A PUF taxonomy

Cite as: Appl. Phys. Rev. **6**, 011303 (2019); https://doi.org/10.1063/1.5079407
Submitted: 30 October 2018 • Accepted: 06 January 2019 • Published Online: 12 February 2019

Thomas McGrath, Ibrahim E. Bagci, Zhiming M. Wang, et al.

Applied Physics Reviews REVIEW scitation.org/journal/are

A PUF taxonomy

Cite as: Appl. Phys. Rev. **6**, 011303 (2019); doi: 10.1063/1.5079407
Submitted: 30 October 2018 · Accepted: 6 January 2019 ·
Published Online: 12 February 2019

Thomas McGrath,[1] Ibrahim E. Bagci,[2] Zhiming M. Wang,[3] Utz Roedig,[2] and Robert J. Young[1,a)]

AFFILIATIONS

[1]Physics Department, Lancaster University, Lancaster LA1 4YB, United Kingdom
[2]School of Computing and Communications, Lancaster University, Lancaster LA1 4YB, United Kingdom
[3]Institute of Fundamental and Frontier Sciences, University of Electronic Science and Technology of China, Chengdu 610054, China

[a)]Author to whom correspondence should be addressed: r.j.young@lancaster.ac.uk

ABSTRACT

Authentication is an essential cryptographic primitive that confirms the identity of parties during communications. For security, it is important that these identities are complex, in order to make them difficult to clone or guess. In recent years, physically unclonable functions (PUFs) have emerged, in which identities are embodied in structures, rather than stored in memory elements. PUFs provide "digital fingerprints," where information is usually read from the static entropy of a system, rather than having an identity artificially programmed in, preventing a malicious party from making a copy for nefarious use later on. Many concepts for the physical source of the uniqueness of these PUFs have been developed for multiple different applications. While certain types of PUF have received a great deal of attention, other promising suggestions may be overlooked. To remedy this, we present a review that seeks to exhaustively catalogue and provide a complete organisational scheme towards the suggested concepts for PUFs. Furthermore, by carefully considering the physical mechanisms underpinning the operation of different PUFs, we are able to form relationships between PUF technologies that previously had not been linked and look toward novel forms of PUF using physical principles that have yet to be exploited.

TABLE OF CONTENTS

I. INTRODUCTION

A Physically Unclonable Function (PUF) is a hardware security fundamental that translates an input challenge into an output response through a physical system in a manner that is specific to the exact hardware instance (unique) and cannot be replicated (unclonable). This allows the system, and by extension any object or device it is attached to or embedded within, to be uniquely authenticated. At the point of manufacture, the system is subjected to one or more challenges, and the response to these challenges is taken and recorded. From then on, it is known that if a challenge is repeated at any point and its

expected response is verified, the device must be the same as the one characterised previously. The characteristics of a PUF are to be robust (stable over time), unique (so no two PUFs are the same), easy to evaluate (to be feasibly implemented), difficult to replicate (so the PUF cannot be copied), and very difficult or impossible to predict (so the responses cannot be guessed). Many concepts have been put forward as candidates for PUFs. Some, such as the Arbiter PUF, have become very well established with a large number of variations (such as the basic Arbiter PUF,[1] N-XOR Arbiter PUF,[2] Double Arbiter PUF,[3] and so forth). Others, such as the MEMS PUF[4] or BoardPUF,[5] do not appear to have significant current industry focus. While papers exist that provide information and organisation to a selection of proposed PUFs, no paper sets out to provide a full review and organisation scheme for all suggested PUFs at the concept level and above. This review will attempt to exhaustively catalogue all the different concepts that have been suggested as ways to implement PUFs and to create a coherent taxonomic system to organise them. This is achieved by first introducing preliminary information (Sec. II) to provide context for the review that follows. The section following this information introduces three different systems of classification (Sec. III). Once these classification systems are discussed, a large number of PUF concepts are listed and explained, ordered by an organic classification system that lends itself to this listed format (Sec. IV). An example of a PUF concept arranged in this organic scheme would be the static random access memory (SRAM) PUF.[6] The SRAM PUF is ordered within a section on volatile memory (including similar volatile-memory-cell PUFs such as the DRAM PUF[7] and the MEmory Cell-based Chip Authentication (MECCA) PUF[8]), which is in turn within a higher-order section of implicit/intrinsic PUFs (alongside racetrack and direct characterisation PUF sections). Finally, the section of implicit/intrinsic PUFs, along with explicit/extrinsic PUFs, is within the classification of all-electronic PUFs (as opposed to "hybrid" PUFs, which probe the unique characteristic of the physical system in a non-electronic way, such as using light). The final sections of this report (Secs. V and VI) provide a number of observations that became apparent as a result of arranging and cataloguing these PUF concepts.

II. PRELIMINARIES

A. Weak and strong PUFs

A key distinctive property of PUFs is what is described as the strength of their implementation.[9] There are two levels of PUF strength—weak and strong. The strength of the PUF depends on the number of challenge response pairs (CRPs) that can be generated from a single device. This, in turn, typically corresponds to how the number of CRPs increases with the increasing device size. This rate of scaling tends to act as the metric that determines the strength of a PUF, although exceptions are argued and will be discussed later in this chapter. Weak PUFs support a relatively small number of CRPs, typically as a consequence of a low-order rate of scaling. This means that the full set of these pairs can be read from the device should an attacker gain physical access to the PUF for any given time. While it would not be possible to copy the physical PUF itself, with knowledge of the PUF's CRPs an attacker could convincingly respond to query as if they still possessed the device—long after the device has left their possession. Weak PUFs can be used for secure key storage and entity authentication techniques, for instance, using the protocol featured in Fig. 1. However, for authentication purposes, the PUF must be examined in an environment where an authenticating party is present to ensure that the PUF itself is being evaluated.

Strong PUFs, on the other hand, scale in a manner as to support a much larger set of CRPs. The number of these pairs is so large, in fact, that even if an attacker has access to the PUF they cannot feasibly record them all. If in the manufacturing stage a sample of these CRPs is randomly taken, the chances that the attacker also recorded the response to the same challenge can be negligible. This results in a system where even if the attacker had access to the PUF at a certain point, only the user with physical access to the PUF at the time of the challenge can give the correct response and be authenticated. Additionally, such a large repertoire of CRPs means that each challenge response pair need only be used once. This protects against an attacker eavesdropping and can facilitate secure communication protocols using the PUF (for instance, with each CRP acting as one unit in a one-time pad, as discussed in the section "PUF applications"). A simple example of a strong PUF authentication protocol is featured in Fig. 2.

The strength of a PUF is generally determined by how the number of potential CRPs scales with the increasing PUF size. In general, if the number of CRPs supported by the PUF scales exponentially with its size, it is considered strong, while linear or polynomial increases typically correspond to weak PUFs. Exponential scaling produces exceptionally large CRP sets with the increasing device size. Occasionally, PUFs with linear or high-order polynomial CRP growth are described as strong. The arguments for this tend to be a limiting read speed, high information density, or the capacity for significant parallel manufacture on a linearly or polynomial increasing PUF (for example, the

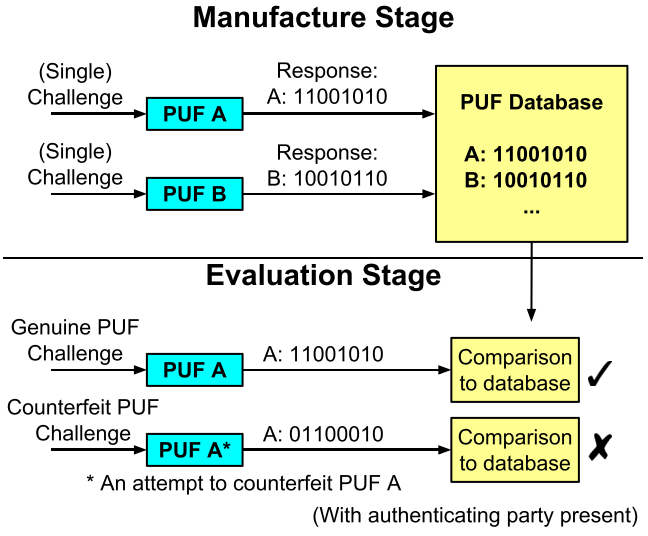

FIG. 1. A simple implementation of the weak PUF. The response of any attempted counterfeit would detectably differ compared to the response recorded of the genuine PUF.

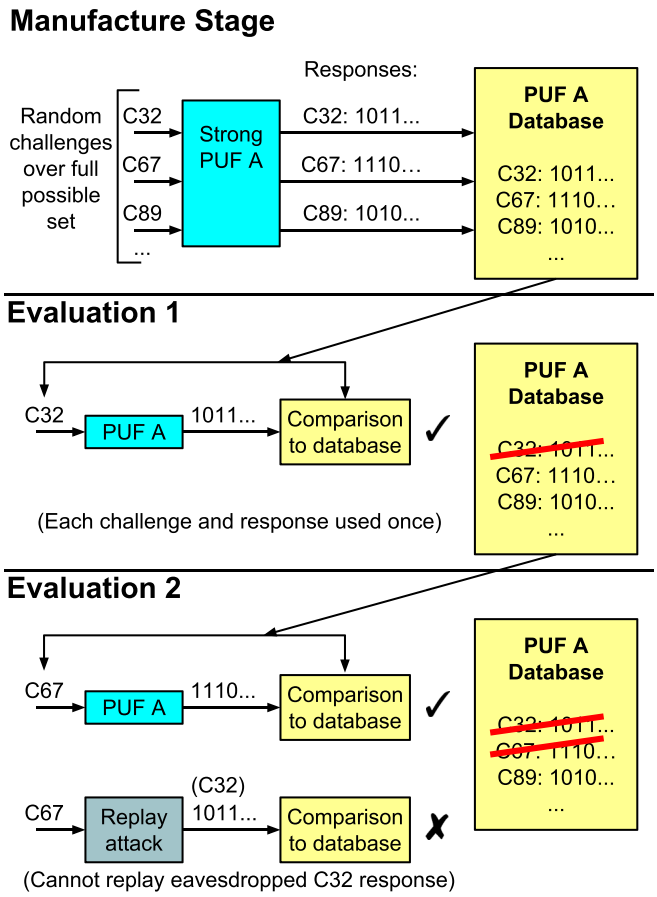

FIG. 2. A simple implementation of the strong PUF. Here, even if the PUF is compromised an attacker would not know the relevant challenges to record, and an eavesdropper could never hear a usable challenge response pair.

super high information content (SHIC)[10] PUF) allow a redundantly large number of CRPs, similar to exponential scaling PUFs. It is apparent that a strong PUF would be inherently more versatile than a weak PUF; however, constructing a true strong PUF is very difficult or impossible since the device should not be vulnerable to modelling attacks.[11] This is where machine learning or physical intuition can be used to "fill in the blanks" of an attacker's limited set of challenge response pairs. In other words, employing techniques aiming to take the responses of a non-exhaustive and obtainable list of challenges and derive rules to calculate the response for any further challenge.[12]

Alongside the disagreement as to what constitutes a "weak" and "strong" PUF, there is a level of disagreement as to what can be called a PUF in the first place. Rührmair *et al.*[13] suggest a definition of a PUF that requires a secret element. This has the consequence that all claimed-to-be weak PUFs that probe physical randomness non-electronically should not be called PUFs at all, as there are no necessarily any hidden secrets, only an unrepeatable fabrication. A less strict definition is suggested by Guajardo *et al.*[6] that allows for the non-electronic examination of weak physically unclonable functions. For impartiality, the criteria for inclusion in this report will be lax and will include any concept that has been described as a PUF, either in the original document or after the fact.

B. Implicit and explicit randomness

One important distinction between architectures of PUFs is how the uniqueness-causing randomness arises. This variation is either applied externally through additional steps (explicit randomisation) or naturally arising from variations in standard manufacturing processes (implicit randomisation).[14] In CMOS electronic PUFs, adding additional CMOS components to the circuit can be done without introducing randomisation through additional steps, with deviation arising from manufacture variation. Therefore, evaluation of typical CMOS electronic components deliberately added to a CMOS circuit is still considered a source of implicit randomness, whereas attaching non-CMOS components to a CMOS circuit would be considered by introducing explicit randomness. In general, implicit randomness arising in PUFs is preferable to explicit varieties, as naturally arising variation requires no additional processing steps to introduce—an operation which adds cost. Additionally, the implicit variation that arises from process variations inherent in typical manufacture processes cannot be directly manipulated. This means that even the fabricator of the device cannot tamper with the manufacture in such a way as to remove or alter the random features of the PUF.

C. Intrinsic and extrinsic evaluation

Further to the distinction between a PUF with implicit or explicit sources of randomness, a device can be classified into intrinsic and non-intrinsic evaluation varieties. An intrinsic PUF has randomness that arises in an implicit manner and also internally evaluates.[15] As a result, the means of measuring or probing the PUF is embedded within, or intrinsic to, the device itself. If these two conditions are not met, for instance, in the case of a non-integrated implicit randomness source or an explicit randomness source, the PUF is described as non-intrinsic, or extrinsic. Currently, this intrinsic property can only be possessed by all-electronic PUFs, since the only way for a PUF to be evaluated and give an electronic readout at this time is through an all-electronic evaluation mechanism. Internal evaluation mechanisms are more desirable than external evaluation as they allow further processing (for instance, hashing) to take place without having the initial PUF response exposed to the outside of the PUF's internal circuitry. This integration of the randomness source and evaluation circuitry greatly helps to resist man in the middle and side channel attacks between the two elements. Evaluation mechanisms internal to the PUF also tend to be more accurate, easier to use, and less prone to malefactor interference.

D. PUF applications

While the most common use of physically unclonable functions is for authentication, many additional applications exist. Fundamentally, the weak PUF can be described as a mechanism to generate on manufacture and store a single (or small number of) cryptographic keys. This key can then be compared to an external database for identification or authentication as

previously discussed, or used as part of other protocols such as secure communication or memory encryption. As with the previously described authentication protocols, the number of keys stored is small, so an attacker could have access to the PUF in such a way as to determine those keys, making the system then unsecure. This would be the same as an attacker discovering the password or key for the communication or encryption in a more conventional system.

The strong PUF can also be used for the same applications and can be considered as a mechanism for generating a large number of keys upon manufacture to be thereafter stored. Like in the strong PUF authentication protocol this means that the keys can be used redundantly, enhancing security. This would operate like a one-time-pad in conventional cryptography, where each authentication exchange, secure communication message, or bit of encrypted data can utilise a different key—and the compromise of a single key would not necessarily impact the whole system. Additionally, should the key be chosen randomly from the large possible set, access to the PUF must occur at the same time as the authentication, communication, or decryption, as determining which key is necessary to record and replay would not be possible ahead of time. In addition to these applications, protocols have been devised that specifically allow for bit commitment,[16] oblivious transfer,[17] and secure key exchanges.[18]

Certain PUF designs can also involve enclosing the PUF evaluation and/or other critical components within the source of entropy itself, in a system commonly known as an enclosure PUF. These can be electronically evaluated, for instance, in the case of the coating PUF,[19] or non-electronically evaluated such as a version of an optically evaluating nanoparticle distribution PUF.[20] The value of this system is tamper evidence, where an attempt to physically access or probe inside the PUF would rearrange the source of entropy and change the readout of the PUF when it is next evaluated. This can be valuable to prevent side channel attacks on the PUF's own electronics, or to even void memory or nullify other circuits should the enclosure be breached.

