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　６ 年　 ６ 月 １４ 日現在

機関番号：８２６２６
研究種目：基盤研究(B)（一般）
研究期間：2021～2023
課題番号：２１Ｈ０３４１３

研究課題名（和文）クラウドFPGAを安全に利用するための信頼起点の構築及びリモート攻撃対策の研究

研究課題名（英文）Study on building root of trust and preventing remote attacks for the security of cloud FPGA systems

研究代表者

堀　洋平（Hori, Yohei）

国立研究開発法人産業技術総合研究所・エレクトロニクス・製造領域・主任研究員

研究者番号：６０５３０３６８

交付決定額（研究期間全体）：（直接経費）　　12,900,000円

研究成果の概要（和文）：物理複製困難回路（Physically Unclonable Function)を用いた信頼起点（Root of Trust）を構築し、暗号技術と組みわせることで、クラウドFPGAのセキュリティの問題を解決する。本研究では、FPGA上でもユニーク性・安定性が高く、機械学習攻撃に耐性のあるPUFの開発を行った。複数のフリップフロップをアンバランスな位置において意図的に遅延差を作り出すことで、FPGA上でMulti-threshod型のArbiter PUFを実現した。本PUFは、他のArbiter型PUFの数倍から数十倍小さな面積でありながら、高い機械学習耐性を有することが示された。

研究成果の学術的意義や社会的意義
本研究は、深層学習攻撃への耐性があり、ユニーク性や安定性の高いPUFをFPGA上において実現した。特に、非常に強力な攻撃手法とされる深層学習攻撃に対して、小面積でありながら高い防御性能を実現することができた。これにより、近年サービスが開始されたクラウドFPGA（FPGAaaS）を安全に利用する手法の一つが示されたと言える。

研究成果の概要（英文）：For the security of cloud FPGAs, we build the root of trust using a Physically Unclonable Function (PUF) on the FPGA. We developed the attack-resistant PUF with high uniqueness and steadiness that is suitable for FPGAs. We realized the multi-threshold arbitering scheme by placing multiple FFs in unbalanced positions. The experimental results show that our PUF achieves much higher attack resistance than the conventional arbiter PUF with the equivalent area and achieves equivalent attack resistance to previous PUFs with areas around several to dozens of times smaller.

研究分野：ハードウェアセキュリティ

キーワード：情報セキュリティ　PUF　FPGA

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

パブリッククラウド上の FPGA (以下「クラウド FPGA」）にユーザがハードウェアを自由に構築できる FPGA-as-a-Service (FPGAaaS) と呼ばれる画期的なサービスが開始された。2017 年の Amazon Web Service (AWS) EC2 F1 に続き、Microsoft Catapult や Alibaba Cloud F3 等のサービスが開始されている。

(1) クラウド FPGA のセキュリティ問題と、PUF を用いた解決

クラウド FPGA で注意すべきは、ユーザは暗号化されていないデザインをサーバに提供する点と、サーバと FPGA 間のあらゆる通信は Shell（固定領域）を介して CPU 経由でやり取りされる点である。すなわち、クラウド側に悪意のある者がいる場合や脆弱性が（FPGA 以外に）存在する場合、平文の FPGA バイナリや演算データが盗まれてしまう可能性がある。これを解決するには、クラウド FPGA 上で、暗号化された FPGA バイナリを復号することや演算データを暗号化することが有効であるが、クラウド FPGA にどのように安全に暗号鍵を送るかという問題がある。この問題を解決するため、本研究ではクラウド FPGA 上に信頼起点となる PUF を構築し、これと楕円曲線暗号に基づく鍵共有方式を組み合わせる。PUF はデバイスのばらつきから固有の値を生成するため、同じ設計の PUF であっても異なる FPGA 上では異なる値を出力する。クラウド FPGA では PUF の以下の性質が特長的な利点となる。

（ア）平文の FPGA バイナリを見ても PUF の出力は分からない（FPGA 上で動作して初めて分かる）→ サーバ側に知られることなく、クラウド FPGA 上に秘密情報を生成し、鍵ペアを生成できる。

（イ）他の FPGA 上で動作させると異なる出力になる → 使用中の FPGA 以外に秘密は漏洩しない。

（ウ）不揮発性メモリを使わずに秘密情報を生成・復元できる → 不揮発メモリに鍵を書き込む場合、サーバに鍵を渡して書いてもらわざるを得ないが、そのような手順は不要。

