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　５ 年　 ４ 月 ２１ 日現在

機関番号：３２６９０
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１９７３

研究課題名（和文）IoTデバイスに適した物理乱数生成器の研究開発

研究課題名（英文）Research and development of true random number generator suitable for IoT devices

研究代表者
鳥居　直哉（Torii, Naoya）

創価大学・理工学部・教授

研究者番号：１０４１７５１１

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：IoT機器の暗号鍵の元となる乱数生成に使用されるTRNG（True Random Number Generator）について，実装が容易で高エントロピーの乱数を出力するTRNGのハードウェア構成について評価しました。5種類のエントロピー源を用いたTRNGについて、出力乱数に対する定常状態および起動時の統計テスト、回路規模、及び消費電力について評価を実施しました。また，TRNGへの攻撃として，5種類のうち1つのエントロピー源を選び，それを用いたTRNGについて周囲温度と入力電圧を変化させた場合の乱数系列の統計テストを行いました。さらに、効果的なサイドチャネル攻撃を行い、対策を明らかにしました。

研究成果の学術的意義や社会的意義
IoTデバイスとの通信には暗号が使用される．安全な暗号鍵の生成には物理乱数生成器（TRNG）が用いられる．TRNGは、小規模、低消費電力で高速な乱数の生成を可能にすることが理想だが全てを満たす方式は存在しない．また，適用する領域によって重視する要件も異なってくる．本研究では，実装の容易さも含めた観点から5種類のエントロピー源について同じFPGA上で実装し、処理性能やハードウェア規模を評価することにより，重視する要件に応じてTRNGのエントロピー源やハードウェア構成を適切に選択することを可能にしている．

研究成果の概要（英文）：We evaluated TRNG (True Random Number Generator), which is used to generate random numbers as the source of encryption keys in IoT devices. The hardware configuration of the TRNG that is easy to implement and outputs high-entropy random numbers was evaluated. Evaluations were conducted for steady-state and startup statistical tests for the output random numbers, circuit size, and power consumption for TRNGs using five different entropy sources. As an attack on the TRNG using one entropy source of five, the randomness of the random number series by varying the ambient temperature and input voltage was investigated. Furthermore, we demonstrated an effective side-channel attack and identified countermeasures.

研究分野：ハードウェアセキュリティ

キーワード：物理乱数生成器　TRNG　リングオシレータ　COSO　TERO　STR　サイドチャネル攻撃

１．研究開始当初の背景

様々な環境に IoT（Internet of Things）デバイスを配置し，IoT デバイスの情報を集約し，分析することにより新しいサービスの提供を目指する IoT システムが注目されている．IoT システムにおいて，セキュリティは必須要件であり，IoT デバイスに適した暗号の実装や各種攻撃に対する対策は喫緊の課題となっている．本研究では，IoT デバイスでの鍵の生成などに用いられる物理乱数生成器(TRNG)について，IoT デバイスに搭載可能な，高エントロピーの乱数系列を生成する小型で低消費電力な物理乱数生成が必要になってきている．

２．研究の目的

本研究の目的は，次の２点に関して明らかにすること．

(1) IoT デバイスに搭載される TRNG のセキュリティの実現のために，温度変化や電池駆動などの厳しい環境条件に加え，回路や計算リソースの制約のなかで，電源を再投入した直後でも安定して高エントロピーを生成する TRNG の構成や実現方法を明らかにする．

(2) セキュアな TRNG の実現のために知られている攻撃について，環境温度や入力電圧の変動に対する生成する乱数系列の無作為性の調査，及び従来提案されたエントロピー源へのサイドチャネル攻撃とは異なるエントロピー源に対し新たな攻撃手法を適用した場合の有効性や対策法について明らかにする．

３．研究の方法

(1) IoT デバイスに搭載される TRNG の構成や実現方法を明らかにするために，５種類のエントロピー源を用いた TRNG を同じ FPGA 上に実装し，比較評価する．評価は，回路規模や乱数生成速度と共に，定常時，及び電源を再投入した直後の出力乱数の無作為性の評価を行う．この評価には米国 NIST 発行の SP800-22，SP800-90B，及びドイツ情報セキュリティ庁の AIS 20/30 の統計テストを参照して実施する．