E. PUF extensions

There also exist a number of additional or alternative extensions to the concepts of PUFs, which can expand their functionality and capability. The two most notable of these are the reconfigurable PUF (rPUF) and the public PUF (PPUF). The rPUF[21] is a device that can deliberately change its response to the same input challenge. This allows for the update of new challenge response pairs, the revoking of previous CRPs and allows a PUF to be reset, for instance, for the reassigning of the device to a new purpose or user. Care must be taken to ensure the new response, reset in the field, is as unique and unpredictable as the responses that were initially generated in the manufacture phase. An example mechanism for this PUF includes melting optical media as part of an optical PUF or the controlled refreshing of a cell of non-volatile memory, such as PCM (Phase Change Memory) RAM[22] or STT-MRAM (Spin-Transfer-Torque Magnetic Random Access Memory) PUFs.[23]

The PPUF,[24] otherwise known as the SIMPL (SIMulation Possible but Laborious) system,[25] is more complex. Here, the PUF can be modelled from parameters in a time laborious process. This means that someone with access to the parameters can, given time, derive one or more of the challenge response pairs that exist within the physical PUF itself. The amount of time that this process takes means that characterising more than a small number of these CRPs is prohibitive, and so a full characterisation of the PUF is said to be prohibited. On the other hand, as expected, the owner of the physical PPUF can very easily challenge their device to receive the corresponding response with very little time burden.

A simple implementation of a PPUF for secret key exchange is featured in Fig. 3. In this scheme, Bob has access to a publicly available model of Alice's physical PPUF. This model can translate a challenge (here a random challenge from a defined set) into the PUF's expected response in a not insignificant time frame. This response can then be sent to Alice through any public or private channel. Alice can then iterate through the full set of possible challenges until she finds the response that matches the one sent from Bob. This iteration can only be done with the physical device due to time constraints on its' modelling. Therefore, only Alice (the owner of the physical device) can translate the response back to find the initial secret key. This protocol is similar to asymmetric key encryption in public key cryptography, where the PPUF model acts as Alice's public key, and the iterable physical device acts as Alice's private key. However, it is worth noting here that this system assumes that this computation-heavy task will always take so long as to inhibit the collection of a large number of these pairs and recreate the PUF. Steps forward in conventional computer power and quantum computing could therefore invalidate or weaken PPUF systems, in the same manner as RSA factorisation key lengths in public key cryptography.[26,27]

III. CLASSIFICATION SYSTEM

Many concepts and variations of physically unclonable functions exist and even more have been suggested for both the

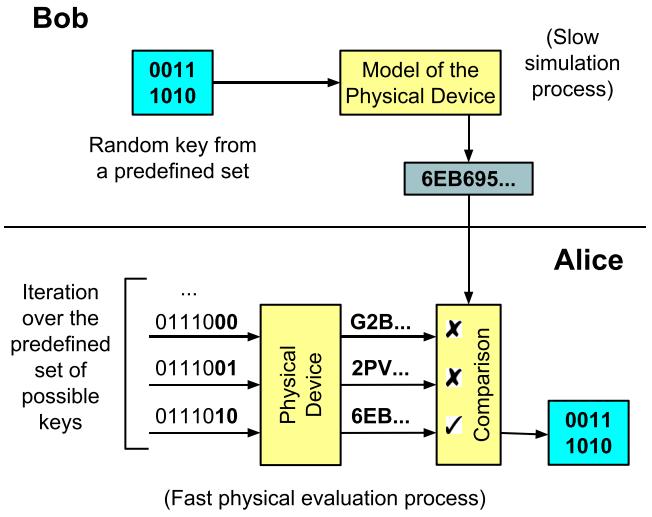

FIG. 3. A diagram showing a simple implementation of the PPUF for secret key exchange. The one way function can only be reversed through the iteration of the physical device, due to speed constraints on the simulation process.

characterisation of circuits and of physical objects. Creating a universal ordering, classification or taxonomic system is therefore non-trivial. Here, 3 different organisation schemes are presented. These are described as Organic (property-driven), Parametric (parameter-driven), and Chronological (timeline-based) classification.

A. Organic system

The first system, featured in Fig. 4, divides the set of PUFs into groups over 6 levels (the level containing the set of all PUFs excluded). These levels start with the Application, Randomness Source (implicity), Family, and Concept—along with two further levels and a grouping of concepts. These further levels are not included in the following organisation scheme diagrams and relate to the specific variation and implementation of a real world PUF, to uniquely identify any device to the smallest level possible.

The first level of categorisation, the Application, intends to differentiate between the environments in which the physically unclonable function is to operate. In this system, this splits into two—the application of PUFs for circuits (electronic applications) using All-Electronic designs and for application on or into real-world objects (physical applications) using Hybrid designs. These Hybrid designs change the medium used to probe the PUF's source of uniqueness, from an electronic signal to, for instance, emitted and detected light. While the mechanisms for the authentication between these two applications vary radically, this is not to say, that a physical application PUF is free from electronics. A response is typically compared to a database-entered pre-measured equivalent, and so digitisation (and therefore typically the use of electronics) must be utilised at some stage in almost every PUF. Additionally, it must be noted that a hybrid PUF can (inefficiently) provide authentication to an electronic circuit, and vice versa. This organisation level is not intended to imply applicational exclusivity—simply the existence of a change in probing medium from electronic, or lack thereof.

The second level of organisation, the Randomness Source, sorts by examining the source of PUF's characteristic randomness. PUFs can have either implicit or explicit randomness sources (see Sec. II B, "Implicit and Explicit Randomness"). Electronic PUFs that rely on implicit randomness have the capacity for having intrinsic evaluation, while explicit randomness electronic PUFs and physical PUFs must be extrinsic (Sec. II C, "Intrinsic and Extrinsic Evaluation"), as reflected in the category labels of the figure.

The third level of organisation in this scheme is what common theme, or Family, the PUFs belong to. These include the racetrack family of PUFs, which include PUFs that rely on comparing or analysing time delays or latency in a signal line, to the small family of RF PUFs that use the alteration of the properties of a radiofrequency signal to authenticate. There exists a certain level of higher-order grouping between these families. These would be grouping the PUFs that analyse a circuit's response in the time domain, those that directly characterise components, validate optically, and those that build PUFs out of units derived from memory cells.

The organic grouping system is more arbitrary and not as concrete as the parametric or chronological organisation scheme but appears as more intuitive. For this reason, the PUF concepts detailed in this paper beyond will be organised by this organic categorisation scheme.

B. Parametric system

The second organisation scheme is the parametric scheme, shown in Fig. 5. This divides the set of PUF concepts into two levels. The first of these levels, the Evaluation Mechanism, organises by what medium the signals that evaluate the PUF exist in, such as an electronic signal, a beam of light or laser, radiofrequency electromagnetic waves, or near-field magnetic radiation. The second level, the Evaluation Parameter, sorts the PUFs into the specific and principal parameter of the evaluated property being examined. An example of this would be the parameter of time for the arbiter PUF (comparing the propagation time between two signal racetracks) or the parameter of capacitance for the capacitor-inlaid BoardPUF. At this second level, there exists an amount of grouping across parameters. These group the parameters into time domain parameters (Time and Frequency), binary state parameters (Binary Connectivity and Bistable State parameters that both provide direct 0/1 responses), and component constant parameters (the constant Voltage-Current Characteristic or Capacitance properties of the circuit or its components). It is worth noting here that many PUF implementations evaluate by comparing the parameters of two components to get a 0/1 response as output (known as pairwise comparison) but are not considered to be fundamentally Binary State parameter PUFs. For the purposes of this organisation scheme, the most apparent property parameter being examined is taken. This means, for instance, that the cross-linked transistor SRAM PUF that examines the value held within the memory cell upon power up is in a different category to the threshold voltage (TV)[28] PUF, even in an implementation that compares two transistors to translate into a 0/1 response. It is possible that a PUF may examine more than one parameter, such as an optical PUF that looks at an image's brightness (optical intensity) and colour (optical frequency). This is a rare occurrence, as it adds another dimension of complexity to the PUF extraction process. In these situations, a similar PUF concept can exist in two or more of these categories. It is also worth noting here that while the implementations cited for the plasmonic nanoparticle distribution[29] and lanthanide luminescence[30] optical PUFs involve the frequency domain by way of splitting into RGB (Red, Green and Blue) or CMYK (Cyan, Magenta, Yellow and Key) channels, they are not considered here as fundamentally having the frequency parameter. This splitting is typically done by evaluating the PUF against a small number of detectors examining different frequencies, and while this increases the parameter space of the PUF, these elements are not a specific requirement for the PUF concept to function and involve a very small number of bins in the frequency domain. Beyond the family in the organic scheme and parameter in the parametric scheme lies the Concept level—the finest level of detail to which this paper will examine PUFs. PUF concepts are the higher-level ideas as to how to design and produce a PUF from a certain physical or electronic system and include the Arbiter PUF, Glitch PUF,[31] SRAM failure PUF,[32] STT-MRAM PUF, and so on. Further to the concept level is suggested to be the Variation and

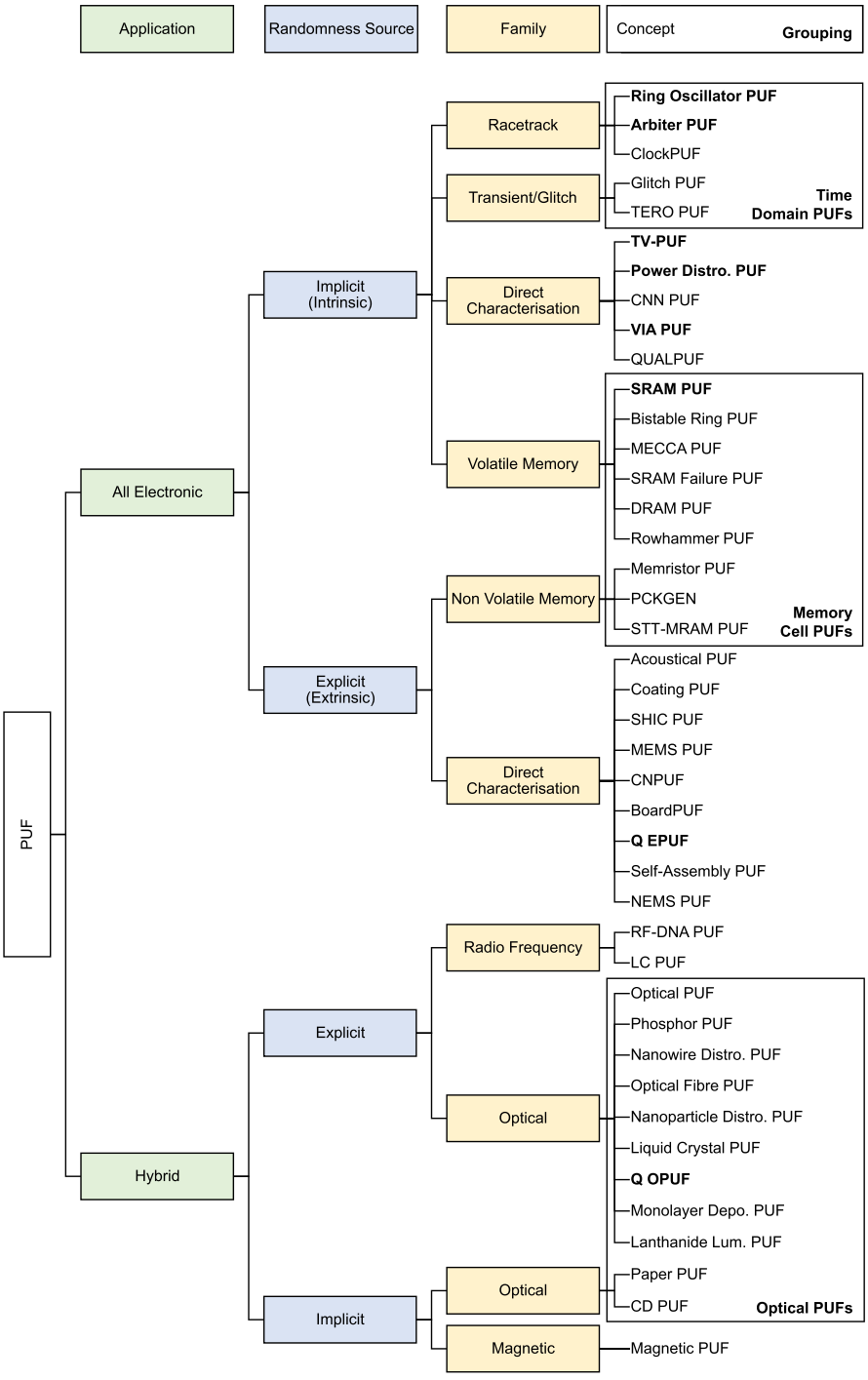

FIG. 4. Graph to show the "organic" organisation scheme for physically unclonable functions. Industry focus in bold font.

Implementation levels. Variation would stand to represent the many different varieties of the same PUF concept, for instance, attempts to make the PUF more secure (such as an Arbiter PUF's repeated application of the XOR operation), or to tailor the overall architecture of the PUF to a specific application (such as a lower power electronics version). These variations do not stray from the initial concept enough to make their own concept category and exist as differing "flavours" of the higher conceptual level. To fully identify any PUF found in the wild, the implementation specifics of the PUF must also be included. This can be done by using the manufacturer and model information. The manufacturer and model may represent a standalone product of

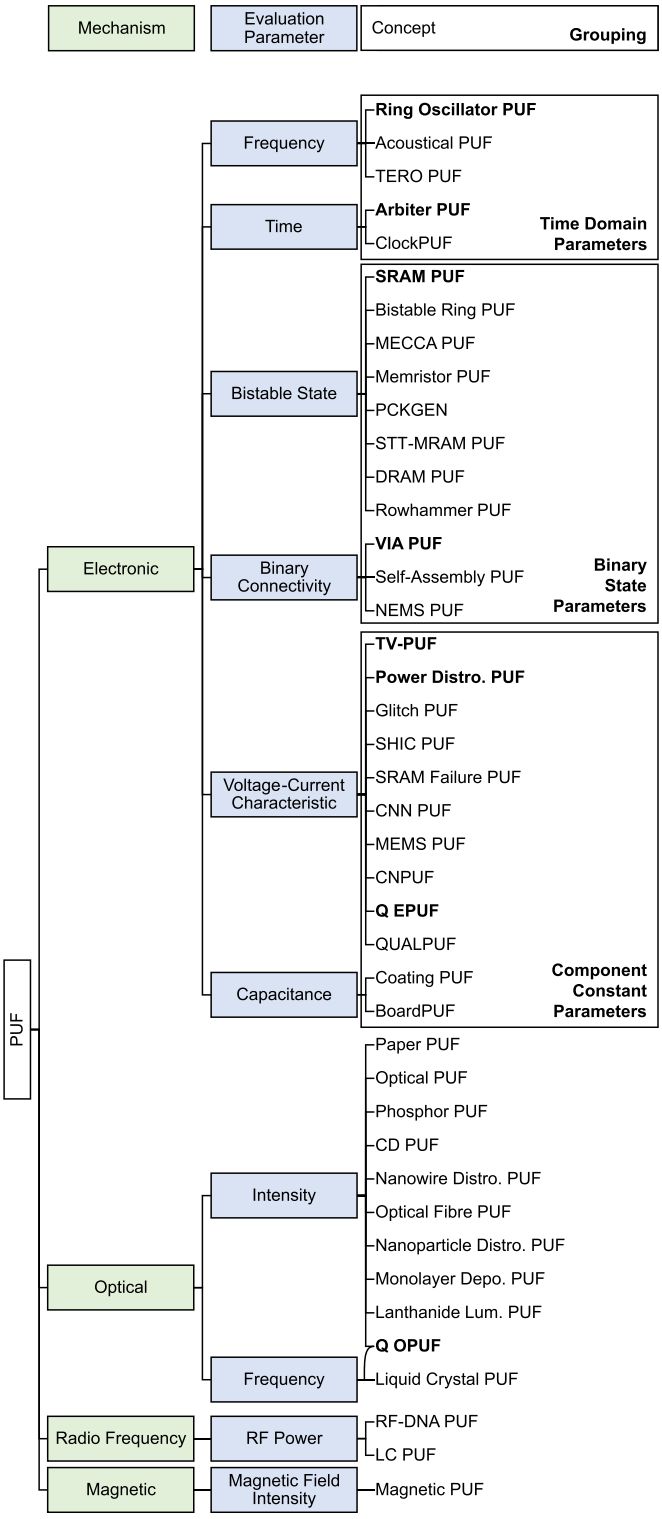

FIG. 5. Graph to show the "parametric" organisation scheme for a range of PUFs. Note that the Q OPUF has both frequency and light intensity evaluation parameters. Industry focus in bold font.

