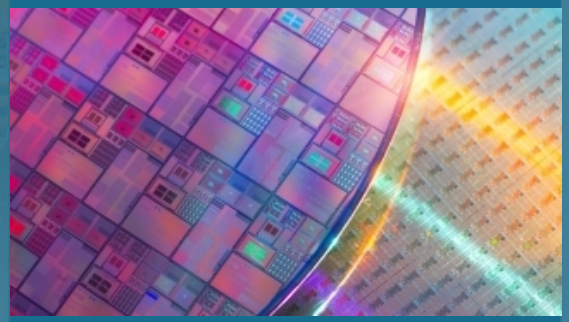
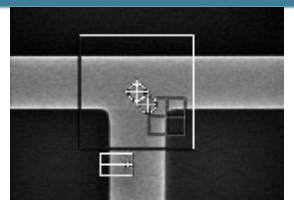
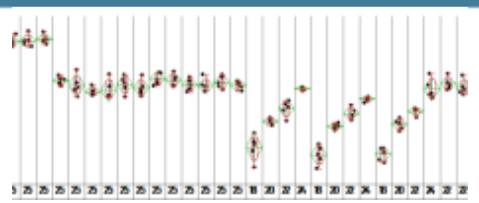
SAND2023-08203C

Sandia National Laboratories

Microelectronics that are continuously verifiable by their users…as inspired by cryptography







Dr. Nick Pattengale, Sandia National Laboratories

Presented in the half day workshop - **Securing the U.S. Electronics Supply Chain** – at the 2023 DARPA Electronics Resurgence Initiative 2.0 Summit

Thursday, August 24, 2023

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY NNSA

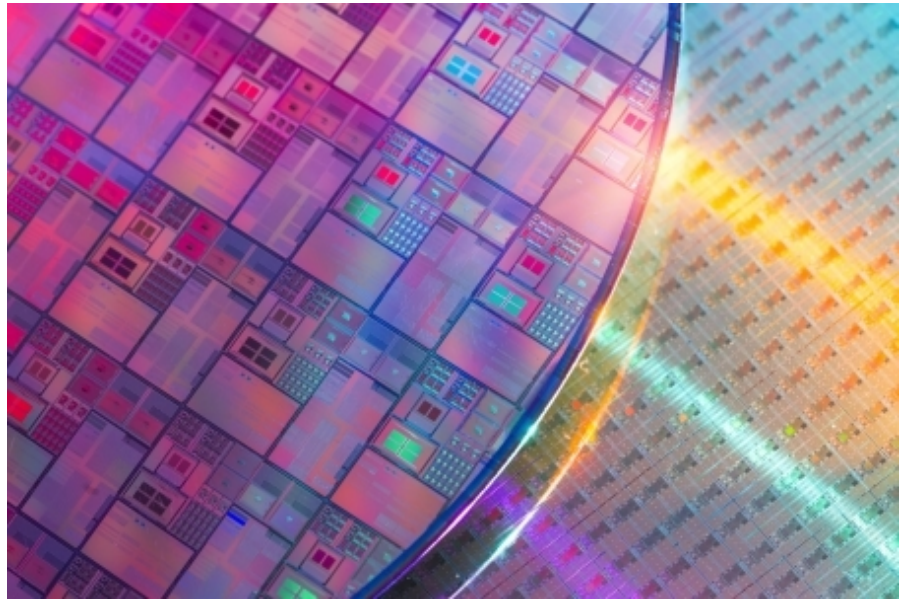
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

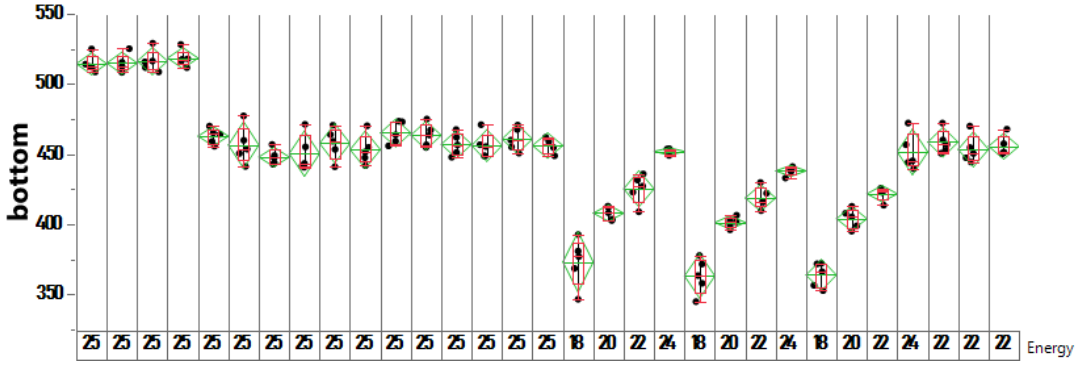
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

