REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
16-01-2023	Final Report	30-May-2016 - 29-Dec-2017

4. TITLE AND SUBTITLE

Final Report: W911NF-12-R-0012-03 Human-to-Device (H2D): A Novel Anti-Tampering Mechanism for DOD Applications Driven by Cardiovascular Biometric and Obfuscation (Research Area 5.35. Hardware Assurance)

5a. CONTRACT NUMBER

W911NF-16-1-0321

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES

University of Florida - Gainesville
219 Grinter Hall
PO Box 115500
Gainesville, FL 32611 -5500

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)

ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

69533-NC-YIP.12

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Domenic Forte
UU	UU	UU	UU		19b. TELEPHONE NUMBER 352-392-1525

RPPR Final Report
as of 25-Jan-2023

Agency Code: 21XD

Proposal Number: 69533NCYIP **Agreement Number: W911NF-16-1-0321**
INVESTIGATOR(S):

Name: Domenic Forte
Email: dforte@ece.ufl.edu
Phone Number: 3523921525
Principal: Y

Organization: **University of Florida - Gainesville**
Address: 219 Grinter Hall, Gainesville, FL 326115500
Country: USA

DUNS Number: 969663814 EIN: 596002052
Report Date: 29-Mar-2017 Date Received: 16-Jan-2023
Final Report for Period Beginning 30-May-2016 and Ending 29-Dec-2017
Title: W911NF-12-R-0012-03 Human-to-Device (H2D): A Novel Anti-Tampering Mechanism for DOD Applications Driven by Cardiovascular Biometric and Obfuscation (Research Area 5.35. Hardware Assurance)
Begin Performance Period: 30-May-2016 **End Performance Period:** 15-Jul-2020
Report Term: 0-Other

Submitted By: Domenic Forte Email: dforte@ece.ufl.edu
Phone: (352) 392-1525

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 2 **STEM Participants:** 5

Major Goals: The objectives for this entire research project (noted by year in brackets) were as follows:
1) ECG-based Key Generation and PPG-based User Authentication and Recognition (Year 1): While ECG-based identification had met with some success in the literature, its investigation with respect to stable, binary key generation (as required by H2D) was limited. ECG signals contain many types of noise such as baseline wander, powerline interference, electromyographic (EMG) noise, and electrode motion artifact noise as well as time-varying anomalies such as arrythmias. PPG-based biometric systems typically rely on fiducial features; that is, extraction of PPG landmarks based on time and amplitude. However, such approaches have a lower tolerance to noise, measurement conditions, and extraction algorithms. Our first objective was to quantize ECG signals into long, reliable, and high-entropy keys and to explore the accuracy of non-fiducial PPG features. This was accomplished by investigating feature extraction methods, dynamic models of ECGs/PPGs, their sources of noise, and optimized encoding algorithms.

2) Security Analysis of ECG-based Biometric Systems (Year 1) and Countermeasures (Year 3): The 7 criteria of the ideal biometric are as follows: (i) universality - possessed by all humans; (ii) distinctiveness - discriminative between individuals in the population; (iii) invariance- stable over time; (iv) collectability - quantifiably measurable; (v) performance - pertains to the availability of resources as well as achievable recognition accuracy and speed; (vi) acceptability - willingness of population to submit the attribute; and (vii) circumvention - reflects how easily a system can be fooled by a falsified biometric. While the first objective would show that how ECG could balance (i-iii) and years of ECG use in the medical field already support (iv-vi), resistance to circumvention remains uncertain. Thus, our third objective was to analyze the security of ECG systems to presentation attacks, and, if vulnerabilities were identified, to develop countermeasures.

3) Security Analysis of PCB Obfuscation including Simple Attacks (Year 1), Side-Channel Attacks (Year 2), and Countermeasures (Years 1 and 2): Previously, we developed the first ever PCB obfuscation approach. It relied on the addition of one obfuscation chip (a CLPD, FPGA, or ASIC) that permutes the connections between a programmable component (e.g., MCU or FPGA) and other chips on the PCB. Our objective here was to analyze the resistance of PCB obfuscation qualitatively and quantitatively (where possible) to non-invasive attacks (brute-force and side-channels) as well as invasive attacks (probing, reverse engineering, and tampering). Similar as above, countermeasures were developed as needed.

4) Practical Framework for Enrolling and Deploying H2D Systems (Years 2 and 3): According to ISO standards and GDPR, biometric systems and their associated biometric templates require 3 characteristics: irreversibility - the

process of obtaining the original biometric input from the protected template should be computationally difficult; unlinkability - preserves the privacy of a user so that an attacker cannot ascertain the user of a system; and revocability – a new biometric template could be issued if the prior one of a user was compromised. Our final objective was to develop a framework that ties biometrics and obfuscation together so that these characteristics are achievable. Compared to typical work in the area, we also set higher goals. That is, rather than only being mathematically secure, H2D biometric systems should also resist hardware security-based attacks against templates and authentication such as probing and fault injection.

Accomplishments: This project explored the security and reliability of these biometrics, PCB-level obfuscation, and their combination. While it was found that cardiovascular biometrics could generate reliable, cryptographic keys, a previously unknown vulnerability to presentation attacks was also discovered and demonstrated. A side-channel attack that exploited aging-related burn-in to non-invasively extract parts of the PCB obfuscation key was also identified. Countermeasures to these vulnerabilities were developed and shown to be effective. Finally, H2D systems were developed to provide secure authentication and template protection for both single- and multi-user applications.

Training Opportunities: Nothing to Report

Results Dissemination: The results of this project were disseminated through publications in conferences, journals, book chapters, and thesis. Further, they were presented at various conferences using powerpoint or posters. The venues can be found in the uploaded document.

Honors and Awards: 1) Zimu Guo and Nima Karimian, Awarded best hardware security poster at FICS Research Annual Conference on Cybersecurity 2016
2) Nima Karimian, Awarded best student paper at International Joint Conference on Biometrics (IJCB) 2017
3) Domenic Forte, NSF Faculty Early Career Development Program (CAREER) Award, 2017

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Domenic Forte
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Nima Karimian
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Zimu Guo
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)

RPPR Final Report
as of 25-Jan-2023

Participant: Janani Prakash
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Sumaiya Shomaji
Person Months Worked: 4.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Ulbert Botero
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Biomedical Engineering
Publication Identifier Type: DOI Publication Identifier: 10.1109/TBME.2016.2607020
Volume: 64 Issue: 6 First Page #: 1400
Date Submitted: 7/21/17 12:00AM Date Published: 6/1/17 8:00AM
Publication Location:
Article Title: Highly Reliable Key Generation From Electrocardiogram (ECG)
Authors: Nima Karimian, Zimu Guo, Mark Tehranipoor, Domenic Forte
Keywords: Authentication, biometrics, electrocardiogram (ECG), feature extraction, key generation, min-entropy, quantization, reliability, wavelet.
Abstract: Traditional passwords are inadequate as cryptographic keys, as they are easy to forge and are vulnerable to guessing. Electrocardiogram (ECG) is an emerging biometric that is extremely difficult to forge and circumvent, but has not yet been heavily investigated for cryptographic key generation. ECG has challenges with respect to immunity to noise, abnormalities, etc. In this paper, we propose a novel key generation approach that extracts keys from real-valued ECG features with high reliability and entropy in mind. Our technique, called interval optimized mapping bit allocation (IOMBA), is applied to normal and abnormal ECG signals under multiple session conditions. We also investigate IOMBA. Experiments of IOMBA show that 217-,38-, and 100-bit keys with 99.9%, 97.4%, and 95% average reliability and high entropy can be extracted from normal, abnormal, and multiple session ECG signals, respectively.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **N**

RPPR Final Report
as of 25-Jan-2023

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: ACM Transactions on Design Automation of Electronic Systems
Publication Identifier Type: DOI Publication Identifier: 10.1145/3035482
Volume: 22 Issue: 3 First Page #: 1
Date Submitted: 7/21/17 12:00AM Date Published: 4/1/17 8:00AM
Publication Location:
Article Title: Obfuscation-Based Protection Framework against Printed Circuit Boards Unauthorized Operation and Reverse Engineering
Authors: Zimu Guo, Jia Di, Mark M. Tehranipoor, Domenic Forte
Keywords: Board-level obfuscation, IP protection, unauthorized operation prevention, Benes network
Abstract: Most efforts to prevent cloning, overproduction, tampering, and unauthorized operation have only focused on the chip level, leaving a void for PCBs and higher levels of abstraction. In this article, we propose the first ever obfuscation-based framework for the protection of PCBs. Central to our approach is a permutation block that hides the inter-chip connections between chips on the PCB and is controlled by a key. If the correct key is applied, then the correct connections between chips are made. Otherwise, the connections are incorrectly permuted, and the PCB/system fails to operate. We propose a permutation network added to the PCB based on a Benes network that can easily be implemented in a CPLD or FPGA. Performance evaluation results on 12 reference designs show that brute force generally requires prohibitive time to break the obfuscation. We also provide detailed requirements for countermeasures for different classes of attackers.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **N**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 4-Under Review
Journal: IEEE Transactions on Dependable and Secure Computing
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 8/8/18 12:00AM Date Published:
Publication Location:
Article Title: EOP: An Encryption-Obfuscation Solution for Protecting PCBs Against Tampering and Reverse Engineering
Authors: Zimu Guo, Xiaolin Xu, Mark Tehranipoor, Domenic Forte
Keywords: PCB, obfuscation, anti-tamper, encryption, stream cipher
Abstract: PCBs are the core components for the devices ranging from the consumer electronics to military applications. Due to the accessibility of the PCBs, they are vulnerable to the attacks such as probing, eavesdropping, and reverse engineering. In this paper, a solution named EOP is proposed to migrate these threats. EOP encrypts the inter-chip communications with the stream cipher. The encryption and decryption are driven by the dedicated clock modules. These modules guarantee the stream cipher is correctly synchronized and free from tampering. Additionally, EOP also incorporates the PCBlevel obfuscation for protection against reverse engineering. EOP is designated to be accomplished by utilizing the COTS components. For the validation, EOP is implemented in a Zynq SoC based system. Both the normal operation and tampering detection performance are verified. The results show that EOP can deliver the data from one chip to another without any errors. It is proved to be sensitive to any active
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 25-Jan-2023

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: ACM Journal of Emerging Technologies in Computing Systems
Publication Identifier Type: DOI Publication Identifier: 10.1145/3371407
Volume: Issue: First Page #:
Date Submitted: 1/16/23 12:00AM Date Published: 1/28/20 10:00AM
Publication Location:
Article Title: Permutation Network De-obfuscation: A Delay-based Attack and Countermeasure Investigation
Authors: ZIMU GUO, SREEJA, CHOWDHURY, MARK TEHRANIPOOR, DOMENIC FORTE
Keywords: obfuscation; Permutation network; side channel attack; Transistor aging; Countermeasure
Abstract: Permutation based obfuscation has been proposed to protect hardware against cloning, overproduction, and reverse engineering with a secret key. In this paper, we propose a new attack where the key is determined by exploring path aging within the permutation network used for obfuscation. Both the theoretical analysis and experimental results are provided in simulation and hardware. The experimental results show the accuracy of identifying the key is over 80% and more than enough to reduce the number of brute force combinations required by an attacker. This attack accuracy reaches 100% when the permutation network has experienced sufficient degradation. Besides the attack, we also proposed a countermeasure which sweeps the permutation network configurations. Incorporating this low-cost countermeasure, the proposed attack becomes no better than brute force guessing.
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Access
Publication Identifier Type: DOI Publication Identifier: 10.1109/ACCESS.2019.2910753
Volume: 7 Issue: First Page #:
Date Submitted: 8/20/19 12:00AM Date Published: 4/12/19 8:00AM
Publication Location:
Article Title: Unlock Your Heart: Next Generation Biometric in Resource-Constrained Healthcare Systems and IoT
Authors: Nima Karimian, Mark Tehranipoor, Damon Woodard, Domenic Forte
Keywords: Internet of Things, ECG, biometric, quantization, PPG, noise, healthcare, resource-constrained, security, access control
Abstract: With the emergence of the Internet-of-Things, there is a growing need for access control and data protection on low-power, pervasive devices. Key-based biometric cryptosystems are promising for IoT due to its convenient nature and lower susceptibility to attacks. However, the costs associated with biometric processing and template protection are nontrivial for smart cards, and so forth. In this paper, we discuss the cost versus the utility of biometric systems and investigate frameworks for improving them. We propose the noise-aware biometric quantization framework (NA-IOMBA) capable of generating unique, reliable, and high entropy keys with low enrollment times and costs with several experiments. Implementation results show that incorporating noise models with NA-IOMBA reduces power and utilization overhead by more than 60% by adapting the pre-processing, feature extraction, and post-processing modules.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 25-Jan-2023