(2) 攻撃による評価

従来提案されている TRNG へのサイドチャネル攻撃について，他のエントロピー源への適用や拡張による攻撃やその対策について検討する．

４．研究成果

4.1 TRNG の構成

(1)評価するエントロピー源

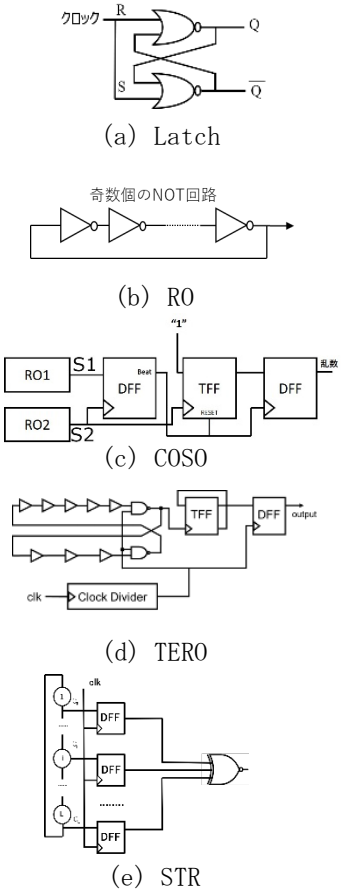
評価対象は，従来から提案されている 5 種類のエントロピー源を用いた TRNG とした．すなわち，SR ラッチ（Latch），リングオシレータ（RO），コヒーレント・サンプリング・リングオシレータ（COSO），遷移効果リングオシレータ（TERO），及び自己時間リングオシレータ（STR)の 5 種である．これらの基本回路を図 1 に示す．

Latch は，2 つの NOR ゲートから構成される回路であり，通常は 1bit の情報を保持するために使われる．この SR ラッチは入力が 0 のとき，出力は，前の状態出力で安定する．入力が 0 から 1 へ立ち上がる時，SR ラッチはメタステーブル状態となり，出力は 0 か 1 のどちらか（不定値）となる．この性質を利用し，入力にクロック信号を与えることで，出力から乱数列を得ることができる．

RO は，奇数個の NOT 回路を繋げた発振回路を用い，RO クロックのジッタをエントロピー源として利用する．このジッタは，RO を実装した回路の電源変動，クロストーク，半導体ノイズ，温度変動，及び配線遅延などにより生じる．

COSO は，2 つの独立した RO，DFF(D フリップフロップ)，及び TFF(T フリップフロップ) で構成される．コヒーレント・サンプリングは，周期 T1 の信号 S1 を周波数が近い S2 を用いてサンプリングする技術である．得られた信号はビート信号となり，(2 つの信号の周期の差Δ)/jitter 比に応じて周期 T2 の整数倍になる．ここで，クロックジッタによって信号 T1 の周期が揺らぐため，ビート信号 T2 の周期はランダムに変化することになる．

TERO は二つの NAND 及び，偶数個のインバータまたはバッファで構成される．二つの NAND ゲートに信号を入力することによって回路が発振を開始し，メタステーブル状態となる．その後，ゲート素子のばらつきや配線容量など様々な要因により，いずれ



(a) Latch

(b) RO

(c) COSO

(d) TERO

(e) STR

図１　エントロピー源

メタステーブル状態から安定状態へと遷移する．この安定状態へと遷移するまでの発振回数がランダムとなる．この発振回数を TFF によりカウントし，偶数であるか奇数であるかを判定することによって 1 bit の乱数を得られる．

STR は，信号の衝突がないマルチイベントオシレータである．STR の L 個の各ステージは 2 入力のミュラーゲートとインバータで構成される．各ステージは 2 相ハンドシェイクプロトコルで通信を行う．また L 個のうち E 個のステージはミュラーゲート出力が 1 となるイベントによって初期化をされ，伝搬を開始する．初期値のイベントの数に関係なく最終的に定常状態に移行する．STR のステージは DFF でサンプリングされる．それの出力は XOR され同じクロックでサンプリングされ，乱数を生成する．

これらのエントロピー源を実装し FPGA 毎にチューニングを行わず TRNG として使用するのは，RO を除いては難しいといわれている．本研究では，この問題を解決するために図 2 に示すようにエントロピー源を n 個準備しその出力を XOR(排他的論理和) する構成で TRNG を構成する．単体のエントロピー源を SES(Single Entropy Source)構成の TRNG，SES を多重化した構成を MES (Multiple Entropy Sources)構成の TRNG と呼ぶ．また，MES における SES の数を段数とよぶ．なお，MES 構成の RO については，MURO (multi-ring oscillator) と呼ばれている[1].