a PUF (such as a standalone circuit or physical object security tag) but can also be a reference to the circuit or object that hosts the PUF. An example of this would be a PUF-capable FPGA (Field-Programmable Gate Array) or PUF-integrated EEPROM (Electrically Erasable Programmable Read Only Memory) circuit designed and sold as a package for a purpose beyond simple authentication. As a full example, the Xilinx Zynq Ultrascale+ MPSoC range utilises ring oscillator PUFs for security.[33] The PUF in a Zynq UltraScale+ CG can therefore be categorised organically as follows: The component is a PUF by fundamental, electronic by Application, implicit by Randomness Source, a racetrack PUF by Family, a ring oscillator PUF by Concept, an in-house design for Variation, with the Implementation being Xilinx as the manufacturer, and the UltraScale+ CG as the model. Alternatively, the PUF can be categorised as electronic by Evaluation Mechanism and as frequency for Evaluation Parameter before the concept, variation, and implementation categories as previous. The properties discussed above are also represented in Table I.

C. Chronological system

The final organisation scheme is the chronological. As the name suggests, this scheme simply orders by the date of the concept's first suggestion. In Table II, these concepts are split up in the All-Electronic mechanism by time domain, memory cell, and direct characterisation—the groupings from the organic organisation scheme. The Hybrid mechanism PUFs are grouped into optical and non-optical PUFs. This division into separate tracks acts to detail the accumulation of concepts in each of these major schools of thought, and the evolution of what novel PUFs are suggested over time.

In the following figures and tables, PUFs that have contemporary industry focus (insofar as there are companies that externally advertise and offer these PUFs as solutions) are highlighted in bold font. These are the SRAM PUF (Intrinsic ID[34]), the Ring Oscillator and Arbiter PUFs (Verayo[2,35]), the power distribution and TV-PUF (examining CMOS component parameters, from Quantum Trace[36]), the VIA (Vertical Interconnect Access) PUF (ICTK[37,38]), and the quantum Electronic PUF (Q-EPUF) and Quantum Optical PUF (Q-OPUF) (Quantum Base[39,40]). Concepts that have received commercialisation focus only in the past, such as the MEMS PUF (Veratag[41,42]), are not included in this scheme.

IV. POPULATING THE PUF TREE

Now that a categorisation and ranking system is put into place, it must be populated. This review aims to examine the PUF "fundamental" down to the conceptual level of detail. This section aims to detail the constituents of each level down to the concept level.

A. Implicit/intrinsic all-electronic PUFs

1. Racetrack PUFs

Racetrack PUFs examines a component of the system's latency—the time taken for a signal to complete a set course of wiring or components. This family is similar to the transient/glitch family of PUFs in that they both operate in the

TABLE I. Table of PUF concept properties with grouping for 40 suggested PUF concepts. Industry focus in bold font.

Concept	Mechanism	Parameter	Implicity	Evaluation	Family
Arbiter PUF[1]	All-electronic	Time	Implicit	Intrinsic	Racetrack
ClockPUF[43]					
Ring oscillator PUF[44]		Frequency			Transient/glitch
TERO PUF[45]					
GlitchPUF[31]		Voltage/current			Volatile memory
SRAM failure PUF[32]					
Bistable ring PUF[46]		Bistable state			
DRAM PUF[47]					
MECCA PUF[8]					
Rowhammer PUF[48]					
SRAM PUF[6]		Voltage/current			Direct characterisation
CNN PUF[49]					
Power distro. PUF[50]					
QUALPUF[51]					
TV PUF[28]					
VIA PUF[38]		Binary connectivity	Explicit	Extrinsic	
NEMS PUF[52]					
Self-assembly PUF[53]		Voltage/current			
CN PUF[54]					
MEMS PUF[55]					
Q EPUF[56]					
SHIC PUF[10]		Capacitance			
BoardPUF[5]					
Coating PUF[19]		Frequency			Non-volatile memory
Acoustical PUF[57]					
Memristor PUF[58]		Bistable state			
PCKGEN[22]					
STT-MRAM PUF[23]					
CD PUF[59]	Hybrid (optical)	Light intensity	Implicit		Optical
Paper PUF[60]					
Nanowire distro. PUF[61]			Explicit		
Optical fibre PUF[62]					
Optical PUF[63]					
Phosphor PUF[64]					
Nanoparticle distro. PUF[29]					
Monolayer depo. PUF[65]					
Lanthanide lum. PUF[30]					
Q OPUF[66]		Intensity and Frequency			
Liquid crystal PUF[67]		Frequency			
LC PUF[68]	Hybrid (RF)	RF power absorption			RF
RF-DNA PUF[69]					
Magnetic PUF[70]	Hybrid (magnetic)	Mag. field intensity	Implicit		Magnetic

time domain, that is to say, that how the system reacts over passing time is examined in both cases. The difference between these two categories is that while racetrack PUFs examine the propagation time of a signal down a defined, typically linear or looping, course transient/glitch PUFs examine the variation over time of a signal arising from a more complex, convolutional system.

a. Ring oscillator PUF. A Ring Oscillator PUF[45] operates by examining the variation in the delay, and therefore frequency, of a signal travelling through an oscillator circuit formed of inverter/NOT logic gates. This is based on the manufacture variation of the signal line and logic gate constituents. The oscillator, known as a ring oscillator, consists of an odd number of NOT gates with the output of the gate chain feeding back into the input of the chain (Fig. 6). An odd number of these gates in a chain ensures that for any input into the first gate of the chain, the inverse leaves the last gate. If this inverted signal is fed back into the system, the next output would be the original signal. As this signal is again fed back into the input, the system would continue to oscillate. A pulse is inputted into the ring oscillator

TABLE II. Timeline of PUF concepts by date of first introduction. PUF concepts that rely on explicit randomness featured in grey boxes, while PUFs with industry focus featured in bold font.

	All-electronic			Hybrid	
Year	Time domain	Memory cell	Direct char.	Optical	Non-optical
1993				Paper PUF	
1994					Magnetic PUF
1995					
1996					
1997					
1998					
1999					
2000			**TV-PUF**		
2001					
2002	**Ring-oscillator PUF**			Optical PUF[a]	
2003					
2004	**Arbiter PUF**		Acoustical PUF		
2005					
2006			Coating PUF		
2007		**SRAM PUF**			RF-DNA PUF
2008				Phosphor PUF	
2009			**Power distro. PUF**	CD PUF	LC PUF
2010	Glitch PUF		SHIC PUF		
2011	TERO PUF	Bistable ring PUF MECCA PUF SRAM fail. PUF			
2012					
2013	Clock PUF	Memristor PUF PCKGEN	CNN PUF MEMS PUF	Nanowire distro. PUF Optical fibre PUF	
2014		STT-MRAM PUF	CN PUF		
2015		DRAM PUF	Board PUF **VIA PUF** **Q EPUF**		
2016			QUALPUF Self-assembly PUF	Nanoparticle distro. PUF	
2017		Rowhammer PUF	NEMS PUF	Liquid crystal PUF **Q OPUF** Monolayer depo. PUF	

[a]First paper to use the term "PUF."

circuit, causing the circuit to oscillate at a frequency (deriving from the input-output time delay) that depends on the unique random variations in the oscillator system. This frequency is measured and either taken as a response itself, or more typically compared to another ring oscillator with the same NOT gate chain length and input challenge (with different variations). In the simplest form, this comparison either returns a binary response depending on which frequency is greater, similar to the arbiter PUF's comparison of time difference. For these PUFs, the challenge is fundamentally the number or position of one ring oscillator, and the response is the oscillation frequency that component.

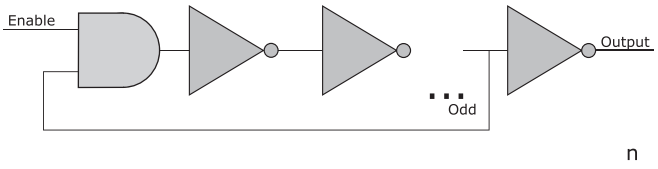

FIG. 6. A diagram displaying the setup of a ring oscillator.

b. Arbiter PUF. An Arbiter[1] PUF characterises a system through the comparative variation in the travel time of two electrical signals propagating down theoretically symmetrical paths. This is based on the manufacture variation in the creation of these paths. The PUF consists of several cells connecting a signal source to an arbiter component. The arbiter component gives a binary output depending on which of two input signals split from the signal source reaches the component first. Each cell has a switch that can route both signals through a different signal line when the switch is in its active state, and the activation state of each cell's switch acts as a unique challenge. Due to the random variations in the conductor and the switching gates that the signal passes down, the speed of both signals will vary relative to each other, resulting in a consistent "winner" signal associated with each "race," or directed route. In the simplest case, an arbitrary number of these directed paths (or permutations of the routing switches) are tested to build up a response with that same length of bits, as seen in Fig. 7. This PUF has a challenge built up from the on/off nature of the routing switches (and arbiter number/position for multiple of these systems) and gives a binary response depending on the faster path after this switching. A version of this concept, utilising race paths directed through cross-linked arrays of XOR gates, has been suggested as a simple PPUF system.[24]

c. ClockPUF. The ClockPUF[43] examines the variation in clock signal propagation speed down various branches of signal line, based on the manufacture variation of these lines. In circuit designs, there exists a clock network that routes a timing signal from the clock to various sections of the circuit itself. This network is designed to try to remove any differences between the time taken for the signal from the clock to reach any given area of the circuit, to ensure synchronicity. The issue of clock latency variation is known as clock skew. Modern designs almost entirely eliminate clock skew; however, variations and skewing still arise. This PUF compares the differences in pairwise signal latencies of ostensibly similar circuit paths to uniquely characterise a circuit, in a similar manner to an arbiter PUF. Here, the challenge would be the clock signal lines in question, and the response would be the latency of each respective line.

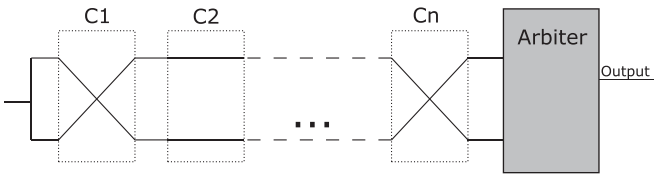

FIG. 7. A diagram showing the mechanism of a basic arbiter PUF.

2. Transient/glitch PUFs

While delay-based PUFs operate by setting up a discrete challenge (sometimes repeatedly, in the case of oscillators), transient/glitch PUFs examine the transient (temporary or changing over time) signals that arise from a circuit. These can consist of 2 or more ring oscillators XORed together to form unique patterns as transient mismatched signals or examine the self-correcting transients that appear in the process of a complex circuits natural operation, such as the glitch PUF.

a. Glitch PUF. The Glitch PUF[31] examines the complex variation of glitches that arise in delay-based circuits that are more complex than the Arbiter and NOT chain ring oscillators discussed above. This is based on the manufacture variation of the signal lines and logic components involved. These more complex circuits perform AND and XOR operations to multiple inputs. A glitch is described as a transient, self-correcting fault in a system. From the operation of these more complex circuitry arrangements, there arise transient output signal states that can be analysed to form a circuit-specific fingerprint, or a PUF. The challenge for this PUF concept would be the circuit itself, and the response would be the specific existence and time evolution of the glitches that emerge.

b. Transient Effect Ring Oscillator (TERO) PUF. The TERO PUF[45] examines the variation in frequency and duration of a signal down signal line and logic gate components, based on the manufacture variation of the components. The PUF consists of two cross-linked bistable ring oscillator chains, as shown in Fig. 8. This arrangement forms an even number of inverters, so the output of the TERO PUF cell settles into a stable state (in the same manner as the bistable ring or buskeeper memory cell), but not before exhibiting a number of temporary (transient) circuit oscillations. The number of oscillations that occur within each TERO cell before settling into the steady state is counted, with the counts for multiple cells combined to form a characteristic response for the TERO PUF. Here, the challenge is the TERO cell number or position (should multiple TERO cells exist), and the response is the transient oscillations that occur as the system comes to rest.

