.

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Cryptanalysis of Shi's White-box Encryption Scheme

HYOUNGSHIN YIM[1], YONGJIN YEOM[1,2], AND JU-SUNG KANG .[1,2]

[1]Department of Financial information security, Kookmin University, Seoul 02707, South Korea

[2]Department of Information Security, Cryptology, and Mathematics Kookmin University, Seoul 02707, South Korea

Corresponding author: Yongjin Yeom (e-mail: salt@kookmin.ac.kr).

This work has supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NO. 2021M1A2A2043893)

ABSTRACT Structural analysis is the study of finding component functions for a given function. In this paper, we proceed with structural analysis of structures consisting of the S (nonlinear Substitution) layer and the A (Affine or linear) layer. Our main interest is the $S^{(2)} \circ A \circ S^{(1)}$ structure with different substitution layers and large input/output sizes. The purpose of our structural analysis is to find the functionally equivalent oracle F^* and its component functions for a given encryption oracle $F = S^{(2)} \circ A \circ S^{(1)}$. As a result, we can construct the decryption oracle ${F^*}^{-1}$ explicitly and break the one-wayness of the building blocks used in a White-box implementation. Our attack consists of two steps: S layer recovery using multiset properties and A layer recovery using differential properties. We present the attack algorithm for each step and estimate the time complexity. Finally, we discuss the applicability of $S^{(2)} \circ A \circ S^{(1)}$ structural analysis in a White-box Cryptography environment.

INDEX TERMS Cryptanalysis, Structural analysis, White-box cryptography, White-box Implementation

I. INTRODUCTION

CRYPTOGRAPHIC technology is widely used in information and communication services for data protection and authentication. In encryption technology, encryption keys are essential for data and information and communication services authentication.

- Intro. to WBC
- Shi's model
- Structural analysis
- Our contribution

The security of the cryptosystem can be guaranteed only when the encryption key is safely protected from various attackers. The attacker models that threaten the security of cryptosystems include black-box attacks, gray-box attacks, and white-box attacks. The black-box attack is carried out through input and output values in unknown assumptions inside the cryptosystem. The gray-box attack is a technique that acquires and attacks side-channel information such as a cryptographic module's power and electromagnetic waves. Among them, the white-box attack assumes the most potent attacker. The white-box attack is a model in which an attacker takes control of the cryptosystem and neutralizes the cryptography. For example, there are dump and change of memory or register, monitoring the execution process, and the like. This has attracted attention to protect encryption keys used for copyright protection from exposure in media players and set-top boxes. Currently, the scope of use is expanding due to the safe execution of financial applications in a mobile environment and the prevention of firmware forgery in embedded devices [1]. In 2002, Chow et al [2, 3]. suggested the possibility of white-box cryptography of AES (Advanced Encryption Standard) and DES (Data Encryption Standard) along with the concept of white-box attackers, and various white-box cryptography technologies were proposed after that. The security of white-box cryptography generally aims at all or part of preventing exposure to encryption keys, one-wayness of encryption or decryption, and preventing the reproduction of cryptosystems [4]. It was analyzed that most of the white-box cryptography designed in a table reference method, including white-box cryptography such as Chow, does not satisfy any security goals. In general, one-wayness, the security of the white-box, cannot be maintained based on the analysis results of the SASAS structure consisting of the non-linear function S-box and the affine function proposed by Biruykov et al. [6, 7]. The analysis results of structures other than the SASAS structure are also the same. However, various attempts are still underway, and white-box cryptographic products that adopt undisclosed techniques are also actively spreading [5]. This paper proposes an attack method on the light-weight white-box encryption scheme for securing distributed embedded devices presented by Shi et al. to IEEE Transaction on Computers in 2019 [8]. The LW-WBC (Light-Weight White-Box Cryptography) proposed by Shi et al. has a Feistel structure and protects the input and output value of the XOR (exclusive or) operation by using a table reference method in each round. In addition, it was argued that it was safe against the existing white-box attack method. The LW-WBC, a 60-bit $S^{(1)}AS^{(2)}$ structure with different nonlinear S-box sizes, increases attack complexity and enhances security by not exposing the linear functions used. However, as a result of applying Biruykov's SASAS structural analysis, it was confirmed that the inverse functions of each round could be efficiently obtained [8]. This cannot guarantee one-wayness, which is the security of the white-box cryptography. This paper presents the existing white-box cryptographic model and structural analysis studies. First, we implement LW-WBC based on C language and analyze the security evidence claimed by Shi. After that, we present the structural analysis algorithm of the $S^{(1)}AS^{(2)}$ structure and calculate the attack complexity based on it. Finally, the attack is carried out by applying structural analysis to the LW-WBC using Python language. The results of this study can be used in commercialized white-box cryptographic models with $S^{(1)}AS^{(2)}$ structures.

II. WHITE-BOX CRYPTOGRAPY AND STRUCTURAL ANALYSIS

White-box cryptographic model uses obfuscation techniques by applying encoding to plaintext, ciphertext, and intermediate values. Various white-box cryptographic model design studies are underway, starting with the symmetric key cryptography AES white-box cryptographic model proposed in 2002 [2]. This white-box cryptographic model is very closely related to cryptographic logic, structural analysis. Structural analysis is a study that started with a different motive than white-box cryptography. This section examines the research trend of the white-box cryptographic model. In addition, we look at the structural analysis research trend closely related to the security of white-box cryptography.

A. RESEARCH TRENDS IN WHITE-BOX CRYPTOGRAPHY

Chow et al. proposed AES' white-box cryptographic model in 2002 and presented a design idea that binds fixed encryption keys into tables, including XOR (exclusive-or) operations. Chow's design ideas are the basis for designing the white-box cryptographic model to date. However, it is not safe with a BGE attack [9], and encryption keys can be extracted by analyzing the table reference method regardless of whether encoding and obfuscation are applied. This is enough to obtain an encryption key from a given table in a few seconds in a PC environment. After that, there have been various studies to supplement Chow's white-box design, but most attack methods have been proposed within a few years. Xiao, Lai [10] presented 16-bit, 32-bit linear function encoding to improve the weakness of 4-bit unit nonlinear encoding in the table reference method. Still, a linear equivalence transformation attack method was discovered by Mulder et al. [11]. In addition, in 2020, vulnerabilities were found in the method of obfuscating the round boundary and adding dummy rounds proposed by Xu et al. [12]. As shown in TABLE I, research on white-box cryptography, which has been steadily improved in table reference methods, has continued until recently [13].