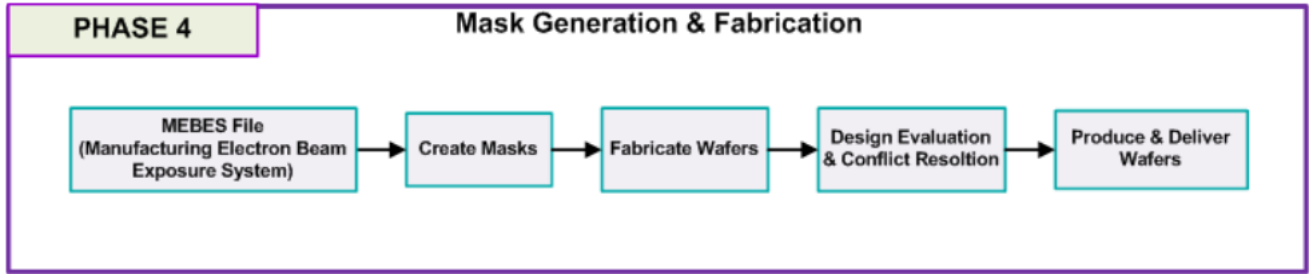
SAND2023-08203C

Outline

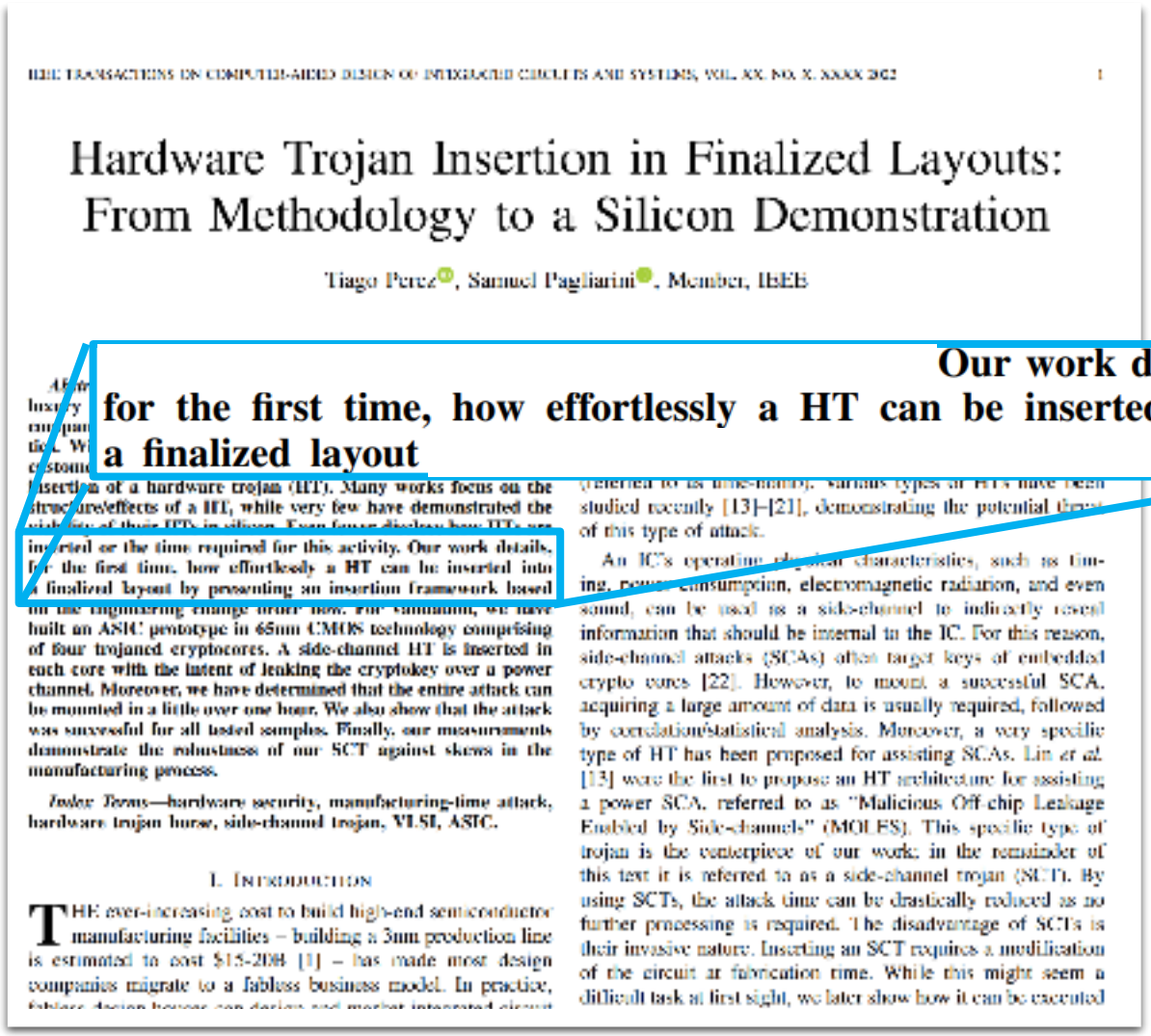
- Motivation
- Audacious Vision
  - Current approaches, limitations
  - What is different about our approach?
- Tangible starting points
- Measuring success