3. Direct characterisation PUFs

The next category for implementing implicit/intrinsic all-electronic PUFs is authentication through direct characterisation of electronic components (that do not require additional fabrication steps to create). This characterisation can examine a number of different properties–for instance, current in

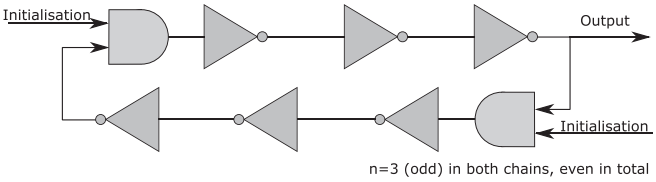

FIG. 8. The layout of a TERO PUF.

response to voltage, capacitance, or existence of circuit interconnects. In other works,[71,72] a similar category is described as "analogue electronic PUFs," since the majority of the PUFs here examine the analogue voltage-current properties of an electronic component. The analogue category does not account for or include, for instance, the VIA PUF,[38] where the existence or absence of an electronic connection results in a discrete binary 1/0 connected/disconnected output.

a. Threshold Voltage (TV) PUF. A Threshold Voltage PUF, TV PUF, or Integrated Circuit IDentification (ICID)[28] typically examines the variation in threshold voltage of integrated transistors based on the variations of these transistors at the point of production. The threshold voltage of a field effect transistor corresponds to the minimum voltage difference between the component's gate and source that is needed to allow current flow between the source and drain of the device. The PUF consists of an array of these transistor components that are tested to determine the point at which current starts to flow. The PUF's challenge is the number or position of the transistor component, and the response is the value of this threshold voltage.

b. Power distribution PUF. A Power Distribution PUF[50] uniquely characterises a system through the variance in resistance of the power distribution system in an integrated circuit, based on the manufacture variation of the power transfer lines. The power distribution system is a grid of conductors that route the power from its input into the circuit to the various components within. For a PUF functionality, additional components are added so that each branch of the power distribution grid can be shorted, bypassing the pre-existing components. The voltage drops (or similarly resistances) over several of these shorted branches within the IC power grid are measured one at a time to form a physically unclonable signature for the device. Here, the challenge is the number or position of power transfer line, and the response is the resistance of the line in question.

c. Cellular Neural Network (CNN) PUF. Another conceptual implementation of physically unclonable functions utilises the variation of the output states of Cellular Non-linear/Neural Networks (CNNs) for the same input states, based on the manufacturer variation of the components within. Cellular neural networks are locally coupled networks of cells, whose dynamics depend on the interconnection strengths to their neighbours. These are used for applications such as vision systems and simulations as they evolve in a non-typical manner over time—in accordance with partial differential equations. Two notable CNN PUFs variations have been suggested. The first concept attempts to directly simulate the non-linear wave propagation in a random media.[73] This in effect translates the complexity of an optical-style PUF into the domain of electronics—albeit evolving at a resolution limited by the number of electronic cells. The second concept involves a network of two coupled cells, or "neurons."[49] The paired system settles on an equilibrium state that is dependent on compounding manufacturing parameter variations. In these PUFs, the challenge is the initial input state of the CNN system, and the response is the final state of this interconnected system.

d. VIA PUF. A VIA (Vertical Interconnect Access) PUF[38] is based on the probability of a physical connection forming between the layers of an integrated circuit. The outcome for this formation is in turn based on the variation of processing conditions which occurs during the production of each circuit. The element of a circuit known as a via is the electrical connection between stacked circuit layers, generally in either integrated circuit or printed circuit board (PCB) designs. In typical circuit design, a regulated size of hole is removed from a metal layer to bridge the two sides. This regulated size ensures that a via is formed between the layers in the fabrication process, something a smaller hole design does not guarantee. If a smaller hole is put into the design, the chance of a via forming becomes probabilistic, relating to this desired hole size. By controlling factors including designed hole size and additional processing steps, a 50% probability of an electrical connection of the fabricated via can be obtained. On this principle, a collection of these vias can be fabricated—where the exact number and positioning of successful, conductive vias are unique to each circuit and considered a PUF. Here, the challenge can be considered as the number or position of the (potential) via interconnect in question and the response as the binary state of either the existence of a conductive connection, or lack thereof. This binary response for uniqueness, deriving from variations of interconnect lithography, is also featured in the LRR-DPUF (Learning Resilient and Reliable Digital Physical Unclonable Function).[74]

e. QUasi-Adiabatic Logic PUF (QUALPUF). A QUasi-Adiabatic Logic based PUF (QUALPUF)[51] utilises adiabatic logic to authenticate circuits in an energy efficient way. This PUF examines the variation in the constituent capacitor and transistor components of an adiabatic logic circuit, deriving from fabrication variation in the manufacture stage. Adiabatic logic is a system that uses design rules to recycle the charge stored in a load capacitor after operations are performed, thereby greatly minimising losses and creating very energy-efficient circuits. The circuit designs allowing this full recycling behaviour tend to be complex and large-area, so here a quasi-adiabatic circuit (that theoretically recovers only most of the capacitor charge) is used. In this PUF, a ramping voltage is put across two theoretically identical transistor elements in a circuit. Manufacturing process variations cause a mismatch between these two transistors, causing one transistor to be more conducting than the other and more readily charge a load capacitor. This results in a consistent response bit from each unit cell of this circuit, in a manner similar to MOS mismatch transistor PUFs. A unique characteristic of this PUF implementation is that any PUF cell is only evaluated at one stage of an equally timed set of 4, because adiabatic logic operates in specific charging/discharging cycles. To account for this, each bit-unit of the PUF consists of 4 of these cells, offset by a 90° phase difference from each other. Consequently, each unit of the PUF would alternate between 4 unique responses and give 4 separate, but repeated bits of response over time. This means that over the whole PUF, four

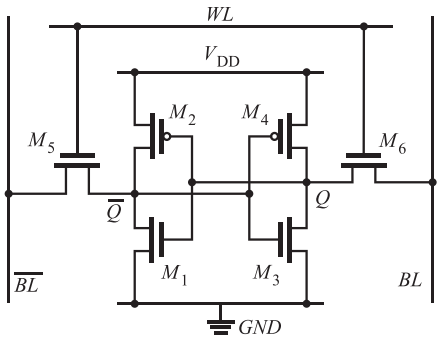

FIG. 9. The circuit diagram for a Static Random Access Memory (SRAM) cell.[75]

changing patterns of signature forming bits are repeated over time, which is claimed to help protect against modelling attacks. A QUALPUF can be considered as having a challenge being the adiabatic logic cell in question, and a binary response of which of the two halves of the coupled circuit gates settles on active.

4. Volatile memory PUFs

The volatile memory family of PUFs derives responses by examining the properties of the unit cell of volatile (state lost on power-down) memory. This includes examining the reaction of the typical static and dynamic random access memory (SRAM and DRAM, respectively) to a challenge, alongside other all-electronic and volatile memory systems. This family can be grouped with the explicit randomness non-volatile memory PUFs, as they both utilise the evaluation of the memory cell as the smallest unit.

a. Static random access memory (SRAM) PUF. The SRAM PUF[6] uniquely characterises a system through the variation of otherwise symmetric transistor branches within static random access memory (SRAM) elements, as a result of the variation in the manufacture process. A SRAM memory element, as featured in Fig. 9, consists of a collection of inverters and access transistors such that there are two stable states at a certain input power (a bistable flip-flop circuit). When power is applied, the cell can be written into either state. The system is kept stable in this state and can later be read as memory. When the circuit is unpowered both states are low, but when power is initially applied to the cell without additional bias the system stabilises at one of the two stable states. Here, the challenge is the address (position) of the SRAM element and the response is this "power up state" of the element.

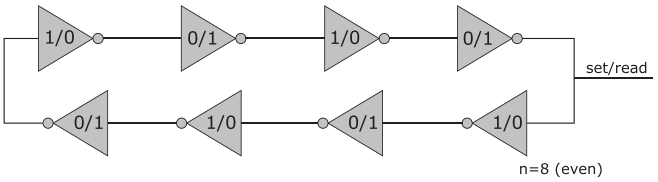

FIG. 11. A diagram displaying the operation of a bistable ring cell, for PUF usage.

Many notable variations of the SRAM PUF concept exist, fulfilling a variety of special purposes and solving a variety of emergent issues. These include flip-flop,[76] latch,[77] butterfly,[78] and buskeeper[79] PUFs, exhibited by Fig. 10. These PUFs rely on the same bistable principle that SRAM PUFs use, where for certain input voltage two potential arrangements of currents and voltages across the circuit are stable. They exist as more advanced storage elements that mitigate issues with the original SRAM setup or adapt the SRAM for different uses. For example, a Butterfly PUF is a variation on a SRAM PUF designed for programming with FPGAs. A cell of a Butterfly PUF is much alike that of a SRAM PUF; however, in most common FPGAs, SRAM cells are hard reset to zero (and thus all randomness is lost) directly after powerup. The cells of this PUF are constructed from cross-coupling two transparent data latch cells. These converge in a manner comparable to SRAM cells after power-up but without being explicitly SRAM elements. In the case of a SRAM cell, a power-up is required to engage in response generation, which similarly is not necessary with the butterfly PUF cell.

b. Bistable ring PUF. The bistable ring PUF[46] is of similar construction to the ring oscillator PUF, but holding a stable state for progressing time. It is again based on the variation in a series of logic gates. Like the ring oscillator PUF, it consists of a chain of NOT (or inverter) gates; however, in this implementation, there is an even number of gates, forming a bistable system instead of an oscillating system (Fig. 11). Since the output being fed into the input would be the same as the initial input, the system would settle at two possible states of the system, alternating a logical 0-1-0-1-0 between the gates or the opposite

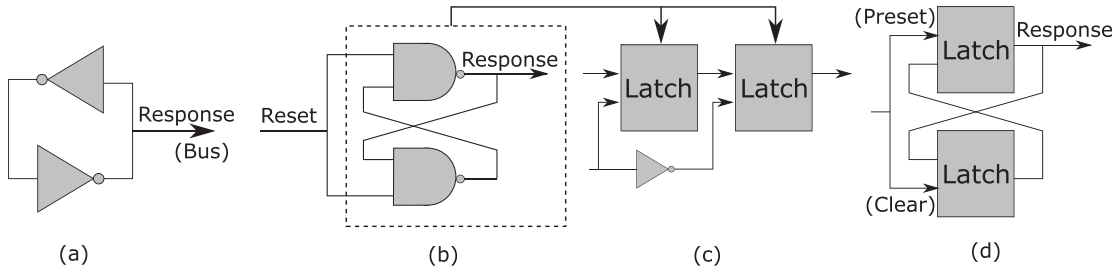

FIG. 10. 4 different memory elements acting as alternatives to the conventional SRAM cell for PUFs. These are the (a) Buskeeper, (b) Latch, (c) Flip-flop, and (d) Butterfly cells.

(1-0-1-0-1). In a similar manner to the SRAM PUF, the system can be destabilised on reset and after a certain time falls in one of the stable states, determined by the unique process variations in the fabrication of the ring. The ring can have many different configurations, each tending towards a preferred state independently. This preferred state acts as the response, and the configuration or bistable ring, in particular, is determined by the PUF's challenge.

c. MEmory Cell-based Chip Authentication (MECCA) PUF. A MEmory Cell-based Chip Authentication (MECCA) PUF[8] consists of an array of SRAM elements in the same manner as the basic SRAM PUF and is again based on the constituent transistor variation. In the case of a MECCA PUF, however, all the SRAM elements are first primed into the same ("0") state before being written into the other ("1") state probabilistically. Once all the SRAM elements are zeroed, a pulse is sent to each element. While this pulse typically flips the SRAM element to the second state with a very high success rate, here the pulse width is reduced such that each element has an equal chance to be written to the second state as to not. This results in a random allocation of 0 and 1 states stored in the SRAM array memory that is unique to that device. Whether the writing process succeeds is determined by the manufacturer variations in SRAM cell manufacture and is consistent across multiple evaluations. In the case of a MECCA PUF, the challenge would be the SRAM cell number or position, and the response is the resulting state of the cell after the pulse is applied.

d. SRAM failure PUF. For any cell of SRAM memory, there exists a property known as the static noise margin. This corresponds to the voltage amplitude of noise that can erase and rewrite the state of the cell, losing the information kept within. The amplitude of noise that induces this change depends on manufacturing variations between each cell. From this, a PUF can be formed.[32] A challenge in the form of a gradually increasing voltage bias is applied to an array of cells. This adds to the voltage from the voltage noise to effectively lower the static noise margin by an increasing amount. At a certain applied voltage, the static noise margin threshold for a certain cell is reached, and the data held by the SRAM are reset and lost (a "bit failure"). By applying this voltage to a large array of SRAM elements and detecting which elements are the first to fail, a stable

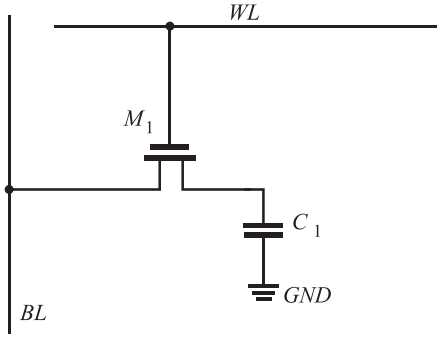

FIG. 12. The circuit diagram for a Dynamic Random Access Memory (DRAM) cell.

characterisation of the array can be built up to act like the signature, or PUF. This concept is very similar to the MECCA PUF, which instead of examining the voltage at which a write error occurs examines the final state of the SRAM element after the process. Here, the challenge to the PUF would be the voltage bias applied to the array of SRAM cells, and the response would be which cells of this array had an induced bit failure as a result.

e. Dynamic random access memory (DRAM) PUF. A DRAM PUF[47] characterises a device by examining variation in the components (the transistor and capacitor) of dynamic random access memory (DRAM) cells, as a result of manufacture variation. A basic DRAM cell consists of a single storage capacitor separated from the rest of the system by a single transistor, as in Fig. 12. To write a logical 1, the capacitor is charged (transistor opened with bias to capacitor) and to write a logical 0 the capacitor is left uncharged. To read the cell, the transistor gate is opened with no external voltage and the discharge or lack of discharge from the capacitor elucidates the state of the cell. When a DRAM cell is initialised (switched on), the cell does not necessarily initialise to the 0 (discharged) state as one might expect. This is because to reduce the electric field stress on the capacitor, the capacitors are pre-charged to half the drive voltage at start-up. This pre-charging makes it theoretically equally likely for a capacitor that is not otherwise deliberately fully charged or discharged to settle on the 1 or 0 state. In fact, the direction a cell switches is determined by the uncontrollable fabrication differences of each cell and is repeatable. The direction in which an adequate number of these cells switch in a DRAM array can therefore be used to uniquely characterise the full collection of DRAM itself, and any attached circuitry. In this case, the challenge would be the number or position of the DRAM cell, and the response would be the 0/1 binary state, or direction, that the cell in question tends to upon initialisation.

f. Rowhammer PUF. The Rowhammer effect is an issue in DRAM memory that causes the memory cells to interact with each other unconventionally through the leaking of charge. This can cause a computer to become vulnerable to an attacker, as they can rewrite memory cells that they would not typically have permission for, by rapidly accessing memory cells in a neighbouring row that they do have permission to write to. The Rowhammer PUF[48] evaluates by rapidly accessing the memory cells neighbouring a test cell to induce a bitflip in that cell. The presence or absence of this bitflip under defined attack parameters is determined by uncontrollable manufacture variations of each cell and can be examined to uniquely characterise an area of DRAM memory. In the case of a rowhammer PUF, the applied challenge is the number or position of the DRAM cell to be attacked with defined parameters, and the response is the presence or absence of a successful bitflip as a result.