TABLE 1. Designs and Attacks in Whitebox cryptography

Whitebox Cryptography	Design	Attack
Whitebox AES	Chow (2002)	Billet (2004)
Whitebox DES	Chow (2002)	(2007)
Perturbated White-box AES	(2006)	(2010)
White-box AES with large linear encoding	(2009)	(2013)

To overcome the limitations of white-box cryptography for standard cryptography, research is also underway to propose white-box cryptography and a suitable cryptographic algorithm. This started in earnest with introducing the space-hard concept by Bogdanov et al. [14] in 2015. WEM (standing for white-box Even-Mansuor) of Chow et al. [26] proposed a new security concept and operation mode of white-box cryptography. Kwon et al. [27] announced FPL (Feistel cipher using Parallel table Look-ups) block ciphers that combine provable security using parallel table reference methods. Along with developing algorithms suitable for this white-box, the security concept was also discussed from various perspectives. Wyseur [4], Saxena [28] in 2009, and Delerablee et al. [29] in 2013 summarized the security concept that white-box cryptography should satisfy, but most of them are difficult to achieve. In 2020, Bock et al. [30, 31] proposed a security concept considering a practical environment and summarized the security of white-box cryptography based on HW-binding and SW-binding. There are various viewpoints on the security concept and goal of white-box cryptography, and commercial products mainly use private white-box cryptography technology that combines solid obfuscation [5, 32, 33]. The white-box cryptography design is also utilized in SM4, a Chinese standard block cipher algorithm. Various designs and analyses of white-box cryptography are in progress in China. Xioa, Lai [18] and Shang [24] and Yao, Chen [25] designed a white-box cryptography model based on SM4 in 2009, 2016, and 2020, but based on a collision attack, the results were announced that it is difficult to maintain security through the analysis method [19]. As a similar research case, an SM4-based light-weight white-box cryptography model suitable for WSNs (Wireless Sensor Networks) environment was proposed by Shi, Yang et al. in 2015. In 2019, a light-weight white-box cryptographic model suitable for distributed resource systems and combining nonlinear and affine functions was proposed [22, 8]. However, a vulnerability in the white-box cryptographic model was

TABLE 2. Structural analysis of Substitution-Affine Iterations

Year	Topic	Authors
2001	Structural cryptanalysis of SASAS	A Biryukov et al.
2003	Affine Equivalance Algorithm	A Biryukov et al.
2015	Structural cryptanalysis of ASASA	I Dinur et al.
2015	Analytic Tools for White-box Cryptography	C.H. Baek et al.
2018	An improved Affine Equivalence Algorithm	I Dinur

discovered in WSNs through collision-based attacks in 2021 [23]. The white-box cryptographic model proposed in 2019 can confirm its applicability to structural analysis attack [7].

B. RESEARCH TRENDS IN STRUCTURAL ANALYSIS

White-box cryptography is closely related to cryptographic logic, structural analysis. In 1997, Paratin et al. [34] attempted to create the function of public-key cryptography by combining S-box, which is the secret key cryptography logic, and higher-order polynomials. However, although it did not yield successful results, it led to a systematic structural analysis study in the future. As shown in TABLE II, security analysis is conducted on functions of various structures in which nonlinear and affine layers (or linear) with multiple S-boxes alternately appear.

Structural analysis is a study of a method of determining each component under conditions in which the structure of a function is known, but the specific function of each component is unknown. In other words, it is a technique of creating an equivalent function having the same function using only the input/output value of a given oracle function. In 2001, Biryukov et al. [6] considered a function of the SASAS structure as an oracle and discovered a way to find an oracle of the same structure with equal functionality. Using this method, you can discover the encryption key hidden inside the SASAS structure. Most of the white-box cryptography using the table reference method can be attacked by this analysis method. The BGE attack [9] can also be interpreted as this analysis method. Baek et al. proposed a toolbox that generalized structural analysis and presented systematic and quantitative attacks on various structures. This structural analysis has expanded its research to various structures such as ASASA and SASASASAS. Typical attacks on white-box cryptography include obtaining encryption keys and attacking one-wayness properties by constructing a decryption algorithm for a given encryption system. White-box cryptography, which combines non-linear and affine functions into tables, is difficult to maintain security through structural analysis. However, various studies are still in progress to design a white-box encryption model based on one-wayness.

III. SHI'S WHITE-BOX ENCRYPTION SCHEME: LW-WBES

In 2019, Shi et al. proposed a white-box encryption scheme for light-weight embedded devices including mobile phones and navigating systems. We denote their scheme by LW-WBES, which means a Light-Weight White-Box Encryption Scheme. LW-WBES has the following features:

- The block size (input/output size) is 120 bits.
- The number of rounds depends on the security level such as 16(default), 10(aggressive), or 32(conservative).
- The encryption process is designed as a variant of Feistel network.
- Two types of keys (black-box key and white-box key) are used for providing black-box security and white-box security simutaneously. Hence, the key size of LW-WBES is extremely large.

A. DESIGN RATIONALE

In order to overcome the difficulties of white-box implementations of standard ciphers, Shi et al. propose a new white-box friendly cipher secure against white-box attack context. Their design stretergies can be summarized as follows:

- The scheme has the secret components based on the Feistel network, which protect the secret white-box keys from white-box attacks including DCA and DFA.
- Since components of three different size (4, 5, 6-bit) are integrated, it is hard to mount the structural analysis directly.
- The secret components can be reused in each round for saving memory usage in light-weight devices.
- The scheme does not require additionaly external encodings nor obfuscation techniques.

We will show that the goal of design rationale cannot be satisfied and weak against structural cryptanalysis in particular.

B. SPECIFICATION

LW-WBES is a 120-bit block cipher and the number of round can be chosen based on the level of security and the constraints of resources. Here, we describe the encryption process of 16-round default version. 120-bit plaintext $PT = (L, R)$ is input for the Feistel network divided into 5-bit variables as:

$$PT = (L, R) = (L_0, L_1, \ldots, L_{11}, R_0, R_1, \ldots, R_{11}),$$

where $L_i, R_i \in GF(2)^5$ for $i = 0, 1, \ldots, 11$. In each round, the round function $F : GF(2)^{60} \times GF(2)^{72} \to GF(2)^{72}$ consumes 72-bit black-box round key rk by

$$F : (x, k) \mapsto (\Theta_0(x) \oplus rk_0, \ldots, \Theta_{11}(x) \oplus rk_{11}),$$

where Θ_i are nonlinear surjective functions whose outputs are 8-bits and rk is divided into 6-bit components rk_i for $i = 0, 1, \ldots, 11$. In fact, we do not need the details of Θ_i to construct our attack algorithm. Instead of usual mixing by exclusive-or in Feistel network, LW-WBES uses non-linear mixing function called T-box which contains white-box key component. The round transformation $(X_L, X_R) \mapsto (Y_L, Y_R)$ can be written as

$$\begin{cases} Y_L = X_R, \\ Y_R = T(X_L, F(X_R, rk)), \end{cases}$$

where T-box $T : GF(2)^{60} \times GF(2)^{72} \to GF(2)^{60}$ consists of 4 sub-components G, F', H^*, and M is defined as

$$T(x, y) = H^*(M(G(x) \oplus F'(y)))$$

- $G : GF(2)^{60} \to GF(2)^{60}$ is composed of 12 bjiections $G_0, G_1, \ldots, G_{11}$ in parallel so that

$$(x_0, x_1, \ldots, x_{11}) \overset{G}{\mapsto} (G_0(x_0), G_1(x_1), \ldots, G_{11}(x_{11})).$$

- $F' : GF(2)^{72} \to GF(2)^{60}$ takes output of round function F and squizes them into 60-bits.

$$(y_0, y_1, \ldots, y_{11}) \overset{F'}{\mapsto} (F'_0(y_0), F'_1(y_1), \ldots, F'_{11}(y_{11})).$$

- $M : GF(2)^{60} \to GF(2)^{60}$ is an invertible linear transformation represented by a binary matrix M whose 5-bit columns are $M_0, M_1, \ldots, M_{11}$.

$$M = (M_0 M_1 \cdots M_{11}),$$

  where M_j are 60×5 submatrices for $j = 0, 1, \ldots, 11$.
- $H^* : GF(2)^{60} \to GF(2)^{60}$ is composed of fifteen 4-bit bijections.

