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　 ６ 月 ２８ 日現在

機関番号：１４３０１
研究種目：挑戦的研究（萌芽）
研究期間：2020～2022
課題番号：２０Ｋ２１７９３

研究課題名（和文）限定的一時複製を可能とする物理的複製困難関数回路

研究課題名（英文）Clonable PUF: Physical Unclonable Function with Limited Replication

研究代表者
佐藤　高史（Sato, Takashi）

京都大学・情報学研究科・教授

研究者番号：２０４３１９９２

交付決定額（研究期間全体）：（直接経費）　　4,800,000円

研究成果の概要（和文）：物理的複製困難関数（PUF）回路は、製造時に制御できない特性ばらつきを用いることで、回路の入出力関数に相当するチャレンジ・レスポンス・ペア（CRP）が個体ごとに異なっているため個体識別等に有効である。本研究では、これまでのPUFと同じ性質を持つと同時に、限定された個数のPUF間では、CRPが共有される限定的一時複製を可能とするPUF（CPUF）を提案した。CRP空間が比較的狭いweak CPUFとCRP空間がチャレンジに対して指数的に広いstrong CPUFの回路構成を具体的に示した。

研究成果の学術的意義や社会的意義
偽造品や悪意ある改ざんが施されたいわゆるハードウェアトロイを含む半導体部品の流通が懸念されている。PUFは半導体の真贋判定やユーザ間認証の手段等として提案されているが、PUFの性質である「複製困難性」のために、CRPを持つサーバとPUFの物理的実体を持つユーザとの間の1対1の認証のみが可能であった。しかし、必ずしもデータベースとの通信機能を持たず、1対1での認証が求められる応用は多い。本研究は、共有的な秘密情報をPUFの実体により分散して保持することにより、CRPをデータとして中央集権的に保存することを不要とするCPUFの設計を与えるものである。

研究成果の概要（英文）：Physically unclonable function (PUF) circuits are effective for identification purposes, etc., because their challenge-response pairs (CRPs), which correspond to the input-output function of the circuit, are different for each instance because the PUFs use characteristic variations that cannot be controlled during the manufacturing process. In this study, we proposed a clonable PUF (CPUF) that has the same characteristics as the existing PUFs and at the same time allows a limited number of replicas with shared CRPs. The circuit design of two types of CPUFs, weak and strong CPUFs, are developed.

研究分野：集積回路工学

キーワード：物理的複製困難関数　特性ばらつき　認証　セキュリティ

１．研究開始当初の背景

シリコン集積回路に代表される半導体の部品市場では、近年、正規品を模した偽造品や、悪意ある改ざんを施したいわゆるハードウェアトロイを含む部品の流通が懸念されている。半導体部品は今や、社会インフラを含むあらゆる分野の中核を支えている。運輸、医療、通信など、高度な安全性、信頼性、および秘匿性が求められる情報機器に不正な半導体部品が用いられることにより、我々の生活が危険にさらされることが危惧されている。

このため、情報機器自体、または情報機器間の通信において、機器の認証を行う仕組みが必要となる。こうした手法の一つとして、物理的複製困難関数（physically unclonable function; PUF）回路 [1,2] がある。PUF は、入力値であるチャレンジ c を与えると、対応するレスポンスを出力値 r として返す関数 $r = f(c)$ として機能する。チャレンジとレスポンスの対応（challenge response pair; CRP）は、半導体部品の製造工程において生じる物理的なばらつきに依存して決まる。このため、同じチャレンジに対するレスポンスは PUF 回路のインスタンスごとに異なると同時に、複製が困難なチップ固有の関数として機能する。PUF 回路は、チップの個体識別、暗号プロトコルにおける使用や、小規模な回路で実現可能である特徴から IoT（Internet of Things）デバイスに埋め込むなど、様々な情報機器に対する応用が検討されている [3,4,7,8]。