B. Explicit/extrinsic all-electronic PUFs

1. Non-volatile memory PUFs

Non-volatile memories are non-conventional memory types that are married to a resettable cell property such that

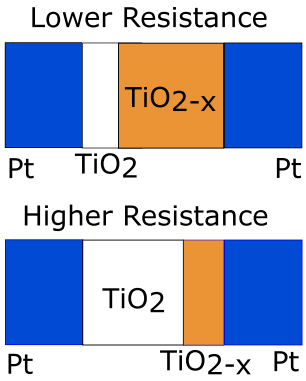

FIG. 13. Diagrams showing the principle of operation for a Memristor cell.[81]

they can physically store data even when not supplied with constant power. These PUFs typically operate by applying a modified writing signal to a unit cell of memory that causes the memory cell to have a 50/50 chance of being written into either the 0 or 1 state, building up a random pattern. This could be considered as the combined equivalent of a random number generator and non-volatile storage to retain a random key. Due to the non-volatility of this memory type, this pattern of writing remains until deliberately reset (a feature of an rPUF). Volatile memory PUFs utilise implicit random variations and can be described as a group of implicit PUFs. Non-volatile memory, on the other hand, must be described as a non-implicit PUF family–at least until fabrication of these types of memory cells becomes mainstream in circuit fabrication.

a. Memristor PUF. Memristors are electronic components that switch between a high and low resistance state once a threshold voltage is reached. Past a forward voltage threshold, the memristor enters low resistance state, and with negative current returns to the high resistance state. An example of a memristive component is a titanium dioxide memristor. One side of device has slightly fewer oxygen atoms than the other, with these vacancies acting as charge carriers–so the depleted layer has much less resistance than the non-depleted layer,[80] as in Fig. 13. When a forward electric field is applied, vacancies drift, causing more of the TiO_2 to be doped and the overall resistance to fall. This is undone with application of reverse electric field. In the most primitive case, a pulse is applied to an array of memristors near the voltage threshold, such that there is a probabilistic (50/50) chance of the resistance transition occurring. This results each memristor in an array having either a high or low resistance state, in an unpredictable but repeatable manner based on variations at both the manufacture and resetting stage. Circuitry is then designed around reading which resistance state each memristor is in, translating into a PUF response[58] based on a challenge of the number or position of the memristor in the array.

b. Phase change key generator (PCKGen) PUF. A phase change memory cell is featured in Fig. 14 and consists of a layer of germanium antimony tellurium (GST), which can be heated via an element and then cooled. Depending on the rate of cooling, the GST can turn into an amorphous form (with quick heating & cooling) or a polycrystalline form (with slower heating & cooling). The amorphous form has a higher resistance than the crystalline form. A controlled heating process can ensure a 50/50 chance of being in either form, determined by unpredictable and uncontrollable variations between each PCM cell at the time of manufacture and of resetting. This can be applied to every cell in an array of PCM, and the response of a single PCM element in an array prepared in this manner can be found and compared with a reference.[22] The phase of each cell of this memory can translate to give a 0 or 1-bit response, forming a unique and resettable output from the array in total. Similar to the memristor and STT-MRAM PUFs, the challenge here is the position or number of a cell of this non-volatile memory, and the response is the corresponding resistance state.

c. Spin-transfer-torque magnetic RAM (STT-MRAM) PUF. The resistance of spin-transfer-torque magnetic RAM (STT-MRAM) cells changes with the parallel or antiparallel alignment of one ferromagnetic layer compared to another in a magnetic tunnel junction. In a magnetic tunnel junction, there are two ferromagnetic layers separated by an oxide layer. One is pinned to a fixed alignment, while the other can switch into parallel or antiparallel alignment, seen in Fig. 15. An electron can more readily tunnel through the oxide layer, and so through the

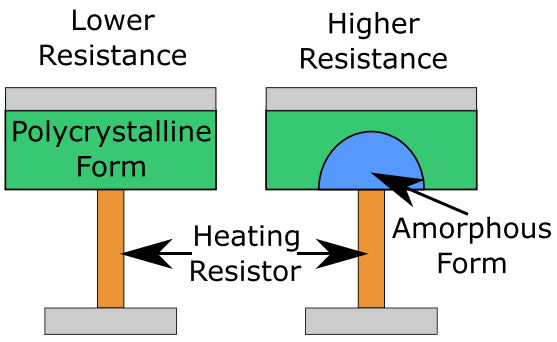

FIG. 14. Diagrams showing the principle of operation for a Phase Change Memory cell.

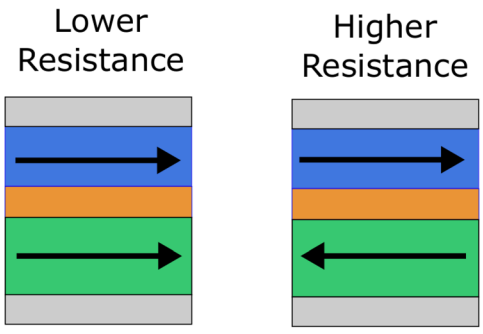

FIG. 15. Diagrams showing the principle of operation an STT MRAM cell.

device, when the spins are in alignment—resulting in a lower resistance. The alignment of the spins in the free layer changes when enough current passes through for enough time, and as such, it is possible to find the point where the chance of being in either state is 50/50. As with a memristor PUF, a setting signal with these parameters is evenly applied to an array of STT-MRAM cells,[23] resulting in a random configuration of high and low resistance states corresponding to a logical 1 or 0. This configuration is based on uncontrollable variation between the STT-MRAM cells during the manufacture and reset process. Here, as before, the challenge is the number or position of an STT-MRAM cell, and the response is the high or low resistance nature of the cell in question.

2. Direct characterisation PUFs

The final category for explicit/extrinsic electronic PUFs is the direct characterisation family of PUFs. These provide responses through the direct characterisation of electronic components that require additional fabrication steps to create and are otherwise as before.

a. Acoustical PUF. Acoustical delay lines are electronic components that convert an alternating electronic signal into a mechanical oscillation and back with the purpose of delaying the signal. The frequency spectrum of these delay lines when stimulated by an electronic signal is unique to the delay line and is influenced by the random, uncontrollable manufacturing variations of the line. This spectrum response can be analysed using principal component analysis and converted to a unique signature, to use acoustical delay lines as a PUF concept.[57] Here, the challenge applied to the PUF would be the position or number of one of more acoustical delay lines, and the response would be the frequency response, and resulting principal component reduction, of the line.

b. Coating PUF. A coating PUF[19] involves the measurement of the capacitance across a pair of comb shaped sensors in the top layer of an integrated circuit. These sensors are sensitive to capacitance and are featured in Fig. 16. A dielectric coating is sprayed on top of the sensors to explicitly introduce significant randomness, resulting from variation in the coating's properties

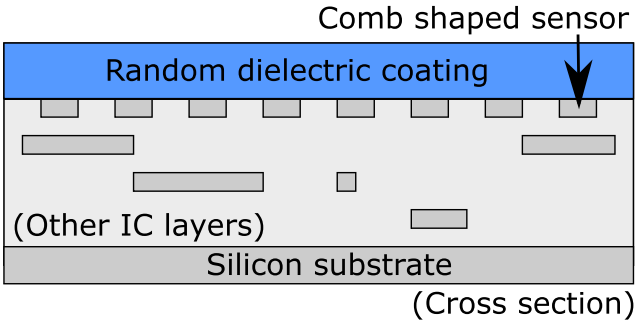

FIG. 16. Cross section of a coating PUF, showing the unique dielectric coating and comb-shaped sensor below.

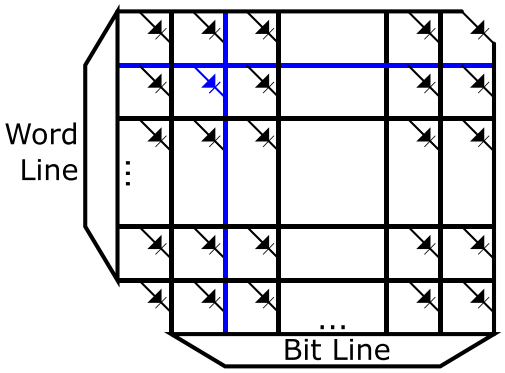

FIG. 17. An example of a SHIC nanocrossbar array, selecting for the diode in blue.

(such as thickness) across the surface of the PUF at the manufacture stage. This dielectric coating helps to physically protect the circuit from tampering, as accessing the circuit would remove or reposition an amount of the dielectric, resulting in a different capacitance output value and causing a different, tamper-evident, response upon challenge. In the case of a coating PUF, the response would be the capacitance measured just below the dielectric, and the challenge would be the one or more distinct positions where the capacitance is to be measured.

c. Super high information content (SHIC) PUF. A super high information content (SHIC) PUF[10] consists of a large collection of nanoscale aluminium/polysilicon diodes in a crossbar array (Fig. 17). Each diode can be translated into a characteristic output, and so a large collection of responses can be derived from one device. Manufacture variation ensures that despite each diode being produced as theoretically identical, they differ from one another in reality. Due to the very large number of diodes that can be accessed as part of a challenge, and an inescapable minimum detection time, it is argued that a malefactor with access to the PUF could not reasonably characterise all of the challenge response pairs of the device. This PUF is therefore described as a strong PUF. Here, the challenge would be the number or position of a diode in the array, and the response would be its electronic voltage-current (VI) characteristics.

d. Micro-Electrico-Mechanical system (MEMS) PUF. MEMS are devices that operate on the microscale with moving parts. These systems are already commonly used in various products for purposes such as motion and rotation detection in smartphones, smartwatches, and cars. The use of different MEMS sensors has been suggested for use in a physically unclonable function, such as MEMS gyroscopes and accelerometers. MEMS accelerometer PUFs apply an electrostatic impulse to an array of accelerometers. How each of these sensors reacts to this impulse varies slightly, and these differences (arising from manufacturing variation) are used to uniquely characterise a device.[55] Here, the challenge is the position or number of the specific accelerometer in the array, and the response is the

reaction of that accelerometer to an electrostatic impulse. MEMS gyroscopes consist of several spring–mass systems that are used to detect physical orientation. The oscillation frequency variation of a number of these devices, arising from physical variations from the manufacture process, can be used as a unique fingerprint for the collection of these devices and the connecting circuit.[4] Here, the challenge is the position or number of a MEMS gyroscope in an array, with a response derived from the difference between the orientation measurement of that gyroscope in comparison to others.

e. Carbon nanotube (CN) PUF. In a CN PUF, an array of Carbon Nanotube Field Effect Transistors (CNFETs) are produced. In the most primitive form, the PUF consists of a collection of parallel CNFETS, selecting a pair and comparing the current between them, returning a 0 or 1 depending on which transistor allows more current to flow.[54] This is a similar principle to the more conventional TV PUF, but instead of using CMOS transistors, the device utilises nanoscale transistors of carbon nanotubes. The CN PUF has a challenge of CNFET position or number in an array, and a response of the current flowing through the component for a defined voltage. This is based on random variations between each CNFET in the process of its fabrication.

f. BoardPUF. A BoardPUF[5] is a technique used to uniquely characterise printed circuit boards. A number of capacitors are embedded into the internal layer of a PCB, and the variations between them (based on manufacture variation) are utilised for key generation and authentication as a PUF. Here, the challenge would the number or position of a particular capacitor, and the response would be its measured capacitance value.

g. Quantum electronic PUF. The Quantum Electronic PUF (Q-EPUF)[56] utilises variations in resonant tunnelling diodes (RTDs) for unique device authentication. RTDs consist of two barriers around a quantum well, such that only electrons of an exact energy can tunnel through from one side to the other. The energy level of the confined quantum well compared to the electron energy level in the emitter is determined by the voltage across the device, and the number of electrons passing through the system corresponds to the current through the diode. From zero voltage, as the applied voltage increases, more electrons have the specific energy required to tunnel past the barriers through the confined energy level in the well, and the current increases. This continues up to a certain point of peak current, when the current through the device starts to decrease. This is because the majority of electrons then have an energy *higher* than that of the quantum well, and further increasing the voltage reduces the number of electrons that have energy *low* enough to pass through the well. This progression is visualised in Fig. 18. Overall, this results in an N shaped IV characteristic and a region of negative differential resistance. The peak current depends on the confined energy level within the quantum well, and this energy level depends heavily on the structure of the quantum well and its nanoscale variation. It can therefore be said that the macroscopic electronic properties of an RTD are highly sensitive to nanoscale variation within the device. Recreating a single resonant tunnelling diode with the same electronic characteristic would require a complete knowledge of the atomic structure of the quantum well and a way to fabricate a device atom-by-atom. The RTDs are small-size, low-resource, extremely stable and can be arrayed to further increase PUF complexity. This PUF is currently utilising III-V semiconductor components (and is thus non-implicit), but work is being undertaken to allow CMOS integration and facilitate an implicit version of this PUF in CMOS circuitry. The challenge in the weak form of the Q-EPUF is the position or number of the RTD in an array, while the response to this challenge is the voltage position of peak current in the tunnelling region of the device.

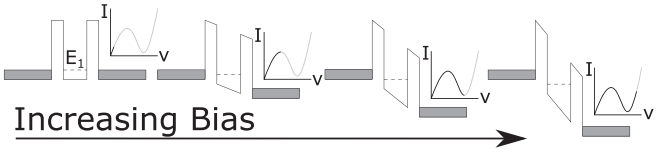

FIG. 18. The band structure of a resonant tunnelling diode, exhibiting how the unique current characteristic arises from increasing voltage as a consequence of the confined quantum well.

h. Self-assembly PUF. A self-assembly PUF utilises the physical phenomena of molecular self-assembly. This is where molecules tend towards arrangement without outside (human) guidance. An example of a self-assembly PUF includes a carbon nanotube self-assembly PUF.[53] Carbon nanotubes are self-assembled into regular trenches of hafnium oxide, creating an electrical contact where they randomly form, and no electrical contact where they do not. This results in arrays where each bit is either forming a connection (and considered a 1) or disconnected (and considered a 0), to create a unique bit signature to uniquely authenticate itself or an attached circuit. Another concept for a PUF using self-assembly is the LEDPUF (Locally Enhanced Defectivity Physical Unclonable Function).[82] Here, the source of randomness derives from the Directed Self Assembly (DSA) of block copolymers through guiding templates. This process either closes or opens a path through the guide randomly and permanently, and whether this path is open or closed translates to a 1 or 0 in a bit signature. This concept is very similar to a VIA PUF, characterised using variation in the directed self-assembly process rather than via hole width variation. The challenge for these PUFs is the number or position of a certain trench, for the case of the CN self-assembly PUF or guidance template, for the LEDPUF. The response in both cases is the binary state of connectivity—whether there is or is not a conductive path across the trench or template, respectively.

i. Nano-Electrico-Mechanical system (NEMS) PUF. Similar to MEMS, NEMS are devices that operate on the nanoscale with moving parts. Unlike the two MEMS PUFs featured in this paper, the suggested NEMS PUF[52] utilises the stiction effect. Typically a problem in NEMS fabrication, stiction is where the van der Waals forces cause usually unwanted adhesions in small-

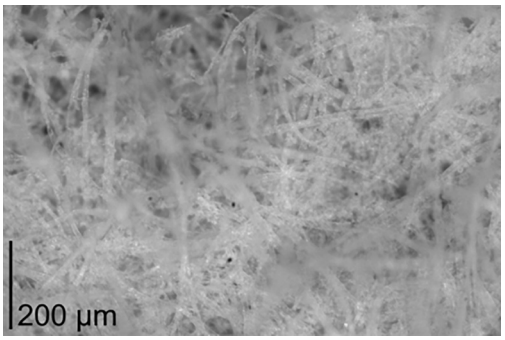

FIG. 19. Image of the pulp fibres of a piece of paper, acting as the fingerprint for a paper PUF.

scale dynamic systems. In the NEMS PUF cell, a nanowire is placed ideally equidistant between two contact gates. When this is done, stiction occurs and randomly adheres the nanowire to one of the two gates, with equal probability of adhering to either. By corresponding a connection to one of these gates as a "0" state and the other as a "1" state, and arraying a number of these cells, a random string of characterising bits can be encoded. Like other PUFs utilising binary connectivity (the VIA and Self-Assembly PUF), this type of PUF advertises high levels of robustness, as the system tends to one discrete state or another in a highly irreversible manner. In this type of PUF, the challenge is position or number of a NEMS gate cell, and the response is which of the two gates the central nanowire adheres to.

C. Implicit hybrid PUFs

1. Optical PUFs

This family of PUFs uses emitted light to evaluate the implicit randomness in an object. The light that is reflected is supplied by the evaluation system, either as a laser in a compact disk (CD) PUF or as directed light in a paper PUF.

a. Paper PUF. The paper PUF[60] was designed for the unique identification of physical fibres such as currency or legal paperwork. It operates by scanning over a section of the fibre structure (Fig. 19) of the piece of paper to establish a unique fingerprint. This fingerprint is based on the variation of the fibres between sections of paper resulting from manufacturer variation. Here, the challenge would be position on the paper, and the response would be the exact arrangement of the fibres within.