The component functions F', G, M, and H^* are white-box keys that cannot be exposed during the white-box implementation of encryption process.

In the white-box encryption algorithm, evaluations of T-box T are possible without knowing its component functions (white-box keys), since T is implemented as several steps of table look-ups. In fact, T-box T without final transformation H^*, say $\tilde{T}(x, y) := M(G(x) \oplus F'(y))$, can be represented by the tables of 12-bit input and 60-bit output as follows:

$$\tilde{T} : GF(2)^{60} \times GF(2)^{72} \to GF(2)^{60},$$

where its first input is $x = (x_0, x_1, \ldots, x_{11})$ and the second is $y = (y_0, y_1, \ldots, y_{11})$. Then we can rewrite $\tilde{T}$ as

$$\tilde{T} : GF(2)^{11} \to GF(2)^{60},$$
$$((x_0, y_0), (x_1, y_1), \ldots, (x_{11}, y_{11})) \overset{\tilde{T}}{\mapsto} (z_0, z_1, \ldots, z_{14}).$$

Define $\tilde{T}_j(x_j, y_j) = M_j(G(x_j) \oplus F'(y_j))$ for $0 \le j \le 11$. Then

$$\begin{aligned}\tilde{T}(x, y) &:= M(G(x) \oplus F'(y)) \\ &= M_0(G_0(x_0) \oplus F'_0(y_0)) \oplus \cdots \\ &\qquad \cdots \oplus M_{11}(G_{11}(x_{11}) \oplus F'_{11}(y_{11})) \\ &= \tilde{T}_0(x_0, y_0) \oplus \cdots \oplus \tilde{T}_{11}(x_{11}, y_{11}).\end{aligned}$$

Note that each $\tilde{T}_j(x_j, y_j)$ can be implemented as a pre-computed table with 2^{11} entries which takes 15,360 bytes. On the other hand, 60-bit output of $\tilde{T}$ can be divided into fifteen 4-bit subblocks $(z_0, z_1, \ldots, z_{14})$. In order to apply a 4-bit nonlinear bijection on each z_k in the output of table $\tilde{T}_j(x_j, y_j)$ lookup, we have to use masked adders depicted in Chow's WB-AES.

C. SECURITY CLAIM

- Design rationale
- specification of WB encrytion scheme
- Security claim

IV. STRUCTURAL ANALYSIS OF $S^{(1)}AS^{(2)}$

- Intro. to structural analysis
- brief history
- Our result

V. CRYPTANALYSIS OF SHI'S ALGORITHM

- round inversion
- Attack algorithm of plaintext recovery attack
- Experimental results
- Possible countermeasures

If your paper is intended for a conference, please contact your conference editor concerning acceptable word processor formats for your particular conference.

IEEE will do the final formatting of your paper. If your paper is intended for a conference, please observe the conference page limits.

A. ABBREVIATIONS AND ACRONYMS

Define abbreviations and acronyms the first time they are used in the text, even after they have already been defined in the abstract. Abbreviations such as IEEE, SI, ac, and dc do not have to be defined. Abbreviations that incorporate periods should not have spaces: write "C.N.R.S.," not "C. N. R. S." Do not use abbreviations in the title unless they are unavoidable (for example, "IEEE" in the title of this article).

B. OTHER RECOMMENDATIONS

Use one space after periods and colons. Hyphenate complex modifiers: "zero-field-cooled magnetization." Avoid dangling participles, such as, "Using (1), the potential was calculated." [It is not clear who or what used (1).] Write instead, "The potential was calculated by using (1)," or "Using (1), we calculated the potential."

Use a zero before decimal points: "0.25," not ".25." Use "cm^3," not "cc." Indicate sample dimensions as "0.1 cm $\times$ 0.2 cm," not "0.1 $\times$ 0.2 cm^2." The abbreviation for "seconds" is "s," not "sec." Use "Wb/m^2" or "webers per square meter," not "webers/m^2." When expressing a range of values, write "7 to 9" or "7–9," not "7$\sim$9."

A parenthetical statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.) In American English, periods and commas are within quotation marks, like "this period." Other punctuation is "outside"! Avoid contractions; for example, write "do not" instead of "don't." The serial comma is preferred: "A, B, and C" instead of "A, B and C."

If you wish, you may write in the first person singular or plural and use the active voice ("I observed that ..." or "We observed that ..." instead of "It was observed that ..."). Remember to check spelling. If your native language is not English, please get a native English-speaking colleague to carefully proofread your paper.

Try not to use too many typefaces in the same article. You're writing scholarly papers, not ransom notes. Also please remember that MathJax can't handle really weird typefaces.

C. EQUATIONS

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Use parentheses to avoid ambiguities in denominators. Punctuate equations when they are part of a sentence, as in

$$E = mc^2. \tag{1}$$

Be sure that the symbols in your equation have been defined before the equation appears or immediately following. Italicize symbols (T might refer to temperature, but T is the unit tesla). Refer to "(1)," not "Eq. (1)" or "equation (1)," except at the beginning of a sentence: "Equation (1) is . . . ."

D. LATEX-SPECIFIC ADVICE

Please use "soft" (e.g., `\eqref{Eq}`) cross references instead of "hard" references (e.g., `(1)`). That will make it possible to combine sections, add equations, or change the order of figures or citations without having to go through the file line by line.

Please don't use the `{eqnarray}` equation environment. Use `{align}` or `{IEEEeqnarray}` instead. The `{eqnarray}` environment leaves unsightly spaces around relation symbols.

Please note that the `{subequations}` environment in LaTeX will increment the main equation counter even when there are no equation numbers displayed. If you forget that, you might write an article in which the equation numbers skip from (17) to (20), causing the copy editors to wonder if you've discovered a new method of counting.

BibTeX does not work by magic. It doesn't get the bibliographic data from thin air but from .bib files. If you use BibTeX to produce a bibliography you must send the .bib files.

LaTeX can't read your mind. If you assign the same label to a subsubsection and a table, you might find that Table I has been cross referenced as Table IV-B3.

LaTeX does not have precognitive abilities. If you put a `\label` command before the command that updates the counter it's supposed to be using, the label will pick up the last counter to be cross referenced instead. In particular, a `\label` command should not go before the caption of a figure or a table.

Do not use `\nonumber` inside the `{array}` environment. It will not stop equation numbers inside `{array}` (there won't be any anyway) and it might stop a wanted equation number in the surrounding equation.