Motivation



IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. XX, NO. X, XXXX 20XX 1

Hardware Trojan Insertion in Finalized Layouts: From Methodology to a Silicon Demonstration

Tiago Perez, Samuel Pagliarini, Member, IEEE

Abstract—The insertion of a hardware trojan (HT). Many works focus on the structure/effects of a HT, while very few have demonstrated the viability of their HTs in silicon. Even fewer disclose how HTs are inserted or the time required for this activity. Our work details, for the first time, how effortlessly a HT can be inserted into a finalized layout by presenting an insertion framework based on the engineering change order flow. For validation, we have built an ASIC prototype in 65nm CMOS technology comprising of four trojaned cryptocores. A side-channel HT is inserted in each core with the intent of leaking the cryptokey over a power channel. Moreover, we have determined that the entire attack can be mounted in a little over one hour. We also show that the attack was successful for all tested samples. Finally, our measurements demonstrate the robustness of our SCT against skews in the manufacturing process.

Index Terms—hardware security, manufacturing-time attack, hardware trojan horse, side-channel trojan, VLSI, ASIC.

I. Introduction

THE ever-increasing cost to build high-end semiconductor manufacturing facilities – building a 3nm production line is estimated to cost $15-20B [1] – has made most design companies migrate to a fabless business model. In practice, fabless design houses can design and market integrated circuits (referred to as ICs) while relying on third-party foundries to manufacture their designs. Various types of HTs have been studied recently [13]–[21], demonstrating the potential threat of this type of attack.

An IC's operating physical characteristics, such as timing, power consumption, electromagnetic radiation, and even sound, can be used as a side-channel to indirectly reveal information that should be internal to the IC. For this reason, side-channel attacks (SCAs) often target keys of embedded crypto cores [22]. However, to mount a successful SCA, acquiring a large amount of data is usually required, followed by correlation/statistical analysis. Moreover, a very specific type of HT has been proposed for assisting SCAs. Lin *et al.* [13] were the first to propose an HT architecture for assisting a power SCA, referred to as "Malicious Off-chip Leakage Enabled by Side-channels" (MOLES). This specific type of trojan is the centerpiece of our work; in the remainder of this text it is referred to as a side-channel trojan (SCT). By using SCTs, the attack time can be drastically reduced as no further processing is required. The disadvantage of SCTs is their invasive nature. Inserting an SCT requires a modification of the circuit at fabrication time. While this might seem a difficult task at first sight, we later show how it can be executed

Our work details, for the first time, how effortlessly a HT can be inserted into a finalized layout

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9956883

dr0wned – Cyber-Physical Attack with Additive Manufacturing

Sofia Belikovetsky
Ben-Gurion University of the Negev

Mark Yampolskiy
University of South Alabama

Jinghui Toh
Singapore University of Technology and Design

Jacob Gatlin
University of South Alabama

Yuval Elovici
Ben-Gurion University of the Negev, Singapore University of Technology and Design

Abstract

Additive manufacturing (AM) has numerous socioeconomic, environmental, and

life cycle of a functional part. We develop a sabotage attack against a specific 3D-printed quadcopter propeller, causing its mid-flight failure, ultimately leading to the quadcopter's fall and destruction. The study described in this paper presents the very first full chain of attack against AM. We present all stages of the attack, beginning with a cyber-attack aimed at compromising a manufacturing environment and ending with the destruction of the target system that employs this part. Among major scientific

with 33.8% of all AM-generated objects used as functional parts. Due to the computerization involved in AM and the differences in the production environment compared to traditional manufacturing, several researchers have raised concerns regarding its security, including intellectual property violation [20, 37, 30, 22, 15, 4, 8] and sabotage [28, 38, 41, 31, 42, 43].

In this paper, we focus on the latter – presenting a

We develop a sabotage attack against a specific 3D-printed quadcopter propeller, causing its mid-flight failure, ultimately leading to the quadcopter's fall and destruction.

https://www.usenix.org/system/files/conference/woot17/woot17-paper-belikovetsky.pdf