Publication Type: Journal Article Peer Reviewed: N **Publication Status:** 1-Published
Journal: The Journal of the Homeland Defense and Security Information Analysis Center (HDIAC)
Publication Identifier Type: Publication Identifier:
Volume: 6 Issue: 1 First Page #:
Date Submitted: 8/20/19 12:00AM Date Published: 3/28/19 4:00AM
Publication Location:
Article Title: Leave Adversaries in the Dark - BLOcKeR: Secure and Reliable Biometric Access Control
Authors: Fatemah Ganji, Nima Karimian, Damon Woodard, Domenic Forte
Keywords: biometric, hardware obfuscation, physical unclonable function
Abstract: Biometric technologies offer major advantages over conventional, legacy identification and authentication methods. In particular, they are more secure, accurate, reliable, and user-friendly. Traditional biometric systems are vulnerable to various physical attacks, which could result in the theft of biometric templates, illegal system access, denial of service, etc.. This holds especially true for systems operating in hostile environments, where resistance to such attacks is paramount, yet difficult to provide at a low cost. To provide such resistance to various attacks like those discussed above, we introduce a security framework called BLOcKeR—Biometric Locking by Obfuscation, Physically Unclonable Keys, and Reconfigurability
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **N**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2016 IEEE International Symposium on Circuits and Systems (ISCAS)
Date Received: 21-Jul-2017 Conference Date: 22-May-2016 Date Published:
Conference Location: Montréal, QC, Canada
Paper Title: Hardware security meets biometrics for the age of IoT
Authors: Zimu Guo, Nima Karimian, Mark Tehranipoor, Domenic Forte
Acknowledged Federal Support: **N**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: International Symposium for Testing and Failure Analysis (ISTFA)
Date Received: 21-Jul-2017 Conference Date: 10-Nov-2016 Date Published:
Conference Location: Fort Worth, Texas, USA
Paper Title: A New Methodology to Protect PCBs from Non-destructive Reverse Engineering
Authors: Zimu Guo, Bicky Shakya, Haoting Shen, Swarup Bhunia, Navid Asadizanjani, Domenic Forte, Mark Teh
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)
Date Received: 21-Jul-2017 Conference Date: 19-Dec-2016 Date Published:
Conference Location: Yilan, Taiwan
Paper Title: Aging Attacks for Key Extraction on Permutation-Based Obfuscation
Authors: Zimu Guo, Mark Tehranipoor, Domenic Forte
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 25-Jan-2023

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: International Conference on Biomedical and Health Informatics (BHI)
Date Received: 21-Jul-2017 Conference Date: 16-Feb-2017 Date Published:
Conference Location: Orlando, FL
Paper Title: Non-Fiducial PPG-based Authentication for Healthcare Application
Authors: Nima Karimian, Mark Tehranipoor, Domenic Forte
Acknowledged Federal Support: **N**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: ", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)
Date Received: 21-Jul-2017 Conference Date: 06-Mar-2017 Date Published:
Conference Location: New Orleans, LA
Paper Title: Human Recognition from Photo-plethysmography (PPG) Based on Non-fiducial Features
Authors: Nima Karimian, Zimu Guo, Mark Tehranipoor, Domenic Forte
Acknowledged Federal Support: **N**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE International Conference on Technologies for Homeland Security (HST)
Date Received: 21-Jul-2017 Conference Date: 26-Apr-2017 Date Published:
Conference Location: Waltham, MA
Paper Title: Noise Assessment Framework for Optimizing ECG Key Generation
Authors: Nima Karimian, Fatemah Tehranipoor, Zimu Guo, Mark Tehranipoor, Domenic Forte
Acknowledged Federal Support: **N**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE International Joint Conference on Biometrics (IJCB)
Date Received: 08-Aug-2018 Conference Date: 02-Oct-2017 Date Published: 01-Feb-2018
Conference Location: Denver, Colorado
Paper Title: On the Vulnerability of ECG Verification to Online Presentation Attacks
Authors: Nima Karimian, Damon Woodard, Domenic Forte
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)
Date Received: 08-Aug-2018 Conference Date: 19-Oct-2017 Date Published: 07-May-2018
Conference Location: Beijing, China
Paper Title: MPA: Model-assisted PCB Attestation via Board-level RO and Temperature Compensation
Authors: Zimu Guo, Xiaolin Xu, Mark Tehranipoor, Domenic Forte
Acknowledged Federal Support: **Y**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution: University of Connecticut
Date Received: 12-Aug-2018 Completion Date: 5/5/18 2:23AM
Title: Cardiovascular Biometrics to Secure the Internet of Things
Authors: Nima Karimianbahnemiri
Acknowledged Federal Support: **N**

RPPR Final Report
as of 25-Jan-2023

Publication Type: Thesis or Dissertation
Institution: University of Florida
Date Received: 08-Aug-2018 Completion Date: 8/8/18 8:00AM
Title: A Framework for Securing Digital Systems against Counterfeiting, Reverse Engineering and Tampering
Authors: Zimu Guo
Acknowledged Federal Support: **N**

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Domenic J Forte
Signature Date: 1/16/23 3:53PM

Abstract

The loss or capture of U.S. military systems could critically hinder DOD mission objectives and endanger lives. In this project, we investigated a new obfuscation approach referred to as “human-to-device” (H2D) authentication. H2D explicitly ties a system’s operation to certain authorized personnel by combining biometrics with new system (printed circuit board or PCB) level obfuscation approaches.

In H2D, obfuscated connections are controlled by a binary key generated from a user’s cardiovascular signal (ECG or PPG), which is never stored on the system. An electrocardiogram (ECG) records the electrical signal from the heart, often to check for different heart conditions. Photoplethysmograph (PPG) is a simple and low-cost optical technique that detects blood volume changes in the blood vessels through measurements at the skin surface. PPG sensors are included in many different wearable devices today. Unlike ECG, PPG measurements only need to be acquired from one side of the body, allowing it to be used in a larger number of access control applications. Compared to other biometrics, cardiovascular signals are touted for having several unique advantages, including: (i) robustness to circumvention; (ii) naturally satisfying user universality and liveliness; (iii) containing many distinctive features; and (iv) being continuous.

In H2D, only if an authorized biometric is applied will the system be activated/unlocked. The use of cardio signals as a biometric guarantee with high confidence that the authorized person is present, thus providing secure access control. Compared to other obfuscation approaches, the key provided from H2D is less vulnerable to theft, brute force attacks, cloning, and other forms of circumvention, thus making the system more robust against unauthorized access, reverse engineering, and cloning if captured by an enemy.

This project explored the security and reliability of these biometrics, PCB-level obfuscation, and their combination. While it was found that cardiovascular biometrics could generate reliable, cryptographic keys, a previously unknown vulnerability to presentation attacks was also discovered and demonstrated. A side-channel attack that exploited aging-related burn-in to non-invasively extract parts of the PCB obfuscation key was also identified. Countermeasures to these vulnerabilities were developed and shown to be effective. Finally, H2D systems were developed to provide secure authentication and template protection for both single- and multi-user applications.

Objectives

The objectives for this entire research project (noted by year in brackets) were as follows:

1) **ECG-based Key Generation and PPG-based User Authentication and Recognition (Year 1):** While ECG-based identification had met with some success in the literature, its investigation with respect to stable, binary key generation (as required by H2D) was limited. ECG signals contain many types of noise such as baseline wander, powerline interference, electromyographic (EMG) noise, and electrode motion artifact noise as well as time-varying anomalies such as arrythmias. PPG-based biometric systems typically rely on fiducial features; that is, extraction of PPG landmarks based on time and amplitude. However, such approaches have a lower tolerance to noise, measurement conditions, and extraction algorithms. Our first objective was to quantize ECG signals into long, reliable, and high-entropy keys and to explore the accuracy of non-fiducial PPG features. This was accomplished by investigating feature extraction methods, dynamic models of ECGs/PPGs, their sources of noise, and optimized encoding algorithms.

2) **Security Analysis of ECG-based Biometric Systems (Year 1) and Countermeasures (Year 3):** The 7 criteria of the ideal biometric are as follows: (i) *universality* - possessed by all humans; (ii) *distinctiveness* - discriminative between individuals in the population; (iii) *invariance*- stable over time; (iv) *collectability* - quantifiably measurable; (v) *performance* - pertains to the availability of resources as well as achievable recognition accuracy and speed; (vi) *acceptability* - willingness of population to submit the attribute; and (vii) *circumvention* - reflects how easily a system can be fooled by a falsified biometric. While the first objective would show that how ECG could balance (i-iii) and years of ECG use in the medical field already support (iv-vi), resistance to circumvention remains uncertain. Thus, our third objective was to analyze the security of ECG systems to presentation attacks, and, if vulnerabilities were identified, to develop countermeasures.

3) Security Analysis of PCB Obfuscation including Simple Attacks (Year 1), Side-Channel Attacks (Year 2), and Countermeasures (Years 1 and 2): Previously, we developed the first ever PCB obfuscation approach. It relied on the addition of one obfuscation chip (a CLPD, FPGA, or ASIC) that permutes the connections between a programmable component (e.g., MCU or FPGA) and other chips on the PCB. Our objective here was to analyze the resistance of PCB obfuscation qualitatively and quantitatively (where possible) to non-invasive attacks (brute-force and side-channels) as well as invasive attacks (probing, reverse engineering, and tampering). Similar as above, countermeasures were developed as needed.

4) Practical Framework for Enrolling and Deploying H2D Systems (Years 2 and 3): According to ISO standards and GDPR, biometric systems and their associated biometric templates require 3 characteristics: *irreversibility* - the process of obtaining the original biometric input from the protected template should be computationally difficult; *unlinkability* - preserves the privacy of a user so that an attacker cannot ascertain the user of a system; and *revocability* – a new biometric template could be issued if the prior one of a user was compromised. Our final objective was to develop a framework that ties biometrics and obfuscation together so that these characteristics are achievable. Compared to typical work in the area, we also set higher goals. That is, rather than only being mathematically secure, H2D biometric systems should also resist hardware security-based attacks against templates and authentication such as probing and fault injection.

ECG-based Key Generation and PPG-based User Authentication and Recognition

Summary of Major Accomplishments: (1) 3 Conference Publications and 1 Journal Publication; and (2) ½ of one PhD thesis.