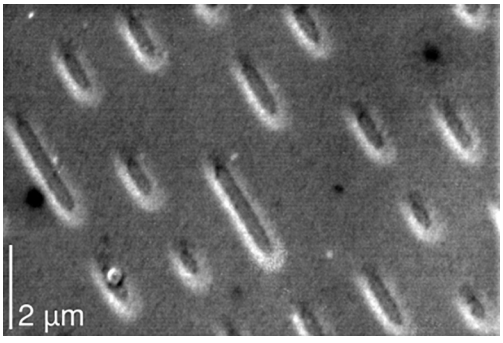

FIG. 20. Close up (SEM image) of the pits and lands in a CD,[83] as would be probed in a CD PUF.

b. Compact disk (CD) PUF. The CD PUF[59] was designed for the unique identification of the compact disk medium. It operates by measuring the length of the lands (reflective state of an area of CD) and pits (non-reflective state) of the CD, and examining how these actual lengths deviate from expected lengths due to variations in the manufacturing of the CD. These length variations are then compared with an entry in a database to authenticate the CD. These CD optical characteristics are visible in Fig. 20. Here, the challenge would be the particular pit or land, and the response would be its exact length.

2. Magnetic PUFs

This family of PUFs examines the magnetic field around an object to probe the manufacture-inherent randomness within.

a. Magnetic PUF. The Magnetic PUF[70] was designed to make unique magnetic swipe cards, such as credit and identity cards. During the manufacturing process, a blended ferromagnetic material is applied to a receptor layer in the card to form the magnetic media. The ferromagnetic particles are of random size, shape, and land randomly on the receptor layer due to manufacturing variation. This randomness in ferromagnetic particle arrangement can be exploited to distinguish cards from each other and verify the authenticity of a magnetic strip card as compared to a database. Here, the challenge would be the position along the magnetic strip, and the response would be exact magnetic field intensity.

D. Explicit hybrid PUFs

1. Optical PUFs

This family of PUFs examines the properties of emitted light to evaluate the explicitly introduced randomness attached to an object.

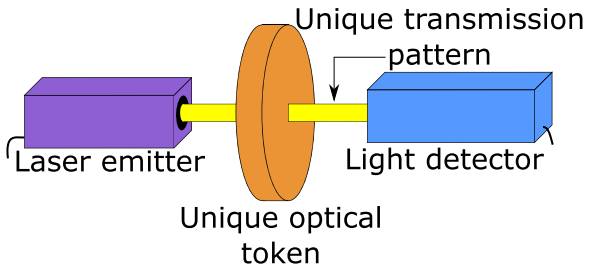

FIG. 21. Diagram displaying the operating principle of the original optical token PUF.

a. Optical PUF. The original optical PUF,[63] of eponymous nomenclature, relies on the interaction of visible light with a randomised microstructure. The propagation of light through this medium is inherently complex, and thus unpredictable. In the original form, a laser is shone through an "optical token," a plate of microscopic refractive particles mixed into an epoxy plate as shown in Fig. 21. These refractive particles are in random positions, sizes, and orientations due to variations in the manufacture process. The light on the other side of this plate is detected and analysed, comparing the produced pattern with the expected pattern algorithmically. In this case, any variation of laser angle of incidence corresponds to a different pattern, and so the laser positioning can be considered the challenge, and the resulting pattern features the response. A notable variation to this is the integrated optical PUF, which integrates the light emitter, scattering medium, and light detectors into one enclosed package. The challenge for this optical PUF would be the angle of incidence of the laser into the token, and the response would be the detected intensity of light measured on the other side. Both of these systems have been suggested as implementations of the PPUF, or SIMPL, system.[25]

b. Phosphor PUF. These PUFs[64] consist of phosphorescent particles of random shape and size that are blended randomly, due to fabrication process variation, into the material for the cover of a product. This unique arrangement of particles is revealed and measured under UV light. This signature is then compared with a database to verify the product. Here, the challenge would be the position across the surface of the particle's substrate, and the response would be the optical intensity of reflected light.

c. Nanowire distribution PUF. This PUF employs the random distribution and characterisation of silver nanowires (AgNWs) to uniquely characterise an object.[61] A collection of silver nanowires are deposited on a flexible polyethylene terephthalate (PET) film—a process that is unpredictable and random (and so impossible to fraudulently recreate). This arrangement of nanowires can be observed using a low resolution optical microscope, to verify that the nanowire distribution in the field corresponds to the expected distribution at manufacture. The complexity of the distribution can be increased by applying dyes to the nanowires. This PUF concept is very similar to the phosphor PUF, except on the nanoscale, insofar as it involves optically imaging hard-to-recreate collections of particles or fibres to verify authenticity. In the same way, this PUF has a challenge of imaging position and a response of reflected light intensity.

d. Optical fibre PUF. A fibre optic PUF[62] has been also been conceptualised. When light passes through a fibre optical cable, it experiences Rayleigh backscattering. This effect operates on and depends on manufacture variations at the molecular level—making the exact backscattering signature impossible to replicate in another piece of fibre. A technique known as optical frequency domain reflectometry (OFDR) can be employed to determine the intensity of light that is backscattered within the wire at varying positions. This is done by sweeping the frequency of the incident light and measuring the phase difference of the returning light compared to a reference arm. This unique characterisation of the refractive index along a piece of optical fibre can then be employed as a physically unclonable function. The challenge input here would be the position along the axis of the cable and the response here is the intensity of the backscattered light. It is worth noting here that this PUF has been categorised as of explicit rather than implicit randomness. This is because in the concept paper featured here the fibre optic cable is envisioned to be attached to internet of things (IOT) devices for authentication purposes only, adding additional manufacturing steps to the devices. If this technique was used to determine the authenticity of an object or device that already features the cable, or for authenticating the fibre itself, the PUF could be described as implicit, as no additional steps would be required to introduce the randomness. A similar concept[84] examines the speckle pattern that arises from a laser incident on a multimode optic fibre. The pattern that arises is a result of mode-mixing and scattering within the fibre, and these effects are determined by internal manufacture variations. Here, the challenge would be the position of light leaving the fibre and therefore position of light incident on a detecting camera, and the response would be the light intensity at that position.

e. Nanoparticle distribution PUF. A plasmonic nanoparticle distribution PUF,[29] or plasmonic PUF, characterises a system through the variation of nanoparticle deposition distribution in a manufacturing process using plasmonic effects. This concept involves the far-field scattering of light off randomly distributed plasmonic nanoparticles of gold, causing a unique and unclonable visible signature at a small size. Pattern recognition is used to verify the similarity or dissimilarity between the measured PUF and a pre-measured signature in a database. This concept is similar to a phosphor PUF, but using smaller (and therefore harder to forge) scales and particles. In the same way as the phosphor and nanowire distribution PUFs, the challenge here is the position across the deposition substrate, and the response is the reflected light intensity.

The nanoparticle distribution PUF[20] conceptualised here examines the positioning of nanoparticles suspended within the volume of a polymer. This polymer is than considered for use as a coating for the purposes of tamper-detection, as an attempt to bypass the polymer would adjust the nanoparticle distribution and therefore the PUF's reading. The positioning of nanoparticles within the polymer is detected by wavefront-shaping controlled reflection, which focuses light scattered by the nanoparticles into a target area where it is then imaged. This is different as compared to the plasmonic PUF as the plasmonic PUF examines plasmonic resonances of light induced by the gold nanoparticles, while the nanoparticle distribution PUF here only examines light reflected off the nanoparticles with no plasmonic effect involved. Beyond this change in mechanism, the source of randomness arising from the random distribution of the nanoparticles at manufacture remains the same, as does the nature of the challenge and response.

f. Liquid crystal PUF. A liquid crystal PUF[67] applies 100–300 μm diameter "shells" of cholesteric liquid crystals

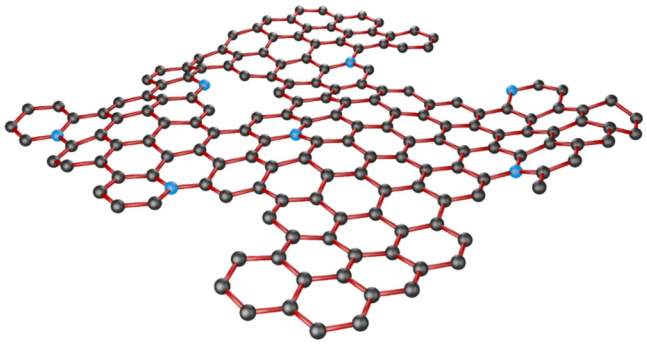

FIG. 22. An example sheet of a naturally imperfect monolayer material.

(CLCs) to the surface of the physical object to be authenticated. Through Bragg reflection, the shell reflects light selectively in relation to the structure of each liquid crystal. Structural variations inherent in the manufacture process cause changes in the exact colour of each shell. These shells are arrayed to produce a pattern of shells each with varying colour. The order and colour of this collection can then be used to uniquely authenticate the attached object optically. Here, the challenge to the PUF is the number or position of the liquid crystal in the array, and the response is the frequency of reflected light.

g. Quantum optical PUF. The Quantum Optical PUF (Q-OPUF)[66] utilises nanometer-scale defects in sheets of 2D materials, such as transition metal dichalcogenides (an imperfect monolayer sheet is depicted in Fig. 22). Defect-free fabrication of monolayers is not possible, and the imperfections that arise locally alter the bandgap structure of a semiconductor material. This bandgap alteration results in a variation in the photoluminescence spectrum of the material at that point. This results in the optically excited monolayer emitting light at different intensities for different frequencies at different locations, in a manner determined by manufacture variation. A band-pass filter can be used to select a single specific emission frequency of a range to examine, adding an additional dimension to the data as compared to most other optical PUFs. The frequency dimension and the nanometre scale of variations help to resist any attempts at physical cloning, as creating a light emitter at such a small scale with the same emission properties over frequency as well as position and intensity would be impossible. The response for this PUF is therefore both the intensity and frequency of the emitted light, and the challenge for this type of PUF is the position across the monolayer.

h. Monolayer deposition PUF. The monolayer deposition PUF[65] examines the presence or absence of monolayer material in various positions across a growth substrate. In this suggested concept, molybdenum disulphide (MoS_2) is grown through chemical vapour deposition across a silicon dioxide substrate which is divided spatially into an array. Due to the emission properties of the material, the positions where a single layer exists in a cell are easily detectable compared to where multiple stacked layers have been grown or no material exists. The position and thickness of the MoS_2 build-up are determined by unpredictable variations in the conditions at the time of growth, and so each deposition can be said to produce a unique and unpredictable pattern. In the case of this PUF, the challenge would be the spatial position across the surface of the PUF, and the response would be dependent on the presence or absence of only a single layer of MoS_2. This is distinct to the Quantum Optical PUF concept as, while both concepts involve monolayer deposition, this Q-OPUF examines the variation in bandgap due through optical excitation, while this concept examines only the variation in physical position on these layers.

i. Lanthanide luminescence PUF. The lanthanide luminescence PUF[30] examines the positions of zeolites doped with lanthanide (III) ions across a substrate by photoluminescence measurement. At the production stage, these doped zeolites are dispersed randomly only on the surface of the substrate in a manner that is unique and dependent on uncontrollable variations of manufacture conditions. To evaluate, a laser scans the surface of this substrate and induces photoluminescence on any doped zeolite it is incident upon. The resultant emission is then registered by a detector, to build up the unique pattern of zeolite position. Here, the challenge is the position across the substrate and the response is the emitted light intensity from the ion doped zeolite against a threshold at that position. The implementation featured in the concept paper includes multiple lasers and detectors that split the detected image into RGB and CYMK components, therefore expanding the parameter space of the PUF.

2. RF PUFs

This family of PUFs examines the properties of radio-frequency electromagnetic radiation interacting with the object to evaluate its explicitly introduced randomness. It is worth noting here that many systems that authenticate RFID tags utilise an all-electronic PUF concept that simply communicates with the receiver through the medium of RFID and do not evaluate the PUF using radiofrequency radiation like those below.

a. RF-DNA PUF. The RF-DNA PUF[69] acts in a very comparable way to an optical PUF, operating using radio frequency scattering rather than optical refracting. The PUF relies on a small token consisting of thin, randomly arranged copper wires in a flexible silicon sealant. These wires influence the near-field scattering of electromagnetic waves at the 5–6 GHz band, which is then detected by a scanner consisting of a matrix of RF antennas. Here, the challenge is the exact radio wave frequency, and the response is the respective level of attenuation caused by the wire arrangement.

b. LC PUF. The LC (Inductor [symbolized by L] - Capacitor) PUF[68] is constructed from a glass plate with a metal plate on each side, forming a capacitor, connected in series to a metal coil, forming an inductor. This passive LC circuit is placed into an RF

field where it absorbs power in a manner that is frequency and amplitude dependent on the inductance and capacitance of the arrangement. These inductance and capacitance characteristics are unique to each PUF due to random and uncontrolled variation in the fabrication process and so can be used to uniquely identify the circuit. This differs from the RF-DNA PUF in that here there exists a construction of plate and coil to specifically produce a passive LC circuit, rather than existing solely as a random collection of copper wire. Here, the challenge would be an exact RF field frequency, and the response would be the power absorbed into LC circuit at that frequency.

V. ANALYSIS

From looking at the suggested PUFs in Sec. IV, it can be noted that the PUF concept can benefit from being considered as made up of 5 sections. These sections are the physical source of entropy, the underlying physical mechanism or process, the entropy extraction device or technique, the examined response properties, and the controlled challenge properties.

The physical source of entropy would mean specifically what physical entity is being randomly distributed to produce the unique characteristics. This is typically the arrangement of varying atomic types, with a resulting variation of some higher-order effect, such as the rearranging of groups of different atoms and their bonding, resulting in variations in the refractive index and scattering centres along an optical fibre PUF.

The underlying physical mechanism or process would be the specific physical process that is occurring that is dependent on the physical source of entropy, for the case of an optical fibre PUF this would be the process of Rayleigh scattering of light. The evolution of the scattering process depends on the exact characteristics of the random refractive index distribution in the cable based on atomic arrangement as the physical source of entropy.

The entropy extraction technique would be the implementational way in which the PUF designer envisions extracting the relevant properties. For instance, in the case of the optical fibre PUF, this would involve a technique called optical frequency domain reflectometry (OFDR) and would require a reference branch alongside a detector and frequency-variable incident laser. The specific technique can often vary within the same PUF concept and so was not always included in Sec. IV.