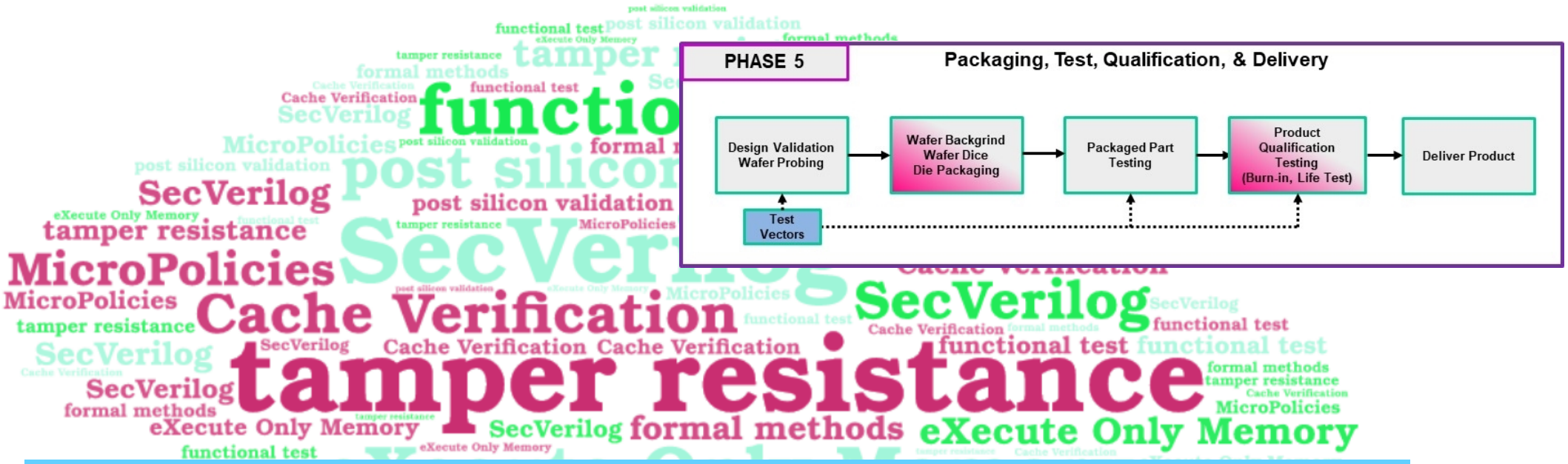
Audacious Vision

Users must be able to continuously measure and verify that…
- chip operations are to (chip) requirements
- only requested chip operations are performed
- real time security attributes (entropy, emanations, etc.)

Manufacturers needn't sacrifice confidence in their sensitive/proprietary

Gaps this exposes
- users must trust manufacturers, entire supply chain
- very little assurance capability exposed *post-boot*
- manufacturers must trust other entities (e.g. mask shop)

Current Practice, Limitations



Gaps this exposes

- users must trust manufacturers, entire supply chain
- very little assurance capability exposed *post-boot*
- manufacturers must trust other entities (e.g. mask shop)

Current Trends, do they address our vision?

- Zero Trust Architecture (ZTA) emphasizes continuous authentication
- Our vision (hardened data architectures) **complements** ZTA by measuring and verifying data, when possible, for intrinsic properties