PUF を用いる認証は、通常、次の２ステップで行われる。(1) 登録: PUF の製造後、製造者自身である、または製造者から PUF 回路を含むチップを受け取った Alice は、認証を行う予定の回数よりも十分大きな回数分の CRP を調べてデータベースに登録する。その後、認証の対象となるユーザ Bob に安全な方法で PUF を渡す。(2) 認証: Bob が Alice に認証を要求する。Alice はデータベースに格納されているチャレンジビット列 $\boldsymbol{c}$ を Bob に送信し、Bob は PUF に $\boldsymbol{c}$ を与えて得られたレスポンス $\boldsymbol{r'}$ を Alice に返す。Alice はデータベース内に格納された期待値と受信したレスポンスを照合し、一致すれば Bob が認証される。

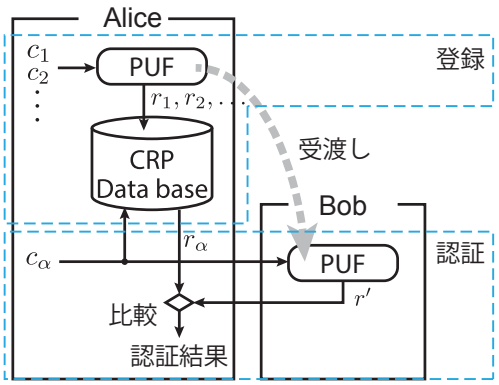

図 1: 従来の PUF による認証

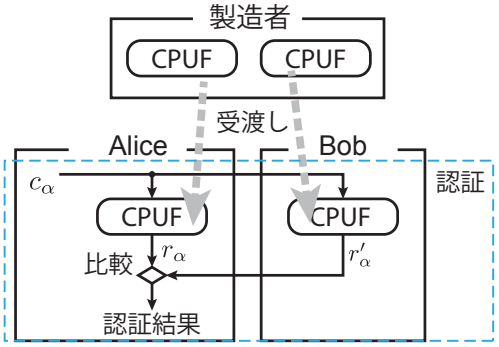

図 2: 提案する CPUF による CRP データベースを介さない直接認証

この認証方式では、CRP の読み出しや登録に大きなコストがかかる課題がある。また秘密情報である CRP が Alice に集中することから、Alice に完全に悪意がないことが保証される必要がある。さらに、ユーザ間（例えば Bob と Charlie の間）では直接の認証ができず、両者の CRP を持つ Alice が必ず仲介をする必要があるなど、データが保存されることに伴う不便が生じる。このように、従来の PUF は、PUF の安全性が依拠する「複製困難性」により CRP をデータとして保存せざるを得ず、結果としてデータを持つサーバと PUF を持つユーザとの間の認証のみが可能であるという強い制限があった。これに対し、例えば、インクジェットプリンタと純正インクカートリッジのように、データベースと通信することなくピア・トゥ・ピアでの認証が必要となる応用は極めて多い [5,6]。

２．研究の目的

前項の課題を鑑み、本研究の目的は、複製困難関数を限定数複製可能として PUF の物理的実体に分散的に共有させることで、CRP のデータによる保存を不要とする CPUF（Clonable PUF）回路を開発することである。CPUF では、限定された複数個の PUF で構成するグ

ループ内では CRP が等価であることから、グループ内の PUF 間ではデータを介さない直接認証が可能となる。一方で、異なるグループに属する CPUF 間では、通常の PUF と同様に CRP が異なる。CPUF は製造の過程でのみ複製が可能であり、製造が終了しパッケージングされると個々の CPUF は従来の PUF と同様の機能を持つように設計されるためである。

３．研究の方法

PUF は、CRP 空間が比較的狭い weak PUF と CRP 空間がチャレンジに対して指数的に広い strong PUF に大別される [1]。本研究でも、weak と strong の二種類の CPUF を構成することを目標とする [8]。PUF 回路は回路構造に差がないため、外観等からそれぞれの応答を予測することはできないが、製造時に制御しきれない特性ばらつきにより CRP が異なる。ここで、特性ばらつきはシステマティックばらつき成分とランダムばらつき成分から成っており、特にシステマティックばらつきは、回路構成と回路のレイアウト構造に依存して変化することが知られていることから、システマティックばらつきを積極的に活用することでグループ内の PUF の特性を近づけることができる。さらに、複製を得たい数の PUF 回路間を製造時のみ配線で接続する回路・レイアウト設計上の工夫を加えることで weak PUF として構成する。さらに、weak PUF を strong PUF に変換する方法が提案されているため、CPUF の枠組み内で同様にして strong PUF の作製にチャレンジする。