Summary of Findings (by Conference and/or Journal Publication):

[1.1] *N. Karimian, M. Tehranipoor, D. Forte, "Non-Fiducial PPG-based Authentication for Healthcare Application", International Conference on Biomedical and Health Informatics (BHI), February 2017.*

In this paper, we compared PPG-based authentication with fiducial (landmark-based) and non-fiducial feature extraction methods. As shown in Figure 1, the main landmarks for PPG are systolic peak, dicrotic notch, and diastolic peak. For the second derivative of PPG, the a and b points are the first peak and valley respectively; the c, d, and e points occur after the location of the systolic peak and have much smaller amplitude. Even with pre-processing, peak detection can be undependable especially in the case of c, d, and e.

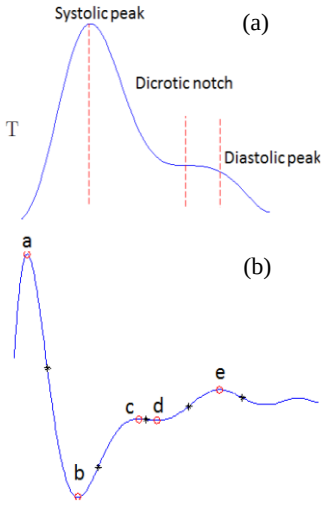


Figure 1. Plots illustrating common fiducial points extracted from (a) PPG signal and (b) its second derivative.

Non-fiducial methods operate in a holistic manner and are therefore less sensitive to noise in landmark detection. In our approach, only the systolic peak which is one of the easier landmarks to extract, needs to be detected. Once this peak is extracted, we take a window around it in each segmented PPG and apply the discrete wavelet transform (DWT). A support vector machine (SVM) and self-organizing map (SOM) were trained to classify 42 subjects from CapnoBase. K nearest neighbor (k-NN) was also applied for unsupervised learning.

Table 1. PPG non-fiducial vs. fiducial authentication.

		SVM	SOM	KNN
Non-Fiducial	Acc	99.75 ± 0.7	99.65 ± 0.9	99.84 ± 0.4
	EER	1.46 ± 2.7	1.70 ± 3.4	1.31 ± 2.6
Fiducial	Acc	91.46 ± 15.24	92.96 ± 15.44	93.76 ± 15.59
	EER	15.35 ± 20.22	11.52 ± 15.84	9.53 ± 15.92

In our evaluation, the target user was randomly chosen, and the experiments were conducted for 50 random trials. The average, standard deviation (STD) of accuracy, and equal error rate (EER) were calculated. The classification accuracy and EER for the above approaches is summarized in Table 1. Comparing the results of non-fiducial and fiducial, non-fiducial had better performance in terms of accuracy and EER. For example, the standard deviation value of fiducial result is 15.59 which is much more than non-fiducial one (2.6) since the features were not well-recognized in noisy signals for some of the subjects. Another one of our findings indicated that unsupervised learning methods had better performance compared to supervised ones, especially in fiducial feature extraction. It can be observed that non-fiducial method results in 99.75% of accuracy based on SVM classifier while fiducial features only succeed in accuracy of 91.46%. This demonstrated that non-fiducial features are far less dependent on peak detection correctness.

[1.2] *N. Karimian, Z. Guo, M. Tehranipoor, D. Forte, "Highly Reliable Key Generation from Electrocardiogram (ECG)" IEEE Transactions on Biomedical Engineering, Vol. 64, No. 6, June 2017.*

In this paper, we proposed a parameterizable key generation approach, called interval optimized mapping bit allocation (IOMBA), that extracts binary keys from real-valued ECG features. The IOMBA framework assumes that the input features and noise are Gaussian in nature – an assumption that was verified in our experiments. IOMBA's parameters, α and β, correspond to entropy and reliability, respectively. $\alpha \in [0,1]$ controls the uniformity of the quantized bits across the population of users while $\beta \in [0,1]$ controls the amount of statistical overlap or error that the designer will tolerate in the ECG features. According to these parameters and the statistics of user ECGs, optimal thresholds are chosen. The features of each user that meet these thresholds are then selected. Note that the indices and quantity of features may vary from user to user. Further, the number of bits that we quantize each feature to is also a variable under optimization. For example, higher entropy features shall result in more bits. Thus, the length of the quantized keys may also differ per user and per feature extraction method.

IOMBA was applied to normal and abnormal ECG signals from longitudinal studies of the PTB Diagnostic and BioSec.Lab databases. We also investigated IOMBA in the context of different feature extraction methods, such as wavelet, discrete cosine transform (DCT), normalize-convolute normalize (NCN), and variants to find the best method for feature extraction. Experiments of IOMBA showed that 217-, 38-, and 100-bit keys with 99.9%, 97.4%, and 95% average reliability and high entropy can be extracted from normal, abnormal, and multiple session (obtained weeks apart) ECG signals, respectively. By allowing more errors or lowering entropy, key lengths could be increased by tunable parameters (α and β) of IOMBA. These relationships are illustrated for abnormal ECGs in Figure 2. We also compared IOMBA to its closest counterpart, dynamic detection-rate-based bit allocation or DROBA which did not possess α and β parameters. While DROBA was able to generate longer keys compared to IOMBA, the key bit reliability was only 91.79% for normal ECG, 89.86% for abnormal ECG, and 65.02% for multiple session ECG. The min-entropy of keys from IOMBA were also higher in all cases.

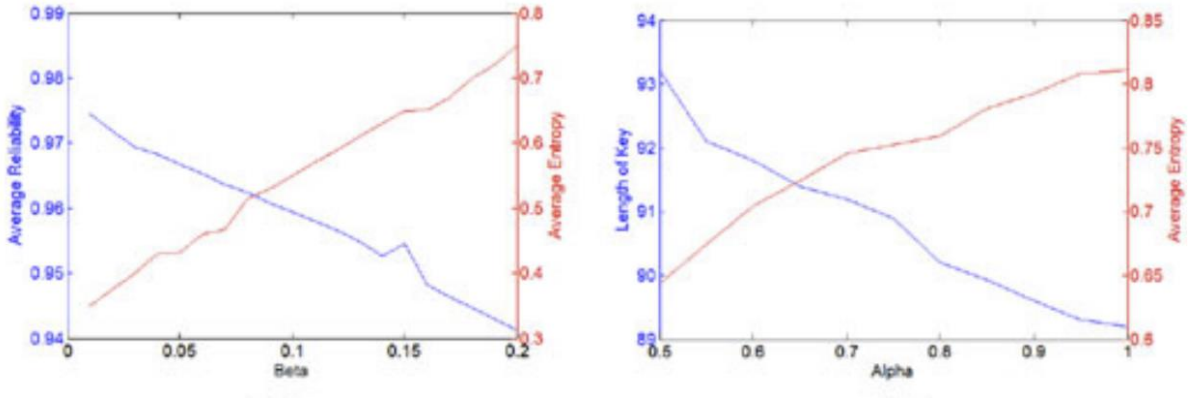
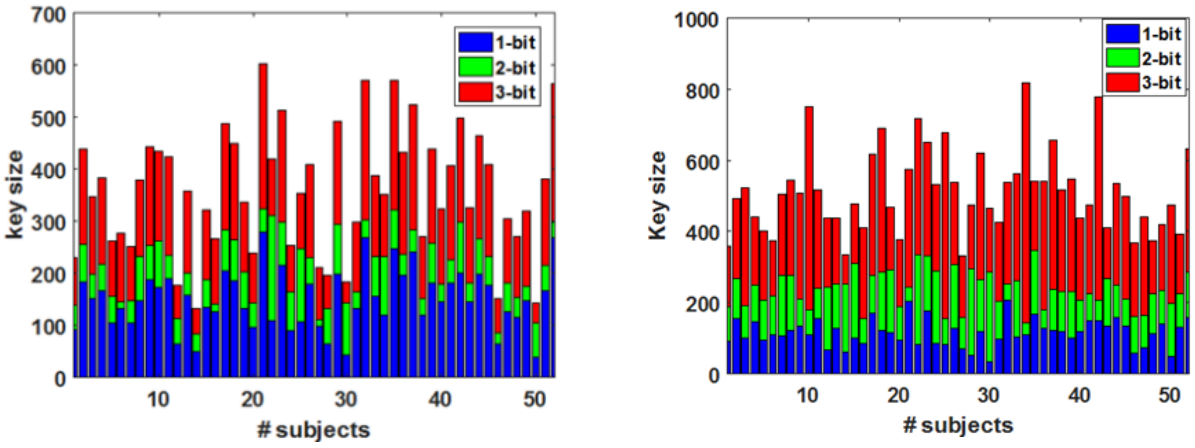


Figure 2. (left) Average reliability and min-entropy for abnormal ECGs verses β; (right) Impact of α parameter on key length and min-entropy.



(a) IOMBA (b) NA-IOMBA

Figure 3. Key length and number of bits per selected feature across subjects for (a) IOMBA and (b) NA-IOMBA.

[1.3] *N. Karimian, F. Tehranipoor, Z. Guo, M. Tehranipoor, D. Forte, "Noise Assessment Framework for Optimizing ECG Key Generation", IEEE International Conference on Technologies for Homeland Security (HST), April 2017.*

In this paper, we investigated the sources of noise and variability in ECG - power line interface, motion artifact (MA), baseline wander (BW), and electromyography (EMG) - which may result errors in key generation based on statistical quantization techniques. Since it is impossible to acquire ECGs at all conditions (e.g., different noise, stress conditions, etc.), we found that IOMBA's margin calculations and enrollment (see [1.2] above) could not account for all levels and types of noise experienced by ECGs. In addition, there may be resource-constrained scenarios where all pre-processing steps are too costly or energy consuming to perform.

To accommodate these issues, we proposed noise-aware IOMBA (NA-IOMBA) that predicts the impact of different noise sources and their scales on ECG keys. To this end, a synthetic ECG signal is generated from a preprocessed ECG and synthetic noise is added to predict its impact on key generation. Depending on the estimated impact and expected noise, IOMBA margins and boundaries are recomputed. While the original IOMBA personalizes features for each user, the proposed assessment framework builds on this personalization approach by accounting for expected noise. In fact, IOMBA assumes an average standard deviation of entire subjects. In NA-IOMBA, the standard deviation is considered as part of optimization per subject in order to further maximize the key length, reliability and entropy. Specifically, the NA-IOMBA optimization module determines new margins based on feedback from various noise (i.e., smallest margins to the most reliable features; highest margins to least reliable features).

Experiments from [1.2] were repeated for NA-IOBMA. Since the standard deviation is optimized for NA-IOMBA, some of the user's features that have been sacrificed from IOMBA could now be selected. Thus, we found that the average key length often increased from original IOMBA margin calculation. Another advantage of NA-IOMBA compared to IOMBA was that the subject's features that had not been selected in IOMBA could be chosen in NA-IOMBA, because the standard deviation is obtained from a dynamic optimization procedure. Hence, this is yet another reason why average key length of NA-IOMBA could increase from IOMBA. Figure 3 illustrates the key length for entire subjects based on IOMBA and NA-IOMBA, respectively. Minimum key length that can be extracted based in IOMBA is 133 while 331 keys can be achieved by NA-IOMBA. Average key length is 358 and 512 for IOMBA and NA-IOMBA, respectively. In addition, three

bits are extracted from the majority of features for NA-IOMBA as compared to one bit from IOMBA. Finally, we also found that reliability significantly improved in NA-IOMBA. Figure 4 shows the average reliability of key for IOMBA and NA-IOMBA vs. signal to noise (SNR) ratio. The minimum reliability of IOMBA for -5dB is 64.67% while the reliability of NA-IOMBA is 97.99%. Even at very low SNR (very noisy ECG) the NA-IOMBA was not affected by noise while the IOMBA was very sensitive to noise.