本研究では，5 種のエントロピー源の MES 構成の TRNG について 5 個の FPGA ボードに実装し統計テストに合格するための段数を明らかにする．実装が難しいといわれている SES では，統計テストに合格するためには，FPGA 毎に回路特性が異なるため配置や配線に考慮が必要とする場合が多い．本研究では，5 個のボードで共通の MES 構成で実装することにより FPGA ごとのチューニングが不要であることを検証する．なお，以降 MES 構成の TRNG について，エントロピー源の名前で呼ぶ．例えば，Latch を MES 構成で実現した Latch 型 TRNG を Latch と呼ぶ．

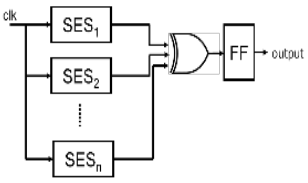


図 2　MES 構成

(2) 測定について

TRNG は，Diligent 社 Zybo Z7 Zynq-7010 評価ボードに実装する．Zynq-7010 は，XC7Z010-1CLG400C とデュアルコア ARM Cortex-A9 が搭載されている．FPGA の開発環境は Xilinx 社，Vivado 2019.1 である．評価ボードで生成した乱数を PC に取り込み，統計評価を行った．統計評価には，ドイツの BSI が定める AIS 20/31 (以下，AIS) と米国の NIST が定める SP800-90B (以下，90B) を用いて，定常時の乱数系列の評価を行なった．また，スタートアップ時の乱数の評価は，90B,相関テスト,パタンカウントテストをおこなった．そのほか，消費電力，生成速度の評価もおこなった．

段数の評価は，統計テストを実施した場合に合格する大きな段数で TRNG を構成し，その後段数を減らして最小の段数を評価している．

評価の結果を表 1 に示している．表 1 で各 TRNG 種類について，エントロピー源による TRNG の行は，2 行からなっているが，上段は，従来の評価結果[1]であり，下段が本研究の結果である．表中に，AIS，及び 90B の定常時，及び電源を再投入した直後の出力乱数の統計テストの結果を記載していないが，5 個ボード全てについて，いずれも統計テストは合格した．また，表 1 のエントロピーは，AIS による評価を記載しているが，非常に高いエントロピーを示している．

表 1 に回路規模，消費電力を記載しているが，これらは，開発環境における評価値である．また生成速度のチューニングは行っていない．評価のために効率性も加えている．

表 1 の実装難度は[1]の評価基準を採用しており，TRNG の構成について 6 つのスコアで評価する．スコア 5 は異なる機種でも簡単に実装できる構成に与えられる．スコア 4 は同一機種ならば簡単なセットアップを行うのみで実装できる構成に与えられる．スコア 3 はパラメータの最適化や一部の機種では難しい設定が必要な構成に与えられる．パラメータは最適化をすれば同一機種でも構成できる．スコア 2 は機種に応じて非常に難しい設定(配線の最適化) が必要な構成に与えられる．設定を行えば同一機種でも構成できる．スコア 1 は，同一機種であっても各デバイスによって最適化をしなければならない構成に与えられる．スコア 0 は，最適化しても乱数が出ない場合がある構成に対し与えられる．本稿では Zynq-7010 ボード，1 機種についての評価のため最高スコアは 4 とした．