VI. UNITS

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage. For example, write "15 Gb/cm^2 (100 Gb/in^2)." An exception is when English units are used as identifiers in trade, such as "3½-in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength H is A/m. However, if you wish to use units of T, either refer to magnetic flux density B or magnetic field strength symbolized as $\mu_0 H$. Use the center dot to separate compound units, e.g., "A·m^2."

VII. SOME COMMON MISTAKES

The word "data" is plural, not singular. The subscript for the permeability of vacuum μ_0 is zero, not a lowercase letter "o." The term for residual magnetization is "remanence"; the adjective is "remanent"; do not write "remnance" or "remnant." Use the word "micrometer" instead of "micron." A graph within a graph is an "inset," not an "insert." The word "alternatively" is preferred to the word "alternately" (unless you really mean something that alternates). Use the word "whereas" instead of "while" (unless you are referring to simultaneous events). Do not use the word "essentially" to mean "approximately" or "effectively." Do not use the word "issue" as a euphemism for "problem." When compositions are not specified, separate chemical symbols by en-dashes; for example, "NiMn" indicates the intermetallic compound $Ni_{0.5}Mn_{0.5}$ whereas "Ni–Mn" indicates an alloy of some composition Ni_xMn_{1-x}.

Be aware of the different meanings of the homophones "affect" (usually a verb) and "effect" (usually a noun), "complement" and "compliment," "discreet" and "discrete," "principal" (e.g., "principal investigator") and "principle" (e.g., "principle of measurement"). Do not confuse "imply" and "infer."

Prefixes such as "non," "sub," "micro," "multi," and "ultra" are not independent words; they should be joined to the words they modify, usually without a hyphen. There is no period after the "et" in the Latin abbreviation "*et al.*" (it is also italicized). The abbreviation "i.e.," means "that is," and the abbreviation "e.g.," means "for example" (these abbreviations are not italicized).

A general IEEE styleguide is available at http://www.ieee.org/authortools.

VIII. GUIDELINES FOR GRAPHICS PREPARATION AND SUBMISSION

A. TYPES OF GRAPHICS

The following list outlines the different types of graphics published in IEEE journals. They are categorized based on their construction, and use of color/shades of gray:

1) Color/Grayscale figures

Figures that are meant to appear in color, or shades of black/gray. Such figures may include photographs, illustrations, multicolor graphs, and flowcharts.

TABLE 3. Units for Magnetic Properties

Symbol	Quantity	Conversion from Gaussian and CGS EMU to SI [a]
Φ	magnetic flux	1 Mx $\rightarrow 10^{-8}$ Wb $= 10^{-8}$ V·s
B	magnetic flux density, magnetic induction	1 G $\rightarrow 10^{-4}$ T $= 10^{-4}$ Wb/m^2
H	magnetic field strength	1 Oe $\rightarrow 10^3/(4\pi)$ A/m
m	magnetic moment	1 erg/G = 1 emu $\rightarrow 10^{-3}$ A·m^2 $= 10^{-3}$ J/T
M	magnetization	1 erg/(G·cm^3) = 1 emu/cm^3 $\rightarrow 10^3$ A/m
$4\pi M$	magnetization	1 G $\rightarrow 10^3/(4\pi)$ A/m
σ	specific magnetization	1 erg/(G·g) = 1 emu/g $\rightarrow$ 1 A·m^2/kg
j	magnetic dipole moment	1 erg/G = 1 emu $\rightarrow 4\pi \times 10^{-10}$ Wb·m
J	magnetic polarization	1 erg/(G·cm^3) = 1 emu/cm^3 $\rightarrow 4\pi \times 10^{-4}$ T
χ, κ	susceptibility	$1 \rightarrow 4\pi$
χ_ρ	mass susceptibility	1 cm^3/g $\rightarrow 4\pi \times 10^{-3}$ m^3/kg
μ	permeability	$1 \rightarrow 4\pi \times 10^{-7}$ H/m $= 4\pi \times 10^{-7}$ Wb/(A·m)
μ_r	relative permeability	$\mu \rightarrow \mu_r$
w, W	energy density	1 erg/cm^3 $\rightarrow 10^{-1}$ J/m^3
N, D	demagnetizing factor	$1 \rightarrow 1/(4\pi)$

Vertical lines are optional in tables. Statements that serve as captions for the entire table do not need footnote letters.

[a]Gaussian units are the same as cg emu for magnetostatics; Mx = maxwell, G = gauss, Oe = oersted; Wb = weber, V = volt, s = second, T = tesla, m = meter, A = ampere, J = joule, kg = kilogram, H = henry.

2) Line Art figures

Figures that are composed of only black lines and shapes. These figures should have no shades or half-tones of gray, only black and white.

3) Author photos

Head and shoulders shots of authors that appear at the end of our papers.

4) Tables

Data charts which are typically black and white, but sometimes include color.

B. MULTIPART FIGURES

Figures compiled of more than one sub-figure presented side-by-side, or stacked. If a multipart figure is made up of multiple figure types (one part is lineart, and another is grayscale or color) the figure should meet the stricter guidelines.

C. FILE FORMATS FOR GRAPHICS

Format and save your graphics using a suitable graphics processing program that will allow you to create the images as PostScript (PS), Encapsulated PostScript (.EPS), Tagged Image File Format (.TIFF), Portable Document Format (.PDF), Portable Network Graphics (.PNG), or Metapost (.MPS), sizes them, and adjusts the resolution settings. When submitting your final paper, your graphics should all be submitted individually in one of these formats along with the manuscript.

D. SIZING OF GRAPHICS

Most charts, graphs, and tables are one column wide (3.5 inches/88 millimeters/21 picas) or page wide (7.16 inches/181 millimeters/43 picas). The maximum depth a graphic can be is 8.5 inches (216 millimeters/54 picas). When choosing the depth of a graphic, please allow space for a caption. Figures can be sized between column and page widths if the author chooses, however it is recommended that figures are not sized less than column width unless when necessary.

There is currently one publication with column measurements that do not coincide with those listed above. Proceedings of the IEEE has a column measurement of 3.25 inches (82.5 millimeters/19.5 picas).

The final printed size of author photographs is exactly 1 inch wide by 1.25 inches tall (25.4 millimeters × 31.75 millimeters/6 picas × 7.5 picas). Author photos printed in editorials measure 1.59 inches wide by 2 inches tall (40 millimeters × 50 millimeters/9.5 picas × 12 picas).

E. RESOLUTION

The proper resolution of your figures will depend on the type of figure it is as defined in the “Types of Figures” section. Author photographs, color, and grayscale figures should be at least 300dpi. Line art, including tables should be a minimum of 600dpi.

F. VECTOR ART

In order to preserve the figures’ integrity across multiple computer platforms, we accept files in the following formats: .EPS/.PDF/.PS. All fonts must be embedded or text converted to outlines in order to achieve the best-quality results.

G. COLOR SPACE

The term color space refers to the entire sum of colors that can be represented within the said medium. For our purposes, the three main color spaces are Grayscale, RGB (red/green/blue) and CMYK (cyan/magenta/yellow/black). RGB is generally used with on-screen graphics, whereas CMYK is used for printing purposes.