The final way of looking at PUFs would be in terms of the properties of the PUF and surroundings that are controlled and varied as a challenge and those which are examined as a resulting response. This would mean, treating the PUF just as a function and a black box, what properties of the PUF are the variable parameters and would be the function's input, and what properties of the PUF are to be measured as function outputs on the other end. As has been seen, most PUFs have the minimum number (dimensionality) of input parameters and these properties. They generally involve a one-dimensional number or two-dimensional (x and y axes) array position of cellular elements as an input, and one particular property (such as the element's electronic resistance) as a dependent output. This is not necessarily the case, however, as can be shown by the Q OPUF, where two independent input properties exist—the position across the deposited monolayer and the frequency being examined, determined by a band pass filter. These correspond to a single dependent property as an output—an optical intensity level specific to a certain position across the monolayer at a certain frequency of output. Increasing the number of properties involved in the PUF evaluation process can serve to increase the challenge-response space of the PUF and increase the difficulty of PUF physical cloning (having more "angles" of input or output variation for a replication to respond correctly to). It can be observed that increasing the number of challenge properties would have a stronger impact on the challenge-response space than increasing the number of response properties (for the same resolution within that property). This is because the challenge properties compound multiplicatively with each other when producing the output, as each permutation of the properties leads to its own response and scales the CRP space polynomially. Response properties compound linearly, as they vary independently, and so lead to a linearly increasing CRP-space. In other words, for the same resolution, doubling the number of controlled properties would square the number of CRPs, while doubling the number of observed properties would simply double the number of CRPs. Either way, assuming the results remain reasonably independent, increasing the number of properties examined or modulated would provide the ability to increase the CRP support of the PUF, at the cost of ease of evaluation. This is a very similar but slightly more nuanced view as the parametric organisation scheme, as it examines and respects the difference between parameters that are challenges and those that are responses. Additionally, the parametric scheme only looks at the domain or units of a property rather than the specific property itself—for instance, the time delay of a signal and the pulse length of a signal would both be described under the "time" parameter.

Examining the constitution of PUFs in this modular way can bring to attention certain potential novel PUF elements and make clear the idea of parameter dimensionality—an idea which could improve pre-existing PUF concepts. An example of a previously unconsidered PUFs through this framework would be utilising the effect of variation in atomic bonds on the procession of the constituent nuclear magnetic moments, examined through the technique of nuclear magnetic resonance (NMR) spectroscopy.[85] Here, the challenge property would be, for example, the physical position across a sample and response property could be the variation of peak intensities of one or more signatures. While the apparatus required to take such a measurement would be significant, NMR and other spectroscopic or microscopic methods (such as Raman spectroscopy[86] or atomic force microscopy[87]) could be used to create a "fingerprint" implicit hybrid PUF solution for more items and at a higher resolution than the previously suggested paper and compact disks.

Another example would utilise the concept of random lasing.[88] Here, the variation in the gain and scattering medium in the active region would constitute the source of uniqueness, and the phenomenon of the lasing itself would provide the underlying physical process. A photodiode array held at a consistent position between devices could provide a challenge

property of photodiode position in the array and a response property of the intensity registered at that diode for a defined input power. This PUF would detect variations of light emission directly from a source rather than after passing through an optical token, which could lower the amount of equipment required for evaluation and help minimise any issues caused by ensuring a consistent incident light source. Some work has already been done regarding this concept, utilising Zinc Oxide random lasers with a focus instead on quantum random number generation.[89]

A further example would use superconducting quantum interference devices (SQUIDs)[90,91] as PUF elements. Here, the physical source of variation would be the atomic variation of the elements inside the SQUID (the superconducting paths and Josephson junctions) that would affect the physical process of operation and in turn the specific voltage drop across the two superconducting paths when presented with a controlled critical current. Here, the device for measuring the specific evolution of physical system can be considered as either the SQUID containing the process itself, or the current-voltage apparatus managing and detecting the flow of electrons through the SQUID. Here, the challenge property would be the position of a particular SQUID element in an array at incident magnetic flux, and the response would be the voltage drop across the element, to be compared with neighbouring elements in the array. The SQUID PUF can be argued as being generally more sensitive to variation than typical consumer-electronic sensors, has the possibility for contactless challenging over a magnetic field, and could be a viable consideration for PUFs in specific applications—especially if they should take over from other magnetometers in future conventional electronic applications. This would be treating the SQUID sensor element as a PUF in a similar way to previously suggested MEMS and NEMS sensor PUFs. By examining the similarities between suggested concepts in this way, an amount of developmental synergy could emerge and remain generic to, for instance, PUFs based on the variation sensor array reaction to a consistent stimulus.

A final example, again in the domain of magnetics and very comparable to SQUIDs, would be the idea of using the Aharonov–Bohm effect[92,93] for a PUF. The Aharonov–Bohm effect is a quantum mechanical effect whereby quantum interference can cause the flow of a stream of electrons to vary based on a magnetic potential, even if no actual magnetic field is directly present. This could be actualised by controlling the potential and measuring the flow of electrons across a substrate hosting a collection of nanorings next to (but outside) a solenoid or similar. Here, the physical process involved would be the Aharonov–Bohm effect and the physical source of variation would be the atomic arrangement, position, and makeup of the nanorings. The device or technique of stimulating and observing this effect would be a current meter and voltage sources to drive current through the substrate and through the solenoid to produce the magnetic potential. The challenge property would be the magnetic potential flux across the substrate with a response property of measured conductivity. As well as being very sensitive to variation in the nanorings, the use of this concept has a unique ramification. A magnetic potential can only be directly measured through this effect, so it is hard for an attacker to have a precise knowledge as to the specifics of the "challenge" magnetic potential until after being acted upon by variations in the Ahamov-Bohm sensor.

In addition to describing completely novel concepts, looking at PUFs in this compartmentalised way allows for the consideration of expanding the number of challenge or response properties of pre-existing PUF concepts. If this is done, care would need to be taken to ensure that variations in challenge properties are not predictable and that variations in response properties are independent from each other. This can be demonstrated with the plasmonic PUF, which typically examines the property of intensity as a response to a challenge of spatial position across the host substrate. This is later processed by applying an intensity threshold and translating above-threshold particle position to a unique signature. While the plasmonic PUF featured in this paper considered examining the colour of the nanoparticles as the response before opting for intensity, including this single measured colour value in addition could add further entropy when combing the measurements. This would result in the PUF outputting both an intensity and colour value as function of spatial position and expand the potential CRP set. Alternatively, frequency can be introduced as a challenge property in the areas containing nanoparticles, drawing up a unique relationship of intensity as a function of frequency as well as a function of position. This would result in a physically unclonable function that outputs an intensity value as a function of both position and frequency and acts to increase the potential support for a challenge-response set at an even faster rate. Something similar to this was suggested in the original plasmonic and lanthanide luminescence PUF paper by examining the RGB and/or CYMK channels of an image to gain three, four, or seven intensity-position profiles rather than one. This is the same idea as more fully involving the frequency domain as a challenge in the evaluation, only at a limited range of frequency values. As a potential extension, if the frequency is treated as a challenge property it may be possible to include a response that involves intensity peak bandwidths; however, this may not be possible to keep independent from the frequency-intensity profile already used for a response and so risks being "filled in" by machine learning or analytics of other CRPs. Another example of the potential to increase response property dimensionality would be looking at the variation of reflected light intensity as well as frequency for the Caloric Liquid Crystal PUF. A final example would be examining the variation in the temporal coherence as well as spatial coherence for a laser that has passed through the optical token of an optical PUF.

VI. CONCLUSION

From this catalogue, it can be clearly seen that a large number of concepts for PUFs have been put forward. From the chronological view in Table II, it can also be seen that the rate at which new PUFs are being suggested is significantly increasing, with half the concepts featured here being suggested in the last 5 years. An increasing number of these concepts utilise explicit sources of randomness, applying novel materials and technologies to the field of PUFs. It is therefore more important than ever to categorise and shape the growth of PUF development.

As well as providing a system by which to make sense of existing PUF concepts and a system by which to categorise new developments, the schemes presented here make apparent a number of areas that would benefit from attention by the community—including those below.

It can be seen that PUF concepts for electronic applications are numerous, and many can be easily integrated and digitised. However, it can also be seen very clearly from the organisational schemes presented, and the parametric scheme especially, that the industrial focus tends to be on the first PUF to be developed in any category—not necessarily the deliberate optimal. It would therefore seem wise (IP issues aside) to investigate the merits of different PUFs and more contemporary concepts for any given application situation before employing any given PUF. Choosing the optimal PUF would need to occur on multiple separate levels. First, the correct "family" of PUF would need to be chosen for a specific situation. For example, binary state parameter PUFs (in particular, binary connectivity PUFs) are typically more robust and are better for extreme-condition and longevity-valued applications compared to Time Domain or Component Constant PUFs. As a downside, these PUFs are generally more easily replicated and less conducive to strong PUF design than the other two groups. At the concept level, a systematic, standardised, and complete comparison is required to determine the optimal PUF concept and specific variation for any given purpose—should no single option be outstanding for all. On the same topic, it can be noted that certain valuable specifications for comparison are not commonly cited in papers introducing concepts or implementations. Most notably, the physical entropy of the suggested system,[94,95] or entropy per unit cost or area, is typically unexamined and unstandardized in evaluation. This is primarily because while there are papers regarding the entropy analysis of PUFs,[96,97] the widely varying physical nature of PUFs makes it difficult to define a coherent standard before the digitisation stage. It may be possible to define a generic standard for physically derived entropy in a single branch of the organisation schemes described in this paper, but this may not be applicable to other branches—for instance, the entropy arising from latency in an FPGA circuit compared to the absorption spectrum of a radiofrequency signal. Since the PUF can be considered as the generation and then permanent storage of a randomly generated key, pre-existing work on the standardisation of dedicated random number generators[98] may be a useful source to help define these areas.

From the organic organisation scheme, it can be also be observed that the industry focus for all-electronic PUFs is almost entirely on PUFs with intrinsic evaluation (and implicit sourced randomness). This can often be considered reasonable, based on the security benefits and ease of fabrication this type of PUF brings. However, some broader attention should be aimed towards the possibility of explicit PUF concepts that would otherwise show significant merits or suitability for certain applications still being worth the additional steps, or the possibility of being converted to an implicit form. Explicit PUF properties of merit would include, for instance, the resettable PUF capability of non-volatile memory material concepts and the intimate atomic-scale dependencies of the Quantum Electronic PUF. This conversion to an implicit form could arise in two ways. The fabrication processes required to make the PUF could adapt to suit current techniques (e.g., CMOS-MEMS[99]), or the adapting and advancing of current techniques for a more general purpose may grow to include the PUF's requirements, such as from a proliferation of novel NVRAM (Non-Volatile Random Access Memory)[100] technology.

One of the most notable observations on hybrid mechanism PUFs is the apparent lack of suggested PUF concepts (less than a third of the total) and industry focus. This is not necessarily the case, for the reason that commercial physical object authentication ventures tend not to describe their technologies as weak PUFs, despite often being just that (attempts at a hard-to-forge authentication marker applied to the product). This results in the myriad of physical authentication techniques and commercialisation ventures not being readily apparent to the PUF community or this survey. It would therefore be of value working to apply the (typically electronic and computer science) academic work and nomenclature of this field to the pre-existing and generally separate world of physical authentication. This issue also arises when it comes to what could be considered biometric PUFs, where authentication occurs by forming a unique signature from variation sources such as the retina,[101] fingerprint,[102] or brainwaves[103] of the user themselves. These are generally not considered to be PUFs in the same way as the typical PUF featured here, despite being considerable as human-based implicit-randomness physically unclonable functions.

It is also apparent that the number of hybrid PUFs in the implicit randomness section is very small. This is because to have implicit randomness the uniqueness must come from the material itself, resulting in one implicit PUF concept per material system (generally by examining the material's nature so closely that each piece becomes close to unique). By nature, all hybrid PUFs evaluate extrinsically and require a conversion to a non-electronic medium to probe the uniqueness of the PUF. However, while implicit-randomness hybrid PUFs are easy to fabricate, they are generally let down by limitations in extracting out responses from the system. Contemporary hybrid PUF concepts tend to involve explicitly introduced randomness with smaller features, which require additional fabrication steps but are generally more readily unique and harder to clone (as an opposite to the preference for implicit PUFs in the all-electronic world). An example of this would be the application of randomly distributed nanoparticles or nanofibers to a substrate for optical evaluation in the case of optical PUFs. While dropping the feature size of the introduced randomness has merits, the equipment requirements and difficulty for evaluating the PUF tend to increase. For instance, most optical PUFs featured in this survey require at least a specialised lighting source, a specialised detector, or controlled conditions to operate. These equipment requirements can make each PUF concept cumbersome to implement for industrial-level operation and prohibitive for consumer-level operation. It would therefore be valuable to perform a systematic comparison of the evaluation requirements of each hybrid physical PUF to help to determine which PUFs are

feasible to use in which environments. Care should also be taken in developing new hybrid PUFs to ensure that the practical constraints of the evaluation are minimised.

ACKNOWLEDGMENTS

R.J.Y. acknowledges support from the Royal Society through a University Research Fellowship (UF160721). This material was supported by the Air Force Office of Scientific Research under Award No. FA9550-16-1-0276. This work was also supported by grants from The Engineering and Physical Sciences Research Council in the UK (EP/K50421X/1 and EP/L01548X/1). T.M. thanks J. Fong and R. B. Gavito for their input and support in the writing of this work.

REFERENCES

[1]J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. v. Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Proceedings of Symposium on VLSI Circuits, Digest of Technical Papers* (2004), pp. 176–179.

[2]G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th ACM/IEEE Design Automation Conference* (DAC) (2007), pp. 9–14.

[3]T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new arbiter PUF for enhancing unpredictability on FPGA," Sci. World J. **2015**, 864812.

[4]O. Willers, C. Huth, J. Guajardo, and H. Seidel, "MEMS gyroscopes as physical unclonable functions," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), pp. 591–602.

[5]L. Wei, C. Song, Y. Liu, J. Zhang, F. Yuan, and Q. Xu, "BoardPUF: Physical unclonable functions for printed circuit board authentication," in *Proceedings of IEEE/ACM International Conference on Computer-Aided Design* (ICCAD) (2015), pp. 152–158.

[6]J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems* (2007), pp. 63–80.

[7]F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "DRAM-based intrinsic physically unclonable functions for system-level security and authentication," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **25**(3), 1085–1097 (2017).

[8]A. R. Krishna, S. Narasimhan, X. Wang, and S. Bhunia, "MECCA: A robust low-overhead PUF using embedded memory array," Cryptographic Hardware Embedded Syst. (CHES) **6917**, 407–420 (2011).

[9]U. Rührmair, H. Busch, and S. Katzenbeisser, "Strong PUFs: Models, constructions, and security proofs," in *Proceedings of Towards Hardware-Intrinsic Security: Foundations Practice* (2010), pp. 79–96.

[10]U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, and M. Stutzmann, "Security applications of diodes with unique current-voltage characteristics," in *Proceedings of the 14th International Conference on Financial Cryptography and Data Security* (2010), pp. 328–335.

[11]U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM Conference on Computer and Communications Security* (2010), pp. 237–249.

[12]U. Rührmair *et al.*, "PUF modeling attacks on simulated and silicon data," IEEE Trans. Inf. Forensics Secur. **8**(11), 1876–1891 (2013).

[13]U. Rührmair, J. Sölter, and F. Sehnke, "On the foundations of physical unclonable functions," in *Proceedings of IACR Cryptology ePrint Archive* (2009).

[14]R. Maes, "Physically unclonable functions: Concept and constructions," in *Physically Unclonable Functions: Construction, Properties and Applications* (Springer, 2013), pp. 11–48.

[15]I. Verbauwhede and R. Maes, "Physically unclonable functions: Manufacturing variability as an unclonable device identifier," in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)* (2011), pp. 455–460.

[16]U. Rührmair and M. van Dijk, "On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols," J. Cryptographic Eng. **3**(1), 17–28 (2013).

[17]U. Rührmair, "Oblivious transfer based on physical unclonable functions," in *Proceedings of the 3rd International Conference on Trust and Trustworthy Computing* (TRUST) (2010), pp. 430–440.

[18]C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, "Physically uncloneable functions in the Universal Composition Framework," in *Proceedings of the 31st Annual Conference on Advances in Cryptology* (CRYPTO) (2011), pp. 51–70.