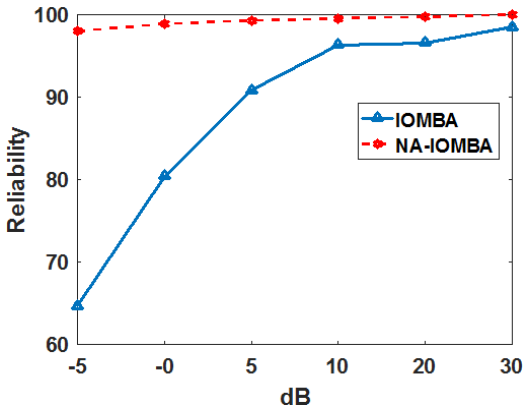


Figure 4. Comparison between IOMBA and NA-IOMBA across different levels of noise.

[1.4] *N. Karimian, Z. Guo, M. Tehranipoor, D. Forte, "Human Recognition from Photoplethysmography (PPG) Based on Non-fiducial Features", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), March 2017.*

In this paper, we expanded our analysis of non-fiducial features for PPG biometrics from user authentication (i.e., a one- to-one problem) to user recognition (i.e., a one-to-many problem). In addition to SVM, we also tested an artificial neural network (ANN). Further, the generic algorithm (GA) was also adopted for dimensionality reduction in both classifiers.

The classification accuracies for the above approaches are summarized in Table 2. One can see that the classification rate for SVM was better than NN for both fiducial and non-fiducial feature cases. Further, it's worth noting that NN not only provides weaker performance, but also requires more computational time than SVM. The identification rates for SVM also showed a significant improvement compared to NN. Moreover, the result of the SVM algorithm was more stable since it is not easily influenced by primal weighting values like the NN.

Table 2 also shows that the classification accuracies using dimensionality reduction outperformed the outcomes of fiducial feature extraction technique achieving identification rates of 100% as compared to 98.58% and 97.15% respectively. It was also observed that wavelet-based technique resulted in 99.23% of accuracy based on ANN classifier while fiducial features only succeeded in identification rate of 95.31%. As discussed before, fiducial features are more sensitive to noise which impacts the result while non-fiducial features are far less dependent on peak detection correctness.

Table 2. PPG fiducial vs non-fiducial recognition accuracy.

	Fiducial	Wavelet	Morphology
SVM	97.57	99.88	99.19
GA+SVM	98.58	100	100
ANN	95.31	99.23	99.18
GA+ANN	97.15	100	100

Security Analysis of ECG-based Biometric Systems and Countermeasures

Summary of Major Accomplishments: (1) 1 Conference Publication and 1 Journal Publication; (2) a Best Student Paper Award from the International Joint Conference on Biometrics (IJCB) 2017; and (3) ½ of one PhD thesis.

Summary of Findings (by Conference and/or Journal Publication):

[2.1] *N. Karimian, D. Woodard, D. Forte, "On the Vulnerability of ECG Verification to Online Presentation Attacks", International Joint Conference on Biometrics (IJCB), October 2017.*

In this paper, we developed the **first ever, full-fledged presentation attack against ECG biometric systems**. Previously, a replay attack was proposed in the literature against the Nymi wristband, a wearable device that supports daily and continuous authentication using fingerprints and ECG signals. ECG signals were recorded and replayed into the Nymi wristband using three different types of devices: arbitrary waveform generators (AWGs), computer sound cards, and off-the-shelf audio players. The replay attack achieved an 81% success rate assuming that the ECG was recorded and replayed from the same device. For the situation where an ECG was obtained from another source, a linear mapping function was employed to map the recording from one source to another. This case only achieved a 50% success rate at best.

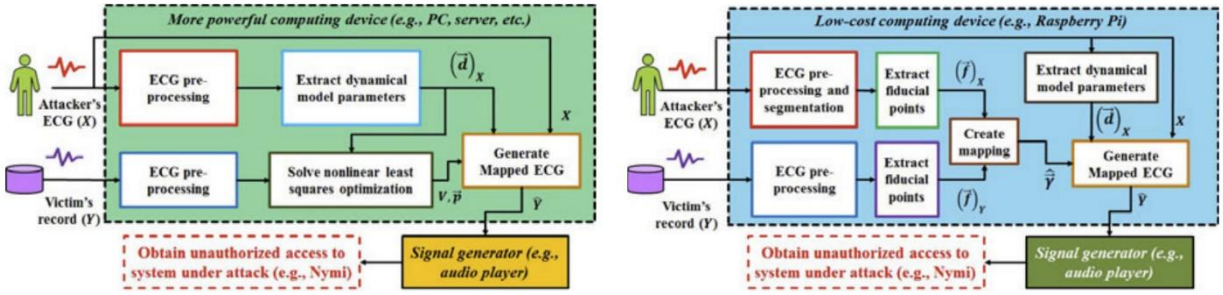


Figure 5. Block diagrams of offline (left) and online (right) presentation attacks.

Two types of our "cross-subject" presentation attack, offline and online, are illustrated in Figure 5. Both approaches involve exploiting dynamic ECG models, characterizing the differences between ECG signals, and developing mapping functions that transform any ECG into one that closely matches an authentic user's ECG. Our attacks assume that an adversary has physical access to a single heartbeat signal of the victim, which can be obtained through social engineering, compromising a medical database, taking a photo of the ECG plot, or sampling a legitimate user's ECG signal. Further, the attacks are independent of the authentication approach used by the biometric system. The offline approach employs an optimization formulation that is too expensive to solve using a low-cost device and in real-time. The online version uses standard ECG fiducial features and linearly maps the attacker's features to the victim's. Once the features are mapped, both approaches use a synthetic ECG modeling function to generate the ECG used in the attack.

In our experiments, the offline approach achieved average success rates of 97.43% and 94.17% for non-fiducial and fiducial-based ECG authentication when only one heartbeat was used. In the online scenario, the performance was degraded by 5.65% for non-fiducial based authentication

but nearly unaffected for fiducial authentication. With a longer victim record and longer time for authentication, success rates increased to more than 98%.

[2.2] *N. Karimian, D. Woodard, D. Forte, "ECG Biometric: Spoofing and Countermeasures", IEEE Transactions on Biometrics, Behavior, and Identity Science (T-BIOM), Vol. 2, No. 3, July 2020.*

In this paper, our presentation attack was expanded into a "cross-device" version where mapping functions were also used to reproduce ECGs collected on a source other than the victim's device and vice versa. Our approach uses a dynamic model of the dipole vector of the heart, that explicitly models the relationship between different ECG lead configurations and their positions. Figure 6 illustrates the attacker's ECG before and after mapping to the victim's ECG. The mapped one overlaps near perfectly with the victim's ECG signal. Cross-device attack results were compared to previous state-of-the-art replay attacks (linear mapping). Our results were superior with success rate of 96%, while the prior ones achieved only 66% success rate.

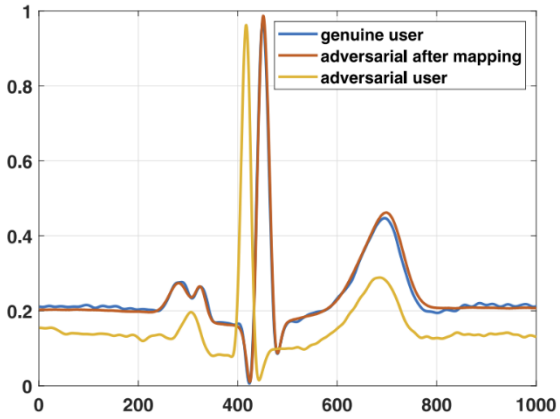


Figure 6. Comparison of victim's ECG signal, corresponding adversarial ECG signal and spoofed ECG after cross-device and cross-subject mapping.

We also proposed the **first ever countermeasures to ECG presentation attacks**. Our countermeasures utilize ECG signal characteristics such as heart rate variability (HRV) and PPG signal to detect and reject spoofed ECG samples. Analysis of variations in the instantaneous heart rate time series using the beat-to-beat RR-intervals is known as HRV analysis. HRV is known to be affected by exercise, stress, emotion, and heart disease. The heart rate may be increased by slow-acting sympathetic activity or decreased by fast-acting parasympathetic activity. The heart rate is given by the reciprocal of the RR-interval in units of beats per minute. Note that the normal heart rate varies continuously between 60 to 100 beats per minute (bpm). By changing HRV, the low and high frequency band may increase or decrease. Since we assume that the attacker only has access to one heartbeat of the victim, she does not know the victim's HRV. In such situations, the success rate of the attack degrades to 28%. The successful cases occurred when the attacker's HRV was similar to the victims (by chance).

For the latter countermeasure, it is assumed that the biometric system captures both ECG and PPG signals simultaneously and the victim's PPG is unknown by the attacker. Since PPG is rather uncommon compared to ECG, this is realistic. The pulse transit time (PTT) and pulse arrival time (PAT) of the PPG are matched to the victim's in a database. If they do not match, then the system considers the ECG a spoofed signal, does not process it, and reject's the user. If they do match, then the ECG signal is also checked for authenticity. This countermeasure was tested using ECGs and PPGs collected by the ProtoCentral MAX86150 in the MIMIC database. Presentation attacks were detected 100% of the time.

Security Analysis of PCB Obfuscation including Simple Attacks, Side-Channel Attacks, and Countermeasures

Summary of Major Accomplishments: (1) 2 Conference Publications and 2 Journal Publications; (2) 1 Book Chapter and 1 e-print; and (3) 1 PhD Thesis.

Summary of Findings (by Conference and/or Journal Publication):

[3.1] *Z. Guo, J. Di, M. Tehranipoor, D. Forte, "Obfuscation-based Protection Framework Against Printed Circuit Boards Unauthorized Operation and Reverse Engineering", ACM Transactions on Design Automation of Electronic Systems (TODAES), Vol. 22, No. 3, April 2017.*

In the proposed PCB obfuscation technique, permutation network inputs are signals connected to a programmable component, and the outputs are attached to non-programmable components. Permutation networks can be classified into blocking and non-blocking networks according to what input/output permutations can be achieved. A blocking permutation network is one that can only realize some of the possible input/output combinations. An example includes the Butterfly network. A non-blocking permutation network is one that can realize all input/output combinations with or without constraints. Examples include multiplexed based network and Benes network. Since PCB obfuscation requires flexibility in I/O combinations (to match any possible user's biometric key), non-blocking permutation networks are therefore deemed more appropriate. Due to its low area and power overhead, we identified the Benes network as the best candidate.

In this paper, we evaluated our PCB obfuscation technique to two brute force attack strategies: (i) on I/O combinations and (ii) on possible keys. We estimated the number of brute force attempts on I/O combinations required by an attacker to break the Benes Network implemented for 12 different PCB benchmarks (found on TI's website). In situations where dummy connections were added to the design, the worst case number of combinations was greater than 10^{17} and the average number of key combinations was even larger. Even assuming that each combination can be validated in one clock cycle (a very pessimistic condition), breaking the obfuscation would take several years.

In the Benes network, multiple keys can be used to achieve the same permutation which could lower the number of brute force attempts needed. We developed an approach to estimate the probability distribution of combinations required across the whole key space. Assuming a 32-bit Benes Network (32 inputs and 32 outputs), we found that for some keys the Benes network were more vulnerable than others. However, on average the probability of breaking the Benes network by brute forcing key combinations (strategy ii) was lower than that of I/O combinations (strategy i). This is illustrated in Figure 7.