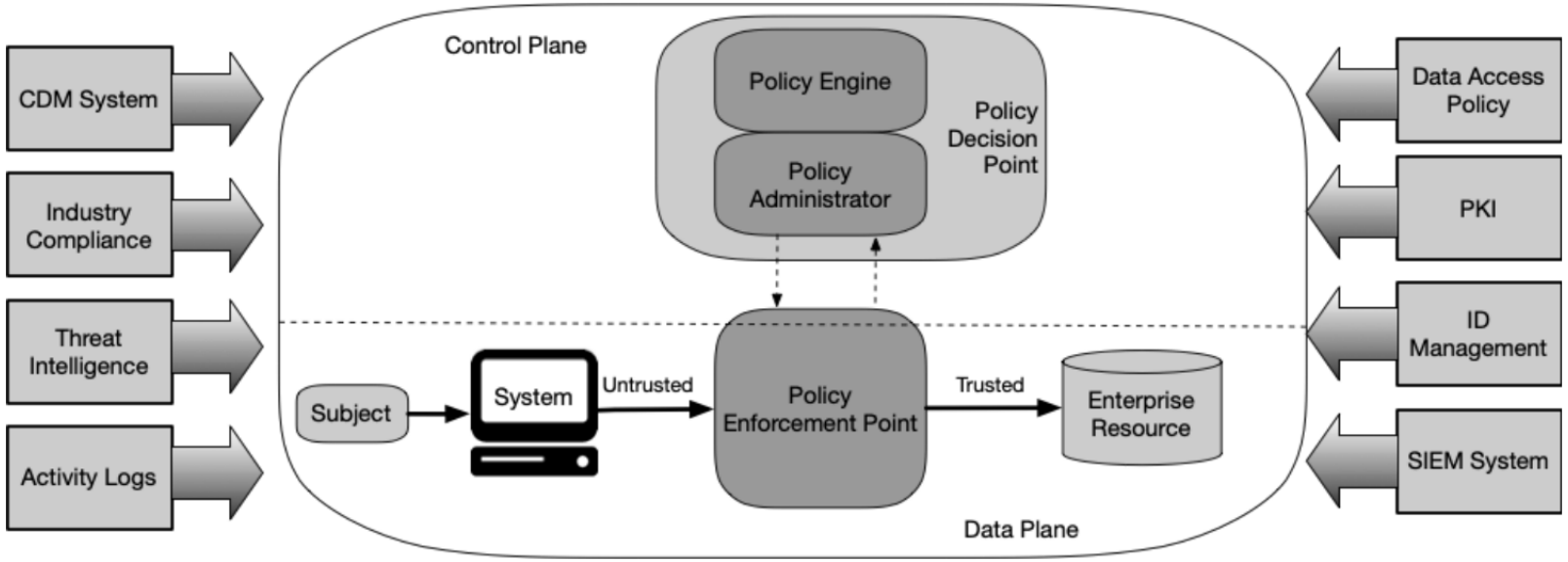
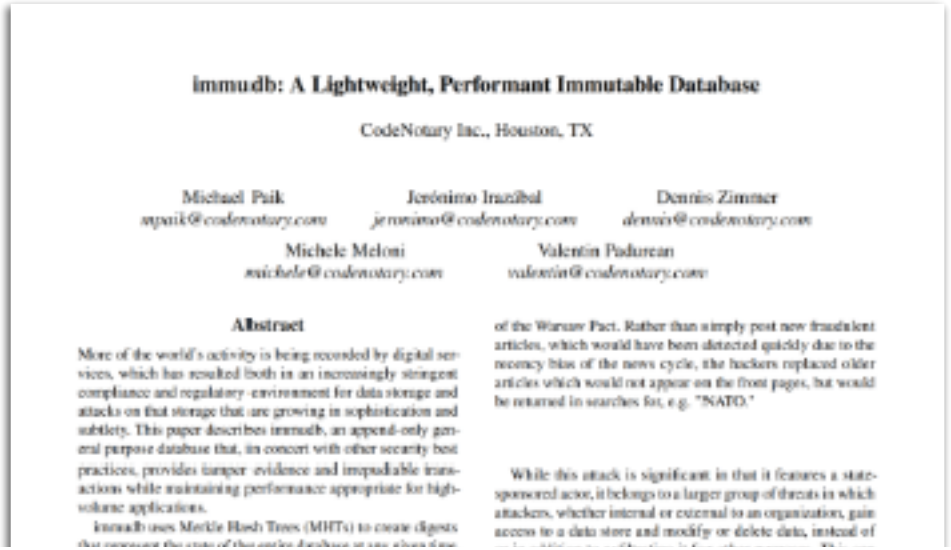


Figure 2: Core Zero Trust Logical Components

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Significant Technical Advances



immudb: A Lightweight, Performant Immutable Database

CodeNotary Inc., Houston, TX

Michael Paik — mpaik@codenotary.com
Jerónimo Irazábal — jeronimo@codenotary.com
Dennis Zimmer — dennis@codenotary.com
Michele Meloni — michele@codenotary.com
Valentin Padureanu — valentin@codenotary.com

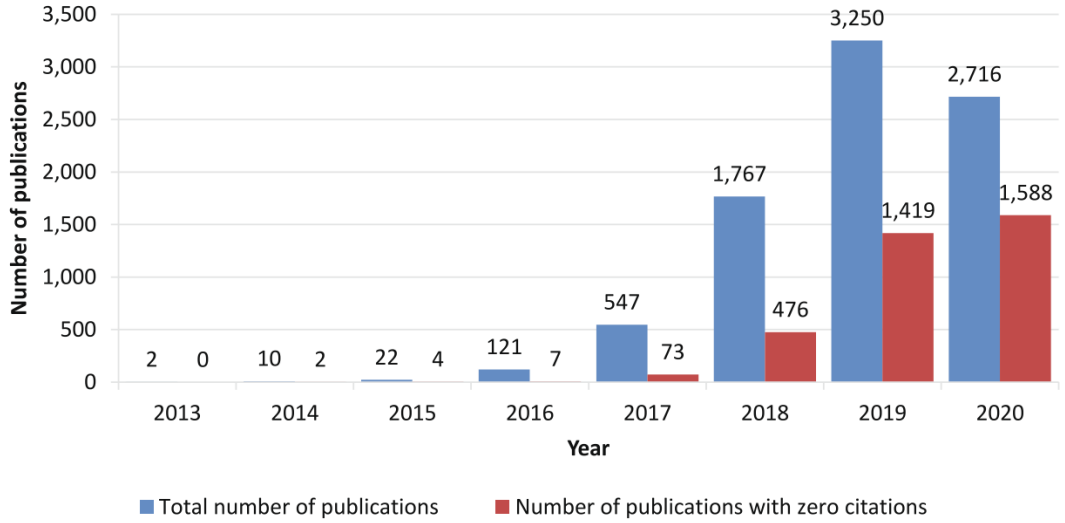
Abstract

More of the world's activity is being recorded by digital services, which has resulted both in an increasingly stringent compliance and regulatory environment for data storage and attacks on that storage that are growing in sophistication and subtlety. This paper describes immudb, an append-only general purpose database that, in concert with other security best practices, provides tamper evidence and irrefutable transactions while maintaining performance appropriate for high-volume applications.