４．研究成果

(1) Coupled-inverter CPUF

weak CPUF 回路の例として、coupled-inverter CPUF を提案した [8]。この CPUF は、以下のように作成する。

1. CPUF はメモリスタアレイを含めて設計し、グループ間を配線により接続する。
2. ウェハープロセスが終了したら、接続された CPUF に書き込み電圧を印加し、メモリスタの値を決定（初期化）する。ここで書き込まれる値は、相互に接続された回路素子のばらつきに依存して決まる。そのため、1 つのメモリスタアレイのレスポンスは、同一グループの CPUF 間で等価であると同時に、既存の PUF と同様、製造者も再現できないユニークなものとなる。
3. ウェハを CPUF インスタンスに分割、パッケージングする。周辺回路はダイシング時に破壊し、書き換え不可能とする。

図 3 に CPUF セルの回路構成を示す。以下、簡単のためグループが 2 個の CPUF からなる場合を例に説明するが、3 個以上への拡張は自明である。各 CPUF セルは、メモリスタとトランジスタで構成する擬似インバータである。ペアとなるセル間を、オンチップ配線接続により相互に結合しラッチを形成する。図中では、ペアをなす CPUF セルを並べて描いているが、2 つの CPUF セルは、物理的に離して（別 CPUF インスタンス中に）配置される。

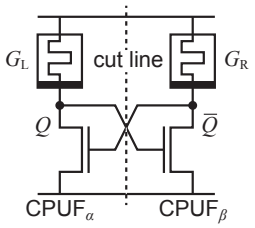

図 3: CPUF セル

書き込み動作では、CPUF ペアをプログラムするため書き込み電圧 V_w が印加される。2 つの疑似インバータの帰還動作により、コンダクタンスが相対的に高いメモリスタ（この例では G_L）が、大きな負電流を流し（図 4）、高抵抗状態（HRS）となる。一方、もう一つのメモリスタ（G_R）は初期の低抵抗状態（LRS）のままとなる。初期状態の抵抗値差が増幅され、最終的に左右のメモリスタはランダムに HRS と LRS となる。