All color figures should be generated in RGB or CMYK color space. Grayscale images should be submitted in Grayscale color space. Line art may be provided in grayscale OR bitmap colorspace. Note that “bitmap colorspace” and “bitmap file format” are not the same thing. When bitmap color space is selected, .TIF/.TIFF/.PNG are the recommended file formats.

H. ACCEPTED FONTS WITHIN FIGURES

When preparing your graphics IEEE suggests that you use of one of the following Open Type fonts: Times New Roman, Helvetica, Arial, Cambria, and Symbol. If you are supplying EPS, PS, or PDF files all fonts must be embedded. Some fonts may only be native to your operating system; without the fonts embedded, parts of the graphic may be distorted or missing.

A safe option when finalizing your figures is to strip out the fonts before you save the files, creating "outline" type. This converts fonts to artwork what will appear uniformly on any screen.

I. USING LABELS WITHIN FIGURES

1) Figure Axis labels

Figure axis labels are often a source of confusion. Use words rather than symbols. As an example, write the quantity "Magnetization," or "Magnetization M," not just "M." Put units in parentheses. Do not label axes only with units. As in Fig. 1, for example, write "Magnetization (A/m)" or "Magnetization ($A{\cdot}m^{-1}$)," not just "A/m." Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)," not "Temperature/K."

Multipliers can be especially confusing. Write "Magnetization (kA/m)" or "Magnetization (10^3 A/m)." Do not write "Magnetization (A/m) $\times$ 1000" because the reader would not know whether the top axis label in Fig. 1 meant 16000 A/m or 0.016 A/m. Figure labels should be legible, approximately 8 to 10 point type.

2) Subfigure Labels in Multipart Figures and Tables

Multipart figures should be combined and labeled before final submission. Labels should appear centered below each subfigure in 8 point Times New Roman font in the format of (a) (b) (c).

J. FILE NAMING

Figures (line artwork or photographs) should be named starting with the first 5 letters of the author's last name. The next characters in the filename should be the number that represents the sequential location of this image in your article. For example, in author "Anderson's" paper, the first three figures would be named ander1.tif, ander2.tif, and ander3.ps.

Tables should contain only the body of the table (not the caption) and should be named similarly to figures, except that '.t' is inserted in-between the author's name and the table number. For example, author Anderson's first three tables would be named ander.t1.tif, ander.t2.ps, ander.t3.eps.

Author photographs should be named using the first five characters of the pictured author's last name. For example, four author photographs for a paper may be named: oppen.ps, moshc.tif, chen.eps, and duran.pdf.

If two authors or more have the same last name, their first initial(s) can be substituted for the fifth, fourth, third... letters of their surname until the degree where there is differentiation. For example, two authors Michael and Monica Oppenheimer's photos would be named oppmi.tif, and oppmo.eps.

K. REFERENCING A FIGURE OR TABLE WITHIN YOUR PAPER

When referencing your figures and tables within your paper, use the abbreviation "Fig." even at the beginning of a sentence. Do not abbreviate "Table." Tables should be numbered with Roman Numerals.

L. CHECKING YOUR FIGURES: THE IEEE GRAPHICS ANALYZER

The IEEE Graphics Analyzer enables authors to prescreen their graphics for compliance with IEEE Access standards before submission. The online tool, located at http://graphicsqc.ieee.org/, allows authors to upload their graphics in order to check that each file is the correct file format, resolution, size and colorspace; that no fonts are missing or corrupt; that figures are not compiled in layers or have transparency, and that they are named according to the IEEE Access naming convention. At the end of this automated process, authors are provided with a detailed report on each graphic within the web applet, as well as by email.

For more information on using the Graphics Analyzer or any other graphics related topic, contact the IEEE Graphics Help Desk by e-mail at graphics@ieee.org.

M. SUBMITTING YOUR GRAPHICS

Because IEEE will do the final formatting of your paper, you do not need to position figures and tables at the top and bottom of each column. In fact, all figures, figure captions, and tables can be placed at the end of your paper. In addition to, or even in lieu of submitting figures within your final manuscript, figures should be submitted individually, separate from the manuscript in one of the file formats listed above in Section VIII-C. Place figure captions below the figures; place table titles above the tables. Please do not include captions as part of the figures, or put them in "text boxes" linked to the figures. Also, do not place borders around the outside of your figures.

N. COLOR PROCESSING/PRINTING IN IEEE JOURNALS

All IEEE Transactions, Journals, and Letters allow an author to publish color figures on IEEE Xplore® at no charge, and automatically convert them to grayscale for print versions. In most journals, figures and tables may alternatively be printed in color if an author chooses to do so. Please note that this service comes at an extra expense to the author. If you intend to have print color graphics, include a note with your final paper indicating which figures or tables you would like to be handled that way, and stating that you are willing to pay the additional fee.

IX. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

.

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in American English is without an "e" after the "g." Use the singular heading even if you have many acknowledgments. Avoid expressions such as "One of us (S.B.A.) would like to thank . . . ." Instead, write "F. A. Author thanks . . . ." In most cases, sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page, not here.

REFERENCES AND FOOTNOTES

A. REFERENCES

References need not be cited in text. When they are, they appear on the line, in square brackets, inside the punctuation. Multiple references are each numbered with separate brackets. When citing a section in a book, please give the relevant page numbers. In text, refer simply to the reference number. Do not use "Ref." or "reference" except at the beginning of a sentence: "Reference [21] shows . . . ." Please do not use automatic endnotes in *Word*, rather, type the reference list at the end of the paper using the "References" style.

Reference numbers are set flush left and form a column of their own, hanging out beyond the body of the reference. The reference numbers are on the line, enclosed in square brackets. In all references, the given name of the author or editor is abbreviated to the initial only and precedes the last name. Use them all; use *et al.* only if names are not given. Use commas around Jr., Sr., and III in names. Abbreviate conference titles. When citing IEEE transactions, provide the issue number, page range, volume number, year, and/or month if available. When referencing a patent, provide the day and the month of issue, or application. References may not include all information; please obtain and include relevant information. Do not combine references. There must be only one reference with each number. If there is a URL included with the print reference, it can be included at the end of the reference.

Other than books, capitalize only the first word in a paper title, except for proper nouns and element symbols. For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation See the end of this document for formats and examples of common references. For a complete discussion of references and their formats, see the IEEE style manual at http://www.ieee.org/authortools.

B. FOOTNOTES

Number footnotes separately in superscript numbers.[1] Place the actual footnote at the bottom of the column in which it is cited; do not put footnotes in the reference list (endnotes). Use letters for table footnotes (see Table 3).

APPENDIX A SUBMITTING YOUR PAPER FOR REVIEW

A. FINAL STAGE

When you submit your final version (after your paper has been accepted), print it in two-column format, including figures and tables. You must also send your final manuscript on a disk, via e-mail, or through a Web manuscript submission system as directed by the society contact. You may use *Zip* for large files, or compress files using *Compress, Pkzip, Stuffit,* or *Gzip.*

Also, send a sheet of paper or PDF with complete contact information for all authors. Include full mailing addresses, telephone numbers, fax numbers, and e-mail addresses. This information will be used to send each author a complimentary copy of the journal in which the paper appears. In addition, designate one author as the "corresponding author." This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only.