(2) クラウド FPGA の新たな課題：リモートサイドチャネル攻撃（Side-Channel Attack: SCA）

SCA は暗号モジュールの消費電力や放射電磁波等の物理情報から秘密情報を抽出する攻撃である。SCA は物理情報を測定するため、従来は攻撃者の手元に攻撃対象がある必要がありサーバ側の脅威とは考えられていなかった。しかし 2018 年に Schellenberg ら[1] 及び Zhao ら[2] が、2019 年に Shanquan ら[3] が、クラウド FPGA 上に実装された不正回路を用いてリモート SCA が可能であることを示した。リモート SCA は PUF の出力及び暗号鍵を漏洩させる可能性のある深刻な脅威となり、上記（ア）～（ウ）の利点を危うくする可能性がある。そのためクラウド FPGA 上のシステムの安全性評価と対策が必須である。

２．研究の目的

本研究の目的は、クラウド FPGA の安全な利用を実現するために、クラウド FPGA 上にセキュアな PUF 及び暗号システムを構築しその実装可能性・安全性・有効性を実証することである。この目的達成のため、クラウド FPGA 上の PUF 及び暗号システムの以下の課題を解決する：

(A) FPGA 上の PUF はユニーク性やランダム性が低く、性能向上が必要。

(B) ランダム性の低い PUF は機械学習攻撃に対して脆弱であり[4]、対策が必要。

(C) クラウド上でサイドチャネル情報を収集するリモート SCA の可能性があり、対策が必要。

３．研究の方法

上で述べた課題(A)～(C)の解決のため、本研究では①～③の研究に取り組む。

① FPGA 上の PUF の高性能実装手法の研究開発

FPGA 上の PUF のユニーク性やランダム性を改善する手法の研究開発を行う。

②機械学習攻撃への耐性評価／耐性向上手法の研究開発

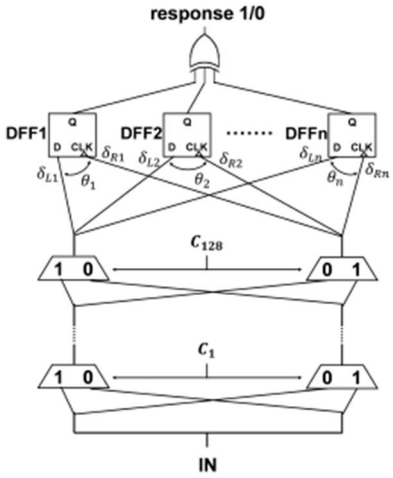
FPGA 上の PUF に対してディープラーニングを用いた機械学習攻撃を行い、安全性の評価と、攻撃耐性向上の研究開発を行う。

③クラウド FPGA 上の PUF 及び暗号システムに対するリモート SCA 対策の研究開発

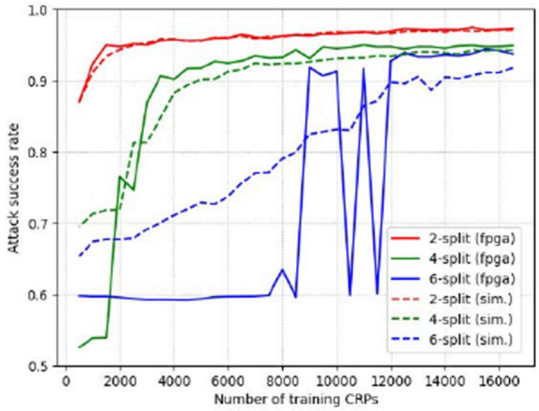
PUF 回路による信頼起点と楕円曲線暗号を含む暗号システムを実際に構築し、リモート SCA に対する安全性を評価及び防御手法の研究開発を行う。そのために、FPGA 上に PUF 回路、誤り訂正回路、鍵生成回路、暗号回路から成る暗号システムを実装する。また、暗号システムとは別の領域に、サイドチャネル情報をリモートで窃取するための不正回路である Time-to-Digital Converter（TDC）を実装する。