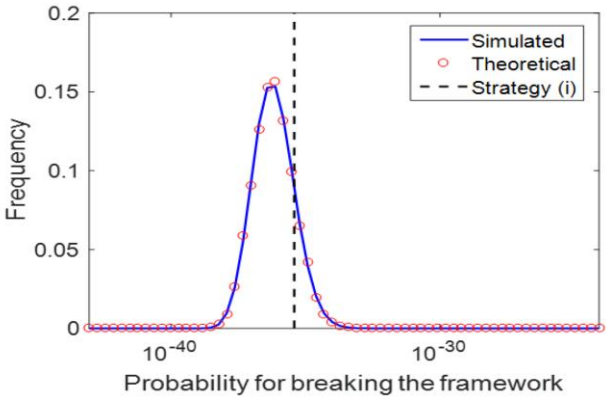


Figure 7. Comparison between probability of breaking H2D through brute force by Strategy i (dashed line) and Strategy ii (blue distribution).

[3.2] *Z. Guo, M. Tehranipoor, D. Forte, "Aging Attacks for Key Extraction on Permutation-Based Obfuscation," IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), December 2016.*

The PCB obfuscation scheme is assumed to store the applied obfuscation key in volatile memory, thus losing it whenever the system loses power. This was done by design in order to keep the secret key safe from invasive attacks and reverse engineering by well-funded attackers when the power is off. However, in this paper, we discovered that it was still remains possible to recover the erased key using non-invasive side channel attacks. Consider a powered off permutation chip which has been working for some time. Even if this key is erased after powering off the chip, some "hints" remain due to the chip aging phenomena. The term "hints" refers the information which can be exploited to discover the content of the key. Our attack framework utilized these "hints" to learn the secret key. Since the degree of transistors aging dependents on the inputs, different input patterns result in different path delays. The attack framework selects the permutation network's paths by manipulating the key. For each selected path, a delay profile is extracted. The secret key is derived by analyzing the measured delays.

In order to apply this attack, the adversary needs to measure several delay values between the inputs and outputs of the permutation network. These delay values are presented in Figure 8 for an 8-bit Benes network as the example. By measuring the delay values: t_{00}, t_{01}, t_{10} and t_{11}, the attacker can discover the correct key bit for a given element of the Benes Network. The decision rules are presented as following by checking the sign of $(\mathrm{t}_{00} + \mathrm{t}_{11} - \mathrm{t}_{10} - \mathrm{t}_{01})$. If the sign is positive, the normal operating key value guessed to be "0", otherwise, the normal operating key value is guessed to be "1".

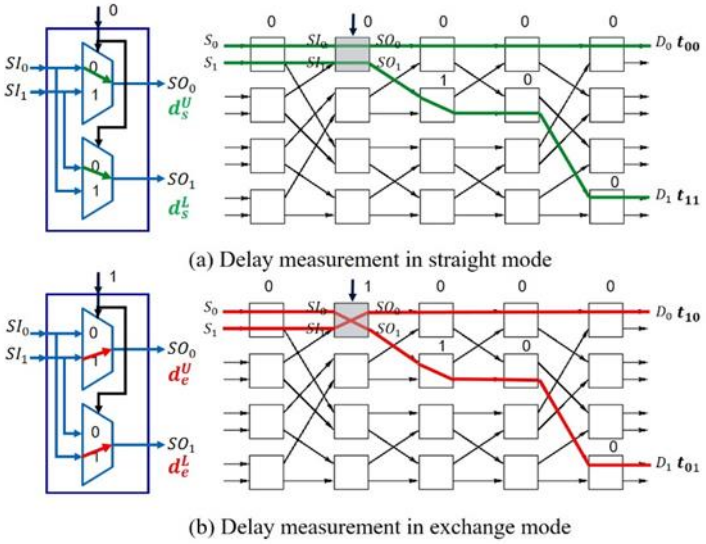
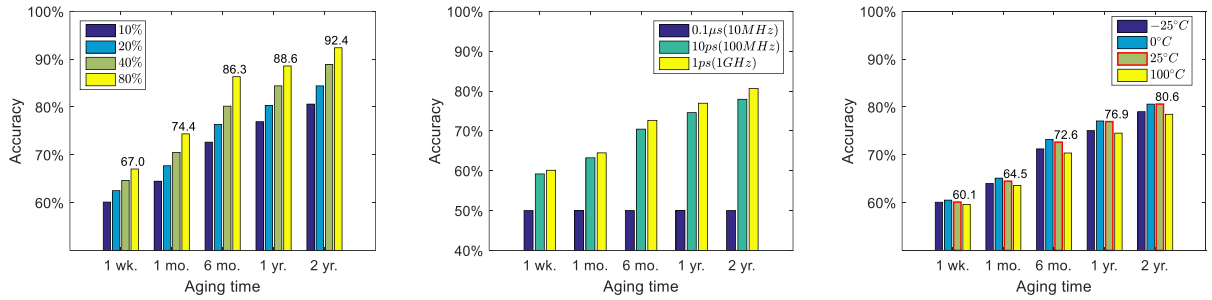


Figure 8. Delay measurements for recovery of each key bit

The proposed attack was simulated in Cadence HSPICE. The attacking accuracy is defined as the percentage of correct keys can be recovered. The comparisons of this attack accuracy under various conditions are provided in Figure 9. These conditions consist of aging length, temperature, measurement resolution, and circuit operation percentage. As the system is used more, it experienced more aging and the attack became more effective. For a system used 80% of the time for 1 week, the attack could successfully recover 67% of the secret key. When the usage time increased to 2 years, the rate of success grew to 92.4%. For delay sample rate of 100MHz or greater, we found that it was possible to execute the proposed attack. Finally, different voltage and thermal corners did not dramatically improve the results of the attack.



(c) Utilization analysis (b) Sampling rate analysis (a) Temperature analysis

Figure 9. Attack accuracy comparisons among various attacking conditions and different aging/use times.

[3.3] *Z. Guo, X. Xu, M. Tehranipoor, D. Forte, "MPA: Model-assisted PCB Attestation via Board-level RO and Temperature Compensation", IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), October 2017.*

In this paper, we investigated another approach to reverse engineering PCBs, including the proposed obfuscation approach, where an adversary monitors traces on the PCB. We also developed a novel approach called MPA that allowed the permutation chip to monitor PCB traces in order to detect the addition of probes, mod-chips, jumpers, desoldering/resoldering, etc. The MPA approach is shown in Figure 10(a). The traces are measured by oscillators (ROs) which are formed by a bank of inverters within the FPGA and the traces between chips on the PCB. The traces to monitor (shown in orange in Figure 10(a)) are few in number and only those typically targeted by probing or mod-chips. During startup, the chips are configured by JTAG into high-Z mode, which essentially disconnects them from the orange traces. This allows the orange traces connected to the chip pads, black traces, and inverter bank to form a closed ring. A counter measures the number oscillations of the trace, which is a function of the orange and black traces. If any change to these traces is made, the number of oscillations changes and can be detected according to a classification boundary.

Since oscillations are also a function of board/FPGA temperature, we have also included a thermal monitor to measure the temperature (see Figure 10(b)) and calibrate for it in the detection

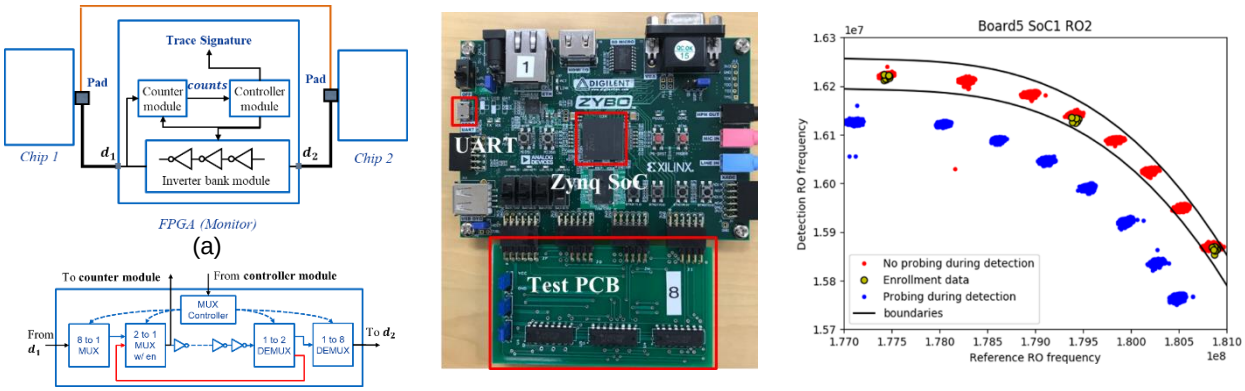


Figure 10. (a) FPGA-based RO trace monitor; (b) FPGA thermal monitor for temperature compensation; (c) experimental setup; and (d) distinction between tampered and non-tampered trace measurements.

scheme. The thermal monitor is a reference RO that uses the red internal trace of the inverter bank rather than the external black and orange traces on the PCB.

Figure 10(c-d) shows our experimental setup and results. In Figure 10(d), green dots represent measurements used to enroll the PCB trace signatures while red and blue dots represent non-tampered and tampered trace measurements respectively. The x and y axes represent frequency of the reference RO (i.e., temperature) and frequency of the trace monitor RO, respectively. Aside from a few outliers, there was a clear separating boundary between the two measurements across temperature. These results were confirmed on five boards, thus showing that tampering/probing can be easily detected by the MPA scheme.

[3.4] *Z. Guo, X. Xu, M. Tehranipoor, D. Forte. "EOP: An encryption-obfuscation solution for protecting PCBs against tampering and reverse engineering." arXiv preprint arXiv:1904.09516 (2019).*

In this paper, we proposed a cryptographic solution called EOP to counter attacks against obfuscated PCBs, which we classify as:

- SR-1: Passive tampering protection. The device shall prevent the disclosure of sensitive information on the PCB obtained by external monitoring of pins and traces.
- SR-2: Active tampering protection. The device shall monitor or prevent unauthorized changes to signals being communicated between chips on the PCB.
- SR-3: Run-time tampering protection. The device shall constantly guarantee SR-1 and SR-2 during any operation stages once the device is on.
- SR-4: Reverse engineering prevention. The PCB design shall be protected from any physical reverse engineering whether power is on or off.

SR-1 and SR-2 define the capability of a mechanism against tampering attack. This capability can be accomplished by either preventing or detecting tampering activities. SR-3 defines the tampering protection capability during runtime. SR-4 ensures that the system cannot be copied by applying a reverse engineering attack.

Figure 11 shows a block diagram of the EOP framework. This framework consists of four major modules: encryption module, decryption module, control clock generation module, and control clock verification module. The first two modules (referred as the crypto modules) encrypt and decrypt the messages from chip 1 and chip 2. The last two modules generate and verify the control clock that is used to drive the first two modules. These modules are elaborated below. In Figure 11, one-way communication is assumed between chip 1 and chip 2 (i.e., data are sent by chip 1 to chip 2) for simplicity. If two-way communication is desired, the control clock generation and

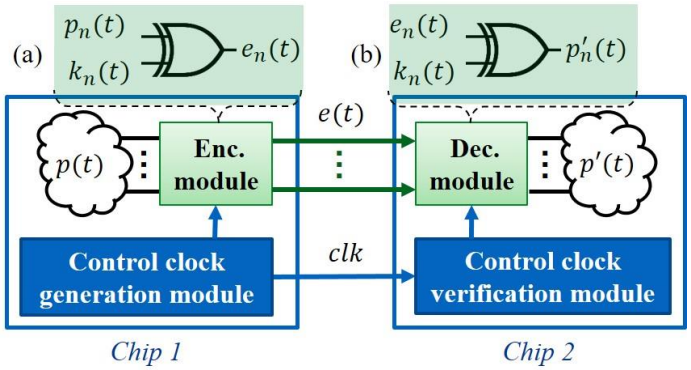


Figure 11. Block diagram of EOP. The internal logic of the encryption module (Enc. module) is presented in (a), and the internal logic of the decryption module (Dec. module) is presented in (b). The notations p, e, and k stands for the plain data, encrypted data, and key pad respectively

verification modules should be implemented in both chips.

