Crypto anchors

V. S. K. Balagurusamy
C. Cabral
S. Coomaraswamy
E. Delamarche
D. N. Dillenberger
G. Dittmann
D. Friedman
O. Gökçe
N. Hinds
J. Jelitto
A. Kind
A. D. Kumar
F. Libsch
J. W. Ligman
S. Munetoh
C. Narayanaswami
A. Narendra
A. Paidimarri
M. A. P. Delgado
J. Rayfield
C. Subramanian
R. Vaculin

Blockchain technology can increase visibility in supply-chain transactions and lead to more accurate tracing of goods as well as provide evidence of whether a product is authentic or not. A shared, distributed ledger or blockchain alone, however, does not guarantee correct and trustworthy supply-chain traceability. We argue that blockchain technology (and any other digital traceability solution) must be enhanced with methods to "anchor" physical objects into information technology, Internet-of-Things and blockchain systems. Only when trust from the digital domain is extended to the physical domain can the movement of goods be accurately traced (e.g., for callbacks and provenance) and product authenticity determined. In this paper, we introduce the concept of crypto anchors, propose a classification and system architecture, and give implementation examples for different use cases and industries.

1 Introduction

Assuring the authenticity of products and assets is a fundamental need across industries like electronics, pharmaceuticals, gas and petroleum, automotive, aerospace, defense, and retail, where there is a high risk of causing major harm when fake products go unnoticed. Authenticity is critical for raw materials, food, drugs, diagnostic tests, electronic components, hardware parts, and finished goods, such as luxury bags and gold bars. A related demand is to track and trace the logical and physical route, condition, and chain of custody (or ownership) of goods throughout the supply chain and the life-cycle of the assets. For both applications, proof of authenticity as well as track and trace, a tight link between physical objects and their digital representation is essential.

Distributed ledgers, or blockchains, have recently gained a lot of attention as a technology that increases trust and visibility along the supply chain for more accurate tracing of goods as well as ascertaining the authenticity of a product. [1]. Trust and controlled visibility is achieved in blockchain systems with cryptography, distributed protocols, and privacy-enabling techniques, such as zero-knowledge or threshold-signature schemes. Complex manufacturing lines and supply chains can be securely monitored and documented such that downstream business processes can validate the provenance of an item. Likewise, upstream business processes can determine the recipients of goods, for instance, in case of a product recall.

A blockchain or any other digital track-and-trace solution alone, however, is often not sufficient to prove originality or provide an uninterrupted chain of custody in supply chains and throughout the product life-cycle. Only when trust from the digital domain is extended to the physical domain can product originality be determined and the movement of goods be accurately traced. The physical object must be tied to its associated digital record.

Typically, an object is linked to a digital record by a unique identifier (UID) that represents either the individual object or a class of objects by model, batch, production site, manufacturer, or similar. The UID is printed, embossed, or attached as a tag to the object or its packaging. Many of these identifiers are easily copied or transferred to a clone of the object. Hence, an identifier alone cannot uniquely and securely identify, i.e., authenticate an object.

Digital Object Identifier: 10.1147/JRD.2019.2900651

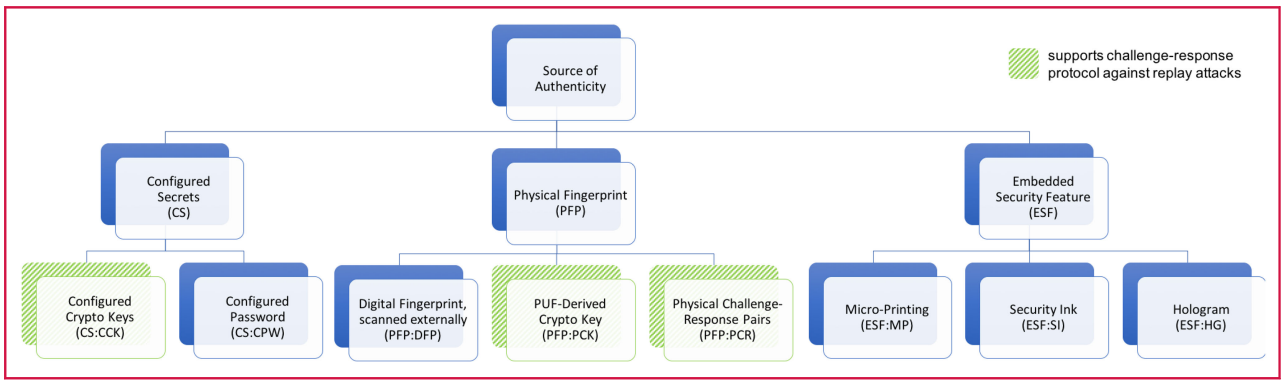

Figure 1

Sources of authenticity for crypto anchors.

This paper introduces the concept of a *crypto anchor* that exploits a range of properties of a physical object to securely associate the object with its UID. The properties encompass configured secrets (for instance in electronic tags), physical fingerprints (such as surface structures), and embedded security features (as in banknotes). We define generic processes for verifying the different types of crypto anchors, authenticating the associated object to arrive at a certified UID that unequivocally links the object to properties asserted in a distributed ledger or any trusted tracking system (database, ERP tool, etc.). Combining crypto anchors with a blockchain ensures that neither the physical identity of an object nor the associated transactions recorded in the ledger can be forged, extending trust from the ledger all the way to physical objects.

The remainder of this paper is structured as follows. Section 2 introduces the crypto-anchor concept, based on the notion of digital fingerprints, physically unclonable functions, and other approaches. With this background, Section 3 surveys related work. Section 4 presents specific implementations and use cases of crypto anchors developed by us. Section 5 describes a crypto anchor architecture and business ecosystems. We conclude in Section 6.

2 Crypto anchors

2.1 Overview

A *crypto anchor* ties a UID to the physical object with a property of the object that is hard to clone, forge, and transfer to another object. Such a property acts as a *source of authenticity*. The property may be inherent to the object, or it may be unalterably attached (entangled), for instance, with a strong adhesive or in a way that destroys the property, the object itself, or a functionality of it when removed. We consider three different types of sources of authenticity: *configured secrets*, *embedded security features*, and *physical fingerprints* (see **Figure 1**).

Electronic devices can be configured with secrets such as cryptographic keys that prove their identity in a challenge-response protocol. In the case of public-key cryptography, the secret is not revealed in the process, but the party that generated and configured the key pair (e.g., the manufacturer, distributor, or owner) might retain a copy and could reuse it in multiple devices. This issue is addressed in Section 2.3.

Physical fingerprints (PFPs) are the result of variability in the material or the manufacturing process of an object. Examples are the structure of leather, the optical characteristics of a type of oil, the imprint of a production line, or the doping in semiconductors. The variability is of a type that cannot be controlled and, therefore, cannot be duplicated—not even by the original manufacturer. The variability may be a common production side-effect (*intrinsic*) or specifically introduced (*extrinsic*), for instance, by adding special fibers into paper.