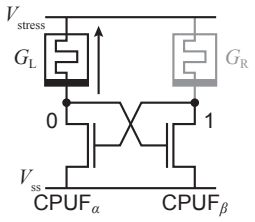

図 4: 書込み

書き込み操作後、CPUF ペアを 2 つの CPUF に分割する。これらのレスポンスである r_α と r_β は、メモリスタの状態に基づいて生成さ

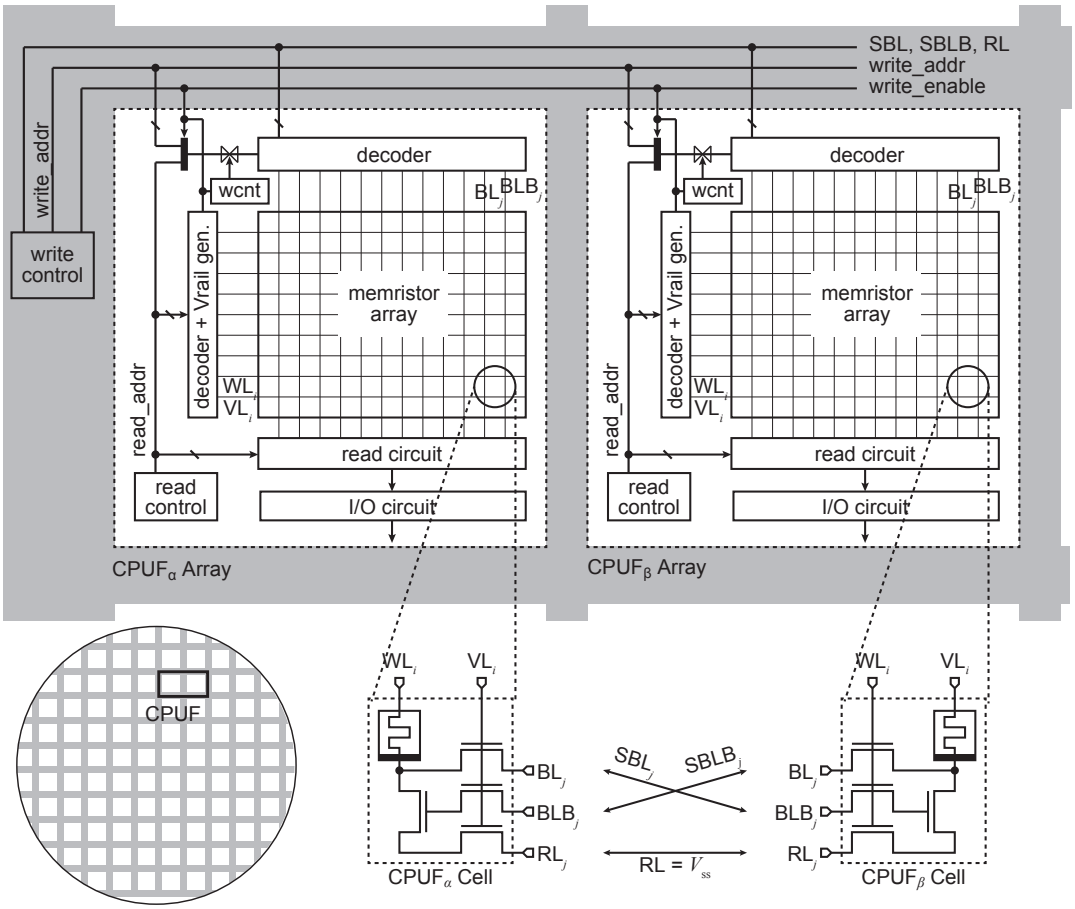

図 5: Coupled inverter CPUF の回路構成

れる。単純なコンパレータにより、HRS は 1 を、LRS は 0 を出力する。この回路では、r_α と r_β は常に相互に反転した値であり両者の応答は等価とみなすことができる。

提案する coupled inverter CPUF の実装例を図 5 に示す。本例は、α と β、2 つの CPUF がグループとなる。これらの回路は、図中左下のウェハーマップに示すように、スクライブラインに置かれる書き込み制御回路と配線を共有する 1 つのチップとして設計し、製造する。ダイシングにより CPUF が個々のチップに分離されると、メモリスタセルを選択するリードアドレス生成部がチャレンジとなり、指定されたアドレスの読み出し値がレスポンスとなる。この CPUF 回路は、CRP の数が限られた weak PUF であるが、大きな CRP 空間が必要な場合は、CPUF を [9,10] などの擬似ランダム関数回路を実装することで、CRP 数を指数関数的に増やすこと（strong 化）ができる。

CPUF は、メモリスタアレイ、読み出し制御回路、行デコーダ、Vrail 生成回路、列デコーダ、入出力回路により構成する。書き込み制御回路は、等価な応答を共有する CPUF ペアごとに置く。書き込み制御回路は初期化時のみ使用して、ダイシングで破壊する。以後は、ライトイネーブル信号のアサート回数を監視するライトカウンター回路 WCNT によりメモリスタアレイの書き換えを防止する。

一つの CPUF を構成する回路はすべて同一である。グローバル接続である SBL と SBLB を用いて擬似インバータを形成する。図 3 との違いは、書込み/読出しモードを決定する 3 つのスイッチ・トランジスタである。セルの入力と出力は、縦に走るバスライン、BL と BLB に接続され、同じ列に位置するセルと共有される。そして、これらのバスラインは、すべての CPUF を横断して走る SBL と SBLB に接続される。SBL と SBLB は、インバータが背中合わせに接続するよう交差して接続する。

(2) 提案 CPUF 回路の評価

提案する結合型インバータ CPUF の性能は、市販の 65nm プロセスライブラリを用いた

表 1: Equivalence (E), Randomness (D), Diffuseness (D), Uniqueness (U), context-tree weighting (CTW) compression, and NIST tests の評価結果

Array	Party	E	R	D	U	CTW	Freq.	CumSums	Runs
8×8	8	1.000	0.974	0.994	0.991	1.049	-	-	-
16×16	2	1.000	0.998	0.999	0.990	1.017	1.00	1.00	0.97