The control clock generation module guarantees that a control clock pulse is produced when any data path changes its value. This control clock drives the stream cipher to produces the keypad vector and fetches new encrypted data. Thus, the encrypted data are generated slightly after the rising edge of the control clock pulse. The control clock verification module accepts the incoming encrypted data and control clock as its inputs. The output is the verification status which is either safe or tampered. This module verifies whether the received control clock is unmodified after generated. To achieve this goal, the flipping events of the control clock and encrypted data path are monitored. The verification status can be developed by comparing the recorded time instances.

EOP was created in hardware as shown in Figure 12. The Xilinx ZYBO development boards with the Zynq SoC are utilized to implement the sender and receiver. This SoC consists of a single-core ARM Cortex-A9 processor and a 28nm Artix-7 based programmable logic. A breadboard is used to connect the sender and receiver through jumper wires. The digital channels of the OSC are connected with this breadboard to monitor the plaintext data and decrypted data. These data are also sent to the host PC through the onboard UART.

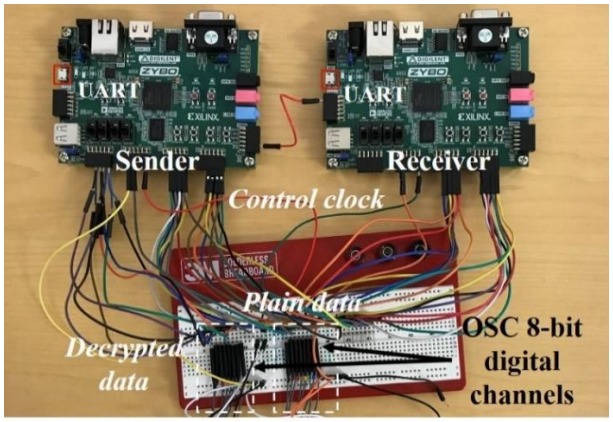


Figure 12. EOP hardware experiment setup.

As the nominal operation validation, no tampering was applied, and the validation target is the decryption correctness. The full encryption-decryption procedure was constantly executed for one hour under all frequency corners. The comparison between plaintexts of the sender and receiver was made. The number of mismatches were reported to the PC at the end of each evaluation. The experimental results demonstrated that the receiver can consistently decrypt the correct data and no decryption errors were found during all the experiments.

For the attack detection evaluation, a function generator and tristate buffers are utilized to actively tamper the connections between the sender and receiver. The function generator controls the tristate buffers to ground these connections for different durations. The basic unit of these durations was the shortest period for the sender to update the plain data (i.e., 200Mhz/5ns). The testing conditions and results are presented in Table 3. The first row indicates the tampering durations which are expressed as how many times of the smallest data path updating period (i.e., 5ns). Theoretically, one violation should be counted once when the tampering period is 5ns. However, since this tampering signal is not aligned with control clock and may last slightly longer than designed, more than one violation was sometimes recorded. This situation was rare, and only appeared when the tampering occurs right after a rising edge of the control clock.

Table 3. Violation counts under different tampering durations.

Tampering durations (5ns base)		1 ×	5 ×	10 ×	100 ×
Average violations	Control clock	1.02	5.08	10.05	100.01
	Data path	1.05	5.10	10.10	100.07

[3.5] *Z. Guo, S. Chowdury, M. Tehranipoor, D. Forte, "Permutation Network De-obfuscation: A Delay-based Attack and Countermeasure Investigation", ACM Journal on Emerging Technologies in Computing Systems (JETC), Vol. 16, No. 2, January 2020*

In the paper, we extended our prior side channel attack to the crossbar switches of a Clos network. The definition of the operation modes of a 4-to-4 crossbar switch is illustrated in Figure 13. The proposed attack was simulated in Cadence HSPICE. For the crossbar switch, the process variations may induce errors during key recovery. These errors were classified as the type of conflicts, such as the single conflict (SC). The conflicts were grouped into three level according to their commonness. The first-level conflicts consisted of the single and double conflicts (i.e., SC and DC). These are the most common conflicts. The due-double conflict (DDC) was classified as the second-level since it is less typical than the first-level conflicts. All the rest of the conflicts were considered as the third-level conflicts. Among all the conflicts, only the first-level conflicts are resolvable.

The conflict rates are presented in Figure 13(a) with respect to aging duration. According to this figure, the first-level and second-level conflicts accounted for more than 99% of all the conflicts. Moreover, the second-level conflict rates dropped rapidly as the aging duration grew. These rates became negligible after about 250 days of normal usage. The conflict rates decrease since effects of the aging gradually override the process variations and environmental noise. Thus, the first-level conflicts became the dominating factors which affected the attack accuracy. Figure 5(b) shows the attack accuracy and the performance of the conflict resolution technique of the proposed attack. More first-level conflicts could be successfully resolved with longer aging duration. Since the SC and DC contribute most of the conflicts, the attack accuracy followed the same trend of the conflict resolution rate. The attack accuracy converged to 100% after 400 days of normal operation.

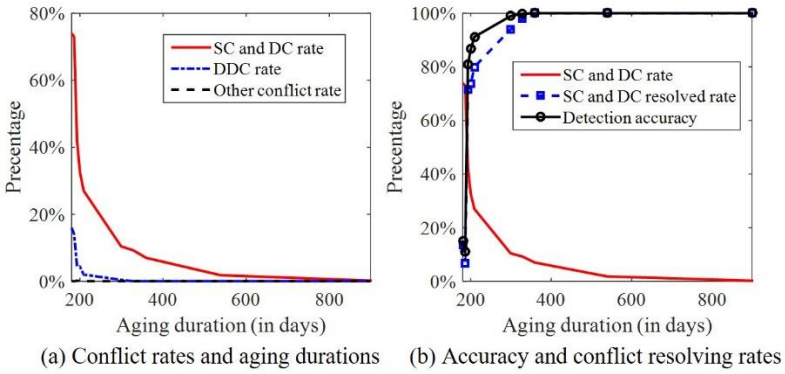


Figure 13. Crossbar switch simulation results for the Clos network. (a) The relationship between the conflict rates and the aging durations. (b) The performance of the conflict resolving performance and overall attack accuracy.

In this paper, we also implemented our previous attack on 8-by-8 Benes network implemented within an FPGA. Thus, the permutation network was formed by transmission gates. Five SoCs were utilized to implement five Benes networks. These SoCs are labeled as SoC '1' to '5' in Table 4. During the hardware experiments, an accelerated aging procedure was executed under the high-temperature condition. Compared to the prior simulation results, the proposed attack framework showed even better performance on the hardware (> 90%). One reason could be that the SoCs which are engaged in our experiments were fabricated in more advanced technology (28nm).

Finally, countermeasures were proposed to prevent the side channel attack. Since the "hints" provided to the attack are based on aging, the idea behind the proposed countermeasure was to

Table 4. Attack accuracy of the Benes network implemented in SoCs					
Accelerated aging durations	SoC 1	SoC 2	SoC 3	SoC 4	SoC 5
60 min	54.1%	48.5%	47.1%	67.1%	54.7%
360 min	60.5%	64.2%	62.0%	74.2%	59.1%
660 min	71.4%	69.4%	71.5%	75.0%	62.3%
960 min	75.1%	71.7%	78.2%	81.2%	65.1%
1560 min	77.9%	75.5%	80.2%	89.1%	70.2%
2160 min	81.5%	77.8%	92.1%	91.0%	75.2%
2760 min	85.8%	76.5%	93.3%	93.7%	79.9%
3360 min	91.2%	83.2%	93.5%	94.1%	85.1%
3960 min	92.1%	91.7%	93.4%	94.2%	92.4%

equally utilize all the regions of the switches and tri-state buffers during the normal operation. This ensures that aging is unform and the hints are minimized.

For the Benes network, a complementary key always exists to make the aging uniform. This complementary configuration can be attained by flipping all the key bits from the original configuration. For the Clos network, its string-sense non-blocking property can be utilized to compute complementary configurations. The initial key can be arbitrarily selected based on permutation requirement. Next, one input-output pair is selected. This input should be routed to its corresponding output following the tri-state buffers which are not activated by the initial key. Once this input-output pair is rerouted, the algorithm moves to another pair and stops when all the input-output pairs are rerouted. This procedure can be repeated until as many of the tri-state buffers are covered. All the covered tri-stated buffers are expected to be activated with the same probability during the normal operation.

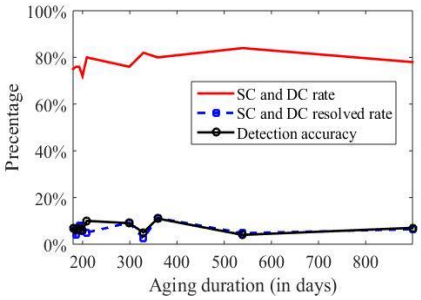


Figure 14. Clos network simulations results with countermeasure.

The proposed countermeasure was validated using simulations and silicon for the Benes network. The total aging duration as set as two years for the HSPICE simulation. For the hardware, the accelerated aging duration is set as 3960 minutes. Each of the two keys occupied roughly half of the time during the aging/accelerated aging. Both the simulation and hardware results showed an average attack accuracy around 50%, which is no better than a random guess. The attack accuracies without the countermeasure were previously over 80% (simulation) and 90% (hardware).

For the Clos network, half of the tri-state buffers were covered and experienced the similar degradations during the normal operation. Even though the optimal condition is full coverage (all the tri-state buffers are equally used), the half coverage created enough confusion for the attacker. Figure 14 provides the simulation results with the countermeasure applied. According to this figure, the persistently high single and double conflict rates indicate that the countermeasure induced significant errors. Moreover, the conflict resolution rate and the attack accuracy remained low (< 10%) even after 800-days of normal operation, which was also close to a random guess on the Clos network. Without the countermeasure, these rates reached 100% in simulations.

Practical Framework for Enrolling and Deploying H2D Systems

Summary of Major Accomplishments: (1) 1 Conference Publication and 2 Journal Publications; and (2) 2 chapters in 2 PhD Theses.

Summary of Findings (by Conference and/or Journal Publication):

[4.1] *Z. Guo, N. Karimian, M. Tehranipoor, D. Forte, "Hardware Security Meets Biometrics for the Age of IoT", IEEE International Symposium on Circuits and Systems (ISCAS), May 2016.*

In this paper, we laid this initial groundwork for H2D systems. That is, we described the challenges of implementing an H2D system such as biometric key reliability, biometric template protection, and revocability, biometric privacy, and low-cost signal processing and feature extraction. Preliminary results for board level obfuscation and IOMBA-based key generation were provided. For the latter, we compared the reliability, entropy, and average key length obtained by IOMBA for normal ECGs, irises, and faces. The results are shown in Table 5. Comparing the three biometric modalities on average, ECG provided the longest key and highest reliability while iris exhibited the highest 1-bit entropy. We drew the conclusion that ECG was likely the best candidate for our key generation approach due to its high quality and difficulty to circumvent. Comparing with the cumbersome high-definition cameras utilized to capture iris images, capturing ECG signals also only requires small, lightweight, and wearable sensors.