Embedded security features require an expensive application process such as micro-printing, hologram generation, or printing with security ink. A bar code produced in this way can be read by anyone but cannot be copied without special equipment. The difficulty and cost to reproduce an embedded security feature should deter most attackers.

2.2 Digital fingerprints

Physical fingerprints can be measured and digitized (scanned) to produce a digital fingerprint (DFP). The DFP can be used directly as a UID (if the probability of ID collisions is sufficiently low), it can certify a separate UID (both have to match), or it can be used as a seed for cryptographic key generation. If the fingerprint is scanned by an external device, this scanner must be trusted as there is no way to detect a replay attack. Challenge-response-type crypto anchors, in contrast, are immune against this type of attack (hatched green in Figure 1), as described in Section 2.3.

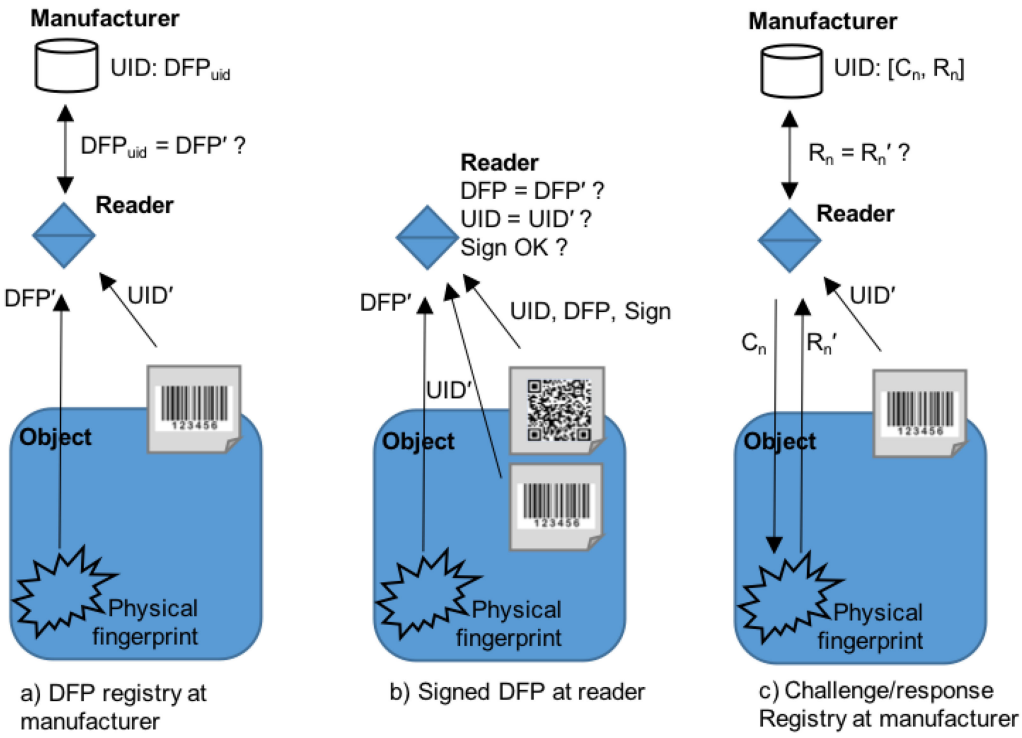

Figure 2

Pairing of unique ID and a digital fingerprint (derived from a physical anchor), certified by (a) a manufacturer-maintained database or (b) by a manufacturer-signed tag. (c) Variant with multiple challenge-response pairs.

For a scanned DFP′ to certify a UID, the pairing must be attested by a trusted party, such as the manufacturer. As **Figure 2(a)** shows, the trusted party might store the UID–DFP pair in a database that can be queried over the Internet. Alternatively (b), the manufacturer could sign the pair with a manufacturer key that can be verified by a public-key infrastructure (PKI). The signed pair would be attached to the object as a tag, for example, a bar code or a near-field communication (NFC) tag.

The database approach provides the ability to revoke, whereas the tag makes offline authentication possible. A central database might be subject to attacks and a single point of failure, for example, if the manufacturer goes out of business. One way to address these issues is to store the UID–DFP pairs on a blockchain, where distribution and consensus algorithms improve the robustness against failure and fraud.

To verify a UID, a reader scans the PFP and the UID′ and checks whether the resulting DFP′ matches the one stored in the manufacturer database under the UID. Alternatively, the reader also scans the tag with the signed UID-DFP pair, validates the signature using the manufacturer's public key, and verifies that the scanned UID′-DFP′ pair matches the UID-DFP pair stored in the tag. In this process, the fingerprint attests that the tag belongs to the object at hand. The tag, in turn, attests that the UID belongs to the object. Finally, the manufacturer signature attests that the UID-DFP pair and, by extension, the object are genuine.

The scenario in **Figure 2(b)** does not strictly need the UID′ shown as a two-dimensional bar code as the signed tag (QR code) also carries the certified UID. The redundant UID′ represents any asserted but insecure ID, e.g., a human-readable, embossed serial number, that can be verified using the signed tag.

2.3 Physically unclonable functions

The concept of physical fingerprints can be pushed further with physically unclonable functions (PUFs) [2, 3]. A PUF can be, for instance, based on the content of an uninitialized SRAM or a ring-oscillator frequency. The chip itself can scan this type of PUF and derive crypto keys from the resulting DFP. With these keys, the chip can authenticate without revealing the DFP, making it very hard to clone.

Unlike with configured keys, this approach ensures that not even the manufacturer has a copy of the secret as it never leaves the chip. The manufacturer does not need any

infrastructure for generating and configuring keys. PUF-generated crypto keys remove the need for nonvolatile memory or security modules and are hard to reverse-engineer [3].

A PFP may give different readings depending on the stimulus. This may be an optical coating that reflects light differently depending on the angle of stimulation, or it may be an electronic circuit measuring many instances of process variability depending on the provided input C_i. The stimuli and their associated readings represent physical challenge-response pairs (CRPs) $[C_i, R_i]$ that can be characterized and stored in a database, shown in **Figure 2(c)**. For authentication, one challenge C_n is applied. If the object's response R_n' corresponds to the expected response R_n according to the database, then authentication is successful. To prevent replay attacks, every CRP is used only once. When the CRPs run out, the object might be recharacterized with previously unused stimuli. A PUF with a large number of CRPs is called *strong* as opposed to a *weak PUF* that produces only a single response [4].

2.4 Additional features

In addition to certifying a UID, crypto anchors can also be used to confirm the physical integrity of the object by choosing them such that the PFP changes along with the physical property that needs protection. The PFP can stretch across a surface affected by tampering such that a modified object will not return the same DFP any longer. A PFP that permanently changes when crossing a temperature threshold can be used to attest a cold chain. Micro-fluidics can be employed in a medical diagnostic test to change a security feature when the test is used, certifying that the test is not just genuine, but also unused. Electronic crypto anchors can be used to attest readings from integrated or attrached sensors.

3 Related work

Table 1 lists examples of existing authentication solutions that can be classified as crypto anchors, including the crypto-anchor solutions presented in Section 4.