この結果をもとに各 TRNG の用途について検討する．

a) 小規模・低消費電力を考慮した TRNG の構成評価

IoT デバイスに実装する際，小規模かつ低消費電力で高エントロピーであることが望ましい．更に，一定以上の生成速度があることが望ましい．この観点から評価した場合，SES 構成の COSO を実装するのが優れている．しかし，SES 構成の COSO の実装はデバイスごとに配置配線の最適化をせねばならず実装難度は非常に高い．次に優れているのは SES 構成の TERO を実装することだが，SES 構成の COSO 同様に実装難度は高い．TRNG の実装難度を考慮すると，SES 構成の RO の実装が望ましい．SES 構成の RO は回路規模・消費電力共にどちらも低く，実装難度もスコア 4 でありデバイスの個体差を意識することなく実装することができる．ただし，生成速度は非常に低い．生成速度が必要な用途には，回路規模・消費電力も大きくなるが，効率性という点で MES 構成の TERO，あるいは STR が候補と考えられる．

b) 乱数生成速度を考慮した TRNG の構成評価

乱数生成速度を考慮した場合，MES 構成の STR が優れている．MES 構成の場合は，配置配線で

表 1　TRNG の実装評価まとめ

TRNG 種類	実装手法	回路規模 LUT/Reg	消費電力 mW	生成速度 Mbit/s	効率性 bits/μ Ws	エントロピー per bit	実装難度
TERO	SES [1]	39/12	3.312	0.625	188.7	0.999	1
	MES (8 SES) [2]	93/16	4	2	500	0.999	4
COSO	SES [1]	18//3	1.22	0.54	442.6	0.999	1
	MES (48 SES) [2]	162/295	2	12.5	6250		
STR	SES [1]	346/256	65.9	154	2343.2	0.999	2
	MES (2 SES) [2]	126/153	27	200	7404	0.999	4
Latch	SES	-	-	-	-	-	-
	MES (256 SES) [3]	660/768	3	15.6	520	0.999	4
RO	SES [1]	46/19	2.16	0.0042	1.94	0.999	5
	SES [4]	12/19	1	0.125	125	0.999	4
MURO	MES (120 SES) [1]	521/131	54.72	2.57	46.9	0.999	4
	MES (2 SES) [4]	20/21	1	0.125	125	0.999	4

デバイスの個体差を意識することなく実装することができる．また，今回の実装では，L = 63 の STR を 2 つ実装し，MES 構成で実装することによって回路規模・消費電力も[1]に示された SES 構成の STR に比べ低く抑えられている．ただし，消費電力は大きくなる．

これらの評価より，MES 構成の場合は，SES 構成に比較すると常に回路規模，消費電力が大きくなるが，実装難易度や乱数生成速度の観点を加えると MES 構成の適用領域も存在することがわかる．

4.2　TRNG の攻撃対策

従来，TRNG に対し様々な攻撃が行われている．これらの攻撃は，乱数性を低下させる攻撃と乱数を予測する攻撃に分類される．乱数性を低下させる攻撃として，周波数インジェクション，グリッチインパクト，温度変化，電圧操作等による攻撃があげられる．これらの攻撃によるエントロピーの低下はヘルステストによって検知される場合が多い．また，乱数を予測する攻撃として機器が動作する際に生じるサイドチャネル情報を利用したサイドチャネル攻撃が挙げられます．この攻撃は，ヘルステストでは検知することができないため，あらかじめ攻撃に対する対策を立てる必要がありる．

a)COSO に対する温度変化，電圧操作等による攻撃

SES 構成の COSO を実装した FPGA の定格範囲内で電圧変化や環境温度を変化させた場合に，出力の乱数の統計的性質について実験評価を行った．

一般に，RO の周波数は，電源電圧や温度に依存しており，デバイスの温度を上昇させることで，RO の周波数が低下することが知られている．温度変化，電圧変化に対する出力変化の評価は，RO [5]，Latch [6]，TERO [7]については報告されている．本研究では，COSO について調査を行った．

先ず，温度変化による攻撃の評価をおこなった．SES 構成の COSO を Zybo Z7，及び Artix7 の FPGA に実装し，FPGA の定格温度の 0 ℃から 85 ℃で変化させた場合について，AIS，及び 90B で評価を行った．その結果，いずれの FPGA でも安定して高いエントロピー (0. 99) の乱数を生成することが分かった．