Table 5. Reliability and Entropy Analysis of Biometric Based Key Generation Algorithm

Biometric Modalities		Normal ECG	Iris	Face
Reliability	Average	0.994	0.953	0.959
	Minimal	0.979	0.906	0.826
	Maximal	1.000	1.000	1.000
Entropy	1-bit	0.7431	0.8550	0.7723
	2-bit	0.5187	0.0100	0.4898
	3-bit	0.2826	0.0000	0.1342
Average Key length		418	168	71

[4.2] *F. Ganji, N. Karimian, D. Woodard, D. Forte, "Leave Adversaries in the Dark- BLOcKeR: Secure and Reliable Biometric Access Control", The Journal of the Homeland Defense and Security Information Analysis Center (HDIAC), Vol. 6, No. 1, Spring 2019.*

In this paper, the single-user version of our H2D framework - Biometric Locking by Obfuscation, Physically Unclonable Keys, and Reconfigurability (BLOcKeR) – was proposed. In this framework, biometrics and hardware obfuscation are combined with physical unclonable functions (PUFs). The reconfigurability is required to enable the hardware obfuscation to be configured to work with any authentic user's biometric key. We analyzed the resistance to various attacks and other useful properties and highlighted the benefits.

BLOcKeR Enrollment Flows. The BLOcKeR enrollment flows are presented in Figure 15. In this figure, the three major phases are marked by different lines: the hardware enrollment in solid lines, the ownership claim in short, dashed lines, and the firmware customization in long, dashed lines.

Hardware enrollment is accomplished before the device is sent to the market and occurs in a trusted environment. During this step, the design house (e.g., DoD) or other trusted party (e.g., defense contractor) builds a strong PUF model for each device using a dedicated firmware, and stores the models in a secure database. The firmware enables the designer to efficiently collect

a sufficient number of challenge response pairs (CRPs) to accurately predict the PUF's behavior through machine learning. After enrolling the PUF model, access to the PUF is disabled (ideally in hardware). Since neither the user nor attacker has high-speed and direct access to the PUF CRPs after this point, the prediction model is therefore accessible only to the designer.

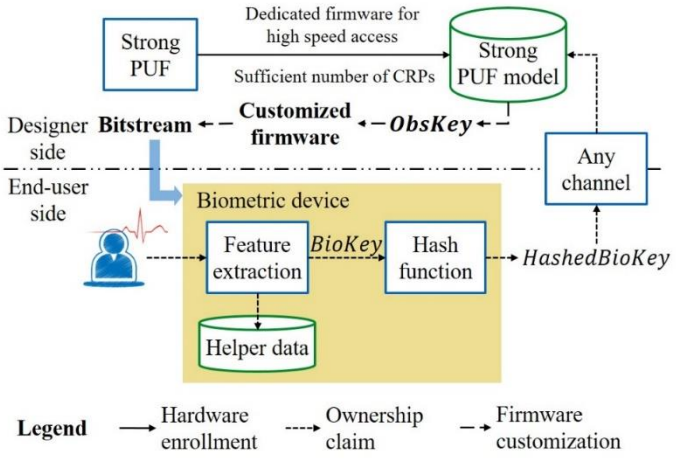


Figure 15. The BLOcKeR enrollment flow consists of the hardware enrollment, ownership claim, and firmware customization.

To register and operate the device, the *ownership claim* step is taken by the legitimate user. In the case of military applications, the owner could be a soldier. The user's ownership is taken by presenting his/her biometric signal to the device. A pre-processing algorithm is applied on the received biometric to extract a binary key (*BioKey*). Along with this process, necessary helper data (i.e., error correction code or ECC) might be generated for correcting errors in BioKey during later authentication steps. To generate the PUF challenge, the BioKey is processed by a secure hash function to the desired length. We refer to the values returned by the hash function as *HashedBioKey*. Due to the non-invertible property of a secure hash function, the raw biometric key, BioKey, cannot be deduced. Thus, *HashedBioKey* may be transmitted to the designer through any public channels without dedicated protections. Note that in BLOcKeR, the raw biometric template is also never stored on the device nor sent to the designer/vendor. This protects the privacy of the user's/solider's biometric.

When the PUF challenge is received by the designer, the *firmware customization* step occurs. This is where the previous strong PUF prediction model (from hardware enrollment) is beneficial. The challenge is fed into the strong PUF model to compute a unique device and biometric dependent response, which will behave as an obfuscation key *ObsKey*. An obfuscated bitstream is produced that exploits this obfuscation key. The obfuscated bitstream is sent to the user and loaded into the device. Note that since the physical device with the PUF is no longer accessible to the designer/vendor, this step is only possible with the previously generated strong PUF model in the vendor's possession. In addition, since this bitstream is generated by the device's PUF and user's biometric, it is unique and will only work with the enrolled device and user.

BLOcKeR Authentication Flow. During the authentication process (shown in Figure 16), the user provides his/her biometric as input. The same pre-processing algorithm as the enrollment process is applied to generate the *BioKey*. Potential errors are corrected with the helper data. Next, the hash function creates the challenge. The *ObsKey* is then generated by applying this challenge to the strong PUF. Different from the enrollment process, this obfuscation key is generated on the physical device's PUF

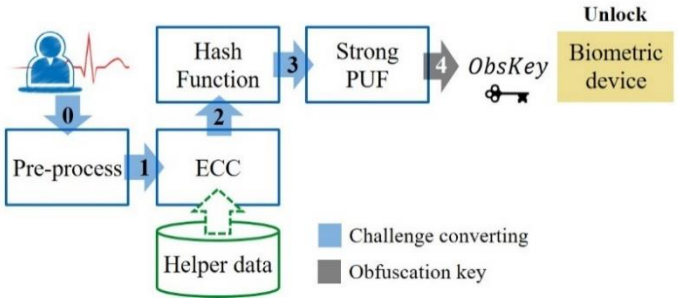
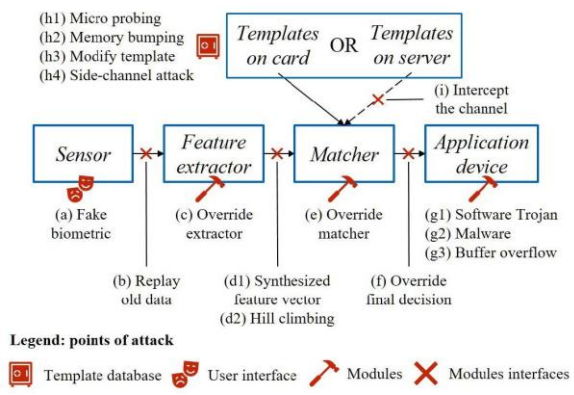


Figure 16. The BLOcKeR authentication flow: the user's biometric is firstly converted to the PUF challenge. A key is generated from this challenge to unlock the device.



Point of Attack	Attacks	Current Solutions	Limitations
User interface	(a) Fake biometric	Liveness detection	Sensor cost increase
Modules interface	(b) Replay old data (d1) Synthetic feature vector (d2) Hill climbing (f) Override final decision (i) Intercept the channel	Channel encryption; Time-stamp	Power/timing over-head
Modules	(c) Override extractor (e) Override matcher (g1) Software Trojan (g2) Malware (g3) Buffer overflow	Secure code execution; Software obfuscation	Dedicated hardware
Template database	(h1) Micro probing (h2) Memory dumping (h3) Modify template (h4) Side-channel attack	Salting; Non-invertible transform	Template collision

Figure 17. (left) Points of attacks against a traditional biometric system; (right) Limitations of existing solutions to these points of attack.

instead of its prediction model. A correct ObsKey unlocks the obfuscated bitstream and brings the device into functional (unlocked) mode. Without the correct key, the device will not work correctly. For example, it will be unable to access data, perform critical protocols, etc. due to errors in the hardware caused by the incorrect key. Note once again that the biometric template, BioKey, HashedBioKey, and ObsKey are never stored in non-volatile (permanent) memory on the card/device or on a server.

It's also important to note that since the obfuscation key is generated from the PUF circuit, it may be subjected to various environmental noise such as temperature instability, supply voltage fluctuation, etc. To address these errors, an additional ECC module can be implemented for the PUF.

Resistance to Attacks. Figure 17 illustrates the points of attack in a traditional biometric system along with current prevention mechanisms and their limitations. BLOcKeR addresses these issues without imposing any significant limitations. For instance, BLOcKeR avoids communication and storage of any form of the biometric template (raw, salted, encrypted, or quantized) at server and device/card. Thus, it eliminates all the attacks which target a stored template. In Figure 17, the attacks (h1-h4) and (i) cannot be applied due to the absence of the attack target. BLOcKeR also overcomes attacks on matching schemes (even invasive and semi-invasive physical attacks such as circuit edit and fault injection), since no such scheme is implemented in our system. Instead, BLOcKeR uses a fuzzy extractor that is often paired with a PUF to address the issue with the noisy measurements. Hence, the attack (f) depicted in Figure 17 is prohibited due to the absence of the matcher module in BLOcKeR. Nevertheless, the attacker may still attempt to apply the hill climbing attack by injecting the synthesized feature vector. This attack improves the key in a bit-wise manner by observing the behavior of the system. All the key bits should be examined before the termination of the attack. However, BLOcKeR's hardware obfuscation thwarts this attack by magnifying any single-bit error. For instance, a single-bit difference in an FPGA LUT may alternate a NAND gate to an XOR gate. This alteration may randomly change the system behavior, and this randomization will not benefit the attacker in obtaining the correct key.

The only points of attack that remain against BLOcKeR are (a) presentation attacks and (g) software attacks against the applications used within the system protected by the biometric system. If ECG/PPG are used, then presentation attacks can be overcome as described in [2.2]. The other attacks are out-of-the-scope for a biometric system and require traditional security protection approaches.

Last but not least, compared to chip-based obfuscation techniques that are vulnerable to so-called oracle attacks, BLOcKeR is resistant. Oracle attacks use the obfuscated design and correct I/O patterns from an unlocked system to non-invasively reverse engineer the obfuscation key. In BLOcKER, the key is stored in volatile memory. Like modern smart phones, access to the system times out after a short period of time and the power to the memory is removed, thereby destroying the key and re-locking the system. This removes that ability of an attacker to obtain enough I/O pairs from the system. Furthermore, this also protects BLOcKeR from invasive probing attacks. Since the key is not permanently stored on the device, it cannot be extracted by time-consuming probing attacks on the obfuscation chip.

[4.3] *S. Shomaji, Z. Guo, F. Ganji, N. Karimian, DL Woodard, D. Forte, "BLOcKeR: A Biometric Locking Paradigm for IoT and the Connected Person", Journal of Hardware and Systems Security (HaSS), Vol. 5, No. 3, Oct. 2021.*

In this paper, we expanded BLOcKeR to multiple users, analyzed the new framework in terms of ISO standard criteria, and measured the obfuscation output using simulations and incorrect biometric keys.

To incorporate multiple users, two assumptions were made:

- The device is authorized for multiple legitimate users during enrolment stage. However, when it is post-enrollment stage, one user is attempting to use the device at a time. Hence, other valid users are not present near the device when a single authorized user is trying to get access in it.
- Each user will be assigned an index no. while using the device and it will be fixed. For example, let's assume Mr. X is an authorized user among the multiple users. He is user no. '1'. That means, when he will try to use the device, along with his biometric template, he has to input his user index as '1'.