回路シミュレータと実機測定結果に基づくメモリスタモデル [9] を用いたシミュレーションにより評価した。MOS トランジスタのしきい値電圧ばらつきはガウス分布に従うと仮定している。また、高インピーダンス領域の長さであるモデルパラメータ gap[10] をガウス分布に従うように変更することで、メモリスタの初期コンダクタンスを決定している。

グループが 2 個の 8×8 アレイを持つ CPUF と、8 個の 16×16 アレイを持つ CPUF を評価した。いずれの構成でも、SRAM 回路を合わせて実装しそのアシスト動作を用いた。各構成の CPUF を 100 個ずつ仮想的に作製し PUF の評価指標を求めた。結果を表 1 に示す。ここで、Equivalence は CPUF の性能を定量化するために新たに定義した指標であり、CPUF の対応するレスポンスの一致率を次式で評価する。

$$E = \frac{1}{C} \sum_{c=1}^{C} g(f_\alpha(c), f_\beta(c), f_\gamma(c), ...) \tag{1}$$

ここで、C はチャレンジの総数、g は対応する CPUF の応答がすべて等しい（少なくとも 1 つの CPUF の応答が等しくない）場合に 1（0）を返す関数である。

等価性 E は理想値 1.0 と評価されており、提案する CPUF が常に等価な応答を生成することを意味する。また、R, D, U の値も理想値に非常に近く、CTW も 1.0 を上回っている。これらの結果は、提案する CPUF が単体の PUF として非常に優れた性能を達成し、かつグループ内の CPUF の応答が完全に一致することを示している。CPUF のインスタンスは、従来の PUF と実質的に同等であり、見分けがつかない。

NIST 試験については、Frequency, CumulativeSums, Runs が 100 ビット以上を必要とするため、16×16 のアレイを持つ CPUF にのみ適用した。2 進数、m=100、有意水準 $\alpha = 0.01$ で信頼区間は 0.96015 であり、すべてのテストについて閾値信頼度を超えている。したがって、提案する CPUF の応答は十分に予測不可能である。CPUF の温度依存性等による信頼性も評価したが、紙幅の都合で省略する。いずれも、十分な信頼性が得られている。

参考文献

[1] B. Gassend 他, “Silicon physical random functions,” in Proc. Comp. Comm. Security Conf., 2002, pp.148–160. [2] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Proc. DAC, 2007, pp.9–14. [3] Y. Tanaka, S. Bian, M. Hiromoto, and T. Sato, “Coin flipping PUF: A novel PUF with improved resistance against machine learning attacks,” IEEE Trans. CAS-II, 65(5), 2018, pp.602-606. [4] H. Awano and T. Sato, “Ising-PUF: A machine learning attack resistant PUF featuring lattice like arrangement of arbiter-PUFs,” in Proc. DATE, 2018, pp.1459-1464. [5] 佐藤他, “PUF 回路群，PUF 回路群の製造方法，PUF 回路の使用方法，及びネットワークシステム,” 特願 2018-154477 [6] T. Sato, Y. Tanaka, and S. Bian, “Clonable PUF: On the design of PUFs that share equivalent responses,” in Proc. IEEE ISCAS, pp.1-5, May 2021. [7] M. Bhargava et al., “An efficient reliable PUF-based cryptographic key generator in 65nm CMOS,” in Proc. DATE, 2014, pp. 1–6. [8] R. Liu et al., “Extending 1kb RRAM array from weak PUF to strong PUF by employment of SHA module,” in Proc. AsianHOST, 2017, pp. 67–72. [9] P. Y. Chen et al., “Compact modeling of RRAM devices and its applications in 1T1R and 1S1R array design,” IEEE Trans. Electr. Dev., 62(12), pp. 4022–4028, 2015. [10] S. Yu et al., “A low energy oxide-based electronic synaptic device for neuromorphic visual systems with tolerance to device variation,” Advanced Materials, 25(12), pp. 1774–1779, 2013.