次に，電圧変化による攻撃評価をおこなった．SES 構成の COSO を Artix7 の FPGA に実装し，FPGA の定格電圧である 0.95 V から 1.05 V の範囲で 0.05 V ステップ毎に AIS を用いて評価を行った．その結果，SES 構成の COSO では，低い電圧 0.95 で 10 回の取得データに対する検定の合格数は 4 回となり，それより高い電圧では，10 回合格しているのに比べ大きく減少した．一方，MES 構成の COSO は電圧を変化させても乱数に影響はなく，高いエントロピーを維持していることがわかった．SES 構成の COSO では，電圧低下に対する耐性が十分でないことが分かった．

b)COSO へのサイドチャネル攻撃

SES 構成の TERO のサイドチャネル情報を利用して乱数出力を予測する攻撃が提案されている [8]．本研究では，この攻撃法を元に，SES 構成の COSO へのサイドチャネル攻撃を行った．

攻撃対象は Diligent 社 Zybo Z-7010 ボードに実装した SES 構成 COSO である．測定環境は FPGA ボード上の FPGA チップに磁界プローブ(LANGER, H-Field Probe 30Mhz up to 3Ghz) を固定する．チップから磁界プローブを通してサイドチャネル情報を取得，ローノイズアンプ (COSMOQAV, LNA270WS) によって増幅されたのちオシロスコープ(Agilent, DSO7104B) に計測される．オシロスコープによって計測されたデータは USB を通して PC に送られ，テキストデータに変換された後，保存される．

サイドチャネル情報である波形測定のために SES 構成の COSO の TFF の出力信号と TFF の Reset 信号を I/O ピンに接続をしている．単純電磁波攻撃では，磁界プローブをできるだけ攻撃対象のチップに近づける必要があるが，攻撃の有効性を図るため，端子に出力をしている．取得波形は Reset 信号をピンで取得しており，トリガーとして 20ns で 1000 回サンプリングし，

2000 波形取得している.

攻撃手法として 2 種類の方法を提案した. ます FFT を用いた方法である. 測定波形を FFT 処理したのち Min-Max Normalization にて正規化処理を行なう. この処理により, 乱数出力が 0 の場合と 1 の場合では, 10 MHz 以上の領域で大きさに差が現れることが分かった. このことから, 周波数成分 10.49 MHz の値が 0.3 以下のデータを 0, 0.3 以上を 1 と閾値を設定し, 2000 波形の出力予測を行ったところ, 2000 波形中 1958 波形, つまり 97.9% で乱数出力を正しく読み取ることができた.

次に, より実際の攻撃環境に近づけた攻撃実験を行った. DFF の近くに実装されている 2 つの RO 擾乱として働くと考えられるため, I/O ピンに接続する信号を TFF の出力信号, Reset 信号に加え, 2 つの RO の出力も接続した. 取得波形は Reset 信号をトリガーとして 20ns で 1000 回サンプリングし, 30000 波形取得した. この測定波形に対し多層パーセプトロン (以下 MLP) を用いた攻撃行った. MLP は入力層, 隠れ層, 出力層のノードが全結合しているモデルで, 隠れノード数 100, 活性化関数 relu, 最適化手法 adam を用いた. 取得した 30000 波形中, 70% を学習データ, 30% はテストデータとして学習させたモデルの乱数予測に使用した. MLP を用いることによって 9000 波形中 8996 波形, 99.95% で乱数の予測が可能になった.

これらの攻撃に対する対策を検討した. 乱数出力のための DFF の前に接続されている TFT へリセット信号を入れない方法 (NR 法) と回路を追加し TFF へリセット信号を入れる方法 (R 法) である. NR 法ではリセット信号が入力されないために SES 構成の COSO の乱数出力の統計的性質に影響がある可能性がある. これらを確認するために NR 法, 及び R 法の対策を行った SES 構成の COSO を実装し, AIS, 及 90B で評価を行った. この結果, どちらの対策法も 5 つの FPGA ボード全てにおいて統計テストに合格し, 高いエントロピーを持つ乱数を生成することが可能となった. この結果より, 統計テストの観点からは, 追加回路の不要な NR 法が有効な対策であることが分かった. 一方, MES 構成の COSO については, ここで述べた攻撃は, 攻撃対象の信号が多いため困難になると考えられる.