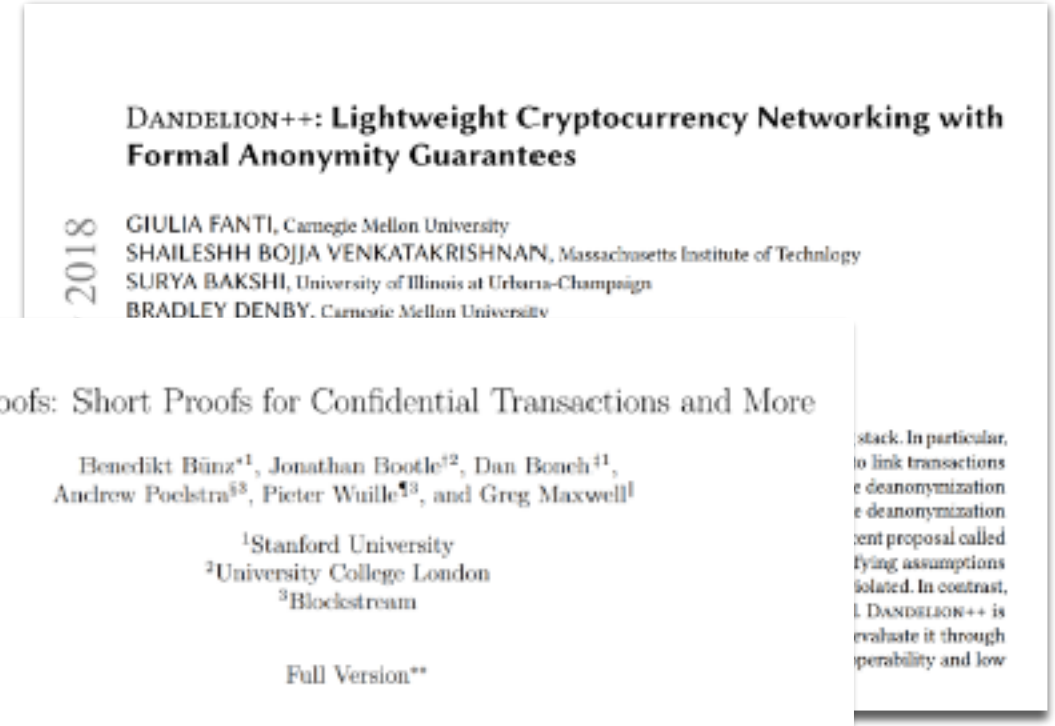
immudb uses Merkle Hash Trees (MHTs) to create digests

of the Warsaw Pact. Rather than simply post new fraudulent articles, which would have been detected quickly due to the recency bias of the news cycle, the hackers replaced older articles which would not appear on the front pages, but would be returned in searches for, e.g. "NATO."

While this attack is significant in that it features a state-sponsored actor, it belongs to a larger group of threats in which attackers, whether internal or external to an organization, gain access to a data store and modify or delete data, instead of