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Morita Shumpei、Bian Song、Shintani Michihiro、Sato Takashi	４．巻 -
２．論文標題 Efficient Analysis for Mitigation of Workload-dependent Aging Degradation	５．発行年 2022年
３．雑誌名 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems	６．最初と最後の頁 1～1
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCAD.2022.3149856	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Bian Song、Kundi Dur E. Shahwar、Hirozawa Kazuma、Liu Weiqiang、Sato Takashi	４．巻 16
２．論文標題 APAS: Application-Specific Accelerators for RLWE-Based Homomorphic Linear Transformations	５．発行年 2021年
３．雑誌名 IEEE Transactions on Information Forensics and Security	６．最初と最後の頁 4663～4678
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2021.3114032	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 －

１．著者名 Qin Zhaoxing、Kuribara Kazunori、Ogasahara Yasuhiro、Sato Takashi	４．巻 -
２．論文標題 Hybrid CMOS and pseudo-CMOS Organic Memory for Flexible Sensors	５．発行年 2022年
３．雑誌名 IEEE Sensors Journal	６．最初と最後の頁 1～1
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSEN.2022.3153714	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Shintani Michihiro、Ueda Aoi、Sato Takashi	４．巻 37
２．論文標題 Accelerating Parameter Extraction of Power MOSFET Models Using Automatic Differentiation	５．発行年 2022年
３．雑誌名 IEEE Transactions on Power Electronics	６．最初と最後の頁 2970～2982
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TPEL.2021.3118057	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 －

1．著者名 Oshima Kunihiro、Bian Song、Kuribara Kazunori、Sato Takashi	4．巻 60
2．論文標題 Separation of bias stress degradation between insulator and semiconductor carrier trapping in organic thin-film transistors	5．発行年 2021年
3．雑誌名 Japanese Journal of Applied Physics	6．最初と最後の頁 SBBG06～SBBG06
掲載論文のDOI（デジタルオブジェクト識別子） 10.35848/1347-4065/abdcb2	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Z. Qin, M. Shintani, K. Kuribara, Y. Ogasahara, and T. Sato	4．巻 20
2．論文標題 Organic Current Mirror PUF for Improved Stability Against Device Aging	5．発行年 2020年
3．雑誌名 IEEE Sensors Journal	6．最初と最後の頁 7569-7578
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSEN.2020.2986077	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Z. Qin, S. Bian, K. Kuribara, and T. Sato	4．巻 60
2．論文標題 Stable Organic SRAM Cell With P-type Access Transistors	5．発行年 2021年
3．雑誌名 Japanese Journal of Applied Physics (JJAP)	6．最初と最後の頁 SBBG04-SBBG04
掲載論文のDOI（デジタルオブジェクト識別子） 10.35848/1347-4065/abd534	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ikeda Sosei、Awano Hiromitsu、Sato Takashi	4．巻 41
2．論文標題 Hardware-Friendly Delayed-Feedback Reservoir for Multivariate Time-Series Classification	5．発行年 2022年
3．雑誌名 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems	6．最初と最後の頁 3650～3660
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCAD.2022.3197488	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計18件（うち招待講演　2件／うち国際学会　13件）

１．発表者名
Kotaro Matsuoka, Ryotaro Banno, Naoki Matsumoto, Takashi Sato, and Song Bian

２．発表標題
Virtual secure platform: A five-stage pipeline processor over TFHE

３．学会等名
Usenix Security Symposium（国際学会）

４．発表年
2021年

１．発表者名
瀬川 七央，佐藤 高史

２．発表標題
量子計算の誤り軽減のための量子ビット初期配置手法

３．学会等名
回路とシステムのワークショップ

４．発表年
2021年

１．発表者名
Kotaro Matsuoka, Yusuke Hoshizuki, Takashi Sato and Song Bian

２．発表標題
Towards better standard cell library: Optimizing compound logic gates for TFHE

３．学会等名
ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC)（国際学会）

４．発表年
2021年

１．発表者名
橋詰 陽太，古川 修平，松本 直樹，伴野 良太郎，松岡 航太郎，佐藤 高史

２．発表標題
完全準同型暗号におけるBNNを用いた高速な秘匿推論手法の実装と評価

３．学会等名
情報処理学会第84回全国大会

４．発表年
2022年

１．発表者名
Takamochi Kanda, Takashi Sato, Hiromitsu Awano, Sota Kondo, and Koji Yamamoto