参考文献

[1] Oto Petura, Ugo Mureddu, Nathalie Bochard, Viktor Fischer, and Lilian Bossuet. ″A Survey of AIS-20/31 Compliant TRNG Cores Suitable for FPGA devices,″ In 26th International Conference on Field Programmable Logic & Applications (FPL),pp.1-10,2016.

[2] Naoya TORII, Ryuichi MINAGAWA, Hideaki OMAE and Kotaro HAYASHI, ″Implementation and Evaluation of Ring Oscillator-based True Random Number Generator, ″ International Journal of Networking and Computing, Vol 12,No 2: pp.372-386,2022

[3] 鳥居直哉, 大前 Kevin 秀明, ″ラッチを用いた物理乱数生成器の乱数の性能評価,″ 信学技法, HWS, IEICE-HWS2020-17, 2020

[4] 林光太郎, 鳥居直哉, ″リングオシレータ型真性物理乱数生成器の実装と評価,″ SCIS2021,4D2-3, 2021.

[5] H. Martin, T. Korak, E. S. Millan, and M. Hutter, ″Fault attacks on strngs: Impact of glitches, temperature, and underpowering on randomness, ″ IEEE Transactions on Information Forensics and Security, vol.10, no.2, pp.266-277, 2015.

[6] N. Torii, H.Kokubo, D.Yamamoto, et al.,″ASIC implementation of random number generators using SR latches and its evaluation,″ EURASIP J. on Info. Security 2016, 10, 2016. https://doi. org/10. 1186/s13635-016-0036-1

[7] Y. Cao, V. Rozic, B. Yang, J. Balasch, and I. Verbauwhede, ″Exploring active manipulation attacks on the tero random number generator, ″ in 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), pp.1-4, 2016.

[8] 大須賀, 藤本, 林. ″単純電磁波解析を用いた tero-based trng の出力ビット推定,″ SCIS2020,3E3-4,2020.

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Naoya Torii, Ryuichi Minagawa, Hideaki Kevin Omae, and Kotaro Hayashi	４．巻 12
２．論文標題 Implementation and Evaluation of Ring Oscillator-based True Random Number Generator	５．発行年 2022年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 372-386
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 皆川隆一，　大前ケヴィン秀明，　林光太郎，鳥居直哉
２．発表標題 リングオシレータ型真性乱数生成器の実装と評価(2)
３．学会等名 電子情報通信学会　ハードウェアセキュリティ研究会
４．発表年 2021年

１．発表者名 林光太郎，　鳥居直哉
２．発表標題 複数のコヒーレント・サンプリングを利用した真性乱数生成器
３．学会等名 情報処理学会　コンピュータセキュリティシンポジウム2021
４．発表年 2021年

１．発表者名 Naoya Torii，　Ryuichi Minagawa，　Hideaki Kevin Omae，　Kotaro Hayashi
２．発表標題 Implementation and Evaluation of a Ring Oscillator-based True Random Number Generato
３．学会等名 The Ninth International Symposium on Computing and Networking (CANDER 2021)（国際学会）
４．発表年 2021年

１．発表者名
林光太郎， 鳥居直哉

２．発表標題
リングオシレータ型真性物理乱数生成器の実装と評価

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021年

１．発表者名
鳥居直哉， 大前 ケビン 秀明

２．発表標題
ラッチを用いた物理乱数生成器の乱数の性能評価

３．学会等名
電子情報通信学会　ハードウェアセキュリティ研究会

４．発表年
2020年

１．発表者名
Kotaro HAYASHI， Ryuichi MINAGAWA， Naoya TORII

２．発表標題
Side-channel attack on COSO-based TRNG to estimate output bits

３．学会等名
Tenth International Symposium on Computing and Networking Workshops (CANDARW) (国際学会)

４．発表年
2022年

１．発表者名
皆川隆一， 林光太郎， 鳥居直哉

２．発表標題
COSO-based TRNG の安全性評価に関する検討

３．学会等名
電子情報通信学会　ハードウェアセキュリティ研究会

４．発表年
2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関