[19]P. Tuyls, G. J. Schrijen, B. Skoric, J. v. Geloven, N. Verhaegh, and R. Wolters, "Read-proof hardware from protective coatings," in *Proceedings of Cryptographic Hardware and Embedded Systems* (CHES) (2006).

[20]B. R. Anderson, R. Gunawidjaja, and H. Eilers, "Initial tamper tests of novel tamper-indicating optical physical unclonable functions," Appl. Opt. **56**(10), 2863–2872 (2017).

[21]K. Kursawe, A. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls, "Reconfigurable physical unclonable functions - Enabling technology for tamper-resistant storage," in *Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust* (HOST) (2009), pp. 22–29.

[22]L. Zhang, Z. H. Kong, and C. Chang, "PCKGen: A phase change memory based cryptographic key generator," in *Proceedings of IEEE International Symposium on Circuits and Systems* (2013), pp. 1444–1447.

[23]L. Zhang, X. Fong, C. Chang, Z. H. Kong, and K. Roy, "Highly reliable memory-based physical unclonable function using spin-transfer torque MRAM," in *Proceedings of IEEE International Symposium on Circuits and Systems* (ISCAS) (2014), pp. 2169–2172.

[24]N. Beckmann and M. Potkonjak, "Hardware-based public-key cryptography with public physically unclonable functions," in *Information Hiding* (Springer-Verlag, 2009), pp. 206–220.

[25]U. Rührmair, "SIMPL systems: On a public key variant of physical unclonable functions," in *Proceedings of IACR Cryptology ePrint Archive* (2009), Vol. 2009, p. 255.

[26]A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," J. Cryptography **14**(4), 255–293 (2001).

[27]M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Ed. (Cambridge University Press, Cambridge, 2010).

[28]K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *Proceedings of IEEE International Solid-State Circuits Conference, Digest of Technical Papers* (2000), pp. 372–373.

[29]A. F. Smith, P. Patton, and S. E. Skrabalak, "Plasmonic nanoparticles as a physically unclonable function for responsive anti-counterfeit nanofingerprints," Adv. Funct. Mater. **26**(9), 1315–1321 (2016).

[30]M. R. Carro-Temboury, R. Arppe, T. Vosch, and T. J. Sørensen, "An optical authentication system based on imaging of excitation-selected lanthanide luminescence," Sci. Adv. **4**(1), e1701384 (2018).

[31]J. H. Anderson, "A PUF design for secure FPGA-based embedded systems," in *Proceedings of 15th Asia and South Pacific Design Automation Conference* (ASP-DAC) (2010), pp. 1–6.

[32]H. Fujiwara, M. Yabuuchi, H. Nakano, H. Kawai, K. Nii, and K. Arimoto, "A chip-ID generating circuit for dependable LSI using random address errors on embedded SRAM and on-chip memory BIST," in *Proceedings of Symposium on VLSI Circuits - Digest of Technical Papers* (VLSIC) (2011), pp. 76 and 77.

[33]E. Peterson, "Developing tamper-resistant designs with zynq ultraScale+ devices (XAPP1323)," Xilinx, 2017.

[34]See www.intrinsic-id.com/sram-puf-technology-solutions for *Technology & Solutions - Intrinsic ID | IoT Security* (last accessed July 17, 2018).

[35]See verayo.com/tech.php for *Verayo - Simply Secure* (last accessed July 17, 2018).

[36]See www.quantumtrace.com/Technology for *QuantumTrace* (last accessed July 17, 2018).
[37]See www.connectsecurityworld.com/partners/ictk for ICTK - *Connect Security World* 2018 (last accessed July 17, 2018).
[38]D. Jeon, J. H. Baek, D. K. Kim, and B. Choi, "Towards zero bit-error-rate physical unclonable function: Mismatch-based vs. physical-based approaches in standard CMOS technology," in *Proceedings of Euromicro Conference on Digital System Design* (DSD) (2015), pp. 407–414.
[39]See www.quantumbase.com/solutions/q-id-optical for *Q-ID Optical - Quantum Base* (last accessed July 17, 2018).
[40]See www.quantumbase.com/solutions/q-id-electronic for *Q-ID Electronic - Quantum Base* (last accessed July 17, 2018).
[41]See www.web.archive.org/web/20110202060624/http://veratag.com for *Veratag Home* (last accessed July 17, 2018).
[42]See www.electroiq.com/2007/10/veratag-licenses-memflake-resonator-ip-to-cornell/ for *Veratag licenses MEMflake resonator IP to Cornell | Solid State Technology* (last accessed July 17, 2018).
[43]Y. Yao, M. Kim, J. Li, I. L. Markov, and F. Koushanfar, "ClockPUF: Physical unclonable functions based on clock networks," in *Proceedings of Design, Automation & Test in Europe Conference & Exhibition* (DATE) (2013), pp. 422–427.
[44]B. Gassend, D. Clarke, M. v. Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security* (2002), pp. 148–160.
[45]L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, "A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon," IEEE Trans. Emerging Top. Comput. **2**(1), 30–36 (2014).
[46]Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust* (HOST) (2011), pp. 134–141.
[47]F. Tehranipoor, N. Karimian, K. Xiao, and J. A. Chandy, "DRAM based Intrinsic physical unclonable functions for system level security," in *Proceedings of the 25th Edition on Great Lakes Symposium on VLSI* (2015), pp. 15–20.
[48]A. Schaller *et al.*, "Intrinsic Rowhammer PUFs: Leveraging the Rowhammer effect for improved security," in *Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust* (HOST) (2017), pp. 1–7.
[49]T. Addabbo, A. Fort, M. D. Marco, L. Pancioni, and V. Vignoli, "Physically unclonable functions derived from cellular neural networks," IEEE Trans. Circuits Syst. I **60**(12), 3205–3214 (2013).
[50]R. Helinski, D. Acharyya, and J. Plusquellic, "A physical unclonable function defined using power distribution system equivalent resistance variations," in *Proceedings of the 46th ACM/IEEE Design Automation Conference* (DAC) (2009), pp. 676–681.
[51]S. D. Kumar and H. Thapliyal, "QUALPUF: A novel quasi-adiabatic logic based physical unclonable function," in *Proceedings of the 11th Annual Cyber and Information Security Research Conference* (CISRC) (2016), pp. 1–4.
[52]K.-M. Hwang *et al.*, "Nano-electromechanical switch based on a physical unclonable function for highly robust and stable performance in harsh environments," ACS Nano **11**(12), 12547–12552 (2017).
[53]Z. Hu *et al.*, "Physically unclonable cryptographic primitives using self-assembled carbon nanotubes," Nat. Nanotechnol. **11**, 559 (2016).
[54]S. T. C. Konigsmark, L. K. Hwang, D. Chen, and M. D. F. Wong, "CNPUF: A carbon nanotube-based physically unclonable function for secure low-energy hardware design," in *Proceedings of 19th Asia and South Pacific Design Automation Conference* (ASP-DAC) (2014), pp. 73–78.
[55]A. Aysu, N. F. Ghalaty, Z. Franklin, M. P. Yali, and P. Schaumont, "Digital fingerprints for low-cost platforms using MEMS sensors," in *Proceedings of the Workshop on Embedded Systems Security* (2013), pp. 1–6.
[56]J. Roberts *et al.*, "Using quantum confinement to uniquely identify devices," Sci. Rep. **5**, 16456 (2015).
[57]S. Vrijaldenhoven, "Acoustical physical uncloneable functions," M.S. thesis (Eindhoven University of Technology, 2004).
[58]P. Koeberl, K. Ünal, and A. Sadeghi, "Memristor PUFs: A new generation of memory-based physically unclonable functions," in *Proceedings of Design, Automation & Test in Europe Conference & Exhibition* (DATE) (2013), pp. 428–431.
[59]G. Hammouri, A. Dana, and B. Sunar, "CDs have fingerprints too," in *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems* (CHES) (2009), pp. 348–362.
[60]D. o. E. a. P. S. National Research Council, Commission on Engineering and Technical Systems, National Materials Advisory Board, Committee on Next-Generation Currency Design, *Counterfeit Deterrent Features for the Next-Generation Currency Design* (The National Academies Press, Washington, DC, 1993), p. 144.
[61]J. Kim, J. Yun, J. Jung, H. Song, J.-B. Kim, and H. Ihee, "Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires," Nanotechnology **25**(15), 155303 (2014).
[62]Z. Chen, Y. Zeng, G. Hefferman, Y. Sun, and T. Wei, "FiberID: Molecular-level secret for identification of things," in *Proceedings of IEEE International Workshop on Information Forensics and Security* (WIFS) (2014), pp. 84–88.
[63]R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," Science **297**(5589), 2026–2030 (2002).
[64]C. N. Chong, D. Jiang, J. Zhang, and L. Guo, "Anti-counterfeiting with a random pattern," in *Proceedings of Second International Conference on Emerging Security Information, Systems and Technologies* (SECURWARE) (2008), pp. 146–153.
[65]A. Alharbi, D. Armstrong, S. Alharbi, and D. Shahrjerdi, "Physically unclonable cryptographic primitives by chemical vapor deposition of layered MoS2," ACS Nano **11**(12), 12772–12779 (2017).
[66]Y. Cao *et al.*, "Optical identification using imperfections in 2D materials," 2D Mater. **4**(4), 045021 (2017).
[67]G. Lenzini *et al.*, "Security in the shell: An optical physical unclonable function made of shells of cholesteric liquid crystals," in *Proceedings of IEEE Workshop on Information Forensics and Security* (WIFS) (2017), pp. 1–6.
[68]J. Guajardo *et al.*, "Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions," Inf. Syst. Front. **11**(1), 19–41 (2009).
[69]G. Dejean and D. Kirovski, "RF-DNA: Radio-frequency certificates of authenticity," in *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems* (CHES) (2007), pp. 346–363.
[70]R. S. Indeck and M. W. Muller, "Method and apparatus for fingerprinting magnetic media," United States of America, 1994.
[71]R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security* (Springer, Berlin, Heidelberg, 2010), pp. 3–37.
[72]J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A survey on silicon PUFs and recent advances in eing oscillator PUFs," J. Comput. Sci. Technol. **29**(4), 664–678 (2014).
[73]G. Csaba *et al.*, "On-chip electric waves: An analog circuit approach to physical uncloneable functions," in *Proceedings of IACR Cryptology ePrint Archive* (2009), Vol. 2009, p. 246.
[74]J. Miao, M. Li, S. Roy, and B. Yu, "LRR-DPUF: Learning resilient and reliable digital physical unclonable function," in *Proceedings of the 35th International Conference on Computer-Aided Design* (ICCAD) (2016), pp. 1–8.
[75]Inductiveload, *SRAM Cell (6 Transistors)* (Wikimedia Commons, 2009).
[76]R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices," in *Proceedings of 3rd Benelux Workshop Information and System Security* (2008), p. 17.
[77]Y. Su, J. Holleman, and B. Otis, "A 1.6pJ/bit 96% stable chip-ID generating circuit using process variations," in *Proceedings of IEEE International Solid-State Circuits Conference, Digest of Technical Papers* (2007), pp. 406–611.
[78]S. S. Kumar, J. Guajardo, R. Maes, G. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust* (HOST) (2008), pp. 67–70.

[79]P. Simons, E. v. d. Sluis, and V. v. d. Leest, "Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs," in *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust* (HOST) (2012), pp. 7–12.
[80]D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," Nature **453**, 80 (2008).
[81]M. Lenz, "Memristor.svg," 2010.
[82]W. Wang, Y. Yona, S. Diggavi, and P. Gupta, "LEDPUF: Stability-guaranteed physical unclonable functions through locally enhanced defectivity," in *Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust* (HOST) (2016), pp. 25–30.
[83]Akroti, "REM CD GEPRESST.jpg" (Wikimedia Commons, 2007).
[84]C. Mesaritakis *et al.*, "Physical unclonable function based on a multi-mode optical waveguide," Sci. Rep. **8**(1), 9653 (2018).
[85]F. Bovey, P. Mirau, and H. S. Gutowsky, *Nuclear Magnetic Resonance Spectroscopy*, 2nd ed. (Academic Press, 1988).
[86]N. Colthup, L. Daly, and S. Wiberley, *Introduction to Infrared and Raman Spectroscopy*, 3rd ed. (Academic Press, 1990).
[87]P. Eaton and P. West, *Atomic Force Microscopy* (OUP, Oxford, 2010).
[88]H. Cao, Y. G. Zhao, S. T. Ho, E. W. Seelig, Q. H. Wang, and R. P. H. Chang, "Random laser action in semiconductor powder," Phys. Rev. Lett. **82**(11), 2278–2281 (1999).
[89]S. H. Choi, Y. J. Yoo, J. W. Leem, J. H. Lee, Y. M. Song, and Y. L. Kim, "Revisitation of ZnO random lasers toward optical security," in *Proceedings of Conference on Lasers and Electro-Optics* (CLEO) (2018).
[90]R. L. Fagaly, "Superconducting quantum interference device instruments and applications," Rev. Sci. Instrum. **77**(10), 101101 (2006).
[91]J. Clarke and A. I. Braginski, *The SQUID Handbook: Fundamentals and Technology of SQUIDs and SQUID Systems* (Wiley-VCH, Germany, 2004).
[92]R. A. Webb, S. Washburn, C. P. Umbach, and R. B. Laibowitz, "Observation of h/e Aharonov-Bohm oscillations in normal-metal rings," Phys. Rev. Lett. **54**(25), 2696–2699 (1985).
[93]H. Hu, J.-L. Zhu, D.-J. Li, and J.-J. Xiong, "Aharonov-Bohm effect of excitons in nanorings," Phys. Rev. B **63**(19), 195307 (2001).
[94]P. Tuyls, B. Škorić, S. Stallinga, A. H. M. Akkermans, and W. Ophey, "Information-theoretic security analysis of physical uncloneable functions," in *Proceedings of Financial Cryptography and Data Security* (2005), pp. 141–155.
[95]R. v. d. Berg, "Entropy analysis of physically unclonable functions," M.S. thesis (Eindhoven University of Technology, 2012).
[96]B. Škorić, "On the entropy of keys derived from laser speckle; statistical properties of Gabor-transformed speckle," J. Opt. A: Pure Appl. Opt. **10**(5), 055304 (2008).
[97]L. Zhang, X. Fong, C. Chang, Z. H. Kong, and K. Roy, "Feasibility study of emerging non-volatile memory based physical unclonable functions," in *Proceedings of IEEE 6th International Memory Workshop* (IMW) (2014), pp. 1–4.
[98]M. S. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," Report No. 800-90B, NIST (National Institute of Standards and Technology), 2018; available at https://csrc.nist.gov/publications/detail/sp/800-90b/final.
[99]H. Qu, "CMOS MEMS fabrication technologies and devices," Micromachines **7**(1), 14 (2016).
[100]A. Chen, "A review of emerging non-volatile memory (NVM) technologies and applications," Solid-State Electron. **125**, 25–38 (2016).
[101]J. R. Samples and R. V. Hill, "Use of the infrared fundus reflection for an identification device," Am. J. Ophthalmol. **98**(5), 636–637 (1984).
[102]M. Trauring, "Automatic comparison of finger-ridge patterns," Nature **197**, 938–940 (1963).
[103]R. B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric," in *Proceedings of Canadian Conference on Electrical and Computer Engineering* (2001), Vol. 2, pp. 1363–1366.