Chronicled [5] provides a CryptoSeal, which is a cryptographic, tamper-proof, NFC-enabled seal that secures the content of packages and containers. Tampering damages the circuitry, preventing subsequent successful verification. It contains a private key and uses public-key cryptography for identification. A broader class of NFC and radio-frequency identification (RFID) tags with cryptographic authentication capabilities is very similar to the Chronicled solution. What is special about the CryptoSeal is its tamper-evidence feature, which guarantees the "entanglement" with the physical object, such as an envelope.

Everledger [6] creates digital fingerprints for individual diamonds using about 40 metadata points, a laser inscription, and the stone's color, clarity, cut, and carat weight. The unique identification of the stone is combined with the Kimberley Process, a certification scheme imposing extensive requirements on the process of diamond production to prevent the insertion of conflict or counterfeit stones into the market.

Table 1 Crypto-anchor solutions.

Solution	UID	Source of authenticity	Validation	Crypto-anchor concept
Chronicled – crypto seal [5]	Embedded ID	Private key in secure element	Blockchain registration of seals	Configured crypto key, PKI
Everledger – Diamond tracking [6]	Laser inscription	PFP Metadata (carat, color, …)	Everledger blockchain registration of diamonds	DFP, scanned externally
MagnePrint [7]	Personal data	PFP magnetic properties & flux transitions	Registration of DFP in Magneprint DB	PUF-derived CRPs
entrupy – Luxury bags [8]	Product label	PFP Leather features bag details	entrupy DB	DFP, scanned externally
Intrinsic ID [9]	Identity Certificate, public key	PFP SRAM-PUF	PKI	PUF-derived crypto
PUF-based RFID chip [10]	Embedded ID	Multiplexers and an arbiter	CRPs in manuf. DB	PUF-derived CRPs
Optical/ photonic crystals [11-13]	Product label	PFP blended with object features, e.g. density, coating	DB registration of DFP by manuf.	DFP, scanned externally
Microfluidics [15,16,18]	Opt. code	inkjet-spotting dyes directly on object	DB registration of code by manuf.	Embedded security feature
Verifier (optical reader device) [19]	Product label	PFP, e.g. Oil: color saturation distribution Paper: lithographic print patterns	Blockchain registration of patterns by manuf.	DFP, scanned externally
PUF-based IOT device identification [21]	e.g. serial number	PFP SRAM-PUF	Zero-knowledge proof	PUF-derived crypto
Small computer [24]	Embedded ID	Private key in secure element	Blockchain registration of devices	Configured crypto key, PKI

Entrupy [8] uses machine-learning algorithms on microscopic images of physical objects to distinguish between genuine and counterfeit versions of the same product with a focus on luxury goods. They exploit microscopic characteristics (such as the leather structure in

handbags) in a genuine product or a class of products to distinguish these products from their corresponding counterfeit versions.

Intrinsic ID [9] uses a weak PUF based on SRAM patterns to securely generate keys for security protocols. The device-specific key is derived from an SRAM-PUF response and helper data. The key can be used to authenticate the device.

A PUF-based RFID chip [10] exemplifies the concept of a strong PUF with PUF-derived challenge-response pairs. The chip features an embedded PUF circuit of multiplexers and an arbiter. A characterization step applies random stimuli to the PUF circuit to obtain unpredictable responses. A trusted party stores these challenge-response pairs in a database for future authentication. The database is indexed by the unique identifier of each RFID. To check the authenticity of the RFID, the trusted party selects a previously unused challenge from the characterization set. The RFID is authentic if it returns the correct response that only the authentic chip and the trusted party should know. Once used, the challenge-response pair is removed from the list of valid CRPs.

"Quantum dots" [11] or photonic crystals [12] are materials with specific optical properties that can be synthesized in bulk quantities and are hard to reproduce without knowing the detailed synthesis conditions which affect their dimensions, density, coating, or molecular weight. Their properties make these materials particularly interesting for crypto anchors. They can be homogeneously blended with an object or localized in particular areas in the case of printed documents. Patterns can be formed by structuring these materials on a surface to make reproduction even harder or to enhance their optical characteristics [13]. Devices for reading such crypto anchors can be smart phones or portable optical readers, but sometimes specific excitation wavelengths, for example, in the near infrared, are needed to induce fluorescence of the materials used.

4 Specific crypto anchors

This section presents four examples of crypto anchors developed by the authors that cover different classes, according to Section 2, supporting distinct use cases with different tradeoffs. The examples range from micro-printing technology (*embedded security feature*) and high-resolution reading of physical fingerprints (producing a *digital fingerprint, scanned externally*) to embedded SRAM (*PUF-derived crypto keys*) and a very small processor tag (*configured crypto keys*).

4.1 Microfluidics

In healthcare, rapid diagnostic tests are critical but are also a prime target for counterfeiting. Such tests are used worldwide for detecting viruses, parasites, and numerous medical conditions in patients; they are also used to monitor therapies and manage diabetes. For malaria alone, the World Health Organization estimated that 314 million tests were used in 2014 [14]. In one format, these tests essentially consist of a stripe of nitrocellulose coated with biochemical reagents that is inserted into a plastic cartridge. This format makes it easy for counterfeiters to fake or mislabel genuine tests or to alter their expiration dates since product information is available mostly on the package. A more recent format involves microfluidics, where samples and reagents are precisely guided through microstructures for realizing fast and precise diagnostic tests. Embedded chemical QR codes on the nitrocellulose that appear upon a biochemical reaction during the use of a test have been proposed for protecting rapid diagnostic tests from tampering [15,16]. Fluorescent microtags carrying QR codes have also been placed inside individual drug capsules [17].

We implemented crypto anchors on both nitrocellulose and microfluidics-based tests while keeping in mind that diagnostic tests:

1) are very cost-sensitive products (production cost $< 1\$$);
2) need to be mass manufactured;
3) contain fragile biological reagents;
4) should not require sophisticated instrumentation for authentication.

For these reasons, we developed optical codes that represent crypto anchors with embedded security features by inkjet-spotting dyes directly on the medium where the diagnostic tests are performed. In order to obtain high optical resolution on the hydrophilic surface of silicon-based microfluidic tests, micro-pillars were fabricated, and individual elements of optical security codes were placed onto these pillars (see **Figure 3**). We achieved a resolution of 32 elements/mm^2 using this strategy.

Such optical codes can be scanned using a smart phone for authentication and represent significantly better protection than just text or labels present on a package: The flow of solutions at submillimeter length scales can be predicted in such devices; it is therefore possible to direct The flow of a sample on particular parts of the code to erase it.

