$ [6 Figure 1 bWgKS3d)

b8d 0[6×Ib 8TOGK

8

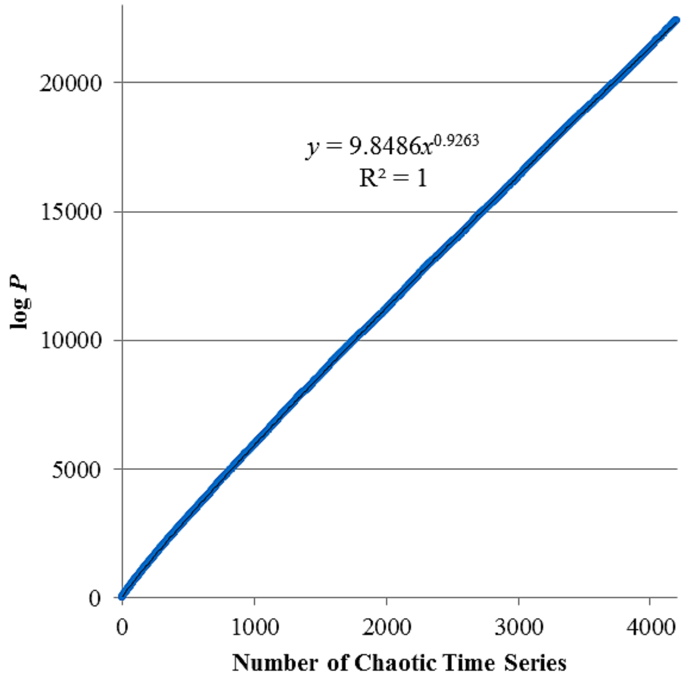

Figure 1: The digit of the whole period of CNNs (log *P*) as a function of the number of chaotic time series (*N*).

[illegible] GPU [6 NVIDIA Tesla P100
8KS)b0(cWb[6
(1) (1 8S 4.383 10^{12} bps 8: 2x9×3KSGb
GPU V[48IOSd×bc 1.34 h4)M Figure2
lg Table 1 b v-CNN 2b[6
(2) [18Sc 0.66 hbd×48I
O 1.7785 10^{12} bps 8:2x9×3KS Figure 3 lg Table 2 b pi-FPA lg pr-FPA
2b[6

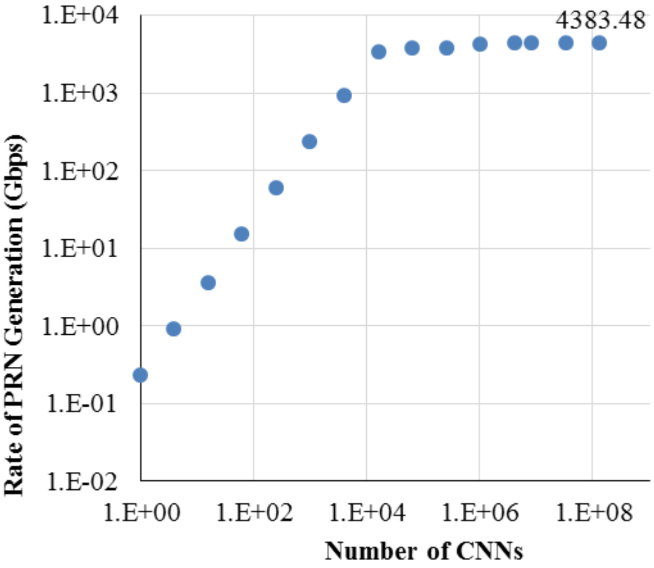

Figure 2. Rate of PRN generation by v-CNN with P100.

Table1. Rate of PRNG with double-precision arithmetic (CNN) and the improved method (v-CNN).

GPU	Tesla Accelerator	P100	K40	K10	C2070
	GPU Architecture	Pascal	Kepler	Kepler	Fermi
CUDA	CUDA Version	8.0	8.0	5.0	5.0
	CUDA Core [a)]	3584	2880	1536	448
	FP64 FMAD	1792	960	64	224
Random Number Generation (Gbps)	CNN	3827 [c)]	1687	191[b)]	320[b)]
	v-CNN	4383 [d)]	1757	-	-

a) FP32 (FMAD). b) Published result in reference 4. c) Number of CNNs is 8.39×10^{6}.
d) Number of CNNs is 1.34×10^{8}.