https://www.sciencedirect.com/science/article/pii/S1319157822000891

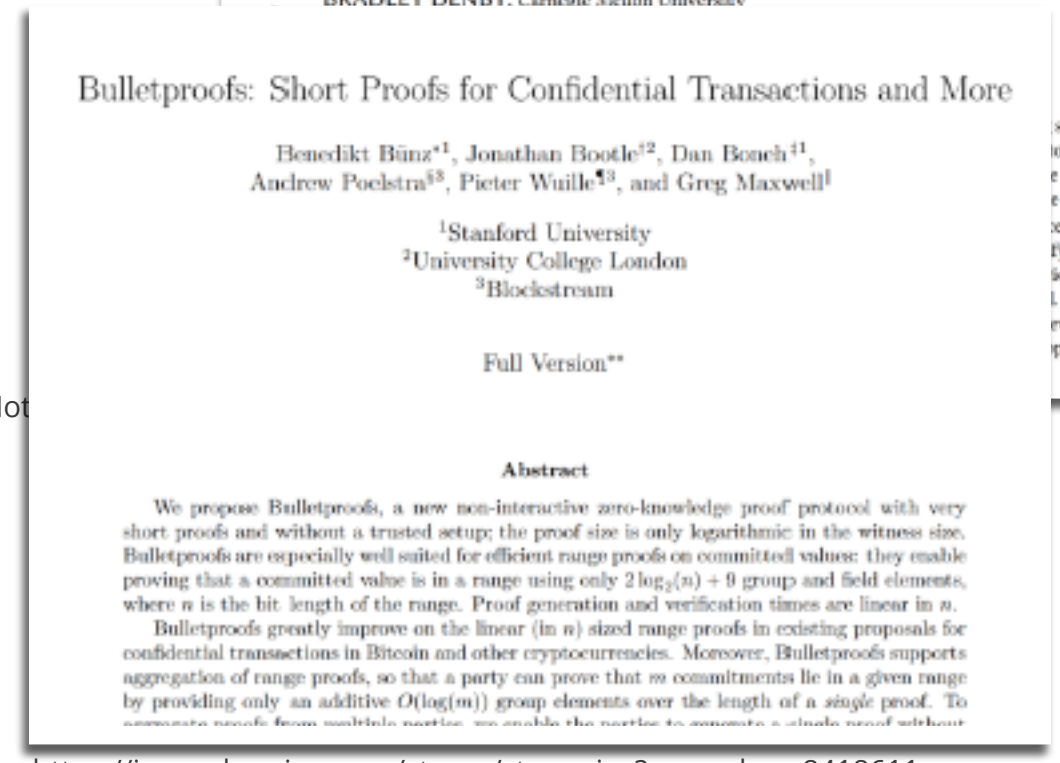


DANDELION++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees

2018

GIULIA FANTI, Carnegie Mellon University
SHAILESHH BOJJA VENKATAKRISHNAN, Massachusetts Institute of Technology
SURYA BAKSHI, University of Illinois at Urbana-Champaign
BRADLEY DENBY, Carnegie Mellon University

stack. In particular,
o link transactions
e deanonymization
e deanonymization
ent proposal called
fying assumptions
olated. In contrast,
DANDELION++ is
valuate it through
perability and low



Bulletproofs: Short Proofs for Confidential Transactions and More

Benedikt Bünz*[1], Jonathan Bootle†[2], Dan Boneh‡[1], Andrew Poelstra§[3], Pieter Wuille¶[3], and Greg Maxwell‖[1]

[1]Stanford University
[2]University College London
[3]Blockstream

Full Version**

Abstract

We propose Bulletproofs, a new non-interactive zero-knowledge proof protocol with very short proofs and without a trusted setup; the proof size is only logarithmic in the witness size. Bulletproofs are especially well suited for efficient range proofs on committed values: they enable proving that a committed value is in a range using only $2\log_2(n) + 9$ group and field elements, where n is the bit length of the range. Proof generation and verification times are linear in n.

Bulletproofs greatly improve on the linear (in n) sized range proofs in existing proposals for confidential transactions in Bitcoin and other cryptocurrencies. Moreover, Bulletproofs supports aggregation of range proofs, so that a party can prove that m commitments lie in a given range by providing only an additive $O(\log(m))$ group elements over the length of a *single* proof. To

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8418611

Audacious, but tactically grounded starting points

Integrity

immudb

TerminusDB

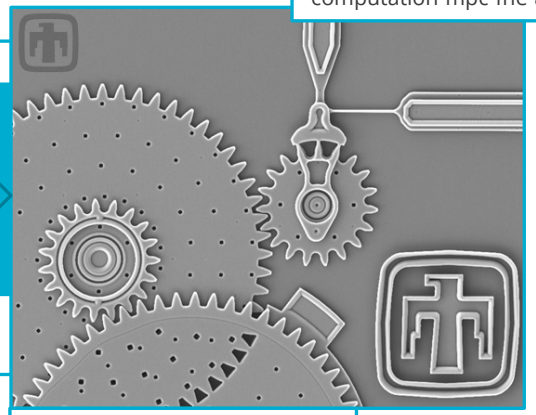
dolt

https://www.dolthub.com/blog/2022-03-21-immutable-database/

Confidentiality

https://www.esat.kuleuven.be/cosic/blog/the-three-musketeers-of-secure-computation-mpc-fhe-and-fe/