Moreover, a code can interact with the liquid sample and be transformed to provide evidence if the test has been used already. Such a transformation can take from a few seconds up to several minutes as shown on a nitrocellulose stripe in Figure 3(d). This timescale is in line with the typical duration of diagnostic tests, which can last up to an hour for challenging biological tests. This transformation also creates a very large number of code combinations. The code on the nitrocellulose membrane stores 152 bits of information (at least 10^{45} combinations) with only 32 code elements. Erasing or altering codes in a non-reversible

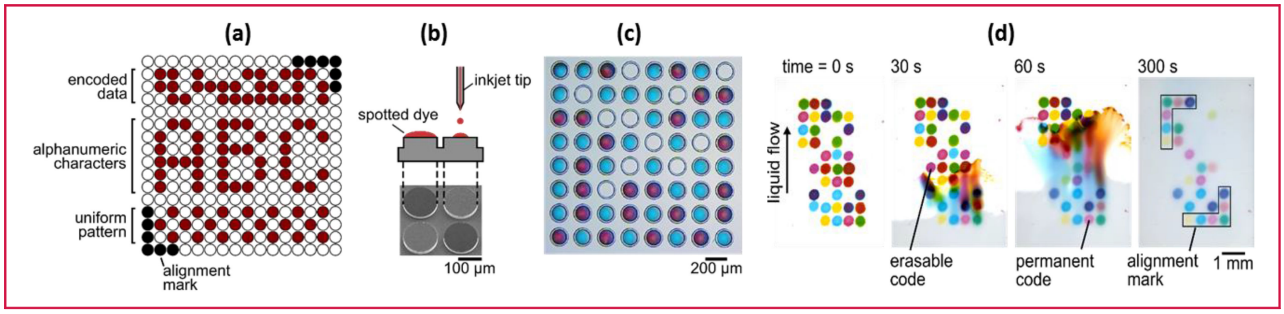

Figure 3

Optical security codes on silicon micro-pillars. (a) Code elements can be arranged to encode data and form alphanumeric characters or patterns. Alignment marks enable correct decoding with optical readers. (b) Code elements are placed with an ink-jet spotter contemporary with the chemicals necessary for the tests. (c) Microscopy image of a multicolor optical security code. (d) Optical security code that transforms with a liquid sample flowing on a diagnostic device can be easily decoded with a smart phone to authenticate diagnostic tests before and after use.

manner prevents the reuse of tests and directly alerts a user of potential anomalies without the need for sophisticated instrumentation, as discussed by Gökçe et al. [18].

It is also possible to increase the security provided by the optical codes by coupling them to QR codes on the package. In this implementation, the QR code contains information about the product, additional security features, and encrypted data that match the optical code. When the QR code is scanned, the reader decrypts the data on the QR code and checks if the optical code has the expected attributes. This ensures that information on the package is accurate.

4.2 Verifier

Many crypto anchors need a more sophisticated reader device to scan the physical fingerprint of an object and characterize or verify its features. The IBM Verifier is such a mobile reader device that captures intrinsic features (a PFP) of a material or object to uniquely identify it and discern it from counterfeits. In contrast to other crypto anchors described in this paper, no external tags or sensors need to be added to the product being tracked or authenticated. The product or substance does not have to be modified in any way. The Verifier is composed of two parts: an optical device to scan the PFP and artificial intelligence models that interpret the data from the optical device to create a DFP and allow the comparison with reference data. The Verifier can be attached to a cell phone, shown in **Figure 4**, tablet, or laptop [19].

The Verifier's optical device is able to obtain light wavelengths and microscopic data from an object. The color of the object is the result of its interaction with the light by which it is illuminated. It is determined by the type of material and its molecular and atomic constituents. Traditionally, this is analyzed by shining light of different wavelengths and measuring their absorption or transmission by the object. This gives the characteristic light absorption or transmission spectrum for the object, which can be obtained with light spectrometers. However, modern light spectrometers are quite bulky and expensive, putting portable solutions outside the reach of common consumers. Our optical device along with our software applies computer vision and image processing techniques to glean information digitally that resembles the light transmission and absorption spectrum and the object's color texture, providing a portable solution for quick online analysis for a number of applications.

We illuminate the object to be verified in a way that covers a broad range of visible light wavelengths and record their image with the cell phone equipped with the IBM Verifier's optical device. The data are then analyzed with digital image processing and computer vision techniques. To compare two related or different materials, we analyze their corresponding distributions or their combinations with machine-learning or deep-learning neural network models, providing a very powerful, low-cost, portable analytical tool.

The Verifier's optical device has a resolution of 1 μm. At 1 μm, the Verifier can see bacteria. Animal cells are 10 μm, plant cells are 100 μm. The width of a single human hair is 17–181 μm. The Verifier software can also measure the viscosity values of liquids in micron-scale regions, making it possible to detect contaminants.

With this resolution and its wavelength-detection capability, the Verifier can examine materials such as metals, drugs, paper products, manufactured parts, liquids, wines, oils, art, luxury goods, etc. The Verifier's artificial-intelligence models can be used to discern counterfeits from the original authentic product once it has acquired reference data for the authentic products.

An example from the automotive industry is shown in Figure 4 to distinguish two different motor oils, where the Verifier is attached to a cell phone. Although they look the same to the human eye (top and bottom left panels) and their color hue distribution is subtly different (lower middle panel), their color saturation distribution is quite different

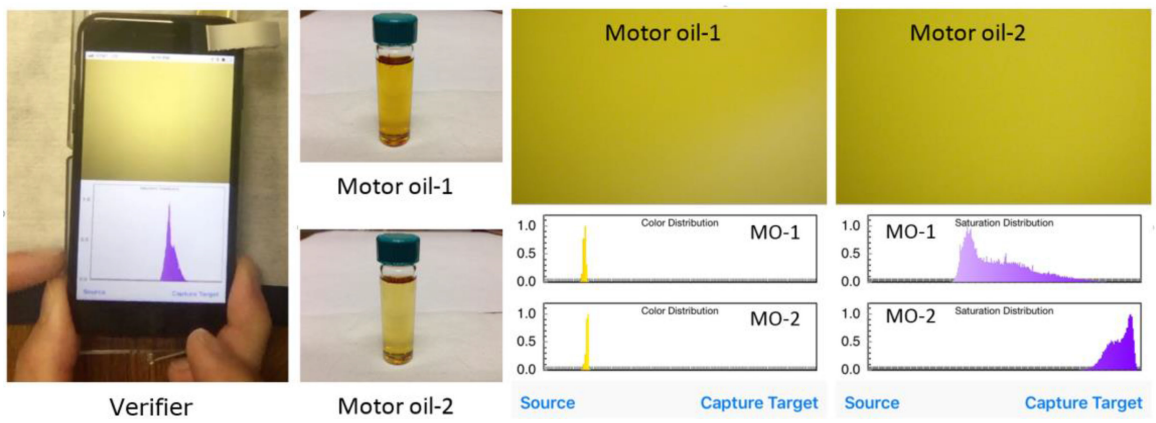

Figure 4

Two motor oils (MO-1 and MO-2) are identified based on their visual digital signature using the IBM Verifier—an optical device and artificial intelligence models combined with a cell phone.

(lower right panel). Deep-learning neural network models learn these distributions, and this software is used to detect which type of motor oil a consumer has purchased. This provides an easy-to-use optical device for quickly analyzing the type of motor oils or any liquid. We have used the Verifier to detect adulerated and counterfeit olive oil, wine, and petroleum products.