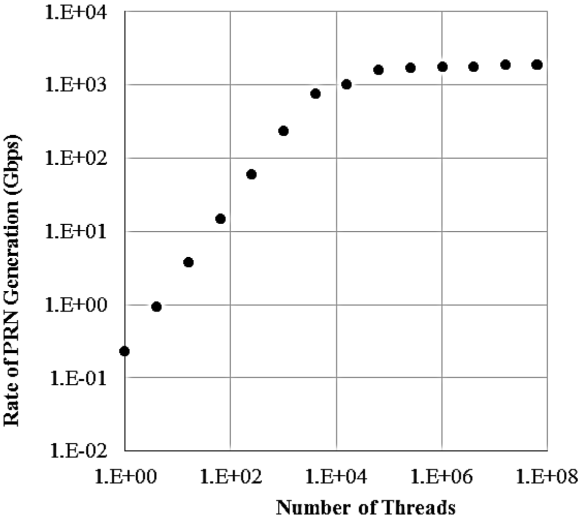

Figure 3. Rate of PRN generation using pr-FPA with GPU (Tesla P100) as a function of the number of threads.

Table 2: Rate of PRN generation by CNN types.

CNN Type	Number of Threads	Max Rate of PRN Generation (Tbps)
i-FPA [a)]	6.6060288×10^{7}	1.8277
pi-FPA [b)]	6.7108864×10^{7}	1.8570
pr-FPA [b)]	6.6060288×10^{7}	1.7785

a) The activation function f_1 is used for α series and f_2 is used for β series respectively to make orbit periods different.
b) The activation function f_1 is used for both subseries and with the perturbation $I_D = 0.119725$ to make orbit periods different.

c□ 2017 b[6IS71□ ITISE 2017 [□ 2 b8□

//8□ 2018 cb[6IS71□ NOLTA 2018 [/b□

8//WSrSb1=e□ 3)KS□

(□ l8/KS/(8cb GPU 8□

bb/[6G33p[b75D

G[A[l[/KS/(8c□ l□

K88)s3s(x IoT bxIv[A[A

3□ x IoT bxPd50[0[(□

/vb□ 3bc9×b GPU 3UI8v

b8 SuGMG[/b CPU lb2,MG□

WS□

3 $e ∴

711=0□ 3 □ 71bK□

[1] H. Yoshida, Y. Kon and T. Murakami, “Chaos Neural Network for Ultra-Long Period Pseudo-Random Number Generator,” *Proceedings of Papers, ITISE 2017*, vol.1, pp.102-113, 2017. 1w□

http://itise.ugr.es/2017/topics.php

[2] H. YOSHIDA, M. SASAKI, T. MURAKAMI, S. SHIMONO and S. KAWAMURA, “Factors Affecting Randomness in Pseudo-Random Number Series Extracted from Chaotic Time Series of Logistic Map and Chaos Neural Network”, Proceedings of Papers, ITISE 2017, vol.2, pp.331-342, 2017. 1w

http://itise.ugr.es/2017/topics.php

[3] H. Yoshida, Y. Akatsuka and T. Murakami, “Implementation of High-Performance Pseudo-Random Number Generator by Chaos Neural Networks using Fix-Point Arithmetic with Perturbation”, Proceedings of Papers, NOLTA 2018, pp46-49, 2018. 1w

https://www.ieice.org/nolta/symposium/archive/2018/HP/index.html

3 □ 71[b8/K□

[1] Yukito Kon, “Chaos Neural Network for Ultra-Long Period Pseudo-Random Number Generator”, International conference on Time Series, Granada, Spain, 2018.

[2] Masatomo Sasaki, “Factors Affecting Randomness in Pseudo-Random Number Series Extracted from Chaotic Time Series of Logistic Map and Chaos Neural Network”, International conference on Time Series, Granada, Spain, 2018.

[3] Yoshino Akatsuka, “Implementation of High-Performance Pseudo-Random Number Generator by Chaos Neural Networks using Fix-Point Arithmetic with Perturbation”, International Symposium on Nonlinear Theory and Its Applications, Taragona, Spain, 2018.

8ü/ 6

[illegible]

[illegible]

[illegible]

(1) [illegible]

[illegible]

[illegible] Kawamura Satoshi

[illegible]

[illegible]

[illegible]

[illegible] 40347919

[illegible] 31 [illegible] 4 [illegible] 1 [illegible]

(2) [illegible]

[illegible]

[illegible] Murakami Takeshi

[illegible]