B. REVIEW STAGE USING SCHOLARONE® MANUSCRIPTS

Contributions to the Transactions, Journals, and Letters may be submitted electronically on IEEE's online manuscript submission and peer-review system, ScholarOne® Manuscripts. You can get a listing of the publications that participate in ScholarOne at http://www.ieee.org/publications_standards/publications/authors/authors_submission.html. First check if you have an existing account. If there is none, please create a new account. After logging in, go to your Author Center and click "Submit First Draft of a New Manuscript."

Along with other information, you will be asked to select the subject from a pull-down list. Depending on the journal, there are various steps to the submission process; you must complete all steps for a complete submission. At the end of each step you must click "Save and Continue"; just uploading the paper is not sufficient. After the last step, you should see a confirmation that the submission is complete. You should also receive an e-mail confirmation. For inquiries regarding the submission of your paper on ScholarOne Manuscripts, please contact oprs-support@ieee.org or call +1 732 465 5861.

ScholarOne Manuscripts will accept files for review in various formats. Please check the guidelines of the specific journal for which you plan to submit.

You will be asked to file an electronic copyright form immediately upon completing the submission process (authors are responsible for obtaining any security clearances). Failure to submit the electronic copyright could result in publishing delays later. You will also have the opportunity to designate your article as "open access" if you agree to pay the IEEE open access fee.

C. FINAL STAGE USING SCHOLARONE MANUSCRIPTS

Upon acceptance, you will receive an email with specific instructions regarding the submission of your final files. To avoid any delays in publication, please be sure to follow these instructions. Most journals require that final submissions be uploaded through ScholarOne Manuscripts, although some may still accept final submissions via email. Final submissions should include source files of your accepted

[1]It is recommended that footnotes be avoided (except for the unnumbered footnote with the receipt date on the first page). Instead, try to integrate the footnote information into the text.

manuscript, high quality graphic files, and a formatted pdf file. If you have any questions regarding the final submission process, please contact the administrative contact for the journal.

In addition to this, upload a file with complete contact information for all authors. Include full mailing addresses, telephone numbers, fax numbers, and e-mail addresses. Designate the author who submitted the manuscript on ScholarOne Manuscripts as the "corresponding author." This is the only author to whom proofs of the paper will be sent.

D. COPYRIGHT FORM

Authors must submit an electronic IEEE Copyright Form (eCF) upon submitting their final manuscript files. You can access the eCF system through your manuscript submission system or through the Author Gateway. You are responsible for obtaining any necessary approvals and/or security clearances. For additional information on intellectual property rights, visit the IEEE Intellectual Property Rights department web page at http://www.ieee.org/publications_standards/publications/rights/index.html.

APPENDIX B IEEE PUBLISHING POLICY

The general IEEE policy requires that authors should only submit original work that has neither appeared elsewhere for publication, nor is under review for another refereed publication. The submitting author must disclose all prior publication(s) and current submissions when submitting a manuscript. Do not publish "preliminary" data or results. The submitting author is responsible for obtaining agreement of all coauthors and any consent required from employers or sponsors before submitting an article. The IEEE Access Department strongly discourages courtesy authorship; it is the obligation of the authors to cite only relevant prior work.

The IEEE Access Department does not publish conference records or proceedings, but can publish articles related to conferences that have undergone rigorous peer review. Minimally, two reviews are required for every article submitted for peer review.

APPENDIX C PUBLICATION PRINCIPLES

The two types of contents of that are published are; 1) peer-reviewed and 2) archival. The Access Department publishes scholarly articles of archival value as well as tutorial expositions and critical reviews of classical subjects and topics of current interest.

Authors should consider the following points:

1) Technical papers submitted for publication must advance the state of knowledge and must cite relevant prior work.
2) The length of a submitted paper should be commensurate with the importance, or appropriate to the complexity, of the work. For example, an obvious extension of previously published work might not be appropriate for publication or might be adequately treated in just a few pages.
3) Authors must convince both peer reviewers and the editors of the scientific and technical merit of a paper; the standards of proof are higher when extraordinary or unexpected results are reported.
4) Because replication is required for scientific progress, papers submitted for publication must provide sufficient information to allow readers to perform similar experiments or calculations and use the reported results. Although not everything need be disclosed, a paper must contain new, useable, and fully described information. For example, a specimen's chemical composition need not be reported if the main purpose of a paper is to introduce a new measurement technique. Authors should expect to be challenged by reviewers if the results are not supported by adequate data and critical details.
5) Papers that describe ongoing work or announce the latest technical achievement, which are suitable for presentation at a professional conference, may not be appropriate for publication.

APPENDIX D REFERENCE EXAMPLES

- *Basic format for books:*
  J. K. Author, "Title of chapter in the book," in *Title of His Published Book, x*th ed. City of Publisher, (only U.S. State), Country: Abbrev. of Publisher, year, ch. x, sec. x, pp. *xxx–xxx.*
  See [**?**], [20].
- *Basic format for periodicals:*
  J. K. Author, "Name of paper," *Abbrev. Title of Periodical*, vol. *x, no*. x,pp. *xxx–xxx,* Abbrev. Month, year, DOI. 10.1109.*XXX*.123456.
  See [21]– [23].
- *Basic format for reports:*
  J. K. Author, "Title of report," Abbrev. Name of Co., City of Co., Abbrev. State, Country, Rep. *xxx*, year.
  See [24], [25].
- *Basic format for handbooks:*
  Name of Manual/Handbook, x ed., Abbrev. Name of Co., City of Co., Abbrev. State, Country, year, pp. *xxx–xxx.*
  See [26], [27].
- *Basic format for books (when available online):*
  J. K. Author, "Title of chapter in the book," in *Title of Published Book*, xth ed. City of Publisher, State, Country: Abbrev. of Publisher, year, ch. x, sec. x, pp. *xxx–xxx*. [Online]. Available: http://www.web.com
  See [28]– [31].
- *Basic format for journals (when available online):*
  J. K. Author, "Name of paper," *Abbrev. Title of Periodical*, vol. x, no. x, pp. *xxx–xxx*, Abbrev. Month, year. Accessed on: Month, Day, year, DOI: 10.1109.*XXX*.123456, [Online].
  See [32]– [34].