To couple physical object characteristics to blockchain transactions, the Verifier reference data can be placed on the ledger and, as the products move through the supply chain, anyone or an automated process can use a Verifier to detect if the original product has been adulterated or replaced with a counterfeit. At the site of creation or packaging, a person or automated process scans the product with a Verifier. This reference data represents the digital fingerprint of the product and is placed on the blockchain. As the product moves through different transport systems, distributors, retailers, consumers, a person, or automated processes can use another Verifier to scan the PFP and derive the DFP′, check it against the reference DFP stored on the blockchain, and check if the fingerprints still match to verify the authenticity of the tested product.

The high optical resolution of the Verifier enables it to discern whether luxury goods—for example, luggage, art, clothing—or paper products—such as labels, health certificates, or diplomas—are counterfeit. The Verifier can discern microscopic lithographic patterns and paper weaves and reveals the differently colored dot patterns that are used to create the appearance of different hues and their shades in the printed paper. If a counterfeiter copies the original product label created by this process, the verifier hardware could identify differences in these patterns from the original as no two papers and no two prints are identical at high resolution. Additionally, the Verifier can use microscopic surface features of drug pills and the drug's wavelength data to distinguish counterfeits and identify bacteria and other contaminants.

4.3 SRAM-derived cryptographic keys

New Internet-of-things (IoT) devices are created every day, and they are usually limited in resources and power consumption. Authenticating such electronic components is complicated, especially when the microcontroller or processor they contain does not have cryptographic capabilities due to resource and cost limitations. This is an important issue for manufacturers of connected electronic devices, such as thermostats, cameras, wearables, or even car electronics. If the product of one manufacturer is sent to warranty service, the manufacturer (or the repair shop) must ensure that the device is authentic and not a forgery. If the device's identifier was a simple number or code, this information could be easily copied to the memory of a fake device, thus imitating the original product's identity.

To solve this problem, we have developed a prototype that authenticates constrained devices using a PUF that uniquely characterizes the IoT devices and allows the derivation of crypto keys. Thanks to the properties of PUFs (unclonability, uniqueness, and reproducibility, among others), manufacturers do not have to spend resources on programming devices with unique identifiers that need to be stored in secure memory, as well as on creating and maintaining a database of all their products. Using PUFs, the identity of a device is created from the unavoidable variability of the manufacturing process of the

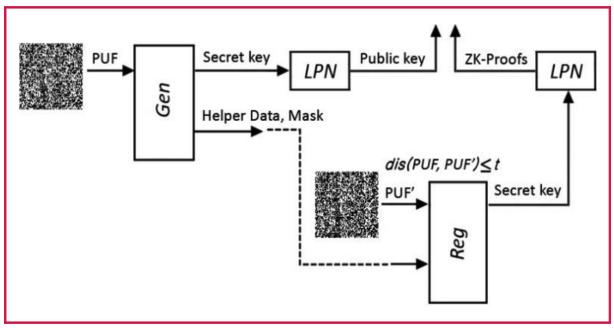

Figure 5

Fuzzy extractor of a secret key using SRAM PUF start-up values, Helper Data, and Mask information. The only information sent outside the device is the public key that identifies the device and the zero-knowledge proofs.

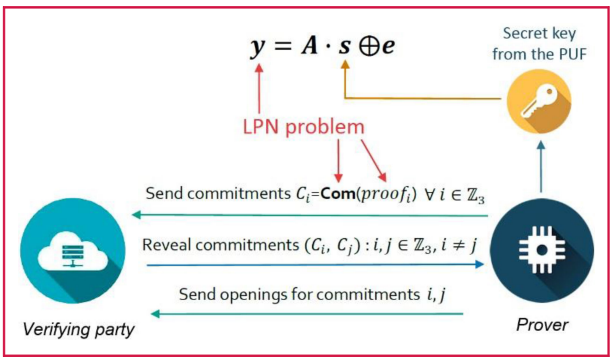

Figure 6

Commitments and exchange of messages for zero-knowledge proofs based on LPN.

microcontroller inside the product; furthermore, it is protected using a public-key scheme based on learning parity with noise (LPN) [20].

We have chosen the SRAM start-up values of microcontroller memories as a suitable PUF, but there will be variability over time. Some bits will flip with changing operating conditions, such as ambient temperature, power-supply voltage, or circuit aging. Thus, to always generate the same identifier or unique key associated with the device, we must use a fuzzy extractor (see **Figure 5**), as in biometrics with fingerprints, that allows us to regenerate the same information from a noisy input [21].

First, the IoT device manufacturer uploads their firmware to the device's microcontroller. No hardware modifications are required to make our protocol work. As a security measure, the manufacturer has to blow or protect the JTAG port and the bootloader (BSL) of the microcontroller in order to avoid unwanted physical access to internal device information and potential side channel attacks.

When the microcontroller is first booted in a controlled environment, the system will be automatically power-cycled multiple times (ideally around 20 times) to self-characterize its SRAM cells. The resulting data, called helper data (necessary for reconstructing the secret key) and mask (to filter the response and reduce the number of flipping bits), do not leak any information about the secret key. This procedure makes the helper data unlinkable and improves the robustness of the PUF response during the reconstruction process. Thanks to this characterization, the flipping bits are reduced by up to 20%, and the minimum entropy of helper data approaches 92% [22].

When the device is powered up after the self-characterization, it will use the mask to filter the SRAM PUF start-up values of its microcontroller, and the helper data to reconstruct the unique secret key. Note that only the genuine device that can produce the required PUF response will be able to regenerate the key using this data, and it will resist aging and voltage and temperature variations. This secret key will be used to generate a public-key pair as well as the hidden element of a zero-knowledge proof game.

The implemented zero-knowledge proofs are also based on the learning-parity-with-noise problem [23], which is a very efficient algorithm for constrained devices thanks to its focus on binary operations. Using this algorithm as detailed in **Figure 6**, the microcontroller (prover) will send commitments to some system (verifying party) that will challenge it.[1] Every time the verifying party challenges the prover, the prover has to convince the verifying party of the authenticity of the claim committed before by sending the opening for the requested commitments. Interaction between the prover and the verifying party is necessary for proving the claim. After multiple iterations, the verifying party will be convinced by the prover with a negligible probability of failure in the authentication (e.g., the probability of a false authentication will be below 2^{-32} after 55 repetitions).

We have built a prototype of the protocol using a small MSP430FR5994 microcontroller produced by Texas Instruments working at 8 MHz. The prototype presents several advantages over the state-of-the-art authentication in IoT products. The manufacturer does not have to program or create the secret keys. Reading the public key generated by the device will enable any third party to verify the authenticity of the device using the zero-knowledge protocol without ever revealing any sensitive information. On the other hand, the secret key is unknown to everybody and uniquely linked to the physical characteristics of the device, making it the only entity that knows the secret. This property allows implementing backup mechanisms that help the

[1]To avoid confusion with the IBM Verifier, we refer to the verifier of a zero-knowledge proof as *verifying party*.

microcontroller to reconstruct the secret key even when all the information and characterization procedure has been deleted from the device. To the best of our knowledge, this is the first time that an authentication mechanism has been implemented exploiting PUFs and using zero-knowledge proofs as the authentication protocol instead of symmetric cryptography schemes for resource-constrained devices.