Once the user inputs his biometric template and user index, the template is hashed. Next, using hashed template, an architecture of Merkle tree, and user index value, the device finds the specific

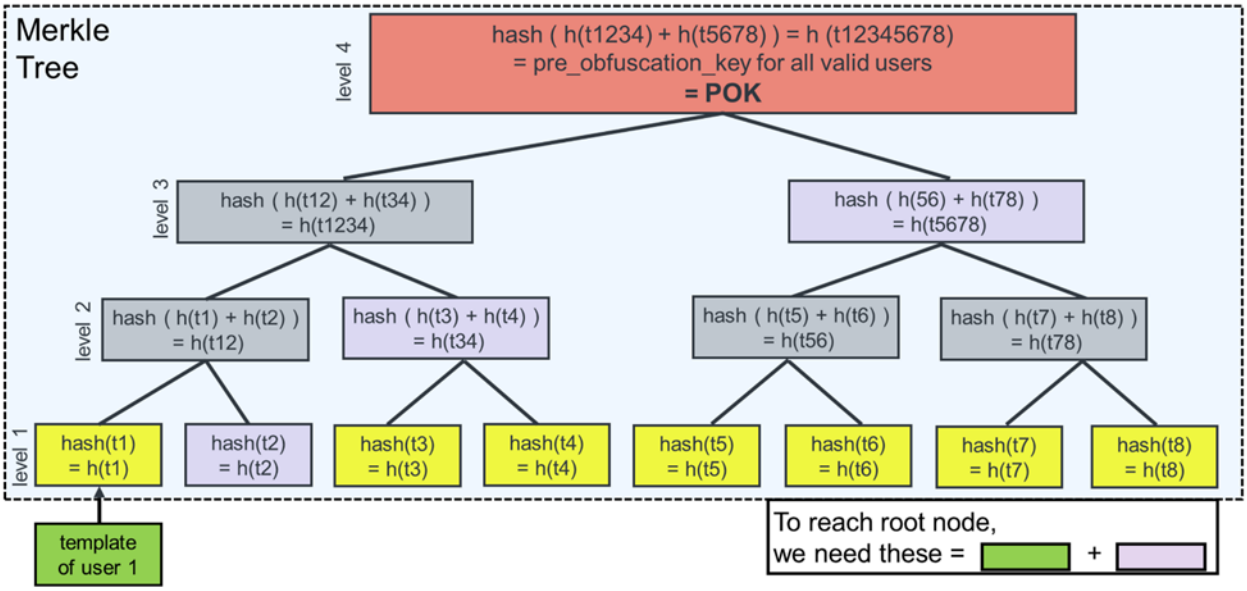


Figure 18. Merkle tree implemented for generating POK in post-enrollment stage.

nodes which are required to generate the root value (=POK) of the tree. An advantage of the Merkle tree is that, in order to track back the root value, we don't need to know all the leaf node values; instead, only few node values are needed to reach the root. The detailed diagram of this Merkle tree can be found in Figure 18.

Regarding BLOcKeR's ability to satisfy irreversibility, unlinkability, and revocability, we drew the following conclusions. First, since no raw, quantized, or encrypted version of the template is stored, the attacker cannot extract the user's original template. Further, the modified template is constructed using a collision-free hash function. Therefore, even if the attacker gets hold of the modified template, she cannot reverse it back to the original one, which denotes BLOcKeR's irreversibility property. Second, the unlinkability property is provided by the one-way hash as well as the PUF (another one-way function). Furthermore, auxiliary data (e.g., helper data) used by BLOcKeR is not made public. This adds another layer of protection because it cannot be used to link the same user to multiple devices. Finally, the BLOcKeR architecture from [4.2] was updated to incorporate supplementary data (random data or password) when the modified biometric template is generated. If the authentic user's biometric template is ever compromised, the authentic user can re-enroll in the system using a different supplementary data. This creates a new challenge for the PUF and therefore a new key. Thus, the firmware that obfuscates the design also needs to be updated.

We performed some attack experiments on BLOcKeR with face templates from publicly available "faces94" datasets. There are 152 classes or individuals in the dataset and each having 20 samples. We examined the case where an unauthorized user tries her biometric in the obfuscate system in single- and multi-user implementations of BLOcKeR.

Single authorized user case: For this experiment, we assumed that only the first user (user index = 1) among 152 users is an authorized user, who is designated to use the device. His template was used while generating the obfuscation key as well as obfuscating the design in enrollment stage. To illustrate, at first, the authorized user's face template was hashed and sent to a PUF as challenge in enrollment stage. The response was collected accordingly to create a key. Using this key, the design was obfuscated. Then in the post enrollment stage, when the same user is attempting to use the device, our objective was to observe what kind of output patterns can be found from the obfuscated design when the authorized user provides the correct obfuscation key which was derived from his biometric template.

To perform this, we provided the device 10,000 input patterns and collected 10,000 output patterns (with each output pattern having 39 bits). We did the same for other unauthorized users, i.e., generated obfuscation keys from their templates and providing the same input patterns and obfuscation keys to the obfuscated design developed in enrollment stage. Note that, we did not obfuscate the design with these unauthorized users' template derived obfuscation keys. Obfuscation took place only once by the OEM, with the authorized user's template derived obfuscation key. Therefore, as a returning user, when the authorized user is attempting to use the device in post enrollment stage, the output he is getting from the obfuscated design is always different from the output when other unauthorized users are attempting to use the same device. To demonstrate the difference, we calculated hamming distances (HDs) between the 10,000 output patterns from the obfuscated key from authentic user vs. when rest 151 unauthorized users are using the device. The overall average hamming distance was 25%. Figure 19 demonstrates the comparison of output patterns between 1 authorized user and 151 unauthorized users.

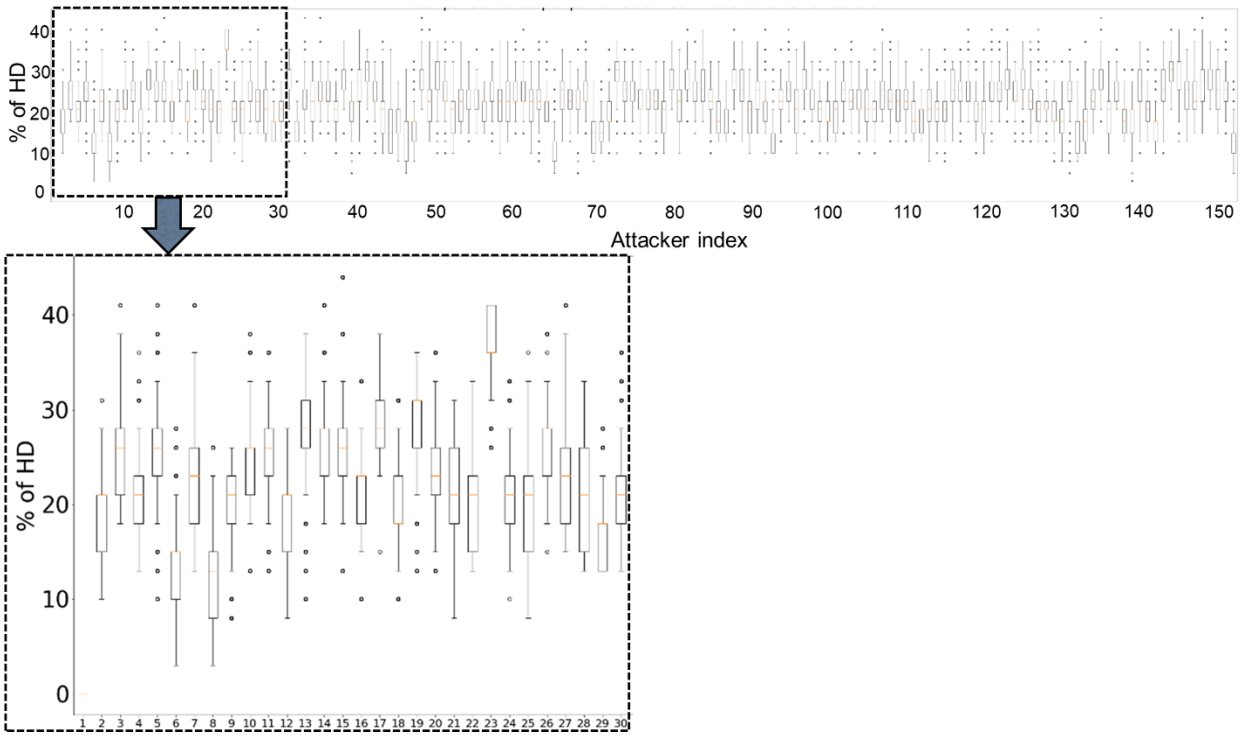


Figure 19: Comparison of output patterns between 1 authorized user and 151 unauthorized users.

Then we specifically determined which unauthorized samples have highest similarity with the only authorized user. We performed hamming distance (HD) again on the features of the users to find the similarity. There were 28 unauthorized users out of those 151 people, who showed around 75% similarity to the authorized user. Therefore, we exclusively calculated HD between the output patterns for authorized user and these 28 unauthorized users. The comparison between user's output and unauthorized user's outputs has been plotted in Figure 20. Here, x-axis shows the index of all the users. Index 1 belonged to authorized user. Index 2 → 29 belonged to all those unauthorized users. The y-axis demonstrates the % of bit flip or difference when output from user with index 'x' is compared to that of authorized user. The figure clearly shows that even if the unauthorized users possess high similarity with the authorized user, their output still hd around 20% difference from authorized user's output.

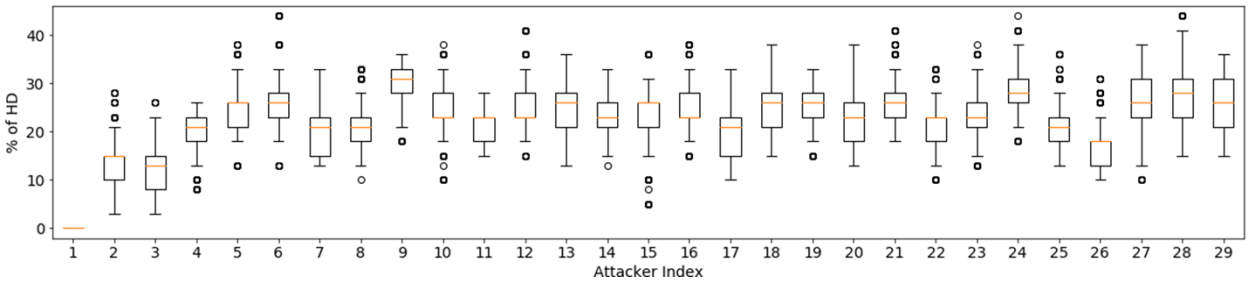


Figure 20: Comparison of output patterns between 1 authorized user and 28 unauthorized users.

Multi-authorized user case: The intruder should never be able to access the device. Because the device was obfuscated by designer using an obfuscation key which was derived from a pre-obfuscation key (POK). Here the POK is directly dependent on each authentic user's biometric

key. Therefore, when an intruder attempts to use the device, first she must provide his biometric template which will be used to produce the POK first. Since she has different biometric template than the user he is pretending to be, the POK generated by the intruder will be totally different from the original POK generated due to the hashing. As a result, the obfuscation key production will be wrong too. With this wrong key, she will never be able to unlock and use the obfuscated design, like the single user case.