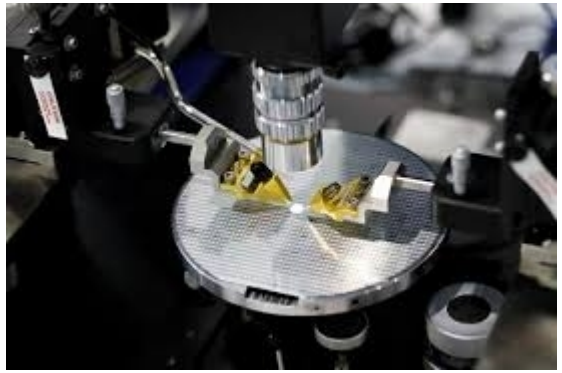
New Features



https://www.sandia.gov/mstc

https://www.sandia.gov/mesa/fabrication-testing-and-validation-capabilities/

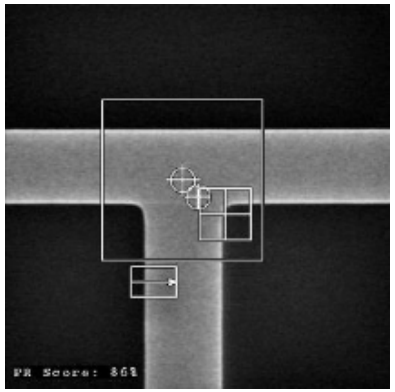
Measuring Success

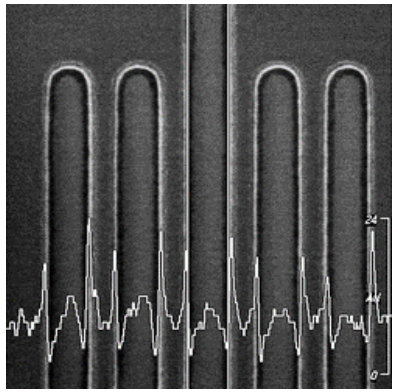


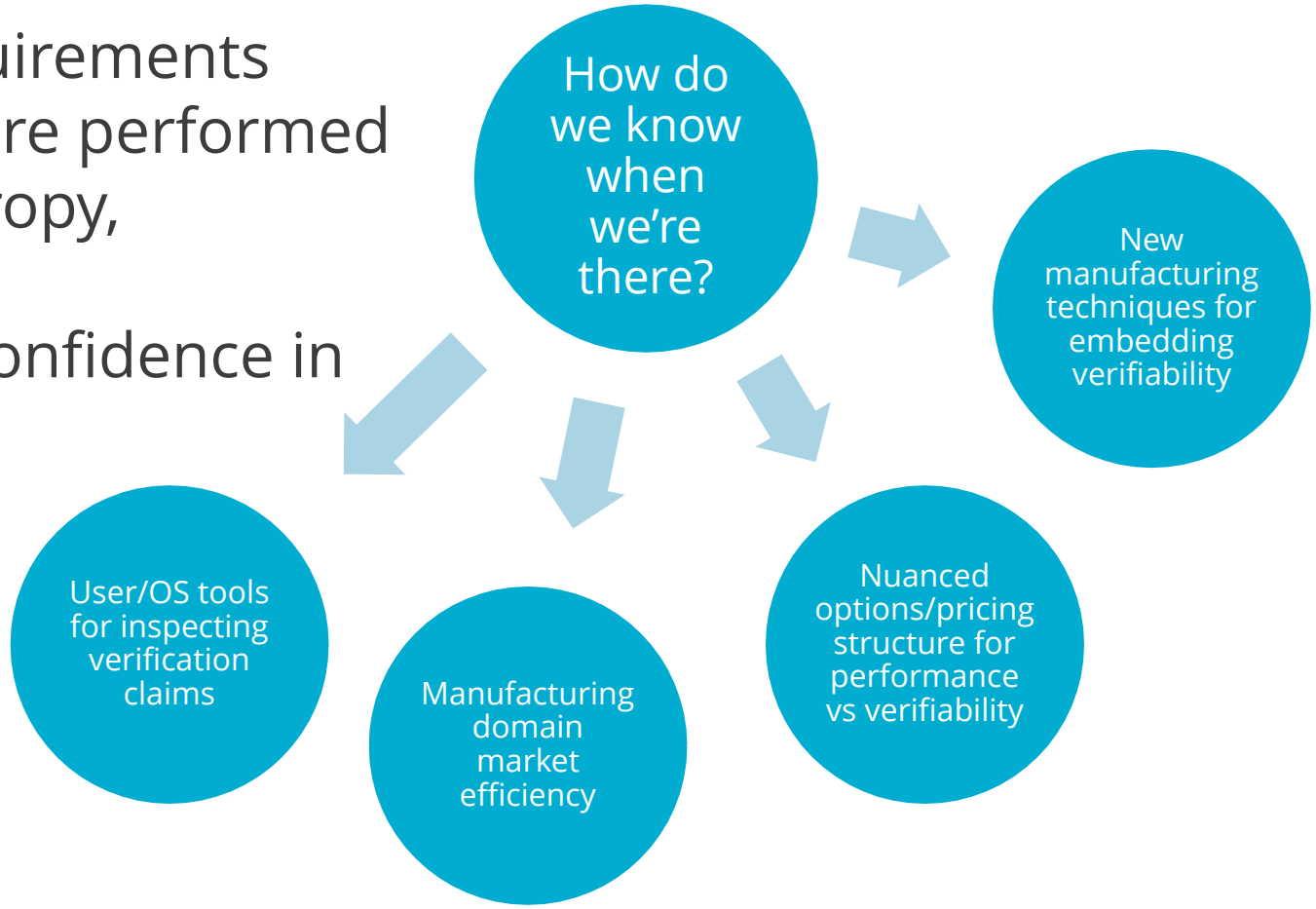
Users must be able to continuously measure and verify that…

- chip operations are to (chip) requirements
- only requested chip operations are performed
- real time security attributes (entropy, emanations, etc.)

Manufacturers needn't sacrifice confidence in their sensitive/proprietary







Thank You!

Questions? Email: ndpatte@sandia.gov