4.4 IBM Small Computer

In addition to uniquely identifying an object, the provisioning of trustworthy data about the environmental conditions of the object, such as temperature, humidity, and location, can be critical when tracking valuable or perishable goods, e.g., pharmaceutical products or food. The physical and cryptographic security (against tampering, side-channel attacks, replay attacks) are in a tradeoff with the size, cost, and form factor of the IoT device and thus the range of protocols and solutions that can be implemented on the devices. In that sense, this section provides an extension of Section 4.3, moving beyond standard microcontrollers and exploring the technology limits and capabilities to build a very small computer that can serve as a crypto anchor with configured secrets and at the same time provide more advanced compute and sensing capabilities.

Current IoT technologies most amenable to supply-chain integration are RFID and NFC tags. In passive modes of operation, these devices provide unique IDs, and in active modes, they support sensor data collection and communications. While these devices are low-cost, their centimeter-scale physical size limits their applicability. Additionally, these protocols typically only support authentication based on shared private keys, thus providing limited security to the system. Additional IoT technologies such as Bluetooth Low Energy (BLE) are active systems, again in the centimeter scale, and are typically more complex and power-hungry while providing support for more complex public-key protocols.

To overcome these limitations, the IBM Small Computer project is intended to develop a ubiquitous compute element in a very compact form factor that could serve multiple applications including to help securely link physical objects to blockchain records. The current implementation includes a 32-bit RISC-V processor core, hardware security accelerators for SHA-3 and AES, an integrated temperature sensor, and a nonvolatile memory interface. It is designed in a 14-nm CMOS process to minimize size and active power consumption [24]. The high performance of the processor, for a given power budget, allows the device to support advanced security protocols including public-key authentication and digital signatures. The device is multimodal, supporting wireless power delivery and bidirectional communication using either optical or radio-frequency operation. We are developing packaging technologies that integrate small optical detectors, LEDs, and antennas in a compact millimeter-scale assembly. **Figure 7** shows an initial prototype with an optical mode of operation that is currently under evaluation. An initial demo using a wire-bonded version of the Small Computer involves the processor performing ECDSA cryptography.

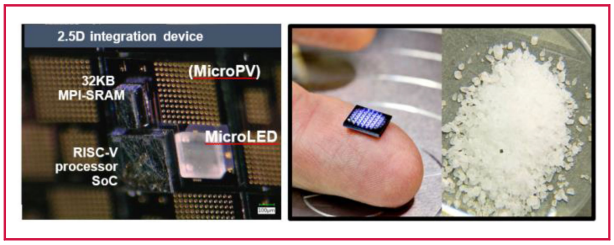

Figure 7

Initial packaged small computer with optical mode of operation.

We are also developing system demos using off-the-shelf tags to provide the enhanced security of public-key authentication, digital signatures, blockchain linkage, and hardware root of trust, at the cost of a larger size. A key advantage could be the use of standard RFID or NFC tag readers in existing supply chains. The protocol and approach could then be incorporated into the Small Computer system for further size and performance gains.

As an example of such an effort, we have developed and prototyped the *bcTracker*, a blockchain-based end-to-end tracking system incorporating off-the-shelf device tags with location sensors and secure authentication via WiFi communication. We have used bcTracker in a demonstration involving the tracking of wafer lots in our pilot microfabrication facility, with smart contracts implemented to track and control the allowed location and sequence of movements of the wafer lots. In this demonstration, transactions are physical movements of silicon wafer boxes between different fabrication stations.

We have also demonstrated the ability to securely integrate with IBM Small Computer and other custom offline (not WiFi-enabled) hardware tags through an intermediate reader device as an extension of the platform. In both cases, we were able to demonstrate end-to-end secure traceability and tracking with the device providing the trusted, authentic source of transactional data and a blockchain providing immutable, trusted cross-organizational recording, tracking, accounting, and compliance.

We have implemented secure signing of measurements and data on an Arduino board as well as on the Small Computer. This information is then sent via a trusted intermediary to the blockchain network. The blockchain network receives this transaction and determines whether this transaction is coming from a legitimate member and either accepts or rejects the transaction. As these events arrive, smart contracts are triggered. Smart contracts can

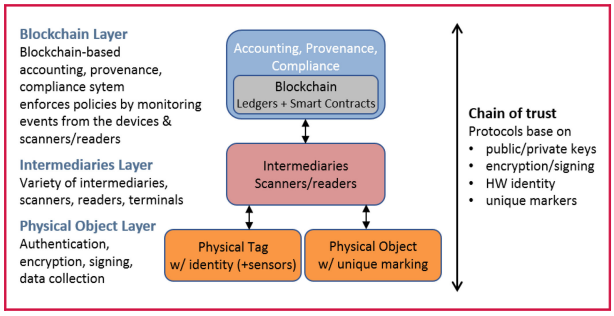

Figure 8

Three-layer architecture of the crypto-anchor concept.

detect wafer boxes that have gone astray or, in other future examples, when they are reporting data at unexpected hours, e.g., due to tampering of the clock on the Arduino board.

Several power-saving techniques have been applied to increase the battery life. These include an adaptive reporting rate that depends on the security needed at a particular time of day, which can be specified in a smart contract. For example, the wafer boxes are in locked premises during evening hours, and no report is needed since intrusion into the premises is detectable by other means. Otherwise, our hardware wakes itself up based on a timer, reports its location to the blockchain, and then goes back to sleep. The value of the timer is adjusted based on the time of day.

5 Blockchain integration

In this section, we establish the link between the physical objects identified by crypto anchors and the blockchain layer. **Figure 8** shows a three-layer architecture for establishing the crypto-anchor concept as an extension of trust into the physical world, for instance, to link shipments with their associated track-and-trace records in global supply chains.

At the physical object level, Figure 1 has introduced sources of authenticity grouped into three main classes: configured secrets, embedded security features, and physical fingerprints. These authenticity features ensure that the physical tags cannot be cloned. The sources of authenticity establish the root of a chain of trust. Beyond uniquely authenticating a physical object, the physical tags can also contain integrated sensors to measure temperature, light, humidity, pH, location, open/shut, smell, fluid speed, medical properties, etc., depending on the domain.

At the intermediaries layer (scanners, readers), there are two broad classes of devices. One class of readers communicates with electronic tags to verify their identity and optionally capture the data from integrated sensors in a secure manner. These reader devices will typically use wireless communication for the verification, via RF or light, but might resort to wired transmission where interference is an issue. Smart phones are attractive as intermediary devices thanks to their ubiquitous availability and wireless interfaces (NFC, RFID, BLE, etc.). If the electronic crypto anchors are active devices, such as microcontrollers or the IBM Small Computer, they may also interact directly with the blockchain layer.