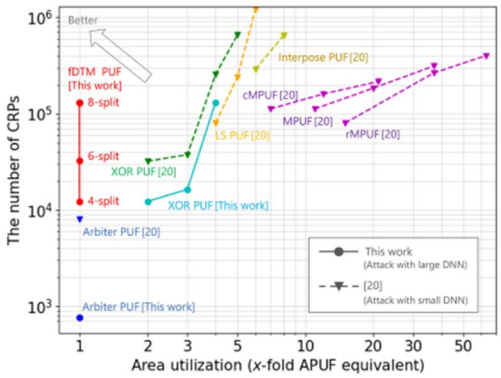
４．研究成果

(1) ①②について、FPGA 上に Arbiter PUF を実装し、ユニーク性および安定性を評価したところ、非常に高い性能を得た。FPGA 上の Arbiter PUF は性能が出づらいため、当初は別の PUF を実装する予定であったが、想定を上回る高い性能を出せたためこれを活用することとした。この Arbiter PUF をベースに、FPGA 上でもユニーク性・安定性が高く、機械学習攻撃に耐性のある PUF の開発を行った。従来提案されていた Multi-threshold 型の Arbiter PUF は、Arbiter 回路にセンスアンプが必要であるため、FPGA には実装できなかった。本研究では、複数のフリップフロップをアンバランスな位置において意図的に遅延差を作り出すことで、FPGA 向けの Multi-threshold 型 Arbiter PUF (Delay Time Measurement PUF (fDTM-PUF)と呼ぶ）を実現した。



fDTM-PUF をシミュレーションおよび FPGA 実装し、深層学習攻撃に対する耐性を評価した。その結果、fDTM-PUF は従来の Arbiter PUF と比較し高い攻撃耐性を有することが示された。また、fDTM-PUF は、攻撃対策を実装した他の改良 Arbiter 型 PUF の数倍から数十倍小さな面積でありながら、高い機械学習耐性を有することが示された。本成果は国際会議 AIHWS2024 で発表を行った[5]。





(2) ③について、PUF を信頼起点として利用するため、楕円曲線暗号およびハッシュ関数の FPGA 実装を行った。楕円曲線暗号のうち電子署名を実現する ECDSA と鍵交換を実現する ECDH のハードウェア、およびハッシュ関数 SHA256 を高位合成を用いて開発した。また、PUF を汎用システムで利用可能とするための RISC-V の実装を行った。さらに、ローカルの FPGA を対象に Time-to-Digital-Converter を実装し、リモートサイドチャネル攻撃の予備実験を行った。多数のフリップフロップが反転することで、TDC の出力が変化することを確認した。一方で、2024 年に国際誌 TCHES において LUT 1 個を用いた手法[6]が提案されたため、その調査と、より洗練された手法の検討を行った。

[1] Schellenberg, F. et al, “An inside job: Remote power analysis attacks on FPGAs,” DATE, 2018.
[2] Zhao, M., and Suh, G. E., “FPGA-based remote power side-channel attacks,” IEEE S&P, 2018.
[3] Tian, S., and Szefer, J., “Temporal thermal covert channels in cloud FPGAs,” FPGA, 2019.
[4] U. Ruhrmair, et al., “Modeling Attacks on Physical Unclonable Functions,” CCS2010, 2010.
[5] Oyama, T. et al, “FPGA Implementation of Physically Unclonable Functions based on Multi-threshold Delay Time Measurement Method to Mitigate Modeling Attacks,” in Proc. AIHWS2024, 2024.
[6] Jayasinghe, D. et al., “1LUTSensor: Detecting FPGA Voltage Fluctuations using LookUp Tables,” IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(1), pp51-86, 2024.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Tatsuya Oyama, Mika Sasaki, Yohei Hori, Toshihiro Katashita, Takeshi Fujino
２．発表標題 FPGA Implementation of Physically Unclonable Functions based on Multi-threshold Delay Time Measurement Method to Mitigate Modeling Attacks
３．学会等名 Artificial Intelligence in Hardware Security (AIHWS) 2024（国際学会）
４．発表年 2024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
研究分担者	今福　健太郎 (Imafuku Kentaro) (10298169)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員 (82626)	
研究分担者	片下　敏宏 (Katashita Toshihiro) (90500215)	国立研究開発法人産業技術総合研究所・エレクトロニクス・製造領域・主任研究員 (82626)	

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