- *Basic format for papers presented at conferences (when available online):*
  J.K. Author. (year, month). Title. presented at abbrev. conference title. [Type of Medium]. Available: site/path/file
  See [35].
- *Basic format for reports and handbooks (when available online):*
  J. K. Author. "Title of report," Company. City, State, Country. Rep. no., (optional: vol./issue), Date. [Online] Available: site/path/file
  See [36], [37].
- *Basic format for computer programs and electronic documents (when available online):*
  Legislative body. Number of Congress, Session. (year, month day). *Number of bill or resolution*, *Title*. [Type of medium]. Available: site/path/file
  NOTE: ISO recommends that capitalization follow the accepted practice for the language or script in which the information is given.
  See [38].
- *Basic format for patents (when available online):*
  Name of the invention, by inventor's name. (year, month day). Patent Number [Type of medium]. Available: site/path/file
  See [39].
- *Basic formatfor conference proceedings (published):*
  J. K. Author, "Title of paper," in *Abbreviated Name of Conf.*, City of Conf., Abbrev. State (if given), Country, year, pp. *xxxxxx.*
  See [40].
- *Example for papers presented at conferences (unpublished):*
  See [41].
- *Basic format for patents*:
  J. K. Author, "Title of patent," U.S. Patent *x xxx xxx*, Abbrev. Month, day, year.
  See [42].
- *Basic format for theses (M.S.) and dissertations (Ph.D.):*
  1) J. K. Author, "Title of thesis," M.S. thesis, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.
  2) J. K. Author, "Title of dissertation," Ph.D. dissertation, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.

  See [43], [44].
- *Basic format for the most common types of unpublished references:*
  1) J. K. Author, private communication, Abbrev. Month, year.
  2) J. K. Author, "Title of paper," unpublished.
  3) J. K. Author, "Title of paper," to be published.

  See [45]– [47].
- *Basic formats for standards:*
  1) *Title of Standard*, Standard number, date.
  2) *Title of Standard*, Standard number, Corporate author, location, date.

  See [48], [49].
- *Article number in reference examples:*
  See [50], [51].
- *Example when using et al.:*
  See [52].

REFERENCES

[1] S. Chow, P. A. Eisen, H. Johnson, and P. C. van Oorschot, "White-box cryptography and an AES implementation", *SAC 2002*, LNCS volume 2595, 2003.

[2] S. Chow, P. A. Eisen, H. Johnson, and P. C. van Oorschot, "A white-box DES implementation for DRM applications", *Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop, DRM 2002*, LNCS volume 2696, 2003.

[3] B. Wyseur, "White-Box Cryptography", PhD thesis, Katholieke University Leuven, 2009.

[4] A. Biryukov, A. Shamir, "Structural cryptanalysis of SASAS", *Eurocrypt 2001, J. of Cryptology*, 23(4), 2010.

[5] H. Yim, J.-S. Kang, Y. Yeom, "An Efficient Structural Analysis of SAS and its Application to White-Box Cryptography", *IEEE TENSYMP*, 2021.

[6] Y. Shi, W. Wei, H. Fan, M. H. Au and X. Luo, "A Light-Weight White-Box Encryption Scheme for Securing Distributed Embedded Devices", *IEEE Transactions on Computers*, vol. 68, no. 10, 2019.

[7] O. Billet, H. Gilbert, C. Ech-Chatbi, "Cryptanalysis of a white box AES implementation", *SAC 2004*, LNCS volume 3357, 2004.

[8] Y. Xiao, X. Lai, "A secure implementation of white-box AES", *2nd International Conference on Computer Science and its Applications, IEEE CSA*, 2009.

[9] Y. De Mulder, P. Roelse, B. Preneel, "Cryptanalysis of the Xiao–Lai white-box AES implementation", *SAC 2013*, LNCS volume 7707, 2013.

[10] T. Xu, C. K. Wu, F. Liu, R. Zhao, "Protecting white-box cryptographic implementations with obfuscated round boundaries", *Sci. China Inform. Sci.*, 61(3), 2018.

[11] Y. Yeom, DC. Kim, C. H. Baek, J. Shin, "Cryptanalysis of the Obfuscated Round Boundary Technique for Whitebox Cryptography", *Sci. China Inform. Sci.*, 63, 2020.

[12] A. Bogdanov and T. Isobe, "White-box cryptography revisited: Space-hard ciphers", *ACM SIGSAG Conference on Computer and Communications Security*, ACM, 2015.

[13] J. Cho, Y. Choi, I. Dinur, O. Dunkelman, N. Keller, D. Moon, A. Veidberg, "WEM: A New Family of White-Box Black Ciphers Based on the Even-Mansour Construction", *CT-RSA 2017*, LNCS volume 10159, 2017.

[14] C. H. Baek, J. H. Cheon, H. Hong, "White-box AES implementation revisited", *Journal of Communications and Networks*, 2016.

[15] A. Biryukov, C. De Canniere, A. Braeken, B. Preneel, "A toolbox for cryptanalysis: Linear and affine equivalence algorithms", *EUROCRYPT 2003*. LNCS volume 2656, 2003.

[16] A. Biryukov, C. Bouillaguet, D. Khovratovich, "Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key", *ASIACRYPT 2014*, LNCS volume 8873, 2014.

[17] I. Dinur, "An Improved Affine Equivalence Algorithm for Random Permutations", *EUROCRYPT 2018*. LNCS volume 10820, 2018.

[18] I. Dinur, O Dunkelman, T Karnz, G Leander, "Decomposing the ASASA Block Cipher Construction", IACR Cryptol, 2015.

[19] A. Biryukov, D. Khovratovich, "Decomposition attack on SASASASAS," *Cryptology ePrint Archive*, Report 2015/646, 2015.

[20] W.-K. Chen, *Linear Networks and Systems.* Belmont, CA, USA: Wadsworth, 1993, pp. 123–135.

[21] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, no. 1, pp. 34–39, Jan. 1959, 10.1109/TED.2016.2628402.

[22] E. P. Wigner, "Theory of traveling-wave optical laser," *Phys. Rev.*, vol. 134, pp. A635–A646, Dec. 1965.

[23] E. H. Miller, "A note on reflector arrays," *IEEE Trans. Antennas Propagat.*, to be published.

[24] E. E. Reber, R. L. Michell, and C. J. Carter, "Oxygen absorption in the earth's atmosphere," Aerospace Corp., Los Angeles, CA, USA, Tech. Rep. TR-0200 (4230-46)-3, Nov. 1988.