The other class of intermediary devices will capture and verify nonelectronic tags or object properties. Such devices may inspect the physical fingerprint of the object or attached tag optically, acoustically, with heat-sensing cameras, by examining a sample of the physical materials via chemical or biological means, etc., and derive a digital fingerprint. Smart phones with their cameras and various sensors are very attractive as intermediary devices also in this case. Moreover, the IBM Verifier belongs in this class. In certain cases, the examination may have to be performed under controlled lighting, temperature ranges, etc.

Intermediary devices themselves may be authenticated by both the physical layer and the blockchain layer to establish their trustworthiness. The hardware and software of the intermediary devices both need to be verified before a complete channel between the physical layer and the blockchain layer is established.

At the blockchain layer, data are stored related to the physical objects, in particular reference data such as the [UID, DFP] pairs, the Verifier reference data, or the tags' public keys, but also any transaction data associated with the objects state. While conceptually this information could also be stored in traditional, centralized databases, a blockchain is a particularly attractive backend as it is independent of any individual operator. Therefore, it can combine information for different types of tags from different vendors, and it guarantees data availability independent of a vendor's fate.

The blockchain layer may be running in the cloud, on premises, or on a hybrid system. It is assumed that the servers are secured with best-of-breed security technologies. The blockchain layer may also store the cryptographic keys for the trusted readers, catalogs of material properties, algorithms for verification of properties, etc. Moreover, this layer houses smart contracts that may be triggered upon receiving relevant data. The blockchain layer has access to on-chain and off-chain storage. In addition, this layer contains the blockchain network with peers and mechanisms for establishing consensus and management of keys and credentials for members of the blockchain network.

Physical objects often change ownership and custody many times over their life-cycle, and associated data need to be passed along with the object. The distributed nature of blockchains makes them well suited to support this life-cycle and related applications, with crypto anchors ensuring the link between object and data.

6 Conclusion and future work

In this paper, we have illustrated the need for automated, trusted identification of physical objects combined with blockchains managing associated data from the source throughout the chain of custody to increase the levels of trust in items people consume or use. We introduced multiple classes and individual types of crypto anchors that enable such automated identification. The concept of crypto anchors refers to a range of technologies that define a source of authenticity in a physical object and read, register, and manage this source, turning it into a root of trust. We have highlighted specific approaches: microfluidics in medical diagnostic tests, the Verifier that uses an optical lens in combination with AI-based classification, IoT device identification based on SRAM fingerprints, and the Small Computer.

Many challenges remain. One area is to drive down the cost of embedding sources of authenticity into physical objects. The aim is to add the source of authenticity with minimal or no changes to the manufacturing process. This is achieved with microfluidics optical codes on diagnostic tests as well as with SRAM fingerprints. In the case of the Verifier, it is possible to deliberately add randomness during the manufacturing process that can be picked up by the AI-based classification.

Future research should address how software versioning is maintained on the reader and how the catalog of material properties is kept in sync. Is it possible to *search* a fluid with the IBM Verifier? It is one thing to confirm a fluid is an oil of a particular type, but determining it is an oil in the first place may be more difficult. Challenges for the Small Computer are to determine the core security algorithms that need to be embedded, how much memory and computation is needed, how much power is consumed, how it is powered, which sensors to integrate, how to support compression, etc., for the device to remain secure yet practical.

At the system level, questions arise around how to manage the crypto anchors and the necessary security keys in a functional ecosystem. How do the security protocols change based on the level of trust in the ecosystem where the crypto anchors are deployed? On the blockchain side, how does one scale the network for billions of crypto anchors and IoT devices? What data should actually be stored in the blockchain?

We believe we have embarked on research into a fundamental problem, solutions to which are going to have profound impacts on ensuring safe supply chains, tamper-evident and tamper-proof devices, scalable and unique device identity, and secure business processes.

References

1. N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, pp. 80–89, 2018.
2. R. Maes, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, KU Leuven, Leuven, Belgium, 2012.
3. C. Böhm, and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. New York, NY, USA: Springer, 2013.
4. U. Rührmair, and D. E. Holcomb, "PUFs at a Glance," in *Proc. Conf. Des. Automat. Test Eur.*, 2014.
5. Chronicled, CryptoSeal (CSS100). 2016. [Online]. Available: https://store.chronicled.com/products/crypto-seal-strip
6. C. Gutierrez, and A. Khizhniak, "A close look at everledger—How blockchain secures luxury goods," 2017. [Online]. Available: https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/
7. K. Gandhi, "Magneprint: A real time risk management tool," MagTek Inc., 2009. [Online]. Available: www.magneprint.com/docs/99875279-3.01%20MP_WP_print.pdf
8. entrupy, "The world's first and only on-demand authentication solution," 2017. [Online]. Available: https://www.entrupy.com/
9. Intrinsic ID, "Flexible Key provisioning with SRAM PUF," 2017. [Online]. Available: http://donar.messe.de/exhibitor/cebit/2017/K172425/flexible-key-provisioning-with-sram-puf-eng-498126.pdf
10. E. Devadas, E. Suh, and S. Paral, "Design and Implementation of PUF-Based 'Unclonable' RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, Las Vegas, NV, USA, pp. 58–64.
11. L. Chen, C. Lai, R. Marchewka, et al., "Use of CdS quantum dot-functionalized cellulose nanocrystal films for anti-counterfeiting applications," *Nanoscale*, vol. 8, pp. 13288–13296, 2016.
12. G. M. Miyake, R. A. Weitekemp, V. A. Piunova, et al., "Synthesis of isocyanate-based brush block copolymers and their rapid self-assembly to infrared-reflecting photonic crystals," *J. Amer. Chem. Soc.*, vol. 134, pp. 14249–14254, 2012.
13. R. Diaz, E. Palleau, D. Poirot, et al., "High-throughput fabrication of anti-counterfeiting colloid-based photoluminescent microtags using electrical nanoimprint lithography," *Nanotechnology*, vol. 25, 2014, Art. no. 345302.
14. S. Incardona, E. Serra-Casas, N. Champouillon, et al., "Global survey of malaria rapid diagnostic test (RDT) sales, procurement and lot verification practices: Assessing the use of the WHO–FIND Malaria RDT Evaluation Programme (2011–2014)," *Malaria J.*, vol. 16, 2017, Art. no. 196.
15. T. F. Scherr, S. Gupta, D. W. Wright, et al., "An embedded barcode for 'connected' malaria rapid diagnostic tests," *Lab Chip*, vol. 17, pp. 1314–1322, 2017.
16. D.-H. Park, C. J. Han, Y.-G. Shul, et al., "Avatar DNA nanohybrid system in chip-on-a-phone," *Sci. Rep.*, vol. 4, 2015, Art. no. 4879.
17. S. Han, H. J. Bae, J. Kim, et al., "Lithographically encoded polymer microtaggant using high-capacity and error-correctable QR Code for anti-counterfeiting of drugs," *Adv. Mater.*, vol. 24, pp. 5924–5929, 2012.
18. O. Gökçe, C. Mercandetti, and E. Delamarche, "High-Content optical codes for protecting rapid diagnostic tests from counterfeiting," *Anal. Chem.*, vol. 90, pp. 7383–7390, 2018.
19. D. Dillenberger, V Balagurusamy, J. Ligman, et al., "IBM crypto anchor verifier," 2017. [Online]. Available: https://www.ibm.com/blogs/research/2018/05/ai-authentication-verifier/
20. K. Pietrzak, "Cryptography from learning parity with noise," in *Proc. Int. Conf. Curr. Trends Theory Practice Comput. Sci.*, 2012, vol. 7147, pp. 99–114, doi: 10.1007/978-3-642-27660-6_9.
21. I. Baturone, M. A. Prada-Delgado, and S. Eiroa, "Improved generation of identifiers, secret keys, and random numbers from srams," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2653–2668, Dec. 2015, doi: 10.1109/TIFS.2015.2471279.
22. R. Arjona, M.A. Prada-Delgado, J. Arcenegui, et al., "A PUF- and biometric-based lightweight hardware solution to increase security at sensor nodes," *Sensors*, vol. 18, no. 8, p. 2429, Jul. 2018, doi: 10.3390/s18082429.
23. A. Jain, S. Krenn, K. Pietrzak, et al. "Commitments and efficient zero-knowledge proofs from learning parity with noise," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2012, vol 7658, pp. 663–680, doi: 10.1007/978-3-642-34961-4_40.
24. S. Munetoh, C. K. Subramanian, A. Paidimarri, et al., "Smallest RISC-V device for next-generation Edge computing," in *Proc. RISC-V Workshop Barcelona*, May 2018.