２．発表標題
Respiratory rate estimation based on WiFi frame capture

３．学会等名
IEEE Consumer Communications & Networking Conference (CCNC)（国際学会）

４．発表年
2022年

１．発表者名
佐藤 高史，塚本 裕貴，辺 松，新谷道広

２．発表標題
統計的回路シミュレーションのための非正規分布モデルパラメータの生成(招待)

３．学会等名
信学技報 SDM研究会（招待講演）

４．発表年
2021年

１．発表者名
Song Bian, Weiweng Jiang, and Takashi Sato

２．発表標題
Privacy-preserving medical image segmentation via hybrid trusted execution environment

３．学会等名
ACM/IEEE Design Automation Conference (DAC)（国際学会）

４．発表年
2021年

１．発表者名
Kyohei Shimozato, Michihiro Shintani, and Takashi Sato

２．発表標題
Adaptive outlier detection for power MOSFETs based on Gaussian process regression

３．学会等名
IEEE Applied Power Electronics Conference and Exposition (APEC)（国際学会）

４．発表年
2021年

１．発表者名
Tatsuki Ono, Song Bian, and Takashi Sato

２．発表標題
Automatic parallelism tuning for module learning with errors based post-Quantum key exchanges on GPUs

３．学会等名
IEEE International Symposium on Circuits and Systems (ISCAS)（国際学会）

４．発表年
2021年

１．発表者名
Takashi Sato, Yuki Tanaka, and Song Bian

２．発表標題
Clonable PUF: On the design of PUFs that share equivalent responses

３．学会等名
IEEE International Symposium on Circuits and Systems (ISCAS)（国際学会）

４．発表年
2021年

１．発表者名
神田 高望，佐藤 高史，粟野 皓光，近藤 綜太，山本高至

２．発表標題
WiFiフレームキャプチャに基づく呼吸数推定に関する検討

３．学会等名
信学技報 SRW SeMI CNR

４．発表年
2021年

１．発表者名
佐藤 高史，塚本 裕貴，辺 松，新谷道広統計的回路シミュレーションのための非正規分布モデルパラメータの生成(招待)

２．発表標題
統計的回路シミュレーションのための非正規分布モデルパラメータの生成

３．学会等名
信学技報 SDM研究会（招待講演）

４．発表年
2021年

１．発表者名
Kyohei Shimozato and Takashi Sato

２．発表標題
dGPLVM: A nonparametric device model for statistical circuit simulation

３．学会等名
IEEE International Conference on Microelectronic Test Structures (ICMTS)（国際学会）

４．発表年
2022年

１．発表者名
S. Bian, W. Jiang, and T. Sato

２．発表標題
Privacy-preserving Medical Image Segmentation via Hybrid Trusted Execution Environment

３．学会等名
ACM/IEEE Design Automation Conference (DAC)（国際学会）

４．発表年
2021年

１．発表者名
T. Sato, Y. Tanaka, and S. Bian

２．発表標題
Clonable PUF: On the Design of PUFs That Share Equivalent Responses

３．学会等名
IEEE International Symposium on Circuits and Systems (ISCAS)（国際学会）

４．発表年
2021年

１．発表者名
S. Bian, W. Jiang, Q. Lu, Y. Shi, and T. Sato

２．発表標題
NASS: Optimizing Secure Inference via Neural Architecture Search

３．学会等名
European Conference on Artificial Intelligence (ECAI)（国際学会）

４．発表年
2020年

１．発表者名
S. Bian, X. Xu, W. Jiang, Y. Shi, and T. Sato

２．発表標題
BUNET: Blind Medical Image Segmentation Based on Secure UNET

３．学会等名
Medical Image Computing and Computer Assisted Interventions (MICCAI)（国際学会）

４．発表年
2020年

１．発表者名
S. Bian, T. Wang, M. Hiromoto, Y. Shi, and T. Sato

２．発表標題
ENSEI: Efficient Secure Inference via Frequency-domain Homomorphic Convolution for Privacy-preserving Visual Recognition

３．学会等名
Computer Vision and Pattern Recognition (CVPR)（国際学会）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

情報回路方式研究室
http://www.pass.cce.i.kyoto-u.ac.jp/

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
研究分担者	Ｂｉａｎ　Ｓｏｎｇ (Bian Song) (00866030)	京都大学・情報学研究科・助教 (14301)	

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