[25] J. H. Davis and J. R. Cogdell, "Calibration program for the 16-foot antenna," Elect. Eng. Res. Lab., Univ. Texas, Austin, TX, USA, Tech. Memo. NGL-006-69-3, Nov. 15, 1987.
[26] *Transmission Systems for Communications*, 3rd ed., Western Electric Co., Winston-Salem, NC, USA, 1985, pp. 44–60.
[27] *Motorola Semiconductor Data Manual*, Motorola Semiconductor Products Inc., Phoenix, AZ, USA, 1989.
[28] G. O. Young, "Synthetic structure of industrial plastics," in Plastics, vol. 3, Polymers of Hexadromicon, J. Peters, Ed., 2nd ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15-64. [Online]. Available: http://www.bookref.com.
[29] *The Founders' Constitution*, Philip B. Kurland and Ralph Lerner, eds., Chicago, IL, USA: Univ. Chicago Press, 1987. [Online]. Available: http://press-pubs.uchicago.edu/founders/
[30] The Terahertz Wave eBook. ZOmega Terahertz Corp., 2014. [Online]. Available: http://dl.z-thz.com/eBook/zomega_ebook_pdf_1206_sr.pdf. Accessed on: May 19, 2014.
[31] Philip B. Kurland and Ralph Lerner, eds., *The Founders' Constitution.* Chicago, IL, USA: Univ. of Chicago Press, 1987, Accessed on: Feb. 28, 2010, [Online] Available: http://press-pubs.uchicago.edu/founders/
[32] J. S. Turner, "New directions in communications," *IEEE J. Sel. Areas Commun*., vol. 13, no. 1, pp. 11-23, Jan. 1995.
[33] W. P. Risk, G. S. Kino, and H. J. Shaw, "Fiber-optic frequency shifter using a surface acoustic wave incident at an oblique angle," *Opt. Lett.*, vol. 11, no. 2, pp. 115–117, Feb. 1986.
[34] P. Kopyt *et al., "*Electric properties of graphene-based conductive layers from DC up to terahertz range," *IEEE THz Sci. Technol.,* to be published. DOI: 10.1109/TTHZ.2016.2544142.
[35] PROCESS Corporation, Boston, MA, USA. Intranets: Internet technologies deployed behind the firewall for corporate productivity. Presented at INET96 Annual Meeting. [Online]. Available: http://home.process.com/Intranets/wp2.htp
[36] R. J. Hijmans and J. van Etten, "Raster: Geographic analysis and modeling with raster data," R Package Version 2.0-12, Jan. 12, 2012. [Online]. Available: http://CRAN.R-project.org/package=raster
[37] Teralyzer. Lytera UG, Kirchhain, Germany [Online]. Available: http://www.lytera.de/Terahertz_THz_Spectroscopy.php?id=home, Accessed on: Jun. 5, 2014
[38] U.S. House. 102nd Congress, 1st Session. (1991, Jan. 11). *H. Con. Res. 1, Sense of the Congress on Approval of Military Action*. [Online]. Available: LEXIS Library: GENFED File: BILLS
[39] Musical toothbrush with mirror, by L.M.R. Brooks. (1992, May 19). Patent D 326 189 [Online]. Available: NEXIS Library: LEXPAT File: DES
[40] D. B. Payne and J. R. Stern, "Wavelength-switched pas- sively coupled single-mode optical network," in *Proc. IOOC-ECOC,* Boston, MA, USA, 1985, pp. 585–590.
[41] D. Ebehard and E. Voges, "Digital single sideband detection for interferometric sensors," presented at the *2nd Int. Conf. Optical Fiber Sensors,* Stuttgart, Germany, Jan. 2-5, 1984.
[42] G. Brandli and M. Dick, "Alternating current fed power supply," U.S. Patent 4 084 217, Nov. 4, 1978.
[43] J. O. Williams, "Narrow-band analyzer," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, USA, 1993.
[44] N. Kawasaki, "Parametric study of thermal and chemical nonequilibrium nozzle flow," M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.
[45] A. Harrison, private communication, May 1995.
[46] B. Smith, "An approach to graphs of linear forms," unpublished.
[47] A. Brahms, "Representation error for real numbers in binary computer arithmetic," IEEE Computer Group Repository, Paper R-67-85.
[48] IEEE Criteria for Class IE Electric Systems, IEEE Standard 308, 1969.
[49] Letter Symbols for Quantities, ANSI Standard Y10.5-1968.
[50] R. Fardel, M. Nagel, F. Nuesch, T. Lippert, and A. Wokaun, "Fabrication of organic light emitting diode pixels by laser-assisted forward transfer," *Appl. Phys. Lett.*, vol. 91, no. 6, Aug. 2007, Art. no. 061103.
[51] J. Zhang and N. Tansu, "Optical gain and laser characteristics of InGaN quantum wells on ternary InGaN substrates," *IEEE Photon. J.*, vol. 5, no. 2, Apr. 2013, Art. no. 2600111
[52] S. Azodolmolky *et al.*, Experimental demonstration of an impairment aware network planning and operation tool for transparent/translucent optical networks," *J. Lightw. Technol.*, vol. 29, no. 4, pp. 439–448, Sep. 2011.

FIRST A. AUTHOR (M'76–SM'81–F'87) and all authors may include biographies. Biographies are often not included in conference-related papers. This author became a Member (M) of IEEE in 1976, a Senior Member (SM) in 1981, and a Fellow (F) in 1987. The first paragraph may contain a place and/or date of birth (list place, then date). Next, the author's educational background is listed. The degrees should be listed with type of degree in what field, which institution, city, state, and country, and year the degree was earned. The author's major field of study should be lower-cased.

The second paragraph uses the pronoun of the person (he or she) and not the author's last name. It lists military and work experience, including summer and fellowship jobs. Job titles are capitalized. The current job must have a location; previous positions may be listed without one. Information concerning previous publications may be included. Try not to list more than three books or published articles. The format for listing publishers of a book within the biography is: title of book (publisher name, year) similar to a reference. Current and previous research interests end the paragraph. The third paragraph begins with the author's title and last name (e.g., Dr. Smith, Prof. Jones, Mr. Kajor, Ms. Hunter). List any memberships in professional societies other than the IEEE. Finally, list any awards and work for IEEE committees and publications. If a photograph is provided, it should be of good quality, and professional-looking. Following are two examples of an author's biography.

SECOND B. AUTHOR was born in Greenwich Village, New York, NY, USA in 1977. He received the B.S. and M.S. degrees in aerospace engineering from the University of Virginia, Charlottesville, in 2001 and the Ph.D. degree in mechanical engineering from Drexel University, Philadelphia, PA, in 2008.

From 2001 to 2004, he was a Research Assistant with the Princeton Plasma Physics Laboratory. Since 2009, he has been an Assistant Professor with the Mechanical Engineering Department, Texas A&M University, College Station. He is the author of three books, more than 150 articles, and more than 70 inventions. His research interests include high-pressure and high-density nonthermal plasma discharge processes and applications, microscale plasma discharges, discharges in liquids, spectroscopic diagnostics, plasma propulsion, and innovation plasma applications. He is an Associate Editor of the journal *Earth, Moon, Planets*, and holds two patents.

Dr. Author was a recipient of the International Association of Geomagnetism and Aeronomy Young Scientist Award for Excellence in 2008, and the IEEE Electromagnetic Compatibility Society Best Symposium Paper Award in 2011.

THIRD C. AUTHOR, JR. (M'87) received the B.S. degree in mechanical engineering from National Chung Cheng University, Chiayi, Taiwan, in 2004 and the M.S. degree in mechanical engineering from National Tsing Hua University, Hsinchu, Taiwan, in 2006. He is currently pursuing the Ph.D. degree in mechanical engineering at Texas A&M University, College Station, TX, USA.

From 2008 to 2009, he was a Research Assistant with the Institute of Physics, Academia Sinica, Tapei, Taiwan. His research interest includes the development of surface processing and biological/medical treatment techniques using nonthermal atmospheric pressure plasmas, fundamental study of plasma sources, and fabrication of micro- or nanostructured surfaces.

Mr. Author's awards and honors include the Frew Fellowship (Australian Academy of Science), the I. I. Rabi Prize (APS), the European Frequency and Time Forum Award, the Carl Zeiss Research Award, the William F. Meggers Award and the Adolph Lomb Medal (OSA).