Received May 31, 2018; accepted for publication February 1, 2019

Venkat S. K. Balagurusamy *IBM Research,Yorktown Heights, NY 10598 USA (vkbalagu@us.ibm.com).* Mr. Balagurusamy is a Research Staff Member working on developing and optimizing the verifier technology for different applications. He has decade-long experience working in bio-nanotechnology and also image analytics.

Cyril Cabral *IBM Research, Yorktown Heights, NY 10598 USA (cabral@us.ibm.com).* Mr. Cabral is a Research Staff Member working on packaging technology for the small computer project.

Srikumar Coomaraswamy *IBM Research, Yorktown Heights, NY 10598 USA (scoomara@us.ibm.com).* Mr. Coomaraswamy is an Engineer who helped develop the bcTracker demonstration.

Emmanuel Delamarche *IBM Research – Zurich, Rüschlikon 8803, Switzerland (emd@zurich.ibm.com).* Mr. Delamarche is a Principal Research Staff Member working on micro/nanotechnologies for medical diagnostic devices and applications.

Donna N. Dillenberger *IBM Research, Yorktown Heights, NY 10598 USA (engd@us.ibm.com).* Ms. Dillenberger is an IBM Fellow working on Enterprise Solutions, including blockchain, analytics, and the Verifier.

Gero Dittmann *IBM Research, Rüschlikon 8803, Zurich, Switzerland (ged@zurich.ibm.com).* Mr. Dittmann is a Research Staff Member focusing on identity management for IoT and blockchain. He previously worked on processor and system design in Switzerland, Germany, and the U.S.

Daniel Friedman *IBM Research, Yorktown Heights, NY 10598 USA (dfriedmn@us.ibm.com).* Mr. Friedman is a Distinguished Research Staff Member working on communications projects and the small computer effort.

Onur Gökçe *IBM Research Rüschlikon 8803, Zurich, Switzerland (ogo@zurich.ibm.com).* Mr. Gök e is a Postdoctoral Researcher developing advanced concepts for the next generation of point-of-care diagnostic devices.

Nigel Hinds *IBM Research, Yorktown Heights, NY 10598 USA (nhinds@us.ibm.com).* Mr. Hinds is a Software Developer who helped develop the bcTracker demonstration.

Jens Jelitto *IBM Research, Rüschlikon 8803, Zurich, Switzerland (jje@zurich.ibm.com).* Mr. Jelitto is a Research Staff Member and is working on the industrial application of Blockchain technologies with focus on role of IoT.

Andreas Kind *IBM Research, Rüschlikon 8803, Zurich, Switzerland (ank@zurich.ibm.com).* Mr. Kind is a Research Staff Member working on IoT, blockchain, and security. He is a member of the IBM Academy of Technology.

Ashwin Dhinesh Kumar *IBM Research, Yorktown Heights, NY 10598 USA (ashwin.dhinesh.kumar@ibm.com*). Mr. Kumar is a Software Developer working on the Verifier**.**

Frank Libsch *IBM Research, Yorktown Heights, NY 10598 USA (libsch@us.ibm.com).* Mr. Libsch is a Research Staff Member working on packaging technology for the small computer project.

Joseph W. Ligman *IBM Research, Yorktown Heights, NY 10598 USA (jwligman@us.ibm.com).* Mr. Ligman is a Senior Software Engineer working on the Verifier.

Seiji Munetoh *IBM Research, Yorktown Heights, NY 10598 USA (munetoh@jp.ibm.com).* Mr. Munetoh is a Research Staff Member working on digital circuit design and chip architecture for the small computer project.

Chandra Narayanaswami *IBM Research, Yorktown Heights, NY 10598 USA (chandras@us.ibm.com).* Mr. Narayanaswami is a Principal Research Staff Member and is currently working on electronic commerce with a focus on self-healing supply chains. He is a Fellow of the IEEE and a member of the IBM Academy of Technology and Industry Academy.

Abhilash Narendra *IBM Research, Yorktown Heights, NY 10598 USA (abhilash.narendra1@us.ibm.com).* Mr. Narendra is a Software Engineer focusing on the development of blockchain solutions, including those linking blockchain to the physical world.

Arun Paidimarri *IBM Research, Yorktown Heights, NY 10598 USA (apaidima@us.ibm.com).* Mr. Paidimarri is a Postdoctoral Researcher working on mixed-signal design for the small computer project and on the linkage between IoT-class devices and blockchain.

Miguel Angel Prada Delgado *Instituto de Microelectrónica de Sevilla, Universidad de Sevilla, Seville 41092, Spain (prada@imse-cnm.csic.es).* Mr. Delgado is working toward the Ph.D. degree in hardware security. He has a particular focus on SRAM-based fingerprints.

James Rayfield *IBM Research, Yorktown Heights, NY 10598 USA (jtray@us.ibm.com).* Mr. Rayfield is a Research Staff Member working on blockchain solutions and industry innovations.

Chitra Subramanian *IBM Research, Yorktown Heights, NY 10598 USA (cksubram@us.ibm.com).* Mr. Subramanian is a Research Staff Member working on digital circuit design for the small computer project.

Roman Vaculin *IBM Research, Yorktown Heights, NY 10598 USA (vaculin@us.ibm.com).* Mr. Vaculin is a Research Staff Member working on blockchain innovations, IoT, and AI.